Zarząd Transportu Miejskiego

Poznań, 11 sierpnia 2021 r.

Znak sprawy: ZTM.TD.3310.4.2021

Wszyscy zainteresowani Oferenci

Zarząd Transportu Miejskiego w Poznaniu, występujący jako Sprzedający w postępowaniu prowadzonym w trybie *Konkursu ofert na wybór Operatora systemu płatności za przejazd transportem publicznym za pomocą zbliżeniowych kart płatniczych i urządzeń mobilnych (m.in. telefonów komórkowych, smartwatchy, etc.) wykorzystywanych w charakterze kart płatniczych w pojazdach komunikacji miejskiej*, przedstawia poniżej odpowiedzi na pytania i wnioski złożone w ramach przedmiotowego postępowania.
Zarówno poniższe wyjaśnienia i stanowisko Sprzedającego, jak i treść ogłoszenia i załączników zmodyfikowana w wyniku udzielonych odpowiedzi staje się skuteczna i obowiązująca dla wszystkich uczestników postępowania.

Termin składania ofert upływa w dniu 31 sierpnia 2021 r. o godz. 15:00.

Treść zapytań wraz z wyjaśnieniami

Lp.	Pytanie/Wniosek	Odpowiedź/Stanowisko ZTM
1.	Zamawiający w ogłoszeniu wymaganiach konkursu w rozdziale III pkt. 3 d wymaga przedstawienia aktualnego certyfikatu PCI DSS. Pytanie 1. „W oparciu o ust. V pkt 10) Otwartego Konkursu Ofert Wykonawca wskazuje, że wymagania posiadania na dzień składania ofert i złożenia wraz z ofertę zgodnie z ust. III pkt 3 lit. d) tiret 3 certyfikatu PCI DSS jest wymaganiem nadmiernym mogącym naruszać regulacje z ustawy o zwalczaniu nieuczciwej konkurencji (art. 15) poprzez faworyzowanie konkretnego wykonawcy i uniemożliwianie wzięcia udziału w procedurze w sposób nieuprawnionym innym podmiotom. Wykonawca wskazuje, że oczekiwany certyfikat PCI DSS można uzyskać pod oferowane rozwiązanie, co jest możliwe dopiero przez wykonawcę, który ma realizować zamówienie. Wnioskowanie o taki certyfikat przez każdego z wykonawców stanowi nieuzasadnione żądania, ograniczające konkurencję. Realizacja przedmiotu konkursu jakim jest operatorstwo systemu płatności za przejazd w pojazdach Zamawiającego wymaga dostawy nie tylko usługi akceptacji płatności, ale również niezbędnego do tego celu sprzętu, jak też tego typu systemy pracują w dedykowanej i odseparowanej od innych tego typu wdrożeń infrastrukturze sprzętowo usługowej. Ta	Sprzedający dokonuje zmiany zapisu Komunikatu na str. 3. Rozdz. III pkt.3 lit d w następujący sposób: *„d) oferent złożył następujące oświadczenia i dokumenty:* • *aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,* • *w przypadku ofert składanych wspólnie przez oferentów – sposób reprezentacji podmiotów, gdy jest inny, niż wynikający z Krajowego Rejestru Sądowego lub innego właściwego rejestru – dokument potwierdzający upoważnienie do działania w imieniu oferenta (-ów),* • *oświadczenie o wykonaniu przynajmniej jednej usługi/ dostawy/ umowy*

POZnań
Zarząd Transportu Miejskiego, ul. Matejki 59, 60-770 Poznań
tel./fax +48 61 834 61 55, tel./fax +48 61 834 61 55 | ztm@ztm.poznan.pl | www.ztm.poznan.pl
|Nr rejestrowy BDO: 000138597

