Plastové karty jako prostředek identifikace i mobilních plateb

Plastic cards as a means of identification and mobile payments

Bc. Miroslav Skoumal

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Miroslav SKOUMAL**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Plastové karty jako prostředek identifikace i mobilních plateb**

Zásady pro vypracování:

1. **Vytvořte literární rešerši na téma Využití plastových karet.**
2. **Zmapujte jednotlivé technologie karet kontaktních i bezkontaktních.**
3. **Rozveďte podrobně otázku bezpečnosti karet a to včetně testu zneužití.**
4. **Prakticky otestuje metody zápisů i čtení na paměťové karty.**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **JUŘÍK, Pavel. Platební karty : Velká encyklopedie 1870–2006. [s.l.] : Grada, 2009. 296 s. ISBN 80-247-1381-0.**
2. **JUŘÍK, Pavel. Svět platebních a identifikačních karet. 2. dopl. vyd. [s.l.] : Grada, 2001. 184 s. ISBN 80-247-0195-2.**
3. **ZOBANÍK, Kamil. Trendy vývoje identifikačních prostředků osob. [s.l.], 2007. 85 s. Diplomová práce na Fakultě aplikované informatiky Univerzity Tomáše Bati. Vedoucí diplomové práce doc. Ing. Luděk Lukáš, CSc.**
4. **STOPPANI, David. IN-KARTA moderní multiplikační karta společnosti České dráhy, a.s. [s.l.], 2006. 88 s. Diplomová práce na Fakultě aplikované informatiky Univerzity Tomáše Bati. Vedoucí diplomové práce Doc. Ing. Ivan Zelinka, Ph.D.**
5. **What is a smart card [online], Dostupné z: http://computer.howstuffworks.com/question332.htm**
6. **Smart card alliance: Contactless technology for secure physical access: Technology and standard choices, [online], Dostupné z: http://www2.cnipa.gov.it/site/_contentfiles/01379900/1379995_Contactless_Technology_Repc**
7. **National institute of standards and technology:Government smart card interoperability specification, [online], Dostupné z: http://csrc.nist.gov/groups/SNS/smartcard/overview.html**
8. **Handschuh, H. Dr.: Contactless technology security issues, security Technologies department Gemplus, Information Security Bulletin, April 2004, [online], Dostupné z: http://www.chi-publishing.com/samples/ISB0903HH.pdf**

Vedoucí diplomové práce: **Ing. Tomáš Sysala, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce je zaměřena na způsoby využití plastových karet. Obsahuje detailní popis tohoto identifikačního prostředku. První část je zaměřena na technologické vlastnosti karet, jejich výrobu a následné zpracování. Jedním z témat je zmapování možných způsobů jejich využití, a s tím související bezpečnosti dat, protože obyčejné karty s potiskem ale i inteligentní karty tedy čipové jsou již běžnou součástí našeho života. Cílem práce je také zaměřit se na nejnovější technologie související s čipovými kartami a uvést konkrétní příklad využití v praxi. V praktické části jsou popsány testy s plastovými kartami jako kódování a čtení dat z mikročipů nebo jejich potisk s využitím profesionálních zařízení.

Klíčová slova: plastová karta, čipová karta, magnetický proužek, EMV, Mifare, NFC, RFID, mobilní platba, identifikace, autentifikace,

ABSTRACT

This thesis is dwell on ways plastic cards utilization. It includes detailed description of this identification subservience. Forepart is centred on technological properties of cards, mode of production and after processing. One of themes is mapped available means of utilization and data safeness related, because usual cards with printing but also ïntelligent cards so chip cards are routine part of our life. Tendency of this thesis is target on the newest technology chip cards related too and concrete illustrate utilization in practice. In practically part are described tests with plastic card like encoding and data reading of microchips or their printig with utilization of professional equipment.

Keywords: plastic card, smart card, chip, magnetic stripe, EMV, Mifare, NFC, RFID, mobile payment, identification, authentification

Rád bych na tomto místě poděkoval Janu Šrejberovi za poskytnuté informace při realizaci mé diplomové práce a také za zapůjčení zařízení k praktickým testům.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **9**

I TEORETICKÁ ČÁST **10**

1 VÝVOJ PLASTOVÝCH KARET **11**

1.1 IDENTIFIKAČNÍ PROSTŘEDKY 11

1.2 OD PAPÍRU K IDENTIFIKAČNÍM KARTÁM 12

2 TECHNOLOGIE PLASTOVÝCH KARET **13**

2.1 VÝROBA KARET 13

2.2 POTISK KARET 14

2.2.1 Přímý tisk: termotransfér a termosublimace 14
2.2.2 Nepřímý tisk: termo re-transfér 15
2.2.3 Offetový tisk 15
2.2.4 Digitální tisk 16
2.2.5 Další povrchové úpravy karet 16
2.2.6 Standardy a normy 17

3 KARTA JAKO DATOVÝ NOSIČ **18**

3.1 MAGNETICKÉ KARTY 19

3.2 ČIPOVÉ KARTY 21

3.2.1 Kontaktní čipové karty 23
3.2.2 Bezkontaktní čipové karty 26
3.2.3 Hybridní čipové karty 27
3.2.4 RFID, NFC a další technologie 28
3.2.5 Přenosový protokol čipových karet 29
Protokol přenosu bezkontaktních čipových karet 31

4 VYUŽITÍ PLASTOVÝCH KARET **33**

4.1 PLATEBNÍ KARTY 35

4.1.1 Historie platebních karet 35
4.1.2 Historie bankovních karet 36
4.1.3 Způsoby použití karty 38
4.1.4 Placení v obchodní síti 42
4.1.5 Výběry hotovosti 42
4.1.6 Rozdělení platebních karet 44
4.1.7 EMV 48

4.2 BUDOUCNOST KARET 49

5 ZABEZPEČENÍ DAT NA KARTĚ **50**

5.1 GRAFICKÉ OCHRANNÉ PRVKY 50

5.2 BEZPEČNOST ČIPOVÝCH KARET 52

5.2.1 Interní fyzické útoky 56
5.2.2 Logické útoky 58
5.2.3 Postraní útoky 62
5.2.4 Hrozby bezkontaktních čipových karet 64

5.2.5 Rozšíření čipových karet 64
II PRAKTICKÁ ČÁST 66
6 PRAKTICKÉ TESTY KARET 67
6.1 POTISK PLASTOVÉ KARTY 67
6.2 KÓDOVÁNÍ A ČTENÍ MAGNETICKÝCH KARET 70
6.3 ČTENÍ RFID KARET 75
6.4 KÓDOVÁNÍ A ČTENÍ BEZKONTAKTNÍCH KARET 77
6.5 ROZBOR FUNKČNOSTI MIFARE KARET 85
ZÁVĚR 89
CONCLUSION 90
SEZNAM POUŽITÉ LITERATURY 92
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 94
SEZNAM OBRÁZKŮ 95
SEZNAM TABULEK 97

