Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Biuro w Warszawie
ul. Adama Branickiego 13
02-972 Warszawa

Tel./Fax.
+48 22 574 88 50
+48 22 574 87 18

Warszawa, dnia 28.08.2019r.

Wykonawca:

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Adres korespondencyjny

ul. Branickiego 13
02-972 Warszawa
Tel: 22 574 88 50

Zamawiający:

Górnośląsko-Zagłębiowska Metropolia
ul. Barbary 21A
40-053 Katowice

Dotyczy: DIALOGU TECHNICZNEGO związanego z postępowaniem o udzielenie zamówienia publicznego na realizację zadania pt.: ***Serwer biletów elektronicznych na potrzeby mobilnych aplikacji sprzedażowych.***
Oznaczenie sprawy: ***ZA.270.2.2.2019***
.

Szanowni Państwo.

W nawiązaniu do ustaleń ze spotkania w dniu 21-09-2019 w załączeniu przesyłam dokument zawierający odpowiedzi Wykonawcy na pytania przedmiotowego Dialogu Technicznego oraz informuję, że Wykonawca wyraża zgodę na dołączenie tego dokumentu do protokołu postępowania.

Z poważaniem,

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Biuro w Warszawie
ul. Adama Branickiego 13
02-972 Warszawa

Tel./Fax.
+48 22 574 88 50
+48 22 574 87 18

Odpowiedzi Wykonawcy na pytania i zagadnienia postawione przez Zamawiającego w trybie Dialogu Technicznego prowadzonego przez Górnośląsko-Zagłębiowską Metropolię pn:

„Serwer biletów elektronicznych na potrzeby mobilnych aplikacji sprzedażowych”

Znak sprawy:
ZA.270.2.2.2019

Warszawa, sierpień 2019

NIP: 517-035-94-58, REGON: 180853177, KRS: 0000421310 Sąd Rejonowy Gdańsk - Północ w Gdańsku
VIII Wydział Gospodarczy Krajowego Rejestru Sądowego. Wysokość kapitału zakładowego 120 002 940,00 zł
Wysokość kapitału wpłaconego 120 002 940,00 zł

assecods.pl
kontakt@assecods.pl

1. **Proszę opisać lub jeżeli jest to możliwe przedstawić architekturę proponowanego rozwiązania.**

Architektura rozwiązania Serwer eProduktów zakłada istnienie części centralnej, osadzonej w chmurze prywatnej Zamawiającego, wykorzystującej również sprzętowe mechanizmu kryptograficzne (Serwer SAM), udostępniające usługi integracyjne (API) w postaci usług sieciowych REST.

Rozwiązanie jest zintegrowane przez API systemu ŚKUP (w zakresie pozyskiwania/aktualizacji definicji taryfy/biletów).

2. **Proszę opisać technologię proponowanego rozwiązania (np. z jakich komponentów będzie zbudowane rozwiązanie: m.in. system/y operacyjny, baza/y danych, Język/i programowania, Dockery, wirtualizacja, oprogramowanie pośrednie).**

Rozwiązanie oparte o architekturę mikrousługową zbudowane z dedykowanych komponentów rozwijanych w oparciu o technologie rodziny Java.

Wykorzystuje relacyjne jak również nierelacyjne silniki bazodanowe.

Rozwiązanie może być uruchomione na maszynach wirtualnych opartych na systemie operacyjnym RHEL/CentOS wykorzystując silnik konterneryzacji Docker zapewniającej klastrowanie i rozłożenie obciążenia dla poszczególnych komponentów rozwiązania.

3. **Czy możecie zaproponować rozwiązanie chmurowe oparte o własną chmurę?**

Tak, możliwe jest umieszczenie rozwiązania w ramach zasobów:

a) chmury hybrydowej Zamawiającego
b) chmurze Wykonawcy
c) chmurze zewnętrznego dostawcy

Każdy wariant ma określone cechy wdrożenia jak i różne koszty.

Możliwe jest też przejście na pełny SaaS, ale przy okrojonej (lub zmienionej) względem wymagań funkcjonalności (w szczególności w zakresie integracji ze ŚKUP).

