MOS – odbavovací zařízení - Příloha č. 1

Technická specifikace

POŽADAVKY MOS NA ODBAVOVACÍ ZAŘÍZENÍ

Níže uvedené specifikace jsou stanoveny OICT coby provozovatelem MOS a bezpečnostním garantem EOC realizovaným prostřednictvím MOS. Dokument je nedílnou součástí Standardů odbavení, které jsou vydány organizátory veřejné dopravy ROPID a IDSK, a je závazný pro správce odbavovacích zařízení, nebude-li určeno jinak.

Informace uvedené v tomto dokumentu jsou neveřejné. Pokud mají být použity jako podklad pro zadávací dokumentaci ve veřejné soutěži, je nutné dané podklady následně upřesnit s provozovatelem MOS.

OBSAH

SHRNUTÍ DOKUMENTU

Dokument popisuje aspekty řešení MOS (Multikanálový odbavovací systém) v souvislosti s funkcionalitami odbavení a kontroly cestujících v rámci Hl. města Prahy a Středočeského kraje.

Textace dokumentu má charakter technických specifikací popisující jednotlivé funkční celky, parametry řešení, procesní stavy a bezpečnostní aspekty.

Dokument je pracovním materiálem OICT a může být následně rozvíjen či jeho části mohou být zapracovány do návazných dokumentů organizátorů dopravy ROPID a IDSK.

ODBAVENÍ S VYUŽITÍM METODY WHITELIST

Nový odbavovací systém pro Prahu a Středočeský kraj je založen na on-line databázovém řešení, s distribucí informací nutných pro odbavení cestujících přímo do odbavovacích zařízení dopravců či do terminal management systémů (TM) správců odbavovacích zařízení. Informace pro odbavení budou obsaženy v tzv. whitelistech (WL – seznam jízdních dokladů vázaných k identifikátoru), denylistech (DL – seznam platebních karet, u kterých není povolena platební transakce – bude použit v případě zavedení agregování platebních transakcí) a blacklistech (BL – seznam zakázaných identifikátorů). Níže jsou uvedena možná řešení odbavení při využití kontrol přes WHITELIST. Předpokladem OICT je využití tohoto způsobu odbavení pro regionální a příměstskou autobusovou dopravu, železniční dopravu a revizorské kontroly v celém PID prostředí.

PŘÍMÁ KOMUNIKACE ODBAVOVACÍHO ZAŘÍZENÍ S MOS

- Komunikační rovina, kdy odbavovací zařízení či revizorská čtečka přistupují na repository MOS (síťově vystavené úložiště) a z daného repository stahují WL a další potřebná data k odbavení či kontrole.
- Stahování dat iniciované koncovým zařízením v definované periodě či vynucené uživatelem koncového zařízení mimo standardní periodu.
  - Data jsou zasílána v šifrované podobě, aby nedošlo při jejich odchycení a následně k jejich zneužití
  - Definice šifrovacího klíče a rozsahu šifrovaných dat bude určena v implementační fázi
- Formát dat WL a dalších je definován provozovatelem MOS:
  - Formát je předpokládán ve standardizovaném formátu databázových indexovaných souborů
  - Formát bude zvolen jako optimální pro rychlost načítání informací a následné rychlé odbavení či kontrolu
  - Konverze dodaných dat do jiného formátu je nevhodná, a to z důvodů:
    - Možnost poškození či pozměnění dat
    - Snížení rychlosti odbavení, pokud formát dat nebude vhodně indexován či mechanismus načtení dat nebude efektivní
    - Další mezikrok, jenž může způsobit neočekávané stavy.
- Uložení stažených dat z MOS na koncové zařízení musí splňovat následující parametry:
  - Data jsou uložena na koncovém zařízení v chráněném repository, do nějž je přístup zajištěn autentizací v rámci zařízení – zajištění odbavovacích dat MOS proti přímému přístupu uživatele, zajištění dat ověřovacím mechanismem na úrovni aplikačního přístupu nutnému pro zajištění bezpečnosti dat v koncovém zařízení
  - Pokud jsou fotografie z WL uloženy v nevolatilní paměti, musí být šifrovány tak, aby použitý algoritmus a klíč byl považován za bezpečný podle aktuálních poznatků z oblasti, např. s doporučeními NIST či požadavků PCI.
  - Klíč pro šifrování fotografií z WL je v nevolatilní paměti uložen některým z následujících způsobů:
    a) v SAM
    b) ve PCI-DSS certifikovaném zařízení
    c) v interním nebo externím HW modulu s bezpečnostními funkcemi
    d) v šifrovaném úložišti s 2FA autorizací. 2FA autorizace může být security smart card + PIN; biometrie + PIN; PIN + OTP, PIN + certifikát; PIN + HW token; nebo obdobně bezpečná kombinace.
- Výkonnostní požadavky
  - Časové požadavky na odbavení bankovních platebních karet jsou dány pravidly karetních společností a musí být dodrženy
  - Iniciální velikost WL bude cca. 2,5 GB a je předpokladem, že nahrání WL je realizováno při nastavení koncových zařízení
  - Aktualizace WL a dalších dat jsou realizovány ve formě inkrementálních dat, kdy koncové zařízení v pravidelné periodě kontroluje nový inkrement na repository MOS a případně jej stahuje a automatizovaným procesem změny zapracovává
    - Kvalifikovaný odhad inkrementu je v rozsahu 120kB bez aktualizace fotografií
    - Předpokládaná četnost aktualizace WL je plánována v rozsahu 5-15min

- Oblast zahrnující uložení fotografií v rámci WL bude separátním datovým souborem s četností aktualizace 1x za den (24h)
- Jedenkrát za den je WL prohlášen za aktuální se zapracovanými rozdíly. Následně se rozbíhá nová sada inkrementů pro další den (24hodin)
- Rozdílové inkrementy po jejich zapracování nejsou odstraněny, ale jsou konsolidovány do tzv. denního uceleného inkrementu. Daný denní inkrement bude uložen v repository MOS a pokud nastane situace, kdy koncové zařízení bude vyžadovat aktualizaci WL při rozsahu aktualizace vyšší než jeden den (24h) využije tento konsolidovaný inkrement.
- V podobném sledu bude vytvářen i týdenní konsolidovaný inkrement.

