

Požadavky na řešení - implementace systému Virtuální karta do prostředí Integrované dopravy Plzeňského kraje

Virtuální karta je systém elektronického odbavení cestujících a karetní systém. Primární funkcí tohoto řešení je nákup dopravního a nedopravního produktu (například dlouhodobé předplatné, apod.) a jeho přiřazení k důvěryhodnému identifikátoru (například: bezkontaktní bankovní kartě, QR kód v aplikaci mobilního telefonu, nebo přiřazení k bezkontaktní paměťové čipové kartě MAP, tj. karta standardu DESFire EV1).

Použitím důvěryhodného identifikátoru ve formě „nosiče“ dlouhodobých časových kupónů budeme pro účel tohoto dokumentu chápat přiřazení již zmiňovaného typu identifikátoru k zakoupenému produktu (dlouhodobému časovému kupónu, apod.), tj. výsledkem výše uvedeného procesu bude vytvoření strukturovaných souborů dat „whitelist“, který obsahuje: identifikátor, informace o držiteli identifikátoru, zakoupených produktech apod. Tento soubor dat je dále použit pro vyhodnocení nároku na přepravu v prostředí IDPK.

V požadovaném řešení je kladen důraz na samoobslužné odbavení cestujících. Systém obsahuje webový portál (webovou aplikaci) a mobilní aplikaci, která slouží pro samoobslužné odbavení cestujících, tj. uživatel systému realizuje veškeré činnosti (například: správu vlastního účtu a identifikátorů/karet, nákup dopravního produktu, apod.) prostřednictvím výše zmíněné webové a mobilní aplikace bez nutnosti návštěvy zákaznického centra dopravce (pokud není tarifním nařízením stanoveno jinak).

Tarifní jádro systému zajišťuje následující funkce:

- Výpočet jízdného (stanovení ceny za produkt)
- Správa životního cyklu uživatele systému
- Správu životního cyklu karty a identifikátorů
- Správu tarifní politiky integrovaného dopravního systému IDPK (definice tarifů, CP, apod.)
- Generování strukturovaných souborů whitelistů
- Komunikaci s externími systémy při procesu ověřování karty
- Generování jedinečných identifikátorů
- Integraci s platebními metodami (e-Commerce platební brána, automatizované zpracování převodních příkazů)
- Příprava a distribuce dat pro zúčtovací systém

Základní funkce samoobslužného systému pro odbavení zákazníků (portál zákazníka, e-shop) jsou:

- Založení a správa uživatelského účtu zákazníka
- Funkce pro přiřazení jednoznačného identifikátoru k účtu uživatele (například prostřednictvím platební brány) a správu těchto identifikátorů
- Správa zakoupených produktů
- Správa zákaznických profilů/kategorií
- Nákup a úhrada dopravního produktu
- Příprava a distribuce dat pro zúčtovací systém

Základní funkce prodejní/přepážkové části systému jsou:

- Správa uživatelů systému
- Správa identifikátorů jednotlivých uživatelů systému
- Ověřování osobních dat uživatele systému

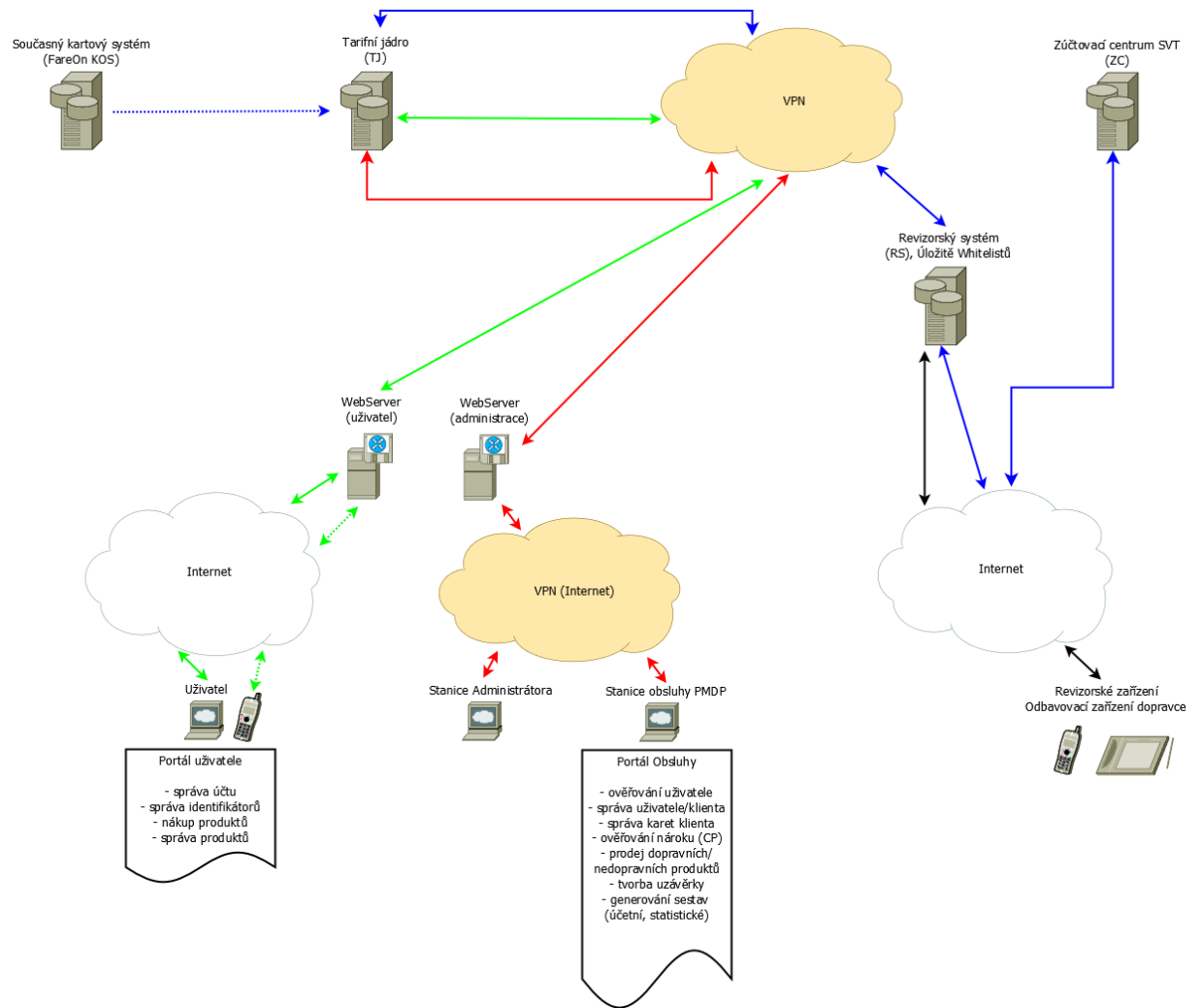
- Správa zákaznických profilů jednotlivých uživatelů systému
- Prodej dopravních produktů (včetně realizace storna produktů)
- Správa reklamací
- Generování účetnických a statistických sestav
- Příprava a distribuce dat pro zúčtovací systém

