

Příloha č. 1 Výzvy k účasti na předběžných tržních konzultacích

-

Technická specifikace

Předmět předběžných tržních konzultací:

Elektronické odbavení cestujících VDV



**Technická zadávací dokumentace na systém odbavení cestujících
v integrovaném dopravním systému Veřejná doprava Vysočiny**

Elektronické odbavení cestujících VDV

**Využití důvěryhodného identifikátoru ve formě nosiče dopravního
produktu**

Požadavky na řešení

Verze 1.5

Obsah

Obsah.....	3
1 Popis verzí.....	5
2 Použité zkratky a pojmy.....	5
3 Úvod.....	6
4 Obecné požadavky.....	7
5 Základní požadavky na architekturu systému	11
6 Typy identifikátorů v systému EOC.....	14
6.1 Bezkontaktní bankovní karta	14
6.2 2D čárový kód generovaný mobilní aplikací	14
6.3 Bezkontaktní čipové karty vydávané dopravcem	15
6.4 NFC čip v mobilním zařízení cestujícího.....	17
7 Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop).....	18
7.1 Základní funkce.....	18
7.2 Životní cyklus uživatele systému.....	19
7.3 Správa uživatelského profilu cestujícího	20
7.4 Registrace identifikátorů	20
7.5 Výběr a úhrada produktu	21
7.5.1 Výběr dle tarifu	21
7.5.2 Výběr pomocí kalkulatoru jízdného.....	21
7.5.3 Výběr pomocí vyhledávače spojení	21
7.6 Správa zakoupených produktů	22
8 Požadavky na systém administrace	23
8.1 Základní funkce.....	23
8.2 Správa subjektů a dopravců	23
8.3 Správa číselníků	23
8.4 Správa tarifu	25
8.5 Správa subjektů a dopravců jako uživatelů systému	25
8.6 Správa prodejních míst.....	26
8.7 Správa sestav	26
9 Požadavky na prodejní portál (prodejní místo –předprodej u dopravce)	28
9.1 Požadované funkcionality prodejního portálu	28
9.2 Ověřování uživatele (cestujícího)	28
9.3 Správa identifikátorů uživatele (cestujícího)	28
9.4 Správa zákaznických (uživatelských) profilů cestujících	29
9.5 Prodej dopravních produktů.....	29

9.6	Prodej doplňkových produktů	30
9.7	Účetní a statistické sestavy.....	30
10	Požadavky na systém mobilních zařízení pro revizory	31
11	Požadavky na odbavovací zařízení dopravců (strojky dopravců)	35
12	Popis whitelistů.....	38
12.1	Základní definice struktury dat.....	38
12.2	Zabezpečení osobních údajů	40
12.3	Číselníky tarifních dat	40
13	Popis požadavků na zúčtovací centrum.....	41
14	Popis požadavků na datovou komunikaci (způsob distribuce dat)	43
14.1	Datové rozhraní pro distribuci whitelistů	43
14.2	Datová komunikace s externími systémy dopravců	43
14.3	Datová komunikace s mobilními zařízeními revizorů	44
15	Bezpečnostní požadavky na systém	46
15.1	Obecné požadavky na návrh systému	46
15.2	Základní požadavky na zabezpečení komunikace	46
16	Požadavky na mobilní aplikaci systému elektronického odbavení cestujících.....	48
	Příloha č. 1 – Základní popis předpokládané implementace EOC ve VDV.....	51
	Příloha č. 2 – Požadavky na vytvoření jedinečného identifikátoru z údajů získaných z bezkontaktní karty	52

1 Popis verzí

- v. 1.0 - odevzdaná Administrátorovi (AK Fiala – Tejkal) k posouzení
- v. 1.1 - dodatečně upraveny všechny kapitoly (1 až 15), přílohy 2,3,5 a přidány poznámky k textu
- v. 1.2 – verze pro PTK, zapracovány některé poznámky k textu z veze 1.1
- v. 1.3 – verze pro PTK, zapracovány podklady k revizorským čtečkám, rozšířen seznam zkratk, doplněn harmonogram, změna počtu příloh
- v. 1.4- verze pro PTK, formální úpravy v textu, zapracování dalších připomínek a doplňování komentářů
- v. 1.4.1 - doplněny a upraveny některé komentáře na základě porady z 15. dubna
- v. 1.4.2 – doplněny a vypořádány komentáře externího poradce
- v. 1.5 - totožná s verzí 1.4.2, pouze odstraněny komentáře

2 Použité zkratky a pojmy

Bezkontaktní Karta (BK)	Identifikátor zákazníka v systému elektronického odbavení cestujících
Black list (BL)	Seznam zakázaných (karet nebo kupónů)
BPK	Bankovní platební karta
BČK	Bezkontaktní čipová karta dopravce
DESfire EV1	Standard/produkt bezkontaktní čipové karty, jehož dodavatelem je společnost NXP Semiconductors N.V.
DPMJ	Dopravní podnik města Jihlavy
EOC	Elektronické odbavení cestujících
Green list (GL)	Seznam aktuálně povolených záznamů (karet nebo kupónů)
HSM	Hardware Security Modul
IIN	Normalizované identifikační číslo vydavatelů karet
IK	In Karta ČD standardu MAP
JD	Jízdní doklad
KV	Kraj Vysočina
MAP	Technické řešení multiaplikační bezkontaktní čipové karty, jehož dodavatelem je společnost ODP-software s.r.o.
PAD	Příměstská autobusová doprava
Panmas	Zkrácené číslo BPK (Prvních 6 a poslední 4 pozice z čísla karty)
REST	Representational State Transfer

SAM	Secure access module, zařízení je určené k bezpečnému uložení kryptografických klíčů a citlivých informací, vnitřní software tohoto zařízení poskytuje kryptografické a jiné funkce k zajištění bezpečných operací nad chráněnými daty
SOAP	Simple Object Access Protocol
SPP	Smluvní a přepravní podmínky
Taplist	Seznam přiložených karet (využívá se u BPK standardu EMV)
TOKEN	Jedinečný identifikátor bezkontaktní karty
VDV	Integrovaný dopravní systém Veřejné dopravy Vysočiny
White list (WL)	Seznam povolených záznamů (karet nebo kupónů)

3 Úvod

Cílem nově požadovaného systému je zajištění elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny (dále jen VDV). Primární funkcí tohoto systému je nákup dopravního produktu (například dlouhodobé předplatné, jednorázová jízdenka) a jeho přiřazení k libovolnému důvěryhodnému identifikátoru (například: bezkontaktní bankovní kartě, QR kódu v aplikaci mobilního telefonu, bezkontaktní paměťové čipové kartě standardu Mifare/DESfire EV1 vydávané cizím subjektem).

Použitím libovolného důvěryhodného identifikátoru budeme pro účel tohoto dokumentu chápat přiřazení již zmiňovaného identifikátoru k zakoupenému produktu (jednorázové jízdenky, dlouhodobému časovému kupónu, apod.), tj. výsledkem výše uvedeného procesu bude vytvoření strukturovaného souboru dat „whitelistu“, který obsahuje informace o držiteli identifikátoru, zakoupených produktech, slevové kategorii cestujícího apod. Tento soubor dat bude dále použit pro vyhodnocení nároku na přepravu v IDS VDV.

V požadovaném řešení je kladen důraz na samoobslužné odbavení cestujících. Systém musí obsahovat webový portál (webovou aplikaci) a mobilní aplikaci, která bude sloužit pro samoobslužné odbavení cestujících, tj. uživatel systému realizuje veškeré činnosti (například: správu vlastního účtu a identifikátorů, nákup dopravního produktu, apod.) prostřednictvím výše zmíněné webové a mobilní aplikace bez nutnosti návštěvy zákaznického centra dopravce. Vybudované řešení musí být univerzální a použitelné i pro dalšího zapojeného partnera (dopravce) v maximálně možné míře.

4 Obecné požadavky

Řešením elektronického odbavení cestujících v integrovaném dopravním systému Veřejné dopravy Vysočiny se pro účel této části zadávací dokumentace rozumí:

1. **Vybudování systému elektronického odbavení cestujících dle požadavků, které jsou uvedeny níže v tomto dokumentu.**

Poznámka

Nově navržený systém musí naplňovat veškeré požadavky dané integrovaným tarifním Systémem Veřejné dopravy Vysočiny (jeho definice je popsána v Příloze č. 1 - Základní popis integrovaného dopravního systému Veřejné dopravy Vysočiny)

2. **Zpracování projektové dokumentace jednotlivých částí systému v rozsahu:**

- Cílový koncept řešení (popisující podrobný návrh řešení díla a jeho jednotlivých funkcí)
- Prováděcí dokumentace (Dokumentace skutečného provedení díla)

3. **Zpracování Bezpečnostního projektu v rozsahu:**

- Zabezpečení klíčů pro generování tokenu
- Systém práce se SAM moduly (bezpečné úložiště přístupových klíčů k datovým sektorům bezkontaktní čipové karty dopravce zapojeného do systému)
- Zabezpečení přístupových klíčů k datovým sektorům bezkontaktní čipové karty dopravce zapojeného do systému (tj. řešení systému bez využití SAM)
- Zabezpečení datové komunikace celého řešení
- Zabezpečení systému elektronického odbavení cestujících proti ztrátě a odcizení dat
- Správu a řízení oprávnění uživatelů (obsluha zákaznického centra) systému elektronického odbavení cestujících
- Zabezpečení odbavovacích míst (zákaznická centra) systému elektronického odbavení cestujících

Poznámka

(Bezpečnostní projekt nově budovaného systému musí být zpracován ve vazbě na již existující bezpečnostní projekty Objednatele, které jsou tímto systémem dotčeny).

