VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

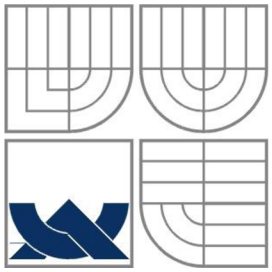
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

KONFIGURACE A PERSONALIZACE BEZKONTAKTNÍCH ČIPOVÝCH KARET

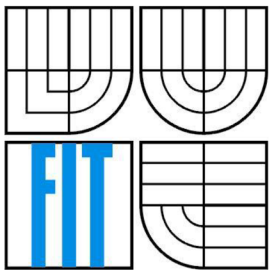
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE PETER ALTAMIRANO
AUTHOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

KONFIGURACE A PERSONALIZACE BEZKONTAKTNÍCH KARET

CONFIGURATION AND PERSONALIZATION OF CONTACTLESS SMART CARDS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETER ALTAMIRANO

VEDOUCÍ PRÁCE
SUPERVISOR

DOC. DR. ING. PETR HANÁČEK

BRNO 2010

Abstrakt

Tato bakalářské práce se zabývá problematikou bezkontaktních čipových karet. Popisuje principy komunikace, konfigurace a personalizace těchto karet. V práci je popsán návrh a implementace systému, který se skládá z aplikace pro konfiguraci a personalizaci bezkontaktních čipových karet a aplikace pro autentizaci osob při vstupu do systému. Na konci je vyhodnocena implementace řešení, jsou popsány další možnosti vývoje aplikací a v závěru je zhodnocena práce jako celek.

Abstract

This bachelor‘s thesis considers problematics of contactless smart cards. It describes principles of communication, configuration and personalization of contactless smart cards. In the thesis is described proposals and implementation of system, which consists of application for configuration and personalization of contactless smart cards and application for authentication of persons entering the system. At the end of thesis is evaluated implemented solutions, are described further possibilities of development of the applications and in conclusion it evaluated thesis as whole.

Klíčová slova

Bezkontaktní čipové karty, Mifare, RFID, bezkontaktní technologie, konfigurace, personalizace, autentizace, čtečka karet, ISO 14443

Keywords

Contactless smart cards, Mifare, RFID, contactless technology, configuration, personalization, authentication, card reader, ISO 14443

Citace

Peter Altamirano: Konfigurace a personalizace bezkontaktních čipových karet, bakalářská práce, Brno, FIT VUT v Brně, 2010

Konfigurace a personalizace bezkontaktních čipových karet

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Doc. Dr. Ing. Petra Hanáčka. Další informace mi poskytl Ing. Peter Pecho, Ph.D. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Peter Altamirano
19. květen 2010

Poděkování

Veľmi rád by som poďakoval vedúcemu mojej bakalárskej práce, pánovi Doc. Dr. Ing. Petrovi Hanáčkovi, za odborné rady, ochotu, pripomienky a návrhy. Taktiež by som rád poďakoval pánu Ing. Petrovi Pechovi, Ph.D za úvodné informácie, odborné rady a venovaný čas.

Obsah

1 Úvod

Táto bakalárska práca sa zaoberá problematikou bezkontaktných čipových kariet a vytvorením systému, ktorý umožňuje vydávať bezkontaktné čipové karty užívateľom a následne na základe bezkontaktnej čipovej karty je možné jednoznačne identifikovať jej držiteľa.

V druhej kapitole je rozobraná problematika bezkontaktných čipových kariet, zameraná na bezkontaktné čipové karty MIFARE, prehľad histórie, typy a komunikačné rozhranie týchto kariet. Taktiež oboznamuje s ISO normami, ktoré definujú vlastnosti bezkontaktných čipových kariet.

Tretia kapitola sa zaoberá návrhom systému a jeho jednotlivých častí. Popisuje spôsob konfigurácie, personalizácie bezkontaktných čipových kariet a identifikáciu ich držiteľov.

Štvrtá kapitola popisuje spôsob implementácie navrhnutého systému, zhodnotenie implementovaného systému a návrh ďalších možných vylepšení a rozvoj aplikácií.

Záverečná kapitola konštatuje a vyhodnocuje celkovú implementáciu, dosiahnuté výsledky a prínos tejto bakalárskej práce ako celku. Navrhuje taktiež niekoľko ďalších možných rozšírení systému.

2 Bezkontaktné čipové karty

V súčasnej dobe sa čoraz viac využívajú bezkontaktné čipové karty na komerčné využitia, keďže nevyžadujú pre prenos dát a energie elektrické prepojenie medzi čipovou kartou a čítačkou kariet, takže počas používania karty ju nemusí mat užívateľ v ruke, ale môže ju mať napríklad v peňaženke, alebo v kabelke. Bezkontaktné karty dokážu pracovať aj na vzdialenosť jeden meter, väčšinou sa táto vzdialenosť pohybuje v pár až desiatkach centimetroch, samozrejme táto vzdialenosť sa môže pomocou špeciálnej antény zväčšiť. Bezkontaktné karty sú vhodné pre aplikácie, v ktorých by mali byť osoby, alebo predmety rýchlo identifikovateľné.

Bezkontaktné karty môžeme použiť napríklad na riadenie prístupu do budov, miestnosti, na identifikáciu študentov, zamestnancov, svoje využitie majú aj ako skipasy, alebo pri identifikácií batožiny. Bezkontaktné čipové majú naozaj veľmi pestré a rozsiahle využitie, taktiež ich nie je možné použiť úplne všade. Napríklad pri platbách bezkontaktnou kartou by mohol držiteľ karty prísť o finančné prostriedky bez jeho vedomia, tento problém sa dá vyriešiť kombinovanou dual-interface kartou, ktorá je kombináciou kontaktnej a bezkontaktnej čipovej karty.

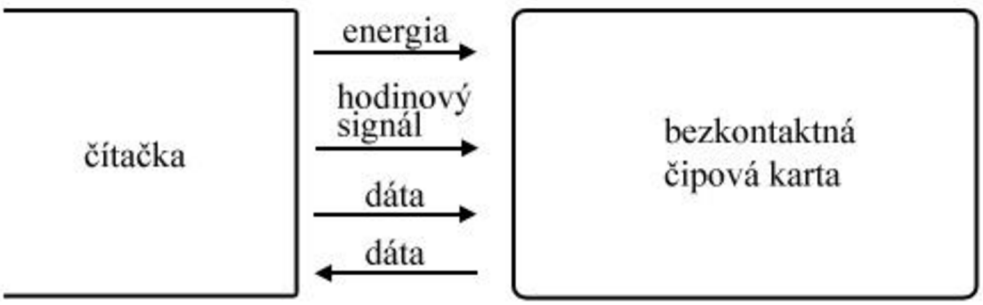
2.1 Technológia bezkontaktných čipových kariet

Technológia bezkontaktných čipových kariet nie je nová, je založená na dlhoročne známej RFID (Radio Frequency Identification) technológií [1][3].

Existuje viacero techník, ktoré je možné rozdeliť podľa viacero parametrov, jedným z nich je spôsob prenosu dát a energie. Najčastejšie používané metódy sú prenos dát pomocou rádiových vĺn, alebo mikrovĺn, optický prenos, kapacitné a indukčné väzby. Kapacitné a indukčné väzby sú najvhodnejšie pre plochý tvar čipovej karty bez prítomnosti interného zdroju energie. Systémy na trhu využívajú výlučne tieto metódy, ktoré sú popísane v skupine ISO/IEC noriem. Indukčná väzba je v súčasnosti najpoužívanejšou technikou pre bezkontaktné čipové karty [2].

Systém využívajúci bezkontaktné karty sa musí skladať z najmenej dvoch častí, z čipovej karty a kompatibilnej čítačky kariet. Pre komunikáciu čítačky kariet a čipovej karty sú nevyhnuté nasledujúce funkcie (vid Obrázok 1):

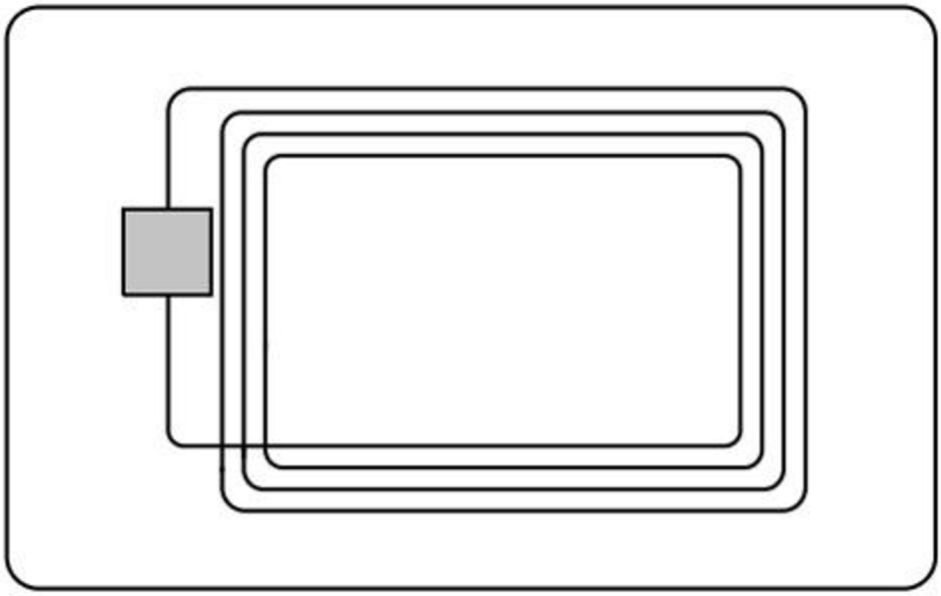
- prenos energie na kartu pre napájanie integrovaného obvodu
- prenos hodinového signálu
- prenos dát na čipovú kartu
- prenos dát z čipovej karty



Obrázok 1: Komunikácia čítačky kariet a čipovej karty [2]

2.1.1 Indukčná väzba

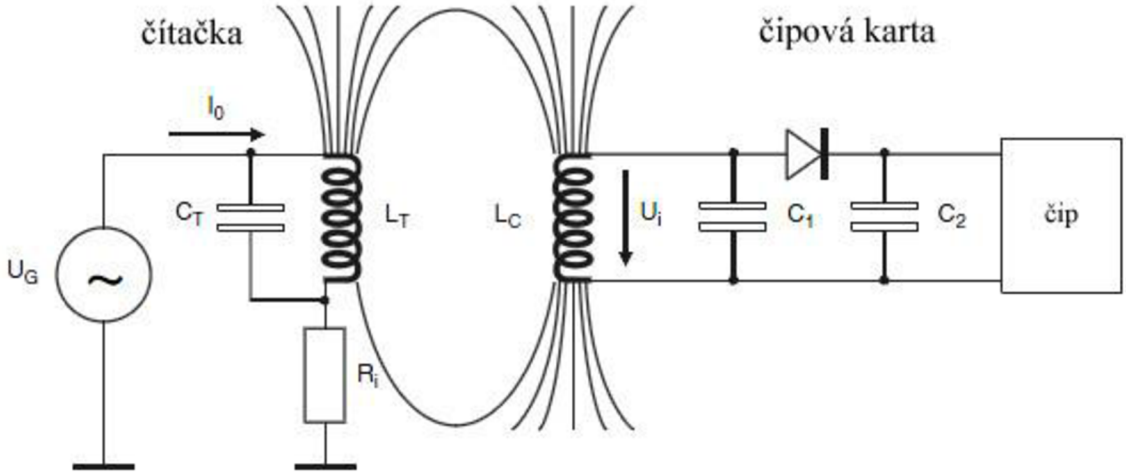
Indukčná väzba je v súčasnosti najpoužívanejšou technikou pre prenos energia a dát u bezkontaktných kartách.
Bez ohľadu na rozsah, alebo spotrebu energie, všetky karty, ktoré využívajú indukčnú väzbu, pracujú na rovnakom princípe.
Jedna, alebo viac cievok sú začlenené do tela karty (vid Obrázok 2), ako spojovací mechanizmus pre prenos dát a energie, spolu s jedným alebo viacerými čipmi [2].



Obrázok 2: Schéma cievok začlenených v bezkontaktnej čipovej karte [2]

2.1.2 Prenos energie

Takmer všetky bezkontaktné karty sa používajú pasívne, to znamená že energiu potrebnú pre prevádzku čipu v čipovej karte a následný prenos dát, je potrebné dodať karte priamo z čítačky kariet.
Prenos energie je založený na princípe voľne zapojeného transformátoru. Pre umožnenie prenosu energie, cievka v termináli generuje vysokofrekvenčné magnetické pole. Ak sa bezkontaktná čipová karta priblíži k terminálu, časť magnetického poľa prechádza cievkou v čipovej karte, ktorá indukuje určité napätie, ktoré poskytuje energiu pre prácu čipu (vid Obrázok 3).
Na dosiahnutie potrebnej sily magnetického poľa sa využíva paralelné zapojenie kondenzátoru a cievky v terminály a na karte [2].



Obrázok 3: Použitie indukčnej väzby ako zdroju energie pre bezkontaktné čipové karty [2]

2.1.3 Prenos dát

Na pre prenos dát z terminálu na bezkontaktnou čipovou kartou sa používajú všetky známe techniky digitálnej modulácie. Najčastejšie sa používajú metódy ASK (amplitude-shift keying), FSK (frequency-shift keying), PSK (phase-shift keying).
V opačnom smere, pri prenose dát z karty na terminál sa využíva metóda ASK (amplitude-shift keying) [2].

2.1.4 Kolízie

Pri používaní bezkontaktných kariet, existuje veľká pravdepodobnosť, že dve, alebo viacero kariet bude v dosahu terminálu v rovnakom čase. Všetky karty sa budú snažiť reagovať na príkazy terminálu, počas súčasného prenosu sa budú navzájom rušiť, dáta budú nespoľahlivo prenášane a môže sa ľahko stať že dáta budú stratené.
Pre zabezpečenie rušenia, bez výmeny dát medzi viacerými kartami v okolí terminálu sa používajú antikolízne metódy.