Odbavovací zařízení dopravců IDPK nerealizují prodejní operace v systému Virtuální karty (tj. neprodávají dlouhodobé časové jízdné).

Modul „prodejního/přepážkového“ pracoviště systému Virtuální karty je realizován formou webové aplikace. Na provozovatele prodejního místa uvedeného systému nejsou kladeny speciální požadavky z pohledu ICT vybavení.

Nutnost využití přepážkového pracoviště (například realizace operací: ztotožnění uživatele systému, přiřazení zákaznické kategorie, prodej dopravních produktů, apod.) se řídí smluvním ustanovením vycházejícím z aktuálně uzavřeného smluvního vztahu mezi dopravcem a objednatelem závazku veřejné dopravy.

Základní schéma systému Virtuální karta



Typy identifikátorů v systému virtuální karta

Typ	Nosič	Požadavky na akceptační zařízení (dále AZ) *	Způsob získání tokenu	V provozu zapojeno od etapy
Bankovní karta	Bezkontaktní bankovní karta vydávaná dle pravidel VISA, MasterCard	1. Certifikovaná čtečka bankovních karet (Platební terminál) 2. Bezkontaktní čtečka karet, která splňuje požadavky PCI DSS pro operace s bankovní kartou, nebo obsahuje certifikace banky v obdobném rozsahu pro bezpečné operace s bankovními kartami, případně má dopravce pro dané zařízení udělenou výjimku od acquirera. Akceptační zařízení je dále vybaveno SAM modulem systému MAP.	1. Komunikací AZ s platebním terminálem prostřednictvím určeného protokolu (například B+, ISFS, POD.) * 2. Zpracováním definované instrukce MAP SAM modulu*	2
Mobilní aplikace Virtuální karta / Vary Virtual	QR kód zobrazený v mobilní aplikaci (dlouhodobý časový kupón)	Čtečka QR kódu	Vyčtením datové struktury QR kódu*	1
Pížeňská karta/Karta Mariánka/Karlovarská karta	Bezkontaktní čipová karta DESfire EV1 popřípadě EV3 (MAP struktura)	Bezkontaktní čtečka karet standardu DESfire EV1, EV3	Zpracováním definované instrukce MAP SAM modulu*	2
Papírová jízdenka s QR vydaná jako doplatek k dlouhodobému časovému kuponu vystavenému k jinému identifikátoru	Papír s QR	Čtečka QR kódu	Vyčtením datové struktury QR kódu*. Poznámka: papírová jízdenka nemá svůj vlastní token. Nese token identifikátoru, k němuž byl vystaven doplatek.	1

* Bližší specifikace je uvedena níže v dokumentu

Token = unikátní identifikátor generovaný (na základě definovaného algoritmu) z dat získaných při komunikaci AZ/čtečky s daným typem média (bankovní karta, Pížeňská karta, ...)

V systému Virtuální karta je možné přiřadit zakoupený dopravní produkt (kupón) právě k jednomu platnému identifikátoru uživatele. Systém však umožňuje k jednomu účtu registrovat libovolný počet identifikátorů různého typu.

