

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - MODERNIZACJA

ŚKUP 1.5 - Unowocześnienie systemu pobierania opłat za przejazdy publicznym transportem zbiorowym

Spis Treści.

1	Wprowadzenie	7
2	Indywidualne Konto Użytkownika (IKU)	9
2.1	Opis ogólny	9
2.2	Rodzaje kont	10
2.3	Migracja kont z systemu ŚKUP	17
2.4	Konto grupujące i firmowe	18
2.5	Możliwości rozwoju	19
2.6	Procesy	20
2.7	Dane /cechy powiązane z kontem	24
2.8	Informacje podstawowe powiązane z kontem	25
3	Identyfikatory pasażera	26
3.1	Opis ogólny	26
3.2	Rodzaje identyfikatorów	28
3.2.1	Karta ŚKUP 1.5	28
3.2.2	Karty z systemu ŚKUP	30
3.2.3	Aplikacja Mobilna ŚKUP 1.5 (MOB)	30
3.2.4	Karta EMV – zbliżeniowa i surogaty	30
4	Podsystem Użytkowników	32
4.1	Portal Klienta Systemu ŚKUP 1.5 (APK)	33
4.1.1	Funkcjonalność dostępna publicznie – Część informacyjna Portalu Klienta dla klienta niezalogowanego	33
4.1.2	Funkcjonalność dostępna po zalogowaniu (Indywidualne Konto Użytkownika) – Część do zarządzania kontem IKU	35
4.1.3	Funkcjonalność dostępna po zalogowaniu (Konto Grupujące) – Część do zarządzania kontem grupującym na Portalu Klienta	36
4.1.4	Funkcjonalność dostępna po zalogowaniu (Konto firmowe) – Część do zarządzania kontem firmowym na Portalu Klienta	37
4.1.5	Funkcjonalność dostępna po zalogowaniu się jako Administrator portalu – zarządzania treścią Portalu Klienta (dostęp przez moduł CRM)	38
4.1.6	Funkcjonalności związane z rozliczeniami	38
4.1.7	Wnioski o fakturę	39

4.1.8	Technologia	39
4.2	Aplikacja Mobilna ŚKUP (MOB)	40
4.2.1	Opis ogólny	40
4.2.2	Funkcjonalności Aplikacji Mobilnej	41
4.2.3	Dostęp do aplikacji	42
4.2.4	Funkcje dostępne dla użytkowników niezalogowanych	42
4.2.5	Funkcje dostępne dla użytkowników zalogowanych	42
4.2.6	Funkcjonalności związane z rozliczeniami	43
4.3	Moduł zarządzania relacjami z klientem (CRM)	45
4.3.1	Komunikacja z Użytkownikiem	45
4.3.2	Zarządzanie komunikatami	45
4.3.3	Zarządzanie wiadomościami	46
4.3.4	Pozostałe założenia	47
4.3.5	Reklamacje	47
4.3.6	Obsługi Call-Center	52
4.3.7	Funkcjonalności	52
4.3.8	IVR (ang. interactive voice response)	53
5	Podsystem Sprzedaży	55
5.1	Moduł taryf i Cenników (MTC)	56
5.1.1	Architektura MTC	57
5.1.2	Funkcjonalności	58
Raport 0.	dotyczący zdefiniowanych, obowiązujących oraz nieaktywnych biletów/taryf	65
Raport 1.	sprzedaży kontraktu/usługi/biletu	65
Raport 2.	transakcji sprzedaży usług	66
Raport 3.	sprzedaży dla agentów sprzedaży:	67
	Metrobilet i inne oferty specjalne:	68
Raport 4.	szczegółowy ze sprzedaży	68
Raport 6.	szczegółowy z rozpatrzonych reklamacji dot. np. metrobiletu lub innej oferty specjalnej, wymagane co najmniej pola:	69
Raport 7.	dot. promocji	69
Raport 8.	ze skasowań biletów/wnoszenia opłat w kasownikach zamontowanych w pojazdach. 70	
Raport 9.	użycia identyfikatora:	71

Raport 10.	dla konta IKU:	72
Raport 11.	zwrotów biletów:.....	72
Raport 12.	z elektronicznego magazynu biletów dla systemu ŚKUP 1.5 (MTC-magazyn)	73
Raport 13.	szczegółowy z wygenerowanych biletów przekazanych dla poszczególnych sprzedawców zaopatrywanych przez odbiorcę raportu,	73
	powinien posiadać informację o statusie każdej transakcji tj. np.: poprawna, niepoprawna, wymagane co najmniej pola:.....	74
5.2	Aplikacja dla Punktów Obsługi Pasażera (APO).....	75
5.2.1	Funkcjonalności	75
5.2.2	Funkcjonalności związane z rozliczeniami.....	77
5.3	Moduł Dystrybucji Kart ŚKUP (MDYS)	78
5.3.1	Funkcjonalności	78
5.4	Moduł Rozliczeń Transakcji i Tokenizacji (MRTT)	80
5.4.1	Model Rozliczeń Pieniężnych	82
5.4.2	Funkcjonalność modułu MRTT	82
5.4.3	Podstawowe procesy realizowane przez moduł MRTT	84
5.4.4	Raportowanie	85
6	Podsystem Infrastruktury	92
6.1	Procesy	94
6.2	Aplikacje Obsługi Żądań (AOZ)	97
6.2.1	Aplikacja Obsługi Żądań dla pojazdów (AOZ-pojazd)	98
6.2.2	Aplikacje Obsługi Żądań dla automatów (AOZ-SADiS)	100
6.2.3	Aplikacje Obsługi Żądań dla kontrolerki (AOZ-UKNT)	106
6.2.4	Aplikacje Obsługi Żądań dla urządzeń u agentów sprzedaży (AOZ-UPOS).....	109
6.3	Infrastruktura wyniesiona - urządzenia.....	114
6.3.1	Infrastruktura pojazdowa	115
6.3.1.1	Uniwersalny Komputer pokładowy (UKP)	116
6.3.1.3	Zestawienie ilościowe.....	124
6.3.2	Kontrolerka (UKNT)	124
6.3.3	Terminal Sprzedażowy (UPOS)	135
6.3.4	Stacjonarny Automat Dystrybucji i Sprzedaży (SADiS)	136
6.3.5	Wyposażenie POP.....	143
6.3.6	Centra przesiadkowe P&R	144

6.4	SAM serwer (HSM)	145
6.4.1	Zarządzanie kluczami.....	145
6.5	Moduł Backupu	147
6.6	Moduł Monitoringu (MMT).....	148
6.7	Moduł Zarządzania Uprawnieniami (AD)	149
7	Podsystem Danych	153
7.1	Moduł Zarządzania Rozkładami Jazdy (MRJ).....	154
7.2	Moduł Wymiany Danych i Integracji (MWD)	156
7.2.1	Stos technologiczny	156
7.2.2	Obszary funkcjonalności	156
7.2.3	Certyfikacja	157
7.2.4	Kluczowe założenia API	158
7.2.5	Zakres funkcjonalny API	159
7.2.6	Założenia architektoniczne API systemu centralnego ŚKUP	160
7.3	Moduł Zarządzania Bazami Danych (MDB)	162
7.4	Moduł Analityczno - Raportowy (MAR).....	163
8	Migracja danych	166
9	MaaS.....	168
10	Bezpieczeństwo	169
10.1	Audyt bezpieczeństwa.....	169
10.2	Inwentaryzacja aktywów IT	170
10.3	Klasyfikacja informacji	170
10.4	Kontrola dostępu.....	171
10.5	Kryptografia.....	171
10.6	Separacja środowisk.....	172
10.7	Procedury operacyjne	172
10.8	Zarządzanie zmianą	172
10.9	Bezpieczeństwo obsługi płatności kart płatniczych EMV	173
10.10	Zarządzanie potencjałem wykonawczym	173
10.11	Monitorowanie i logowanie	173
10.12	Bezpieczeństwo aplikacji	174
10.13	Wymagania dot. realizacji obowiązków administratora danych oraz praw osób, których dane będą przetwarzane w systemie informatycznym.....	175

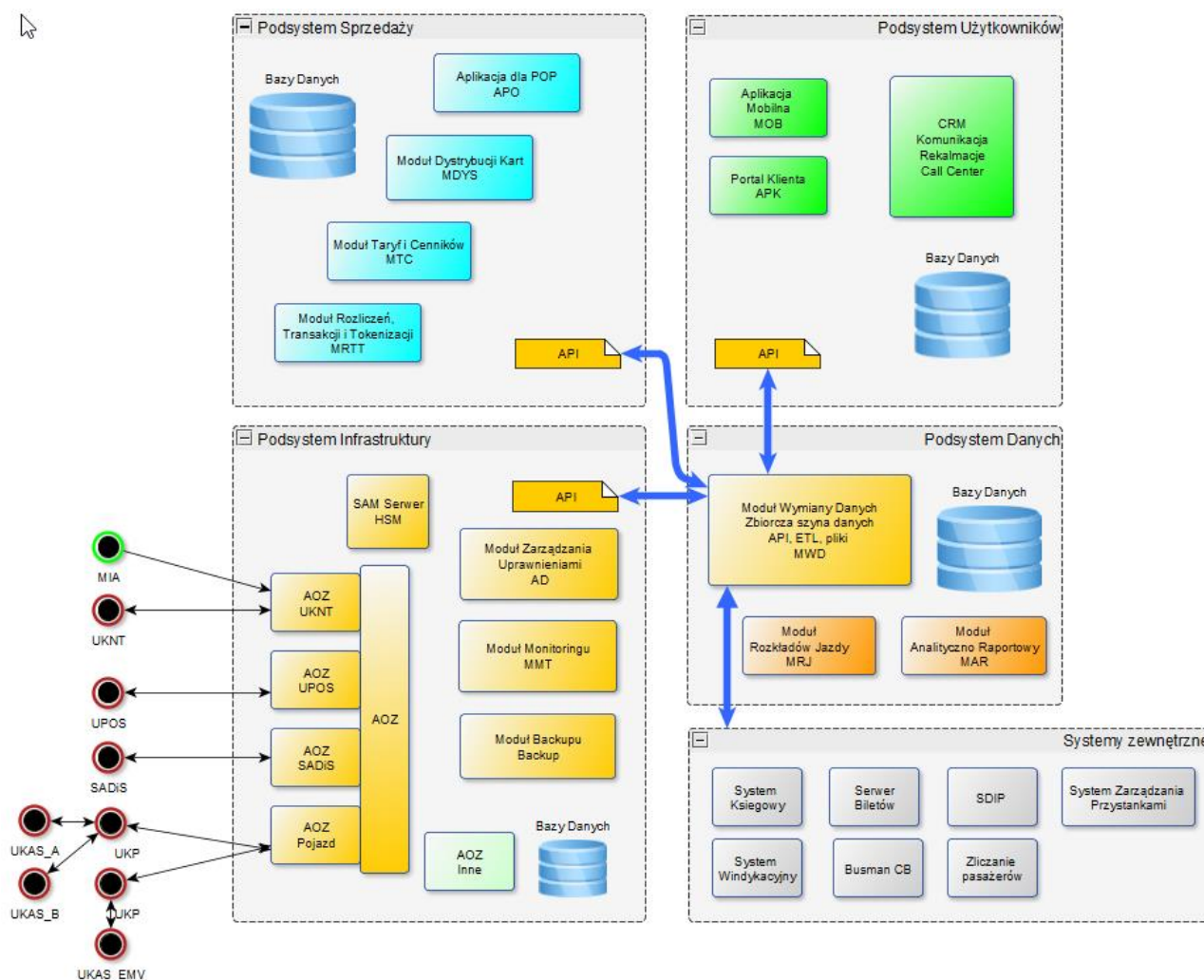
11	Stos technologiczny.....	182
11.1	Architektura.....	182
11.2	Zasoby chmurowe	182
11.3	Łączność.....	185
11.4	Oprogramowanie	186
11.5	Uwzględnione standardy danych	186
11.6	Analiza bezpieczeństwa.....	188
11.7	Systemy operacyjne	189
11.8	Serwery WWW	189
11.9	Interfejs graficzny oprogramowania	190
11.10	Aplikacje Mobilne.....	190
11.11	Aplikacje WEB.....	190
11.12	Urządzenia infrastruktury wyniesionej (UKP, UKAS, UKAS-EMV, UKNT, SADiS, UPOS) ..	191
11.13	Bazy danych.....	191
11.14	Migracja do innego centrum przetwarzania	191
12	Licencje, prawa autorskie.....	193
12.1	Oprogramowanie dedykowane.....	193
12.2	Oprogramowanie standardowe:	193
12.3	Oprogramowanie narzędziowe	193
12.4	Dokumenty i inne utwory.....	194
13	Dokumentacje i repozytoria	195
13.1	Repozytoria	197
14	Szkolenia.....	199
14.1	E-Learning.....	201

1 Wprowadzenie

Przedstawione w dokumencie, nazwy oraz opisy modułów, aplikacji i interfejsów, stanowią jedynie logiczne odwzorowanie pogrupowanych funkcjonalności. Rolą Wykonawcy jest zaproponować docelowy układ, nazewnictwo tworzonego oprogramowania oraz nadać im funkcjonalności i cechy opisane w OPZ oraz dodatkowo nadać im cechy realizowalności. Zamawiający informuje, że poniższe opisy stanowią jedynie podstawę do stworzenia przez Wykonawcę kompletnych rozwiązań i mają charakter nakierunkowujący Wykonawcę na oczekiwania Zamawiającego. Przedstawione funkcjonalności i nazewnictwo mogą się pokrywać z nazewnictwem i funkcjonalnością obecnego systemu ŚKUP.

Zamawiający oczekuje od Wykonawcy stworzenia opisywanych funkcjonalności poprzez modernizację obecnie eksploatowanego oprogramowania (o ile pozwalają na to zapisy licencyjne lub posiadane przez Zamawiającego prawa autorskie i kody źródłowe) – szczegółowy wykaz posiadanych praw i licencji znajduje się w **załączniku nr 3.1 do OPZ – „Wykaz oprogramowania ŚKUP”** lub wytworzenie oprogramowania od nowa na podstawie posiadanych opisów, dokumentacji oraz na podstawie uzgodnień z Zamawiającym. Zamawiający oczekuje od Wykonawcy przedstawienia kompletnej architektury systemu oraz koncepcji realizacji poszczególnych jej elementów (KIAS), przed przystąpieniem do części realizacyjnej. W przypadku oprogramowania, co do którego Zamawiający nie posiada prawa do modyfikacji, należy zaproponować w jego miejsce nowe oprogramowanie wraz z kodami źródłowymi i prawem do modyfikacji.

Zamawiający oczekuje, przekazania kodów źródłowych i licencji niewyłącznej z prawem do modyfikacji dla wszystkich komponentów systemu.



Rysunek 1. Poglądowy rysunek architektury systemu wraz z podziałem na podsystemy

Zamawiający oczekuje, podziału architektury systemu na odizolowane i niezależne od siebie podsystemy. Każdy podsystem musi być niezależny od siebie w zakresie architektury serwerowej tzn. w obrębie jednego dostawcy usług chmurowych, ale osobna grupa zasobów (serwery, zasoby dyskowe, warstwa sieciowa, usługi, osobne uprawnienia, bazy danych, API). Podsystemy będą integrowane ze sobą na poziomie interfejsów i API w sposób analogiczny jak miałyby to miejsce dla systemów zewnętrznych.

2 Indywidualne Konto Użytkownika (IKU)

2.1 Opis ogólny

Z konta IKU będzie mógł korzystać każdy użytkownik systemu ŚKUP 1.5. Na Indywidualnym Koncie Użytkownika (IKU) będą zapisywane i przechowywane wszystkie dane dotyczące użytkownika systemu (reprezentowanego przez identyfikatory) oraz uprawnień przez niego zakupionych (np. bilety) lub nabytych (np. ulgi), informacja o punktach zgromadzonych na koncie IKU (e-portmonetka) oraz innych aktywnościach użytkownika w systemie. Konto będzie mogło być zarządzane:

- **samodzielnie** przez użytkownika w następujących kanałach: Portal Klienta, Aplikacja Mobilna ŚKUP 1.5, SADiS (w ograniczonym zakresie);
- **przez obsługę** w Punkcie Obsługi Pasażera (aplikacja APO) oraz Call-Center (ACC) w ograniczonym zakresie.

Do konta będzie można podpiąć różne identyfikatory pasażera jednak, aby można było z niego aktywnie korzystać będzie musiał być podpięty do niego co najmniej jeden identyfikator. Tylko jeden z wielu przypisanych do konta identyfikatorów, może być aktywny w danym dniu. Zmiana aktywnego identyfikatora może być wykonywana tylko wg parametryzowanych w systemie reguł (np. tylko raz na dzień i tylko przed jego pierwszym użyciem w danym dniu). Do danego konta IKU można przypiąć po jednym identyfikatorze z każdego rodzaju (ograniczenie nie dotyczy identyfikatorów, które wygasły, te nie wliczają się do limitu).

Każde konto będzie posiadało indywidualny, niepowtarzalny login składający się z cyfr oraz hasło dostępowe zmieniane przez użytkownika. Ilość cyfr w loginie oraz minimalny poziom skomplikowania hasła rozumianego jako minimalna ilość znaków i minimalny rodzaj znaków (cyfry, litery małe i duże, znaki specjalne) zaproponuje Wykonawca adekwatnie do poziomu ryzyka (wraz z jego uzasadnieniem) - propozycja Wykonawcy wymaga akceptacji przez Zamawiającego. Analizę i zarządzanie ryzykiem, w tym określenie podatności, wdrażanie zabezpieczeń, raportowanie są w gestii Wykonawcy. Login będzie posiadał cyfrę kontrolną, algorytm wyliczania cyfry kontrolnej zaproponuje Wykonawca. Algorytm ten podlega akceptacji Zamawiającego. Wykonawca ponosi pełną odpowiedzialność za bezpieczeństwo systemu i w razie skompromitowania systemu, Wykonawca będzie zobowiązany do wprowadzenia stosownych zmian w systemie (bez dodatkowego wynagrodzenia).

2.2 Rodzaje kont

Lp.	Rodzaje Kont	Wymagania		Identyfikatory
		podstawowe	do aktywacji tego rodzaju konta	
1	nieprofilowane	wymaga posiadania identyfikatora	nie wymaga aktywacji, zakładane automatycznie w przypadku: 1. pierwsze użycie karty EMV albo 2. pozyskanie lub migracja karty ŚKUP/ŚKUP1.5	I. Karta EMV II. Karta ŚKUP1.5 III. Karta ŚKUP niespersonalizowana
2	profilowane	dodatkowo ujawniany jest login (identyfikator konta), zdefiniowanie hasła, adresu email/numeru tel. komórkowego , opcjonalnie aliasu do konta <i>*może zostać założone bez identyfikatora na określony czas</i>	1. weryfikacja adresu email lub 2. weryfikacja numeru telefonu (przez kod SMS)	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Aplikacja mobilna na telefon ŚKUP1.5 <i>* bez identyfikatora – przez określony czas</i>
3	profilowane imienne	dodatkowo wymaga podania imienia, nazwiska, zdjęcia, nr PESEL <i>*może zostać założone bez identyfikatora na określony czas</i>	1. osobiście lub przez pełnomocnika z dokumentem tożsamości w Punkcie albo 2. zdalnie z wykorzystaniem profilu zaufanego lub innej bezpiecznej metody weryfikacji tożsamości albo 3. W procesie migracji danych ze ŚKUP albo <i>innej niezaprzeczalnej metody weryfikacji zaproponowanej przez Wykonawcę</i>	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana V. Aplikacja mobilna ŚKUP 1.5 na telefon <i>* bez identyfikatora – przez określony czas</i>
4	nieprofilowane imienne	wymaga posiadania identyfikatora wymaga podania imienia, nazwiska, zdjęcia, nr PESEL	1. osobiście lub przez pełnomocnika z dokumentem tożsamości w Punkcie albo <i>innej niezaprzeczalnej metody weryfikacji zaproponowanej przez Wykonawcę</i>	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana
5	archiwalne	wygasła ważność lub został odpięty od konta ostatni	<i>do reaktywacji konta należy podpiąć nowy identyfikator</i>	brak

		ważny/aktywny identyfikator		
--	--	--------------------------------	--	--

Tabela 1. Rodzaje kont w systemie ŚKUP 1.5 – wymagania proceduralne

Bazowym rodzajem konta, będzie konto nieprofilowane. Nie będzie ono wymagało wprowadzenia żadnych danych przez użytkownika, będzie natomiast posiadało nadany automatycznie przez system login. Znajomość loginu nie jest wymagana do posługiwania się tym kontem przez użytkownika. Konto takie zakładane będzie automatycznie przez system dla każdego identyfikatora, który zaistnieje w systemie, nie przypisanego wcześniej do żadnego innego konta (np. karta EMV). Konto to będzie powiązane tylko z jednym identyfikatorem (z wyjątkiem surogatów karty EMV) oraz będzie umożliwiało doładowanie i zwrot niewykorzystanych punktów (z wyjątkiem kont do których jest podpięta wyłącznie karta płatnicza EMV). Na takim koncie (wyłącznie z kartą płatniczą) będzie można zakodować tylko bilety na okaziciela. Dla karty płatniczej będzie można skorzystać z taryfy CICO wyłącznie obciążając kartę płatniczą. Dla kont z dodatnim, odpowiednim saldem punktowym będzie można skorzystać z taryfy CICO. Jako funkcjonalność dodatkowa będzie istniała możliwość: wygenerowania historii operacji, złożenia wniosku o fakturę (wprowadzając wszystkie niezbędne dane), złożenia reklamacji (wprowadzając wszystkie niezbędne dane), zmiana i reset PIN-u do powiązanych kart ŚKUP i ŚKUP 1.5, zasilenia i zwrot salda punkowego oraz przekształcenia konta w konto profilowane.

Dla karty płatniczej i jej surogatów wykorzystanej do zapłaty za przejazd po raz pierwszy, konto IKU będzie utworzone automatycznie przez system i identyfikowane przez token karty lub login. Dostęp do konta będzie możliwy dla posiadacza tego identyfikatora zdalnie poprzez Portal Klienta oraz w Punktach Obsługi Pasażera. Na Portalu Wykonawca zapewni oprogramowanie pozwalające na tokenizację karty EMV, co umożliwi identyfikację karty oraz jej surogatów i w konsekwencji powiązanie z kontem i operacjami przechowywanymi w systemie, a w konsekwencji realizowanie funkcjonalności powiązanych z kontem IKU.

W Punktach Obsługi Pasażera użytkownik karty EMV lub surogatu będzie przykładał identyfikator do czytnika, który przy pomocy odpowiedniego oprogramowania (dostarczonego przez Wykonawcę wraz z czytnikiem) zapewni wygenerowanie tokena dla karty EMV i w konsekwencji do operacji wykonanych dla tego konta.

Dla kart ŚKUP 1.5 podczas ich wydawania zostanie utworzone konto powiązane z tym identyfikatorem i z startowym PIN-em do karty. W trakcie wydawania karty PIN może zostać zmieniony przez użytkownika. Startowy PIN może zostać wydrukowany na potwierdzeniu wydania karty w przypadku nie nadania PIN-u przez użytkownika. Dostęp do konta dla tego identyfikatora będzie możliwy zgodnie z opisem przedstawionym w tabeli nr 2 Rodzaje kont w systemie ŚKUP 1.5 – kanały dostępowe.

LP	Rodzaje Kont	Identyfikatory	Uzyskanie dostępu do konta z wykorzystaniem kanału				
			Portal	Aplikacja Mobilna ŚKUP (MOB)	SADiS	Punkty obsługi POP	Agenci sprzedaży (Kioski)
1	nieprofilowane	I. Karta EMV II. Karta ŚKUP1.5 III. Karta ŚKUP niespersonalizowana	Dla I. numer karty zamieniony na token (wykonuje aplikacja) Dla II. numer karty + PIN Dla III. Alias lub numer karty i hasło lub PIN z ŚKUP (migracja) <i>istnieje możliwość sprofilowania konta</i>	brak	Dla I. brak Dla II. i III. zbliżenie karty do czytnika	Dla I. numer karty zamieniony na token (wykonuje czytnik) Dla II. i III. numer karty + PIN lub zbliżenie karty do czytnika <i>istnieje możliwość sprofilowania konta</i>	Dla I. brak Dla II. i III. zbliżenie karty do czytnika
2	profilowane	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Aplikacja mobilna na telefon ŚKUP1.5	login/alias i hasło;	login/alias i hasło	Dla I - brak II, III zbliżenie identyfikatora do czytnika	Dla I, II III - zbliżenie identyfikatora do czytnika lub login (identyfikator konta) + (Kod SMS/email)	Dla I-brak II,III zbliżenie identyfikatora do czytnika
3	profilowane imienne	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana V. Aplikacja mobilna ŚKUP 1.5 na telefon	login/alias i hasło;	login/alias i hasło	Dla I-brak II, III, IV zbliżenie identyfikatora do czytnika	Dla I, II, III, IV zbliżenie identyfikatora do czytnika lub PESEL + (Kod SMS/email)	Dla I-brak II, III, IV zbliżenie identyfikatora do czytnika
4	nieprofilowane imienne	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana	Dla II. numer karty + PIN Dla III., IV Alias lub numer karty i hasło lub PIN z ŚKUP (dotyczy tylko danych migrowanych z systemem ŚKUP 1.0) <i>istnieje możliwość sprofilowania konta</i>	brak	Dla I-brak II, III IV zbliżenie identyfikatora do czytnika	1. zbliżenie identyfikatora do czytnika 2. PESEL	Dla I-brak II, III, IV zbliżenie identyfikatora do czytnika
5	archiwalne	brak	1. login/alias i hasło	1. login/alias i hasło	brak	PESEL + (Kod SMS/email)	brak

Tabela 2. Rodzaje kont w systemie ŚKUP 1.5 – kanały dostępne

Konto profilowane może zostać utworzone przy wydawaniu identyfikatora (w POP) lub z przekształcenia konta nieprofilowanego (w POP, na Portalu Klienta) lub przy uruchamianiu Aplikacji mobilnej ŚKUP 1.5. Będzie wymagało dodatkowo podania przez użytkownika co najmniej: **hasła** i do wyboru **adresu e-mail** lub **numeru telefonu** do przesyłania kodów SMS. Przy zakładaniu tego rodzaju konta ujawniany jest **login**. Może być również zdefiniowany **Alias** do loginu konta. Alias musi być unikatowy w całym systemie ŚKUP 1.5 – struktura aliasu (grupa znaków i ich ilość) ma być adekwatna do poziomu ryzyka wynikającego z przeprowadzonej analizy przez Wykonawcę i powinna dopuszczać co najmniej cyfry, małe i duże litery. Konto to będzie posiadało znacznie więcej funkcjonalności niż konto nieprofilowane, w tym możliwość przypinania i zarządzanie wieloma identyfikatorami, reset hasła realizowane zgodnie z procedurą polegającą na przestaniu na przypisany do konta adres mailowy aktywnego linka (aktywowanego tylko raz, ważnego nie dłużej niż przez czas określony parametrem w systemie) do nadania nowego hasła, otrzymywanie powiadomień na maila lub na telefon (SMS-em oraz Aplikacji Mobilnej ŚKUP 1.5) oraz możliwość obsługi w Aplikacji Mobilnej ŚKUP 1.5. oraz będzie umożliwiało doładowanie i zwrot punktów. Nie będzie posiadało funkcjonalności związanych z identyfikacją użytkownika (np. bilety imienne). Wykaz minimalnych dostępnych funkcjonalności znajduje się w Tabeli nr 4.

*- konto może zostać utworzone w Portalu klienta bez identyfikatora na określoną parametrem ilość dni. Parametr będzie definiowany przez administratora Zamawiającego i może wynosić również 0 (zero). Dla tego konta nie można zasilić e-portmonetki bez podłączenia identyfikatora w postaci karty ŚKUP, SKUP 1,5 lub aplikacji mobilnej MOB.

Lp.	Rodzaje Kont	Identyfikatory	Dostępne bilety (dla poszczególnych identyfikatorów)			
			krótko i średnio okresowe	CICO	okresowe na okaziciela	okresowe imienne
1	nieprofilowane	I. Karta EMV II. Karta ŚKUP2 III. Karta ŚKUP niespersonalizowana	I. Tak (tylko w systemie dla MZK-płatność EMV) II, III Tak	I. Tak (tylko w systemie dla MZK- płatność EMV) II, III Tak	Tak	Nie
2	profilowane	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Aplikacja mobilna na telefon ŚKUP 1.5 -MOB	I Tak (tylko w systemie dla MZK-płatność EMV)) II, III, IV, Tak	I. Tak (tylko w systemie dla MZK- płatność EMV) II, III IV Tak	Tak	Nie
3	profilowane imienne	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana	I Tak (tylko w systemie dla MZK-płatność EMV)) II, III, IV, V Tak	I. Tak (tylko w systemie dla MZK- płatność EMV)	Tak	Tak

		V. Aplikacja mobilna ŚKUP 1.5 na telefon -MOB		II, III, IV, V Tak		
5	nieprofilowane imienne	I. Karta EMV II. Karta ŚKUP 1.5 III. Karta ŚKUP niespersonalizowana IV. Karta ŚKUP spersonalizowana	I Tak (tylko w systemie dla MZK-płatność EMV)) II, III, IV Tak	I. Tak (tylko w systemie dla MZK- płatność EMV) II, III, IV Tak	Tak	Tak
6	archiwalne	brak	Nie	Nie	Nie	Nie

Tabela 3. Rodzaje kont w systemie ŚKUP 1.5 – dostępność identyfikatorów i biletów

Konto profilowane imienne również może zostać utworzone w POP od razu podczas wydawania identyfikatora lub z przekształcenia konta profilowanego w POP lub na Portalu Klienta lub w Aplikacji Mobilnej. Do utworzenia tego konta wymagane jest dodatkowo powiązanie z kontem danych użytkownika takich jak **imię, nazwisko, zdjęcie** i **PESEL** (przechowywane w postaci zaszyfrowanej). Dane te muszą zostać zweryfikowane przez operatora lub z wykorzystaniem metody automatycznej weryfikacji tożsamości dostarczonej przez Wykonawcę (np. profil zaufany). W ramach prac rozwojowych system musi dopuszczać możliwość wprowadzenia innych metod weryfikacji tożsamości w razie pojawienia się takich możliwości. Dopiero pozytywna weryfikacja tożsamości będzie umożliwiała funkcjonowanie konta profilowanego imiennego. Na takim koncie będzie można (poza funkcjami dostępnymi na koncie profilowanym) zapisywać i przechowywać uprawnienia spersonalizowane takie jak bilety imienne i uprawnienia do ulg. Będzie również możliwość zidentyfikowania użytkownika konta w POP z wykorzystaniem dokumentu tożsamości. W systemie ŚKUP 1.5 nie mogą istnieć dwa aktywne konta IKU z tym samym numerem PESEL.

Lp.	Rodzaje Kont	Podstawowa funkcjonalność dodatkowa (poza biletami)	
		funkcjonalność	warunki i cechy funkcjonalności
1	nieprofilowane	a) pobranie historii użycia na Portalu, w POP i w SADiS (tylko wyświetlenie), b) złożenie reklamacji osobiście lub przez pełnomocnika na Portalu i w POP, c) złożenie wniosku o fakturę na Portalu i w POP d) zmiana lub reset PIN identyfikatora (tylko dla kart ŚKUP i ŚKUP 1.5) e) zasilenie i korzystanie z e-portmonetki	a) tylko dla jednego identyfikatora, identyfikator ten musi być aktywny b) podanie wszystkich danych niezbędnych do przyjęcia reklamacji w tym danych osobowych, c) podanie wszystkich danych odbiorcy i płatnika faktury d) na podstawie znajomości dotychczasowego PIN albo (tylko w POP) potwierdzenia wydania identyfikatora lub pisemnego oświadczenia użytkownika. e) tylko dla identyfikatorów innych niż karta EMV
2	profilowane	a) pobranie historii użycia na Portalu, w POP, w Aplikacji mobilnej, b) złożenie reklamacji osobiście lub przez pełnomocnika na Portalu w Aplikacji mobilnej i	a) dla wielu identyfikatorów podłączonych do konta w tym dla identyfikatorów które utraciły ważność lub zostały zablokowane, b) możliwość zdefiniowania domyślnych danych

		<p>w POP, śledzenie stanu i otrzymywanie odpowiedzi na reklamacje w kanałach elektronicznych</p> <p>c) złożenie wniosku o fakturę na Portalu w Aplikacji mobilnej i w POP</p> <p>d) podłączenie i zarządzania kilkoma identyfikatorami w Portalu klienta i w Aplikacji mobilnej,</p> <p>e) otrzymywania powiadomień o zdarzeniach związanych z kontem (IKU) na adres email lub SMS-em,</p> <p>f) możliwość stworzenia konta grupującego lub włączenia konta użytkownika (IKU) do już istniejącego konta grupującego oraz możliwość odpięcia konta IKU od konta grupującego,</p> <p>g) zdefiniowanie aliasu do konta IKU</p> <p>h) odzyskanie aliasu, loginu lub reset hasła do konta IKU albo reset PIN-u do identyfikatora,</p> <p>i) wnioskowanie o zwrot niewykorzystanego biletu w trybie automatycznym na Portalu klienta i w Aplikacji mobilnej i SADiS</p> <p>j) zasilenie i korzystanie z e-portmonetki</p>	<p>niezbędnych do przyjęcia reklamacji w tym danych osobowych oraz możliwość otrzymywania odpowiedzi na reklamację (poza portalem i aplikacją mobilną) na adres email lub powiadomień SMS-em,</p> <p>c) możliwość zdefiniowania domyślnych danych odbiorcy i płatnika faktury oraz możliwość otrzymania faktury na adres email,</p> <p>d) możliwość podłączania i zarządzania wieloma identyfikatorami w tym podglądu danych dla identyfikatorów których ważność wygasła lub zostały zablokowane,</p> <p>e) wybranie kanału do powiadomień (mail, SMS, Aplikacja mobilna),</p> <p>f) stworzenie nowego konta grupującego lub wyrażenie zgody użytkownika konta na włączenie do konta grupującego, musi istnieć również możliwość odpięcia konta od konta grupującego z kontekstu pojedynczego konta użytkownika (musi ono cały czas istnieć w systemie),</p> <p>g) możliwość zdefiniowania aliasu przez użytkownika do logowania się na Portalu i w Aplikacji mobilnej.</p> <p>h) odzyskanie loginu, aliasu lub reset hasła albo PIN-u jest możliwe zdalnie na Portalu klienta lub w POP z wykorzystaniem zdefiniowanego kanału powiadomień (email lub SMS). Dodatkowo PIN można zmienić lub zresetować na zasadach opisanych dla konta nieprofilowanego.</p> <p>i) zwrot biletu w trybie automatycznym może zostać wykonany po spełnieniu warunków z taryfy i podaniu wymaganych danych np. numeru rachunku bankowego do zwrotu, pozostałe zwroty są możliwe tylko w POP lub w trybie reklamacyjnym.</p> <p>j) tylko dla identyfikatorów innych niż karta EMV</p>
3	profilowane imienne	<p>funkcjonalność dostępna dla konta profilowanego i dodatkowo</p> <p>+ j) odzyskanie loginu i hasła do konta IKU na podstawie PESEL.</p> <p>+ k) definiowanie domyślnych ulg</p>	<p>warunki i cechy funkcjonalności dotyczące konta profilowanego i dodatkowo:</p> <p>+ j) na podstawie dokumentu tożsamości można odzyskać login i zresetować hasło do konta</p> <p>+ k) przy samodzielnym zdefiniowaniu ulg należy przy kontroli okazać dokument potwierdzający ulgę (funkcjonalność ta służy do wybierania taryf ulgowych podczas zakupów biletów)</p>
4	nieprofilowane imienne	<p>a) pobranie historii użycia na Portalu, w POP,</p> <p>b) złożenie reklamacji osobiście lub przez pełnomocnika na Portalu i w POP,</p> <p>c) złożenie wniosku o fakturę na Portalu i w POP</p> <p>d) reset PIN</p> <p>e) zasilenie i korzystanie z e-portmonetki</p> <p>f) definiowanie i domyślnych ulg</p>	<p>a) z wykorzystaniem jednego identyfikatora, identyfikator ten musi być aktywny</p> <p>b) podanie wszystkich danych niezbędnych do przyjęcia reklamacji w tym danych osobowych,</p> <p>c) podanie wszystkich danych odbiorcy i płatnika faktury</p> <p>d) na podstawie dokumentu tożsamości</p> <p>e) tylko dla identyfikatorów innych niż karta EMV</p> <p>f) w POP od razu z autoryzacją.</p>
6	archiwalne	<p>a) pobranie historii użycia na Portalu, w POP</p> <p>b) złożenie reklamacji osobiście lub przez pełnomocnika na Portalu i w POP,</p>	<p>Konto może funkcjonować przy ograniczonej funkcjonalności również w ramach konta grupującego.</p>

		c) złożenie wniosku o fakturę na Portalu i w POP d) zwrot niewykorzystanych punktów z e-portmonetki	a) funkcjonalność dostępna przez okres xx miesięcy wyłącznie dla użytkowników posiadających login i hasło do konta (przez Portal Klienta i Aplikację mobilną) lub dla użytkowników, którzy zdefiniowali swój PESEL, adres email lub numer telefonu (np. w POP). Parametr xx musi być możliwy do zdefiniowania/zmiany w systemie przez administratora Zamawiającego. b) i c) jak dla a) d) po zdefiniowaniu rachunku bankowego albo adresu do przekazu pocztowego
--	--	--------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabela 4. Rodzaje kont w systemie ŚKUP 1.5 – podstawowe rodzaje funkcjonalności

Konto nieprofilowane imienne posiada funkcjonalność zbliżoną do funkcjonalności konta nieprofilowanego rozszerzoną o możliwość zapisywania na nim uprawnień imiennych w tym uprawnień do ulg. Konto to jest przeznaczone dla użytkowników, którzy nie chcą lub nie mogą posługiwać się elektronicznymi kanałami dostępu do konta. Założenie tego konta jest możliwe od razu podczas wydawania identyfikatora lub z przekształcenia konta nieprofilowanego w POP. Użytkownik tego konta musi posiadać jeden identyfikator z aktualnym terminem ważności oraz musi powiązać z kontem swoje dane takie jak imię, nazwisko i PESEL (przechowywany w postaci zaszyfrowanej). Po upływie terminu ważności identyfikatora do konta można podpiąć kolejny identyfikator. Operacja podpięcia kolejnego identyfikatora może być dokonana również przed zakończeniem ważności identyfikatora w okresie definiowanym parametrem w systemie dostępnym dla administratora Zamawiającego (np. 1 miesiąc przed), w tym przypadku dotychczasowy identyfikator (tego samego rodzaju) musi zostać zdezaktywowany.

Konto archiwalne jest przekształcane z dowolnego innego konta po tym jak wygaśnie ważność lub zostanie odpięty od konta ostatni aktywny identyfikator. Dostęp do tego konta jest ograniczony i uzależniony od tego z jakiego rodzaju konta zostało utworzone konto archiwalne. Funkcjonalność konta jest ograniczona wyłącznie do możliwości sprawdzenia i pobrania wykonanych operacji w systemie, zwrotu niewykorzystanych środków z e-portmonetki oraz do złożenia reklamacji i wniosków o fakturę. Nie można dla takiego konta dokonywać żadnych operacji związanych z zakupem i kodowaniem nowych uprawnień oraz zasileniem punktów. Można natomiast reaktywować to konto (przywrócić funkcjonalność konta) w określonym czasie poprzez podłączenie do niego aktywnego identyfikatora. Wykonanie reaktywacji konta archiwalnego będzie możliwe na Portalu Klienta w Aplikacji Mobilnej ŚKUP 1.5 oraz w POP przy wykorzystaniu mechanizmu, który pozwoli na jednoznaczny identyfikację jego użytkownika. Maksymalny czas reaktywacji konta archiwalnego będzie zdefiniowany parametrem w systemie, do którego będzie miał dostęp administrator systemu po stronie Zamawiającego. W ramach danych konta są przechowywane archiwalne informacje dotyczące identyfikatorów. Konto archiwalne będzie funkcjonowało również w ramach konta grupującego w zakresie opisanym powyżej (jeśli zostało do niego wcześniej podłączone).

2.3 Migracja kont z systemu ŚKUP

Do systemu ŚKUP 1.5 muszą zostać zmigrowane wszystkie aktywne konta utworzone na portalu ŚKUP wraz z zapisanymi tam danymi w tym konta grupujące. Do zmigrowanych kont w systemie ŚKUP 1.5 będzie można zalogować się z dotychczasowym „loginem” (aliasem lub numerem karty w systemie ŚKUP) i hasłem, ale podczas migracji zostaną utworzone dodatkowo loginy zgodne ze standardem obowiązującym w systemie ŚKUP 1.5. Dotychczasowe loginy kont staną się dodatkowymi aliasami (wiele aliasów do jednego konta IKU). Konta te będą miały specjalny status, który będzie wymagał potwierdzenia lub uzupełnienia danych przy pierwszym logowaniu w systemie ŚKUP 1.5 zgodnie z Tabelą nr 5 Migrowanie danych, lub wymuszenia zmiany hasła w przypadku niespełnienia wymogów dla nowego systemu. W okresie przejściowym, gdy będą funkcjonowały równocześnie dwa systemy: ŚKUP i ŚKUP 1.5 dane będą synchronizowane w trybie ciągłym (max. co 5 min.) między systemami do całkowitego przejścia infrastruktury przez Wykonawcę systemu ŚKUP 1.5. Konta z systemu ŚKUP zostaną zmigrowane na następujące rodzaje kont w systemie ŚKUP 1.5:

ŚKUP rodzaj karty, do której jest utworzone konto		ŚKUP 1.5		
		warunki		rodzaj konta
niespersonalizowana	→	brak	→	nieprofilowane
spersonalizowana	→	podanie adresu email lub numeru telefonu	→	profilowane imienne
		brak	→	nieprofilowane imienne;

Tabela 5. Migrowanie kont

2.4 Konto grupujące i firmowe

Pojedyncze konta IKU (nawet z kilkoma identyfikatorami) będą mogły być grupowane w konta grupujące w celu łatwiejszego zarządzania grupą kont. Konto grupujące może zostać utworzone tylko na podstawie zwykłego, pojedynczego konta IKU. Wszystkie operacje podpięcia i odpięcia konta IKU z konta grupującego muszą być informacyjnie wysyłane na adresy mailowe powiązane z kontem grupującym, jak i z kontem IKU którego dotyczy wykonywana operacja.

Konto grupujące musi posiadać swój login i hasło nadawane w trakcie procesu jego zakładania, musi być również powiązane z istniejącym adresem email - opcjonalnie dodatkowo nr tel. komórkowego (mogą to być dane jednego z kont IKU powiązanych z kontem grupującym). Użytkownik konta grupującego może do niego zdefiniować unikatowy w skali systemu Alias. Będzie również możliwość zdalnego odzyskania hasła w oparciu o podany adres email/SMS.

Konto grupujące może występować w dwóch wariantach jako konto „rodzinne” lub jako konto „firmowe” (np. firmy lub instytucji takiej jak np. placówka opiekuńcza). Szczegółowa funkcjonalność obydwu wariantów kont zostały opisane w rozdziale opisującym funkcjonalności dostępne po zalogowaniu się do Portalu Klienta.

W ramach zarządzania kontem grupującym musi istnieć możliwość opisywania każdego z kont IKU w celu ułatwienia identyfikacji (np. przypisania konta IKU do osoby lub czynności). Pole opisu będzie pozwalało na wprowadzenie minimum 35 znaków alfanumerycznych.

2.5 Możliwości rozwoju

Zestaw danych powiązanych z kontem powinien mieć możliwość rozbudowy o dodatkowe pola, które mogą być wykorzystane w przyszłości np. numer rejestracyjny samochodu, preferowane miasto, rodzaje ulg, powiązane systemy (MaaS), itp.

2.6 Procesy

2.6.1 Utworzenie konta

1. Dla karty ŚKUP 1.5 – predefiniowane konto tworzone jest automatycznie dla numeru karty z startowym PIN-em. Ostateczne zasady generowania i zmiany PIN-u zaproponuje Wykonawca na podstawie przeprowadzonej analizy ryzyka. Konta IKU będą predefiniowane dla każdej wydanej karty ŚKUP 1.5.

Konto będzie można zmodyfikować:

- a. Samodzielnie - poprzez logowanie się na Portalu lub w Aplikacji Mobilnej;
 - b. W POP – z wykorzystaniem numeru karty;
2. Z wykorzystaniem tokena karty EMV lub surogatu – konto jest tworzone automatycznie przy pierwszym użyciu identyfikatora. Login jest ujawniany dopiero na żądanie użytkownika karty. Ujawnienie loginu/Modyfikacja konta będzie mogła następować:
 - a. Samodzielnie – przez uruchomienie aplikacji do tokenizacji na Portalu;
 - b. W POP – wykonując tokenizację identyfikatora na dedykowanym urządzeniu w POP.
 3. Z wykorzystaniem Aplikacji Mobilnej:
 - a. Samodzielnie – wykorzystując Aplikację Mobilną i przypisując do numeru telefonu konto w systemie centralnym. Numer telefonu jako identyfikator będzie przechowywany w systemie w postaci zaszyfrowanej.
 4. Rejestrując konto na Portalu klienta przed pozyskaniem identyfikatora:
 - a. Samodzielnie – definiując dane niezbędne do utworzenia wybranego typu konta. Konto może zostać utworzone w Portalu klienta bez identyfikatora na określoną parametrem ilość dni. Parametr będzie definiowany przez administratora Zamawiającego i może wynosić również 0 (zero). Tego typu konto nie będziemy miały aktywnej e-portmonetki oraz nie będzie możliwości zakupu biletów do momentu podpięcia jakiegokolwiek identyfikatora.

2.6.2 Przypisanie i odpinanie identyfikatora do konta

Przypisanie kolejnego identyfikatora do konta IKU może nastąpić dla kont profilowanych oraz dla konta archiwalnego i dla konta nieprofilowanego imiennego (przy zachowaniu warunków opisanych przy tym rodzaju konta). Proces przypisywania będzie możliwy do wykonania w kontekście konta IKU, do którego identyfikator jest dodawany, ale pod warunkiem jednoznacznego zidentyfikowania identyfikatora (np. numer karty + PIN, wygenerowanie tokenu). Jeżeli do konta nie był przypisany aktywny identyfikator, to przypisywany identyfikator stanie się automatycznie identyfikatorem aktywnym, w przeciwnym wypadku system musi wygenerować zapytanie, czy przypisywany identyfikator ma się stać identyfikatorem aktywnym i umożliwić działanie adekwatne do decyzji użytkownika IKU.

Użytkownik konta IKU może odpiąć identyfikator od konta. Informacja o tym zdarzeniu zostanie rozdystrybuowana do infrastruktury ŚKUP 1.5 w czasie zbliżonym do rzeczywistego. Z zasady nie będzie można już posługiwać się identyfikatorem w postaci kart ŚKUP lub karty ŚKUP 1.5 w systemie ŚKUP 1.5. Przed taką operacją użytkownik musi otrzymać komunikat, że taki identyfikator (karta ŚKUP i ŚKUP 1.5) nie może być już ponownie użyty w systemie. Użytkownik musi potwierdzić dodatkowo taką operację.

Dla kart płatniczych EMV muszą zostać zastosowane zasady obowiązujące dla tych kart. Sposób obsługi identyfikatora w postaci aplikacji mobilnej proponuje Wykonawca, zaproponowane rozwiązanie będzie podlegało akceptacji Zamawiającego.

Dane dotyczące transakcji wykonanych tym identyfikatorem w trakcie gdy był przypięty do konta nadal pozostają dostępne z poziomu konta IKU.

Jeżeli jest to ostatni aktywny identyfikator, to zostanie wyświetlony i wygenerowany możliwy do wydrukowania (np. w PDF) komunikat o tym, że konto zostanie zmienione na archiwalne, a po okresie zdefiniowanym przez parametr w systemie, dostęp do niego zostanie wyłączony. Komunikat będzie zawierał również informacje o pozostających na koncie ważnych uprawnieniach do usług.

Informacja o wyżej wymienionych operacjach musi zostać przesłana na zdefiniowany do konta IKU adres e-mail lub SMS-em. Szczegółowa treść informacji zostanie uzgodniona z Zamawiającym na etapie projektowania funkcjonalności.

2.6.3 Wybór identyfikatora aktywnego

Użytkownik konta będzie mógł zmieniać aktywny identyfikator wg parametryzowanych w systemie reguł (np. przed pierwszą transakcją w danym dniu). W przypadku skorzystania z identyfikatora w danym dniu, zmiana aktywnego identyfikatora na inny nastąpi ze skutkiem w kolejnym dniu. Parametryzacja reguł będzie dostępna z poziomu administratora systemu po stronie Zamawiającego. Reguły będą określały ilość możliwych zmian w ciągu dnia, tygodnia, miesiąca w zależności od użycia identyfikatora (tak jak w podanym wyżej przykładzie). Użytkownik IKU będzie mógł dokonać zmiany identyfikatora samodzielnie na Portalu Klienta i w Aplikacji Mobilnej ŚKUP 1.5 albo w POP.

2.6.4 Zablokowanie i odblokowanie identyfikatora

Użytkownik konta może zablokować identyfikator w aktywnych kanałach dostępu do IKU. Zablokowanym identyfikatorem nie można posługiwać się w systemie ŚKUP 1.5. Odblokowanie może nastąpić w POP lub na Portalu Klienta lub Aplikacji Mobilnej ŚKUP 1.5 pod warunkiem podania danych jednoznacznie identyfikujących prawowitego użytkownika identyfikatora (dane proponuje Wykonawca do akceptacji Zamawiającego na etapie projektowania rozwiązania). Okres obowiązywania blokad musi być parametrem w systemie możliwym do zmiany przez administratora Zamawiającego. Po upływie okresu blokady identyfikator zostanie nieodwracalnie dezaktywowany.

2.6.5 Zmiana rodzaju konta

Zmiana rodzaju konta jest możliwa pod warunkiem, że powiązane z nim identyfikatory i uprawnienia, mogą być powiązane z docelowym rodzajem konta. Przed przystąpieniem do operacji, system będzie informował użytkownika o wszelkich wykluczających się elementach oraz sugerował ewentualny scenariusz naprawczy. W takim wypadku należy najpierw odpiąć od konta identyfikatory oraz wykorzystać lub zwrócić uprawnienia. Podczas zmiany rodzaju konta musi zostać zmodyfikowany zakres danych powiązanych z kontem, tak aby odpowiadał zakresowi danych wymaganych dla konta docelowego. Przed dokonaniem zmiany użytkownik konta musi zostać poinformowany odpowiednim

komunikatem, możliwym do wydrukowania, o wymaganiach i konsekwencjach dokonywanej zmiany rodzaju konta.

2.6.6 Modyfikacja lub usunięcie danych osobowych z konta imiennego

Użytkownik konta może wnioskować o usunięcie lub zmianę danych osobowych powiązanych z kontem IKU (w tym adresu e-mail i numeru telefonu) na Portalu klienta lub w POP. W przypadku zmiany imienia lub nazwiska przypisanego do konta IKU. Wniosek może być złożony w POP lub zdalnie na Portalu Klienta. W POP zmiana zostanie dokonana na podstawie przedstawionego dokumentu, a wniosek złożony na Portalu Klienta musi zostać potwierdzony z wykorzystaniem profilu zaufanego lub innej bezpiecznej metody weryfikacji tożsamości. Jeżeli użytkownik konta posiada identyfikator w postaci karty ŚKUP spersonalizowanej, to musi go wymienić na inny identyfikator (odpowiedni komunikat zostanie wyświetlony/przekazany użytkownikowi przed wprowadzeniem zmiany).

Użytkownik konta może usunąć swoje dane osobowe rozumiane jako imię, nazwisko, PESEL, adres e-mail lub numer telefonu, zdjęcie przypisane do konta, ale może to zrobić po spełnieniu następujących warunków:

- Do konta nie ma przypisanych biletów imiennych;
- Identyfikatorem aktywnym nie jest karta ŚKUP imienna;

Skutkiem usunięcia danych jest przekształcenie konta na konto profilowane lub nieprofilowane oraz brak możliwości używania karty ŚKUP imiennej (jeżeli taka jest na liście identyfikatorów przypisanych do konta). Odpowiedni komunikat zostanie przekazany użytkownikowi konta przed wprowadzeniem zmiany.

2.6.7 Blokada i odblokowanie konta

W każdej chwili dostęp do konta może zostać zablokowany. Blokada konta polega na czasowym wyłączeniu dostępu do konta we wszystkich lub wybranych kanałach dla użytkownika. Przy zablokowaniu wszystkich kanałów dostępu muszą zostać zablokowane w systemie również wszystkie identyfikatory do konta. Użytkownik konta będzie mógł dokonać blokady konta we wszystkich dostępnych kanałach (po zweryfikowaniu posiadanych uprawnień). Okres obowiązywania blokad musi być parametrem w systemie możliwym do zmiany przez administratora Zamawiającego. Po upływie okresu blokady konto będzie automatycznie zamykane. Konto może zostać również zablokowane na określony okres czasu przez operatora APO ze specjalnymi uprawnieniami (np. w przypadku fraudów).

Odblokowanie może nastąpić w POP lub (poza przypadkiem zablokowania konta przez operatora w POP) na Portalu Klienta lub Aplikacji Mobilnej ŚKUP 1.5 pod warunkiem podania i zweryfikowania przez system lub operatora danych jednoznacznie identyfikujących prawowitego użytkownika konta np. PESEL, imię, nazwisko, e-mail, numer telefonu, PIN. Sposób weryfikacji danych i zasady odblokowania konta proponuje Wykonawca w trakcie projektowania funkcjonalności.

2.6.8 Zamknięcie konta

Przed zamknięciem konta użytkownik musi otrzymać komunikat o konsekwencjach tej operacji. Zamknięcie konta może nastąpić dopiero w momencie pokrycia zaległych zobowiązań wobec

dostawców usług. Podczas zamykania konta użytkownik musi mieć możliwość zwrotu uprawnień i punktów zgromadzonych na e-portmonetce. Zamknięcie konta jest związane z dezaktywowaniem wszystkich identyfikatorów. Operacja zamknięcia konta jest nieodwracalna, a dane będą usuwane lub przechowywane do czasu usunięcia zgodnie z prawem dotyczącym przetwarzania danych osobowych oraz prawem podatkowym. Operacja może zostać wykonana w POP lub z wykorzystaniem Portalu klienta lub Aplikacji mobilnej.

2.6.9 Bilety kodowane dla wielu kont IKU

System musi umożliwiać Zamawiającemu automatyczne kodowanie uprawnień/ulg dla wielu kont (np. kodowanie biletów R1, realizacja wniosków reklamacyjnych, zapisanie ulgi itp.) na podstawie listy identyfikatorów lub loginów kont zawartych w pliku. Rozwiązanie dla tej funkcjonalności oraz możliwe formaty pliku zostaną uzgodnione z Zamawiającym w trakcie projektowania funkcjonalności. Należy przewidzieć pełną audytowalność operacji (Id konta, id operatora, data, co zakodował).

2.7 Dane /cechy powiązane z kontem

Dane / cechy charakteryzujące konto zależy od jego rodzaju. Podstawowy wykaz danych / cech, które muszą zostać zapisane na poszczególnych rodzajach kont został przedstawiony poniżej. Wykonawca zaproponuje pozostałe dane / cechy, które muszą być zapisane na koncie IKU, aby zrealizować wszystkie funkcjonalności opisane w zakresie zamówienia oraz zapewnić wysoki poziom bezpieczeństwa systemu.

Lp.	Rodzaje Kont	Podstawowy wykaz danych zapisywanych na koncie	
		obowiązkowo	opcjonalnie
1	nieprofilowane	- identyfikator + PIN, - status konta (minimum: aktywne/nieaktywne/zablokowane), - kanały dostępu do konta i ich status (Aktywny/Nie aktywny).	
2	profilowane	- identyfikatory + PIN i ich statusy (np. aktywny, nieaktywny, zablokowany, zastrzeżony)* - status konta (minimum: aktywne/nieaktywne/zablokowane), - kanały dostępu do konta i ich status (Aktywny/Nie aktywny). - adres email lub nr telefonu do powiadomień SMS * za wyjątkiem konta o ograniczonym okresie obowiązywania	- Alias
3	profilowane imienne	- identyfikatory + PIN i ich statusy (np. aktywny, nieaktywny, zablokowany, zastrzeżony)* - status konta (minimum: aktywne/nieaktywne/zablokowane), - kanały dostępu do konta i ich status (Aktywny/Nie aktywny). - adres email lub nr telefonu do powiadomień SMS - PESEL - imię i nazwisko - zdjęcie pozwalające na jednoznaczna identyfikację użytkownika konta IKU * za wyjątkiem konta o ograniczonym okresie obowiązywania	- Alias - Gmina - Ulga
4	nieprofilowane imienne	- identyfikator + PIN, - status konta (minimum: aktywne/nieaktywne/zablokowane), - kanały dostępu do konta i ich status (Aktywny/Nie aktywny). - PESEL - imię i nazwisko - zdjęcie pozwalające na jednoznaczna identyfikację użytkownika konta IKU	- Alias - Gmina - Ulga
6	archiwalne	<i>zależy od tego z jakiego rodzaju konta IKU zostało przekształcone konto,</i>	

Tabela 6. Rodzaje kont w systemie ŚKUP 1.5 – zbiór niezbędnych danych

2.8 Informacje podstawowe powiązane z kontem

1. Zadeklarowane ulgi – jako lista zawierająca zdefiniowane typy ulg, z historią ich przypisania do konta i datami obowiązywania (pozycja słownikowa z MTC). Zamawiający oczekuje możliwości definiowania więcej niż jednej ulgi dla danego konta użytkownika, z rozróżnieniem ulg dla różnych organizatorów transportu/dostawców usług; ulgi mogą być autoryzowane (w APO – pracownik POP, UKNT - kontroler biletowy) przez pracowników Zamawiającego lub nieautoryzowane (APK, MOB) wprowadzone przez użytkownika. Bez autoryzacji pasażer musi posiadać dokument uprawniający do ulgowych przejazdów. Ulga autoryzowana nie wymaga przez użytkownika posiadania przy sobie dokumentu uprawniającego do ulgi;
2. Bieżąca ilość punktów na e-portmonetce;
3. Posiadane uprawnienia – np. zakupione bilety wraz ze wszystkimi parametrami, w tym datą i godziną zakupu/nabycia uprawnienia i jego okresem obowiązywania;
4. Historia wszystkich operacji wykonanych poszczególnymi identyfikatorami powiązanych z kontem w tym historia operacji z wykorzystaniem e-portmonetką oraz wykonane kontrole;
5. Prowadzona korespondencja wewnętrzna z użytkownikiem wraz z informacjami o ich odczycie;
6. Złożone reklamacje, ich stan oraz odpowiedzi;
7. Komunikaty globalne (np. zmiana taryfy) oraz wiadomości indywidualne (np. ostrzeżenie o zadłużeniu, kończących się biletach, kończącym się terminie zadeklarowanej ulgi itp.) wraz z informacjami o ich odczycie;
8. Domyślne dane do wystawiania faktury (nie muszą być identyczne z danymi identyfikacyjnymi, ponieważ faktura może być wystawiona np. na zakład pracy);
9. Wnioski i faktury wygenerowane dla konta wraz z historią ich złożenia/odczytania/pobrania przez użytkownika;
10. Informacja o powiązaniu z kontem grupującym lub firmowym;
11. Wyrażone zgody między innymi na przetwarzanie danych wraz z datą i godziną ich akceptacji;
12. Historia zmian konta w tym zmiany danych powiązanych z kontem, przypisania do konta grupującego, zmiana rodzaju konta itd.;
13. Historia przeglądania, modyfikowania konta (obowiązek RODO).

Wykonawca zapewni dla użytkowników po stronie Zamawiającego zestaw raportów pozwalających na ujawnienie wszystkich danych i informacji powiązanych z kontem na podstawie znajomości loginu, dowolnego z aliasów lub dowolnych cech identyfikatorów (np. numer karty ŚKUP, token karty EMV), które były i są powiązane z kontem IKU. Dostarczy również raport/kalkulator pozwalający na podstawie jednej z cech charakteryzujących konto IKU odczytanie w czasie zbliżonym do rzeczywistego pozostałych cech charakteryzujących konto IKU w tym login, aliasy, nr Pesel oraz ewentualne inne cechy identyfikujące konto IKU wprowadzone przez Wykonawcę do systemu. Wykonawca zapewni dostęp do danych w tym do danych dotyczących zamknięcia konta (np. data, identyfikator z pomocą którego zamknięto konto) nawet po zamknięciu konta przez użytkownika zgodnie z prawem dotyczącym przetwarzania danych osobowych oraz prawem podatkowym.

3 Identyfikatory pasażera

3.1 Opis ogólny

Identyfikatorami Indywidualnych Kont Użytkownika (IKU) funkcjonującymi w centralnym systemie ŚKUP 1.5 mogą być: karty ŚKUP, karty ŚKUP 1.5, oraz Aplikacja Mobilna ŚKUP 1.5. Mogą to być również inne identyfikatory, które obecnie nie są identyfikowane. Wykonawca zapewni w systemie ŚKUP 1.5 możliwość używania kart dotychczas wydanych w ramach systemu ŚKUP. W systemie ŚKUP 1.5 Wykonawca zapewni możliwość ich obsługi w zakresie funkcjonalności identyfikatora. W systemie może być zdefiniowanych kilka identyfikatorów konta IKU jednak tylko jeden identyfikator może być w danej chwili aktywny. Użytkownik konta będzie mógł zmieniać aktywny identyfikator wg parametryzowanych w systemie reguł (np. zmiana identyfikatora tylko raz na dobę lub przy zakupie uprawnienia z wykorzystaniem nieaktywnego identyfikatora, który od tego momentu będzie aktywny). Związane to jest z użytkowaniem w systemie biletów (imiennych, na okaziciela) – bilet zakupiony na konto IKU użytkownika nie może być wykorzystywany przez kilka identyfikatorów równocześnie. W przeciwnym wypadku z jednego biletu będzie mogło korzystać w tym samym czasie kilku podróżnych posiadających różne identyfikatory do jednego konta.

Specjalnym identyfikatorem konta IKU mogą również być zbliżeniowe karty płatnicze EMV (w tym surogaty kart EMV takie jak aplikacje mobilne z wirtualną kartą EMV, breloki, zegarki itp.)

Należy zwrócić uwagę, że karty EMV i surogaty mogą pełnić kilka funkcji w systemie. Mogą być identyfikatorem konta (tylko w zakresie zakupionych biletów okresowych bez limitu przejazdu) oraz mogą pełnić funkcję instrumentu płatniczego, za pomocą którego będą opłacane zakupy usług (np. w kasownikach zainstalowanych w pojazdach byłego MZK oraz kasowniki z autonomicznych systemów, które zostaną zintegrowane z systemem ŚKUP 1.5) lub realizowane opłaty (np. opłata dodatkowa w kontrolerze) wykonywane w systemie ŚKUP 1.5.

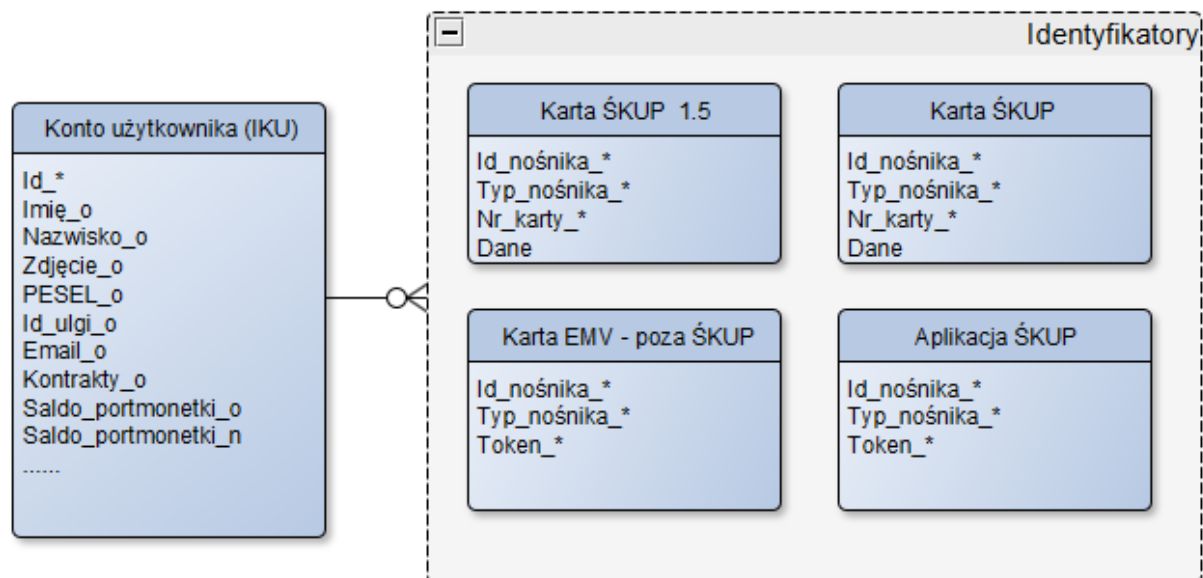
Użytkownik konta IKU musi mieć możliwość opisywania (co najmniej w Portalu i Aplikacji Mobilnej) każdego ze swoich identyfikatorów w celu ułatwienia identyfikacji. Pole opisu będzie pozwalało na wprowadzenie minimum 35 znaków alfanumerycznych.

L.P.	Typ	Pozyskanie	Funkcjonalność	
			Wniesienie opłaty za przejazd	Identyfikator uprawnienia/biletu
1.	Zbliżeniowa Karta EMV i surogaty	Poza systemem ŚKUP 1.5	TAK (tylko w pojazdach wyposażonych w kasowniki EMV)	TAK
2.	Karta ŚKUP 1.5	Osobiście: 1. Punkt Obsługi Pasażera 2. Stacjonarny Automat Dystrybucji i Sprzedaży 3. Agenci sprzedaży (Kioski)	TAK	TAK

3.	Karta ŚKUP niespersonalizowana	Migracja z systemu ŚKUP	TAK	TAK
4.	Karta ŚKUP spersonalizowana	Migracja z systemu ŚKUP	TAK	TAK
5.	Aplikacja mobilna ŚKUP 1.5	Dystrybucja poprzez sklep Android i iOS	TAK	TAK

Tabela 7. Rodzaje identyfikatorów wykorzystywanych w systemie ŚKUP 1.5

3.2 Rodzaje identyfikatorów



Rysunek 2. Rodzaje identyfikatorów.

3.2.1 Karta ŚKUP 1.5

- Plastikowa Karta z interfejsem bezprzewodowym wydawana bez umieszczenia na jej warstwie fizycznej cech użytkownika – karty będą umożliwiały bezpieczną identyfikację powiązanego z nią konta pasażera w systemie ŚKUP 1.5 (pozwolą na powiązanie karty z kontem pasażera);
- Karta będzie miała z definicji przyporządkowane konto inicjalne IKU, do którego np. aliasem będzie numer karty. Szczegóły rozwiązania proponuje Wykonawca na etapie projektowania funkcjonalności. Zaproponowane rozwiązanie będzie podlegało akceptacji Zamawiającego;
- Na karcie musi istnieć aplikacja identyfikacyjna (szyfrująca), pozwalająca na bezpieczną identyfikację karty w systemie, oraz określenie aktualnego statusu karty (np. data ważności, wydana, nie wydana, aktywna, zablokowana itp.). Wykonawca proponuje miarodajne stany, które będą gwarantowały rozliczalność i bezpieczeństwo systemu kartowego;
- Zamawiający dopuści inne aplikacje, które proponuje Wykonawca na potrzeby realizacji wymagań stawianych systemowi, w szczególności w celu osiągnięcia wymaganych parametrów wydajnościowych i ergonomicznych przy posługiwaniu się kartą w pojazdach. W celu uniknięcia sytuacji, kiedy pojazd traci łączność z systemem centralnym, a wymagana jest obsługa procesów realizowanych przez UKAS, UKAS-EMV;
- Pozyskanie karty musi się wiązać z kaucją, której wartość będzie parametrem w systemie możliwym do zmiany przez operatora z odpowiednimi uprawnieniami po stronie Zamawiającego; Mechanizm ten ma zapobiec masowemu pozyskiwaniu kart i wykorzystywaniu ich jednorazowo;
- Karta może być zwrócona w POP w okresie jej ważności lub po jej upływie. Jeżeli identyfikator nie będzie nosił śladów fizycznego uszkodzenia przez użytkownika, to będzie zwracana kaucja (w aplikacjach obsługujących zwrot kart musi być znacznik/flaga określający/a stan karty).

- Wymagane jest od Wykonawcy przygotowanie procedury, która już po procesie produkcji i wydaniu karty, pozwoli na zapisanie na karcie nowych aplikacji, odizolowanych od identyfikatora karty, dotyczy przyszłościowego wykorzystania karty jako nośnika lub innego identyfikatora dla innych systemów.

1) Cechy karty ŚKUP 1.5 - identyfikatora NFC

Na potrzeby projektu Wykonawca dostarczy 200 tys. kart w prawie opcji, z technologią NFC zgodnych ze standardem ISO/IEC 14443, zabezpieczonych przed kopiowaniem, klonowaniem i dokonywaniem innych nadużyć w ramach systemu ŚKUP 1.5 przez nieautoryzowane osoby lub procesy. Karta ŚKUP 1.5 z NFC będzie klasy co najmniej Mifare DesFire 8KB EV2 lub EV3 lub równie bezpieczna. Jej trwałość będzie wynosić co najmniej 5 lat. Karta nie może generować konfliktów związanych z obsługą w tym samym systemie kart, które zostały zmigrowane z systemu ŚKUP (wymagana kompatybilność z nośnikami EV1).

