**SOFTVÉR – TECHNICKÁ ŠPECIFIKÁCIA PREDMETU PLNENIA**

**BBSK – ELEKTRONICKÉ ODBAVOVANIE CESTUJÚCICH**

**POŽIADAVKY NA SLUŽBY ACQUIRERA**

1. **PREDMET VEREJNEJ ZÁKAZKY**

Predmetom tejto verejnej zákazky je zaistenie poskytovania služieb tzv. „merchant acquiring“, teda služieb spojených s prijímaním platobných kariet a uskutočňovaním bezhotovostných platieb za služby a tovary zadávateľa prostredníctvom platobných kariet, resp. kartových platobných prostriedkov a platobných terminálov (ďalej len „**Predmet zákazky**“).

Predmet zákazky zahŕňa:

* akceptáciu platobných kariet štandardov VISA (vrátane VISA Electron) a MasterCard (vrátane Maestro) s možnosťou dohody o akceptácii ďalších druhov kompatibilných kariet
* procesovanie platieb bankovými kartami v dopravnom režime (s prípadným denným cappingom)
* procesovanie platieb bankovými kartami v režime retail
* zaistenie dodávky tokenizačného SW
* posúvanie potrebných informácií o transakciách vrátane použitých tokenov do back-office zadávateľa
* vytvorenie potrebných dátových rozhraní a pripojení
* dodávku SW do platobných terminálov potrebného pre procesovanie platieb bankovými kartami v dopravnom režime a jeho aktualizáciu v priebehu trvania zmluvy (teda prispôsobovanie tohto SW aktualizáciám platobných terminálov a udržovanie tohto SW v súlade s požiadavkami kartových asociácií)
* spoluprácu a dodávku SW pre procesovanie platieb bankovými kartami v dopravnom režime do bankových čítačiek pri rozširovaní systému IDS aj do MHD
* poskytovanie servisu a údržby inštalovaného SW, vrátane dodanie dokumentácie
* zaistenie nepretržitého poskytovanie služieb

1. **PREHĽAD SKRATIEK**

|  |  |
| --- | --- |
| BBSK | Banskobystrický kraj a súčasne označenie pre integrovaný systém EOC v tomto kraji |
| DZC | Dopravné Zúčtovacie Centrum |
| EOC | Elektronické Odbavovanie Cestujúcich |
| IDS | Integrovaný Dopravný Systém |
| Integrátor | Nová spoločnosť, ktorú kraj plánuje založiť v septembri 2021 a ktorý bude mať na starosť EOC pre BBSK. |
| Token | Alfanumerický reťazec umožňujúci identifikáciu zákazníka, ako aj bankovej alebo nebankovej bezkontaktnej karty či v inej forme (2D kódy), ktorá umožňuje identifikáciu zákazníka. |
| Tokenizácia | Proces, vytvorenia identifikátoru zákazníka z čísla bankovej karty |
| Zadávateľ | Objednávateľ Služby (IDS alebo BBSK) |
| Zákazník | Cestujúci v systéme EOC. Či už je aktívnym držiteľom prístupu k zákazníckemu účtu, alebo ho používa iba pasívne. |

1. **ZÁKLADNÉ INFORMÁCIE O EOC A O OBSAHU ZÁKAZKY**

**3.1 Aktuálna situácia**

V Banskobystrickom samosprávnom kraji je v pláne vybudovanie integrovaného dopravného systému. Kraj súťaží dopravcu na desaťročné obdobie od roku 2024. Súčasne plánuje zaviesť elektronické odbavovanie cestujúcich. Všetky odbavovacie systémy budú vytvárané novo (a budú vyhotovované integrátorom) a systém nebude nadväzovať na nič z toho, čo sa aktuálne používa (napríklad čipové karty v časti kraja).

Systém bude najprv zavádzaný na území kraja v podobe autobusovej regionálnej prepravy. Bude snahou tiež rovno zapojiť lokálnu mestskú hromadnú dopravu menších obcí. Spôsob a čas prípadnej integrácie MHD je nejasný.