NEPŘÍMÁ (TM SERVER) KOMUNIKACE ODBAVOVACÍHO ZAŘÍZENÍ S MOS

- Komunikační rovina, kdy TM servery přistupují na repository MOS (síťově vystavené úložiště) a z daného repository stahují WL (či další potřebná data k distribuci pro odbavení či kontrolu).
- Stahování dat iniciované TM servery v definované periodě či vynucené uživatelem TM serveru mimo standardní periodu
- Pro přenos dat a uložení platí shodné požadavky jako u přímé komunikace popsané výše.
- Uložení stažených dat z MOS na TM serveru musí splňovat následující parametry:
  - Data jsou uložena na TM serveru takovým způsobem, aby nebylo možné je modifikovat, poškodit, zneužít, zcizit či k nim bez řádného důvodu a autorizace přistupovat.
  - Správce TM serveru zajišťuje dostupnost, důvěrnost a integritu dat MOS u něj uložených. Dbá zejména na oddělení rolí, autorizaci uživatelů a auditování jejich činnosti.
  - Po stažení dat z MOS je provozovatel TM serveru odpovědný za dodaná data.
  - Samotný obsah dat není provozovatel TM serveru oprávněn měnit (strukturu ano).
- Následná distribuce dat a jejich použití je v gesci provozovatele TM serveru (správce odbavovacích zařízení).

PRINCIP KOMUNIKACE/PŘÍSTUPU K ODBAVOVACÍM DATŮM PRO PŘÍMOU I NEPŘÍMOU KOMUNIKACI

Zásadní předpoklady zajišťující funkční proces

- MOS prostředí vystavuje datové soubory s inkrementy dle výše uvedené definice v pravidelných intervalech a zajišťuje neustálou dostupnost těchto dat pro jejich následné stažení
- MOS garantuje integritu a správnost poskytovaných dat
- MOS vystavuje data pro přístup na Frontend řešení MOS ve formě publikovaných souborů umožňujících jejich stažení pro autorizované klienty (TMS, odbavovací zařízení)
- Ověření klientů je oproti MOS autentizačnímu řešení
- Tento typ komunikace neslouží pro iniciální nasazení WL(odbavovacích dat) jehož velikost může být mezi 1-2,5 GB. Iniciální nasazení dat do odbavovacího zařízení je realizováno offline přes zabezpečené přenosné repository.

Princip předpokládané komunikace

- Klient (TMS, odbavovací zařízení) volá přes své rozhraní prezentační vrstvu MOS. V rámci volání je MOS dotazován, zdali není publikována aktuálnější verze odbavovacích dat, než je verze umístěná v TMS či v odbavovacím zařízení (na pozadí probíhá proces ověření).
  - Pokud data na MOS **nejsou** novější než data v TMS, komunikace je ukončena a záznam o komunikaci je uložen do logu TMS či OZ.
  - Pokud data na MOS prezentační vrstvě jsou **novějšího** typu, je zpětně informován TMS či odbavovací zařízení o tomto stavu.
    - Následně TMS či odbavovací zařízení iniciuje požadavek na stažení těchto dat
    - Po stažení dat je navrácena informace o úspěšném stažení

        - Následně jsou odbavovací data dešifrována a rozdílové soubory zapracovány do odbavovacího zařízení (u TMS jsou připravena rozdílová dat pro další zpracování)
- Pokud v rámci komunikace s TMS či odbavovacím zařízením dojde k selhání ověření verze odbavovacích dat či přerušení komunikace nebo chybnému stažení, je následně komunikace opakovaně navazována co nejdříve po obnovení datového připojení.

ON-LINE KOMUNIKACE ODBAVOVACÍHO ZAŘÍZENÍ S MOS

- Nově uvažované propojení koncových zařízení typu revizorská čtečka či odbavovací zařízení na prostředí MOS.

Parametry:

- Komunikační rozhraní LTE, 4G, 3G, GPRS, v definovaných oblastech WIFI
- Pro on-line komunikaci bude v rámci implementace MOS vydefinováno komunikační API mezi koncovými zařízeními a MOS prostředím
    - V kontextu on-line komunikace není možné uvažovat napojení koncových zařízení na WL a další data uložená na chráněném repository MOS
- Přímá on-line komunikace koncových zařízení do MOS je přímým přístupem přes Front-End vrstvu MOS do "živého" prostředí k on-line datům.
    - Není předpokladem provozovatele, že daný způsob komunikace přesáhne 30 % běžného provozu koncových zařízení na MOS.

ODBAVOVACÍ ZAŘÍZENÍ – TECHNICKÉ VYMEZENÍ, PROCESY

Popis požadavků na koncové zařízení z pohledu zpracování odbavovacích dat MOS a předpokládaných procesů a bezpečnostních aspektů.

Proces komunikace – v rámci komunikace načítání WL z MOS repository či TMS (Terminal Management System) bude zařízení iniciovat následující procesy:

- Vyvolání spojení na MOS ve formě autentizovaného spojení přes definovaný komunikační port na TCP-IP úrovni bude zabezpečeno šifrováním na úrovni HTTPS s použitím HSTS a DNSSEC validace a autorizováno pomocí přihlašovacích údajů případně certifikátu. Spojení je možné zabezpečit i pomocí VPN.
    - Princip komunikace s TMS je v gesci Dopravce/Provozovatele koncového zařízení
- Vyvolání kontroly aktualizace - kontrola verze WL oproti aktualizaci na zdrojovém místě (MOS/TMS)
- Pokud je aktualizace nalezena je v rámci zabezpečené komunikace (MOS) zajištěn přenos dané aktualizace do úložiště koncového zařízení
    - Je požadavkem MOS jako poskytovatele odbavovacích dat, aby úložiště na koncovém zařízení splňovalo následující parametry
        - Úložiště neumožňuje přístup jakémukoliv uživateli přihlášenému do odbavovacího zařízení
        - Přístup je zajištěn pouze přes aplikační úroveň lokálním servisním účtem pod, kterým běží aplikační rozhraní.
        - Jakýkoliv přístup do úložiště (mimo operace odbavení) je plně logován a data jsou 1x denně zasílána do backendu MOS (zdrojové úložiště MOS)

Proces uložení a zpracování

Výše uvedený komunikační proces zajistil dodání datové aktualizace do cílového úložiště koncového zařízení.

Následuje proces, který zajistí data pro zpracování:

- Aktualizace (inkrement) – je aplikačně načtena na straně koncového zařízení.
- Následně je inkrement zapracován do WL (proběhne aktualizace záznamů v WL , jež jsou součástí inkrementu)
- Pokud je proces zapracování úspěšný je povýšena verze WL
- Jestli je zapracování neúspěšné jsou rozběhnuty opravné mechanismy
    - Je zasláno hlášení o chybném zapracování

-
- Obdobně v případě selhání načtení a opakovaných pokusů o načtení (3 pokusy) je zařízení prohlášeno za neaktuální a je o daném stavu zasláno hlášení do MOS a k dopravci/-provozovateli

Zabezpečení dat a procesu

Jak bylo výše uvedeno, je komunikace mezi koncovým zařízením a zdrojovými systémy MOS/TMS zajištěna. Taktéž je potřebné zajištění dat na cílovém úložišti v požadovaném rozsahu. V neposlední řadě je nutné zajistit informovanost o stavech v úložišti a na komunikační úrovni formou logování/auditování dění.