4. Předpokládaný harmonogram dodávky včetně stanovení hlavních milníků projektu

Etapizace	Název	Charakteristika	Předpoklad časové náročnosti (měsíce)
Etap 0	Předprojektová příprava	• Příprava Zadávací dokumentace • Provedení předběžných tržních konzultací • Provedení veřejné obchodní soutěže • Uzavření smluvního vztahu s dodavatelem platební brány (bankou) • Uzavření (zveřejnění) smluvního vztahu s dodavatelem EOC (okamžik T0)	T0
Etap 1	Projektování	• Zpracování prováděcího projektu • Příprava testovacího prostředí • Zajištění vybavení a součinnosti zadavatele • Zajištění vybavení a součinnosti dopravců	T0 až T0+3
Etap 2	Vývoj a implementace	• Vývoj základního jádra zúčtovacího systému • Vývoj mobilní aplikace • Vývoj webové aplikace • Vývoj revizorského systému • Implementace zadané platební brány • Instalace HW a SW do prostředí Kraje Vysočina	T0+3 až T0+7
Etap 3	Testování	• Testování řešení dílčích částí systému dodavatelské testy • Beta testování u zadavatele • Pilotní provoz • Zahájení rutinního provozu	T0+7 až T0+9

Jako čas T0 je považován den uveřejnění smlouvy s dodavatelem

5. Integrace dodaného řešení do odbavovacího systému společnosti České dráhy a.s.

6. Zaškolení pracovníků zadavatele pro užívání a správu systému

7. Návrh pravidel budoucího update a upgrade systému, včetně jeho profylaxe

8. **Návrh servisních podmínek (záručních, mimozáručních, pozáručních) vč. uvedení reakční doby na incident. Po vzájemném odsouhlasení budou tyto podmínky uvedeny v závazné servisní smlouvě.**
9. **Dodání dokumentace systému – příručky obsluhy systému, příručka administrátora systému, technické výkresy a schémata řešení, dokumentace popisující možnosti a limity systému, postupů zálohování a obnovy systému apod.**

Řešení projektu jako celek bude mít formu tří vrstvé architektury:

- Prezentační vrstva (například: e-shop, aplikace pro správu systému, mobilní aplikace)
- Aplikační vrstva – vlastní funkce/logika systému
- Datová vrstva (databáze osobních dat uživatelů systému a jejich identifikátorů, databáze prodejních transakcí, databáze číselníků a tarifních dat)

Požadavky kladené na systém EOC VDV:

- Systém bude dimenzován pro minimálně 500.000 uživatelů
- Systém bude dále dimenzován pro minimálně 9.5 milionu prodejních transakcí za kalendářní rok
- Řešení musí umožnit zapojení minimálně 200 odbavovacích přepážek dopravců (jedná se o kontaktní místo určené pro odbavení klienta, vyřizování reklamací, apod.)
- Dostupnost systému bude 24/7
- Systém bude provozovaný v geograficky oddělených lokalitách
- Data systému budou pravidelně zálohována
- Rozhraní pro předávání dat (například: strukturovaných souborů pro odbavovací zařízení ve voze dopravce) bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy. Je však nutné dodržet vysoké bezpečnostní standardy tohoto řešení.
- Veškerá datová komunikace bude šifrovaná
- Osobní údaje budou v databázi uchovávány v šifrované podobě s oddělením identifikátorů a osobních údajů

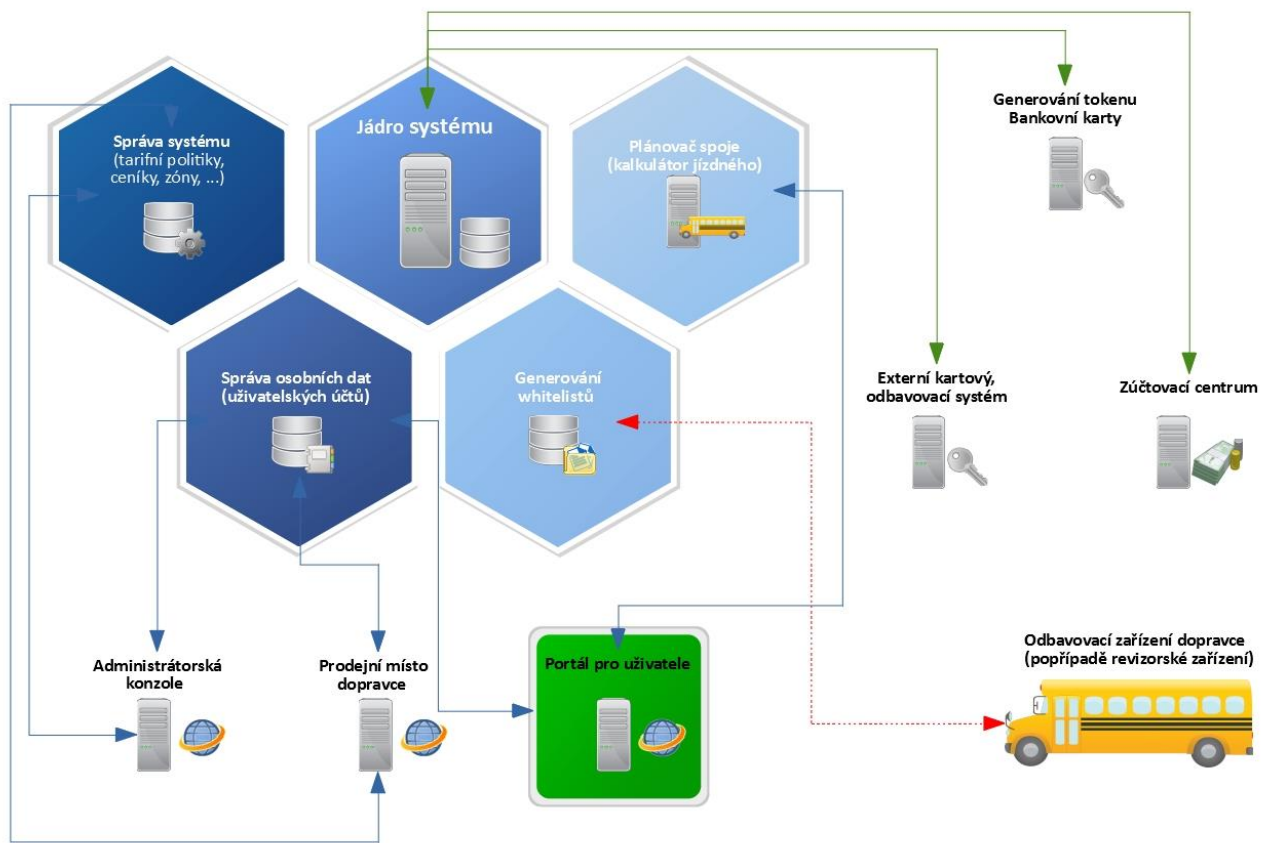
- Zadavatel požaduje instalaci a provozování nově vybudovaného systému ve vlastním serverovém prostředí (tj. hardwarovém, softwarovém a síťovém prostředí).

Předpokládané kapacity Technologického centra KV:

Řešení bude provozováno v Technologickém centru Kraje Vysočina v prostředí serverové virtualizace (farma VMware vSphere Enterprise verze 6+) typicky na serverové platformě MS Windows 2016. Předpokládaný výkon alokovaný z fyzických hostů všemi virtuálními stroji (cca 6 kusů VM, libovolný OS podporovaný VMWarem) je 6 GHz CPU, max. spotřeba paměti RAM je 200GB GB, disková storage SSD max 2TB, NLSAS max 20TB. K dispozici jsou mechanismy vysoké dostupnosti (HA režim VMW), síťové ochrany VMWare NSX, Web Application Firewallu (F5 BIG IP) a zálohování je zajištěno nativními nástroji použité serverové virtualizace, systémem Veeam. Licence OS Microsoft Windows Server Datacenter a sdíleného MS SQL 2016 Standard serveru jsou zajištěny zadavatelem.

Zhotovitel je povinen Zadavateli předložit požadavky na zajištění odpovídající a přiměřené serverové části na provozování systému elektronického odbavení cestujících.

5 Základní požadavky na architekturu systému



Požadavky na systém elektronického odbavení cestujících shrnuje výše uvedené schéma.

Jádro systému

Základní prvek systému, zajišťující vlastní aplikační logiku celého systému, musí plnit minimálně tyto funkce:

- Výpočet jízdného (stanovení ceny za produkt)
- Správa životního cyklu uživatele systému EOC VDV
- Správu životního cyklu karty a ostatních identifikátorů EOC VDV
- Správu tarifní politiky integrovaného dopravního systému VDV
- Generování strukturovaných souborů- whitelistů

- Komunikaci s externími systémy při procesu ověřování Identifikátorů EOC VDV
- Generování jedinečných identifikátorů
- Integraci s platebními metodami (e-Commerce platební brána, automatizované zpracování převodních příkazů)
- Komunikaci s externími kartovými a odbavovacími systémy při procesu prodeje dopravního produktu pro uživatele systému
- Příprava a distribuce dat pro zúčtovací systém

Správa systému

musí zajišťovat minimálně následující funkce:

- Správu subjektů a dopravců zapojených do systému
- Definici a správu jednotlivých číselníků (typy identifikátorů, zákaznické kategorie, tarify, zóny, ceníky pro jednotlivé tarify, trasy a linky, zastávky, účetní položky, sazby DPH, apod.)
- Administraci jednotlivých dopravních produktů dle tarifní politiky VDV (včetně parametrů, které jsou nutné k realizaci prodeje dopravního produktu)

Správa osobních dat

musí zajistit minimálně následující funkce:

- Bezpečné uchování osobních dat uživatelů systému (archiv osobních údajů)
- Realizovat změnové požadavky při správě osobních údajů (změna jména, příjmení, fotografie, apod.)

Ostatní části systému

požadavky na ostatní části systému jsou dále podrobně popsány v jednotlivých kapitolách:

- Portál zákazníka, e-shop – uvedeno v kapitole 7
- Administrátorská konzole – uvedeno v kapitole 8
- Prodejní místo u dopravce – uvedeno v kapitole 9
- Požadavky na systém mobilních zařízení pro revizory – uvedeno v kapitole 10
- Odbavovací zařízení dopravce – uvedeno v kapitole 11
- Generování whitelistu – uvedeno v kapitole 12
- Zúčtovací centrum – uvedeno v kapitole 13
- Popis požadavků na rozhraní systému (kalkulátor jízdného, napojení na externí odbavovací systémy) – uvedeno v kapitole 14

6 Typy identifikátorů v systému EOC

6.1 Bezkontaktní bankovní karta

Jedná se o jeden z možných identifikátorů zákazníka v systému elektronického odbavení cestujících. Z důvodu komfortního a rychlého odbavení držitele karty v odbavovacím zařízení ve voze veřejné dopravy budou v systému využity pouze bankovní karty bezkontaktní.

Odbavení karet v odbavovacím zařízení ve vozech veřejné dopravy/platebním terminálu bude řešeno v tzv. *off-line režimu*. Tento způsob odbavení ovlivňuje parametry nastavené na čipu bankovní karty. Parametry definují např. off-line limity pro počet a objem transakcí, které lze provést bezkontaktně, aniž by bylo vyžadováno potvrzení PINem v rámci tzv. online transakce.