EOC bude založené na centralizovanej architektúre. Všetky lístky budú evidované v Dopravnom zúčtovacom centre (DZC), ktoré bude vytvárané počas roku 2022. Do DZC sa budú odovzdávať všetky informácie o zakúpených lístkoch (z eshopu, mobilné aplikácie a ďalších kanálov). Do DZC budú odovzdávané informácie o všetkých transakciách vykonaných na bankových čítačkách vo vozidlách obsluhovaných acquirerom (tokeny a súvisiace údaje o cestovnom lístku pre zúčtovanie). DZC následne po skončení dňa vykoná hodnotenie všetkých transakcií (kontrola na vlastníctvo predplatných cestovných lístkov), podľa stanovených tarifných pravidiel aplikuje pravidlá denného zastrešenia (tzv. Capping) a následne zadá voči rozhraniu acquirera požiadavky na zúčtovanie prostriedkov z bankových kariet (pre každú kartu jednu sumu ako jednu súhrnnú transakciu).

**3.2 Regionálne autobusy v rámci IDS**

IDS bude najprv zahŕňať cca 500 regionálnych autobusov, kde budú cestujúci nastupovať len prednými dverami cez vodiča, ktorý bude obsluhovať odbavovacie zariadenie. U vodiča síce pôjde platiť aj v hotovosti, ale lístky platené v hotovosti budú mať vyššie ceny a systém bude preferovať platenia bankovou kartou.

Predpokladá sa otvorené riešenie odbavovacieho zariadenia, teda kombinácia riadiaceho zariadenia (tabletu či adekvátneho zariadenia), oddelené samostatné termotlačiarne (pre vydávanie účteniek za platby v hotovosti) a jednej samostatnej oddelenej bankovej čítačky, ktorá sa bude používať na tokenizáciu a platenie iba v dopravnom režime.  Pri platení kartou sa nebude k transakcii vydávať žiadna účtenka, budú sa vykonávať len bezkontaktné transakcie s obmedzenou maximálnou výškou tak, aby sa nikdy nezadal PIN. Banková čítačka by vždy mala riadiacemu zariadeniu vrátiť token pre vykonanú transakciu, aby ho bolo možné priradiť k údajom o cestovnom lístku. Súčasne by banková čítačka mala vygenerovať a odovzdať aj potrebné zašifrované informácie o vykonanej bankovej transakcii v dopravnom režime, ktoré budú následne odovzdané cez riadiace zariadenie a GSM anténu do back-office rozhranie acquirer.

Aplikácia v riadiacom zariadení bude komunikovať s bankovou čítačkou a bude jej dávať pokyny k tokenizácia či prevedenie bankovej transakcie v dopravnom režime (teda čítačka nebude sama automaticky čítať karty a vykonávať transakcie jednoduchým priložením karty bez príjmu konkrétneho typu pokynu z riadiaceho zariadenia).

**3.3 Predajné miesta v rámci IDS**

V rámci IDS bude integrátor prevádzkovať vyšší počet zákazníckych centier, kde si budú môcť cestujúci u pracovníkov týchto centier kupovať lístky. V týchto centrách by sa mali používať rovnaké bankové terminály ako v regionálnych autobusoch (teda vrátane tokenizačnej funkcie), ale bude sa využívať iba "retail" mód pre platby kartou. Čítačky budú komunikovať s predajným zariadením (tabletom s OS Android), ktoré bude dávať čítačke pokyny k iniciácii tokenizácie či požiadavku na platenie.

**3.4 Prepravná kontrola v rámci IDS**

V rámci IDS sa budú pohybovať revízori, ktorí budú môcť kontrolovať lístky cestujúcich. Za pomoci bankových čítačiek s tokenizačnou rovnicou, ktoré budú cez Bluetooth komunikovať s mobilným telefónom (OS Android), budú načítať nosiče cestovných lístkov a na základe tokenu potom voči informáciám z centrálnej databázy DZC zisťovať vlastníctvo platného cestovného dokladu cestujúceho. All in one riešenie je taktiež akceptované.