2.1.4.1 Antikolízne metódy

Antikolízne metódy môžeme rozdeliť do štyroch typov.
SDMA (space division multiple access) sa pokúša skenovať prevádzkovú oblasť, tak aby bolo možné získať len jednu kartu v danej dobe. Keďže táto metóda vyžaduje zložité a drahé antény, nevyužíva sa u kontaktných kariet.
Najčastejšou používanou metódou pri bezkontaktných kartách je metóda TDMA (time division multiple access). Táto metóda príma opatrenia na zabezpečenie rôzneho časového správania sa kariet, tak aby mohli byť samostatne identifikované a adresované terminálom.
Techniky FDMA (frequency division multiple access) a CDMA (code division multiple access) sa pri bezkontaktných kartách nepoužívajú, keďže sú tieto metódy komplikované a finančne náročné [2].

2.2 Bezkontaktné čipové karty MIFARE

MIFARE je ochranná známka spoločnosti NXP Semiconductors založenou spoločnosťou Philips. MIFARE technológia je najčastejšie používaná pri projektoch využívajúcich bezkontaktné čipové karty. S viac ako 1 miliardou predaných kariet a cez 10 miliónov predaných čítačiek kariet je najúspešnejšou značkou na svete.
MIFARE technológia je založená na štandarde ISO/IEC 14443 Type A [4].

2.2.1 Prehľad typov MIFARE kariet

Ochranná známka MIFARE zahŕňa v súčasnej dobe sedem druhov kariet.

2.2.1.1 MIFARE Classic (Standard)

Využíva patentovaný high-level protokol namiesto ISO/IEC 14443-4, s NXP patentovaným bezpečnostným protokolom pre overovanie a šifrovanie.
MIFARE Classic karta je v podstate len pamäťové úložné zariadenie, kde je pamäť rozdelená do segmentov a blokov s jednoduchými bezpečnostnými mechanizmami na kontrolu prístupu. Je založená na ASIC a má obmedzený výpočtový výkon. Vďaka svojej spoľahlivosti a nízkej cene, sú tieto karty bežne používané pre elektronické peňaženky, riadenie prístupu, firemné ID karty, prepravu alebo lístky.

MIFARE Classic 1K ponúka 1024 bytov pre ukladanie dát, rozdelené na 16 sektorov, každý sektor je chránený dvoma rôznymi kľúčmi, tzv. A a B. Môžu byť naprogramované pre operácie, ako je čítanie, písanie, zvyšovanie hodnoty blokov, atď.
MIFARE Classic 4K ponúka 4096 bytov rozdelených do štyridsať sektorov, z toho 32 sú rovnakej veľkosti ako v 1K, ďalších osem sektorov sú štvornásobnej veľkosti.
MIFARE Classic mini ponúka 320 bytov rozdelený do piatich sektorov.

Pre každý z týchto typov kariet, je vyhradených 16 bajtov na sektor pre kľúče a podmienok prístupu a nemožno ich použiť pre používateľské dáta. Tiež úplne prvých 16 bytov obsahuje poradové číslo karty a niektoré ďalšie údaje výrobcu, ktoré sú len na čítanie. To znižuje čistú užívateľom použiteľnú kapacitu týchto kariet na 752 bytov pre Classic 1k, na 3440 bytov pre Classic 4k a na 224 bytov pre Classic Mini.

Jednoduchosť základnej karty znamená, že sú lacné, čo je do značnej miery dôvodom pre ich úspech vo veľkom nasadení.

MIFARE Classic karty nie sú príliš bezpečné, keďže použité šifrovanie Crypto-1 môže byť prelomené za pár sekúnd, ako ukázali útoky na tieto typy kariet [4][5].

2.2.1.2 MIFARE Ultralight

Nízko-nákladové karty, ktoré využívajú rovnaký protokol ako MIFARE Classic karty, ale bez bezpečnostnej časti a mierne odlišné príkazy.
MIFARE Ultralight má len 64 bytov pamäte, bez šifrovacieho zabezpečenia. Pamäť je poskytovaná na 16 stránkach po 4 bytoch. Tieto karty sú tak lacné, že sa často používajú pre jednorazové použitie [4][5].

2.2.1.3 MIFARE Ultralight C

Prvé nízko-nákladové karty, pre aplikácie s obmedzeným použitím, ktoré ponúkajú výhody otvoreného 3DES šifrovania. Najčastejšie sa používajú pre jednorazové lístky. S 3DES používa široko podporovaného formátu, ktorý umožňuje jednoduchú integráciu do existujúcej infraštruktúry.

Integrované 3DES overovanie poskytuje efektívne protiopatrenia proti falšovaniu lístkov (klonovaniu).

Vlastnosti kariet MIFARE Ultralight C:

- kompatibilné s ISO / IEC 14443 A 1-3 vrátane anti-kolízie
- 192 bytov EEPROM pamäte
- chránený prístup k dátam pomocou 3DES
- štruktúra pamäte ako u MIFARE Ultralight (jedná stránka má 4 byty)
- spätná kompatibilita s MIFARE Ultralight
- 16 bitový čítač
- unikátne 7 bytové sériové číslo

MIFARE Ultralight C sa využívajú napr. v MHD, pri jednorazových lístkov a akciový letenkách [4][5].

2.2.1.4 MIFARE ProX, SmartMX

Čipové karty založené na mikroprocesore v súlade s normou ISO / IEC 14443-4. Hardware sám o sebe je nepoužiteľný, musí byť naprogramovaný špeciálnym softwarom – operačný systém. Väčšinu času mikroprocesor spolu s co-procesorom venujú rýchlim šifrovacím výpočtom (napr. 3DES, AES, RSA, atď.).

Tieto karty sú schopné realizovať zložité operácie, ktoré sú rovnako bezpečné a rýchle ako operácie na kontaktných kartách. V skutočnosti sú k dispozícii aj ako kontaktné karty, alebo karty s viacerými rozhraniami a ponúkajú vysoký stupeň flexibility. Tieto karty sú schopné podporovať celý rad operačných systémov, vrátane Java Card operačného systému (JCOP).

V závislosti na inštalovanom softwari, je možné kartu použiť pre takmer akékoľvek použitie. Tento typ kariet sa väčšinou používajú tam, kde je vysoká úroveň bezpečnosti (napr. na bezpečné cestovné doklady, elektronické pasy, platobné karty, atď.), a je certifikovaný nezávislými stranami, ako sú Common Criteria. Sú vysoko odolné voči útokom [4][5].

2.2.1.5 MIFARE DESFire

Čipové karty, ktoré spĺňajú normy ISO / IES 14443-4 s mask-ROM operačným systémom od NXP. Ďalšia mikroprocesorová platforma, založená na rovnakom jadre ako MIFARE ProX / SmartMX s viacerými hardwarovými a softwarovými ochrannými prvkam. Karty sa predávajú už naprogramované, so všeobecným softwarom (DESFire operačný systém), ktorý ponúka jednoduchú adresárovú štruktúru so súbormi, podobný tomu, aký sa zvyčajne nachádza na čipových kartách.

DESFire karty sa predávajú v štyroch variantoch. Jedna s Triple-DES a iba 4 KByte pamäte a tri s AES s kapacitou pamäte 2, 4 a 8 KB. AES varianty majú pridané ďalšie bezpečnostné prvky, t.j. CMAC.

Sú kompatibilné s využitím štandardov (ISO / IEC 14443-4) protokol. Karta je založená na procesore 8051 s 3DES a AES crypto akcelerátorom, takže uskutočňuje naozaj rýchlo operácie. Maximálna vzdialenosť pre čítanie/zápis medzi kartou a čítačkou je 10 cm, ale skutočná vzdialenosť je závislá na elektrickom poli čítačky a rozmerov antény [4][5].

2.2.1.6 MIFARE DESFire EV1

Nová verzia karty DESFire, viac-menej spätne kompatibilná. K dispozícii s 2 KB, 4 KB a 8 KB NV-Pamäťou [4][5].
Medzi ďalšie funkcie patrí:

- podpora náhodného ID
- podpora pre 128 bit AES
- hardware a operačný systém je overený Common Criteria na úrovni EAL 4 +
- technológia DESFire EV1 bola zverejnená v novembri 2006

2.2.1.7 MIFARE Plus

Náhrada za MIFARE Classic s certifikovanou bezpečnostnou úrovňou (základ 128 AES). Umožňuje ľahký upgrade existujúcej infraštruktúry smerom k vysokej bezpečnosti [4][5].

Vlastnosti:

- 2 KB, alebo 4 KB pamäte
- 7 alebo 6 bytový UID, podpora náhodného UID
- podpora pre 128-bit AES
- certifikovaný Common Criteria na úrovni EAL 4 +
- bezpečnostný upgrade s kartami na poli

2.2.2 História

Prvou kartou z rady MIFARE na základe bezkontaktnej technológii bola karta MIFARE Classic 1K, zavedená v roku 1994. O dva roky neskôr (1996) v Seoule bola predstavená prvá transportná schéma MIFARE Classic 1K.

V ďalších rokoch boli postupne predstavené ďalšie MIFARE karty, v roku 1997 MIFARE PRO s Triple-DES co-procesorom, v roku 1999 MIFARE PROX s PKI co-procesorom a v roku 2001 Mifare Ultralight.

Ďalšou radou kariet Mifare sa stala MIFARE DESFire, ktorej základom je mikroprocesor. Náprotivok k DESFire bol zavedený v roku 2004 ako MIFARE DESFire SAM. V roku 2006 prišiel na trh prvý produkt na podporu 128-bit AES šifrovania MIFARE DESFire EV1.

V Roku 2008 bola predstavená MIFARE Plus, postavená na 128-bit AES šifrovaní, ako náhrada za MIFARE Classic. Taktiež bola predstavená MIFARE Ultralight C s Triple DES autentizáciou [6] [7].

2.2.3 Špecifikácia MIFARE Classic 1K kariet

MIFARE Classic karty boli vyvinuté spoločnosťou NXP podľa normy ISO/IEC 14443 Type A.

2.2.3.1 Rádiofrekvenčné rozhranie

Napájacie pole je stále prítomné (s krátkymi prestávkami pri prenose), pretože sa používa pre napájanie karty. Umožňuje bezkontaktný antikolízny prenos dát a prenos energie, nie je potrebná žiadna batéria. Pre oba smery prenosu dát je len jeden štart bit na začiatku každého rámca. Každý bajt je prenášaný s bitom parity (nepárna parita) na konci. Najmenej významné bity bajtu s najnižšou adresou vybraného bloku sú odovzdané ako prvé. Maximálna dĺžka rámca je 163 bitov (16 bajtov dát + bit parity pre každý bajt + 2 CRC bajty = 16 * 9 + 2 * 9 + 1 start bit).

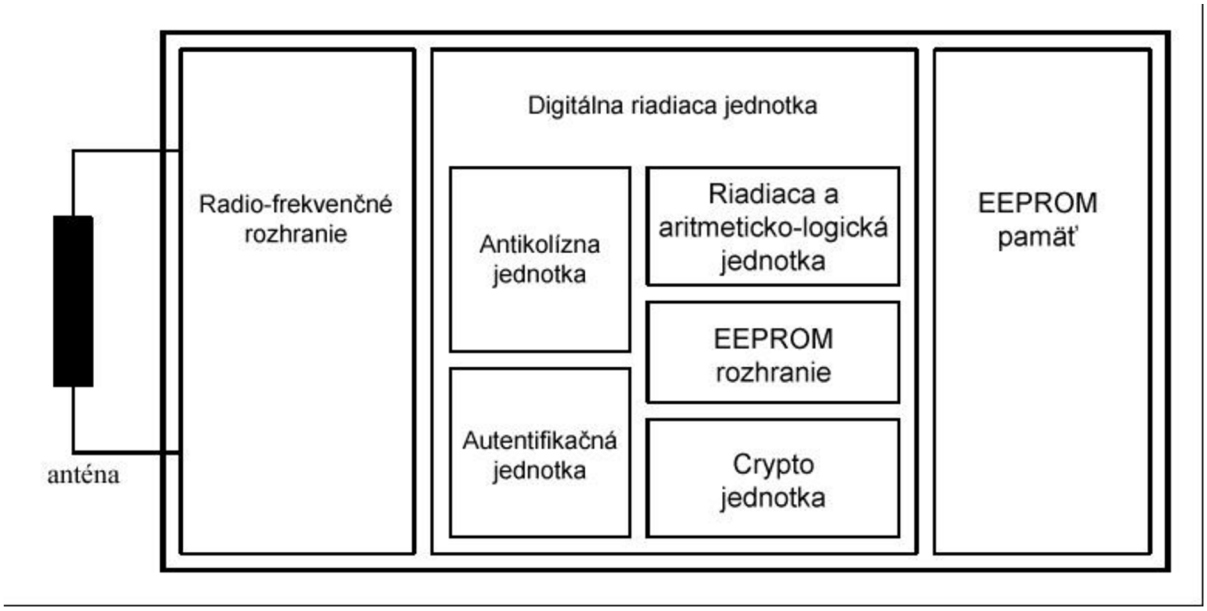
Prevádzková vzdialenosť kariet je až 10 cm v závislosti od antény. Prevádzková frekvencia je 13, 56 MHz. Prenos dát prebieha rýchlosťou 106 kbit/s. Úplnosť dát zabezpečuje 16 Bit CRC, parita, bitové kódovanie. Typická operácia s kartou trvá menej ako 100 ms [8].

2.2.3.2 EEPROM pamäť

1 KByte pamäte je organizovaný v 16 sektoroch, každý sektor má 4 bloky, ktoré sa skladajú zo 16 bytov (vid Obrázok 6). Umožňuje užívateľsky definovateľné podmienky prístupu pre každý pamäťový blok. Pamäť dokáže uchovať spoľahlivo dáta 10 rokov a zvládne 100 000 zápisov [8].

2.2.3.3 Čip karty

Čip sa skladá z 1KB EEPROM pamäte, radio-frekvenčného rozhrania a digitálnej riadiacej jednotky (vid Obrázok 4). Energia a dáta sú prenášané cez anténu, ktorá sa skladá z cievky s niekoľko otáčkami, pripojenej priamo k čipu (vid Obrázok 2) [8].



