TECHNICKÁ SPECIFIKACE – VALIDAČNÍ ZAŘÍZENÍ PVP

SHRNUTÍ

Předmětem poptávky je závazek Dodavatele zhotovit a předat do užívání Objednateli až 100 ks validačních zařízení (sestavy) a to dle konkrétního požadavku objednatele. Každé zařízení (sestava) se skládá z mobilního zařízení definovaných parametrů a z instalované funkční aplikace pro provádění operací spojených s validací slevového balíčku PVP či jiných dalších dat dostupných pro validaci či odbavení.

HW POŽADAVKY, NEFUNKČNÍ POŽADAVKY

Minimální požadavky na hardware a výkonnost mobilní telefonu jsou následující.

Základní parametry

Úhlopříčka displeje	6“
Rozlišení displeje	2220x1080
Operační systém	Android 8.0 OREO a vyšší
Operační paměť	3 GB
Vnitřní paměť	32 GB
Slot na paměťové karty	ANO
Typ paměťové karty	Micro SDXC
Počet jader CPU	8x
Kapacita baterie	3 500 mAh
Konektory	USB C nebo USB micro

Fotoaparát

Rozlišení zadní kamery	16 Mpx

Funkce

Dotykový displej	ANO
Zaostřování kamer	Automatické
Přisvětlovací dioda	ANO

Konfigurace karet

Dual SIM + karta (SIM nebo nano SIM)	ANO

Datové služby

Bezdrátové technologie	LTE(4G), HSPA (3.5G), UMTS/CDMA (3G), EDGE (2.5G), GPRS (2G)
Frekvence LTE	800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2600 MHz

Další požadavky:

Zařízení bude certifikováno výrobcem na EMV level 1, přičemž zařízení musí umět bezpečně pracovat s kryptografickými klíči. Samotný operační systém Android tuto funkci nepodporuje. Dodavatel musí dále prokázat existenci a funkční implementaci nadřazených bezpečnostních vrstev, které tuto práci s klíči zajistí, a to včetně bezpečného uložení klíčů.

SYSTÉM VALIDACE

Proces validace je založen na on-line databázovém řešení, s distribucí informací nutných pro odbavení zákazníků přímo do odbavovacích zařízení umístěných na koncových místech. Informace pro odbavení budou obsaženy v tzv. whitelistech (WL – seznam produktů vázaných k identifikátoru). Formát whitelist je definován zadavatelem a jeho kompletní popis bude předán dodavateli. Jedná se o strukturovaný formát TLV. Další možností je odbavení přímým dotazem validačního zařízení na webovou službu zadavatele. Tzv. Online dotaz.

Zařízení umožní odbavení oběma dvěma způsoby s možností nastavení primárního způsobu. Tedy jestli po přiložení identifikátoru dojde k vyčtení potřebných informací z lokálně uloženého whitelist či dotazem na webovou službu zadavatele.

VALIDACE POMOCÍ WHITELIST

Validační zařízení umožní

- pravidelné dotazování a stahování nových přírůstků datových souborů whitelist z repository MOS (síťově vystavené úložiště).
- Stahování dat bude iniciované validačním zařízením v definované periodě či vynucené uživatelem koncového zařízení mimo standardní periodu.
- Data jsou zasílána v šifrované podobě, aby nedošlo k jejich odchycení a následně k jejich zneužití
- Formát dat WL a dalších je definován zadavatelem. Viz. část dokumentu Struktura whitelist
- 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

- Výkonnostní požadavky
    - Časové požadavky na odbavení karet jsou dány pravidly karetních společností a musí být dodrženy
    - Iniciální velikost WL bude cca. 50 MB 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 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 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 (24 h) využije tento konsolidovaný inkrement. Konsolidované inkrementy jsou k dispozici hodinové a denní.

Princip komunikace

- Validační zařízení volá přes své rozhraní webovou službu systému zadavatele. V rámci volání je systém dotazován, zdali není publikována aktuálnější verze validačních dat (WL), než je verze umístěná ve validačním zařízení.

- Pokud data v systému zadavatele **nejsou** novější než data ve validačním zařízení, komunikace je ukončena a záznam o komunikaci je uložen do logu validačního zařízení.
- Pokud data v systému zadavatele jsou **novějšího** typu, je zpětně informováno validační zařízení o tomto stavu.
  - Následně validační zařízení iniciuje požadavek na stažení těchto dat
  - Po stažení dat je navrácena informace o úspěšném stažení
  - Následně jsou validační data dešifrována a rozdílové soubory zapracovány do validačního zařízení

- Pokud v rámci komunikace s validačním zařízením dojde k selhání ověření verze validačních dat či přerušení komunikace nebo chybnému stažení, je následně komunikace opakovaně navazována co nejdříve po obnovení datového připojení.