Soubor strukturovaných dat whitelist:

Soubor strukturovaných dat whitelist je v systému Virtuální karty pravidelně generován s cílem poskytování informací o aktuálně platných kupónech, identifikaci držitele dopravního produktu (po rozšíření v etapě 2 včetně zákaznické kategorie) a jeho kartách evidovaných v systému (jedinečné identifikátory/tokeny). Příjemcem a zpracovatelem whitelistů jsou dopravci, kteří na základě takto poskytnutých dat vyhodnocují nárok na přepravu a dále zajišťují proces přepravní kontroly cestujících. Systém Virtuální karty je připraven generovat whitelisty dle typu zapojeného subjektu (tj. rozsah poskytovaných dat může být 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). V rámci projektu využití Virtuální karty v IDPK budou všichni zapojení dopravci stahovat tentýž whitelist.

Whitelist obsahuje data aktuálně platných dopravních produktů a dle administrátorsky definované hodnoty je možné ve whitelistu zachovat již neplatné produkty, nebo naopak produkty, u kterých ještě nenastala platnost (například: whitelist obsahuje produkty, jejichž platnost vypršela nebo ještě nenastala).

Způsob generování whitelistů:

- Plný formát (Obsahuje kompletní informace o produktech, identifikátorech a uživateli)
- Změnový formát (Obsahuje změny ve whitelistu oproti předchozímu stavu)

Formát whitelistu

- Binární soubory, kódování DER/BER.

Režim generování whitelistů

Full Whitelist

- statický snapshot dat
- generování 1x denně - vždy k půlnoci každého dne
- určen k počátečnímu nahrání dat do nového/zresetovaného revizorského zařízení
- předpokládaná velikost - cca 500 MB (odhad: 100 tis. dokladů x 5kB na jeden doklad)
- maximální velikost – 2 GB
- např. full-14.whl - číslo 14 je číslo posledního inkrementálního whitelistu, který je ve full whitelistu obsažen. Jinými slovy, whitelist full-14.whl je generován ke stejnému datumu a času jako související inc-14.whl.

Inkrementální změny

- změny ve whitelistu oproti předchozímu stavu, tj. oproti předchozímu inkrementu
- záznamy jsou označeny typem modifikace - přidání vs. odebrání záznamu z whitelistu, týká se všech 3 typů entit
- generování každých 15 minut (lze konfiguračně upravit)

- určeny k aktualizaci whitelistů v zařízeních bez zbytečného přenášení velkého objemu dat
- soubory jsou číslované absolutní sekvencí se startem od 1 (první inkrement)
- z názvu nelze určit, jaké změny (za jaké období) inkrement obsahuje např.: inc-1.whl, inc-2.whl, ..., inc-24123.whl
- synchronizace s full whitelitem - full whitelist obsahuje číslo posledního inkrementu, který je ve full whitelistu "obsažen"
- entity beze změn se do inkrementálního whitelistu nevkládají, počítá se s tím, že si je revizorské zařízení podle ID dohledá. Tj. když je např. přidán nový produkt na již existující identifikátor, ve whitelistu je pouze záznam o novém produktu, data klienta ani identifikátoru se nevloží.

Seznam změn, které inkrementální whitelist zahrnuje:

1. Již dříve vytvořený kupón začne být validní s ohledem na předem definovaný interval¹, ve kterém mají být zveřejněny kupóny s předstihem (a zároveň nebyl ještě zveřejněn v minulém whitelistu).
2. Od posledního whitelistu byl vytvořen kupón, který má již být i zveřejněn s ohledem na definovaný interval¹ (Nově vytvořené, ale zároveň stornované kupóny nebudou do whitelistu zahrnuty).
3. Od posledního whitelistu byla zaregistrována změna² na zákazníkovi, kterému patří aktuálně validní kupón (nebo od etapy 2 profil).
4. Od posledního whitelistu byla zaregistrována změna² na identifikátoru, ke kterému patří aktuálně validní kupón (nebo od etapy 2 profil).
5. Od posledního whitelistu byla zaregistrována změna² na kupónu.
6. Od etapy 2: od posledního whitelistu byla zaregistrována změna na profilu zákazníka

Body 1 a 2 znamenají vložení kompletních informací o kupónu zahrnující informace o klientovi, identifikátoru a samotném kupónu.

Body 3, 4, 5, 6 znamenají vložení pouze informací o klientovi (bod 3), resp. identifikátoru (bod 4) a kupónu (bod 5).

V případě aktualizace klienta/identifikátoru/kupónu/(od etapy 2 i profilu) je vložena kompletní entita, nikoliv pouze změněné položky.

Kupóny, kterým skončila od posledního generování whitelistu platnost, nejsou do inkrementálního whitelistu vloženy jako "deleted". Jako "deleted" jsou vloženy takové kupóny, u kterých byl od posledního generování změněn stav z "platný" na "stornovaný".

Přesná specifikace datových struktur whitelistu je uvedena v samostatném dokumentu „Virtuální karta – datová struktura Whitelist“

Synchronizace číselníků

¹ Interval, v jakém mají být zveřejněny kupóny před svou faktickou platností.

² Za změnu se považuje jak editace entity, tak i její výmaz. U kupónu má výmaz podobu změny stavu z "platný" na "stornovaný".