Obrázok 4: Bloková schéma čipu implementovaného v MIFARE Classic kartách [8]

Radio-frekvenčné rozhranie tvorí [8]:

- modulátor / demodulátor
- usmerňovač
- hodinový regenerátor
- power-on-reset generátor
- regulátor napätia

Digitálnu riadiacu jednotku tvorí [8]:

- **Antikolízna jednotka**: karty v oblasti terminálu môžu byť vybrané jednotlivo a prevedú sa s nimi operácie v poradí, nevznikne kolízna situácia
- **Autentifikačná jednotka**: Akejkoľvek operácií s pamäťou predchádza autentifikačný proces, prístup k bloku v pamäti je možný len po úspešnej autentifikácií pomocou špecifikovaných kľúčov k danému bloku
- **Riadiaca a aritmeticko-logická jednotka**: Hodnoty sú uložené v špeciálnom redundantnom formáte a môžu byť inkrementované alebo dekrementované
- **EEPROM rozhranie**
- **Crypto jednotka**: šifra CRYPTO1 je použitá pre autentifikáciu a šifrovanie výmeny dát

EEPROM pamäť

- 1 KB je organizovaný v 16 sektoroch, každý obsahuje 4 bloky. Blok obsahuje 16 bajtov. Posledný blok každého z týchto sektorov sa nazýva "trailer", obsahuje dve tajné kľúče a programovateľné podmienky prístupu pre každý blok v tomto sektore (vid Obrázok 6) [8].

2.2.3.4 Bezpečnosť

Využíva sa vzájomná trojprechodová autentifikácia (ISO / IEC DIS 9798-2), individuálne nastavenie dvoch kľúčov pre každý sektor pre podporu multi-aplikácií, unikátne sériové číslo pre každé zariadenie [8].

2.2.3.5 Princíp komunikácie

Príkazy sú inicializované zo strany čítačky kariet a riadené sú digitálnou riadiacou jednotkou čipovej karty podľa platných prístupových podmienok k príslušnému sektoru. Schému znázorňujúcu princíp komunikácie nájdete na Obrázku 5.

Po vykonaní power-on-reset karty, odpovedá karta na príkaz, ktorý bol zaslaný čítačkou kariet všetkým kartám v dosahu čítačky kariet, zaslaním kódu odpovede na žiadosť (ATQA podľa ISO/IEC 14443A).

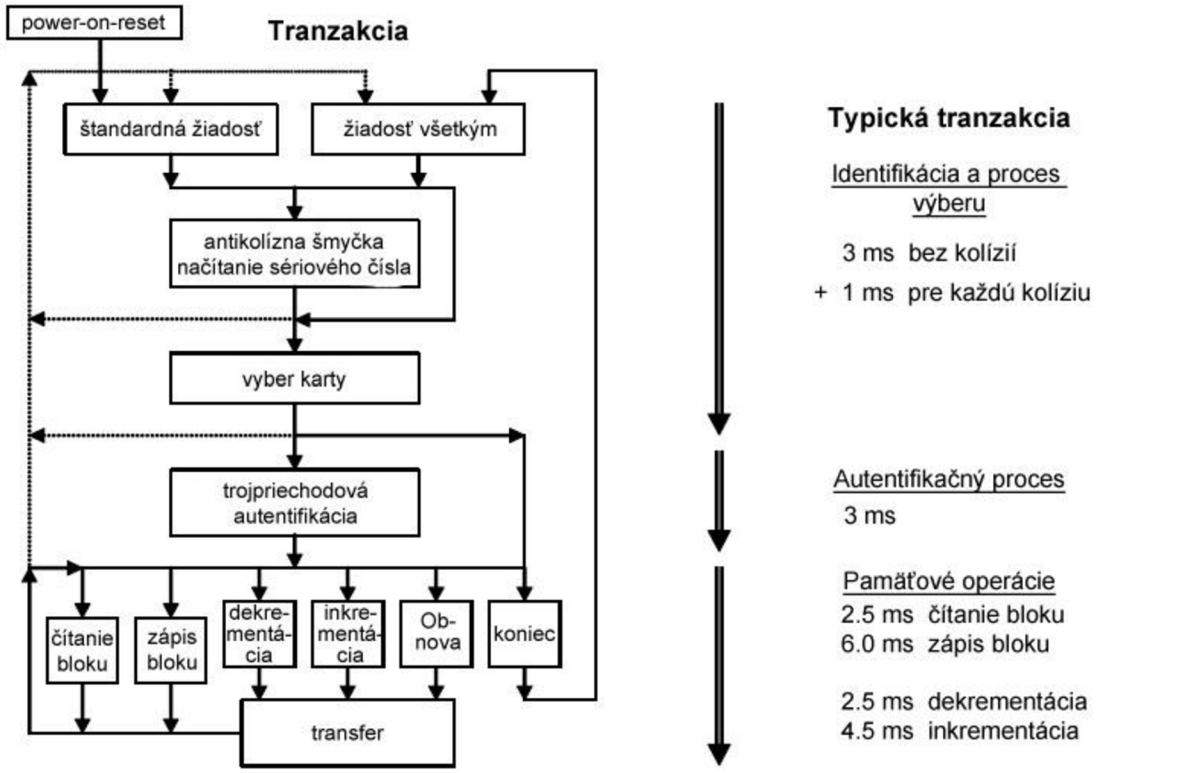
V antikolíznej šmyčke je prečítané sériové číslo karty. Ak sa nachádza viacero kariet v dosahu terminálu, rozlišujú sa podľa unikátneho sériového čísla a jedna z nich bude vybraná pre ďalšie transakcie. Ostatné nevybrané karty sa vrátia do pohotovostného režimu a čakajú na nový príkaz.

Príkazom pre vybranie karty vyberie čítačka kariet jednu z dostupných kariet pre autentizáciu a operácie súvisiace s pamäťou. Karta vráti kód odpovede na príkaz select (Answer To Select - ATS), ktorý určuje typ vybranej karty.

Po vybraní karty čítačka kariet špecifikuje pamäťové miesto pre nasledujúci prístup do pamäti a využíva zodpovedný kľúč k trojpriechodovej autentifikácií. Po úspešnej autentifikácií sú všetky pamäťové operácie šifrované [8].

Po autentifikácií sa môžu vykonávať nasledujúce operácie [8]:

- čítanie bloku pamäte
- zápis do bloku pamäte
- dekrementácia – zníži hodnotu bloku a výsledok uloží do dočasného interného dáta registru
- inkrementácia - zvýši hodnotu bloku a výsledok uloží do dočasného interného dáta registru
- obnova – presunie obsah bloku do interného dáta registru
- transfer – zapíše obsah interného dáta registru do bloku v pamäti



Obrázok 5: Schéma komunikácie s bezkontaktnou čipovou kartou [8]

2.2.3.6 Integrita dát

Pre zabezpečenie veľmi spoľahlivého prenosu dát sú v bezkontaktnom komunikačnom spojení medzi čítačkou kariet a čítačkou implementované nasledujúce mechanizmy [8]:

- 16 bitový CRC súčet
- bit parity pre každý byte
- kontrolný bitový súčet
- bit kódovanie
- kanálový monitoring

2.2.3.7 Trojpriechodová autentifikácia

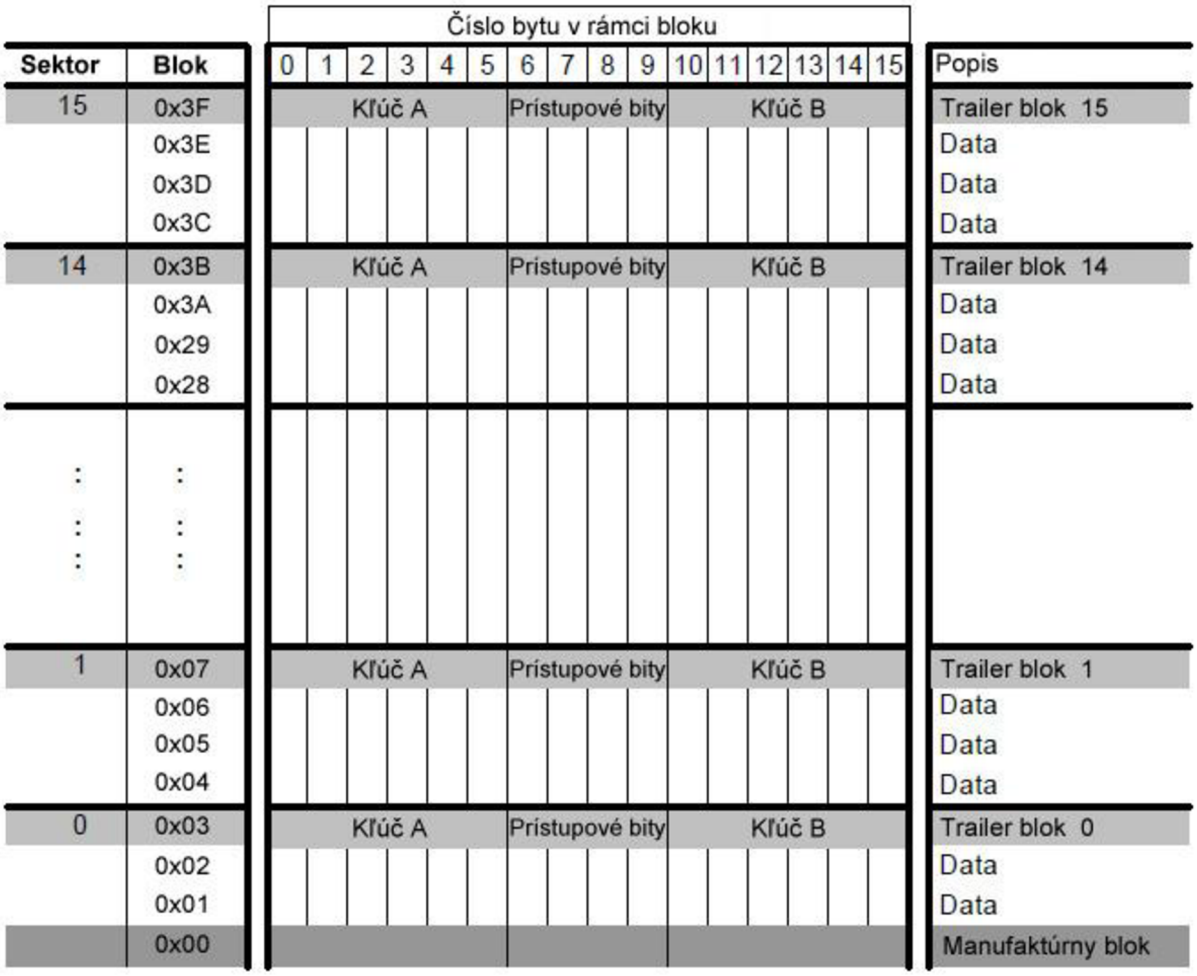
Postup trojpriechodovej autentifikácie:

1. Čítačka špecifikuje pamäťový sektor, ku ktorému chce pristupovať a pre autentifikáciu vyberie kľúč A alebo kľúč B.
2. Karta načíta tajný kľúč a špecifikované podmienky prístupu k danému sektoru. Následne odosiela náhodné číslo čítačke (prvý priechod)
3. Čítačka kalkuluje odpoveď pomocou tajného kľúča a dodatočného vstupu. Karte je odoslaná odpoveď spolu s náhodným číslom od čítačky kariet (druhý priechod)
4. Karta overí odpoveď s jej vlastnou výzvou, následné skalkuluje odpoveď a odošle ju (tretí priechod)
5. Čítačka overí odpoveď s jej vlastnou výzvou

Po prenesení prvej výzvy je komunikácia medzi čítačkou a kartou šifrovaná [8].

2.2.3.8 EEPROM pamäť

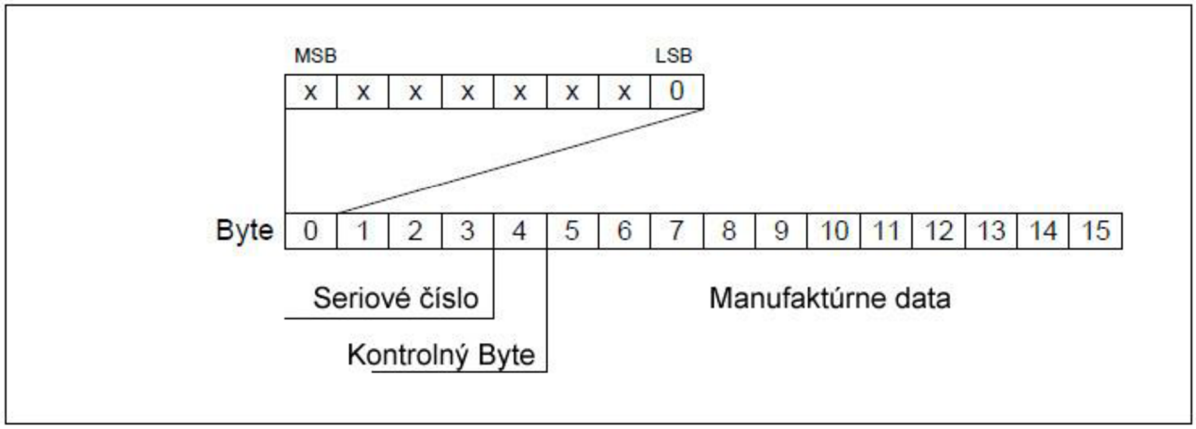
Pamäť o veľkosti 1 kB je organizovaná v 16 sektoroch, každý sektor obsahuje 4 bloky a každý blok má 16 bytov (vid Obrázok 6).



Obrázok 6: Organizácia pamäte Mifare Classic 1K

Manufaktúrny blok

Je prvý dátový blok (blok 0) prvého sektoru (sektor 0). Obsahuje manufaktúrne dáta (vid Obrázok 7). Vzhľadom na bezpečnosť a systémových požiadaviek je tento blok chránený proti zápisu po tom čo bol naprogramovaný výrobcom pri výrobe [8].