ÚVOD

V dnešním, rychle se měnícím světě technologií, můžeme pozorovat stále zvyšující se nároky na identifikaci osob, a to např. pro věrohodné ověření totožnosti nebo pouze prokázání důvěryhodnosti za účelem přístupu k informacím obecně. Důvodem je doba maximálního rozvoje a využívání informačních technologií, kdy jsou informace to nejcennější, s čím přicházejí lidé denně do styku a logicky je musí také dostačujícím způsobem chránit. Jedním ze způsobů identifikace lidí je ověřování totožnosti pomocí plastových karet. Cílem této práce je právě detailní popis způsobu využití těchto identifikačních prostředků, se kterými se každý z nás denně, byť i nevědomky, setkává. Takovýchto způsobů je nesčetné množství, nicméně dají se rozdělit do několika základních skupin. Jednou z hlavních možností způsobu využití karet je identifikaci držitele na základě informací uložených na kartě v grafické podobě. Máme tím na mysli jakousi plastovou vizitku, kterou může obdržet například registrovaný návštěvník komerční společenské akce. Dalším způsobem je využití karty jako datového nosiče. Data, která v tomto případě karta obsahuje, nejsou nijak chráněna a na základě jejich přečtení, a tedy následného ověření identity či pravosti karty, je jejímu držiteli umožněn přístup do chráněné místnosti nebo aktivována sleva při nákupu zboží. Obecně jde tedy o prokázání oprávněnosti za účelem získání přístupu k dalším informacím či službám. Posledním ze způsobů využití, o kterém bude tato práce pojednávat, jsou platební karty. Využíváme je denně pro bezhotovostní platby v obchodech, na internetu nebo restauracích. V tomto případě tedy slouží karta jako prostředek identifikace i mobilních plateb. Aby mohly plnit takovýto složitý účel, musí být samozřejmě vybaveny již nejen základní pamětí, ale také i procesorovou jednotkou, jež je schopna manipulovat s jednoduchými aplikacemi a daty, která obsahuje. Ovšem platební karty, nebo chceme-li obecně čipové, mohou být útočníky zneužity, za účelem získání informací, jež mohou vést k velkým ztrátám, a to nejen finančním. Proto také bude věnována část práce bezpečnosti a možným fyzickým, či logickým útokům na data obsažená v kartách. Dá se říci, že plastové karty poskytují lidem mnohé výhody plynoucí již z jejich technologických vlastností. Tato práce si klade za cíl detailně popsat jak pozitiva, tak i úskalí jejich využívání. Příkladem budiž jejich přenositelnost, jedna z hlavních výhod tohoto hardwarového tokenu, ale rovněž i zřejmým rizikem. V práci jsou obsaženy také poznatky z mnohaleté praxe z oboru firem jež v této technologii podnikají.

I. TEORETICKÁ ČÁST

1 VÝVOJ PLASTOVÝCH KARET

1.1 Identifikační prostředky

Karty, ať už máme na mysli čipové, magnetické nebo jen obyčejné identifikační, jsou pouze jednou z několika možností identifikace osob. Kdysi v minulosti, kdy se lidé potřebovali vzájemně jednoznačně identifikovat mezi ostatními, vznikla první hesla. Jejich účelem bylo odlišit osoby patřící do určitého společenství. Typickým příkladem z dávnověku může být takové rozeznání skrytého vojáka z nepřátelské armády. Prvními z fyzických identifikátorů byly amulety a pečetě, které se používaly k ověření důvěryhodnosti zpráv a zásilek.

V současné době se jako identifikační prostředky využívají hesla, čárové kódy, ID karty, různé druhy tokenů, a lidská biometrie. Jelikož jsou hesla ve smyslu alfanumerických řetězců v současnosti brány jako nedostačující prostředek autentizace, a čárové kódy se využívají především pro označování zboží, zmíním se podrobněji jen o zbylých metodách.

Podstatou biometrických systémů je schopnost na základě unikátnosti získaných vlastností člověka, jej s velmi vysokou pravděpodobností identifikovat. Takových vlastností je několik a s postupem času se objevují stále nové, důmyslnější metody. Nicméně lze je všechny rozdělit do dvou základních skupin, a to: fyziologické a behaviorální. Jak je již z názvu patrné, do první skupiny patří metody verifikace dle fyziologických vlastností člověka, např. otisky prstů, oční duhovky či geometrie obličeje. Metody behaviorálné jsou založeny na principech rozeznání jedinečného chování člověka. Příkladem je dynamika stisku kláves, dynamika podpisu, chůze či hlas.

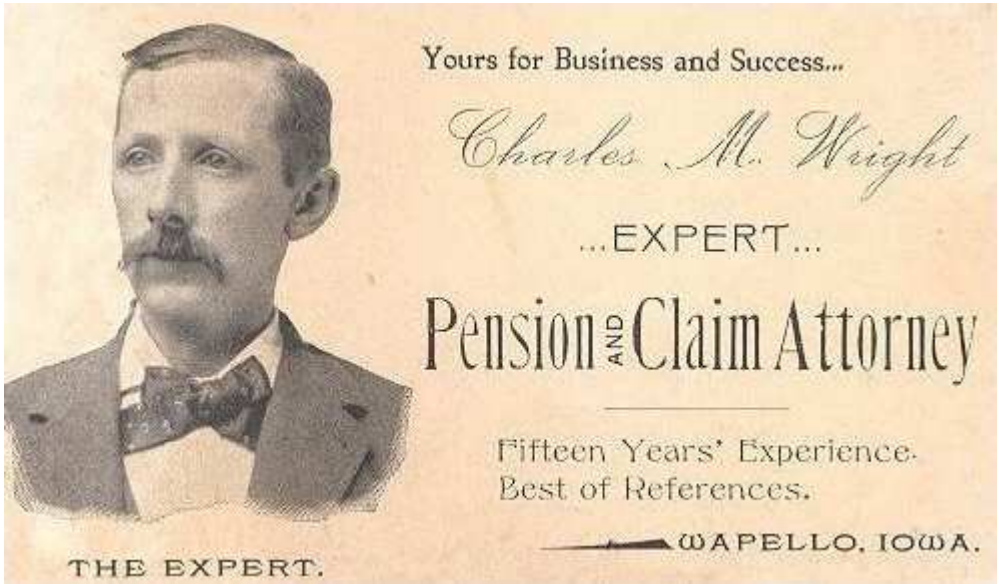
Tokeny jsou předměty, které se rovněž používají jako autentizační nástroje potvrzující identitu svého vlastníka. Informace, které jsou v tokenech uloženy, jsou jedinečné a proto by měly být dostatečně zabezpečeny proti duplikaci i krádeži. Protože hlavní nevýhodou je jeho přenostitelnost, používá se často kombinace tokenu a hesla, která ještě zvyšuje o řád bezpečnost metody [23]. Mezi běžně používané autentizační předměty patří:

- tokeny s pamětí (mechanické klíče, elektromagnetické karty)
- tokeny udržující hesla (po zadání uživatelského hesla vydají určený klíč)
- tokeny s logikou (jsou schopny zpracovávat jednoduché podněty)
- inteligentní tokeny (jsou schopny interakce s okolím, např. čipové karty)

1.2 Od papíru k identifikačním kartám

Historie plastových karet je samozřejmě velmi úzce spjata s historií karet platebních. I když se první platební karty objevily již v roce již 1918 a většího rozšíření se dočkaly až v druhé polovině 20tého století, plastové karty bez inteligence jsou tu pouhých 30 let. Plast se jako materiál pro výrobu platebních karet začal používat až s nástupem on-line terminálů - bankomatů.

Mimo těchto věrnostních karet byl druhý směr vývoje zaměřen více na identifikaci držitele. Postupem času karty začaly nahrazovat navštívenky a firemní vizitky. Historie vizitek se dá počítat již na celá století, ale hlavně z důvodů finanční dostupnosti, drží papírové identifikační karty prim i v současnosti. Teprve od té doby, co postoupila technologie výroby PVC a především mobilního tisku, staly se plastové karty bez inteligence jednoznačně nejvyužívanějšími na společenských a především obchodních setkáních, kde je zapotřebí tisknout identifikační karty dle požadavků až v místě konání.



Obr. 1. Obchodní vizitka z roku 1895 [10]

2 TECHNOLOGIE PLASTOVÝCH KARET

2.1 Výroba karet

Materiál karty je většinou dán předpokládaným způsobem jejího použití. Použité materiály nabízí různé přednosti ale také nedostatky a také představují rozdílné náklady. Jiný typ zvolíme pro jednorázové nebo občasné použití a jiný pro výrobu karty platební, u které se předpokládá dlouhodobé využívání a pravidelná mechanická manipulace, např. v bankomatech.