Whitelisty obsahují pouze reference na číselníkové entity. Konzumenti whitelistů (dopravci) obecně mají k dispozici API, které vrací aktuální podoby číselníků, které jsou ve whitelistech použité.

Číselníky jsou generovány pro následující soubory dat:

- Subjekty
- Zákaznické profily
- Tarify
- Zóny

Pro řešení v rámci IDPK budou jediným zdrojem stávající číselníky IDPK, manuálně vystavované formou CSV souborů na FTP server PMDP. Automatická synchronizace číselníků nebude pro IDPK implementována.

Popis požadavků na systém odbavení – strojky dopravců

Tato kapitola popisuje základní nároky na odbavovací zařízení dopravců zapojených do integrovaného dopravního systému IDPK. Jedná se o funkci akceptace/odbavení dopravního produktu zakoupeného prostřednictvím systému Virtuální karta. Zda a do jaké míry bude po dohodě mezi POVED a dopravcem konkrétní zařízení požadavek na HW uvedený v této kapitole splňovat, shrnuje sekce „Upřesnění řešení“ na konci tohoto dokumentu.

Pro zajištění výše uvedené funkce musí být akceptační 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.
- Akceptačním zařízením bankovních karet/platebním terminálem 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 (dle specifikace uvedené v příloze č. 2, 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 PTP /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 bud jeho další část zpracována do 1100 ms)
- LCD panelem minimální velikosti 9“ s rozlišení minimálně 800x600 (pokud nebude s Objednatelům dohodnuto jinak) 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 2 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 (tj. vyhledání záznamu dle načteného jedinečného identifikátoru, dešifrování osobní dat držitele identifikátoru a jejich zobrazení, vyhodnocení platnosti dopravního produktu a jeho zobrazení) do maximálně 700 ms.

Odbavovací zařízení dopravce, resp. back-office dopravce, musí dále zajistit:

- Realizaci funkcí symetrické a asymetrické kryptografie (dešifrování osobních dat držitele karty, ověření pravosti QR kódu)
- Pravidelnou komunikaci s rozhraním pro předávání dat strukturovaných souborů whitelistů, tj. musí zajistit podporu standardně používaných technologií pro výměnu dat mezi systémy, tj. zabezpečený FTP server/SFTP. Četnost této komunikace (pravidelný interval) bude možné upravovat. Četnost stahování Whitelistu bude nastavena na 10 minut (zařízení bude garantovat dostupnost změnových dat maximálně do 1 hodiny od jejich zveřejnění na SFTP serveru).
- Generování transakčních dat a jejich přenos do zúčtovacího systému. Datová struktura transakčních dat je dle platné datové věty IDPK (struktura ČSAD SVT).

Základní popis procesu odbavení:

- Vygenerování/načtení jedinečného identifikátoru dle uživatelem předloženého typu média (bankovní karta, dopravní karta, mobilní aplikace, papírová jízdenka vydaná jako doplatek)
- Vyhledání identifikátoru ve whitelistu
- Získání dat z whitelistu (osobní data uživatele, zakoupený dopravní produkt)
- Vyhodnocení územní a časové platnosti (dle aktuálně navolené trasy/linky v aplikačním software odbavovacího zařízení) – dle tarifních pravidel systému IDPK
- Případný výpočet/dopočet ceny jízdného dle zvolené trasy/linky – dle tarifních pravidel systému IDPK
- Zobrazení výsledku vyhodnocení územní a časové platnosti dopravního produktu, zobrazení osobních dat uživatele (včetně fotografie a zákaznické kategorie)
- Realizace možného doplatku za jízdné

Současný způsob tvorby transakčních vět pro Zúčtovací centrum ČSAD SVT bude pro potřebu akceptace Virtuální karty upraven o typ média (medium="token-pk") a vlastní 32B identifikátor karty (například: _____ card-id="4d5157111233574c756cCC564133536c354c11156b767432503211146242754b").

Algoritmus pro generování jedinečného identifikátoru bankovní karty:

- Bude předán v samostatném dokumentu po podpisu Smlouvy o ochraně důvěrných informací

Algoritmus pro generování jedinečného identifikátoru z údajů získaných z Plzeňské karty:

- Bude předán v samostatném dokumentu po podpisu Smlouvy o ochraně důvěrných informací

Popis způsobu získání jedinečného identifikátoru z datové struktury QR kódu mobilní aplikace Virtuální karta

- Bude předán v samostatném dokumentu po podpisu Smlouvy o ochraně důvěrných informací

Rozlišení QR jízdenky mobilní aplikace od papírové varianty QR jízdenky

- Datová struktura QR kódu bude doplněna v části REC_TICKET_BASIC o položku TicketForm, která určuje, na jakém médiu je jízdenka vystavena (příčemž: 0 = nespecifikováno, 3 = QR jízdenka mobilní aplikace)

Další přílohy tohoto dokumentu budou předány samostatně po podpisu Smlouvy o ochraně důvěrných informací.

Doplnění dokumentu – upřesnění řešení systému Virtuální karty u dopravců zapojených v IDPK

Tabulka níže shrnuje dohodu mezi POVED a dopravci zapojenými v IDPK ohledně naplnění požadavků na HW odbavovacích zařízení.