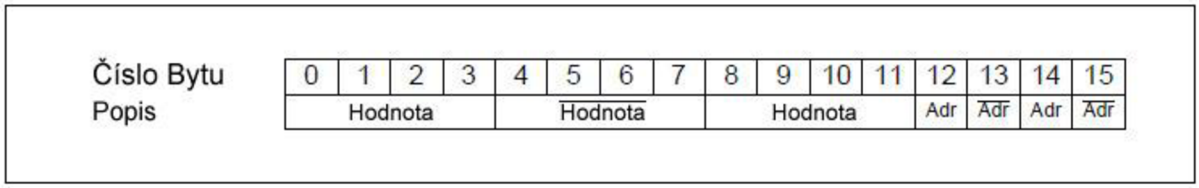
Obrázok 7: Manufaktúrny blok pamäte [8]

Dátový blok
Všetky sektory obsahujú 3 bloky, každý ma 16 bytov, pre uchovávanie dát (sektor 0 obsahuje len dva bloky a manufaktúrny blok).
Dátové bloky môžu byť nakonfigurované pomocou prístupových bitov ako:

- čítaco-zapisovacie bloky, napr. u bezkontaktnej kontroly prístupu
- hodnotové bloky, kde sa využívajú ďalšie príkazy (inkrementácia a dekrementácia), napr. u elektronickej peňaženky

Autentifikácia musí byť vykonaná pred každou pamäťovou operáciou s cieľom umožniť ďalšie príkazy [8].

Hodnotové bloky
Hodnotové bloky majú pevný formát dát, ktorý umožňuje detekciu a opravu chýb a správu zálohovania (vid Obrázok 8). Využívajú sa pri elektronický peňaženkách.
Hodnotový blok môže byť vytvorený len s operáciou zápisu v hodnotovo-blokovom formáte [8].



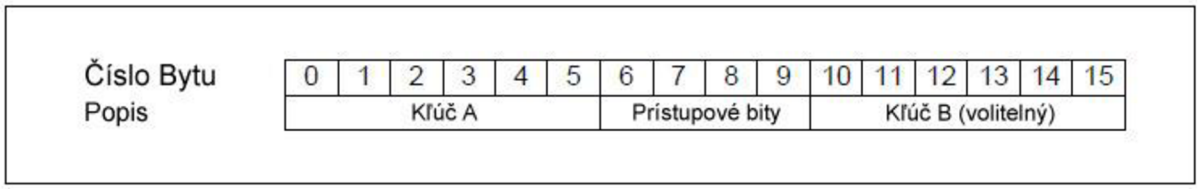
Obrázok 8: Hodnotový blok

- **Value (hodnota)**: predstavuje 4 bytovú hodnotu. Najmenej významný byte hodnoty je uložený v najmenej významnom adresovom byte. Znegované hodnoty sú uložené v štandardnom dvojkovom doplnkovom formáte. Z dôvodu úplnosti a bezpečnosti dát sa hodnota uloží trikrát, dvakrát neinvertovaná a raz invertovaná.

- **Adr (adresa)**: predstavuje 1 bytovú adresu, ktorá môže byť použitá k uloženiu uchovávacej adresy bloku, pri implementovaní správy zálohovania . Adresa je uložená štyrikrát, dvakrát invertovaná a dvakrát neinvertovaná. Adresa môže byť zmenená jedine príkazom zápisu, pri vykonávaní ostatných príkazov ostane táto hodnota nezmenená.

Trailer blok
Každý sektor obsahuje trailer blok (vid Obrázok 9), ktorý obsahuje:

- tajné kľúče A a B (nepovinný), ktoré vracajú logickú 0 pri čítaní
- podmienky pre prístup k blokom v danom sektore



Obrázok 9: Trailer blok

Prístupové byty špecifikujú taktiež typ bloku (čítaco-zapisovací, alebo hodnotový blok). Ak kľúč B nie je potrebný, posledné 6 byty bloku 3 môžu byť použité pre dáta. Deviaty byt môže byť použitý pre dáta, platia pre neho rovnaké prístupové práva ako pre byty 6, 7 a 8. Všetky kľúče sú pri dodaní čipu nastavené na hodnotu FF FF FF FF FF FF [8].

Prístupové byty

Prístupové byty špecifikujú podmienky prístupu k danému sektoru. Prístupové podmienky pre každý dátový blok a trailer blok sú definované troma bytmi, ktoré sú uložené invertované a neinvertované v trailer bloku daného sektoru (vid Obrázok 10).

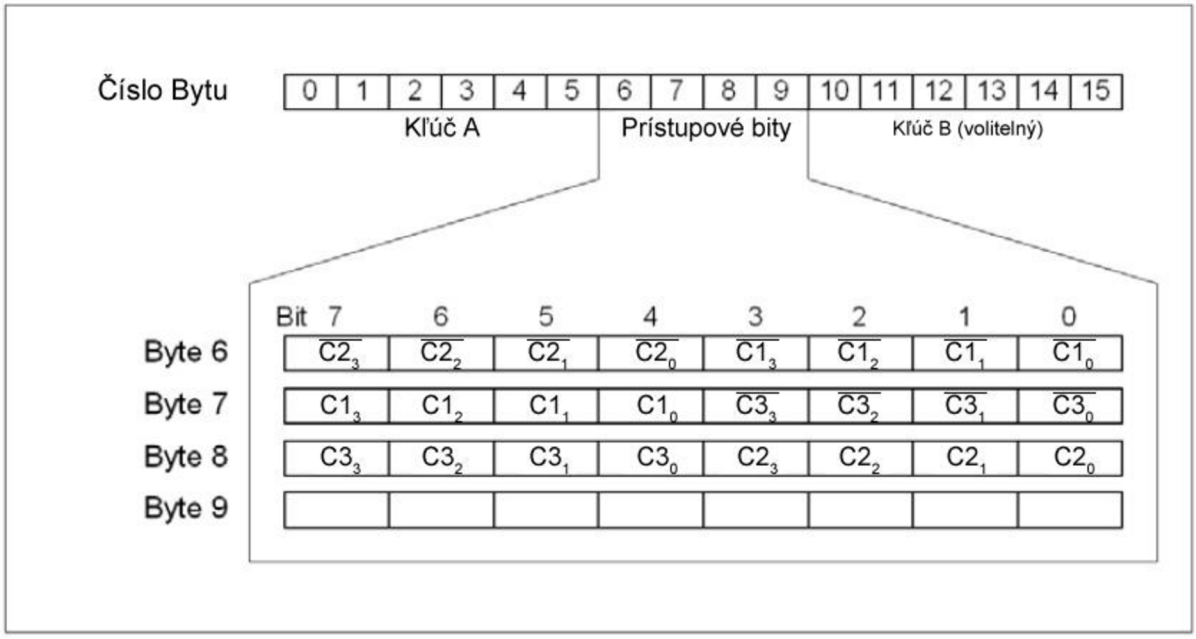
Prístupové byty kontrolujú prístupové práva k pamäti použitím tajných kľúčov A a B. Prístupové podmienky sa môžu zmeniť ak je známi odpovedajúci kľúč a aktuálne nastavenie prístupových podmienok , ktoré umožňujú túto operáciu.

Pri každom prístupe do pamäte je vnútornou logikou kontrolovaný formát prístupových bytov, ak sa zistí porušenie formátu celý sektor je nenávratne blokovaný.

Vnútorná logika čipu zabezpečuje že príkazy sú vykonané po úspešnej autentifikácií, alebo nikdy [8].

Prístupové byty	Povolené príkazy	Blok	Popis
$C1_3\ C2_3\ C3_3$	čítanie, zápis	3	trailer sektor
$C1_2\ C2_2\ C3_2$	čítanie, zápis, inkrementácia, dekrementácia, transfer, obnova	2	dátový blok
$C1_1\ C2_1\ C3_1$	čítanie, zápis, inkrementácia, dekrementácia, transfer, obnova	1	dátový blok
$C1_0\ C2_0\ C3_0$	čítanie, zápis, inkrementácia, dekrementácia, transfer, obnova	0	dátový blok

Tabuľka 1: Závislosti prístupových bytov



Obrázok 10: Prístupové byty [8]

Prístupové podmienky pre trailer blok

Závislosti prístupových bitoch pre čítanie a zápis trailer bloku (blok 3) a prístupových bitov sú špecifikované ako nikdy, kľúč A, kľuč B, kľuč A|B (kľúč A alebo B).

Pri dodaní čipu sú prístupové podmienky pre trailer blok a kľúč A preddefinované ako transportná konfigurácia.

Vzhľadom k tomu že kľúč B môže byť v transportnej konfigurácií čítaný, nové karty musia byť overené kľúčom A. Prístupové byty sa môžu samy o sebe zablokovať, preto je potrebné venovať zvýšenú pozornosť hlavne pri personalizácií kariet [8].

Prístupové byty			Prístupové podmienky pre						Poznámka
			Kľúč A		Prístupové byty		Kľúč B		
C1	C2	C3	čítanie	zápis	čítanie	zápis	čítanie	zápis	
0	0	0	nikdy	kľúč A	kľúč A	nikdy	kľúč A	kľúč A	Kľúč B môže byť čítaný a použitý pre dáta
0	1	0	nikdy	nikdy	kľúč A	nikdy	kľúč A	nikdy	Kľúč B môže byť čítaný a použitý pre dáta
1	0	0	nikdy	kľúč B	kľúč A|B	nikdy	nikdy	kľúč B	
1	1	0	nikdy	nikdy	kľúč A|B	nikdy	nikdy	nikdy	
0	0	1	nikdy	kľúč A	kľúč A	kľúč A	kľúč A	kľúč A	Kľúč B môže byť čítaný, transportná konfigurácia
0	1	1	nikdy	kľúč B	kľúč A|B	kľúč B	nikdy	kľúč B	
1	0	1	nikdy	nikdy	kľúč A|B	kľúč B	nikdy	nikdy	
1	1	1	nikdy	nikdy	kľúč A|B	nikdy	nikdy	nikdy	

Tabuľka 2: Prístupové podmienky pre trailer blok

Prístupové podmienky pre dátový blok
Závislosti prístupových bitoch pre čítanie a zápis dátových blokov (bloky 0-3) sú špecifikované ako nikdy, kľúč A, kľuč B, kľuč A|B (kľúč A alebo B).

Nastavenie príslušných prístupových bitov definuje typ bloku a odpovedajúce platné príkazy:

- čítaco-zapisovací blok - operácie čítania a zápisu sú povolené
- hodnotový blok - umožňuje dodatočné transakcie inkrementáciu, dekrementáciu, transfer a obnovu. V prípade hodnoty „001“ je možné len čítanie a dekrementácia pre nedobíjacie karty. V druhom prípade je možne pre dobitie (zápis) karty využiť kľúč B
- manufaktúrny blok – ochrana proti zápisu do tohto bloku, nie je nijako ovplyvnená nastavenými prístupovými bytmi
- v transportnej konfigurácie musí byť použitý k autentifikácií kľúč A

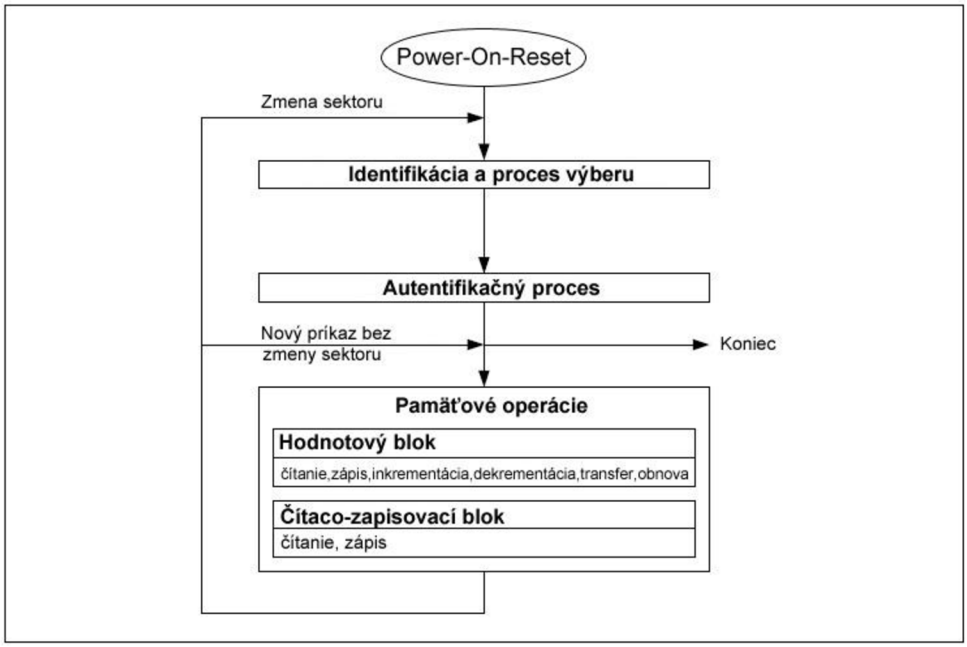
Prístupové byty			Prístupové podmienky pre				Poznámka
C1	C2	C3	čítanie	zápis	inkrementácia	Dekrementácia, transfer, obnova	
0	0	0	kľúč A|B	kľúč A|B	kľúč A|B	kľúč A|B	transportná konfigurácia
0	1	0	kľúč A|B	nikdy	nikdy	nikdy	čítaco-zapisovací blok
1	0	0	kľúč A|B	kľúč B	nikdy	nikdy	čítaco-zapisovací blok
1	1	0	kľúč A|B	kľúč B	kľúč B	kľúč A|B	hodnotový blok
0	0	1	kľúč A|B	nikdy	nikdy	kľúč A|B	hodnotový blok
0	1	1	kľúč B	kľúč B	nikdy	nikdy	čítaco-zapisovací blok
1	0	1	kľúč B	nikdy	nikdy	nikdy	čítaco-zapisovací blok
1	1	1	nikdy	nikdy	nikdy	nikdy	čítaco-zapisovací blok

Tabuľka 3: Prístupové podmienky pre dátový blok

Ak môže byť kľúč B čítaný, nemôže sa použiť pre autentifikáciu. Ak sa v tomto prípade užívateľ pokúsi využiť kľúč B k autentifikácii, karta bude odmietať akékoľvek ďalšie prístupy do pamäti po autentifikácií [8].