Karty z PVC

PVC (polyvinylchlorid) je základním materiálem pro běžné identifikační karty. Jeho vlastnosti zajišťují vysokou kvalitu potisku, střední pružnost ale nevalnou tepelnou odolnost. Předpokládaná životnost PVC karet je 24 měsíců, to předurčuje jejich využívání nejčastěji pro identifikační, návštěvní a věrnostní systémy. Bohužel jejich výroba i likvidace je značně neekologická a zatěžuje životní prostředí.

Karty z ABS

ABS (Acrylonitril butadien styren) je běžný termoplast, jehož hlavní výhodou je vyšší odolnost vůči chemickým a fyzikálním vlivům, samozřejmě na úkor horších schopností absorpce barvy. Pro potisk ABS karet nelze použít přímou termosublimaci, proto se s ABS kartami nejčastěji setkáme při ofsetové produkci nebo re-transferu. (metodám tisku je věnována kapitola 2.2) Nejčastěji se karty z ABS plastu využívají jako platební.

Karty z PET

Karty vyrobené z polyetylénu (PET) jsou rovněž velmi odolné vůči mechanickému namáhání. Jejich potisk je možný pouze metodou Termo-Retransfer. PET karty nabízí mnohem vyšší tuhost a proto jsou s oblibou používány v náročných podmínkách – identifikace osob v těžkém průmyslů, ocelárnách apod. Při teplotách pod bodem mrazu se mechanické vlastnosti PET i PVC karet rapidně zhoršují. Na rozdíl od PVC jsou snadno recyklovatelné a neškodné životnímu prostředí. Tento materiál je ale potisknutelný pouze metodou Termo Re-Transfer.

Kompozitní karty

Kompozitní karty (označovány jako PVH) se skládají z několika vrstev. Jádro je tvořeno polyesterem a povrch PVC. Díky kombinaci různých materiálů si karta zachovává poměrně dobrou odolnost vůči vysokým teplotám a zároveň umožňuje potisk v běžných tiskárnách karet. Díky zvýšené tepelné odolnosti lze PVH karty úspěšně laminovat a výrobce je označují jako „ideální pro laminaci“. Běžná životnost kompozitních karet je 4 – 7 let. To je předurčuje k použití jako identifikační či přístupové karty, nebo obecně všude tam, kde je častá výměna poškozených karet nežádoucí, nákladná, nebo nemožná.

2.2 Potisk karet

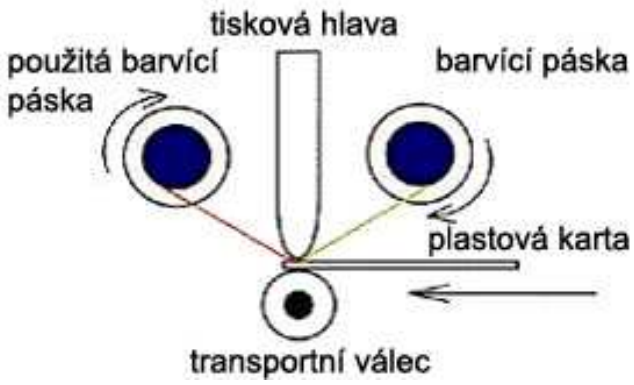
2.2.1 Přímý tisk: termotransfér a termosublimace

Termotransfer je tiskový proces, při kterém dochází k otisku barviva na bázi vosku nebo pryskyřice z pásky na kartu vlivem zahřívání jednotlivých tiskových bodů (200 nebo 300 bodu na palec) pod tiskovou hlavou. Termotransfer neumožňuje volbu intenzity přenosu, vždy je tak přeneseno veškeré zahřáté barvivo.

Zatímco u sublimace dojde zahřátím pásky tiskovou hlavou k chemické změně - sublimaci, díky níž barvivo přechází z pevného skupenství do plynného a to je následně absorbováno povrchem karty. V závislosti na teplotě bodu tiskové hlavy se mění i intenzita (odstín) barvy. Tato technologie primárně využívá žlutou (yellow), purporovou (magenta) a modrou (cyan) barvu. Pomocí tří základních barev lze složit jakoukoliv jinou barvu včetně složené černé. Pásky jsou tedy v tomto případě tvořeny třemi oddělenými bloky YMC. Velkou předností metody sublimace je možnost vytvoření miliónů odstínů barev. To je možné díky kombinaci barevných bloků na pásce, jak již bylo zmíněno, a nejsme tedy prakticky nijak omezeni ve výběru barvy.

Běžné barvící pásky pro potisk karet obsahují sublimační barvy YMC v kombinaci s termostransfgerovou složkou označovanou písmenem „K“ –odtud název pásek YMCK nebo YMCKO, kde „O“ označuje Overlay, tedy poslední, krycí vrstvu.

Na následujícím obrázku je znázorněn mechanismus termotransférové tiskárny.



Obr. 2. Princip termotransféru barvy [12]

2.2.2 Nepřímý tisk: termo re-transfér

Jak je již z názvu patrné, při této metodě není barva z termotransferové pásky přenášena přímo na povrch karty, ale je nejprve aplikována na tzv. Re-Transfer film, který je vždy 100% čistý a bez povrchových vad, na rozdíl od možných prolisů či jiného poškození karty. Na film se tedy barvy nanáší již popsaným termotransférem, či termosublimací. Otisk z filmu je pak pomocí tepla aplikován na kartu. Tato metoda zaručuje vysokou kvalitu tisku a také delší životnost karet, neboť barvivo zůstává po potisku „uvězněno“ mezi povrchem karty a filmem.

2.2.3 Offetový tisk

Samotný princip offsetového tisku spočívá v laminaci několika vrstev PVC, za působení teploty a tlaku, v podobě velkých štítů. Na štíty se nanáší barva, která se pak suší ve speciální sušárně. Potisknuté a suché štíty se následně opět laminují a pomocí výsekových nástrojů se ze štítů vyseknou karty požadovaných velikostí. Offsetový tisk je vhodný především pro vyšší náklady, přibližně od 500 kusů výše. Standardně se používá pro potisk škála CMYK, nebo přímé Pantone barvy, které jsou tisknuty technologií UV, takže je možné karty ihned po potisku laminovat, vysekávat a personalizovat. Digitální personalizace spočívá v nahrání dat na čip, nebo magnetický pruh. Grafickou personalizací je myšleno opatření karty čárovým kódem, osobními údaji, ražbou (embossing), či podpisovým polem. To, že je možné s kartami ihned dál manipulovat, je hlavní výhodou této technologie, neboť ostatní tiskové technologie, které používají pro schnutí barev vzdušnou oxidaci, lze použít až po několika dnech schnutí. Velkovýrobou je samozřejmě

možné dosáhnout snížení cen karet, nicméně ještě vedle časové úspory je nutné dodat, že kvalita potisku zde není tak vysoká.

2.2.4 Digitální tisk

Digitální tisk je moderní technologií, která se používá převážně pro výrobu malých nákladů karet od několika desítek kusů až do několika tisíců karet jednoho designu. Lze takto tisknout sdružené archy, na kterých je několik odlišných grafických designů, což znamená úsporu času a možnost souběžného plnění několika zakázek najednou. Jde sice o technologii určenou k masové produkci karet (například Opencard), ale tisk až v 24 pozicích umožňuje tvorbu 24 různých designů při jednom tiskovém průchodu.

Na závěr bych se chtěl zmínit také o technologii inkoustového tisku, která se ovšem v současné době používá pouze při offsetu. Po několika pokusech bylo od přenosných inkoustových tiskáren na karty upuštěno z důvodů složité mechanické konstrukce. Lakovaný povrch karet musí být v tomto případě opatřen speciální vrstvou, jež bude schopna pojmout barvu.

2.2.5 Další povrchové úpravy karet

Mimo embossingu, což je metoda ražení reliefního (plastického) písma na plastovou kartu, existují další způsoby úpravy povrchu karet.

