Sygn. akt KIO 350/21

WYROK
z dnia 22 marca 2021 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący:	**Monika Kawa-Ogorzałek**
Członkowie:	**Danuta Dziubińska**
	Andrzej Niwicki
Protokolant:	**Adam Skowroński**

po rozpoznaniu na rozprawie w dniu 9 marca 2021r., w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 1 lutego 2021 r. przez wykonawcę ubiegającego się o udzielenie zamówienia **NTT Technology Sp. z o.o. z siedzibą w Warszawie** w postępowaniu prowadzonym przez **Centrum Informatyki Resortu Finansów z siedzibą w Radomiu**

przy udziale:

wykonawcy **IMMITIS Sp. z o.o. z siedzibą w Bydgoszczy** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **odwołującego**

oraz

przy udziale wykonawcy **Integrale IT Sp. z o.o. z siedzibą w Poznaniu** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **odwołującego**

oraz

przy udziale wykonawcy **PRZP Systemy Informacyjne Sp. z o.o. z siedzibą w Połańcu** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **odwołującego**

oraz

przy udziale wykonawcy **Towarzystwo Handlowe Alplast Sp. z o.o. Sp.k. z siedzibą w Niekaninie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **odwołującego**

oraz

przy udziale wykonawcy **Computex Sp. z o.o. Sp.k. z siedzibą w Warszawie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **Egida IT Solutions Sp. z o.o. z siedzibą w Warszawie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **GALAXY Systemy Informatyczne Sp. z o.o. z siedzibą w Zielonej Górze** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **INTARIS Sp. z o.o. z siedzibą w Warszawie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **MAXTO ITS Sp. z o.o. Sp. k z siedzibą w Modlniczce** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **SUNTAR Sp. z o.o. z siedzibą w Tarnowie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

oraz

przy udziale wykonawcy **MBA System Sp. z o.o. z siedzibą w Warszawie** zgłaszającego przystąpienia do postępowania odwoławczego po stronie **zamawiającego**

orzeka:

1. oddala odwołanie;
2. Kosztami postępowania obciąża Odwołującego i zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez Odwołującego tytułem wpisu od odwołania.

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

Przewodniczący : ……

Członkowie: ……

……

UZASADNIENIE

Zamawiający - Centrum Informatyki Resortu Finansów z siedzibą w Radomiu prowadzi na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t. j. Dz. U. z 2019 r., poz. 1843 ze zm.; dalej: „Pzp") postępowanie o zawarcie umowy ramowej w trybie przetargu nieograniczonego na: „Dostawę komputerów typu AiO wraz z oprogramowaniem, komputerów stacjonarnych wraz z oprogramowaniem i tabletów graficznych wraz z oprogramowaniem".

Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 28 grudnia 2020r., pod numerem 2020/S 252-635428.

Szacunkowa wartość zamówienia jest wyższa od kwot wskazanych w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 Pzp.

W dniu 1 lutego 2021 r. – wykonawca NTT Technology spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie (dalej: „Odwołujący") wniósł do Prezesa Krajowej Izby Odwoławczej odwołanie wobec treści specyfikacji istotnych warunków zamówienia (dalej: „SIWZ") zarzucając Zamawiającemu naruszenie art. 90 ust. 1 ustawy z dnia 11 września 2019r. Przepisy wprowadzające ustawę – prawo zamówień publicznych w zw. z art. 7 ust. 1 w zw. z art. 29 ust. 1 ust. 2 i ust. 3 Pzp poprzez: wprowadzenie do SIWZ wymogu w zakresie płyty głównej: „Wbudowany w płytę główną dedykowany moduł sprzętowy szyfrujący w standardzie TPM w wersji min. 2.0 z certyfikatem TCG tzw. Hardware TPM", podczas gdy jest to wymóg naruszający zasadę uczciwej konkurencji, ograniczający w sposób nieuzasadniony dostęp do zamówienia znacznej części wykonawcom, prowadzący do nieuzasadnionego uprzywilejowania niektórych wykonawców, a co za tym idzie niezgody z Pzp.

W oparciu tak sformułowany zarzut Odwołujący wniósł o nakazanie Zamawiającemu przywrócenia brzmienia SIWZ sprzed modyfikacji, tj. zmianę postanowień SIWZ z wersji obecnej: „*Wbudowany w płytę główną dedykowany moduł sprzętowy szyfrujący w standardzie TPM w wersji min. 2.0 z certyfikatem TCG tzw. Hardware TPM*" na „*Zintegrowany z płytą główną moduł TPM 2.0*".

Uzasadniając powyższy zarzut Odwołujący wskazał, że Zamawiający w dniu 21 stycznia 2021 r. w Tomie III SIWZ - OPIS MINIMALNYCH WYMAGAŃ TECHNICZNYCH dokonał zmiany wymogu w zakresie płyty głównej sprzętu będącego przedmiotem postępowania z zapisu „zintegrowany z płytą główną moduł TPM 2.0" na „wbudowany w

płytę główną dedykowany moduł sprzętowy szyfrujący w standardzie TPM w wersji min. 2.0 z certyfikatem TCG tzw. Hardware TPM".