Bankovní karty, které budou integrovány do nově budovaného systému:

- Bezkontaktní bankovní karta (možno použít také hybridní bankovní karty obsahující: magnetický proužek, kontaktní a bezkontaktní čip)
- Kreditní, debetní a předplacená bankovní karta vydaná asociací Mastercard, VISA (popřípadě další: Diners Club)
- Bankovní karta vydaná ve formě „mezinárodní karty“ (mezinárodně akceptované bankovní karty) nebo „domácí karty“ (bankovní karty akceptované pouze na území České republiky)

Požadavky na získání jedinečného identifikátoru z bezkontaktní bankovní karty:

V systému elektronického odbavení cestujících bude využita pouze identifikační funkce karty, tj. z vyčtených údajů z bankovní karty bude vytvořen unikátní identifikátor. Z takto vytvořeného identifikátoru nebude možné standardním způsobem zpětně zjistit zdrojová data získaná z bankovní karty.

Požadavky na vytvoření jedinečného identifikátoru bankovní karty jsou uvedeny v příloze č. 2

6.2 2D čárový kód generovaný mobilní aplikací

Další možností vytvoření jedinečného identifikátoru v systému EOC bude vygenerování tohoto identifikátoru prostřednictvím mobilní aplikace.

Požadavky na získání jedinečného identifikátoru z mobilní aplikace:

- Jedinečný identifikátor (token) bude počítat platební brána (respektive SAM) stejně jako u ostatních identifikátorů. Algoritmus zůstává stejný jako u bezkontaktních karet. (mobilní aplikace by jen měla být odlišena jiným prefixem v prvním bytu na vstupu). Identifikátor bude jedinečný pro každou jednotlivou instalaci mobilní aplikace v telefonu i v rámci jednoho uživatelského účtu (z uvedeného vychází i požadavek na unikátnost v rámci instalace do různých mobilních zařízení)
- Identifikátor(-y) bude(budou) automaticky přiřazen(-y) k účtu uživatele (pro možnost nákupu a přiřazení dopravního produktu)

Systém elektronického odbavení cestujících musí zajistit rozlišení tohoto typu identifikátoru.

Prezentace jednoznačného identifikátoru bude v mobilní aplikaci realizována prostřednictvím 2D čárového kódu (například QR kód). Takto generovaný kód musí být zabezpečen možností ověření získaných dat (například budou data elektronicky podepsána pomocí asymetrické kryptografie).

Mobilní aplikace, která bude tento 2D čárový kód zobrazovat musí zajistit ochranu proti vytvoření tzv. snímku obrazovky (například: využitím dynamického 2D čárového kódu, apod.)

6.3 Bezkontaktní čipové karty vydávané dopravcem

Hlavní požadavkem této funkcionality je využití existujících dopravních karet (bezkontaktních čipových karet) jejichž vydavateli jsou subjekty poskytující veřejnou dopravu na území IDS VDV.

Dopravní karty, které budou integrovány do nově budovaného systému:

- In Karta (nový typ karty typu/standardu MAP)
 - Vydavatelem je společnost České dráhy a.s.
 - Technologie: DESfire EV1 8kB
 - Rozlišení nového typu karty: symbol MAP ready (grafický prvek vytištěný na kartě)
 - Typ vydávané karty: personalizovaná a nepersonalizovaná karta (pro registrované uživatele dle kap 7.2)
 - Dále lze karty rozlišit dle použití: zákaznická karta (personalizovaná), služební karta (personalizovaná), business karta (nepersonalizovaná karta)

- Karta je vydávána s platností 5 let
- Identifikační údaje na kartě (personalizované): Jméno, příjmení, datum narození, fotografie držitele karty, unikátní číslo vydané karty a platnost karty
- Jihlavská karta
 - Vydavatelem je společnost Dopravní podnik města Jihlavy, a.s.,
 - Technologie: DESfire 4kB
 - Typ vydávané karty: personalizovaná a nepersonalizovaná karta
 - Karta je vydávána s platností 4 roky
 - Identifikační údaje na kartě (personalizované): Jméno, příjmení, fotografie držitele karty, unikátní číslo vydané karty

Požadavky na získání jedinečného identifikátoru z IN Karty:

Registrace karty do systému bude realizována na základě vyplnění unikátního čísla karty (18-místné číslo karty definované dle ISO/IEC 7812-1, postup přidělování tohoto čísla pak normou ISO/IEC 7812-2) a platnosti karty (oba údaje jsou vytištěny na kartě).

- Systém následně ověří platnost zadaného čísla karty za použití metody Luhnův algoritmus (tj. shoda výpočtu s kontrolní číslicí 18. pozice v čísle karty). Dále ověří, zda je karta platná.
- Po vyhodnocení výše uvedených dat bude vygenerován jednoznačný identifikátor (obdobným způsobem, který je uveden v případě bankovní karty). Specifikace algoritmu je uvedena v příloze č. 2

Požadavky na získání jedinečného identifikátoru z Jihlavské karty:

- Registrace karty do systému bude realizována na základě vyplnění unikátního čísla karty, případně iniciálu jména, příjmení držitele karty.

- Pro výpočet vstupních dat do tokenizačního algoritmu bude využito pouze UID karty (resp. číslo Jihlavské karty)
- Systém následně prostřednictvím externí webové služby ověří platnost zadaného čísla karty. Externí webová služba poskytne vstupní data pro vygenerování jednoznačného identifikátoru. Specifikace algoritmu je uvedena v příloze č. 2

Zapojení karet dalších dopravců do systému EOC VDV

Systém musí být navržen tak, aby umožňoval budoucí zapojení dalších dopravců, u kterých mohou být použity odbavovací technologie využívající BPK, nebo karty Mifare (Standard, nebo DesFire).

6.4 NFC čip v mobilním zařízení cestujícího

Jedná se o jeden z možných identifikátorů zákazníka v systému elektronického odbavení cestujících prostřednictvím NFC technologie v mobilních telefonech (dle ISO Standardu 18092 s požadavkem zpětné kompatibility na ISO 14443). Čip v telefonu je na bázi NFC, v tomto případě předpokládáme funkci jako u čipu BPK a tím může sloužit jako identifikátor. Pro chytré telefony je také dostupná řada mobilních aplikací, které slouží pro uložení a manipulaci BPK v telefonu.

7 Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop)

7.1 Základní funkce

Tuto část systému je nutné navrhnout formou webové aplikace. Z pohledu bezpečnosti je nutné použití zabezpečené komunikace se severem prostřednictvím https protokolu.

Webová aplikace musí být vytvořena principem responzivního designu webu (tj. aplikaci bude možné „použít“ i v mobilním telefonu, tabletu, apod.) Aplikace musí být použitelná ve všech aktuálně dostupných internetových prohlížečích.

Základní požadavky kladené na samoobslužný systém odbavení zákazníků (portál zákazníka, e-shop) :

- Založení a správa uživatelského účtu zákazníka (vč. podúčtů celého platebního systému)
- Funkce registrace (přiřazení jednoznačného identifikátoru k účtu uživatele)
- Správu identifikátorů
- Správa zakoupených produktů
- Správa zákaznických profilů/kategorií
- Nákup a úhrada dopravního produktu
- Systém musí umožňovat budoucí rozšíření o funkci automatické registrace a autentizace prostřednictvím elektronické identity s úrovní záruky střední a vysoká dle zákona 250/2017 Sb. o elektronické identifikaci (např. elektronickým Občanským průkazem)

7.2 Životní cyklus uživatele systému

Každý uživatel (cestující), který bude evidován v systému EOC, musí být zařazen do jedné z níže uvedených kategorií:

Definice kategorie uživatele

- **Uživatel registrovaný**, došlo k vyplnění a následnému ověření přihlašovacích údajů v rozsahu: jméno (emailová adresa uživatele) a heslo
- **Uživatel personalizovaný**, došlo k vyplnění osobních údajů, minimálně v tomto rozsahu:
 - Jméno a příjmení
 - Datum narození
 - Bydliště
 - Fotografie (rozměr průkazové fotografie, systém musí ověřovat formát a kvalitu vloženého souboru)
 - V případě uživatele, který ještě nedosáhl věku 15 let, bude nutné doplnit i osobní údaje zákonného zástupce
- **Uživatel s platným účtem**, došlo k ověření osobních údajů klienta (například prostřednictvím kontaktního místa, automatických procesem, apod.)

Pokud se uživatel systému rozhodne upravit vlastní osobní údaje (například jméno, příjmení nebo fotografii), které již byly ověřeny, tak bude nutné tento stav identifikovat a zamezit neoprávněné manipulaci s účtem, tj. stav přesunout do „nižší“ kategorie – Uživatel personalizovaný.

Každý z výše uvedených stavů musí být v systému zohledněn v podobě rozsahu nabízených služeb (například: registrovaný (anonymní) uživatel nebude mít možnost nákupu nepřenositelného typu dopravního produktu, naopak uživatel s platným účtem bude mít možnost nákupu také přenosných typů dopravních produktů.

Definice zákaznického (uživatelského) profilu cestujícího

Zákaznickým profilem budeme pro účel tohoto dokumentu chápat identifikaci slevové (nebo jiné) kategorie, která je uživateli systému (držiteli karty) přiznána na základě pravidel uvedených ve Smluvních přepravních podmínkách VDV. Dále je možné výše uvedené označit *jen zkratkou CP „Customer Profile“*. Vlastní číselník zákaznických profilů vychází z EN 1545-1.

7.3 Správa uživatelského profilu cestujícího

Z pohledu prokázání nároku na nákup daného typu dopravního produktu je nutné uživateli systému přiřadit tzv. uživatelský profil (například: dospělý, dítě, student, důchodce, ZTP, apod.).

Způsoby přiřazení uživatelského profilu:

- Automaticky přiřazen (například uživatelský profil- dospělý)
- Přiřazen na základě správcem systému schválené žádosti podané ze strany uživatele systému

Portál pro uživatele musí zajistit možnost podání žádosti o přiřazení uživatelského profilu (žádost bude uživateli systému automaticky nabídnuta v případě splnění věkového nebo jiného omezení pro daný profil). Vlastní proces schválení žádosti již bude probíhat v části systému „Prodejní místo“.

7.4 Registrace identifikátorů

Uživateli systému (bez ohledu na kategorii uživatele) bude umožněno přiřazení libovolného počtu nabízených typů identifikátorů.

Uživateli systému musí být umožněno realizovat zablokování identifikátoru v případě jeho ztráty, krádeže, apod.

Při prvotní on-line registraci libovolného identifikátoru (jen a pouze při prvotní registraci), platební brána generuje token. Vypočtený token zasílá do Backoffice VDV. Vlastní výpočet tokenu tedy bude realizován prostřednictvím přesměrování na platební bránu banky, kterou určí Objednatel.