Pro tisk hologramů, textu a log se využívá hotstamping. Je to technologie horké ražby, pomocí které se za vysoké teploty "vtiskne" speciální metalická fólie různých barev do těla karty. Vylepšuje se tímto grafický design karty a zhoršuje možnosti jejího padělání. V případech, kdy chceme karty potisknout po celé ploše jednobarevně, speciálně metalickými barvami (zlatou nebo stříbrnou) nebo tam, kde se nachází podpisové pole, se používá sítotisk. Technika tisku spočívá v protlačování tiskové barvy na plochém sítu, které tvoří výsledný motiv. Tento způsob tisku umožňuje nanášení několikanásobně silnější vrstvy barvy než ofsetový či digitální tisk. Vzhledem k vysokému krytí se využívá při výrobě plastových karet k tisku podpisového proužku nebo metalických barev [12].

Hologramům, UV potisku, gravírování a dalším značkám se budeme více věnovat v kapitole bezpečnosti karet.

2.2.6 Standardy a normy

Veškeré fyzikální charakteristiky identifikačních karet jsou definovány normou ČSN EN ISO/IEC 7810. Standardní rozměry karet jsou:

šířka: 85,60 mm (± 0,12 mm)

výška: 54 mm (± 0,08 mm)

tloušťka: 0,76 mm

Tato mezinárodní norma stanovuje fyzikální charakteristiky identifikačních karet včetně materiálů karet, konstrukce, charakteristik a rozměrů délka, šířka a výška.

Samozřejmě dle požadavků zákazníka lze rozměry karet na přání upravit. Obvykle se používají také tloušťky karet od 0,3 mm do 0,9 mm [8].

3 KARTA JAKO DATOVÝ NOSIČ

Až do této chvíle byly v práci popisovány pouze karty, které mohly být držiteli informace pouze v grafické (tištěné) podobě. Požadované údaje na kartu se zaznamenávají pomocí výše zmíněných tiskových technologií. Způsoby jak tiskem zaznamenat na kartu větší množství jsou omezené.

Jednou z možností je využití čárového kódu. Popisu funkcí a využití čárových kódů by se dala věnovat celá studie. Nicméně pro naše účely bude stačit, když budeme vědět, že čárový kód je prostředek pro automatizovaný sběr dat, vytvořený černotiskem vytištěnými pruhy definované šířky, umožňující přečtení pomocí technických prostředků - čteček či skenerů. Každý čárový kód je tvořen sekvencí čar a mezer s definovanou šířkou. Ty jsou při čtení transformovány podle své sytosti na posloupnost elektrických impulsů různé šířky a porovnávány s tabulkou přípustných kombinací. Pokud je posloupnost v tabulce nalezena, je prohlášena za odpovídající znakový řetězec. Nositelem informace je nejenom tištěná čára, ale i mezera mezi jednotlivými dílčími čarami. Krajní skupiny čar mají specifický význam - slouží jako synchronizační pro čtecí zařízení, které podle nich generuje signál Start/Stop. Technická specifikace pak vyžaduje ochranné světlé pásmo bez potisku před a za synchronizačními čarami [1]. Všichni známe běžné kódy, kterými se označuje veškeré zboží které koupíme, ale v posledních letech se začíná značně využívat i dvourozměrných čárových kódů. 2D kód funguje na podobném principu jako čárové 1D kódy. Ovšem zejména požadavky na navýšení datového prostoru, který by pojal mnohem více informací, nevyužití potenciálu, který vzniká přepisováním tiskové informace do elektronické podoby, vedly k vývoji nové generace těchto záznamových značek.

Do 2D kódu jsme schopni uložit stránky textu a jiných informací, na rozdíl od běžných jednorozměrných kódů, kde se s množstvím obsažených informací značně zvětšuje i jeho velikost. Příkladem je 2D Superscript. Jedná se o speciální dvourozměrný kód s vysokou hustotou záznamu. Takový kód o velikosti 0,9 x 7,6 cm může nést až 2,2 kB informací. Je tedy vhodný pro ukládání fotografií, biometrických informací i běžného textu. Nejvíce se tento způsob uložení informací využívá na cestovních dokladech, peněžních kartách a podobných dokumentech, jež je zapotřebí strojově zpracovávat. Určitou nevýhodou pro běžné užívání je nutnost snímače 2D kódu a jeho připojení k systému, který jej zpracuje.

V současnosti ovšem již existují tzv. mobilní terminály, což jsou průmyslové PDA vybavené nejmodernější komunikační technologií jako je WiFi, GPS, GSM funkcemi a

také snímači 1D/2D kódů nebo čteček RFID tagů. Takové zařízení je tedy schopno zpracovávat načtené informace v reálném čase.Text, čísla a kódy jsou tedy tisknutelná data, jež lze využít k identifikaci.Ovšem co v případě, že chceme aby karta nesla množství informací, které mají být navíc čitelné kontaktními nebo bezkontaktními čtečkami a je požadována jakási kooperace mezi kartou a čtecím zařízením? Zde přicházejí na řadu tzv. karty s inteligencí, kterým je věnována kapitola 3.2.

3.1 Magnetické karty

Stejně jako čipové karty, o kterých bude řeč později, se karty s magnetickým pruhem začaly používat začátkem 70tých let minulého století. V té době se používali na papírových identifikačních a platebních kartách. V současnosti papírové magnetické karty nacházejí uplatnění především jako nosiče informací v parkovacích nebo vjezdových systémech. Umístění a rozměry magnetického proužku na kartě jsou definovány normou ISO7811 (viz. příloha č. 1). Každý proužek může obsahovat až tři stopy.

1. stopa (IATA) - má 79 znaků, dají se na ní nahrát jen alfanumerické znaky.
2. stopa (ABA) - má 40 znaků, dají se na ní nahrát jen čísla 0-9 a rovnítko.
3. stopa (THRIFT) - má 107 znaků, dají se nahrát jen čísla 0-9, rovnítko, dvojtečka.

Magnetické karty rozdělujeme na dva základní typy: HiCo a LoCo. Tyto názvy vznikly ze zkratek pro vysokou, resp. nízkou koercivitu. Což je vlastně míra intenzity magnetického pole, která způsobí změnu dat magnetické stopy. Jinými slovy určuje, jak náročné je zakódování dat do magnetické stopy. [12].

Obr. 3. Karta s magnetickým pruhem[13]

- HiCo – Tyto karty disponují nejvyšší úrovní odolnosti vůči poškození rozptýleným magnetickým polem. Z toho, co již bylo řečeno o koercivitě, je tedy zřejmé, že kódování HiCo karet bude poněkud složitější, protože je k tomu zcela logicky zapotřebí vyššího výkonu, než je tomu u typu LoCo. Z toho plynou také vyšší pořizovací náklady. Karty tohoto typu se používají v aplikacích, kde se magnetický pruh používá velmi často, tzn. denně. Jsou to např. docházkové systémy, kontroly přístupu, či platební karty.
- LoCo – Kódování tohoto typu karet je jednodušší, tím pádem i levnější. LoCo karty se používají tam, kde se předpokládá méně častější použití, a s tím spojené strojové mechanické čtení. Například zákaznické, věrnostní či členské karty jsou aplikace, kde se karta využívá řekněme s týdenní, či měsíční pravidelností.

Magnetické pruhy mohou být umístěny buď v horní nebo dolní polovině karty, a z toho plyne také laické označování „horní“ a „dolní“. Tato skutečnost musí být rozlišována nejen při čtení, ale již při kódování dat. Kódováním máme na mysli proces zapisování dat do čipu nebo v tomto případě magnetické stopy.

Rozlišení HiCo a LoCo stopy je možné také opticky. HiCo stopy jsou černé, zatímco LoCo stopy světle hnědé. Samozřejmě čtecí zařízení jsou konstruovány tak, aby četly oba typy karet.

