

Sygn. akt: KIO 1942/12

**WYROK**  
**z dnia 27 września 2012 r.**

**Krajowa Izba Odwoławcza** - w składzie:

**Przewodniczący: Andrzej Niwicki**  
**Protokolant: Paulina Nowicka**

po rozpoznaniu na rozprawie w dniu 26 września 2012 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 13 września 2012 r. przez wykonawcę **Enigma Systemy Ochrony Informacji Sp. z o.o., ul. Jutrzenki 116, 02-230 Warszawa** w postępowaniu prowadzonym przez **Komenda Główna Straży Granicznej, ul. Podchorążych 38, 00-463 Warszawa**.

**orzeka:**

1. oddala odwołanie;
  
2. kosztami postępowania obciąża wykonawcę **Enigma Systemy Ochrony Informacji Sp. z o.o. z siedzibą w Warszawie** i:
  - 2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych, zero groszy) uiszczoną przez tytułem wpisu od odwołania.
  - 2.2. zasądza od **Enigma Systemy Ochrony Informacji Sp. z o.o. z siedzibą w Warszawie** na rzecz **Komendy Głównej Straży Granicznej** kwotę **3.598 zł 98 gr** (słownie: trzy tysiące pięćset dziewięćdziesiąt osiem złotych dziewięćdziesiąt osiem groszy) tytułem wynagrodzenia pełnomocnika.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2010 r. 113, poz. 759 ze zm.) 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**

Zamawiający: Komenda Główna Straży Granicznej w Warszawie prowadzi postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na „zakup szyfratorów IP (numer sprawy: 44/ZP/BŁN/12).

Enigma Systemy Ochrony Informacji sp. z o.o. z siedzibą w Warszawie (dalej „Odwołujący”) złożył do Prezesa Krajowej Izby Odwoławczej odwołanie zarzucając Zamawiającemu przy formułowaniu postanowień specyfikacji istotnych warunków zamówienia (dalej: siwz) naruszenie art. 7 ust. 1, art. 29 ust. 1, 2 i 3 ustawy Prawo zamówień publicznych (dalej: ustawa pzp) poprzez sporządzenie opisu przedmiotu zamówienia w sposób utrudniający uczciwą konkurencję i równe traktowanie wykonawców;

Odwołujący wniósł o nakazanie Zamawiającemu: dokonania modyfikacji SIWZ w sposób wskazany w uzasadnieniu odwołania.

Uzasadniając zarzuty i wnioski odwołania odwołujący wskazał, co następuje.

Zamawiający określił parametry dotyczące szyfratora IP w taki sposób, że ofertę w przedmiotowym postępowaniu może złożyć wyłącznie jeden dostawca sprzętu KRYPTON Polska sp. z o.o. z siedzibą w Warszawie oferujący jedno konkretne urządzenie. Formułując wymogi w zakresie opisu przedmiotu zamówienia Zamawiający winien kierować się celem, jakiemu zamawiane produkty mają służyć. SIWZ zawiera postanowienia nieznajdujące żadnego uzasadnienia merytorycznego, a uniemożliwiającą uczciwą konkurencję.

Zamawiający wskazał w SIWZ (Rozdział IV pkt 1), iż: „Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 7 miesięcy przed dostawą oraz muszą posiadać w momencie dostawy Certyfikat Ochrony Kryptograficznej wydany przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego, zapewniający ochronę informacji niejawnych o klauzuli „poufne” z terminem ważności minimum 4 lata od dnia dostawy urządzeń szyfrujących IP do Zamawiającego”.

W ocenie odwołującego Wymóg ten ogranicza uczciwą konkurencję i w świetle postanowień projektu umowy nie znajduje żadnego uzasadnienia. Wykaz urządzeń (szyfratorów IP) posiadających certyfikat znajduje się na liście prowadzonej przez SKW ([http://www.skw.gov.pl/ZBIN/Crypto\\_lista.htm](http://www.skw.gov.pl/ZBIN/Crypto_lista.htm)) oraz na liście certyfikatów wydanych przez Jednostkę Certyfikującą DBTI ABW dla urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych, dostępnych w ofercie handlowej producentów (opublikowana na: [http://bip.abw.gov.pl/download/1/752/List\\_a\\_UC\\_ed45\\_Ochrona](http://bip.abw.gov.pl/download/1/752/List_a_UC_ed45_Ochrona)

Kryptograficzna 28 06 2012.pdf). Z zestawień urządzeń zamieszczonych na ww. listach wynika, iż następujące urządzenia posiadają Certyfikat Ochrony Kryptograficznej:

1. T/7/2012 Urządzenie kryptograficzne KRYPTON K2 w wersji 1.3.0 ważny do 30.06.2018 produkcji - Krypton Polska sp. z o.o.
2. 309/2007 Urządzenie kryptograficzne CompCrypt ETA-VPN 100P z oprogramowaniem systemowym w wersji 3.0 ważny do 31.08.2012 produkcji Pacomp sp. z o.o.
3. 55/2009 Urządzenie kryptograficzne CompCrypt ETA-VPN 100P z oprogramowaniem systemowym w wersji 3.50.05 produkcji Pacomp sp. z o.o. certyfikat ważny do 27.02.2014
4. 41/2011 SKW Urządzenie utajniające w sieci IP CompCrypt ETA - MIL 10P – Ex 01.03.2014 prod. Pacomp sp. z o.o.
5. 40/2011 SKW Urządzenie utajniające w sieci IP CompCrypt ETA - MIL 10P certyf. ważny do 01.03.2014 prod. Pacomp sp. z o.o.