- Podrobný popis výpočtu jedinečného identifikátoru (tokenu) při registraci bezkontaktní karty v systému je uveden v příloze č .2 *Požadavky na vytvoření jedinečného identifikátoru z údajů získaných z bezkontaktní karty.*

7.5 Výběr a úhrada produktu

Systém musí zajistit výběr dopravních produktů dle tří níže uvedených postupů.

7.5.1 Výběr dle tarifu

Uživateli systému bude umožněn nákup dopravního produktu dle aktuálně přiřazeného zákaznického (uživatelského) profilu, tj. bude zobrazena nabídka všech tarifů, které se vážou k profilu uživatele. Na základě realizovaného výběru tarifu bude uživateli dále nabídnuto období platnosti a možnost výběru územní platnosti.

7.5.2 Výběr pomocí kalkulátoru jízdného

Uživateli systému bude umožněn nákup dopravního produktu, jehož definici určí na základě zvolené trasy, přiřazeného zákaznického profilu a období platnosti. Na základě zpracování tohoto požadavku datovým rozhraním „Kalkulátoru jízdného“ bude uživateli nabídnut nejvhodnější produkt včetně stanovení jeho ceny v tarifu VDV.

7.5.3 Výběr pomocí vyhledávače spojení

Uživateli systému bude umožněn výběr vhodného spojení (zvolené trasy) pomocí vyhledávače spojení. Řešení musí být navrženo tak, aby bylo možné na základě zvolených začátečních a koncových stanic cesty, zákaznického profilu a období platnosti nabídnout uživateli nákup nejvhodnějšího dopravního produktu v tarifu VDV, včetně možnosti prodeje prostřednictvím e-shopu.

Vlastní úhrada za produkt bude řešena formou:

- On-line transakce prostřednictvím platební brány
- Převodním příkazem (a následným automatickým párováním platby, tj. zpracováním datových souborů avíz získaných z rozhraní banky). Platební informace (potvrzení o platbě) bude zaslána uživateli na email, který uvedl při založení účtu. Zadavatel požaduje garanci úhrady jízdního dokladu před zahájením jeho platnosti (např. Dokončení nákupu bude podmíněno odesláním převodního příkazu)

Zjednodušený daňový doklad o realizované úhradě dopravního produktu bude uživateli zaslán na email, který uvedl při založení účtu.

7.6 Správa zakoupených produktů

Uživateli systému musí být umožněno zobrazení transakční historie zakoupených (platných/neplatných) dopravních produktů.

Transakční historie musí obsahovat minimálně:

- Stav produktu (platný/neplatný, stornováno, neuhrazeno, apod.)
- Typ produktu
- Časová platnost
- Územní platnost
- Zákaznický profil
- Datum a čas pořízení produktu, datum a čas úhrady produktu
- Typ platební metody

Uživateli systému bude dále umožněno:

- Požádat o storno produktu (jehož platnost nebyla zahájena), nebo o přerušení aktuálně platného produktu. Vlastní proces vyřízení této žádosti musí být následně realizován prostřednictvím pracovníka obsluhy systému v části „Prodejní místo“
- Přeřadit aktuálně platný produkt (popřípadě platný v budoucnosti) na libovolný typ zaregistrovaného a platného identifikátoru v účtu uživatele. Tento proces nebude možno realizovat s okamžitou účinností z důvodu času nutného pro vygenerování a distribuci whitelistu do akceptačních zařízení dopravců.

8 Požadavky na systém administrace

8.1 Základní funkce

Administrátorská část systému bude určena pro základní definici hodnot nutných pro správu subjektů a dopravců zapojených do systému, dále musí zajistit možnost stanovení tarifních ukazatelů nutných pro vytvoření dopravního produktu určeného k prodeji prostřednictvím e-shop zákaznického portálu. Minimální požadavky na administraci celého systému jsou uvedeny níže v jednotlivých bodech.

8.2 Správa subjektů a dopravců

Pro každý partnerský subjekt nebo každého dopravce, který je zapojen do systému EOC musí existovat záznam určující rozsah jeho oprávnění k vykonávání jednotlivých funkcí systému (prodej dopravního produktu, ověřování osobních dat uživatelů, právo schválení zákaznické kategorie, apod.).

Oprávnění každého subjektu nebo každého dopravce musí v systému definovat:

- Samostatná skupina oprávnění pro obsluhu systému

Pro každý subjekt nebo každého dopravce musí být v systému vytvořeny minimálně tyto funkcionality:

- Samostatná evidence prodeje dopravních produktů
- Účetní a statistický reporting vázaný k danému subjektu/dopravci
- Samostatné generování a distribuce dat do zúčtovacího centra

8.3 Správa číselníků

Pro vlastní definici jednotlivých dopravních produktů/tarifů bude nutné v systému umožnit správu vstupních dat. (tyto data určují parametry pro nabízení a prodej dopravních produktů, popřípadě definují vazby mezi těmito parametry).

Systém musí obsahovat správu minimálně těchto číselníků:

- Dopravní produkt/Tarif bude obsahovat minimálně atributy:
 - Identifikace tarifu
 - Slovní označení tarifu

- Typ tarifu (definice časové období určující jeho platnost, například na pevný počet dnů, volitelný počet dnů, apod.)
- Příslušnost ke kategorii cestujících
- Vazbu na územní platnost (definice dle zónově relačního tarifu)
- Propojení na ceník
- Definice parametrů určující vlastní nabízení a prodej dopravního produktu
- Ceník dopravního produktu/Tarifu bude obsahovat minimálně atributy:
 - Identifikaci ceníku
 - Platnost ceníku
 - Účinnost ceníku
- Kategorie cestujících bude obsahovat minimálně atributy:
 - Identifikátor kategorie cestujících (číselník musí vycházet z EN 1545-1)
 - Slovní označení kategorie cestujících
 - Platnost kategorie cestujících
 - Definice nároku dle věkového omezení
 - Vazbu na stav účtu uživatele
- Definice zóny bude obsahovat minimálně atributy:
 - Identifikace zóny
 - Slovní označení zóny
 - Vazba na nadzóny
 - Počet tarifních jednic v zóně
 - Vazba na hraniční zastávky/referenční zastávku v zóně

- Definice nadzóny bude obsahovat minimálně atributy:
 - Identifikace nadzóny
 - Slovní označení nadzóny
- Číselník zastávek
- Číselník linek/spojů
 - Možnost definice povolené trasy v rámci výčtu zón
- Číselník typů dokladů (příjmový, výdajový, reklamační, apod. včetně definice číselných řad)
- Číselník sazeb DPH

8.4 Správa tarifu

Tato část systému musí zajistit vlastní sestavení/definici dopravního produktu dle zvolených hodnot vycházejících z výše uvedených číselníků (například určením vazby mezi tarifem, kategorií cestujícího, definicí územní platnosti a ceníkem).

Nově navrhovaný tarif bude možné přiřadit k využití (nabízení k prodeji) u definovaného subjektu, popřípadě konkrétně specifikovaného prodejního místa.

8.5 Správa subjektů a dopravců jako uživatelů systému

Oprávnění každého subjektu nebo každého dopravce musí v systému definovat samostatná skupina oprávnění pro přístup do systému. Uživatelské přístupy do systému se budou realizovat prostřednictvím rolí, které definují oprávnění k jednotlivým funkcionalitám systému (tj. podle povahy činnosti uživatele v systému).

Základní uživatelské role a příslušná oprávnění jsou následující:

- Administrátor systému
- Správce subjektu
- Pracovník prodejního místa

- Správce prodejního místa
- Pracovník informační přepážky

Každou roli bude možné přiřadit/definovat samostatně pro konkrétní subjekt/dopravce zapojeného do systému.

Využití Identity managementu KV

Pro získání oprávnění uživatelů a jejich metadat (autorizace) bude využit Identity management KV (IDM AC Identita). IDM má vystaveno uživatelské rozhraní (API) ve formě web služeb SOAP (WS). Aplikace získává profil daného uživatele včetně oprávnění (rolí) prostřednictvím API na IDM KV, ukládá tyto parametry do svého interního nástroje správy uživatelů a v proceduře autorizace přiděluje na základě úspěšné autorizace příslušná oprávnění. V aplikaci budou vytvořené 2 tabulky, které budou obsahovat data o prováděných synchronizacích mezi aplikací a API IDM. První tabulka bude souhrnná a bude obsahovat záznamy o provedených synchronizacích (id, začátek synchronizace, konec synchronizace, stav (OK, Error), druhá tabulka bude detailová a bude obsahovat změněné záznamy v rámci dané synchronizace (ID, ID_synchronizace, změna, stav (Ok,Error)). Dané tabulky budou sloužit k napojení na monitorovací systém Kraje Vysočina (PRTG) a jejich přesnou definici poskytne zadavatel v rámci implementace, výše uvedené hodnoty jsou pouze demonstrativní.

8.6 Správa prodejních míst

Nabídka a prodej dopravních produktů bude (mimo jiné) prováděn prostřednictvím dvou hlavních prodejních kanálů systému. E-shopu zákazníka (portálu zákazníka) a prodejního místa dopravce.

Každý subjekt/dopravce zapojený do systému bude mít definován vlastní seznam prodejních míst (například z důvodu rozlišení prodejních míst do logických celků). Uvedené členění bude realizováno i z důvodu účetní evidence transakcí (prodeje produktů koncovým zákazníkům) za jednotlivá prodejní místa subjektu/dopravce a přípravy dat pro zúčtování prostřednictvím zúčtovacího centra, tj. prodejní místa je nutné označit jednoznačným identifikátorem v rámci daného subjektu/dopravce včetně vlastní transakční/dokladové číselné řady.

U každého dopravního produktu bude možné určit jeho vazbu k prodejnímu místu.

8.7 Správa sestav

Systém musí zajistit generování účetních a statistických sestav minimálně v níže uvedeném rozsahu:

- Účetní uzávěrky (souhrn prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu). Sestava musí obsahovat sumu za prodej/storno dle jednotlivého typu produktu, platební metody, uživatele/prodejního místa/subjektu).
- Seznam všech prodejních transakcí (přehled prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu)
- Seznam všech objednávek produktů prostřednictvím e-shop (přehled objednávek, dle definovaného období, typu produktu, platební metody, stavu objednávky /zaplaceno, čeká na zaplacení z platební brány, stornováno, apod./)
- Statistická sestava počtu prodaných dopravních produktů dle jednotlivého tarifu a zákaznické kategorie (přehled minimálně dle definovaného období)
- Statistická sestava o počtu evidovaných identifikátorů v systému z pohledu jejich platnosti platný/blokovaný/vyřazený z důvodu překročení platnosti (přehled minimálně dle definovaného období)
- Statistická sestava o počtu evidovaných identifikátorů v systému dle typu bankovní karta/2D kód/dopravní karta/NFC (přehled minimálně dle definovaného období)
- Statistická sestava o počtu registrovaných uživatelů v systému z pohledu stavu účtu (přehled minimálně dle definovaného období)
- Statistická sestava – demografická data o uživatelích systému (přehled minimálně dle definovaného období)

Systém dále umožní generování vlastních uživatelských sestav na základě dostupných nástrojů „generátorů sestav“ (v rámci přípravy Cílového konceptu budou stanoveny/popsány datové matice určené pro využití v generátoru sestav).