W celu zapewnienia standardów bezpieczeństwa szyfrowania informacji, karta musi wykorzystywać co najmniej algorytm 3KDES lub AES. Zastosowane karty muszą zawierać unikalny i niezmienny numer, zgodny z numeracją kart płatniczych. Każda karta powinna mieć zapisany w układzie pamięciowym na trwałe numer UID. Zastosowane karty muszą zawierać unikalny i niezmienny numer PAN, zgodny z numeracją kart płatniczych. Unikalny numer karty będzie naniesiony na karcie w technologii embossing. Numer karty będzie zgodny ze standardem ISO/IEC 7812. Karty będą współpracować z modułami SAM przy wykorzystaniu czytników urządzeń infrastruktury systemu. Karta będzie umożliwiała wgranie aplikacji zdefiniowanej przez Zamawiającego, innej niż dostarczanej w ramach Systemu ŚKUP 1.5.

2) Projekt karty ŚKUP 1.5

Wykonawca przedstawi 3 propozycje szaty graficznej karty, do uzgodnienia z Zamawiającym.

3) Zasady zamawiania i wydawania kart ŚKUP 1.5.

W systemie nie przewiduje się wydawania kart z umieszczonymi na jej warstwie fizycznej cech użytkownika.

Karty dedykowane do systemu ŚKUP 1.5 będą zamawiane i dostarczane przez Wykonawcę do punktów dystrybucji kart (PDK) zdefiniowanych w systemie. Pozwoli to na natychmiastowe wydawanie tych kart w każdym z kanałów dystrybucji. Trzeba jednak pamiętać, że karta musi być „aktywowana” w systemie w trakcie wydawania. Nieaktywowana karta nie będzie obsługiwana w systemie jako identyfikator.

Możliwe kanały pozyskiwania kart dedykowanych do systemu ŚKUP 1.5:

- POP-y;
- SADiS;
- UPOS - Agenci sprzedaży (tzw. kioski).

3.2.2 Karty z systemu ŚKUP

Wydawcą kart ŚKUP jest mBank S.A. zgodnie z regulaminem karty ŚKUP.

Wykonawca będzie zasiliał System ŚKUP 1.5 danymi (Gwarant systemu SKUP przygotowuje paczki danych w uzgodnionym formacie) o kartach z systemu ŚKUP na potrzeby wykorzystywania ich w systemie ŚKUP 1.5 (patrz **Migracja kont z systemu ŚKUP** opisana w pkt. 2.3). Zamawiający posiada ok 700 000 wydanych kart, z czego aktywnych tj. nie zastrzeżonych i nie zablokowanych jest ok. 400 000. W ramach migracji danych Wykonawca zasili system ŚKUP 1.5 danymi o kartach ŚKUP niezbędnymi do obsługi wszystkich funkcjonalności ŚKUP 1.5 opisanych przez Zamawiającego w tym zwrotów kaucji za karty ŚKUP.

Zamawiający posiada karty SAM oraz bibliotekę API do obsługi karty ŚKUP wraz z dokumentacją.

Karta ŚKUP spersonalizowana i na okaziciela wydawane w ramach funkcjonowania systemu ŚKUP do zakończenia okresu swojej ważności będą pełniły funkcje jednego z identyfikatorów w systemie ŚKUP 1.5;

W zmodernizowanym systemie ŚKUP 1.5 funkcjonalność kart ŚKUP będzie taka sama, jak kart dedykowanych do systemu ŚKUP 1.5.

3.2.3 Aplikacja Mobilna ŚKUP 1.5 (MOB)

Funkcjonalność Aplikacji Mobilnej (MOB) została opisana w rozdziale 4.2.

Aplikacja będzie do pobrania w sklepie Google Play i App Store. Aplikacja poprzez wykorzystanie szyfrowanego w systemie numeru telefonu będzie spełniała rolę identyfikatora konta IKU w pojeździe, w tym w kontrolerze. Funkcjonalność identyfikatora będzie dostępna dopiero po zalogowaniu się do konta IKU (wymaga dostępu do internetu).

- 1) W ramach procesu instalacji aplikacji na telefonie, może następować sparowanie aplikacji (numeru telefonu) jako identyfikatora z kontem IKU w systemie centralnym:
 - nowym - w tym przypadku realizowany jest proces utworzenia nowego konta IKU z podstawowymi danymi: identyfikator, hasło, e-mail, opcjonalnie numer telefonu (nr telefonu w postaci jawnej);
 - już istniejącym - jako kolejny identyfikator;

3.2.4 Karta EMV – zbliżeniowa i surogaty

Opisane funkcjonalności karty EMV muszą być dostępne również dla jej surogatów takich jak aplikacja w telefonie z wirtualną kartą (aplikacja inna niż Aplikacja MOB, np. GPay, ApplePay, HCE) oraz inne surogaty karty EMV (breloczki, zegarki itp.). W systemie musi być zapewniona identyfikacja surogatu karty i możliwość powiązania jej z oryginalną kartą poprzez numer PAR (Payment Account Reference) lub w inny równoważny sposób.

Zbliżeńiowe karty płatnicze EMV mogą być wykorzystywane w systemie zarówno jako identyfikatory jak i instrumenty płatnicze. Dlatego Wykonawca zapewni komplet usług Agenta rozliczeniowego kart EMV oraz Payment Gateway spełniające wymagania organizacji kartowych Visa/Mastercard (między

innymi do rozliczeń transakcji i tokenizacji). Zapewni również interfejsy, biblioteki do urządzeń/modułów w których może być wykorzystywany ten identyfikator.

Jako instrument płatniczy karta EMV będzie mogła zostać wykorzystana w pojazdach byłego MZK – do bezpośredniego zakupu biletu w pojeździe, dane o tych transakcjach będą zapisywane na koncie IKU (dla którego identyfikatorem jest ta karta EMV). W pozostałej części infrastruktury pojazdowej ŚKUP będzie można wykorzystywać jedynie bilety zapisane na koncie IKU powiązane z tym identyfikatorem, które można zakupić i aktywować na Portalu klienta lub w aplikacji mobilnej MOB lub w POP (nie wymagające aktywacji/skasowania w pojeździe).

Użytkownik tego identyfikatora musi mieć możliwość sprawdzenia historii operacji wykonywanych kartą EMV (i surogatem) oraz złożenia reklamacji i wnioskowania o fakturę zarówno w POP jak i na Portalu Klienta, również bez konieczności logowania się loginem na konto, poprzez wywołanie usługi tokenizującej numer PAN karty lub surogatu;

Powiązanie karty EMV do konta w systemie ŚKUP 1.5. musi być możliwe zarówno w POP jak i na Portalu Klienta (z wykorzystaniem mechanizmu tokenizacji);

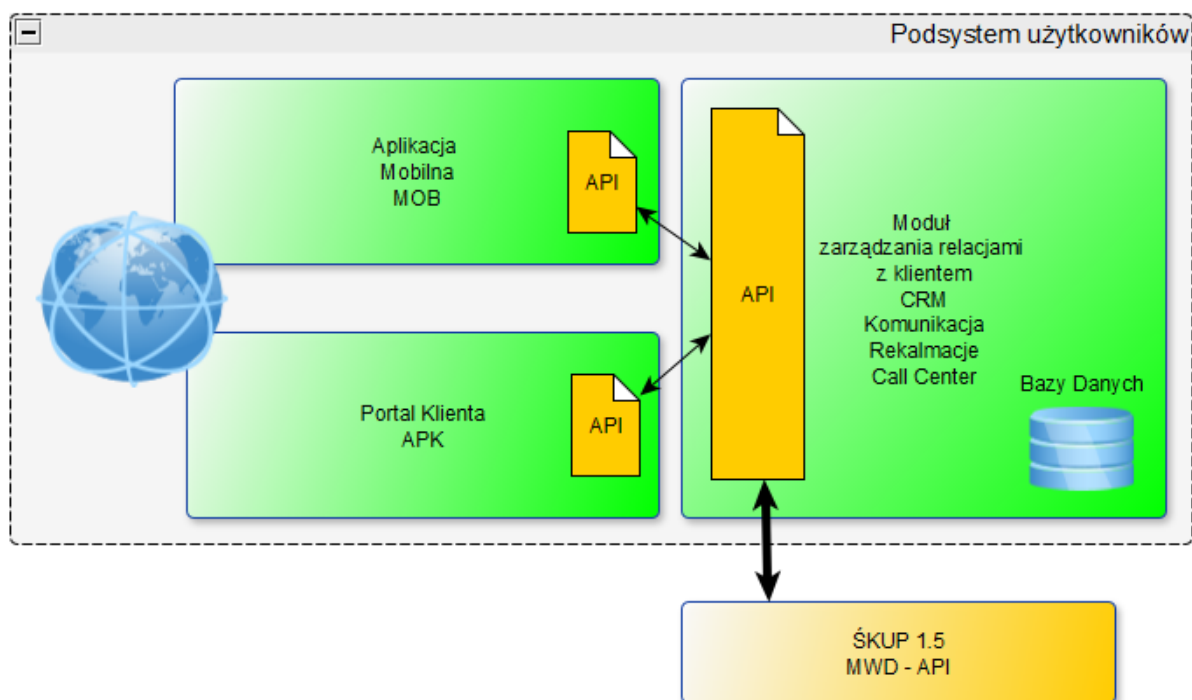
W systemie muszą zostać zapewnione wszystkie inne funkcjonalności związane z wymaganiami organizacji płatniczych oraz wymagania bezpieczeństwa przetwarzania operacji wykonywanych kartami płatniczymi, w tym zapewnienie zgodności z wymaganiami organizacji Visa oraz MasterCard czytników kart płatniczych w urządzeniach przez cały okres obowiązywania umowy - Wykonawca przed zgłoszeniem do odbioru winien dostarczyć prawidłowe i ważne certyfikaty potwierdzające zgodność z ww. wymogami. Koszty ewentualnej wymiany czytników kart płatniczych w okresie obowiązywania umowy, jeżeli zaistniałaby taka konieczność, pokrywa Wykonawca;

Zamawiający musi posiadać mechanizm blokowania identyfikatora w systemie ŚKUP 1.5 – w przypadku podejrzenia fraudów lub nieuprawnionego pozyskania usług.

4 Podsystem Użytkowników

Zadaniem modułów\aplikacji podsystemu użytkowników jest bezpośrednia obsługa użytkownika systemu ŚKUP z poziomu Portalu Klienta oraz Aplikacji Mobilnej. Operatorzy systemu będą mogli komunikować się z użytkownikami korzystając z modułu zarządzania relacjami z klientem. Funkcje dostępne z poziomu Portalu Klienta i Aplikacji Mobilnej powinny zapewnić jak największą samodzielność użytkownika, by odciążyć pracowników Zamawiającego. Podsystem powinien realizować procesy: kompleksowej obsługi konta użytkownika, reklamacyjne, informacyjne. W ramach podsystemu użytkowników wstępnie zaproponowano podział na następujące moduły\aplikacje\portal:

- Portal Klienta (APK);
- Aplikacja Mobilna (MOB);
- Moduł Zarządzania relacjami z klientami (CRM).



Rysunek 3. Poglądowy schemat Podsystemu Użytkowników.

4.1 Portal Klienta Systemu ŚKUP 1.5 (APK)

Podstawowy, dostępny publicznie w sieci internetowej z poziomu przeglądarki internetowej kanał do zarządzania kontem użytkownika oraz realizujący szereg innych funkcjonalności dostępnych w systemie. Portal Klienta Systemu ŚKUP 1.5 powinien być wizytówką systemu i wraz z Aplikacją Mobilną będzie stanowić kluczowy kanał do zarządzania kontem klienta. Funkcjonalność portalu należy rozpatrywać w kilku aspektach:

- Funkcjonalność części portalu dostępna dla klienta niezalogowanego;
- Funkcjonalność części portalu dostępna dla klienta zalogowanego do Indywidualnego Konta Użytkownika (IKU);
- Funkcjonalność części portalu dostępna dla klienta zalogowanego do Konta grupującego/firmowego;
- Funkcjonalność w ramach modułu CRM dostępna na potrzeby administrowania treścią portalu, obsługą reklamacji i infolinii.

Wykonawca przygotuje i będzie aktualizował w czasie całego okresu utrzymania interaktywną instrukcję obsługi (Pomoc) dla użytkowników portalu. Na każdym etapie obsługi portalu użytkownik będzie mógł wywołać pomoc, która wyświetli instrukcje dla aktualnego kontekstu.

4.1.1 Funkcjonalność dostępna publicznie – Część informacyjna Portalu Klienta dla klienta niezalogowanego

Funkcjonalność dostępna publicznie dla każdego użytkownika powinna umożliwiać w sposób łatwy i intuicyjny uzyskanie podstawowych informacji przede wszystkim o tym:

- W jaki sposób stać się pełnoprawnym użytkownikiem systemu ŚKUP 1.5, który ma dostęp do funkcjonalności po zalogowaniu;
- W jaki sposób dokonać rejestracji/modyfikacji konta IKU;
- Informacje o systemie ŚKUP 1.5;
- Chatroom;
- Opisy i instrukcje dot. funkcjonalności dostępnych w systemie ŚKUP 1.5;
- Odnośniki do stron prowadzonych przez ZTM zawierających: rozkłady jazdy i wyszukiwarę połączeń oraz stron podmiotowych ZTM i GZM, możliwość dodawania kolejnych stron.

Informacja dot. zakładania/zmiany rodzaju konta IKU powinna być udostępniona w atrakcyjnej postaci interaktywnego przewodnika, a sam proces powinien być ograniczony do niezbędnego minimum i dostępny na kilku zakładkach, na których zdefiniowane zostaną wszystkie konieczne informacje, a każda zakładka będzie krokiem widocznym jako postęp procesu (max 3-4 kroki). Dla użytkownika, który w jakikolwiek sposób przerwie proces, nie zostaną zarejestrowane w systemie wprowadzane dane i zostaną one usunięte.

Istotną częścią portalu będzie obszar, w którym publikowane będą wszelkiego rodzaju dokumenty dotyczące regulaminów, cenników, taryf itp. Sekcja ta powinna posiadać możliwość wersjonowania każdego rodzaju dokumentu oraz publikacji jego treści w postaci umożliwiającej jego wydruk i zapisanie na dysk (format pdf).

Kolejną częścią dostępną publicznie z poziomu portalu powinna być informacja ogólna zawierająca treść dotyczącą możliwości kontaktu z właścicielem systemu, funkcjonowania infrastruktury systemu ŚKUP 1.5 wraz z wykazem infrastruktury tj. liczbą wyposażonych pojazdów, zamontowanych automatów, tablic SDIP, przystanków, wraz z informacją zawierającą ich lokalizację, dostępnością funkcjonowania placówek POP, punktów dystrybucji biletów itp. (np. godziny ich otwarcia) z podziałem na gminy i możliwością ich wyszukiwania i prezentowania na mapie.

Poza tym powinien zawierać zawsze aktualne instrukcje obsługi urządzeń samoobsługowych w tym symulatory wideo urządzeń w pojazdach, jak i wykaz spraw, możliwych do załatwienia w danym kanale.

Na portalu powinien być dostępny chatroom jako kanał kontaktu bezpośredniego z użytkownikiem, który chce uzyskać informację, a nie potrafi jej znaleźć. Kanał ten powinien być obsługiwany przez pracowników infolinii oraz wspomaganych przez chatboota (do zainicjowania rozmowy i udzielania oczywistych odpowiedzi – definiowanych w przygotowanym do tego celu narzędziu). Zarządzanie chatroomem powinno uwzględniać statystyki zadawanych pytań, tak by można było przygotować i zaimplementować dla nich odpowiedzi. Podniesie to jakość oferowanej usługi.

Istotną rolę informacyjną na portalu ma sekcja przeznaczona do publikowania komunikatów alarmowych. Powinny one zawierać informacje dotyczące przerw w funkcjonowaniu elementów infrastruktury systemu lub uruchomieniu nowego rodzaju usługi. Treść powinna być ograniczona i pojawiać się w widocznym, lecz dyskretnym miejscu (np.: górny pasek przewijany w sposób jak na stronie notowań giełdowych).

Ostateczny wizerunek portalu, szata graficzna i wszelkie elementy interakcji z użytkownikiem powinny być responsywne w stosunku do różnych urządzeń oraz dostosowane do innych stron Metropolii i ZTM.

Użytkownik będzie miał możliwość obsługi konta nieprofilowanego na portalu w zakresie do niego przypisanym, wykorzystując do tego dane identyfikatora (np. numer i PIN dla karty ŚKUP i ŚKUP 1.5).

Użytkownik będzie miał możliwość przekształcenia konta nieprofilowanego w konto profilowane w oparciu o dane/mechanizmy pozwalające na obsługę na portalu konta IKU nieprofilowanego i podany adres e-mail lub numer telefonu (do weryfikacji poprzez SMS).

Użytkownik będzie miał możliwość resetowania hasła do indywidualnego konta klienta oraz konta grupującego, realizowanego zgodnie z procedurą polegającą na przesłaniu na przypisany do konta adres mailowy aktywnego linka (aktywowanego tylko raz) lub kodu wysłanego SMS-em do nadania nowego hasła.

Użytkownicy kart płatniczych EMV i surogatów będą mieli możliwość sprawdzenia historii operacji wykonywanych tymi identyfikatorami, spłaty zadłużenia, możliwość złożenia reklamacji i śledzenia jej stanu oraz złożenia wniosku i pobrania faktury (bez konieczności posiadania loginu do konta IKU) oraz możliwość założenia konta profilowanego. Funkcjonalność będzie realizowana z wykorzystaniem procesu tokenizacji obowiązującego w systemie.

4.1.2 Funkcjonalność dostępna po zalogowaniu (Indywidualne Konto Użytkownika) – Część do zarządzania kontem IKU

Proces logowania wymaga podania Loginu lub Aliasu konta oraz hasła zachowującego określone zasady bezpieczeństwa.

W sekcji zarządzania kontem użytkownika powinny być dostępne następujące funkcjonalności:

- Zarządzanie danymi użytkownika i cechami konta IKU;
- Samodzielne definiowanie, zmianę, resetowanie hasła do konta z zachowaniem mechanizmów autoryzacji (email/SMS);
- Zmiana rodzaju konta;
- Reaktywacja konta archiwalnego;
- Dodanie, zmiana (X razy w ciągu dnia, zgodnie z parametrem (X) zdefiniowanym w systemie;) i usunięcie identyfikatora;
- Usunięcie dostępu do historii operacji dla usuniętego identyfikatora (domyślnie historia dla każdego identyfikatora nawet usuniętego powinna być dostępna. Klient wyłącza jedynie dostęp do historii w ramach swojego konta);
- Informacja o statusie identyfikatora/ów oraz dacie jego/ich ważności;
- Zakup biletu/biletów, w tym kilku biletów różnego rodzaju w jednej transakcji (tzw. koszyk biletów);
- Zasilenie i wnioskowanie o zwrot środków dla niewykorzystanych punktów;
- Zwrot biletu/ów wg zadanego algorytmu uzgodnionego z Zamawiającym;
- Dostęp do historii operacji finansowych i niefinansowych na koncie IKU w zdefiniowanym przez użytkownika okresie czasu z możliwością wyeksportowania do pliku PDF i CSV. Historia powinna zawierać minimum następujące dane: data i czas zdarzenia, saldo punktów, kwota operacji (dla operacji finansowej), liczba zakupionych/użytych biletów/usług, nazwa biletu/usługi, nr linii (jeśli dotyczy), przystanek/lokalizacja wykonania operacji, rodzaj operacji, GIT, użyty identyfikator;
- Wnioskowanie o fakturę w oparciu o zakupione usługi zgodnie z obowiązującym prawem podatkowym oraz pobieranie wystawionych faktur (wykonywane poprzez zaznaczanie pozycji na liście zakupionych usług, nie można zaznaczyć usług, dla których już był wniosek o fakturę);
- Spłata zadłużenia na karcie EMV;
- Zablokowanie/odblokowanie identyfikatora (zagubienie, kradzież, itp.) z wykorzystaniem mechanizmów bezpieczeństwa zaproponowanych przez Wykonawcę opartych o analizę ryzyka;
- Możliwość zdefiniowania domyślnej ulgi/ulg na okres zgodny z przysługującym uprawnieniem (np. wskazanie daty od-do, bezterminowo itp.), na podstawie słownika ulg definiowanego w MTC, musi istnieć możliwość wskazania jednej lub więcej ulg. Ulga wprowadzona do systemu przez użytkownika nie jest autoryzowana, wymaga autoryzacji w POP lub przez kontrolera podczas prowadzonych czynności (UKNT);
- Zarządzanie notyfikacją (możliwość włączenia lub wyłączenia powiadomień) w zakresie:
 - przypominania o kończącym się terminie ważności biletu okresowego;

- wygasania ulgi (profilu przejazdu) i konieczności jej odnowienia;
- dostępu do publikowanych informacji dotyczących utrudnień w funkcjonowaniu komunikacji miejskiej;
- dostępu do informacji specjalnej (specjalnych ofertach, zdarzeniach organizowanych przez przewoźników – dni otwarte, akcji promocyjnych Metropolii itp.);
- powiadomienia o aktualnym stanie przetwarzania skarg, wniosków i reklamacji;
- powiadomienia o statusie przetwarzanej transakcji;
- Możliwość utworzenia konta grupującego poprzez założenie loginu w postaci unikatowego Aliasu, składającego się z ilości cyfr adekwatnej do poziomu ryzyka wynikającego z przeprowadzonej analizy przez Wykonawcę, który może być zmienione przez użytkownika;
- Możliwość personalizacji konta (proces personalizacji powoduje udostępnienie dodatkowych informacji do przetwarzania w procesie obsługi klienta);
- Możliwość komunikacji z infolinią poprzez moduł CRM: predefiniowane formularze wysyłania wiadomości w zależności od wyboru rodzaju wiadomości, odczyt wiadomości poprzez skrzynkę wiadomości z widoczną ikoną informującą o wiadomościach oczekujących na odczytanie;
- Odbiór, wysyłanie i prezentacja wiadomości pokrywającej się z funkcjonalnością programów do obsługi poczty elektronicznej;
- Możliwość złożenia reklamacji i zarządzania nią oraz odbieranie informacji związanych z koniecznością uzupełnienia i rozstrzygnięciem reklamacji oraz uzupełnienia reklamacji i złożenia odwołania do rozstrzygniętej reklamacji (integracja z CRM);
- Możliwość zaakceptowania regulaminów/zgód itp. wygenerowanych w module CRM;
- Możliwość wypełniania ankiet formularzy wygenerowanych w module CRM.

Profilowanie konta IKU

Użytkownik uzupełnia dane przy użyciu formularza ze zdefiniowanymi polami, dane takie jak adres mailowy, nr tel. komórkowego są autoryzowane przez przesłanie kodu do potwierdzenia w kolejnym kroku.

Personalizacja konta IKU profilowanego

Użytkownik uzupełni dane osobowe przy użyciu formularza ze zdefiniowanymi polami, w tym ma mieć możliwość przesłania zdjęcia, ze swoim wizerunkiem. Portal musi wspierać autoryzację danych użytkownika poprzez wykorzystanie metod zdalnych takich jak podpis kwalifikowany, profil zaufany, platforma EPUAP, bankowe kanały autoryzacji. Jeśli metoda umożliwia takie działanie, użytkownik nie wprowadza danych jedynie je akceptuje. Dane autoryzowane metodą zdalną nie wymagają autoryzacji danych w POP lub UKNT.

4.1.3 Funkcjonalność dostępna po zalogowaniu (Konto Grupujące) – Część do zarządzania kontem grupującym na Portalu Klienta

W założeniu konto grupujące służy do pełnego zarządzania Indywidualnymi Kontami Użytkowników np. rodzice zarządzający kontami dzieci/współmałżonka/inne.

W sekcji zarządzania kontem grupującym powinny być dostępne następujące funkcjonalności:

- Dodanie, usunięcie Indywidualnego Konta Użytkownika do grupy (pojedyncze konto indywidualne może być podłączone do jednej grupy). Proces dodania konta indywidualnego do grupy wymaga potwierdzenia przez właściciela konta indywidualnego (aktywacja usługi w postaci przesłanego linku aktywacyjnego). Proces usunięcia IKU z grupy musi być możliwy zarówno z poziomu konta grupującego jak i z poziomu dodanego konta IKU;
- Dokonywanie zakupu i zwrotu biletów w tym w postaci koszyka zakupu, dla wielu kont równocześnie, w tym biletów R1;
- Zasilanie konta e-portmonetki dla kilku kont indywidualnych podłączonych do konta grupującego;
- Zwroty biletów pojedynczych, wybranych, wszystkich, pojedynczo lub dla wielu kont równocześnie;
- Zarządzanie kontami w poszczególnych, oddzielnych widokach lub w widoku zbiorczym (np. zbiorczy widok biletów);
- Definiowanie ulgi dla określonego konta indywidualnego;
- Usunięcie/zamknięcie konta grupującego;
- Przechowywanie historii operacji dokonywanych w ramach konta grupującego;
- Wnioskowanie o fakturę w oparciu o zakupione kontrakty oraz pobieranie wystawionych faktur; prawo do wnioskowania o fakturę dla kontraktów zakupionych przy wykorzystaniu konta grupującego pozostaje w zakresie konta grupującego;
- Samodzielne definiowanie, zmiana, resetowanie hasła z zachowaniem mechanizmów autoryzacji (adresu email lub SMS), hasło powinno umożliwiać wprowadzenia dużych, małych liter, cyfr i znaków specjalnych oraz powinno się składać z minimalnej ilości znaków (dla poszczególnych rodzajów znaków) zgodnie z regułami definiowanymi przez Administratora Zmawiającego na podstawie analizy ryzyka przedstawionego przez Wykonawcę.

4.1.4 Funkcjonalność dostępna po zalogowaniu (Konto firmowe) – Część do zarządzania kontem firmowym na Portalu Klienta

W założeniu konto firmowe służy do grupowego kupowania i zwrotów kontraktów dla Kont Użytkowników np. pracownicy, członkowie i podopieczni instytucji społecznych itp.

W sekcji zarządzania kontem firmowym powinny być dostępne następujące funkcjonalności:

- Zdefiniowanie danych firmy/instytucji itp. niezbędnych do wystawienia faktury zgodnie z obowiązującymi przepisami prawa;
- Dodanie, usunięcie Indywidualnego Konta Użytkownika do grupy (pojedyncze konto indywidualne może być podłączone do jednej lub wielu grup). Proces dodania konta indywidualnego do grupy wymaga potwierdzenia przez właściciela konta indywidualnego (np. aktywacja usługi w postaci przesłanego linku aktywacyjnego), usunięcie konta z grupy nie wymaga potwierdzenia;
- Dokonywanie zakupu i zwrotu uprawnień do usług dla zdefiniowanych i wybranych kont indywidualnych podłączonych do konta firmowego, w kontekście konta indywidualnego można jedynie przeglądać te uprawnienia do usług bez prawa zwrotu i bez prawa wnioskowania o fakturę;

- Możliwość wnioskowania o fakturę w oparciu o zakupione uprawnienia do usług w ramach konta firmowego, odbiór faktury jedynie w kontekście konta firmowego;
- Z poziomu konta można zarządzać (przeglądać, zwracać) tylko tymi uprawnieniami do usług, które zostały nabyte przy użyciu konta firmowego, pozwoli to na izolację usług pochodzących od różnych kont firmowych oraz indywidualnych pochodzących od Konta Indywidualnego;
- Usunięcie/zamknięcie konta firmowego;
- Przechowywanie i generowanie historii operacji dokonywanych w ramach konta grupującego;
- Definiowanie, zmiana, odzyskiwanie hasła zgodnie z zasadami opisanymi dla Konta Grupującego.

4.1.5 Funkcjonalność dostępna po zalogowaniu się jako Administrator portalu – zarządzania treścią Portalu Klienta (dostęp przez moduł CRM)

Część portalu udostępniająca funkcjonalności administracyjne i zarządzania treścią dostępne będą po zalogowaniu użytkownika ze specjalnymi uprawnieniami przyznanymi adekwatnie do pełnionej roli. Zarządzanie treścią portalu powinno być zbudowane w oparciu o funkcjonalność modułu CRM umożliwiającą:

- Publikację artykułów w ramach zdefiniowanych szablonów;
- Zarządzanie wersjami publikowanych artykułów;
- Generowanie raportów dotyczących popularności poszczególnych artykułów;
- Podłączenie portalu do narzędzia uzgodnionego z Zamawiającym do analizy statystyk serwisów WWW, oraz jego utrzymywanie;
- Tworzenie użytkowników z odpowiednim poziomem uprawnień do zarządzania treścią (redaktor, recenzent, administrator);
- Możliwość publikacji i zarządzania treścią multimedialną;
- Publikowanie artykułów wg zdefiniowanej daty publikacji i ważności;
- Prezentowanie licznika odwiedzin;
- Prezentowanie redaktorów artykułu;
- Zarządzanie pozycjami menu;
- Możliwość publikacji treści w tle (np. z bazy danych w której zmieniają się wartości i są one dynamicznie odświeżone na stronie);
- Budowanie własnych szablonów strony i elastycznego ich modyfikowania;
- Zarządzanie usługą chatroom i chatbootem (prezentacja, statystyki pytań, odpowiedzi itp.);
- Budowanie wielu mini portali (podstrony tematyczne, posiadające własny układ i menu) i zarządzanie nimi w ramach jednego Web CMS;
- Zarządzanie warstwą danych GIS prezentowanych na mapach.

Poza tym Portal ma mieć możliwość integracji z popularnymi portalami społecznościowymi oraz powinien mieć możliwość korzystania z API GoogleMaps/OpenstreetMaps i innych otwartych systemów GIS w celu wizualizacji warstw danych.

4.1.6 Funkcjonalności związane z rozliczeniami

- 1) Rodzaje operacji finansowych:

- zasilenie konta e-portmonetki i sprawdzenie jego salda;
- zakup biletu i koszyka biletów;
- zwrot biletu – we wniosku musi być możliwość podania rachunku, na który dokonany zostanie zwrot;
- uiszczenie opłaty dodatkowej;
- spłata zadłużenia EMV;

2) Rodzaje płatności:

- obciążenie konta e-portmonetki punktowej;
- płatność kartą płatniczą z wykorzystaniem bramki internetowej;
- metody płatności takie jak BLIK, OneClick, Google Pay, Apple Pay;
płatności pay-by-link (szybki przelew internetowy), np. z wykorzystaniem bramek internetowych takich jak „przelewy24” lub „payu” lub równoważne zadeklarowane przez Wykonawcę w ofercie + dodatkowo metody/płatności internetowe zadeklarowane przez Wykonawcę w ofercie.

W ramach wynagrodzenia Wykonawcy wymagana jest maksymalna dostępna w czasie wdrożenia ilość metod płatności dla użytych bramek internetowych w tym metody obejmujące konta biznesowe (dla banków które udostępniają takie metody) oraz ich uzupełnianie lub modyfikację w trakcie okresu utrzymania np. w przypadku pojawienia się nowych metod płatności lub zmian organizacyjno-prawnych po stronie banku (np. przejęcie). Zamawiający przewiduje dodanie maksymalnie dwóch tego typu metod rocznie. Każdorazowo dodanie nowej metody płatności zostanie uzgodnione z Zamawiającym.

4.1.7 Wnioski o fakturę

Interfejs faktur musi zapewniać dwustronną komunikację pomiędzy systemem ŚKUP 1.5 i systemem księgowym Zamawiającego (przy zachowaniu tych samych zasad i formatów plików) z innymi Dostawcami usług, którzy będą chcieli z niego skorzystać. Parametryzowanie nowego odbiorcy faktur musi odbywać się poprzez interfejs użytkownika udostępniony Zamawiającemu. Wnioski o fakturę muszą być możliwe do pobrania z systemu ŚKUP 1.5 maksymalnie co godzinę. Czas ten musi być określony parametrem systemu. Wnioski muszą zawierać wszystkie informacje niezbędne do wystawienia i udostępnienia faktury (dane odbiorcy lub płatnika faktury, kanał udostępnienia faktur itd.), dane systemowe (parametry kontraktu) oraz identyfikator konta, z którego został wygenerowany wniosek. Nie można wnioskować o wystawienie faktury na transakcje, do której faktura już wcześniej została wystawiona. Zwrotnie musi być uruchomiony proces importujący przygotowane faktury w formacie PDF do systemu ŚKUP 1.5 i udostępniający je w odpowiednich kanałach (np. informacja na Portalu, Aplikacji Mobilnej, w aplikacji APO, na adres poczty elektronicznej użytkownika). Dodatkowo użytkownik konta powinien otrzymać powiadomienie o fakcie udostępnienia dla niego faktury, w kanałach, które wskazał (np. Portal, Aplikacja Mobilna, e-mail, SMS). Proces importowania faktur do systemu ŚKUP 1.5 również powinien być uruchamiany zgodnie z parametrem ustawianym w systemie przez Zamawiającego.

4.1.8 Technologia

- Pełna zgodność ze standardem WCAG 2.1;

- Zaimplementowany mechanizm CAPTCHA;
- Strona musi być responsywna i obsługiwana poprawnie na co najmniej pięciu najbardziej popularnych przeglądarkach internetowych (na chwilę obecną są to: Mozilla Firefox, Google Chrome, Microsoft Edge, Opera, Safari), Zamawiający wymaga utrzymywania kompatybilności z najnowszymi wydaniem przeglądarek;
- Możliwość zalogowania się operatora aplikacji Call-Center (CRM) w kontekście konta konkretnego pasażera (po wcześniejszej autoryzacji osoby dzwoniącej w systemie IVR);
- Możliwość interakcji z pracownikiem infolinii (CRM) do obsługi klientów chatroomu;
- Portal Klienta powinien być rozwiązaniem klasy Enterprise i powinien zostać przetestowany pod kątem bezpieczeństwa z przeprowadzeniem testów penetracyjnych włącznie;
- Należy zastosować mechanizmy typu Web Application Firewall do ochrony zasobów portalu;
- Wykupienie i zabezpieczenie strony certyfikatem SSL z pełną weryfikacją podmiotu, szyfrowaniem 256 bitów, certyfikat odpowiedni dla instytucji publicznych/banków z gwarancją finansowania;
- Należy zastosować mechanizmy balansowania obciążenia i skalowalności rozwiązania w sytuacji dużego obciążenia strony.

4.2 Aplikacja Mobilna ŚKUP (MOB)

Podstawowy, instalowany na urządzeniach mobilnych działający w środowiskach Android i iOS, dostępny publicznie w sieci internetowej, kanał do zarządzania kontem użytkownika oraz realizujący szereg innych funkcjonalności dostępnych w systemie.

4.2.1 Opis ogólny

Aplikacja Mobilna ŚKUP powinna umożliwiać pasażerowi zakup wszystkich biletów analogicznie jak na Portalu Klienta (APK), realizować wszystkie funkcje Portalu Klienta ŚKUP 1.5 m.in.: zarządzanie swoim Indywidualnym Kontem Użytkownika, zarządzanie identyfikatorami, wyszukiwanie połączeń oraz lokalizowanie pozycji pojazdu w czasie rzeczywistym (funkcjonalność do uruchomienia w ramach godzin rozwojowych).

Jest możliwość uruchomienia aplikacji bez konieczności powiązania jej z kontem IKU. Bez powiązania z kontem IKU będzie możliwe skorzystanie z funkcji opisanych w punkcie dot. użytkowników niezalogowanych.

Aplikacja powinna reagować na zdarzenia (komunikaty) przypisane do danych linii/przystanków/przystanków sąsiednich na podstawie pozycjonowania GPS, użytkownik, który znajdzie się w obrębie danego przystanku otrzyma komunikaty dot. wszystkich zdarzeń (komunikaty, odjazdy) przypisanych dla danego przystanku (jeżeli komunikaty występują w kontekście linii, to należy uwzględnić wszystkie przystanki, które dana linia obsługuje). Komunikaty powinny być wyświetlane także (bez lokalizowania GPS) w przypadku wskazanych w ustawieniach aplikacji linii i przystanków obserwowanych.

Wykonawca proponuje rozwiązanie uniemożliwiające korzystanie z Aplikacji Mobilnej ŚKUP na kilku urządzeniach równocześnie, w ramach jednego konta IKU.

Ze względu na wrażliwy charakter przetwarzanych danych, należy zastosować mechanizmy informacyjne i bezpieczeństwa zgodne z polityką RODO w tym prawo do sprawdzenia, modyfikacji i zapomnienia danych.

4.2.2 Funkcjonalności Aplikacji Mobilnej

- a) Zakładanie konta;
- b) Zarządzanie kontem i identyfikatorami;
- c) Funkcja informacyjna – komunikaty, historia użycia ŚKUP 1.5;
- d) Zarządzanie treścią – po stronie część back-office (CRM);
- e) Funkcja zakupowa - możliwość dokonywania zakupów usług (wszystkich rodzajów biletów jednorazowych/krótkookresowych, średniookresowych, długookresowych) biletów wspólnych z innymi organizatorami (oferta specjalna tj. np. Metrobilet) oraz w taryfie CICO;
- f) Zwrot biletów wg zadanego algorytmu uzgodnionego z Zamawiającym;
- g) Pay and go (zakup biletu krótkookresowego aktywowanego w momencie zakupu);
- h) Zasilenie e-portmonetki i zwrot niewykorzystanych środków;
- i) Uprawnienie do przejazdu – kontrola biletów (kody QR dla kontrolerki);
- j) Aktywacja biletów z konta IKU;
- k) Wnioskowanie i otrzymywanie faktur (wysyłanych na maila);
- l) Skrzynka kontaktowa z ZTM;
- m) Składanie reklamacji;
- n) Funkcja widżetu prezentująca rozkłady jazdy z przystanków, z których użytkownik będzie najczęściej realizował swoją podróż komunikacją miejską – w trybie rzeczywistym, w tym prezentacja komunikatów dotyczących wybranych linii, przystanków, globalnych komunikatów.

Opcjonalne funkcjonalności do realizacji w ramach godzin rozwojowych:

- Integracja z SDIP (w tym możliwość sprawdzenia ewentualnego opóźnienia danego połączenia);
- Wyświetlenie mapy i wskazanie (dzięki usłudze lokalizacji) najbliższych przystanków, po ich naciśnięciu wyświetlenie linii obsługujących dany przystanek oraz możliwości przejścia poprzez kliknięcie w nie do rozkładów jazdy;
- Wyszukiwanie połączeń;
- Aplikacja ma posiadać funkcję nawigowania podróznego wg zaplanowanej trasy, a w tym funkcję budzika/przypomnienia o zbliżającym się przystanku docelowym oraz funkcję budzika/przypomnienia o zbliżającym się czasie rozpoczęcia zaplanowanej wcześniej podróży;
- Wybór i prezentację także w trybie offline rozkładów jazdy oraz przystanków, z których użytkownik najczęściej korzysta;
- Wyszukiwanie pojedynczych rozkładów jazdy;
- Po wybraniu przystanku możliwość sprawdzenia najbliższych przyjazdów, a po kliknięciu w numer linii środka komunikacji pokazanie jego położenia na mapie i pokazanie przebiegu kursu (opóźnienia/przyspieszenia);
- Funkcja planowania podróży (w tym przejścia piesze) z wykorzystaniem dostępnych środków transportu (cały ŚKUP 1.5, docelowo przewiduje integrację z Maas) oraz z uwzględnieniem ich rzeczywistych pozycji (algorytm planowania musi uwzględniać opóźnienia/wypadnięcia i przyspieszenia co jest szczególnie istotne przy planowaniu przesiadek – dotyczy wyszukiwania

w trybie „teraz”, nie dotyczy wyszukiwań wg zadanej daty i czasu) oraz powinna wskazywać cenę przejazdu.

4.2.3 Dostęp do aplikacji

Aplikacja powinna umożliwiać dostęp do podstawowych funkcji dla użytkowników niezalogowanych oraz dostęp do wszystkich funkcjonalności dla użytkowników zalogowanych.

4.2.4 Funkcje dostępne dla użytkowników niezalogowanych

Aplikacja umożliwia użytkownikom niezalogowanym dostęp do ograniczonej liczby funkcji oraz wymusza autentykację w przypadku chęci dokonywania zakupów. Aplikacja działająca w trybie niezalogowanym umożliwia:

- Dostęp do funkcji informacyjnych takich jak: komunikaty organizatora komunikacji miejskiej, dostęp do rozkładów jazdy, dokumentów, taryfy i regulaminów;
- Linki do stron wskazanych przez Zamawiającego;
- Możliwość wyświetlania treści/komunikatów o charakterze informacyjno-promocyjnym.

4.2.5 Funkcje dostępne dla użytkowników zalogowanych

W przypadku smartfonów posiadających zaawansowane funkcje autoryzacji z poziomu systemu operacyjnego (skanowanie odcisku palca, rozpoznawanie twarzy), należy przewidzieć możliwość ich wykorzystania w celu zalogowania, bez konieczności wpisywania loginu i hasła, wymaga wcześniejszego poprawnego zalogowania oraz świadomej akceptacji użytkownika (na poziomie urządzenia). Aplikacja nie będzie przechowywała danych biometrycznych użytkownika, a jedynie korzystała z funkcjonalności systemu operacyjnego urządzenia.

Aplikacja umożliwia użytkownikom zalogowanym dostęp do pełnej funkcjonalności, w tym opisanej w części dla użytkowników niezalogowanych, a w szczególności:

- Obsługę konta (IKU) w przypadku konta: profilowanego, profilowanego imiennego (personalizowanego);
- Zakupy usług w uproszczonej formule w tym bez konieczności każdorazowej autentykacji, płatności jednym kliknięciem lub równoważne;
- Zasilenie e-portmonetki;
- Zakupy biletów krótkookresowych oraz w taryfie CICO – tryb ręczny (może wymagać podania nr linii i nr wozu, zalecane aby aplikacja podpowiadała taką informację na podstawie pozycji GPS) oraz w trybie automatycznym z wykorzystaniem kodów QR lub Tag NFC umieszczonych w pojeździe, z których zostaną czytane informacje niezbędne do zakupienia biletów;
- Funkcja widżetu szybki zakup ulubionego biletu;
- Sprawdzenie liczby i rodzajów biletów zakupionych na konto IKU;
- Po wybraniu biletu ma być możliwe rozwinięcie jego szczegółów: strefa obowiązywania, czas ważności, cena, pozostały limit przejazdów i inne uzgodnione z Zamawiającym;

- Możliwość zmiany identyfikatora do konta IKU - X razy w ciągu dnia, zgodnie z parametrem (X) zdefiniowanym w systemie;
- Możliwość zakupu biletów okresowych oraz ofert wspólnych z innymi Organizatorami;
- Zwrot biletów wg zadanego algorytmu uzgodnionego z Zamawiającym;
- Możliwość kontroli biletów aktywowanych przez pasażera, bezpośrednio w aplikacji poprzez kontrolę wzrokową i skanowanie kodu QR przez kontrolera;
- Wygenerowanie historii operacji finansowych i niefinansowych na koncie IKU w zadanym przez użytkownika okresie czasu oraz eksport historii do plików PDF, CSV;
- Wnioskowanie o fakturę zgodnie z zasadami określonymi dla Portalu Klienta;
- Możliwość napisania i odczytywania wiadomości do/od administratora (uwagi, propozycje, awarie) -> integracja z modułem CRM;
- Reklamacje: składanie wg tematów, przegląd, uzupełnianie, informowanie o przebiegu – integracja z modułem CRM w zakresie reklamacji;
- Zgłaszanie awarii i utrudnień w ruchu (stan taboru także czystość, wiaty, uszkodzona tablica SDIP, uszkodzona tabliczka rozkładu jazdy na przystanku, słownik do uzgodnienia z Wykonawcą);
- Możliwość powiadamiania pasażera o kończącej się ważności biletów okresowych, małej ilości pozostałego limitu przejazdów w bilecie wieloprzejazdowym, kończących się środkach na rachunku punktowym;
- Możliwość zbudowania programu lojalnościowego w oparciu o historię korzystania z biletów okresowych, jednorazowych;
- Możliwość zamknięcia lub zablokowania lub zarchiwizowania konta klienta;
- Blokowanie/odblokowanie identyfikatora;
- Aplikacja ma zostać zabezpieczona loginem i hasłem konta IKU, oraz ma mieć możliwość wykorzystania (po pierwszym udanym logowaniu) mechanizmów zabezpieczających wykorzystywanych na poziomie systemu operacyjnego (odcisk palca, rozpoznawanie twarzy itp.).

4.2.6 Funkcjonalności związane z rozliczeniami

1) Rodzaje operacji finansowych:

- Zakup biletów jednorazowych/krótkookresowych w taryfie czasowej, strefowej i odległościowej z możliwościami przesiadki, średniookresowych, długookresowych, ofert wspólnych z innymi organizatorami) oraz w taryfie CICO ;
- Zakup w pojeździe biletu krótkookresowego, wymagający interakcji z użytkownikiem/odczytanie Kodu QR lub Tag NFC;
- Zwrot biletu we wniosku musi być możliwość podania rachunku, na który dokonany zostanie zwrot;
- Zasilenie rachunku e-portmonetki i sprawdzenie jej salda;
- Spłata zadłużenia karty EMV;
- Uiszczenie opłaty dodatkowej;

2) Rodzaje płatności:

- obciążenie konta e-portmonetki

Górnośląsko-Zagłębiowska Metropolia
40-053 Katowice
ul. Barbary 21A
tel. +48 32 718 07 00, fax +48 32 718 07 99
email: za@metropoliagzm.pl
www.metropoliagzm.pl

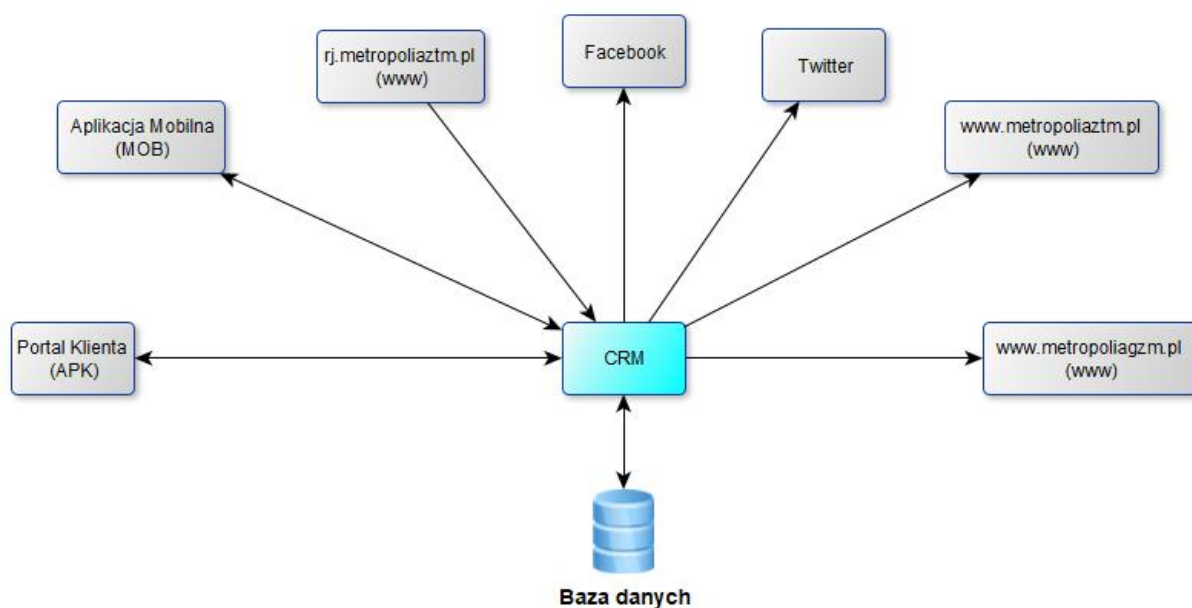


- płatność kartą płatniczą z wykorzystaniem bramki internetowej;
- metody płatności takie jak BLIK, OneClick, Google Pay, Apple Pay;
- płatności pay-by-link na takich samych zasadach jak dla Portalu Klienta włącznie z zasadami dodawania nowych metod;

4.3 Moduł zarządzania relacjami z klientem (CRM)

4.3.1 Komunikacja z Użytkownikiem

CRM pełni rolę kompleksowej obsługi wiadomości między użytkownikami, a operatorami systemu ŚKUP 1.5, oraz centralnej obsługi i wymiany komunikatów, w tym z innymi systemami informacyjnymi Zamawiającego składających się z CMS (ang. Content Management System), API wymiany danych, zintegrowany z funkcjonalnościami Portalu Klienta (APK), Aplikacją Mobilną (MOB), zasilany danymi m.in. z serwera rozkładów jazdy Zamawiającego (rj.metropoliagzm.pl), udostępniający komunikaty na potrzeby innych serwisów.



Rysunek 4. Schemat obsługi komunikacji z użytkownikami

4.3.2 Zarządzanie komunikatami

- Kompleksowe zarządzanie zawartością stron (artykuły, menu, formularze), komunikatami: tworzenie, modyfikowanie, usuwanie, wyświetlanie, przypisywanie, publikowanie (wg zadanej daty i czasu od - do, dla: APK, MOB, inne poprzez API), dane o: utworzeniu, każdej kolejnej modyfikacji, usunięciu - (użytkownik, data, czas) itp.;
- Możliwość umieszczania obiektów takich jak: obrazy (JPG, PNG, GIF), tabelki, znaczniki mapowe, linki z wykorzystaniem wbudowanego edytora treści (podstawowe formatowanie tekstu: rodzaj czcionki i wielkość, pogrubienie, pochyleniem, podkreślenie, kolor czcionki i tła, itp.);
- Struktura komunikatów wg przyjętych standardów RSS;
- Kompleksowe zarządzanie rodzajami komunikatów: tworzenie, modyfikowanie, usuwanie, wyświetlanie, przypisywanie, definiowanie zakresu uprawnień redaktorom, itp.;

- e) Predefiniowane rodzaje komunikatów: dot. funkcjonowania komunikacji (objazdów, opóźnień, wypadnięć, planowanych i nieplanowanych zmian tras autobusów tramwajów i trolejbusów, pociągów);
- f) Wysyłania komunikatów dotyczących marketingu, wizerunku, informacji;
- g) Definiowanie priorytetów komunikatów (trzy poziomy);
- h) Definiowanie zasięgu komunikatów wg obszaru (wbudowany edytor mapowy pozwalający zdefiniować obszar przy użyciu obiektów: koło, prostokąt wielobok);
- i) Definiowanie zasięgu komunikatów w zakresie określonych gmin (dot. filtra w Aplikacji Mobilnej wg nazwy gminy oraz wg obszaru terytorium);
- j) Definiowanie zasięgu w zakresie linii komunikacyjnych (dot. filtra w Aplikacji Mobilnej oraz wg obszarów przystanków);
- k) Definiowanie zasięgu w zakresie przystanków (dla linii automatycznie powinno nastąpić przypisanie obsługiwanych przystanków).

4.3.3 Zarządzanie wiadomościami

- a) Kompleksowe zarządzanie wiadomościami do/od użytkowników systemu ŚKUP 1.5;
- b) Odbiór, wysyłanie i prezentacja wiadomości od/do użytkowników pokrywająca się z funkcjonalnością programów do obsługi poczty elektronicznej;
- c) Zdefiniowane katalogi: odebrane, wysłane, usunięte, archiwum;
- d) Opcja odpowiedz, przekaż dalej, eksportuj do pliku;
- e) Grupowanie wiadomości wg konwersacji;
- f) Książka adresowa użytkowników systemu (wyślij DO);
- g) Zdefiniowana grupa globalna wszyscy użytkownicy;
- h) Opcja wysłania wiadomości na zewnątrz na wskazany adres mailowy;
- i) Możliwość definiowania własnych katalogów;
- j) Możliwość definiowania rodzajów wiadomości, w tym wiadomości wymagające akceptacji;
- k) Dostępne pola: adresaci, nadawca, temat, treść, załączniki, identyfikator wiadomości, rodzaj wiadomości, priorytet, data wysłania, data odczytu, [data akceptacji];
- l) Potwierdzanie przeczytania wiadomości, zatwierdzania w przypadku nadania statutu akceptacji;
- m) Wyszukiwanie wiadomości wg występujących pól;
- n) Definiowanie niepowtarzalnego id wiadomości;
- o) Grupowanie wiadomości wg występujących pól;
- p) Tworzenie wiadomości we wbudowanym edytorze (podstawowe formatowanie tekstu: pogrubienie, pochycenie, podkreślenie, kolor czcionki), osadzanie wielu załączników (obrazy JPG, PNG, pliki PDF) inne powinny być zabronione (stosowny komunikat), ograniczone co do wielkości (łącznie max 5 MB), możliwość wstawienia pól o akceptację (wymaga interakcji z użytkownikiem);
- q) Predefiniowane rodzaje wiadomości wysyłane globalnie do użytkowników: regulaminy, informacje ważne itp.;
- r) Możliwość wygenerowania raportu zbiorczego dla wiadomości wysyłanych globalnie zawierające informacje o odczytaniu, zaakceptowaniu (o ile wstawiono pytania);
- s) Możliwość przekazania do procesu reklamacji;

- t) Zarządzanie operatorami poziomem uprawnień i w zakresie rodzajów wiadomości;
- u) Definiowanie wspólnych i indywidualnych skrzynek;
- v) Możliwość weryfikacji przez Administratora konta użytkownika czy komunikat do niego wysłany został odczytany (data i godzina odczytania).

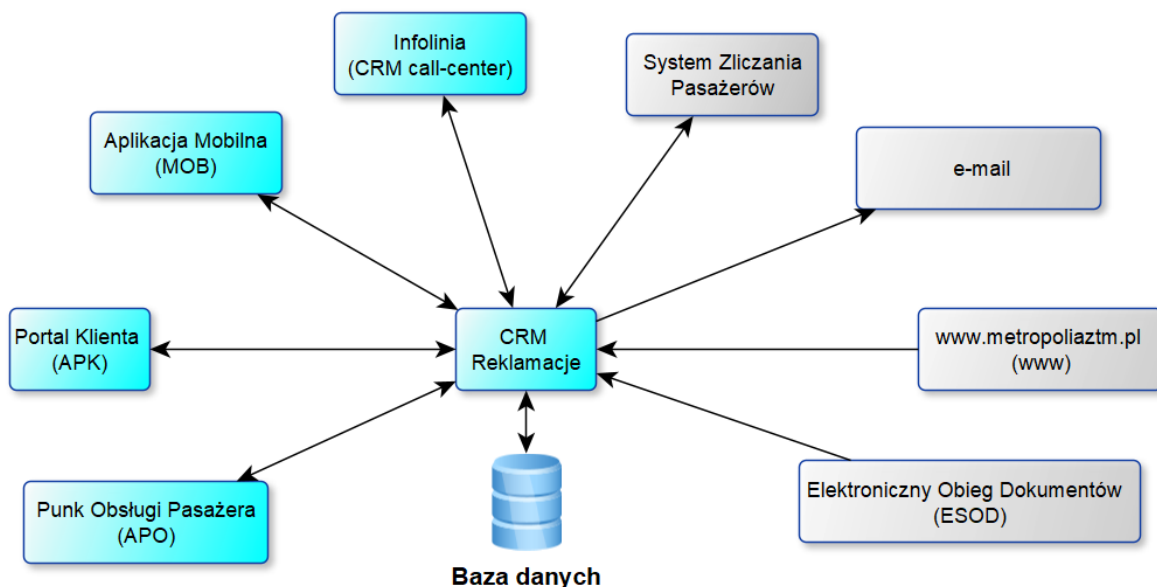
4.3.4 Pozostałe założenia

- 1) Moduł powinien udostępniać API dla gromadzenia komunikatów z innych systemów oraz dystrybucji wszystkich przetwarzanych komunikatów wg zdefiniowanych kryteriów;
- 2) Moduł powinien być przystosowany do publikowania danych w mediach społecznościowych takich jak Facebook czy twitter oraz kanały obsługujące protokół RSS;
- 3) API modułu powinno umożliwiać obustronną wymianę danych;
- 4) Zamawiający przekaże strukturę wymiany danych z portalem rj.metropoliagzm.pl.

4.3.5 Reklamacje

Element odpowiedzialny za kompleksowe zarządzanie procesem reklamacji (w tym także skarg i wniosków) w ramach obsługi systemu i zadań realizowanych przez ZTM, połączony z modułami ŚKUP 1.5: APK, MOB, APO, obsługą operatorów Call-Center oraz zintegrowany z elektronicznym systemem obiegu dokumentów Zamawiającego (ESOD). Pozwoli to zoptymalizować prace zespołu zajmującego się reklamacjami, pozwoli kontrolować poprawność i terminowość realizacji zgłoszeń oraz przyspieszyć procesy reklamacyjny, składania skarg i wniosków.

Moduł CRM jest odpowiedzialny za kompleksową obsługę reklamacji składanych przez uczestników Systemu ŚKUP 1.5, jak również pasażerów korzystających z innych usług ZTM. Moduł umożliwia pełną ewidencję zgłoszeń oraz daje możliwość sprawdzenia, na jakim etapie dane zgłoszenie reklamacyjne się znajduje. Pełni on rolę elektronicznego obiegu dokumentów (ograniczonego w swoim zakresie tylko do obsługi procesu reklamacji skarg i wniosków), niezależnie od kanału komunikacyjnego, jakim dotarł do ZTM-u. Pozwala na archiwizację oraz dokonywanie analiz pod różnym kątem (z zastosowaniem szerokiej możliwości filtrowania).



Rysunek 5. Kanały zgłaszania reklamacji

Rolą modułu jest także „pilnowanie”, aby te same sprawy wpływające różnymi, wskazanymi powyżej kanałami były procedowane tylko raz. Wykonawca musi opracować w uzgodnieniu z Zamawiającym odpowiedni mechanizm scalający reklamacje, skargi i wnioski, dotyczące tej samej sprawy.

Model obsługi reklamacji:

- 1 LINIA – przyjmowanie reklamacji z wykorzystaniem dostępnych kanałów komunikacyjnych;
- 2 LINIA – rozpatrywanie reklamacji (delegowani pracownicy, w tym działający w ramach odrębnych podmiotów);
- 3 LINIA – rozpatrywanie odwołań od reklamacji/opłat dodatkowych (kierownicy komórek merytorycznych);
- JEDNOSTKA NADZORUJĄCA – administracja i nadzór nad modułem reklamacji.

Moduł umożliwia:

- Usystematyzowanie zgłoszeń reklamacyjnych;
- Przyjmowanie reklamacji/skarg/wniosków/odwołań wszystkich uczestników Systemu ŚKUP 1.5 oraz pasażerów, także poza Systemu ŚKUP;
- Uzupełnianie wniosków reklamacyjnych, ewidencjonowanie procesu od zgłoszenia, rozpatrywania, po decyzję i dalsze odwołania, w formie konwersacji (z uwzględnieniem osi czasu);
- Definiowanie kategorii zgłoszeń i czasu ich realizacji;
- Definiowanie zespołów odpowiedzialnych za realizację zgłoszeń reklamacyjnych;
- Definiowanie podmiotów/organizacji odpowiedzialnych za realizację zgłoszeń reklamacyjnych;
- Definiowanie zaawansowanych scenariuszy postępowania reklamacyjnego w zależności od zgłoszenia;
- Rejestrację zgłoszeń reklamacyjnych;

- Automatyczne delegowanie zgłoszeń do odpowiednich zespołów odpowiedzialnych za ich realizację wg scenariuszy;
- Wyróżnienie reklamacji przeznaczonych do ręcznego obsłużenia, które nie zostały przydzielone automatycznie;
- Kontrolowanie poprawności i terminowości realizacji zgłoszeń;
- Automatyzację powiadomień dla zespołów rozpatrujących reklamację oraz dla składającego reklamację;
- Rozpatrywanie reklamacji;
- Wgląd w historię zgłoszeń reklamacyjnych i analizę danych;
- Przyjmowanie odwołań od otrzymanej decyzji;
- Raportowanie prac zespołów reklamacyjnych (statystyki: dzienne, tygodniowe, miesięczne, roczne, rozpatrzone, nierozpatrzone).

Usystematyzowanie zgłoszeń reklamacyjnych

W celu usystematyzowania zgłoszeń reklamacyjnych, wszelkie reklamacje, skargi, wnioski zgłoszone do ZTM niezależnie od kategorii i typu odnoszących się zarówno do uczestników Systemu ŚKUP 1.5 jak i pasażerów korzystających z usług ZTM poza Systemem ŚKUP 1.5 powinny wpływać do modułu MRK. Oczekuje się również możliwości kategoryzowania zgłoszeń, określenia czasu reakcji i priorytetów, a także możliwości definiowania zespołów odpowiedzialnych za realizację zgłoszenia, definiowania scenariuszy obsługi reklamacji. Scenariusz taki będzie w sposób jednoznaczny definiował, jak dane zgłoszenie ma zostać obsłużone, przez kogo i w jakim czasie.

Rejestracja zgłoszeń reklamacyjnych

Zgłoszenie reklamacji w module powinno powodować automatyczne założenie sprawy reklamacyjnej do której będą mogły być dodawane różnego typu dokumenty (PDF, JPG, PNG). Dzięki temu będzie istniała możliwość dokumentowania reakcji na zgłoszenie. Przy rejestracji zgłoszenia wybór odpowiedniego scenariusza obsługi reklamacji pozwoli na odpowiednie przekierowanie zgłoszenia do kompetentnego zespołu, który od razu będzie miał informację o dostępnym czasie na reakcję i obsługę reklamacji. Dla każdej kategorii zgłoszeń musi istnieć możliwość przygotowania autoodpowiedzi dla zgłaszającego. Autoodpowiedź powinna zawierać przygotowaną wcześniej informację (odpowiednią do kategorii), nr zgłoszenia oraz przewidywany termin rozpatrzenia. Analogiczna odpowiedź powinna być automatycznie generowana w przypadku braku rozpatrzenia reklamacji i osiągnięcia granicznego terminu przewidywanego na rozpatrzenie reklamacji, informacja powinna zawierać zdefiniowaną treść.

Delegowanie zgłoszeń

W momencie zarejestrowania reklamacji zgłoszenie zostanie automatycznie przekierowane do odpowiedniej osoby. Jeżeli jednak zgłoszenie nie spełnia wymagań reklamacji wówczas zgłoszenie jest przekazywane do administratora celem dalszego procesowania jako skarga, wniosek lub zwracane do autora w celu uzupełnienia treści reklamacji.

Wymagana jest możliwość określenia listy osób odpowiedzialnych za realizację danego zgłoszenia z określeniem kolejności powiadamiania. Listę osób aktualizuje przełożony komórki reklamacji. Dzięki

temu w przypadku braku reakcji na zgłoszenie przez daną osobę po 24 godzinach, System automatycznie przekieruje zgłoszenie do kolejnej uprawnionej osoby.

Kontrolowanie poprawności i terminowości realizacji zgłoszeń

Dzięki gromadzeniu odpowiednich danych na temat zgłoszeń reklamacyjnych (jak np. status zgłoszenia czy czas realizacji) powinna istnieć możliwość kontroli poprawności i terminowości realizacji zgłoszeń. W przypadku wykrycia nieprawidłowości, jak np. brak reakcji na zgłoszenie w ustalonym terminie, czy też opóźnienie w realizacji zgłoszenia, System powinien wysyłać alerty i powiadomienia do odpowiednich osób (zdefiniowanych w Systemie), które będą mogły zareagować i wpłynąć na prawidłową realizację zgłoszenia.

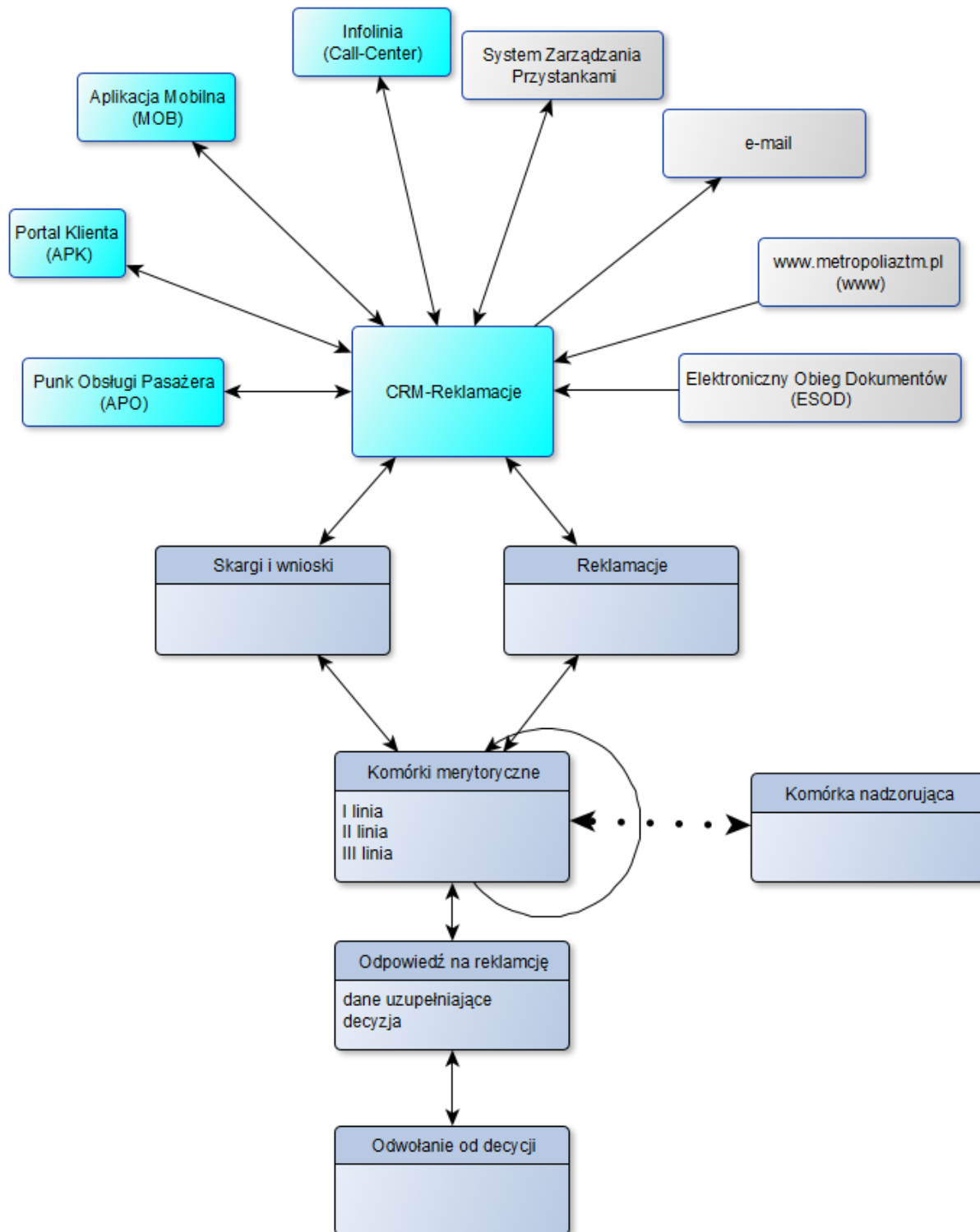
Wgląd w historię zgłoszeń i analiza danych

Oprócz gromadzenia w Systemie danych na temat każdego zgłoszenia reklamacyjnego wymagana jest możliwość przeglądania historii zgłoszeń oraz przeprowadzania różnego rodzaju analiz. Rejestr zgłoszeń powinien umożliwiać szczegółowy wgląd we wszystkie zgłoszone reklamacje wg różnych kryteriów (np. wg statusu realizacji, czasu realizacji, osoby, operatora, tematu, itp.). Ponadto umożliwi kontrolę działań reklamacyjnych oraz analizę poniesionych kosztów.

Przyjmowanie odwołań od decyzji

W przypadku odwołań od rozpatrzonych reklamacji, zgłoszenia takie powinny trafić do Jednostki Nadzorującej, a następnie zostać ręcznie przydzielone do kierownika komórki merytorycznie odpowiedzialnej za rozpatrzenie zakwestionowanej reklamacji. Odpowiedzi udziela, przez moduł MRK, kierownik komórki merytorycznej.

a) Schemat procesu reklamacji



Rysunek 6. Schemat procesu reklamacji

b) integracje

- W ramach obsługi reklamacji Wykonawca przygotowuje odpowiednie mechanizmy integracyjne oraz formatki wprowadzania danych dotyczących reklamacji, skarg i wniosków w modułach: Portal Klienta (APK), Aplikacja Mobilna (MOB), aplikacja dla POP (APO);
- Wykonawca przygotowuje i udokumentuje stosowne Web-Services do obsługi całego procesu reklamacyjnego omówionego w ramach modułu reklamacji;
- Ze względu na wrażliwy charakter przetwarzanych danych, należy zastosować mechanizmy informacyjne i bezpieczeństwa zgodne z polityką RODO.

4.3.6 Obsługa Call-Center

Kompleksowa obsługa infolinii w zakresie informowania użytkowników, przyjmowania reklamacji, zintegrowana z systemem IVR, chatroomem, zapewniająca możliwość wglądu w dane kont użytkowników (w ograniczonym zakresie, po wstępnej autoryzacji użytkownika), które są dla nich dostępne na Portalu i w Aplikacji Mobilnej.

Moduł CRM w zakresie Call-Center – jest rozwinięciem aplikacji APO o cechy pozwalające na wsparcie obsługi klientów w kanale Call-Center ŚKUP.