Z zestawienia wynika, iż jedynie urządzenie kryptograficzne KRYPTON K2 w wersji 1.3.0 produkcji Krypton Polska sp. z o.o. spełnia kwestionowany wymóg Zamawiającego. Odwołujący - pomimo to, że sprzedaje sprawdzone i renomowane urządzenia, dla których certyfikaty ochrony kryptograficznej wydawane są od 2000r - nie może złożyć oferty. Na polskim rynku istnieje tylko dwóch producentów urządzeń kryptograficznych posiadających certyfikaty ochrony kryptograficznej, jeden który swoje urządzenia oferuje od 2000r. i które działają w większości służb (w tym służb specjalnych), agend, urzędów etc. oraz drugi, który swoje urządzenia zaczyna dopiero oferować od połowy tego roku. Powyższy wymóg zawarty w SIWZ eliminuje znane, uznane i sprawdzone rozwiązania, a preferuje z nieznanymi powodów rozwiązania które jeszcze nigdzie nie zostały wykorzystane i sprawdzone w warunkach pracy rzeczywistego systemu przetwarzającego informacje niejawne. W trakcie wieloletniej działalności odwołujący nie spotkał się z uwagami kwestionującymi jakość oferowanych przez niego szyfratorów IP.

Wymóg, aby urządzenie posiadało 4 lata ważności certyfikatu ochrony kryptograficznej, narusza zasadę z art. 7 Pzp. W chwili obecnej na świecie istnieje tylko jedno urządzenie z tak długim okresem ważności certyfikatu - ponieważ certyfikat na to urządzenie został wydany trzy miesiące temu (w czerwcu 2012r.). Natomiast pozostałe urządzenia, które spełniają wymagania techniczne, i które mógłby zaoferować Odwołujący w tym postępowaniu, miały wydany certyfikat w 2006r. który po kolejnych przedłużeniach jest na dzień dzisiejszy ważny do 2014r. - tj. łącznie 8 lat od chwili wydania. Praktyką stosowaną przez producentów jest, że certyfikaty są odnawiane pod koniec okresu ich ważności. Z uwagi na to, że jest to proces długotrwały, producent od dwóch miesięcy prowadzi z ABW uzgodnienia w sprawie kolejnych badań certyfikacyjnych, które powinny rozpocząć się

jeszcze w tym roku, a zakończyć najpóźniej w drugiej połowie roku 2013r. wydaniem certyfikatu ochrony kryptograficznej na okres nie krótszy niż trzy kolejne lata - czyli w efekcie na okres taki jak jest literalnie wymagany przez Zamawiającego.

O zbędności wymogu świadczą postanowienia Załącznika nr 4 do SIWZ (umowa na zakup szyfratorów). Zgodnie z §11 ust. 1 czteroletni termin ważności nie jest wymagany, co więcej §11 ust. 3 i 4 przewidują sytuację utraty ważności certyfikatu z przyczyn innych niż te, które wynikają ze strony Zamawiającego - a zatem także ze względu na upływ czasu. W takim przypadku musi nastąpić „aktualizacja” certyfikatu na koszt wykonawcy, a gwarancja na urządzenie ulega odpowiedniemu przedłużeniu.

Ze względu na fakt, iż Zamawiający odnosi się tu do gwarancji jakości rzeczy wskazać należy, iż brak stosownego certyfikatu jest wadą, która podlega usunięciu poprzez działania wykonawcy. Tym samym żądanie czteroletniego okresu ważności certyfikatu w chwili dostawy stanowi jedynie utrudnienie uczciwej konkurencji a nie przejaw uzasadnionych potrzeb Zamawiającego.

Wymóg aby zamawiane urządzenia przez cały okres ich użytkowania posiadały ważny certyfikat można osiągnąć w sposób, który nie ograniczałby uczciwej konkurencji. Dlatego też odwołujący wnosi o nakazanie zmiany postanowień SIWZ w ten sposób, iż „oferowany przez Wykonawcę szyfrator IP będzie posiadał ważny certyfikat ochrony kryptograficznej przez okres co najmniej 1 roku od dostawy i wykonawca zobowiązuje się do dostarczenia nowego certyfikatu na co najmniej 3 miesiące przed upływem ważności certyfikatu.”