Według Odwołującego Zamawiający dokonując ww. zmiany diametralnie ograniczył możliwości zastosowania alternatywnych, równoważnych rozwiązań dostępnych na rynku, a co za tym idzie znacząco ograniczył krąg wykonawców zdolnych do złożenia w przedmiotowym postepowaniu oferty niepodlegającej odrzuceniu jako niezgodnej z SIWZ. Podkreślił, że wprowadzone postanowienie wymusza zastosowanie rozwiązań które są przestarzałe i nie wspierane przez większość producentów płyt głównych, ponieważ zdecydowana większość producentów sprzętu ogranicza się do rozwiązań typu fTPM (firmeware TPM) i nie oferuje modułu wymaganego przez Zamawiającego w aktualnej wersji SIWZ. Odwołujący wyjaśnił, że fTPM to implementacja modułu TPM 2.0 oparta na oprogramowaniu układowym. Platforma obsługuje wymagania firmy Microsoft dotyczące modułu trusted platform 2.0 (fTPM), a ponadto rozwiązanie fTPM jest rozwiązaniem rekomendowanym przez firmę Microsoft. Wyjaśni, że rozwiązanie typu fTPM obsługuje m. in. przechowywanie poświadczeń i zarządzanie kluczami oraz wszelkie inne funkcje typowe dla najpopularniejszych systemów operacyjnych (Windows 8 i Windows® 10). Zaletą rozwiązania fTPM jest możliwość ciągłej jego aktualizacji, co powoduje iż nie starzeje się on tak jak sprzętowy układ. Odwołujący wyjaśnił również, że w przypadku rozwiązania wymaganego aktualnie przez Zamawiającego w przypadku uszkodzenia samego układu należy wymienić całą płytę główną komputera, co może niewątpliwie narazić w przyszłości zamawiającego na dodatkowe koszty, podczas gdy w przypadku fTPM awarie płyty głównej można rozwiązać systemowo bez wymiany uszkodzonej płyty.

Ponadto Odwołujący podkreślił, że pod względem bezpieczeństwa użytkowania oba rozwiązania, tj. TPM oraz fTPM są dokładnie identyczne, a posługując się nomenklaturą Pzp są rozwiązaniami równoważnymi, ponieważ z punktu widzenia użytkownika, rozwiązanie oparte o hardwareowy moduł wlutowany w płytę główną daje dokładnie taki sam efekt jak rozwiązanie typu fTPM (firmeware TPM). Użytkownik w BIOS komputera widzi urządzenie TPM 2.0, które może włączyć lub wyłączyć i z użyciem tego urządzenia może pomyślnie przeprowadzić szyfrowanie dysku. Odwołujący dodał również, że samo urządzenie TPM nie szyfruje, ale służy do przechowywania kluczy szyfrujących. Efekt zastosowania TPM sprzętowego czy fTPM jest dokładnie taki sam.

Odwołujący podkreślił, że zrozumiałym jest niechęć Zamawiającego do rozwiązania w którym chip TPM wkłada się na tzw. piny wyprowadzone z płyty głównej i można ten moduł usunąć, ale rozwiązanie fTPM nie używa w ogóle tego modułu, a całe rozwiązanie jest sprzętowo – programowe jest wbudowane w płytę główną i nieusuwalne. Ponadto podkreślił,

że najważniejszym aspektem rozwiązań fTPM jest ich dostępność w płytach głównych większości producentów. Aktualnie jest to rozwiązanie stosowane powszechnie przez producentów płyt głównych i wspierane przez producentów procesorów takich jak Intel i AMD oraz producenta oprogramowania Microsoft. Rozwiązania sprzętowe hardware TPM są używane natomiast przez międzynarodowych producentów komputerów i zapis taki ich faworyzuje.

Powyższy zapis stanowi więc utrudnienie konkurencji i prowadzi do preferowania producentów międzynarodowych, którzy używają mechanizmu Hardware TPM. Wyjaśnił, że wyrażony w art. 29 ust. 2 Pzp zakaz utrudniania uczciwej konkurencji przy opisywaniu przedmiotu zamówienia zostanie naruszony, gdy przy jego dokonaniu Zamawiający użyje określeń czy parametrów wskazujących na konkretnego producenta lub konkretny produkt. Działaniem wbrew ww. zasadzie jest również na tyle rygorystyczne określenie wymagań w zakresie przedmiotu zamówienia, że nie jest to uzasadnione potrzebami Zamawiającego, a jednocześnie ogranicza krąg wykonawców zdolnych do wykonania zamówienia. Zdaniem Odwołującego Zamawiający w niniejszym postępowaniu naruszył zasadę uczciwej konkurencji poprzez wymóg oferowania tego typu rozwiązań technicznych, które wskazują wyłącznie na określony, wąski krąg producentów sprzętu komputerowego, eliminując jednocześnie z postępowania pozostałych. Zamawiający dokonując modyfikacji SIWZ w dniu 21 stycznia 2021r. nie tyle zmienił wymagania techniczne na inne, co dokonał zawężenia rozwiązań, które można skutecznie zaoferować w przedmiotowym postępowaniu. Rozwiązanie w zakresie płyty głównej wymagane przez Zamawiającego po zmianie SIWZ zawierało się w wymogu SIWZ w brzmieniu przed zmianą, tj. mogło zostać skutecznie zaoferowane również przed zmianą SIWZ. Natomiast po zmianie SIWZ, wykonawcy mogą zaoferować w zakresie płyty głównej wyłącznie jedno rozwiązanie techniczne, tj. wbudowany w płytę główną dedykowany moduł sprzętowy szyfrujący w standardzie TPM w wersji min. 2.0 z certyfikatem TCG tzw. Hardware TPM. Jedocześnie wykonawcy zostali pozbawieni możliwości zaoferowania innych wariantów technicznych płyty głównej, które spełniały pierwotny wymóg.

