

Příloha č.1 – STANDARDY ODBAVENÍ

MOS – POŽADAVKY NA ODBAVOVACÍ ZAŘÍZENÍ

Verze: 2.3

ropid



idsk

1 Obsah

2	<i>Historie verzí</i>	3
3	<i>Shrnutí dokumentu</i>	4
4	<i>Odbavení pomocí přenosu souborů whitelist</i>	4
4.1	Přímá komunikace odbavovacího zařízení se systémem MOS	4
4.2	Nepřímá (Terminal management server) komunikace odbavovacích zařízení s MOS	6
4.3	Princip komunikace/přístupu k odbavovacím datům pro přímou i nepřímou komunikaci	6
4.4	Online komunikace odbavovacího zařízení s MOS.....	7
5	<i>Odbavovací zařízení – technické vymezení, procesy.....</i>	7
6	<i>Souběžné procesy související s odbavením.....</i>	9
6.1	Komunikace správců odbavovacích zařízení vůči MOS	9
6.2	Tokenizace v odbavovacích zařízeních a práce s identifikátory.....	10
7	<i>Odbavení pomocí mobilní aplikace.....</i>	11
7.1	Technické parametry	11
8	<i>Seznam příloh</i>	12
8.1	Příloha č.1 – Struktura whitelist.....	12
8.2	Příloha č.2 – datová věta cards Exchange	12
8.3	Příloha č.3 – procesy odbavení	12
8.4	Příloha č.4 – technická dokumentace mobilní aplikace PID Lítačka.....	12
8.5	Příloha č.5 – dokumentace SAM modul.....	12

2 Historie verzí

Verze	Datum	Autor	Popis změn
2.3	22.4.2022	Michal Beránek, OICT	Konsolidace původního dokumentu verze 2.2 na základě připomínek ROPID, nové formátování

3 Shrnutí dokumentu

Níže uvedené specifikace jsou stanoveny Operátorem ICT, a.s. (dále OICT) jakožto provozovatelem systému MOS (multikanálový odbavovací systém) a bezpečnostním garantem EOC realizovaným prostřednictvím MOS. Dokument je nedílnou součástí Standardů odbavení, které jsou vydávány organizátory veřejné dopravy ROPID a IDSK, a je závazný pro správce odbavovacích zařízení, nebude-li určeno jinak.

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.

4 Odbavení pomocí přenosu souborů whitelist

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 (TMS) správců odbavovacích zařízení. Informace pro odbavení časových jízdenek jsou obsaženy v tzv. whitelitech (WL – seznam jízdních dokladů vázaných k identifikátoru). Níže jsou uvedena možná řešení odbavení při využití kontrol přes WHITELIST. Požadavkem je využití tohoto způsobu odbavení pro regionální a příměstskou autobusovou dopravu, železniční dopravu a revizorské kontroly v celém prostředí PID.

4.1 Přímá komunikace odbavovacího zařízení se systémem 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.
 - Komunikace probíhá přes šifrovaný protokol, aby nedošlo k odchycení a následně k jejich zneužití
- Formát dat WL a dalších je definován provozovatelem MOS:
 - Formát TLV
 - Bližší popis jak struktury souboru, tak souboru samotného poskytuje dokumentace struktury whitelist ve své aktuální platné verzi. Viz. příloha č.1 tohoto dokumentu.

- Uložení stažených dat z MOS na koncové zařízení musí splňovat následující parametry:
 - Data jsou uložena na koncovém zařízení v chráněném repository, do něž je přístup zajištěn autentizací v rámci zařízení – zajištění odbavovacích dat MOS proti přímému přístupu uživatele.
 - Klíč pro šifrování fotografií z WL je v nevolatilní paměti uložen některým z následujících způsobů:
 - v SAM (preferovaná varianta)
 - ve PCI-DSS certifikovaném zařízení
 - v interním nebo externím HW modulu s bezpečnostními funkcemi

Výkonnostní požadavky

- Časové požadavky na odbavení bankovních platebních karet jsou dány pravidly karetních společností a musí být dodrženy
- Aktuální provozní velikost absolutního whitelist pro PID se pohybuje kolem 700 MB. Absolutní whitelist může v průběhu životního cyklu systému nabývat a odbavovací zařízení musí mít kapacitu na příjem a práci s absolutním WL o velikosti až 2 GB. Předpokladem je, že nahrání WL je realizováno při nastavení koncových zařízení.
- Odbavovací zařízení a celý systém odbavení je schopen přehrání nového absolutního WL, a to na vyžádání bez dalších provozních či implementačních vícenákladů. Tato operace bude prováděna primárně vzdáleně bez nutnosti ručního fyzického zásahu.
- Aktualizace WL a dalších dat jsou realizovány ve formě inkrementálních dat, kdy koncové zařízení v pravidelné periodě kontroluje nový inkrement na repository MOS, stahuje jej a automatizovaným procesem změny zpracovává
 - Kvalifikovaný odhad běžného inkrementu v periodě 15 min je v rozsahu 1 kB – 1 500 kB. Běžná střední hodnota 15 min WL je cca 40 kB.
 - Základní četnost aktualizace WL je v periodě 15 min
 - Rozdílové inkrementy po jejich zpracování 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 (24 h) využije tento konsolidovaný inkrement. Konsolidované inkrementy jsou k dispozici hodinové a denní.
 - WL přírůstky jsou k dispozici až 14 dní zpětně. Pokud má odbavovací zařízení lokální whitelist starší než 14 dní, je zapotřebí stáhnout absolutní whitelist.
 - Na základě dosavadních zkušeností doporučujeme/vyžadujeme možnost stažení absolutního whitelistu pověřenou osobou na vyžádání – wifi, SIM

4.2 Nepřímá (Terminal management server) komunikace odbavovacích 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).

4.3 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 ucelenost a správnost poskytovaných dat
- MOS vystavuje data prostřednictvím webové služby ve formě publikovaných souborů umožňujících jejich stažení pro autorizované klienty (TMS, odbavovací zařízení)
- Ověření klientů je oproti MOS autentizačnímu řešení

Princip 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 navracena informace o úspěšném stažení
- 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.

