Příloha č. 1

Technická specifikace

(Příloha č. 5 Zadávací dokumentace bude přiložena k této Smlouvě při podpisu)

OPERÁTOR ICT

Příloha Zadávací Dokumentace

Obsah:

1 Seznam zkratek

MOS	Multikanálový odbavovací systém
DOS	Dopravní odbavovací systém – stávající systém prodeje elektronických jízdních dokladů na území PID, provozovaný DPP
PDOS	Dopravní odbavovací systém DPP, který DPP plánuje zavést jako náhradu DOS v termínu, který bude předcházet spuštění MOS.
DPP	Dopravní podnik Hlavního města Prahy
MC	MasterCard
BPK	Bezkontaktní platební karta vydaná s obchodními značkami MasterCard či Visa
DB	Databáze
HSM	Hardware security module
API	Application Interface (programové rozhraní)
UID	Hardware číslo BČK přiřazené výrobcem karty
CLN	Logické číslo BČK přiřazené vydavatelem karty a viditelné pro držitele
BČK	Bezkontaktní čipová karty používaná v dopravě, nejčastěji Mifare technologie

2 Obecný popis tokenizace

2.1 Výklad pojmů

Identifikátor

Obecný pojem pro kartu, přívěšek či jiný předmět sloužící cestujícímu pro odbavení ve veřejné dopravě.

Lítačka

Souhrnné označení pro stávající provozovatelské karty jak Lítačka, tak Opencard.

Provozovatelská karta

Nosič ve formě bezkontaktní čipové karty, přívěšku či jiné nositelné elektroniky či mobilní aplikace, který je vydán provozovatelem. Grafická podoba karty a její elektronické prvky jsou pod kontrolou provozovatele a může být využita k odbavení. Příkladem stávající provozovatelské karty je např. Lítačka.

Partnerská karta

Nosič ve formě bezkontaktní čipové karty, přívěšku či jiné nositelné elektroniky či mobilní aplikace, který je vydán a provozován externím subjektem mimo kontrolu provozovatele a akceptován v EOC na základě partnerské smlouvy o akceptaci. Grafická podoba může být využita k odbavení zcela nebo částečně, a to případ od případu, např. pro kontrolu fotografie držitele. Zvláštním případem partnerských karet jsou BPK.

Token

Zástupné číslo identifikátoru. Zatímco číslo identifikátoru (např. PAN pro BPK) může být citlivým platebním údajem, token není citlivou informací a jeho vyzrazení nemůže způsobit finanční či jinou újmu

Tokenizace

Proces, během kterého je z citlivého platebního údaje vypočten Token.

Tokenizační autorita

Určuje tokenizační algoritmus či algoritmy, stanovuje a distribuuje případné utajené kryptografické údaje, např. klíče či hesla. Role autority nezahrnuje faktické vykonávání tokenizace.

Tokenizační klíče

Vstupní údaje tokenizačního výpočtu. Souhrnný pojem pro klíče symetrických algoritmů, privátních či veřejných klíčů nesymetrické kryptografie nebo salt (sůl) pro hashovací funkce.

Tokenizační procesor

Systém či společnost, který fakticky provádí tokenizaci s využitím tokenizačního algoritmu a tokenizačních klíčů, které určila Tokenizační autorita. Protože Tokenizační procesor zpracovává citlivou hodnou (např. PAN), bude muset být pro tuto činnost dostatečně certifikován podle PCI DSS požadavků. Výkon činnosti Tokenizačního procesora je předmětem této veřejné zakázky.

Typ karty nebo typ identifikátoru

Určuje vydávající portfolio vydaného identifikátoru. Typem identifikátoru tedy není Mifare dopravní karta, ale konkrétní aplikace Mifare karet např. Lítačka, Plzeňská karta apod.

2.2 Tokenizační algoritmus

Jako základní variantu tokenizačního algoritmu navrhujeme použít:

Token=SHA256(Key||Data)[0...15],

tedy tokenizační klíč se zřetězí s daty, zahashuje pomocí SHA256 a výsledný token se omezí na prvních 16 bytů. Tokenizační klíč bude mít délku 128 bitů (16 bytů).

Tato varianta byla zvolena z důvodu široké podpory SHA256. Obavy o využití Length-Extension Attacku nejsou na místě, jelikož se výsledek omezuje pouze na 16 bytů. Na druhou stranu, 16 bytů je naprosto dostačující k zabránění kolizí, navíc sníží nepatrně velikost přenášených a vyhledávaných dat.

O klíč též není potřeba se obávat: přestože hashovací funkce nemá z definice vlastnost skrývání obsah vstupu, konkrétně SHA256 k tomuto účelu využít lze, podobné využití totiž nalézá např. při použití v HMAC.

2.3 Vstupní data

Data vstupující do tokenizace budou v případě použití s platebními kartami kódovat Primary Account Number (PAN) a platnost karty. V případě dalších nebankovních partnerských karet to bude namísto PAN tokenizováno UID, CLN nebo obdobný identifikátor karty (toto bude určeno až při zapojení jednotlivých partnerských nosičů do systému).

Z možných variant zakódování PANu a platnosti se zvolí ta, která nevyžaduje žádné nebo minimální přeformátování dat získaných přímo ze čtečky, přičemž zakódování PANu a platnosti se zřetězí. Takto formátovaná data budeme dále nazývat jen platební data.

V případě platebních dat je délka i formát daný, v případě využití tokenizačního algoritmu s jinými kartami se opět zvolí formát s ohledem na data získaná ze čtečky, aby nebylo nutné přeformátovávat.

Ke vstupním datům se váže jedno doporučení: délku vstupu do SHA256 je vhodné omezit na 55 bytů včetně, aby se počítal jediný blok, kvůli zřetězení s tokenizačním klíčem dostáváme doporučený limit délky vstupních dat 39 bytů.

2.4 Tokenizační proces

Tokenizační proces je souhrn činností, během kterého je z citlivého platebního údaje vypočten Token. Tokenizační proces bude mít odlišný průběh podle místa tokenizace a může mít odlišný průběh pro různé typy identifikátorů.