Zamawiający w odpowiedzi na odwołanie z dnia 8 marca 2021r. wniósł o jego oddalenie. Na wstępie wyjaśnił, że TPM (Trusted Platform Module) to mikroukład umożliwiający korzystanie ze wszystkich zaawansowanych funkcji zabezpieczeń (w przypadku systemów Windows jest to np. szyfrowanie dysków funkcją BitLocker). Służy on do zabezpieczania danych przed nieupoważnionym dostępem w przypadku kradzieży lub zagubienia urządzenia, zarówno w komputerach stacjonarnych, notebookach jak też

komputerach typu All i One. Układ TPM, w sposób bezpieczny przechowuje unikalny klucz szyfrujący i znacząco utrudnia dostęp do danych komputera niepowołanym osobom. Wymaganie aby urządzenia, których dostawę obejmuje przedmiotowe zamówienie, posiadały opisywane zabezpieczenie, uzasadnione jest koniecznością ochrony danych znajdujących się na komputerze, w sytuacji, gdy komputer (PC/Notebook/All in One) trafi w niepowołane ręce w wyniku kradzieży czy tez bezprawnego dostępu, w takiej sytuacji, dane zawarte na nośnikach są praktycznie niemożliwe do odczytania dzięki szyfrowaniu. Podkreślił, że układy TPM poza bezpiecznym przechowywaniem kluczy szyfrujących, zapewniają skuteczną ochronę certyfikatom i hasłom używanym do logowania się do systemu – jest to pewniejsza metoda niż przechowywanie ich na dysku twardym. Wymaganie posiadania układów TPM, jest stosowane w zakresie sprzętu posiadanego przez Zamawiającego, jako jedno z niezbędnych zabezpieczeń urządzeń komputerowych, będące w zgodzie z polityką bezpieczeństwa.

Rozwiązanie wymagane przez Zamawiającego jest rozwiązaniem stricte sprzętowym – do płyty głównej montowany jest mikroukład, który zapewnia bezpieczne przechowywanie kluczy szyfrujących, oraz skuteczną ochronę certyfikatom i hasłom używanym do logowania się do systemu. Natomiast rozwiązanie wnioskowane przez Odwołującego, tj. dopuszczenia ochrony wyłącznie w standardzie FTPM stanowi rozwiązanie działające jedynie w warstwie aplikacyjnej, nie stanowi fizycznego elementu (jak przy rozwiązaniu TPM). W związku z powyższym, w celu złamania zabezpieczenia wprowadzonego w standardzie FTMP i uzyskania dostępu do danych, wystarczające jest jedynie znalezienia luki w oprogramowaniu. Takie ataki są najprostsze do przeprowadzenia i nie wymagają posiadania specjalistycznego sprzętu, dlatego też FTPM stanowi rozwiązanie znacznie mniej bezpieczne.

Zamawiający podkreślił, że w przeciwieństwie do rozwiązania fTPM, rozwiązanie Hardware TPM (tzw. „kostka”) działa w warstwie fizycznej dlatego nie jest podatna na ataki softwareowe co znacząco zwiększa bezpieczeństwo danych.

Zamawiający wyjaśnił dodatkowo, że wymagania w przedmiotowym zakresie podyktowane są także doświadczeniami Resortu Finansów – zgodnie z którym rozwiązanie szyfrujące oparte na warstwie software – TruCrypt czyli aplikacyjnej zostało „złamane” – zhakowane, w rezultacie czego wszystkie komputery wykorzystujące tę technologię straciły jeden z poziomów zabezpieczeń. Zdarzenie takie nie miałoby miejsca gdyby komputery były zabezpieczone w standardzie TPM.