4.3.7 Funkcjonalności

W kontekście konsultanta:

- a) Logowanie do aplikacji przez podanie loginu i hasła wraz ze wskazaniem numeru telefonu który konsultant w danym momencie obsługuje;
- b) Wgląd do informacji zapisanych na koncie centralnym klienta (bez możliwości ingerencji w nie, z wyjątkiem możliwości wykonania procedury resetu hasła, realizowanego poprzez wysłanie linka aktywacyjnego dla nowego hasła – na adres zdefiniowany przez użytkownika w systemie ŚKUP 1.5);
- c) Możliwość przyjęcia reklamacji analogicznie jak w APO:
 - możliwość rejestrowania, przyjęcia, przeglądu i podglądu reklamacji;
 - wgląd do bazy zgłoszonych reklamacji oraz udzielanych odpowiedzi;
 - możliwość sprawdzenia na jakim etapie jest rozpatrywana reklamacja;
 - czas na zarejestrowanie/ przyjęcie reklamacji (konieczne jest określenie ram czasowych) w tym czasie konsultant nie dostaje wezwań do odebrania kolejnej rozmowy;
- d) Możliwość odbioru rozmowy telefonicznej za pomocą ikon, w tym możliwość zawieszenia, przerwania, przekazywania oraz odrzucenia rozmowy;
- e) Wymagana rejestracja połączeń, z możliwością:
 - oddzwonienia do klienta;
 - wyszukiwania historii połączeń;
 - zapamiętywanie numerów tel. – możliwość tworzenia notatek i informacji dotyczących konkretnego użytkownika nr tel.;
- f) Widoczna informacja z liczbą osób czekających w kolejce na połączenie;
- g) Możliwość odbioru rozmowy tekstowej - chatroom za pomocą ikon, w tym możliwość zawieszenia, przerwania, przekazywania oraz odrzucenia rozmowy; podczas prowadzenia

rozmowy widoczne propozycje pytań i odpowiedzi (wg słowników), z opcją prezentacji jako drzewa kontekstowego oraz opcją wyszukiwania słów kluczowych, słowa kluczowe do wskazania myszką w polu tekstowym rozmowy;

- h) Po uwierzytelnieniu się przez klienta (system IVR, lub dane wprowadzane przez konsultanta) – podgląd do zaktualizowanej historii przejazdów i operacji na koncie IKU w tym w kontekście Portalu Klienta i Aplikacji Mobilnej;
- i) Widoczny podgląd skarg i wniosków:
 - możliwość przyjęcia skargi/wniosków oraz odwołań od mandatów;
 - wgląd do bazy skarg/wniosków i odwołań;
- j) Wgląd do informacji na koncie analogicznie jak w APO (po autoryzacji klienta);
- k) Zarówno w trakcie rozmowy, jak i po jej przeprowadzeniu konsultant może wprowadzić do systemu notatkę podsumowującą kontekst rozmowy, słownik tematów, interaktywne formularze;
- l) Przegląd historii prowadzonych rozmów wraz z notatkami.

W kontekście administratora:

- a) Logowanie do aplikacji przez podanie loginu i hasła;
- b) Przegląd historii prowadzonych rozmów przez konsultantów (telefonicznych i chatroom), oraz zawartości notatek;
- c) Przegląd historii przeglądanych kont użytkowników (bez wglądu w dane użytkowników);
- d) Definiowanie słowników do notatek rozmów, chatroomów;
- e) Definiowanie formularzy notatek;
- f) Definiowanie słowników i parametrów chatroom/chatboot;
- g) Przegląd statystyk chatroom;
- h) Włączanie i wyłączanie chatroom;
- i) Przypisywanie stanowisk konsultantów (powiązanie loginu z nr telefonu);
- j) Statystyki prowadzonych rozmów (z podziałem na konsultantów, zawierające rodzaje rozmów, długości rozmów, czasy bezczynności, czasy oczekiwania na zgłoszenie konsultanta, długość kolejki oczekujących);
- k) Alarmy w przypadku przekroczenia zdefiniowanych parametrów: kolejki osób oczekujących (np. 10 osób), braku zadeklarowanej liczby konsultantów.

4.3.8 IVR (*ang. interactive voice response*)

Wykonawca uruchomi, zintegruje z centralą telefoniczną Zamawiającego, specjalny publiczny nr telefonu ((42) 291 04 05) na potrzeby realizacji funkcji IVR oraz Call-Center. Wszelkie opłaty telekomunikacyjne będzie ponosił Zamawiający. Połączenia krajowe dla osób dzwoniących muszą być bezpłatne w tym dla połączeń z sieci komórkowych, nie dotyczy połączeń zagranicznych.

Wykonawca zbuduje odpowiednie Web-services do obsługi wymienionych funkcjonalności w tym na potrzeby autoryzacji klienta wdzwanającego się na wskazany powyżej numer. Zamawiający posiada centralę telefoniczną DGT Milenium wraz z serwerem obsługującym funkcję IVR. Wykonawca może zrealizować funkcjonalność na centrali Zamawiającego, z zastrzeżeniem, że będą realizowane przez certyfikowany przez producenta centrali podmiot. Wykonawca może również dostarczyć funkcjonalność realizując ją na dostarczonym przez siebie rozwiązaniu.

Wykonawca przedstawi do uzgodnienia z Zamawiającym, drzewo zapowiedzi IVR, a następnie je wdroży i integruje z oprogramowaniem i funkcjami Call-Center.

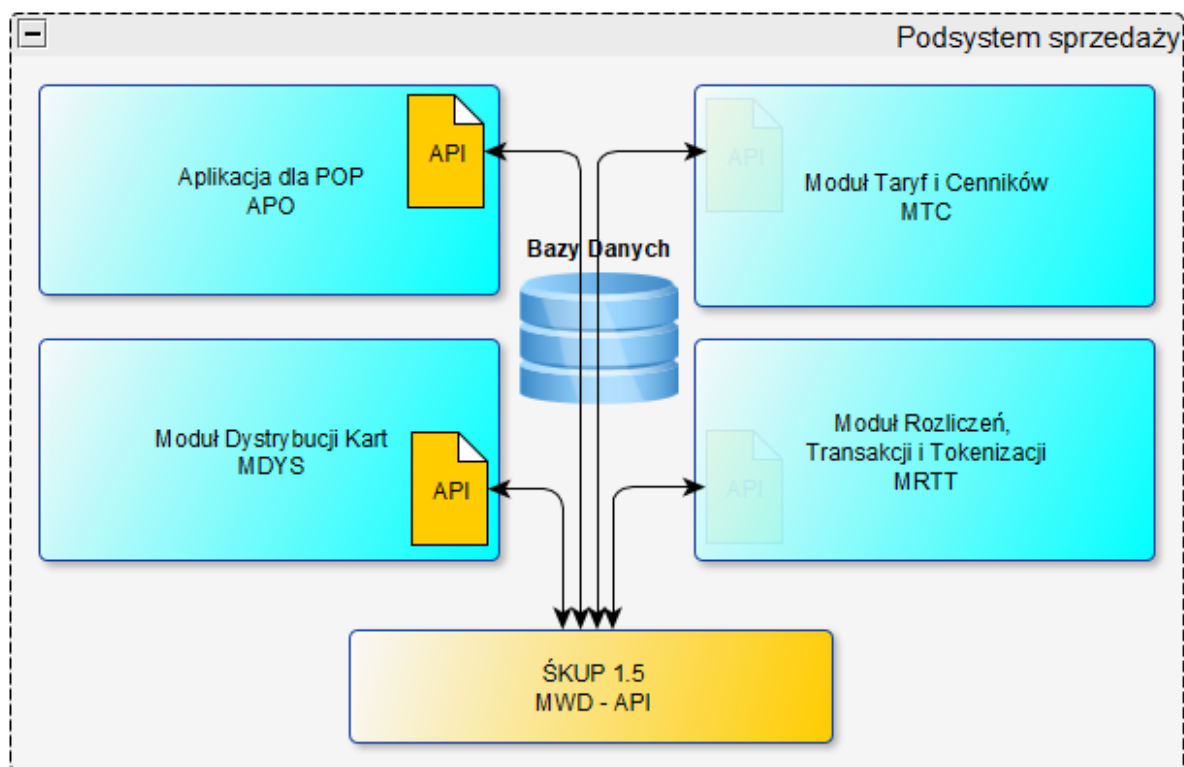
Wdrożone rozwiązanie musi sterować pracą konsultantów i rozpoznawać, czy konsultant jest zalogowany i wolny do odebrania połączenia, w przypadku przejęcia rozmowy przez konsultanta jego status zmienia się na zajęty i kolejne rozmowy w kolejce są kierowane do pozostałych wolnych konsultantów. Odebrane połączenie przez konsultanta wywołuje na jego ekranie kontekst osoby dzwoniącej, w przypadku przeprowadzenia z powodzeniem autoryzacji, konsultant ma wgląd w kontekst konta dzwoniącego. W przypadku braku autoryzacji, konsultant może przeprowadzić autoryzację wg danych przekazywanych przez osobę dzwoniącą.

5 Podsystem Sprzedaży

Zadaniem modułów\aplikacji podsystemu sprzedaży jest kompleksowa obsługa realizacji procesu sprzedaży i rozliczeń usług w zakresie tzw. „back office”. Zamawiający oczekuje zgrupowania procesów odpowiedzialnych za parametryzowanie cenników usług, obsługi zamawiania i dystrybucji kart ŚKUP, kompleksowej obsługi kont i użytkowników przez operatorów, Agentów Sprzedaży oraz za wszystkie procesy związane z prowadzeniem, rozliczaniem oraz raportowaniem transakcji finansowych, między agentami rozliczeniowymi oraz w zakresie płatności internetowych, kartowych, tokenizacji kart EMV, bezpieczeństwem transakcji oraz prowadzeniem doładowywanych rachunków punktowych w ramach e-portmonetki punktowej. Podsystem będzie posiadał możliwość obsługi transakcji pochodzących z innych podsystemów ŚKUP m.in. Portalu Klienta i Aplikacji Mobilnej, oraz urządzeń podłączonych do systemu ŚKUP przez podsystem infrastruktury. Bezpieczeństwo i architektura zastosowanych rozwiązań musi być zgodna ze standardem systemów płatniczych i normą PCI DSS. Moduł rozliczeń transakcji i tokenizacji (MRTT) będzie integrowany z systemem księgowym Zamawiającego, przy pomocy plików transakcyjnych o wskazanej strukturze.

W ramach podsystemu sprzedaży wstępnie zaproponowano podział na następujące moduły\aplikacje:

- Moduł Taryf i Cenników (MTC);
- Aplikacja dla Punktów Obsługi Pasażera (APO);
- Moduł Dystrybucji Kart ŚKUP (MDYS);
- Moduł Rozliczeń Transakcji i Tokenizacji (MRTT).



Rysunek 7. Poglądowy schemat Podsystemu Sprzedaży.

5.1 Moduł taryf i Cenników (MTC)

Moduł taryf i cenników powinien pozwalać na kompleksową obsługę cenników usług: od zdefiniowania nowych taryf i cenników, przez modyfikację istniejących, po definiowanie jego poszczególnych elementów i właściwości (poszczególne bilety, promocje, parametry itd.). Musi posiadać możliwość zdefiniowania taryfy i cennika i przypisania ich do obiektów tj. organizatorów, linii, pojazdów, bądź wydzielonej grupy, do której pojazdy należą (np. linie ekspresowe). Powinien również umożliwiać tworzenie biletów lub całych cenników zintegrowanych, obowiązujących u więcej niż jednego podmiotu, np. bilety obowiązujące w komunikacji ZTM i Kolei Śląskich (Metrobilet). MTC ma zapewniać wspieranie rozliczania pomiędzy podmiotami środków z biletów (np. bilet komunikacji miejskiej wraz z kolejowym – cena jest sumą składową z dwóch biletów lub posiada uzgodniony procentem/kwotą udziału stron – każdego z organizatorów i rozliczanie udziałów stron, na podstawie składowych części biletów, udziałów wartościowych lub procentowych). MTC powinno uwzględniać także funkcjonalność rozliczania wpływów z poszczególnych biletów lub grup biletów (np. Metrobilet) pomiędzy poszczególne podmioty oraz funkcjonalność zwrotu biletów oraz rozliczenia zwrotu na poszczególne podmioty.

Moduł taryf i cenników musi zapewniać również nadawanie i ewidencjonowanie numerów dla każdego biletu funkcjonującego w systemie (funkcjonalność elektronicznego magazynu biletów – MTC-magazyn dla systemu ŚKUP 1.5). Seria i numer ten musi być unikatowy w skali całego systemu.

MTC ma wspierać obsługę wnoszenia opłat dla przejazdów ulgowych (zarówno poprzez wybór opcji biletu ulgowego na kasowniku, jak i wykorzystanie zakodowanej ulgi w systemie). Pasażer musi mieć możliwość wyboru w systemie domyślnego pobierania opłat w taryfie ulgowej, aby system automatycznie pobierał opłaty ulgowe (weryfikacja prawa do korzystania z ulgi w pojeździe dokonywana będzie przez kontrolera w przypadku niezautoryzowania ulgi). MTC ma umożliwiać zarządzanie słownikiem poszczególnych ulg oraz ich parametrów.

MTC będzie wspierał sprzedaż/dystrybucję biletów do Dystrybutorów w modelu prowizyjnym i opustowym. Będzie pozwalał na definiowanie parametrów pozwalających na rozliczanie prowizji i opustu dla poszczególnych Dystrybutorów w zależności od przyjętego modelu.

System powinien umożliwiać zwrot biletu przez pasażera w Punktach Obsługi Pasażera, automatach biletowych, przez Portal Klienta i Aplikację Mobilną. W przypadku zwrotu biletu już rozpoczętego, system naliczy kwotę zwrotu zgodnie z zasadami zwrotu biletu przyjętymi Zarządzeniem Dyrektora ZTM. Sposób naliczania zwrotu musi być konfigurowalny. Ponadto w przypadku biletów kolejowych/łączonych z koleją i innymi organizatorami transportu publicznego należy przewidzieć dokonywanie zwrotów wg regulacji kolejowych. Tym samym w przypadku biletu wspólnego z koleją zwrot biletu miesięcznego będzie możliwy tylko np. do 10 dnia ważności biletu. Ponadto od zwracanej części „kolejowej” ma być pobierane 10% odstępnego lub nie. Termin przyjmowania zwrotów oraz % odstępnego, musi być parametrem konfigurowalnym (może być również wartością 0). Dodatkowo system powinien dawać możliwość przyjmowania zwrotów w trybie specjalnym – o kwocie zwrotu decyduje pracownik ZTM.

Moduł taryf i cenników ma posiadać zbiór definicji, nazw i cen opłat dodatkowych wystawianych w kontrolerze wraz z możliwymi kombinacjami opłaty przewozowej (tzw. przewożne). Szczegółowe

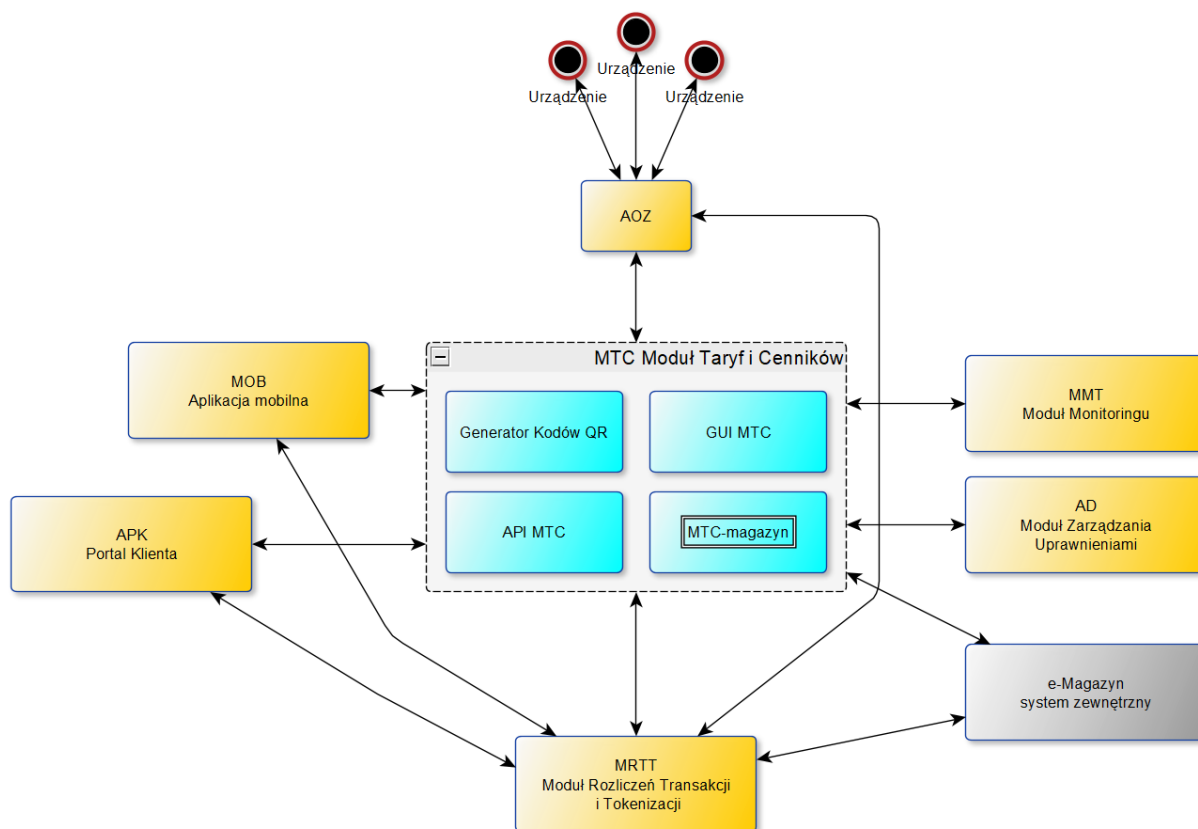
opisy nazw opłat dodatkowych i przypisanych do nich wartości tzw. przewoźnego zawiera rozdział dotyczący Podsystemu Infrastruktury w module Kontrolerka (UKNT).

Moduł MTC będzie umożliwiał eksportowanie cenników, taryf, biletów przygotowanych w środowisku testowym do plików edytowalnych (np.CSV, XML), a następnie będzie pozwalał na ich import (np. po modyfikacji) do środowiska produkcyjnego.

5.1.1 Architektura MTC

Moduł można podzielić na następujące elementy logiczne:

1. GUI – interfejs użytkownika zarządzającego wszystkimi elementami przypisanymi do funkcjonalności MTC;
2. API MTC – interfejs wymiany danych między poszczególnymi modułami oraz urządzeniami systemu, w tym do zewnętrznych systemów transportowych i usługowych, zintegrowanych z systemem ŚKUP 1.5. Należy uwzględnić integrację z zewnętrznym systemem Zamawiającego, magazynem biletów elektronicznych (eMagazyn), tak by umożliwić jednolite zarządzanie cennikami, numeracją biletów, oraz kodami QR.
3. MTC-magazyn – Oprogramowanie w ramach modułu MTC, realizujące funkcje elektronicznego magazynu biletów, pozwalające na zakup i zwrot poszczególnych pojedynczych lub złożonych (pakietowych) pozycji biletowych, udostępniające API dla urządzeń i aplikacji w ramach systemu ŚKUP 1.5 oraz innych zintegrowanych z nim systemów;
4. Cenniki utworzone na podstawie generowanych taryf i parametrów (ulgi, promocje itd.) posiadające określone pozycje cennikowe (bilety), stany magazynowe, definicje opłat dodatkowych i przewoźnego;
5. Generator Kodów QR – element odpowiedzialny za generowane sekwencje kodów, prezentowane dalej w postaci obrazka QR (spójne z eMagazynem).



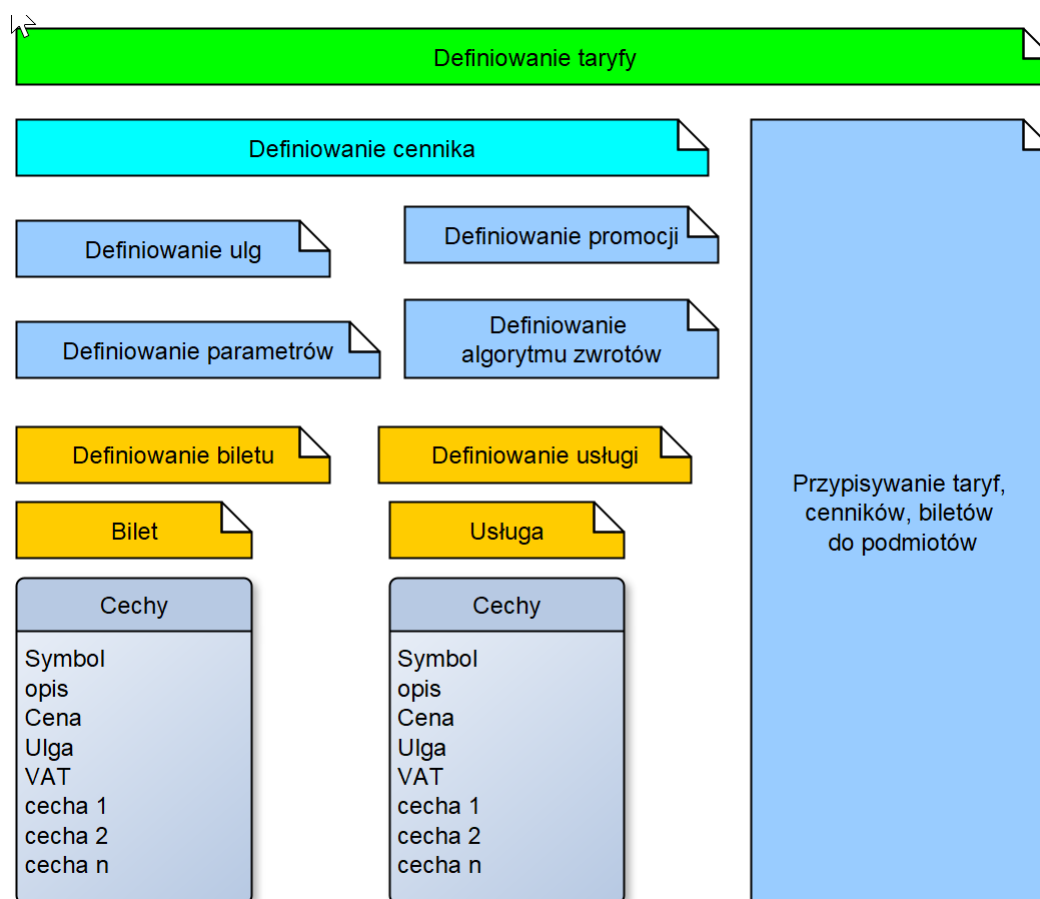
Rysunek 8. Architektura moduł MTC

5.1.2 Funkcjonalności

Moduł taryf i cenników powinien umożliwiać:

- a) definiowanie rodzajów taryf:
 - definiowanie taryf z podziałem na dostawców usług (dla każdego indywidualnie);
 - usługi parkowania w zakresie P&R – parametr przypisany do wybranych biletów, które będą stanowiły podstawę do bezpłatnego parkowania w ramach P&R;
 - definiowanie podmiotów zintegrowanych z systemem ŚKUP 1.5 i zasad rozliczeń między systemami;
- b) Definiowanie cennika;
- c) Definiowanie biletów;
- d) definiowanie biletów dla wybranych/wskazanych urządzeń;
- e) definiowanie biletów dla wybranych/wskazanych dystrybutorów/operatorów;
- f) definiowanie biletów na określoną/wskazaną linię/ wskazane linie (np. linie lotniskowe, wskazane nr linii etc.);
- g) Definiowanie promocji (np. procentowa, kwotowa, punktowa - tańsze bilety dla stałych klientów itp);

- h) Definiowanie parametrów (stawki VAT, ulgi handlowe i ustawowe, czasy obowiązywania biletów, zasięg przejazdu (strefy, miasta), czas obowiązywania (bilety weekendowe, wakacyjne), przypisania do podmiotu, grupy linii itp.;
- i) Definiowanie cennika usług dodatkowych (np. doładowanie e-portmonetki, duplikat karty, kaucja, itp.);
- j) Definiowanie algorytmu i cennika zwrotu biletów;
- k) Raporty sprzedażowe;
- l) Raporty zwrotów;
- m) Definiowanie opłat dodatkowych i przewoźnego;
- n) API dla zewnętrznych systemów (m.in. e-Magazyn).



Rysunek 9. Definiowanie taryf

Ad. A Definiowanie cennika

Na pojedynczy cennik powinny składać się promocje, parametry (stawki VAT, ulgi handlowe, ustawowe, gminne, ze względu na grupy społeczne, wiek, nabyte uprawnienia, inne uwarunkowania społeczne wraz z możliwością definiowania okresu jej obowiązywania), taryfy i bilety oraz usługi dodatkowe, z możliwością definiowania różnych stawek dla kont imiennych oraz kont na okaziciela. Promocje i parametry definiowane mogą być dla pojedynczego rodzaju biletu lub ich grupy. Cena biletu

po zdefiniowaniu ulg, promocji i innych parametrów naliczana będzie automatycznie. Użytkownik tworząc projekt cennika będzie określał jego poszczególne pozycje. Jeśli cennik ma być cennikiem aktualnym, użytkownik będzie musiał zmienić jego stan na aktywny i określić czas obowiązywania cennika. Zdefiniowany cennik zostanie zapisany w Systemie, przy czym w danej chwili w Systemie będzie mógł być tylko jeden cennik aktywny dla danego podmiotu. W przypadku cennika aktywnego nie będzie istniała możliwość jego modyfikacji z wyjątkiem dodawania/modyfikacji promocji. Cenniki ze statusem aktywny będą automatycznie pobierane z systemu przez urządzenia wchodzące w skład Systemu (komputery pokładowe, kasowniki każdego typu, automaty biletowe, Terminale Sprzedażowe, Portal Klienta, APO, Aplikacja Mobilna). Do cennika przypisana jest data obowiązywania, więc cennik może zostać pobrany przez urządzenia zanim wejdzie w życie bez kolizji z aktualnie obowiązującym cennikiem.

Ad. B Definiowanie biletów

Definiowanie biletów (jednorazowych, krótkookresowych, okresowych, wieloprzejazdowych, n-grupowych, weekendowych itp.), powinno się odbywać w ramach danego cennika. W zależności od stanu wybranego cennika powinny być możliwe różne operacje. W przypadku cennika w fazie projektu, użytkownik powinien posiadać możliwość dowolnego tworzenia, modyfikowania i usuwania biletów. Natomiast w przypadku cennika aktywnego nie powinny być możliwe żadne operacje na biletach z wyjątkiem ich podglądu oraz dodawania/usuwania promocji powiązanej z biletem. W celu zdefiniowania biletu użytkownik powinien posiadać możliwość określenia jego parametrów (np. rodzaj – jednorazowy, okresowy; zakres obowiązywania – czasowy lub ilościowy lub z dwoma parametrami n-przejazdów ważne n-dni; zasięg przejazdu/ilość wejść; ulga – np. uczniów, senior, mieszkaniowiec danego miasta/gminy, strefa – np. ilość gmin, środek lokomocji, dni obowiązywania, w tym bilet roczny), w tym nadawanie szczegółowych i skróconych nazw i opisów, nadawanie opisów w językach obcych, określanie typu taryfy, nadawanie okresu ważności (w tym czasu sprzedaży oraz obowiązywania), sposobu aktywacji (od pierwszego użycia lub od zadeklarowanej przy zakupie daty obowiązywania), nadawanie właściwości dot. miejsca sprzedaży (powiązania z urządzeniami, które będą je dystrybuować wraz z parametrami dystrybutora), użycia, określanie parametrów dostawcy usługi/biletu, nadawanie cen (kody cen, typy opłat, promocji). Długości nazw biletów powinny być ograniczona wyłącznie parametrami wyświetlaczy urządzeń w systemie ŚKUP 1.5. Akceptacja zmian powinna powodować, że definiowany bilet zostanie zapisany w systemie i zostanie powiązany z odpowiednim cennikiem. Moduł powinien posiadać walidację wypełnianych pól i w przypadku niewypełnienia któregoś z nich lub niewłaściwego wypełnienia, powinien uniemożliwić utworzenie i zapisanie w systemie nowego biletu/usługi, oraz wskazanie błędnie wypełnionych pól. Przy tworzeniu nowego cennika/taryfy moduł musi umożliwić zdefiniowanie nowych biletów poprzez zmianę cen biletów istniejących, bez konieczności ponownego definiowania parametrów (np. poprzez klonowanie).

Ad. C Definiowanie taryfy dynamicznej – CICO

Taryfy dynamiczne opierają się na obciążaniu pasażera za przejazd wg. faktycznego zużycia, które jest wyliczone w następstwie przykładania „tapowania” identyfikatorów do kasowników podczas wsiadania (check in) i wysiadania z pojazdu (check out). Następnie system zaokrągla wg. zdefiniowanego algorytmu zużycie (np. czas), wycenia przejazd i obciąża konto pasażera.

Zamawiający wymaga, aby system był przygotowany na obsługę następujących rodzajów taryf CICO:

- Wg czasu przejazdu (gradacja w przedziałach minutowych);
- Wg przejechanych kilometrów (gradacja w przedziałach jedno kilometrowych);

Dodatkowo, każdy z powyższych wariantów musi uwzględniać podział ze względu na rodzaj środka transport (inne dla autobusów, tramwajów, trolejbusów, pociągów) oraz rodzajów linii (zwykłe, pospieszne, ekspresowe, nocne).

Ad. D Definiowanie promocji

Definiowanie promocji powinno się odbywać w ramach danego cennika. W zależności od stanu wybranego cennika muszą być możliwe różne operacje. W przypadku cennika w fazie projektu, użytkownik powinien móc dowolnie tworzyć, modyfikować i usuwać promocje. W celu zdefiniowania promocji użytkownik powinien określić typ promocji (np. procentowa, kwotowa, punktowa) oraz jej parametry (kwotę podstawową promocji oraz wartość promocji, warunki uzyskania promocji). Powinna istnieć możliwość dodania zakresu czasu, dla którego promocja będzie obowiązywać. Akceptacja zmian powinna powodować, że definiowana promocja zostanie zapisana w Systemie i powinna być powiązana z odpowiednim cennikiem, a ceny biletów automatycznie przeliczone.

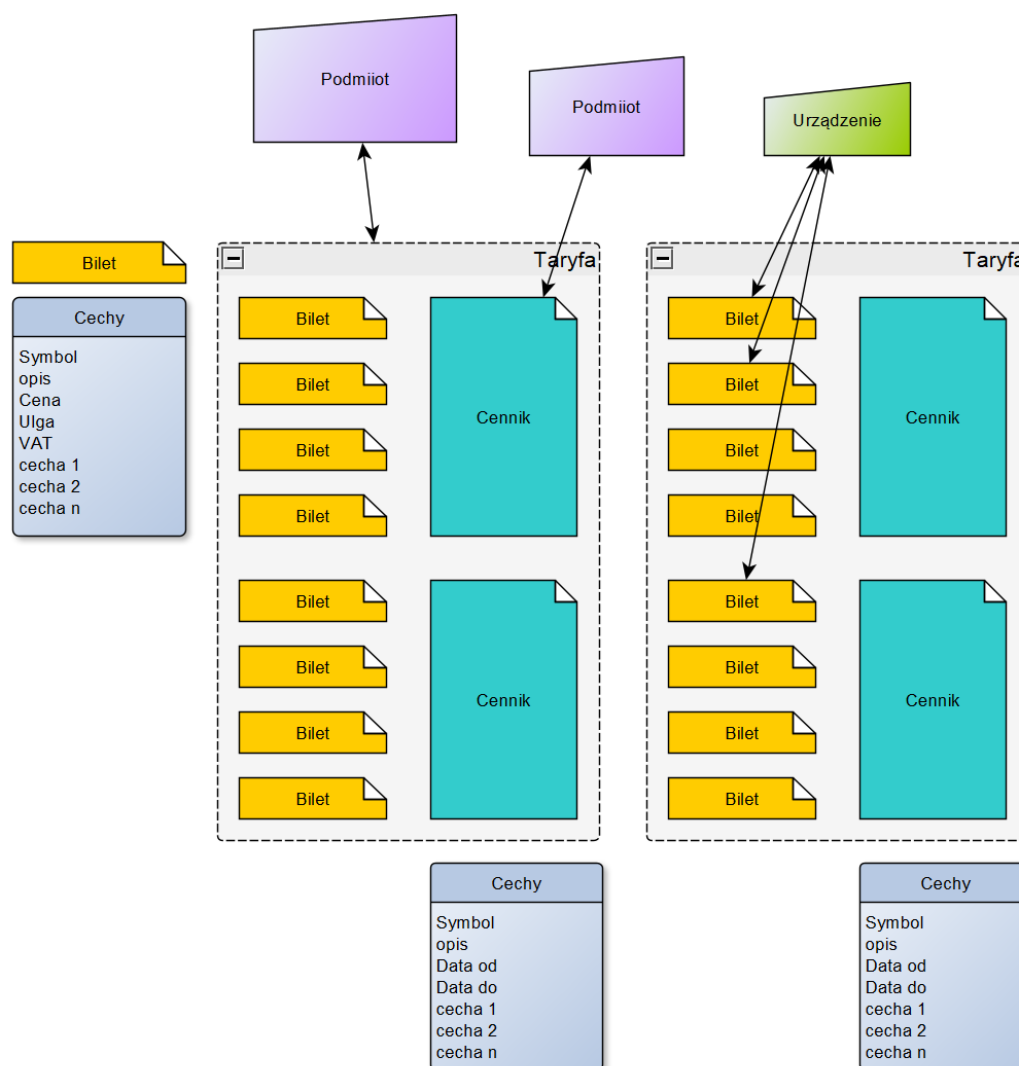
Ad. E Definiowanie parametrów

Definiowanie parametrów powinno odbywać się w ramach danego cennika. Parametrami będą m.in.: stawki VAT, poziom i rodzaje akceptowanych ulg (handlowa, ustawowa) zakresy czasowe biletów, zasięg przejazdu, grupa linii - np. ekspresowe, mające ograniczoną pulę biletów. W zależności od stanu wybranego cennika powinny być możliwe różne operacje. W przypadku cennika w fazie projektu, użytkownik powinien móc dowolnie tworzyć, modyfikować i usuwać parametry. Natomiast w przypadku cennika aktywnego nie będą możliwe żadne operacje na parametrach z wyjątkiem ich podglądu. W celu zdefiniowania parametru użytkownik powinien móc określić typ parametru (np. zakresy czasowe biletów, zasięg przejazdu) oraz parametry definiowanego parametru (np. typ okresu – dniowy / miesięczny / godzinowy / minutowy, czy typ zakresu – sieć/strefy/miasta/linie/odcinki linii – dla zasięgu przejazdu). Akceptacja zmian powinna powodować, że definiowany parametr zostanie zapisany w Systemie i będzie powiązany z odpowiednim cennikiem.

Definiowanie słownika i parametru ulg w zakresie wartości (np. % wartości nominalnej kontraktu, wartość zł w stosunku do wartości kontraktu), opisu, przypisanie do taryfy/usługi dla każdego dostawcy usług indywidualnie.

Powinna istnieć możliwość objęcia przejazdami bezpłatnymi wszystkich linii np. w wybranym dniu (globalnie) lub wybranych linii oraz dowolnych odcinków trasy dla wybranych linii (lokalnie np. Katowice Dworzec – Katowice Sądowa Dworzec). Funkcjonalność zintegrowana z modułem INT.BUS.

Ad. F Definiowanie rodzajów taryf



Rysunek 10. Definiowanie rodzajów taryf, rysunek poglądowy

Definiowanie pozycji i rodzajów opłat powinno odbywać się w ramach danego cennika. W zależności od stanu wybranego cennika powinny być możliwe różne operacje. W przypadku cennika w fazie projektu, użytkownik powinien móc dowolnie tworzyć, modyfikować i usuwać rodzaje taryfy. Natomiast w przypadku cennika aktywnego nie powinny być możliwe żadne operacje na rodzajach taryf z wyjątkiem ich podglądu oraz zmiany daty końca obowiązywania. Moduł powinien umożliwić na zdefiniowanie taryfy czasowej, strefowej i odległościowej. W celu zdefiniowania rodzaju taryfy użytkownik powinien posiadać możliwość określenia typu biletu oraz jego parametry (np. ulga, zakres - dobowy/godzinowy, typ linii - normalna / przyspieszona / metropolitalna/ lotniskowa/ekspresowa/nocna/ w dni robocze/weekendy itp., rodzaj pomiaru - strefa (ilość gmin) / czas / itp.). Akceptacja zmian powinna powodować, że definiowany rodzaj taryfy zostanie zapisany w systemie i zostanie powiązany z odpowiednim cennikiem.

Zakłada się, że dla przejazdów jednorazowych/krótkookresowych taryfą domyślną będzie taryfa czasowa.

Powinna być przewidziana możliwość stosowania taryf w ramach jednego przejazdu, jak również w ramach podróży (przesiadek), uwzględniając korzystanie z różnych środków transportu (np. bilety n-minutowe z możliwością przesiadek).

Powinna być przewidziana możliwość konfiguracji wybranej taryfy na określonych liniach, gminach (np. bilet na wspólnym odcinku Gliwice-Katowice, zarówno komunikacją zbiorową ZTM oraz umożliwienie sterowania tym, jakie bilety są ważne na poszczególnych typach linii (np. bilety na linie ekspresowe, lotniskowe, nocne, specjalne).

Moduł powinien umożliwiać definiowanie taryf i cenników indywidualnie dla każdego usługodawcy zdefiniowanego w systemie, w tym m.in. dla:

- usług komunikacji zbiorowej;
- innych podmiotów przyłączanych i zintegrowanych z systemem ŚKUP 1.5 (opcjonalnie w ramach godzin rozwojowych).

Poza tym, w ramach przedmiotowego modułu ma być możliwość definiowania udziału (np. procentowego, kwotowego) przy taryfach/biletach wspólnych udział poszczególnych dostawców, tak aby system mógł właściwie rozliczać środki pomiędzy dostawcami usług.

System ŚKUP 1.5 powinien uwzględniać obecnie funkcjonujące wspólne bilety elektroniczne ZTM i Kolei Śląskich (np. Metrobilet) i innych ewentualnych organizatorów transportu zbiorowego/publicznego. Poza tym planowane jest uruchomienie w wersji elektronicznej, wspólne bilety krótko i średniookresowe z Kolejami Śląskimi: n-minutowy, n-godzinny i ewentualnie innymi organizatorami transportu zbiorowego/publicznego (zakres i realizowalność zależna od zawartych umów, proponowany zakres jest opcją kompletną). W przypadku wspólnych biletów n-minutowych i n-godzinnych należy przewidzieć możliwość pobierania biletów kolejowych i biletów z taryf wspólnych z elektronicznego magazynu biletów Kolei Śląskich, których emitentem są Koleje Śląskie (decyzja zależna od uzgodnień z KŚ).

Ad. G Definiowanie cennika usług dodatkowych

Definiowanie usług dodatkowych powinno się odbywać w ramach danego cennika. Usługami dodatkowymi powinny być m.in.: opłaty manipulacyjne, opłaty gminne (nie będą uruchamiane na wdrożeniu), zasilania e-portmonetki, zwroty kaucji, duplikat karty, kaucja za kartę, opłata za parkowanie w systemie P&R, w przyszłości opłata za korzystanie z roweru metropolitalnego lub innych usług mobilnych (np. carsharing) w kontekście pierwszej i ostatniej mili, w tym możliwości wykonywania przejazdów rowerem/inym pojazdem w ramach posiadanego biletu okresowego/wieloprzejazdowego. W zależności od stanu wybranego cennika powinny być możliwe różne operacje. W przypadku cennika w fazie projektu, użytkownik powinien posiadać możliwość dowolnie tworzyć, modyfikować i usuwać usługi dodatkowe. Natomiast w przypadku cennika aktywnego nie powinny być możliwe żadne operacje na usługach dodatkowych z wyjątkiem ich podglądu oraz dodawania/usuwania promocji powiązanych z usługą. W celu zdefiniowania usługi dodatkowej użytkownik powinien posiadać możliwość określenia typu usługi oraz jej cenę. Opcjonalnie powinna istnieć możliwość dodania do usług zdefiniowanych w cenniku promocji. Akceptacja zmian powinna powodować, że definiowana usługa dodatkowa zostanie zapisana w systemie i zostanie powiązana z odpowiednim cennikiem.

Ad. H Definiowanie algorytmu i cennika zwrotu biletów

Moduł musi umożliwiać definiowanie algorytmu, zasad zwrotu biletów zakupionych przez użytkowników systemu, który powinien uwzględniać m.in. możliwość potrącenia odstępnego (w tym z uwzględnieniem podziału wartości biletu na poszczególnych operatorów), określenie terminów w jakich będzie możliwość zwrotu (np. do 10 dnia od jego zakupu), potrącenie za zużyty okres/przejazdy według zasad, które określi Zamawiający. Musi istnieć możliwość zwrotu dowolnego zakupionego biletu w systemie.

Moduł musi definiować także parametr pozwalający na zwrot biletu bez potrąceń np. w sytuacji pomyłki operatora/sprzedawcy.

Dodatkowo system musi umożliwiać dokonywanie zwrotów biletów, które zostały zakupione w modelu opustowym przez Dystrybutora (np. z powodu zmiany taryfy).

Szczegółowe zasady zwrotów zostaną uzgodnione z Wykonawcą po podpisaniu umowy.

Ad. I Generowanie na żądanie i przechowywanie biletów

Funkcjonalność elektronicznego magazynu biletów dla systemu ŚKUP 1.5 (MTC-magazyn) umożliwiająca generowanie na żądanie biletów z niepowtarzalnym, indywidualnym numerem i serią. Operacja wykonywana online i umożliwiająca pobranie n-biletów. Dla każdego sprzedanego biletu musi istnieć powiązanie z konkretną transakcją – z Globalnym Identyfikatorem Transakcji (GIT), a przez nią z konkretnym miejscem i czasem sprzedaży biletu. Szczegółowe zasady numerowania biletów Wykonawca uzgodni z Zamawiającym w trakcie projektowania modułu. Wszystkie numery biletów będą przechowywane w centralnym magazynie biletów, który poza numerami biletów będzie przechowywał ich parametry i statusy (np. wygenerowany, sprzedany, aktywny, zużyty). Zadaniem centralnego magazynu biletów będzie generowanie, dystrybuowanie oraz utrzymywanie informacji o wszystkich biletach funkcjonujących w ramach systemu ŚKUP 1.5. Centralny magazyn biletów będzie miał możliwość generowania paczek biletów dla urządzeń, które mogą funkcjonować off-line nawet przez krótkie okresy (np. urządzenia w pojeździe, który znajduje się chwilowo poza zasięgiem sieci). Centralny magazyn biletów musi mieć możliwość wygenerowania na żądanie Zamawiającego paczki biletów w postaci pliku o uzgodnionym z Zamawiającym formacie (np. PDF), który będzie służył do wydruku biletów papierowych z kodami QR.

Magazyn będzie umożliwiał obsługę sprzedaży/dystrybucje biletów przez Dystrybutorów w modelu prowizyjnym i upustowym. Będzie pozwalał na definiowanie parametrów dla obydwu modeli sprzedaży/dystrybucji pozwalających na bieżące monitorowanie i rozliczanie sprzedaży w obydwu modelach.

Zamawiający oczekuje integracji MTC-magazynu z eMagazynem (zewnętrzny) Zamawiającego w zakresie definicji biletów, numeracji biletów i kodów QR.

Ad. J Raporty sprzedażowe

Zamawiający oczekuje funkcjonalności umożliwiającej wygenerowanie raportów i ich eksport do plików Excel, CSV, PDF w tym możliwości generowania szczegółowych raportów analitycznych z możliwością ich filtrowania oraz raportów syntetycznych zawierających zbiorcze raporty np. dla zadanego okresu z podziałem na rodzaje biletów, podmioty (Dostawców usługi i Dystrybutora), urzędnika. Raporty (plikowe) muszą zawierać dane, które będą stanowiły podstawę do wygenerowania faktur prowizyjnych lub opustowych dla Dystrybutorów za sprzedaż biletów (integracja z systemem księgowym Zamawiającego). Będzie również możliwość wygenerowania raportów konfiguracji MTC takich jak: cennik, taryfy, biletów obowiązujących oraz archiwalnych.

Ze względu na rozwój systemu komunikacji zbiorowej, możliwość dołączenia innych organizatorów czy wprowadzenia rozwiązań obecnie niemożliwych do przewidzenia musi istnieć możliwość zdefiniowania dodatkowych raportów. Poza poniższym wykazem, w ramach niniejszego zamówienia Wykonawca będzie zobowiązany do wykonania dodatkowo (w okresie trwania umowy) 10 raportów. Zakres tych raportów zostanie określony przez Zamawiającego w momencie zaistnienia takiej potrzeby.

Wykaz raportów:

Raport 0. dotyczący zdefiniowanych, obowiązujących oraz nieaktywnych biletów/taryf

Raport umożliwiający wygenerowanie wszystkich obowiązujących i zdefiniowanych biletów i taryf, pozwalający na analizę i przegląd obowiązujących, ale również już nieaktywnych/nieobowiązujących biletów w całym systemie

Zawierający co najmniej dane:

- kod/kody kontraktu/usługi/biletu;
- numer kontraktu/usługi/biletu (indywidualny, unikatowy);
- rodzaj taryfy;
- nazwa /opis kontraktu/usługi/biletu;
- data zdefiniowania danego kontraktu/usługi/biletu;
- login użytkownika, który dokonał definicji/modyfikacji danego biletu/usługi/kontraktu;
- okres obowiązywania danego kontraktu/usługi/biletu/taryfy;
- okres sprzedaży danego kontraktu/usługi/biletu;
- cena podstawowa;
- cena sprzedaży;
- kanał dystrybucji danego biletu/kontraktu/usługi (np. bilet stref-czas na kasownik, bilet okresowy na SAD, UPOS itp.).

z możliwością filtracji dla dowolnego przedziału okresu obowiązywania, okresu sprzedaży, daty zdefiniowania, numeru biletu, kodu biletu, nazwy biletu, taryfy, kanału dystrybucji itp.

Raport 1. sprzedaży kontraktu/usługi/biletu

umożliwiający analizę sprzedaży wybranego jednego rodzaju (kodu) kontraktu/usługi/biletu lub kilku rodzajów (kodów) lub wszystkich rodzajów (kodów) w zadanym okresie, pozwalający na określenie sprzedaży za dany okres tj. dzień, dekada, miesiąc, rok

Zawierający co najmniej dane:

- data sprzedaży;
- kod/kody kontraktu/usługi/biletu;
- numer kontraktu/usługi/biletu (indywidualny, unikatowy);
- rodzaj taryfy;
- nazwy kontraktu/usługi/biletu;
- ważność kontraktu/usługi/biletu od....do....;
- cena jednostkowa;
- liczba przejazdów;
- GIT (unikatowy identyfikator transakcji);
- liczba;
- wartość brutto;
- kod typu punktu sprzedaży/kanału dystrybucji;
- kod punktu sprzedaży;
- konto użytkownika IKU;
- wykorzystany identyfikator (identyfikacja konkretnego identyfikatora);
- forma/rodzaj dokonanej płatności.

z możliwością filtracji dla dowolnego przedziału czasu, numeru biletu, kodu biletu, nazwy biletu, taryfy, kanału dystrybucji itp.

Raport 2. transakcji sprzedaży usług

Zawierający co najmniej dane:

- kod typu punktu sprzedaży;
- kod punktu sprzedaży;
- nr urządzenia;
- data transakcji;
- GIT, unikatowy identyfikator transakcji;
- rodzaj płatności;
- kod/nip dystrybutora;
- kod/nip dostawcy usług;
- numer kontraktu/usługi/biletu;
- kod biletu/usługi/kontraktu;
- nazwa katalogowa kontraktu/usługi/biletu;
- ważność kontraktu/usługi/biletu od....do....;
- rodzaj zastosowanej ulgi;

- cena jednostkowa;
- waluta;
- liczba;
- wartość brutto;
- potwierdzenie statusu: np. transakcja udana, nieudana;
- konto IKU dla którego została zawarta transakcja;
- typ/rodzaj identyfikatora.

z możliwością filtracji dla dowolnego przedziału czasu, kanału dystrybucji, urządzenia, identyfikatora, dystrybutora, nr biletu, nazwy biletu, taryfy, itp..

Raport 3. sprzedaży dla agentów sprzedaży:

Raport sprzedaży ma posiadać informację o statusie każdej transakcji (poprawna, niepoprawna), wymagane co najmniej pola:

- nazwa terminala;
- numer terminala;
- kod punktu sprzedaży;
- kod Dystrybutora;
- data godzina;
- rodzaj transakcji i płatności;
- GIT, unikatowy identyfikator transakcji;
- kod biletu/usługi/kontraktu;
- numer kontraktu/usługi/biletu;
- ilość;
- wartość;
- czy wydano potwierdzenie;
- numer konta IKU;
- identyfikator konta IKU (identyfikacja konkretnego identyfikatora);
- status płatności – np. udana, nieudana, anulowana.

z możliwością filtracji dla:

- typu płatności;
- konta użytkownika IKU;
- Typ/rodzaj identyfikatora;
- Po kodach biletów/usług/kontraktów;
- Data, godzina [przedział];
- Ilość [przedział];
- Wartość [przedział]
- Kod Dystrybutora

z możliwością filtracji dla dowolnego przedziału czasu, urządzenia.

Metrobilet i inne oferty specjalne:

Raporty powinny umożliwić rozliczenie dot. sprzedaży biletów z oferty specjalnej METROBILET lub innych ofert z innymi organizatorami transportu publicznego (kolejowego, autobusowego, tramwajowego, trolejbusowego, miejskiego, podmiejskiego, międzynarodowego itp.) w tym rozpatrzonych reklamacji i ich rozliczeń.

Raport 4. szczegółowy ze sprzedaży, wymagane co najmniej pola:

- Numer konta IKU;
-
- Identyfikator (identyfikacja konkretnego identyfikatora);
- Numer biletu;
- Kod biletu;
- GIT; unikatowy identyfikator transakcji;
- Data i godzina sprzedaży;
- Nazwa kontraktu;
- Cena składowa 1 (np. ZTM)
- Cena składowa 2 (innego operatora/ innych operatorów)
- Cena całkowita, łączna
- Typ urządzenia;
- Nr urządzenia
- TID;
- Data ważności biletu od;
- Data ważności biletu do;
- Normalny;
- Ulgowy (różne ulgi);
- Ilość;
- Typ/rodzaj płatności;

Raport generowany według potrzeb np.: za dowolny okres, dla wybranego rodzaju biletu itp..

Raport 5. szczegółowy z przyjętych zwrotów biletów

z oferty specjalnej METROBILET lub innych ofert z innymi organizatorami transportu publicznego (kolejowego, miejskiego itp.) wymagane co najmniej pola:

- Numer konta IKU ;
- Data ważności biletu od;
- Data ważności biletu do;
- Data operacji;
- Kod kontraktu;
- Nazwa biletu;
- Numer biletu
- Cena biletu;

- Liczba dni do zwrotu (do końca ważności biletu);
- Kwota zwrotu;
- Kwota części ZTM;
- Kwota części Kolei Śląskich lub innego operatora;
- Wartość odstępnego;
- Identyfikacja POP dokonującego zwrotu;
- Forma zwrotu (np. gotówka, przelew na konto etc.
- Identyfikacja osoby wykonującej zwrot;
- GIT zwrotu;
- GIT Sprzedaży;
- Tryb zwrotu (np. tryb specjalny, tryb pomyłka, z potrąceniem etc.)

Raport generowany według potrzeb np.: za dowolny okres, dla wybranego rodzaju biletu, dla wybranej formy zwrotu itp.

Raport 6. szczegółowy z rozpatrzonych reklamacji dot. np. metrobiletu lub innej oferty specjalnej, wymagane co najmniej pola:

- Numer konta IKU;
- Data złożenia reklamacji;
- ID kontraktu;
- Nazwa biletu;
- Numer biletu
- Cena biletu;
- GIT transakcji zakupu;
- Data ważności biletu od;
- Data ważności biletu do;
- Liczba dni za które uznano zwrot;
- Kwota zwrotu z tytułu pozytywnego rozpatrzenia reklamacji;
- Kwota ZTM;
- Kwota Kolei Śląskich lub innego operatora;
- Odstępne;
- Data rozpatrzenia reklamacji;
- Data przesłania zwrotu;
- Tryb zwrotu;

Raport generowany według potrzeb np.: za dowolny okres, dla wybranego rodzaju biletu, dla wybranej formy typu zwrotu itp.

Raport 7. dot. promocji

Raport szczegółowy ze sprzedaży biletów z oferty promocyjnej wymagane co najmniej pola:

- Nr konta IKU;
- Rodzaj identyfikatora;
- kod typu punktu sprzedaży;
- kod punktu sprzedaży;
- nr urzędu;
- data transakcji;
- GIT, nr transakcji;
- Rodzaj płatności;
- kod/nip dystrybutora;
- kod/nip dostawcy usług;
- kod biletu;
- numer biletu;
- nazwa katalogowa usługi;
- ważność biletu od...do....;
- Rodzaj ulgi;
- cena jednostkowa nominalna;
- rodzaj promocji (np. %, „święteczna”, „okolicznościowa”..itp.);
- Cena jednostkowa promocyjna;
- Waluta;
- Liczba;
- wartość brutto;
- potwierdzenie statusu: np. transakcja udana, nieudana.

Z możliwością filtracji dla dowolnego przedziału czasu, rodzaju promocji, daty obowiązywania promocji, kanału dystrybucji, po cenie biletu nominalnej i promocyjnej itp.

Raport 8. ze skasowań biletów/wnoszenia opłat w kasownikach zamontowanych w pojazdach.

Raport szczegółowy ze skasowań biletów w kasownikach zamontowanych w pojazdach powinien posiadać informację o statusie każdej transakcji (poprawna, niepoprawna), zawiera transakcje z użyciem identyfikatorów i skasowania biletów papierowych z kodem QR - wymagane co najmniej pola:

- Data, godzina- minuty-sekundy skasowania/ transakcji;
- Nazwa Operatora;
- Numer Urzędu;
- Pojazd;
- Linia;
- Kierunek Trasy;
- Gmina;
- Nazwa przystanku;
- Typ biletu (np. elektroniczny, papierowy);
- Kod biletu;
- Numer biletu
- Nazwa biletu;

- Rodzaj biletu/Nazwa kontraktu;
- Cena biletu skasowanego;
- Identyfikator (identyfikacja konkretnego identyfikatora);
- GIT;
- TID - identyfikator terminala;

Przy założeniu, że nie wymagają kasowania bilety zakupione w kasowniku – system powinien zaciągać sprzedaż jako skasowanie do Raportu skasowań.

z możliwością filtracji dla:

- Przewoźnika
- Linii
- Pojazdu
- Urządzenia
- Daty
- Typ biletu
- Kod biletu;
- Nazwa biletu;

z możliwością filtracji dla dowolnego przedziału czasu, urządzenia, linii, po cenie biletu itp.

Raport 9. użycia identyfikatora:

Raport szczegółowy dot. użycia identyfikatora przez pasażera powinien posiadać wymagane co najmniej pola:

- Data i czas operacji;
- Identyfikator (identyfikacja konkretnego identyfikatora);
- Rodzaj operacji: zakup kontraktu/biletu, zasilenie, zwrot, wydanie identyfikatora, kaucja, wydanie dupliktu, usunięcie kontraktu/biletu, zablokowanie identyfikatora, odblokowanie identyfikatora, zmiana pinu itp.;
- KOD Kontraktu/biletu/operacji;
- Numer biletu;
- Nazwa Kontraktu/Biletu;
- Data ważności biletu od ...;
- Data ważności biletu do ...;
- Cena Kontraktu/ biletu;
- ID punktu/Miejsce dokonanej operacji (np. POP, SAD, UPOS itp.);
- Wykonał - identyfikacja osoby wykonującej zwrot;
- Wartość;
- Kod/NIP Punktu;
- GIT operacji;
- Rodzaj płatności.

z możliwością filtracji dla:

- Poszczęólnego identyfikatora;
- Data od..... do.....

Raport 10. dla konta IKU:

Raport szczegłowy dot. operacji na koncie IKU, powinien posiadać wymagane co najmniej pola:

- Data Operacji;
- Identyfikator (identyfikacja konkretnego identyfikatora);
- Rodzaj operacji: zakup kontraktu/biletu, zasilenie, zwrot, wydanie identyfikatorów, kaucja, usunięcie kontraktu/biletu, zablokowanie identyfikatorów, odblokowanie identyfikatorów, zmiana hasła, pinu, danych osobowych itp.;
- KOD Kontraktu/biletu/operacji;
- Numer biletu;
- Nazwa Kontraktu/Biletu;
- Data ważności biletu od ...;
- Data ważności biletu do ...;
- Cena Kontraktu/ biletu;
- ID punktu/Miejsce dokonanej operacji (np. POP, SAD, UPOS itp.);
- Wykonał - Identyfikacja osoby wykonującej zwrot;
- Wartość;
- Kod/NIP Punktu;
- GIT operacji;
- Rodzaj płatności.

z możliwością filtracji dla:

- Poszczęólnego identyfikatora;
- Data od..... do.....

Raport 11. zwrotów biletów:

Raport szczegłowy dot. zwrotów biletów przez pasażera powinien posiadać wymagane co najmniej pola:

- Data Operacji;
- Rodzaj Identyfikatora (Karta ŚKUP/ŚKUP2.0, Aplikacja mobilna, karta płatnicza itp.);
- Identyfikator (identyfikacja konkretnego identyfikatora);
- KOD Kontraktu/biletu/operacji;
- Nazwa Biletu;
- Numer biletu;
- Data ważności biletu od ...;
- Data ważności biletu do ...;
- Cena biletu;
- Liczba dni do zwrotu (do końca ważności biletu);
- Kwota zwrotu;

- Forma zwrotu;
- Tryb zwrotu;
- ID punktu/Miejsce zwrotu (np. POP, SAD, itp.);
- Wykonał - Identyfikacja osoby wykonującej zwrot;
- Wartość;
- Identyfikacja POP dokonującego zwrotu;
- GIT Zwrotu;
- GIT Sprzedaży;
- Odstępne/opłata.

z możliwością filtracji dla:

- Daty;
- Rodzaj kontraktu/biletu (taryfy);
- KOD USŁUGI;
- Numer biletu;
- Poszczególnego identyfikatora.

Raport 12. z elektronicznego magazynu biletów dla systemu ŚKUP 1.5 (MTC-magazyn)

Raport szczegółowy z wygenerowanych biletów powinien posiadać informację o statusie każdej transakcji tj. np.: poprawna, niepoprawna, wymagane co najmniej pola:

- Odbiorca (nazwa, numer identyfikacyjny);
- Numer urzędu;
- Numer paczki;
- Numery wygenerowane (zawarte w paczce lub pojedyncze) dla każdego poszczególnego biletu, serie biletów;
- Data godzina transakcji;
- Termin rozliczenia;
- Rodzaje biletów/nazwa katalogowa biletów zawartych w paczce;
- Cena jednostkowa dla poszczególnych rodzajów biletów;
- Liczba poszczególnych biletów w danej transakcji;
- Wartość dla poszczególnego rodzaju biletów;
- Ogólna wartość transakcji;
- Wysokość prowizji/upustu;
- Wartość naliczonej prowizji/upustu (od wartości i ilości);
- Zaległości płatnicze;
- Stan (liczba poszczególnych rodzajów biletów u odbiorcy);
- Numeracja poszczególnych rodzajów biletów niesprzedanych;
- Statut odbiorcy np. czynny/zablokowany/nieaktywny.

Raport generowany według potrzeb np.: za dowolny okres, dla wybranego Odbiorcy, dla wybranego rodzaju biletów itp.

Raport 13. szczegółowy z wygenerowanych biletów przekazanych dla poszczególnych sprzedawców zaopatrywanych przez odbiorcę raportu,

powinien posiadać informację o statusie każdej transakcji tj. np.: poprawna, niepoprawna, wymagane co najmniej pola:

- Sprzedawca (nazwa, numer identyfikacyjny);
- Lokalizacja punktu sprzedaży;
- Numer urządzenia;
- Data i godzina logowania;
- Numer otrzymanej paczki;
- Numery wygenerowane (zawarte w paczce lub pojedyncze) dla poszczególnych rodzajów biletów, serie biletów;
- Data godzina otrzymania dostawy;
- Rodzaje biletów/według nazwy katalogowej biletów zawartych w paczce;
- Cena jednostkowa dla poszczególnych rodzajów biletów;
- Liczba poszczególnych biletów w danej transakcji;
- Wartość dla poszczególnego rodzaju biletów;
- Ogólna wartość transakcji tj. otrzymania dostawy;
- Data sprzedaż biletu pasażerowi;
- Rodzaj/nazwa katalogowa sprzedanego biletu;
- Cena jednostkowa;
- Numer sprzedanego biletu;
- GIT; unikatowy identyfikator transakcji;
- Status transakcji (np. zakończona, przzerwana, niezrealizowana itp.);
- Status wydruku (np. poprawny, częściowy, brak wydruku itp.);
- Forma płatności (np. gotówka, karta płatnicza itp.);
- Stan (liczba poszczególnych rodzajów biletów u sprzedawcy);
- Statut sprzedawcy np. czynny/zablokowany/nieaktywny.

Raport generowany według potrzeb np.: za dowolny okres, dla wybranego Sprzedawcy, dla wybranego rodzaju biletów, dla wybranej formy płatności itp.

Ad. J Definiowanie opłat dodatkowych i przewoźnego

Opis definicji opłat dodatkowych i przypisywania do nich wysokości opłaty przewozowej, tzw. przewoźnego został opisany w rozdziale dotyczącym Podsystemu Infrastruktury w module Kontrolerka (UKNT).

5.2 Aplikacja dla Punktów Obsługi Pasażera (APO)

Realizuje funkcje kompleksowej obsługi użytkownika systemu i jego konta przez operatora Punktu Obsługi Pasażera, przy użyciu przeglądarki internetowej w ramach wewnętrznej sieci LAN, współpracuje z urządzeniem (zblizeniowy czytnik kart), które potrafi komunikować się z identyfikatorami/nośnikami (odczyt, zapis) oraz pin-padem do nadawania PIN/Hasła. Aplikacja ma również możliwość pracy poza punktem POP w zakresie, który pozwala na wykonywanie wybranych czynności nie wymagających współpracy z czytnikiem.

Obsługiwane (fizyczne) identyfikatory:

- Karta ŚKUP;
- Karta ŚKUP 1.5;
- Karta EMV i jej surogaty.

5.2.1 Funkcjonalności

1. Aplikacja Punktów Obsługi (APO) musi zapewnić:
 - a. Zakładanie / Aktywowanie / Modyfikowanie konta na podstawie posiadanego identyfikatora (identyfikator może zostać pozyskany w innym kanale np. w kiosku lub w SADiS) w tym automatyczne generowanie przez system PIN-u lub Hasła dla konta, skanowanie lub wykonywanie na miejscu i wprowadzanie do systemu zdjęcia użytkownika z wykorzystaniem podłączonego do komputera skanera lub kamery USB;
 - b. Udostępnienie loginu pasażerowi na podstawie identyfikatora;
 - c. Wprowadzanie, modyfikację i autoryzację danych powiązanych z kontem, w tym danych osobowych, ulg (na podstawie weryfikacji dokumentów);
 - d. Przechowywanie logów zmian danych, historii zmian, możliwość generowania pełnej historii konta użytkownika;
 - e. Obsługa użytkownika bez fizycznego identyfikatora po wyszukaniu na podstawie ustalonych danych np. pesel, email, telefon, numer konta/identyfikatora (co jednoznacznie zidentyfikuje pasażera);
 - f. Weryfikacja i potwierdzanie tożsamości klienta i jego obsługa na podstawie identyfikatorów;
 - g. Wykonywanie czynności związanych ze zmianą rodzaju konta;
 - h. Przypisywanie i usuwanie identyfikatorów do konta;
 - i. Wydawanie karty ŚKUP 1.5 jako identyfikatora do konta;
 - j. Zmiana aktywnego identyfikatora;
 - k. Zasilenie e-portmonetki;
 - l. Zwrot niewykorzystanych środków z e-portmonetki;
 - m. Generowanie historii użyc identyfikatorów oraz historii operacji dla konta IKU;
 - n. Usuwanie/Zwrot uprawnień/biletów zapisanych na koncie (opcjonalnie z wykorzystaniem PINu);
 - o. Odzyskiwanie Loginu/PINu/Hasła na adres e-mail lub z wykorzystaniem danych wcześniej zdefiniowanych dla konta (np. PESEL – na podstawie weryfikacji Dokumentu tożsamości);
 - p. Blokowanie, odblokowywanie i zwrot identyfikatorów w tym obsługa zwrotu kaucji;
 - q. Dla operatorów ze specjalnymi uprawnieniami zawansowane zarządzanie kontem, w tym blokowanie i odblokowywanie konta lub usuwanie lub dodawanie, blokowanie

- i odblokowywanie uprawnień bez obecności identyfikatora lub użytkownika (np. w przypadku fraudów lub rozpatrzenia reklamacji);
- r. Dodawanie uprawnień (ulg), sprzedaż biletów/usług (w tym parametryzowanie kwestii rozliczeniowych, np. zakodowanie jednego lub wielu biletów bez ponoszenia kosztów, lub wg określonej ceny, do fakturowania / rozliczania) dla wielu kont równocześnie na podstawie wybranej operacji, parametru i zaimportowanych list loginów kont lub list identyfikatorów (np. pliki CSV). Przeglądanie historii operacji wykonywanych w takim trybie (id operatora, id konta, data, rodzaj i wartość operacji, parametry itp.);
 - s. Obsługę faktur w tym wnioskowania i drukowania;
 - t. Integrację z urządzeniami peryferyjnymi: czytnik identyfikatorów (kart ŚKUP, kart EMV i jej surogatów), kamera, drukarki i skanera oraz możliwość wymiany danych z informatycznym systemem finansowo-księgowym Zamawiającego (raz na dobę);
 - u. Integrację i obsługę zdefiniowanych metod płatności;
 - v. Możliwość generowania raportów z pracy każdego operatora oraz z całego dnia (raporty kasowe). Raporty powinny zawierać informacje o wszystkich przeprowadzonych transakcjach z podziałem na typy/rodzaje transakcji wraz z podziałem na metody płatności. Opcjonalnie operator w POP musi mieć możliwość wygenerowania raportu szczegółowego zawierającego listę wszystkich przeprowadzonych przez siebie transakcji (w tym anulowanych). Raporty operatora nie powinny się zerować po wygenerowaniu – jeśli w tym samym dniu operator obsługiwałby system kilkakrotnie z przerwami (np. na obsługę przez innego operatora), to raport musi sumować transakcje od danego operatora (dla całego dnia pracy). Raporty muszą być możliwe do wygenerowania bezpośrednio po wykonaniu ostatniej transakcji – wymagany jest brak zwłoki czasowej powyżej 1 minuty od ostatniej operacji do wygenerowania kompletnego raportu;
 - w. Administrator merytoryczny APO ma mieć możliwość elastycznego zarządzania uprawnieniami dla poszczególnych użytkowników (np. nadanie uprawnień do sprzedaży biletów R1, obsługi zwrotów biletów i inne).
 - x. drukowanie potwierdzeń wykonywanych operacji finansowych i niefinansowych, formularzy, reklamacji, druków zgód na przetwarzanie danych oraz wszystkich innych dokumentów niezbędnych do obsługi użytkownika Systemu ŚKUP 1.5.
2. Rodzaje operacji finansowych:
- a. Wniesienie kaucji za kartę ŚKUP 1.5;
 - b. Zwrot kaucji za kartę ŚKUP 1.5;
 - c. Zwrot kaucji za kartę ŚKUP w odpowiedniej wysokości (wartości kaucji muszą zostać zmigrowane z systemu ŚKUP);
 - d. Zakup biletów/usług w tym wielu rodzajów biletów w jednej transakcji (tzw. koszyk biletów);
 - e. Zasilenie i zwrot środków z e-portmonetki;
 - f. Kodowanie biletów/usług (w tym biletów R1), informacja dot. powodu (wymaga odpowiednich uprawnień, raporty użycia takiej funkcji);
 - g. Anulowanie zakupu biletu w trybie pomyłka (operatora);
 - h. Zwrot biletu w trybie automatycznym lub reklamacyjnym/specjalnym;
 - i. Uiszczenie opłaty dodatkowej;
 - j. Spłata zadłużenia na karcie EMV (w systemie ŚKUP).

5.2.2 Funkcjonalności związane z rozliczeniami

1) Obsługiwane (fizycznie) identyfikatory:

- Karta ŚKUP;
- Karta ŚKUP 1.5;
- Karta EMV i jej surogaty.

2) Rodzaje płatności (w tym zwrotów):

- Gotówka;
- Karta płatnicza i surogaty (w tym HCE);
- BLIK;
- Google Pay;
- Apple Pay;
- Inne nowoczesne rodzaje i metody płatności w tym portfele elektroniczne zadeklarowane przez Wykonawcę w ofercie.