Prístup do pamäti

Pred každou pamäťovou operáciou musí byť karta vybraná a musí prebehnúť úspešná autentifikácia. Možné pamäťové operácie nad adresovaným blokom závisia od použitého kľúča a nastavených podmienok pre prístup k danému bloku [8]. Princíp prístupu do pamäti je zobrazený na Obrázku 11.



Obrázok 11: Schéma prístupu do pamäti [8]

2.3 ISO/IEC normy

Vzhľadom k rôznym technikám pri používaní bezkontaktných kariet od rôznych výrobcov, bolo potrebné vytvoriť štandardy, ktoré zjednotia všetky techniky. Pracovná skupina mala za úlohu vytvoriť štandard pre bezkontaktné karty, ktorý bude kompatibilný s inými normami pre identifikačné karty. Štandardizácia sa ukázala ako zložitá a časovo náročná. Technické možnosti pre prenos energie a dát medzi kartou a terminálom závisia od požadovanej vzdialenosti karty od terminál. Nepodarilo sa vytvoriť jednotný štandard, ktorý by poskytoval jednotné technické riešenie pre všetky typy aplikácií a riešení.

V súčasnosti existujú tri štandardy (ISO/IES 10536, ISO/IEC 14443, ISO/IEC 15693) [3]. Každý z týchto štandardov obsahuje viacero technických riešení, pretože členovia štandardizačného výboru sa nevedeli dohodnúť na jedinom riešení. Terminály musia byť kompatibilné so všetkými možnosťami, ktoré ponúka daný štandard.

2.3.1 ISO/IEC 14443

Norma ISO / IEC 14443, ktorá nesie originálny anglický názov Identification cards – Contactless integrated circuit(s) cards – Proximity cards, popisuje vlastnosti bezkontaktných čipových kariet.

Skladá sa zo štyroch častí:

- časť 1: fyzikálne vlastnosti
- časť 2: rádio frekvenčné napájanie a rozhranie signálov
- časť 3: inicializácia a protikolízne techniky
- časť 4: prenosové protokoly

2.3.1.1 Fyzikálne vlastnosti

Karta nesmie utrpieť trvalé poškodenie pri vytavení do elektromagnetických polí terminálov, taktiež musí vydržať záťaž bežných elektromagnetických polí v životnom prostredí. Štandard špecifikuje maximálne hodnoty záťaží, vzhľadom k pôsobeniu striedavého elektrického a magnetického poľa, ktoré musí karta zvládnuť bez poškodenia. Úlohou výrobcov kariet je navrhnúť bezkontaktné čipové karty tak, aby splňovali tieto požiadavky [9] [2].

2.3.1.2 Rádio frekvenčné napájanie a rozhranie signálov

Bezkontaktné karty pracujú na základe induktívnej väzby. Napájanie a dáta sú prenášané pomocou striedavého magnetického poľa generovaného terminálom.
Vysielacia frekvencia je nastavená na hodnotu fc= 13.56 MHz ± 7 kHz s magnetickou intenzitou poľa najmenej 1.5 A/m, vo väčšine 7.5 A/m (efektívna hodnota). Týmto nastavením terminálu dosiahneme funkčnosť kariet na vzdialenosť približne 10 cm [10] [2].

2.3.1.3 Signály a komunikačné rozhranie

V norme ISO/IEC 14443 sú definované dve rôzne typy komunikačného rozhrania, typ A a typ B. V čase príprav ISO štandardu existovali dve rôzne riešenia od rôznych výrobcov, čo znemožnilo vytvoriť jednotnú metódu komunikačného rozhrania. V súčasnosti terminály, kvôli kompatibilite so štandardom, podporujú obidva typy, počas komunikácie môže byť použitý iba jedna metóda, terminály vedia rozoznať o ktorý typ kariet sa jedná [11] [2].

ISO / IEC 14443 Typ A

Prenos dát prebieha obojsmerne rýchlosťou približne 106 kbit / s. Na prenos dát z terminálu na kartu sa využíva digitálne amplitúdová modulácia (100 % ASK – amplitude-shift keying), spolu s modifikovaným Miller kódovaním a s dĺžkou prázdneho intervalu (medzerou) obmedzenou na 3 ms. Tento relatívne krátky interval umožňuje stály prísun energie z terminálu na kartu.

Prenos dát z karty na terminál pracuje na princípe záťažovej modulácie (load modulation) so signálom, ktorý je generovaný spínaním záťaže vo vnútri karty. Signál je modulovaný pomocou prepínania signálu (on / off) pomocou Manchaster kódovania [11] [2].

ISO / IEC 14443 Typ B

Pri prenose z terminálu na kartu sa využíva ASK (amplitude-shift keying) s indexom modulácie 10%. Prísun energie je zabezpečený malým indexom modulácie, ktorý je definovaný tak, že najmenej 86 percent prenosového poľa je stále dostupných. Prenosová rýchlosť je taktiež približne 106 kbit /s. A využíva sa jednoduché bit kódovanie NRZ (non-return to zero).

Na prenos dát z karty na terminál sa využíva tak ako pri type A záťažová modulácia so signálom, ktorý je na rozdiel od typu A modulovaný pomocou posunu fázy o 180 stupňov (BPSDK - binary phase-shift keying). Použité je taktiež NRZ kódovanie a prenosová rýchlosť približne 106 kbit/s [11] [2].

2.3.1.4 Inicializácia a protikolízne techniky

Ak kartu privedieme do pracovného rozsahu terminálu, musí sa vytvoriť komunikácia medzi terminálom a kartou. Môže sa však stať, že terminál je v spojení s inou kartou, alebo že sa dve karty súčasne pokúšajú nadviazať spojenie s terminálom., takto vznikajú kolízne situácie, ktoré je potrebné vyriešiť a predísť im. Musíme zabezpečiť komunikáciu s jedinou kartou, alebo so špecifickou skupinou kariet. V štandarde sú popísane metódy pre ustanovenie komunikácie medzi kartou a terminálom a protikolízne metódy. Vzhľadom k dvom typom komunikačného rozhrania (typ A, typ B), ktoré využívajú rôzne protokoly, sú metódy komunikácie a protikolízne metódy popísané zvlášť pre typ A a pre typ B [12] [2].

Inicializácia a protikolízne techniky pre ISO / IEC 14443 typ A

Pre inicializáciu a výber kariet typu A je použitý dynamický binárny vyhľadávací algoritmus. Terminál musí byť schopný rozpoznať kolíziu dát na bitovej úrovni, použité Manchester kódovanie nám to umožňuje, avšak vyžaduje to aby všetky karty v pracovnom rozsahu terminálu odosielali svoje údaje synchrónne.

Ak sa karta dostane do blízkosti terminálu a mikroprocesor je napájaný z elektromagnetického poľa terminálu, karta sa po power-on resete dostane do stavu pokoja (idle state), do tohto stavu sa musí karta dostať do 5ms od začiatku napájania z poľa terminálu. V stave pokoja karta reaguje len na príkaz REQA (request type-A) a príkaz WUPA (wake-up type-A), všetky ostatné príkazy vydávane terminálom sú v tejto chvíli ignorované, aby nedošlo k rušeniu.

Kvôli zabezpečeniu vysokej spoľahlivosti príkazov REQA a WUPA sú tieto príkazy prenášane pomocou špeciálnych krátkych rámcov. Všetky ostatne príkazy, s výnimkou protikolíznych príkazov, sú prenášane pomocou štandardných rámcov. Pre protikolízne príkazy sú definované špeciálne rámce s názvom bitovo-orientované protikolízne rámce [12] [2].

Krátke rámce
Krátke rámce sa používajú len na inicializačné príkazy. Krátky snímok sa skladá z deviatich bitov v nasledujúcom poradí:

- start bit
- 7 dátových bitov (LSB)
- stop (end) bit

Príkazy REQA a WUP sú vysielané terminálom, aby zistil, či sú nejaké karty dostupné v pracovnom rozsahu terminálu [12] [2].

Štandardné rámce
Štandardné rámce sa používajú pre pravidelnú výmenu dát, skladajú sa z:

- start bit
- n x (8 dátových bitov + paritný bit), $n \geq 1$
- stop (end) bit

Ak karta zmení svoj stav na pripravený (ready state), odošle odpoveď (ATQA – answer to request, typ A) terminálu po presne definovanom rámcovom meškaní (pauze). ATQA sa skladá z dvoch bajtoch, všetky ATQA správy sa odosielajú synchrónne. Ak terminál obdrží ATQA, zistí, že nejaká karta je v jeho pracovnom rozsahu a môže začať protikolízne opatrenia, ktoré umožňujú čítať unikátny identifikátor (UID) karty, zaslaním príkazu SELECT. Karta s odpovedajúcim identifikátorom zašle potvrdenie pre select (SAK) a zmení svoj stav na aktívny (active state). Karta v aktívnom stave môže komunikovať pomocou protokolov vyššej úrovne (sú definované v ISO / IEC 14443-4). Karta môže byť uvedená do stavu halt, zaslaním príkazu HLTA. Do stavu halt môže byť karta uvedená aj pomocou špeciálnych príkazov, ktoré patria do vyššej úrovne protokolov. V stave halt reaguje karta jedine na príkaz WUPA, na ktorý odpovedá ATQA a následne zmení svoj stav na ready*. Stav ready* je podobný stavu ready. Do stavu active* sa dostane po zaslaní potvrdenia na príkaz SELECT.

Postup používaný na prevenciu konfliktov a zistenie identifikátora, pracuje tak, že pokiaľ sú dve alebo viac kariet, v stave ready, v pracovnom rozsahu terminálu v ten istý čas, reagujú súčasne na príkaz SELECT, odpovedajú zasielaním časťou svojich identifikátorov, ktoré sú rôzne. To sa vykonáva pomocou špeciálneho bitovo-orientovaného rámca, ktorý umožňuje smer prenosu dát medzi kartou a terminálom obrátiť po prenesení určitého počtu bitov. Ak niekoľko kariet odovzdáva rôzne dáta súčasne, terminál bude primať dáta navrstvené od každej karty. Takto môže detekovať kolíziu, pretože navrstvenie spôsobí že signál bude modulovaný subsignálom po celú dobu jedného alebo viacerých bitových intervalov.

Aby terminál bol schopný detekovať kolíziu na úrovni bitov, musia všetky karty, v pripravenom stave, nachádzajúce sa v dosahu terminálu, musia reagovať na antikolízny príkaz presne v rovnakom čase. Toto načasovanie je špecifikované v ISO / IEC 14443-3 [12] [2].

2.3.2 Prehľad ďalších noriem

2.3.2.1 ISO/IEC 7816

ISO/IEC 7816 s anglickým názvom Identification Cards - Integrated Circuit Cards with Contacts je medzinárodné uznávaný štandard zaoberajúci sa kontaktnými kartami s integrovanými obvodmi, najmä čipovými kartami.

ISO 7816 je rad noriem primárne sa zaoberajúcich aspektmi interoperability čipových kariet týkajúcich sa komunikačných vlastnosti, fyzikálnych vlastnosti a použitia identifikátorov implantovaných čipov a dát [13].

Jednotlivé časti normy ISO/IEC 7816 sa aktualizujú, prebieha ich revízia. Štandard pozostáva z nasledujúcich častí [13]:

- časť 1: Fyzikálne charakteristiky
- časť 2: Rozmery a umiestnenie kontaktov
- časť 3: Elektrické rozhranie a prenosové protokoly
- časť 4: Organizácia, bezpečnosť a príkazy pre výmenu
- časť 5: Registrácia poskytovateľov aplikácií
- časť 6: Medziodborové dátové prvky pre výmenu
- časť 7: Medziodborové príkazy pre štruktúrovaný kartový dotazovací jazyk (SCQL)
- časť 8: Príkazy pre bezpečnostné príkazy
- časť 9: Príkazy pre správu kariet
- časť 10: Elektronické signály a odpoveď na reset pre synchrónne karty
- časť 11: Overovanie osôb biometrickými metódami
- časť 12: USB elektrické rozhranie a prevádzkové procedúry
- časť 13: Príkazy pre správu aplikácií v multi-aplikačnom prostredí
- časť 15: Kryptografické informačné aplikácie

Časť 14 normy ISO/IEC 7816 neexistuje.

2.3.2.2 ISO/IEC 10536

ISO/IEC 10536 štandard popisuje karty s blízkou väzbou, nesie originálny anglický názov Identification Cards – Contactless Integrated Circuit(s) Cards. Aplikácie podľa tohto štandardu sú označované ako slotovo, alebo povrchovo prevádzkové, čo vyjadruje že karty pri použití musia byť vložené do slotu, alebo priložené na vyznačené miesto na čítačku kariet [2].

Štandard sa skladá zo štyroch častí [2]:

- časť 1: Fyzikálne charakteristiky
- časť 2: Rozmery a umiestnenie spojových oblastí
- časť 3: Elektronické signály a reset procedúry
- časť 4: Odpoveď na reset a prenosové protokoly

Časti 1 až 3 sa už stali medzinárodnými štandardmi, zatiaľ čo časť 4 je stále v príprave.

Požiadavky pre tento štandard boli [2]:

- rozsiahla kompatibilita so štandardom ISO 7816
- prenosová frekvencia medzi 3 a 5 MHz
- prevádzka s ľubovoľne orientovanou kartou k čítačke kariet
- obojsmerný prenos dát s indukčnou alebo kapacitnou väzbou
- spotreba energie karty menej ako 150 mW (vhodné pre mikroprocesorové čipy)

2.3.2.3 ISO/IEC 15 693

Štandard s anglickým názvom Identification cards – Contactless integrated circuit(s) cards – Vicinity cards, popisuje vlastnosti a prevádzkové režimy bezkontaktných kariet s dosahom 1 až 1,5 metra. Systémy podľa tohto štandardu pracuje na frekvencií 13,56 MHz. Tento typ kariet sa využíva prednostne pri aplikáciách, u ktorých nie je nutné aby bola bezkontaktná karta v ruke užívateľa, môže ostať v peňaženke, kabelke, apod. Tento štandard však zatiaľ nenašiel široké využitie v systémoch čipových kariet [2].