Tokenizační proces při přiložení identifikátoru

Tokenizační proces začne v případě platební karty ověřením její autenticity. V případě jiného typu karty se provede ekvivalentní postup (preferujeme princip challenge-response, pokud to daný typ karty podporuje). Celý tokenizační proces bude probíhat v zabezpečeném prostředí – nebude možné oddělit tokenizační funkcionalitu od autentizace karty. Pokud by se dala autentizace karty jakkoliv obejít, bylo by možné zneužít tokenizační jednotku jako orákulum a provést slovníkový útok. Použitý hardware/firmware/software bude schopen takovému útoku čelit využitím příslušných opatření.

Tokenizační procesor zajistí bezpečné provedení procesu tokenizace v registračních terminálech, které jsou součástí plnění Tokenizačního procesora.

Proces tokenizace v odbavovacích zařízeních a revizorských čtečkách bude garantovat příslušný provozovatel na základě smlouvy s organizátory veřejné dopravy.

Tokenizační proces při použití identifikátoru na e-shopu

E-shop MOS, e-shop dopravce či mobilní aplikace předá pro provedení registrace nového identifikátoru kontrolu Tokenizačnímu procesorovi, který zobrazí formulář pro bezpečné zadání údajů o identifikátoru. Po provedené tokenizaci vrátí Tokenizační procesor e-shopu/mobilní aplikaci vedle informace o úspěšné registraci spolu s dalšími údaji popsanými v této Příloze a předá kontrolu nad registrací/nákupem zpět do e-shopu či mobilní aplikace, která registraci vyvolala.

2.5 Příklad

Testovací vektory v hexadecimálním zápisu

Tokenizační klíč	Data	Token
0000000000000000 0000000000000000	0000000000000000	9D908ECFB6B256DE F8B49A7C504E6C88
CAFEBABEDEADBEEF F00DBADA55BADA55	5465737420646174612E0A (v ACSII „Test data.“)	8C1F55E05DB1E61A 0E8BB841CE28BA2A

2.6 Alternativní tokenizační algoritmus

Do budoucna je třeba počítat i s variantou, že bude potřeba aktualizovat tokenizační algoritmus (např. pokud by byla kompromitována SHA2, viz nedávný případ SHA1, i když se to dnes jeví jako krajně nepravděpodobné). Pro takový případ navrhujeme ještě jeden algoritmus založený na nedávno představené SHA3:

Token=KMAC128(Key,Data,128).

Pokud by byla tato implementace byla dostupná, doporučujeme použít tento algoritmus z důvodu rychlosti SHA3 a standardizace KMAC.

3 Tokenizace v systému MOS

3.1 Výkon rolí tokenizace v systému MOS

Tokenizační autorita

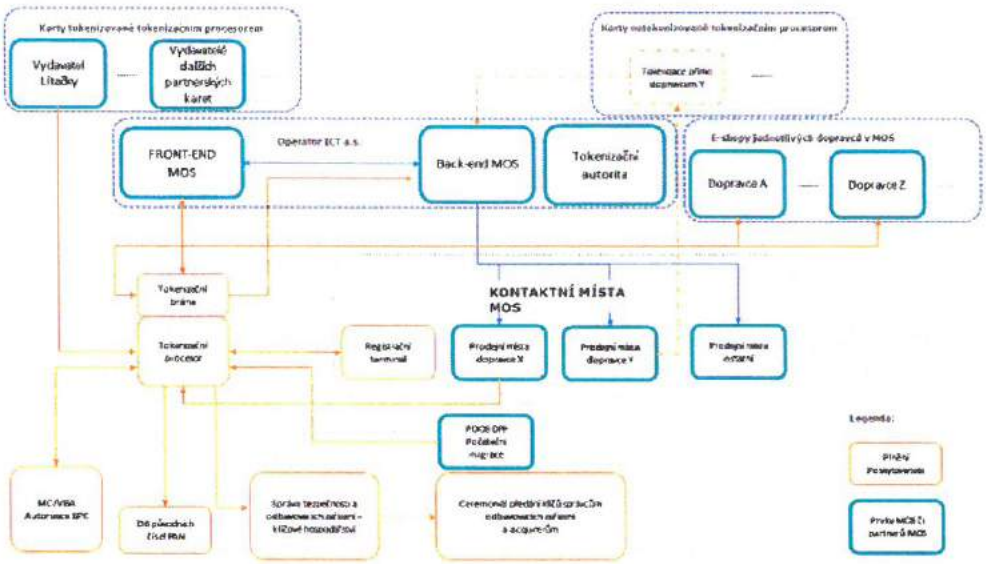
V systému MOS bude centrální Tokenizační autorita; tuto roli bude vykonávat Operátor ICT a.s.

Tokenizační autorita pouze stanovuje obecné a bezpečnostní parametry tokenizace v systému MOS. Tokenizační autorita stanovuje parametry s ohledem na soulad PCI-DSS a na soulad s platnou legislativou.

Acquirer a Tokenizační procesor

Tokenizační procesor bude v případech specifikovaných Tokenizační autoritou provádět sám (pokud je acquirer BPK) nebo přes svého acquirera (kterého si sám vybere a s kterým uzavře smluvní vztah) autorizace BPK. Tokenizační autorita nebude uzavírat smluvní vztah s dalším acquirerem za účelem tokenizace.

3.2 Tokenizační architektura



Obrázek č.1 Schéma tokenizace MOS

Token se bude využívat jako náhradní číslo identifikátoru a bude součástí databáze předplatitelů, ze které se budou získávat např. whitelisty cestujících s platným jízdním dokladem.

Součástí Front-end MOS bude mobilní aplikace, která v 2. etapě bude poskytovat služby self-care obdobné e-shopu MOS. Tokenizační procesor navrhne rozhraní mezi k Front-end MOS tak, aby registrační formulář byl funkční i v mobilních zařízeních a následně i mobilní aplikaci.

