**Príloha č. 1 –** Opis predmetu zákazky, tejto Výzvy

„Bezkontaktné čipové karty \_CP 19/2024“

**ŠPECIFIKÁCIA TOVARU A JEDNOTKOVÉ CENY**

Predmetom obstarávania je dodanie predpokladaného množstva 100.000 ks BČK typu MIFIRE DESFIRE EV1, ktoré budú slúžiť ako nosič predplatných cestovných lístkov a elektronickej peňaženky, s pamäťou a možnosťou zápisu, elektronicky inicializované pre potreby DPB, a.s. v rámci IDS BK, plne dispozičné (kompatibilné), špeciálne kryptované, založené na otvorených štandardoch pre bezdrôtové rozhranie a pre šifrovacie metódy, s jedinečným sériovým číslom (SNR). Multifunkčné použitie BČK v dopravných systémoch DPB, a.s. v súlade s požiadavkami na rýchly a vysoko bezpečný prenos dát do existujúcej infraštruktúry.

Dodávateľ sa zároveň zaväzuje udeliť licenciu na kľúč (kryptovací).

Dodávateľ sa zaväzuje dodávať bezkontaktné čipové karty typu MIFIRE DESFIRE EV1, s jednostrannou ofsetovou potlačou 4/0 CMYK podľa vizuálu potlače predloženej Objednávateľom, vrátane dopravy a poistenia, ktoré slúžia ako nosič predplatných cestovných lístkov a elektronickej peňaženky, pričom ich Objednávateľ môže využiť aj na ďalšie systémy ovládané kartou – prístupový, dochádzkový, stravovací a pod.

Minimálne objednané množstvo: 2 500 kusov.

Vizuál potlače záväzný pre 10 000 kusov BČK.Kľúčové vlastnosti MIFARE DESFire EV1:

* plne kompatibilný s ISO 14443A 1-4
* 2/4/8 Kbytes EEPROM s rýchlym programovaním
* bezpečný, vysokorýchlostný príkazový súbor
* flexibilná súborová štruktúra
* jedinečné seriálové 7 bytové číslo (ISO kaskádová úroveň 2)
* integrita dát: CRC a načítavanie bitov na fyzickej vrstve
* otvorený DES/2K3DES/3K3DES/AES kryptovací algoritmus ako súčasť hardwaru
* dostupnosť v moduloch MOA4 alebo 8 “ (pílený alebo vytlačený wafer – podľa typu technológie)

Dodacia lehota: 30 dní odo dňa objednávky.

Miesto dodania: Olejkárska 1, 814 52 Bratislava, Oddelenie tarifných služieb.

Podrobné požadované technické parametre sú uvedené nižšie v bode č. 1 a v bode č. 2.

1. **Čipová karta Mifare DESFire EV1**

Bezkontaktná čipová karta MF3 IC D41 (obchodný názov MIFARE DESFire EV1 4 kB) je určená pre poskytovateľov, ktorí chcú kombinovať a podporovať viac aplikácií na jednej bezkontaktnej inteligentnej karte. Je plne v súlade s požiadavky na rýchly a bezpečný prenos údajov, flexibilnú organizáciu pamäte a interoperabilitu s existujúcou infraštruktúrou.

Bezkontaktná čipová karta MIFARE DESFire EV1 je vhodná pre rýchle a bezpečné riešenia v oblasti

* moderná verejná doprava
* prístupové systémy
* verejná správa
* mikroplatby v uzavretom platobnom systéme
* vernostné systémy