9 Požadavky na prodejní portál (prodejní místo –předprodej u dopravce)

Požadovaný způsob pro návrh aplikace prodejního místa (prodejního portálu)

Portál je určen pro využívání na počítačích dopravců, na pokladních předprodejních místech dopravců. Portál bude vytvořen prostřednictvím webové aplikace, která bude přístupná ze sítě Internet na základě definovaného/povoleného rozsahu IP adres. Z pohledu bezpečnosti bude nutné využití zabezpečené komunikace se serverem prostřednictvím https protokolu. Přístupová oprávnění k aplikaci budou řešena na úrovni Administrátorské části systému. Navržené řešení musí zajistit zprovoznění prodejního místa u dopravce bez velkých nároků na hardwarové a softwarové vybavení. Součástí vybavení prodejního místa bude tiskárna pro tisk prodejních dokladů, zařízení pro skenování dokladů a fotoaparát pro zhotovení fotografie uživatele (cestujícího)

9.1 Požadované funkcionality prodejního portálu

Obsluhu portálu bude umožněno (dle typu oprávnění) minimálně:

- Vyhledání detailu uživatele (s možností definice filtru: jméno, příjmení; uživatelské jméno)
- Úprava osobních dat uživatele včetně pořízení (například webovou kamerou, apod.) a výměny fotografie
- Zrušení účtu
- Vytvoření dodatečných údajů k účtu uživatele (například formou poznámky)

9.2 Ověřování uživatele (cestujícího)

Obsluha portálu bude zajišťovat ověřování osobních dat uživatelů systému (například ověřením prostřednictvím občanského průkazu) a na základě tohoto úkonu bude umožněno přepnutí účtu do stavu popsaného v kapitole 7.2.

9.3 Správa identifikátorů uživatele (cestujícího)

Obsluhu portálu bude umožněna správa identifikátoru (m.j. bezkontaktní bankovní karty a dopravní karty) přiřazeného k účtu uživatele. Jedná se o blokování a odstranění identifikátoru.

9.4 Správa zákaznických (uživatelských) profilů cestujících

Obsluha portálu bude:

- na přepážce fyzicky přijímat žádosti o přiřazení uživatelského profilu k účtu uživatele
- ověřovat a schvalovat žádosti o přiřazení uživatelského profilu k účtu uživatele (včetně žádostí vzniklých na straně uživatele systému dle kapitoly 7.3.).

V případě schválení žádosti (předložení požadovaných dokladů dle pravidel SPP VDV) o zákaznickou kategorii bude obsluha systému definovat pouze období platnosti uvedené kategorie (profilu).

V systému musí být umožněno přiřazení uživatelského profilu (zákaznické kategorie) k účtu i bez odeslání žádosti ze strany uživatele. Například uživatelský profil- dospělý bude přiřazen automaticky.

9.5 Prodej dopravních produktů

Úhrada za produkt bude řešena formou:

- Hotovostní úhrady
- Bezhotovostní úhrady prostřednictvím platebního terminálu

Zjednodušený daňový doklad o realizované úhradě dopravního produktu bude uživateli zaslán buď na email, který uvedl při založení účtu, nebo bude vytištěn na pokladní tiskárně.

Systém musí zajistit prodej dopravních produktů dle níže uvedených postupů:

- Výběr produktu dle tarifu

Obsluze portálu bude umožněn prodej dopravního produktu dle aktuálně přiřazeného uživatelského profilu (zákaznické kategorie) daného uživatele (tj. bude zobrazena nabídka všech tarifů, které se vážou k zákaznické kategorii uživatele). Na základě realizovaného výběru tarifu bude Obsluze dále nabídnuto časové období platnosti a možnost výběru územní platnosti.

- Výběr produktu pomocí kalkulátoru jízdného

Obsluze portálu bude umožněn prodej dopravního produktu, jehož definici určí na základě zvolené trasy, výběru aktuálně přiřazené zákaznické kategorie (uživatelského profilu) zvoleného

uživatele a období platnosti. Na základě zpracování tohoto požadavku datovým rozhraním „Kalkulátoru jízdného“ bude Obsluze nabídnut nejvhodnější produkt včetně stanovení jeho ceny.

- Výběr pomocí vyhledávače spojení

Obsluze portálu bude umožněn výběr vhodného spojení (zvolené trasy) pomocí vyhledávače spojení. Řešení musí být navrženo tak, aby bylo možné na základě zvolených začátečních a koncových stanic cesty, zákaznického profilu a období platnosti nabídnout uživateli nákup nejvhodnějšího dopravního produktu v tarifu VDV.

9.6 Prodej doplňkových produktů

Portál bude zajišťovat i prodej produktů, které nesouvisí s odbavením ve veřejné dopravě (například reklamních předmětů, obalů na kartu, apod.).

Vlastní definice těchto produktů bude spravována v Administrátorské části systému.

Úhrada za produkt bude řešena formou:

- Hotovostní úhrady
- Bezhotovostní úhrady prostřednictvím platebního terminálu

Zjednodušený daňový doklad o realizované úhradě doplňkového produktu bude uživateli zaslán buď na email, který uvedl při založení účtu, nebo bude vytištěn na pokladní tiskárně.

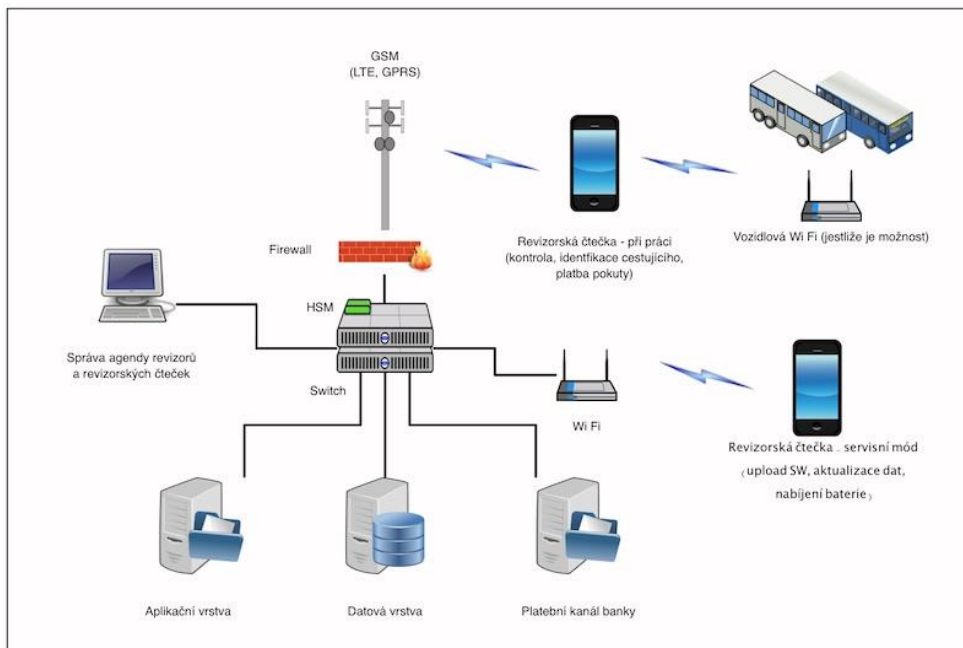
9.7 Účetní a statistické sestavy

Portál musí zajistit generování účetních a statistických sestav pro pracovníka obsluhy minimálně v níže uvedeném rozsahu:

- Účetní uzávěrky (souhrn prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu). Sestava musí obsahovat sumu za prodej/storno dle jednotlivého typu produktu, platební metody, uživatele/prodejního místa/subjektu).
- Seznam všech prodejních transakcí (přehled prodejních transakcí, dle definovaného období, typu produktu, platební metody, uživatele/prodejního místa/subjektu)

10 Požadavky na systém mobilních zařízení pro revizory

Architektura a celková funkce systému mobilních čteček



Požadované funkce systému:

Poptávané mobilní čtečky musí být schopny rutinního provozování následujících funkcí:

- Kontroly identifikátorů cestujícího v předpokládaných podobách:
 - karet dopravců (karet MAP, karet Mifare dopravců PAD),
 - kontrola bankovních karet,
 - NFC čipů v mobilu cestujícího.
 - QR kódu na displeji mobilního zařízení cestujícího
- Kontroly SMS jízdenek (MHD).
- Kontroly jednorázového jízdného (zakoupeného v papírové podobě, nebo přes mobilní aplikaci).
- Schopnost zadání typu přestupku, údajů o přestupci a volba způsobu řešení.
- Úhrada pokut BKP EMV.
- Tisk dokladu o provedené revizi, nebo o úhradě pokuty.
- Úplná evidence provedených revizí a jejich výsledků.

Základní požadované funkce aplikací Správa agendy revizorů a Správa mobilních zařízení

- Z PC je možno se přihlásit k **aplikaci pro správu agendy revizorů** s funkcemi:
 - správa a evidence revizorů (zavádění/evidence/vyřazení revizorů do/v/ze systému),
 - prohlížení výsledků kontrol revizorské činnosti (evidence stavu přestupku),
 - propojení na systémy zadavatele ekonomického a správního typu (evidence pokuty, podklady k úhradě pokuty na přepážce, podklady pro vymáhání pohledávek),
 - propojení na e-shop k řešení některých přestupků v systému.
 - zadavatel požaduje aplikaci ve formě webové aplikace.
- Z PC je možno se přihlásit k **aplikaci pro správu mobilních zařízení** s funkcemi:
 - správa připojených mobilních zařízení ve wi-fi (upgrade OS/SW bez nutnosti fyzického připojení zařízení kabelem),
 - správa dat (aktualizace dat v mobilních zařízeních)
 - zadavatel požaduje aplikaci ve formě webové aplikace.

Základní požadovaná funkce serverů:

V souladu s globálním požadavkem bude veškerá serverová část řešení aplikací správy agendy revizorů provozována v Technologickém centru Kraje Vysočina v prostředí serverové virtualizace (v duchu kap 4. Obecné požadavky).

Veškerá data jsou aplikačním serverem ukládána do databázového serveru nebo čtena z databázového serveru, na aplikačním serveru je pouze prezentační vrstva a aplikační logika.