**3.5 MHD v rámci IDS**

Ambíciou IDS BBSK je postupne integrovať aj menšie lokálne systémy MHD a prípadne i MHD mesta Banská Bystrica. Tu sa počíta s odlišnou podobou fungovania platenia kartou. Cestujúci budú totiž môcť nastupovať všetkými dverami. Vo vozidle budú validátory, ktoré budú umožňovať opäť transakcie v dopravnom režime (bezkontaktné, bez zadávania PIN a tlačenia účtenky). Tieto transakcie bude realizovať sám cestujúci buď tým, že iba priloží kartu (defaultný check-in režim), prípadne si sám zvolí na validátore produkty a následne priloží kartu.

Zaistenie takýchto validátorov prebehne v budúcnosti. Acquirer sa zaviaže v rámci zmluvy na služby acquringu k honorovanej spolupráci na dodanie potrebného SW pre zaistenie transakcií v dopravnom režime a pre zaistenie tokenizácie pre bankové terminály integrované vo validátore. IDS bude pri tvorbe štandardov zapojenia MHD prihliadať na oprávnené technické pripomienky Acquirera.

1. **POŽIADAVKY NA SLUŽBY ACQUIRING**

**Súhrn požiadaviek na služby acquiring**

• Poskytovateľ služieb dodá SW pre vykonávanie tokenizácie čísel kariet v bankových termináloch

• Poskytovateľ služieb dodá služby a SW pre platenie v "dopravnom" režime v bankových termináloch

• Poskytovateľ služieb dodá služby a SW pre platenie v "retail" režime v bankových termináloch

• Poskytovateľ služieb dodá rozhranie pre DZC a umožní zabezpečenie inkasa peňažných prostriedkov z bankových kariet z transakcií v "dopravnom" režime (na základe prevedenie denného zúčtovania v DZC)

• Poskytovateľ služieb dodá prístup a funkčné webové administratívne rozhranie (tzv. "Merchant" rozhranie) pre zobrazenie a vyhľadávanie informácií o transakciách a možnosť riešenia reklamácií a storna platieb voči cestujúcim, prípadne môže byť táto funkcionalita vyriešená ako služba poskytovaná zo strany Poskytovateľa, napr. prostredníctvom helpdesku alebo technickej podpory

• Poskytovateľ dodá bankové terminály (spĺňajúce špecifikácie a počty podľa bodu 4.6) do regionálnych autobusov, predajných miest a pre využívanie revízormi IDS, ktoré budú vedieť vykonávať tokenizácia a platby v "dopravným" či "retail" režime

• Poskytovateľ služieb sa zaväzuje v budúcnosti na vyžiadanie do určenej lehoty dodať obslužný SW do bankových terminálov (ktoré budú súčasťou validátorov vo vozidlách MHD), ktorý umožní vykonávanie tokenizácie a transakcií v "dopravnom" režime

• Poskytovateľ služieb sa zaväzuje na požiadanie do určenej lehoty k úprave tokenizačného SW v prípade, ak by došlo k zmene parametrov tokenizačnej rovnice či jej rozšíreniu o ďalšiu rovnicu

Poskytovateľ služieb môže niektoré služby dodávať prostredníctvom subdodávateľov, ale v takom prípade ručí za dodanie týchto služieb.

**Podrobné požiadavky na služby acquiring**

Súčasťou zákazky sú nasledujúce činnosti:

1. Dodanie SW pre vykonávanie tokenizácie čísel kariet v bankových termináloch

2. Dodanie služieb a SW pre platenie v "dopravnom" režime v bankových termináloch

3. Dodanie služieb a SW pre platenie v "retail" režime v bankových termináloch

4. Dodanie rozhrania pre DZC na zabezpečenie inkasa peňazí z platieb v "dopravnom" režime platenia

5. Dodanie tzv. "Merchant" administrácie platieb s možnosťou riešenia reklamácií formou funkcionality alebo služby

6. Dodanie bankových terminálov vrátane obslužného SW (v počtoch podľa bodu 4.6)

7. Záväzok dodania SW pre tokenizáciu a "dopravný" režim platenia do bankových terminálov v MHD

8. Záväzok budúcich úprav tokenizačného SW

Vyššie uvedené body sú podrobne popísané v nasledujúcom texte.