5.3 Moduł Dystrybucji Kart (MDYS)

Moduł ma umożliwiać zarządzanie zamawianiem i dystrybucją kart ŚKUP 1.5, jednocześnie pełniąc funkcję magazynu kart. Zarządzanie cyklem życia karty od jej zamówienia przez wyprodukowanie, dostarczenie do magazynu, przypisanie do dystrybutora, Punktów Dystrybucyjnych Kart (PDK – maksymalna planowana ilość punktów dystrybucji - 10 szt.), aktywowanie, wydanie, zablokowanie itp. Zarządzanie statusami karty w systemie – bieżącymi oraz archiwalnymi (np.: karta zamówiona, w produkcji, wyprodukowana, wysłana, odebrana/przyjęta na stan, wydana, aktywna, zablokowana, zastrzeżona, itp.). Zarządzanie paczkami dystrybucyjnymi, przypisanie odpowiedzialności materialnej na każdym etapie cyklu życia. Obsługa stanów magazynowych w tym u dystrybutorów (PDK). Operator PDK dysponując danymi na temat ilości minimalnego stanu kart zdefiniowanymi dla każdego urządzenia/ swojego punktu dystrybucyjnego, na podstawie przekroczenia stanów minimalnych powinien utworzyć w systemie zamówienia częściowe, które na koniec dnia zostaną podsumowane i będą podstawą wygenerowania zamówienia zbiorczego. Po zrealizowaniu zamówienia zbiorczego magazyn kart wykaże listę zamówień częściowych zrealizowanych w ramach zamówienia zbiorczego. Do producenta kart, zamówienie zbiorcze może być generowane maksymalnie raz w ciągu dnia, z zastrzeżeniem, że dostawa kart do PDK będzie realizowana tylko raz w tygodniu (w uzgodnionym z Zamawiającym dniu). Operator modułu będzie miał możliwość zdefiniowania parametrów ilości minimalnego stanu kart oraz ilości kart zamawianych dla wybranego urządzenia (z zastrzeżeniem, że minimalna ilość paczki kart to 5 szt., a maksymalna to 50 szt.). Dlatego też zamówienie składane przez Operatora będzie wielokrotnością ilości paczek kart. W przypadku przekroczenia stanu minimalnego Operator powinien otrzymywać z modułu informację o takim zdarzeniu, celem dokonania zamówienia kolejnej partii kart. Wyprodukowane karty będą dostarczane do PDK, z którego zostało złożone zamówienie na karty. W ramach niniejszego zamówienia, Wykonawca będzie świadczył usługę produkcji oraz dostawy kart do PDK. Karty dostarczone do PDK, które zostały wadliwe wyprodukowane zostaną zwrócone Wykonawcy w ramach reklamacji i nie będą się wliczały w pulę kart wydanych.

5.3.1 Funkcjonalności

- Zamawianie i drukowanie kart u Wykonawcy;
- Ustawienie globalnego parametru w celu zdefiniowania minimalnych i maksymalnych wielkości paczek przesyłanych do PDK;
- Dystrybucja kart do sieci urządzeń i punktów dystrybucyjnych (punkty Agentów Sprzedaży, SADiS, POP, inne punkty dystrybucji);
- Obsługa zwrotów kart do magazynu Wykonawcy (niewykorzystanych, uszkodzonych, zwróconych);
- Zapewnienie możliwości relokacji kart między urządzeniami/punktami dystrybucji (w sytuacji występujących braków i jednoczesnych nadwyżek w innych punktach dystrybucji);
- Monitorowanie stanu kart w urządzeniach i magazynie centralnym i punktach dystrybucyjnych;
- Monitorowanie ilości kart będących w obiegu i ich statusu (aktywne, zablokowane, wycofane, daty zmian statusów – historycznie, itd.);
- API do AOZ urządzeń (w kwestii dystrybucji kart SADiS, APO, UPOS);

Górnośląsko-Zagłębiowska Metropolia
40-053 Katowice
ul. Barbary 21A
tel. +48 32 718 07 00, fax +48 32 718 07 99
email: za@metropoliagzm.pl
www.metropoliagzm.pl



- API do producenta kart (kwestie produkcji, zamawiania i dostawy);
- Raporty magazynowe - zestawienia wg statusów kart (w tym statusów historycznych), dystrybutorów i punktów Agentów Sprzedaży (np.: sieć sprzedaży kioski), z możliwością definiowania przedziałów czasowych, eksportu do plików CSV, PDF;
- Zarządzanie uprawnieniami (profile wg. roli/użytkowników modułu: np. administrator, operator oraz wg funkcji: np. zamawianie kart; raportowanie itp.).

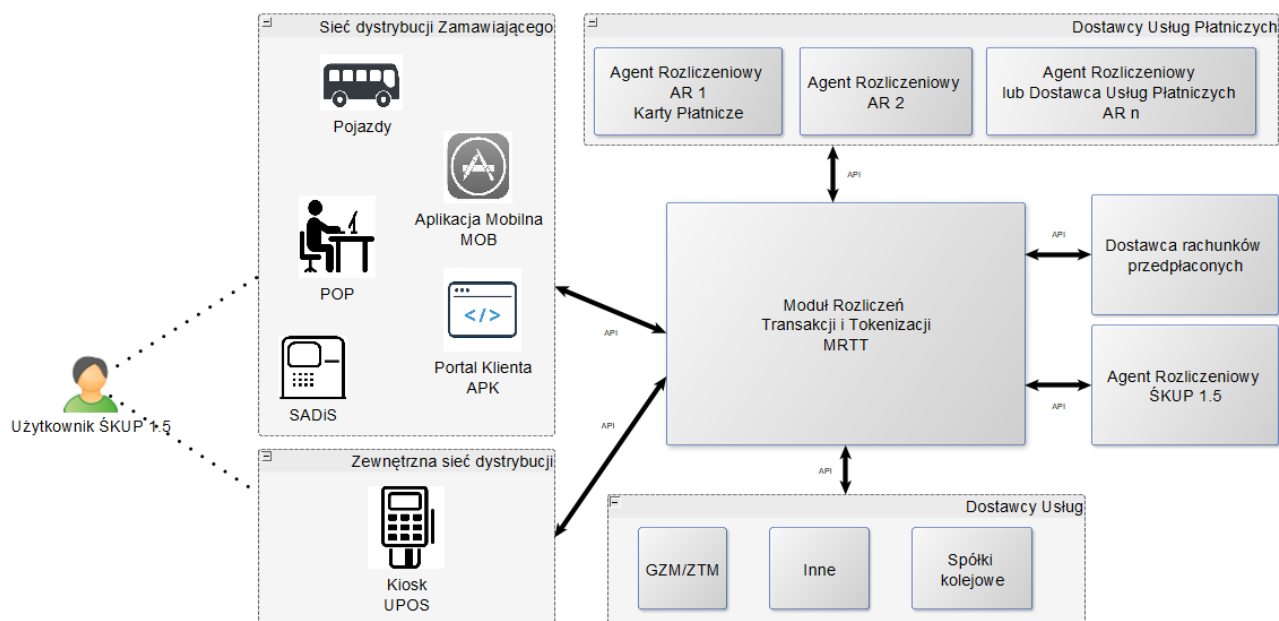
5.4 Moduł Rozliczeń Transakcji i Tokenizacji (MRTT)

Moduł rozliczeń funkcjonuje w ścisłym powiązaniu z AR ŚKUP 1.5. Centralny moduł rozliczeniowy będzie przetwarzał wszystkie transakcje (finansowe i niefinansowe) oraz będzie obsługiwał wszystkie usługi związane z rozliczeniami realizowane w systemie. Moduł będzie odpowiedzialny za przetwarzanie danych transakcyjnych systemu ŚKUP 1.5 oraz wymianę danych z usługami realizowanymi przez usługodawców zewnętrznych takich jak Agenci Rozliczeniowi, instytucje płatnicze, payment Gateway. Będzie realizował między innymi takie funkcjonalności jak: biling transakcji, raportowanie, rozliczanie (w tym rozliczanie środków z tytułu zakupu i stopnia wykorzystania punktów z e-portmonetki), rozrachunek z podmiotami uczestniczącymi w systemie.

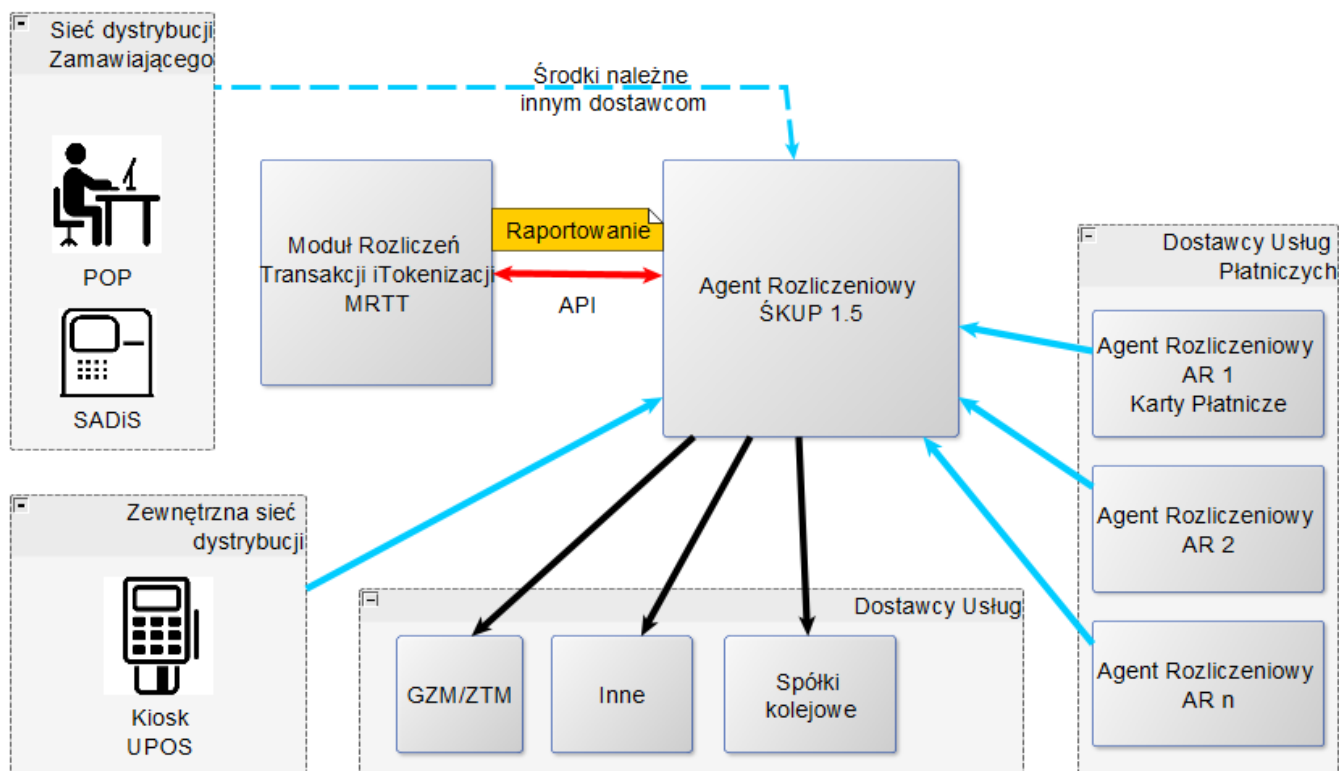
Wymiana danych będzie odbywała się przez otwarte interfejsy danych zdefiniowane i opisane przez Wykonawcę, co pozwoli na wymianę lub dołączanie kolejnych usług związanych z rozliczeniami transakcji (np. dołożenie kolejnych metod płatności). Moduł będzie zapewniał monitoring transakcji w trybie rzeczywistym, ma posiadać zaawansowane funkcje raportowe dot. transakcji i rozrachunków. Moduł musi przetwarzać w tym gromadzić dane i dostarczać raporty ze stanów rozrachunków pomiędzy poszczególnymi podmiotami jak np. codzienne raportowanie stanu rozrachunków pomiędzy Dystrybutorami usług i Dostawcami usług (raporty dla każdego z Dystrybutorów – zbiorcze i szczegółowe, na dany dzień, zobowiązania Dystrybutorów wobec poszczególnych Dostawców, a dla Dostawców usług będzie dostarczał raporty, na dany dzień, kto ma zobowiązania wobec nich). Będzie również korelował operacje rozliczeniowe z rozrachunkiem i udostępniał raporty z transakcji podmiotom biorącym udział w rozliczeniach z dokładnością do pojedynczych transakcji i jej aktualnego statusu. Szczegóły zostaną zaproponowane przez Wykonawcę w opisie Modelu Rozliczeń Pieniężnych.

Będzie automatycznie generował raporty dla systemów księgowych i kontrolingu podmiotów uczestniczących w systemie. Obsługiwał będzie żądania dot. faktur dla użytkowników systemu i je przekazywał do i z systemu księgowego Zamawiającego.

Wykonawca przekaze Zamawiającemu opisy wszystkich interfejsów API Modułu MRTT. Przekazanie i akceptacja przez Zamawiającego tego dokumentu jest wymagana do odbioru etapu modernizacji systemu. W trakcie utrzymania systemu Wykonawca będzie aktualizował ten dokument po każdej wprowadzonej zmianie nie później niż 30 dni od wprowadzenia zmian.



Rysunek 11. Uproszczony przepływ informacji o transakcjach.



Rysunek 12. Uproszczony przepływ środków pieniężnych.

5.4.1 Model Rozliczeń Pieniężnych

Wykonawca przygotowuje projekt Modelu Rozliczeń Pieniężnych (MRP) dla projektu ŚKUP 1.5. Projekt MRP musi być uzgodniony i zaakceptowany przez Zamawiającego, w terminie do 90 dni od podpisania umowy. MRP musi uwzględniać realizację wszystkich funkcjonalności/procesów/usług rozliczeniowych, rozrachunkowych, płatniczych wymaganych dla funkcjonowania systemu ŚKUP 1.5 oraz wymogi organizacji płatniczych i spełniać wymogi prawa w zakresie rozliczeń finansowych, w szczególności przepisów w zakresie podatku VAT oraz zasad gospodarki finansowej samorządowych jednostek budżetowych.

Musi również uwzględniać reguły wykrywające ewentualne fraudy i nadużycia w systemie.

W ramach MRP Wykonawca przygotowuje i uzgodni z Zamawiającym projekty wszystkich niezbędnych dokumentów związanych z uruchomieniem funkcjonalności opisanych w MRP w tym wszelkie umowy i regulaminy, w tym regulamin obsługi punktów e-portmonetki na koncie IKU.

Przekazanie i akceptacja przez Zamawiającego docelowego MRP jest wymagana do odbioru etapu modernizacji systemu. W trakcie utrzymania systemu Wykonawca będzie aktualizował ten dokument po każdej wprowadzonej zmianie nie później niż 30 dni od wprowadzenia zmian.

5.4.2 Funkcjonalność modułu MRTT

W systemie ŚKUP 1.5 może funkcjonować, w ramach usług świadczonych przez Wykonawcę, jeden lub kilku Agentów rozliczeniowych, ale muszą zostać zrealizowane przez niego/nich wszystkie funkcjonalności wymagane do działania systemu rozliczeniowego i rozrachunkowego. Wykonawca świadczący usługi Agentów lub Agentów rozliczeniowych zapewni rozliczenia i rozrachunek dla wszystkich transakcji realizowanych w systemie (w tym wykonywanych kartami płatniczymi i ich surogatami), tj. na Portalu Klienta, w Aplikacji Mobilnej (MOB), automatach biletowych (SADiS), Punktach Obsługi Pasażera (POP), w pojazdach i u Dystrybutorów usług - UPOS (z wyjątkiem płatności kartami płatniczymi). Rozliczenie i rozrachunek dotyczy transakcji inicjalizowanych identyfikatorami ŚKUP oraz innych rodzajów transakcji przygotowanych przez Wykonawcę w ramach realizacji wymagań Zamawiającego dotyczących funkcjonalności systemu ujętych w opisie przedmiotu zamówienia oraz w Modelu Rozliczeń Pieniężnych. Uproszczony, proponowany przez Zamawiającego sposób funkcjonowania został pokazany na rysunkach 8 i 9. Wybór Agentów rozliczeniowych lub Agentów rozliczeniowych jest obowiązkiem Wykonawcy. Wszystkie koszty związane z funkcjonowaniem Agentów rozliczeniowych, w tym za świadczenie usług przez instytucje płatnicze, finansowe i rozrachunkowe, za rozliczeniami i rozrachunkiem transakcji i inne usługi niezbędne do funkcjonowania systemu rozliczeń i rozrachunku pokrywa Wykonawca ramach wynagrodzenia za realizację zamówienia w całym okresie obowiązywania umowy, chyba że zostało to inaczej zapisane w niniejszym dokumencie. Wykonawca ponosi ryzyko braku rozliczenia wszystkich transakcji w systemie również wykonanych kartami płatniczymi EMV.

Wykonawcy systemu dostarczy i będzie świadczył przez cały okres umowy usługę finansową (Agent Rozliczeniowy ŚKUP 1.5 – integrator płatności) polegającą na obsłudze rozliczeń wszystkich transakcji (gotówkowych i bezgotówkowych) i rozrachunku środków (w zakresie płatności bezgotówkowych, gotówkowe będą rozliczane we własnym zakresie przez ZTM) pomiędzy wszystkimi uczestnikami w systemie ŚKUP 1.5 w ścisłym powiązaniu (poprzez zdefiniowane przez Wykonawcę API) z Modułem

Rozliczeń Transakcji i Tokenizacji. AR ŚKUP 1.5 będzie pośredniczył w przekazywaniu środków pomiędzy uczestnikami rozliczeń w szczególności Agentami Rozliczeniowymi, Dystrybutorami i Dostawcami usług. Szczegółowe działanie AR ŚKUP 1.5 będzie zdefiniowane przez Model Rozliczeń Pieniężnych. Kodowanie poszczególnych urządzeń/modułów w systemie AR ŚKUP 1.5 powinno być zgodnie z kodowaniem tych elementów w systemie ŚKUP 1.5.

Transakcje wykonywane w pojazdach kartami ŚKUP i ŚKUP 1.5 są rozliczane z punktów e-portmonetki powiązanej z kontem IKU. Do wszystkich urządzeń w systemie (szczególnie do Pojazdów) są dystrybuowane salda e-portmonetek powiązanych z kontami IKU. Dystrybucja tych sald odbywa się w czasie zbliżonym do rzeczywistego. Zmawiający dopuszcza dodatkowo wykorzystanie karty jako nośnika do przechowywania salda e-portmonetki powiązanej z kontem IKU w celu wymiany punktów na uprawnienia do usług w systemie ŚKUP pod warunkiem zapewnienia synchronizacji danych w czasie zbliżonym do rzeczywistego.

Jeżeli nie zapisano inaczej to wszystkie koszty związane z obsługą transakcji pokrywa Wykonawca w ramach wynagrodzenia za realizację zamówienia, a do odbiorców środków zawsze trafia pełna kwota należności za usługę (nie będzie pomniejszana o żadne koszty związane z wykonaniem transakcji).

Za transakcje uznawane są również transakcje zwrotu środków np. za zwrócone bilety, punkty.

Pozyskanie nowej karty ŚKUP 1.5 jest związane z wniesieniem kaucji, której wysokość jest parametrem definiowanym w systemie. Kaucja ma zabezpieczyć przed nadmiernym popytem na karty. Kaucje będą przechowywane na rachunku Zamawiającego. Wszystkie procesy związane z obsługą kaucji w tym jej zwrotu, będą zaprojektowane, dostarczone, realizowane i utrzymywane w systemie dostarczonym przez Wykonawcę w ramach realizacji zamówienia. Koszt zwrotu kaucji przekazem pocztowym pokrywa użytkownik karty, koszty zwrotu innymi kanałami płatności (np. przelewem na wskazany przez użytkownika IKU rachunek bankowy) pokrywa Wykonawca w ramach wynagrodzenia za realizację zamówienia.

Wykonawca zapewni obsługę zwrotów kaucji za karty ŚKUP na okaziciela (niespersonalizowane) wydawane w trakcie funkcjonowania obecnego systemu ŚKUP. Środki na te transakcje są zdeponowane na rachunku bankowym Zamawiającego. Koszt zwrotu kaucji przekazem pocztowym pokrywa użytkownik karty, koszty zwrotu innymi kanałami płatności (np. przelewem na wskazany przez użytkownika IKU rachunek bankowy) pokrywa Wykonawca w ramach wynagrodzenia za realizację zamówienia;

Rozliczenie środków (zaraportowanie transakcji) musi następować najpóźniej następnego dnia po wystąpieniu transakcji. Rozrachunek środków (uznanie rachunku bankowego odbiorcy środków pieniężnych) musi nastąpić najpóźniej następnego dnia roboczego od postawienia środków do dyspozycji przez dłużnika. Wykonawca zbuduje mechanizmy ponawiania obciążeń dla transakcji, które nie zostały zapłacone przy pierwszym żądaniu (minimum 3 ponowienia). Wykonawca zapewni, że wszystkie transakcje, wykonywane przez użytkowników systemu w pojazdach, muszą zostać zapłacone Zamawiającemu do 16 dnia miesiąca następującego po miesiącu, w którym nastąpiła transakcja nawet jeżeli dłużnik/użytkownik nie udostępni środków.

Za bezpieczeństwo i monitoring transakcji przetwarzanych w systemie ŚKUP 1.5 i w usługach dostarczonych przez Wykonawcę (w tym Agentów Rozliczeniowych) poprzez wprowadzenie rozwiązań

uniemożliwiającego zniekształcenie, skasowanie lub pozyskiwanie przez osoby nieuprawnione informacji o rozliczeniach prowadzonych w systemie ŚKUP 1.5 odpowiada Wykonawca. Zamawiający zastrzega sobie prawo do prowadzenia własnego monitoringu systemu rozliczeń, w tym z wykorzystaniem narzędzi dostarczonych przez Wykonawcę, w tym raportów opisanych w Module Rozliczania Transakcji i Tokenizacji. W razie skompromitowania zastosowanych metod zabezpieczeń Wykonawca jest zobowiązany na własny koszt przebudować mechanizmy bezpieczeństwa systemu.

Ryzyko związane z brakiem środków na pokrycie transakcji wykonanych w systemie ŚKUP 1.5 w kanałach płatności dostarczonych przez Wykonawcę (dotyczy nie tylko kart płatniczych, lecz wszystkich transakcji) ponosi Wykonawca. Ryzyko to jest bezpośrednio związane z koniecznością szybkiego blokowania identyfikatorów/kont IKU, które nie mają pokrycia finansowego/punktowego za dokonywane transakcje. Również wszystkie koszty związane z utratą lub zniekształceniem danych przez system, w tym w usługach dostarczonych przez Wykonawcę, pokrywa Wykonawca.

Wszystkie koszty związane z rozliczeniami i rozrachunkiem transakcji, w tym za świadczenie usług przez instytucje płatnicze, finansowe i rozrachunkowe pokrywa Wykonawca w ramach wynagrodzenia za realizację zamówienia, chyba że w niniejszym dokumencie zapisano inaczej;

Wykonawca zapewni komplet usług i funkcjonalności pozwalających na zamianę środków pieniężnych na punkty gromadzone na e-portmonetkach powiązanych z kontami IKU systemu ŚKUP 1.5, w ramach, których użytkownik systemu może dokonywać zakupu biletów lub wносить opłaty za przejazd. Zasilenia e-portmonetki będzie można dokonać z wykorzystaniem elementów systemu ŚKUP 1.5 w tym Portalu Klienta, Aplikacji Mobilnej, POP, SADiS, opcjonalnie u Agentów Sprzedaży. Użytkownik konta IKU w kontekście tego konta będzie mógł wnioskować o zwrot środków za niewykorzystane punkty na wskazany rachunek bankowy lub przekazem pocztowym na wskazany adres. Koszt zwrotu środków przekazem pocztowym pokrywa użytkownik karty. Wszystkie pozostałe koszty związane z funkcjonowaniem i obsługą e-portmonetki (rachunku punktowego) pokrywa Wykonawca w ramach wynagrodzenia za realizację zamówienia.

5.4.3 Podstawowe procesy realizowane przez moduł MRTT

- 1) Obsługuje procesy tokenizacji kart płatniczych (należy przewidzieć różne podmioty rozliczeniowe EMV);
- 2) Obsługuje wszystkie formy i kanały płatności dostępne w systemie ŚKUP 1.5;
- 3) Gromadzi wszystkie zdarzenia związane z użyciem identyfikatora/konta mogące mieć wpływ na transakcje lub rejestrację zdarzeń w podróży (np. limity przejazdów) w tym rodzące skutki finansowe i nie rodzące takich skutków (np. operacja sprawdzenia stanu konta centralnego w urządzeniu ŚKUP);
- 4) Nadaje transakcjom unikalne identyfikatory;
- 5) Generuje i przekazuje obciążenia do Agentów Rozliczeniowych;
- 6) Gromadzi dane i pośredniczy w przekazywaniu do systemów zewnętrznych (np. Agentów Rozliczeniowych, banków) transakcji/obciążeń wynikających ze zdarzeń finansowych w systemie ŚKUP 1.5 (np. opłaty dodatkowe realizowane kartami płatniczymi);
- 7) Gromadzi i utrzymuje dane prowadzonych rachunków punktowych przypisanych do poszczególnych kont IKU w systemie centralnym, w tym odpowiada za operację zamiany wpłacanych/wypłacanych środków na punkty oraz odpowiada za salda punktów dla

- poszczególnych kont IKU. Za niezgodności danych na rachunkach punktowych odpowiada Wykonawca;
- 8) Rozlicza transakcje (również zwroty za niewykorzystane usługi, środki z tytułu zakupu i wykorzystania punktów jak i kaucje) pomiędzy uczestnikami systemu ŚKUP 1.5, w tym dokonuje podziału środków pomiędzy dostawców usług (patrz Metrobilet – wspólny bilet ZTM i KŚ);
 - 9) Generuje polecenia przelewów do systemów bankowych w tym do banku GZM/ZTM związane z rozliczeniami transakcji (również zwroty za niewykorzystane usługi, środki z tytułu zakupu i wykorzystania punktów jak i kaucje);
 - 10) Udostępnia codziennie każdemu uczestnikowi systemu rozliczeń raporty rozliczeniowe z dokładnością do pojedynczej transakcji (o zawartości minimum **Strumienia 1** opisanego poniżej) w tym również dotyczące zwrotów (niewykorzystanych usług i kaucji). Każdy z uczestników otrzymuje raporty z transakcjami, które jego dotyczą, a Zamawiający otrzymuje raport ze wszystkimi transakcjami;
 - 11) Gromadzi i przetwarza niezbędne raporty (w tym zestawienia wykonanych rozrachunków) pochodzące od Agentów Rozliczeniowych i z innych źródeł;
 - 12) Monitoruje i weryfikuje poprawność dostarczania raportów finansowych, rozliczeniowych i rozrachunkowych z zewnętrznych systemów w tym od Agentów rozliczeniowych;
 - 13) Na podstawie zgromadzonych i pozyskanych danych w tym z systemów Agentów Rozliczeniowych raportuje dziennie stany rozrachunków z dokładnością do pojedynczej transakcji i udostępnia raporty dla każdego z uczestników rozliczeń w tym zwroty za niewykorzystane usługi i kaucje. Każdy z uczestników rozliczeń otrzymuje raporty z danymi, które jego dotyczą, a Zamawiający otrzymuje raporty globalne;
 - 14) Udostępnia w postaci raportów, na żądanie uprawnionych użytkowników, kody słownikowe wykorzystywane w procesie identyfikacji i rozliczania transakcji (np. kody typów usług, kody Dostawców, kody Dystrybutorów, kody typów urządzeń itd.);
 - 15) Analizuje i utrzymuje aktualne statusy poszczególnych transakcji (np. do zapłaty, zapłacona, zrefundowana itd.) do czasu ich ostatecznego rozliczenia oraz raportuje te stany (o zawartości minimum **Strumienia 2** opisanego poniżej);
 - 16) Obsługuje i utrzymuje statusy poszczególnych identyfikatorów takie jak: aktywowanie w systemie, blokowanie i odblokowywanie, kwalifikowanie do różnych funkcjonalności, saldo środków z tytułu punktów e-portmonetki (np. dopuszczanie do transakcji zakupu biletu w pojazdach po zweryfikowaniu salda punktów).

5.4.4 Raportowanie

1) Serwer raportów plikowych

Wykonawca przygotowuje w infrastrukturze ŚKUP 1.5 bezpieczny zarządzalny z poziomu GUI, serwer do udostępniania plików raportów SFTP/WebDav (zaimplementowane przynajmniej wymienione mechanizmy), który będzie służył do bezpiecznej wymiany plików raportów pomiędzy uczestnikami systemu rozliczeń. Każdy z uczestników systemu rozliczeń będzie dysponował własnym kontem systemowym na serwerze SFTP/WebDav z odpowiednimi uprawnieniami do odpowiedniej struktury katalogów, w których będą umieszczane raporty. Zarządzanie uprawnieniami będzie po stronie

Zamawiającego. Struktura katalogów będzie dostosowana do funkcjonowania modelu rozliczeń przygotowanego przez Wykonawcę.

Dostawca raportów wszystkie pliki wytworzone przez siebie będzie przysyłał do własnego katalogu na serwerze SFTP/WebDav. Następnie automatycznie zostaną one rozdzielone do odpowiednich katalogów. Każdy odbiorca raportów otrzyma raporty, które będą zawierały tylko transakcje których jest stroną. Rozdzielanie to będzie uruchamiać się cyklicznie (skrypt + cron) w synchronizacji z cyklami zasilania dostawcy raportów. W nazwie każdego pliku będzie „klucz-kod-nazwa” katalogu, do którego ma trafić dany plik. Nazwa katalogu docelowego będzie odpowiadała fragmentowi nazwy pliku (np. 6 pierwszych znaków).

W przypadku większej liczby dostawców raportów, dla każdego z nich zostanie utworzony osobny katalog roboczy, a pliki w nim umieszczane automatycznie będą rozdzielane w osobnym skrypcie.

Każdy odbiorca raportów będzie miał dostęp tylko do swojego katalogu z danymi z uprawnieniami do odczytu plików, nie będzie mógł tego pliku usunąć ani dodać nowego.

Będzie możliwe zdefiniowanie kont z uprawnieniami pozwalającymi na odczyt danych z kilku katalogów.

Pliki będą składowane w katalogach przez okres definiowany parametrem przez Administratora Zamawiającego, po czym będą usuwane lub archiwizowane.

Każdemu katalogowi w drzewie odpowiada jedno konto użytkownika. Każde konto użytkownika należy do własnej grupy. Prawa do odczytu zawartości katalogu i nawigowania (rx) w danym katalogu ma własną grupę. Konto użytkownika z uprawnieniami do kilku katalogów należy do kilku grup.

Dla każdego pliku udostępnianego przez serwer SFTP/WebDav generowany jest plik skrót z wykorzystaniem funkcji kryptograficznej SCrypt (lub nowszy) w celu sprawdzenia integralności danych. Skrót pliku, wygenerowany za pomocą algorytmu SCrypt, tworzony jest w dodatkowym pliku podczas kopiowania plików raportów z systemu źródłowego. Następnie udostępniany odbiorcy raportu jako dodatkowy plik w tym samym katalogu.

Dostęp do serwera SFTP/WebDav będzie możliwy po zainstalowaniu na nim kluczy publicznych zainteresowanych odbiorców. Każdy z odbiorców samodzielnie generuje dla swoich potrzeb parę kluczy (długość klucza: 2048 bitów). Każdy odbiorca generuje oraz przechowuje swój klucz prywatny, wykorzystując w tym celu godny zaufania system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Każdy dostawca/odbiorca dostarcza swój klucz publiczny do systemu ŚKUP 1.5.

Klucze publiczne odbiorców zainstalowane na serwerze SFTP/WebDev będą dodatkowo skatalogowane przez system ŚKUP 1.5 w celu zarządzania nimi. Klucze te będą przechowywane na innym serwerze w pliku zip zabezpieczonym hasłem. W pliku tym powinien znaleźć się dokument Excel (xls), w ramach którego przechowywane będą informacje: od kogo i kiedy został przekazany danych klucz/unieważniony klucz.

2) Raporty plikowe

Transakcje realizowane w systemie będą raportowane w raportach plikowych, których ostateczna zawartość będzie uzgodniona i zaakceptowana przez Zamawiającego na etapie przygotowywania

Modelu Rozliczeń Pieniężnych (MRP) przez Wykonawcę. Ich ostateczna zawartość będzie uzależniona od MRP.

Zamawiający oczekuje spełnienia następujących minimalnych wymagań dotyczących plikowych raportów rozliczeniowych:

- Pliki raportów będą przygotowane w formacie „File CSV ISO-8859-2, delimiter ';'”
- Raport jest zakończony wierszem podsumowania zawierającym liczbę wierszy z danymi;
- Raporty będą umieszczane codziennie przed godziną 7:00 rano na dedykowanym serwerze raportów SFTP/WebDav systemu ŚKUP 1.5 w odpowiednich katalogach odbiorców raportów – uczestników rozliczeń. Każdy odbiorca raportów będzie otrzymywał raporty tylko z transakcjami których jest stroną. Raporty zbiorcze dla Zamawiającego będą umieszczane w dedykowanym do tego celu katalogu;
- Dla każdego uczestnika rozliczeń wymagane jest dostarczenie raportu **Strumień 1**, zawierającego wszystkie transakcje wykonane w ciągu minionej doby, których jest stroną rozliczeń. Raport będzie zawierał minimum następujące dane (ostateczna zawartość będzie uzależniona od MRP):

Nazwa pola	Opis (dane słownikowe do uzgodnienia)
Data Raportu	Data wygenerowania raportu
Data transakcji	Data transakcji (informacja kiedy zarejestrowano transakcję na terminalu) w formacie RRRR-MM-DD. Data zakupu dla transakcji nabycia.
Termin płatności środków	Termin, w jakim Dystrybutor/Dostawca usług (Akceptant dla zwrotów) ma wpłacić środki pod rozrachunek. Termin ten będzie wyznaczany wg zasady Data transakcji + 2 dni robocze. Format RRRR-MM-DD. <i>Nie jest prezentowany w sytuacji, gdy Dystrybutor jest jednocześnie Dostawcą sprzedanej usługi</i>
Kod Typu Punktu Sprzedaży	Kod punktu sprzedaży (powiązany z rodzajem terminala/urządzenia) np. SADiS, POPitd.
Kod Punktu Sprzedaży	Punkt (powiązany z miejscem/lokalizacją danego urządzenia/terminala) gdzie usługa, bilet została nabyta, np. SADiS1, POP2, POP3,
GIT	Globalny Identyfikator Transakcji identyfikujący unikalnie każdą zarejestrowaną Transakcję w Systemie ŚKUP 1.5
Rodzaj transakcji i płatności	Rodzaj transakcji (zakup usług, punktów, pobranie kaucji,, oraz wykorzystana forma płatności do zapłaty (gotówka, karta płatnicza,,) oddzielone uzgodnionym z Zamawiającym znakiem,
Kod Dystrybutora	Kod Dystrybutora
Kod Dostawcy Usługi	Kod Dostawcy Usługi

Nazwa pola	Opis (dane słownikowe do uzgodnienia)
Kod usługi	Kod identyfikujący określoną pozycję taryfową w Module Taryf i Cenników. Wyświetlany jest np. kod rodzaju biletu, który został zakupiony podczas transakcji.
Nazwa Katalogowa	Nazwa katalogowa pozycji taryfowej
Ilość	Ilość biletów, usług, punktów zakupionych podczas transakcji.
Cena jednostkowa brutto	Np. Cena za jeden bilet, usługę, punkt
Wartość brutto	Kwota transakcji liczona, jako ilość biletów, punktów zakupionych w danej transakcji pomnożona przez cenę jednostkową biletu, usługi, punktu wyrażona w walucie.
Waluta	Waluta (np. PLN)
Nr Konta	Login konta IKU dla którego była przeprowadzona transakcja Wypełniane zawsze, gdy pozycja dotyczy konta IKU. Uwaga! Login nie będzie prezentowany np. dla biletu kartonikowego opłaconego gotówką.
TID	Terminal ID – identyfikator terminala w ŚKUP 1.5, na którym dokonano zakupu.
Numer referencyjny płatności	Identyfikator płatności u dostawcy usług płatniczych (np. agenta rozliczeniowego) obsługującego metodę płatniczą np. kartą płatniczą lub przelewu internetowego Wypełniany, gdy transakcja procesowana jest metodą płatniczą obsługiwaną przez dostawcę usług płatniczych np. Agentu rozliczeniowego kart płatniczych lub przelewów internetowych.
Numer kontrolera	Informacje związane z nałożeniem mandatu na pasażera.
Rodzaj mandatu	
Numer mandatu	

- Dla każdego uczestnika rozliczeń wymagane jest dostarczenie raportu **Strumień 2** zawierającego transakcje rozliczone przez dostawców usług płatniczych (np. Agentu Rozliczeniowego) w ciągu ostatniej doby oraz wszystkie wcześniejsze transakcje nierozliczone (tzn. te, za które Dostawca Usług nie otrzymał jeszcze środków, z wyszczególnieniem terminu wymagalności zapłaty dla Dostawcy Usług dla każdej transakcji). Raport zawiera minimum następujące dane (ostateczna zawartość będzie uzależniona od MRP):

Nazwa pola	Opis
Data Raportu	Data raportu
Data transakcji	Data transakcji (informacja kiedy zarejestrowano transakcję na terminalu) w formacie RRRR-MM-DD. Data zakupu dla transakcji nabycia.

Nazwa pola	Opis
Termin płatności środków	Termin, w jakim Dystrybutor/Dostawca usług (Akceptant) (dla zwrotów) ma wpłacić środki pod rozrachunek. Termin ten będzie wyznaczany wg zasady Data transakcji + 2 dni robocze. Format RRRR-MM-DD. <i>Nie jest prezentowany w sytuacji, gdy Dystrybutor jest jednocześnie Dostawcą sprzedanej usługi</i>
Data wpłaty środków	Data, w jakiej AR ŚKUP 1.5 (w Module Rozliczeń Transakcji) odnotował wpływ środków od Dystrybutora pod rozrachunek transakcji <i>Wypełniane wówczas, gdy AR ŚKUP 1.5 odnotuje potwierdzenie wpłaty środków od Dystrybutora</i>
Data wymagalności środków	Wymagany dzień przekazania środków do Dostawcy usług (Akceptanta). Format RRRR-MM-DD
Data zapłaty	Data, pod jaką AR ŚKUP 1.5 wystawił polecenia przekazania środków na rachunki odbiorców Dostawców Usług (Akceptantów). <i>Wypełniane wówczas, gdy AR ŚKUP 1.5 (Moduł Rozliczeń Transakcji) wystawi polecenie przelewu środków na rzecz Dostawcy Usług lub Dystrybutora (przy zwrotach)</i>
Kod Typu Punktu Sprzedaży	Kod punktu sprzedaży (powiązany z rodzajem terminala/urządzenia) np. SADiS, POPitd.
Kod Punktu Sprzedaży	Punkt (powiązany z miejscem/lokalizacją danego urządzenia/terminala) gdzie usługa, bilet została nabyta, np. SADiS1, POP2, POP3,
GIT	Globalny Identyfikator Transakcji identyfikujący unikalnie każdą zarejestrowaną Transakcję w Systemie ŚKUP
Rodzaj transakcji i płatności	Rodzaj transakcji (zakup usług, pobranie kaucji, ..., oraz wykorzystana forma płatności do zapłaty (gotówka, karta płatnicza, rachunek punktowy,.....) oddzielone uzgodnionym z Zamawiającym znakiem,
Kod Dystrybutora	Kod Dystrybutora
Kod Dostawcy Usługi	Kod Dostawcy Usługi
Kod usługi	Kod identyfikujący określoną pozycję taryfową w Module Taryf i Cenników. Wyświetlany jest np. kod rodzaju biletu, który został zakupiony podczas transakcji.
Nazwa Katalogowa	Nazwa katalogowa pozycji taryfowej
Ilość	Ilość biletów, usług zakupionych podczas transakcji.
Cena jednostkowa brutto	Np. Cena za jeden bilet
Wartość brutto	Kwota transakcji liczona, jako ilość biletów zakupionych w danej transakcji pomnożona przez cenę jednostkową biletu wyrażona w walucie.

Nazwa pola	Opis
Kwota wpłacona	Kwota, jaka wpłynęła za daną pozycję do AR ŚKUP 1.5
Kwota należna	Kwota, jaka pozostała do uiszczenia dla danej pozycji
Waluta	Np. PLN
Nr Konta	Login konta IKU dla którego była przeprowadzona transakcja Wypełniane zawsze, gdy pozycja dotyczy konta IKU. Uwaga! Login nie będzie prezentowany np. dla biletu kartonikowego opłaconego gotówką.
TID	Terminal ID – identyfikator terminala ŚKUP 1.5, na którym dokonano zakupu.
Numer referencyjny płatności	Identyfikator płatności kartą płatniczą lub przelewu internetowego lub inną metodą płatniczą Wypełniany zawsze, gdy transakcja opłacona jest kartą płatniczą lub inną automatyczną/elektroniczną metodą płatniczą - poza gotówką
Status środków	Potwierdzony status płatności z punktu widzenia Dystrybutora (np. do zapłaty, do zapłaty spóźnione, zapłacone, zapłacone spóźnione, nie dotyczy, zrefundowane {przez Wykonawcę} itd.)
Numer kontrolera	Informacje związane z nałożeniem mandatu na pasażera.
Rodzaj mandatu	
Numer mandatu	

- Raporty Sprzedażowo-Rozrachunkowe dla Dystrybutora lub dla Dostawcy usług będący podsumowaniem **Strumienia 2**

Raport będzie zawierał zagregowane dane pochodzące ze Strumienia 2. Raport zaprezentuje wszystkie rozliczenia przetworzonych transakcji, a także wszystkie należności i zobowiązania (stan na dany dzień) z identyfikacją Dostawcy usług/Dystrybutora i daty rozliczeń dla każdego z otwartych należności/zobowiązań.

- Raporty Dostawców usług płatniczych (np. Agentów Rozliczeniowych) uczestniczących w systemie ŚKUP 1.5

Każdy z Dostawców usług płatniczych (np. Agent Rozliczeniowy) będzie generował w cyklach dobowych raporty, w których będą umieszczane zestawienia obciążeń, które zostały poprawnie rozliczone w ciągu danej doby rozliczeniowej i za które zostanie dokonany przelew na wskazane konto AR ŚKUP 1.5 w celu przekazania środków do Dostawcy usług.

- Raport błędów

Raport błędów będzie zawierał transakcje finansowe zarejestrowane w systemie, które nie zostały przyjęte do rozliczenia przez dostawców usług płatniczych (np. Agentów Rozliczeniowych) lub zostały

przez nich odrzucone. Raport poza parametrami transakcji pozwalającymi na jej jednoznaczne zidentyfikowanie będzie zawierał opis powodu odrzucenia lub nie przyjęcia transakcji.

3) Pozostałe raporty

W ramach realizacji zamówienia Wykonawca przygotowuje 20 raportów predefiniowanych służących do monitorowania poprawności funkcjonowania systemu i jego konfiguracji w których skład wejdą m.in:

- Historia użycia identyfikatora w zadanym okresie obejmująca wszystkie zdarzenia finansowe i niefinansowe również te zakończone niepowodzeniem, powodzeniem oraz oczekujące na realizację wraz z ich szczegółami w tym statusami i czasem ich uzyskania;
- Historia statusów identyfikatora oraz powiązania z kontami IKU wraz z określeniem czasu miejsca i operatora zdarzenia;
- Historia zdarzeń na koncie IKU w zadanym okresie obejmująca wszystkie zdarzenia finansowe i niefinansowe również te nie zakończone powodzeniem, zawierająca dokładną datę, czas, lokalizację wykonanych operacji, wykorzystany identyfikator;
- Historie statusów poszczególnych operacji finansowych wraz z dokładnym czasem i datą uzyskania statusu, lokalizacją i ewentualnie operatorem (przy ręcznej zmianie statusu);
- Rozwinięcie GIT na czas, lokalizację (np. rodzaj i lokalizacja punktu obsługi), składowe (np. numery biletów wchodzących w skład transakcji);
- Rozwinięcie TID z podaniem wszystkich szczegółów w tym numer seryjny urządzenia, typ, szczegóły lokalizacji oraz inne cechy powiązane w systemie w tym w systemach dostawców usług płatniczych;
- Transakcje nie rozliczone lub dla których nie nastąpił rozrachunek w zadanym okresie czasu wraz z ich szczegółami;
- Historia ulg zapisanych na poszczególnych kontach IKU wraz z dokładnym czasem, lokalizacją, operatorem, statusem wykonanej operacji;
- Oznaczenia i kody konfiguracji poszczególnych urządzeń/modułów lub całych grup urządzeń/modułów zastosowane w systemie informatycznym i u dostawców usług płatniczych w tym Agentu rozliczeniowego ŚKUP 1.5 (np. oznaczania poszczególnych SADiS w systemie ŚKUP 1.5 oraz w systemie Agentu rozliczeniowego kart płatniczych i u Agentu rozliczeniowego ŚKUP 1.5 – jeśli nie będą takie same);
- Innych wynikających z MRP lub konfiguracji systemu ŚKUP 1.5 oraz usług finansowo-rozliczeniowych, w ilości nie większej niż 20 raportów.

Przygotowane raporty zostaną udostępnione pracownikom Zamawiającego i ewentualnie innym uczestnikom rozliczeń posiadającym odpowiednie uprawnienia do ich uruchamiania. Raporty będą dostępne użytkownikom z poziomu przeglądarki webowej. Wszystkie generowane raporty mają mieć możliwość filtrowania po wybranych kryteriach, eksportowania do plików CSV, PDF oraz wydruku.

6 Podsystem Infrastruktury

Podsystem odpowiada za globalne, centralne zarządzanie i monitorowanie oprogramowania i urządzeń w szczególności infrastruktury wyniesionej.

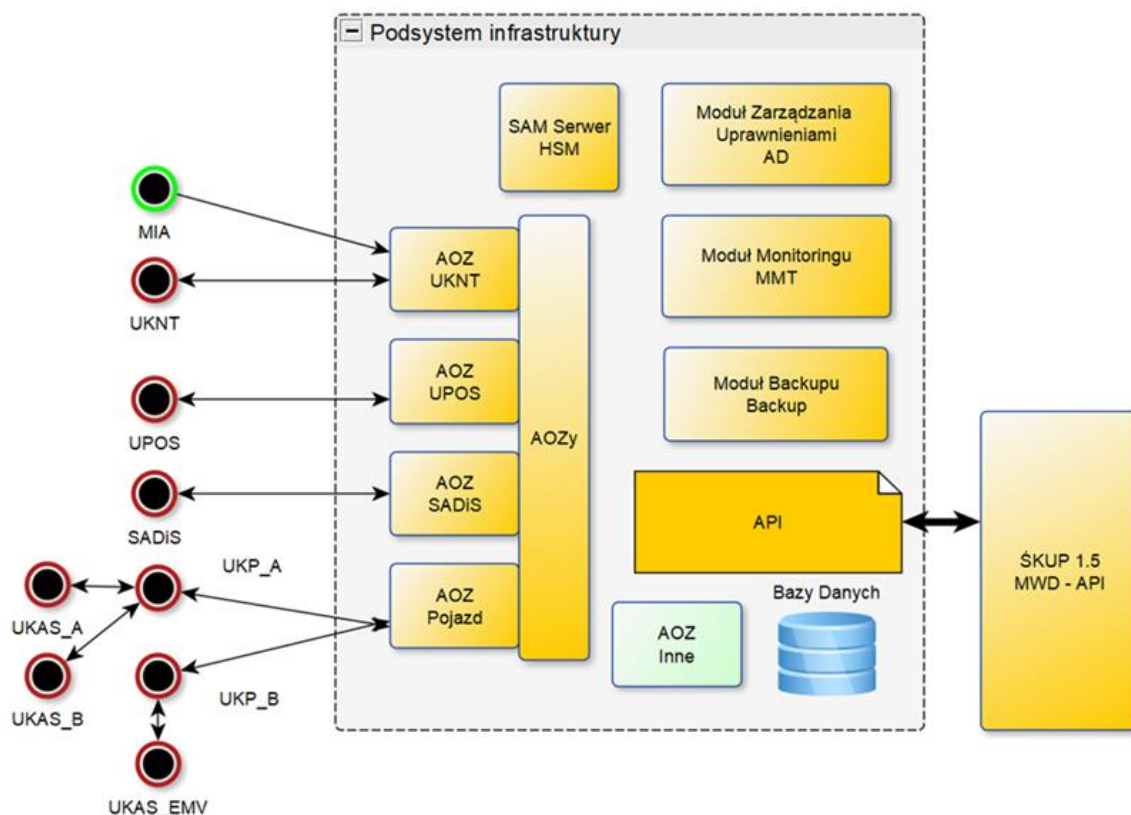
Podsystem odpowiada za komunikację między aplikacjami obsługi żądań (AOZ) dla poszczególnych urządzeń i resztą systemu. W ramach systemu będzie funkcjonowało zdefiniowane otwarte API pozwalające na integrację urządzeń w systemie i realizowanie zadań transakcyjnych oraz informacyjnych w ramach obsługi serwisowej urządzeń.

Moduł będzie pośredniczył w przesyłaniu danych pomiędzy różnymi elementami systemu ŚKUP 1.5. Komunikacja będzie się odbywała w ściśle zdefiniowany i opisany przez dostawcę modułu sposób (otwarte API). W ramach podsystemu konieczne będzie stworzenie GUI, które będzie służyło do definiowania wybranych parametrów systemu lub urządzeń, sterowania urządzeniami oraz do prowadzenia monitoringu w trybie on-line.

W ramach podsystemu utworzone zostanie centralne repozytorium konfiguracji wszystkich urządzeń i programów – CMDB. Zamawiający oczekuje funkcjonalności umożliwiającej przegląd archiwalnych konfiguracji (sposób implementacji do uzgodnienia).

W ramach podsystemu infrastruktury wstępnie zaproponowano podział na następujące moduły/aplikacje:

- Aplikacje obsługi żądań AOZ-pojazdy dla pojazdów;
- Aplikacje obsługi żądań AOZ-SADiS dla automatów sprzedażowych;
- Aplikacje obsługi żądań AOZ-UKNT dla kontrolerki;
- Aplikacje obsługi żądań AOZ-UPOS dla urządzeń u Agentów Sprzedaży;
- SAM serwer (HSM);
- Moduł zarządzania uprawnieniami AD;
- Moduł monitoringu MMT;
- Moduł Backupu.



Rysunek 13. Poglądowy schemat Podsystemu Infrastruktury.

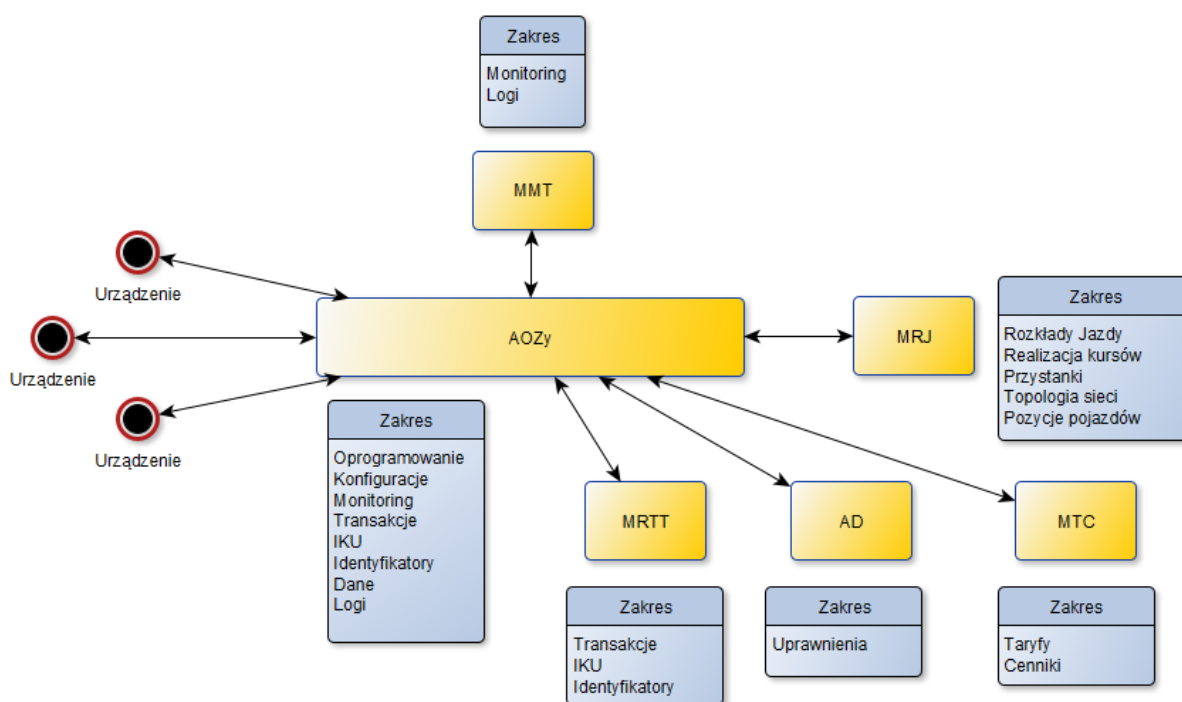
6.1 Procesy

a) Wymiana danych między urządzeniami a AOZ oraz systemem centralnym z wykorzystaniem API

Wymiana danych będzie odbywać się poprzez zdefiniowany interfejs API. API powinno być tak przygotowane, aby umożliwiała wymianę danych, z każdym rodzajem urządzeń wykorzystywanych w systemie ŚKUP 1.5, np. inne dane będą wymieniane z kontrolerką, a inne z urządzeniami w punktach sprzedaży. Należy również przewidzieć możliwość modyfikacji zestawu danych obsługiwanych przez API w momencie pojawienia się w systemie ŚKUP 1.5 nowych typów urządzeń. API musi uwzględniać także wymianę danych z systemem centralnym: dane taryfowe, dane rozkładów jazdy, dane kont i identyfikatorów, inne procesy realizowane przez urządzenia (transakcyjne, diagnostyczne), będą przesyłane bezpośrednio między modułami, a AOZ z wykorzystaniem API.

Urządzenia z którymi będzie występowała wymiana danych:

- Kontrolerki (UKNT);
- Urządzenia w POP (APO + komponenty);
- Urządzenia u Agentów Sprzedaży (UPOS);
- Stacjonarne Automaty Dystrybucji i Sprzedaży (SADiS);
- Urządzenia w pojazdach Komputer pokładowy (UKP), Kasownik (UKAS, UKAS-EMV).



Rysunek 14. Logiczny przepływ danych między modułami i urządzeniami

Rodzaje danych wymienianych z AOZ:

- Taryfa (w tym również konfiguracja usług);
- Informacje o transakcjach finansowych np. zakup usługi z dyspozycją zmniejszenia salda rachunku punktowego e-portmonetki w systemie ŚKUP 1.5 lub karty płatniczej, opłaty dodatkowe;
- Informacja o transakcjach niefinansowych w tym informacje o tapnięciach kartami płatniczymi (karty po tokenizacji) oraz skasowania/rejestracje biletów nabytych wcześniej;
- Weryfikacja prawa do skorzystania z usługi lub prawa do ulgi np. w kontrolerce;
- Informacja o przeprowadzonych kontrolach;
- Rozkłady jazdy;
- Sterowanie urządzeniami, w tym blokowanie, odblokowywanie, restarty, itp;
- Przekazywanie list dystrybucyjnych (np. aktywne kontrakty dla poszczególnych kont użytkowników, aktywne identyfikatory kont użytkowników, zastrzeżone identyfikatory, saldo punktowe e-portmonetki);
- Dane związane z bezpieczeństwem systemu;
- Dane eksploatacyjne z urządzeń;
- Konfiguracja urządzeń wraz z zarządzaniem wersjami oprogramowania i jego dystrybucją;
- Informacje o uprawnieniach użytkowników/operatorów systemu (np. kierowcy, kontrolerzy, sprzedawcy, serwisanci);
- Inne (zdefiniowane przez Wykonawcę) niezbędne do realizacji zadań przewidzianych urządzeniom.

b) Wymiana danych z systemem obsługującym tokenizowane karty płatnicze na potrzeby systemu rozliczeń transakcji wykonywanych kartami EMV

API będzie pośredniczyło w wymianie danych dotyczących operacji wykonywanych kartami EMV w systemie ŚKUP 1.5 używanych jako identyfikator pasażera (tapnięcia/użycia kart płatniczych). Dla potrzeb tych operacji numery kart zostaną zastąpione tokenami już na poziomie oprogramowania poszczególnych urządzeń. Urządzenia i AOZ będą przetwarzały tego typu informacje (tapnięcia/użycia kart płatniczych) wyłącznie w oparciu o tokeny, a nie numery kart. Moduł, do którego API przekaże dane będzie dokonywał przetwarzania transakcji, będzie je agregował i na tej podstawie będzie wyliczał obciążenie dla konkretnej karty (tokenu) i kierował transakcje do systemu Agenta Rozliczeniowego w celu wygenerowania ostatecznego obciążenia karty EMV.

c) Wymiana danych z systemami Agentów Rozliczeniowych kart płatniczych EMV

API będzie pośredniczyć w przesyłaniu danych o płatnościach/transakcjach dokonanych kartami płatniczymi (EMV), np. wniesienie opłaty za bilet lub opłaty dodatkowej. Operacje te są rozumiane jako wniesienie opłaty za transakcję. Karta jest tu użyta jako instrument płatniczy, a nie jako identyfikator pasażera. Operacje te podlegają zasadom, które obowiązują dla płatności kartami płatniczymi za zakupy towarów i usług. AOZ musi obsługiwać informacje, które pozwolą zidentyfikować transakcje np. na potrzeby reklamacji (musi być możliwość zidentyfikowania dla konkretnej transakcji takich danych jak dokładny czas i miejsce płatności oraz numer referencyjny nadawany przez Agenta Rozliczeniowego kart płatniczych).

d) Interfejs GUI dla Administratorów/operatorów do wprowadzania danych i monitorowania systemu

Interfejs GUI powinien w czytelny sposób prezentować stan urządzeń i procesów, które obsługuje. Wprowadzanie danych powinno odbywać się w sposób intuicyjny i ergonomiczny. W przypadkach konieczności powiązania wprowadzonych danych z danymi już istniejącymi (np. słownikowymi) powinny być wykorzystywane listy rozwijalne lub przyciski wyboru. Podczas wykorzystywania funkcji monitorowania informacja powinna być prezentowana wielopoziomowo, czyli na najwyższym poziomie powinna być prezentowana informacja najbardziej ogólna (np. dotycząca grupy urządzeń) wraz z ostrzeżeniami i alertami dla poszczególnych pozycji, a po wybraniu konkretnej pozycji powinna być zaprezentowana informacja szczegółowa dotycząca wyświetlanego ostrzeżenia lub alarmu (już dla poszczególnego urządzenia lub procesu).

Obsługiwane funkcjonalności:

- Definiowanie grup urządzeń w systemie;
- Zarządzanie taryfami/cennikami pobranymi z modułu MTC, do grup urządzeń i urządzeń;
- Zarządzanie ulgami i ich parametrami pobranymi z MTC;
- Zarządzanie kartami SAM, w tym przypisanie karty do konkretnego urządzenia, komunikacja z serwerem SAM (moduł HSM);
- Definiowanie Podmiotów (Operatorów/Przewoźników, Dostawców Usług)/Pojazdów, użytkowników;
- Definiowanie globalnych parametrów pracy urządzeń w tym przypisania urządzeń do odpowiednich Podmiotów;
- Blokowanie i odblokowywanie urządzeń;
- Monitorowanie pracy urządzeń w trybie online;
- Raportowanie stanów urządzeń;
- Konfigurowanie i parametryzowanie urządzeń;
- Zarządzanie uprawnieniami do AOZ.

e) Zarządzanie bazą kodów QR/NFC

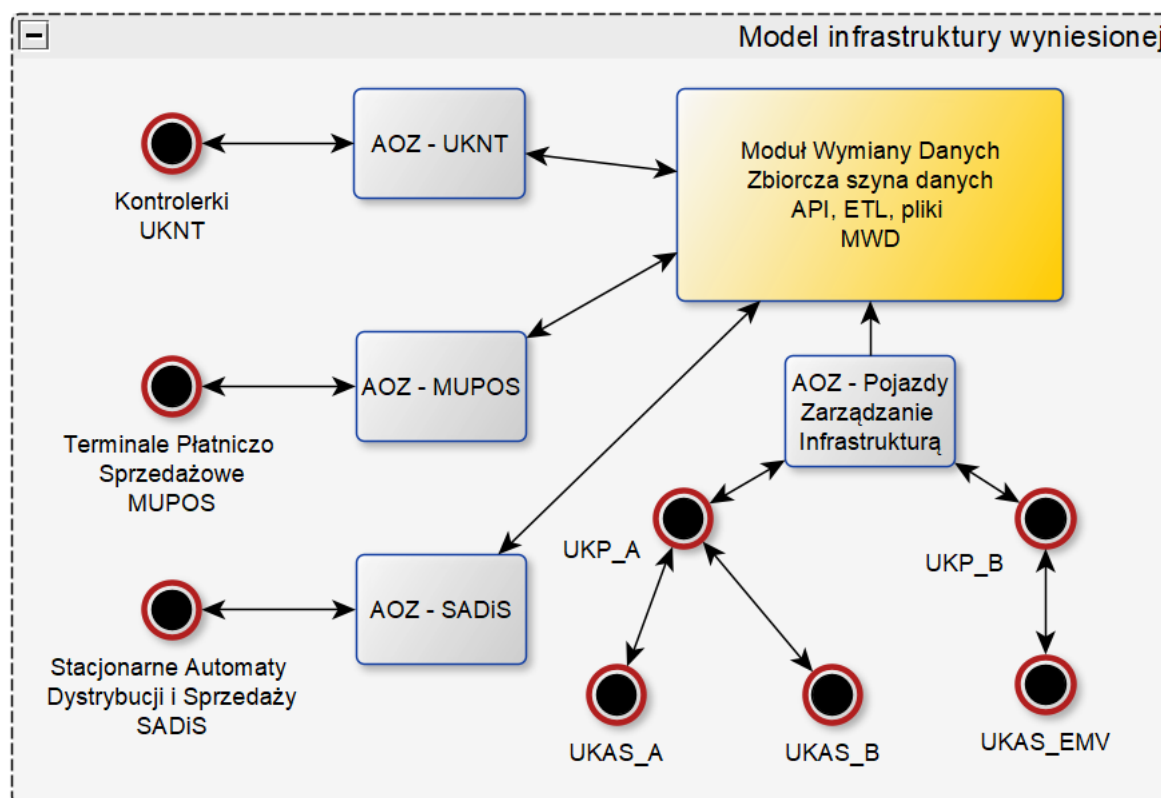
- Drukowanie do pliku wygenerowanych kodów QR (wg zdefiniowanego parametrem rozmiaru obrazka, format strony (A4, A3), liczby wierszy i kolumn na stronie);
- Zarządzanie oraz przypisywanie kodu QR oraz Tag NFC do konkretnego pojazdu lub lokalizacji (słupek przystankowy); pojazdy oraz przystanki zgodne z modułem MRJ;
- Przyjazny interfejs edycji i zarządzania kodami.
- Dostarczenie i rozmieszczenie naklejek z kodami w pojazdach jest elementem niniejszego zamówienia.

Uwaga

Nie chodzi o kody QR prezentujące zakupiony bilet, tylko o identyfikację pojazdów i przystanków, na potrzeby Aplikacji Mobilnych.

6.2 Aplikacje Obsługi Żądań (AOZ)

Stanowią oprogramowanie umożliwiające konfigurowanie, monitorowanie i zarządzanie poszczególnymi urządzeniami infrastruktury wyniesionej. Potrafią realizować wszystkie funkcje w trybie autonomicznym. Ujednolicona szata graficzna i UX dla wszystkich rodzajów urządzeń. Otwarte interfejsy wymiany danych między: systemem centralnym <--> AOZ <--> Urządzenia, pozwalające na dodawanie nowych urządzeń tego samego rodzaju, po pozytywnej procedurze certyfikacji i integracji. Hierarchiczne zarządzanie uprawnieniami, pozwalające na grupowanie urządzeń i ich przypisywanie do operatorów/podmiotów. Operatorzy danego podmiotu będą mogli zarządzać tylko przypisaną im infrastrukturą.



Rysunek 15. Schemat zarządzanie urządzeniami

AOZy będą pośredniczyły w wymianie danych On-line pomiędzy urządzeniami, a system centralnym. Wymieniane dane muszą umożliwiać konfigurowanie i monitorowanie pojedynczych urządzeń jak i całych grup urządzeń On-line. AOZy będą pozwalały na szczegółowy monitoring przypisanych urządzeń w trybie On-line. Muszą również umożliwiać pełną ręczną konfigurację urządzenia. Wszystkie parametry konfiguracyjne muszą być możliwe do wprowadzenia poprzez GUI użytkownika w taki sposób, że jeśli dotyczą grupy urządzeń to wystarczy wprowadzenie ich jeden raz i rozdystrybuowaniem ich do całej grupy. Rodzaje danych zostały opisane powyżej.

W AOZ ma być funkcjonalność zarządzania wersjami oprogramowania we wszystkich podłączonych urządzeniach: podgląd obecnie zainstalowanej na urządzeniu wersji, podgląd daty i numeru/nazwy ostatnio wysłanej wersji oprogramowania, możliwość wysłania z poziomu administratora najnowszej wersji oprogramowania, po czym urządzenie rozpocznie jej automatyczne pobranie i zainstalowanie.

6.2.1 Aplikacja Obsługi Żądań dla pojazdów (AOZ-pojazd)

Aplikacja musi umożliwiać zarządzanie wybraną grupą urządzeń instalowanych w pojazdach, pełną parametryzację i konfigurację urządzeń, funkcje monitorujące, diagnostyczne, aktualizacje, podgląd danych z urządzeń w czasie zbliżonym do rzeczywistego, sterowanie urządzeniami z poziomu użytkownika systemu ŚKUP 1.5. Każdy raport udostępniony w ramach AOZ ma mieć możliwość filtrowania po wszystkich kolumnach oraz wyeksportowania do plików XLSX, CSV, PDF. Raporty mają mieć możliwość ustawienia parametrów wstępnych ograniczających zakres danych np. do danego okresu (danego roku, miesiąca, dnia itp.), przewoźnika, pojazdu itp.

Wymagana funkcjonalność dla obszaru AOZ-pojazd została zaimplementowana w systemie ŚKUP „System dla MZK” i jest szczegółowo opisana w Dokumentacji użytkownika AOZ (System dla MZK). Zamawiający posiada licencję z prawem do modyfikacji dla przedmiotowego oprogramowania i oczekuje w ramach niniejszego zamówienia dostarczenia rozwiązania tożsamego w zakresie funkcjonalnym opisanym w ww. dokumentacji. Szczegółowy zakres poniżej opisanych funkcjonalności/raportów zostanie uzgodniony między stronami w ramach realizacji umowy.

Poniżej przedstawiono wymagane funkcjonalności AOZ:

1. Funkcjonalność Monitorowania

Monitorowanie powinno obejmować:

a) Monitorowanie stanu infrastruktury (jako całości pojazdu) oraz szczegółową informację dotyczącą elementów infrastruktury pojazdowej, w tym UKP, UKAS, UKAS-EMV oraz innych wykorzystywanych modułów zainstalowanych w pojeździe. Monitorowanie powinno być prezentowaniem aktualnego stanu systemu bazującego na ostatnim zestawie danych przekazanych z monitorowanych modułów.

Monitorowanie pojazdów powinno obejmować dane dynamiczne i statyczne, a ich odświeżanie będzie się odbywać w trybie zbliżonym do rzeczywistego, czyli on-line. Szczegółowy zakres danych, których zakres monitorowania powinien obejmować zawiera dokumentacja użytkownika AOZ_System Tychy, o której mowa powyżej.

2. Funkcjonalność Raportowania

a) **Raport operacji w pojazdach** powinien prezentować wszystkie operacje w zadanym przedziale czasu związane z:

- Użyciem karty ŚKUP lub ŚKUP 1.5 jako identyfikatora;
- Użyciem karty płatniczej lub jej surogatu (jako identyfikatora oraz środka płatniczego);
- Aktywacją biletów papierowych w kasownikach, na których będzie nadrukowany kod QR – system ma być gotowy na uruchomienie takiej funkcjonalności w przyszłości;

- Operacjami powodującymi zmianę salda na rachunku punktowym e-portmonetki.

Zakres danych raportu powinien być tożsamy z zakresem opisanym w dokumentacji użytkownika AOZ_System Tychy.

b) Raport Konfiguracji powinien prezentować aktualną konfigurację oraz wersję historyczne wykonanych konfiguracji, wraz z informacją o wersji oprogramowania na danym urządzeniu (UKP, UKAS, UKAS-EMV). Zakres danych raportu powinien być tożsamy z zakresem opisanym w dokumentacji użytkownika AOZ_System Tychy.

c) Raport poprawności powinien prezentować informację o stanie urządzeń, tj. awarię lub nieprawidłową pracę urządzenia (brak łączności, niesprawność urządzenia, brak dostępu funkcji, itp.).

3. Funkcjonalność Zarządzania powinna obejmować:

- Przypisywanie komponentów sprzętowych wchodzących w skład danego pojazdu do identyfikatora pojazdu (realizowane jako numer przewoźnika i numer boczny pojazdu);
- Zarządzanie ustawieniami mającymi wpływ na działanie poszczególnych aplikacji klienckich;
- Wywoływanie akcji wykonywanych na aplikacjach modułów klienckich;
- Zdalną aktualizację oprogramowania.

a) Zarządzanie konfiguracją pojazdu.

Obiektem w konfiguracji infrastruktury pojazdowej powinny być pojazdy. Do pojazdu przypisywane będą komputer pokładowy oraz kasowniki poprzez wybór numeru seryjnego urządzenia dotychczas nieprzypisanego do żadnego pojazdu. Każdy pojazd powinien posiadać parametr konfiguracyjny definiujący ilość kasowników jakie zostały zamontowane w pojeździe. Ilość kasowników będzie odpowiadała ilości zamontowanych podstawek umożliwiających zamontowanie kasowników. Nie powinna być dopuszczalna sytuacja, kiedy urządzenie będzie przypisane do więcej niż jednego pojazdu. Przypięcie kasownika do pojazdu w sytuacji, kiedy był on wcześniej przypisany do innego pojazdu będzie musiało być poprzedzone jego odpięciem od pierwszego pojazdu. Operacja konfiguracji przez operatora/administradora musi być intuicyjna i maksymalnie zautomatyzowana.

b) Zarządzanie ustawieniami.