Zde jsou uvedeny požadované aspekty takového zabezpečení:

- **Komunikace zajištěna** připojením point to point (koncové zařízení „to“ zdrojový systém)
  - Zabezpečení pro takové spojení na úrovni ověření přístupu
  - Komunikace zapouzdřena pro zajištění nečitelnosti komunikace a dat při útoku zvenčí
  - Logované stavy propojení
- **Úložiště**
  - Úložiště zajištěné proti uživatelskému a datovému vstupu (načtení/manipulace/stažení)
  - Přístup pouze přes definované aplikační rozhraní vytvořené ve spolupráci s provozovatelem MOS
  - Přístup/ověření přes lokální účet navázaný na servisní službu aplikace
- **Logování/auditování**
  - Zajištění logování všech stavů spojených s řešením odbavení při využití úložiště a procesů MOS
  - Auditování přístupu na úložiště
- Synchronizace času
  - Zařízení synchronizují a udržují přesný čas

SOUBĚŽNÉ PROCESY SOUVISEJÍCÍ S ODBAVENÍM

KOMUNIKACE SPRÁVCŮ ODBAVOVACÍCH ZAŘÍZENÍ VŮČI MOS

- Provozovatel řešení MOS předpokládá, že v rámci běžné komunikace MOS vůči okolnímu prostředí bude v komunikační rovině probíhat i výměna dat mezi Správci odbavovacích zařízení (ve většině případů se bude jednat o Dopravce) a MOS ve smyslu dodávky informací o stavech a dění v prostředí v rámci odbavení a kontroly. MOS předpokládá následující stavy komunikace Správce -> MOS.
  - Správce odbavovacích zařízení/Dopravce poskytuje provozovateli MOS komplexní a aktualizovaný seznam odbavovacích zařízení/vozidel a revizorských zařízení, a to ve stavu aktuální poskytované informace.
    - Forma výměny a četnost bude definována.
  - Poskytovaná data dopravcem jsou informativního charakteru a zahrnují následující statistické a provozní informace:
    - Stav aktuálnosti WL a ostatních MOS dat
    - 1x za den informace o odbavení identifikátory, ke kterým je vázán jízdní doklad
    - Selhání, nestandardní stavy, a další provozní informace ovlivňují poskytované služby MOS
    - Informace bezpečnostního charakteru spojené s přístupem k MOS poskytovaným službám
- Výše uvedené požadavky na datové toky mají následující význam
  - Analytické informace spojené s provozem, užíváním WL a ostatních MOS dat
  - Statistické vyhodnocení odbavení či kontroly
  - Dohled stavů s dopadem na provoz MOS funkcionalit
  - Bezpečnostní analytika

- Předávané informace musí respektovat zajištění bezpečného předání dat mezi Správcem a MOS provozovatelem.
    - Data jsou předána do MOS repository Správcem/dopravcem či koncovým zařízením (odbavovací terminál či revizorská čtečka)
    - Daný přenos je předán zabezpečenou formou v předem definovaném formátu pro následné načtení do DB řešení MOS.
    - Úroveň požadovaného zabezpečení bude definována v analytické fázi projektu MOS.

TOKENIZACE V KONCOVÝCH ZAŘÍZENÍCH A PRÁCE S IDENTIFIKÁTORY

BPK jsou na koncových odbavovacích zařízeních tokenizována už v PCI-DSS certifikované části zařízení, ostatní identifikátory MOS mohou být tokenizovány tamtéž, nicméně je přípustné tuto funkcionalitu řešit i v mimo PCI-DSS certifikovanou část. Minimálně musí být odbavovacími zařízeními podporovány všechny v současnosti vydávané BPK od VISA a Mastercard.

Odbavovací zařízení musí podporovat čtení a práci minimálně s následujícími typy karet:

Mifare DesFire EV1 (všechny dostupné velikosti)

Mifare DesFire EV2 (všechny dostupné velikosti)

Dále musí plně implementovat ISO/IEC 14443 tak aby v budoucnu byla možná podpora i dalších typů nosičů.

- Pokud je i tokenizace ostatních partnerských karet prováděna v PCI-DSS certifikované části postačí z bezpečnostního hlediska pouze dodržování PCI-DSS.
- Pokud je tokenizace prováděna mimo PCI-DSS část jsou požadavky na uložení klíčů v nevolatilní paměti následující:
    a) v SAM
    b) ve PCI-DSS certifikovaném zařízení
    c) v interním nebo externím HW modulu s bezpečnostními funkcemi
    d) v šifrovaném úložišti s 2FA autorizací
        2FA autorizace může být security smart card + PIN; biometrie + PIN; PIN + OTP, PIN + certifikát; PIN + token; nebo obdobně bezpečná kombinace

V koncových odbavovacích zařízeních je doporučeno pracovat s oběma platnými tokeny ke každému nosiči z důvodu bezešvého přechodu celého systému v době expirace jednoho z klíčů/algoritmů na nový, byť v případě, že správce TMS je schopen veškerá svá zařízení dálkovým přenosem v řádu hodin převést na nové tokenizační algoritmy a klíče, lze zajistit funkčnost odbavení i pouze s jedním platným tokenem.

Odbavovací zařízení budou podporovat ověření pravosti a jedinečnosti vybraných identifikátorů/karet prostřednictví otevření zabezpečeného úložiště (nebo jeho části) za pomoci čtecích klíčů uložených na SAM.

Zároveň umožní i možnou budoucí implementací ověření ostatních partnerských karet v režimu challenge-response.

Správce TMS obdrží stanoveným klíčovacím ceremoniálem od tonizačního procesora nové klíče a algoritmy pro tokenizace dle schématu životnosti párů algoritmus/klíč MOS. Výchozí hodnota je obnova páru algoritmus/klíč každé 3 roky.

Klíčovací ceremoniál bude detailně popsán až v implementační fázi dle dohody s tokenizačním procesorem.

ODBAVENÍ POMOCÍ MOBILNÍ APLIKACE

Popis požadavků na koncové zařízení z pohledu zpracování odbavení cestujících využívající mobilní aplikaci pro nákup jednotlivých jízdenek.