4.4 Online komunikace odbavovacího zařízení s MOS

- Mobilní datová síť nebo v dopravcem definovaných oblastech pomocí WIFI
- Pro on-line komunikaci je v rámci implementace MOS vydefinováno komunikační API mezi koncovými zařízeními a MOS prostředím
- Přímá on-line komunikace koncových zařízení do MOS je přímým přístupem přes webovou službu MOS do "živého" prostředí k on-line datům.
- Mimo standardního odbavení za pomoci dat uložených offline na WL v zařízení, umožní zařízení vyvolání online dotazu na daný konkrétní identifikátor cestujícího. Webová služba MOS data navrátí ve stejné struktuře jako standardní inkrement WL, ale o velikosti pouze 1 záznamu. Blíže příloha č.1.

5 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 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.

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 zpracován do WL (proběhne aktualizace záznamů v WL, jež jsou součástí inkrementu)
- Pokud je proces zpracování úspěšný je zvýšena verze WL. Číslo verze aktuálního WL je obsluze snadno zobrazitelné v menu zařízení včetně času a data stažení.
- Jestli je zpracování neúspěšné jsou rozběhnuty opravné mechanismy. Pokus o stažení a načtení inkrementů opakovaně.
- Aktualizace a zpracování inkrementu nesmí zásadním způsobem ovlivňovat chod koncového zařízení (zpomalení apod.) Akceptovatelné zpomalení standardní odbavovací funkcionality je v řádu 50 % oproti standardnímu času trvání těchto funkcionalit. V případě právě probíhajícího zpracování inkrementu, je nutné, aby zařízení disponovalo možností upozornění na tuto skutečnost nebo aby obsluha mohla informaci o stavu zpracování jednoduše dohledat v rámci administrace zařízení.

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**
 - Odbavovací zařízení synchronizují a udržují přesný čas dle GNSS.

6 Souběžné procesy související s odbavením

6.1 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 Správcí 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. Tento seznam aktualizuje a dává na vědomí neprodleně po zařazení či vyřazení odbavovacího zařízení.
 - 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 předávána ve formě definované datové věty Cards Exchange. Její popis je součástí přílohy č.2.

6.2 Tokenizace v odbavovacích 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 a vyšší verze kromě verze 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:
 - v SAM
 - ve PCI-DSS certifikovaném zařízení
 - v interním nebo externím HW modulu s bezpečnostními funkcemi

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/algorithmů 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 prostřednictvím otevření zabezpečeného úložiště (nebo jeho části) za pomoci čtecích klíčů uložených na SAM. Zároveň umožní i možnou budoucí implementaci ověření ostatních partnerských karet v režimu challenge-response.

Správce TMS obdrží stanoveným klíčovacím ceremoniálem od provozovatele systému MOS nové klíče a algoritmy pro tokenizaci dle schématu životnosti párů algoritmus/klíč MOS. Výchozí hodnota je obnova páru algoritmus/klíč každé 3 roky, nestanovili provozovatel systému jinak.

Bližší práci s identifikátory a celkové procesy odbavení popisuje dokument v příloze č.3 ve své aktuální verzi.

7 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. Strojové načtení 2D kódu
2. NFC
3. Vizuální kontrola pomocí porovnání RVI prvku (nepovinné)

Odbavovací zařízení musí zajistit kompatibilitu odbavení přes NFC i v momentě kdy v telefonu, který je využíván jako identifikátor či nese jednorázovou jízdenku, je aktivní emulovaná platební karta, tedy telefon vysílá obě tyto věci zároveň. Odbavovací zařízení musí správně vyhodnotit, zda je v režimu platby a případně využít emulovanou kartu v mobilním telefonu pro platbu za jízdenku, či je v režimu odbavení identifikátoru nebo jízdenky, a tedy korektně načíst NFC vysílání mobilní aplikace.

7.1 Technické parametry

Bližší informace o způsobu kontroly mobilní aplikace popisuje technická dokumentace v příloze č.4

8 Seznam příloh

8.1 Příloha č.1 – Struktura whitelist

Poskytnutí pouze na základě uzavření NDA.

8.2 Příloha č.2 – datová věta cards Exchange

Poskytnutí pouze na základě uzavření NDA.

8.3 Příloha č.3 – procesy odbavení

Poskytnutí pouze na základě uzavření NDA.

8.4 Příloha č.4 – technická dokumentace mobilní aplikace PID Lítačka

Poskytnutí pouze na základě uzavření NDA.

8.5 Příloha č.5 – dokumentace SAM modul

Poskytnutí pouze na základě uzavření NDA.