4. **Czy występują płatne licencje lub ograniczenia ilościowe itp.?**

Zakłada się że istnieje płatna licencja lub subskrypcja dla dostarczanego oprogramowania aplikacyjnego lub usługi Wykonawcy (w zależności od wariantu zamówienia).

W ramach komponentów wspomagających (system operacyjny, konteneryzacja, baza danych itd.) wykorzystywane są technologie opensource nie wymagające dodatkowych płatnych licencji.

5. **Czy możliwe będzie skalowanie rozwiązania, jako parametr wydajności proszę wziąć pod uwagę liczbę transakcji (obszar danych) oraz ich jednoczesność (czas dostępu do usługi)?**

Tak, z uwagi na nowoczesną architekturę możliwość skalowania horyzontalnego.

Na etapie definiowania zamówienia niezbędne jest dodefiniowanie pojęć „liczba transakcji" oraz ich jednoczesność, w szczególności wskazanie poziomu wolumetrii dla którego wyskalowane ma być rozwiązanie.

Rekomendujemy aby konstrukcja rozwiązania przewidywała obok mechanizmu „on-line" również mechanizm dystrybucji identyfikatorów produktów off-line, na potrzeby obsługi sprzedaży w zewnętrznym kanale sprzedaży (aplikacji mobilnej). W taki sposób znacząco zmniejsza się wymagania na wydajność i dostępność usług centralnych – aplikacje sprzedażowe posługując się nadal bezpiecznymi i unikalnymi identyfikatorami produktów mogą pracować w znacznej autonomii od usługi centralnej – usuwa się silną zależność i kolejny punkt awarii w rozwiązaniu, przy czym biznesowo nadal oczekuje się posługiwania się przez aplikacje sprzedażowe jedynie identyfikatorami produktów udostępnionymi przez Serwer.

6. **Jakie możecie zaproponować zabezpieczenia (np., szyfrowanie, klucze, certyfikaty), oparte o jakie komponenty (software oraz hardware)?**

Komunikacja i transmisja danych jako taka – standardowo SSL/TLS 1.2+.

Do kodowania identyfikatora biletu – funkcja skrótu SHA256 32b

Do szyfrowania zawartości biletu – szyfrowanie symetryczne AES-192

Klucze kryptograficzne przechowywane w dedykowanym hardware systemu centralnego (karty SAM lub HSM).

7. **Czy będzie wykorzystywana szyna danych, jeżeli tak to jakie rozwiązanie?**

Wykorzystana jest koncepcja Mikrousług która zapewniając odpowiednie mechanizmy integracyjne nie wprowadza dodatkowego pojedynczego punktu awarii w postaci middleware typu „szyna danych/usług" który w dodatku musi być odpowiednio skalowany.

Występuje tutaj natomiast Broker wiadomości (Message Broker) działający głownie w oparciu o lekki protokół MQTT lub AMQP

Usługi integracyjne (API) wykonane będą analogicznie jak udostępniona przez Zamawiającego Platforma Integracyjna ŚKUP

8. **Jak zostaną zaprojektowane zapytania i odpowiedzi, np. SOAP, REST itp.?**

Usługi integracyjne (API) wykonane będą analogicznie jak udostępniona przez Zamawiającego Platforma Integracyjna ŚKUP

Zapytania i odpowiedzi w zakresie usług systemu centralnego: interfejs REST z danymi w formacje JSON

9. **Proszę opisać proponowane zabezpieczenia przed fraudami ze strony użytkowników aplikacji (np. QRcode, animowany gif, kod, itp.).**

Zabezpieczenie przed generowaniem identyfikatorów biletów przez nieautoryzowane generatory poprzez niejawną strukturę i kodowanie identyfikatora.

Zabezpieczenie przed przeniesieniem biletu na inny nośnik elektroniczny przez kodowanie biletu wraz z danymi „identyfikującymi" nośnik.

Zabezpieczenie przed wielokrotnym użyciem biletu jednokrotnego użycia przy braku komunikacji z systemem centralnym przez wykorzystanie rejestru udostępnionych identyfikatorów (weryfikacja on-line lub off-line).