Základné vlastnosti karty MIFARE DESFire EV1

* Pamäť
  + veľkosť EEPROM [Byte]
    - MF3 IC D41 4096
  + počet zápisových cyklov 500 000
  + doba uchovania dát [roky] 10
* Organizácia pamäte
  + organizácia pamäte flexibilný súborový systém
  + počet aplikácií max 28
  + počet súborov v aplikácii max 32
  + typy súborov štandardný, záložný, hodnotový, lineárny, cyklický
  + identifikátor aplikácie 3 byte AID
* RF interface
  + prenos dát bezkontaktný prenos
  + napájanie RF pole antény čítačky (bez batérie)
  + protokol ISO/IEC 14443A-4
  + frekvencia [MHz] 13,56
  + komunikačná rýchlosť [kbit/s] 106, 212, 424, 848
  + komunikačná vzdialenosť [mm] do 100
* Práca s dátami
  + autentifikácia vzájomná autentifikácia
  + antikolízny mechanizmus áno
  + integrita dát 16/32 bit CRC na fyzickej vrstve
  + protokol ISO/IEC 7816-3 APDU
  + príkazy ISO/IEC 7816-4
  + transakčnosť operácii s dátami áno
* Bezpečnosť
  + jedinečné výrobné číslo [Byte] 7
  + možnosť použiť náhodné ID áno
  + vzájomná trojcestná autentifikácia áno
  + autentifikácia podľa ISO/IEC 7816-4 áno
  + generátor náhodných čísiel áno
  + prístupové kľúče 1 master kľúč karty

max 14 kľúčov pre aplikáciu

* + prístupové práva nastaviteľné pre každý súbor
  + DES/2K3DES/3K3DES HW koprocesor
  + AES HW koprocesor
* Certifikácia
  + certifikácia CC EAL 4+

1. **Inicializácia čipovej karty Mifare DESFire EV1**

**Inicializácia kariet** je vytvorenie aplikácií na čipovej karte (vrátane dopravnej aplikácie) a ich zabezpečenie proti zneužitiu, proces nastavenia počiatočných hodnôt a otestovanie funkčnosti čipovej karty. Ide o proces nevyhnutný pre elektronickú autorizáciu držiteľa karty a pre použitie čipových kariet v akceptačných zariadeniach vydavateľa karty a dopravcu.

**Kľúč** je dátová štruktúra (dáta a algoritmus), ktorá slúži na zabezpečenie elektronických dát na karte voči neoprávnenému použitiu. Kľúče sa na kartu nahrávajú v procese inicializácie kariet.

**Prístupový kľúč** je kľúč, ktorý umožňuje autentifikáciu pre čítanie a/alebo zápis dát na kartu.

**Šifrovací kľúč** je kľúč, ktorý umožňuje šifrovať dáta, ktoré sa zapisujú na kartu a dešifrovať dáta, ktoré sa vyčítajú z karty.

**Podpisovací kľúč** je kľúč, ktorý umožňuje podpísať dáta, ktoré sa zapisujú na kartu a overiť podpis dát, ktoré sa vyčítajú z karty.

**Kryptografická operácia** je operácia šifrovania, dešifrovania, autentifikácia, podpisovanie, overovanie podpisu, generovanie kľúčov a pod.

**Hardvérový bezpečnostný modul** (Hardware Security Module, HSM) je zariadenie, ktoré slúži ako bezpečné úložisko prístupových, šifrovacích a podpisovacích kľúčov. Bezpečné úložisko kľúčov znamená, že tieto kľúče nesmú opustiť bezpečné úložisko v otvorenom tvare. Všetky kryptografické operácie sa musia vykonávať vnútri HSM. Na tento účel HSM obsahuje špecializované, dostatočne výkonné hardvérové kryptoprocesory ako aj ďalšie komponenty, zabezpečujúce toto úložisko dát.

**Technické požiadavky na inicializáciu dopravných kariet:**

* inicializácia dopravnej karty musí byť realizovaná takým spôsobom, aby všetky kryptografické operácie vykonávané počas inicializácie kariet spĺňali požiadavky informačnej bezpečnosti, t.j. takým spôsobom, aby žiadny prístupový, šifrovací alebo podpisovací kľúč nikdy neopustil hardvérové prostredie bezpečného úložiska kľúčov (HSM) v otvorenom tvare
* technické riešenie inicializačného pracoviska na platforme HSM je certifikované nezávislou certifikačnou autoritou

**Inicializovaná dopravná karta musí spĺňať nasledovné požiadavky:**

* multi-aplikačné použitie čipových kariet v dopravných systémoch objednávateľa v súlade s požiadavkami na rýchly a vysoko bezpečný prenos dát, flexibilnú organizáciu pamäte a interoperabilitu (funkčnú spoluprácu) s existujúcou infraštruktúrou
* plná kompatibilita s doteraz emitovanými bezkontaktnými čipovými kartami, ktoré slúžia ako nosič predplatných cestovných lístkov a jednorazových cestovných lístkov objednávateľa