



Príloha č. 18 – Kompatibilita Akceptačných zariadení s bezkontaktnými čipovými kartami používanými v rámci TTSK

1. Skratky a pojmy

1.1. Skratky

APDU – Application Protocol Data Unit (komunikačný protokol)

BČK – Bezkontaktná Čipová Karta

EP – Elektronická Peňaženka

PCL – Predplatný Cestovný Lístok

SAM – Secure Access Module (bezpečnostný hardvérový modul)

SNR – Serial Number (výrobné číslo karty)

1.2. Pojmy

Akceptačné zariadenie – zariadenie, ktoré umožňuje čítanie a zápis dát na BČK. Bezpečnostné požiadavky zariadenie zabezpečuje prostredníctvom SAM modulu.

Dodávateľ – vybraný dodávateľ, ktorý na základe osobitnej zmluvy s Trnavským samosprávnym krajom zabezpečuje integráciu Akceptačných zariadení Dopravcu s bezkontaktnými čipovými kartami TTSK.

SAM modul – bezpečnostný modul (secure cryptoprocessor), ktorý slúži ako bezpečné úložisko šifrovacích kľúčov.

2. Podmienky integrácie Dopravcu v TTSK

2.1. Za účelom integrácie Dopravcu v TTSK je Dopravca povinný si zabezpečiť na vlastné náklady Akceptačné zariadenia, ktoré budú kompatibilné s bezkontaktnými čipovými kartami používanými v TTSK.

2.2. Pre prispôsobenie Akceptačných zariadení cestujúcich Dopravcu tak, aby boli kompatibilné s bezkontaktnými čipovými kartami používanými v TTSK, zabezpečí Objednávateľ pre Dopravcu súčinnosť Dodávateľa.

2.3. Dopravca je však povinný splniť nasledovné povinnosti:

2.3.1. zabezpečiť si na vlastné náklady Akceptačné zariadenia, ktoré spĺňajú minimálne technické požiadavky stanovené v čl. 3 tejto Prílohy;

2.3.2. uzavrieť Dohodu o zachovaní obchodného tajomstva s Dodávateľom v súlade s návrhom uvedeným v Prílohe č. 19 Zmluvy, a riadne si plniť všetky povinnosti v zmysle uzavretej Dohody o zachovaní obchodného tajomstva;

2.3.3. poskytovať Dodávateľovi, prípadne Objednávateľovi akúkoľvek súčinnosť pri integrácii svojich Akceptačných zariadení do kartového systému TTSK, minimálne v rozsahu:

2.3.3.1. súčinnosti pri preberaní tzv. kartových štandardov definovaných od Dodávateľa, ktoré sú nevyhnutné na zabezpečenie kompatibility Akceptačných zariadení cestujúcich Dopravcu s bezkontaktnými čipovými kartami používanými v TTSK (ďalej len „Kartové štandardy“);

2.3.3.2. súčinnosti pri implementácii Kartových štandardov do Akceptačných zariadení cestujúcich Dopravcu;