Výhodou magnetických karet oproti ostatním je cenová dostupnost a poměrně snadná identifikace. Nevýhodou je hlavně malá odolnost proti poškození a ztrátě dat, a to jak mechanicky, tak i magnetickým polem. Míra zabezpečení a jejich snadná duplikovatelnost způsobily, že magnetické karty jsou postupně nahrazovány kartami čipovými.

Výrobci i distributoři těchto karet musí věnovat značnou pozornost tomu, že informace uložené na magnetickém proužku mohou být znehodnoceny jeho kontaminací při dotyku s nečistotou a některými běžně používanými chemikáliemi, včetně změkčovadel. Je rovněž důležité, aby jakýkoliv tisk nebo sítotisk umístěný na povrchu magnetického proužku nenarušil jeho funkci. Při manipulaci s magnetickými kartami musíme dbát na to, aby nedošlo k nadměrnému prohnutí oblasti s magnetickým proužkem, či k deformaci povrchu. Ty by mohly narušovat kontakt mezi magnetickou hlavou a proužkem.

Technika kódování pro každou stopu je známa jako dvoufrekvenční záznam. Při sériovém zápisu umožňuje tato metoda samočinnou časovou synchronizaci dat. Zakódování zahrnuje dohromady data a synchronizační změny. Změny toku, které se vyskytují mezi

synchronizačními přechody, značí, že bit je „jedna“, a nepřítomnost změny toku mezi synchronizačními přechody značí, že bit je „nula“. Data tedy musí být zaznamenána jako synchronní posloupnost znaků bez přerušení mezerami. Při kódování se musí dodržet rovněž úhel záznamu. Ten musí být 90° vůči nejbližší hraně karty rovnoběžné s magnetickým proužkem s tolerancí 20 minut. Úhel záznamu se určí měřením úhlu mezery hlavy. Průměrná hustota bitů záznamu musí být dle normy 8,27 bitů/mm (210bpi) [12].

V ideálním případě by magnetické proužky s vysokou koercivitou měly mít významně zlepšenu odolnost proti vymazání, avšak měly by mít identické charakteristiky čteného signálu jako magnetické proužky s nízkou koercivitou. Nicméně prakticky rozdíl v magnetických charakteristikách proužků s vysokou a nízkou koercivitou způsobuje, že charakteristiky čteného signálu se výrazně liší.

3.2 Čipové karty

V roce 1970 byl prvně patentován způsob zasazení mikročipu do karty, nicméně až rok 1974 je všeobecně považován za začátek éry čipových karet. Ještě koncem sedmdesátých let měl ale mikroprocesor u čipových karet zatím pouze jedinou funkci – staral se o bezpečnost přístupu k informacím uloženým v paměti. Těmito informacemi mohly být v té době např. údaje o pacientově zdraví (zdravotní karty), množství peněz (elektronická peněženka) apod. – většinou vždy data hodná pečlivé ochrany před přístupem osob nepovolaných.

Nejvýznamnější zkouškou čipových karet byl v té době projekt řízený francouzskou asociací pro bankovní karty v letech 1982 až 1984, po jehož úspěšném skončení vznikl ve Francii největší trh s čipovými kartami. Během následujících deseti let jich bylo vydáno na 21 miliónů kusů. Testováno bylo tehdy více než 100 tisíc čipových karet od třech různých výrobců. Bylo rozhodnuto o tom, že bude vybrán čip od Motoroly s 8 kB paměti. Tento typ ze zdál být pro platební aplikace vhodnější než např. dvoučipový model Intel, kde jeden čip fungoval jako mikroprocesor a druhý jako paměť. Výrobcem zvolené karty byla firma Bull, která se poté stala nejvýznamnějším vývojovým centrem čipových karet.

Francie se tedy stala průkopníkem této technologie. V roce 1992 zde vyvrcholil postupný přechod na technologii hybridních karet (čip + magnetický proužek). V současné době je všech 20 milionů francouzských bankovních karet na území Francie vybaveno čipem pro vnitrostátní transakce a magnetickým proužkem pro platební transakce v zahraničí. Díky

zavedení čipů klesly ve Francii v devadesátých letech podvody s platebními kartami více než desetinásobně, z 0,27 na 0,026%. V současné době mají všichni výrobci čipových karet licence od firmy Innovatron [11].

Druhy čipových karet

V současné době rozeznáváme tři základní druhy čipových karet, které se od sebe liší použitou technologií, stupněm bezpečnosti, mírou flexibility, počtem aplikací a také cenou.

Paměťová karta (Memory Card) – tyto karty nedisponují žádnou inteligencí, mají pouze vlastní paměť. Výroba paměťových karet je poměrně levná a veškeré funkce jsou naprogramovány již výrobcem. Používají se především tam, kde se neklade velký důraz na bezpečnost, mohou to být tedy různé předplatní karty.

Paměťová karta s autentizační logikou (Hard-Wired Logic Card) – funkce těchto karet jsou pevně určeny již při výrobě. Oproti předchozí verzi, je bezpečnost proti padělání zvýšena požadavkem na vložení tajného kódu. Tímto kódem se potvrzuje právo na přístup k datům uloženým v paměti.

Mikroprocesorová karta (Microprocesor Card) – je karta s tzv. aktivní inteligencí. Mikroprocesor umožňuje přístup k datům, případně provádět jejich změny, ale to pouze takovým subjektům, jež prokáží své oprávnění přístupovými kódy. Programové vybavení karty je schopno odhalit pokusy o neautorizovaný přístup k datům, v takovém případě se karta zablokuje nebo smaže veškerá data a programy. Mikroprocesorové karty mohou obsahovat i několik takovýchto funkcí, respektive aplikací, jež se dají naprogramovat buď již při výrobě, nebo až dodatečně.

Základní vybavení čipové karty:

- CPU – procesor zajišťuje výpočty a přenos dat
- bezpečnostní logika – kryptografické funkce
- I/O / komunikační rozhraní – zajišťuje komunikaci s okolím
- testovací logika – slouží k testování procesů interních obvodů
- ROM – paměť např. pro OS
- RAM – pomocná paměť procesoru, úložiště pomocných dat
- EEPROM – slouží k uložení aplikačních dat, jako jsou klíče, PIN, stav účtu
- datová sběrnice – komunikační kanál spojující jednotlivé komponenty

V terminologii panuje určitá volnost a definice jednotlivých typů se mohou lišit. Nicméně jednoznačnými rysy čipových karet mimo standardizované velikosti (85,60 x 53,98 x 0,76 mm) a dalších fyzikálních charakteristik definovaných normami ISO7816, je zejména mikročip, respektive integrovaný obvod. Odtud také plyne anglické označení ICC – Integrated Circuit Card [2].

Z hlediska přenosu dat mezi kartou a čtecím zařízením dělíme čipové karty na:

- kontaktní
- bezkontaktní
- hybridní (kombinace výše zmíněných)

3.2.1 Kontaktní čipové karty

Jak je z názvu patrné, karty disponují plochou s osmi kontakty, které slouží k výměně informací mezi integrovaným obvodem a vnějším zařízením rozhraní. Funkce a umístění kontaktů na kartě je přesně definováno normou ČSN ISO/IEC 7816-2. Minimální rozměry každého z osmi kontaktů musí být 2 x 1,7 mm a každému z nich je přiřazena funkce.

Obr. 4. Kontaktní plošky čipové karty [1]

V tabulce č. 1 vidíme dva nevyužité kontakty C4 a C8, jež byly vyhrazeny pro budoucí použití v dalších částech ISO/IEC 7816. Ty se v současnosti používají pro alternativní USB rozhraní.