Mobilní aplikace podporuje několik variant kontroly jednotlivých jízdných dokladů podle typu:

1. Vizuální kontrola
2. Strojové načtení 2D kódu
3. Dotaz do DB

VIZUÁLNÍ KONTROLA

ÚVOD

Na zobrazení jednotlivé jízdenky v mobilní aplikaci bude zobrazena vizuální informace o její platnosti zároveň s ochrannými bezpečnostními prvky zamezující jejímu padělání a/nebo redistribuci. Platnost a správnost zobrazených dat bude ověřitelná pouhým pohledem kontrolující osoby.

Pro kontrolu, zda zobrazená vizuální informace odpovídá současnému nastavení, zajistí backend mobilní aplikace vizuální informaci pro následnou kontrolu (referenční zobrazení). **Pro zobrazení na koncových zařízeních bude nutný barevný displej.**

TECHNICKÉ PARAMETRY

Pro vizuální informaci v mobilní aplikaci je po dodavateli požadováno

- jednoznačnost a jednoduchost kontroly pouhým okem,
- co možná největší velikost textu,
- zřetelné zobrazení informace o časové i pásmové platnosti a ověřovacího kódu,
- kód nesmí obsahovat zaměnitelné znaky, musí být segmentově členěný,
- zobrazení unikátní informace o kupujícím (např. kombinace verze systému a názvu zařízení),
- zabránění prolomení bezpečnosti pomocí zaslání screenshotu jízdenky, sdílení obrazovky apod., např. zobrazením informací na nezaměnitelném pozadí, na dynamicky měnícím se pozadí unikátním v každý okamžik, zobrazením informací o platnosti jako pohyblivého textu, nebo jinak,
- bude vždy obsažen interaktivní prvek, reagující na vstup uživatele.

STROJOVÉ ČTENÍ 2D KÓDU

ÚVOD

Na jízdence bude zobrazen 2D kód (QR, Aztec či podobný) a jeho kontrola bude probíhat optickým načtením a automatickým zobrazením platnosti. **Koncové kontrolní zařízení bude vybaveno optickou čtečkou, jejíž parametry jsou předpokládány:**

- Načtení kódu v průměrném čase do 1500 ms od zaostření (je-li na displeji mobilního telefonu zobrazována sekvence takových 2D kódů, pak musí zaostření probíhat pouze pro první z nich,
- každý další 2D kód tedy musí být přečten průměrně do 1000 ms od zobrazení bez nutnosti dalšího zaostření).
- Typ kódu: QR kód bez dalších hash kódů
- Korekce: 8% (Level L)
- Verze: 23 (109 x 109 modulů)
- Schopnost načtení jak elektronické, tak papírové verze kódu.

TECHNICKÉ PARAMETRY

Pro 2D kód v mobilní aplikaci je po dodavateli požadováno

- jeden ze standardně používaných 2D kódů (QR nebo Aztec),
- změna 2D kódu každých 10 vteřin,
- tato změna probíhá offline, bez konektivity na server,
- po jeho změně je platný současně zobrazený a jeden předchozí kód, všechny ostatní předchozí jsou neplatné,
- tato změna je robustní vůči prolomení nastavením jiného času v zařízení apod. (používá vnitřní čítač CPU v režimu „stopky“),
- kódování informace do 2D kódu v takové podobě, aby byly splněny veškeré technické parametry a limity na spolehlivost a rychlost čtení (odbavení),
    - Proces validace jízdenky v aplikaci trvá od doby úspěšného načtení 2D kódu do zobrazení informace o jeho platnosti maximálně 1s,
    - Doba odezvy backendu pro online transakce je menší než 900ms (neřeší komunikační trasu, GSM/LTE/WiFi).
- robustnost vůči nepřesnosti čtení, dostatečná korekce chyb a tolerance různým častým distorzím,
- rozsvícení displeje zařízení na maximální jas v momentě zobrazení kódu ke kontrole.

V případě on-line komunikace odbavovacího zařízení se provede ihned plnohodnotná validace s provedením záznamu do jádra dopravce/MOS; v opačném případě (tedy kdy není k disposici konektivita – online) se s využitím asymetrické kryptografie a veřejného klíče provede ověření kódu na vystavené jízdence a zároveň se informace o provedené validaci zařadí do fronty k dávkovému odeslání směrem do jádra dopravce/MOS prostřednictvím REST API rozhraní.

NFC KONTROLA

ÚVOD

V cílovém stavu bude kontrola jízdenek probíhat přes přenos dat pomocí technologie NFC. V současnosti bude tato funkcionalita dostupná pouze pro mobilní zařízení, které funkcionalitu podporují. **Koncová kontrolní zařízení musí obsahovat NFC technologii pro přenos dat o platnosti jízdenek v mobilní aplikac**i.

TECHNICKÉ PARAMETRY

Na NFC kontrolu je po dodavateli mobilní aplikace požadováno

- dodržení standardu ISO 18092:2004 pro přenos dat.

ONLINE DOTAZ

ÚVOD

Možnost zaslání ad hoc dotazu do backendu (BE) mobilní aplikace, který obsahuje DB všech jízdenek. BE obratem zašle do kontrolní aplikace informaci o tom, zdali je jízdenka skutečně zakoupená/platná.

TECHNICKÉ PARAMETRY

Na realizaci online dotazu je po dodavateli požadováno

- jedná se o definované a popsané API pro komunikaci dalších subjektů s BE mobilní aplikace,
- doba odezvy backendu pro online transakce je menší než 900ms (neřeší komunikační trasu, GSM/LTE/WiFi).