Każdy moduł typu UKAS, UKAS-EMV, UKP powinien posiadać zestaw ustawień, które będą miały wpływ na jego działanie. W systemie będzie możliwość zdefiniowania dowolnej grupy ustawień w skład której będą mogły wejść ustawienia powiązane z danym typem urządzeń. Zarządzanie ustawieniami będzie odbywało się poprzez przypisanie grupy ustawień do urządzenia oraz poprzez zmianę ustawień indywidualnych dla danego urządzenia.

c) Zarządzanie akcjami.

W odróżnieniu od ustawień, które będą miały wpływ na pracę urządzeń po wykonaniu kolejnego uruchomienia, w systemie powinien zostać zaimplementowany mechanizm „akcji” rozumianych jako np. wysłanie nowej wersji oprogramowania, blokada i odblokowanie kasowników, czy też wykonanie restartu (ponownego uruchomienia) urządzenia zawieszono. Wszystkie „akcje” wykonane w systemie będą wykonywane natychmiast po przesłaniu żądania na urządzenie.

Aktualizacje oprogramowania urządzeń mobilnych (UKP, UKAS, UKAS-EMV).

Z poziomu aplikacji AOZ będzie istniała możliwość dodania paczki z nową wersją oprogramowania danego modułu infrastruktury wyniesionej oraz wykonanie zlecenia aktualizacji oprogramowania. Operacja powinna odbywać się poprzez wybór typu urządzeń, dla których dane oprogramowanie będzie dedykowane, a następnie wyboru wersji oprogramowania, która ma zostać zainstalowana. Z tego poziomu będzie możliwość dodania pliku z paczką oprogramowania z możliwością wpisania komentarza opisującego wydanie. Wersja oprogramowania poprawnie dodana do AOZ będzie mogła zostać zainstalowana na urządzeniach, do którego jest dedykowana. Zlecenie instalacji nowej wersji oprogramowania będzie mogło zostać wykonane zarówno w odniesieniu do pojedynczego urządzenia jak również dla określonej grupy urządzeń (np. danego Operatora) lub wszystkich urządzeń danego typu lub spełniających kryterium filtrowania. Standardowo - zlecona instalacja - będzie wykonywana podczas kolejnego uruchamiania urządzenia. AOZ będzie pozwalał na zaplanowanie instalacji w przyszłości poprzez wskazanie daty instalacji oprogramowania. Dodatkowo będzie możliwość zlecenia instalacji natychmiastowej poprzez wymuszenie restartu danego urządzenia.

d) Zarządzanie użytkownikami Systemu.

Dostęp do systemu będą mieli użytkownicy z odpowiednim poziomem uprawnień. Dostęp do systemu będzie poprzedzany autoryzacją. Grupy użytkowników definiowanych na potrzeby infrastruktury pojazdowej to: kierowcy, kontrolerzy, użytkownicy AOZ (z różnymi profilami użytkowników, np. obszar dla Operatorów – dla każdego w ramach swojej floty, konfiguracja urządzeń, dane transakcyjne, w tym profil dla użytkownika mającego dostęp do wszystkich pojazdów, itp.), serwisanci urządzeń.

e) Obsługa serwisowa – Zarządzanie konfiguracją urządzeń.

Moduł AOZ służy do zarządzania konfiguracją urządzeń zamontowanych w pojazdach, a w szczególności do przypisywania urządzeń do identyfikatora pojazdu. Z tego powodu w module AOZ będzie można zainicjować podmiannę wymienianych urządzeń w sposób uproszczony tak, by nie trzeba było wprowadzać wszystkich parametrów konfiguracyjnych od początku. Dzięki temu bezpośrednio po wymianie uszkodzonego urządzenia serwisant będzie miał możliwość wykonania zmiany konfiguracji w sposób uproszczony, wprowadzając jedynie zmienione dane (np. nr seryjny).

Operacja wymiany urządzenia będzie obejmowała następujące kroki konfiguracyjne:

1. Przypisanie UKP do pojazdu – w przypadku wymiany;
2. Przypisanie UKAS, UKAS-EMV do UKP (lub tryb autonomiczny) oraz do nr słupka, przy czym konieczne będzie wskazanie kolejnego nr urządzenia (pozycji kasownika od UKP);
3. Po wykonaniu konfiguracji pojazdu w AOZ, wysłane jest żądanie aktualizacji danych, tj. usługi aktualizującej powiązanie przewoźnika z komputerem pokładowym i kasownika z komputerem pokładowym, które zatwierdza operator AOZ.

6.2.2 Aplikacje Obsługi Żądań dla automatów (AOZ-SADiS)

Aplikacja Obsługi Żądań (AOZ-SADiS) stanowi dedykowaną, autonomiczną aplikację do zarządzania, konfigurowania i pełnej parametryzacji urządzeń, monitorowania, diagnostyki, aktualizacji, podglądu danych w czasie rzeczywistym, rejestrowania i sterowania pracą automatów SADiS oraz zarządzania

jego użytkownikami. Aplikacja AOZ ma być dostępna jako aplikacja webowa oraz w wersji na androida. Jedną z zakładek aplikacji ma być mapa z zaznaczonymi lokalizacjami i sygnalizacją o aktualnym stanie urządzeń (np. zielony – ok; żółty – sprawdź, problem; czerwony – awaria/włamanie). Po kliknięciu w ikonę urządzenia ma być wyświetlana pełna informacja o danym urządzeniu. Szczegółowy zakres informacji zostanie uzgodniony z Zamawiającym po podpisaniu umowy. Po zalogowaniu się do aplikacji użytkownik ma mieć dostęp do zawartości zdefiniowanej dla jego profilu/grupy.

Ekran z listą urządzeń ma się odświeżać automatycznie, np. co 60 sekund aktualizując w ten sposób wszystkie dane zawarte w zestawieniu. Powinna być również dostępna funkcja wyłączenia odświeżania automatycznego, wówczas odświeżanie zawartości danych będzie następowało manualnie przez operatora.

Aplikacja Obsługi Żądań (AOZ), przewidziana jest do:

1. Definiowania urządzeń, w co najmniej następującym zakresie:
 - Nazwa;
 - Adres lokalizacji;
 - Położenie na mapie (GUI z dostępem do mapy);
 - Seria i numer urządzenia;
 - Producent i model urządzenia;
 - Grupa urządzeń (wg zdefiniowanych funkcjonalności).
2. Definiowania aktywności funkcjonalności aplikacji oraz parametrów pracy urządzenia, w co najmniej następującym zakresie:
 - Ustawienia trybu sprzedaży (włącz/wyłącz);
 - Ustawienia obsługi kart płatniczych i ich surogatów (włącz/wyłącz);
 - Ustawienia obsługi kart ŚKUP, ŚKUP 1.5 (włącz/wyłącz);
 - Ustawienia płatności gotówką (włącz/wyłącz);
 - Definiowania timeout-u (dla wygaszacza ekranu, pop-upów, od wykonania ostatniej operacji);
 - Ustawienia częstotliwości pobierania list dystrybucyjnych, konfiguracji;
 - Ustawienia maksymalnej ilości biletów w ramach jednej transakcji;
 - Ustawienia maksymalnej kwoty wartości transakcji;
 - Zarządzania czujnikiem zbliżania się końca papieru;
 - Zarządzania pracą drukarek (tryb pracy np. naprzemiennie);
 - Zarządzania przyjmowaniem poszczególnych monet (włącz/wyłącz);
 - Zarządzania przyjmowaniem poszczególnych banknotów (włącz/wyłącz);
 - Zarządzania nominałami do wydawania reszty (włącz/wyłącz) wraz z określaniem progu o małej ilości monet w zasobnikach;
 - Zarządzania nominałami w hopperach (włącz/wyłącz) wraz z określaniem progu o małej ilości monet w hopperach;
 - Definiowania zasad wydawania reszty w zależności od przyjętych wartości (tj. progów przy jakich ma być przyjmowany dany nominał);
 - Definiowania wzoru biletów papierowych;

- Definiowania/modyfikowania kontraktów zaimportowanych z MTC – usług, które będą dostępne w automatach biletowych (opcjonalnie z eMagazynu w ramach godzin rozwojowych);
- Definiowania, do których transakcji ma istnieć możliwość drukowania potwierdzenia (np. poprzez parametr dotyczący kwoty transakcji definiowany w AOZ);
- Definiowania treści (tekstu, grafiki) wygaszacza ekranu.

Powyższe ustawienia mają być możliwe jako ustawienia globalne w wariantach: dla wszystkich urządzeń, dla grupy urządzeń oraz jako ustawienia indywidualne dla wybranego urządzenia.

3. Monitorowania pracy urządzeń – stanu poszczególnych podzespołów, oprogramowania danego urządzenia, w co najmniej następującym zakresie:

- Nazwy urządzenia wraz z jego numerem;
- Trybu pracy automatu – sprzedaż, informacyjny;
- Stanu łączności – online, offline – czas ostatniego kontaktu z serwerem;
- Stanu drukarek – ok, awaria, problem (np. zbliża się koniec papieru);
- Stanu modułu gotówkowego, w tym informacji o poziomie napełnienia kaset końcowych, aktywności kanałów – banknot, bilon;
- Działania dyspensera Kart ŚKUP (ok., awaria, problem);
- Daty konfiguracji – dane o pobraniu konfiguracji na urządzenie (rok, miesiąc, dzień, godzina, minuta, sekunda);
- Wersji oprogramowania – wskazanie numeru wersji wraz z oznaczeniem kolorystycznym czy jest aktualna, czy nieaktualna;
- Daty wgrania wersji oprogramowania;
- Wersji oprogramowania oczekującej na aktualizację;
- Wysłanie wersji oprogramowania z poziomu administratora i automatyczne pobranie oraz zainstalowanie jej w urządzeniu;
- Zaniku zasilania;
- Stanu alarmu – uzbrojony, wyłączony, włączony (np. nieautoryzowane otwarcie drzwi);
- Otwarcia drzwi przy zaniku zasilania;
- Stanu wszystkich czujników zainstalowanych w urządzeniu;
- Informacji o wykonanych restartach;
- Informacji o wymianach/aktywacjach kaset (banknot, bilon);
- Informacji o wymianach/aktywacjach hopperów;
- Informacji o uzupełnieniu/opróżnieniu zasobników;
- Logowania informacji o wrzucanych i wydawanych monet w ramach transakcji;
- Informacji dotyczącej wejścia/wyjścia do panelu administratora;
- Przypisania paczek z kartami ŚKUP;
- Informacje o danych transakcyjnych i sprzedażowych (raport online z uwzględnieniem urządzenia, rodzaju transakcji, rodzaju i nominału biletu, typu identyfikatora użytkownika).

4. Wglądu w zdarzenia (logi) oraz komunikaty wymagające obsługi serwisowej w automatach, w co najmniej następującym zakresie:

- Nazwy automatu;
- Daty logowania do panelu administratora na urządzeniu;

- Nazwy operatora;
- Nazwy wykonanej czynności np.:
 - poprawne/niepoprawne zalogowanie się;
 - obsługa paczek kart (dodanie/usunięcia paczki kart do dyspensera);
 - wymiana kaset na bilon, banknoty;
 - uzupełnienie/opróźnienie zasobników do wydawania reszty;
 - wymiana papieru;
 - obsługa drukarek;
 - aktualizacja oprogramowania z USB;
 - wyjście z panelu administratora;
 - test podzespołów;
 - restart aplikacji, komputera, zasilania.

Zamawiający musi mieć możliwość zdalnego (z poziomu komputera pracownika) połączenia się do automatu i pobrania logów szczegółowych (zapisów oprogramowania) dotyczących pracy automatu.

5. Wykonywania zdalnych operacji na automatach w tym obsługi wersji oprogramowania instalowanych na automatach z możliwością ustawiania akcji (natychmiast, w przyszłości z określeniem daty i czasu), w co najmniej następującym zakresie:
 - Prezentacji aktualnej wersji oprogramowania;
 - Wymuszenia aktualizacji oprogramowania;
 - Aktualizacji ustawień;
 - Restartu aplikacji/komputera;
 - Alarmu (włącz/wyłącz);
 - Restartu zasilania;
 - Wyłączenia komputera.
6. Dodawania, edycji i zarządzania operatorami uprawnionymi do obsługi automatów, w tym co najmniej w następującym zakresie:
 - Definiowania nazwy operatora wraz z przypisaniem indywidualnego ID;
 - Definiowania ważności uprawnienia;
 - Definiowania zakresu uprawnień, np. obsługa monetarna, obsługa drukarek, obsługa kart, itp.;
 - Przypisywania adresu e-mail;
 - Definiowania hasła do logowania się w automacie;
 - Przypisywania operatorowi dostępu do wskazanych urządzeń.
7. Dodawania i edycji użytkownikom odpowiednich uprawnień – profili, pozwalających na dostęp do poszczególnych funkcjonalności w aplikacji AOZ, w tym co najmniej w następującym zakresie:
 - Administrator – pełne uprawnienia;
 - Organizator – nadawanie uprawnień (wraz z ich edycją) operatorom i użytkownikom, w tym nadawanie haseł dostępu, konfiguracja urządzeń (aktualizacje ustawień, wyłączenia i restarty urządzeń, ustawienia globalne oraz lokalne urządzeń, wzory biletów, definiowanie taryfy/usług), aktualizacja urządzeń (dodawanie nowych wersji

- oprogramowania, zdalne podgrywanie wersji na automaty, podgrywanie wersji na urządzenia USB);
- Finanse – dostęp do danych finansowych, w tym wgląd do wszystkich transakcji przeprowadzonych na automatach (kwota, kanał płatności, wpłacane i wydawane nominały, nr karty ŚKUP, numer karty płatniczej, ilość zakupionych kontraktów), stanu gotówki w automatach w poszczególnych podzespołach (kasety końcowe, zasobniki do wydawania reszty, hoppery);
 - Eksploatacja – dostęp do wszystkich zdarzeń, stanu podzespołów automatów, łącznie z danymi finansowymi;
8. Prezentowania kodów błędów, wyjątków występujących w automatach wraz z ich opisami.
9. Aplikacja ma umożliwiać generowanie co najmniej następujących raportów;
- a. Raport z inwentaryzacji – stan gotówki (wymagane pola):
- Urządzenie – lokalizacja;
 - Data i czas;
 - Stan monet w zasobnikach do wydawania reszty;
 - Wartość w zasobnikach;
 - Stan monet w hopperach;
 - Wartość w hopperach;
 - Stan monet w kasecie;
 - Wartość w kasecie;
 - Stan banknotów w kasecie;
 - Wartość w kasecie;
 - Procentowe zapełnienie zasobnika, hoppera, kasety.

Raport z inwentaryzacji ma być prezentowany w konkretnych momentach/zdarzeniach tj. przy wymianie kasety na monety/banknoty, uzupełnieniu zasobników/hopperów do wydawania reszty, przy opróżnieniu zasobników/hopperów do wydawania reszty, zalogowaniu się do serwisu, wylogowaniu się z serwisu, zaniku zasilania, powrotu zasilania, restarcie.

- b. Raport sprzedaży z informacją o statusie każdej transakcji (poprawna, niepoprawna) (wymagane pola):
- Data i czas;
 - Kwota;
 - Typ płatności – gotówka, karta ŚKUP - punkty, karta EMV – styk, bezstyk oraz jej surogaty, Blik, itp.;
 - Rodzaj, nazwa, ilość biletów/usług;
 - Wartość transakcji;
 - Unikatowy identyfikator transakcji (GIT);
 - Typ kontraktu/usługi – nazwa bilet papierowy, bilet elektroniczny, wydanie karty;
 - Czy wydano potwierdzenie;
 - Numer karty ŚKUP/karty EMV oraz identyfikator innych metod płatności dostępnych w automatach;
 - Status płatności – udana, nieudana – błąd reszty, błąd wydawania karty, anulowana;
 - TID;

- MID.

z możliwością filtracji dla:

- Gotówka;
- Karta płatnicza;
- Karta ŚKUP;
- Po rodzajach biletów;
- Data, czas;
- Ilość;
- Wartość.

Z możliwością filtracji dla dowolnego przedziału czasu, urządzenia, z exportem do plików CSV, XLS, XLSX, PDF oraz drukuj.

- c. Raport ze szczegółami transakcji (wymagane pola):
 - Liczba wrzuconych monet, wydanych monet, suma;
 - Liczba wrzuconych banknotów, wydanych monet, suma;
 - Dla transakcji kartą płatniczą – ilość, kwota, wartość, data, godzina, TID, MID, nr karty (niepełny), kod autoryzacji;
- d. Raport z wymiany kaset:
 - Urządzenie – nazwa, lokalizacja;
 - Data, godzina operacji;
 - Data, godzina poprzedniej operacji;
 - Numer kasy;
 - Nazwa operatora;
 - Numer kolejnej wymiany;
 - Ilość monet/banknotów w kasie;
 - Suma ilości poszczególnych nominałów;
 - Wartość poszczególnych nominałów;
 - Łączna wartość – utarg.
- e. Raport z opróżnienia/uzupełnienia zasobników (wymagane pola):
 - Urządzenie – nazwa, lokalizacja;
 - Data, godzina operacji;
 - Nazwa operatora;
 - Stan początkowy;
 - Stan końcowy;
 - Ilość wrzuconych/opróżnionych monet;
 - Suma ilości poszczególnych nominałów;
 - Wartość poszczególnych nominałów.
- f. Raport z opróżnienia/uzupełnienia hopperów (wymagane pola):
 - Urządzenie – nazwa, lokalizacja;
 - Data, godzina operacji;
 - Nazwa operatora;

- Stan początkowy;
 - Stan końcowy;
 - Ilość wrzuconych/opróżnionych monet;
 - Suma ilości poszczególnych nominałów;
 - Wartość poszczególnych nominałów.
- g. Raport z uzupełnienia/opróżnienia paczek z kartami ŚKUP 1.5 (wymagane pola):
- Urządzenie – nazwa, lokalizacja;
 - Data, godzina operacji;
 - Nazwa operatora;
 - Numer paczki;
 - Liczba kart w paczce;
 - Wykaz kart w paczce.
- h. Raport z wydania kart (wymagane pola):
- Urządzenie – nazwa, lokalizacja;
 - Data, godzina operacji;
 - Nazwa operatora;
 - Gotowych do wydania;
 - Wydanych;
 - Odrzuconych/błędnych;
 - Przeterminowanych;
 - Nieznalezionych.

6.2.3 Aplikacje Obsługi Żądań dla kontrolerki (AOZ-UKNT)

Aplikacja powinna umożliwiać zarządzanie wybraną grupą urządzeń typu kontrolerka (UKNT) w co najmniej następującym zakresie:

1. Pełnej parametryzacji i konfiguracji urządzeń;
2. Zarządzania wersjami oprogramowania, w tym: podglądu obecnie zainstalowanej na urządzeniu wersji, podglądu daty i numeru/nazwy ostatnio wysłanej wersji oprogramowania, możliwości wysłania zdalnego z poziomu administratora najnowszej wersji oprogramowania i automatycznego jej pobrania oraz zainstalowania w urządzeniu bez możliwości ingerencji kontrolera w ustawienia urządzenia;
3. Funkcji monitorującej aktywność urządzenia: zalogowanie – przez kogo lub niezalogowanie;
4. Funkcji diagnostycznych dot. komunikacji urządzenia z systemem centralnym;
5. Sygnalizowania administratorowi nieudanych prób synchronizacji urządzenia z systemem centralnym;
6. Możliwości zdalnego zablokowania urządzenia na wypadek kradzieży bądź zgubienia;
7. Zdefiniowania powodów nieważności biletu;
8. Zdefiniowania powodów wystawienia opłaty dodatkowej;
9. Zdefiniowania komunikatów wyświetlanych przez kontrolerkę;
10. Zarządzania numeracją opłat dodatkowych;
11. Zarządzania dostępem do urządzeń, dane kontrolera (nr kontrolera, rodzaj: zawodowy/społeczny/konduktor KŚ), definiowania loginów, haseł;

12. Możliwości filtrowania w AOZ wyników kontroli (bez danych osobowych) prowadzonych przez kontrolerów, w tym z uwzględnieniem kontroli biletowych i pojazdowych;
13. Zarządzania synchronizacją danych do/z systemów zewnętrznych Zamawiającego;
14. Śledzenia pozycji GPS urządzenia i ich prezentacji na mapie (dane udostępniane także przez API).

Zarządzanie uprawnieniami dla użytkowników modułu UKNT, w co najmniej następującym zakresie:

1. Administrator/kierownik: główny odbiorca raportów, użytkownik mający możliwość parametryzowania urządzeń i komunikatów, przypisywania urządzeń do kontrolerów, administrowania kontami kontrolerów, wysyłania nowych wersji na urządzenia, wysyłania do kontrolerów wiadomości, zdalnego zablokowania urządzenia, możliwość podglądu danych diagnostycznych, monitorujących;
2. Kontroler zawodowy (zatrudniony w oparciu o umowę o pracę): wystawianie opłat dodatkowych, raportowanie czasu pracy, raportowanie wystawionych opłat, raportowanie skontrolowanych identyfikatorów, raportowanie do modułu zewnętrznego Busman CB nieprawidłowości (dot. pracy przewozowej, zastrzeżenia dot. pracy kierowców, opóźnienia itp.);
3. Kontroler społeczny (zatrudniony w oparciu o umowę zlecenie): wystawianie opłat dodatkowych, raportowanie czasu pracy, raportowanie wystawionych opłat, raportowanie skontrolowanych identyfikatorów;
4. Konduktor KŚ – grupa kontrolerów zatrudnionych przez Koleje Śląskie z uprawnieniami tylko do wykonywania kontroli; kontrole przez nich przeprowadzone powinny być wyróżnione w sposób odmienny od kontroli prowadzonych przez kontrolerów etatowych i kontrolerów zatrudnionych w oparciu o umowę zlecenie co ma odzwierciedlenie w słowniku pola „Typ kontrolera”.

Raportowanie wyników kontroli

Wynik kontroli powinien mieć odzwierciedlenie w dedykowanych raportach kontroli. Każdy rekord powinien dotyczyć kontroli jednego pasażera i zawierać minimum wymienione poniżej dane:

- Nr pojazdu;
- S/N urz. kontrolerskiego;
- Identyfikator kontrolera słownik do zdefiniowania w AOZ;
- Typ kontrolera: słownik do zdefiniowania w AOZ (zawodowy, społeczny, konduktor KŚ);
- Dane wpisano: słownik do zdefiniowania w AOZ (automatycznie/ręcznie);
- Numer linii (z oznaczeniem środka transportu, tj. autobus, tramwaj, trolejbus);
- Numer boczny pojazdu;
- Numer kursu;
- Przystanek;
- Pozycję GPS;
- Kierunek;
- PAN karty ŚKUP lub token karty EMV;
- Jednoznaczne określenie rodzaju kontrolowanego identyfikatora wraz z jego numerem;

- Rozpoczęcie kontroli, zakończenie kontroli, brak biletu, sprawdzone bilety wraz ze szczegółami;
- Data kontroli: RRRR-MM-DD;
- Czas kontroli: HH:MM:SS;
- Status kontroli: słownik do zdefiniowania w AOZ opłata dodatkowa, nieprawidłowa;
- Numer nałożonej opłaty: numeracja do zdefiniowania w AOZ;
- Powód nałożenia opłaty: słownik do zdefiniowania lub obecnie obowiązujący;
- Powód rezygnacji: słownik do zdefiniowania w AOZ lub obecnie obowiązujący;
- Sposób płatności: gotówka, karta płatnicza.

Raportowanie czasu pracy kontrolera

Czas pracy kontrolera powinien mieć odzwierciedlenie w dedykowanych raportach i powinien zawierać minimum wymienione poniżej dane:

- Identyfikator kontrolera;
- Typ kontrolera;
- Datę zalogowania: RRRR-MM-DD;
- Czas zalogowania: HH:MM:SS;
- Datę wylogowania: RRRR-MM-DD;
- Czas wylogowania: HH:MM:SS;
- S/N urzędnika.

Utworzenie raportu prezentującego przepracowaną ilość godzin dla danego kontrolera (od zalogowania w pojeździe do wylogowania z pojazdu), ilość dni, w których były prowadzone kontrole w zadanym okresie, możliwość wygenerowania ilości kontroli w pojazdach w zadanym przedziale godzinowym.

Raportowanie wyników kontroli dla grupy kontrolerów

Musi być możliwość wskazania w AOZ do pięciu Identyfikatorów kontrolerów w parametrach generowania raportu (ilość kontrolerów do uzgodnienia z Zamawiającym). Wygenerowany raport ma zawierać rekordy wszystkich kontroli wykonanych przez wszystkich kontrolerów we wskazanej grupie.

Raport dla grupy kontrolerów co do zasady jest raportem dziennym. Każdy rekord powinien dotyczyć kontroli jednego pojazdu i zawierać informacje o skontrolowanych identyfikatorach pasażerów w danym pojeździe oraz ilość wypisanych opłat dodatkowych. Minimalna ilość kolumn w raporcie powinna zawierać:

- Nr pojazdu;
- Identyfikator kontrolera;
- Typ kontrolera;
- Numer linii (z oznaczeniem środka transportu, tj. autobus, tramwaj, trolejbus);
- Numer boczny pojazdu;
- Numer kursu;
- Przystanek;
- Kierunek;

- Czas kontroli w pojeździe od: HH:MM:SS;
- Czas kontroli w pojeździe do: HH:MM:SS;
- Ilość skontrolowanych identyfikatorów;
- Ilość wypisanych opłat dodatkowych.

W pierwszej części podsumowania raportu powinny znaleźć się informacje o łącznych ilościach opłat dodatkowych wg rodzajów wypisanych w ciągu całego dnia roboczego przez grupę kontrolerów. Podsumowanie powinno zawierać następujące kolumny:

- Ilość opłat kredytowych pasażerskich;
- Ilość opłat kredytowych bagażowych;
- Ilość opłat gotówkowych pasażerskich;
- Ilość opłat gotówkowych bagażowych;
- Ilość opłat kredytowych policyjnych (podjazdowych).

Druga część podsumowania raportu powinna w sposób analityczny prezentować ilości opłat dodatkowych wypisanych przez poszczególnych kontrolerów, tj.:

- Numer kontrolera;
- Ilość opłat kredytowych pasażerskich;
- Numery opłat kredytowych pasażerskich;
- Ilość opłat kredytowych bagażowych;
- Numery opłat kredytowych bagażowych;
- Ilość opłat gotówkowych pasażerskich;
- Numery opłat gotówkowych pasażerskich;
- Ilość opłat gotówkowych bagażowych;
- Numery opłat gotówkowych bagażowych;
- Ilość opłat kredytowych policyjnych (podjazdowych);
- Numery opłat kredytowych policyjnych (podjazdowych).

Wszystkie raporty udostępnione w ramach AOZ mają mieć możliwość filtrowania po wszystkich kolumnach oraz wyeksportowania do plików xls, xlsx, pdf, doc, csv. Raporty mają mieć możliwość ustawienia parametrów wstępnych ograniczających zakres danych np. do zadanego okresu (danego roku, miesiąca, dnia itp.), przewoźnika, kontrolera itp. Po wydrukowaniu raportu powinno być przewidziane miejsce na podpis osoby zlecającej pracę kontrolerom oraz podpisy poszczególnych kontrolerów.

6.2.4 Aplikacje Obsługi Żądań dla urzędzeń u agentów sprzedaży (AOZ-UPOS)

Aplikacja Obsługi Żądań (AOZ-UPOS) stanowi dedykowaną, autonomiczną aplikację do zarządzania, konfigurowania i pełnej parametryzacji urzędzeń, monitorowania, diagnostyki, aktualizacji, podglądu danych w czasie rzeczywistym, rejestrowania i sterowania pracą terminali UPOS oraz zarządzania jego użytkownikami. Aplikacja AOZ ma być dostępna jako aplikacja webowa i w wersji na androida. Jedną z zakładek aplikacji ma być mapa z zaznaczonymi lokalizacjami i sygnalizacją o aktualnym stanie urzędzeń

(np. zielony – ok; żółty – sprawdź, problem; czerwony – awaria). Po kliknięciu w ikonę urządzenia ma być wyświetlana pełna informacja o danym urządzeniu. Szczegółowy zakres informacji zostanie uzgodniony z Zamawiającym po podpisaniu umowy. Po zalogowaniu się do aplikacji użytkownik ma mieć dostęp do zawartości zdefiniowanej dla jego profilu/grupy.

Ekran z listą urządzeń ma się odświeżać automatycznie, np. co 60 sekund aktualizując w ten sposób wszystkie dane zawarte w zestawieniu. Powinna być również dostępna funkcja wyłączenia odświeżania automatycznego, wówczas odświeżanie zawartości danych będzie następowało manualnie przez operatora.

Aplikacja Obsługi Żądań (AOZ), przewidziana jest do:

1. Definiowania urządzeń, w co najmniej następującym zakresie:
 - Nazwa terminala;
 - Adres lokalizacji;
 - Położenie na mapie (GUI z dostępem do mapy);
 - Seria i numer urządzenia;
 - Przypisywanie urządzeń do grup (np. w ramach jednego operatora).
2. Definiowania aktywności funkcjonalności aplikacji oraz parametrów pracy urządzenia, w co najmniej następującym zakresie:
 - Tryb sprzedaży (włącz/wyłącz);
 - Obsługa kart ŚKUP, ŚKUP 1.5 (włącz/wyłącz), w tym wydawanie kart ŚKUP z pełną funkcjonalnością tj. wydawanie kart za kaucja, akceptacja regulaminy, nadawanie pinu i hasła, przyjmowanie zwrotów kart od pasażerów, rozliczanie pobranych do wydania kart;
 - Częstotliwość pobierania: list dystrybucyjnych, konfiguracji, taryf z modułu MTC;
 - Maksymalna ilość biletów w ramach jednej transakcji;
 - Maksymalna wartość transakcji na danym terminalu/grupach terminali;
 - Maksymalna liczba transakcji/biletów na danym terminalu/grupach terminali;
 - Definiowania wzoru biletów papierowych z QRkodem (opcjonalnie w ramach godzin rozwojowych);
 - Definiowania kontraktów/biletów – usług, które będą dostępne na terminalu;
 - Blokowania urządzeń;
 - Blokowanie sprzedaży;
 - Zasilenie e-portmonetki.

Powyższe ustawienia mają być możliwe jako ustawienia globalne dla wszystkich urządzeń oraz ustawienia indywidualne dla wybranego/ych urządzeń/grup urządzeń.

3. Monitorowania pracy urządzeń, oprogramowania danego urządzenia, w co najmniej następującym zakresie:
 - Nazwa urządzenia wraz z jego numerem;
 - Tryb pracy terminala;
 - Stan łączności – online, offline – czas ostatniego kontaktu z serwerem;
 - Stan drukarki – ok, awaria, problem;

- Data konfiguracji – dane o pobraniu konfiguracji na urządzenie (rok, miesiąc, dzień, godzina, minuta, sekunda);
 - Wersja oprogramowania – wskazanie numeru wersji wraz z oznaczeniem kolorystycznym czy jest aktualna, czy nieaktualna;
 - Data wgrania wersji;
 - Wersja oczekująca;
 - Data ostatniej zmiany;
 - Osoba wykonująca zmianę w systemie;
 - Wykonanych restartach;
 - Przypisaniem paczek z kartami ŚKUP;
 - Alarmów generowanych przez terminal.
4. Wglądu w zdarzenia (logi) oraz komunikaty urządzenia, w co najmniej następującym zakresie:
- Nazwa terminala;
 - Data logowania do aplikacji sprzedażowej zainstalowanej na urządzeniu;
 - Nazwa operatora;
 - Nazwa wykonanej czynności np. poprawne/niepoprawne zalogowanie się; obsługa paczek kart (dodanie/usunięcia paczki kart; wydanie/zablokowanie karty); aktualizacja oprogramowania; restart aplikacji;
 - Zamawiający musi mieć możliwość zdalnego (z poziomu komputera pracownika) połączenia się do terminala i pobrania logów szczegółowych (zapisów oprogramowania) dotyczących jego pracy.
5. Obsługi wersji oprogramowania instalowanych na terminalach z możliwością ustawiania akcji (natychmiast, w przyszłości z określeniem daty i czasu), w co najmniej następującym zakresie:
- Prezentacji aktualnej wersji oprogramowania;
 - Aktualizacji oprogramowania oraz taryfy z poziomu AOZ (wysłanie wersji oprogramowania z poziomu administratora i automatyczne pobranie oraz zainstalowanie jej w urządzeniu);
 - Aktualizacji ustawień, w tym konfiguracja punktu sprzedaży oraz terminala;
 - Restartu aplikacji.
6. Dodawania, edycji i zarządzania operatorami uprawnionymi do obsługi terminali, w tym co najmniej w następującym zakresie:
- Zdefiniowania nazwy operatora wraz z przypisaniem indywidualnego ID;
 - Definiowania ważności uprawnienia;
 - Definiowania zakresu uprawnień, np. sprzedaż usług konkretnego dostawcy, wydawanie kart, przyjmowanie płatności gotówką, zasilenie e-portmonetki;
 - Zdefiniowania hasła/pin-u do logowania się na urządzeniu. Zarządzanie tym uprawnieniem ma być możliwe w ramach grupy terminali przypisanych do operatorów, tj. administrator operatora ma mieć możliwość zarządzania pin-ami w ramach urządzeń swojej grupy;
 - Przypisania operatorowi dostępu do wskazanych urządzeń.
7. Dodawania i edycji użytkownikom odpowiednich uprawnień – profili, pozwalających na dostęp do poszczególnych funkcjonalności w aplikacji AOZ, w tym co najmniej w następującym zakresie:

- Administrator – pełne uprawnienia;
 - Organizator – nadawanie uprawnień (wraz z ich edycją) operatorom i użytkownikom, w tym nadawanie haseł dostępu, konfiguracja urządzeń (aktualizacje ustawień, restarty urządzeń, ustawienia globalne oraz lokalne urządzeń, wzory biletów, definiowanie taryfy/usług), aktualizacja urządzeń (dodawanie nowych wersji oprogramowania);
 - Administrator operatora – zarządzanie pin-ami w ramach urządzeń swojej grupy terminali przypisanych do operatorów;
 - Finanse – dostęp do danych finansowych, w tym wgląd do wszystkich transakcji przeprowadzonych na terminalach (kwota, typ płatności: gotówka, nr karty ŚKUP, numer karty płatniczej, ilość zakupionych kontraktów, wartość), z możliwością nadawania uprawnień dla wszystkich urządzeń lub grupy urządzeń danego operatora;
 - Eksploatacja – dostęp do wszystkich zdarzeń, łącznie z danymi finansowymi.
8. Kody błędów terminala.
9. Aplikacja ma umożliwiać generowanie co najmniej następujących raportów:
- Audyt działania kasjera/serwisanta w punkcie sprzedaży;
 - Raporty sprzedaży dzienny, tygodniowy, miesięczny za wskazany okres, itp.;
 - Generowanie raportów sprzedaży dla operatorów.
- a) raport sprzedaży ma posiadać informację o statusie każdej transakcji (poprawna, niepoprawna) (wymagane pola):
- Nazwa terminala;
 - Data godzina;
 - Kwota;
 - Typ płatności – gotówka;
 - Unikatowy identyfikator transakcji;
 - Typ i ID kontraktu/usługi – nazwa bilet papierowy, bilet elektroniczny, wydanie karty, zasilenie e-portmoentki;
 - Ilość;
 - Wartość;
 - Czy wydano potwierdzenie;
 - Numer karty ŚKUP;
 - Status płatności – udana, nieudana – błąd wydawania karty, anulowana;
 - TID;
 - MID.
- z możliwością filtracji dla:
- Gotówka;
 - Po rodzajach biletów;
 - Data, czas;
 - Ilość;
 - Wartość;
 - Nazwa terminala;
 - Nazwa operatora.

z możliwością filtracji dla dowolnego przedziału czasu, urządzenia, z exportem do plików CSV, XLS, XLSX, PDF oraz drukuj.

b) raport z przyjęcia/zwrotu paczek kart ŚKUP 1.5 (wymagane pola):

- Urządzenie – nazwa, lokalizacja;
- Data, godzina operacji;
- Nazwa operatora;
- Numer paczki;
- Liczba kart w paczce;
- Wykaz kart w paczce.

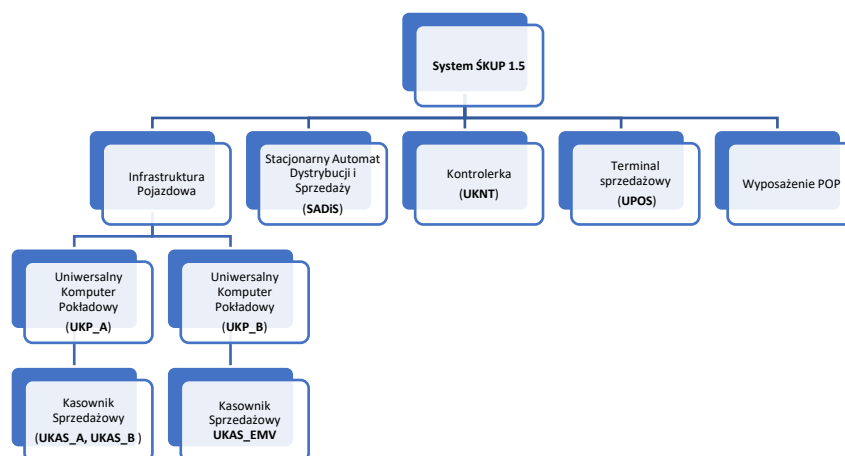
c) raport z wydania kart (wymagane pola):

- Urządzenie – nazwa, lokalizacja;
- Data, godzina operacji;
- Nazwa operatora;
- Gotowych do wydania;
- Wydanych;
- Przeterminowane;
- Nieznalezione.

6.3 Infrastruktura wyniesiona - urządzenia

W ramach planowanej modernizacji infrastruktury wyniesionej systemu ŚKUP możemy wyróżnić następujące grupy urządzeń, które Wykonawca musi zmodernizować w obecnie eksploatowanym systemie ŚKUP, tzn. zainstalować i uruchomić oprogramowanie spełniające wymagania funkcjonalne opisane w niniejszym dokumencie. Jeżeli będzie konieczne, to Zamawiający dopuszcza możliwość wymiany podzespołów pod warunkiem zastosowania elementów charakteryzujących się parametrami technicznymi co najmniej takimi jak urządzenia wymieniane w załączniku nr 2.2 do OPZ -Parametry techniczne urządzeń lub zastosowania dodatkowych elementów/modułów, które będą realizować funkcjonalności przewidziane w systemie ŚKUP 1.5. Za jakiegokolwiek czynności opisane powyżej Wykonawcy nie będzie przysługiwało dodatkowe wynagrodzenie, dlatego koszty z tym związane musi skalkulować w złożonej ofercie.

Zamawiający oczekuje przekazania parametrów techniczno-eksploatacyjnych urządzeń (infrastruktury pojazdowej), które będą gwarantowały kompatybilność odebranego w ramach niniejszego zamówienia oprogramowania.



Rysunek 16. Wykaz urządzeń systemu ŚKUP 1.5

W ramach infrastruktury wyniesionej można wyróżnić następujące rodzaje urządzeń:

1. Infrastruktura Pojazdowa:
 - a) Rejon Tyski:
 - Komputer pokładowy RTC 1200SK (UKP_B);
 - Czytnik kart ŚKUP oraz kart płatniczych CVB48.TY (UKAS-EMV);
 - Switch SWR 11;
 - Drukarka Plus2 – urządzenia nie będą wykorzystywane;
 - PMU/Konwerter;
 - Stacja dokująca do tabletu;
 - b) Rejon Systemu z urządzeniami firmy AEP:
 - Uniwersalny komputer pokładowy CDB-6 (UKP_A);
 - Kasownik dualny F240B z możliwością kasowania biletów papierowych (UKAS_A);
 - Kasownik F3A tylko i wyłącznie do czytania kart ŚKUP (UKAS_B);

- Drukarka Deon E – urządzenia nie będą wykorzystywane;
 - Switch SW 16;
 - Zasilacz RSD 150 C-24;
2. Stacjonarny Automat Dystrybucji i Sprzedaży (SADiS);
 3. Kontrolerka Biletów (UKNT);
 4. Terminal Sprzedażowy (UPOS);
 5. Wyposażenie POP.

Szczegółowy opis parametrów technicznych ww. urządzeń wraz z ich ilością znajduje się w **załączniku nr 2.2 Parametry Techniczne Urządzeń**.

6.3.1 Infrastruktura pojazdowa

System pojazdowy powinien przetwarzać wszystkie transakcje i zdarzenia występujące pomiędzy urządzeniami UKP, UKAS, UKAS-EMV oraz identyfikatorami w celu realizacji przypisanych im funkcji. W Aplikacji Obsługi Żądań (AOZ – Pojazdy) powinna być widoczna każda interakcja identyfikatora z UKAS, UKAS-EMV. Natomiast w Module Rozliczeń Transakcji i Tokenizacji (MRTT) widoczna powinna być każda transakcja wykonana z ich użyciem. Wymiana danych pomiędzy urządzeniami zainstalowanymi w pojeździe, a systemem centralnym i modułami logicznymi ma odbywać się w czasie zbliżonym do rzeczywistego, (dotyczy to transakcji, oraz innych danych, które zaistnieją w systemie w celu realizacji przypisanych im funkcji). System ma umożliwiać obsługę zewnętrznych systemów pokładowych takich jak: moduły informacji pasażerskiej – tablice informacyjne i kierunkowe w pojeździe, bramki zliczające pasażerów, system zapowiadania przystanków, połączenie z systemem szybkiego reagowania przeniesienie dźwięku oraz obrazu z pojazdu do komputera który znajduje się np. na dyspozytorni - realizowane przez zaimplementowane w UKP otwarte protokoły komunikacyjne wymiany danych (API-UKP) – w ramach umowy nie jest wymagana integracja, tylko otwartość na integrację. UKAS, UKAS-EMV w pojazdach, powinny identyfikować dane z konta użytkownika oraz przeprowadzać transakcję kartową w czasie zadeklarowanym w formularzu ofertowym (nie dłuższym niż 2 sekundy).

We wszystkich pojazdach w liczbie odpowiadającej liczbie drzwi, w łatwo dostępnym miejscu, ma się znaleźć naklejka z kodem QR lub Tag NFC, która będzie służyła do identyfikacji pojazdu w Aplikacji Mobilnej. Wykonawca zdefiniuje relację/powiązanie kodów QR lub Tag NFC z pojazdami oraz umożliwi Zamawiającemu zarządzanie tymi relacjami.

Oprogramowanie

Tworzone oprogramowanie powinno spełniać normę ISO/IEC 25010:2011.

6.3.1.1 Uniwersalny Komputer pokładowy (UKP)

Uniwersalny Komputer Pokładowy (UKP) to urządzenie mające zapewniać komunikację z systemem centralnym, komunikację z komponentami wchodzącymi w skład infrastruktury pojazdowej "ŚKUP 1.5" z możliwością monitorowania ich pracy, oraz komunikację z innymi podsystemami informacyjnymi pojazdu (otwarty i opisany interfejs API wymiany danych). Umożliwia on interakcję z użytkownikiem (kierowcą), powinien także podlegać zdalnemu zarządzaniu z poziomu modułów AOZ-pojazdy. Realizację funkcjonalności powinien wykonywać w czasie zbliżonym do rzeczywistego (online), w przypadku braku łączności musi buforować dane, celem ich natychmiastowego wysłania w chwili przywrócenia łączności.

Lista Procesów obsługiwanych przez moduł:

- a) Sterowanie pracą (kierowca, operator AOZ-pojazdy) oraz kontrola sprawności modułów do pobierania opłat za przejazd (UKAS, UKAS-EMV i inne podłączone urządzenia);
- b) Interakcja z użytkownikiem (kierowca, serwisant) w zakresie autoryzacji i uruchamiania urządzeń;
- c) Interakcja z użytkownikiem (kierowca) w zakresie blokady kasowników (UKAS, UKAS-EMV);
- d) Interakcja z użytkownikiem (kierowca) w zakresie realizacji funkcjonalności związanych z obsługą linii, kursu, kontakt z dyspozytorem, diagnostyka urządzeń (ekran dotykowy tylko w „Systemie tyskim”, przyciski manualne w obu systemach);
- e) Interakcja z użytkownikiem (serwisant) w zakresie realizacji czynności serwisowych (gromadzenie logów, komunikaty diagnostyczne, funkcje serwisowe);
- f) Współpraca z modułami komunikacyjnymi, wbudowanymi lub zewnętrznymi: GSM/4G w standardzie LTE lub nowszym (w systemie „tyskim”), a w standardzie 3G w systemie „urządzeń AEP”, GPS;
- g) Komunikacja z innymi zewnętrznymi podsystemami pojazdu takimi jak: moduły informacji pasażerskiej – tablice informacyjne i kierunkowe w pojeździe, bramki zliczające pasażerów, system zapowiadania przystanków, UKP ma mieć otwarty protokół komunikacyjny wymiany danych (API-UKP) – w ramach umowy nie jest wymagana integracja, tylko otwartość na integrację – tj. dostarczenie API. Możliwość podpięcia realizowana np. przez przełącznik sieciowy;
- h) Interakcja z użytkownikiem (kierowca -> dyspozytor) w zakresie wysyłania alarmów (SOS), funkcjonalność przycisku SOS zaimplementowana jako element GUI w UKP lub zewnętrzny wyzwalacz (np. Przycisk);
- i) Interakcja z użytkownikiem (kierowca <-> dyspozytor (AOZ-pojazdy) w zakresie przesłania np. krótkich komunikatów do/od dyspozytora;
- j) Umożliwienie współpracy z kontrolerami biletów w zakresie, blokowania i odblokowania kasowników.

Komunikacja z systemem centralnym oraz usługami zewnętrznymi w zakresie wymiany informacji dotyczących:

- a) Sprzedaży uprawnień do przejazdu, zbieranych z kasowników (w tym CICO);
- b) Synchronizacja zegarów urządzeń z centralnym serwerem czasu;

- c) Pobieranie rozkładów jazdy, przetwarzanie ich, przesyłanie ich do kasowników (danych o realizacji linii, kursie, kierunku, przystanku);
- d) Komunikatów o pozycji pojazdu (przesłania ramki do systemu centralnego, zgodnie z formularzem ofertowym, nie rzadziej niż co 6 sekundy);
- e) Monitorowania pracy komponentów wchodzących w skład infrastruktury pojazdowej;
- f) Monitorowania komunikacji wewnątrz pojazdowej;
- g) Przekazywanie danych z podejmowanych akcji automatycznych w oparciu o dane z monitorowania;
- h) Zmian parametrów pracy modułów UKP, UKAS, UKAS-EMV;
- i) Zmian konfiguracji (przypisania do pojazdu) urządzeń pokładowych;
- j) Blokowania urządzenia;
- k) Aktualizacji wersji oprogramowania UKP, UKAS, UKAS-EMV;
- l) Aktualizacji danych o użytkownikach i identyfikatorach, przyznawanie uprawnień/blokowanie dostępu;
- m) Wymiany danych i przesyłanie ich do kasowników w celu:
 - o Aktualizacji danych o identyfikatorze (aktywne kontrakty, stan e-portmonetki);
 - o Blokady obsługi identyfikatora;
- n) stanu konta e-portmonetki oraz zapisanych na koncie użytkownika biletów;
- o) Udostępnienia oferty usług do zakupu oraz innych informacji w kasowniku;
- p) Udostępnienia danych na potrzeby dynamicznej informacji pasażerskiej;
- q) Otwarty interfejs wymiany danych (API) dostępny w ramach wbudowanych portów komunikacyjnych;
- r) Otwarty na rozbudowę system operacyjny pozwalający na dodawanie kolejnych komponentów programowych i sprzętowych (z wykorzystaniem dostępnych interfejsów).

Szata interfejsu graficznego UKP, UKAS, UKAS-EMV powinna być spójna z szatą graficzną innych komponentów. Wykonawca zaproponuje projekty, a następnie uzgodni z Zamawiającym szatę graficzną oraz poszczególne ekrany funkcjonalne dla urządzeń przed ich implementacją.

Podstawowe funkcje uniwersalnego komputera to:

- a) Ciągła wymiana on-line (pobieranie i wysyłanie) właściwych danych z systemem centralnym i kasownikami w wymaganym zakresie, w tym rozkładów jazdy, taryf, danych transakcyjnych, aktualnej lokalizacji pojazdu, informacji o numerze linii, kursu, identyfikatorze kierującego, listach dystrybucyjnych. Wymiana danych pomiędzy elementami Systemu nie może powodować przerw w pracy kasowników i komputera pokładowego. Pobierane dane z systemu powinny być gromadzone na urządzeniu lokalnym (mainserwer) i dystrybuowane do wszystkich urządzeń bez przerywania ich pracy;
- b) Przesyłanie danych lokalizacyjnych (pozycji GPS) do systemu centralnego, zgodnie z formularzem ofertowym, nie rzadziej niż co 6 sekund z możliwością modyfikacji (skrócenia/wydłużenia) tego czasu przez Zamawiającego – parametr konfigurowalny w systemie SKUP 1.5. W przypadku braku możliwości przesłania danych lokalizacyjnych (np. z uwagi na brak dostępnej sieci GSM) komputer zapewni gromadzenie tych danych w pamięci urządzenia, a następnie niezwłocznie przekaże je na serwer po uzyskaniu połączenia z serwerem w kolejce FIFO;

- c) Sterowanie pracą oraz kontrola sprawności kasowników wraz z ich blokadą;
- d) Wymiana danych z systemem centralnym i kasownikami (w tle), m.in. w zakresie list dystrybucyjnych, wniesionych opłat i ich wykorzystywania, w czasie rzeczywistym bez przerw w pracy komputera w trakcie trwania kursu;
- e) Dopuszcza się możliwość odblokowania kasowników po wjechaniu pojazdu do strefy następnego przystanku od rozpoczęcia kontroli;
- f) Aktualizacja oprogramowania – nie może następować w trakcie trwania kursu, gdyż komputer przez cały kurs musi zapewniać nieprzerwaną pracę, musi następować na rozpoczęcie lub zakończenie zmiany;
- g) Pobieranie, przechowywanie i realizacja rozkładów jazdy z wyświetlaniem na wyświetlaczu komputera, wraz z informacją o przyspieszeniu lub opóźnieniu;
- h) Kierowca na ekranie komputera powinien mieć zaprezentowane następujące dane: aktualnie realizowany kurs z kierunkiem (przystanek końcowy), aktualny czas, odchylenie od realizowanego rozkładu jazdy (w minutach), nazwę bieżącego przystanku (po wjeździe w strefę przystankową), nazwę następnego przystanku (po ruszeniu pojazdu z przystanku);
- i) Logowanie kierującego i serwisanta do komputera, poprzez podanie identyfikatora kierowcy/serwisanta i kodu PIN;
- j) Automatyczna zmiana kursów na kolejny – obecnie funkcjonalność dostępna w systemie "Tyskim", ma być wprowadzona również w urządzeniach AEP, na podstawie danych lokalizacyjnych i rozkładowych oraz umożliwienie kierowcy ręczną zmianę przystanków i kursów w przypadkach awaryjnych (np. objazdy, wypadki) – w przypadku ręcznej zmiany przystanków wymagane potwierdzenie przez kierującego zmiany przystanku;
- k) Przechowywanie danych identyfikacyjnych pojazdu;
- l) Współpraca z modułem komunikacyjnym GSM/4G w standardzie LTE lub nowszym i GPS;
- m) Obsługa przycisku umożliwiającego wysłanie komunikatu do dyspozytora – po naciśnięciu tego przycisku pojawia się ekran umożliwiający wprowadzenie i wysłanie krótkiej informacji dla dyspozytora;
- n) Obsługa przycisku alarmowego umożliwiającego wysyłanie informacji w przypadku zagrożenia. Jeżeli kierowca naciśnie przycisk alarmowy, ID pojazdu oraz jego położenie zostają przesłane do systemu centralnego ŚKUP 1.5;
- o) Przekazywanie do systemu centralnego informacji o numerze linii, kursu, numerze identyfikacyjnym kierującego pojazdem, danych identyfikacyjnych pojazdu;
- p) Możliwość przekazywania danych lokalizacyjnych, danych o numerze linii, nazwy zadania przewozowego, kursu, danych rozkładowych, w tym przyspieszeniu i opóźnieniu do innych systemów wskazanych przez Zamawiającego, w szczególności do systemów ITS zamontowanych poza pojazdem oraz wykorzystywanych przez Zamawiającego systemów informacji pasażerskiej z częstotliwością i na zasadach określonych w punkcie b).

W celu zapewnienia maksymalnego bezpieczeństwa i poufności transmitowanych drogą radiową wrażliwych danych (zwłaszcza informacji o operacjach finansowych oraz danych osobowych), komputer powinien też spełniać funkcje szyfrujące – kryptograficzne. Oprogramowanie komputera musi mieć konstrukcję otwartą, tzn. musi istnieć w przyszłości możliwość rozbudowy jego funkcji poprzez zmianę oprogramowania przy użyciu złącza USB, jak również drogą radiową poprzez moduł komunikacyjny GSM/4G w standardzie LTE lub nowszym.

6.3.1.2 Kasownik (UKAS, UKAS-EMV)

Kasownik Sprzedażowy (UKAS, UKAS-EMV), to urządzenie mające zapewnić komunikację z użytkownikiem (pasażer), komunikację z komputerem pokładowym UKP i poprzez komputer pokładowy z modułami systemu centralnego. Kasownik pobiera z UKP dane konfiguracyjne, aktualną wersję aplikacji, dane informacyjne np. realizowana linia, kierunek, aktualny i następny przystanek itp., do UKP przykazywane są dane transakcji i zdarzeń.

Z uwagi na obszar, którego dotyczy przedmiotowe postępowanie możemy podzielić cały obszar na dwa rodzaje dotyczące zamontowanego sprzętu ŚKUP w pojazdach:

- Obszar Tyski (UKAS-EMV)
- Obszar urządzeń firmy AEP (UKAS_A, UKAS_B)

Biorąc pod uwagę powyższe dokonano podziału urządzeń ze względu na obszar:

UKAS „Tyski” (UKAS – EMV)

1. Lista Procesów obsługiwanych przez moduł UKAS - EMV:

- a) Interakcja z użytkownikiem w celu inicjowania realizacji funkcjonalności związanych z wnoszeniem opłat za przejazd (kartami EMV i punktami z e-portmonetki) i ich anulowania (ekran dotykowy, czytnik identyfikatora). Wyraźny do odczytania przez pasażera „sygnał” informujący o poprawności bądź nie, wykonania transakcji;
- b) Interakcja z użytkownikiem w celu wniesienia opłaty za przejazd w taryfie CICO. Wyraźny do odczytania przez pasażera „sygnał” informujący o poprawności bądź nie, wykonania transakcji;
- c) Interakcja z użytkownikiem w celu wyboru biletów zapisanych na koncie centralnym (ekran dotykowy, czytnik identyfikatora);
- d) Interakcja z użytkownikiem (kontroler) w celu blokady kasowników (sygnał z kontrolerki UKNT, lub zbliżenie specjalnego identyfikatora);
- e) Interakcja z użytkownikiem w celu udostępnienia i informacji na temat dostępnych biletów do zakupu, informacji na temat zakupionych wcześniej biletów sprawdzanie czy są jeszcze ważne itp. (ekran dotykowy);
- f) Prezentacja na wyświetlaczu obecnej lokalizacji (np. nazwa przystanku, nr linii, czas, kierunek);
- g) Komunikacja z modułami systemu centralnego, poprzez komputer pokładowy UKP w zakresie:
 - sprzedaży uprawnień do przejazdu, w tym realizacja płatności kartami EMV i surogatami oraz kartą ŚKUP w ramach e-portmonetki;
 - pobieranie informacji z rozkładów jazdy;
 - zmian parametrów pracy kasownika;
 - zmian konfiguracji (przypisania do pojazdu), kasownika;

- blokowania urządzenia;
- aktualizacji wersji oprogramowania kasownika;
- pobierania danych w celu:
 - aktualizacji danych o identyfikatorach (aktywnych, zablokowanych itp.);
 - blokady obsługi identyfikatora w kasowniku;
- h) Prezentacji informacji zapisanych na koncie identyfikatora lub na karcie ŚKUP w zakresie ulg, uprawnień, biletów jak również stanu posiadanych środków na e-portmonetce;
- i) Możliwość zakupu biletów z wykorzystaniem środków zgromadzonych na e-portmonetce oraz prezentacja salda rachunku.

Do najważniejszych funkcji UKAS – EMV należy:

- a) Wnoszenie opłat za przejazdy jednorazowe wg taryf obowiązujących w ZTM i pobieranych z systemu ŚKUP 1.5 – musi być możliwość wnoszenia opłat poprzez wybór taryfy wskazanej w module MTC (domyślnie taryfa czasowa oraz taryfa strefowo-czasowa wraz z biletami dobowymi i dziennymi) oraz w modelu CICO, zarówno kartami EMV, jak i Kartami ŚKUP (w ramach e-portmonetki);
- b) Obsługa biletów w zakresie ich „skasowania”, w przypadku biletów od pierwszego użycia oraz wieloprzejazdowych;
- c) Możliwość ręcznego wyboru opcji wnoszenia w pojeździe opłat ze zniżką oraz wykorzystanie informacji o uldze zdefiniowanej na koncie, do którego jest przypisany identyfikator;
- d) Wnoszenie opłat za współpasażera, w tym wyboru dla wszystkich biletów i opłat wnoszonych bezpośrednio w pojeździe zapłaty za przejazd ulgowy;
- e) Obsługa biletów okresowych w zakresie ich aktywacji, rejestracji wejścia, w tym zmniejszanie liczby przejazdów do wykorzystania (w przypadku biletów z limitem przejazdów);
- f) Pojawienie się komunikatu z informacją o ważnym bilecie lub zakupionym dla tego przejazdu w przypadku przyłożenia identyfikatora do kasownika;
- g) Możliwość dokupienia biletu w trakcie realizowanego przejazdu;
- h) Informacja o biletach, które są dostępne na ww. koncie;
- i) Informacja o biletach zakupionych kartą płatniczą/kartą ŚKUP (funkcja info) – wyświetlana ma być informacja wyłącznie o biletach ważnych lub o biletach do wykorzystania – nie mają być wyświetlane informacje o biletach już wykorzystanych/nieważnych;
- j) Obsługa tzw. Blue-Listy, czyli propagacja informacji o zakupach, aktywacjach, rejestracjach wejść dokonanych przez użytkowników kont posługujących się identyfikatorem;
- k) Blokowanie i nieobsługiwanie identyfikatorów: zablokowanych, zastrzeżonych oraz odpiętych z konta znajdujących się na tzw. Black-liście;
- l) Obsługa tzw. Stop-List, które zawierają identyfikatory kont, dla których w systemie widnieje zadłużenie;
- m) Przechodzenie pomiędzy zakładkami powinno odbywać się w sposób płynny i intuicyjny. Czas przejścia do innej zakładki lub innego ekranu nie może być dłuższy niż 1 sekunda;

- n) Przechodzenie kasownika do ekranu głównego, jeżeli użytkownik po wybraniu dowolnej opcji, w tym również zmiany języka, w ciągu 5 sekund użytkownik nie wybierze kolejnej opcji lub nie przyłoży karty w celu dokonania zapłaty;
- o) Potwierdzanie akustycznie i wizualnie zrealizowanych operacji – w przypadku pozytywnego zakończenia operacji (wniesienie opłaty, zakup biletu, aktywacja lub rejestracja biletu) oczekuje się potwierdzenie w postaci zmiany koloru wyświetlacza (na kolor zielony) lub zapalenia się wbudowanego w obudowę kasownika oświetlenia (również kolor zielony) oraz odpowiedniego komunikatu na ekranie wyświetlacza i sygnału dźwiękowego; w przypadku niepomyślnego zakończenia operacji, w tym przyłożenia identyfikatora przypisanego do konta który znajduje się na Black-List, Stop-List lub identyfikatora który jest przypisany do konta użytkownika ŚKUP 1.5, na którym nie ma biletów, oczekuje się informacji w postaci jw. z tym, że kolorem ma być czerwony, a sygnał dźwiękowy ma być inny niż przy weryfikacji pozytywnej;
- p) Wymiana danych z komputerem w tle, m.in. w zakresie list dystrybucyjnych, wniesionych opłat i ich wykorzystywanie w czasie rzeczywistym bez przerw w pracy modułu w trakcie trwania kursu;
- q) Aktualizacja oprogramowania – nie może następować w trakcie trwania kursu, gdyż kasownik przez cały kurs musi zapewniać nieprzerwaną pracę. Powinna nastąpić dopiero na zakończenie zmiany lub rozpoczęcia kolejnego kursu/zmiany;
- r) Rejestracja wszystkich wykonywanych operacji i zdarzeń systemowych;
- s) Raportowanie wszystkich szczegółów transakcji wykonanych w kasownikach do systemu centralnego w sposób umożliwiający raportowanie i rozliczanie transakcji; każdy bilet zakupiony w urządzeniu powinien mieć zapisany unikalny identyfikator - numer biletu, co pozwoli m.in. weryfikować kompletność danych przekazywanych do systemu centralnego;
- t) Każda paczka danych o transakcjach wysyłana do systemu centralnego musi mieć swoją unikalną numerację, co pozwoli na weryfikację kompletności przekazywania danych do systemu centralnego;
- u) Umożliwianie automatycznej zmiany taryf biletowych (cen biletów) – poprzez pobranie ich z modułu MTC i uruchomienie od zdefiniowanej daty;
- v) Współpracę z kontrolerką – w zależności od przyjętego rozwiązania, w tym blokada pracy po rozpoczęciu kontroli;
- w) Kasownik musi umożliwiać obsługę w języku polskim oraz dodatkowo w co najmniej 4 językach obcych (szczegóły opisuje pkt. 11.5.3 niniejszego dokumentu).

Pobieranie opłat/rejestracja użyciu identyfikatora, będzie następować poprzez interfejs zbliżeniowy, co będzie potwierdzone sygnałem dźwiękowym. Sygnał dźwiękowy nie może trwać dłużej niż 100 –200 ms i musi być dla pozytywnej weryfikacji karty/identyfikatora inny niż w przypadku braku akceptacji karty/identyfikatora. Informacja wizualna nie może trwać dłużej niż 3 sekundy. Informacja wizualna musi mieścić się na jednym ekranie bez konieczności przewijania, a wysokość czcionki najmniejszego z prezentowanych znaków nie może być mniejsza niż 8 mm. Informacje prezentowane w języku polskim w sposób wizualny nie mogą zawierać skrótów innych niż dostępne w słowniku języka polskiego. Po zarejestrowaniu użycia karty/identyfikatora, urządzenie zapisze na koncie użytkownika ŚKUP 1.5 lub karcie ŚKUP stosowne informacje w związku z ich użyciem. Czas operacji od przytknięcia identyfikatora

do jej akceptacji lub odmowy akceptacji zgodnie z zadeklarowanym w formularzu ofertowym (nie dłuższym niż 2 sekundy).

2. Lista Procesów obsługiwanych przez moduł UKAS:

- a) Interakcja z użytkownikiem w celu inicjowania realizacji funkcjonalności związanych z wnoszeniem opłat za przejazd z e-portmonetki punktowej i ich anulowania (przyciski funkcjonalne), w tym w taryfie CICO. Wyraźny do odczytania przez pasażera „sygnał” informujący o poprawności bądź nie, wykonania transakcji;
- b) Kasowanie biletów papierowych, kasownik dualny UKAS_A (UKAS_B brak takiej możliwości);
- c) Interakcja z użytkownikiem w celu wyboru biletów zapisanych na koncie centralnym (poprzez wybór odpowiedniej funkcji naciskając odpowiedni przycisk) i ich skasowaniem (w tym biletów wieloprzejazdowych);
- d) Interakcja z użytkownikiem (kontroler) w celu blokady kasowników (zbliżenie karty do kasownika oraz zatwierdzenie blokady poprzez wybór odpowiedniego przycisku);
- e) Interakcja z użytkownikiem w celu udostępnienia informacji zapisanych na karcie (ekran dotykowy) - tylko kasownik UKAS_B, kasownik UKAS_A brak takiej funkcjonalności;
- f) Prezentacja na wyświetlaczu obecnej lokalizacji (np. nazwa przystanku, czas, kierunek);
- g) Komunikacja z modułami systemu centralnego, poprzez komputer pokładowy UKP w zakresie:
 - sprzedaży uprawnień do przejazdu, w tym bilety jednorazowe i CICO;
 - pobieranie informacji z rozkładów jazdy;
 - zmian parametrów pracy kasownika;
 - zmian konfiguracji (przypisania do pojazdu), kasownika;
 - blokowania urządzenia;
 - aktualizacji wersji oprogramowania kasownika;
 - pobierania danych w celu:
 - aktualizacji danych o identyfikatorach (aktywnych, zablokowanych itp.);
 - blokady obsługi identyfikatora w kasowniku;
- h) Prezentacji informacji zapisanych na koncie IKU/karcie ŚKUP w zakresie zapisanych uprawnień, biletów jak również stanu posiadanych środków na e-portmonetce;
- i) Możliwość zakupu biletów z wykorzystaniem środków zgromadzonych na e-portmonetce.

Do najważniejszych funkcji UKAS należy:

- a) Wnoszenie opłat za przejazdy jednorazowe wg taryf obowiązujących w ZTM (pobieranych z systemu ŚKUP 1.5) – musi być możliwość wnoszenia opłat poprzez wybór taryfy wskazanej w module MTC (domyślnie taryfa czasowa, taryfa strefowo-czasowa wraz z biletami dobowymi i dziennymi) oraz taryfą CICO;
- b) Obsługa biletów w zakresie ich „skasowania”, w przypadku biletów od pierwszego użycia oraz wieloprzejazdowych;

- c) Możliwość ręcznego wyboru tylko kasownik UKAS_B opcji wnoszenia w pojeździe opłat ze zniżką oraz wykorzystanie informacji o uldze zdefiniowanej na koncie, do którego jest przypisana karta ŚKUP;
- d) Wnoszenie opłat za współpasażera, w tym wyboru dla wszystkich biletów i opłat wnoszonych bezpośrednio w pojeździe zapłaty za przejazd ulgowy tylko kasownik UKAS_B;
- e) Obsługa biletów okresowych w zakresie ich aktywacji, rejestracji wejścia, w tym zmniejszanie liczby przejazdów do wykorzystania (w przypadku biletów z limitem przejazdów);
- f) Prezentowanie komunikatu o ważnym bilecie lub zakupionym dla tego przejazdu w przypadku przyłożenia identyfikatora do kasownika;
- g) Możliwość dokupienia biletu w trakcie realizowanego przejazdu tylko kasownik UKAS_B;
- h) Informacja o biletach i saldzie e-portmonetki, które są dostępne na koncie IKU - tylko kasownik UKAS_B;
- i) Obsługa tzw. Blue-Listy, czyli propagacja informacji o zakupach, aktywacjach, rejestracjach wejść dokonanych przez użytkowników kont posługujących się kartą ŚKUP;
- j) Blokowanie i nieobsługiwanie użytkowników kart ŚKUP: zablokowanych, zastrzeżonych oraz odpiętych z konta znajdujących się na tzw. Black-liście;
- k) Obsługa tzw. Stop-List, użytkowników kart ŚKUP dla których w systemie widnieje zadłużenie;
- l) Przechodzenie pomiędzy zakładkami powinno odbywać się w sposób płynny i intuicyjny. Czas przejścia do innej zakładki lub innego ekranu nie może być dłuższy niż 1 sekunda;
- m) Przechodzenie kasownika do ekranu głównego, jeżeli użytkownik po wybraniu dowolnej opcji, w tym również zmiany języka, w ciągu 5 sekund użytkownik nie wybierze kolejnej opcji lub nie przyłoży karty w celu dokonania zapłaty;
- n) Potwierdzanie akustycznie i wizualnie zrealizowanych operacji – w przypadku pozytywnego zakończenia operacji (wniesienie opłaty, zakup biletu, aktywacja lub rejestracja biletu, rejestracja wejścia/wyjścia CI/CO) oczekuje się potwierdzenie w postaci zmiany koloru wyświetlacza (na kolor zielony) lub zapalenia się wbudowanego w obudowę kasownika oświetlenia (również kolor zielony) oraz odpowiedniego komunikatu na ekranie wyświetlacza i sygnału dźwiękowego; w przypadku niepomyślnego zakończenia operacji, w tym przyłożenia karty ŚKUP do konta które znajduje się na Black-List, Stop-List lub jest przypisana do konta użytkownika, na którym nie ma biletów, oczekuje się informacji w postaci jw. z tym, że kolorem ma być czerwony, a sygnał dźwiękowy ma być inny niż przy weryfikacji pozytywnej;
- o) Wymiana danych z komputerem w tle, m.in. w zakresie list dystrybucyjnych, wniesionych opłat i ich wykorzystywanie w czasie rzeczywistym bez przerw w pracy modułu w trakcie trwania kursu;
- p) Aktualizacja oprogramowania – nie może następować w trakcie trwania kursu, gdyż kasownik przez cały kurs musi zapewniać nieprzerwaną pracę. Powinna nastąpić dopiero na zakończenie zmiany lub rozpoczęcia kolejnego kursu/zmiany;
- q) Rejestracja wszystkich wykonywanych operacji i zdarzeń systemowych;
- r) Raportowanie wszystkich szczegółów transakcji wykonanych w kasownikach do systemu centralnego w sposób umożliwiający raportowanie i rozliczanie transakcji; każdy bilet

- zakupiony w urządzeniu powinien mieć zapisany unikalny identyfikator - numer biletu, co pozwoli m.in. weryfikować kompletność danych przekazywanych do systemu centralnego;
- s) Każda paczka danych o transakcjach wysyłana do systemu centralnego musi mieć swoją unikalną numerację, co pozwoli na weryfikację kompletności przekazywania danych do systemu centralnego;
 - t) Umożliwianie automatycznej zmiany taryf biletowych (cen biletów) – poprzez pobranie ich z modułu MTC i uruchomienie od zdefiniowanej daty;
 - u) Współpracę z kontrolerką – w zależności od przyjętego rozwiązania, w tym blokada pracy po rozpoczęciu kontroli;
 - v) Kasownik musi umożliwiać obsługę w języku polskim.