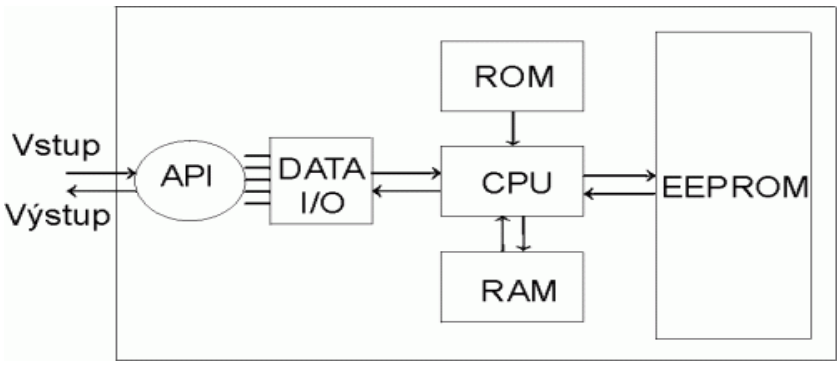
Číslo kontaktu	**Přiřazení**	**Číslo kontaktu**	**Přiřazení**
C1	VCC napájecí napětí	C5	GND zem
C2	RST signál reset	C6	VPP proměnné napájecí
C3	CLK hodinový signál	C7	I/O vstup/výstup dat
C4	Vyhrazeno pro budoucí použití	C8	Vyhrazeno pro budoucí

Tab. 1. Kontaktní plošky čipové karty

Fyzikální charakteristiky

Nepoužité kontaktní oblasti musí být nevodivé nebo musí být izolovány od ostatních kontaktních oblastí, aby se zabránilo potencionálním zkratům v zařízení rozhraní. Norma ISO/IEC 7816-1 definuje fyzikální charakteristiky karty jako je např. profil povrchu kontaktů. Zde platí, že žádný bod povrchu kontaktu integrovaného obvodu nesmí být výše než 0,1 mm nad nebo pod sousedním povrchem karty. Karta by také měla odolávat poškození svého povrchu a libovolných komponentů v ní obsažených, a měla by zůstat neporušena při běžném používání, skladování a manipulaci. Povrch všech kontaktů a kontaktní oblast (celý vodivý povrch) nesmí být poškozeny tlakem, ekvivalentním působením tlaku 1,5 N ocelovou kuličkou o průměru 1 mm. Integrovaný obvod karty nesmí být při běžném používání poškozen osobou nabitou statickou elektřinou a musí pracovat při teplotě okolí v rozsahu mezi 0 °C a 50 °C. A v neposlední řadě tepelná ztráta integrovaného obvodu nesmí být větší než 2,5 W [8].

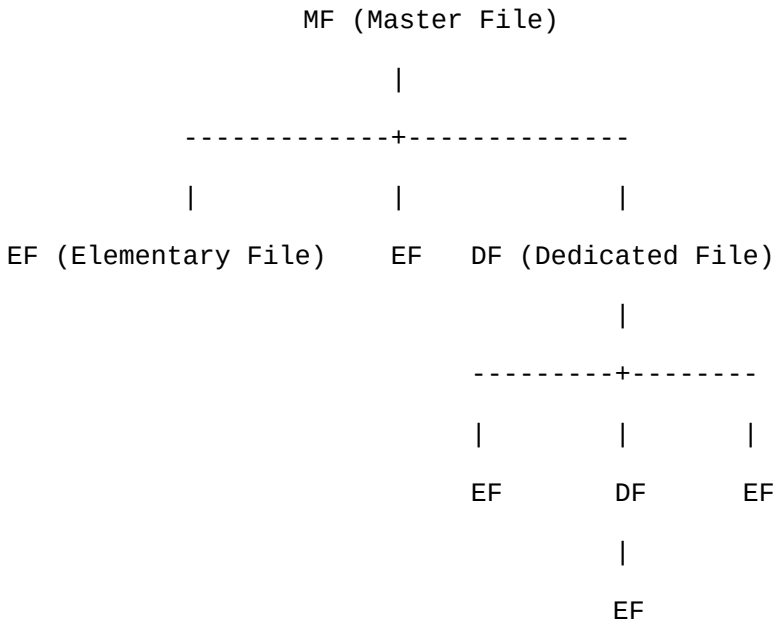
Jak již bylo uvedeno výše, čipové karty bez ohledu na způsob přenosu dat obsahují podobné komponenty jako osobní počítač. Najdeme procesor, různé typy pamětí a vstupně/výstupní kanály. Do jedné z pamětí ROM je již během výroby umístěn software, jež pracuje jako operační systém karty. Zbývá již jen propojení čipu s kontaktními ploškami a zalisování do plastového nosiče.



Obr. 5. Struktura čipové karty

Mezi základní funkce operačního systému karty patří správa jednoduchého souborového systému uloženého v paměti EEPROM. Není tedy možné ukládat data na kartu podle požadavků každého uživatele, ale děje se tak právě řízením OS. Data se řadí do souborů dle systému, který je velmi podobný souborovému systému osobních počítačů. Tento model má jistá omezení, mezi něž patří zejména to, že jednotlivé soubory nejsou rozlišovány jménem, ale jednobajtovým až dvoubajtovým číslem, a také to, že maximální

úroveň vnoření adresářů bývá obvykle dva. Na rozdíl od běžných souborů jsou ovšem vybaveny obstojným bezpečnostním mechanismem, který většinou umožňuje definovat několik klíčů, které je třeba pro konkrétní operace se soubory znát. Souborový systéme čipové karty je zde znázorněn níže.



Na vrcholu stromu se nachází tzv. MF (Master File), což je kořenový adresář, který organizuje další podadresáře DF (Dedicated Files). Zbylé datové soubory se značí jako EF (Elementary File).

Podobně jako u osobních počítačů mohou být soubory na kartě opatřeny přístupovými právy:

ALW – volný přístup

NEV – zakázaný přístup

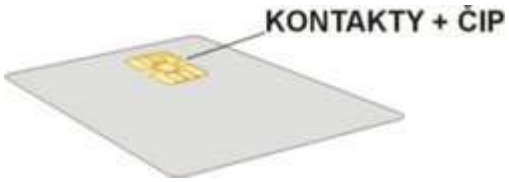
PRO – přístup pouze s privátním klíčem

ENC – data s šifrováním

Díky definovaným výrobním standardům se mohou prodejci a uživatelé čipových karet spolehnout na to, že nebudou nijak omezeni a zaručuje se tím zároveň kompatibilita s již existujícími systémy.

Česká státní norma ISO/IEC 7816 definující vlastnosti kontaktních čipových karet sestává z následujících částí, pod společným názvem **Identifikační karty – karty s integrovanými obvody a kontakty** [8]:

- 7816-1: Karty s kontakty - Fyzikální charakteristiky
- 7816-2: Karty s kontakty - Rozměry a umístění kontaktů
- 7816-3: Karty s kontakty - Elektrické rozhraní a protokoly přenosu
- 7816-4: Organizace, bezpečnost a příkazy pro výměnu
- 7816-5: Registrace poskytovatelů aplikací
- 7816-6: Mezioborové datové prvky pro výměnu
- 7816-7: Mezioborové příkazy pro strukturovaný kartový dotazovací jazyk (SCQL)
- 7816-8: Příkazy pro bezpečnostní operace
- 7816-9: Příkazy pro správu karet
- 7816-10: Karty s kontakty - Elektronické signály a odpověď na reset pro synchronní karty
- 7816-11: Ověřování osob biometrickými metodami
- 7816-12: Karty s kontakty - Elektrické rozhraní USB a provozní procedury
- 7816-13: Příkazy pro správu aplikací v multiaplikačním prostředí
- 7816-15: Aplikace kryptografické informace