Registrace identifikátoru

Před zakoupením prvního jízdního dokladu musí cestující provést registraci identifikátoru. Registrace identifikátoru musí být zajištěna jak na e-shopech MOS a dopravců, tak i na jejich přepážkách. Řešení musí počítat se situací, kdy je acquirer dopravce odlišný od Tokenizačního procesora (či jeho smluvního

acquirera). Pro registraci na přepážkách bude využit registrační terminál, který bude sloužit pouze pro účely tokenizace a nebude provádět platební transakce.

Tokenizace bude (mimo jiné) probíhat na několika místech interakce identifikátoru se systémem:

- přepážka – při prodeji jízdního dokladu či asistenčních činnostech
- odbavovací místa ve vozidlech či přepravním prostoru
- revizorská zařízení při přepravní kontrole
- při registraci nového identifikátoru na e-shopu, přepážce či mobilní aplikaci.

Vstupní data pro tokenizaci v rozsahu číslo karty (PAN, číslo karty nebo logické číslo karty dle typu tokenizované karty), expirace karty (rok a měsíc) a typ karty (BPK, Mifare, Lítačka atd.) budou k Tokenizačnímu procesorovi přicházet třemi kanály:

1. Elektronicky, a to dávkově nebo i jednotlivě od každého z vydavatelů karet tokenizovaných Tokenizačním procesorem. A to při zapojení provozovatele do systému a dále při vydání nových karet provozovatelem.

2. Skrze přesměrování z Front-endu MOSu, mobilní aplikace a e-shopů/selfcare jednotlivých dopravců MOS

3. Z registračních čteček, které pro účely tokenizace provozuje sám Tokenizační procesor.

Tokenizace bude probíhat jednosměrným algoritmem, který stanoví Tokenizační autorita s využitím návrhu Tokenizačního procesora.

3.3 Tokenizační algoritmy a klíče

Tokenizační autorita stanoví sady algoritmy/klíče s ohledem na aktuální požadavky PCI-DSS a aktuální poznatky z oblasti kryptografie. Algoritmy a klíče budou mít plánovanou životnost. Výchozí doba životnosti je 6 let. V případě nepředvídané události (například nečekaný pokrok v technice, který způsobí zranitelnost použitého algoritmu či kompromitaci klíče) může být zcela výjimečně přistoupeno ke zkrácení životnosti sady. Naopak je možné, že Tokenizační autorita jeden algoritmus či klíč použije i vícekrát. Tokenizační autorita předá v případě změny nový algoritmus a parametry klíče Tokenizačnímu procesorovi s minimálně 6 měsíčním předstihem (pokud jde o plánovanou změnu algoritmu či výměnu klíče).

Tokenizační klíč bude bezpečně vygenerován a uložen v zařízeních Tokenizačního procesora (v HSM). Tokenizační klíč (a algoritmus) jako takový je však majetkem Tokenizační autority.

[redacted]

Klíč pro tokenizaci BPK a pro tokenizaci všech ostatních partnerských karet může být odlišný, pokud to bude v budoucnu Tokenizační autorita požadovat.

Ke každé kartě budou v jeden okamžik vytvořeny dva tokeny, každý s odlišným párem klíč-algoritmus. Plánovaná životnost těchto dvou tokenů se bude překrývat o 3 roky. Jeden z úplně prvního páru klíč-algoritmus bude mít zkrácenu životnost na 3 roky, aby došlo k přirozenému překryvu.

Tokenizační procesor v případě výměny párů klíč-algoritmus (plánované i neplánované) provede přetokenizaci, tak aby ke všem kartám existoval token vygenerovaný aktuálním párem klíč-algoritmus.

Verze tokenu bude číslo z postupně zvyšující se celočíselné řady označující jednotlivé použité páry klíč/algoritmus, seznam použitých verzí tokenů spolu s informací platí/neplatí bude ve strojově čitelné formě zveřejněn přes API. Tokenizační procesor povede u každé verze tokenu informaci, zda jde o provozní či testovací klíč/algoritmus, aby byl umožněn testovací provoz služby.

3.4 Tokenizované typy identifikátorů

Tokenizační procesor bude přes svoji tokenizační bránu provádět tokenizaci provozovatelských karet systému MOS a bude taktéž provádět tokenizaci některých vybraných partnerských karet MOS podle rozhodnutí Tokenizační autority. Mezi partnerské karty budou patřit i bankovní karty (BPK).

Pro některé typy identifikátorů bude proto třeba evidovat ke každému identifikátoru dvě čísla, např. UID a CLN. Podle způsobu registrace může být vstupním údajem jedno číslo karty, ale podkladem pro token bude druhé číslo karty. Příklad: Při registraci na e-shopu cestující bude zadávat CLN, ovšem podkladem pro token bude UID. Tokenizační procesor bude připraven na všechny kombinace vstupních/výstupních čísel karet pro konkrétní typ identifikátoru. Potřebné kombinace souvisejících čísel k identifikátoru by v takovém případě obdržel Tokenizační procesor předem od vydavatele karty během spouštění jednotlivých typů identifikátorů, nebo by je získával on-line dotazem k vydavateli identifikátoru během registrace. Tokenizační procesor bude v rámci plnění připraven na obě takové alternativy.

Při připojení nového typu identifikátoru do systému MOS provede Tokenizační procesor po obdržení vstupních dat od takového nového vydavatele úvodní migraci – tokenizaci stávajících karet takového vydavatele, a to dávkovým způsobem obdobně jako při registraci nové karty do systému.

Při spuštění typu identifikátoru Tokenizační autorita stanoví, zda a jakým postupem bude identifikátor tokenizován. Pro identifikátory, které nebude třeba tokenizovat, bude v systému MOS na místě tokenu použito

hardware či logické číslo identifikátoru. Tokenizační procesor bude v případě potřeby nadále zajišťovat stejné funkce i pro netokenizované typy identifikátoru, jako by šlo o identifikátory tokenizované.

