Príloha č. 1 - Podrobná špecifikácia

Predmetom zákazky je dodávka inicializovaných bezkontaktných čipových kariet s pamäťou a možnosťou zápisu pre využitie karty ako preukazu študenta a zamestnanca v automatizovanom identifikačnom systéme Univerzity Komenského v Bratislave, ako aj pre použitie v externých aplikáciách so súvisiacimi službami.

Čipová karta musí spĺňať nasledovné technické parametre:

- odolnosť voči kopírovaniu, mechanickému poškodeniu a opotrebovaniu
- stabilita a bezpečnosť záznamu, pričom minimálna trvanlivosť zachovania obsahu identifikačnej informácie musí byť pri dennom viacnásobnom používaní:
    - pre študentov najmenej 5 rokov
    - pre zamestnanca najmenej 10 rokov
- spoľahlivosť prenosu informácie

Inicializované bezkontaktné čipové karty majú:

- formátovaný čip MIFARE Desfire EV1 8kB
- čip predisponovaný pre všetky aktívne interné a externé aplikácie
- v čipe nahranú funkčnú aplikáciu Salto spoločnosti EVVA
- implementované príslušné príznaky a kľúče

Inicializované čipové karty umožňujú nielen čítanie z pamäte karty, ale aj zapisovanie a validáciu údajov a funkcií.

Inicializované čipové karty sú použiteľné ako preukaz študentov, učiteľov a ostatných zamestnancov verejného obstarávateľa (ďalej len „používatelia preukazov“). Preukaz študentov študujúcich dennou formou štúdia (ďalej len „denní študenti“) je zároveň použiteľný ako medzinárodný preukaz ISIC. Licenčne chránená vizuálna podoba ISIC a jej cena je predmetom osobitého zmluvného vzťahu medzi verejným obstarávateľom a CKM SYTS, ktorý je t. č. výhradným zástupcom externého grafického dizajnu pre Slovenskú republiku.

Preukaz študenta je vyhotovený v súlade s aktuálne platným “Metodickým usmernením č. 16/2014 o použití, štruktúre údajov a technickom vyhotovení preukazu študenta“ vydaného rozhodnutím Ministerstva školstva, vedy, výskumu a športu Slovenskej repibliky (ďalej len „usmernenie“) z 1. 9. 2014.

Preukaz je realizovaný na báze bezkontaktnej čipovej karty zodpovedajúcej štandardu MIFARE MF1 IC S70 alebo Mifare DESfire EV1, ktorý spĺňa normu ISO/IEC 14443A, časti 1 až 3.
Inicializované čipové karty umožňujú pri akceptovaní ich technických možností použitie v ďalších oblastiach, ktorých realizáciu verejný obstarávateľ predpokladá, sú to napr.:

- stravovací systém;
- platené služby (elektronická peňaženka);
- riadená automatická reprografická služba;
- technicky kompatibilné automaty na pôde UK;
- preukazom riadený prístup k chráneným priestorom.

Služby súvisiace s dodávkou inicializovaných čipových kariet:

- telekomunikačné skúšky s vyradením chybných kariet;
- nastavenie MAD adresára (definícia postavenia aplikácií na karte);
- správa MAD adresára (správa aplikácií s predeľovaním sektorov vrátane pridelenia kľúčov aplikáciám);
- formátovanie čipu (prekľúčovanie všetkých relevantných sektorov a ich následná predispozícia);
- príprava externých funkcionalít – formátovanie dotknutého priestoru;

- príprava pamäte čipu na použitie externých funkcionalít (bez nahratia akýchkoľvek osobných údajov);
- testovanie implementovaných plnení na karte;
- konečná skúška karty

Grafická vizualizácia karty v sebe obsahuje:

- zabezpečenie príslušnej obojstrannej farebnej potlače pre účely použitia karty ako medzinárodného preukazu denného študenta – ISIC, hologramizáciu karty hologramom ISIC. Obsah, forma a spôsob potlače musí byť v legislatívne upravenej podobe podľa ISIC Association, a to ako medzinárodný identifikačný preukaz denného študenta – ISIC. Umiestnenie čipu na karte s vizuálom ISIC je ľavý horný kvadrant karty – pri pohľade z lícnej časti príslušného vizuálu.