<u>Odbavovací zařízení</u>	<u>Naplnění požadavků na HW</u>
<u>UNIPOK ČD</u>	Pro 1. etapu projektu bude UNIPOK ČD doplněn o čtečku 2D kódů. POVED souhlasí s tím, že v rámci projektu nedojde k dalším změnám HW nad rámec současného stavu (k 1. 7. 2022). Pro 2. etapu budou bankovní karty tokenizovány na čtečce dopravních karet na základě výjimky udělené dopravci acquirerem.
<u>POP ČD/GWTR</u>	POVED souhlasí s tím, že v rámci projektu nedojde ke změnám HW nad rámec současného stavu (k 1. 7. 2022), přestože některé obecné požadavky na HW uvedené výše v tomto dokumentu nejsou naplněny (velikost LCD panelu, počet SAM slotů vyhrazených pro IDPK, atd.). Pro 2. etapu projektu budou bankovní karty tokenizovány na čtečce dopravních karet na základě výjimky udělené dopravci acquirerem.
<u>Revizorská aplikace PMDP</u>	POVED souhlasí, že v rámci projektu nedojde ke změnám HW nad rámec současného stavu (k 1. 9. 2022), přestože některé obecné požadavky na HW uvedené výše v tomto dokumentu nejsou naplněny

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

	(velikost displeje, počet SAM slotů vyhrazených pro IDPK, atd.).
--	---

Následující tabulky popisují specifika práce s jednotlivými identifikátory na konkrétních typech zařízení a procesy týkající se Virtuální karty v IDPK na základě dohod mezi POVED a dopravci.

		Typy identifikátorů VK				
		Vlastnost	Bankovní karta	Mobilní aplikace	Dopravní karta	Jízdenka vydaná jako doplatek k VK
Obecné vlastnosti	Od etapy		2	1	2	1
	Popis		Bankovní karta VISA nebo MasterCard	QR kód zobrazený v mobilní aplikaci	Bezkontaktní čipová karta DESfire EV1 popřípadě EV3 (MAP struktura). Plzeňská, Karlovarská nebo Mariánskolázeňská karta	QR kód vytištěný na papíře, obsahuje data jednotlivé jízdenky vydané jako doplatek k VK a token toho identifikátoru VK, který byl použit při prodeji
	Zdroj dat pro kontrolu		Whitelist	Whitelist + obsah zobrazené jednotlivé jízdenky	Whitelist + obsah karty	Whitelist + obsah zobrazené jednotlivé jízdenky
	Obsah dat		Profily (od etapy 2) Nárokové kupony Kupony OÚ + foto	Profily (od etapy 2) Nárokové kupony Kupony Jednotlivá jízdenka (v těle QR) OÚ + foto	Profily (ve WL od etapy 2 a na kartě) Nárokové kupony (ve WL a na kartě) Kupony (ve WL a na kartě) Jednotlivé jízdenky (na kartě) Další (kupony IDOK, produkty ČD, ...) OÚ + foto (z WL) OÚ z karty Foto (na těle karty)	Profily (od etapy 2) Nárokové kupony Kupony Jednotlivá jízdenka (v těle QR) OÚ + foto
	HW pro kontrolu		RFID čtečka	Čtečka 2D	RFID čtečka	Čtečka 2D
	Typ tokenu		Token trvale svázaný s fyzickou kartou, do systému zaveden prvotní tokenizací na platební bráně	Token trvale svázaný s konkrétní instalací mobilní aplikace Virtuální karta, vygenerován v okamžiku přihlášení uživatele v nové instanci aplikace	Token trvale svázaný s fyzickou kartou, vzniká prvotní tokenizací na HSM PMDP.	Nemá vlastní token, nese token toho identifikátoru, který byl použit při prodeji
	Způsob získání tokenu v OZ		PCI DSS čtečka nebo MAP SAM	Token je součástí 2D kódu	MAP SAM	Token je součástí 2D kódu
	Tokenizační klíč		Klíč vydavatele PMDP, bude předán formou MAP SAM PMDP nebo	-	Klíč vydavatele PMDP, bude předán formou MAP SAM PMDP nebo bude předán	