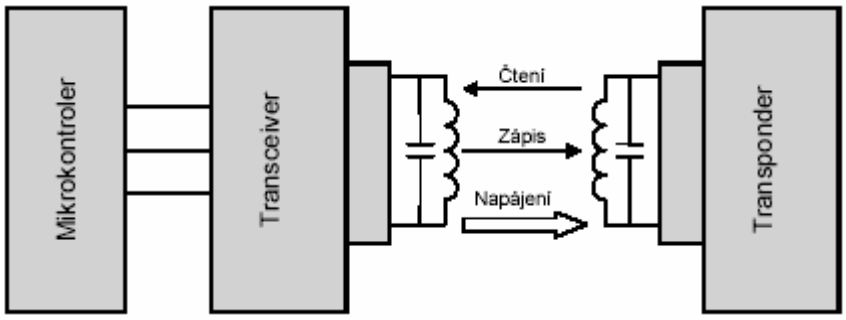


Obr. 6. kontaktní čipová karta [12]

3.2.2 Bezkontaktní čipové karty

Jsou podobné jako kontaktní čipové karty, avšak oproti nim je na čip připojena zalitá anténa, která umožňuje bezdotykové čtení a zápis informací do paměti. Bezkontaktní čipové karty se tedy nemusí vkládat do čtečky karet, stačí být pouze v dosahu radiofrekvenční čtečky. Operační dosah je typicky do 10cm, v závislosti na použitém snímači. Nosná frekvence je nejčastěji 13,56 MHz a čtecí vzdálenost závisí ne použitém typu karty a čtečky. Zřídka se používají karty s nosnou frekvencí 125 kHz, nicméně disponují nedostatečnou ochranou přenášených dat. Energie je přenášena ve formě indukce elektromagnetického pole ze čtečky do antény čipové karty a slouží k napájení čipu. Při vzájemné komunikaci se využívá principu zátěžové modulace. Karta je schopna si sama

odebrat určité množství energie z elektromagnetického pole čtecího zařízení a následně ho využít pro zpětnou komunikaci [18].

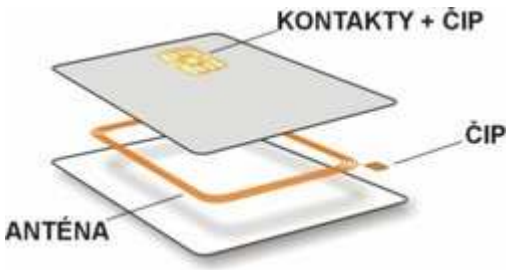


Obr. 7. Princip bezdotykové komunikace

Norma ISO/IEC 14443 definující vlastnosti bezkontaktních karet s integrovanými obvody rozlišuje dva typy A a B. Hlavní rozdíl mezi těmito typy se týká modulačních metod, kódování a protokolu inicializace procedur. Nicméně oba využívají stejný přenosový protokol. Tyto dva typy stále přetrvávají především z důvodů zástupcích silných komerčních firem ve standardizačních výborech.

3.2.3 Hybridní čipové karty

Hybridní karty jsou takové, které obsahují dvě nebo více čipových technologií, jako např. bezkontaktní čip s anténou, kontaktní čip s kontaktním polem a/nebo proximitní čip s anténou. Bezkontaktní čip lze použít pro aplikace vyžadující rychlé přenosy, jako je hromadná přeprava. Kontaktní čip se pak používá v aplikacích, kde je vyžadováno vysoké zabezpečení. Individuální komponenty nejsou vzájemně propojeny, díky čemuž může jedna takováto karta sloužit pro více aplikací.



Obr. 8. Hybridní karta [12]

3.2.4 RFID, NFC a další technologie

Se stále více se rozšiřujícím komerčním využitím bezkontaktních čipových karet vznikají také nové technologie, jež jsou odvozeny z již existující normy ISO/IEC 14443. Většinou byl jejich vznik reakcí na poptávku na komerčním trhu, jinými slovy využití nové technologie bylo již předem známo.

Mifare je proprietární technologie kontaktních a proximitních karet. Její hlavní vlastností a velkou výhodou je dispozice několika oddělených paměťových sektorů, které mohou obsahovat data pro různé aplikace. V praxi to může vypadat tak, že uživatel používá jedinou Mifare kartu pro vstup do knihovny, na parkoviště, k hromadné přepravě či ke kontrole docházky zaměstnání. Existuje celkem sedm typů Mifare karet: Ultrilight, Ultrilight C, Classic, Plus, Desfire, Prox, SmartX. Této technologii se bude věnovat více praktická část této práce.

Jednotlivé typy se liší velikostí paměti, schopností kryptografie, rychlostí komunikace, aj. Mifare karty obsahují čipy NXP, jež vyrábí firma Philips semicoductors. Jsou pokládány za jedny z nejlepších a nejrozšířenějších typů bezkontaktních čipových karet v současnosti.

NFC je technologie vysokofrekvenční bezdrátové komunikace, která umožňuje výměnu informací na krátké vzdálenosti okolo 10 cm. Z toho plyne anglické označení Near Field Communication. Tato technologie je stejně jako předchozí rozšířením normy proximitních karet ISO/IEC 14443, jež kombinuje rozhraní čipové karty a čtečky do jednoho zařízení. NFC umožňuje rychlé spojení, odeslání, příjem i sdílení předem definovaných dat sloužících pro identifikaci, šíření souborů či v budoucnosti pro bezpečné a rychlé platby. NFC využívá frekvenci 13,56 MHz, data přenáší rychlostí až 848 kbit/s a může být použito v mnoha zařízeních, od mobilních telefonů, digitálních kamer, klíčů, různých identifikačních karet až po reklamní poutače.

RFID (Radio Frequency Identification) - radiofrekvenční systém identifikace je moderní technologie identifikace objektů pomocí radiofrekvenčních vln. Informace jsou v elektronické podobě ukládány do malých čipů-tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln, toto zpracování se však neděje po jednotlivých čteních jako u v současnosti používaných čárových kódů, ale hromadně. Současná čtecí zařízení dokážou najednou načíst až několik set tagů za minutu.

S myšlenkou na vznik bezdrátové technologie zpracování informací přišla před lety největší maloobchodní firma WalMart, která před několika desetiletími stála u zrodu čárového kódu. Základem byla myšlenka vyvinout takovou technologii, která dokáže objekt identifikovat na větší vzdálenost bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více objektů současně. V současné době se technologie RFID velice rozvíjí a dochází k nasazení v mnoha dalších oblastech trhu, největší uplatnění nachází v logistice, výrobě, sledování objektů - logistických jednotek (zboží, palet, kontejnerů), sledování majetku, sledování zavazadel na letištích a evidence osob. A právě tady nachází tato technologie ve spojní s kartami své největší uplatnění, tedy k identifikaci a autorizaci osob.

Podobně jako u čárových kódů se informace zaznamenávají na nosič dat - tzv. RFID tag, který je připevněn na sledované objekty. RFID tagy jsou základem systému pro ukládání a přenos informací pomocí elektromagnetických vln. Může je hromadně přečíst a zaznamenat příslušné čtecí zařízení, které může být pevné nebo mobilní. Pomocí vln vyzářených z čtecího zařízení dojde k nabití čipu a následně se informace uložená v čipu bezdrátově přenese zpět do čtecího zařízení [14].

3.2.5 Přenosový protokol čipových karet

Elektrické obvody čipové karty nesmí být aktivovány, dokud nejsou kontakty karty mechanicky připojeny ke kontaktům zařízení rozhraní – čímž je myšleno čtecí zařízení.