Pobieranie opłat/rejestracja użyciu karty ŚKUP, będzie następować poprzez interfejs zbliżeniowy, co będzie potwierdzone sygnałem dźwiękowym. Sygnał dźwiękowy nie może trwać dłużej niż 100 –200 ms i musi być dla pozytywnej weryfikacji karty/identyfikatora inny niż w przypadku braku akceptacji karty/identyfikatora. Informacja wizualna nie może trwać dłużej niż 3 sekundy. Po zarejestrowaniu użycia karty/identyfikatora, urządzenie zapisze na koncie użytkownika ŚKUP 1.5 stosowne informacje w związku z ich użyciem. Czas operacji od przytknięcia identyfikatora do jej akceptacji lub odmowy akceptacji zgodnie z zadeklarowanym w formularzu ofertowym (nie dłuższym niż 2 sekundy).

6.3.1.3 Zestawienie ilościowe

Wykaz obecnie eksploatowanej infrastruktury pojazdowej zawiera załącznik nr 3.3 „Zestawienie Pojazdów”. Z uwagi na ciągłą eksploatację oraz podejmowanie decyzji przez operatorów o wycofaniu lub zakupie nowego taboru załącznik ten może ulec zmianie.

Wykonawca zmodernizuje sprzęt w zakresie opisanym w OPZ Zestawienie ilościowe obecnie eksploatowanego sprzętu w pojazdach:

Lp.	Typ urządzeń ŚKUP/producent/model	Liczba [szt.]
1	UKP_A – model AEP CDB6	1562
2	UKAS_A – model AEP F240B (dualny)	1539
3	UKAS_B – model AEP F3A	3865
4	UKP_B – model AEON RTC-1200SK	190
5	UKAS-EMV - Mikroelektronika CVB48.TY (EMV)	560

Tabela 8. Ilość urządzeń pojazdowych

6.3.2 Kontrolerka (UKNT)

Zamawiający w ramach systemu ŚKUP eksploatuje 180 urządzeń kontrolerskich firmy PAX model A920, z czego 170 sztuk pełni rolę urządzeń kontrolerskich z możliwością wnoszenia opłat dodatkowych kartami płatniczymi, natomiast 10 sztuk zostało zainstalowanych w Punktów Obsługi Pasażera, gdzie przy ich użyciu są przyjmowane i rozpatrywane reklamacje (pełnią tam rolę

tokenizatora kart płatniczych). Wszystkie ww. urządzenia zostały dostarczone w ramach tzw. „Systemu dla MZK” i są eksploatowane przez Zamawiającego od lutego 2020 r.

Wykonawca będzie musiał zapewnić ciągłe, nieprzerwane funkcjonowanie wszystkich funkcjonalności (np. zapewnienie płatności EMV) i podzespołów, łącznie z wymianą (w trybie serwisowym) komponentów, które ulegną zużyciu. Wykonawca będzie zobowiązany do wymiany ww. elementów na każdy wniosek Zamawiającego. Wykonanie powyższych czynności nie będzie stanowić dodatkowego wynagrodzenia dla Wykonawcy i muszą być one uwzględnione w ofercie Wykonawcy.

Urządzenie kontrolerskie umożliwia kontrolę ważności biletów okresowych, opłat za przejazdy jednorazowe, kontrolę opłat za przejazdy dodatkowe (bagaż, dodatkowa osoba) dla danego identyfikatora zdefiniowanego na koncie centralnym lub zapisanych na karcie ŚKUP, w czasie zbliżonym do rzeczywistego. Wyniki kontroli po zakończeniu sesji kontroli w danym pojeździe są automatycznie wysyłane do Aplikacji Obsługi Żądań. Dane powinny być dostępne w postaci zdefiniowanych raportów w module AOZ oraz przesyłane w czasie zbliżonym do rzeczywistego do ww. modułu. Dane z kontroli tj. informacja o skontrolowanym identyfikatorze muszą również zostać zapisane na koncie IKU użytkownika i będą dostępne zarówno w APK i MOB.

6.3.2.1 Procesy

a) Logowanie

Urządzenie kontrolerki uniemożliwia dostęp osobom postronnym do funkcji odczytu identyfikatorów powiązanych z kontem pasażera. Do uruchomienia odczytu kart pasażerów wymagane jest zalogowanie się poprzez podanie loginu tzn. numeru służbowego kontrolera oraz hasła. Login to co najmniej czteroznakowy ciąg cyfr, przy czym dopuszcza się, że pierwszą cyfrą może być „0” (zero) lub puste miejsce. Zamawiający dopuszcza hasło składające się tylko z cyfr, jednak ich ilość nie powinna być mniejsza niż sześć (zgodnie z wytycznymi po przeprowadzeniu analizy ryzyka). Wprowadzenie czterech znaków loginu (wypełnienie pola login) powinno bez względu na poprawność przenosić automatycznie do następnego pola tj. hasło. Jeśli Zamawiający zdecyduje się na cyfry w loginie i/lub hasle, pola do wpisywania powinny automatycznie zmieniać zakres wyświetlanych na klawiaturze ekranowej znaków. Trzykrotne błędne wprowadzenie hasła, skutkuje zablokowaniem urządzenia oraz wygenerowaniem odpowiedniego alarmu w aplikacji AOZ – UKNT, odblokowanie urządzenia może nastąpić tylko przez operatora AOZ-UKNT.

b) Urządzenie gotowe do pracy

Od momentu uruchomienia systemu operacyjnego urządzenie ma być gotowe do pracy w czasie nie dłuższym niż 60 sekund, tj. ma umożliwić wpisanie loginu i hasła. Po tej operacji kontroler ma mieć możliwość wprowadzenia danych inspekcyjnych i w ciągu kilku następnych sekund (max 5 sekund) urządzenie ma pozwolić odczytywać karty pasażerów.

Gotowość urządzenia powinna być rozumiana jako:

- pobranie aktualnych rozkładów jazdy dla wszystkich przewoźników obsługujących linie komunikacyjne GZM/ZTM ;
- pobranie Blue-List;

- pobranie Black-List;
- pobranie Stop-List;
- pobranie wszelkich innych danych niezbędnych do prawidłowego prowadzenia kontroli w pojazdach.

Powyższe pakiety danych powinny być uaktualniane on-line w tle działającego urządzenia nie rzadziej niż co 5 minut.

W przypadku braku połączenia kontrolerki z systemem centralnym urządzenie ma umożliwiać rozpoczęcie pracy w trybie autonomicznym, obejmującym pełen zakres funkcjonalności.

Urządzenie posiadają funkcjonalność powiadamiania kierownika/administradora o potencjalnym zagrożeniu i jest ona realizowane poprzez tzw. przycisk antynapadowy (funkcjonalność realizowana poprzez ekran dotykowy).

c) Wprowadzanie danych inspekcyjnych

Komputer pokładowy (UKP) ma zapewnić urządzeniu kontrolerka (UKNT) bezpośrednie przesłanie danych inspekcyjnych, tj. rodzaju środka transportu (autobus, tramwaj, trolejbus), numeru bocznego pojazdu, numeru linii komunikacyjnej, numeru kursu, daty wykonywania pracy przewozowej przez pojazd, kierunek, przystanek, danych o wykonanych transakcjach identyfikatorami. W czasie trwania kontroli w danym pojeździe urządzenie ma wskazywać aktualny przystanek. Ma on być na bieżąco automatycznie aktualizowany zgodnie z lokalizacją pojazdu. Można wykorzystać w tym celu łączność 3G/4G lub inne zaproponowane przez Wykonawcę medium transmisyjne, kompatybilne z dostępnymi urządzeniami, zapewniające bezpieczeństwo i niezawodność transmisji.

W wyjątkowych sytuacjach wykorzystuje się możliwość ręcznego wprowadzenia danych inspekcyjnych. Funkcja umożliwia wybór pojazdu (środka trakcyjnego: autobus, tramwaj, trolejbus, pociąg), np. w postaci napisu lub ikon. Dopuszcza się wpisanie ręczne numeru linii lub wyboru z listy oraz wpisanie ręczne numeru bocznego pojazdu. Dostępne kierunki jazdy oraz przystanki i godziny odjazdu dla danej linii powinny być wyświetlane w postaci listy wyboru. Kolejność ustalanych parametrów powinna być następująca: środek trakcyjny, numer linii, kierunek jazdy, przystanek, godzina odjazdu z wybranego przystanku, numer boczny pojazdu. Po wybraniu wszystkich koniecznych parametrów kursu urządzenie powinno być gotowe do weryfikacji uprawnień przejazdowych w ciągu max 5 sekund. Kontroler ma mieć możliwość przełączać się między kolejnymi przystankami z linii za pomocą przycisków „dalej” i „wstecz”, np. w postaci strzałek.

Podczas prowadzenia kontroli w danym pojeździe i blokadzie kasowników nie może być możliwości wniesienia opłaty za przejazd. Sposób blokowania kasowników proponuje Wykonawca.

d) Przyłożenie identyfikatora

Przyłożenie karty ŚKUP lub innego identyfikatora uruchamia zapytanie do Indywidualnego Konta Użytkownika i ma powodować wyświetlenie biletów. W przypadku biletów imiennych mają zostać wyświetlone dane użytkownika (imię, nazwisko, zdjęcie, rodzaj i czas obowiązywania zdefiniowanej ulgi oraz czy ulga została autoryzowana przez personel ZTM). W przypadku wskazania ulgi z informacją o braku autoryzacji przez personel ZTM biletu ulgowego i braku wgranej ulgi na karcie ŚKUP, pasażer musi okazać dokument uprawniający do ulgi. Kontroler może autoryzować ulgę w systemie, łącznie z

uzupełnieniem danych na jej temat (dane słownikowe dot. ulg, data ważności ulgi – okno kalendarza). Dane dotyczące przeprowadzonej autoryzacji ulgi, muszą trafić do systemu centralnego.

W przypadku biletu imiennego jeśli zdjęcie nie zostało zautoryzowane przez personel ZTM, wówczas w oparciu o dokument tożsamości potwierdzający wizerunek użytkownika, kontroler ma mieć możliwość potwierdzenia/autoryzacji danych, co musi zostać odnotowane w systemie centralnym. Przy kolejnej kontroli użytkownik nie będzie musiał posiadać dowodu tożsamości (po zautoryzowaniu zdjęcia).

W przypadku braku biletów powinien być wyświetlany komunikat: „Brak ważnych biletów na przejazd”.

Jeżeli karta jest na Black-Liście powinien zostać wyświetlony stosowny komunikat, np. „Karta na Black-Liście”.

Jeżeli karta jest na Stop-Liście powinien zostać wyświetlony stosowny komunikat, np. „Karta na Stop-Liście”.

Jeżeli proces odczytu karty (karty inspekcyjnej ŚKUP, karty ŚKUP, innego identyfikatora zakończy się niepowodzeniem (błąd odczytu, timeout odczytu danych karty), powinien być wyświetlany komunikat „Błąd odczytu karty”.

Powyższe komunikaty są propozycją, a ostateczny ich kształt Wykonawca ma uzgodnić z Zamawiającym.

W przypadku kontroli negatywnej kontroler powinien mieć możliwość wyboru powodu nieważności biletu np. poprzez zaznaczenie pola typu „radio button” lub innego pola wyboru zaproponowanego przez Wykonawcę. Zamawiający określi powody nieważności biletu - powyższe parametry powinny być w definiowane przez administratora AOZ i dystrybuowane na urządzenia kontrolerskie z poziomu AOZ bez konieczności zmiany (kolejnej iteracji wersji) oprogramowania kontrolerki.

Wstępną ocenę ważności przejazdu urządzenie ma przeprowadzać automatycznie, pozostawiając kontrolerowi podjęcie ostatecznej decyzji.

Jeżeli do weryfikowanego identyfikatora jest przypisana e-portmonetka, to urządzenie ma prezentować ilość środków na niej zgromadzonych.

Każdy bilet powiązany z identyfikatorem przedstawiony kontrolerowi ma być oznaczony kolorem, tzn:

Bilety oznaczone kolorem zielonym: ważne w kontrolowanym pojeździe ze względu na przebieg trasy, ważne w danej strefie taryfowej, ważne w dacie, godzinie i minucie kontroli ze względu na czas ważności biletu oraz bilety ulgowe nie wymagające konieczności weryfikacji dokumentów uprawniających do przejazdów ulgowych lub bezpłatnych.

Bilety oznaczone kolorem żółtym: ważne w kontrolowanym pojeździe, ale wymagające weryfikacji dokumentów uprawniających do przejazdów ulgowych lub bezpłatnych.

Bilety oznaczone kolorem szarym: bilety skasowane w ostatnich 2 godzinach lub których ważność upłynęła w ostatnich 2 godzinach.

Bilety oznaczone kolorem czerwonym: bilety nieważne, bilety przeznaczone do aktywacji.

Bilety mają być opatrzone piktogramem jednoznacznie określającym środek lokomocji w jakim/jakich obowiązują. Ponadto wyświetlane są podstawowe informacje o bilecie: ilość biletów każdego rodzaju (przynajmniej wtedy, jeśli ilość jest większa od 1 sztuki), data i godzina zakupu/skasowania, data i godzina upływu ważności biletu, rodzaj biletu, pochodzenie biletu: system ŚKUP 1.5 (MTC-magazyn) lub system zewnętrzny (eMagazyn) będącymi niezależnymi dystrybutorami biletów i taryfy, nominał oraz jednoznaczne określenie, czy jest to bilet normalny czy ulgowy. Jeśli dany bilet obowiązuje w określonej strefie, to taka informacja powinna być wyświetlana kontrolerowi.

Bilety na liście mają być sortowane według powyższych statusów/kodów kolorystycznych w następującej kolejności od góry: zielony, żółty, niebieski, szary, czerwony. Lista biletów, jeżeli nie mieści się na ekranie (co powinno być kontrolerowi sygnalizowane pionowym paskiem lub strzałkami), ma być przewijana poprzez skrołowanie listy.

Wszelkie komunikaty wyświetlane przez kontrolerkę muszą być uzgodnione z Zamawiającym i muszą być raportowane w AOZ. Zamawiający nie dopuszcza do sytuacji kontaktu identyfikatora z kontrolerką i wyświetlenia komunikatu, o którym nie będzie informacji w AOZ.

Każdy kontakt kontrolerki z dowolnym identyfikatorem ma mieć odzwierciedlenie w raportach dedykowanych dla kontroli biletów oraz w Indywidualnym Koncie Użytkownika wraz z prezentowanymi na kontrolerze biletami i ich szczegółami.

Każdy wynik kontroli wraz z numerem oraz rodzajem opłaty ma mieć odzwierciedlenie w raportach dedykowanych dla kontroli biletów.

Dane dot. kontroli powinny mieć odzwierciedlenie w historii konta IKU i raportach użycia karty/identyfikatora.

e) Odczyt kodu QR wbudowaną w urządzenie kamerą

Po wejściu w opcję Odczyt kodu QR, następuje automatyczne przełączenie aplikacji w tryb odczytu kodu QR, wydrukowanego na legitymacji osoby niepełnosprawnej, wbudowanym w urządzenie aparatem fotograficznym, w celu rozszyfrowania zakodowanych informacji o numerze PESEL, symbolu przyczyny niepełnosprawności, stopniu niepełnosprawności i numerze legitymacji. Aplikacja korzysta z fabrycznego oprogramowania aparatu fotograficznego w urządzeniu. Oprogramowanie aparatu po wycelowaniu na kod QR (kod QR musi znaleźć się w prostokącie zaznaczonym żółtymi narożnikami na ekranie) automatycznie wykona czytanie kodu QR i przejdzie do ekranu prezentacji zawartości kodu QR. Możliwe jest cofnięcie się z tego ekranu do aplikacji poprzez naciśnięcie systemowej ikony powrotu: (na przykład w sytuacji rezygnacji z odczytu kodu QR lub w sytuacji, kiedy nie udaje się odczytać kodu QR). Wynik kontroli powinien być wyświetlany w przejrzysty sposób na ekranie urządzenia. Ponadto z ekranu wyniku skanowania, ma być możliwość wystawienia opłaty dodatkowej (wszystkie rodzaje).

Możliwe ma być także odczytanie innych kodów QR, np. nadrukowanych na biletach papierowych (opcja realizowana w ramach godzin rozwojowych), identyfikatorach, z legitymacji szkolnych i studenckich itp., kodów z aplikacji mobilnych własnych Zamawiającego (MOB), z aplikacji mobilnych dostawców zewnętrznych np. SkyCash, mPay, Mobilet, itp., którzy korzystają z systemu eMagazyn.

Kontrolerka musi zostać zintegrowana z zewnętrznym systemem eMagazyn w zakresie obsługi QR kodów generowanych przy sprzedaży biletów w aplikacjach mobilnych. Minimalny zbiór odczytanych danych powinien umożliwiać kontrolerowi ocenę, czy pasażer przedstawiający kod do zeskanowania posługuje się ważnym uprawnieniem na przejazd, czy też nie. Wstępną ocenę ważności przejazdu urządzenie ma przeprowadzać automatycznie, pozostawiając kontrolerowi podjęcie ostatecznej decyzji.

Wynik kontroli wraz ze szczegółami identyfikującymi pojazd, w którym była prowadzona kontrola oraz ze szczegółami kontrolowanego identyfikatora ma mieć odzwierciedlenie w dedykowanych raportach kontroli.

f) Parametry opłaty dodatkowej

Kontroler w zależności od posiadanych przez pasażera biletów lub dokumentów uprawniających do przejazdu ulgowego lub bezpłatnego decyduje o wyniku kontroli. Jeśli wynik kontroli jest negatywny, należy wybrać z rozwijalnej listy odpowiednią kombinację parametrów spośród podanych poniżej.

Każda zastosowana kombinacja parametrów opłaty powoduje automatyczne wyliczenie ostatecznej ceny opłaty dodatkowej zdefiniowanej w Module Taryf i Cenników z opcją zmiany w AOZ dla opłaty kredytowej są następujące:

- opłata kredytowa-pasażerska+przewoźne normalne;
- opłata kredytowa-pasażerska+przewoźne ulgowe;
- opłata kredytowa-bagażowa+przewoźne normalne.

Do powyższych opłat może być dodatkowo wystawiona opłata policyjna. Do niej nie nalicza się przewoźnego.

Zdefiniowane w MTC opłaty gotówkowe z dozwolonymi kombinacjami przewoźnego z opcją zmiany w AOZ są następujące:

- opłata gotówkowa-pasażerska+przewoźne normalne;
- opłata gotówkowa-pasażerska+przewoźne ulgowe;
- opłata gotówkowa-bagażowa+przewoźne normalne.

Zdefiniowane w MTC opłaty uiszczone kartą płatniczą z dozwolonymi kombinacjami przewoźnego z opcją zmiany w AOZ są następujące:

- opłata uiszczona kartą płatniczą-pasażerska+przewoźne normalne;
- opłata uiszczona kartą płatniczą-pasażerska+przewoźne ulgowe;
- opłata uiszczona kartą płatniczą-bagażowa+przewoźne normalne.

Powyższe parametry wraz z wartościami powinny być w łatwy sposób definiowane przez administratora MTC i dystrybuowane na urządzenia kontrolerskie z poziomu AOZ bez konieczności zmiany (kolejnej iteracji wersji) oprogramowania kontrolerki. Wszystkie wymienione powyżej opłaty powinny zostać wydrukowane z urządzenia kontrolerki. Szczegóły zakresu wydruków do ustalenia z Zamawiającym.

Opłata dodatkowa powinna mieć charakter transakcji koszykowej, tj. powinna być widoczna w raportach finansowych z podziałem na dwie wartości (dwa kody usług):

- zasadniczą kwotę opłaty dodatkowej oraz
- przewoźne.

Ponadto w raportach finansowych powinien być widoczny numer opłaty dodatkowej, rodzaj opłaty, oraz numer kontrolera.

g) Wprowadzanie danych pasażera (dot. opłat kredytowych pasażerskich i bagażowych)

Na ekranie prezentującym wyniki kontroli oraz na ekranie wyświetlanym po wprowadzeniu danych inspekcyjnych pojazdu ma być udostępniona funkcja wypisywania opłaty dodatkowej. Kontroler ma mieć możliwość po numerze PESEL wywołania usług przeszukujących bazę „gapowiczów” oraz bazę kont imiennych IKU i jeśli pod danym numerem są już zarejestrowane dane pasażera mają one zostać zaprezentowane z możliwością edycji (jeżeli dane z bazy mandatów i kont IKU różnią się od siebie to dla tych pól powinno zostać wybrane domyślnie pole z rekordu o nowszej dacie aktualizacji). Kontroler po weryfikacji danych spisywanego pasażera, wysyła do systemu opłatę dodatkową wraz z danymi osobowymi. Opłata jest rejestrowana i widoczna w AOZ (dane osobowe nie są widoczne), a dane osobowe zasilają plik bazy danych pasażerów (eksport do systemu po stronie Zamawiającego) w taki sposób, że rekordy, w których nie dokonano zmian są odmiennie oznaczane od rekordów wymagających modyfikacji po stronie oprogramowania ZTM.

W przypadku, kiedy kontroler nie uzyska informacji o występowaniu danych pasażera w bazie (np. z powodu braku zasięgu sieci 4G/LTE, braku pasażera w bazie), istnieje możliwość ich ręcznego wprowadzenia w formularzu opłaty dodatkowej.

Wprowadzanie danych adresowych pasażera ma usprawnić planowane zaimplementowanie rejestru urzędowego pn. TERYT. Identyfikatory rejestru TERYT stanowią obowiązujący standard identyfikacji terytorialnej dla organów prowadzących urzędowe rejestry i systemy informacyjne administracji publicznej i stosowane w innych ewidencjach, rejestrach i systemach odnoszących się do jednostek terytorialnych, umożliwiają integrację danych gromadzonych w tych systemach. Wspomaganie polega na tym, że po wpisaniu pierwszej litery w danym polu pojawia się kilkupozycyjna lista wyboru sortowana alfabetycznie, a po wpisaniu kolejnych znaków lista dostępnych wartości jest odpowiednio dopasowywana.

Po wpisaniu nazwy miasta mają być dostępne tylko takie nazwy ulic, które są w granicach administracyjnych miasta lub po wpisaniu kodu pocztowego - lista ulic podlegająca pod dany kod pocztowy.

h) Wprowadzanie danych pasażera – opłata policyjna

Podczas wypisywania opłaty kredytowej pasażerskiej oraz opłaty kredytowej bagażowej ma być udostępniona możliwość opcjonalnego automatycznego wypełnienia danych pasażera dla opłaty kredytowej policyjnej. Jeśli kontroler wypisał ręcznie lub pobrał z systemu dane pasażera, to ma mieć możliwość opcjonalnego wydrukowania opłaty policyjnej bez konieczności ponownego wypisywania tych samych danych osobowych. Numeracja opłaty policyjnej ma być powiązana w systemie z numeracją opłaty kredytowej pasażerskiej lub bagażowej.

i) Zgłaszanie nieprawidłowości w pojazdach

Kontroler ma mieć możliwość zgłoszenia nieprawidłowości stwierdzonych w pojeździe (słownik nieprawidłowości do zaciągnięcia z Busmana 240 CB oraz możliwość ręcznego definiowania) lub w obsłudze linii poprzez sporządzenie krótkiej treści tekstowej oraz ma mieć możliwość załączenia zdjęć oraz wysłania niniejszego zgłoszenia do zewnętrznego modułu będącego w posiadaniu Zamawiającego. Wgląd w tego typu zgłoszenie powinien mieć także pracownik z uprawnieniem kierownik/administrator.

Powiązania do innych modułów ŚKUP 1.5:

- Modułu taryf i cenników (MTC);
- Powiązanie do bazy transakcyjnej (MRTT);
- Kont pasażerów i identyfikatorów;
- Komputera pokładowego (UKP);
- Kasownik UKAS, UKAS-EMV;
- Modułu MAR;
- Moduł Wymiany Danych (MWD);
- Modułu AOZ-UKNT.

Zewnętrzne systemy

Oczekuje się integracji z wykorzystaniem AOZ-UKNT w celu wymiany danych z systemami zewnętrznymi:

- System windykacyjny z bazy danych dłużników;
- Program Busman 240 CB, Busman 240, bazy danych operatorów celem wprowadzania danych inspekcyjnych (w zakresie opisanym w pkt. i);
- eMagazyn (m.in. walidacja biletów z QR kodem i funkcjonalność Push);
- Zewnętrzny moduł mapowy;
- Rejestr TERYT.

6.3.2.2 Mobilna Aplikacja Kontrolera (MIA) Kolei Śląskich (KŚ)

Górnośląsko-Zagłębiowska Metropolia, Zarząd Transportu Metropolitalnego oraz Koleje Śląskie wprowadziły na obszarze swojego działania wspólny bilet pn. Metrobilet. Jest to bilet miesięczny uprawniający do odbywania wielokrotnych przejazdów na terenie objętym zasięgiem działania ZTM w autobusach, tramwajach, trolejbusach i pociągach Kolei Śląskich. Bilet jest sprzedawany w ramach Systemu Śląskiej Karty Usług Publicznych i nagrywany na kartę ŚKUP. Kontrola biletu w pojazdach ZTM odbywa się przy pomocy aplikacji kontrolerskiej zainstalowanej na urządzeniu PAX A920. Natomiast konduktorzy w pociągach Kolei Śląskich są wyposażeni w urządzenia kontrolerskie JZIOT V9000 z dedykowaną Mobilną Aplikacją Kontrolerską (MIA v 2.3) dostarczoną w ramach systemu ŚKUP.

Obowiązkiem Wykonawcy w ramach przedmiotowego zamówienia jest modyfikacja oprogramowania MIA, tak aby umożliwiała ona odczytywanie identyfikatorów użytkowników zdefiniowanych na kontach pasażerów i odczytywania za ich pomocą ww. urządzeń, w celu weryfikacji czy pasażer ma

zakupione Metrobiletu. MIA w ŚKUP 1.5 ma być dostosowana przez Wykonawcę do nowej architektury systemu i ma mieć możliwość połączenia z usługami nowego systemu centralnego celem zapewnienia poprawnej pracy. Zamawiający oczekuje, aby wszystkie funkcjonalności nowej aplikacji zawsze funkcjonowały w połączeniu z systemem centralnym – w odróżnieniu do obecnie wykorzystywanej aplikacji. Tym samym nie zakłada się prowadzenia kontroli w trybie off-line. Istotnym jest, aby w zaproponowanej przez Wykonawcę nowej wersji MIA dla ŚKUP 1.5 nie uległa zmianie szata graficzna i rozmieszczenie najczęściej wykorzystywanych funkcji.

Obecnie aplikacja MIA stanowi autonomiczne rozszerzenie aplikacji sprzedażowej KŚ o możliwość kontrolowania Metrobiletów zakodowanych na Kartach ŚKUP. Aplikacja sprzedażowa KŚ **nie podlega modyfikacji** w ramach przedmiotowego zamówienia.

W ramach rzeczzonego zamówienia Wykonawca nie jest zobowiązany do wymiany, a tym samym dostawy urządzeń kontrolerskich dla Kolei Śląskich, Wykonawca zmodernizuje lub wymieni oprogramowanie MIA, dostosowując jego funkcjonalność do pracy w systemie ŚKUP 1.5.

Zamawiający posiada prawo do modyfikacji oraz dokumentację techniczną oprogramowania MIA.

1. Informacja o obecnej funkcjonalności aplikacji MIA:

- Mobilna Aplikacja Kontrolera umożliwia wykonanie procesu kontroli uprawnień na przejazd realizowany w oparciu o tzw. „Metrobilet” zakupiony w sieci sprzedaży Śląskiej Karty Usług Publicznych;
- Aplikacja funkcjonuje w dwóch trybach: offline – nie wymagającym dostępu do sieci oraz online – wymagającym dostępu do sieci. Oznacza to, że aplikacja potrafi funkcjonować w trybie bez stałego dostępu do sieci umożliwiając weryfikację, czy pasażer posługujący się Kartą ŚKUP posiada zakupiony Metrobilet;
- W sytuacjach specyficznych – upłynęło mało czasu pomiędzy zakupem biletu, a kontrolą biletu – może być niezbędne odczytanie kompletu danych z karty;
- Aplikacja w trybie online aktualizuje informacje z systemem. Oznacza to, że w celu utrzymania aktualności danych w aplikacji, a także w systemie - wymagany jest dostęp do sieci;
- Aplikacja obsługuje tylko jeden rodzaj użytkownika – kontroler;
- Instalacja i pierwsze uruchomienie aplikacji wymagają dostępu kontrolerki do sieci Internet i synchronizowanie danych z systemem (tj. pobranie znacznej ilości danych);
- Połączenie internetowe w kontrolerze realizowane jest w ramach prywatnego APN.

Podczas każdego uruchomienia aplikacji sprawdzany jest jej dostęp do sieci Internet. Pozytywna weryfikacja dostępu przełącza aplikację w tryb online i uruchamia proces aktualizacji danych. Wówczas następuje synchronizacja z systemem w zakresie:

- Operatorów – Konduktorów KŚ;
- Black-List – listy identyfikatorów zastrzeżonych i zablokowanych w systemie;
- Blue-List – zakupionych Metrobiletów za pomocą portalu klienta ŚKUP;
- Definicji biletów – listy Metrobiletów oraz ich parametrów;
- Słowników – wartości niektórych słowników systemowych koniecznych do interpretacji Blue-List i Metrobiletów;
- Aktywnych kontraktów - zakupionych Metrobiletów, które zostały zapisane na karcie.

Podczas uruchamiania aplikacji, do systemu wysyłane zostają (do tej pory nieprzesłane) informacje o wykonanych kontrolach w ramach sesji kontroli. Pozytywna synchronizacja kończy się wyświetlaniem stosownego komunikatu. W przypadku braku dostępu do Internetu pojawi się ekran negatywnej synchronizacji. Negatywna synchronizacja ze względu na obsługiwany tryb offline nie przeszkadza w kontynuowaniu pracy z aplikacją.

Powyższe pakiety danych powinny być uaktualniane on-line w tle działającego urządzenia nie rzadziej niż co 5 minut.

Podstawowe funkcje obecnego oprogramowania MIA:

Dostęp do wszystkich funkcji aplikacji wymaga poprawnej weryfikacji użytkownika w procesie logowania. Użytkownik wprowadza 5-znakowy login oraz 4-znakowe hasło. Użytkownik ma możliwość zapamiętania ostatnio wprowadzanego loginu co powoduje, że kolejne uruchomienia aplikacji nie będą wymagały podawania loginu, a jedynie wprowadzenie hasła.

Po poprawnym zalogowaniu, aplikacja udostępnia użytkownikowi ekran panelu centralnego oznaczony loginem użytkownika, na którym znajdują się poszczególne funkcje aplikacji:

- Rozpocznij kontrolę – funkcja umożliwiająca rozpoczęcie sesji kontroli w pociągu oraz przeprowadzanie poszczególnych kontroli Metrobiletów pasażerów pociągu;
- Rozpocznij kontrolę (wyświetlane opcjonalnie w przypadku wykrycia przez aplikację niezamkniętej poprzedniej sesji kontroli) – funkcja umożliwiająca wznowienie niezamkniętej wcześniej sesji kontroli w pociągu lub zamknięcie poprzedniej sesji kontroli i uruchomienie nowej sesji kontroli w pociągu;
- Informacje - funkcja umożliwiająca podgląd najważniejszych informacji o statusie aplikacji;
- Wyloguj – funkcja umożliwiająca wylogowanie użytkownika z aplikacji.

1.1 Sesja kontroli oraz kontrole Metrobiletów

Wybranie przez użytkownika funkcji rozpocznij kontrolę, umożliwia rozpoczęcie sesji kontroli we wskazanym pociągu. W pierwszym kroku należy wprowadzić (zgodnie z formatem XXXXX lub XXXXX/X) numer pociągu, w którym będzie odbywała się kontrola. Na ekranie umożliwiającym wprowadzenie numeru będą podpowiadane przez aplikację ostatnio wprowadzane przez użytkownika numery pociągów. Wprowadzenie numeru niezgodnego z formatem spowoduje wyświetlanie komunikatu błędu. Wprowadzenie poprawnego numeru pociągu powinno zostać zatwierdzone przez użytkownika kliknięciem przycisku OK, co powoduje uruchomienie synchronizacji danych i przejście do funkcji kontroli biletów. Wybranie ikony spowoduje powrót do panelu centralnego aplikacji. Każda sesja kontroli powinna się zakończyć jej zamknięciem, co umożliwi przesłanie informacji o kontrolach do systemu centralnego. W przypadku niezakończenia poprzedniej sesji kontroli, po rozpoczęciu kolejnej kontroli, wyświetlany jest komunikat o niezakończonych sesji kontroli i możliwe są następujące akcje:

- Wznowienie niezamkniętej wcześniej sesji kontroli w pociągu, co powoduje przejście do ekranu kontroli identyfikatorów;
- Zamknięcie poprzedniej sesji kontroli i uruchomienie nowej sesji kontroli w pociągu, co powoduje przejście do ekranu rozpoczynania sesji kontroli.

Po poprawnym rozpoczęciu sesji kontroli, uruchomiona zostaje funkcja NFC, a urządzenie jest przygotowane do odczytywania Kart ŚKUP i innych identyfikatorów. Przyłożenie identyfikatora kontrolowanego pasażera spowoduje odczytanie informacji o Metobiletach pochodzących z systemu centralnego i wyświetli ekran szczegółów Metrobiletów. Jeżeli podczas zamykania sesji kontroli kontrolerka nie ma dostępu do sieci, to dodatkowo pojawia się komunikat informujący, że dane dotyczące przeprowadzonych kontroli nie mogą zostać zapisane w systemie. Aplikacja będzie przechowywała dane do czasu pojawienia się takiej możliwości. Na ekranie panelu centralnego będzie widoczna kafelka informująca o potrzebie synchronizacji.

Każdy Metrobilet charakteryzuje się informacjami dotyczącymi:

- Strefy biletu oznaczonej odpowiednio kolorem nagłówka Metrobiletu;
- Nazwy biletu – kod Metrobiletu pobrany z systemu;
- Stacji granicznej;
- Końca ważności – data i czas końca ważności Metrobiletu;
- Początku ważności – data i czas od kiedy ważny jest Metrobilet;
- Ceny – cena zakupu Metrobiletu.

Konduktor po zapoznaniu się z informacjami wyświetlanymi o danym Metrobilecie decyduje, czy bilet w danym pociągu jest ważny czy też nie i dalej postępuje zgodnie z wewnętrznym regulaminem kontroli KŚ. Tym samym możliwy jest odczyt kolejnego identyfikatora z Metrobiletem w danej sesji kontroli.

1.2 Raportowanie sesji kontroli

Każda sesja kontroli powinna mieć odzwierciedlenie w systemie w dedykowanych raportach. Informacje w raportach zawierają następujące informacje:

- Data i godzina rozpoczęcia sesji kontroli;
- Login konduktora;
- Ilość sesji kontroli;
- Numery kontrolowanych pociągów;
- Data i godzina zakończenia sesji kontroli;
- Oznaczenie numeru wersji aplikacji kontrolerskiej.

Informacja o skontrolowanych Kartach ŚKUP i identyfikatorach zostaje zarejestrowana i jest dostępna w raportach w następującym zakresie:

- Data i godzina kontroli;
- Login konduktora;
- Numer karty;
- Nazwa biletu z systemu;
- Numer biletu;
- Cena biletu;
- Data rozpoczęcia obowiązywania biletu;
- Data zakończenia obowiązywania biletu;
- Strefa obowiązywania biletu.

6.3.3 Terminal Sprzedażowy (UPOS)

Terminal Sprzedażowy jest uniwersalnym mobilnym urządzeniem obsługującym identyfikatory dostępne w systemie ŚKUP 1.5, poprzez interfejs bezstykowy (NFC, z wyłączeniem aplikacji MOB i kart EMV i jej surogatów). Obecnie Zamawiający posiada 1200 szt. urządzeń typu Bitel Flex 7000 i wraz z PIN PAD-em Bitel Flex 6000, w tym eksploatowanych jest 800 sztuk, a kolejne 400 przewidziane jako urządzenia magazynowe na wymianę uszkodzonych terminali (Zamawiający przekaże Wykonawcy w depozyt urządzenia magazynowe). Wykonawca dostarczy i zainstaluje oprogramowanie realizujące funkcjonalności opisane w niniejszym dokumencie.

6.3.3.1 Procesy realizowane w Terminalach Sprzedażowych

1. Sprawdzenie stanu e-portmonetki;
2. Sprzedaż biletów i zapis informacji w koncie użytkownika (IKU)/na karcie:
 - a. Rozpoczęcie i zakończenie zmiany kasjera w punkcie sprzedaży, wpisanie hasła dostępowego, indywidualnego dla każdego użytkownika;
 - b. Anulowanie/wycofanie wykonanej transakcji, dokonanej każdą formą płatności (pomyłka sprzedawcy/klienta, rezygnacja z zakupu itp.);
 - c. Sprzedaż biletów - płatność gotówką;
 - d. Zasilenie e-portmonetki;
 - e. Funkcjonalność „koszyka zakupu” - sprzedaż wielokrotności uprawnień podczas jednej transakcji;
 - f. Możliwość powtórnego wydruku potwierdzeń z dokonanej transakcji również w przypadku awarii/zawieszenia/zresetowania terminala;
 - g. Funkcjonalność „wydruk kontrolny/Wydruk Próbnny” – wydruk prezentujący wybraną pozycję biletu do zakupu, przed dokonaniem transakcji;
 - h. Generowanie szczegółowego raportu sprzedaży z poziomu Terminala, dla operatorów w punkcie sprzedaży po zakończeniu dnia;
 - i. Generowanie ogólnego raportu sprzedaży z poziomu Terminala, dla operatorów w punkcie sprzedaży za dany dzień (lokalne przechowywanie danych przez co najmniej 7 dni);
 - j. Generowanie raportów zakończenia zmiany/zakończenia dnia.
3. Wydawanie, sprzedaż karty ŚKUP 1.5:
 - a. Sprzedaż i aktywacja kart ŚKUP 1.5 (nadawanie hasła i pinu przez użytkownika karty), pobieranie kaucji możliwe kanałami płatności: gotówka;
 - b. Akceptacja regulaminu karty;
 - c. Generowanie z systemu startowego pin-u do karty (wraz z jego wydrukiem).
4. Sprzedaż biletów papierowych drukowanych przez Terminal z kodem QR – ewentualna realizacja w ramach godzin rozwojowych;
5. Sprawdzenie informacji o IKU i jego prezentacja na ekranie Terminala:
 - a. Uprawnienia;
 - b. Zakupione bilety;
 - c. Informacja o środkach pieniężnych dostępnych na e-portmonetce;
 - d. Identyfikacja konta klienta poprzez przyłożenie identyfikatora.

6. Zarządzanie identyfikatorami (karta ŚKUP 1.5):
 - a. Zamówienie identyfikatorów dla danego terminala w punkcie sprzedaży;
 - b. Rozliczanie zamówionych identyfikatorów;
 - c. Przyjmowanie zwrotów identyfikatorów;
 - d. Wydanie identyfikatora w punkcie sprzedaży;
 - e. Zarządzanie stanem identyfikatorów w punkcie sprzedaży (raportowanie aktualnego stanu kart w punkcie).

6.3.3.2 Interfejs graficzny

Szata graficzna Terminala Sprzedażowego musi uwzględniać wszystkie jego funkcjonalności. Każda z funkcji powinna zostać umieszczona na ekranie Terminala poprzez zastosowanie odrębnych ikon, pogrupowanych tematycznie. Funkcjonalności Terminala wybierane będą na ekranie dotykowym urządzenia lub poprzez klawiaturę zintegrowaną z urządzeniem.

Sprzedaż usług komunikacyjnych/biletów stanowić będzie funkcjonalność nadrzędną, w związku z tym musi zostać w sposób wyraźny wyeksponowana za pomocą czytelnej ikony np. pod nazwą: „SPRZEDAŻ BILETÓW ZTM”.

Ponadto Terminal Sprzedażowy musi posiadać funkcjonalność wygaszania ekranu urządzenia podczas braku aktywności operatora z możliwością ustawiania czasu bezczynności parametrem.

Terminal na ekranie głównym prezentować będzie poziom naładowania baterii.

Interfejs Terminala powinien również uwzględniać prezentację wyników zrealizowanych procesów (np.: wyniki wykonania transakcji, wydania karty, rejestracji identyfikatora itp.), odrębnych dla procesów zakończonych wynikiem pozytywnym i negatywnym (komunikat, różna kolorystyka), połączonych z emisją sygnałów dźwiękowych, odmiennych dla procesów zakończonych wynikiem pozytywnym i negatywnym.

Menu ekranowe Terminala Sprzedażowego powinno być zaprojektowane i uzgodnione z Zamawiającym z zachowaniem zasad ergonomii, z maksymalną ilością informacji na pierwszym ekranie. Treść menu Terminala powinna być opracowana w języku polskim.

Oprogramowanie zainstalowane w Terminalach Sprzedażowych będzie bazować na danych pobieranych z systemu centralnego, niezbędnych do realizacji wszystkich funkcjonalności. Z drugiej strony Terminale muszą wysyłać do systemu centralnego (w trybie online lub zbliżonym do online) dane transakcyjne, celem zapisania uprawnień, kontraktów na koncie użytkownika. Dane, o których mowa powyżej, muszą być przekazywane w sposób bezpieczny i zaszyfrowany.

Wykonawca w terminie do 3 miesięcy od podpisania umowy zaproponuje Zamawiającemu układ ekranów i menu Terminali, jak i przyjęte rozwiązania zapewniające realizację funkcjonalności opisanych w niniejszym dokumencie. Zamawiający ma prawo wnieść uwagi, m.in. wpływające na funkcjonalność, ergonomię pracy użytkownika lub zdaniem Zamawiającego w lepszym stopniu zapewniające realizację wymagań Zamawiającego. Uwagi te muszą zostać uwzględnione przez Wykonawcę.

6.3.4 Stacjonarny Automat Dystrybucji i Sprzedaży (SADiS)

Zamawiający obecnie posiada i eksploatuje urządzenia następujących producentów, których szczegółowy opis techniczny zawiera **załącznik nr 2.2 Parametry Techniczne Urządzeń**:

- a. Hoeft&Wessel – 109 szt. – eksploatowane od 2014 roku;
- b. Automatikon – 14 szt. – eksploatowane od 2019 roku;
- c. Zamówienie dodatkowych max. 71 urządzeń w ramach odrębnego postępowania – od 2021 r.

Zamawiający posiada pełną dokumentację techniczną, serwisową i eksploatacyjną automatów, ich części składowych oraz instalacji sporządzonej w języku polskim.

Poza ww. automatami trwa proces certyfikacyjny automatów firmy MP Technology, Scheidt&Bachmann, które zostały zainstalowane na centrach przesiadkowych, a które docelowo będą zintegrowane z systemem ŚKUP i zostaną przekazane do eksploatacji ZTM-owi.

Obowiązkiem Wykonawcy (dotyczy tylko urządzeń Hoeft&Wessel) będzie modyfikacja obecnego oprogramowania lub dostarczenie nowego oprogramowania w zakresie AOZ oraz aplikacji zainstalowanej na urządzeniu, tak aby realizowały one funkcjonalności określone w OPZ. Zamawiający zastrzega sobie również prawo do zlecenia z wykorzystaniem godzin rozwojowych, wykonania lub modernizacji oprogramowania zainstalowanego na urządzeniach podłączanych w przyszłości do systemu. W przypadku pozostałych firm, modyfikacja oprogramowania nie leży w zakresie czynności Wykonawcy, natomiast obowiązkiem Wykonawcy będzie integracja urządzeń, ich certyfikowanie, przyłączenie oraz utrzymywanie infrastruktury serwerowej do dalszej eksploatacji wszystkich ww. urządzeń. Z tego tytułu Wykonawcy nie będzie przysługiwało dodatkowe wynagrodzenie. Wszystkie niezbędne prace, o których mowa powyżej Wykonawca jest zobowiązany wykonać w ramach realizacji przedmiotu zamówienia. Łączna liczba wszystkich Stacjonarnych Automatów Dystrybucji i Sprzedaży w systemie ŚKUP 1.5 nie przekroczy 300 sztuk.

W zakresie niniejszego zamówienia obowiązkiem Wykonawcy będzie serwisowanie obecnie funkcjonujących urządzeń (Hoeft&Wessel). Wykonawca będzie musiał zapewnić ciągłe, nieprzerwane funkcjonowanie wszystkich funkcjonalności (np. zapewnienie płatności EMV) i podzespołów, łącznie z wymianą (w trybie serwisowym) komponentów, które uległy zużyciu np.: ekran automatu (wypalenie, pożółknienie), drukarki, gilotyny, na komponenty, które są o co najmniej takich samych lub wyższych parametrach technicznych (np. ekran). Wykonawca będzie zobowiązany do wymiany ww. elementów na każdy wniosek Zamawiającego. Poza tym Wykonawca będzie zobowiązany do zmiany oznakowania automatów (logo na obudowie) na wzór uzgodniony z Zamawiającym. Ponadto na wniosek Zamawiającego Wykonawca jest zobowiązany do odpowiedniego, dostrojenia czytnika monet/banknotów, tak aby przyjmował/nie przyjmował określone nominały monet/banknotów (np. monet w obiegu, wycofanych z obiegu, „fałszywek”), a także do dostrojenia czytnika monet/banknotów w przypadku wprowadzenia do obiegu przez NBP nowych monet/banknotów, jak również w przypadku stwierdzenia niskiego poziomu przyjmowania monet/banknotów, w tym również dostosowanie oprogramowania do obsługi Euro w przypadku jej wprowadzenia.

Ww. czynności nie będą stanowić dodatkowego wynagrodzenia dla Wykonawcy i muszą być uwzględnione w ofercie Wykonawcy.

6.3.4.1 Wymagania funkcjonalne Stacjonarnych Automatów Dystrybucji i Sprzedaży

Stacjonarne Automaty Dystrybucji i Sprzedaży powinny posiadać co najmniej następujące funkcje:

- a. Wydawanie za kaucją oraz aktywowanie elektronicznych kart ŚKUP 1.5, z interfejsem bezstykowy zgodnym z ISO 14443, interfejs stykowy zgodny z PN-EN ISO/IEC 7816);
- b. Sprawdzenie danych przypisanych do konta użytkownika, m.in.: okresu ważności i rodzaju biletu, zapisanych ulg, historii 10 ostatnich transakcji;
- c. Prezentacja loginu do konta IKU dla pasażera posługującego się obsługiwany przez SADiS identyfikatorem, zakończona jego wydrukowaniem lub wygenerowaniem kodu QR;
- d. Zasilenie e-portmonetki dostępnymi w SADiS formami płatności;
- e. Prezentacja salda e-portmonetki;
- f. Sprzedaż biletów papierowych według zdefiniowanego wzoru, w którym ma być zawarty kod QR (kody QR w ramach godzin rozwojowych);
- g. Sprzedaż i zwrot biletów elektronicznych zapisanych na koncie użytkownika (pod warunkiem przypisania do konta użytkownika własnego rachunku bankowego, na który zostanie zrealizowany zwrot);
- h. Sprzedaż wielu biletów (różnego rodzaju) i usług w jednej transakcji (funkcja „koszyka” zakupów);
- i. Realizacja płatności poprzez przyjmowanie i wydawanie monet o nominałach 10 gr, 20 gr, 50 gr, 1 zł, 2 zł, 5 zł;
- j. Wydawanie monet za pośrednictwem zasobników do wydawania reszty (samoczynnie uzupełnianych się wrzucanymi pieniędzmi);
- k. Realizacja płatności poprzez przyjmowanie banknotów o nominałach 10 zł, 20 zł, 50 zł, 100 zł;
- l. Wykonywanie transakcji płatniczych kartami płatniczymi (Visa, Mastercard), w tym również dokonywanie płatności „zbliżeniowej” kartami typu Visa payWave i Mastercard payPass oraz surogatów tych kart (np. wirtualna karta EMV w telefonie, zegarku itp., za pośrednictwem NFC, HCE, Google Pay, Apple Pay itp.), a także wykonywanie transakcji płatniczych w systemie BLIK;
- m. Automat musi pobierać z systemu centralnego (MTC-magazynu biletów) lub eMagazynu (zewnętrzny system) serię oraz numer dla sprzedawanych biletów (do uzgodnienia z Zamawiającym);
- n. Informowanie o komunikacji miejskiej oraz rozkładach jazdy wg linii wraz z umożliwieniem wyszukiwania połączeń i podaniem obowiązującej ceny przejazdu dla wyszukanego połączenia i podaniem obowiązującej ceny przejazdu dla wyszukanego połączenia (w przypadku udostępnienia danych na stronie ZTM), obowiązujących taryfach, a także innych komunikatach informacyjnych podanych przez ZTM. Informacje mają być tożsame z tymi prezentowanymi w witrynie internetowej ZTM (mają być pobierane z tego samego źródła);
- o. Prezentowanie w czasie rzeczywistym informacji o komunikacji miejskiej pobieranych z Systemu Dynamicznej Informacji Pasażerskiej (SDIP) na ekranie automatu. Informacje te mają być wyświetlane na wygaszaczu ekranu w czasie, gdy automat nie jest użytkowany (o ile Zamawiający nie zdefiniuje innej treści wygaszacza) oraz na żądanie użytkownika po wyborze przez niego stosownej opcji na ekranie automatu. W przypadku wyświetlania informacji SDIP na wygaszaczu ekranu, wygaszacz powinien jednocześnie wyświetlać informację o konieczności wzbudzenia automatu poprzez dotknięcie ekranu (dane pozyskiwane z systemu SDIP przy użyciu udostępnionych Web Services);
- p. Obowiązkiem Wykonawcy (po konsultacji z Zamawiającym) będzie wprowadzenie ograniczeń płatności dużymi banknotami za bilety o niewielkich nominałach. Podczas wykonywania

- transakcji, na ekranie ma być prezentowana czytelna dynamiczna informacja dla pasażera, jakimi nominałami może dokonać płatności;
- q. Każda transakcja finansowa musi być oznaczona unikatowym identyfikatorem (GIT);
- r. Automat musi prowadzić rejestrację wydanych i aktywowanych kart ŚKUP. W momencie wydania karty użytkownikowi, w pamięci urządzenia ma zostać zapisany automatycznie numer wydanej i aktywowanej karty, poza tym ta informacja ma zostać przesłana do systemu centralnego;
- s. Operacja wydania karty ŚKUP 1.5 użytkownikowi przez automat, musi być zakończona nadaniem startowego numeru PIN, wydrukowanego na potwierdzeniu;
- t. Możliwość prezentowania na ekranie wygaszacza dowolnych treści tekstowych, graficznych oraz audio-video. Musi istnieć możliwość samodzielnego zdalnego modyfikowania tych treści;
- u. Realizacja funkcjonalności związanych z obsługą stref Park&Ride, w szczególności wydawanie użytkownikom tzw. biletów zerowych, uprawniających do parkowania na podstawie posiadanych przez nich ważnych biletów transportu publicznego przypisanych do konta użytkownika (rodzaje biletów uprawniających do biletów zerowych mają być parametrem w MTC);
- v. Oprogramowanie automatu musi umożliwiać sprzedaż papierowych biletów jednorazowych i elektronicznych biletów okresowych Zamawiającego, według różnych taryf oraz wzorów biletów. Aktualna taryfa i wzory biletów określane są każdorazowo w odrębnych dokumentach, zaakceptowanych i przyjętych przez organy Zamawiającego;
- w. W automacie muszą być przechowywane informacje o liście zastrzeżonych kart ŚKUP/identyfikatorów (tzw. czarna lista), aby niemożliwe było wykonanie żadnej operacji przy użyciu takiej karty/identyfikatora. Lista ta musi być na bieżąco aktualizowana;
- x. Menu sprzedażowe musi być dostępne w co najmniej 4 językach (polski, niemiecki, angielski, ukraiński). Wersje językowe będą oznaczone tekstowo oraz flagą kraju. Wykonawca jest zobowiązany do wykonania tłumaczeń treści prezentowanych w automacie, również w przypadku ich zmiany w trakcie trwania umowy, np. w wyniku modyfikacji oprogramowania automatu. Ponadto Wykonawca zobowiązany jest dostarczyć takie rozwiązanie, aby Zamawiający samodzielnie, bez zmian systemowych, mógł dokonywać zmian wyświetlanego na ekranie tekstu;
- y. Prowadzenie zestawień i statystyk zbiorczych i szczegółowych (raportów), z uwzględnieniem m.in. daty i godziny sprzedaży biletów/usług lub zdarzeń, z uwzględnieniem ilości oraz wartości ze względu na rodzaj. Szczegółowy zakres raportów Wykonawca uzgodni z Zamawiającym po podpisaniu umowy. Raporty powinny zawierać co najmniej informację o:
- sprzedanych biletach papierowych i elektronicznych;
 - wydanych kartach ŚKUP;
 - rejestrowanych usterkach i błędach wraz z określeniem ich rodzaju;
 - rejestrowanych statusów i stanów podzespołów automatów;
 - stanu gotówki w automacie;
 - stanu kart ŚKUP w automacie;
 - wykonanych czynnościach serwisowych przez poszczególnych pracowników, np. wymiana papieru, uzupełnienie kart ŚKUP;
 - wykonanych czynnościach związanych z obsługą gotówki, np. wymiana kasety, uzupełnienie lub opróżnienie monet do wydawania reszty w zasobnikach;

- z. Raport dotyczący czynności związanych z obsługą gotówki musi zawierać co najmniej następujące dane:
- rodzaj czynności (wymiana kasety, uzupełnienie lub opróżnienie monet do wydawania reszty w zasobnikach);
 - symbol i nazwa automatu;
 - data poprzedniej czynności;
 - data obecnej czynności;
 - ilość poszczególnych nominałów monet;
 - kwota monet;
 - ilość poszczególnych nominałów banknotów;
 - kwota banknotów;
 - numer kasety;
 - nazwa pracownika wykonującego czynność;
 - kolejny numer dokonanej czynności wymiany kasety w danym automacie.
- aa. Ww. zakres danych powinien być przesyłany automatycznie do systemu AOA (moduł zarządzania automatami), co do zasady w czasie rzeczywistym (on-line). Zamawiający ma mieć możliwość pobrania ww. informacji zdalnie z dowolnego automatu, w dowolnym momencie z wykorzystaniem różnego rodzaju filtrów, w szczególności zakresu dat, wyboru poszczególnych automatów, rodzaju biletów, rodzaju czynności serwisowej, rodzaju kanału płatności itp. (co najmniej w formacie CSV i XLSX,);
- bb. Wszelkie informacje o stanie urządzenia (poprawności działania poszczególnych komponentów), stanie monetarnym kaset końcowych, zasobników do wydawania reszty oraz powinny być na bieżąco przesyłane do systemu AOA;
- cc. Transfer danych pomiędzy automatem, a systemem AOA może odbywać się poprzez sieć LAN (podłączenie automatu z najbliższym punktem dostępowym umożliwiającym łączność internetową). W przypadku braku możliwości wykonania ww. połączenia dopuszcza się łączenie w technologii LTE lub nowszej, z komunikacją opartą o protokół TCP/IP. Za pomocą połączenia LAN lub LTE monitorowana będzie praca automatu, a w szczególności przesyłane będą raporty statystyczne oraz informacje o funkcjonowaniu urządzenia (tj. operacje serwisowe, pobranie utargu, awarie i usterki). Karty SIM oraz koszty związane z transmisją danych leżą w gestii Wykonawcy;
- dd. Logowanie w automacie będzie możliwe za pomocą identyfikatora osoby logującej się, którym może być np. karta pamięci, pendrive, Karta ŚKUP;
- ee. W automatach muszą być przechowywane dane dotyczące wszystkich transakcji (rozliczeń) za okres co najmniej ostatnich 7 dni (dotyczy danych przekazanych do systemu centralnego) oraz operacji obsługi serwisowej (naprawy, usuwanie usterek, wymiana gotówki, wymiana materiałów eksploatacyjnych) za okres co najmniej ostatnich 6 miesięcy z ich archiwizacją do systemu centralnego;
- ff. Układ graficzny ekranów, na podstawie wytycznych Zamawiającego, Wykonawca uzgodni i przedstawi do akceptacji Zamawiającemu.

6.3.4.2 Płatności

- a. Automat obsługuje transakcje realizowane za pomocą:

- Bilonu PLN;
 - Banknotów PLN;
 - Karty płatniczej/kredytowej, w tym jej surogaty (np. wirtualna karta EMV w telefonie, zegarku itp., za pośrednictwem NFC, HCE, Google Pay, Apple Pay itp.), a także wykonywanie transakcji płatniczych w systemie BLIK;
 - Karty ŚKUP w ramach e-portmonetki.
- b. System obiegu monet w automacie posiada taką konstrukcję, że zwrot monet, w przypadku rezygnacji z transakcji, przebiega w sposób kontrolowany, zapewniając wydanie tych samych pieniędzy (fizycznie te same monety/banknoty) wrzuconych przez kupującego;
- c. Automat przyjmuje monety w następujących nominałach: 10gr, 20gr, 50gr, 1zł, 2zł, 5zł. Posiada możliwość programowego włączenia lub wyłączenia dowolnego typu monet samodzielnie przez Zamawiającego;
- d. Wydawanie reszty, poprzez zasobniki do wydawania reszty, odbywa się monetami, w 6 nominałach (10gr, 20gr, 50gr, 1zł, 2zł, 5zł). Moduły do wydawania reszty posiadają pojemność 50 szt. na każdą monetę. Istnieje możliwość programowego włączenia lub wyłączenia dowolnego typu przyjmowanych monet samodzielnie przez Zamawiającego;
- e. Moduły wydawania reszty posiadają opcję samoczynnego uzupełniania się wrzucanymi przez kupującego monetami. W przypadku pełnych zasobników monety kierowane są do kasety końcowej;
- f. W przypadku braku monet do wydawania reszty automat sprzedaje bilety za odliczoną gotówkę oraz automatycznie wyświetla informację „sprzedaż tylko za odliczoną gotówkę”;
- g. Przy braku łączności dostępna jest płatność gotówką i kartą płatniczą zbliżeniowo zgodnie z limitem organizacji płatniczych;
- h. W przypadku zablokowania płatności banknotami, dostępna jest płatność bilonem;
- i. W przypadku napełnienia się kasety na monety lub kasety na banknoty w ok. 80%, automat wysyła stosowną informację do systemu AOZ. W przypadku całkowitego zapełnienia się którejkolwiek z kaset, automat automatycznie wyłącza funkcje związane z transakcjami gotówkowymi (bilon lub banknot), a w przypadku zapełnienia się obu kaset, wykonuje operacje bezgotówkowe i posiadać aktywny tryb informacyjny;
- j. Nie realizuje transakcji mieszanych (gotówkowa i bezgotówkowa) podczas wykonywania jednej operacji;
- k. Automat przyjmuje banknoty w następujących nominałach: 10zł, 20zł, 50zł, 100zł;
- l. Przy jednej transakcji istnieje możliwość dokonania płatności min. 6 banknotami;
- m. Istnieje możliwość programowego włączania i wyłączania dowolnego typu przyjmowanych banknotów samodzielnie przez Zamawiającego;
- n. Czytnik banknotów posiada taką konstrukcję, aby użytkownik w przypadku rezygnacji z transakcji otrzymał zwrot tych samych pieniędzy (fizycznie te same banknoty);
- o. Czytnik kart płatniczych i kredytowych wyposażony jest w specjalną klawiaturę służącą do wprowadzania kodu PIN dla transakcji opłacanych kartą z ułożeniem klawiszy i funkcjonalność taką jak w przypadku bankomatów;
- p. Czytnik kart płatniczych oraz kredytowych zamontowany w automacie jest zgodny ze standardem EMV, posiada certyfikację międzynarodowych organizacji płatniczych Visa i Mastercard; Wykonawca jest zobowiązany do zapewnienia zgodności terminali (czytników

kart) z wymogami organizacji kartowych Visa/Mastercard przez cały okres obowiązywania umowy na swój koszt.

- q. Czytnik kart ŚKUP realizuje algorytmy kryptograficzne 3DES, RSA, AES oraz jest zgodny z elektronicznymi kartami bezstykowymi spełniającymi następującą normę:
- ISO/IEC 14443-1,
 - ISO/IEC 14443-2,
 - ISO/IEC 14443-3,
 - ISO/IEC 14443-4.

6.3.4.3 Oprogramowanie dla serwisu

- Logowanie w automacie odbywa się za pomocą identyfikatora osoby logującej (np. pendrive, karta ŚKUP);
- Funkcje serwisowe są dostępne dopiero po właściwym zalogowaniu się w automacie;
- W automacie istnieje możliwość przeprowadzenia diagnostyki głównych elementów urządzenia (np. drukarka-wydruk próbny);
- Automat wyposażony są w pamięć umożliwiającą przechowywanie danych dotyczących wszystkich transakcji (rozliczeń) oraz operacji obsługi serwisowej (naprawy, usuwanie usterek, wymiana gotówki, wymiana materiałów eksploatacyjnych). Ww. dane powinny rejestrowane są na dwóch niezależnych układach pamięciowych (w przypadku uszkodzenia jednej z pamięci dane będą czytane z drugiego układu pamięci lub systemu AOZ);
- Moduł pamięci wyposażony jest w niezależne zasilanie, tak aby zabezpieczyć wszystkie dane przed utratą w razie zaniku napięcia lub innych zakłóceń zasilania. W przypadku awarii następuje automatyczne odtworzenie danych dot. sprzedaży, środków finansowych, nr biletów etc.
- Zamawiający posiada możliwość do samodzielnego i bezpiecznego wykonywania aktualizacji i zmiany w oprogramowaniu (np. taryfa, rozkład jazdy inne informacje) w sposób zdalny. Poza tym istnieje możliwość wykonywania aktualizacji w sposób „ręczny”, np. przy użyciu laptopa, karty pamięci, pendrive, itp.
- Zamawiający posiada dedykowaną aplikację do zarządzania i monitorowania pracą automatami – AOZ (w postaci aplikacji webowej). W aplikacji tej dostępne są w trybie on-line dane dotyczące wszystkich wykonanych w automacie operacji, transakcji, awarii i błędów, które przesyłane są z automatów do systemu AOZ za pomocą LTE. Dane te można również pobrać bezpośrednio z automatu za pomocą nośnika danych (np. karta pamięci, pendrive). Ponadto aplikacja AOZ umożliwia m.in. parametryzację automatów, restart urządzeń, aktualizacje oprogramowania, pobieranie/przeglądanie logów, konfigurację wzorów biletów, podpowiedzi do biletów lub procesu zakupu wyświetlanych dla użytkowników na ekranie automatu, uprawnień dostępu pracowników do automatów;
- W przypadku usterki elementów odpowiedzialnych za sprzedaż biletów, automat wyświetla informację o braku sprzedaży biletów i pracuje w trybie informacyjnym;
- W przypadku nieużywania, automat przechodzi w tryb czuwania poprzez uruchomienie wygaszacza ekranu. Ponowne uruchomienie następuje po dotknięciu panelu ekranu.

6.3.5 Wyposażenie POP

W ramach realizacji zadań Punktu Obsługi Pasażera w zakresie systemu ŚKUP 1.5, Zamawiający oczekuje wyposażenia* co najmniej 25 stanowisk w:

1. Zewnętrzny czytnik odczytujący wszystkie karty dostępne w systemie podłączony do zestawu komputerowego; w zakresie obsługi kart EMV - Wykonawca jest zobowiązany do zapewnienia zgodności terminali (czytników kart) z wymogami organizacji kartowych Visa/Mastercard przez cały okres obowiązywania umowy na swój koszt (w chwili obecnej funkcjonalność realizowana poprzez urządzenie PAX 920 – dla kart EMV oraz PEGODA RD 710 – dla kart ŚKUP);
2. Zewnętrzną klawiaturę numeryczną umożliwiającą użytkownikom nadawanie PIN-u do identyfikatora;
3. Dostęp do oprogramowania APO z poziomu przeglądarki – Wykonawca musi przewidzieć, że z uwagi na częste aktualizacje systemów operacyjnych, javy oraz przeglądarek internetowych musi on zapewnić kompatybilność urządzeń oraz systemów z najnowszymi wersjami oprogramowania firm trzecich. Zamawiający nie dopuszcza pracy na nieaktualnej wersji systemu operacyjnego, przeglądarki internetowej lub innych komponentów zestawu.

*Zamawiający dysponuje sprzętem o parametrach określonych w **załączniku nr 2.2 Parametry Techniczne Urządzeń**, które mogą zostać wykorzystane przez Wykonawcę.

Stacje robocze wraz z system operacyjnym Windows (w najnowszej wersji, obecnie Windows 10 prof. PL, x64), oprogramowanie antywirusowe, łączność z Internetem (tunel site-to-site), wewnętrzną sieć LAN każdego z punktów POP, prąd i obsługę zapewnia Zamawiający.

6.3.6 Centra przesiadkowe P&R

Funkcjonalność P&R

W dedykowanych urządzeniach typu parkomat posadowionych w centrach przesiadkowych użytkownik systemu ŚKUP posiadający kartę ŚKUP, będzie mógł skorzystać z funkcjonalności P&R, tj. darmowego postoju, w następujących wariantach:

- Użytkownik posiada wykupiony aktywny bilet komunikacji miejskiej, np. bilet okresowy (do zdefiniowania jako parametr, które bilety) na podstawie, którego w danym dniu (dzień postoju samochodu na parking) wykonał podróż środkiem komunikacji publicznej tzn. dokonał zbliżenia identyfikatora do urządzenia typu kasownik i zarejestrował przejazd;
- Użytkownik posiada wykupiony aktywny bilet komunikacji miejskiej, np. bilet okresowy (do zdefiniowania jako parametr, które bilety), bez konieczności jego użycia w dniu postoju.

Wykaz urządzeń podłączanych do systemu ŚKUP, które będą wymagały integracji w ramach realizacji umowy ŚKUP 1.5:

- Parkomaty centrum Katowice Ligota (Mera);
- Parkomaty centrum Zawodzie (Green Center);
- Parkomaty Brynów (Green Center);
- Automaty centrum Zawodzie (S&B);
- Automaty centrum Sądowa (MPTechnology);
- Automaty centrum Brynów (MPTechnology).

6.4 SAM serwer (HSM)

6.4.1 Zarządzanie kluczami

Klucze kryptograficzne muszą być chronione przed nieautoryzowanymi zmianami, utratą lub zniszczeniem. Klucze prywatne oraz klucze tajne muszą być chronione przed dostępem przez pojedyncze osoby. Klucze prywatne lub tajne, które są wykorzystywane w procesie związanym z realizacją transakcji, muszą być przechowywane w dedykowanych modułach kryptograficznych (HSM ang. *Hardware Security Module*).

W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS 140-2 Level 2 lub równoważne.

Zastosowane rozwiązanie musi zostać wyposażone w funkcjonalność umożliwiającą w sposób bezpieczny wymianę kluczy tajnych lub prywatnych we wszystkich składnikach systemu w przypadku ich kompromitacji. Wymaganie to dotyczy również kluczy przechowywanych w urządzeniach infrastruktury wyniesionej.

Umożliwienie pełnej konfiguracji, administracji i użytkowania urządzenia HSM.

Cechy HSM opisano poniżej:

- Możliwość wykonania następujących operacji:
 - generowanie par kluczy kryptograficznych,
 - fizyczna i logiczna ochrona kluczy kryptograficznym,
 - kontrola dostępu do kluczy kryptograficznych,
 - wykonywanie operacji z użyciem kluczy kryptograficznych,
 - archiwizacja kluczy,
 - odtwarzanie kluczy po awarii urządzenia.
- Możliwość generowania kluczy dla algorytmu RSA o różnej sile: klucze 1024 bity, 2048 bitów oraz 4096 bitów;
- Archiwizacja kluczy i ich odtwarzanie. Archiwizacja kluczy musi wykorzystywać mechanizm podziału sekretu;
- Pełne wykonanie kopii zapasowych materiału kryptograficznego i pełne odtworzenie materiału kryptograficznego;
- Pojemność min. 100 kluczy kryptograficznych RSA 2048 oraz możliwość tworzenia slotów. Możliwość zarządzania urządzeniem z poziomu linii poleceń jak i interfejsu graficznego;
- Prędkość wykonywania operacji kryptograficznych z użyciem algorytmu RSA z kluczem o długości 2048 bity min. 16 operacji na sekundę lub większą adekwatną do wymagań systemu;
- Przechowywanie kluczy kryptograficznych wewnątrz modułu HSM;
- Moduł kryptograficzny posiadający poziom bezpieczeństwa FIPS 140-2 Level 2 potwierdzony wydanym certyfikatem;
- Brak limitu ilości klientów lub aplikacji podłączających się;

Górnośląsko-Zagłębiowska Metropolia
40-053 Katowice
ul. Barbary 21A
tel. +48 32 718 07 00, fax +48 32 718 07 99
email: za@metropoliagzm.pl
www.metropoliagzm.pl



- Wsparcie interfejsów programistycznych (API): PKCS#11, Java Cryptography Extension (JCE), Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM), Cryptographic eXtended services Interface (CXI);
- Wsparcie algorytmów: RSA, DSA, ECDSA with NIST and Brainpool curves, DH, ECDH with NIST and Brainpool curves, AES, Triple-DES, DES, MAC, CMAC, HMAC, SHA-1, SHA2-Family, SHA3, RIPEMD, Hash-based Deterministic Random Number Generator (DRNG), True Random Number Generator (TRNG acc. AIS31 class PTG.2).