Příloha č. 1 Smlouvy o úpravě software odbavovacího zařízení POP a UNIPOK

České dráhy			bude předán dopravci pro uložení ve vlastních MAP SAMech.		dopravci pro uložení ve vlastních MAP SAMech.	
		Médium pro dokup jízdenky	Papír	Papír nebo jízdenka v MA	Datový prostor karty	Neumožňuje dokup
		Obsah položky "medium" ve větě SVT (kontrola)	token-pk	token-pk (pozor, týká se pouze kuponů z WL, nikoli jednotlivé jízdenky obsažené v 2D kódu)	token-pk (pozor, týká se pouze kuponů z WL, nikoli kuponů a jednotlivých jízdenek vyčtených z datového obsahu karty)	token-pk (pozor, týká se pouze kuponů z WL, nikoli jednotlivé jízdenky obsažené v 2D kódu)
		Obsah položky "card-id" ve větě SVT (kontrola)	Číslo uživatele z WL (32 B, hex)	Číslo uživatele z WL (32 B, hex) (pozor, týká se pouze kuponů z WL, nikoli jednotlivé jízdenky obsažené v 2D kódu)	Číslo uživatele z WL (32 B, hex) (pozor, týká se pouze kuponů z WL, nikoli kuponů a jednotlivých jízdenek vyčtených z datového obsahu karty)	Číslo uživatele z WL (32 B, hex) (pozor, týká se pouze kuponů z WL, nikoli jednotlivé jízdenky obsažené v 2D kódu)
	UNIPOK	Způsob akceptace	Čtečkou dopravních karet se souhlasem ČD i POVED na základě výjimky udělené dopravci acquirerem. WL (nebude stahován lokálně na UNIPOK, ale na server (PoMK))	2D čtečkou přes USB, WL (nebude stahován lokálně na UNIPOK, ale na server (PoMK))	RFID čtečka, WL (nebude stahován lokálně na UNIPOK, ale na server (PoMK))	Neakceptuje
		Způsob tokenizace				
		Dokup jízdenky	ANO	ANO	ANO	NE
		Informace o kartě	ANO	ANO	ANO, včetně obsahu WL (i fotografie)	NE
	Kontaktní místo	Správa uživatelského účtu	Po dohodě mezi POVED a ČD bude řešeno jako samostatný projekt. Není součástí zadání.			
	POP	Způsob akceptace	RFID čtečka, WL, se souhlasem ČD i POVED na základě výjimky udělené dopravci acquirerem.	Čtečka 2D, WL	RFID čtečka, WL	Čtečka 2D, WL

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

		Způsob tokenizace	MAP SAM ČD	Vyčtení 2D kódu	MAP SAM ČD	Vyčtení 2D kódu
		Kontrola	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)
		Dokup jízdenky	ANO	ANO, papír	ANO, do karty	NE
PMDP	Mobilní aplikace	Způsob akceptace	Neakceptuje	Online dotaz na server Virtuální karty	Neakceptuje	Neakceptuje
		Způsob tokenizace	Netokenizuje	Token je v paměti telefonu	Netokenizuje	Netokenizuje
		Dokup jízdenky	NE	ANO, jízdenka v MA	NE	NE
	Revizorská aplikace	Způsob akceptace	RFID čtečka, WL	Čtečka 2D, WL	RFID čtečka, WL	Čtečka 2D, WL
		Způsob tokenizace	PCI DSS čtečka	Vyčtení 2D kódu	MAP SAM PMDP	Vyčtení 2D kódu
		Kontrola	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)
		Dokup jízdenky	NE	NE	NE	NE
	Kontaktní místo	Správa uživatelského účtu	ANO	ANO	ANO	NE
GWTR	POP	Způsob akceptace	RFID čtečka, WL	Čtečka 2D, WL	RFID čtečka, WL	Čtečka 2D, WL
		Způsob tokenizace	MAP SAM PMDP	Vyčtení 2D kódu	MAP SAM PMDP	Vyčtení 2D kódu
		Kontrola	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)
		Dokup jízdenky	ANO	ANO, papír	ANO, do karty	NE
ARRIVA	AZ Telmax	Způsob akceptace	RFID čtečka, WL	Čtečka 2D, WL	RFID čtečka, WL	Čtečka 2D, WL
		Způsob tokenizace	PCI DSS čtečka	Vyčtení 2D kódu	MAP SAM PMDP	Vyčtení 2D kódu
		Kontrola	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)	ANO (včetně fotografie)
		Dokup jízdenky	ANO	ANO, papír	ANO, do karty	NE

Varianty prodeje (procesy)

Číslo / obecné	Druh prodávajícího produktu	Původní stav (1. etapa, 2020)	Zapojení VK do prodejního procesu na OZ	1. Bez karty (fyzické i virtuální)	2. Bankovní karta (od etapy 2)	3. Mobilní aplikace	4. Fyzická (dopravní) karta (od etapy 2)	Prodejní transakce do SVT
1	Síťová jízdenka	Vzniká (vždy nadzóna 255) zadáním více než 7 zón libovolné jízdenky (mimo přestupní z MHD Plzeň, Nepřestupní). Případný kupón se neuplatňuje, přestože by vedl na nižší cenu.	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru zařízení podporuje)	Papír, beze změny oproti současnému stavu	Profil: z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL nebo obsahu karty Médium: karta	Beze změny
2	Doplatková jízdenka (ke kupónu)	Platné kupóny musí být na kartě. Jízdenka se vždy zapisuje na kartu. Doplatkovou jízdenku nelze vydat k jízdence. Sleva (profil) jízdenky se NEMUSÍ rovnat slevě z uplatňovaných kupónů. Může vést k síťové jízdence	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru zařízení podporuje)	Papír, beze změny oproti současnému stavu	Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL Kupony (i nárokové): z WL nebo obsahu karty Médium: karta	Beze změny
3	Přestup z MHD Plzeň (P+V) - (prolongace)	Původní platná jízdenka vždy papírová obsahuje zóny 1, 199. Přestup vždy v P (zóna 1), jinak nelze prodat. Původní jízdenka slouží i k následné kontrole. Přestup se neuplatňuje, pokud původní jízdenka obsahuje jen zónu 1 nebo grupované sleva původní jízdenky neodpovídá slevě nové jízdenky. Nová jízdenka jen papírová. Počet osob vždy 1.	NE, beze změny					
4	Přestup z MHD Plzeň(V) - (prolongace)	Původní jízdenka vždy papírová obsahuje zónu 199. Přestup vždy v zóně V, jinak nelze prodat. Původní jízdenka slouží i k následné	NE, beze změny					