**4.1 Dodanie SW pre vykonávanie tokenizácie čísel kariet v bankových termináloch**

Do bankových terminálov bude dodané SW riešenie, ktoré bude vykonávať tokenizáciu načítaných bankových kariet. Vykonanie tokenizácie musí byť možné volať buď samostatne, alebo sa bude automaticky vykonávať aj ako súčasť transakcie v "dopravnom" režime platenia. Bude sa rovno vytvárať jedna (produkčná) finálna verzia.

Detaily vykonávania tokenizácie sú popísané v kapitole 5.2.

**4.2 Dodanie služieb a SW pre platenie v "dopravnom" režime v bankových termináloch**

Do bankových terminálov bude Poskytovateľom služieb dodané SW riešenie, ktoré umožní realizáciu transakcií bezkontaktnými bankovými kartami v "dopravnom" režime platenia. Teda transakcia, pre ktorú sa nezadáva PIN a transakcia sa neschvaľuje ako v "retail" móde, ale slúži len ako preukazná informácia o transakcii pre neskoršie odložené zúčtovanie.

V prípade bankových terminálov (z bodu 4.6) pôjde o režim, kedy inicializáciu transakcie bude vyvolávať (cez Bluetooth) napojené riadiace zariadenie (tablet). Poskytovateľ tak musí dodať SW riešenie pre OS Android, ktoré umožní inicializáciu takejto transakcie na bankovom terminále (napríklad v prípade čítačiek firmy Ingenico by išlo o definíciu názvu obsiahnutej metódy, ktorá by sa mala volať voči čítačke za pomoci mPOS Service APK).

Súčasne Poskytovateľ služieb dodá funkčné rozhrania a jeho opis, kam sa budú odovzdávať súvisiace dáta o vykonanej transakcii do back-office acquirera (bankový terminál využívaný v "dopravnom" režime platenia nebude mať priame pripojenie k dátovej sieti). V rámci potvrdenia úspešnej transakcie je potrebné odovzdať:

- informáciu o výsledku (úspechu či neúspechu)

- tokenom načítané bankové karty (pozri tokenizačné riešenia)

- v prípade úspechu balík zašifrovaných dát, ktoré prijme riadiace zariadenie a odovzdá ho cez GSM dátové telekomunikačné služby na určené rozhranie do back-office acquirera

Poskytovateľ služieb sa zaväzuje k trvalej (99,9%) dostupnosti svojho back-office pre tieto účely.

**4.3 Dodanie služieb a SW pre platenie v "retail" režime v bankových termináloch**

Do bankových terminálov bude Poskytovateľom služieb dodané SW riešenie, ktoré umožní vykonávanie transakcií bankovými kartami v "retail" režime platenia. Teda klasických transakcií, ktoré sa budú rovno online schvaľovať a vysporiadavať. V prípade týchto transakcií bude možné zadávať PIN. Takéto bankové terminály budú mať zabudované riešenie pre priamy prenos dát voči back-office acquirera.

Poskytovateľ služieb musí dodať SW riešenie pre OS Android, ktoré umožní inicializáciu takejto transakcie na bankovom terminále = odovzdanie čiastky, meny a variabilného symbolu transakcie (napríklad v prípade čítačiek firmy Ingenico by išlo o "PayInvoice" metódu, ktorá by sa volala voči čítačke za pomoci mPOS Service APK). Dodané riešenie tiež umožní prijatie výsledku transakcie, vrátane prijatia informácií k tlači bankových účteniek pre zákazníka i predajcu.

Prostriedky z platieb v "retail" móde budú prevedené na bankový účet určený Zadávateľom.

Tieto čítačky budú obsahovať aj možnosť samostatného volania iba tokenizácie bankovej karty, bez vykonávania transakcie, kedy čítačka vráti iba token a maskované číslo karty.