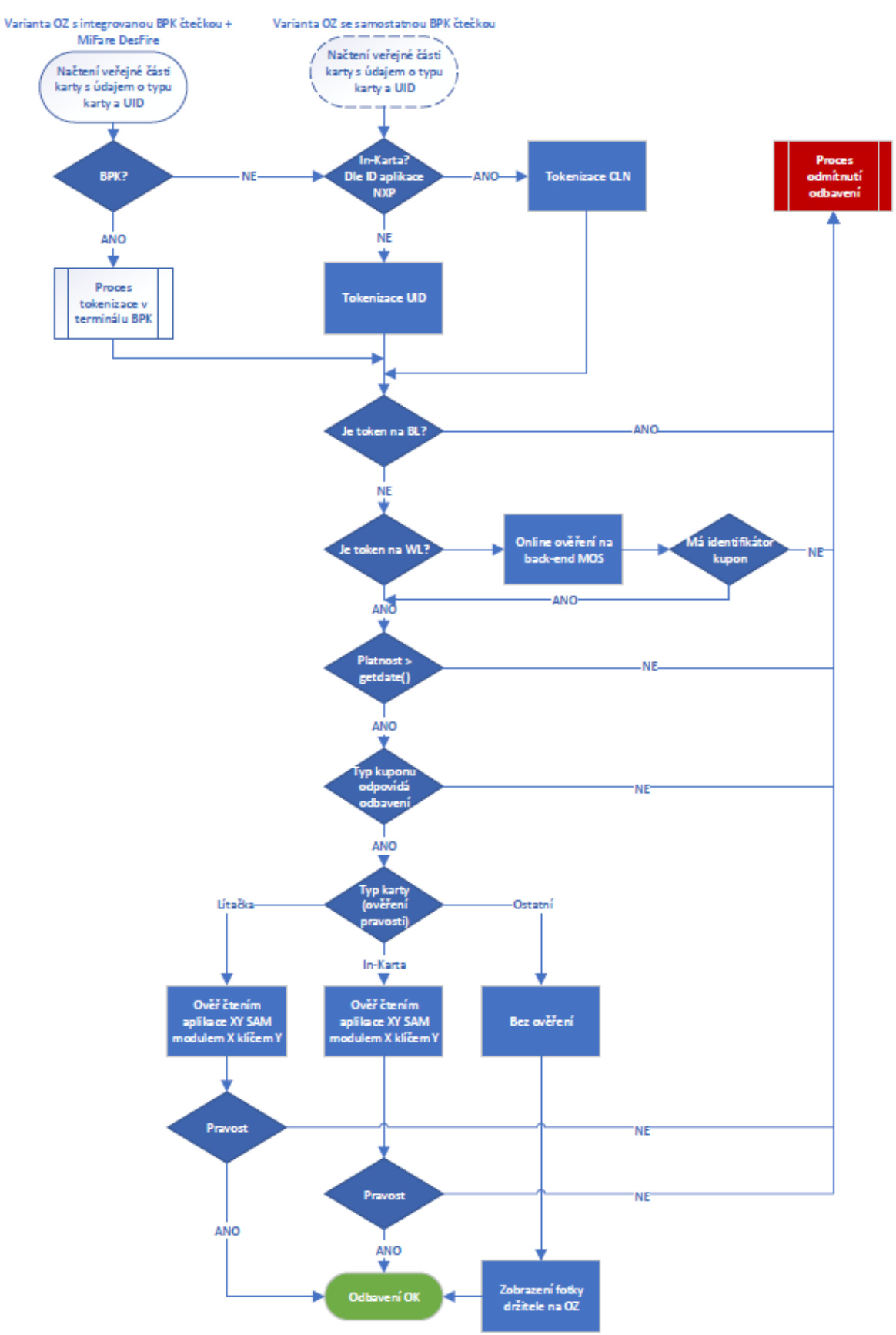
SCHÉMATICKÁ ZNÁZORNĚNÍ ODBAVENÍ

Níže jsou uvedeny předpoklady OICT ohledně možných scénářů odbavení. Jedná se o příkladová schémata nikoliv o komplexní množinu možných situací.

Rychlost odbavení při odbavení identifikátoru, ke kterému může být vázán jízdní doklad, včetně následujících operací s identifikátorem:

- Načtení veřejné části karty s údajem o typu karty a UID
- Přepnutí integrované čtečky s rozhraním pro čtení BPK a Mifare na potřebné rozhraní
- Ověření identity karty a autentizace (v případě Mifare)
- Vytvoření tokenu z ID nosiče dle definovaných postupů
- Vyhledání tokenu na whitelistu
- Kontrola platnosti jízdního dokladu vázaného k tokenu v místě a čase – výběr platného jízdního dokladu
- Zobrazení informací o platném jízdním dokladu na displeji palubního počítače/kontrolního zařízení

Nesmí trvat déle než 2,5 s. Střední doba pro odbavení (výše uvedené operace) je stanovena na 1,5 s.


Varianta OZ s integrovanou BPK čtečkou + MiFare DesFire
Varianta OZ se samostatnou BPK čtečkou
Načtení veřejné části karty s údajem o typu karty a UID
Načtení veřejné části karty s údajem o typu karty a UID
BPK?
NE
In-Karta? Dle ID aplikace NXP
ANO
Tokenizace CLN
Proces odmítnutí odbavení
ANO
NE
Proces tokenizace v terminálu BPK
Tokenizace UID
Je token na BL?
ANO
NE
Je token na WL?
Online ověření na back-end MOS
Má identifikátor kupon
NE
ANO
ANO
Platnost > getdate()
NE
ANO
Typ kuponu odpovídá odbavení
NE
ANO
Typ karty (ověření pravosti)
Létačka
Ostatní
In-Karta
Ověř čtením aplikace XY SAM modulem X klíčem Y
Ověř čtením aplikace XY SAM modulem X klíčem Y
Bez ověření
Pravost
NE
Pravost
NE
ANO
ANO
Odbavení OK
Zobrazení fotky držitele na OZ

ODBAVOVACÍ DATA

Následující popis datového formátu slouží pro ilustraci datových položek a není konečným formátem WL. MOS bude whitelisty generovat minimálně ve formátu xml/json.

ODBAVOVACÍ DATA – SEMI-ONLINE SOUBORY

WHITELIST (WL)

Komunikace MOS -> OZ/TM.

ZPRÁVY

Zpráva	Popis
GetWL	Vrátí WL podle požadavku. Pro inkrementy v rámci dne obsahovat všechny inkrementy od WLScopeLastReq do aktuální edice. Určeno pro přímou komunikaci.
GetIncList	Vrátí seznam inkrementů mezi WLScopeLastReq do aktuální edice. Určeno pro nepřímou komunikaci.
GetInc	Vrátí specifický inkrement. Určeno pro nepřímou komunikaci.