Zamawiający zauważył również, że z uwagi na zmiany społeczno – gospodarcze wywołane pandemią COVID – 19, w sferze administracji publicznej, upowszechniła się praca

zdalna, do której wykonywania pracownicy Zamawiającego używają sprzętu (w tym komputerów) udostępnionego przez Zamawiającego. Konieczne jest przy tym zapewnienie dla całego sprzętu wykorzystywanego w resorcie finansów jednolitości w zakresie poziomu zabezpieczeń. Należy zauważyć, że w celu świadczenia pracy zdalnej wydawane są nie tylko komputery przenośne, ale z powodu dużego zapotrzebowania również komputery stacjonarne. Szyfrowanie dysków jest jednym z niezbędnych wymagań dopuszczających zastosowanie sprzętu komputerowego do pracy zdalnej. Zamawiający oświadczył również, że wymaganie w zakresie TPM, zostało wprowadzone dla każdego z kupowanych Produktów - Sprzętu, jako główne rozwiązanie szyfrujące Zamawiającego, zatem wprowadzanie innych standardów miałoby negatywny wpływ także na standaryzację obsługi sprzętu i tym samym na świadczone wewnętrznie usługi wsparcia informatycznego. Aktualnie Resort Finansów liczy ponad 60 000 pracowników, z których każdy posiada przynajmniej jedną jednostkę komputerową, dlatego też tak ważna jest standaryzacja pozwalająca zapewnić odpowiedni poziom bezpieczeństwa informatycznego. W Resorcie Finansów wykorzystanie TPM zostało określone w procedurze przygotowania komputerów które będą wykorzystywane poza siedzibą MF.

Zamawiający wskazał, że nie sposób również zgodzić się z twierdzeniem iż rozwiązanie TPM, ogranicza konkurencję zarówno pomiędzy produktami jak i wykonawcami. Rozwiązanie to stosuje wielu producentów komputerów m. in. DELL,HP, Lenovo, Apple, Acer, ASUS, Fujitsu (również serwery), Gigabyte (płyty główne), , Intel, IBM, Toshiba, MSI posiadających w swojej ofercie w sumie kilkadziesiąt sztuk sprzętu w których TPM jest standardem w linii biznesowej.

Odnosząc się natomiast, do wymogu zgodności rozwiązania TPM ze standardem TCG, Zamawiający wskazał, że wprowadzenie tego standardu, niejako dopełnia rozwiązanie TPM, bowiem umożliwia certyfikowanym dyskretnym modułom TPM zabezpieczenie się w większym stopniu przed atakami fizycznymi.

Odnosząc się natomiast do twierdzenia Odwołującego, że wprowadzonym zapisem diametralnie ograniczył możliwości zastosowania alternatywnych, równoważnych rozwiązań dostępnych na rynku, a co za tym idzie znacząco ograniczył krąg wykonawców Zamawiający podkreślił, że rozwiązanie TPM, certyfikowane przez TCG, jest rozwiązaniem powszechnym i nawet jeśli istnieją produkty posiadające zabezpieczenia w standardzie TPM i nie posiadające jednocześnie certyfikacji TCG, to stanowią one niewielki odsetek produktów oferowanym na rynku. Należy przy tym wskazać, że Odwołujący nie wykazał, jakie produkty zostały wyeliminowane przez zamawiającego poprzez doprecyzowanie postanowień SIWZ.

Zamawiający nie podzielił również stanowiska Odwołującego jakoby zmiana SIWZ wymuszała od wykonawców zastosowanie rozwiązań które są przestarzałe i nie wspierane przez większość producentów płyt głównych oraz, jakoby zdecydowana większość producentów sprzętu ograniczała się do rozwiązań typu fTPM (firmeware TPM) i nie oferowała modułu wymaganego przez zamawiającego w aktualnej wersji SIWZ. FTPM to implementacja modułu TPM 2.0 oparta na oprogramowaniu układowym. Zamawiający wskazał bowiem, że rozwiązanie TPM nie może być uznane za przestarzałe bądź niewspierane przez producentów płyt głównych. Rozwiązanie to jest w dalszym ciągu rozwijane i powstają jego kolejne wersje, nie ma również statusu end of life. Nie jest też prawdą, iż wiodący producenci rezygnują z wykorzystania TPM w produkowanych przez siebie produktach, bowiem jak wskazano wyżej wśród producentów komputerów wyposażonych w układy zgodne z TPM, wymienić można m. in.: Apple, Acer, ASUS, Dell, Fujitsu (również serwery), Gigabyte (płyty główne), HP, Intel, Lenovo/IBM, Toshiba, MSI. Wobec powyższego należy uznać, że wiodący producenci w dalszym ciągu wykorzystują rozwiązanie TPM.

Zamawiający podkreślił również, że rozwiązania aplikacyjne – softweare'owe są bardziej podatne na włamania. W zakresie bezpieczeństwa, znaczenia nie ma bowiem, wyłącznie efekt, ale również sposób jego osiągnięcia. Wyłączenie modułu TMP w BIOS-ie nie spowoduje automatycznego dostępu do zaszyfrowanych danych, gdyż klucze pozwalające na ich rozszyfrowanie znajdują się w mikroukładzie TPM. Zamawiający wskazał, że rozwiązanie TPM można porównać do sejfu niedostępnego dla kogokolwiek oprócz systemu, który się do tych kluczy odwołuje w celu odszyfrowania danych. Pozostawienie kwestii zabezpieczeń wyłącznie w wersji aplikacyjnej obarczone jest ryzykiem nie powołanego dostępu, tym samym zwiększając ryzyko w zakresie bezpieczeństwa, na które zamawiający pozwolić sobie nie może.