Rozwiązanie adresuje m.in. poniższy zestaw fraudów ze strony Użytkowników:

Lp.	**Scenariusze - nośnik przechowuje metadane produktu (biletu):**
1.	Generowanie nowych biletów na podstawie sprzedanego biletu ze zmienionym identyfikatorem (identyfikatorem produktu)
2.	Przeniesienie blietu (dane) na inny nośnik
3.	Kopiowanie biletu (dane) na inny nośnik
4.	Kopiowanie biletu (obraz) na inny nośnik (np. zdjęcie w trakcie prezentacji QR kodu biletu tworzone na podstawie metadanych)
5.	Wielokrotne użycie jednego biletu niezgodne z jego definicja czyli np. wielokrotne pierwsze skasowanie

Lp.	**Scenariusze - nośnik przechowuje obraz produktu (biletu):**
1	Generowanie nowych biletów na podstawie sprzedanego biletu ze zmienionym identyfikatorem produktu
2	Kradzież biletu i użycie go przez nie uprawnioną osobę
3	Kopia biletu i użycie kopi biletu wcześniej niż uprawniona osoba
4	Kopia biletu i użycie kopi biletu poźniej niż uprawniona osoba
5	Kopia biletu i użycie kopi biletu niemal równocześnie z uprawnioną osobą
6	Wielokrotne użycie jednego biletu niezgodne z jego definicja czyli np. wielokrotne pierwsze skasowanie

10. Nie chcemy prezentować operatorowi numeru biletu, w jaki sposób go zaprezentować?

Numer biletu który podlega dystrybucji na zewnątrz jest zakodowany algorytmem jednostronnym (np. SHA-256).

Rozwiązanie wprowadzi pojęcie Identyfikatora Produktu który będzie unikalnym i bezpiecznym mechanizmem identyfikującym każdy sprzedany produkt z oferty GZM.

Jednocześnie należy zaznaczyć że identyfikator produktu to inne pojęcie niż GIT (identyfikator transakcji). Należy mieć świadomość realizacji transakcji koszykowych, w ramach których sprzedaży podlega wiele produktów. Identyfikator produktu ma za zadanie zapewnić rozliczalność systemu w zakresie cyklu życia produktu – od momentu zaoferowania do sprzedaży, przez zakup (w takim czy innym kanale) po użycie czy też zwrot.

Możliwa prezentacja wybranych elementów identyfikatora produkt w formie czytelnej dla człowieka lub systemów nie wymagających ścisłej integracji.

Każde zdarzenie spływające do systemu posługiwać się będzie identyfikatorem produktu umożliwiając Właścicielowi systemu docelowo pełny audyt i analitykę.

Rekomendowane rozwiązanie to dalsza integracja API ŚKUP (oraz kanałów sprzedaży przez nie integrowanych ze ŚKUP) z rozwiązaniem Serwera eProduktów.

11. Proszę opisać minimalny zestaw danych niezbędny do świadczenia usługi.

W przypadku zapotrzebowania na świadczenie usługi w modelu SaaS:

- Konfiguracja taryfy
- Konfiguracja integracji z API ŚKUP / F-K
- Wolumetria zdarzeń
- Użytkownicy z dostępem do raportów monitorowania

12. Zamawiający będzie wymagał integracji z systemem ŚKUP w zakresie Modułu Taryf i Cenników - MTC (pobieranie raz na dobę, z możliwością jego edycji), systemu księgowo-finansowego, Modułu Analityczno-Raportowego (MAR) – dane transakcyjne, z przeprowadzonych kontroli.

Wymaganie realizowalne.

W przypadku obsługi Taryf i Cenników: rekomendowane wdrożenie rozwiązania w taki sposób że GUI Serwera eProduktów przejmuje rolę jedynego interfejsu użytkownika dla zarządzania taryfą biletową, rozwiązanie jest zintegrowane z API ŚKUP tak że umożliwia zarówno pozyskanie informacji o obowiązującej definicji ale i umożliwia wykonanie eksportu zmian definicji do struktur ŚKUP umożliwiając wykorzystanie przez odpowiednie kanały sprzedaży.

13. **Propagacja informacji o biletach (serwer->klient czy inaczej).**

Z perspektywy technicznej będzie to złożenie „push" notification (tj. serwer -> klient) wraz z pobraniem aktualnego zestawu danych konfiguracyjnych lokalnego magazynu biletów (tj. klient -> serwer).