GETWL REQUEST

Pole	Popis	Typ	Pozn.
WLLogin	Uživatelské jméno TM/OZ	string	WLLogin podle databáze MOS, buď OZ nebo TM
WLPswrd	Heslo TM/OZ	string	
WLFormatReq	Požadovaný formát WL	byte	0 – obecný MOS formát 1 – formát 1 2 – formát 2 atd. číselník MOS
WLFormatVer	Verze formátu	byte	číselník MOS
WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndirReq	Přímá/nepřímá komunikace	byte	0 – přímá komunikace s OZ 1 – nepřímá komunikace s TM číselník MOS
WLBodyTypeReq	Požadovaný typ obsahu	byte	0 – jízdní doklady 1 – fotografie a další identifikace číselník MOS
WLScopeReq	Požadovaný rozsah WL	byte	0 – plný WL (full refresh) 1 – týdenní inkrement 2 – denní inkrement 3 – inkrement v rámci dne číselník MOS
WLScopeLastReq	Poslední edice WL na TM/OZ	datetime	Nepovinný pro WLScopeReq=0

GETWL RESPONSE

HEADER

Pole	Popis	Typ	Pozn.
WLFileType	Vystavovatel a typ souboru	string	„MOS_WL“
WLFormat	Formát WL	byte	Podle WLFormatReq
WLFormatVer	Verze formátu	byte	Podle WLFormatVer

WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndir	Přímá/nepřímá komunikace	byte	Podle WLDirIndirReq
WLBodyType	Typ obsahu	byte	podle WLBodyTypeReq
WLScope	Rozsah WL	byte	Podle WLScopeReq
WLScopeTimeFrom	Počáteční datum/čas WL	datetime	Pro WLScope=3 počáteční čas WL inkrementu, shodný s WLScopeLastReq
WLScopeTimeTo	Konečný datum/čas edice WL	datetime	

BODYFARE

Jeden záznam pro každý jízdní doklad = možné více záznamů pro identifikátor

Vazba na fotografie (BodyPhoto) přes WLMOSPssngrAcct

Pole	**Popis**	**Typ**	**Pozn.**
WLBodyType	Typ obsahu	byte	0 – jízdní doklady
WLEdition	EdiceWL	datetime	
WLAction	Operace s WL záznamem	char	N – Nový záznam C – Změna záznamu D – Výmaz záznamu číselník MOS
Identifikátor a cestující			
WLMOSPssngrAcct	Číslo interního účtu cestujícího v MOS	string	
WLCardType	Typ identifikátoru	byte	0 – Lítačka 1 – BPK 2 – In Karta ... číselník MOS
WLToken2From	Platnost tokenu 2 nejdříve od	datetime	
WLToken1Ver	Verze tokenizačního algoritmu/klíčů	byte	číselník MOS
WLToken1	Token 1 podle WLToken1Ver	string	
WLToken2Ver	Verze tokenizačního algoritmu/klíčů	byte	číselník MOS
WLToken2	Token 2 podle WLToken1Ver	string	
WLLogicalNum	Logické číslo karty	string	Podle pravidel k WLCardType - BPK poslední čtyři číslice
WLUID	HW číslo karty	string	Podle pravidel k WLCardType
WLCardStatus	Stav identifikátoru	byte	0 – platný 1 – blokovaný držitelem 2 – blokovaný vydavatelem 3 – expirovaný číselník MOS
WLCardExpdate	Datum platnosti identifikátoru	datetime	
WLFormFactor	Forma identifikátoru	byte	0 – plastová karta plné velikosti 1 – plastová karta zmenšené velikosti 2 – náramek, nálepka, wearables 3 – mobilní telefon číselník MOS k verifikaci MC/Visa

WLFareRecs	Počet jízdních dokladů ve WL	int	Pokud 0 (nula), pak další pole irelevantní a záznam WL pouze pro stanovení tarifní kategorie
WLPhotoRecs	Počet fotografií ve WL	int	Pokud 0 (nula), pak identita ověřena jinak
Tarifní kategorie cestujícího			
WLIDS	Tarif – IDS	byte	0 – PID ... později další sousedící kraje číselník MOS
WLTarCathAct	Tarifní kategorie - současná	byte	číselník PID
WLTarCathActFrom	Počátek platnosti tarifní kategorie	datetime	
WLTarCathActExp	Expirace současné tarifní kategorie	datetime	
WLTarCathLast	Tarifní kategorie – minulá	byte	číselník PID
Jízdní doklad			
WLTarItem	Tarifní položka	int	Druh jízdenky číselník PID
WLTicketNo	Číslo jízdního dokladu	string	
WLTicketStatus	Stav jízdního dokladu	byte	0 – platný 1 – blokovaný 2 – expirovaný 3 – převedený číselník MOS, vstup SPP/Tarif PID
WLIDType	Způsob ověření identity	byte	0 – fotografie na kartě WLCardType 1 – žákovský průkaz ... číselník MOS, vstup tarif PID
WLIDLogicalNum	Viditelné číslo průkazu podle WLIDType	string	
WLPssngrNo	Počet cestujících	byte	
WLZones	Zóny pro danou tarifní položku	string	Čísla zón oddělená čárkou, pokud relevantní pro WLTarItem, číselník PID
WLSupZones	Povolené nadzóny nad rámec tarifu	string	Čísla nadzón oddělená čárkou číselník PID
WLStationFromPID	Relační jízdenka – zastávka od PID	int	ID zastávky číselník PID
WLStationFromDPP	Relační jízdenka – zastávka od DPP	int	ID zastávky číselník DPP
WLStationToPID	Relační jízdenka – zastávka do PID	int	ID zastávky číselník PID
WLStationToDPP	Relační jízdenka – zastávka do DPP	int	ID zastávky číselník DPP
WLPurchased	Objemový tarif km/počet	int	Pro budoucí použití: km tarif nebo karnet
WLLeft	Objemový tarif km/počet	int	Pro budoucí použití: km tarif nebo karnet
WLToPWL	Odbavení dokladu do on-line PWL	logical	Pro budoucí použití: aktivace jízdenky přiložením – začátek platnosti
WLValidFrom	Platnost od	datetime	
WLValidTo	Platnost do	datetime	
WLOperator	Omezení na dopravce	string	Čísla povolených dopravců oddělená čárkou číselník PID

WLWeekDays	Povolené dny v týdnu	string	Povolené dny v týdnu, oddělené čárkou, 1-Po, ... 7-Ne

BODY PHOTO

Pole	Popis	Typ	Pozn.
WLBodyType	Typ obsahu	byte	1 – fotografie
WLEdition	EdiceWL	datetime	
WLAction	Operace s WL záznamem	char	N – Nový záznam C – Změna záznamu D – Výmaz záznamu číselník MOS
WLMOSPssngrAcct	Číslo interního účtu cestujícího v MOS	string	
WLCardType	Typ identifikátoru	byte	Definice viz BodyFare
WLToken2From	Platnost tokenu 2 nejdříve od	datetime	
WLToken1Ver	Verze tokenizačního algoritmu/klíčů	byte	Definice viz BodyFare
WLToken1	Token 1 podle WLToken1Ver	string	
WLToken2Ver	Verze tokenizačního algoritmu/klíčů	byte	Definice viz BodyFare
WLToken2	Token 2 podle WLToken1Ver	string	
WLLogicalNum	Logické číslo karty	string	Definice viz BodyFare
WLUID	HW číslo karty	string	Definice viz BodyFare
WLPhoto	Fotografie	jpg	