2.4 Bezpečnosť kariet Mifare Classic

Mifare Classic karty sú najčastejším druhom využívaným pre bezkontaktné systémy, hlavným dôvodom je ich nízka cena. A však bezpečnosť Mifare Classic kariet je v súčasnej dobe takmer nulová. Karty využívajú šifrovanie CRYPTO-1, ktoré bolo prelomené a je možné ho prelomiť za pár sekúnd. Aj napriek tejto vážnej bezpečnostnej chybe, ktorú spoločnosť NXP Semiconductors verejne priznala, sa karty Mifare Classic naďalej s obľubou využívajú, keďže sú lacné.

Existuje viacero možností ako predísť zneužitiu bezkontaktnej čipovej karty Mifare Classic, ale nie je možné mu úplne zabrániť. Jedným zo spôsobom je využívať unikátne identifikačné číslo (UID) karty, ktoré sa zviaže s identitou držiteľa karty a nasledne je možné pomocou UID zistiť či je UID už v systéme zaznamenané, alebo nie a ide o klonovanú kartu. UID je zatiaľ nemodifikovateľné, ale je len otázkou času kedy bude táto vlastnosť prelomená.

Ani jeden zo spôsobov však neochráni Mifare Classic karty na 100% pred zneužití, či naklonovaním. Preto je najlepšou variantov prechod na vyššiu radu Mifare kariet, napríklad karty Mifare DesFire. Tieto karty sú však drahšie ako Classic karty, preto výmena za tieto karty nie je zatiaľ príliš obľúbená [14].

3 Návrh systému

Cieľom tejto bakalárskej práce je navrhnúť a implementovať systém aplikácií, ktorý umožní konfigurovať a personalizovať bezkontaktné čipové karty a následne autentifikovať držiteľov kariet pri vstupe do systému.

Základnou úlohou je vybrať správny hardware pre naše riešenie, čítačku bezkontaktných čipových kariet a samotné bezkontaktné čipové karty.

Ďalšou úlohou je navrhnúť aplikáciu pre konfiguráciu a personalizáciu bezkontaktných čipových kariet a aplikáciu pre autentifikáciu držiteľov bezkontaktných čipových kariet.

3.1 Vývojový kit

Jednou z hlavných úloh je vybrať čítačku bezkontaktných kariet. Dobrou alternatívou je vývojový kit. Pre naše riešenie bude použitý vývojový kit ACR128 SDK.

3.1.1 Vývojový kit ACR128 SDK

Kompletný vývojový kit pre programátorov a vývojárov v oblasti kontaktných a bezkontaktných čipových kariet (vid Obrázok 12).

Obsahuje duálnu USB čítačku čipových kariet ACR128, 5ks bezkontaktných čipových kariet Mifare 1K, 5ks kontaktných kariet ACOS3 a 1 kartu ACOS6 SAM pre testovanie aplikácií plus CD s dokumentáciou a softwarom pre programovanie aplikácií vrátane predpripravených programov a ukážok zdrojových kódov.

Obrázok 12: Vývojový kit ACR128 SDK [18]

Pre naše riešenie budeme využívať rozhranie čítačky pre bezkontaktné karty a vyžijeme Mifare 1K karty.

3.1.2 ACR128 DualBoost čítačka čipových kariet

ACR128 DualBoost je bezpečná, ekonomický navrhnutá čítačka s duálnym rozhraním. Je v súlade s normou ISO 7816 časť 1-3 pre kontaktné čipové karty a s normou ISO 14443 časť 1-4 pre bezkontaktné čipové karty.

Čítačka ACR128 umožňuje integrovať samostatné a nezávislé aplikácie pre kontaktné a bezkontaktné technológie. Využíva vysokorýchlostnú komunikáciu pre bezkontaktné karty, ktoré dosahuje až 848 kbps pre Mifare DESFire karty. Poskytuje podporu pre hybridné a kombinované karty a detekuje bezkontaktnú čipovú kartu aj keď je vložená do slotu pre kontaktné karty.

ACR128 má taktiež vstavaný SAM slot pre zvýšenie bezpečnosti a minimalizovanie poškodenia karty pre spoľahlivejšie operácie s kartou.

Duálna ACR128 čítačka využíva USB rozhranie, ktoré umožňuje ľahké pripojenie k PC. Je ideálna pre širokú škálu aplikácií, vrátane verejných dopravných terminálov, fyzické a logické kontroly prístupu, predajné automaty, apod [15].

3.1.2.1 Princíp SAM slotu

SAM (Secure Access Module) je ďalšia funkcia čítačky kariet, ktorá môže zvýšiť úroveň zabezpečenia vašich aplikácií.

Za normálnych okolností je autentifikácia karty vykonávaná v PC, alebo aplikačnej úrovni. Avšak, s prítomnosťou SAM, môže byť vzájomná autentizácia vykonaná medzi kartou a čítačkou, čo znamená, že PC nebude vykonávať overovanie, ale bude realizované ako card-to-reader a reader-to-card autentifikácia, čo zabezpečí váš systém aby bol viac bezpečný a menej náchylný na nabúranie [15].

3.1.2.2 Podporované typy čipových kariet

Kontaktné čipové karty

ACR128 pracuje s MCU kartami, ktoré sa riadia normou ISO 7816 T = 0 a T = 1 protokol.

Bezkontaktné čipové karty

ACR128 pracuje s rôznymi 13.56 MHz bezkontaktnými čipovými kartami, okrem iného podporuje:

- MIFARE karty (Classic, DESFire)
- karty podľa ISO 14443 Type A
- karty podľa ISO 14443 Type B

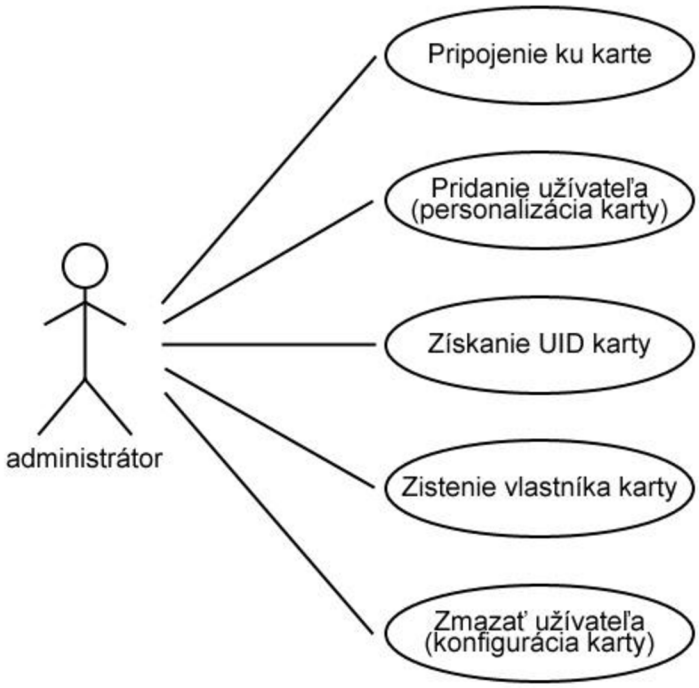
SAM podpora

ACR128 pracuje s SAM kartami, ktoré sa riadia normou ISO 7816 T = 0 a T = 1 protokol [15].

3.2 Konfigurácia a personalizácia čipových kariet

Aplikácia by mala obsahovať grafické užívateľské rozhranie. Je potrebné aby aplikácia pracovala s databázou, kde bude ukladať dáta a samozrejme bude komunikovať s ACR128 čítačkou čipových kariet.

Aplikácia by mala umožňovať taktiež jednoduché pridávanie nových užívateľov do databázy, vymazávanie užívateľov a zistenie vlastníka aktuálne priloženej čipovej karty (vid Obrázok 13).



Obrázok 13: Use Case Diagram aplikácie pre konfiguráciu a personalizáciu kariet

3.2.1 Návrh riešenia

Grafické užívateľské rozhranie aplikácie musí umožňovať vyvolanie nového dialógového okna pre pridanie nového užívateľa, kde bude možné vyplniť meno a priezvisko užívateľa, oddelenie v ktorom pracuje a vybrať práva prístupu z troch dostupných možností: zamestnanec, vedúci, riaditeľ.

Po vyplnení údajov a potvrdení by mala aplikácia uložiť tieto dáta do vytvorenej databázy a následne ID užívateľa, ktoré mu bolo pridelené v databáze, nakopírovať na bezkontaktnú čipovú kartu, ktorá je priložená k terminálu do bloku 1. Taktiež je potrebné zmeniť autentifikačný kľúč, z defaultného na autentifikačný kľúč zvolený pre naše riešenie. Pred samotnou operáciou zápisu ID a nového autentifikačného kľúča na čipovú kartu je potrebné overiť či je karta v defaultnom stave, tzn. že nie je ešte pridelená žiadnemu zamestnancovi. V prípade, že čipová karta má už svojho držiteľa, pridanie nového užívateľa musí skončiť chybou, vymaže sa záznam o novom používateľovi z databázy a vypíše sa chybové hlásenie.

Aplikácia by mala v svojom grafickom rozhraní zobrazovať všetkých pridaných užívateľov, ktorých by umožňovala vymazávať. Pri vymazávaní užívateľa je potrebné overiť či priložená karta k terminálu naozaj patrí príslušnému užívateľovi, ktorého chceme vymazať. Po úspešnej kontrole by mala byť karta nakonfigurovaná, vymazaním ID užívateľa, do defaultného stavu a následne by mal byť užívateľ vymazaný z databázy.

Ďalšou požadovanou vlastnosťou je zistenie užívateľa aktuálne priloženej čipovej karty. Aplikácia pomocou načítaného ID užívateľa z priloženej čipovej karty, zistí pomocou databázy a následné zobrazí informácie o užívateľovi.

Pre informatívny charakter by bolo vhodné implementovať možnosť zobrazenia sériového kľúča priloženej bezkontaktnej čipovej karty.

3.2.2 Návrh databázy

K vytvoreniu databázy bude použitý software Microsoft Access, ktorého výsledkom bude súbor s príponou .accbd. Základom riešenia bude jednoduchá databáza, ktorá umožní jedinečné generovanie

ID užívateľov, uloženie mena, priezviska a oddelenia pre každého užívateľa, tieto dáta budú uložené v jednej tabuľke (vid Obrázok 14).

K prístupu k databáze využijeme ODBC.

Obrázok 14: Navrhnutá databáza pre aplikáciu

3.2.2.1 ODBC

ODBC z anglického názvu Open Database Connectivity, je rozhranie, ktoré umožňuje aplikáciám prístup k dátam z rôznych systémov pre správu databáz (DBMSs - database management systems). ODBC je nízkoúrovňové, vysokovýkonné rozhranie, ktoré je navrhnuté špeciálne pre ukladanie relačných dát a bolo vyvinuté SQL Access skupinou v roku 1992.

ODBC vkladá strednú vrstvu, tzv. databázový ovládač, medzi aplikáciu a systém pre správu databáz. Účelom tejto vrstvy je prekladať dátové dotazy aplikácie do príkazov, ktorým systém pre správu databáz rozumie.

Rozhranie ODBC umožňuje maximálnu interoperabilitu. Aplikácia môže pristupovať k dátam v rôznych systémoch pre správu databáz prostredníctvom jediného rozhrania. Okrem toho je aplikácia nezávislá na akomkoľvek systéme pre správu databáz, z ktorých sa pristupuje k dátam [16].

3.3 Autentizácia osôb pri vstupe do systému

Na autentifikáciu osôb, poslúži aplikácia, ktorá bude obsahovať grafické užívateľské rozhranie, v ktorom by malo byť možné nastaviť prístupové práva pre určitý typ (zamestnanec, vedúci, riaditeľ) užívateľov. Aplikácia by mala po priložení čipovej karty k čítačke kariet autentifikovať užívateľa, ktorý je držiteľom karty a na základe nastavených práv vyhodnotiť prístup do systému a informovať o výsledku užívateľa.

3.3.1 Návrh riešenia

Po spustení by mala aplikácia umožniť nastavenie práv pre prístup do systému. Následne by malo byť možné zapnúť sledovanie zmenu stavu čítačky kariet a po detekovaní karty previesť autentifikáciu. Taktiež by malo byť možné vypnúť toto sledovanie, aplikácia pri vypnutom stave by mala slúžiť na nastavenie prístupových práv.

Aplikácia bude mať informatívny charakter a mala by slúžiť na otestovanie implementovaného riešenia. Pre využitie v praxi by bolo potrebné navrhnúť a implementovať rozsiahlejšiu aplikáciu, ktorá by okrem čítačky kariet komunikovala aj s ďalším hardwarom, napr. elektronickým zámok, turniketom, a pod.

4 Implementácia

Praktické riešenie je zložené z dvoch častí. Pozostáva z aplikácie pre personalizáciu a konfiguráciu bezkontaktných kariet a aplikácie, ktorá sleduje aktiváciu čipovej karty na terminál, po detekovaní priloženej karty autentifikuje užívateľa a vyhodnotí prístupové práva držiteľa karty.

Naše aplikácie boli vyvinuté vo vývojovom prostredí Microsoft Visual Studio 2008, napísane v jazyku C++ pod operačným systémom Windows 7. Ku komunikácií s čítačkou kariet sme využili knižnicu *winscard.h* [17], všetky spomenuté funkcie v implementácií, ktorých názov začína spojením „*SCard*“ sú práve funkcie popísané v tejto knižnici.