3.5 Autorizace bankovních karet

Ve výchozím stavu se počítá s autorizací BPK při první registraci do systému a dále při přiřazení jízdního dokladu k BPK. Případy autorizace stanoví Tokenizační autorita na doporučení Tokenizačního procesora. Tokenizační procesor musí sledovat pravidla společností MC a Visa pro přiřazení jízdního dokladu k BPK a svá doporučení průběžně upravovat podle těchto pravidel. Tokenizační procesor bude aktivně sledovat úpravy pravidel společností MC a Visa ve spolupráci se svým acquirerem a nebude spoléhat na součinnost Tokenizační autority. Pokud požadavky Tokenizační autority přesahují možnosti společností MC a Visa, pak Tokenizační procesor a jeho acquirer vyvinou veškeré úsilí pro úpravu pravidel společností MC a Visa podle záměrů Tokenizační autority.

I kdyby jedna z karetních společností nevyžadovala nebo neumožňovala autorizaci karet, Tokenizační procesor získá přístup k některým informacím o kartách, které bude předávat do systému MOS, např. form factor, země vydavatele, a zda jde o předplatní kartu.

3.6 Vedení údajů o identifikátorech

Tokenizační procesor bude ve své databázi (která je v PCI-DSS level 1 certifikovaném perimetru Tokenizačního procesora) uchovávat tabulku s původními informacemi o kartě (PAN/číslo karty, expirace, typ karty, form factor karty, země vydavatele a k tomu všechny příslušné tokeny).

Karty v databázi Tokenizačního procesora budou uchovány ve výchozím stavu 3 roky po skončení platnosti – expirace takové karty. Dobu uchování karet po expiraci v sytému stanoví Tokenizační autorita, a to zejména s ohledem na aktuální legislativní požadavky.

Na pokyn Tokenizační autority může být nařízeno Tokenizačnímu procesorovi i smazání jednotlivé karty dříve.

Tokenizační procesor předá informace o ztokenizovaných identifikátorech do back-endu systému MOS přes předávací rozhraní API. Požadavky na API je uvedeno jako samostatná kapitola této přílohy. Pro BPK půjde alespoň o informace v rozsahu tokeny, verze tokenů, expirace, typ, maskované číslo karty ve tvaru 6 čísel zleva-hvězdičky-poslední 4 čísla, form factor, příznak předplatní karty a země vydavatele V systémech MOS se bude pracovat a zobrazovat maskované číslo BPK ve tvaru hvězdičky a 4 posledních čísel. Prvních šest čísel bude viditelných pouze z vysoce privilegovaných účtů z důvodu řešení technických problému (prvních 6 čísel obsahuje

informaci o typu karty a vydavateli). Závazný rozsah předávaných informací o ztokenizovaných identifikátorech bude stanoven při integraci příslušného typu identifikátoru.

Tokenizační procesor předá na dotaz přes předávací rozhraní API s back-endem MOS informaci o tom, zda již token dotazovaný back-endem existuje v databázi Tokenizačního procesora. Součástí této odpovědi v případě pozitivní odpovědi budou i všechny ostatní uložené tokeny svázané s touto kartou. Požadavky na API je uvedeno jako samostatná kapitola této přílohy. Obdobnou informaci podá Tokenizační procesor i při registraci identifikátoru, kde Tokenizační procesor zjistí, že daný identifikátor je již registrován. Informaci o požadavku na registraci již registrované karty předá Tokenizační procesor rovněž do MOS přes předávací rozhraní API.

3.7 Registrace identifikátorů na přepážkách

Tokenizační procesor dodá a bude provozovat registrační terminály na kontaktních místech MOS, v případě dohody s provozovatelem prodejního terminálu (POS) kontaktního místa MOS lze funkce těchto terminálů sloučit.

Registrační terminál musí být schopen samostatně indikovat úspěšné ztokenizování přiložené karty a její předání do systému MOS přes tokenizační bránu.

4 Součásti plnění Tokenizačního procesora

Tato kapitola shrnuje dílčí služby Tokenizačního procesora (Poskytovatele) k Objednateli jako výsledek předmětu plnění smlouvy. Všechny součásti plnění musí být v souladu s ustanoveními této přílohy, smlouvy a dalších příloh. Služby nepopisují veškeré činnosti Poskytovatele vedoucí k naplnění účelu popsaného v této příloze, Smlouvě a dalších přílohách. Při identifikaci a zajištění takových činností – i pokud nejsou přímo vyjmenovány v této Příloze – bude Poskytovatel vycházet ze svých zkušeností a znalostí, a neomezí se na pokyny či instrukce Objednatele.

Všechny prvky systému Tokenizačního procesora pracující s původními kartovými daty platebních karet budou mít PCI DSS certifikaci pro daný účel.

Součástí akceptace všech služeb i jejich částí bude podrobná dokumentace. Dokumentace bude obsahovat uživatelskou příručku určenou pro výkonné pracovníky Objednatele či dalších účastníků MOS, a dále bude obsahovat technickou dokumentaci určenou pro rozvojové a vedoucí pracovníky, která bude popisovat technické řešení, bezpečnostní pravidla, popis procesů, implementační požadavky a případné obchodní aspekty.

Souhrn služeb:

Inicializace	4.1	Návrh API pro front-end a back-end MOS
	4.2	Vytvoření systému včetně souvisejících služeb a API
	4.3	Spouštění jednotlivých typů identifikátorů
Průběžné služby	4.4	Provozní tokenizace a registrace identifikátorů
	4.5	Pronájem a údržba registračních terminálů
	4.6	Klíčové hospodářství MOS
	4.7	Podpora a údržba dodávaných služeb
	4.8	Jednotné kontaktní místo
Exit	4.9	Předání dat při ukončení smlouvy
	Další činnosti podle Exitového plánu	
Rozvoj	4.10	Implementační podpora a rozvoj

Následující části dokumentu popisují podrobně jednotlivé služby, související SLA a další požadavky.

4.1 Návrh API pro front-end a back-end MOS

Vzhledem k tomu, že front-endová a back-endová infrastruktura MOS není ještě ke dni uveřejnění Zadávací dokumentace vytvořena, vytvoří Tokenizační procesor v rámci Inicializace návrh předávacího API, a to na úrovni detailu potřebné pro vytvoření software realizující funkce API (varianty jsou přípustné). Tokenizační autorita tento návrh může i upravit a následně ho předá zpět Tokenizačnímu procesorovi jako zadání pro předávací rozhraní API. Podmínkou je použití webového rest API ve formátu JSON se zabezpečením dle nejnovějších bezpečnostních poznatků a OWASP guidelines.