	infrastruktura powinna być utworzona na potrzeby dostawy i zgodnie z wymogami reguł akceptacji płatności będzie wymagała odrębnej certyfikacji PCI DSS. Wykonawca wnosi, aby Zamawiający przeniósł wymaganie przedstawione w ust. III pkt 3 lit. d tiret 3 na etap realizacji i sformułował je jako wymaganie docelowe, które zobliguje dostawcę do przeprowadzenia na uruchomionym dla Zamawiającego środowisku procesu certyfikacji PCI DSS, potwierdzonym stosownym certyfikatem w terminach zgodnych z wymogami norm organizacji płatniczych. Tym samym dopuści do postępowania potencjalnych wykonawców, którzy w chwili składania ofert nie posiadają certyfikacji PCS DSS co skutecznie rozszerzy grono potencjalnych Oferentów.”	*odpowiadającej przedmiotowi konkursu w okresie ostatnich 3 lat wraz z dokumentem potwierdzającym jej należyte wykonanie.”* Sprzedający informuje, iż kwestie dotyczące bezpieczeństwa transakcji zbliżeniowymi kartami płatniczymi (w tym certyfikacji i spełnienia wymogów międzynarodowych organizacji płatniczych, dostosowania wymagań i architektury proponowanego rozwiązania) zostaną określone na etapie negocjacji i uwzględnione w docelowej umowie.
2.	W nawiązaniu do Państwa odpowiedzi na pytanie nr 1 z dnia 5 sierpnia 2021 roku, dotyczącej wymogu przedstawienia certyfikatu PCI DSS jako obligatoryjnego warunku udziału w konkursie, Wykonawca pragnie wyjaśnić i doprecyzować, że w zeszłym roku wdrożył z sukcesem w jednym z większych polskich miast rozwiązanie transportowe w którym urządzenia mobilne zainstalowane w środkach transportu publicznego obsługują transakcję zbliżeniowymi kartami płatniczymi w dwóch następujących modelach (taryfach): 1. Known Fare w trybie Online (nomenklatura organizacji Visa) i 2. Mass Transit Trasaction (MIT) / Pay As You Go (PaYG) w trybie odroczonej autoryzacji płatności. W przypadku podróży z taryfą MTT/PaYG pasażer zobligowany jest tylko (bez wybierania na ekranie urządzenia jakichkolwiek opcji) do przykładania karty płatniczej zarówno przy wejściu (Check In) i wyjściu (Check Out). Rejestracja karty płatniczej w taryfie MTT/PaYG odbywa się w trybie odroczonej autoryzacji (offline). Oprogramowanie BackOffice na koniec dnia (okresu rozliczeniowego) w oparciu o zgromadzone (zarejestrowane) dane nt. przejazdów a także istniejącą taryfę biletową Organizatora Transportu, dokonuje automatycznego wyliczenia najkorzystniejszej opłaty (przy czym system nie pobierze nigdy więcej niż ustalony górny limit kwoty o równowartości biletu 24 godzinnego). W następnym kroku oprogramowanie BackOffice za pośrednictwem Agenta Rozliczeniowego (ACQ / Operatora Płatności) obciąża konto bankowe do którego przypisana jest karta płatnicza wyliczoną optymalną kwotą. Kontrola biletów odbywa się na certyfikowanym terminalu, do którego pasażer przykłada kartę a system weryfikuje online czy dla jej tokenu jest aktywny produkt/ produkty. W przypadku, kiedy na koncie bankowym nie ma środków, karta płatnicza trafia na tzw. Deny List (listę kart posiadających dług) i znajduje się na niej do momentu ściągnięcia zaległych środków. Do tego czasu korzystanie z karty płatniczej i taryfy MTT/PaYG w środkach transportu publicznego jest niemożliwe. Opisane powyżej referencyjne wdrożenie (po ustaleniu z samym	Sprzedający dokonuje zmiany zapisu Komunikatu na str. 3. Rozdz. III pkt.3 lit d w następujący sposób: *„d) oferent złożył następujące oświadczenia i dokumenty:* • *aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,* • *w przypadku ofert składanych wspólnie przez oferentów – sposób reprezentacji podmiotów, gdy jest inny, niż wynikający z Krajowego Rejestru Sądowego lub innego właściwego rejestru – dokument potwierdzający upoważnienie do działania w imieniu oferenta (-ów),* • *oświadczenie o wykonaniu przynajmniej jednej usługi/ dostawy/ umowy odpowiadającej przedmiotowi konkursu w okresie ostatnich 3 lat wraz z dokumentem potwierdzającym jej należyte wykonanie.”* Sprzedający informuje, iż kwestie dotyczące bezpieczeństwa transakcji zbliżeniowymi kartami płatniczymi (w tym certyfikacji i spełnienia wymogów międzynarodowych organizacji płatniczych, dostosowania wymagań i architektury proponowanego rozwiązania) zostaną określone na etapie negocjacji i uwzględnione w docelowej umowie.

