Kartový štandard IDS Východ – Minimálne technické požiadavky

1. Účel dokumentu

Dokument opisuje Minimálne technické požiadavky, ktoré musia spĺňať Akceptačné zariadenia tarifno-informačného systému Dopravcu zapojeného do systému IDS Východ, pre akceptáciu elektronických cestovných lístkov na Dopravných kartách.

2. 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)

3. Pojmy

Akceptačné zariadenie – zariadenie, ktoré umožňuje čítanie a zápis dát na BČK. Bezpečnostné požiadavky zariadenie zabezpečuje prostredníctvom SAM modulu.
SAM modul – bezpečnostný modul (secure cryptoprocessor), ktorý slúži ako bezpečné úložisko šifrovacích kľúčov.

4. Požiadavky na hardvér

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
    - 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 3G/4G modem pre prenos dát z/do Akceptačného zariadenia

5. 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

6. Požiadavky na aplikačný softvér

Akceptačné zariadenie musí spĺňať nasledovné požiadavky na aplikačný softvér:

- 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
- 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
- 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
- požiadavky na knižnicu pre 3G/4G komunikáciu s Akceptačným zariadením
    - nahrávanie vstupných dát z Centrálneho systému do Akceptačného zariadenia – konfiguračný súbor, blokované karty, produkty predané cez internet (kartové udalosti)
    - nahrávanie výstupných dát z Akceptačného zariadenia do Centrálneho 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
- požiadavky na knižnicu pre spracovanie vstupných dát
    - práca so zoznamom zablokovaných kariet
    - práca so zoznamom produktov predaných cez internet (kartové udalosti)
- 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

7. Požiadavky na BČK

Požiadavky na BČK

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

Požiadavky na konfiguráciu karty

- inicializáciu kariet zabezpečí IDS Východ

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)

8. Testovacia transakcia

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