Inicializované bezkontaktné čipové karty

Funkcia		
Preukaz študenta VŠ		
Preukaz zamestnanca		
Technické vlastnosti	**Jednotka**	**Počet**
Kapacita pamäte čipu	kB	8
Mifare DESFire EV1 8kB inic. s vizuálom ISIC	ks	6.100
Mifare DESFire EV1 8kB inic. bez potlače	ks	8.500
Technické vlastnosti	**Hodnota / charakteristika**	
Typ karty	Mifare DESFire EV1 8kB	
Formát karty	podľa normy ISO 7816	
Typ pamäte	s možnosťou zápisu	
Inicializácia čipu	podľa Metodického usmernenia MŠVVaŠ SR č. 16/2014	
Funkcia čipu 1	pripravený pre dopravné systémy dopravcov združených v systéme TransCard	
Funkcia čipu 2	administrácia a správa kľúčov	
Funkcia čipu 3	pripravený pre knižnice na Slovensku (tzv. knižničný pas)	
Funkcia čipu 4	nahraná funkčnú aplikáciu Salto spoločnosti EVVA	
Vizuál karty študenta	medzinárodnej študentskej karty ISIC schválený pre príslušný akademický rok združením CKM SYTS http://ckmsyts.sk/	
Potlač karty študenta	bez aktuálnej validácie karty	
Vizuál a potlač karty zamestnanca	biela, bez potlače	

Technická špecifikácia tovaru

Čipová karta Mifare DESFire
1 FUNKCIE

1.1 RF (Radio frequency) rozhranie ISO/IEC 14443 typ A

- bezkontaktný prenos dát a napájanie z RF poľa (nie sú potrebné batérie)
- pracovná vzdialenosť: až do 100 mm (závisí od antény)
- pracovná frekvencia: 13,56 MHz
- rýchly prenos dát: 106 kbit/s, 212 kbit/s, 424 kbit/s
- vysoká integrita dát: 4 Byte MAC, 16 Bit CRC, parita, bit kódovanie, bit počítanie
- pravá deterministická antikolízia
- 7 bajtový jedinečný identifikátor (kaskádový level 2 podľa ISO/IEC 14443-3)
- používa ISO/IEC 14443-4 prenosový protokol

1.2 ISO/IEC 7816 kompatibilita (iba pre softvérovú verziu 0.6 a vyššiu)

- podporuje 7816-4 APDU štruktúru správ
- podporuje 7816-4 INS kód A4 VÝBER APLIKÁCIE
- podporuje 7816-4 INS kód A4 VÝBER ADRESÁRA
- podporuje 7816-4 INS kód A4 VÝBER SÚBORU
- podporuje 7816-4 INS kód B0 ČÍTAŤ BINÁRNE
- podporuje 7816-4 INS kód D6 AKTUALIZOVAŤ BINÁRNE

1.3 Nevolatilná pamäť

- 4 kbyte NV-pamäť
- rýchlosť zápisu NV-pamäte 2ms (1 ms mazanie, 1 ms program)
- uchovanie dát 10 rokov
- životnosť 100 000 zápisov

1.4 NV - organizácia pamäte

- flexibilný súborový systém
- súčasne až 28 aplikácií na jednom PICC
- až 16 súborov v každej aplikácii

1.5 Bezpečnosť

- jedinečné 7 bytové sériové číslo pre každé zariadenie
- súčasné trojité overovanie – autentifikácia
- hardvérové DES/3DES dátové šifrovanie na RF-kanály s ochranou proti prepísaniu v prípade zneužitia
- pravosť dát od 4 Byte MAC a identifikácia na aplikačnej úrovni

2 VŠEOBECNÝ POPIS

Philips vyvinul MIFARE DESFire (MF3 IC D40) na použitie blízkeho spájania zariadení (PCDs) podľa ISO/IEC 14443 typ A. Prenosový protokol vyhovuje časti ISO/IEC 14443-4. MF3 IC D40 je primárne navrhnutá pre bezpečné bezkontaktné transportné (prenosové) aplikácie a s nimi spojené vernostné programy.