Platební kanál banky bude zadavatel poptávat jako samostatnou službu a uchazeč jej nebude oceňovat do své nabídky.

Požadavky na mobilní zařízení pro revizory:

Zařízení bude běžně používáno ve 3 modech, které si bude obsluha schopná přepínat při práci se zařízením (v kanceláři i v terénu):

1. Servisní mód:

Servisní funkce v kanceláři

- Před použitím provede revizor **aktualizaci SW a dat** (za využití bezdrátového připojení k síti, bez nutnosti fyzického připojení revizorského zařízení kabelem) v prostorách pracoviště, které je pokryto Wi-fi signálem. Použití Wi-fi umožňuje provést aktualizace v dostatečném objemu dat rychle a s minimálními náklady na přenosové služby.

Servisní funkce v terénu

- Při **aktualizaci** musí být zařízení schopno ze serveru stáhnout všechny potřebné údaje, tedy **BL, GL, WL** karet a kupónů (podle metody zvolené dodavatelem při řešení EOC VDV a také podle metod systémů ostatních akceptovaných identifikátorů), číselníky zón a profilů, seznam revizorů a konfigurační parametry a odeslána data o provedených kontrolách.
- V průběhu přepravní kontroly musí být možné kdykoliv provést **on-line dotaz** do centra nebo po přepnutí do základního režimu i provést **celou aktualizaci**.

2. Kontrolní mód

Kontrola v PAD (teoreticky využitelné i pro přepravní kontroly v železniční dopravě)

- Přiložením karty/NFC čipu/načtením QR kódu cestujícího na čtečku se provede kontrola

Kontrola v MHD

- Přiložením čtečky kontrolora k validátoru ve vozidle se Validátor přepne do revizorského módu. Přiloženému revizorskému zařízení předá validátor, prostřednictvím NFC komunikace, taplist (v případě Chec in/check out).
- Přiložením karty/NFC čipu/načtením QR kódu cestujícího na čtečku revizora se provede kontrola

3. Platební mód

Platby bankovní kartou provedené revizorským zařízením jsou zasílány přímo do banky k realizaci (rozhraní banky pro platební terminály).

Komunikace a její zabezpečení:

SW Revizorského systému musí být schopen průběžně komunikovat s těmito okolními systémy:

- Skupinou mobilních zařízení (revizorských čteček)

Předpokládá se ověření (autorizace), vč. aktualizace, vyčtení počtu operací revizorského zařízení (kontrola výkonu revizora/kontrolora).

11 Požadavky na odbavovací zařízení dopravců (strojky dopravců)

Tato kapitola popisuje základní požadavky na odbavovací zařízení dopravců zapojených do integrovaného dopravního systému VDV. Odbavovací zařízení dopravců provádí akceptaci (odbavení) dopravního produktu zakoupeného prostřednictvím systému elektronického odbavení cestujících.

Pro zajištění výše uvedené funkce musí být odbavovací zařízení minimálně vybaveno:

- Čtečkou bezkontaktních čipových karet dle ISO 14443 A/B (Mifare Standard, Mifare DESfire EV1). Tato čtečka bude dále vybavena minimálně 4 sloty pro SAM paměťové kontaktní karty dle ISO 7816.
- Platebním terminálem (akceptačním zařízením bankovních karet) s certifikovaným EMV level 1 a 2 kernelem se schopností akceptovat bezkontaktní karty modelů VISA a Mastercard s možností zadávat PIN.

Pro úlohu generování jednoznačného identifikátoru je nutné zařízení vybudovat tak, aby splňovalo požadavky PCI DSS (například řešení vybudované v souladu se standardem PTPE /Point-to-Point Encryption/).

- Optickou čtečkou 2D čárového kódu, která musí splňovat minimálně níže uvedené parametry:
 - Zpracování 2D kódu typu: QR kód
 - Korekce: Level L (8%)
 - Verze: 23 (109 x 109 modulů)
 - Zpracování (načtení) QR kódu musí realizováno cca do 1500 ms (v případě dynamicky zobrazovaného QR kódu bude jeho další část zpracována do 1100 ms)
- LCD panelem minimální velikosti 9" s rozlišení minimálně 800x600 bodů a hloubkou barev 32-bitů. Tento panel musí být uzpůsoben tak, aby zajišťoval dobrou viditelnost na přímém slunci. Dále musí splňovat požadavky na vyšší odolnost zařízení (z pohledu každodenního použití minimálně 10 hodin, provozní rozsah teplot od -20°C od 50°C, apod.)

LCD panel bude mj. zajišťovat zobrazení informací o dopravním produktu a držiteli karty (včetně fotografie průkazového formátu) získaných z whitelistu
- Interní paměť, která zajistí uložení a zpracování souboru strukturovaných dat whitelistu o minimální velikosti 1 GB

- Modulem pro zajištění mobilní datové komunikace standardu GPRS, 3G, LTE (určené minimálně pro aktualizaci whitelistu).
- Výpočetní jednotkou (řídícím PC) jehož výpočetní výkon zajistí zpracování dat whitelistu do maximálně 500 ms.

Zpracováním dat z Whitelistu se rozumí : vyhledání záznamu dle načteného jedinečného identifikátoru, dešifrování osobních dat držitele identifikátoru a jejich zobrazení, vyhodnocení platnosti dopravního produktu a jeho zobrazení).

Odbavovací zařízení dopravce musí dále zajistit:

- Realizaci funkcí symetrické a asymetrické kryptografie (dešifrování osobních dat držitele karty, ověření jedinečnosti QR kódu)
- Pravidelnou komunikaci s rozhraním pro předávání dat strukturovaných souborů whitelistů a číselníků, tj. musí zajistit podporu standardně používaných technologií pro výměnu dat mezi systémy (například: zabezpečený FTP server/SFTP, využití webových služeb založených na principu REST, SOAP). Četnost této komunikace (pravidelný interval) bude možné libovolně upravovat.
- Generování transakčních dat o prodeji/(akceptaci-použití) dopravního produktu a jejich přenos do zúčtovacího systému.

Základní popis procesu odbavení:

- Načtení vstupních dat pro výpočet jedinečného identifikátoru (tokenu) z uživatelem předloženého média (bankovní karta, NFC čip, dopravní karta, QR kód mobilní aplikace)
- Vygenerování jedinečného identifikátoru
- Vyhledání jedinečného identifikátoru ve whitelistu
- Získání příslušných dat z whitelistu (osobní data uživatele, zakoupený dopravní produkt)
- Vyhodnocení územní a časové platnosti zakoupeného dopravního produktu v aplikačním software odbavovacího zařízení. (dle aktuálně zvolené trasy/linky)
- Případný výpočet/dopočet ceny jízdného dle zvolené trasy/linky

- Zobrazení výsledku vyhodnocení územní a časové platnosti dopravního produktu (včetně informace o případném doplatku), zobrazení osobních dat uživatele (včetně fotografie a zákaznické kategorie)
- Realizace možného doplatku za jízdné

Další požadavky na odbavovací zařízení

Pro případ aktuálního, nebo budoucího vybavení odbavovacího zařízení validátorem (typicky při sdílení vozidla v systému PAD a MHD), musí zařízení disponovat funkcí módu revize, kdy po přiložení čtečky kontrolora k validátoru se validátory zablokují pro prodej JD.

Další požadavky na odbavovací zařízení mohou být zadavatelem specifikovány v průběhu realizace projektu.

12 Popis whitelistů

Soubor strukturovaných dat whitelist bude využit pro poskytování informací o aktuálně platných kupónech, identifikaci držitele dopravního produktu (včetně zákaznické kategorie) a jeho kartách evidovaných v systému (jedinečných identifikátorech). Příjemcem a zpracovatelem whitelistu jsou dopravci, kteří na základě takto poskytnutých dat vyhodnocují nárok na přepravu a dále zajišťují proces přepravní kontroly cestujících. Systém umožní generovat whitelisty dle typu zapojeného subjektu (tj. rozsah poskytovaných dat bude určen na základě typu dopravce. Primárním cílem je zamezit distribuci osobních dat uživatelů pro subjekty/dopravce, kteří nebudou tyto údaje aktivně využívat pro svou činnost).

Whitelist musí obsahovat data aktuálně platných dopravních produktů a dle administrátorsky definované hodnoty bude možné ve whitelistu zachovat již neplatné produkty, nebo naopak produkty, u kterých ještě nenastala platnost (například: whitelist bude obsahovat produkty, jejichž platnost vypršela maximálně před 14 dny, nebo nastane za 2 dny).

Pokud budou z whitelistu odstraněny záznamy o všech zakoupených produktech zákazníka, tak automaticky budou odstraněny i osobní údaje zákazníka.

Pro personalizovaný typ bezkontaktní čipové karty dopravce by nemusela být ve whitelistu zanesena fotografie držitele karty (ztotožnění cestujícího by mohlo být realizováno vizuálně na základě předložení dopravní karty).

12.1 Základní definice struktury dat

Whitelist musí obsahovat minimálně níže uvedené údaje:

- Datové záznamy o cestujícím -uživateli systému (držiteli identifikátoru) minimálně v rozsahu:
 - Identifikátor držitele
 - Jméno
 - Příjmení
 - Datum narození
 - Fotografie držitele identifikátoru (v průkazovém formátu s optimalizované velikosti fotografie do maximální velikosti cca 2 kB)

- Datové záznamy o zakoupeném dopravním produktu:
 - Identifikace tarifu
 - Identifikace zákaznické kategorie
 - Platnost tarifu od – do (včetně časové)
 - Definice územní platnosti (na základě výčtu povolených a volitelných zón)
 - Definice vazby na identifikátor
- Datové záznamy o kartách (jedinečných identifikátorech)
 - ID jedinečného identifikátoru (tokenu)
 - Vlastní hodnota (datový záznam) jedinečného identifikátoru, ke kterému je dopravní produkt přiřazen
 - Typ jedinečného identifikátoru (bankovní karta, 2D čárový kód, karta dopravce, NFC čip)
 - Stav (platný/neplatný)
 - Vstupní hodnota pro vygenerování klíče určeného k dešifrování osobních údajů

Režim generování whitelistů

- Plný formát
 - Generování 1x denně
 - Obsahuje kompletní informace o produktech, identifikátorech a uživateli
 - Určen především do nového zařízení (popřípadě do zařízení, které nebylo delší dobu aktualizováno)
- Změnový formát (greenlist)
 - Obsahuje změny ve whitelistu oproti předchozímu stavu

Čas a četnost pravidelného generování whitelistu (green listu) bude možno spravovat administrátorem systému.