	Klientem zostało wdrożone — system BackOffice na serwerach lokalnie u klienta) zbudowane zostało przy założeniu, bezwzględnego zakazu przetwarzania w systemie BackOffice numerów kart PAN (Permanent Account Number) stanowiących dane wrażliwe operując wyłącznie na tokenach tych kart. W zapisach OPZ powyższego zrealizowanego przez Wykonawcę postępowania można znaleźć jednoznaczne oczekiwania w zakresie bezpieczeństwa: . „...Zamawiający wyklucza konieczność certyfikacji oprogramowania BackOffice pod względem wymagań PA-DSS i PCI DSS; dane kartowe przesyłane z terminala EMV za pośrednictwem BackOffice do ACQ będą zaszyfrowane i dla oprogramowania BackOffice niedostępne..." . a także Zamawiający wyklucza konieczność certyfikacji swojego systemu i dostarczanego oprogramowania BackOffice z PCI DSS i PA-DSS, w związku z powyższym na żadnym etapie transakcji nie ma mieć styku z numerami kart płatniczych oraz innymi wrażliwymi danymi płatniczymi (kod PIN itp)..." Opisane i narzucone w powyższym postępowaniu przez Klienta podejście, w praktyce jest zgodne z regułami PCI DSS ponieważ poza certyfikowanym terminalem płatniczym unattended EMV i systemami ACQ nie przetwarza danych kartowych, a dodatkowo zastosowany sposób pozwala na wyłączenie rozwiązania z corocznych kosztownych audytów tzw. QSA (w Polsce tylko jedna firma może dokonywać takiej certyfikacji). Przedstawione rozwiązanie ze względu na fakt nieprzetwarzania danych wrażliwych kart płatniczych jest także zdecydowanie bezpieczniejsze ze względu na fakt, że nawet jeśli uda się komuś sforsować zabezpieczenia systemu BackOffice, nie dotrze do danych wrażliwych (nr PAN) ponieważ ich tam najzwyczajniej nie ma. Dane wrażliwe dotyczące płatności w takim systemie są przetrzymywane tylko przez podmioty związane prawem bankowym, oraz wymaganiami Organizacji Płatniczych za bezpieczeństwo transakcji tj.: ACQ, wystawca karty (BANK) i Organizacje Płatnicze. Oczywiście wspomniane podmioty podlegają pod prawo bankowe a także wymogi bezpieczeństwa PCI które określają reguły obsługi transakcji płatniczych i nigdy (pod groźbą wykluczenia ze strony samych organizacji płatniczych — Visa czy też Mastercard) nie zgodziłyby się na wdrożenie systemu, który jest rozwiązaniem niebezpiecznym. Wykonawca a także Operator Płatności, który był jego partnerem w opisanym postępowaniu w zakresie certyfikacji aplikacji płatniczej terminala unattended EMV a także procesowania transakcji płatniczych w taryfach KnownFare i MTT/PaYG, pomimo posiadanych referencji i doświadczenia w zakresie budowy tak innowacyjnego rozwiązania płatniczego (pierwsze rozwiązanie MTF/PaYG w Polsce) nie dysponuje oczekiwanym przez Zamawiającego certyfikatem przez co nie jest w stanie złożyć	

	oferty w rzeczowym konkursie. Opisany przez Zamawiającego wymóg certyfikatu wg najlepszej wiedzy Wykonawcy w zakresie transakcji kartowych spełnia w Polsce tylko jeden Merchant, który ze względu na architekturę swojego rozwiązania i fakt stosowania w kasownikach czytników EMV w wersji OEM (urządzenie bez własnej obudowy zabudowane jako płytką PCB wewnątrz kasownika) koduje numer karty (PAN) poza samym czytnikiem EMV. Opisane podejście i przetwarzanie nr karty płatniczej poza terminalem EMV wydaje się rozwiązaniem mniej bezpiecznym, a zatem wymusza konieczność przeprowadzania przez QSA audytów takiego rozwiązania celem weryfikacji podatności systemu na fraudy. Wdrożenie którego dokonał i omówił powyżej Wykonawca, nie przetwarza numerów kart płatniczych poza terminalem EMV (terminal ma zamkniętą obudowę tzw. blackbox z zabezpieczenia tamper które w przypadku nieautoryzowanego otwarcia unieruchamiają terminal), stokenizowane dane w sposób zakodowany są przesyłane do systemów ACQ w związku z powyższym wymóg audytu rozwiązania BackOffice pod kątem bezpieczeństwa staje się zbędny. Czy zatem biorąc pod uwagę przedstawioną powyżej argumentację oraz opis zrealizowanego wdrożenie, który w jasny, obrazowy sposób dowodzi, że oczekiwany przez Zamawiającego system można zrealizować w całkowicie bezpieczny sposób (całkowity brak dostępu do numerów PAN), a co za ty idzie brak konieczności certyfikacji PCI DSS, Zamawiający dopuści udział w konkursie Wykonawców posiadających referencje z wdrożenia takiego systemu (płatności zbliżeniowymi kartami płatniczymi w transporcie publicznym w trybie m.in. odroczonej autoryzacji płatności, w którym dane wrażliwe dot. kart płatniczych (PAN) nie są na żadnym etapie dostępne dla oprogramowania BackOffice) nie posiadających wymaganego certyfikatu PCI DSS ? Mając na uwadze powyższe informacje zdaniem Wykonawcy wymóg dotyczący certyfikatu PCI DSS w systemie o architekturze zapewniającej całkowite bezpieczeństwo, a opisanym powyżej jest wymaganiem ponadnormatywnym ograniczającym udział w konkursie podmiotom takim jak Wykonawca tj. posiadającym doświadczenie w realizacji innowacyjnych, oczekiwanych przez Zamawiającego całkowicie bezpiecznych rozwiązań płatniczych.	

Signed by / Podpisano przez:
Jan Paweł Gosiewski
Date / Data: 2021-08-11 12:40

……

Dyrektor ZTM