Zamawiający dokonując opisu przedmiotu zamówienia powinien uwzględnić istniejące realia rynkowe oraz potencjalnych wykonawców zainteresowanych udziałem w postępowaniu tak, aby nie doprowadzić do sytuacji, w której dochodzi do zawężenia kręgu wykonawców. Jeżeli Zamawiający zamierza dokonać zakupu konkretnego urządzenia od konkretnego producenta, to winien dokonać tego w trybie zamówienia z wolnej ręki po wyczerpaniu przesłanek uzasadniających zastosowanie tego trybu. Skoro jednak przeprowadza postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego to oznacza, iż przesłanek zakupu tego konkretnego urządzenia nie ma, a zatem Zamawiający powinien dopuścić możliwość zaoferowanie także innych urządzeń.

Na poparcie argumentacji odwołujący powołał orzecznictwo Krajowej Izby Odwoławczej.

Zamawiający wniósł o oddalenie odwołania. Wskazał, że realizując zadania ustawowe przetwarza informacje niejawne. Tworzy system teleinformatyczny zbudowany na bazie urządzeń i narzędzi kryptograficznych. Wskazał, że podstawą akredytacji systemu jest. m.in. posiadanie przez urządzenia wchodzące w jego skład (szyfratory) certyfikatu ochrony kryptograficznej uzyskiwanego na podstawie art. 50 ustawy o ochronie informacji niejawnych. Powołał się na treść Polityki Kryptograficznej ABW wydanej w 2011 r. przez

Agencję Bezpieczeństwa Wewnętrznego. Wskazał, że udzielanie akredytacji systemu następuje na okres nie dłuższy niż 5 lat. Wskazał na zapisy siwz.

W ocenie Zamawiającego najbezpieczniejszym jest nabycie urządzeń z certyfikatem ważnym na okres przewidywanej akredytacji systemu. Stwierdził, że w razie utraty ważności certyfikatu, zachodzi ryzyko utraty akredytacji systemu.

Stwierdził, że wykonawca nie może zagwarantować w sposób pewny przedłużenia ważności certyfikatu na oferowane urządzenie.

Zauważył, że interesuje go certyfikat ważny, począwszy od dnia dostawy i nie jest wiadomo, jakie szyfratory będą spełniać wymogi w tej dacie.

Krajowa Izba Odwoławcza po rozważeniu sprawy na rozprawie z udziałem stron, wzięwszy pod uwagę postanowienia siwz, stanowiska stron wyrażone na piśmie i do protokołu, zważyła, co następuje.

Odnosnie stanu faktycznego Izba uznaje, że odwołujący wykazał, iż na dzień rozpatrywania istnieje jedno urządzenie spełniające wymogi siwz postawione w zakresie okresu ważności certyfikatu. Okoliczność ta nie ma jednak znaczenia przy ocenie zarzuty, skoro wymóg ważności certyfikatu ustalony został nie w celu oceny spełniania warunków przedmiotowych przez potencjalnych wykonawców, lecz jest odniesiony do konkretnych dostaw, mających być wykonaniem umowy w sprawie zamówienia publicznego. Izba uznaje także za wiarygodne twierdzenie odwołującego, że w praktyce podmiot zainteresowany przedłużeniem ważności występuje do właściwego podmiotu przed upływem terminu ważności. Natomiast przepisy ustawy o ochronie informacji niejawnych nie uniemożliwiają uzyskania nowego certyfikatu na określone urządzenie w okresie znacznie wyprzedzającym termin upływu ważności, w tym np. na potrzeby udziału w konkretnym zamówieniu publicznym.

Skład orzekający zauważa, że procedura certyfikacji i ewentualne procedury przedłużania prowadzone są wyłącznie na wniosek zainteresowanego podmiotu (najczęściej producenta takich urządzeń) i nie ma przeszkód prawnych w uzyskaniu stosownego certyfikatu odpowiadającego oczekiwaniom zamawiającego.

W ocenie Izby zamawiający opisując przedmiot zamówienia miał prawo sformułować opis uwzględniając cel, jakim jest zminimalizowanie ryzyka użytkowania urządzenia kryptograficznego nie posiadającego ważnego certyfikatu.

Biorąc powyższe pod uwagę w ocenie składu orzekającego zamawiający formułując warunki udziału w postępowaniu oraz obowiązki wykonawcy określone we wzorze umowy nie naruszył przepisów ustawy, a tym samym zarzuty zamawiającego nie potwierdziły się.

Uwzględniając powyższe, na podstawie art. 192 ust. 1 Pzp orzeczono jak w sentencji.

Biorąc powyższe pod uwagę w ocenie składu orzekającego zamawiający formułując warunki jakie zostały postawione wobec przedmiotu zamówienia, nie naruszył przepisów Prawa zamówień publicznych, a tym samym zarzuty odwołania nie potwierdziły się.

Uwzględniając powyższe, na podstawie art. 192 ust. 1 Pzp orzeczono jak w sentencji.

O kosztach postępowania orzeczono na podstawie art. 192 ust. 9 i 10 Pzp stosownie do wyniku sprawy oraz zgodnie rozporządzeniem 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).

**Przewodniczący:** .....