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

		kontrole. Přestup se neuplatňuje, pokud grupované sleva původní jízdenky neodpovídá slevě nové jízdenky. Nová jízdenka jen papírová. Počet osob vždy 1						
5	Nepřestupní	Jízdenka jen papírová (do 10 km). Neobsahuje QR. Na ČD obsahují výjimečně názvy železničních stanic	NE, beze změny					
6	Jízdenka MHD Plzeň	Zóny relace obsahují pouze 1	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru podporuje)	Papír, beze změny oproti současnému stavu	Zóny relace Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL Kupony (i nárokové): z WL nebo obsahu karty Médium: karta	Beze změny
7	Jízdenka s MHD Plzeň	Zóny relace obsahují i 1						
8	Jízdenka bez MHD Plzeň	Zóny relace neobsahují 1						
9	Turistická	Vždy síťová (vždy nadzóna 255 i když bude zvolena varianta bez DPH). Papírová i elektronická (karta, mobil) platí 24H od prodeje	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru podporuje)	Papír, beze změny oproti současnému stavu	Profil: z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL Kupony (i nárokové): z WL nebo obsahu karty Médium: karta	Beze změny
10	Zavazadlo/kolo/pes	Jízdenka jen papírová. Vždy síťová	NE, beze změny					
11	Jízdenka s Německem	Zóny relace obsahují německou zónu (parametr 2)	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru zařízení podporuje)	Papír, beze změny oproti současnému stavu	Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Kupony (i nárokové): z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL Kupony (i nárokové): z WL nebo obsahu karty Médium: karta	Beze změny

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

12	Turistická s Německem	Vždy síťová (vždy nadzóna 253). Papírová i elektronická (karta, mobil) platí 24H od prodeje	ANO, zákazník místo fyzické karty může předložit virtuální kartu (pokud daný typ identifikátoru podporuje)	Papír, beze změny oproti současnému stavu	Profil: z WL Médium: papír Token v QR: bankovní karty	Profil: z WL Médium: papír Token v QR: mobilní aplikace	Profil: z WL Kupony (i nárokové): z WL nebo obsahu karty Médium: karta	Beze změny
----	-----------------------	---	--	---	--	--	--	------------

Etapizace projektu:

- **Etapa 1 (POP – spuštění 11. 7. 2022; UNIPOK – spuštění říjen 2022)**
 - Whitelist neobsahuje informace o profilech
 - Jako identifikátor slouží pouze mobilní aplikace (pro dokup i kontrolu) a doplťková jízdenka vydaná k mobilní aplikaci (pouze pro kontrolu)
 - Vzhledem k absenci profilů ve whitelistu bude odbavovací zařízení při dokupu jízdenky odvozovat profily cestujícího z jeho aktuálně časově platných kuponů ve whitelistu (a volit mezi nimi na základě stávající prioritní tabulky). Pokud k identifikátoru nebude veden ve whitelistu žádný časově platný kupon, nebude dokupování umožněno a cestující bude odbaven papírovou jízdenkou bez vazby na virtuální kartu.
- **Etapa 2 (spuštění 30. 11. 2022 po dohodě s dopravci a dodavateli OZ)**
 - Do whitelistu bude zpětně kompatibilním způsobem doplněna informace o profilech cestujících, úprava struktury whitelistu je uvedena níže v této příloze
 - Jako identifikátor slouží nově i bankovní karta a karty Plzeňského typu
 - Odbavovací zařízení bude při dokupu jízdenky čerpat profily cestujícího z whitelistu (a volit mezi nimi na základě stávající prioritní tabulky). Pokud k identifikátoru nebude veden ve whitelistu žádný časově platný profil, nebude dokupování umožněno a cestující bude odbaven papírovou jízdenkou bez vazby na virtuální kartu.

Popis formátu Whitelistu

Tag Name		BerTl v Tag (hex)	Primitive/ Construct ed	Type	Fixed/Varia ble length	Length (bytes)	Description
Header		0xE1	C		F	29	
	Increment Offset	0xC1	P	NUMBER	V	4	value = 0 - full whitelists value > 0 - increment whitelists value < 0 - never, wrong value
	Increment Number	0xC2	P	NUMBER	V	4	
	Generated Date Time	0xC3	P	GeneralizedTime	F	15	in UTC Timezone, format: YYYYMMDDHHMM SSZ
Client		0xE2	C		V		
	ID	0xC1	P	NUMBER	V	8	
	Delete d	0xC6	P	BYTE	F	1	True - 0xFF, False - 0x00
	Person al Data	0xC7	P	BYTE_ARRAY	V		Encrypted data
	First name	0xC2	P	STRING	V	-	UTF-8 encoding
	Last name	0xC3	P	STRING	V	-	UTF-8 encoding
	Birt h Date	0xC4	P	DATE	F	4	example data: 0x19881027 - 27.10.1988
	Phot o	0xC5	P	BYTE_ARRAY	V		
Identifier		0xE3	C		V		
	ID	0xC1	P	NUMBER	V	8	