Bilety publikowane również w ramach mechanizmu off-line (publikacja rejestru wydanych identyfikatorów produktów) – również w trybie przyrostowym, z możliwością realizacji wydajnego cache po stronie mobilnej aplikacji.

14. **Propozycja zaimplementowania taryfy CICO, czy jest możliwa? (zintegrowanej z MTiC ŚKUP).**

Jest możliwe do realizacji przy czym zagadnienie wykracza z perspektywy architektury logicznej rozwiązania poza „Serwer Biletów" – w szczególności wymagana jest świadomość kontekstu podróży pasażera (możliwa do ustalenia w oparciu o API ŚKUP) oraz automatyzacja/wygoda rejestracji CiCo w aplikacji mobilnej.

Mechanizmu Serwera eProduktów mogą być jak najbardziej wykorzystane do zapewnienia wydajnego i bezpiecznego kanału przekazywania informacji o „tapnięciach" użytkownika (oddzielna kwestia – w jaki sposób wykonać) do systemu centralnego gdzie przez analogię do modeli MTT (i w integracji z modułem MTT) odbywa się obciążenie stosownej (powiązanej z kontem klienta) karty kredytowej.

Rekomendujemy wykonanie rozwiązania w formie referencyjnej w pierwszej kolejności w Mobilnej Aplikacji Pasażera ŚKUP dokumentując jednocześnie mechanizmy integracyjne i udostępniając je w drugiej kolejności innym dostawcom aplikacji mobilnych dla transportu zbiorowego.

15. **Integracja z kontrolerkami.**

Możliwość integracji:

- Kontrolerki z usługami centralnymi Serwera eProduktów (REST API) oraz ŚKUP (REST API)
- Kontrolerki z usługami lokalnymi Aplikacji Mobilnej:
    - możliwość użycia dedykowanej biblioteki która za pomocą NFC umożliwia komunikację Aplikacji Kontrolerki z Aplikacją Mobilną
    - wykorzystanie prezentowanego przez aplikację mobilną pasażera QR kodu generowanego w oparciu o bezpieczny mechanizm biblioteki Serwera eProduktów

16. **Raporty Real Time**

Część centralna na bieżąco gromadzi via API dane w modelu „transakcyjnym", możliwe wdrożenie raportów zbudowanych w oparciu o wyniki analizy przedwdrożeniowej adresując wymagania Zamawiającego – bazując na modelu danych rozwiązania Serwer eProduktów.

Wymaga dodefiniowania wolumetria raportów oraz zakres informacyjny oczekiwany przez klienta.

17. Raporty dzienne

Wykonane analogicznie jak w przypadku ŚKUP (RD/RS/DD/A1 etc.).

Możliwe wykorzystanie również interfejsu integracji SKUP (INT.FK – serwer SFTP z odpowiednią strukturą katalogów) – uproszczenie integracji z systemem Finansowo - Księgowym GZM.

18. Blokowanie sprzedaży

Jako podstawa należy wykorzystać mechanizm bezpiecznego (autoryzowanego przez GMZ) stempla czasu transakcji sprzedaży danego produktu w oparciu o referencyjną usługę serwera czasu ŚKUP. Kontrolerki zintegrowane również z serwerem czasu – kontrolerka wskazuje czy zakupu dokonano przed rozpoczęciem kontroli czy też już w jej trakcie. Kontrole mają wtedy charakter dyscyplinujący ale nie blokowana musi być fizycznie możliwość szybkiego kupienia biletu po pozyskaniu informacji przez pasażera o rozpoczęciu kontroli.

Kontrolerki raportują on-line fakt realizacji kontroli uprawnień na przejazd w konkretnym pojeździe.

Założyć należy że pasażerowie powinni być informowani za pomocą infrastruktury pojazdu (wyświetlacze informacji pasażerskiej / kasowniki) o godzinie rozpoczęcia kontroli.

Z pewnością kluczem do sukcesu jest odpowiedni regulamin precyzujący reguły postępowania (np. dozwolony zakup biletu w ciągu 1 minuty od rozpoczęcia kontroli, później już opłata dodatkowa.