- 2.3.3.3. súčinnosti pri implementácii prípadného rozvoja a úprav Kartových štandardov zo strany Objednávateľa alebo Dodávateľa do Akceptačných zariadení cestujúcich Dopravcu.
- 2.4. V prípade porušenia akejkoľvek z povinností Dopravcu uvedených v ods. 2.3. vyššie, ktoré bude brániť v zabezpečení akceptácie kariet používaných v PAD TTSK, je Dopravca povinný zaplatiť Objednávateľovi zmluvnú pokutu vo výške 30 000 eur za každé takéto porušenie povinností. Týmto nie je dotknutý nárok Objednávateľa na náhradu celej škody spôsobenej porušením týchto povinností Dopravcu.
- 2.5. Pre vylúčenie pochybností Dopravca berie na vedomie, že súčasťou poskytnutej súčinnosti zo strany Objednávateľa a Dodávateľa nie je:
- 2.5.1. samotná implementácia Kartových štandardov do Akceptačných zariadení cestujúcich Dopravcu, ktorú si Dopravca bude uhrádzať na vlastné náklady podľa dohody s jeho dodávateľom Akceptačných zariadení cestujúcich, resp. dodávateľom IT riešení do Akceptačných zariadení cestujúcich;
- 2.5.2. rozvoj, resp. úpravy Kartových štandardov realizované z iniciatívy Dopravcu, ktoré si Dopravca bude uhrádzať na vlastné náklady podľa jeho dohody s Dodávateľom;
- 2.5.3. inicializácia bezkontaktných čipových kariet používaných v TTSK, ktorá je tiež nevyhnutná na zabezpečenie kompatibility Akceptačných zariadení cestujúcich Dopravcu s bezkontaktnými čipovými kartami používanými v TTSK, ktorú si je Dopravca povinný uhrádzať na vlastné náklady tak, aby bezkontaktné čipové karty v súčasnosti používané v TTSK a v budúcnosti vydané boli kompatibilné s Akceptačnými zariadeniami Dopravcu.
- 2.6. Pre vylúčenie pochybností Zmluvné strany uvádzajú, že Objednávateľ pre Dopravcu zabezpečí tiež tzv. SAM moduly (hardvérové moduly určené pre Akceptačné zariadenia, ktoré umožňujú bezpečnú komunikáciu s bezkontaktnými čipovými kartami používanými v TTSK) a ktoré sú rovnako nevyhnutné na zabezpečenie kompatibility podľa tejto Prílohy, a to na základe osobitnej zmluvy s Dodávateľom. Tieto SAM moduly Objednávateľ bezodplatne poskytne Dopravcovi počas platnosti tejto Zmluvy v dostatočnom časovom predstihu do užívania. Implementáciu (inštaláciu) SAM modulov do Akceptačných zariadení cestujúcich si Dopravca zabezpečí na vlastné náklady. Dopravca je však povinný poskytovať na požiadanie Objednávateľa bez zbytočného odkladu a podľa jeho požiadaviek všetky údaje v rozsahu nevyhnutnom na identifikáciu priestorov (najmä dopravných prostriedkov), v ktorých budú SAM moduly nainštalované v Akceptačných zariadeniach umiestnené. Zároveň Dopravca je povinný umožniť Dodávateľovi správu SAM modulov, vrátane aktualizácie aplikácie a dát v SAM moduloch, a poskytnúť mu pre tento účel potrebnú súčinnosť. V prípade porušenia akejkoľvek povinnosti Dopravcu podľa tohto ods. 2.6. je Dopravca povinný zaplatiť Objednávateľovi zmluvnú pokutu vo výške 5 000 eur za každé jednotlivé porušenie povinnosti.
- 2.7. SAM moduly budú dodávané Dopravcovi výlučne na použitie pre Akceptačné zariadenia Dopravcu používané v rámci prímestskej autobusovej dopravy Trnavského samosprávneho kraja na základe výkonov, ktoré objednáva Objednávateľ v zmysle tejto Zmluvy.
- 2.8. Dopravca nie je oprávnený použiť SAM moduly na iný účel alebo v inom rozsahu ako je definované v odseku 2.7 tejto Prílohy. Porušenie povinnosti podľa predchádzajúcej vety Objednávateľ považuje za podstatné porušenie Zmluvy a Dopravca je povinný



zaplatiť Objednávateľovi zmluvnú pokutu vo výške 50 000 eur za každé takéto porušenie povinností.

2.9. Ďalšie dojednania týkajúce sa Kartových štandardov:

2.9.1. akékoľvek požiadavky Objednávateľa týkajúce sa rozvoja, úprav, zmien Kartových štandardov budú riešené osobitnou dohodou medzi Objednávateľom a Dodávateľom.

2.9.2. Kartové štandardy umožňujú prepojenie dopravných služieb medzi jednotlivými samosprávnymi krajinami v rámci celého územia SR. Za účelom zachovania previazanosti Kartových štandardov a teda zabráneniu ich diverzifikácii v rámci SR sa Objednávateľ aj Dopravca zaväzujú:

2.9.2.1. pri svojich požiadavkách na rozvoj Kartových štandardov podľa ods. 2.5.2. a ods. 2.9.1. tejto Prílohy rešpektovať kompatibilné prostredie BČK a Akceptačných zariadení v rámci územia SR, a

2.9.2.2. na každú žiadosť Dodávateľa umožniť implementáciu a zabezpečiť, aby aj dodávateľ Akceptačných zariadení Dopravcu umožnil implementáciu, takých úprav Akceptačných zariadení a systémov, ktoré vyplynú z rozvoja Kartových štandardov používaných v ostatných krajinách SR alebo v rámci celého územia SR, a za takým účelom poskytnúť všetku potrebnú súčinnosť. Dodávateľ je povinný o každej takej úprave informovať Objednávateľa aspoň 30 kalendárnych dní vopred.

3. Minimálne technické požiadavky

3.1. Požiadavky na Akceptačné zariadenia – Akceptačné zariadenie musí spĺňať nasledovné hardvérové požiadavky:

- súčasťou zariadenia musí byť dostatočne výkonný procesor, ktorý umožní v akceptačnom zariadení použiť štandardný operačný systém vhodný pre Akceptačné zariadenia v aktuálnej verzii
- súčasťou zariadenia musí byť dostatočne veľká pamäť pre uloženie zoznamu zablokovaných kariet (black list) a zoznamu produktov predaných cez internet (green list)
- súčasťou zariadenia musí byť čítačka bezkontaktných kariet, ktorá spĺňa požiadavky normy ISO/IEC 14443 so SAM slotom, ktorý spĺňa požiadavky normy ISO/IEC 7816
 - o akceptačné zariadenie umiestnené vo vozidle, v predpredaji alebo v automate – min 2 sloty pre SAM modul, form factor 2FF (Mini-SIM)
 - o prenosné Akceptačné zariadenie (revízorská čítačka) – min 1 slot pre SAM modul, form factor 2FF (Mini-SIM) alebo 1 slot pre SAM modul vo forme secure microSD karty
- súčasťou zariadenia musí byť 3G/4G modem pre prenos dát z/do Akceptačného zariadenia