6.5 Moduł Backupu

Moduł odpowiada za wykonywanie i przechowywanie kopii zapasowych oraz danych archiwalnych dla kluczowych elementów systemu w szczególności dane transakcyjne, dane umożliwiające odtworzenie zasobów do przywrócenia pełnej sprawności procesów biznesowych. Kopie zapasowe należy przechowywać na zasobach chmurowych z zastosowaniem przepisów dot. przetwarzania i przechowywania (dane nie powinny opuszczać UE) danych osobowych w tym prawo do zapomnienia. System musi posiadać następujące cechy:

- Wdrożony system backupowy musi w pełni zarządzać usługami tworzenia kopii zapasowych, w sposób scentralizowany i automatyczny. Korzystając z modułu można centralnie konfigurować zasady tworzenia kopii zapasowych i monitorować aktywność tworzenia kopii zapasowych zasobów;
- Możliwość przywrócenia danych w możliwie krótkim czasie (zgodne z czasami SLA) w przypadku awarii sprzętu lub oprogramowania;
- Możliwość przywrócenia działania infrastruktury IT po atakach typu ransomware;
- Możliwość przywrócenia danych po przypadkowym usunięciu przez użytkownika;
- Możliwość przywrócenia plików po przypadkowym nadpisaniu przez użytkownika;
- Możliwość odtworzenia całego serwera, partycji oraz pojedynczych plików;
- Szyfrowanie archiwów;
- Wykorzystanie mechanizmów deduplikacji;
- Kopie przyrostowe i pełne.
- Zgodność z wymogami RODO w tym zachowanie prawa do zapomnienia.

Wykonawca wdroży system backupowy dla całego systemu (dot. centrów przetwarzania danych CPD), w ramach systemu zostaną zastosowane następujące polityki retencji danych:

- Kopie dzienne przechowywane przez 7 dni;
- Kopie tygodniowe przechowywane przez 1 miesiąc;
- Kopie miesięczne przechowywane przez 12 miesięcy;
- Kopie roczne do końca umowy;
- Coroczne wykonanie zapisu kopii całego systemu (kopia wynoszona) na zewnętrzny przenośny zasób dyskowy i przekazanie Zamawiającemu na własność. Przekazane archiwum musi posiadać strukturę umożliwiającą odtworzenie poza środowiskiem (katalog archiwum). Pierwsza kopia systemu zostanie dostarczona Zamawiającemu po zamknięciu roku kalendarzowego w okresie eksploatacji systemu do dnia 14 stycznia.

W ramach umowy Wykonawca zbuduje rozwiązanie i będzie realizował zadania wykonywania kopii zapasowych, będzie monitorował ich poprawne wykonywanie oraz odtwarzał wedle potrzeb. Do zadań Wykonawcy należeć będzie także testowe weryfikowanie i odtwarzanie kopii wg harmonogramu (przynajmniej raz na kwartał).

6.6 Moduł Monitoringu (MMT)

Moduł Monitoringu regularnie sprawdza stan elementów poszczególnych komponentów systemu i infrastruktury. Sposób i częstotliwość monitoringu są definiowalne indywidualnie dla każdego elementu.

Zadaniem MMT nie jest monitorowanie urządzeń infrastruktury wyniesionej: pojazdowe (UKP, UKAS, UKAS-EMV), SADiS, UPOS, UKNT, które są szczegółowo monitorowane i raportowane w ramach AOZ, zadaniem MMT jest natomiast monitorowanie całych procesów oraz prezentowanie ilościowe stanów (liczba niesprawnych/sprawnych urządzeń) z podziałem na rodzaje i typy urządzeń.

Uzyskanie informacji dla każdego komponentu systemu w podziale na poszczególne podsystemy, aplikacje/moduły/interfejsy i procesy biznesowe.

System umożliwia modyfikowanie parametrów monitorowania na bieżąco w trakcie pracy. Uzyskane dane diagnostyczne - jakościowe i ilościowe o elementach infrastruktury będą przechowywane historycznie w Systemie ŚKUP 1.5.

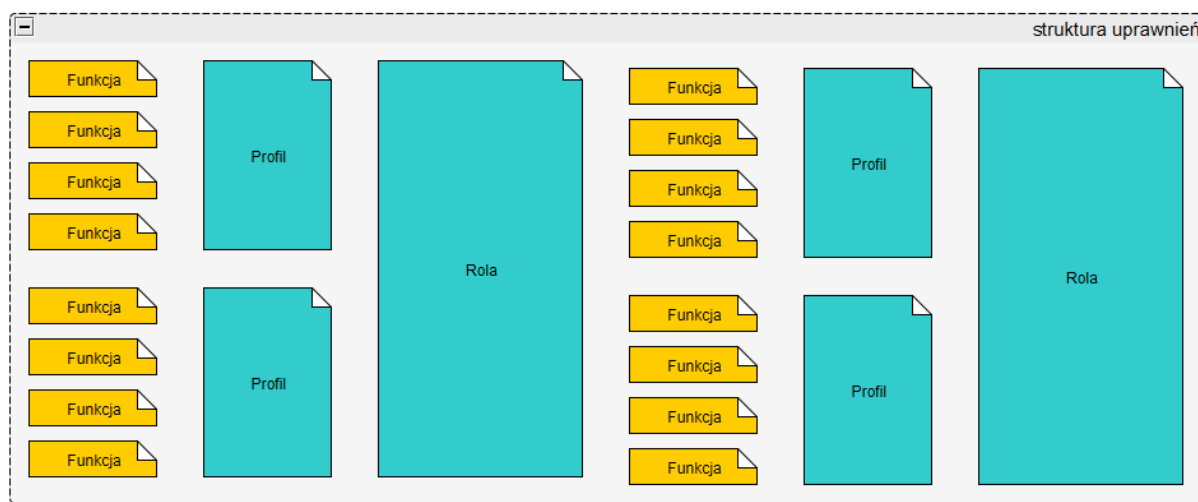
Użytkownicy modułu mogą przeglądać wizualizowane dane na bieżąco w postaci odpowiednio grupowanych raportów i dashboardów zaprojektowanych w uzgodnieniu z Zamawiającym. Użytkownik powinien mieć możliwość szybkiej wzrokowej diagnostyki sprawności całego systemu oraz miarę potrzeb, możliwość doszczegółowienia widoków o dodatkowe informacje podążająca za potrzebami operatora, który steruje w kierunku uzyskania potrzebnych danych.

Założenia dla modułu:

- spełnia założenia wysokiej dostępności (HA).
- posiada interfejs GUI w postaci cienkiego klienta WWW.
- umożliwia konfigurację środowiska monitoringu w szerokim zakresie tak, aby możliwe było dynamiczne dostosowanie monitoringu do zmieniającej się infrastruktury (rozbudowa istniejącej, dołączanie nowych podmiotów, zmiana wartości progów poprawności).
- wspiera technologie wektorowe, umożliwiające tworzenie dowolnych ekranów synoptycznych z możliwością prezentacji na ekranach wielkoformatowych, jak również zapewnia dowolną skalowalność, bez utraty jakości.
- każdemu użytkownikowi można przypisać prawa do poszczególnych funkcji Systemu. Jest możliwość samodzielnego tworzenia praw dla poszczególnych użytkowników oraz modułu do zarządzania prawami użytkowników.
- zapewnia stworzenie rozbudowanych schematów technologicznych.
- system monitorowania jest dostarczony z dedykowanymi sterownikami komunikacyjnymi, umożliwiającymi podłączenie urządzeń do systemu monitorowania.

6.7 Moduł Zarządzania Uprawnieniami (AD)

Zakres uprawnień zarządzanych w module AD zostanie ustalony między Zamawiającym i Wykonawcą na etapie realizacji. Wykonawca w ramach systemu ŚKUP 1.5 zaprojektuje procedury oraz wykona i udostępni Zamawiającemu moduł lub odpowiednie narzędzia IAM (ang. *identity management*) do zarządzania określonymi uprawnieniami w systemie ŚKUP 1.5, które spełniać będą następujące wymagania:



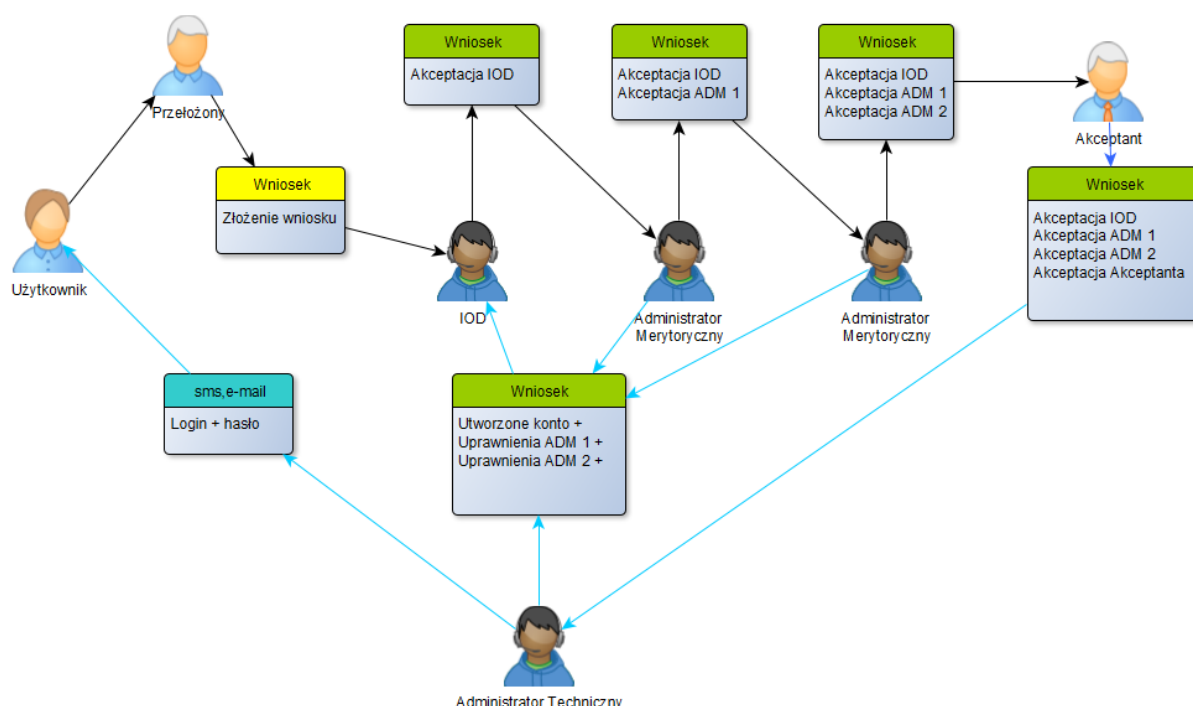
Rysunek 17. Typy struktur wykorzystywanych w procesie nadawania uprawnień

- Zakładanie konta użytkownika umożliwiającego dalszą pracę z modułami w systemie ŚKUP 1.5;
- Zarządzanie kontami oraz uprawnieniami dla wszystkich modułów systemu ŚKUP 1.5 w jednym miejscu (AD) ŚKUP; (Zamawiający w wyniku uzgodnień z Wykonawcą może odstąpić od tego wymagania w uzasadnionych przypadkach);
- Nie dopuszcza się sytuacji posiadania przez użytkownika więcej niż jednego konta w systemie (zasada nie dotyczy kont administratorów technicznych, serwisantów urządzeń);
- Zakłada się, że z poziomu jednego konta będzie możliwy dostęp do wszystkich modułów systemu ŚKUP 1.5 (Zamawiający w wyniku uzgodnień z Wykonawcą może odstąpić od tego wymagania w uzasadnionych przypadkach) ;
- Wykonawca zaproponuje klucz wg, którego będą nadawane nazwy loginów;
- Zarządzanie polityką haseł zgodnie z przyjętą polityką bezpieczeństwa adekwatną do występujących ryzyk;
- Mechanizm uniemożliwiający usunięcie konta;
- Umożliwi definiowanie i zarządzanie pojedynczym uprawnieniem, nazewnictwo uprawnienia powinno być jednoznaczne co do jego przeznaczenia, może zawierać skróconą nazwę modułu, skrótowy opis czynności;
- Umożliwi definiowanie i zarządzanie profilami uprawnień, przez profil należy rozumieć zgrupowanie pojedynczych uprawnień (funkcji) w ramach nadawanych funkcjonalności, nazewnictwo profilu powinno być jednoznaczne co do jego przeznaczenia, może zawierać skróconą nazwę modułu, skrótowy opis uprawnienia;

- Wykonawca zdefiniuje wszystkie pojedyncze uprawnienia dla całego systemu, podzieli je ze względu na moduły/programy/urządzenia przypisze do profili i ról, opíše w polu opis;
- Umożliwi definiowanie i zarządzanie grupami użytkowników;
- Oprócz typowych ról wynikających z realizacji przewidzianych w systemie funkcji, należy przewidzieć w systemie role specjalne:
 - tylko do przeglądania (read-only), bez prawa do jakiegokolwiek modyfikacji;
 - dla operacji finansowych;
 - do pracy na danych osobowych;
 - administrator merytoryczny (nadawanie/odbieranie uprawnień do modułu, parametryzowanie pracy modułu);
 - audytor RODO.
- Umożliwi bezpieczne dostarczanie haseł za pomocą komunikacji poprzez SMS oraz pocztę elektroniczną;
- Umożliwi definiowanie i zarządzanie hasłami dostępów w tym również ich odzyskiwaniem w sposób bezpieczny poprzez zdefiniowane kanały komunikacji SMS, poczta elektroniczna;
- Udostępni mechanizm samodzielnego bezpiecznego resetowania hasła użytkownikowi (wykorzystanie kanału SMS, e-mail);
- Udostępni mechanizm resetowania haseł użytkowników z poziomu administratora; administrator nie może mieć możliwości podglądu nadanego hasła;
- Umożliwi gromadzenie i analizę logowań i aktywności kont operatorów/administratorów w systemie ŚKUP 1.5;
- Będzie udostępniał dane na potrzeby składania wniosków o nadanie uprawnień;
- Wykaz szczegółowych uprawnień dla wybranych kont (w tym dla wszystkich) – wraz z datą obowiązywania uprawnienia – na podstawie fizycznie nadanych uprawnień.

Składanie wniosku o nadanie uprawnień w systemie ŚKUP 1.5

Wykonawca udostępni mechanizm elektronicznego obiegu wniosków o nadanie/modyfikację uprawnień, w formie platformy umożliwiającej wypełnianie elektronicznego formularza, ze zdefiniowaną ścieżką składania, wieloosobowej akceptacji i rozpatrzenia wniosku (Zamawiający oczekuje możliwości zarządzania ścieżką procedowania, aktorami i procesami zachodzącymi między nimi).



Rysunek 18. Schemat wnioskowania o nadanie uprawnień

- Praca na formularzu (wymagane jest wcześniejsze indywidualne zalogowanie do portalu):
 - Wnioskujący (przełożony):** wprowadza dane osoby, dla której wnioskuje (imię, nazwisko, adres email, nr tel. - zalecane podanie nr komórkowego), jednostkę organizacyjną, firmę, zaznacza poszczególne role w systemie, dodaje/odbiera uprawnienia szczegółowe ewentualne profile funkcje, akceptuje i wysyła wniosek;
 - IOD:** analizuje wniosek pod względem danych osobowych, akceptuje wniosek;
 - Administratorzy merytoryczni:** odbiera i przegląda wniosek, dodaje/odbiera uprawnienia szczegółowe ewentualne profile funkcje, akceptuje i wysyła wniosek;
 - Akceptant:** odbiera i przegląda wniosek, dodaje/odbiera uprawnienia szczegółowe ewentualne profile funkcje, akceptuje/odrzuca i wysyła wniosek;
 - Administratorzy techniczni:** odbiera i przegląda wniosek, zakłada/blokuje konto, nadaje/odbiera wskazane uprawnienia, akceptuje/odrzuca i wysyłają wniosek;
 - Użytkownik:** przegląda wniosek, odbiera login hasło;
- Elektroniczny formularz musi być tożsamy ze zdefiniowanymi w systemie uprawnieniami, które powinny być automatycznie zaciągane i prezentowane (role, profile, funkcje);
- Użytkownik (wnioskujący) powinien także mieć możliwość ręcznego zdefiniowania wymagań (np. w przypadku, kiedy oczekuje uprawnień, które jeszcze nie istnieją w systemie);
- Użytkownik, dla którego wnioskowano, Wnioskujący, administratorzy merytoryczni, administratorzy techniczni, akceptant, muszą posiadać dostęp do wypełnionego formularza, w celu jego podglądu, wydruku, akceptacji, modyfikacji;

- W sytuacji odrzucenia/modyfikacji wniosku na którymkolwiek z etapów, wniosek wraca do wnioskującego z informacją zwrotną (np. z przyczyną odrzucenia, koniecznością jego modyfikacji, rozszerzenia bądź zawężenia uprawnień);
- Należy zaimplementować przeglądanie historycznych wniosków wraz z datą ich obowiązywania;
- Każda modyfikacja wniosku już po akceptacji wymaga ponowienia ścieżki akceptacji i jest traktowana jako nowy wniosek;
- Co do zasady to przełożony (wnioskujący) wnioskuje o założenie konta użytkownika i nadawanie uprawnień, należy zdefiniować w systemie schemat organizacyjny przekazany przez Zamawiającego (co nastąpi w procesie implementacji rozwiązania), Zamawiający przypisze pracownikom role: użytkownik, przełożony (wnioskodawca), administrator merytoryczny, administrator techniczny, akceptant;
- Wnioskujący musi mieć możliwość zaznaczania uprawnień bez konieczności ich ręcznego opisywania, do dyspozycji wnioskodawcy powinny być dostępne predefiniowane obiekty ze zdefiniowanymi wcześniej typowymi dla modułu uprawnieniami – rolami w module (np. operator APO, Operator infolinii, itp.). Użytkownik powinien móc przeglądać swoje historyczne wnioski o nadanie uprawnień, móc bezpośrednio w nich dokonywać modyfikacji uprawnień, a następnie wnioskować o ich aktualizację;
- Przeglądanie stanu akceptacji formularza, wg zaplanowanych kroków;
- Oczekujemy możliwości wygenerowania raportów:
 - Wykaz aktywnych kont w systemie (wraz z datą obowiązywania);
 - Wykaz aktywnych kont wg modułów w systemie;
 - Wykaz szczegółowych uprawnień dla wybranych kont (w tym dla wszystkich) – wraz z datą obowiązywania uprawnienia – na podstawie wniosków;
 - Szczegółowy wykaz zmian na koncie wraz z datami.

Implementacja modułu musi być zgodna z aktualnie obowiązującymi przepisami prawa o ochronie danych osobowych oraz polityką bezpieczeństwa informacji oraz procedurą zarządzania uprawnieniami, do której opracowania zobowiązany będzie Wykonawca, na podstawie przeprowadzonej analizy ryzyka dla tego typu systemów.

7 Podsystem Danych

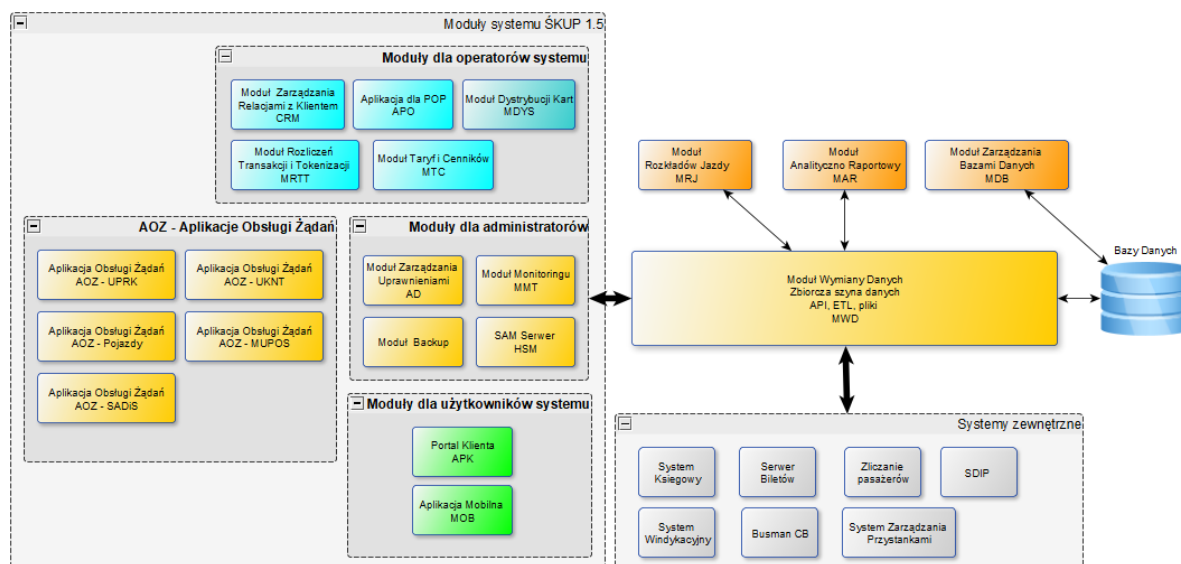
Podsystem odpowiada za globalne centralne zarządzanie i monitorowanie przepływem danych w systemie oraz jego komunikację z zewnętrznymi systemami. W ramach systemu będzie funkcjonowało zdefiniowane otwarte API pozwalające na wymianę danych.

Podsystem będzie odpowiedzialny za przesyłanie danych pomiędzy różnymi elementami systemu ŚKUP 1.5 oraz systemami zewnętrznymi. Przesył danych będzie odbywał się w ściśle zdefiniowany i opisany sposób (otwarte API). W ramach podsystemu konieczne będzie stworzenie GUI, które będzie służyło do definiowania parametrów oraz do prowadzenia monitoringu w trybie on-line.

W ramach podsystemu danych Wykonawca dostarczy szynę danych oraz oprogramowanie umożliwiające plikową wymianę danych, oprogramowanie do zarządzania bazami danych oraz zbuduje hurtownię danych wraz z procesami ją zasilającymi (ETL) oraz dostarczy oprogramowania klasy BI do projektowania i udostępniania raportów.

W ramach podsystemu danych wstępnie zaproponowano podział na następujące moduły/aplikacje:

- Moduł Zarządzania Rozkładami Jazdy (MRJ);
- Moduł Wymiany Danych (MWD);
- Moduł Zarządzania Bazami Danych;
- Moduł Analityczno-Raportowy (MAR);



Rysunek 19. Poglądowy schemat Podsystemu Danych.

7.1 Moduł Zarządzania Rozkładami Jazdy (MRJ)

Rozkłady jazdy i sieć komunikacyjna

1. Zamawiający oczekuje zasilania systemu ŚKUP 1.5 danymi dotyczącymi rozkładów jazdy i sieci komunikacyjnej (uwzględniającymi m.in. połączenia międzyprzystankowe (ścieżki przejazdu) z przydziałem odległości do gmin i płatników, czasów przejazdów z uwzględnieniem pór i wyjątków, godzin odjazdów z podziałem na typy i klasy, nr linii, wzorców dni, datą obowiązywania), operatorów poszczególnych linii (m.in. nazw operatorów, zawartych umów, słownika kar umownych, czasu ich trwania), przystanków i słupków (m.in. nazw, numerów, symboli i lokalizacji przystanków oraz poszczególnych słupków), konfiguracji kalendarza (m.in. przyporządkowania poszczególnych wzorców do dat), dla których źródłem będzie baza danych AGC BusMan 240 CB bądź tożsamy program używanego przez Zamawiającego. Dodatkowo należy przewidzieć import tożsamych danych od innych przewoźników m.in. kolejowych, format pliku wymiany danych będzie oparty o format GTFS oraz normę NeTEx. Całkowity zakres posiadanych i dostępnych danych Zamawiającego stanowi **załącznik nr 2.1 „struktury danych”**.
2. Dane opisane w pkt. 1 stanowić powinny podstawę do tworzenia danych słownikowych, które będą używane w pozostałych modułach systemu ŚKUP 1.5. Dane te powinny być spójne w całym systemie.
3. System powinien umożliwiać (dane nie będą importowane, należy stworzyć mechanizm wprowadzania tych danych w sposób ergonomiczny) definiowanie tzw. odległości i czasów taryfowych, które niezależnie oddziałują na zagadnienia taryfowe bez konsekwencji dla odległości i czasów międzyprzystankowych handlowych, będących podstawą do rozliczeń z Operatorami, gminami, oraz przyjętymi płatnikami.
4. Domyślnie sposób przekazywania danych do systemu ŚKUP 1.5 powinien być automatyczny. Wszystkie możliwe do importu dane automatycznie powinny być pobierane do systemu ŚKUP 1.5. Automatyczna synchronizacja danych przeprowadzana powinna być raz na dobę w uzgodnionej porze. Dodatkowo możliwe powinno być manualne wymuszenie synchronizacji danych.
5. System powinien umożliwiać alternatywną drogę zasilania danymi poprzez dane plikowe np. pliki CSV lub JSON. Zamawiający udostępni przykładowe pliki w podanych wyżej formatach, **załącznik nr 2.1 „struktury danych”**.
6. Moduł MRJ musi umożliwiać przegląd zaimportowanych danych oraz ich uzupełnianie i modyfikację.
7. Moduł MRJ musi umożliwiać wycofanie wprowadzonych zmian, przywrócenie stanu sprzed wprowadzenia zmian, tzw. Rollback.
8. Moduł MRJ musi umożliwiać sklonowanie i dalszą modyfikację danych rozkładowych, które były już wcześniej wykorzystywane w systemie (analogia do szablonu).

9. System ŚKUP 1.5 powinien zwrotnie zasilać aplikację bazę Busman CB_RT lub tożsamą w dane dotyczące realizacji poszczególnych kursów (real-time). Struktura, zasilanej niniejszymi danymi, bazy stanowi **załączniku nr 2.1 „struktury danych”**.

7.2 Moduł Wymiany Danych i Integracji (MWD)

Poszczególne moduły należy zaprojektować i wykonać w taki sposób, aby umożliwiały wymianę danych między sobą z wykorzystaniem technologii opisanych w stosie technologicznym. Komunikacja oraz wymiana danych z innymi systemami zewnętrznymi GZM/ZTM: System Dynamicznej Informacji Pasażerskiej, eMagazyn, System Zliczania Pasażerów, program dyspozytorski, program Busman CB, AZP-WARP (księgowo-rozliczeniowy), system windykacyjny, WEB-API systemu ŚKUP – w okresie przejściowym, ma się odbywać na poziomie wywołania odpowiednio zaprojektowanego API, procesu ETL oraz płaskiego pliku wymiany (w zależności od potrzeb, preferowane jest stosowanie API wszędzie gdzie to możliwe). Wykonawca zobowiązany jest dostarczyć szczegółową dokumentację w szczególności dotyczącą budowy API i parametrów dla prawidłowych i błędnych wywołań wraz z przykładami i opisem generowanych błędów. API poszczególnych modułów stanowić będzie szynę danych do wymiany informacji i integracji między modułami systemu ŚKUP 1.5, innymi systemami wewnętrznymi GZM/ZTM oraz systemami zewnętrznymi.

7.2.1 Stos technologiczny

Wykonawca w dokumentacji opisie wymagany stos technologiczny wraz z jego konfiguracją konieczną do prawidłowego działania uruchomionych Funkcji API. Wykonawca może do budowy systemu ŚKUP 1.5 zastosować oprogramowanie typu open source jeśli gwarantuje ono wymagany poziom bezpieczeństwa, wydajność oraz odpowiada wymaganiom opisanym w niniejszym OPZ.

Zakłada się wykorzystanie przez Wykonawcę standardów do budowy rozwiązań integracyjnych zgodnych z najnowszymi trendami, obsługujących m.in. standardy:

- Dostępu do danych: JDBC i ODBC - przy zachowaniu szyfrowania transmisji;
- Protokołów, HTTPS, MQTT;
- Usług sieciowych: SOAP i REST;
- Standardów komunikatów: GML;
- XML;
- JSON;
- Usług w ramach szyny usług.

7.2.2 Obszary funkcjonalności

Wykonawca zaproponuje logiczny podział zaimplementowanych funkcji API na obszary w celu usprawnienia procesu i zarządzania uprawnieniami do ich udostępniania. Każdy obszar powinien obejmować wszystkie funkcje niezbędne do jego działania. Wykonawca opracuje sposób zarządzania dostępem do API w oparciu o użytkowników i podział na obszary. Dla systemów wewnętrznych dostęp do funkcji API będzie uzgadniany pomiędzy Wykonawcą, a Zamawiającym. W przypadku podmiotów zewnętrznych dostęp będzie przydzielany po złożeniu formalnego wniosku opisującego w szczegółach

zakres integracji z systemem. Po pozytywnym rozpatrzeniu wniosku podmiot rozpocznie proces certyfikacji.

7.2.3 Certyfikacja

Wykonawca zobowiązany jest do przeprowadzenia procesu certyfikacji i integracji z systemem ŚKUP 1.5 urządzeń i systemów/aplikacji firm trzecich, które wyrażą taką intencję, poprzez złożenie do Zamawiającego stosownego wniosku. Integracja z systemem będzie się odbywać przy wykorzystaniu API na środowisku testowym. Jeżeli w procesie certyfikacji w okresie utrzymania, zaistnieje konieczność modyfikacji definicji funkcji API Wykonawca przygotuje w ramach godzin rozwojowych systemu odpowiednią poprawkę i w trybie procedury zarządzania zmianą wprowadzi ją po akceptacji wniosku przez Zamawiającego, a także dokona niezbędnych zmian w dokumentacji.

Po stronie Wykonawcy na etapie rozpatrywania wniosku o certyfikację leży określenie i szacowanie wpływu i obciążenia systemu w przypadku podłączenia deklarowanego urządzenia i systemu/aplikacji do systemu ŚKUP 1.5 oraz wskazanie kosztów (jeśli takie wystąpią) związanych z wykonaniem jego modernizacji. Wykonawca ma obowiązek obsługi wolumenu urządzeń/obrotu (w ramach otrzymywanego wynagrodzenia) na poziomie nieprzekraczającym 50% wzrostu w stosunku do wolumenu wskazanego w OPZ.

Po pomyślnej certyfikacji urządzenia i ewentualnych modyfikacjach koniecznych do wprowadzenia w systemie ŚKUP 1.5 w celu zachowania parametrów wydajnościowych, może nastąpić przyłączenie do systemu i jego integracja.

Nowo przyłączane urządzenia powinny być zarządzalne z poziomu AOS systemu ŚKUP 1.5.

Do systemu ŚKUP 1.5 mogą zostać przyłączone tylko takie urządzenia, które otrzymały certyfikat zgodności lub w przypadku systemów i aplikacji pomyślnie przeszły proces integracji na środowisku testowym.

Wykonawca uzgodni z Zamawiającym i przedstawi kompletną procedurę certyfikacyjną urządzeń i systemów/aplikacji. W ramach procedury Wykonawca przedstawi m.in. wniosek certyfikacyjny zawierający szereg pytań dookreślających co będzie certyfikowane i w jakim zakresie, oraz jak może wpłynąć na system ŚKUP 1.5, na podstawie którego Wykonawca w odpowiedzi przygotuje komplet dokumentów i narzędzi umożliwiających firmie trzeciej zbudowanie urządzenia/systemów/aplikacji, w tym m.in. przypadki użycia, scenariusze testowe, biblioteki programistyczne (do zaimplementowania w środowisku Linux, Windows, Android) wraz z opisami (np. do tokenizacji i odczytu kart, identyfikatorów), projekty ekranów, opis wykorzystanych interfejsów. Poza tym przygotuje środowisko testowe pod certyfikację, udostępni zasoby, loginy i hasła, wypożyczy karty SIM, SAM oraz testowe Karty ŚKUP 1.5.

W przypadku, gdy Zamawiający dostarczy urządzenia spełniające wymagania wskazane przez Wykonawcę, Wykonawca będzie zobowiązany do instalacji na nich oprogramowania dostarczonego w ramach umowy (rozliczenie prac nastąpi w ramach godzin rozwojowych).

Po zgłoszeniu gotowości do certyfikacji przez firmę trzecią, Wykonawca wspólnie z Zamawiającym przystąpi do procesu certyfikacji, rozpoczynający od weryfikacji spełnienia wymogów technicznych

i funkcjonalnych, a następnie Wykonawca potwierdzi kwestie bezpieczeństwa przeprowadzając audyt bezpieczeństwa rozwiązania.

W ramach niniejszego zamówienia Wykonawca będzie zobowiązany do bezpłatnego certyfikowania i przyłączenia do systemu ŚKUP 1.5 następujących typów urządzeń:

Certyfikacja nowych urządzeń:

- Stacjonarne Automaty Dystrybucji i Sprzedaży – do 3 modeli;
- Kontrolerki – 1 model;
- Terminal sprzedażowy do dystrybucji biletów/usług zdefiniowanych w systemie – 1 model;
- Kasowniki – do 4 modeli;
- Komputery pokładowe – do 4 modeli.

Przyłączanie urządzeń do systemu w ramach wynagrodzenia:

- Stacjonarne Automaty Dystrybucji i Sprzedaży – do 450 szt.;
- Kontrolerki – do 300 szt.;
- Terminal sprzedażowy do dystrybucji biletów/usług zdefiniowanych w systemie – do 1800 szt.;
- Kasowniki – do 9450 szt.;
- Komputery pokładowe – do 2600 szt.

Po przekroczeniu powyższych ilości Wykonawcy będzie przysługiwało dodatkowe wynagrodzenie z tytułu certyfikowania i przyłączenia do systemu ŚKUP 1.5 nowych typów urządzeń, które zostanie określone w procedurze certyfikacji oraz przyłączenia.

7.2.4 Kluczowe założenia API

Mechanizmy API dla systemu ŚKUP 1.5 mają umożliwić realizację kompletu procesów biznesowych związanych z obsługą systemu dla następujących segmentów urządzeń oraz być otwarty na integrację z zewnętrznymi systemami:

- Wyposażenie pojazdów: uniwersalne komputery pokładowe (w tym UKP) i kasowniki (w tym UKAS, UKAS-EMV);
- Kontrolerki (w tym UKNT);
- Stacjonarne Automaty Dystrybucji i Sprzedaży (w tym SADiS);
- Terminale sprzedaży (w tym UPOS);
- oraz wszystkich modułów logicznych realizujących procesy biznesowe.

Systemy zewnętrzne

- System finansowo księgowy Zamawiającego (AZP-WARP);
- System windykacyjny;
- Magazyn biletów elektronicznych (eMagazyn);
- Systemy informacyjne typu dynamiczne informacje pasażerskie;
- System zliczania Pasażerów, łączność pojazdu z dyspozytornią;

- Hurtownie danych, platformy otwartych danych (mechanizmy ETL (ang. Extract, Transform and Load), pliki płaskie);
- Systemy MaaS;
- Zasilanie rozkładami jazdy;
- SDIP;
- System zarządzania przystankami;
- Platforma ePUAP;
- Strony www Zamawiającego;
- Centrala telefoniczna DGT.

7.2.5 Zakres funkcjonalny API

Udostępnia usługi i komponenty obejmujące zakresem obszary:

- **API Systemu Centralnego** – usługi zrealizowane w formule REST API udostępnianego centralnie w oparciu o dedykowane komponenty programistyczne;
- **API karty ŚKUP 1.0/1.5** – komponenty do integracji z oprogramowaniem Wykonawcy, umożliwiające współpracę oprogramowania urządzenia z identyfikatorami kont.

Poniżej przedstawiono oczekiwany zakres funkcjonalny interfejsu:

Obszar API Systemu Centralnego:

1. Usługa kolekcji transakcji sprzedaży biletów (zgodnie z taryfą ZTM);
2. Usługa kolekcji zdarzeń aktywacji/skasowań biletów;
3. Usługa kolekcji zdarzeń kontroli uprawnień na przejazd;
4. Usługa kolekcji zdarzeń o realizacji rozkładu jazdy;
5. Usługa kolekcji zdarzeń diagnostycznych pojazdu i urządzenia;
6. Usługa kolekcji zdarzeń o pozycji GPS pojazdu na potrzeby integracji z SDIP lub modułami mapowymi; Dane powinny być udostępniane w taki sposób, by możliwe było korzystanie z nich przez kilkadziesiąt systemów równocześnie przy założeniu, że każdy z nich będzie pobierał dane z częstotliwością nie większą niż 1s.
7. Usługa autoryzacji transakcji identyfikatorem;
8. Usługa udostępniania konfiguracji taryfy (pozycje cennikowe, taryfy);
9. Usługa udostępniania konfiguracji rozkładu jazdy (linie, przystanki, topologia połączeń, obszary, brygady, kursy, zmiany);
10. Usługa udostępniania rejestru urządzeń;
11. Usługa udostępniania rejestru pojazdów;
12. Usługa udostępniania rejestru operatorów (kierujących i kontrolerów);
13. Usługa uwierzytelnienia operatora;
14. Usługa udostępniania rejestru identyfikatorów zablokowanych i zastrzeżonych (Black-Listy, Stop-Listy), w tym możliwość odpytania o pojedynczy identyfikator/konta IKU;
15. Usługa udostępniania rejestru aktywnych kontraktów i zasilanych kont (listy dystrybucyjne);

16. Usługa bezpieczeństwa karty ŚKUP, ŚKUP 1.5 (odblokowywanie Kart SAM, aktualizacja liczników kart SAM);
17. Usługa udostępniania danych słownikowych i referencyjnych;
18. Usługa udostępniania danych dot. kontroli biletów.

Obszar API kart ŚKUP

1. Usługa odblokowania karty SAM;
2. Usługa aktualizacji liczników karty SAM;
3. Usługa uwierzytelnienia;
4. Usługa odczytu danych konta;
5. Usługa odczytu danych identyfikatorów;
6. Usługa odczytu/zapisu/usunięcia kontraktów/ulg;
7. Usługa odczytu/zapisu/usunięcia punktów;
8. Usługa zakupu kontraktów/usług z wykorzystaniem e-portmonetki;
9. Usługa weryfikacji stanu konta – rachunek punktowy;
10. Usługa zapisu aktywacji/skasowania/zmiany limitu biletu;
11. Usługa tokenizacji identyfikatora.

Zamawiający rozpiął tylko minimalny zestaw obszarów, który jego zdaniem powinien zostać obsługiwany przez API, jednakże, jeżeli wymagane będzie rozbudowanie obszarów z uwagi na niewymienione funkcje, które będą niezbędne do prawidłowego funkcjonowania systemu ŚKUP 1.5 oraz jego integrację z systemami zewnętrznymi to Wykonawca zobowiązany będzie do ich wykonania.

7.2.6 Założenia architektoniczne API systemu centralnego ŚKUP

1. Usługi API Systemu Centralnego ŚKUP 1.5 mogą zostać zrealizowane w architekturze REST z wykorzystaniem metod: *GET, POST, PUT, DELETE* protokołu *HTTPS* (odpowiednio: *pobranie, wprowadzenie, modyfikacja i usunięcie danych*). Tylko metoda *POST* nie jest idempotentna. Pozostałe obsługiwane metody zapewniają idempotentność wywołań. Zamawiający dopuszcza również inne rozwiązania np. WebSocket zamiast protokołu HTTPS;
2. Dane usługi API (zasób REST + metoda HTTPS) pracują w trybie synchronicznym albo asynchronicznym. Obsługa metody GET jest zawsze synchroniczna. Dla pozostałych metod HTTPS, tryb synchroniczny oznacza wygenerowanie odpowiedzi usługi po zapisaniu/modyfikacji/usunięciu danych w systemie. W trybie asynchronicznym wygenerowanie odpowiedzi oznacza jedynie przyjęcie danych do dalszego przetworzenia w systemie;
3. Określenie dostępności konkretnej metody HTTPS dla danej usługi, trybu pracy usługi (synchroniczny/asynchroniczny) oraz obsługiwane przez usługę adresy zasobów stanowić będą część szczegółowej specyfikacji API;
4. Komunikacja z serwerem udostępniającym API systemu realizowana będzie z wykorzystaniem protokołu HTTPS zabezpieczonego protokołem min. TLS 1.2;
5. W API obsługiwane będą tylko żądania wysłane na porty HTTPS/WSS (443);

6. Proces uwierzytelnienia realizowany będzie przez udostępnioną w ramach API usługę uwierzytelnienia zgodnie ze standardem OAuth 2.0;
7. Każde wywołanie usługi API wymagać będzie przekazania tokenu autoryzacyjnego ustalonego w procesie uwierzytelnienia. Tokeny autoryzacyjne mają być zgodne ze standardem JWT (JSON Web Token);
8. Udostępniana w ramach API usługa uwierzytelnienia będzie obsługiwać odnawianie tokenu autoryzacyjnego (tzw. refresh token);
9. Usługi API mają być wersjonowane. Wszelkie ich zmiany łamiące kompatybilność wsteczną wprowadzane będą w nowych wersjach metod. Wywołując metodę należy w URI podać numer wersji zasobu;
10. W ramach wywołań usług API obsługiwane będą określone parametry zapytania REST;
11. Przez parametry zapytania REST rozumiane są parametry wywołania REST przekazywane w URI po nazwie endpoint i znaku '?'. Poszczególne parametry rozdzielane są znakiem '&', kolejność parametrów nie jest istotna;
12. Podanie w wywołaniu nieobsługiwanych nazw parametrów powoduje zwrócenie błędu;
13. Ze względu na przeznaczenie rozróżnia się następujące rodzaje obsługiwanych parametrów:
 - 13.1. Parametry filtracji (ograniczają wielkość zwracanych kolekcji obiektów do spełniających warunek filtrowania);
 - 13.2. Parametry sortowania (wskazują porządek sortowania zwracanych kolekcji obiektów);
 - 13.3. Parametry stronicowania (wskazują sposób porcjowania zwracanych kolekcji obiektów).
14. Sortowanie przeprowadzane jest na kolekcji wcześniej odfiltrowanej, zaś stronicowanie na kolekcji wcześniej odfiltrowanej i posortowanej;
15. W wyniku sortowania wraz z danymi kolekcji zwracane są hiperlinki dedykowane nawigowaniu między stronami danych;
16. Wszystkie wywołania i odpowiedzi powinny być przekazane w kodowaniu UTF-8 (polish_ci);
17. Wszystkie dane, wysyłane i odbierane z serwera (kontent) są w formacie JSON i kodowaniu UTF-8 (charset=utf-8_polish_ci). Do przekazywania informacji w zakresie hiperlinków wykorzystywany jest standard HAL;
18. Każda odpowiedź HTTPS zawiera m.in. nagłówki Span-Id i Trace-Id, których wartości jednoznacznie identyfikują zapytanie HTTP klienta oraz proces obejmujący zestaw wywołań usług API. Spinanie zestawu usług w jeden proces leży po stronie klienta usług – w kolejnych wywołaniach HTTPS powinna być przekazywana wartość nagłówka Trace-Id uzyskana z informacji zwrotnej pierwszego wywołania HTTPS w ramach procesu;
19. Wszystkie używane w kontekście wartości daty i czasu prezentowane są w standardzie ISO 8601: yyyy-mm-ddThh:mm:ss.sss±hh:mm lub yyyy-mm-ddThh:mm:ss.sssZ;
20. Wszystkie używane w treści wartości numeryczne wykorzystują „.” (kropka) jako delimiter dziesiętny i nie wykorzystują separatora tysięcy;
21. W razie wystąpienia błędów wykorzystywany jest ogólny mechanizm zwracania błędów zdefiniowany dla protokołu https/WebSocket oraz dodatkowa specyfikacja błędów w treści odpowiedzi.

7.3 Moduł Zarządzania Bazami Danych (MDB)

W ramach modułu Wykonawca dostarczy i udostępni Zamawiającemu narzędzie do administracyjnej obsługi instancji wszystkich baz danych stanowiące dedykowane składnice danych poszczególnych podsystemów i modułów wchodzących w skład systemu ŚKUP 1.5. Narzędzie to będzie umożliwiało kierowanie zapytań w języku SQL wprost do wybranych źródeł danych oraz pozwoli administratorom baz danych na pełne zarządzanie bazami danych w systemie w sposób centralny. Oprogramowanie zawierać będzie GUI do edytora skryptów SQL umożliwiające wywołanie zapytań oraz śledzenie ich pod względem wydajności i optymalizacji oraz zarządzające obiektami takimi jak bazy danych, tabele, pola, funkcje, skrypty i konfiguracją silnika baz danych. Oprogramowanie umożliwiać będzie również wykonanie kopi zapasowej i jej odtworzenie, eksportów oraz importów danych w typowych formatach w tym wybór kodowania, śledzenie zadań, monitoring procesów bazodanowych, zarządzanie uprawnieniami do poszczególnych baz, tabel, wizualizację i zarządzanie relacjami. Dostarczone narzędzie będzie umożliwiało obsługę wszystkich baz danych dostępnych w ramach systemu ŚKUP 1.5 i będzie je wspierać niezależnie od wersji silnika bazodanowego.

Do zadań Wykonawcy w ramach MDB należy również opracowanie polityki archiwizacji i polityki retencji danych i dostarczenie ich w formie opisanych szczegółowo procedur, dołączonych do dokumentacji. Zadania archiwizacji i retencji danych Wykonawca powinien wykonać w postaci automatycznych skryptów kontrolowanych w module monitoringu nadzorowanych przez niego w czasie okresu utrzymania systemu. Zamawiający zastrzega, iż dane transakcyjne nie podlegają retencji i tym samym muszą być dostępne przez cały okres utrzymania systemu.

7.4 Moduł Analityczno - Raportowy (MAR)

Moduł oparty o otwartą architekturę, umożliwiającą pozyskiwanie danych z wielu źródeł w tym zewnętrznych systemów, przekształca je i łączy do wielowymiarowych struktur, a następnie dostarcza zapytania i analizy wspierające podejmowanie decyzji.

Zasilanie hurtowni będzie realizowane w procesach ETL (ang. Extract, Transform and Load) – przy użyciu narzędzia wspomagającego proces pozyskania danych dla baz danych. Pozyskane dane będą przechowywane w hurtowni w sposób zamodelowany i uporządkowany w postaci tzw. wymiarów i faktów stanowiących podstawowe komponenty do budowy raportów w narzędziu do projektowania raportów BI (ang. Business intelligence).

Modułu Analityczno-Raportowy (MAR) jest oprogramowaniem wspierającym obsługę danych tworzenia ścieżek przetwarzania, służy do definiowania i generowania raportów oraz prowadzenia analiz danych zgromadzonych w Systemie ŚKUP oraz innych z nim zintegrowanych (eMagazyn, Busman 240 CB, Busman 240, bramki liczące, inne).

Lista podstawowych funkcjonalności:

- Zarządzanie raportami;
- Zarządzanie dostępem w tym podział na grupy użytkowników;
- Definiowanie raportów;
- Definiowanie ścieżek przetwarzania danych;
- Definiowanie szablonów;
- Harmonogramowanie;
- Zarządzanie hierarchią zdefiniowanych elementów;
- Generowanie raportów;
- Prezentacja wyników na mapach;
- Graficzna prezentacja raportów;
- Eksport danych do plików;
- Pobieranie i agregowanie danych;
- Prowadzenie analiz (m.in. detekcja nadużyć);
- Udostępnienie danych raportowych dla innych modułów ŚKUP oraz zewnętrznych systemów.

Założenia podstawowe:

- a) Powołuje się hurtownie danych opartą o wydajny silnik bazodanowy;
- b) Aplikacja spełnia założenia wysokiej dostępności (HA);
- c) Aplikacja posiada interfejs GUI w postaci cienkiego klienta WWW;
- d) Dostęp do bazy w schematach innych aplikacji jest ograniczony do operacji tylko do odczytu (np. poprzez widoki w centralnej bazie danych);
- e) Definiując źródła danych do raportów i analiz, użytkownik w każdej chwili ma dostęp do podglądu tych danych, a także możliwość wyeksportowania ich do formatu XLSX;
- f) Dane ze źródeł przetwarzane są przez definiowalne, wg założonych harmonogramów mechanizmy ETL;

- g) Projektowanie raportów odbywa się za pomocą narzędzie klasy BI (ang. Business Intelligence)
- h) Zdefiniowane w module obiekty mogą być kopiowane, dzięki czemu nie jest konieczne tworzenie od podstaw skomplikowanych analiz;
- i) Moduł analityczno-raportowy umożliwia definiowanie źródeł danych opartych o dowolne informacje, gromadzone przez system, oraz pochodzące z zewnątrz;
- j) Moduł analityczno-raportowy umożliwia:
 - definiowanie źródeł danych opartych o dowolne informacje gromadzone przez system;
 - definiowanie ścieżek przetwarzania danych, które pozwolą na manipulację źródłami danych z wykorzystaniem m.in. agregacji, filtrowania i wyrażeń wyliczanych;
 - definiowanie szablonów raportów w postaci tabel;
 - definiowanie szablonów raportów w postaci wykresów;
 - definiowania harmonogramu generowania raportów;
 - definiowanie hierarchii folderów, w ramach których będą tworzone źródła danych i szablony raportów;
 - udostępnianie stworzonych źródeł, generacji i szablonów innym użytkownikom.
- k) Każdy proces generowania raportu trwający dłużej niż 10 sekund można przerwać przy pomocy przycisku „Anuluj”;
- l) Istnieje możliwość wywoływania, czy też przedstawiania analiz dla danego obszaru, na mapie (np. open street map OST) - należy zaimplementować również odpowiednie oprogramowanie warstwy mapowej.
- m) Istnieje możliwość prezentowania dowolnych wskaźników odpowiadających wielkością prezentowane wartości;
- n) Definiowane źródła, generacje i szablony są zorganizowane z wykorzystaniem folderów. Foldery mają organizację drzewiastą: jeden folder ma tylko jeden folder nadrzędny, ale sam może posiadać wiele podfolderów (do przeglądania folderów służył eksplorator folderów). Dodatkowo folder posiada możliwość udostępnienia innym użytkownikom poprzez nadanie odpowiednich uprawnień. Jeśli folder jest udostępniony, wówczas pojawia się w części folderów publicznych w podgałęzi odpowiadającej użytkownikowi, który udostępnił folder. Jeśli w ramach udostępnionego folderu zostaną stworzone jakieś raporty, źródła bądź generacje, wówczas one także pojawiają się w części folderów publicznych, jako zawartość danego folderu. Jest dostępny mechanizm zarządzania listą folderów z wykorzystaniem funkcji kopiowania i przenoszenia folderów/szablonów/generacji (kopiuj, wytnij, wklej);
- o) Źródło danych pozwala na zdefiniowanie danych, na podstawie których, są tworzone raporty. Źródło danych opiera się na typach źródeł, którymi są zdefiniowane w bazie widoki bądź tabele. Istnieje możliwość nakładania filtrów na źródło, dzięki czemu można ograniczać dane. Podczas tworzenia/edycji źródła użytkownik w każdej chwili może sprawdzić dane zwracane przez zdefiniowane źródło, dzięki czemu na bieżąco może kontrolować poprawność jego definicji. Dodatkowo użytkownik może wyeksportować dane zwracane przez zdefiniowane źródło do formatu XLSX;

- p) Moduł analityczno-raportowy pozwala w prosty sposób tworzyć ścieżkę przetwarzania danych pochodzących z wielu źródeł. Jest możliwe m.in. definiowanie agregacji, filtrów i wyrażeń wyliczanych, co pozwala na uzyskanie danych zgodnych z pewną, z góry założoną koncepcją;
- q) Do definiowania ścieżki przetwarzania danych służy dostarczony z modułem edytor generacji, który jest narzędziem umożliwiającym zdefiniowanie zakresu danych prezentowanych w tworzonych raportach, z wykorzystaniem następujących elementów:
- źródło – element pozwalający na określenie początkowego źródła danych;
 - złączenie – element pozwalający na określenie złączeń pomiędzy źródłami (tabelami);
 - agregacja – element pozwalający na określenie agregacji przeprowadzanych na danych;
 - wyrażenie – element pozwalający na określenie wyrażenia wyliczanego;
 - filtr – element pozwalający na określenie warunków filtrujących dane;
 - unia – element pozwalający na określenie operacji UNION na danych wejściowych elementu.
- r) Generacja składa się z ww. elementów powiązanych ze sobą w odpowiedni sposób, tworząc hierarchię;
- s) Zdefiniowane szablony raportów (tabele i wykresy) można uruchamiać z poziomu eksploratora folderów. Wybranie odpowiedniej opcji spowoduje uruchomienie generowania raportu. Wygenerowany raport można otworzyć, wydrukować, lub zapisać na dysku w jednym z popularnych formatów obsługiwanych przez aplikacje biurowe(PDF, MS Excel, Open Office, CSV).

Źródła Danych



ETL



Hurtownia Danych



Raporty + BI +
Udostępnianie



8 Migracja danych

W ramach uruchamiania usług systemu ŚKUP 1.5 Wykonawca musi inicjalnie:

- Zaimportować bazę kont użytkowników z systemu ŚKUP wraz z powiązаныmi danymi w tym transakcyjnymi, w tym również dla kont grupujących;
- Zaimportować bazę kart ŚKUP jako jeden z identyfikatorów ŚKUP 1.5;
- Zasiłać system ŚKUP 1.5 rozkładami jazdy podmiotów uczestniczących w realizacji transportu publicznego na terenie GZM (ZTM: autobusy, tramwaje, trolejbusy);
- Zasiłać system bazą słupków przystankowych;
- Zasiłać system ŚKUP 1.5 topologią sieci komunikacyjnej realizowanych linii;
- Zasiłać system ŚKUP 1.5 informacjami o kursach;
- Zasiłać system informacjami o taborze (rodzaj taboru, wyposażeniu, numerze bocznym, rejestracyjnym itp.);
- Zasiłać system informacjami o taryfach;
- Zasiłać moduł CRM kompletem informacji dotyczących aktywnych reklamacji w systemie ŚKUP 1.0.

Zamawiający oczekuje spójnego i jednoznacznego modelu danych na każdym z etapów przetwarzania, tzn. np.: id kursu, id linii, id przystanku, id słupka, itp. muszą być ze sobą powiązane i tożsame ze źródłem. Niedopuszczalne jest, aby po drodze w procesie przetwarzania nastąpiła zamiana, któregośkolwiek z id na inne niż pochodzące ze źródła.

Szczegóły na temat struktur danych zostały opisane w **załączniku nr 2.1 „struktury danych”**.

W ramach okresu przejściowego tzn. do czasu wygaszenia systemu ŚKUP Wykonawca będzie synchronizował (częstotliwość do ustalenia z podmiotem utrzymującym systemy ŚKUP, jednak nie rzadziej niż 5 min) dane transakcyjne między systemami ŚKUP i ŚKUP 1.5, w tym celu będzie mógł skorzystać z API systemu ŚKUP oraz API karty ŚKUP, które zostało opisane w **załączniku nr 30 (do załącznika nr 3 do OPZ) - Zakres danych dostępnych poprzez funkcje API obecnego systemu ŚKUP.**

W ramach eksploatacji systemu ŚKUP 1.5 przewiduje się jego integrację z systemami informatycznymi Zamawiającego:

- Oprogramowaniem Busman CB – w zakresie importu: kalendarza rozkładowego, rozkładów jazdy, przystanków, topologii sieci komunikacyjnej, planowego przebiegu tras linii (ścieżki przejazdu), danych o Operatorach (przewoźnikach), oraz eksportu do bazy Busman RT (real-time) lub tożsamej danych zwrotnych dotyczących realizacji poszczególnych kursów.
- Systemem księgowym – w zakresie danych transakcyjnych o sprzedaży usług;
- Systemem księgowym – w zakresie przekazywania danych niezbędnych do wystawiania faktur za usługi ŚKUP 1.5;
- Systemem windykacyjnym – w zakresie przekazywania danych z wystawionych opłat dodatkowych przez urządzenia UKNT, ewidencji kontroli biletowych, pobierania bazy gapowiczów do autouzupełniania danych na opłacie dodatkowej;
- Centralą telefoniczną i IVR – w zakresie sterowania połączeniami telefonicznymi infolinii, autoryzacją dzwoniących przez IVR;

- System dyspozytorski – w zakresie przekazywania danych o realizacji i zrealizowaniu kursów, pozycjach pojazdów;
- Systemem SDIP – w zakresie ciągłego przekazywania informacji o pozycjach GPS pojazdów i realizowanych liniach, kursach, typie taboru, rodzaju środka transportu, opóźnieniu/przyspieszeniu względem rozkładowego czasu itp.;
- Serwerem biletów (eMagazyn) – w zakresie przekazywania informacji taryfowych (cenników biletów), integracją algorytmów generowania kodów QR, pobieraniem danych transakcyjnych z eMagazynu, pobieraniem danych na potrzeby prowadzenia kontroli biletów w urządzeniach UKNT ŚKUP 1.5.

Przed przystąpieniem do wykonania procesu migracji Wykonawca przedstawi Zamawiającemu scenariusz migracji danych i określi w nim planowane terminy wykonania poszczególnych Etapów migracji.

Wykonawca na potrzeby procesu migracji może powołać dedykowaną instancję bazy danych na środowisku testowym. W ramach tego środowiska opracuje niezbędne skrypty ETL, które zostaną wykorzystane w docelowym procesie migracji.

Etap testowania przygotowanych skryptów powinien być przeprowadzony w uzgodnieniu z Zamawiającym w taki sposób, by nie zakłócał pracy na wykorzystywanych systemach poprzez generowanie dodatkowego obciążenia. Testy mogą być przeprowadzane na losowej próbce danych w przypadku tabel posiadających wiele atrybutów i wiele rekordów.

Przed przystąpieniem do ostatecznej migracji danych Wykonawca przedstawi stosowne raporty z wykonanych testów wykazujących liczbę przypadków pozytywnych, negatywnych i wprowadzi stosowne poprawki w scenariusz migracji w taki sposób, by ostateczny proces migracji odbył się w możliwie sprawny sposób.

9 MaaS

System ŚKUP 1.5 z założenia ma być przyjazny i otwarty na wiele rozwiązań, w tym na rozwiązania Mobility as a Service (MaaS), jego rolą nie jest integrowanie w ramach systemu usług MaaS różnych operatorów, raczej udostępnianie im niezbędnych danych oraz funkcjonalności.

Jeżeli mówimy o wymianie danych, musimy mieć na względzie interfejsy API obsługujące czynności:

1. Raportowanie aktualnego położenia pojazdów wraz z informacją o realizowanej linii;
2. Zbieranie i udostępnianie zanonimizowanych danych na temat przejazdów.

Rower metropolitalny – to projekt realizowany równolegle do ŚKUP 1.5, należy przewidzieć jego integrację w ramach platformy ŚKUP 1.5, w zakresie możliwości korzystania z konta i identyfikatorów ŚKUP 1.5 w ramach realizowania płatności za przejazdy rowerem, prezentacji na mapie (Portal Klienta APK, Aplikacja Mobilna MOB) stacji wypożyczeń wraz z informacją o liczbie dostępnych rowerów, prezentowanie rowerów na mapie (dotyczy rowerów udostępniających taką informację), wgląd w historię wypożyczeń (z wykorzystaniem konta ŚKUP 1.5).

Wymienione funkcjonalności należy rozumieć jako gotowość systemu do realizowania funkcji w przypadku pojawienia się oczekiwań. Należy zaprojektować system ŚKUP 1.5 oraz jego architekturę i API w taki sposób by, gdy pojawią się potrzeby integracji była ona realizowalna.

10 Bezpieczeństwo

Wybudowany przez Wykonawcę system musi być zgodny z wytycznymi dotyczącymi bezpieczeństwa systemów informatycznych określonymi w normie PN-ISO/IEC 27001:2017 oraz z wymaganiami dotyczącymi bezpieczeństwa dla przetwarzania danych osobowych ISO/IEC 27701:2019;

- Wybudowany system musi być zgodny z założeniami PCI DSS;
- System wdrażany przez Wykonawcę w zakresie usług w chmurze musi być zaprojektowany z uwzględnieniem aktualnie obowiązujących przepisów o ochronie danych osobowych oraz wytycznych ministerstwa cyfryzacji oraz spełniać wymogi norm ISO/IEC 27018:2019 i PN-ISO/IEC 27017:2017. Wykonawca potwierdzi to stosownym certyfikatem z przeprowadzonego audytu.
- Analiza i zarządzanie ryzykiem w systemie, w tym określenie podatności, wdrażanie zabezpieczeń, raportowanie są w gestii Wykonawcy.
- Opracowanie procedury zarządzania ryzykiem (w tym identyfikowanie ryzyka, analiza ryzyka, szacowanie następstw, szacowanie prawdopodobieństwa incydentu, określenie poziomu ryzyka, postępowanie z ryzykiem, sterowanie ryzykiem) leży po stronie Wykonawcy systemu. Procedura musi spełniać wymogi:
 - Ustawa z dnia 10 maja 2018 o ochronie danych osobowych (Dz.U. 2018.1000)
 - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
 - Normę PN-ISO/IEC 27001:2014-12.

Wykonawca ponosi pełną odpowiedzialność za bezpieczeństwo systemu i w razie skompromitowania systemu, Wykonawca będzie zobowiązany do wprowadzenia stosownych zmian w systemie (bez dodatkowego wynagrodzenia) oraz poniesienia ewentualnych konsekwencji względem Zamawiającego i użytkowników systemu (wyrównanie strat).

10.1 Audyt bezpieczeństwa

Przed produkcyjnym uruchomieniem systemu Wykonawca przedstawi wyniki audytu bezpieczeństwa i cyberbezpieczeństwa (oprogramowania i infrastruktury) systemu wykonany przez zewnętrzny niezależny podmiot posiadający certyfikat ISO 27006 (PN-ISO/ IEC 27006) na zgodność z normami:

- PN-ISO/IEC 27001:2017,
- ISO/IEC 27701:2019.

Dla infrastruktury chmurowej dopuszczalne jest przedstawienie dokumentów potwierdzających przeprowadzenie audytu przez niezależne instytucje działające na zlecenie dostawcy usług chmurowych na zgodność z ISO/IEC 27018:2019 i PN-ISO/IEC 27017:2017 najbardziej aktualnego na dzień oddania systemu do użytku, przeprowadzonego nie wcześniej niż 1,5 roku od dnia oddania systemu do użytku albo przedstawienia ważnego certyfikatu ISO/IEC 27018 i PN-ISO/IEC 27017:2017.

Wykonawca ma obowiązek powtarzać audyt co roku i przedstawić stosowny raport Zamawiającemu. Do obowiązków Wykonawcy należy wdrożenie ewentualnego planu naprawczego wynikającego z raportu oraz przeprowadzanie ponownego audytu, aż do czasu uzyskania pozytywnego wyniku, potwierdzającego zgodność z ww. normami. Z tego tytułu nie należy się Wykonawcy dodatkowe wynagrodzenie, które Wykonawca powinien w kalkulować w ofercie.

10.2 Inwentaryzacja aktywów IT

Wykonawca systemu zobowiązany jest do dostarczenia rejestru aktywów IT. Wskazany rejestr musi zawierać min. poniższe informacje:

- Właściciel (osoba odpowiedzialna po stronie Wykonawcy lub Zamawiającego);
- Producent/Dostawca;
- Opis;
- Typ;
- Używana wersja;
- Lokalizacja;
- Szczegóły dotyczące licencji (np. klucze licencyjne, dowody);
- Wiek i estymowany czas do końca życia aktywu;
- Szczegóły techniczne;
- Szczegóły dotyczące SLA.

Rejestr aktywów musi być aktualizowany co najmniej raz w miesiącu i odzwierciedlać faktyczny stan działającego systemu.

10.3 Klasyfikacja informacji

Obowiązkiem wykonawcy systemu ŚKUP 1.5 będzie opracowanie modelu klasyfikacji informacji oraz jego uzgodnienie z Zamawiającym. Celem tych czynności będzie zdefiniowanie jakiego rodzaju środki kontroli będą zastosowane (organizacyjne, technologiczne) celem ograniczenia prawdopodobieństwa ujawnienia, modyfikacji lub utraty informacji.

Informacje przetwarzane w systemie (zarówno elektroniczne jak i inne) ŚKUP powinny być sklasyfikowane co najmniej wg. następujących kategorii:

Poufność – rozumiana jako klasyfikacja wymaganego poziomu ochrony informacji oraz przyjętych środków kontroli przed nieautoryzowanym dostępem lub ujawnieniem wrażliwych informacji oraz środkami podjętymi celem ochrony danych osobowych lub innych danych stanowiących tajemnicę przedsiębiorstwa.

Integralność – rozumiana jako klasyfikacja wymaganego poziomu ochrony informacji zapewniająca ich autentyczność i niezaprzeczalność oraz przyjętych środków kontroli jako zabezpieczenie przed przypadkową lub celową modyfikacją lub zniszczeniem danych.

Dostępność – rozumiana jako klasyfikacja wymaganego poziomu dostępności informacji w ujęciu czasowym i niezawodnościowym oraz przyjętych metod celem zapewnienia właściwej dostępności.

10.4 Kontrola dostępu

Wykonawca tak zaprojektuje system ŚKUP 1.5, aby zapewniał on dostęp do aktywów IT (np. informacji, aplikacji biznesowych, systemów, sieci, urządzeń, dokumentacji) wyłącznie uwierzytelnionemu użytkownikowi oraz autoryzowanemu dostępu do żadanego zasobu zgodnie z zasadą niezbędnej wiedzy (ang. need-to-know) i najmniejszych uprawnień (ang. least privilege).

Wykonawca opracuje i wdroży formalny proces dodawania i usuwania użytkowników oraz nadawania niezbędnych uprawnień dających dostęp do określonych zasobów.

Procedury kontroli dostępu do modułów/komponentów systemu ŚKUP 1.5 muszą zostać uzgodnione i potwierdzone z właściwymi osobami odpowiedzialnymi po stronie Wykonawcy przed pilotażowym lub produkcyjnym uruchomieniem systemu.

System kontroli dostępu użytkowników wewnętrznych (np. pracowników Zamawiającego) musi być odseparowany od systemu kontroli dostępu dla użytkowników zewnętrznych rozumianych jako klientów usług Zamawiającego.

Aplikacje biznesowe używane przez wewnętrznych użytkowników muszą korzystać z mechanizmu singlesign on. W przypadku awarii systemu ŚKUP lub nieprawidłowości działania mechanizmów kontroli dostępu dostęp do systemu powinien być domyślnie zablokowany.

Użytkownicy systemu (włączając w to użytkowników technicznych używanych przez systemy IT) powinni posiadać unikalny identyfikator umożliwiający identyfikację czynności i aktywności realizowanych w systemie. Wykonawca zapewni również, aby możliwe było zdefiniowanie innych standardów haseł dla różnych grup użytkowników (min. wewnętrznych, zewnętrznych, technicznych).

Wykonawca zapewni techniczną możliwość zmiany przez użytkownika inicjalnego hasła wygenerowanego przez system, możliwość jego zmiany w trakcie użytkowania systemu lub ponownej aktywacji konta w sytuacji, kiedy dotychczasowe poświadczenia stracą ważność. Hasła nie mogą być przesyłane w sieci jawnym tekstem oraz muszą być przechowywane w formie zaszyfrowanej.

W ramach przedmiotu zamówienia zostanie dostarczony centralny system zarządzania i uwierzytelniania użytkowników systemu.

10.5 Kryptografia

Komunikacja pomiędzy komponentami systemu ŚKUP 1.5 musi być realizowana za pomocą protokołów zapewniających warstwę kryptograficzną (np. HTTPS). W przypadku wymiany danych pomiędzy elementami systemu, które powodują skutki finansowe (np. doładowanie konta, pobranie środków, zakup usług) dodatkowo muszą być stosowane mechanizmy kontroli integralności, gwarantujące, że dane nie zostały zmienione poczynając od miejsca ich wytworzenia, a kończąc na końcowym punkcie ich przetwarzania i przechowywania.

10.6 Separacja środowisk

Wykonawca w ramach przedmiotu zamówienia dostarczy środowiska produkcyjne, testowe, rozwojowe zgodnie z treścią niniejszego dokumentu. Środowiska te muszą być od siebie odseparowane co najmniej na poziomie logicznym celem ograniczenia nieautoryzowanego dostępu lub wykonania zmian na środowisku produkcyjnym. Środowiska testowe i rozwojowe muszą być zaimplementowane w innych segmentach sieci niż środowisko produkcyjne oraz rozdzielone przez firewall. Wykonawca zadba o odpowiednie zestawy danych dla środowisk testowych i rozwojowych, aby możliwe było prowadzenie testów, w tym procesów biznesowych, musi także zadbać o zaimplementowanie usług testowych agenta rozliczeniowego i agentów płatności.

10.7 Procedury operacyjne

Wykonawca wraz z dokumentacją systemu ŚKUP dostarczy procedury operacyjne oraz zapewni ich aktualizację w trakcie całego okresu utrzymania systemu.

Procedury operacyjne muszą co najmniej zawierać informacje dotyczące:

- Wykonywania, przechowywania i odtwarzania kopii bezpieczeństwa systemu oraz urządzeń infrastruktury wyniesionej;
- Przywracania systemu do normalnej pracy po jego awarii lub planowym zatrzymaniu;
- Opisu cyklicznych zadań konserwacyjnych niezbędnych od prawidłowej i nieprzerwanej pracy systemu;
- Informacje kontaktowe do pomocy technicznej dla wszystkich składników systemu.

10.8 Zarządzanie zmianą

Wszystkie zmiany w aplikacjach biznesowych oraz innych składnikach systemu lub infrastruktury muszą być realizowane zgodnie z procedurą zarządzania zmianą, która będzie obejmowała proces od zgłoszenia zmiany do weryfikacji prawidłowości wdrożenia na środowisku produkcyjnym.

