

A. Opis predmetu zákazky - Bezkontaktné čipové karty (BČK)

- 1) Predmetom obstarávania je dodanie 45.000 kusov BČK počas doby platnosti zmluvy ktorá predstavuje 36 mesiacov, užívateľsky nových, nepoužívaných, naformátovaných a preskúšaných bezkontaktných čipových kariet typu MIFARE DESFIRE EV1, ktoré budú slúžiť ako nosič predplatných cestovných lístkov a elektronickej peňaženky, s pamäťou a možnosťou zápisu, plne dispozičné (kompatibilné) s inicializáciou, ktorú zabezpečí následne Objednávateľ, špeciálne kryptované, založené na otvorených štandardoch pre bezdrôtové rozhranie a pre šifrovacie metódy, s jedinečným sériovým číslom (SNR). Samotná inicializácia kariet nie je predmetom obstarania, Inicializáciu kariet zaistí Objednávateľ. Objednávateľ využije BČK multifunkčne v dopravných systémoch Objednávateľa v súlade s požiadavkami na rýchly a zabezpečený prenos dát do existujúcej infraštruktúry Objednávateľa. Dĺžka platnosti karty je 5 rokov.
- 2) Dodávateľ sa zaväzuje dodávať nové, nepoužité biele bezkontaktné čipové karty (grafické vyhotovenie čipovej karty - biele BČK bez potlače 0/0) typu MIFARE DESFIRE EV1, vrátane dopravy, 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. Z tohto dôvodu budú karty dodané s transportnými kľúčmi.
- 3) Kľúčové vlastnosti MIFARE DESFire EV1:
 - plne kompatibilná s ISO 14443A 1- 4
 - min. 4 Kbytes EEPROM s rýchlym programovaním
 - bezpečný, vysokorýchlostný príkazový súbor
 - flexibilná súborová štruktúra
 - Formát karty 85,60 x 53,98 x 0,76 mm.
 - antikolízna
 - jedinečné sériové 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

B. TECHNICKÁ ŠPECIFIKÁCIA TOVARU BČK:

- 1) Bezkontaktná čipová karta Mifare DESFire EV1
- 2) 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 požiadavkami na rýchly a bezpečný prenos údajov, flexibilnú organizáciu pamäte a interoperabilitu s existujúcou infraštruktúrou.

3) Bezkontaktná čipová karta MIFARE DESFire EV1 musí byť vhodná pre rýchle a bezpečné riešenia v oblasti:

- verejná doprava
- prístupové systémy
- verejná správa, štátna správa
- mikropłatby v uzavretom platobnom systéme - peňaženka
- vernostné systémy pre užívateľov

4) Základné vlastnosti karty MIFARE DESFire EV1:

● **Pamäť :**

- veľkosť ■ EEPROM [Byte] ■ MF3 IC D41 4096
- min. 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 čísel áno
- prístupové kľúče 1 master kľúč karty max 14 kľúčov pre aplikáciu
- prístupové práva nastaviteľné pre každý súbor
- DES/2K3DES/3K3DES HW koprocessor
- AES HW koprocessor

● **Certifikácia**

- certifikácia CC EAL 4+

C. Dodanie Bezkontaktných čipových kariet:

- 1) Objednávateľ požaduje dodanie kariet vrátane dopravy na náklady Dodávateľa na miesto určenia v rámci SR. Presné miesto určenia upresní Objednávateľ pri každej jednotlivej, čiastkovej objednávke.
- 2) Doba dodania Čipových kariet môže byť maximálne do 10 kalendárnych dní od termínu potvrdenia objednávky dodávateľom čipovej karty. Zmena termínu dodania môže byť Zmluvnými stranami osobitne dojednaná vzhľadom na termíny výroby, dopravy a komplexnú logistiku dodania BČK.
- 3) Dodanie Čipových kariet Zmluvné strany potvrdia v písomnom dodacom protokole. Súčasťou dodacieho protokolu musí byť:
 - a) určenie počtu dodaných Čipových kariet a rozdiel oproti objednávke;
 - b) vady Čipových kariet zistené pri preberaní;
 - c) dátum a miesto vystavenia protokolu;
 - d) podpis oprávneného zástupcu Objednávateľa;
 - e) Objednávateľ je povinný nedostatky dodania týkajúce sa počtu Čipových kariet uplatniť u Dodávateľa bez zbytočného odkladu po prevzatí Čipových kariet.
 - f) Minimálny počet BČK pri jednej objednávke je 5.000 kusov.
 - g) Po vzájomnej dohode medzi DPMK, a.s. a Dodávateľom je Dodávateľ oprávnený dodať objednané Čipové karty aj v čiastkových plneniach.

D. Testovanie VZORKY Bezkontaktných čipových kariet:

V prípade, ak Dodávateľ bude chcieť použiť možnosti dodať Čipové karty typu MIFARE DESfire ev1, bližšie špecifikované v Prílohe č. 1 - Technická špecifikácia a ich inú

modernejšiu verziu, je tak možné až po otestovaní funkčnosti s inicializovanou Dopravnou aplikáciou. Postup testovania VZORKY si Dodávateľ vopred dohodne mailom s osobou zodpovednou za plnenie zmluvy.