12.2 Zabezpečení osobních údajů

Osobní údaje o držiteli karty budou ve whitelistu zašifrovány (dle standardů šifrování, například: AES - Advanced Encryption Standard). Architektura přípravy whitelistu bude v nově budovaném systému implementována, tak aby každý záznam o uživateli systému byl zašifrovaný samostatně. Vstupní hodnota pro stanovení klíče bude odvozena až při vlastním použití daného identifikátoru zákazníkem, (požadavek na zajištění bezpečnosti dat z pohledu neoprávněného přístupu k osobním údajům.)

12.3 Číselníky tarifních dat

Vzhledem k datové úspoře při vlastní tvorbě (generování) whitelistů jsou jednotlivé informace o produktech (například zákaznická kategorie, označení tarifu, apod.) interpretovány pouze identifikátorem, je tedy nutné vytvářet a distribuovat pro příjemce whitelistů převodní tabulky (číselníky).

Vlastní generování těchto číselníků musí zajišťovat Jádru systému elektronického odbavení cestujících a každý subjekt (příjemce whitelistu) musí v odbavovacím zařízení zabezpečit jejich příjem a zpracování.

Za správu a vydávání těchto číselníků bude odpovědný provozovatel systému, tj. subjekt určený VDV.

Rozhraní pro předávání dat (číselníků) mezi jádrem systému elektronického odbavení cestujících a subjektem (příjemcem whitelistu) bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například využitím webových služeb založených na principu REST, SOAP). Při návrhu rozhraní musí být kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

13 Popis požadavků na zúčtovací centrum

Zúčtovací centrum musí zajistit evidenci všech transakcí (prodeje, storna, částečné užití produktu) vzniklých při prodeji dopravního produktu subjekty zapojenými do integrovaného dopravního systému VDV. Tento transakční přehled bude sloužit jako podklad pro výpočet podílu z tržeb pro jednotlivý subjekt zapojený do systému (dopravce).

Vlastní dělení tržeb bude realizováno modelem tzv. dohodnutého poměru (tj. maticí, která jasně určuje procentní podíl dopravce z celkového objemu tržeb za prodej dopravního produktu).

Zúčtovací centrum musí minimálně umožnit:

- Definici a správu subjektů (dopravců) zapojených do systému
- Správu uživatelů a uživatelských rolí aplikace zúčtovacího centra
- Evidenci odbavovacích zařízení/prodejních míst za jednotlivý subjekt (dopravce)
- Evidenci mobilních zařízení revizora
- Příjem a zpracování transakcí za jednotlivá odbavovací zařízení (včetně rozlišení typu transakce: prodej, storno, částečné užití produktu)
- Příjem a zpracování dat (příp. transakcí) z mobilních zařízení revizora (např. zneplatnění jízdenky)
- Kontrolu vstupních a transakčních dat zaslaných do zúčtovacího centra z pohledu úplnosti (tj. identifikaci nedodaných transakcí a upozornění na takovou skutečnost)
- Realizaci výpočtu podílu dopravce z celkového objemu tržeb za prodej dopravního produktu
- Vytváření podrobných přehledů o zúčtování dat
- Zúčtování transakcí s různou hodnotou DPH
- Generování účetních podkladů (včetně vzájemných zápočtů mezi jednotlivými dopravci)
- Generování statistických podkladů
- Export všech výstupů do *.xls souborů

Požadovaný způsob návrhu aplikace zúčtovacího centra

Požadovaný způsob návrhu aplikace zúčtovacího centra je vytvoření webové aplikace, která bude přístupná ze sítě Internet na základě definovaného/povoleného rozsahu IP adres. Z pohledu bezpečnosti bude nutné využití zabezpečené komunikace se serverem prostřednictvím https protokolu. Přístupová oprávnění k aplikaci budou řešena na úrovni Administrátorské části systému.

Formát předávaných dat mezi subjektem integrované dopravy VDV (dopravcem) a zúčtovacím centrem bude realizován prostřednictvím XML zpráv.

Rozhraní pro komunikaci dopravce se zúčtovacím centrem bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: využitím webových služeb založených na principu REST, SOAP). Při návrhu rozhraní musí být kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

14 Popis požadavků na datovou komunikaci (způsob distribuce dat)

14.1 Datové rozhraní pro distribuci whitelistů

Požadavky na datové rozhraní pro distribuci whitelistů

Rozhraní pro předávání dat uložených ve strukturovaném souboru whitelistu bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: zabezpečený FTP server/SFTP, využitím webových služeb založených na principu REST, SOAP, ...). Je však nutné dodržet vysoké bezpečnostní standardy tohoto řešení.

Předávání dat (whitelistu) mezi systémem EOC a příjemcem whitelistu (dopravcem) bude realizováno prostřednictvím definovaného/navrženého rozhraní, které bude Zadavateli předáno v písemné formě při realizaci díla. Zadavatel se po předání díla stává vlastníkem uvedeného rozhraní a může jej bez dalšího omezení a licenčních poplatků používat i pro další účely.

14.2 Datová komunikace s externími systémy dopravců

Z důvodu požadavku na integraci nově budovaného systému EOC s kartově-odbavovacími systémy dalších dopravců, je nutné navrhnout a vybudovat rozhraní, které zajistí minimálně níže uvedené funkce:

Minimální požadavky na rozhraní pro datovou komunikaci s externími systémy dopravců

- Poskytnutí informací o uživateli systému (personalizační data)
- Ověření personalizačních dat uživatele systému
- Poskytnutí informací o registrovaných identifikátorech
- Předání dat o zákaznických kategoriích
- Potvrzení zákaznické kategorie uživatele (popřípadě vytvoření nové zákaznické kategorie)
- Nákup dopravního produktu dle postupů popsanych v kapitole 9.5
 - Výběr produktu dle tarifu
 - Výběr produktu pomocí kalkulátoru jízdného
 - Výběr pomocí vyhledávače spojení
- Storno dopravního produktu

Rozhraní pro komunikaci s externími systémy dopravců bude vybudováno s využitím standardně používaných technologií pro výměnu dat mezi systémy (například: využitím webových služeb založených na principu REST, SOAP, ...). Zde je však opět kladen důraz na dodržení vysokých bezpečnostních standardů tohoto řešení.

Při realizaci prodeje/nákupu dopravního produktu (dle kapitoly 9.5) v kartově-odbavovacím systému dopravce je nutné vycházet z požadavku Zadavatele na jednotný způsob zpracování transakcí:

Požadavky na realizaci prodeje/nákupu dopravního produktu

- Vlastní proces nákupu musí být uskutečněn formou dotazování do systému EOC („tzv. postupné sestavení produktu“). Na základě dotazu dopravce (kartově-odbavovacího systému) poskytne systém EOC soubor dat, který umožní další krok v sestavení produktu (například: dotazem na ověření cestujícího systém EOC poskytne údaje o uživateli a jeho zákaznických kategoriích; dalším krokem bude dotaz/požadavek na předání souboru tarifů ke zvolené zákaznické kategorii)
- Záznam o prodejní transakci (popřípadě stornu) bude vždy zaznamenán v systému EOC. Transakční data budou dále ze systému EOC předávána k zúčtování.
- Každý subjekt/dopravce, který bude komunikovat prostřednictvím toho rozhraní, musí být evidován v systému EOC (včetně jednotlivých prodejních míst).

Nově navržené rozhraní „Datová komunikace s externí systémy dopravců“ bude Zadavateli předáno v písemné formě v průběhu realizace díla. Zadavatel se po předání díla stává vlastníkem uvedeného rozhraní a může jej bez dalšího omezení a licenčních poplatků používat i pro další účely.

14.3 Datová komunikace s mobilními zařízeními revizorů

Pro možnost návrhu technických parametrů mobilních zařízení a odhadu objemu datové komunikace uvádíme následující předpoklady komunikace zařízení.

Ze zařízení budou odcházet tato data:

- Informace o zahájení kontrolní činnosti
- Informace o provedených kontrolách
- Chybové a stavové informace
- Komunikace na bankovní rozhraní platebních terminálů

Do zařízení budou přicházet tato data:

- Seznam zakázaných karet (BL)
- Seznam elektronických časových kupónů určený k nahrání (GL, vč. foto)
- Seznam karet přepravních kontrolorů
- Číselník názvů zón
- Číselník názvů profilů cestujícího
- Ostatní konfigurační parametry (pro technické nastavení zařízení)
- Informace o nahrání nových časových elektronických jízdenek
- Informace o změně linky a spoje

15 Bezpečnostní požadavky na systém

15.1 Obecné požadavky na návrh systému

- Nově vybudovaný systém musí zajistit vysoký bezpečnostní standard tak, aby konkrétní data byla dostupná jen pro odpovědné osoby a subjekty. V tomto případě se nejedná pouze o zajištění bezpečnosti dat (zabezpečené uchovávání dat), ale zejména o proces jejich zpracování, které nesmí ohrožovat důvěrnost dat o uživatelích systému.
- Bezpečnost musí být řešena nejenom z pohledu základní části systému elektronického odbavení cestujících, ale z pohledu bezpečnosti celého systému, tj. včetně dalších napojených systémů.
- Velký důraz je kladem na ochranu kryptografických klíčů použitých v systému tak, aby nemohlo dojít k jejich zpřístupnění (např. při odcizení odbavovacího zařízení, „nabourání“ do systému, apod.).
- Dodavatel nesmí provádět žádné kroky vedoucí ke zjištění kryptografických klíčů použitých v systému (pokud nebude se Zadavatelem dohodnuto jinak).
- Systém musí být navržen tak, aby zajistil účinnou bezpečnost z pohledu důvěrnosti dat a nemožnosti zneužití (prolomení) systému např. formou využití cizích zařízení.
- Bezpečnost celého systému musí být řešena v souladu s platnou legislativou (zákonem o ochraně osobních údajů, platebním styku, dále musí být řešena v souladu s čl. 28 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, apod.).
- Řešení musí být navrženo tak, aby byla v maximální možné míře zajištěna bezpečnost dat (zajištění dat proti ztrátě, nekonzistenci, nežádoucí modifikaci a proti neoprávněnému přístupu).
- V celém Řešení se nebudou vyskytovat jakékoli nedokumentované funkcionality (tj. funkcionality SW, které nejsou popsány v žádné k tomu určené dokumentaci).

15.2 Základní požadavky na zabezpečení komunikace

- Jednotlivé části systému mezi sebou komunikují s využitím dostupných technologií - Internet, TCP/IP. Veškerá komunikace probíhá s využitím kryptografie a šifrování. V případě přenosu

GSM/GPRS, 3G, LTE jsou SIM karty speciálně zabezpečeny (APN, VPN). Při návrhu celého systému je nutné dodržet vysoké bezpečnostní standardy pro datovou komunikaci.