**4.4 Dodanie rozhrania pre DZC na zabezpečenie inkasa peňazí z platieb v "dopravnom" režime platenia**

Poskytovateľ služieb dodá SW riešenie a potrebné rozhrania voči DZC. Toto riešenie bude:

- odovzdávať do DZC informácie o zaevidovaných transakciách v dopravnom režime (čas + zariadenie + token, pre možnosť kontroly, či o transakcii prišli informácie z validátora ako do banky, tak do DZC)

- dodať funkčný a procesne efektívny postup vyradenia karty Zákazníka z denylistu

- umožní DZC poslať požiadavku na vyradenie karty z denylistu (v prípade, že cestujúci uhradí dlhy voči integrátorovi za neúspešné sprocesovanie platby)

- umožní DZC zadať požiadavky na inkaso prostriedkov (vyčíslená v rámci denného zúčtovania) voči kartám použitým v rámci "dopravného" módu platenia

- vráti do DZC informácie o výsledku požadovaných inkás prostriedkov (vrátane kódu transakcie). Inkasované prostriedky z platieb v "dopravnom" móde budú po inkase bezodkladne prevádzané na bankový účet určený Zadávateľom.

Poskytovateľ služieb dodá dokumentáciu a popis vyššie spomínaných rozhraní a poskytne potrebnú súčinnosť, aby firma spravujúca DZC pre Zadávateľa mohla realizovať potrebné integrácie. Súčasťou dodávky budú ako produkčné, tak testovacie rozhrania jednotlivých funkcionalít.

Za "blacklist" sa považuje zoznam neplatných kariet, ktoré nemajú byť ďalej využívané na platenie. Za "denylist" sa považuje zoznam kariet, ktoré sú dočasne zakázané pre použitie v IDS BBSK.

Poskytovateľ služieb sa zaväzuje k trvalej (99,9%) dostupnosti svojho back-office pre tieto účely.

**4.5 Dodanie tzv. "Merchant" administrácie platieb s možnosťou riešenia reklamácií**

Poskytovateľ služieb dodá prístup a funkčné webové administratívne rozhranie (tzv. "Merchant" rozhranie), v ktorom bude možné zobrazovať a vyhľadávať informácie o transakciách (z "retail" režimu aj o inkasných platbách v dôsledku "dopravného" režimu platenia).

Toto rozhranie musí umožniť riešenie reklamácií a storno platieb voči bankovým kartám cestujúcich, a to buď priamo funkciou alebo službou (napr. Helpdesk).

Poskytovateľ služieb sa zaväzuje k trvalej (99,9%) dostupnosti svojho "merchant" rozhrania pre tieto účely.

**4.6 Dodanie bankových terminálov vrátane obslužného SW**

Poskytovateľ služieb dodá a prevedie do vlastníctva Zadávateľa nižšie uvedené počty bankových terminálov, ktoré budú spĺňať špecifikácie podľa bodu 5.1. Poskytovateľ dodá aj potrebnú dokumentáciu a obslužnú OS Android aplikáciu pre riadiace zariadenia.

**4.7 Záväzok dodania SW pre tokenizáciu a "dopravný" režim platenia do bankových terminálov v MHD**

Poskytovateľ služieb sa zaväzuje poskytnúť v budúcnosti súčinnosť a na vyžiadanie do zmluvne dohodnutej lehoty zabezpečiť dodanie obslužného SW do bankových terminálov, ktoré budú súčasťou validátorov vo vozidlách MHD. Toto riešenie umožní ako samostatné vykonávanie tokenizácia kariet, tak vykonávanie transakcií v "dopravnom" režime.

V prípade tokenizácia ide o rovnaké funkčné riešenie, ako v bode 4.1. Detaily vykonávanie tokenizácia sú popísané v kapitole 5.2.