API bude zahrnovat nejméně následující vazby a/nebo funkce:

1) Registrace identifikátorů na e-shopech MOS, e-shopech dopravců a mobilní aplikaci (vazby Tokenizační brána – Front-end MOS a Tokenizační brána – E-shopy jednotlivých dopravců v MOS)
2) Přenos informací o identifikátorech a jejich tokenech (vazba Tokenizační brána – Back-end MOS)
3) Přenos údajů k/od vydavatelů identifikátorů (vazba Tokenizační brána – Vydavatel partnerských karet)
4) Správa identifikátorů a tokenů (vazba Back-end MOS – Tokenizační brána) např. pokyn ke smazání karty.
5) Rozhraní mezi Tokenizačním procesorem a Vydavatelem partnerské/provozovatelské karty bude navrženo tak, aby do budoucna umožnilo výměnu dat nejenom vůči vydavateli, ale i vůči dalšímu Tokenizačnímu procesorovi; mj. umožní výměnu dat k více než jednomu portfoliu identifikátorů.

Při vytváření rozhraní API bude Tokenizační procesor spolupracovat s dalšími subjekty, které určí Tokenizační autorita. Půjde především o dodavatele SW pro front-end systému MOS, tj. systém, se kterým bude Tokenizační procesor komunikovat. Tato spolupráce je součástí plnění Inicializace.

4.2 Vytvoření Systému včetně souvisejících služeb a API

Tokenizační procesor v této fázi připraví Služby tak, aby bylo možné zahájit integraci identifikátorů a poskytování Průběžných služeb, a to zejména:

1. Realizace předávacího rozhraní API
2. Realizace a zprovoznění komunikace s ostatními systémy, např. Mastercard a Visa
3. Příprava registračních terminálů
4. Příprava registračního formuláře pro registraci identifikátorů v prostředí e-shopu
5. Inicializace klíčového hospodářství
6. Příprava jednotného kontaktního místa

Příprava všech služeb zahrnuje zpracování a předání dokumentace. Akceptace bude provedena především na základě úspěšné demonstrace jednotlivých služeb. Poskytovatel vytvoří v rámci plnění potřebné vzorky, testovací data a veškeré potřebné vybavení pro provedení dostatečné a průkazné demonstrace.

Příprava registračních terminálů zahrnuje předání jednoho vzorku registračního terminálu, a to od každého použitého modelu.

Příprava registračního formuláře pro registraci identifikátorů v prostředí e-shopu zahrnuje grafickou úpravu registračního formuláře podle vizuálu dodaného Objednatelem.

Inicializace klíčového hospodářství je popsána v kapitole 4.6.

4.3 Spouštění jednotlivých typů identifikátorů

Součástí služby Inicializace je spuštění následujících typů identifikátorů:

1. Lítačka
2. BPK

3. -5. upřesní OICT na základě preferenci organizátorů.

Cena za integraci těchto typů identifikátorů je součástí ceny Inicializace. Poskytovatel bude připraven provést integraci i dalších typů identifikátorů, které budou hrazeny jako součást Rozvoje. Integrace může u jednotlivých typů identifikátorů zahrnovat i migraci čísel identifikátorů a přetokenizaci podle aktuálních algoritmů/klíčů. Spuštění integrace každého typu identifikátoru bude zahájeno na pokyn Objednatele. Objednatel není povinen integrovat všechny typy identifikátorů uvedené výše.

Součástí spuštění identifikátoru Lítačka a BPK bude i migrace již registrovaných karet ze systému PDOS do MOS. Tokenizační procesor bude spolupracovat na migraci z PDOS (provozovaný DPP a.s.) do systému MOS. Bude řešena přetokenizace již uložených karet. Preferovanou metodou bude využití tokenizačního algoritmu a klíčů z PDOS, za předpokladu, že takové algoritmy/klíče budou splňovat požadavky PCI-DSS. Pro první 3 roky fungování systému (polovina 6letého životního cyklu klíč a tokenizačního algoritmu) může být za těchto podmínek převzat algoritmus použitý u DPP, během následujícího životního cyklu tokenizačních klíčů/algoritmu dojde postupně k nasazení klíčů/algoritmu projektu MOS pro tokenizaci všech nosičů MOS.

Typy identifikátorů Lítačka a BPK jsou prioritní a jejich spouštění bude provedeno co nejdříve. Odměna za spuštění Lítačky nebo BPK bude větší než pro další identifikátory vzhledem i k potřebné migraci z PDOS. Konkrétní výše odměny je součástí Přílohy 6 – Cenová tabulka.

Součástí integrace nového typu identifikátoru s výjimkou BPK a Lítačky je výměna SAM modulů registračních terminálů; tato výměna bude provedena pouze na pokyn Objednatele v tom případě, že si ji vyžádají bezpečnostní požadavky. Objednatel není povinen tuto výměnu využít.

4.4 Provozní tokenizace a registrace identifikátorů

Tokenizační procesor bude provádět provozní registraci, tokenizaci a případnou autorizaci identifikátorů, a to podle postupů a požadavků uvedených v této příloze.

Služba provozní tokenizace	
Popis služby	Registrace, tokenizace a případná autorizace identifikátoru vyvolané aktivitami cestujících nebo vydavatelů identifikátorů, monitorování a reportování.