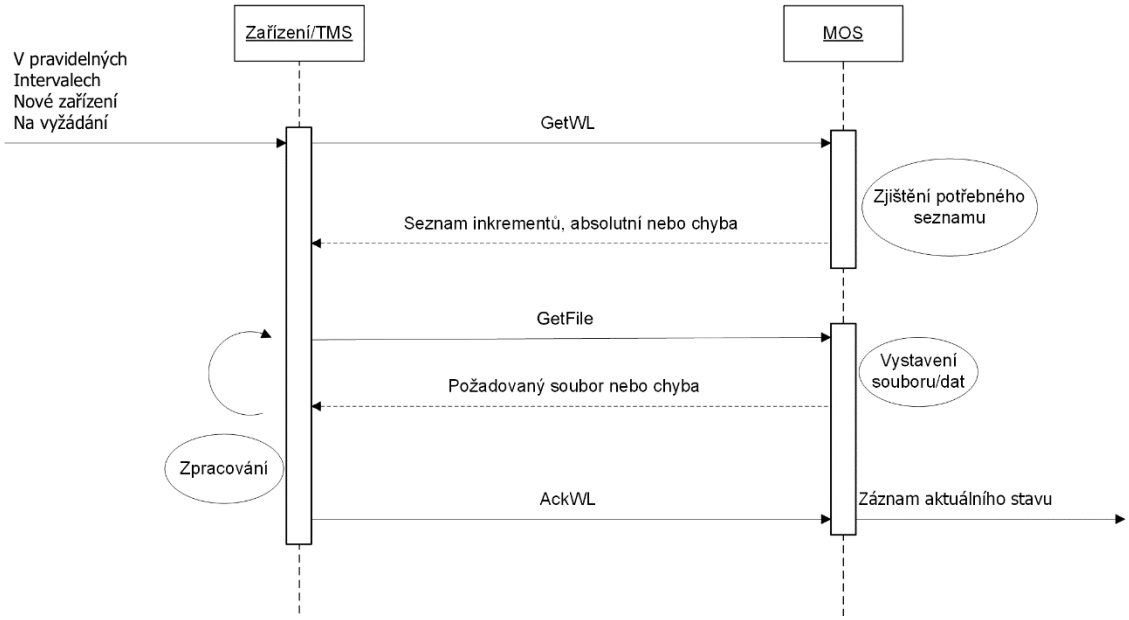
Proces uložení a zpracování

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

Následuje proces, který zajistí data pro zpracování:

- Aktualizace (inkrement) – je aplikačně načtena na straně validačního 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. Pokus o stažení a načtení inkrementů opakovaně.
- Aktualizace a zpracování inkrementu nesmí zásadním způsobem ovlivňovat chod validačního zařízení (zpomalení apod.) Akceptovatelné zpomalení standardní validační 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.

SCHÉMA KOMUNIKACE A AKTUALIZACE WHITELIST



STRUKTURA WHITELISTU

X – Povinná položka

0 – Povinná položka s hodnotou 0

- - Položka není součástí daného typu whitelistu

Úroveň vnoření struktury 1 2 3	Data	Datový typ	WL		Popis
			Absolutní	Delta	
Header					hlavička souboru se základními informacemi
	WLVer	Byte	X	X	Verze whitelistu
	WLFormatVer	Byte	X	X	Formát whitelistu dle číselníku
	Seq	Int	X	X	Pořadové číslo whitelistu
	SeqPrev	Int	0	X	Číslo whitelistu, ke kterému se vztahuje tato delta
	Typ	Int	X	X	Typ Whitelistu podle zařízení pro budoucí rozvoj (0=defaultní)
	WLScopeTimeTo	DateTime	X	X	Datum a čas generování
	WLTokenVer	Byte	X	X	Číslo algoritmu tokenizace
	WLTest	Char	X	X	Zda se jedná o testovací data
	SigNo	Byte	X	X	Číslo verze podpisu (1 – CRC)
Identifiers					Data o nosičích
Added					Data, která přibývají oproti předchozímu whitelistu (data v absolutním WL)
	VLMOSIdentId	Int	X	X	Jedinečný identifikátor identifikátoru
	WLToken1	Byte[32]	X	X	Token nosiče pro zařízení možná délka jenom 16 Byte
	WLToken1Ver	Byte	-	-	číslo algoritmu tokenu
	WLCardType	Byte	X	X	typ nosiče dle číselníku MOS 0 – Turistická karta 1 – Čipový náramek MiFare DesFire 2 - BPK
	WLCardStatus	Byte	X	X	Status identifikátoru
	WLCardExpdate	DateTime	X	X	Datum expirace identifikátoru
	WLToken2	Byte[32]	-	-	Token 2 nosiče pro zařízení možná délka jenom 16 Byte
	WLToken2Ver	Byte	-	-	číslo algoritmu tokenu 2

