

Technické požiadavky pre zapojenie dopravcu do Systému SDP

1. Skratky a pojmy

Skratky:

- **APDU** – Application Protocol Data Unit (komunikačný protokol)
- **BČK** – Bezkontaktná Čipová Karta
- **EP** – Elektronická Peňaženka
- **HSM** – Hardware Security Module
- **PCL** – Predplatný Cestovný Lístok (predplatný časový lístok)
- **SAM** – Secure Access Module (bezpečnostný hardvérový modul)
- **SDP** - Slovenský Dopravný Pas
- **SNR** – Serial Number (výrobné číslo karty)
- **ViK** - Virtuálna Karta

Pojmy:

- **Akceptačné zariadenie** – zariadenie, ktoré umožňuje čítanie a zápis dát na BČK. Bezpečnostné požiadavky zariadenie zabezpečuje prostredníctvom SAM modulu.
- **Dopravná karta** – BČK s dopravnou aplikáciou, ktorá slúži ako nosič elektronických cestovných lístkov a elektronickej peňaženky.
- **Elektronická peňaženka** - aplikácia v dopravnej karte, ktorá slúži na uloženie dopravného kreditu určeného na kúpu elektronických cestovných lístkov
- **HSM služba** – služba zúčtovacieho centra, ktorá umožní bezpečným spôsobom aktualizovať aplikáciu a dáta v SAM module.
- **SAM modul** – bezpečnostný modul (secure cryptoprocessor), ktorý slúži ako bezpečné úložisko šifrovacích kľúčov.
- **Virtuálna dopravná karta** – do mobilného zariadenia prenesená, digitalizovaná dopravná karta, uložená v Google aplikácii Peňaženka, ktorá predstavuje plnohodnotnú alternatívu k plastovej dopravnej karte.
- **Zúčtovacie centrum** – systém pre správu dopravných kariet a dátové zúčtovanie transakcií z elektronickej peňaženky.

2. 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 (blacklist) 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
 - akceptačné zariadenie umiestnené vo vozidle, v predpredaji alebo v automate – min 2 sloty pre SAM modul, form factor 2FF (Mini-SIM)
 - 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 min. 3G/4G modem pre prenos dát z/do Akceptačného zariadenia

3. 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 GSM modem

4. Požiadavky na aplikačný softvér

4.1. Všeobecné požiadavky

Akceptačné zariadenie musí spĺňať nasledovné požiadavky na aplikačný softvér:

- 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

4.2. Požiadavky na knižnicu pre prácu s BČK a ViK

Knižnica pre prácu s BČK a ViK musí spĺňať nasledovné požiadavky:

- karta Mifare DESFire – natívne príkazy karty Mifare DESFire, zapuzdrené do formátu APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu BČK
- virtuálna karta Mifare2GO - natívne príkazy emulovanej karty Mifare DESFire, zapuzdrené do formátu APDU správ podľa normy ISO/IEC 7816-4

4.3. Požiadavky na knižnicu pre prácu so SAM modulom

Knižnica pre prácu so SAM modulom musí spĺňať nasledovné požiadavky:

- 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
- HSM služba – transparentný prenos dát medzi HSM a SAM modulom

4.4. Požiadavky na knižnicu pre komunikáciu s Akceptačným zariadením

Knižnica pre prácu so SAM modulom musí spĺňať nasledovné požiadavky:

- nahrávanie vstupných dát zo Zúčtovacieho centra do Akceptačného zariadenia – konfiguračný súbor, blokové karty, produkty predané cez internet (kartové udalosti)
- nahrávanie výstupných dát z Akceptačného zariadenia do Zúčtovacieho centra – 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

4.5. Požiadavky na knižnicu pre spracovanie vstupných dát:

Knižnica pre spracovanie vstupných dát musí spĺňať nasledovné požiadavky:

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

4.6. Požiadavky na knižnicu pre generovanie výstupných dát pre zúčtovanie transakcií s EP

Dátová veta výstupných dát musí obsahovať (v závislosti od vykonaných transakciách) nasledovné položky:

- Predajca, Číslo zariadenia, 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

5. Požiadavky na bezkontaktné čipové karty

Čipové karty musia spĺňať nasledovné technické parametre:

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

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)

6. Procesné požiadavky

Spracovanie udalostí:

- akceptácia Dopravnej karty na základe kontroly podľa zoznamu akceptovaných dopravcov zo Zúčtovacieho centra

7. Integračné testy

Požiadavky na vykonanie integračných (akceptačných) testov:

- vzorka z každého typu Akceptačného zariadenia, ktorý bude pracovať s Dopravnou kartou

Požiadavky na priebeh integračných (akceptačných) testov:

- vykonanie transakcie s každým typom karty
 - overenie rýchlosti transakcie
- vykonanie transakcie s každým typom Akceptačného zariadenia
- spracovanie a overenie štatistiky z každého typu Akceptačného zariadenia
- otestovanie vykonávania kartových udalostí každého typu Akceptačného zariadenia

Architektúra systému vzájomnej akceptácie