Możliwe również wykonanie usług integracyjnych przekazujących informację z urządzenia kontrolerskiego do aplikacji pasażerów o rozpoczęciu kontroli (via system centralny, push-notification) przy czym problematyczne będzie ustalenie zbioru pasażerów do których skierowane powinno być takie powiadomienie (większość aplikacji nie posługuje się kontekstem konkretnej podróży w konkretnym pojeździe i nie wykonuje CheckIN). Dlatego tego typu mechanizm do zaplanowania po wypracowaniu modelu korzystania z biletów w kontekście przejazdu.

Sprzedaż realizowana w oparciu o bezpieczne usługi centralne które są „we władaniu" Klienta (GZM).

Istotną rolę będą miały „wymagania" dla aplikacji sprzedażowych (mobilnych) których zakres powinien obejmować również pewne istotne funkcjonalne cechy aplikacji mobilnych wykraczające poza techniczną jedynie sferę integracji z usługami Serwera eProduktów. W ramach takich wymagań należy zablokować możliwość długotrwałego przebywania aplikacji w stanie oczekiwania na sprzedaż biletu.

19. Diagnostyka

Z perspektywy usług centralnych Serwera eProduktów - możliwość wykorzystania mechanizmów Platformy Integracyjnej ŚKUP tj. narzędzia serwer logów.

Z perspektywy integrujących się klientów (np. aplikacji mobilnych) – opracowane wymagania integracyjne na wysyłanie szeregu metryk do serwera zarządzania/logowania.

20. Tokenizacja nr tel.

Możliwe uruchomienie takiej cechy rozwiązania.

W praktyce rekomendowane nie budowanie autorskiego algorytmu a użycie kodowania funkcją skrótu rodziny SHA-2 (np. SHA-256) co zapewnia należyty poziom zabezpieczenia przez dostępem do źródłowej informacji o numerze telefonu przez osoby postronne dając jednocześnie identyfikator do użycia w przetwarzaniu.

21. Jakie dane od użytkownika są niezbędne w aplikacjach sprzedających bilety elektroniczne?

Stokenizowane informacje o numerze telefonu i identyfikatorze konta użytkownika systemu sprzedażowego (danej aplikacji mobilnej).

22. Zarządzanie kluczami prywatnymi i publicznymi

W zależności od obszaru (komunikacja sieciowa, dostęp administracyjny, szyfrowanie biletów, autentykacja użytkowników, podpisywanie danych itd.) sposób zarządzania kluczami może być odmienny.

W obszarach masowych użyć kryptografii (jak np. szyfrowanie biletów) zakłada się przechowywanie kluczy w sposób zabezpieczony hardware'owo (SAM lub HSM)

23. Nr seryjne, git, identyfikacja biletu

Każdy bilet opatrzony jest unikalnym identyfikatorem który dodatkowo w przypadku publikacji na zewnątrz podlega zakodowaniu algorytmem uniemożliwiającym odtworzenie jego dokładnej wartości przez zewnętrzną aplikację (SHA-256)

Zakłada się stopniowe wykorzystywanie identyfikatora produktu w innych kanałach sprzedaży (np. USAD, nowe Kasowniki) tak aby docelowo zapewnić pełną rozliczalność i audyt systemu sprzedaży i korzystania z biletów elektronicznych (jednorazowych jak i długookresowych).

24. Ważność biletu do kontroli

Patrz pkt. 18.

Bilety „jednorazowe" sprzedawane są jako skasowane.

Rekomendowanym rozwiązaniem jest wprowadzenie po stronie aplikacji mobilnych możliwości sprawnego podania linii/pojazdu/kursu w ramach którego realizowana jest podróż (np. poprzez skan tagu NFC lub kodu QR umieszczonego w pojeździe).

Aplikacje kontrolerskie muszą mieć zapewniony interfejs umożliwiający szybkie odczytanie danych biletu z aplikacji sprzedażowej – np. kod QR biletu (przynajmniej w zakresie identyfikatora produktu oraz informacji i transakcji zakupu i podróży).

Aplikacje kontrolerskie muszą być zintegrowane z usługami Serwera eProduktów umożliwiając szybkie potwierdzenie autentyczności przedstawionego identyfikatora produktu (on-line lub off-line) oraz przedstawienie wyniku kontrolerowi.

Rekomendowane zbudowanie rozwiązania w taki sposób aby kontrolerki mogły pracować off-line.