Procedura zarządzania zmianą zostanie opracowana przez Wykonawcę i będzie zawierała co najmniej poniższe kroki, które powinny być wykonane przed wdrożeniem zmiany na środowisku produkcyjnym:

- Zarejestrowanie zmiany wraz z jej opisem w rejestrze zmian;
- Ocena wpływu zmiany na system ŚKUP oraz jego otoczenie;
- Zgoda na realizację zmiany wydana przez osobę odpowiedzialną za dany obszar/aplikację lub inny składnik systemu/infrastruktury;
- Zdefiniowane scenariusze testowe umożliwiające potwierdzenie prawidłowości wdrożonej zmiany;
- Weryfikację, że wprowadzana zmiana nie wpływa negatywnie na bezpieczeństwo systemu oraz nie spowoduje powstania niezgodności względem obowiązujących przepisów prawa lub regulacji (np. RODO);
- Harmonogram wdrożenia zmiany (terminy, środowiska);
- Plan wycofania zmiany w przypadku jej nieprawidłowego wdrożenia.

10.9 Bezpieczeństwo obsługi płatności kart płatniczych EMV

Wykonawca systemu zobowiązany jest do utrzymania urządzeń oraz systemu informatycznego zapewniającego przyjmowanie zapłaty za transakcje zainicjowane przy użyciu instrumentów płatniczych, w szczególności takich jak karty płatnicze, spełniającego obowiązujące standardy bezpieczeństwa obowiązujące wszystkich uczestników obrotu kartowego określonych przez organizacje płatnicze w szczególności standardu PCI/PA DSS.

Warunkiem odbioru systemu jest przedstawienie przez Wykonawcę raportu z audytu w zakresie spełnienia norm PCI od kwalifikowanego Audytora (Qualified Security Assessor) na swój koszt.

10.10 Zarządzanie potencjałem wykonawczym

Wykonawca systemu ŚKUP opracuje, wdroży i utrzyma proces zarządzania potencjałem wykonawczym (ang. capacity management). W ramach procesu i z uwzględnieniem opisanych w niniejszym dokumencie cech systemu zostanie zidentyfikowany, wdrożony oraz monitorowany potencjał wykonawczy celem zapewnienia oczekiwanej dostępności systemu ŚKUP 1.5.

Wykonawca zobowiązany będzie do zapewnienia wymaganego potencjału wykonawczego w całym okresie utrzymania systemu tak, aby wydajność usług dostarczanych przez system była zgodna z wymaganiami przedstawionymi w niniejszym OPZ. Monitorowanie elementów potencjału wykonawczego ma zapewnić odpowiednio wczesne wykrywanie możliwości wystąpienia problemów wydajnościowych, które mogą w przyszłości skutkować zagrożeniami dla bezpieczeństwa i dostępności systemu. W przypadku wykrycia potencjalnych zagrożeń Wykonawca zobowiązanych będzie do ich przedstawiania Zamawiającemu wraz z planem ich usunięcia.

Zarządzanie potencjałem wykonawczym musi zawierać co najmniej następujące elementy:

- Wydajność oraz wykorzystanie nośników danych;
- Obciążenie infrastruktury teleinformatycznej (w tym monitorowanie przepustowości łącz);
- Dostępność mocy obliczeniowej;
- Dostępność pamięci operacyjnej;
- Wydajność i wykorzystanie urządzeń/komponentów odpowiadających za bezpieczeństwo systemu (np. HSM, firewall, Web Application Firewall).

10.11 Monitorowanie i logowanie

Wykonawca dostarczy centralny system logowania zdarzeń. W ramach realizacji przedmiotu zamówienia zostanie uzgodnione z Zamawiającym jakie zdarzenia będą logowane, jakie informacje będzie zawierał pojedynczy rekord logu oraz jak długo będzie przechowywany. Ponadto log musi posiadać cechy umożliwiające identyfikację w zakresie kto, kiedy, co i gdzie w kontekście zarejestrowanego zdarzenia.

Logi powinny obejmować co najmniej następujące kategorie zdarzeń:

- Aktywności użytkownika, wyjątki, błędy;
- Bezpieczeństwo systemu;

- Informacje o transakcjach, w tym możliwość prześledzenia transakcji biznesowej od miejsca źródłowego do docelowego;
- Czynności realizowane przez administratorów i operatorów systemu.

Logi muszą być chronione przed modyfikacją oraz nieautoryzowanym dostępem.

10.12 Bezpieczeństwo aplikacji

Wykonawca w ramach przedmiotu zamówienia opracuje i uzgodni z Zamawiającym model zagrożeń aplikacji (ang. application threat model) wraz ze wskazaniem jakie środki bezpieczeństwa zostaną wykorzystane celem ograniczenia zidentyfikowanych zagrożeń. W przypadku aplikacji dostępnych z publicznego Internetu wymaga się, aby ruch do/z aplikacji był dodatkowo filtrowany z zastosowaniem firewall'a aplikacyjnego (ang. web application firewall).

10.13 Wymagania dot. realizacji obowiązków administratora danych oraz praw osób, których dane będą przetwarzane w systemie informatycznym

Planując przetwarzanie przy pomocy systemu informatycznego (w szczególności stron www, aplikacji mobilnych, dedykowanych systemów) zgodnie z art. 25 RODO należy wdrożyć odpowiednie środki techniczne i organizacyjne, takie jak zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń. Przy projektowaniu należy uwzględnić:

- stan wiedzy technicznej,
- koszt wdrażania,
- charakter przetwarzania,
- zakres przetwarzania,
- kontekst i cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania.
- domyślnie przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (dotyczy ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności).

Należy zapewnić w projektowanym systemie informatycznym realizację, w miarę możliwości (technicznych oraz finansowych, zgodnie z realizowanymi funkcjonalnościami systemu) poniższych praw osób i obowiązków administratora danych:

1. Obowiązki administratora danych:

1.1. Realizacja art. 5 RODO:

1.1.1. Minimalizacja przetwarzania danych osobowych – wykorzystywanie w procesie przetwarzania tylko niezbędnych danych osobowych, przykładowo:

- 1.1.1.1. Ograniczenie ilości gromadzonych danych;
- 1.1.1.2. Ograniczenie prezentacji danych;
- 1.1.1.3. Ograniczenie czasu przetwarzania danych;
- 1.1.1.4. Ograniczenie dostępu do danych;
- 1.1.1.5. Ograniczenie zwielokrotniania tych samych danych.

1.1.2. Prawidłowość przetwarzanych danych osobowych – zapewnienie prawidłowości danych poprzez zastosowanie adekwatnych walidacji, przykładowo:

- 1.1.2.1. Walidacja poprawności struktury adresu e-mail, nr telefonu, nr pesel podczas wprowadzania;
- 1.1.2.2. Walidacja poprawności wprowadzonego adresu e-mail lub nr telefonu poprzez wysłanie linku aktywującego lub kodu aktywującego za pomocą sms.

1.1.3. Przejrzystość przetwarzania danych osobowych – zapewnienie dostępu do informacji osobom, których dane dotyczą w sposób dostosowany do ich poziomu percepcji, przykładowo:

- 1.1.3.1. Dostosowanie warstwy prezentacji zgodnie wymogami ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;

- 1.1.3.2. Zastosowanie wersji językowych w przypadku, gdy treści są przewidziane dla odbiorców nie posługujących się językiem polskim;
- 1.1.3.3. Zastosowanie różnych wersji treści przekazu uwzględniających wiek.
- 1.2. W zakresie w jakim przewidziano zgodę jako podstawę przetwarzania danych osobowych (art. 7 RODO) należy zapewnić rozliczalność administratora oraz zautomatyzować zarządzanie procesem wyrażania i wycofywania zgody. Przykładowo:
 - 1.2.1. W zakresie udokumentowania wyrażenia zgody odnotowanie w logach na czas jej wyrażenia, przynajmniej danych takich jak:
 - 1.2.1.1. Kto wyraził zgodę;
 - 1.2.1.2. Komu zgoda została wyrażona;
 - 1.2.1.3. Dla jakiego celu przetwarzania;
 - 1.2.1.4. Kiedy została wyrażona;
 - 1.2.1.5. W jaki sposób została wyrażona (świadome działanie w poprzez uruchomienie elementu aplikacji/ strony albo wprowadzenie danych osobowych itp., zaznaczenie checkbox'a, z wykorzystaniem jakiego elementu).
 - 1.2.2. Zapewnienie prostego i automatycznego mechanizmu wycofania wyrażonej zgody po uwierzytelnieniu osoby wycofującej zgodę oraz automatycznego usunięcia wszelkich kopii danych przetwarzanych na zgodzie. Przykładowo:
 - 1.2.2.1. Odznaczenie checkbox'a w aplikacji lub na stronie portalu z zastosowaniem potwierdzenia wykonania czynności po uprzednim zalogowaniu. Usunięcie danych osobowych;
 - 1.2.2.2. Usunięcie przez użytkownika danych osobowych po uprzednim zalogowaniu i odnotowanie w logach datę wycofania zgody.
- 1.3. Wyrażenie zgody przez dziecko w przypadku usług społeczeństwa informacyjnego (art. 8 RODO):
 - 1.3.1. Weryfikacja wieku czy poniżej 16 roku życia;
 - 1.3.2. Weryfikacja czy zgodę udziela opiekun prawny/ rodzic stosując dostępne i rozsądne środki, w tym technologiczne;
 - 1.3.3. Udokumentowanie wyrażenia zgody (rozliczalność administratora danych):
 - 1.3.3.1. Kto wyraził zgodę (opiekun czy użytkownik);
 - 1.3.3.2. Komu zgoda została wyrażona;
 - 1.3.3.3. Dla jakiego celu przetwarzania;
 - 1.3.3.4. Kiedy została wyrażona;
 - 1.3.3.5. W jaki sposób została wyrażona (świadome działanie w poprzez uruchomienie elementu aplikacji/ strony albo wprowadzenie danych osobowych itp., zaznaczenie checkbox'a, z wykorzystaniem jakiego elementu);
 - 1.3.3.6. W czym imieniu, jeśli wyrażona przez opiekuna.
 - 1.3.4. Zapewnienie prostego i automatycznego mechanizmu wycofania wyrażonej zgody po uwierzytelnieniu osoby wycofującej zgodę oraz automatycznego usunięcia wszelkich kopii danych przetwarzanych na zgodzie. Przykładowo:
 - 1.3.4.1. Odznaczenie checkbox'a w aplikacji lub na stronie portalu z zastosowaniem potwierdzenia wykonania czynności po uprzednim zalogowaniu. Usunięcie danych osobowych;

- 1.3.4.2. Usunięcie przez użytkownika danych osobowych po uprzednim zalogowaniu i odnotowanie w logach datę wycofania zgody.
- 1.4. Przejrzyste informowanie i przejrzysta komunikacja (art. 12 RODO).
 - 1.4.1. Zapewnienie dostępu do informacji osobom, których dane dotyczą w sposób dostosowany do ich poziomu percepcji, przykładowo:
 - 1.4.1.1. Dostosowanie warstwy prezentacji zgodnie wymogami ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
 - 1.4.1.2. Zastosowanie wersji językowych w przypadku, gdy treści są przewidziane dla odbiorców nie posługujących się językiem polskim;
 - 1.4.1.3. Zastosowanie różnych wersji treści przekazu uwzględniających wiek.
 - 1.4.2. Zapewnienie dostępu do informacji na etapie podejmowania działań oraz w dowolnym momencie.
 - 1.4.2.1. Zapewnienie realizacji art. 13 RODO w momencie podejmowania działań, przykładowo:
 - 1.4.2.1.1. Prezentowanie informacji dot. przetwarzania na etapie wyrażania zgody lub podawaniu konsekwencji jej wycofania;
 - 1.4.2.1.2. Udostępnianie dla użytkownika zbiorczej informacji o przetwarzaniu danych osobowych, w szczególności wyrażonych zgodach, sprzeciwach wobec przetwarzania.
- 1.5. Zapewnienie realizacji obowiązku informacyjnego art. 13 RODO. Prezentacja informacji dot. przetwarzania i zarządzanie treścią zgodnie z brzmieniem art. 13 RODO najpóźniej na etapie zbierania danych. Można zrealizować warstwowo za pomocą tego samego kanału komunikacji. Realizacja przy zastosowaniu wymogów określonych w punktach 1.1.3 oraz 1.4.
- 1.6. Zapewnienie realizacji obowiązku informacyjnego z art. 14 RODO.
 - 1.6.1. Prezentacja informacji dot. przetwarzania i zarządzanie treścią zgodnie z brzmieniem art. 14 RODO, w zależności który warunek wystąpi wcześniej:
 - 1.6.1.1. Przy pierwszym kontakcie (zalogowaniu przez użytkownika do systemu wraz z odnotowaniem daty przekazania informacji) albo przesłanie informacji na adres e-mail albo na nr telefonu. Można zrealizować warstwowo za pomocą tego samego kanału komunikacji lub kanału, do którego użytkownik na pewno ma dostęp;
 - 1.6.1.2. Przesłanie informacji przed udostępnieniem informacji innym administratorom;
 - 1.6.1.3. W ciągu 30 dni, jeżeli poprzednie warunki nie zostały spełnione.
 - 1.6.2. Odnotowanie daty przekazania informacji i środka komunikacji.
- 1.7. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO). Jeżeli jest funkcjonalność wymiany danych z innymi systemami, które przetwarzają dane osobowe (przekazywanie/ udostępnianie danych innemu administratorowi lub jakimkolwiek odbiorcy) należy zapewnić realizację poinformowania tych odbiorców o sprostowaniu (zmianie lub usunięciu lub ograniczeniu przetwarzania danych osobowych). Należy uwzględnić także informowanie pracowników Zamawiającego o tym fakcie.
- 1.8. Bezpieczeństwo przetwarzania (art. 32 RODO).

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Ww. zadania będzie realizował podmiot przetwarzający będzie tym samym ponosił ryzyko i brał odpowiedzialność na siebie.

Przykładowe sposoby realizacji:

- 1.8.1.1. Pseudonimizacja i szyfrowanie danych osobowych;
 - 1.8.1.2. Zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
 - 1.8.1.3. Zapewnienie zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. (kopie zapasowe, redundancja systemów przetwarzania, autoodtworzenie);
 - 1.8.1.4. Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (regularne testy, audyty);
 - 1.8.1.5. Wymuszenie okresowej zmiany hasła;
 - 1.8.1.6. Blokowanie dostępu po określonym czasie braku logowania w sposób pozwalający na samodzielne odblokowanie przy wykorzystaniu innego kanału uwierzytelnienia;
 - 1.8.1.7. Dwufazowe (czyli za pomocą 2 różnych kanałów komunikacyjnych) logowanie do systemu;
 - 1.8.1.8. Dwufazowe uwierzytelnienie przed wykonaniem czynności o wysokim ryzyku, jako jego obniżenie do poziomu akceptowalnego;
 - 1.8.1.9. Ograniczenie prezentowanych danych;
 - 1.8.1.10. Ograniczenie możliwości realizacji praw do sprostowania lub usunięcia lub pozyskania kopii czy przenoszenia.
- 1.9. Określić kwestie dotyczące czasu przechowywania danych (Termin ważności konta lub umowy z użytkownikiem) i umożliwić w systemie mechanizm automatycznego usuwania danych albo ich archiwizowania pod zadanymi warunkami, mechanizm przypominania o terminie.

2. Prawa osób, których dane dotyczą:

2.1. Prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO).

- 2.1.1. Po uwierzytelnieniu poprzez zalogowanie udostępnienie informacji dot. przetwarzania danych osobowych osoby zalogowanej, przykładowo w formie raportu lub podsumowania prezentowanego w określonym miejscu. Odnotowanie w logach daty udostępnienia danych. Minimalny zakres prezentowanych danych:

- 2.1.1.1. Cele przetwarzania;
- 2.1.1.2. Kategorie odnośnych danych osobowych, przykładowo: imię, nazwisko, adres e-mail, nr telefonu, pesel. Nie oznacza to prezentacji samych danych;
- 2.1.1.3. Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- 2.1.1.4. Planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- 2.1.1.5. Informacje o prawach przysługujących użytkownikowi w zależności od podstaw przetwarzania: przykładowo: prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- 2.1.1.6. Informacje o prawie wniesienia skargi do organu nadzorczego;
- 2.1.1.7. Jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- 2.1.1.8. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
- 2.1.1.9. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.
- 2.1.2. Po uwierzytelnieniu poprzez zalogowanie umożliwienie pobrania kopii swoich danych osobowych w formie pliku w ogólnodostępnym formacie. Odnoszenie w logach daty pobrania kopii danych;
- 2.1.3. Realizacja powyższego prawa osób przy zastosowaniu zasad opisanych w punktach 1.1.3 i 1.4.
- 2.2. Prawo do sprostowania swoich danych (art. 16 RODO). Umożliwienie uwierzytelnionemu użytkownikowi (po zalogowaniu) bezpośrednią modyfikację swoich danych w zależności od ich istotności po autoryzacji przez operatora (administratora danych) lub bez autoryzacji. Modyfikacja powinno zostać potwierdzona za pomocą innego kanału komunikacji, który określił użytkownik (e-mail albo SMS). Modyfikacja nie jest traktowana jako osobne operacje usunięcia i wprowadzenia nowych wartości ale jako nadpisanie istniejących wartości. Odnoszenie przynajmniej: daty modyfikacji (sprostowania), identyfikator zmieniającego, daty i identyfikatora autoryzującego, jeśli dotyczy, identyfikator zmienianej wartości.
- 2.3. Prawo do usunięcia danych (art. 17 RODO).
 - 2.3.1. Umożliwienie uwierzytelnionemu użytkownikowi (np. po zalogowaniu) bezpośrednio usunięcie danych określonych jak możliwe do usunięcia przez Zamawiającego. Usunięcie powinno zostać potwierdzone za pomocą innego kanału komunikacji, który określił użytkownik (e-mail albo SMS). Dane możliwe do usunięcia (rozumiane jako dane

usunięte nie modyfikowane) przez użytkownika są danymi dodatkowymi, których przetwarzanie jest oparte na zgodzie. Usunięcie należy traktować jako wycofanie zgody. Odnotowanie przynajmniej: daty usunięcia = dacie wycofania zgody (odnotowanie obydwu wartości jako osobne rekordy), identyfikator użytkownika, identyfikator zmienianej wartości.

2.4. Prawo do ograniczenia przetwarzania (art. 18 RODO).

2.4.1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

2.4.1.1. Osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

2.4.1.2. Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

2.4.1.3. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

2.4.1.4. Do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą (użytkownika).

2.4.2. Niezależnie od tego czy prawo żądania do ograniczenia będzie realizowane za pomocą systemu czy poza nim (zgłoszenie żądania) należy odnotować (data i zakres) fakt ograniczenia przetwarzania danych osobowych w systemie uwzględniając operacje przetwarzania i zastosować adekwatne mechanizmy ograniczenia przetwarzania;

2.4.3. Należy umożliwić poinformowanie osobę, której dane dotyczą, która żądała ograniczenia o uchyleniu ograniczenia przetwarzania;

2.4.4. Przykładowo:

2.4.4.1. Czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania;

2.4.4.2. Uniemożliwienie użytkownikom dostępu do wybranych danych;

2.4.4.3. Nie wysyłanie wiadomości za pomocą wskazanego kanału komunikacyjnego.

2.5. Prawo do przenoszenia danych (art. 20 RODO).

Umożliwienie uwierzytelnionemu użytkownikowi (np. zalogowanemu) pobranie danych w ustrukturuowanym i powszechnie używanym formacie, nadającym się do odczytu maszynowego. Pobranie powinno zostać potwierdzone za pomocą innego kanału komunikacji, który określił użytkownik (e-mail albo SMS). Odnotowanie przynajmniej: daty pobrania, identyfikator użytkownika.

2.6. Prawo do sprzeciwu (art. 21 RODO).

Umożliwić uwierzytelnionemu użytkownikowi (np. zalogowanemu) wyrażenie sprzeciwu wobec przetwarzania w przypadkach, gdy przetwarzanie jest oparte na art. 6 ust. 1 lit. e lub f RODO, przykładowo poprzez przygotowany formularz. Należy przynajmniej odnotować sprzeciw (data wyrażenia sprzeciwu, identyfikator użytkownika, jakich danych sprzeciw dotyczył, jakiej operacji przetwarzania, daty rozpatrzenia sprzeciwu, czy uwzględniono sprzeciw). Zapewnić realizację pkt 1.7 jeżeli jest to możliwe.

2.7. Prawo do niepodlegania zautomatyzowanych decyzji (art. 22 RODO).

Umożliwić, jeżeli dotyczy, uwierzytelnionemu użytkownikowi (np. zalogowanemu) wyrażenie sprzeciwu wobec podleganiu zautomatyzowanemu podejmowania wobec niego decyzji, bez udziału człowieka, wywołującego wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Każda odnotowana realizacja ww. praw i obowiązków jest oznaczona rodzajem zdarzenia w postaci określonego tagu. Jedno zdarzenie może posiadać wiele tagów.

System zapewnia odnotowanie niezbędnych informacji w postaci logów, które można pobrać w ustrukturyzowanym i powszechnie używanym formacie, nadającym się do odczytu maszynowego przy zastosowaniu zadanych kryteriów (min. zakres dat, rodzaj zdarzenia, identyfikator użytkownika).

11 Stos technologiczny

11.1 Architektura

Przy projektowaniu architektury systemu ŚKUP 1.5 Wykonawca musi wziąć pod uwagę poniższe założenia:

- System musi być zgodny z wytycznymi dotyczącymi bezpieczeństwa systemów informatycznych PN-ISO/IEC 27001:2017-06 lub równoważny;
- Architektura systemu będzie zaprojektowana z zachowaniem międzynarodowych standardów, a ich weryfikacja będzie możliwa z zachowaniem Common Criteria ISO/IEC 15408 lub równoważnych z możliwością certyfikacji systemu;
- Praktyki rozwojowe muszą być zgodne normą ISO 27001;
- Dane osobowe muszą być monitorowane i możliwe do prześledzenia za pomocą aplikacji, system musi być zgodny z przepisami RODO;
- System musi być wydajny;
- System musi być skalowalny;
- System musi być elastyczny umożliwiając rozbudowę i integrację z innymi systemami za pomocą interfejsów API;
- Musi opierać się o usługi mikroserwisów;
- Musi wykorzystywać technologie wirtualizacji, konteneryzacji oraz zasoby chmury publicznej i prywatnej;
- Zasoby zostaną uruchomione w środowisku wysokiej dostępności (HA) zbudowane bez pojedynczego punktu awarii sprzętowej;
- System zapewni redundancję wszystkich krytycznych elementów w szczególności w zakresie obsługi pasażerów; pasażer nie może odczuć awarii krytycznej systemu w ramach bieżącej obsługi w systemie;
- Zakładane parametry czasowe dla scenariusza Disaster Recovery (DR), bazującego na odtworzeniu całego środowiska produkcyjnego z backupów, wyniosą: RPO = 1 h, RTO = 6 h;
- Wszystkie dane muszą być przenaszalne i przechowywane z uwzględnieniem wymagań bezpieczeństwa;
- Każde urządzenie walidujące lub pojazd musi mieć wystarczający bufor pamięci na wypadek awarii łączności lub braku zasięgu obu operatorów, aby dane z okresu braku łączności mogły być utrwalone w pamięci buforowej urządzenia i przekazane do głównego serwera po odzyskaniu połączenia;
- O ile to możliwe powinien być oparty o rozwiązania na licencjach typu open-source.

11.2 Zasoby chmurowe

Zamawiający oczekuje wykorzystania najnowocześniejszych technologii z zakresu wirtualizacji, hybrydowych zasobów chmurowych IaaS, PaaS, SaaS. Technologii wysoko skalowalnych opartych na

konteneryzacji usług, zarządzanych w zaawansowanym panelu administracyjnym pozwalającym na powoływanie nowych obiektów typu serwer, infrastruktura, zasób dyskowy lub usługi.

Środowiska dostępne w zasobach chmurowych

W ramach umowy Wykonawca przygotowuje wysokodostępne, wydajne środowisko produkcyjne spełniające kryteria SLA, środowisko testowe z przeznaczeniem do testowania wprowadzanych na produkcję modyfikacji oprogramowania oraz do certyfikacji urządzeń dołączanych do systemu, oraz środowisko developerskie (rozwojowe) służące do przygotowania poprawek i modyfikacji. Wykonawca przydzieli Zamawiającemu dostęp do wszystkich środowisk.

- Praca ośrodków CPD dostawcy rozwiązania chmurowego w trybie Active-Active;
- Zastosowanie mechanizmów równoważenia obciążenia (load-balancing).

Poziom bezpieczeństwa

Zamawiający oczekuje, że Wykonawca zapewni zasoby chmurowe posiadające certyfikat klasy Tier III według klasyfikacji Uptime Institute lub spełniających normę TIA-942 w klasie Tier 3.

Zamawiający dopuszcza model hybrydowy z elementami chmury prywatnej, dla tych obszarów, których uwarunkowania bezpieczeństwa systemu lub danych osobowych będą tego wymagały. W procesie projektowania rozwiązania Wykonawca powinien kierować się aktualnie obowiązującymi przepisami prawa (w szczególności o ochronie danych osobowych) a także wytycznymi dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych.

Zamawiający nie dopuszcza, aby dane osobowe były przechowywane i przetwarzane poza terenem Unii Europejskiej.

Skalowalność

Zamawiający oczekuje użycia zasobów serwerowych (pamięć operacyjna, moc obliczeniowa procesorów, zasoby dyskowe, użycie łącza) nieprzekraczających poziomu 80%. Każdorazowo w przypadku przekroczenia takiego wskaźnika wiązać się to będzie z rozszerzeniem zasobów przez Wykonawcę. Dlatego wymagane jest, aby architektura systemu, zastosowana technologia i wykupione usługi umożliwiały swobodne skalowanie:

- Skalowanie horyzontalne: tj. ingerencje w daną strukturę, poprzez dodawanie lub usuwanie serwerów „cloud”;
- Skalowanie wertykalne: tj. ingerencje na danym serwerze „cloud” polegającą na zwiększaniu lub zmniejszaniu poszczególnych komponentów (vCPU, RAM, zasoby dyskowe).

W celu optymalizacji kosztów, Zamawiający dopuszcza skalowanie w dół w przypadku posiadania wolnych zasobów.

Wykonawca przedstawi scenariusze wyjścia z chmury oraz na wniosek Zamawiającego dokona migracji środowiska i danych na zakończenie umowy.

Założenia realizacyjne na usługi IaaS i PaaS:

Usługa budowy i dostarczania usług chmurowych obejmuje:

- a) Finansowanie wymaganej infrastruktury IT;
- b) Pokrycie kosztów kolokacji oraz publicznej adresacji IP dla środowiska IT;
- c) Pokrycie kosztów energii elektrycznej;
- d) Ciągłe monitorowanie parametrów fizycznych w serwerowni (klimatyzacja, zasilanie, wilgotność, temperatura);
- e) Ciągły monitoring infrastruktury serwerowej, macierzowej oraz urządzeń sieciowych, a także środowiska wirtualizacyjnego i systemów operacyjnych w nim posadowionych;
- f) Zarządzanie (w tym procedury naprawcze) infrastrukturą serwerową, macierzową i sieciową;
- g) Zapewnienie prawa użytkowania oprogramowaniem;
- h) Monitoring środowiska;
- i) Zarządzanie środowiskiem wirtualizacyjnym, konteneryzacyjnym, maszynami wirtualnymi i systemami operacyjnymi;
- j) Zapewnienie licencji/maintenance system backupu;
- k) Zapewnienie licencji/maintenance systemów operacyjnych;
- l) Zapewnienie licencji/maintenance systemów antywirusowych i innych niezbędnych systemów odpowiadających za bezpieczeństwo systemu;
- m) Zarządzanie polityką, środowiskiem oraz zadaniami backupu i odtworzeniami;
- n) Zapewnienie ciągłości działania systemów operacyjnych;
- o) Zapewnienie ciągłości działania baz danych;
- p) Pełną obsługę serwisowo-gwarancyjną;
- q) Helpdesk dostawcy usług chmurowych w trybie 24/7/365;
- r) Zapewnienie dla infrastruktury usługi chmurowej instalacji podtrzymywania zasilania umożliwiającej bezpieczne wyłączenie systemów w przypadku braku zasilania.

Zakłada się zapewnienie licencji maintenance dla każdego z wykorzystywanego oprogramowania infrastrukturalnego, dla oprogramowania open-source zakłada się model zapewniania ciągłości działania takiego oprogramowania, w oparciu o kompetencje ekspertów Dostawcy, bez wykupienia licencji maintenance samego oprogramowania (ze względu na brak takiej możliwości dla wybranych w projekcie dystrybucji oprogramowania).

W ramach umowy dostarczania usług chmurowych zostanie zapewnione:

- a) Dostarczenie gotowego do użycia środowiska, w tym:
 - Kolokacja sprzętu;
 - Konfiguracja środowiska wirtualizacji i maszyn wirtualnych zgodnie z projektem technicznym;
 - Instalację i konfigurację systemów operacyjnych zgodnie z projektem technicznym;
 - Konfigurację dostępów i sieciową zgodnie z projektem technicznym;
 - Konfigurację monitoringu zgodnie z projektem technicznym;
 - Instalację i konfigurację systemu backupu z projektem technicznym;
 - Instalację i konfigurację silnika bazy danych z projektem technicznym;
- b) Model abonamentowy zapewniania dostępności usług;
- c) Rozliczenia usług w sposób uzależniony od realnego zużycia zasobów;
- d) SLA na poziomie opisanym w **załączniku nr 4.1 warunki SLA**;
- e) Możliwość skalowania poziomego i pionowego każdego z elementów infrastruktury (IaaS);

- f) Możliwość objęcia monitoringiem baz danych i aplikacji (PaaS);
- g) W ostatnim roku trwania umowy, zagwarantowanie możliwości przedłużenia usługi chmurowej lub umożliwienie jej migracji do innego miejsca (wg uznania Zamawiającego).

Wolumetria danych

Wykonawca w ramach umowy zapewni zasoby infrastruktury pozwalające na wydajne przetwarzanie danych w czasie zbliżonym do rzeczywistego dla wielkości wskazanych w poniższej tabeli.

Lp.	Kategoria	Wolumetria
1.	Przewidywana kwota transakcji w ciągu roku	100 mln zł
3.	Liczba transakcji elektronicznych / 1 dzień	60.000 szt.
4.	Liczba transakcji elektronicznych / 1 miesiąc	1.250.000 szt.
5.	Liczba kont IKU	500 000 szt.
6.	Liczba identyfikatorów	1.000.000 szt.
7.	Pojazdy wraz z infrastrukturą pojazdową	2000 szt.
8.	Urządzenia SADiS	300 szt.
9.	Urządzenia kontrolerskie	200 szt.
10.	Urządzenia UPOS	1200 szt.
11.	Wozokilometry	100 mln
12.	Tablice informacyjne SDIP	600 szt.

Tabela 9. Wolumetria

W ramach umowy (bez dodatkowego wynagrodzenia) Wykonawca musi przewidzieć i zapewnić funkcjonowanie systemu, z uwzględnieniem 50% wzrost w stosunku do wolumetrii podanej w tabeli.

11.3 łączność

Podobnie jak w przypadku chmurowych zasobów serwerowych, Zamawiający wymaga, aby utylizacja łączy transmisji danych nie przekraczała poziomu 80%, po przekroczeniu tego poziomu Wykonawca musi wykonać podniesienia wydajności łączy tak by zachować wymagany poziom.

Wszystkie urządzenia infrastruktury wyniesionej, o których mowa w punkcie 6, należy wyposażyć w karty SIM działające w wydzielonej sieci APN, ilość montowanych kart zależy od wymogów stawianych urządzeniom. Zamawiający oczekuje, aby sieć komórkowa oparta była o technologię LTE lub nowszą. Miesięczny transfer danych nie może w żaden sposób ograniczać funkcjonalności urządzeń, należy przewidzieć odpowiedni wolumen danych, a w przypadku przekroczenia jego wartości, Wykonawca rozszerzy jego wartość (wykupi u operatora) adekwatnie do rzeczywistych warunków.

Obecnie urządzenia infrastruktury wyniesionej realizują usługi kryptograficzne w oparciu o moduły kart SAM. Każde urządzenie jest wyposażone w kartę SAM (odpowiednią według poziomu dostępu). Do Wykonawcy należy podjęcie decyzji o wykorzystaniu kart SAM lub zastosowanie innego adekwatnego rozwiązania.

11.4 Oprogramowanie

Zamawiający dopuszcza zastosowanie dostępnych na rynku gotowych rozwiązań open-source lub opartych na innych licencjach, o ile Wykonawca zapewni ich dalszy rozwój i przekaze pełną dokumentację, licencję z prawem do modyfikacji i kody źródłowe.

11.5 Uwzględnione standardy danych

W wyniku badania architektury rozwiązań referencyjnych przeanalizowano standardy wykorzystywane w projektach o podobnej tematyce. Wymaga się od Wykonawcy korzystania z następujących standardów w ramach budowy systemu ŚKUP 1.5:

- Transmodel:
 - DVC (Data Communication on Vehicles);
 - IFOPT (Identification of Fixed Objects in Public Transport);
 - SIRI (Standard Interface for Real-Time Information);
 - DJP/OJP (Open API for distributed journey planning);
 - NeTEx (Network Timetable Exchange);
 - GTFS (General Transit Feed Specification);
 - GTFS-RT;
 - OpRa (Operating Raw Data and statistics exchange).
- Norma EN ISO 24014-1;
- Standard ISO/IEC 14443 A i B;
- Standard bezpieczeństwa 15408 (Common Criteria);
- Certyfikacja zestawu czytnik-aplikacja, przez organizację płatniczą;
- Obsługa transakcji płatniczych z uwzględnieniem obowiązującego prawa krajowego – Ustawa o Usługach Płatniczych oraz Dyrektyw PSD (2015/2366);
- Aztec (ISO/IEC 24778:2008);
- QR (ISO/IEC 18004:2015);
- FCB – Flexible Content Barcode;
- Data Matrix;
- HAFAS;
- TAP TSI;
- Standard EMV i dokumentów powiązanych regulujących wykorzystanie kart EMV w systemach transportowych VISA i Mastercard;
- Standardy udostępnienia danych na rzecz: Krajowego Punktu Dostępu do informacji o podróżach multimodalnych (KPD) w rozumieniu rozporządzenia 2017/1926.

11.5.1 Cechy funkcjonalne

- Eksploatowane w ramach systemu oprogramowanie będzie integrowane w ramach spójnego słownika danych i obiektów, przez co Zamawiający oczekuje wprowadzania funkcjonalności jednorazowego definiowania obiektów, które stają się dostępne w ramach pozostałych modułów;

- Zamawiający nie dopuszcza sytuacji, że pola tekstowe są hardkodowane w kodzie aplikacji, a ich zamiana wymaga ponownej kompilacji kodów źródłowych. Dopuszczalne jest natomiast słownikowanie wartości na poziomie tabel baz danych oraz pików konfiguracyjnych;
- Dostęp do funkcji w ramach tej samej aplikacji w liczbie nie więcej niż 6 kroków;
- Czas odpowiedzi systemu na kliknięcie myszką nie dłuższy niż 200ms;
- Rozliczalność, tj. autoryzacja do systemu ma być oparta o system uprawnień wewnętrznych (do funkcji i zasobów). W systemie zapisywane powinno być każde logowanie i wylogowanie z systemu. Każda tabela bazy danych systemu powinna posiadać informacje o czasie i użytkowniku wprowadzającym rekord oraz o czasie i użytkowniku modyfikującym rekord. Dane w systemie nie powinny być usuwane z systemu bazodanowego a jedynie oznaczane jako archiwalne;
- Globalnie transfer danych powinien odbywać się różnicowo w celu ograniczania ilości przesyłanych danych oraz skrócenia czasu transmisji, dane powinny być gromadzone w ujęciu przyrostowym;
- Nadawanie poziomu zabezpieczeń ze względu na rolę użytkownika w systemie (użytkownik standardowy, administrator).

Dla użytkownika standardowego powinno się zastosować następujące wymagania:

- Uwierzytelnianie użytkownika przez podanie loginu i hasła (zgodnego z polityką bezpieczeństwa informacji);
- Możliwość wymuszenia / zmiany siły hasła przez administratora;
- Mechanizm „odzyskiwania” hasła;
- Mechanizm zakończenia sesji po zamknięciu przeglądarki oraz wylogowaniu się użytkownika (w celu uniemożliwienia powrotu do sesji poprzez naciśnięcie przycisku „wstecz” bez ponownego logowania);
- Mechanizm logowania działań użytkownika na minimalnym poziomie (zalogowanie, Wylogowanie, błędna próba logowania, zmiana danych, dokonanie transakcji);
- Automatyczne wylogowanie użytkownika przy braku aktywności dłuższej niż X, gdzie parametr X ustawia administrator systemu.

Dla administratorów systemu, merytorycznych powinno się zastosować następujące wymagania:

Wymagania podstawowe oraz dodatkowe:

- Mechanizm silnego uwierzytelniania oparty o uwierzytelnienie dwuskładnikowe (token/certyfikat etc.);
- Wymuszona składnia hasła na poziomie 3 z 4 grup tematycznych znaków (duże małe litery, znaki specjalne, cyfry) długość minimum 12 znaków, okres trwałości hasła, maks. 30 dni, historia haseł – 15 ostatnich;
- Mechanizm logowania działań użytkownika na minimalnym poziomie: zalogowanie, wylogowanie, błędna próba logowania, zmiana danych, zmiana ustawień konfiguracyjnych, tworzenie/usuwanie użytkownika;
- Mechanizm blokowania użytkownika po określonej przez administratora liczbie błędnych prób logowania;

- Dostęp do panelu logowania tylko ze wskazanych adresów IP.

11.5.2 Obsługa walut

System ŚKUP 1.5 będzie obsługiwał walutę polską PLN zgodnie z obowiązującymi przepisami. Wykonawca w ramach realizacji przedmiotu zamówienia, jednorazowo dokona migracji do innej waluty (dotyczy sytuacji wstąpienia Polski do unii walutowej EURO).

11.5.3 Wersje językowe

Wymagane wersje językowe: **1) Polski, 2) Angielski, 3) Ukraiński, 4) Niemiecki** dla: urządzeń udostępnianych użytkownikom, Aplikacji Mobilnej oraz Portalu Klienta w tym chatroom. Przygotowanie wersji językowych leży w gestii Wykonawcy. Należy zaimplementować funkcjonalność pozwalającą na swobodne, przeglądanie i edycję zawartości słowników np. w formie plików JSON lub XML lub CSV, tak by możliwy było ich export i import z poziomu administratorów Zamawiającego. Wykonawca jest zobowiązany do wykonania tłumaczeń treści, również w przypadku ich zmiany w trakcie trwania umowy, np. w wyniku modyfikacji oprogramowania.

Należy tak zaprojektować ekrany aplikacji by wyświetlany tekst, który ma być tłumaczony był polem tekstowym, a nie osadzoną grafiką. Należy przewidzieć i opisać maksymalne długości tekstów, żeby tłumaczony tekst mieścił się na ekranie. Urządzenia muszą wspierać znaki charakterystyczne dla wymienionych języków. Wybór języka na ekranie urządzenia może być prezentowany jako ikony flag, rozwijane po wyborze jednej z nich. Domyślnym językiem jest język polski. Portal Klienta i Aplikacja Mobilna powinny zapamiętywać poprzedni wybór języka, dla użytkownika.

11.6 Analiza bezpieczeństwa

System musi być wyposażony w dedykowany serwer SIEM, czyli Security Information and Event Management, na który będą zgrywane i przetwarzane w czasie rzeczywistym logi z poszczególnych urządzeń/systemów.

Na serwer logów muszą być zgrywane logi z każdego urządzenia, serwera, aplikacji.

Serwer logów musi mieć możliwość przechowywania logów w stanie surowym przez okres definiowany w polityce bezpieczeństwa, jednak nie krótszy niż rok od czasu zarchiwizowania logów.

System musi posiadać następujące elementy:

- Log Management (LMS) – narzędzia używane do tradycyjnego zbierania i przechowywania logów;
- Security Information Management (SIM) – narzędzia lub systemy koncentrujące się na gromadzeniu i zarządzaniu danymi związanymi z bezpieczeństwem z wielu źródeł, takimi jak: zapory, serwery DNS, routery, antywirusy;
- Security Event Management (SEM) – systemy oparte na proaktywnym monitorowaniu i analizie, w tym wizualizacji danych, korelacji zdarzeń i alarmowaniu.

Wszystkie powyższe elementy powinny być, w miarę możliwości, połączone w jedną platformę, która będzie automatycznie zbierać i przetwarzać informacje z rozproszonych źródeł, przechowywać je w jednej scentralizowanej lokalizacji, porównywać różne zdarzenia i generować alerty na podstawie tych informacji.

11.7 Systemy operacyjne

- Zamawiający dopuszcza zastosowanie dostępnych na rynku gotowych rozwiązań open-source lub opartych na innych darmowych jak również płatnych licencjach o ile Wykonawca zapewni ich dalszy rozwój;
- Systemy operacyjne muszą mieć stale zainstalowane wszelkie dostępne aktualizacje bezpieczeństwa;
- Systemy operacyjne muszą być poddane hardeningowi ograniczającemu powierzchnię ataku, minimum poprzez:
 - Instalację minimalnego zestawu funkcji systemowych (pakietów) krytycznych dla działania aplikacji. Wszelkie niepotrzebne aplikacje i pakiety zostaną odinstalowane;
 - Ograniczenie funkcjonujących na serwerze usług do niezbędnego minimum;
 - Ograniczenie otwartych portów;
 - Stosowanie osobnych interfejsów sieciowych do zarządzania oraz do obsługi aplikacji;
 - Zastosowanie wyłącznie szyfrowanych protokołów (HTTPS, SSH, SCP) do zarządzania systemem;
 - Utworzenie dedykowanych personalnych kont dla osób utrzymujących system;
 - Przydzielanie uprawnień zgodnie z regułą minimalnych wymaganych uprawnień (need to know);
 - Usunięcie domyślnych kont lub ich zablokowanie, jeśli nie jest możliwe ich usunięcie.

11.8 Serwery WWW

- Ograniczenie usług uruchomionych na serwerze do niezbędnego minimum;
- Ograniczenie dostępu do katalogów serwera;
- Wykorzystywanie serwera zawsze w aktualnej wersji;
- Implementacja wszystkich poprawek bezpieczeństwa dla danego serwera;
- Wykorzystanie silnego szyfrowania w komunikacji;
- Wyłączenie niepotrzebnych modułów serwera;
- Wyłączenie prezentowania podpisu serwera;
- Wyłączenie prezentowania banerów serwera;
- ;
- Blokowanie kontekstów groźnych dla aplikacji już w warstwie dostępowej;
- Utworzenie dedykowanej strony błędu (Error Page) niezawierającej wersji serwera WWW czy adresacji IP;
- Wyłączenie możliwości uruchamiania skryptów użytkownika po stronie serwera;
- Usunięcie domyślnych kont lub ich zablokowanie, jeśli nie jest możliwe ich usunięcie;
- Usunięcie plików służących do konfiguracji inicjalnej serwera (jeśli nie są wymagane do funkcjonowania serwera);
- Zmiana domyślnej ścieżki dostępu do panelu administracyjnego.

11.9 Interfejs graficzny oprogramowania

- a) Interfejs przygotowany w technologii RWD (Responsive Web Design, strona responsywna) – tak aby w przyszłości w przypadku zmiany typu urządzeń na np. terminale formatu tabletu, interfejs się dostosowywał;
- b) Podczas pracy w wątku danego konta klienta operator powinien widzieć dane pozwalające stwierdzić w jakim wątku pracuje (w tym nawigowanie);
- c) Łatwy i szybki dostęp do historii (przynajmniej do fragmentu, np. 5/10/15 ostatnich) zakupionych biletów/usług w momencie sprzedaży nowego/ej biletu/usługi (bez przerywania procesu sprzedaży) – np. gdy klient chce kupić bilet/usługę „taki sam jak poprzednio”, a obowiązywanie takiego biletu/usługi już się zakończyło to musi istnieć możliwość podejrzenia historii bez przerywania procesu sprzedaży;
- d) Interfejs przystosowany do urządzeń dotykowych (np. rozmiar przycisków, odstęp między przyciskami, nieumieszczanie przycisków o przeciwstawnych funkcjach koło siebie <np. kontynuuj i anuluj> również w formacie dla dużych ekranów np. monitora do komputera PC;
- e) Uruchamianie poszczególnych funkcji w ramach tego samego wątku bez kolejnego wyszukiwania np. konta klienta i konieczności odczytu karty;
- f) Możliwość ponawiania wszystkich generowanych wydruków.

11.10 Aplikacje Mobilne

- Zapewnienie działania aplikacji na dostępnych na rynku polskim platformach mobilnych (Android, IOS) zawsze (w trakcie całego okresu utrzymania) ma być kompatybilna z najnowszą wersją systemu operacyjnego i dwoma wstecznymi. Ponadto Zamawiający dopuszcza zastosowanie narzędzi, które umożliwią Wykonawcy przenoszenie kodu między różnymi platformami;
- Analiza cykliczna – co najmniej raz w miesiącu – zgłoszeń w zakresie funkcjonowania aplikacji mobilnych (wraz z miesięcznym raportem);
- Analiza cykliczna – co najmniej raz na pół roku – bezpieczeństwa aplikacji mobilnych;
- Aktualizacja aplikacji ze względów bezpieczeństwa na skutek wykrytych nieprawidłowości w mobilnych systemach operacyjnych (luki bezpieczeństwa w systemach);
- Aktualizacja aplikacji w związku z nową wersją systemu operacyjnego (nie wcześniej niż dwa miesiące po dacie dostępności nowej wersji systemu i nie później niż 4 miesiące po dacie dostępności nowej wersji systemu);
- Modyfikacja aplikacji w związku z ujawnionymi przez Zamawiającego nieprawidłowościami w działaniu/funkcjonowaniu aplikacji;
- Modyfikacja aplikacji w związku ze zgłaszanymi przez użytkowników nieprawidłowościami, które zostaną potwierdzone przez Zamawiającego.

11.11 Aplikacje WEB

- W przypadku wykorzystania komponentów dostarczanych przez stronę trzecią zawsze wykorzystywanie najbardziej aktualnych, posiadających wsparcie producenta komponentów;
- Implementacja mechanizmów uodparniających aplikację WEB na ataki;

- Prowadzenie regularnych (min. raz na rok) testów penetracyjnych aplikacji przez podmiot niezwiązany z Wykonawcą aplikacji;
- Implementacja mechanizmów zarządzania zmianą, w szczególności testowania pod kątem funkcjonalnym oraz działania podstawowych mechanizmów bezpieczeństwa.

11.12 Urządzenia infrastruktury wyniesionej (UKP, UKAS, UKAS-EMV, UKNT, SADiS, UPOS)

- Łączność z infrastrukturą centralną przez VPN (APN);
- Urządzenia znajdować się muszą w dedykowanej podsieci/podsieciach;
- Urządzenia powinny mieć funkcję przywrócenia do ustawień fabrycznych;
- Wszystkie porty umożliwiające podłączenie się do urządzenia muszą być zabezpieczone przed nieautoryzowanym dostępem (aktywacja portu z systemu centralnego – włączenie możliwości przejścia w tryb serwisowy);
- Autentykacja urządzenia w systemie centralnym po certyfikacie;
- Możliwość aktualizacji/wymiany certyfikatu w sposób centralny – bez konieczności kontaktu fizycznego z urządzeniem;
- Szyfrowanie pamięci wewnętrznej urządzenia.

11.13 Bazy danych

Podstawowe założenia:

- Rozwiązania skalowalne;
- Wysoka wydajność;
- Praca w klastrze wydajnościowym;
- Relacyjność;
- Transakcyjność;
- Zapewniająca spójność danych;
- Kompatybilność z SQL;
- Pozwalające na prace zasobach chmurowych;
- Przechowywanie danych osobowych w postaci zaszyfrowanej;
- Audytowalność wprowadzanych, usuwanych i edytowanych danych.

11.14 Migracja do innego centrum przetwarzania

Wykonawca w ramach realizacji przedmiotu zamówienia (nie wcześniej jednak niż na rok przed zakończeniem umowy), jednorazowo, na pisemne żądanie Zamawiającego (jeżeli takowe wystąpi), dokona migracji (w czasie nie dłuższym niż 180 dni od wystąpienia żądania) rozwiązania informatycznego przedmiotu zamówienia wraz z kompletem danych na inne rozwiązanie chmurowe wskazane przez Zamawiającego. Wśród możliwych do wyboru przez Zamawiającego rozwiązań chmurowych znajdują się:

- Chmura Krajowa;
- AWS;
- GOOGLE CLOUD;
- MS AZURE;

Górnośląsko-Zagłębiowska Metropolia
40-053 Katowice
ul. Barbary 21A
tel. +48 32 718 07 00, fax +48 32 718 07 99
email: za@metropoliagzm.pl
www.metropoliagzm.pl



- IBM CLOUD;
- ORACLE CLOUD
- Inne w uzgodnieniu z Wykonawcą.

Wykonawca będzie zobowiązany do cesji wszystkich usług abonamentowych na Zamawiającego, jeżeli wyrazi on taką wolę.

12 Licencje, prawa autorskie

Zamawiający oczekuje zaprojektowania i stworzenia systemu ŚKUP 1.5 odpowiadającego opisom umieszczonym w niniejszym dokumencie oraz dokumentom powiązanym, bazując na, oprogramowaniu (programach) do którego Zamawiający uzyska prawo do modyfikacji, oraz przekazania odpowiednio do niego majątkowego prawa własności lub licencji niewyłącznej.

W przypadku wątpliwości, braku innego uzgodnienia Stron, oprogramowanie stanowi domyślnie Oprogramowanie Dedykowane.

Zamawiający zastrzega sobie prawo do instalacji dostarczonego w ramach niniejszego zamówienia oprogramowania na urządzeniach zakupionych we własnym zakresie, bez ponoszenia dodatkowych kosztów licencyjnych.

12.1 Oprogramowanie dedykowane

GZM nabywa do niego autorskie prawa majątkowe – oprogramowanie stworzone na potrzeby projektu ŚKUP 1.5, w tym w szczególności projekty graficzne, UX/UI, Aplikacja Mobilna, Portal Klienta, oprogramowanie służące do obsługi urządzeń (m.in. automatów biletowych, terminali sprzedażowych, kasowników, autokomputerów, kontrolerek).

Wykonawca regularnie przekazuje do repozytorium GZM kody źródłowe, tym samym GZM zyska stały dostęp do aktualnych kodów źródłowych.

12.2 Oprogramowanie standardowe:

Pozostałe oprogramowanie (inne niż: Opr. Dedykowane, Oprogramowanie Open Source i Oprogramowanie Narzędziowe) – GZM nabywa niewyłączną licencję bez ograniczeń terytorialnych, czasowych, ilościowych, równoległych użytkowników i innych, z dostępem do kodu i prawem do jego modyfikacji.

Dopuszczalne jest także zastosowanie rozwiązań płatnych (wszystkie koszty muszą być wliczone w cenę składanej oferty), ostateczna decyzja należy do Wykonawcy, który odpowiada za bezpieczeństwo całego systemu oraz za jego bezawaryjną ciągłą pracę – patrz czasy SLA. Zamawiający oczekuje, że w przypadku zastosowania licencji płatnych, Wykonawca wykupi wsparcie producenta na aktualizacje na cały okres trwania umowy. Licencje nie mogą ograniczać możliwości rozbudowy systemu przez Zamawiającego w przyszłości.

Wykonawca regularnie przekazuje do repozytorium GZM kody źródłowe; GZM ma stały dostęp do aktualnych kodów źródłowych.

12.3 Oprogramowanie narzędziowe

Oprogramowanie niewyprodukowane przez Wykonawcę, niezbędne do korzystania i obsługi Systemu – licencjonowane na podstawie licencji producentów tego Oprogramowania Narzędziowego, to także systemy operacyjne, bazy danych, biblioteki programistyczne.

W przypadku wykorzystywania oprogramowania, które nie zostało stworzone na potrzeby niniejszego systemu lub zostały zakupione na potrzeby realizacji systemu ŚKUP 1.5, konieczne jest przekazanie odpowiedniej licencji i kompletnej dokumentacji pozwalającej na swobodne korzystanie z nich, nie mogą one być ograniczone co do dalszego korzystania w ramach systemu lub jego rozbudowy i modyfikacji.

Licencja nie może być w żaden sposób ograniczona ilościowo, sprzętowo, wolumetrycznie, terytorialnie i czasowo.

Licencja nie może być wypowiedziana wcześniej niż po 20 latach licząc od dnia zakończenia umowy.

12.4 Dokumenty i inne utwory

Zamawiający oczekuje przekazania praw autorskich do całej stworzonej dokumentacji w tym diagramów i schematów oraz materiałów szkoleniowych w tym w ramach platformy e-learningowej, na następujących polach eksploatacji:

1. Trwałego lub czasowego zwielokrotnienia w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania niezbędne jest jego zwielokrotnienie;
2. Tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian, z zachowaniem praw osoby, która tych zmian dokonała;
3. Rozpowszechniania.

13 Dokumentacje i repozytoria

Wykonawca w ramach systemu powoła usługę serwera dokumentacyjnego, na którym utworzy repozytorium dokumentacji. Przekazywane materiały (kody źródłowe, dokumentacje, wszelkie inne) będą w języku polskim lub w szczególnych przypadkach w języku angielskim, czytelne i nieobfuskowane oraz aktualne ze stanem faktycznym systemu. Repozytorium dokumentacji zostanie podzielone według logicznych obszarów zaproponowanych przez Wykonawcę i ustalonych z Zamawiającym. Dokumentacja umieszczana w repozytorium powinna być udostępniana od ostatniej aktualizacji do pierwotnej dokumentacji dostarczonej przez Wykonawcę w momencie odbioru. Repozytorium dokumentacji powinno charakteryzować się funkcjonalnością pozwalającą w sposób intuicyjny wyszukiwać żadaną informację według określonych kryteriów:

- Przegląd według wybranego obszaru;
- Przegląd według wybranej wersji;
- Przegląd według wybranej daty;
- Przegląd i wyszukiwanie według wybranej frazy.

Dokumentacja umieszczona w repozytorium powinna być wersjonowana i uaktualniana po każdej zmianie (dotyczy całego cyklu systemu to znaczy okresu wdrażania i utrzymania), która wymaga takiego działania ze względu na wprowadzone zmiany. Dokumentacja powinna posiadać cechy, wskazujące na jej jakość. Aby wytworzyć dokument dobrej jakości należy spełnić wybrane podstawowe warunki:

- **Kompletność** - Nie można dopuścić do sytuacji, gdy pewne części systemu zostaną pominięte w opisie;
- **Spójność** - Nie można dopuścić do sprzeczności poszczególnych fragmentów treści w dokumentacji;
- **Poprawność formalna** - Dokumentowanie projektu musi być prowadzone zgodnie z przyjętym standardem, szczególnie, gdy komponenty systemu są wytwarzane przez różne zespoły;
- **Zrozumiałość** - Należy uważać na język i styl stosowany przy tworzeniu dokumentów. Stosowanie języka technicznego należy wyważyć, gdyż dokumentacja tworzona jest dla ludzi i powinna być dla nich zrozumiałą;
- **Aktualność** - Dokumenty muszą podlegać procesowi zarządzania oraz posiadać aktualną zawartość.

W ramach realizacji umowy Wykonawca przekaze Zamawiającemu edytowalne elektroniczne wersje następujących dokumentów:

Dokumentacja projektowa składająca się na:

1. Harmonogram realizacji - przedstawienie terminów realizacji poszczególnych etapów umowy;
2. Zasady współpracy – uwzględniające wybraną metodykę zarządzania projektem oraz opis ról, uzgadniane z Zamawiającym;
3. Zespół projektowy – wykaz osób Wykonawcy odpowiedzialnych za realizację poszczególnych komponentów systemu oraz ich rola w projekcie;

4. Koncepcja i Architektura Systemu (KIAS) – podstawowy dokument zawierający kompletny opis realizacji systemu uwzględniający stos technologiczny, warstwę serwerową, zasoby chmurowe, powiązania poszczególnych elementów, procesy biznesowe;
5. Model rozliczeń pieniężnych (MRP);
6. Modelu klasyfikacji informacji;
7. Szczegółowe Koncepcje Realizacji (SKR) - dla poszczególnych komponentów systemu (każdy dokument wymaga uzgodnienia z Zamawiającym w ramach prac zespołów projektowych):
 - 7.1. Szczegółowe Koncepcje Realizacji (uwzględniające schematy i opis w notacji BPMN), uwzględniające realizowane procesy biznesowe, funkcjonalne oraz szczegółowe sposoby ich implementacji, z uwzględnieniem projektów poszczególnych ekranów oraz ich zależności w postaci schematów wywołań;
8. Plan testów oraz Scenariusze i Przypadki Testowe (SiPT) – na potrzeby przeprowadzenia odbiorów, uwzględniające wszystkie procesy biznesowe, oraz funkcjonalne, uwzględniające przypadki pozytywne oraz negatywne;
9. Raport z przeprowadzenia testów funkcjonalnych oraz bezpieczeństwa i cyberbezpieczeństwa systemu przez niezależny podmiot specjalizujący się w testach, posiadający certyfikat ISO 27006 (lub równoważny). Raport musi być zakończony pozytywnie z rekomendacją na uruchamianie eksploatacyjne systemu.

Dokumentacja powykonawcza składająca się na:

1. Dokumentacje użytkownika dla wszystkich modułów i aplikacji funkcjonującej w systemie. Dokumentacje należy podzielić na operatorów tzw. back-office - obsługa (wszystkie moduły i aplikacje) oraz użytkowników końcowych (użytkownicy końcowi dotyczą wyłącznie: Portalu (APK), Aplikacji Mobilnej (MOB), urządzeń (UKAS UKAS-EMV, SADiS).
Dla Portalu klienta (APK) Aplikacji Mobilnej (MOB), urządzeń (UKAS, UKAS-EMV, SADiS) zamawiający oczekuje przygotowania filmików instruktażowych oraz symulatorów i opublikowanie ich w ramach portalu (APK);
2. Dokumentacje instalacji i wdrożenia dla poszczególnych modułów i aplikacji;
3. Dokumentacja administratora dla poszczególnych modułów i aplikacji;
4. Schematy i opis baz danych uwzględniające poszczególne modele danych, relacje pól, procedury, klucze powiązań itp.;
5. Pełny szczegółowy opis web-services wraz ze scenariuszami i przykładami wywołania (wszystkie wykorzystane w systemie) w szczególności:
 - Typu danych zwracanych;
 - Zakresu wartości zwracanych;
 - Formatu danych zwracanych;
 - Nazw parametrów wejściowych;
 - Typów parametrów wejściowych;
 - Formatów parametrów wejściowych;
 - Adresu URI niezbędnego do wywołania funkcji/klasy, w której jej szukać/odwołać do dokumentacji;oraz implementacją w poszczególnych modułach/urządzeniach (kompletne scenariusze użycia).

Udostępnienia w ramach środowiska testowego platformy dokumentującej web-services zawierającej szczegółowy opis każdego z WS.

Zamawiający oczekuje przekazania do testowania usług web-services skonfigurowanych narzędzi (dla środowiska testowego) np. Postman, SOAP UI, Insomnia lub inne;

6. Dokumentację urządzeń końcowych (w tym DTR);
7. Dokumentacja warstwy serwerowej;
8. Dokumentacja warstwy sieciowej;
9. Dokumentacja wdrożonych mechanizmów bezpieczeństwa;
10. Dokumentacja udostępnianych zasobów dyskowych;
11. Wykaz wszystkich urządzeń wraz z numerami seryjnymi i podziałem na miejsce instalacji;
12. Ważne certyfikaty potwierdzające zgodność oferowanego rozwiązania sprzętowego do obsługi płatności bezgotówkowych z obowiązującymi wymaganiami organizacji Visa oraz MasterCard;
13. Kosztorys powykonawczy jako załącznik do faktury;
14. Dokumentacja eksploatacyjna:
 - 15.1. Procedury zachowania ciągłości działania systemu;
 - 15.2. Procedury DRP (Disaster Recovery Planning);
 - 15.3. Procedura monitorowania systemu;
 - 15.4. Procedura zarządzania zmianami systemu;
 - 15.5. Procedura zgłaszania błędów, awarii;
 - 15.6. Procedura retencji danych w systemie zawierająca skrypty i mechanizmy realizacji archiwizacji danych;
 - 15.7. Procedura wykonywania kopii bezpieczeństwa i ich odtwarzania;
 - 15.8. Procedura zarządzania uprawnieniami, w tym polityką haseł;
 - 15.9. Polityka Bezpieczeństwa Systemu ŚKUP 1.5 zawierająca analizę ryzyk dla systemu;
 - 15.10. Procedury aktualizacji systemów, usług, modułów;
 - 15.11. Dokumentację procesu zarządzania incydentami i zgłoszeniami;
16. Procedury integracji i certyfikacji oraz procedury przyłączenia do systemu ŚKUP 1.5 zawierająca m.in. formularz zgłoszenia do certyfikacji/przyłączenia, scenariusze podłączania urządzeń/aplikacji (SADiS, UPOS, UKNT, UKP, UKAS, UKAS-EMV) wraz z czynnościami konfiguracyjnymi po stronie systemu. Na potrzeby certyfikacji urządzeń należy przygotować także dokumentację niezbędną do zaimplementowania funkcjonalności wskazanej w formularzu zgłoszenia do certyfikacji. Wykonawca będzie prowadził i udostępniał dziennik certyfikacji uwzględniający istotne dla procesu wpisy;
17. Dokumentację dotyczącą przetwarzania danych osobowych w budowanym systemie, celu realizacji zapisów RODO.

13.1 Repozytoria

Zamawiający oczekuje utrzymywania i udostępniania Zamawiającemu repozytoriów w postaci kompletnych zbiorów danych:

1. Repozytorium konfiguracji (CMDB) aplikacji, urządzeń, może być zrealizowane np. jako zbiór plików konfiguracyjnych wszystkich aplikacji i modułów w jednym miejscu, tak by możliwe było

ich przeglądanie (np. w pliku tekstowym). Repozytorium stanowić będzie kopię konfiguracji. Oczekujemy pełnego ewidencjonowania historii zmian konfiguracji;

2. Repozytorium wersji oprogramowania - Zamawiający oczekuje przechowywania plików instalacyjnych wszystkich aplikacji i modułów występujących w systemie. Oczekujemy ewidencjonowania historii zmian konfiguracji;
3. Repozytorium dokumentacji – zawierające wszystkie powstałe dokumentacje związane z funkcjonowaniem systemu;
4. Repozytorium wniosków o zmianę;
5. Repozytorium wniosków o nadanie uprawnień;
6. Repozytorium nieobfuskowanych kodów źródłowych do oprogramowania dedykowanego – oczekujemy wykorzystania narzędzia typu GIT/SVN itp.

Zamawiający oczekuje zagwarantowania poziomu uprawnień umożliwiającego zarządzanie dostępem do zasobów repozytoriów.

14 Szkolenia

Wykonawca w ramach realizacji umowy przeszkoli operatorów systemu ŚKUP 1.5 w zakresie:

LP	Zakres szkolenia	Rodzaj szkolenie /warsztaty	Miejsce Szkolenia	Liczba szkoleń stacjonarnych X osoby	Liczba godzin / 1szkolenie	e-learning /[egzamin]
1.	Kierowców pojazdów (UKP, UKAS, UKAS-EMV)	Szkolenie	Zewnętrzne	5 x 20 liderzy	3	T/T
2.	Obsługę urządzeń pojazdowych (AOZ – pojazdy)	Warsztaty	GZM	1 x 10	6	T/N
3.	Obsługę urządzeń SADiS (AOZ – SADiS)	Warsztaty	GZM	1 x 10	6	T/N
4.	Obsługę terminali sprzedażowych (UPOS, AOZ-UPOS)	Warsztaty	Zewnętrzne	2 x 10 liderzy	4	T/T
5.	Służby kontrolerskie obsługujące moduły kontrolerskie (UKNT, AOZ - UKNT)	Szkolenie	GZM	2 x 10 liderzy	4	T/T
6.	Obsługę Punktów Obsługi Pasażera (APO)	Szkolenie	GZM	6 x 10	6	T/T
7.	Operatorów modułu zarządzania relacjami z klientem (CRM-reklamacje, wiadomości/komunikacja z użytkownikami, infolinia)	Warsztaty	GZM	3 x 10	6	T/T
8.	Operatorów modułu MTC	Warsztaty	GZM	2 x 5	6	T/T
9.	Operatorów modułu APK	Warsztaty	GZM	2 x 5	6	T/N
10.	Operatorów modułu MOB	Warsztaty	GZM	2 x 5	6	T/N

11.	Operatorów modułu MRTT	Warsztaty	GZM	2 x 5	6	T/N
12.	Operatorów modułu MDYS	Warsztaty	GZM	2 x 5	6	T/N
13.	Operatorów modułu MAR	Warsztaty	GZM	1x10	60 (10 dni)	N
14.	Administratorów Zamawiającego z zakresu architektury, procedur eksploatacyjnych,	Warsztaty	GZM	2 x 5	16 (3 dni)	N
15.	Operatorów modułu rozkładów jazdy MRJ	Warsztaty	GZM	1 x 10	6	T/N
16.	Administratorów Zamawiającego z zakresu modułu MDB	Warsztaty	GZM	1 x 5	12 (2 dni)	N
17.	Administratorów Zamawiającego z zakresu modułu AD	Warsztaty	GZM	2 x 5	12 (2 dni)	T/N
18.	Administratorów Zamawiającego z zakresu modułu MWD	Warsztaty	GZM	2 x 5	12 (2 dni)	N
19.	Administratorów Zamawiającego z zakresu modułu MMT	Warsztaty	GZM	2 x 10	6	T/N
20.	Platforma e-learning	Warsztaty	GZM	1 x 10	4	N

W ramach organizacji szkoleń Wykonawca musi przygotować materiały szkoleniowe (edytowalna wersja elektroniczna), udostępnić salę (w przypadku szkoleń zewnętrznych) i stanowiska na odpowiednią liczbę osób (nie dopuszcza się, aby było szkolonych jednocześnie więcej niż 20 osób). W przypadku omawiania urządzeń infrastruktury oczekuje się przedstawienia w pełni funkcjonalnej makiety urządzenia oraz oczekuje się umożliwienia osobie szkolonej przejścia pełnej ścieżki funkcjonalnej na urządzeniu. Wykonawca ma obowiązek przeprowadzenia egzaminu potwierdzającego umiejętności posługiwania się urządzeniem lub modułem oprogramowania.

Wykonawca przygotuje materiały szkoleniowe co najmniej na 14 dni roboczych przed rozpoczęciem szkolenia.

Miejsce odbywania się szkoleń:

- W przypadku wskazania GZM, Zamawiający zapewni salę na przewidzianą liczbę uczestników, rzutnik, dostęp do Internetu, do Wykonawcy należy zapewnienie zestawów komputerowych i makiet urzędzeń;
- W przypadku wskazania na zewnętrzne szkolenie, to Wykonawca zapewni salę na przewidzianą liczbę uczestników, rzutnik, dostęp do Internetu, zestawy komputerowe (o ile będzie taka potrzeba) i makiet urzędzeń.

Pozostałe wymagania:

- Szkolenia mogą się odbywać w dni robocze między godzinami 8:00-15:00 (chyba że Zamawiający uzgodni inaczej);
- Minimalny czas trwania szkolenie to 4 godziny (4x45 min, 15 minutowe przerwy pomiędzy);
- Maksymalny czas trwania szkolenia to 6 godzin (6x45 min, 15 minutowe przerwy pomiędzy) w ciągu jednego dnia, szkolenie nie może trwać dłużej niż 5 dni, nie dopuszcza się odbywania szkolenia w dniach nienastępujących po sobie;
- Zamawiający zastrzega sobie prawo do rejestracji audio sesji szkoleniowej oraz robienia zrzutów ekranów (w tym sekwencji ruchomych). Nie będzie rejestrowany wizerunek osób uczestniczących w szkoleniu.

Wykonawca może zaproponować inne formy, zakresy, podziały, szkoleń natomiast ostateczna decyzja będzie należała do Zamawiającego.

14.1 E-Learning

Wykonawca ma obowiązek przygotowania materiałów szkoleniowych oraz egzaminacyjnych z wykorzystaniem wybranej elektronicznej platformy szkoleniowej (e-learningowej), którą musi udostępniać i rozwijać przez okres utrzymania systemu. Przygotowane materiały muszą uwzględniać specyfikę i kompletną funkcjonalność poszczególnych urzędzeń i modułów, powinny zawierać informacje zawarte w dokumentacji użytkownika oraz o ile to możliwe grafiki i filmy instruktażowe. Platforma nie może być ograniczona co do liczby prowadzonych szkoleń ich powtórzeń lub co do liczby osób. Nadawanie dostępów będzie realizowane po stronie Zamawiającego. Zamawiający oczekuje możliwości weryfikacji postępów osób szkolonych, w tym potwierdzenia o pozytywnym lub negatywnym zakończeniu egzaminu. Egzamin powinien składać się z co najmniej z 20 pytań/zadań. Parametry zdawalności będą ustalane według uznania Zamawiającego. Platforma powinna pozwolić na wydrukowanie raportu oraz certyfikatu ukończenia kursu, egzaminu. Zamawiający zastrzega sobie prawo do modyfikowania treści szkoleń. Platformę e-learningową Wykonawca połączy z usługą serwera dokumentacyjnego jako źródła danych dla wybranych, udostępnianych na niej materiałów szkoleniowych by zapewnić spójność i aktualność wiedzy przekazywanej za pomocą publikowanych na platformie kursów.