GETINCLIST REQUEST

Pole	Popis	Typ	Pozn.
WLLogin	Uživatelské jméno TM/OZ	string	WLLogin podle databáze MOS, buď OZ nebo TM
WLPswrd	Heslo TM/OZ	string	
WLFormatReq	Požadovaný formát WL	byte	0 – obecný MOS formát 1 – formát 1 2 – formát 2 atd. číselník MOS
WLFormatVer	Verze formátu	byte	číselník MOS
WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndirReq	Přímá/nepřímá komunikace	byte	0 – přímá komunikace s OZ 1 – nepřímá komunikace s TM číselník MOS
WLBodyTypeReq	Požadovaný typ obsahu	byte	0 – jízdní doklady 1 – fotografie a další identifikace číselník MOS
WLScopeReq	Požadovaný rozsah WL	byte	Pouze 3 – inkrement v rámci dne
WLScopeLastReq	Poslední edice WL na TM/OZ	datetime	

GETINCLIST RESPONSE

Pole	Popis	Typ	Pozn.
WLFileType	Vystavovatel a typ souboru	string	„MOS_WL“

WLFormat	Formát WL	byte	Podle WLFormatReq
WLFormatVer	Verze formátu	byte	Podle WLFormatVer
WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndir	Přímá/nepřímá komunikace	byte	Podle WLDirIndirReq
WLBodyType	Typ obsahu	byte	podle WLBodyTypeReq
WLScopeReq	Požadovaný rozsah WL	byte	Pouze 3 – inkrement v rámci dne
WLScopeTimeFrom	Počáteční datum/čas WL	datetime	Pole WLScopeLastReq
WLScopeIncList	Seznam edicí WL	string	Seznam edicí inkrementů WL od WLScopeLastReq do aktuální

GETINC REQUEST

Pole	Popis	Typ	Pozn.
WLLogin	Uživatelské jméno TM/OZ	string	WLLogin podle databáze MOS, buď OZ nebo TM
WLPswrd	Heslo TM/OZ	string	
WLFormatReq	Požadovaný formát WL	byte	0 – obecný MOS formát 1 – formát 1 2 – formát 2 atd. číselník MOS
WLFormatVer	Verze formátu	byte	číselník MOS
WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndirReq	Přímá/nepřímá komunikace	byte	0 – přímá komunikace s OZ 1 – nepřímá komunikace s TM číselník MOS
WLBodyTypeReq	Požadovaný typ obsahu	byte	0 – jízdní doklady 1 – fotografie a další identifikace číselník MOS
WLScopeReq	Požadovaný rozsah WL	byte	Pouze 3 – inkrement v rámci dne
WLIncReq	Požadovaný inkrement	datetime	

GETINC RESPONSE

HEADER

Pole	Popis	Typ	Pozn.
WLFileType	Vystavovatel a typ souboru	string	„MOS_WL“
WLFormat	Formát WL	byte	Podle WLFormatReq
WLFormatVer	Verze formátu	byte	Podle WLFormatVer
WLTest	Testovací provoz	char	T – testovací provoz
WLDirIndir	Přímá/nepřímá komunikace	byte	Podle WLDirIndirReq
WLBodyType	Typ obsahu	byte	podle WLBodyTypeReq
WLScope	Rozsah WL	byte	Podle WLScopeReq
WLScopeTimeFrom	Požadovaná edice WL	datetime	Shodný s WLIncReq
WLScopeTimeTo	Požadovaná edice WL	datetime	Shodný s WLIncReq

Body záznamy stejné jako u GetWL Response

ODBAVENÍ V OZ, KONTROLNÍ LOG, DIAGNOSTIKA

Komunikace OZ/TM -> MOS

Dávková komunikace, typicky na konci dne či směny.

Nepřímá komunikace: Hlášení podává TM či dopravce.

Přímá komunikace: Hlášení podává vozidlo.

Odbavení v OZ: (PP: Načtení, přiložení): Data o provedených odbaveních, které nevyžadovaly nákup jízdních dokladů, např. při přiložení nosiče s evidovaným kupónem.

- Kontrolní log: Data o provedených přepravních kontrolách průvodčím či revizorem.
- Diagnostika: Poruchy odbavovacích zařízení či dalších systémů dopravce.
- Statistika prodejů: Denní sumarizace prodaných jízdenek.

ZPRÁVY

Zpráva	Popis
SendCD	Zašle odbavovací (check-in) data a diagnostické informace o poruchách

SENDCD

HEADER

Pole	Popis	Typ	Pozn.
CDLogin	Uživatelské jméno TM/OZ	string	Login podle databáze MOS, buď OZ nebo TM
CDPswrd	Heslo TM/OZ	string	
CDFileType	Typ souboru	string	„CD“
CDFormat	Formát CD	byte	0 – obecný MOS formát 1 – formát 1 2 – formát 2 atd. číselník MOS
CDFormatVer	Verze formátu	byte	číselník MOS
CDTest	Testovací provoz	char	T – testovací provoz
CDDirIndirReq	Přímá/nepřímá komunikace	byte	0 – přímá komunikace s OZ 1 – nepřímá komunikace s TM číselník MOS
CDTransOp	ID Dopravce	string	Číselník PID
CDFullTransOp	Plný soubor dopravce?	logical	True – kompletní údaje pro dopravce, nepřímá komunikace
CDDate	Služební den hlášení	datetime	
CDFileNo	Pořadové číslo hlášení v rámci dne	int	Nepřímá komunikace
CDVehicleNo	ID vozidla	char	Přímá komunikace

BODY CHECK-IN DATA

Pole	Popis	Typ	Pozn.
CDBodyType	Typ obsahu	char	„CDC“
CDVehicle	Číslo vozidla	char	Číselník PID