Úroveň vnoření struktury	Data	Datový typ	WL		Popis
1 2 3			Absolutní	Delta	
Changed					Měněné záznamy (absolutní WL tuto sekci neobsahuje)
	jako Added				Stejné položky jako u záznamu Added
Deleted					Data, která se mají smazat (absolutní WL tuto sekci neobsahuje)
	VLMOSIdentId	Int	X	X	Jedinečný identifikátor identifikátoru
Contracts					
Added					Data, která přibývají oproti předchozímu whitelistu (data v absolutním WL)
	ConId	Int	X	X	jedinečný identifikátor kontraktu
	ELIdentId	Int	X	X	Vazba na identifikátor
	WLValidFrom	DateTime	X	X	Platnost Od, datum a čas
	WLValidTo	DateTime	X	X	Platnost Do – NULL platí neomezeně, datum a čas
	Data	Struktura	X	X	Data kontraktu dle typu
Changed					Měněné záznamy (absolutní WL tuto sekci neobsahuje)
	jako Added				Stejné položky jako u záznamu Added
Deleted					Data, která se mají smazat (absolutní WL tuto sekci neobsahuje)
	ConId	Int	-	X	jedinečný identifikátor kontraktu
Footer					patička souboru
	Sig	byte[n]	X	X	Podpis, n dle verze podpisu

STRUKTURA KONTRAKTU

Typ kontraktu	Popis	Položky	Datový typ	Popis	Pozn
1	Slevový balíček	DT	Byte	Discount type dle definovaného číselníku OKUL/PIS	
		DA	Byte	Discount amount – v procentech	Není povinné
		WLZones	String	názvy míst, pro které slevový balíček platí, názvy míst (čísla, případně písmena) oddělaná středníkem. Dle definovaného čísleníku	Není povinné, A – all, nevyplněno platí all
		NetworkID	Int	číslo sítě, pro který balíček platí dle číselníku.	0 - Prague
		IDType	Byte	Způsob ověření - žákovský průkaz ISIC. Dle číselníku	není povinné

TECHNICKÉ VYMEZENÍ, PŘEDPOKLADY

Zásadní předpoklady zajišťující funkční proces validace

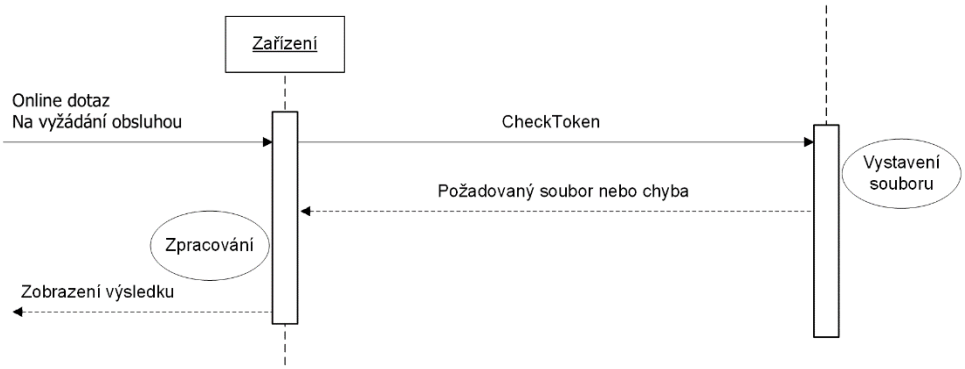
- Systém zadavatele vystavuje datové soubory s inkrementy dle výše uvedené definice v pravidelných intervalech a zajišťuje neustálou dostupnost těchto dat pro jejich následné stažení
- Systém zadavatele garantuje integritu a správnost poskytovaných dat
- Systém zadavatele vystavuje data na webové službě systému zadavatele ve formě publikovaných souborů umožňujících jejich stažení pro autorizované validační zařízení
- Ověření uživatele validačních zařízení je oproti autentizačnímu řešení zadavatele
- Synchronizace času
    - Validační zařízení synchronizují a udržují přesný čas dle GNSS.