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

Client ID	0xC2	P	NUMBER	V	8	
Token Hash	0xC3	P	BYTE_ARRAY	F	20	SHA1(Token), see
PDEK	0xC4	P	BYTE_ARRAY	F	16/32	Encrypted using IPEK (IPEK = MD5(Token)), Encryption standards: AES-128-CBC-PKCS5
Type	0xC5	P	BYTE	F	1	See Identifier Type Definition table
State	0xC7	P	BYTE	F	1	See Identifier State Definition table
Deleted	0xC6	P	BYTE	F	1	True - 0xFF, False - 0x00
Coupon	0xE4	C				
ID	0xC1	P	NUMBER	V	8	
Identifier ID	0xC2	P	NUMBER	V	8	
Start Date Time	0xC3	P	GeneralizedTime	F	15	in UTC Timezone, format: YYYYMMDDHHMMSSZ
End Date Time	0xC4	P	GeneralizedTime	F	15	in UTC Timezone, format: YYYYMMDDHHMMSSZ
Subject ID	0xC5	P	NUMBER	V	8	
Subject Registration Number	0xD5	P	NUMBER	V	4	
Customer Profile ID	0xC7	P	NUMBER	V	8	
Customer Profile Registration Number	0XD7	P	NUMBER	V	4	Zde je číslo CP odpovídající tabulce CP/TP (synchronizace číselníků) pro vyhodnocení u dopravců a ostatních subjektů
Tariff ID	0xC8	P	NUMBER	V	8	

Příloha č. 1 Smlouvy o úpravě software
odbavovacího zařízení POP a UNIPOK

Tariff Registration Number	0xD8	P	NUMBER	V	4	Zde je číslo TP odpovídající tabulce CP/TP (synchronizace číselníků) pro vyhodnocení u dopravců a ostatních subjektů
Zones (IDs)	0xC9	P	STRING	V		Comma-delimited number values, UTF-8 encoding
Zones (Registration Numbers)	0xD9	P	STRING	V		Comma-delimited numeric values, UTF-8 encoding
Deleted	0xC6	P	BYTE	F	1	True - 0xFF, False - 0x00
Profile	0xE5	C				
ID	0xC1	P	NUMBER	V	8	Internal ID of the customer profile.
Customer Profile Registration Number	0xD1	P	NUMBER	V	4	Registration number "CP" of the customer profile.
Client ID	0xC2	P	NUMBER	V	8	ID of the client (0xE2 → 0xC1).
Start Date Time	0xC3	P	GeneralizedTime	F	15	Start of profile assignment validity period, in UTC Timezone, format: YYYYMMDDHHMM SSZ
End Date Time	0xC4	P	GeneralizedTime	F	15	End of profile assignment validity period, in UTC Timezone, format: YYYYMMDDHHMM SSZ
Subject ID	0xC5	P	NUMBER	V	8	ID of the subject who owns the profile.
Subject Registration Number	0xD5	P	NUMBER	V	4	Registration number of the subject who owns the profile.

	Deleted	0xC6	P	BYTE	F	1	True - 0xFF, False - 0x00
--	---------	------	---	------	---	---	---------------------------

Identifier Type Definition

Name	Value (hex)	Description
APPLICATION	0x01	
BANK_CARD	0x02	

Identifier State Definition

Name	Value (hex)	Description
ACTIVE	0x01	
BLOCKED	0x02	
SUSPENDED	0x03	
EXPIRED	0x04	
DELETED	0x05	

Example of encrypting personal data

Clear input personal data

Field	Value
Firstname	Josef
Lastname	Novák
Birthdate	31.12.1985
Photo	not set (field will be missing)

Encryption inputs

Name	Value
Clear PDEK (hex)	013D7D16D7AD4FEFB61BD95B765C8CEB

Clear Personal Data before encryption (hex)	C2054A6F736566C3064E6F76C3A16BC40419851231
Initial Vector (hex)	00000000000000000000000000000000
Encrypte d Personal Data (using AES-CBC with PKCS5 padding) (hex)	6A9176F74182EF4FA44A34644843B3F8DBDB569967728D6992BFFD2DA6478C3 B

Example of encrypting PDEK

Encryption inputs

Name	Value
Clear token value	104eded71764d7e7818513ee9c08770ca01f85a2618c0713315dfaa6ecc57f41
Clear PDEK (hex)	013D7D16D7AD4FEFB61BD95B765C8CEB
MD5(token) = IPEK (hex)	e90d33f346ef68cd17293631b5d67946
Initial Vector (hex)	00000000000000000000000000000000

Encrypted PDEK using IPEK (AES-CBC with PKCS5 padding) (hex)	CDE0240B286761E14985BA1CAAF545D56814BB907AB315FF0CB48FD98DE20 BBD
---	--

Example of hashing token value

Name	Value
Clear token value	104eded71764d7e7818513ee9c08770ca01f85a2618c0713315dfaa6ecc57f41
SHA1(token)(hex)	0548C028856178297F9A4E2C311BD22FF1720B21