

VYSVĚTLENÍ, ZMĚNA NEBO DOPLNĚNÍ DOKUMENTACE VÝBĚROVÉHO ŘÍZENÍ

Č. II

Identifikační údaje o koncesi malého rozsahu a zadavateli

KONCESE MALÉHO ROZSAHU:

Platební brána pro elektronické odbavení cestujících

výzva k podání nabídek byla uveřejněna na profilu zadavatele dne: **20.01.2021**

spisová značka zadavatele: **KVPB0720**

(dále jen „**koncese malého rozsahu**“)

ZADAVATEL KONCESE MALÉHO ROZSAHU:

Kraj Vysočina

IČO: 70890749

se sídlem: Žižkova 57, 587 33 Jihlava

(dále jen „**zadavatel**“)

ZÁSTUPCE ZADAVATELE:

Fiala, Tejkal a partneři, advokátní kancelář, s.r.o.

IČO: 28360125

se sídlem: Brno, Helfertova 2040/13, Černá Pole, PSČ 613 00

tel.: +420 541 211 528

e-mail: zakazky@akfiala.cz

ID datové schránky: vb7kdaz

(dále jen „**zástupce zadavatele**“)

Zástupcem zadavatele při provádění úkonů souvisejících s výběrovým řízením je obchodní společnost **Fiala, Tejkal a partneři, advokátní kancelář, s.r.o.**

V souladu s čl. 16 dokumentace výběrového řízení zadavatel vysvětluje dokumentaci výběrového řízení na žádost dodavatele takto:

Dotaz č. 1

Zadavatel obdržel dotaz v tomto znění:

V dokumentu VYSVĚTLENÍ, ZMĚNA NEBO DOPLNĚNÍ DOKUMENTACE VÝBĚROVÉHO ŘÍZENÍ č.1 (dále jen „Vysvětlení č.1“) je popsán hrubý způsob integrace platební brány a back office VDV. Zároveň popisuje způsob výpočtu tokenu pro nosiče typu InKarta a Jihlavská karta. Prosíme o přibližný počet jednotlivých identifikátorů nosičů, tj. kolik EMV karet, InKaret a Jihlavských karet bude v systému EOC.

Odpověď na dotaz č. 1

Zadavatel tímto na shora uvedený dotaz odpovídá následovně:

Technická zadávací dokumentace (specifikace) počítá s těmito typy identifikátorů v systému EOC:

Bezkontaktní bankovní karta (BPK)

Bankovní karty, které budou integrovány do nově budovaného systému:

- *Bezkontaktní bankovní karta (možno použít také hybridní bankovní karty obsahující: magnetický proužek, kontaktní a bezkontaktní čip)*
- *Kreditní, debetní a předplacená bankovní karta vydaná asociací Mastercard, VISA (popřípadě další: Diners Club)*
- *Bankovní karta vydaná ve formě „mezinárodní karty“ (mezinárodně akceptované bankovní karty) nebo „domácí karty“ (bankovní karty akceptované pouze na území České republiky)*

QR kód generovaný mobilní aplikací

- *Jedinečný identifikátor (token) bude počítat platební brána (respektive SAM) stejně jako u ostatních identifikátorů. Algoritmus zůstává stejný jako u bezkontaktních karet. (mobilní aplikace by jen měla být odlišena jiným prefixem v prvním bytu na vstupu)*
- *Prezentace jednoznačného identifikátoru bude v mobilní aplikaci realizována prostřednictvím 2D čárového kódu (QR kód). Takto generovaný kód musí být zabezpečen možností ověření získaných dat (například budou data elektronicky podepsána pomocí asymetrické kryptografie)*
- *Identifikátor bude jedinečný pro každou jednotlivou instalaci mobilní aplikace v telefonu i v rámci jednoho uživatelského účtu (z uvedeného vychází i požadavek na unikátnost v rámci instalace do různých mobilních zařízení)*
- *U mobilní aplikace (QR kódu) bude pro výpočet vstupních dat k tokenizaci použit jednoznačný identifikátor kódovaný do pole bajtů a předávaný v QR kódu v části „Datová část specifická pro zákazníka“. Vnitřní struktura identifikátoru bude stanovena dodavatelem mobilní aplikace*

Bezkontaktní čipové karty vydávané dopravcem (BČK)

Hlavním požadavkem této funkcionality je využití existujících dopravních karet (bezkontaktních čipových karet) jejichž vydavateli jsou subjekty poskytující veřejnou dopravu na území IDS VDV

- *In Karta (nový typ karty typu/standardu MAP)*
- *Jihlavská karta*

Systém musí být navržen tak, aby umožňoval budoucí zapojení karet dalších dopravců, u kterých mohou být použity odbavovací technologie využívající karty Mifare Desfire (Mifare Desfire EV1).