VALIDACE POMOCÍ PŘÍMÝCH ONLINE DOTAZŮ

ON-LINE KOMUNIKACE ODBAVOVACÍHO ZAŘÍZENÍ S MOS

- Pro on-line komunikaci je v rámci systému zadavatele vydefinováno komunikační API mezi validačními zařízeními a systémovým prostředím
- Přímá on-line komunikace validačních zařízení do systému zadavatele je přímým přístupem přes webovou službu systému do "živého" prostředí k on-line datům.
- Mimo validace za pomocí dat uložených offline na WL v zařízení, umožní zařízení vyvolání online dotazu na daný konkrétní načtený identifikátor klienta nebo je validační zařízení do tohoto režimu přepnuto defaultně a online dotaz na systém zadavatele provádí automaticky po načtení identifikátoru.
- Webová služba MOS data navrátí ve stejné struktuře jako standardní inkrement WL, ale o velikosti pouze 1 záznamu. Viz struktura whitelist.

SCHÉMA ZÍSKÁNÍ VALIDAČNÍCH DAT ZA POMOCÍ ONLINE DOTAZU



SOUBĚŽNÉ PROCESY SOUVISEJÍCÍ S ODBAVENÍM

TOKENIZACE A PRÁCE S IDENTIFIKÁTORY

- Validační zařízení umožní načtení identifikátoru a vypočítání tokenu (tokenizace) na základě vyčtených vstupních dat z daného identifikátoru. Tento token následně vstupuje do procesu získání validačních dat přes metodu whitelist či přímým online dotazem do systému zadavatele.
- Zadavatel požaduje podporu čipových karet či wearables MiFare DesFire EV1 a možnost opticky načítat QR kód.
- Dále musí plně implementovat ISO/IEC 14443 tak aby v budoucnu byla možná podpora i dalších typů nosičů.
- Validační zařízení budou podporovat ověření pravosti a jedinečnosti vybraných identifikátorů prostřednictví otevření zabezpečeného úložiště (nebo jeho části) za pomoci čtecích klíčů uložených v certifikované chráněné části validačního zařízení.
- Dodavatel obdrží stanoveným klíčovacím ceremoniálem od zadavatele klíče a algoritmy pro tokenizaci.
- Klíčovací ceremoniál bude detailně popsán až po podpisu smlouvy s dodavatelem.

SCÉNÁŘ VALIDAČNÍHO PROCESU

Odbavení identifikátoru, včetně definice rychlosti, ke kterému může být vázán slevový balíček či jiná data vstupující do validace, včetně následujících operací s identifikátorem:

1. Načtení veřejné části karty s údajem o typu karty a UID
2. Ověření identity karty a autentizace (v případě Mifare)
3. Vytvoření tokenu z ID/CLN/PAN nosiče dle definovaných postupů
4. Vyhledání tokenu na whitelistu či provedení přímého online dotaz na daný token
5. Přehledné a jasné zobrazení získaných dat kontraktu přiřazeného k danému identifikátoru. Kontrakt, tedy zejména slevový balíček, bude jasně barevně odlišen dle časové, místní a stavové platnosti. (blokovaný, neblokovaný, využití na daném místě apod.)

Celý proces nesmí trvat déle než 4 s. Střední doba pro odbavení (výše uvedené operace) je stanovena na 2,5 s.

Validační zařízení musí být schopno a způsobem implementace připraveno na případné provolání externího API pokladního systému prodejce v později definované struktuře. Tedy pokud se při validačním procesu ukáže, že daný identifikátor má přiřazen platný kontrakt – slevový balíček, provolá externí API a dojde k vytištění vstupenky a evidenci v systému kontaktního místa.

LOGOVÁNÍ

Validační zařízení loguje veškeré operace včetně komunikace se systémem zadavatele, a to nejméně v následujícím rozsahu:

- Záznam o kontrole konkrétního tokenu (WL i online dotaz)
    - Datum, čas
    - GPS poloha
    - Výsledek operace
- Záznamy o stahování, dotazování webové služby pro stažení WL
    - Datum, čas
    - Výsledek
- Uchovává průběžnou historii verzí WL