4.1 Popis Implementácie

Aplikácie boli implementované podľa vytvoreného návrhu riešenia. Ako v aplikácií pre konfiguráciu a personalizáciu kariet tak aj v aplikácií pre kontrolu a vyhodnocovanie povolenia pre prístup boli implementované zhodné funkcie. Funkcia *GetErrMsg()* pre získanie chybového hlásenia podľa navráteného čísla chyby, ktorá mohla vzniknúť pri komunikácií s terminálom. Funkcia *clearBuffers()* vyprázdni prijímací aj odosielací buffer. Funkcia *sendApdu()* odošle odosielací buffer, v ktorom je uložená inštrukcia, ktorá sa ma vykonať, pomocou funkcie *SCardTransmit()*, ktorá vracia návratový kód a v prijímacom buffry sú vrátené dáta odpovedajúce zaslane inštrukcii a návratový kód tejto inštrukcie. Funkcie *loadKey()* a *authCard()* slúžia k autentifikácií prístupu na kartu, funkcia *loadKey()* nahrá kľúč do pamäte čítačky kariet, následne pomocou implementovanej funkcie *authCard()* autentizujeme kľúč nahraný v karte s kľúčom v bloku ku ktorému chceme pristupovať.

Pri každom prístupe na kartu, musí prebehnúť autentifikácia pomocou kľúča. V implementovanom riešení sa využíva kľúč typu A s hodnotou F1 F2 F3 F4 F5 F6. Kľuč sa nahrá do pamäte čítačky kariet. Čítačka umožňuje nahranie viacero kľúčov do pamäte. Následne prebehne autentifikácia s vybraným kľúčom a s číslom bloku ku ktorému chceme pristupovať. Každý sektor na karte ma vlastný kľuč.

4.2 Nahranie autentizačných kľúčov

Príkaz pre nahranie autentizačného kľúča nahrá kľúč do pamäte čítačky kariet. Existujú dva druhy umiestnenia v energeticky závislej pamäti a v energeticky nezávislej pamäti. V našich aplikáciách využívame energeticky závislú pamäť a kľúč s hodnotou F1 F2 F3 F4 F5 F6. Tento kľúč je použitý k overovaniu prístupu k danému sektoru Mifare kariet.

Príkaz	Trieda	Inštrukcia	P1	P2	Lc	Dáta
Nahranie autentizačného kľúča	FF	82	Štruktúra kľúča	Číslo kľúča	06	Kľúč (6 bytov)

Tabuľka 4: Štruktúra príkazu pre nahranie autentizačného kľúča [15]

Štruktúra kľúča (1 Byte):

- 0x00 – Kľuč je nahraný v energeticky závislej pamäti
- 0x20 – Kľúč je nahraný v energeticky nezávislej pamäti
- Ostatne hodnoty sú rezervované

Číslo kľúča (1 Byte):

- 0x00 - 0x1F – číslo kľúča, ktorý je nahraný v energeticky nezávislej pamäti. Kľúče po odpojení čítačky kariet nebudú vymazané. Energetická nezávislá pamäť umožňuje nahranie 32 kľúčov
- 0x20 – kľúč je nahraný v energeticky závislej pamäte, ktorá umožňuje nahranie len jedného kľúča. Predvolená hodnota = { FF FF FF FF FF FF }

Kľúč (6 Bytov):

- Hodnota kľúča, ktorá je nahraná do pamäte čítačky

Odpoveď na príkaz (2 byte):

- 90 00 – operácia bola úspešná
- 63 00 – operácia bola neúspešná

4.3 Autentifikácia

Pri autentifikácia s Mifare kartou sa využíva kľúč z pamäte čítačky kariet a kľúč na Mifare karte, existujú dva typy autentizačných kľúčov typ A a typ B.

Príkaz	Trieda	Inštrukcia	P1	P2	Lc	Dáta
Autentifikácia	FF	86	00	00	05	Autentifikačné dáta (5 bytov)

Tabuľka 5: Štruktúra príkazu pre autentifikáciu [15]

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
Verzia 0x01	0x00	Číslo bloku	Typ kľúča	Číslo kľúča

Tabuľka 6: Štruktúra autentifikačných dát v príkaze pre autentifikáciu [15]

Číslo bloku (1 byte):

- číslo pamäťového bloku, ktorý sa bude autentifikovať

Typ kľúča (1 byte):

- 0x60 – Pre autentifikáciu sa použije kľúč ako Typ A
- 0x61 – Pre autentifikáciu sa použije kľúč ako Typ B

Číslo kľúča (1 byte):

- 0x00 - 0x1F – číslo kľúča, ktorý je nahraný v energeticky nezávislej pamäti. Kľúče po odpojení čítačky kariet nebudú vymazané. Energetická nezávislá pamäť umožňuje nahranie 32 kľúčov
- 0x20 – kľúč je nahraný v energeticky závislej pamäte, ktorá umožňuje nahranie len jedného kľúča.

Odpoveď na príkaz (2 byte):

- 90 00 – operácia bola úspešná
- 63 00 – operácia bola neúspešná

4.4 Čítanie binárnych dát

Pomocou príkazu pre čítanie binárnych dát môžeme čítať z bezkontaktnej čipovej karty bloky dát. Pred načítaním musí byť blok dát autentifikovaný.

Príkaz	Trieda	Inštrukcia	P1	P2	Le
Čítanie binárnych dát	FF	B0	00	Číslo bloku	Počet bytov k načítaniu

Tabuľka 7: Štruktúra príkazu pre načítanie dát [15]

Číslo bloku (1 byte):

- číslo pamäťového bloku, od ktorého začína načítanie dát

Počet bytov k načítaniu (1 byte):

- počet bytov, ktoré majú byť načítané. U Mifare kariet 1K/4K sa musí jednať o násobky čísla 16, maximum je 48 u Mifare 1K a 240 u Mifare 4K

Odpoveď na príkaz (násobok 4/16 bytov + 2 byty):

- výstupné dáta (násobok 4/16 bytov) – načítané dáta z karty
- návratový kód (2 byty):
  90 00 – operácia bola úspešná
  63 00 – operácia bola neúspešná

4.5 Zápis binárnych dát

Príkaz pre zápise binárnych dát umožňuje zapísať dáta do blokov na bezkontaktnej čipovej karte. Pred načítaním musí byť blok dát autentifikovaný.

Príkaz	Trieda	Inštrukcia	P1	P2	Lc	Dáta
Zápis binárnych dát	FF	D6	00	Číslo bloku	Počet bytov k zápisu	Dáta k zapísaniu

Tabuľka 8: Štruktúra príkazu pre zápis dát [15]

Číslo bloku (1 byte):

- číslo pamäťového bloku, od ktorého začína zápis dát

Počet bytov k zápisu (1 byte):

- počet bytov, ktoré majú byť zapísané. U Mifare kariet 1K/4K sa musí jednať o násobky čísla 16, maximum je 48 u Mifare 1K a 240 u Mifare 4K

Dáta k zapísaniu (násobky 16 + 2 byty, alebo 6 bytov):

- dáta, ktoré budú zapísané do binárnych blokov na karte

Odpoveď na príkaz (2 byte):

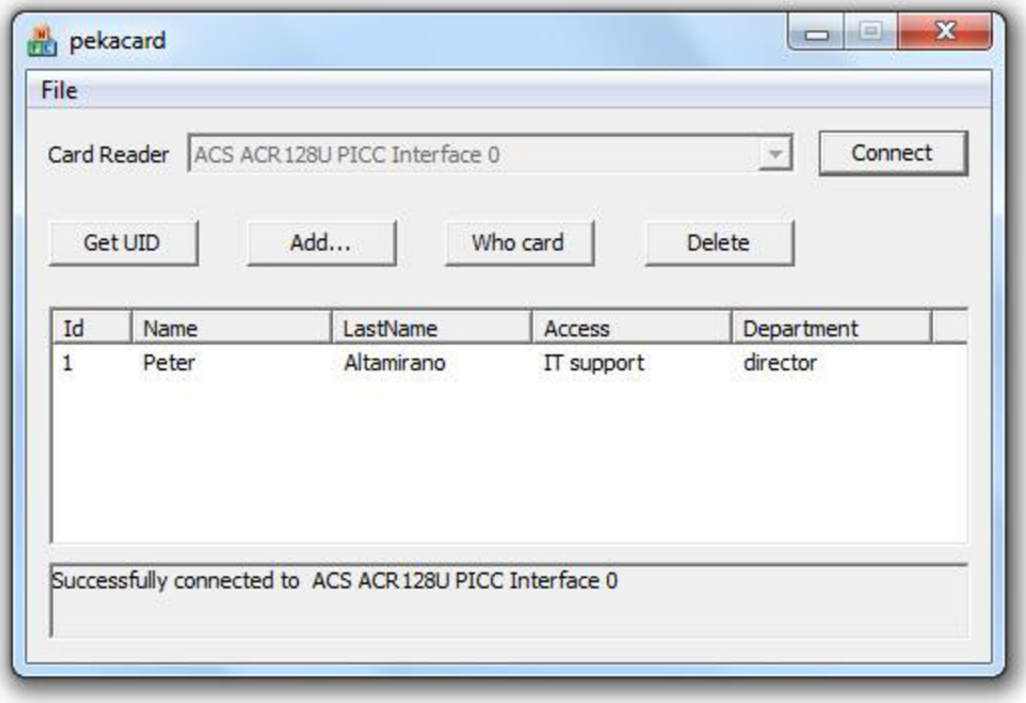
- 90 00 – operácia bola úspešná
- 63 00 – operácia bola neúspešná

4.6 Konfigurácia a personalizácia čipových kariet

Aplikácia inicializuje pripojenú čítačku kariet a zobrazí grafické užívateľské rozhranie (vid Obrázok 15). Grafické rozhranie obsahuje tlačidlo „*Connect*" pre nadviazanie komunikácie s priloženou čipovou kartou k terminálu, tlačidlo „*Add*" pre pridanie nového užívateľa do databázy automatické nakonfigurovanie karty pre tohto užívateľa, tlačidlo „*Delete*" pre vymazanie užívateľa z databázy a automatické nakonfigurovanie karty do pôvodného stavu, tlačidlo „*Who card*" pre zistenie vlastníka aktuálne pripojenej bezkontaktnej karty. Grafické rozhranie obsahuje taktiež pole pre výpis všetkých užívateľov z databáze, stavový riadok, kde sa zobrazujú statusy o aktuálne vykonaných operáciách a taktiež systémové menu aplikácie s položkami „*About*", zobrazí dialógové okno o aplikácií, a položkou „*Exit*", ukončí aplikáciu.

Aplikácia obsahuje taktiež systémové menu, ktoré ma dve položky. Po kliknutím na položku „*About*" vyvoláme nové dialógové okno, ktoré zobrazuje informácie o programe. Kliknutím na položku „*Exit*" uzavrieme aplikáciu.

Pri spustení aplikácie je sprístupnené len tlačidlo „*Connect*", ostatné tlačidlá sa sprístupnia až po úspešnom pripojení k priloženej karte na termináli.



Obrázok 15: Grafické užívateľské rozhranie aplikácie pre konfiguráciu a personalizáciu kariet

4.6.1 Inicializácia čítačky bezkontaktných čipových kariet

Po spustení aplikácie zabezpečí inicializáciu čítačky implementovaná funkcia *initAcrReader()*. K nadviazaniu spojenia sa využíva funkcia *SCardEstablishContext()*, ktorá detekuje všetky prístupne čítačky kariet, pomocou funkcie *SCardListReaders()* získame zoznam mien pripojených čítačiek kariet.

4.6.2 Nadviazanie spojenia s kartou

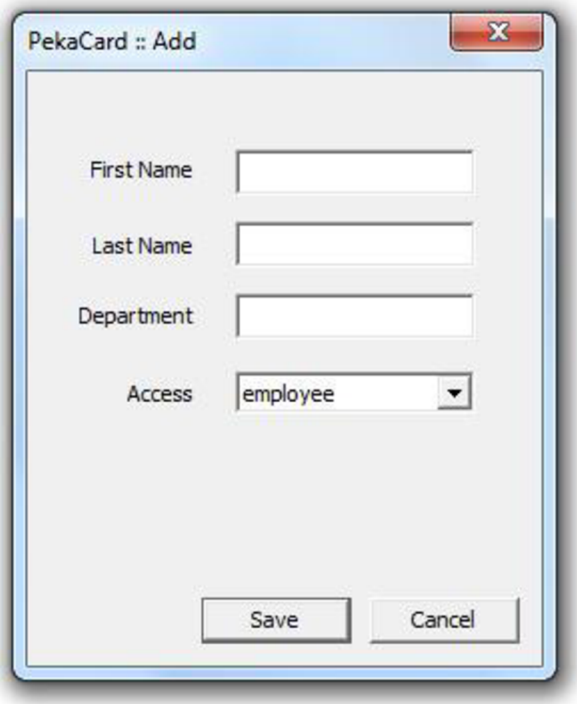
Kliknutím na tlačidlo „*Connect*“ sa zavolá funkcia *connectToReader()*, ktorá nadviaže spojenie s priloženou kartou k čítačke kariet pomocou funkcie *SCardConnect ()*, ktorej sa predá ako jeden z parametrov meno čítačky kariet a protokol.

4.6.3 Pridávanie nových užívateľov

V novom dialógovom okne, ktoré sa vyvolá po stlačení tlačidla „*Add*“, sa nachádzajú text boxy pre vyplnenie, mena, priezviska, oddelenia a comboBox pre výber práv prístupu pre nového užívateľa (vid Obrázok 16). Aplikácia umožňuje vybrať z troch typov prístupových práv employee, manager, director. Po stisnutí tlačidla „*Save*“, prebehne kontrola vyplnených údajov, po úspešnej kontrole je volaná funkcia *addToDatabase()*, ktorá pridá nového užívateľa do databázy a následne funkcia *sendIdToCard()* nahrá id užívateľa na kartu do bloku 1. Pri neúspešnej konfigurácií karty sa zavolá funkcia *deleteFromDatabase()* aby odstránila pridaného užívateľa, ku ktorému nebola úspešne nakonfigurovaná karta.

Pred nahraním id na kartu je potrebné nahrať defaultný kľúč (FF FF FF FF FF FF) do pamäte čítačky, to zabezpečí funkcia *loadKey()*, pomocou kľúča funkcia *authCard()* autentizuje prístup k bloku na karte. Funkcia *isEmpty()* otestuje či je karta prázdna, tzn. nie je pridelená žiadnemu inému užívateľovi a používa defaultný kľúč (FF FF FF FF FF FF).