Zamawiający podkreślił również, że celem wymagań zawartych w SIWZ jest zapewnienie odpowiedniego poziomu bezpieczeństwa, nie zaś preferowanie rozwiązań konkretnych producentów czy konkretnych produktów mogące ograniczać konkurencję. Podkreślił, że przeprowadzona przez niego analiza rynku wskazuje na powszechność i szeroką dostępność rozwiązania TMP, znajdującego odzwierciedlenie w liczbie produktów oraz producentów wykorzystujących to rozwiązanie. Z informacji zawartych na stronie Microsoft, wynika iż: „Moduły TPM są pasywne: odbierają polecenia i zwracają odpowiedzi. Aby w pełni wykorzystać zalety modułu TPM, producent OEM musi dokładnie zintegrować sprzęt systemowy i oprogramowanie układowe z modułem TPM, aby wysyłać mu polecenia i reagować na jego odpowiedzi. Moduły TPM zostały pierwotnie zaprojektowane, aby

zapewnić korzyści w zakresie bezpieczeństwa i prywatności właścicielowi i użytkownikom platformy, ale nowsze wersje mogą zapewnić korzyści w zakresie bezpieczeństwa i prywatności samego sprzętu systemowego. Jednak zanim będzie można go użyć w zaawansowanych scenariuszach, należy udostępnić moduł TPM. System Windows 10 automatycznie udostępnia moduł TPM, ale jeśli użytkownik planuje ponowną instalację systemu operacyjnego, może być konieczne wyczyszczenie modułu TPM przed ponowną instalacją, aby system Windows mógł w pełni wykorzystać moduł TPM". Powyższe przeczy więc twierdzeniom Odwołującego, iż Microsoft nie wykorzystuje tego rozwiązania.

Zamawiający stwierdził również, że okolicznością uzasadniającą zastosowanie rozwiązania TPM jest także to, że producenci komputerów, wdrażają moduł TPM jako składnik zaufanej platformy komputerowej, takiej jak komputer, tablet lub telefon. Zaufane platformy komputerowe wykorzystują moduł TPM do obsługi scenariuszy dotyczących prywatności i bezpieczeństwa, których samo oprogramowanie (w tym rozwiązanie fTPM) nie jest w stanie osiągnąć. W szczególności oprogramowanie nie może wiarygodnie zgłosić obecności złośliwego oprogramowania podczas procesu uruchamiania systemu. Ścisła integracja między modułem TPM a platformą zwiększa przejrzystość procesu uruchamiania i wspiera ocenę stanu urządzenia, umożliwiając wiarygodne pomiary i raportowanie oprogramowania, które uruchamia urządzenie. Wdrożenie modułu TPM jako części zaufanej platformy komputerowej zapewnia sprzętowe źródło zaufania - to znaczy zachowuje się w zaufany sposób. Na przykład, jeśli klucz przechowywany w module TPM ma właściwości, które uniemożliwiają eksportowanie klucza, klucz ten nie może opuścić modułu TPM, co przekłada się na większe bezpieczeństwo gwarantowane przez to rozwiązanie w stosunku do innych rozwiązań.

Również dla konsumentów końcowych zastosowanie rozwiązania TPM ma znaczenie. TPM jest używany w Windows Hello, Windows Hello dla firm, a w przyszłości będzie składnikiem wielu innych kluczowych funkcji zabezpieczeń w systemie Windows. TPM zabezpiecza kod PIN, pomaga w szyfrowaniu haseł i opiera się na naszej ogólnej historii korzystania z systemu Windows 10, aby zapewnić bezpieczeństwo jako kluczowy filar. Korzystanie z systemu Windows w systemie z modułem TPM zapewnia wyższy poziom ochrony.

Zamawiający podkreślił, że również zgodnie z najnowszymi „Rekomendacjami Prezesa Urzędu Zamówień Publicznych dotyczącymi udzielania zamówień publicznych na dostawę zestawów komputerowych" z marca 2021r., wymaganie nie tylko jest właściwe, ale forma wymagania przyjęta przez Zamawiającego, wskazana jest jako rozwiązanie rekomendowane.

Powyższe, w ocenie Zamawiającego potwierdza prawidłowość zastosowanych wymagań.

Przystępujący po stronie Zamawiającego - wykonawca Egida IT Solutions Sp. z o.o. z siedzibą w Warszawie w piśmie z dnia 8 marca 2021r. wniósł o oddalenie odwołania jako bezzasadnego.

Krajowa Izba Odwoławcza uwzględniając dokumentację z przedmiotowego postępowania o udzielenie zamówienia publicznego, jak również oświadczenia, stanowiska stron złożone w trakcie rozprawy, ustaliła i zważyła, co następuje:

Odwołanie nie zasługiwało na uwzględnienie.