**4.8 Záväzok budúcich úprav tokenizačného SW**

Poskytovateľ služieb sa zaväzuje poskytnúť v budúcnosti súčinnosť a na vyžiadanie do 6 mesiacov od vyzvania zaistiť úpravu a dodanie obslužného tokenizačného SW do všetkých bankových terminálov (ako terminály z bodu 4.6, tak pre terminály riešené v bode 4.7).

Ide o prípady, kedy by malo dôjsť k zmene tokenizačnej rovnice alebo oveľa pravdepodobnejšie na doplnenie tokenizačnej rovnice (pri prepájaní viacerých IDS systémov) o ďalšie výpočtovú rovnicu, a teda o výpočet ďalšieho tokenu a jeho odovzdávanie tak, ako je to popísané v kapitole 5.2.

**5 TECHNICKÉ PODROBNOSTI**

**5.1 Detaily o bankových termináloch (čítačkách)**

Predpokladá sa dodanie čítačiek, ktoré spĺňajú túto špecifikáciu:

- Možnosť stabilného Bluetooth pripojenia voči Android zariadeniu

- Malé kompaktné rozmery pre možnosť mobilného používania (napríklad revízorov)

- Možnosť čítanie 2D kódov

- Možnosť "field" výmeny batérie

- Možnosť volať čítačku v režime "GetToken", kedy čítačka iba načíta číslo karty a dátum platnosti a vypočíta a vráti token (a to aj pre neplatné karty) + maskované číslo karty. V tomto režime sa môžu čítať aj nebankové RFID karty, s ktorými možno komunikovať (rovnakou technickou formou) ako s bankovými kartami. Ak načítaná karta nebude banková, tak sa nebude počítať token, ale iba sa vráti UID (zistené číslo čipu) načítanej karty

- Možnosť volať v režime "PayInvoice", teda prevedenie bežnej platby v bežnom "retail" režime, kedy sa odovzdá suma a variabilný symbol transakcie a bude sa čakať na výsledok platby

- Možnosť volať v režime "PayTransport", teda vykonanie platby v "dopravnom" režime, kedy dôjde k vykonaniu len dopravnej transakcie (poznamenanie údajov o karte) a čítačka v prípade úspešnej realizácie dopravnej transakcie vráti token karty a zašifrovaný balík dát pre odovzdanie do back -office acquirera. V prípade neúspešnej transakcie (karta nie je platná alebo nastane iný problém), vráti token a informáciu o chybe

- Možnosť volať v režime "GetCode", kedy čítačka načíta svoju čítačkou 2D kódov príslušný kód a vráti ho

Očakáva sa, že dôjde k voľbe jedného typu čítačiek, ktoré sa budú používať ako vo vozidlách (v dopravnom móde), a druhého typu, ktorý bude na predajných miestach (retail mód), prípadne ich budú pri sebe nosiť revízori. Niektoré z čítačiek sa pravdepodobne budú používať len pre tokenizáciu, teda neboli by "nakľúčované" na spracovanie transakcií.

**5.2 Detaily k tokenizácii bankových kariet**

Tokenizačné riešenie musí spĺňať tieto požiadavky:

- tokenizácia sa týka čítačiek kariet, ktorá vie čítať bezkontaktné bankové karty (asociáciou VISA a Mastercad) a príslušný obslužný tokenizačný SW musí vedieť vykonávať tokenizácie nižšie popísaným spôsobom. Tokenizácia sa týka i nebankových kariet, ktoré zvládne takáto čítačka načítať. V ich prípade však nedochádza k výpočtu cez tokenizačnú rovnicu, ale vracia sa rovno identifikácia (číslo) načítaného čipu.

- Súčasťou informácií o načítanej bankovej karte je okrem tokenu aj maskované číslo karty (pozri nižšie).

- tokenizáciu musí byť možné vykonávať aj samostatne bez súvisiacej platobnej transakcie (napríklad pre zobrazenie a výpis informácií a v takom prípade môže dôjsť aj k načítaní napríklad neplatnej bankovej karty). Tokenizácia by vždy mala prebiehať ako paralelná súčasť na prekonanie platobnej transakcie kartou v "dopravnom" režime.