Po úspešnej autentifikácií a karty, zabezpečí funkcia *sendApdu()* nahranie id na kartu do bloku 1 a zmenenie defaultného kľúča na autentifikačný kľúč s hodnotou F1 F2 F3 F4 F5 F6. Pomocou funkcie *SCardTransmit()* sa odošle príkaz s nastavenými hodnotami.



Obrázok 16: Grafické užívateľské rozhranie dialógového okna pre pridanie nového užívateľa

4.6.4 Zistenie vlastníka karty

Funkcia *whoCard()* vypíše informácie o užívateľovi, ktorému patrí karta priložená k terminálu. Na kartu pristupuje pomocou kľúča, ktorý sa funkciou *loadKey()* nahrá do pamäte čítačky a následne

funkcia *authCard()* použije tento kľúč k prístupu k bloku, kde je uložene id užívateľa. Funkcia *readId()* zašle príkaz na kartu a získa id užívateľa. Id spolu s ďalšími údajmi zobrazí v okne.

4.6.5 Odmazávanie užívateľov

V poli, kde sú vypísaní všetci užívatelia, je potrebné vybrať konkrétneho užívateľa, ktorého chceme odstrániť. Po vybraní a priložení užívateľovej čipovej karty k terminálu stlačením tlačidla „*Delete*“ sa karta automaticky nakonfiguruje do pôvodného stavu, je zavolaná funkcia *deleteCard()*, ktorá autentizuje prístup pomocou funkcií *loadKey()* a *authCard()*, následne funkcia *isRightCard()* overí či sa jedná skutočne o kartu patriacu užívateľovi, ktorého chceme odstrániť. Odošle sa na kartu príkaz, ktorý vynuluje id užívateľa na karte a nastaví defaultný autentifikačný kľúč. Po úspešnej konfigurácií sa užívateľ odstráni z databázy pomocou funkcie *deleteFromDatabase()*. Karta je pripravená k znovu prideleniu novému užívateľovi.

4.6.6 Zobrazenie identifikačného čísla karty

Táto funkcia aplikácie ma len informačný charakter. Po stlačení tlačidla Get UID sa zobrazí identifikačné číslo, vyvolaním implementovanej funkcie *getUid()*.

4.7 Autentizácia osôb pri vstupe do systému

Aplikácia inicializuje pripojenú ACR128 čítačku kariet a zobrazí grafické užívateľské rozhranie, ktoré umožňuje nastaviť prístupové práva a spustenie sledovania zmenu stavu čítačky kariet (vid Obrázok 17).

Po spustení aplikácií je sprístupnený box, v ktorom je možné vybrať z troch typov prístupových práv employee, manager, director. Po vybraní typu užívateľov, ktorým umožníme prístup do systému sprístupneným tlačidlom *START* sa spustí detekovanie čipových kariet priložených k čítačke kariet. Tlačidlo *STOP* je po spustení aplikácie neprístupne. Po stlačení tlačidla *START* sa tlačidlo *START* zneprístupní a tlačidlo *STOP* sa sprístupní. Následne sa funkciou *AfxBeginThread()* vytvorí nové vlákno, ktoré vykonáva kód popísaný vo funkcií MyThreadProc(). V tejto funkcií je vyvolaná funkcia checkChange(), ktorá kontroluje zmenu stavu čítaťky kariet pomocou funkcie SCardGetStatusChange(). Po zistení zmenu stavu čítačky kariet sa pokúsi aplikácia nadviazať spojenie s priloženou čipovou kartou funkciou connectToReader(). Pri neúspešnom nadviazaní komunikácie sa vráti aplikácia spať do stavu kedy sleduje zmenu čítačky kariet. Po úspešnom nadviazaní komunikácie s priloženou akrtou k čítačke je vyvolaná funkcia checkAccess(), ktorá zabezpečí vyhodnotenie prístupu pre daného užívateľa. Funkciou loadKey() nahrá autentifikačný kľúč do pamte čítačky kariet, funkciou authCard() vykoná autentifikáciu s kartou. Následne pomocou funckie readId() načíta ID užívateľa uložené na karte a volaní funkcie getAccess(), zistí na základe načítaného ID aké ma užívateľ práva prístupu, tie porovná s akualne nastavenými právami a vyhodnoti či má daný užívateľ pravo na prístup alebo nema. V prípade povolenia prístupu vypíše aplikácia hlášku „*Access allowed !*“, v prípade zamietnutia prístupu vypíše „*Access not allowed !*“.

Po stlačení tlačidla STOP sa detekcia zmenu stavy čítačky kariet zastaví a vytvorené vlákno sa ukončí.

Obrázok 17: Grafické užívateľské rozhranie aplikácie pre autentifikáciu užívateľov

Aplikácia využíva system tray menu operačného systému Windows. Po minimalizovaní aplikácie sa aplikácia zobrazuje v system tray menu, v task bare operačného systému sa aplikácia nezobrazuje. Po dvoj-kliknutí na ikonu v system tray menu sa aplikácia maximalizuje a zobrazí sa taktiež v task bare. Pravým kliknutím na system tray ikonu vyvoláme vyskakovacie menu, ktoré obsahuje tri položky. Kliknutím na položku „*Open*“ sa aplikácia maximalizuje, po kliknutí na položku „*About*“ sa zobrazí dialógové okno, ktoré obsahuje informácie o programe, kliknutím na poslednú položku „*Exit*“ aplikácia vyvolá potvrdzovacie okno, v ktorom po kliknutí na tlačidlo „Yes“ potvrdíte zatvorenie programu a program sa ukončí. Po kliknutí na tlačidlo „*No*“ sa aplikácia neukončí.

4.8 Zhodnotenie implementovaného riešenia

Implementované riešenie napĺňa požiadavky navrhovaného riešenia. Riešenie sa podarilo implementovať v navrhovanom rozsahu a spĺňa všetky navrhované funkcie. Implementované riešenie slúži k oboznámeniu sa s technológiou, personalizáciou a konfiguráciu bezkontaktných čipových kariet. Približuje princípy programovania aplikácií pre bezkontaktné čipové karty Mifare podľa ISO/IEC 14443 štandardu. V prípade rozšírenia implementovaného riešenia, môže byť v systém nasadený a využitý aj v praxi.

4.9 Ďalšie možné rozšírenia systému

Vyvinuté aplikácie sa môžu ďalej rozvíjať rôznymi smermi. Implementované riešenie obsahuje základne možnosti práce s bezkontaktnými čipovými kartami. Poskytuje dobrý základný kameň pre ďalšie rôzne rozšírenia a ďalší vývoj aplikácií.

Pre využitie v praxi by bolo dobre aplikáciu pre autentifikáciu užívateľov prepojiť s ďalším hardwarom, napríklad elektronickým zámkom, ktorý by umožňoval v prípade povolenia prístupu automaticky odomknúť dvere držiteľovi karty, ďalšou možnosťou je prepojenie s turniketom, ktorý by mohol následne riadiť prístup do systému, napríklad vstup do budovy, a pod.

S myšlienkou rozvinúť systém tak aby mohol byť nasadený v praxi nesmieme zabúdať ani na stránku bezpečnosti, preto by bolo dobré zvážiť použitie aj druhého autentifikačného kľúču typu B, nastavenie prístupových bitov, ktoré by neumožňovali meniť autentifikačné kľúče a taktiež možnosť nasadenia bezpečnejších kariet Mifare DesFire namiesto Mifare Classic, ktorých bezpečnosť už bola prelomená.

Ďalšou možnosťou je rozšírenie aplikácie na personalizáciu kariet, rozšíriť záznamy v databáze, pridanie užívateľom časové intervaly v ktorých majú prístup do systému.

V prípade využívania systému na kontrolu prístupu by bolo vhodne implementovať zaznamenávanie prístupov do databázy, čas prístupu a id užívateľa, ktorý vstúpil do systému.

Implementované riešenie umožňuje naozaj veľký priestor pre rozšírenia, je potrebné rozhodnúť sa aké využitie budú mať implementované aplikácie v praxi a týmto smerom uberať ďalší vývoj a rozvoj aplikácie.

5 Záver

Cieľom tejto práce bolo oboznámiť sa s technológiou bezkontaktných čipových kariet Mifare, princípom komunikácie s týmito kartami, princípmi konfigurácie a personalizácie kariet a na základe týchto poznatkov navrhnúť a implementovať vhodné riešenie pre konfiguráciu a presonalizáciu bezkontaktných čipových kariet.

Na základe naštudovanej problematiky bezkontaktných čipových kariet bol vytvorený návrh riešenia a úspešná implementácia systému podľa navrhovaného riešenia.

Aplikácia pre konfiguráciu a personalizáciu bezkontaktných čipový kariet umožňuje pohodlnú personalizáciu čipových kariet pre používateľov systému. Aplikácia pre autentifikáciu osôb, následne vyhodnocuje povolenia pre prístup do systému a kontroluje vstup do systému.

Táto práca okrem oboznámenia technológie bezkontaktných čipových kariet poskytla možnosť zdokonaliť sa v objektovom programovaní, vo vývoji aplikácií v prostredí operačného systému Windows a taktiež bližšie poznanie vývojového prostredia Microsoft Visual Studia.

Implementované riešenie umožňuje veľké množstvo rozšírení a bude určite nápomocné pri mojom ďalšom osobnom rozvoj v oblasti technológií bezkontaktných čipových kariet, ktorej by som sa rád v budúcnosti venoval, preto bola táto bakalárska práca pre mňa osobne veľmi prospešná.

Literatúra

[1] KLAUS, Finkenzeller. *RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification*. 2nd Edition. [s.l.] : John Wiley & Sons, 2003. 446 s. ISBN 0-470-84402-7.

[2] RANKL, Wolfgang; EFFING, Wolfgang. *Smart Card Handbook*. 3rd edition. [s.l.] : John Wiley & Sons, 2003. 1088 s. ISBN 0-470-85668-8.

[3] *Smart Cards, Tokens, Security and Applications*. Edited by Keith E. Mayes, Konstantinos Markantonakis. [s.l.] : Springer - Verlag, 2008. 406 s. ISBN 978-0-387-72197-2.

[4] *NXP Semiconductors* [online]. 2006, 2010 [cit. 2010-02-14]. Mifare Classic from NXP Semiconductors. Dostupné z WWW: <http://www.nxp.com/#/homepage/cb=[t=p,p=/53420/71108/53422/41863]|pp=[t=pfp,i=41863]>.

[5] *MIFARE.net : contactless smart cards RFID* [online]. 2002, 2008 [cit. 2010-02-15]. MIFARE Smartcard IC's. Dostupné z WWW: <http://www.mifare.net/products/smartcardics/index.asp>.

[6] *MIFARE.net : contactless smart cards RFID* [online]. 2002, 2008 [cit. 2010-03-20]. MIFARE Milestones. Dostupné z WWW: <http://www.mifare.net/about/milestones.htm>.

[7] MIFARE#History In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , 13. 5. 2010 [cit. 2010-05-14]. Dostupné z WWW: <http://en.wikipedia.org/wiki/MIFARE#History>.

[8] *NXP Semiconductors - MF1ICS50 : Functional specification*. [s.l.] : [s.n.], 2007. 19 s. Dostupné z WWW: <http://www.nxp.com/acrobat_download2/other/identification/001055.pdf>.

[9] ISO 14443-1. *Identification cards - Contactless integrated circuit(s) cards - Proximity cards : Part 1: Physical characteristics*. Geneva, Switzerland : ISO, 2008. 4 s. Dostupné z WWW: <http://www.waazaa.org/download/fcd-14443-1.pdf>.

[10] ISO/IEC 14443-2. *Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards : Part 2: Radio frequency power and signal interface*. Geneva, Switzerland : ISO , 2001. 15 s. Dostupné z WWW: <http://www.waazaa.org/download/fcd-14443-2.pdf>.

[11] ISO/IEC 14443-3. *Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards : Part 3: Initialization and anticollision*. Geneva, Switzerland : ISO , 2001. 32 s. Dostupné z WWW: <http://www.waazaa.org/download/fcd-14443-3.pdf>.

[12] ISO/IEC 14443-4. *Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards : Part 4: Transmission protocol*. Geneva, Switzerland : ISO, 2008. 32 s. Dostupné z WWW: <http://www.waazaa.org/download/fcd-14443-4.pdf>.

[13] ISO In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , 2. 5. 2010 [cit. 2010-05-14]. Dostupné z WWW: <http://en.wikipedia.org/wiki/ISO/IEC_7816>.

[14] *Nethemba* [online]. 2009 [cit. 2010-05-01]. Oficiálne zverejnenie zraniteľností slovenských a českých Mifare Classic kariet. Dostupné z WWW: <http://www.nethemba.com/mifare-classic-zranitelnosti.pdf>.

[15] *Advanced Card Systems Ltd* [online]. 2008 [cit. 2010-04-28]. ACR128U Dual-Interface Reader. Dostupné z WWW: <http://www.acs.com.hk/drivers/eng/API_ACR128_v1.9.pdf>.

[16] *MSDN: Microsoft Developer Network* [online]. 2010 [cit. 2010-04-25]. Microsoft Open Database Connectivity (ODBC). Dostupné z WWW: http://msdn.microsoft.com/en-us/library/ms710252%28VS.85%29.aspx.

[17] *PCSC-Lite Home page on Alioth* [online]. 2009 [cit. 2010-04-05]. Pcsc-lite: winscard.h File Reference.
Dostupné z WWW: <http://pcsclite.alioth.debian.org/api/winscard_8h.html>.

[18] *R.A.S., spol. s.r.o.* [online]. 1994, 2010 [cit. 2010-05-16]. ACR128 SDK . Dostupné z WWW: <http://rassro.cz/vyvojove-kity-sdk/acr128-sdk-pro-programatory-a-vyvojare.html>.

Zoznam príloh

Príloha 1. CD obsahujúce zdrojové texty aplikácií a technickú správu bakalárskej práce