2.1 Bezkontaktný prenos dát a bezkontaktné napájanie

V MIFARE systéme je MF3 IC D40 spojená s cievkou, ktorá pozostáva z niekoľkých otáčok, ktoré sú vsadené do štandardov ISO pre čipové karty (smart karty). Žiadne batérie nepotrebuje. Keď je karta v blízkosti PCD antény, vysokorýchlostné RF komunikačné rozhranie dovoľuje prenos dát rýchlosťou až do 424 kbit/s.

2.2 Typy dodávok

- vyrážané na 8 palcový wafer, pílené na FFC, 150 um hrúbka
- zlatom poznačené sú vyrážané do 8 palcového wafera, pílené na FFC (film frame carrier), 150 um hrúbka
- bezkontaktný modul čipovej karty MOA4

2.3 Antikolízia

Inteligentný antikolízny mechanizmus umožňuje viac ako jeden PICC v poli súčasne. Antikolízny algoritmus vyberá každý PICC individuálne a zabezpečí, že vykonanie transakcie s vybraným PICC je vykonané správne bez poškodenia dát bez vplyvu na ostatné ostatné PICC v poli.

2.4 UID/sériové číslo UID – Unique identification

Jedinečné 7 bajtové sériové číslo (UID) je naprogramované do zamknutej časti NV-pamäte, ktorá jej rezervovaná pre výrobcu. Vzhľadom k bezpečnosti a systémovým požiadavkám sú tieto bajty zabezpečené proti prepísaniu hneď po naprogramovaní u výrobcu počas výroby. Podľa ISO/IEC 14443-

3 prvá antikolízna slučka sa vráti na označený stupeň 0x88 a prvé 3 bajty UID – jedinečného označenia, SN0 na SN2 a BCC.
SN0 ponecháva výrobca ID pre Philips (04h) podľa ISO/IEC 1444-3 a podľa ISO/IEC 7816-6 AM1.

2.5 Organizácia pamäte

4 kilobajtová nevolatilná pamäť je riadená (organizovaná) použitím flexibilného súborového systému. Tento súborový systém umožňuje maximálne 28 rozdielnych aplikácií na jednom PICC. Každá aplikácia môže použiť až 16 súborov. Každá aplikácia je zastúpená 3 bajtovým AID (aplikačným identifikátorom). Je podporovaných 5 rôznych typov súborov, viď bod 2.6 Každý súbor môže byť vytvorený buď na PICC inicializácii (výroba kariet / potlač kariet), na PICC personalizácii (výdajný automat) alebo v poli.
Ak sa súbor alebo aplikácia stane zastaranou v operácii, môže byť natrvalo zrušená.
Príkazy, ktoré majú vplyv na štruktúru súborov samých seba (napr. vytváranie alebo mazanie aplikácií, zmena kľúčov ...) aktivujú rollback mechanizmus, ktorý celú štruktúru súborov pred poškodením.
Pokiaľ je rollback nevyhnutný, je vykonaný bez akéhokoľvek zásahu užívateľa.
Aby sa zabezpečila integrita dát na každej aplikačnej úrovni, bola implementovaná automatická záloha prenosu pre všetky typy súborov.
Je možné zmiešať súbory s a bez zálohy v rámci jednej aplikácie, kde záloha bude možná iba pre súbory 0 ..7, súbory 8 ..15 nemajú (neobsahujú) funkciu zálohovacieho mechanizmu.

2.6 Dostupné typy súborov

- Súbory v aplikácii môžu byť tieto typy:
- Štandardné dátové súbory
- Zálohové dátové súbory
- Cenné súbory so zálohou
- Lineárne nahrávacie súbory so zálohou
- Cyklické nahrávacie súbory so zálohou