Mając na uwadze treść art. 92 ust. 2 ustawy z dnia 11 września 2019 r. Przepisy wprowadzające ustawę - Prawo zamówień publicznych (Dz.U. z 2019 poz. 2020), do postępowań odwoławczych oraz postępowań toczących się wskutek wniesienia skargi do sądu, o których mowa w ustawie uchylanej w art. 89, wszczętych po dniu 31 grudnia 2020 r., dotyczących postępowań o udzielenie zamówienia wszczętych przed dniem 1 stycznia 2021r., stosuje się przepisy ustawy, o której mowa w art. 1, Izba do postępowania odwoławczego w przedmiotowej sprawie zastosowała przepisy ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm., dalej jako „ustawa nPzp"). Do rozpoznania odwołania zastosowanie natomiast znajdowały przepisy Pzp obowiązujące w dacie wszczęcia postępowania o udzielenie zamówienia.

Izba dopuściła do udziału w postępowaniu wykonawców zgłaszających swoje przystąpienie do postępowania odwoławczego po stronie Odwołującego oraz Zamawiającego, stwierdzając, iż spełnione zostały przesłanki, o których mowa w art. 525 ust. 1-3 ustawy nPzp. Izba stwierdziła, iż nie została wypełniona żadna z przesłanek skutkujących odrzuceniem odwołania na podstawie art. 528 ustawy nPzp i skierowała sprawę na rozprawę.

Izba dopuściła i przeprowadziła dowody z treści SIWZ, odwołania, odpowiedzi na odwołanie oraz pisma procesowego Przystępującego Egida, a także dowodów złożonych na rozprawie przez uczestników postępowania:

- dowodów złożonych przez Przystępującego INTARIS – wydruk i tłumaczenie ze strony internetowej: https://docs.microsoft.com/en-us/windows/security,information-

protection/tpm/tpm-recommendations, wydruk i tłumaczenie broszury TPM 2.0 – krótki wstęp”

- „Rekomendacji Prezesa Urzędu Zamówień Publicznych dotyczących zamówień na zestawy komputerowe”,

- dowodów złożonych przez Przystępującego MBA – „Funkcje modułow TPM 1.2 i 2.0.”, wydruku ze strony internetowej www.mazowieckie.kas.gov.pl

Izba zważyła:

Na wstępie podkreślić należy, że Izba zgodnie z art. 555 nPzp Izba nie może orzekać co do zarzutów, które nie były zawarte w odwołaniu. W związku z powyższym Izba będąc związana powyższym przepisem, rozpoznała tylko zarzuty sformułowane przez Odwołującego w odwołaniu, w konsekwencji czego Izba nie rozpoznała zarzutów dotyczących konieczności posiadania certyfikatu TCG, bowiem zarzut ten został podniesiony przez Odwołującego dopiero na rozprawie. Ponadto wskazać należy, że argumenty i stanowisko dotyczące możliwości zaoferowania zabezpieczenia opartego na rozwiązaniu INTEL PTT również wykraczały poza zakres odwołania, w którym Odwołujący dążył do wykazania równoważności rozwiązania TPM i fTPM. Ponadto podkreślić należy, że z odwołania nie wynikało również, że Odwołujący kwestionuje zapis dotyczący „dedykowania modułu sprzętowego” jako zapis uniemożliwiający złożenie oferty w postępowaniu.

Podsumowując, Izba w składzie orzekającym pominęła przy orzekaniu powyższe i orzekła tylko w granicach wynikających z odwołania.

Przechodząc więc do merytorycznego rozpoznania zarzutów wskazać należy, że zgodnie z art. 29 ust. 2 Pzp przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Stosownie do art. 7 ust. 1 Pzp Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób zapewniający zachowanie uczciwej konkurencji i równe traktowanie wykonawców oraz zgodnie z zasadami proporcjonalności i przejrzystości.

W ocenie Izby w rozpoznawanym stanie faktycznym Odwołujący nie zdołał wykazać, aby zaskarżone postanowienie opisu przedmiotu zamówienia naruszało przytoczone wyżej przepisy Pzp. W pierwszej kolejności podkreślić należy, że odwołania dotyczące postanowień SIWZ, tak jak dotyczące każdej innej czynności lub zaniechania Zamawiającego, służą ochronie wykonawców przed działaniami niezgodnymi z przepisami prawa, a Izba może uwzględnić odwołanie wyłącznie w sytuacji, gdy stwierdzi naruszenie