Postup při zavedení služby	Služba bude spouštěna postupně pro každý typ identifikátoru. Podmínkou spuštění služby je dosažení milníku C3 pro daný typ identifikátoru.
Akceptace služby	Služba je akceptována dosažením milníku B3.
Předpokládaný rozsah služby	Služba je poskytována v nepřetržitém provozu.
Kvalitativní ukazatele služby	Dostupnost, rychlost registrace

SLA parametry

Ukazatel	Parametr	Rozsah zaručeného provozu služby	Max. doba jednoho výpadku služby (v minutách)
Dostupnost	99,9%	7x24 Po-Ne 0:00 – 24:00	30
Maximální doba zpracování operace Tokenizačního procesora s využitím předávacího rozhraní API od/k MOS a dalších účastníků (dopravci, vydavatelé) s výjimkou registrace.	300 ms	7x24 Po-Ne 0:00 – 24:00	-
Maximální doba každé jedné registrace na registračním terminálu. Doba bude měřena od přiložení identifikátoru do zobrazení výsledku registrace na displeji terminálu.	4 sekundy	7x24 Po-Ne 0:00 – 24:00	-
Maximální doba každé jedné registrace na webu či mobilní aplikaci. Doba bude měřena od předání kontroly Tokenizačnímu procesorovi do obdržení registračních údajů pomocí rozhraní, nepočítaje v to dobu zadání cestujícího.	1 sekunda	7x24 Po-Ne 0:00 – 24:00	-

SLA parametry – Incident Management

Parametr	Popis	Kategorie	Reakční doba	Doba vyřešení
Dostupnost	Celkový výpadek komunikace se sítí registračních terminálů.	A	15 minut	30 minut
Dostupnost	Částečný výpadek komunikace se sítí	B	15 minut	60 minut

	registračních terminálů.			
Dostupnost	Celkový výpadek komunikace s vydavateli	A	15 minut	30 minut
Dostupnost	Výpadek komunikace s jedním z vydavatelů, nemožnost registrace identifikátoru.	B	15 minut	60 minut
Dostupnost	Výpadek komunikace se sítí MC nebo VISA a nemožnost registrace BPK.	A	15 minut	30 minut
Dostupnost	Výpadek komunikace se systémem back-end a front-end MOS	A	15 minut	30 minut
Dostupnost	Výpadek komunikace s e-shopy dopravců	A	15 minut	30 minut
Plánované odstávky				
1x měsíčně 01:00 – 3:00, maximálně na dobu 3 hodin				
Sankce za nedodržení parametru dostupnosti.				
V případě, že v kterémkoliv Vyhodnocovacím období není tato služba poskytována v souladu se SLA, má Objednatel nárok na slevu z ceny Průběžných služeb ve výši 1.000 Kč za každých započatých 0,1 % snížení dostupnosti v daném Vyhodnocovacím období oproti SLA. V případě nedodržení závazného parametru maximální doby zpracování operace Tokenizačního procesora s využitím předávacího rozhraní API od/k MOS a dalších účastníků (dopravci, vydavatelé) s výjimkou registrace má Objednatel nárok na slevu z ceny Průběžných služeb za 1 měsíc ve výši 10 Kč za každý jednotlivý případ překročení parametru maximální doby zpracování v daném Vyhodnocovacím období. V případě nedodržení závazného parametru maximální doby zpracování každého jednoho požadavku na registraci má Objednatel nárok na slevu z ceny Průběžných služeb za 1 měsíc ve výši 100 Kč za každý jednotlivý případ překročení parametru maximální doby zpracování požadavku na registraci v daném Vyhodnocovacím období.				

4.5 Pronájem a údržba registračních terminálů

Tokenizační procesor dodá jako službu na vybraná kontaktní místa MOS (prodejní a kontaktní místa Objednatele a dopravců zapojených v MOS – tedy místa u externích subjektů) registrační čtecí terminály pro provedení tokenizace nově registrovaných karet do systému (BPK, NFC, Mifare). Umístění a počet registračních terminálů stanoví Tokenizační autorita na základě požadavků od Organizátorů dopravy. Registrační terminály budou rozmístěny v celém integrovaném dopravním systému, tj. na celém území hlavního města Prahy a Středočeského kraje v odhadovaném počtu 50 ks. Součástí plnění bude instalace registračních terminálů na těchto místech externích subjektů, a to včetně zaškolení obsluhy.

Součástí dodávky bude návod k použití pro obsluhu registračního místa. Tento návod bude obsahovat vyobrazení terminálu v dostatečné kvalitě, aby obsluha podle něj mohla vizuálně zkontrolovat integritu terminálu. Návod může obsahovat pokyny k běžným očekávaným operacím např. zapnutí, vypnutí a registrace identifikátoru, dále k vizuální inspekci registračního terminálu. Další pokyny, zejména servisního, bezpečnostního či revizního typu, jsou nepřípustné.

Registrační terminál bude splňovat následující požadavky a technické parametry:

1. Po celou dobu plnění budou registrační terminály splňovat aktuální požadavky společností Mastercard, Visa a budou mít platné PCI certifikace.
2. Bude obsahovat displej zobrazující přehledně v českém jazyce alespoň následující stavy: připravenost k funkci, poruchu s uvedením identifikace poruchy, výsledek registrace s uvedením případné chyby a další obvyklé informace pro obsluhu registračního terminálu za účelem jednoznačného ovládání přístroje. Pokus o registraci již registrovaného identifikátoru nebo pokus o registraci identifikátoru nevyžadujícího registraci nebude hlášen jako chyba, ale jako úspěšný úkon s podáním doplňující informace.
3. Napájení z běžné elektrické sítě; je přípustné, aby napájení bylo řešeno odděleným adaptérem. Délka přívodního kabelu napájení bude alespoň 250 cm.
4. Půdorysná plocha celého registračního terminálu musí být menší než 250 cm^2 a výška menší než 15 cm, nepočítaje v to případný napájecí adaptér.
5. Poskytovatel nemůže garantovat dostupnost pevného či wi-fi datového připojení na všech místech instalace, proto registrační terminál bude dostupný i ve verzi s mobilním datovým připojením. Systém bude vytvořen tak, aby byl schopen funkce podle níže uvedených SLA parametrů i s datovým připojením na úrovni GPRS. Mobilní datové spojení v takovém případě zajistí a uhradí Poskytovatel v rámci plnění, tj. bez dalších nároků na odměnu nebo úhradu takto vzniklých nákladů.
6. Náběh registračního terminálu od zapnutí do funkčního stavu nesmí být delší než 2 minuty.
7. Registrační terminál bude obsahovat jeden slot na SAM modul, který bude využit pro ověření autenticity identifikátoru. SAM moduly bude dodávat Objednatel. Poskytovatel bude instalovat a vyměňovat SAM moduly v registračních terminálech. Programové vybavení registračního terminálu bude umožňovat ověření autenticity identifikátoru s využitím SAMu či bez něj. Postup ověření autenticity se může pro různé typy identifikátorů lišit a bude stanoven během integrace příslušného typu identifikátoru. SAM modul může do budoucna obsahovat více klíčů pro ověření autenticity různých typů identifikátoru a registrační terminál musí takovou konfiguraci podporovat.