25. QR kod z zaszyfrowaną informacją o transakcji

Technicznie zagadnienie jest realizowalne, przy czym GIT zakodowany tak aby nie było możliwe w prosty sposób jego odczytanie – np. SHA-256.

Założyć należy że mechanizm QR Code w przypadku aplikacji mobilnych może być używany do:

- wsparcia „maszynowej" identyfikacji konta klienta (zawierając zakodowany identyfikator klienta w systemie sprzedaży)
- wsparcia „maszynowej" identyfikacji produktu/biletu (zawierając zakodowany bezpieczny identyfikator produktu wraz z wybranymi metadanymi niezakodowanymi)
- wsparcia „maszynowej" identyfikacji transakcji sprzedaży w ramach której zakupiono dany produkt (z tym że transakcja sprzedaż jest innym obiektem niż produkt).

Kodowanie GIT (transakcji) nie zastąpi wprowadzenia bezpiecznego, unikalnego identyfikatora produktu

26. Zarządzanie podmiotami, przypisywanie biletów, prowizji, od kiedy, do kiedy

Funkcjonalność przewidziana do uruchomienia w ramach wdrożenia Konsoli Operatora

27. Sposób, warunki podłączania aplikacji sprzedających bilety (np. jak dojadę, skycash)?

Dostawcy aplikacji muszą wykonać integrację z mechanizmami SBE zgodnie z instrukcją integracji. Muszą poddać się testowi akceptacyjnemu (SiPT oraz oświadczenie o byciu zgodnym z wytycznymi).

28. Detekcja nadużyć

W sytuacji posługiwania się przez aplikacje sprzedażowe unikalnym bezpiecznym identyfikatorem produktu generowanym przez „trzecią stronę" tj, GZM możliwe jest za pomocą dość prostych raportów analizowanie i wykrywanie ew. nieprawidłowości/nadużyć w procesie dystrybucji biletów GZM.

Dodatkowo wartością podnoszącą bezpieczeństwo całego systemu będzie zintegrowanie pozostałych kanałów (kontrolerek, kasowników) umożliwiając spójną rejestrację całego cyklu życia produktu typu bilet.

Scenariusze nadużyć dla których projektowane jest rozwiązanie przedstawiono w innej części dokumentu. Zagadnienie do omówienia w trakcie spotkania dialogowego.

29. Backupowanie danych

Dane systemu centralnego podlegają backupowi na zasadach przyjętych dla ośrodka przetwarzania wspierającego system centralny. Nie przewiduje się dodatkowych mechanizmów backupu na poziomie aplikacyjnym.

W przypadku wdrożenia w chmurze Wykonawcy - założenia do ustalenia. Z uwagi na krytyczną rolę rejestru identyfikatora produktu – niezbędne zapewnienie trwałości.

30. Praca w klastrze

Możliwość pracy w chmurze hybrydowej. W ramach takiej architektury możemy mówić o klastrach silnika konteneryzacji rozciągniętych na maszynach fizycznych/wirtualnych oraz o bazodanowych klastrach active-pasive.

31. Możliwa integracja z urządzeniami

Mechanizmy integracji przygotowane w taki sposób że możliwe „natywne" zintegrowanie API ŚKUP a co za tym idzie w przyszłości kompletu urządzeń integrowanych via API ŚKUP z systemami wewnętrznymi/dziedzinowymi GZM.

Rozwiązanie zapewnić musi komplet usług integracyjnych (API) dla co najmniej:

- aplikacji sprzedażowych (głównie mobilnych), w tym zapewniając możliwość realizacji procesu sprzedaży on-line (wydajność i dostępność tego typu usług jest wtedy krytyczna)
- aplikacji kontrolerskich
- aplikacji back-office Zamawiającego (systemy finansowo-księgowe, rozliczeniowe, raportujące)

32. Wydajność rozwiązania

Odpowiednią wydajność rozwiązania umożliwiają następujące jego cechy:

1. Architektura umożliwiająca loadbalancing i skalowanie poziome
2. Preferowanie symetrycznych algorytmów szyfrujących
3. Mechanizmy archiwizowania danych historycznych
4. Asynchroniczne przetwarzanie danych tam gdzie to możliwe

Key Account Manager
Mariusz Szul