przez Zamawiającego przepisów ustawy mające wpływ lub mogące mieć istotny wpływ na wynik postępowania (art. 554 ust. 1 pkt 1 Pzp). Nie korzystają zatem z ochrony prawnej dążenia wykonawców ukierunkowane jedynie na ukształtowanie takiej treści SIWZ, która pozwoli na złożenie oferty na korzystniejszych warunkach, jeżeli zaskarżona treść SIWZ nie stoi w sprzeczności z przepisami prawa. Kolejno podkreślić należy, że Zamawiający, jako podmiot dokonujący zakupów, jest uprawniony do określenia swoich oczekiwań dotyczących przedmiotu zamówienia, jego cech i funkcjonalności. Każde z takich wymagań w większym lub mniejszym stopniu ogranicza konkurencję, jednak tak długo, jak wymagania te są podyktowane obiektywnie uzasadnionymi potrzebami Zamawiającego, a ich celem nie jest zawężenie kręgu wykonawców mogących je wykonać, to Zamawiający jest uprawniony do ich sformułowania. Nie jest natomiast celem systemu zamówień publicznych i obowiązującej w nim zasady uczciwej konkurencji, umożliwienie uzyskania zamówienia wszystkim wykonawcom działającym w danej branży, bez względu na to, jakie cechy i właściwości ma przedmiot zamówienia, który mogą lub chcą zaoferować i bez uwzględnienia potrzeb Zamawiającego. To bowiem Zamawiający jest uprawniony do określenia tego co, zamierza nabyć i jeśli tylko nie stawia wymagań, które mają za cel ograniczenie konkurencji, nie zaś zrealizowanie jego potrzeb, to nie można mu w drodze środków ochrony prawnej nakazywać, aby nabył produkty lub rozwiązania, które jego potrzeb nie zaspokoją. Natomiast okoliczność, że dany wykonawca nie jest w stanie dostarczyć produktów spełniających wymagania określone przez Zamawiającego, nie może być automatycznie utożsamiana z naruszeniem konkurencji. Tym bardziej nie można utożsamiać z takim naruszeniem sytuacji, w której wykonawca jest w stanie dostarczyć produkty zgodne z wymaganiami Zamawiającego, ale zaoferowanie innych produktów pozwoliłoby na złożenie korzystniejszej (np. bardziej konkurencyjnej cenowo) oferty.

W ocenie Izby w rozpoznawanej sprawie Zamawiający przedstawił konkretne i racjonalne uzasadnienie do wprowadzenia do OPZ zaskarżonego wymagania, co w ocenie składu orzekającego pozwala uznać to wymaganie za mające oparcie w jego uzasadnionych potrzebach, nie zaś za podyktowane dążeniem do ograniczenia konkurencji. Co istotne również w rozpoznawanej sprawie - Odwołujący, na którym zgodnie z art. 534 ust. 1 zd. 1 nPzp spoczywał ciężar dowodu, nie przedstawił żadnych dowodów podważających twierdzenia Zamawiającego w tym zakresie.

Podkreślić należy, że bezsporne między stronami jest, że na rynku funkcjonują rozwiązania techniczne TPM sprzętowego jak też fTPM, czyli TPM aplikacyjny, softwearowy. Zdaniem Odwołującego Zamawiający dopuszczając możliwość zaoferowania rozwiązania fTPM uzyskałby taki sam efekt i poziom zabezpieczenia jak przy zastosowaniu wymaganego

przez siebie TPM sprzętowego. Natomiast Zamawiający wskazywał, że rozwiązanie przez niego żądane jest rozwiązaniem zapewniającym wyższy poziom zabezpieczenia i ochrony danych przed nieupoważnionym dostępem do nich w przypadku kradzieży lub zagubienia urządzenia, zarówno w komputerach stacjonarnych, notebookach jak też komputerach typu All i One.

Zgodnie ze stanowiskiem Zamawiającego, układy TPM poza bezpiecznym przechowywaniem kluczy szyfrujących, zapewniają skuteczną ochronę certyfikatom i hasłom używanym do logowania się do systemu. Ponadto, jak wskazał Zamawiający wymaganie posiadania układów TPM, jest stosowane w zakresie sprzętu posiadanego przez Zamawiającego, jako jedno z niezbędnych zabezpieczeń urządzeń komputerowych, będące w zgodzie z polityką bezpieczeństwa. Zdaniem Zamawiającego również żądane przez niego rozwiązanie jest rozwiązaniem stricte sprzętowym, który zapewnia bezpieczne przechowywanie kluczy szyfrujących, oraz skuteczną ochronę certyfikatom i hasłom używanym do logowania się do systemu. Natomiast rozwiązanie wnioskowane przez Odwołującego, tj. dopuszczenia ochrony wyłącznie w standardzie fTPM stanowi rozwiązanie działające jedynie w warstwie aplikacyjnej, nie stanowi fizycznego elementu (jak przy rozwiązaniu TPM). W związku z powyższym, w celu złamania zabezpieczenia wprowadzonego w standardzie fTMP i uzyskania dostępu do danych, wystarczające jest jedynie znalezienia luki w oprogramowaniu. Takie ataki są najprostsze do przeprowadzenia i nie wymagają posiadania specjalistycznego sprzętu, dlatego też fTPM stanowi rozwiązanie znacznie mniej bezpieczne. Zamawiający wyjaśnił również, że w przeciwieństwie do rozwiązania fTPM, rozwiązanie Hardware TPM działa w warstwie fizycznej dlatego nie jest podatne na ataki softwareowe, co znacząco zwiększa bezpieczeństwo danych.