3.2. Požiadavky na systémový softvér - Akceptačné zariadenie musí spĺňať nasledovné požiadavky na systémový softvér:

- štandardný operačný systém (linux, android, windows embedded) vhodný do Akceptačných zariadení
- ovládač pre čítačku BČK podľa normy ISO/IEC 14443
- ovládač pre SAM modul podľa normy ISO/IEC 7816
- ovládač pre 3G/4G modem



3.3. Požiadavky na aplikačný softvér - Akceptačné zariadenie musí spĺňať nasledovné požiadavky na aplikačný softvér:

3.3.1. všeobecné požiadavky:

- možnosť vzdialenej aktualizácie aplikácie pre Akceptačné zariadenie
- možnosť vzdialenej autorizácie SAM modulu
- možnosť vzdialenej aktualizácie aplikácie a dát v SAM module
- ak zariadenie obsahuje kombinovanú čítačku dopravných kariet a bankových kariet, možnosť definovať, ktorá čítačka má prednosť pri použití karty s dopravnou aj bankovou funkcionalitou

3.3.2. požiadavky na knižnicu pre prácu s BČK:

- karta Mifare Classic – natívne príkazy karty Mifare Classic podľa špecifikácie výrobcu média
- karta Mifare DESFire – natívne príkazy karty Mifare DESFire vrátane jej emulácie, zapuzdrené do formátu APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu média

3.3.3. požiadavky na knižnicu pre prácu so SAM modulom:

- karta JavaCard (SAM modul) – natívne príkazy vo formáte APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu karty
- secure microSD karta (SAM modul) – natívne príkazy vo formáte APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu karty

3.3.4. požiadavky na knižnicu pre 3G/4G komunikáciu s Akceptačným zariadením

- nahrávanie vstupných dát z Centrálného systému do Akceptačného zariadenia – konfiguračný súbor, blokovanie kariet, produkty predané cez internet (kartové udalosti)
- nahrávanie výstupných dát z Akceptačného zariadenia do Centrálného systému – informácie o vykonaných kartových transakciách a kartových udalostiach, informácie o stave Akceptačného zariadenia
- nahrávanie aktualizácií aplikačného softvéru – aktualizácia aplikácie pre Akceptačné zariadenie, aktualizácie SAM modulu
- vzdialená autorizácia SAM modulu

3.3.5. požiadavky na knižnicu pre spracovanie vstupných dát:

- práca so zoznamom zablokovaných kariet
- práca so zoznamom produktov predaných cez internet (kartové udalosti)

3.3.6. požiadavky na knižnicu pre generovanie výstupných dát

- Predajca, Číslo strojčeka, Číslo odpočtu, Číslo transakcie, Kód tarify, Zoznam a počet všetkých zón, Cena cestovného s DPH a bez DPH, Dátum a čas predaja, Spôsob predaja, Dátum začiatku platnosti, Dátum konca platnosti, Číslo nástupnej zastávky a číslo nástupnej zóny, Číslo výstupnej zastávky a číslo výstupnej zóny, Poradie PCL, Linka, Spoj, Tarifné kilometre, Časová platnosť, Typ platby, SNR karty, Emitent karty, Storno, Hodnota vkladu na EP, Počiatočný a konečný zostatok na BČK, Číslo operácie s EP, Emitent EP

3.4. Požiadavky na bezkontaktné čipové karty

- požiadavky na karty:
 - o v súlade so špecifikáciou:
https://www.nxp.com/docs/en/data-sheet/MF3DHx3_SDS.pdf
 - o minimálna veľkosť pamäte 4 kB
- výkonnostné požiadavky:



- Akceptačné zariadenie musí spĺňať nasledovné výkonnostné požiadavky na hardvér, systémový softvér a aplikačný softvér: celkový čas Testovacej transakcie s Mifare DESFire kartou musí byť menší ako 600 ms (mimo času, ktorý spotrebuje SAM modul)

3.5. Testovacie transakcie - pre overenie funkčnosti HW čítačky a SW komponent akceptačného zariadenia je možné použiť nasledovnú testovaciu transakciu:

- vytvorenie spojenia v súlade s ISO/IEC 14443-4
- výber aplikácie (Select)
- autentifikácia (Authenticate, prístupový kľúč v SAM module)
- čítanie súboru (Read Backup Data File, 96 B, 3DES MAC)
- čítanie súboru (Read Value File, 3DES MAC)
- zápis súboru (Write Backup Data File, 96 B, 3DES MAC)
- zápis súboru (Write Value File, 3DES MAC)
- potvrdenie transakcie (Commit)
- ukončenie spojenia v súlade s ISO/IEC 14443-4