- Súčasťou dodávky tokenizácie v čítačkách musí byť i SW knižnica alebo iný SW, ktorý umožní odovzdanie a prijatie vypočítanej hodnoty tzv. "Tokenu" o realizovanom načítaní karty.

- Dodávateľ tokenizácie musí tiež zabezpečiť prevzatie a implementáciu kľúčov do tokenizačného algoritmu osobou a spôsobom zodpovedajúcim certifikácii podľa PCI DSS (podľa bezpečnostných štandardov kartových asociácií)

- Riešenie musí byť pripravené na to, že sa budú údaje tokenizovať podľa viacerých rôznych tokenizačných rovníc, teda, že sa môže vracať viac ako jeden token pre jednu bankovú kartu (oddelené znakom "pipe", pozri nižšie).

Podoba správy o tokenizácií z čítačky (platobného terminálu) je "token" a "panmasked". V prípade načítania bezkontaktných bankových kariet sa vracia "token" v podobe presne 64 znakov =

"TOKEN = 0123456789012345678901234567890123456789012345678901234567890123 & PANMASKED = 123456 \*\*\*\* 1234-MMDD |"

V prípade načítanie čipu nebankovej karty sa vracia =

"UID = 012345 ..." (max 64 znakov)

V prípade chyby sa vracia prázdny Token ( "TOKEN = |"). Na konci je vždy znak pipe "|", aby mohli nasledovať ďalšie tokeny ( "TOKEN = VALUE1 | TOKEN2 = VALUE2 | ...") v prípade, že by sa karty tokenizovali pomocou viacerých tokenizačných rovníc.

Tokenizácia má nasledovné parametre (klasifikácia podľa Tokenization Product Security Guidelines - viď PCI DSS):

- jednosmerný (Irreversible)

- autentizačný (Identifikujúca)

Predvolené uvažovaný tokenizačný algoritmus je **HMAC-SHA256:**

Kde:

• K je kľúč (secret key)

• m je číslo kreditnej karty + časová platnosť mmrr

• K 'je derivovaný tajný kľúč

• || je konkatenace

• ⊕ je operácia XOR

Parametre:

• H (Hash funkcia): SHA 256

• Secret key (double-length, hexadecimálne) 14 bytu

• derivované klic K '= K || [14-krát 0x00].

• m je reťazec s pevnou dĺžkou 23 alfanumerických znakov (tzn. 23 Bytov), ​​kódovanie ASCII. Preberajú sa iba znaky, ktoré sú viditeľné na karte. Ak znaky chýba, doplní sa nuly.

prevod z PAN bude nasledujúci:

Zdrojový PAN: 5101 3650 0030 1667, Platnosť: 10/17 (16 znakov)

Výsledné m = "51013650003016671017000"

Zdrojový PAN: 5101 3650 0030 1667 123, Platnosť: 10/17 (19 znakov)

Výsledné m = "51013650003016671231017"

Zdrojový PAN: 5101 3650 0030 16, Platnosť: 10/17 (14 znakov)

Výsledné m = "51013650003016101700000"

Príklady výpočtu HMAC s použitím 14 bytového kľúča 000102030405060708090A0B0C0D

KORDIS TEST # 1

KEY [14] = 000102030405060708090A0B0C0D

DATA [23] = 3531303133363530303033303136363731303137303030

HMAC-SHA256[32]=2dc02119b61e96a0b848982f47080367b3f9bf28c424229718542cb127ce13dc

KORDIS TEST # 2

KEY [14] = 000102030405060708090A0B0C0D

DATA [23] = 3531303133363530303033303136363731323331303137

HMAC-SHA256[32]=58624f895d53a826e71d033a99bf0e4505bddb7dd83c5982b412bb73f50d9c87

KORDIS TEST # 3

KEY [14] = 000102030405060708090A0B0C0D

DATA [23] = 3531303133363530303033303136313031373030303030

HMAC-SHA256 [32] = 3504b31bc8026c55d197cf6f6a0b0c3adf9789d9f7c989a6dd7f1a4fcb8eee98