Ponadto podkreślić należy, że z dowodu przedłożonego przez Przystępującego Intaris wynika, że: „wbudowany TPM zapewnia najwyższy poziom bezpieczeństwa (…). Celem tego *poziomu jest zapewnienie, że urządzenie, które chroni, działa w ten sposób aby nie dać się zhakować nawet wyrafinowanymi metodami. Aby to osiągnąć, zaprojektowano i wbudowano chip w celu zapewnienia najwyższego poziomu bezpieczeństwa, który jest odporny na manipulacje przy chipie, w tym sondowanie go i zamrażanie za pomocą różnego rodzaju wyrafinowanych ataków*”. Natomiast fTPM: „*jest zaimplementowany w chronionym oprogramowaniu. Kod działa na głównym procesorze, więc oddzielny chip nie jest wymagany. Podczas działania jak każdy inny program kod jest chroniony w środowisku wykonawczym zwanym zaufanym środowiskiem wykonawczym (TEE), które jest oddzielone od reszty programów uruchomionych na CPU. W ten sposób mogą to być sekrety, takie jak*

klucze prywatne wymagane przez TPM, ale nie powinny być dostępne dla innych, mogą być przechowywane w TEE, tworząc bardziej utrudniony dostęp dla hakerów.

Oprócz braku odporności na manipulacje, wadą TEE lub oprogramowania układowego TPM jest to, że w tym przypadku TPM jest zależny od wielu dodatkowych aspektów zapewniających jego bezpieczeństwo, w tym działania systemu TEE, błędy w kodzie aplikacji działającej w TEE itp."

Uwzględniając powyższe wyjaśnienia Zamawiającego, a także dowody przedłożone przez Przystępujących po stronie Zamawiającego, Izba w składzie orzekającym stwierdziła, że decyzję Zamawiającego o wprowadzeniu wymagania dotyczącego żądania aby oferowane urządzenia posiadały wbudowany *w płytę główną dedykowany moduł sprzętowy szyfrujący w standardzie TPM w wersji min. 2.0 z certyfikatem TCG tzw. Hardware TPM* należy uznać za podyktowaną dążeniem do zapewnienia najwyższego poziomu ochrony danym zawartym na zamawianych urządzeniach, tj. w stopniu uniemożliwiającym ich pozyskanie przez osoby nieuprawnione.

Podkreślić należy, że Zamawiający uzasadnił swoją decyzję o niedopuszczeniu określonego rozwiązania technicznego, tj. proponowanego przez Odwołującego rozwiązania fTPM, natomiast Odwołujący, na którym spoczywał ciężar dowodu, że zaskarżone postanowienia SIWZ narusza przepisy Pzp, nie zdołał podważyć zasadności takiego rozwiązania. Odwołujący nie udowodnił w żaden sposób, że brak jest istotnych różnic pomiędzy poziomem zabezpieczenia urządzeń. Ponadto wbrew twierdzeniom Odwołującego Zamawiający wykazał, że rozwiązanie TPM sprzętowe nie ogranicza konkurencji zarówno pomiędzy produktami jak i wykonawcami. Rozwiązanie to, jak wskazał Zamawiający stosuje wielu producentów komputerów m. in. DELL, HP, Lenovo, Apple, Acer, ASUS, Fujitsu (również serwery), Gigabyte (płyty główne), Intel, IBM, Toshiba, MSI posiadających w swojej ofercie w sumie kilkadziesiąt sztuk sprzętu w których TPM jest standardem w linii biznesowej. Odwołujący natomiast nie przedłożył żadnego dowodu potwierdzającego niemożność nabycia przez niego płyty głównej spełniającej wymagania Zamawiającego, np. od swojego partnera biznesowego Gigabyte, który jak wskazywał Zamawiający takie płyty oferuje. Twierdzenie Odwołującego co do trudności pozyskania takiego dowodu od ww. podmiotu Izba uznała za nieudowodnione, bowiem po pierwsze zauważyć należy, że Odwołujący miał ponad miesiąc czasu na pozyskanie takiego oświadczenia, a po drugie nie uprawdopodobnił, że o takie oświadczenie w ogóle występował. Zauważyć również należy, że zgodnie z „Rekomendacjami Prezesa Urzędu Zamówień Publicznych dotyczącymi udzielania zamówień publicznych na dostawę zestawów komputerowych" z marca 2021,

wprowadzone do SIWZ wymaganie nie tylko jest właściwe, ale forma wymagania przyjęta przez Zamawiającego wskazana jest jako rozwiązanie rekomendowane.

W konsekwencji powyższych rozważań Izba stwierdziła, że Odwołujący nie podważył uzasadnionych potrzeb Zamawiającego wyrażonych w opisie przedmiotu zamówienia i za nieuzasadnione uznała zarzuty naruszenia art. 29 ust. 1 i 2 w zw. z art. 7 ust. 1 Pzp.

Mając na uwadze powyższe orzeczono jak w sentencji.

O kosztach postępowania odwoławczego Izba orzekła na podstawie art. 557 i 575 Pzp z 2019 r. w zw. z § 8 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania z dnia 30 grudnia 2020 r. (Dz. U. z 2020r. poz. 2437).

Przewodniczący:……..

Członkowie: ……..

……..