CDTerminal	Číslo terminálu	char	
CDLine	Linka	int	Číselník PID
CDConn	Spoj	int	Číselník PID
CDOperType	Operace	byte	0 – Odbavení ve vozidle 1 – Revizor MHD 2 – Průvodčí železnice 3 – Poskytnutí informace OZ ... číselník MOS
CDOperTime	Čas operace	datetime	vč. vteřin
CDCardType	Typ identifikátoru	byte	0 – Lítačka 1 – BPK 2 – In Karta ... číselník MOS
CDReadStatus	Výsledek načtení identifikátoru	byte	0 – OK 1 – Karta nekomunikuje 2 – Chyba ověření pravosti ... číselník MOS
CDTokenStatus	Výsledek tokenizace identifikátoru	byte	0 – OK 1 – Chyba tokenizace ... číselník MOS
CDToken1Ver	Verze tokenizačního algoritmu/klíčů	byte	číselník MOS
CDToken1	Token 1 podle WLToken1Ver	string	
CDToken2Ver	Verze tokenizačního algoritmu/klíčů	byte	číselník MOS
CDToken2	Token 2 podle WLToken1Ver	string	
CDLogicalNum	Logické číslo karty	string	Podle pravidel k CDCardType - BPK poslední čtyři číslice
CDUID	HW číslo karty	string	Podle pravidel k CDCardType
CDCardExpdate	Přečtená platnost identifikátoru	datetime	
CDFormFactor	Přečtená forma identifikátoru	byte	viz WLFormFactor
CDWLSource	Zdroj informací WL	byte	0 – identifikátor nenalezen 1 – identifikátor nalezen v místním WL 2 – WL na on-line dotaz ... číselník MOS
CDWLNo	Edice místního WL	datetime	
CDOnlWLNo	Číslo on-line dotazu	char	
WLCardStatus	Stav identifikátoru z WL	byte	0 – platný 1 – blokovaný držitelem 2 – blokovaný vydavatelem 3 – expirovaný číselník MOS
WLCardExpdate	Datum platnosti identifikátoru z WL	datetime	
WLFormFactor	Forma identifikátoru z WL	byte	0 – plastová karta plné velikosti 1 – plastová karta zmenšené velikosti 2 – náramek, nálepka, wearables 3 – mobilní telefon číselník MOS k verifikaci MC/Visa
WLIDS	Tarif – IDS	byte	0 – PID ... později další sousedící kraje číselník MOS

WLTarCathAct	Tarifní kategorie z WL	byte	číselník PID
WLTarItem	Tarifní položka	int	Druh jízdenky číselník PID
WLTicketNo	Číslo jízdního dokladu	string	
WLTicketStatus	Stav jízdního dokladu	byte	0 – platný 1 – blokovaný 2 – expirovaný 3 – převedený číselník MOS, vstup SPP/Tarif PID
WLIDType	Způsob ověření identity	byte	0 – fotografie na kartě WLCardType 1 – žákovský průkaz ... číselník MOS, vstup tarif PID
CDOperRes	Výsledek operace	byte	0 – OK 1 – Neúspěšné odbavení 2 – Neúspěšné odbavení, povolen nástup podle pravidla ... číselník MOS
CDOverRule	Pravidlo pro povolení nástupu	byte	číselník MOS
WLPurchased	Objemový tarif km/počet z WL	int	Pro budoucí použití: km tarif nebo karnet
WLLeft	Objemový tarif km/počet z WL	int	Pro budoucí použití: km tarif nebo karnet
CDDeduct	Odpočet objemového tarifu	int	Pro budoucí použití: km tarif nebo karnet
WLToPWL	Odbavení dokladu do on-line PWL	logical	Pro budoucí použití: aktivace jízdenky přiložením – začátek platnosti

BODY DIAGNOSTICS DATA

Záznam se použije pro hlášení o výpadku (CDTermStatus > 0) nebo jako hlášení o provozovaném zařízení ve vozidle dopravce (CDTermStatus = 0).

Pole	**Popis**	**Typ**	**Pozn.**
CDBodyType	Typ obsahu	char	„CDD“
CDVehicle	Číslo vozidla	char	Číselník PID
CDTerminal	Evidenční číslo terminálu	char	
CDLine	Linka	int	Číselník PID
CDConn	Spoj	int	Číselník PID
CDTermStatus	Stav zařízení	byte	0 – OK. Další datová pole neobsahují hlášení o výpadku, záznam slouží pro evidenci terminálu do MOS či hlášení přístupu do úložiště OZ 1 – Následují data o výpadku ... číselník MOS
CDFailType	Rozsah výpadku	byte	0 – TM Dopravce 1 – Vozidlo 2 – Terminál 3 – Funkce terminálu ... číselník MOS

CDFailStart	Čas zahájení výpadku	datetime	vč. vteřin
CDFailEnd	Čas ukončení výpadku	datetime	vč. vteřin
CDFailIdent	Čas zaznamenání výpadku	datetime	vč. vteřin
CDFailCardType	Typ neakceptovaného identifikátoru	byte	0 – Lítačka 1 – BPK 2 – In Karta ... číselník MOS
CDFailComp	Selhání komponenty	byte	0 – Datová komunikace 1 – Čtečka dopravních karet 2 – Čtečka bankovních karet 3 – Čtečka 2D kódů 4 – Tiskárna 5 – SAM modul ... číselník MOS
CDReposDate	Přístup na úložiště OZ	datetime	
CDReposOper	Typ přístupu na úložiště OZ	char	0 – nevyjmenovaná operace 1 – zahájení provozu – otevření 2 – uzávěrka ... číselník MOS
CDReposUser	Identifikace uživatele	string	

BODY SALES DATA

Datový formát bude obsahovat položky prodaných jízdenek pro každé zařízení a druh jízdenky zvlášť. Data budou kombinace výše uvedených datových polí pro jízdenky (WL) a doplněna na o datová pole Jednotného datového formátu pro výstupy z odbavovacích zařízení (CHAPS).

PŘÍMÁ ON-LINE KOMUNIKACE ODBAVOVACÍHO ZAŘÍZENÍ S MOS

ZÁZNAM WL

Request bude obdobný GetWL Request, bude dále obsahovat token, na který je dotazováno.

Response bude shodný s GetWL Response. Odpovědi budou číslovány MOSem, to pak bude použito do SendCD: CDOnlWLNo.

ON-LINE HLÁŠENÍ O CHYBÁCH ZPRACOVÁNÍ WL

Závažné chyby zpracování WL bude zařízení hlásit v on-line režimu, aby případná chyba WL byla identifikována co nejdříve nebo aby bylo možné řešit odbavení v konkrétním vozidle.

Soubor bude obdobný diagnostice z SendCD (Body diagnostics data), bude doplněn číselník možných chyb zpracování WL.

FORMÁT PWL – INFORMACE O PRODEJÍCH A PODOBNÉ

PWL bude obsahovat data z Body Sales data souboru SendCD tj. kombinaci WL a JDF pro výstupy odbavovacích zařízení. Hlášeny budou prodané jízdenky vázané k identifikátorům a dále odbavené jízdenky s příznakem WLToPWL.