8. Programové vybavení registračního terminálu včetně změn tokenizačních algoritmů, změn tokenizačních klíčů či postupů ověření autenticity identifikátoru bude možné měnit vzdáleně bez nutnosti fyzické instalace či výměny registračního terminálu.

Služba pronájmu a údržby registračních terminálů				
Popis služby	Instalace, zprovoznění a výměna registračních terminálů ze strany dodavatele služby.			
Postup při zavedení služby	Služba musí být dostupná od milníku B3.			
Akceptace služby	Služba je akceptována jako součást milníku B3.			
Předpokládaný rozsah služby	Služba provozu registračních terminálů je poskytována v nepřetržitém provozu. Služby opravy - je poskytována v režimu 5x16. Opravy budou prováděny výhradně výměnným způsobem.			
Kvalitativní ukazatele služby (SLA)	Dostupnost. Doba výměny Doba instalace			
SLA parametry				
Ukazatel	Parametr	Rozsah zaručeného provozu služby	Max. doba jednoho výpadku služby	
Dostupnost	99,9 %	7x24 Po-Ne 0:00 – 24:00	30 minut	
Doba výměny	4 hod	5 x 16 Po-Pa 5:00 – 21:00		
	6 hod	So-Ne 5:00 – 21:00		
Doba instalace	48 hod	5 x 8 Po-Pa 8:00 – 16:00		
SLA parametry – Incident Management				
Parametr	Popis	Kategorie	Reakční doba	Doba vyřešení
Dostupnost	Výpadek komunikace se síti registračního terminálu	A	15 minut	30 minut
Dostupnost	Nefunkčnost jednoho registračního terminálu.	C	30 minut	dle SLA parametru
Doba výměny	Registrační terminál nevyměněn	C	30 minut	dle SLA parametru
Doba výměny	Registrační terminál vyměněn a nefunguje	C	30 minut	dle SLA parametru
Doba instalace	Registrační terminál nenaistalován	C	30 minut	dle SLA parametru

Doba instalace	Registrační terminál naistalován a nefunguje	C	30 minut	dle SLA parametru
Plánované odstávky				
1x měsíčně 00:00 – 5:00, maximálně na dobu 4 hodin				
Sankce za nedodržení parametru dostupnosti				
V případě, že v kterémkoliv Vyhodnocovacím období není tato služba poskytována v souladu se SLA, má Objednatel nárok na slevu z ceny Služeb podpory provozu ve výši 1.000 Kč za každých započatých 0,1 % snížení dostupnosti v daném Vyhodnocovacím období oproti SLA. V případě nedodržení závazného parametru doba výměny, doba instalace má Objednatel nárok na slevu z ceny Průběžných služeb za 1 měsíc ve výši 1000 Kč za každý jednotlivý případ překročení parametru doby vyřešení v daném Vyhodnocovacím období.				

4.6 Klíčové hospodářství MOS

Tokenizační procesor bude ve svých systémech spravovat klíče pro tokenizační proces a zajišťovat jejich uchování a distribuci dále do systému, zároveň bude zodpovídat za provádění bezpečných klíčovacích ceremoniálů při generování a přenosech klíčů ze svých HSM úložišť.

Tokenizační procesor bude na vlastní zálohované infrastruktuře HSM generovat a uchovávat klíče pro tokenizaci v MOS (karet netokenizovaných Tokenizačním procesorem se to přirozeně netýká).

Tokenizační procesor provede předání klíčů a algoritmů v případě prvotního spouštění systému, zapojení nového dopravce a při přechodu MOS na nový pár klíč/algoritmus. V součinnosti s pokyny Tokenizační autority zajistí Tokenizační procesor bezpečné předání Tokenizačních klíčů předávacím ceremoniálem všem správcům odbavovacích zařízení u dopravců zapojených do systému MOS. Tito správci, kterých nepředpokládáme víc než 10, budou klíče dále bezpečným způsobem nahrávat do zabezpečených úložišť v odbavovacích zařízeních a v revizorských čtečkách. Obdobně bude Tokenizační procesor předávat tokenizační klíče acquirerským bankám dopravců pro případ kontroly dodržení pravidel bankovních karet.

Pravidla společností Visa či Mastercard mohou vyžadovat, aby tokenizaci prováděl i acquirer nákupu jízdního dokladu. Přestože tento případ tokenizace není součástí plnění Tokenizačního procesora, Tokenizační procesor bude předávat algoritmy/klíče i zúčastněným acquirerům. Počet takových acquirerů se neočekává větší než 5.

Inicializace klíčového hospodářství bude provedena během Inicializace fáze 2 a bude zahrnovat prvotní vytvoření a předání klíčů podle předchozích odstavců, zejména vytvoření prvního páru sad algoritmus/klíče, návrh distribuce algoritmu a klíčů a samotná distribuce první sady algoritmus/klíče po schválení návrhu distribuce Tokenizační autoritou.

4.7 Podpora a údržba dodávaných služeb

Tokenizační procesor se zavazuje provozovat službu Tokenizačního procesora ve stavu plné shody s požadavky PCI-DSS (level 1), požadavky společností Mastercard/Visa a legislativními a regulatorními požadavky platnými na území České republiky. Tokenizační procesor je povinen po celou dobu trvání smlouvy udržovat svoji certifikaci na PCI-DSS level 1 a bude průběžně a proaktivně monitorovat i připravované změny v této oblasti, aby včas připravil možné požadované úpravy systému.