16 Požadavky na mobilní aplikaci systému elektronického odbavení cestujících

Součástí celého řešení bude i dodávka mobilní aplikace, která zajistí shodné funkce odbavení uživatele systému EOC popsané v kapitole 7 „Požadavky na samoobslužný systém pro odbavení zákazníků (portál zákazníka, e-shop)“.

Aplikace musí být navržena minimálně pro provozování na mobilních zařízeních s operačním systémem Android (od verze 4.4 a dále) a iOS (od verze 9.0 a dále). Dále musí splňovat požadavek na veřejnou dostupnost v obchodech Apple Store (App Store), Google Play (Obchod Play).

Mobilní aplikace samoobslužného systému pro odbavení cestujících musí mít tyto základní funkce:

- Zobrazení profilu zákazníka v mobilní aplikaci (včetně fotografie), zobrazení zakoupeného produktu a identifikátoru (2D čárový kód)
- Založení a správa uživatelského účtu zákazníka (při personalizaci účtu bude pořízená fotografie uživatele - realizováno prostřednictvím integrovaného fotoaparátu mobilního zařízení, nebo načtením souboru z paměti tohoto zařízení)
- Funkce pro přiřazení identifikátorů k účtu uživatele
- Správa těchto identifikátorů
- Správa zakoupených produktů
- Správa zákaznických profilů/kategorií
- Nákup a úhrada dopravního produktu
- Nákup a úhrada jednorázových časových jízdenek

Poznámka:

Řešení musí vycházet z dostupných metod vývoje mobilních aplikací pro operační systémy Android a iOS. Z důvodu zjednodušení správy/udržování mobilní aplikace je požadováno využít k jednotlivým výše uvedeným funkcím aplikace (mimo funkce: generování identifikátoru, zobrazení zakoupeného dopravního produktu, nákup jednorázových jízdenek) tzv. zobrazení responzivních webových stránek

systému „portál zákazníka, e-shop“ (jak je popsáno v kapitole 7.) Pro vyloučení všech pochybností je nutné zdůraznit, že se nejedná o vytvoření mobilní aplikace metodou „samostatného“ zobrazení responzivních webových stránek.

Minimální požadavky na jedinečný identifikátor mobilní aplikace

- Generovaný identifikátor bude ve shodné velikosti jako tzv. token bankovní karty
- Identifikátor bude unikátní pro každou jednotlivou instalaci mobilní aplikace v telefonu i v rámci jednoho uživatelského účtu (z uvedeného vychází i požadavek na unikátnost v rámci instalace do různých mobilních zařízení)
- Identifikátor bude automaticky přiřazen k účtu uživatele (pro možnost nákupu a přiřazení dopravního produktu)
- Systém EOC musí zajistit rozlišení tohoto typu identifikátoru

Mobilní aplikace musí zajistit vytvoření/vygenerování jedinečného identifikátoru mobilní aplikace, který bude presentován formou QR kódu na displeji mobilního zařízení, aby na jeho základě mohl být vypočítán token a vyhledán příslušný záznam ve whitelistu. Token mobilní aplikace bude počítat platební brána (respektive SAM) stejně jako u ostatních identifikátorů. Tokenizační algoritmus zůstává stejný jako u ostatních identifikátorů.

Generovaný QR kód musí být zabezpečen možností ověření získaných dat (například budou data elektronicky podepsána pomocí asymetrické kryptografie).

Mobilní aplikace, která bude tento 2D čárový kód zobrazovat musí zajistit ochranu proti vytvoření tzv. snímku obrazovky (například: využití dynamického 2D čárového kódu, apod.).

Minimální požadavky na definici jednorázových časových jízdenek:

Pro funkci „Nákup a úhrada jednorázových časových jízdenek“ musí být systém EOC vybaven modulem pro správu těchto produktů. Ke každému subjektu, zavedenému v systému EOC bude umožněno samostatně definovat soubor těchto produktů.

- Unikátní identifikátor jízdenky/tarifu
- Označení jízdenky (slovní popis)

- Definice územní platnosti
- Definice časové platnosti
- Omezení platnosti jízdenky (například na den v týdnu)
- Omezení zahájení platnosti (čas nutný pro zahájení platnosti jízdenky po jejím nákupu a vygenerování)
- Kategorie zákazníka
- Cena

Z důvodu požadavku na okamžité ověření platnosti jednorázové jízdenky je nutné výše uvedená data doplnit do generovaného 2D čárového kódu, tj. umožnit realizaci ověření platnosti jízdenky prostřednictvím načtení 2D čárového kódu. Ochrana těchto dat proti zneužití musí vycházet z výše uvedených požadavků.

Příloha č. 1 – Základní popis předpokládané implementace EOC ve VDV

Základní popis (definice) stávajícího Integrovaného dopravního (tarifního) systému Veřejné dopravy Vysočiny je obsažen v dokumentech Smluvních přepravních podmínek a dalších na webu:

<https://www.kr-vysocina.cz/tarif%2Dvdv/ds-304441/p1=106091>

Při implementaci nového systému EOC se předpokládá, že jízdní doklady budou ukládány na nosičích a identifikátorech:

Název	Způsob úhrady	Nosič (identifikátor)
obyčejná jednosměrná jízdenka	hotovost, BČK dopravce, BPK	papír, mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
celodenní jízdenka-síťová jízdenka	hotovost, BČK dopravce, BPK,	papír, mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
roční síťová jízdenka	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
jednozónová jízdenka (i v případě integrace MHD)	hotovost, BČK dopravce, BPK	papír, mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
integrovaná sedmidenní jízdenka	hotovost, BPK,	mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
integrovaná třicetidenní jízdenka	hotovost, BPK,	mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
integrovaná devadesátidenní jízdenka	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK, NFC
předplatné MHD (v případě integrace MHD)	hotovost, BPK	mobilní aplikace - QR kód, BČK dopravců, BPK, karta dopravce dané MHD (např. Jihlavská karta), NFC

Prodej roční síťové jízdenky a předplatného pouze na předprodeji (prodejní místo dopravce, portál zákazníka-e-shop, mobilní aplikace)

Úhrada pomocí BČK (el. Peněženky dopravce) pouze u řidiče dopravce, který kartu vydal.

Jako u stávajícího tarifu, platný jízdní doklad ve vyjmenovaných linkách VDV a jejich vyznačených úsecích dle přílohy č. 2 SPP VDV bude uznáván i jízdní doklad IDS JMK, IREDO, SID a PID včetně dokládání nároku na slevu.

Příloha č. 2 – Požadavky na vytvoření jedinečného identifikátoru z údajů získaných z bezkontaktní karty

Každá karta se v systému eviduje pod speciálním číslem (jedinečným identifikátorem - tzv. tokenem). Tento token se používá, aby se v systému neuchovávaly potenciálně zneužitelné údaje (například číslo bankovní karty). Token je potřeba spočítat vždy, když se do systému přidává nová karta nebo když se mají v systému vyhledat informace svázané s konkrétní o kartou. Výpočet tokenu z karty provádí platební brána (on-line tokenizace) nebo SAM modul v odbavovacím zařízení (off-line tokenizace). Tokenizační algoritmus platební brány a odbavovacího zařízení je totožný.

Výpočet jedinečného identifikátoru (tokenu) při registraci bezkontaktní karty v systému

Při prvotní on-line registraci libovolného identifikátoru (jen a pouze při prvotní registraci), token generuje platební brána. Vypočtený token zasílá do Backoffice VDV. Vlastní výpočet tokenu tedy bude realizován prostřednictvím přesměrování na platební bránu banky, kterou určí Objednatel.

- Uživatel, který se bude registrovat pomocí IN-karty nebo Jihlavské karty, bude do systému zaregistrován pouze na základě zadání čísla karty, případně její expirace
- Uživatel, který se bude registrovat pomocí bankovní karty, během registrace do systému provede navíc „standardní“ on-line platební transakci s využitím metod ověření platby (zadání čísla karty, platnosti karty, CVV kód, popřípadě 3D secure klíč). V případě úspěšné transakce platební brána vygeneruje token, který zašle do Backoffice VDV s potvrzením platby. Tento postup zaručí ověření identity uživatele.

Poznámka

Popis rozhraní platební brány bude Zhotoviteli předán v průběhu přípravy Cílového konceptu.

Výpočet jedinečného identifikátoru (tokenu) v odbavovacím zařízení dopravce

Při odbavení ve vozidle/vlaku/na přepážce bude výpočet tokenu realizován SAM modulem v odbavovacím zařízení dopravce za pomoci akceptačního zařízení bankovních karet/platebního terminálu s certifikovaným EMV level 1 a 2 kernelem se schopností akceptovat bezkontaktní karty modelů VISA a Mastercard s možností zadávat PIN.

Čtečka bankovních karet bude zajišťovat jak funkci generování jedinečného identifikátoru bankovní karty, tak platební funkci (tj. umožní úhradu jízdného prostřednictvím bankovní karty). Pro úlohu generování jednoznačného identifikátoru je nutné akceptační zařízení bankovních karet vybudovat tak, aby splňovalo požadavky PCI DSS (například řešení vybudované v souladu se standardem PTPE /Point-to-Point Encryption/).

Algoritmus pro výpočet jedinečného identifikátoru (tokenu) bezkontaktní karty:

Tokenizační algoritmus bude součástí zadání pro zhotovitele platební brány, a bude předán až přihlášeným uchazečům.

V odbavovacím zařízení je tokenizační algoritmus bezpečně uložen přímo v SAM modulu, který provádí vlastní výpočet tokenu.

Výpočet vstupních dat pro tokenizační algoritmus

(vstupní data budou dosazena do tokenizačního algoritmu (vzorce))

U bankovní karty pro výpočet vstupních dat budou použity následující údaje vytištěné na těle nosiče:

- Číslo karty
- Exspirace karty

U In Karty pro výpočet vstupních dat budou použity následující údaje vytištěné na těle nosiče:

- Číslo karty (PAN)
- Exspirace karty

U Jihlavské karty bude pro výpočet vstupních dat využito:

- UID karty Mifare DESFire dle standardu ISO-14443A (resp. číslo Jihlavské karty)

Hodnota UID není z karty lidským okem čitelná (na rozdíl od čísla Jihlavské karty). Pro případnou registraci Jihlavské karty prostřednictvím webového rozhraní bude nutné vytvořit v Backoffice EOC KV převodní službu, která zajistí převod čísla Jihlavské karty na UID a zároveň dotazem do Backoffice DPMJ ověří platnost Jihlavské karty.