Systém musí navíc být připravený pro budoucí možné rozšíření o funkci akceptace dalších typů identifikátorů (např. elektronická karta ISIC a pod).

Příklady výpočtu dat pro tokenizační algoritmus uvedené ve vysvětlení č.1 z pochopitelných důvodů nemohou zahrnovat všechny karty dopravců/typy identifikátorů, které se v budoucnu do systému EOC VDV zapojí.

Co se týká počtu identifikátorů (cestujících) registrovaných v systému EOC. Odhadujeme celkem 20 000 zaregistrovaných identifikátorů po 1 roce provozu systému.

Dotaz č. 2

Zadavatel obdržel dotaz v tomto znění:

Zpracování MiFare Desfire karet na platební bráně pro zpracování EMV karet není zcela standardní požadavek. Prosíme o bližší specifikaci formátu InKarty a Jihlavské karty (délka čísla a formát InKarty a Jihlavské karty). Zároveň prosíme o popis toho, jak je možné od sebe odlišit InKartu a Jihlavskou kartu a jaké jsou dostupné kontroly platnosti identifikátoru InKarta a Jihlavská karta? Jihlavská karta se má podle Vysvětlení zadávat bez data expirace, jak jí odlišíme od identifikátoru InKarta? Vyjasnění těchto nestandardních požadavků na zpracování MiFare Desfire karet na platební bráně pro zpracování karet asociací Mastercard a VISA je nutné pro zajištění úprav, pro které potřebujeme vstupy pro nacenění implementace.

Odpověď na dotaz č. 2

Zadavatel tímto na shora uvedený dotaz odpovídá následovně:

Specifikace formátu Jihlavské karty a InKarty (dle technické specifikace projektu EOC):

- *In Karta (nový typ karty typu/standardu MAP)*
 - *Vydavatelem je společnost České dráhy a.s.*
 - *Technologie: DESfire EV1 8kB*
 - *Rozlišení nového typu karty: symbol MAP ready (grafický prvek vytištěný na kartě)*
 - *Typ vydávané karty: personalizovaná a nepersonalizovaná karta*
 - *Dále lze karty rozlišit dle použití: zákaznická karta (personalizovaná), služební karta (personalizovaná), business karta (nepersonalizovaná karta)*
 - *Karta je vydávána s platností 5 let*
 - *Identifikační údaje na kartě (personalizované): Jméno, příjmení, datum narození, fotografie držitele karty, unikátní číslo vydané karty a platnost karty*

Registrace karty do systému EOC uživatelem bude realizována na základě vyplnění unikátního čísla karty (18místné číslo karty je definované dle ISO/IEC 7812-1, postup přidělování tohoto čísla pak normou ISO/IEC 7812-2) a platnosti karty (oba údaje jsou vytištěny na kartě).

- *Systém následně ověří platnost zadaného čísla karty za použití metody Luhnův algoritmus (tj. shoda výpočtu s kontrolní číslicí 18. pozice v čísle karty). Dále ověří, zda je karta platná.*
- *Po vyhodnocení výše uvedených dat bude vygenerován jednoznačný identifikátor (obdobným způsobem, který je uveden v případě bankovní karty).*

U In Karty (na platformě MAP s nosičem Mifare DESFireEV1) pro výpočet vstupních dat k tokenizaci budou použity následující údaje vytištěné na těle nosiče:

- *Číslo karty (PAN) a*
- *Expirace karty,*
které BackOffice odešle jako vstupní data (vstupní pole bytů) k tokenizaci na platební bránu.

Poznámka k off-line tokenizaci v SAM modulech:

Nelze bez ověření (odemčení) přečíst číslo karty z Desfire (EV1). Čtecí a Ověřovací klíč In-karty je uložen v SAMu.

- *Jihlavská karta*

- *Vydavatelem je společnost Dopravní podnik města Jihlavy, a.s.,*
- *Technologie: DESfire 4kB*
- *Typ vydávané karty: personalizovaná a nepersonalizovaná karta*
- *Karta je vydávána s platností 4 roky*
- *Identifikační údaje na kartě (personalizované): Jméno, příjmení, fotografie držitele karty, unikátní číslo vydané karty*

Registrace karty do systému EOC uživatelem bude realizována na základě vyplnění unikátního čísla karty, případně iniciálů jména, příjmení držitele karty.

- *Pro výpočet vstupních dat do tokenizačního algoritmu bude využito pouze UID karty (resp. číslo Jihlavské karty)*
 - *UID karty Mifare DESFire dle standardu ISO-14443A (resp. číslo Jihlavské karty)*

Hodnota UID není z karty lidským okem čitelná (na rozdíl od čísla Jihlavské karty). Pro registraci Jihlavské karty prostřednictvím webového rozhraní bude nutné vytvořit v Backoffice EOC KV převodní službu, která zajistí převod čísla Jihlavské karty na UID a zároveň dotazem do Backoffice DPMJ ověří platnost Jihlavské karty.