Součástí podpory a údržby je průběžná implementace služeb, které MC a Visa v budoucnu na území ČR zavedou, byť i jako nepovinné, ale které mohou rozšířit Funkcionality v rámci předmětu plnění. Mezi tyto služby patří např. Payment Account Reference (PAR), Visa Account Updater (a obdobná služba MC), nové verze protokolu 3D Secure a další.

4.8 Jednotné kontaktní místo

Jednotné kontaktní místo slouží pro poskytování uživatelské podpory a správu incidentů při výkonu Průběžných služeb. Tato služba musí být připravena tak, aby jí mohl využívat jak přímo Objednatel, tak i obsluha míst s registračními terminály, a to na základě pokynu Objednatele, který může být během plnění změněn.

Při hlášení incidentů a požadavků emailem bude Poskytovatel zasílat automatizované potvrzení o přijetí emailu.

Služba jednotného kontaktního místa (ServiceDesk)	
Popis služby	Hlášení, monitorování a reportování incidentů a uživatelských požadavků. Monitorování Funkcionality.
Postup při zavedení služby	Služba bude spuštěna dosažením milníku D1.
Akceptace služby	Služba je akceptována dosažením milníku B3. Součástí akceptace služby bude podrobná bezpečnostní a provozní dokumentace.
Předpokládaný rozsah služby	Služba je poskytována v nepřetržitém provozu.
Kvalitativní ukazatele služby (SLA)	Dostupnost.
SLA parametry	

Parametr	Dostupnost služby měsíční v %	Rozsah zaručeného provozu služby	Max. doba jednoho výpadku služby (v minutách)
Dostupnost Servicedesk (web a email rozhraní)	99,9%	7x24 Po-Ne 0:00 – 24:00	30
Dostupnost Servicedesk (telefonická podpora)	99,9%	7x24 Po-Ne 0:00 – 24:00	30
Dostupnost monitorování	98%	7x24 Po-Pá 0:00 – 24:00	30

SLA parametry – Incident Management				
Parametr	Popis	Kategorie	Reakční doba	Doba vyřešení
Dostupnost Servicedesk	Výpadek webového hlášení, potvrzování emailů nebo dostupnosti telefonické podpory	A	15 min.	30 min.
Dostupnost monitoringu	Výpadek monitoringu.	C	60 min.	6 hod.
Plánované odstávky				
1x měsíčně 01:00 – 3:00, maximálně na dobu 3 hodin				
Sankce za nedodržení parametru dostupnosti				
V případě, že v kterémkoliv Vyhodnocovacím období není tato služba poskytována v souladu se SLA, má Objednatel nárok na slevu z ceny Průběžných služeb ve výši 1.000 Kč za každých započatých 0,1 % snížení dostupnosti v daném Vyhodnocovacím období oproti SLA.				

4.9 Předání dat při ukončení smlouvy

Tokenizační procesor je povinen v případě ukončení smlouvy předat veškerý aktuální obsah databáze původních čísel karet včetně popisu datové struktury databáze jinému nástupnickému PCI-DSS certifikovanému subjektu, který si zvolí OICT.

4.10 Implementační podpora a rozvoj

Tokenizační procesor bude na základě pokynů od Tokenizační autority provádět rozvoj a úpravy systému, a to v případech kdy vyvstane potřeba akceptovat další nové typy partnerských karet MOS, případě budě potřeba tokenizace i pro nové funkce pro tzv. „smart cities" a regionální či pražské karty.

5 SLA

Měření dostupnosti

Dostupnost bude měřena jako podíl rozdílu celkové odsouhlasené provozní doby za sledované období a doby nedostupnosti služby, za niž nese odpovědnost dodavatel, a odsouhlasené provozní doby za sledované období vynásobené 100. Do odsouhlasené provozní doby za období se pro potřebu výpočtu dostupnosti promítnou plánované odstávky, pokud se uskutečnily v období zaručeného provozu služby. Dostupnost bude uvedena v %.

Dostupnost = (PDobdobí – Nslužby) / PDobdobí * 100 [%]

Kde:

PDobdobí .... Odsouhlasená provozní doba za sledované období

Nslužby ..... Doba úplné nedostupnosti služby ve sledovaném období, za niž odpovídá dodavatel

Definice kategorií incidentů

Kategorie	Definice
Kategorie A	Služba je celkově nedostupná a nedostupností jsou postiženi všichni uživatelé dané služby. Dopad je vysoký, činnost dotčená daným incidentem nemůže být vykonána náhradním způsobem, jde o problém všech skupin uživatelů. Naléhavost je vysoká, neboť incident prokazatelně ohrožuje splnění termínu prováděné činnosti a neexistuje žádné náhradní řešení Nebo Služba je celkově nedostupná a nedostupností je postižena jen některá skupina uživatelů. Dopad je střední, protože se nejedná o problém všech uživatelů, naléhavost je vysoká, protože incident prokazatelně ohrožuje splnění termínu prováděné činnosti a neexistuje žádné náhradní řešení. Nebo Služba je částečně nedostupná, tj. není dostupný některý funkční modul dané služby. Touto částečnou nedostupností jsou postiženi všichni uživatelé dané služby. Dopad je

	vysoký, protože se týká všech skupin uživatelů, naléhavost je však střední, neboť existuje známé náhradní řešení.
Kategorie B	Služba je mírně omezená a touto mírnou omezeností jsou postiženy pouze některé skupiny uživatelů. Dopad je střední, protože činnost sice nemůže vykonat někdo jiný, nejde však o problém všech uživatelů a jejich skupin. Nebo Služba je částečně nedostupná a touto částečnou nedostupností je postižen jednotlivý uživatel. Dopad je střední, protože dotčenou činnost může vykonat někdo jiný. Naléhavost je střední, protože je sice prokazatelně ohroženo splnění termínu prováděné činnosti, pro vykonání této činnosti však existuje známé náhradní řešení.
Kategorie C	Služba je mírně omezená a touto mírnou omezeností je postižen jednotlivý uživatel. Dopad je nízký, protože dotčenou činnost může vykonat někdo jiný a naléhavost je nízká, protože nedochází k ohrožení termínu.