- *Následně BackOffice odešle vstupní data (vstupní pole bytů) k tokenizaci na platební bránu: UID s prefixem 00 (prefix FF bude pro QR kód)*

Poznámka k off-line tokenizaci v SAM modulech:

Rozhodnutí tokenizovat Jihlavskou kartu jen pomocí UID bez autentizace je nutné zlo, ke kterému KV došel, protože není k dispozici čtecí klíč od dopravního podniku.

Dotaz č. 3

Zadavatel obdržel dotaz v tomto znění:

V dokumentu Vysvětlení č.1 je popsán tokenizační algoritmus jako AES256. Klíč bude transportován na dvou komponentách zašifrovaných klíčem 3DES. Použitím způsobu výpočtu tokenu jako samotného šifrování pomocí algoritmu AES256 odporuje požadavkům na funkční tokenizaci dle bezpečnostního standardu PCI. Celý systém EOC VDV by pak musel být prověřen na soulad se standardem PCI DSS, aby jej bylo možné provozovat s EMV kartami. Pro rozptýlení pochybností prosíme o zaslání celého algoritmu pro výpočet tokenu (pozn. postup výpočtu tokenu by neměl být citlivý, klíčové je obvykle zabezpečit vlastní klíče pro výpočet tokenu nikoliv postup).

Odpověď na dotaz č. 3

Zadavatel tímto na shora uvedený dotaz odpovídá následovně:

V dokumentu Vysvětlení č. 1 je v odpovědi zmíněno šifrování AES256 pouze v souvislosti s tokenizačním klíčem.

Tokenizační algoritmus EOC VDV netvoří jen samotné šifrování pomocí algoritmu AES256 (to by skutečně odporovalo standardu), ale i další kroky (sestavení vstupních dat pro zvolený identifikátor, doplnění paddingem, hashování pomocí SHA-256).

Všechny požadavky na funkční tokenizaci dle zmíněného standardu tak jsou v navrženém algoritmu dodrženy (analogický algoritmus už je používán v ostrém provozu v obdobných systémech v ČR).

Dotaz č. 4

Zadavatel obdržel dotaz v tomto znění:

V dokumentu Vysvětlení č.1 bylo doplněno, že Zadavatel požaduje připojit také nabídku na acquiring do platebních terminálů. Zadávací dokumentace obsahuje Přílohu č.4 s názvem „Předloha pro zpracování ceny“. Zde jsou uvedeny objemy na e-commerce i platební terminály dohromady? Pro přesnější cenovou kalkulaci bychom uvítali mít kategorie rozdělené dle typu prodeje (eshop/mobilní aplikace/předprodejní místa/revizoři atd).

Odpověď na dotaz č. 4

Zadavatel tímto na shora uvedený dotaz odpovídá následovně:

Ano, oba v tabulce uvedené prodejní kanály

- *Jednotlivé jízdné (prodej ve vozidlech a v mobilní aplikaci)*
- *Časové jízdné (prodej na předprodejích a v e-shopu)*

uvádějí celkovou sumu předpokládaných tržeb bez ohledu na způsob platby.

Oba prodejní kanály umožňují platby v hotovosti, kartou, platbu po internetu (e-commerce).

V současnosti ale nemáme k dispozici relevantní data, která by nám umožňovaly poskytnout požadované údaje s dostatečným stupněm přesnosti.

Dotaz č. 5

Zadavatel obdržel dotaz v tomto znění:

V případě, že bude nutné poskytnout některou z požadovaných funkcionalit prostřednictvím subdodavatele, požaduje Zadavatel tohoto subdodavatele uvést? Jaké dokumenty požaduje Zadavatel za subdodavatele dodat?

Odpověď na dotaz č. 5

Zadavatel tímto na shora uvedený dotaz odpovídá následovně:

Dle dokumentace výběrového řízení je dodavatel povinen předkládat doklady ke svým poddodavatelům pouze v situaci, kdy jimi prokazuje nějakou část kvalifikace (viz odst. 10.3 až 10.4 DVŘ). K pouze realizačním poddodavatelům (nekvalifikačním) nemusí dodavatel předkládat žádné dokumenty.

Zadavatel upozorňuje, že v souvislosti s výše uvedeným vysvětlením dokumentace výběrového řízení se lhůta pro podání nabídek nemění.

V Brně dne 25.02.2021

Kraj Vysočina

v.z. Fiala, Tejkal a partneři,
advokátní kancelář, s.r.o.
Mgr. Jan Tejkal, advokát
společník a jednatel