Interakce mezi zařízením rozhraní a kartou musí být prováděna pomocí následujících, po sobě jdoucích operací:

- aktivace elektrických obvodů zařízení rozhraní
- výměna informací mezi kartou a zařízením rozhraní iniciována vždy kartou, která odpovídá na studený reset
- deaktivace elektrických obvodů zařízení rozhraní

Pro započetí interakce s mechanicky připojenou kartou musí zařízení rozhraní aktivovat elektrické obvody v následujícím pořadí [8]:

- kontakt RST musí být nastaven do stavu, který odpovídá hodnotám veličin

  $U = 0{,}12 \times V_{CC}$ přičemž musí zůstav v rozsahu -0,3 až 0,3 V

  $I = -200$ až $20\ \mu A$

  $C_{IN} = 30$ pF

- kontakt VCC musí být napájen podle zvolené třídy zařízení rozhraní
- kontakt I/O zařízení rozhraní musí být nastaven do režimu příjmu
- VPP musí být nastaven do stavu čekání
- na kontakt CLK musí být přiváděn hodinový signál, v průběhu odpovědi na reset musí být kmitočet hodinového signálu v rozsahu f = 1 až 5 MHz

Poté je již karta připravena na studený reset, což je první reset po aktivaci. Okamžitě poté, co jsou aktivovány elektrické obvody karty, vyšle do rozhraní zařízení požadavek ATR (answer to reset). Maximální velikost ATR zprávy je 33 bytů a obsahuje parametry vyžadované kartou pro stanovení cesty datové komunikace, mezi které patří například i hardwarové parametry, jako je sériové číslo čipu. Veškerá komunikace probíhá vždy poloduplexně, tzn. že přenos dat může probíhat v každém okamžiku pouze jedním směrem. Buď z karty do zařízení nebo naopak, ale nikdy oběma směry najednou. Pro komunikaci mezi čipovou kartou a zařízením rozhraní se využívá protokol APDU (Application Protocol Data Units). Jedná se o protokol na aplikační vrstvě, jež se stará o samotný přenos datových paketů. APDU rozeznává příkazy a odpovědi. V praxi to znamená např., že po vložení platební karty do bankomatu tento terminál odešle příkaz a čeká na odpověď z karty. Formát APDU příkazu je zobrazen v následující tabulce.

CLA	INS	P1	P2	Lc	Data	Le

Tab. 2. Struktura příkazu APDU

CLA – třída instrukce, identifikuje kategorii příkazu a odpovědi

INS – kód instrukce, specifikuje instrukci příkazu

P1 a P2 – parametry používající se k nastavení dalších oprávnění instrukcím

Lc – specifikuje délku datového pole

Data – obsahuje data poslaná kartě k vykonání instrukcí (příkazů)

Le – specifikuje délku očekávané odpovědi (v Bytech)

Formát APDU odpovědi na příkaz má pouze dva parametry:

Data	SW

Data – datové pole s odpovědí, jehož délka je daná parametrem Le

SW – (status word SW1 & SW2) označuje procesní stav v kartě po vykonání příkazu, např SW 0x9000 značí, že příkaz byl vykonán kompletně a úspěšně

Rozlišují se čtyři APDU případy příkazu a odpovědi.

1) host [příkaz] ←→ karta [SW]

2) host [příkaz] ←→ karta [data + SW]

3) host [příkaz + data] ←→ karta[SW]

4) host [příkaz + data] ←→ karta [data + SW]

V druhé vrstvě tzv. transportní nalezneme dva typy protokolů, které se rozlišují dle typu komunikace, pod označením T=0 bytově orientovaný poloduplexní přenos asynchronních znaků a T=1 blokově orientovaný asynchronní přenos bloků. Tyto protokoly definují strukturu dat při výměně mezi kartou a zařízením rozhraní.

Protokol přenosu bezkontaktních čipových karet

Poloduplexní protokol přenosu po blocích, jež využívají bezkontaktní čipové karty pro komunikaci, je analogické již zmíněnému APDU. Hlavním rozdílem je nutnost specifikace typu A nebo B z normy ISO/IEC 14443. Následující obrázek popisuje schéma aktivace protokolu proximitní karty neboli karty s vazbou na blízko.

Použité značky ve schématu:

ATS – odpověď na volbu

ATQA – odezva na žádost, typ A

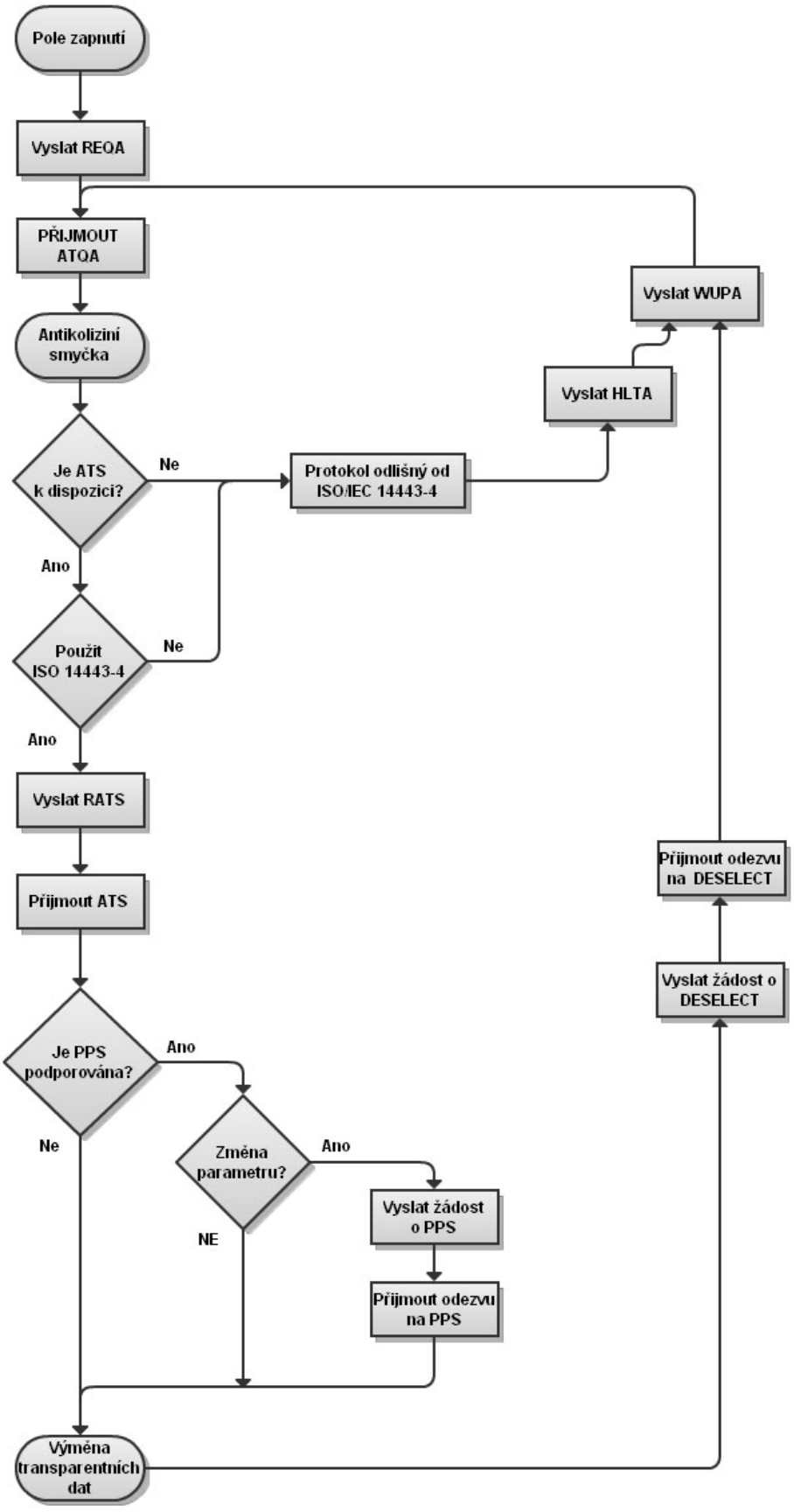
HLTA – příkaz HALT, typ A

PPS – volba protokolů a parametrů

REQA- příkaz REQUEST, typ A

RATS – žádost o odpověď na volbu

WUPA – příkaz WAKE-UP, typ A



Obr. 9. Aktivace protokolu karty s vazbou na blízko typu A [12]

4 VYUŽITÍ PLASTOVÝCH KARET

Z výše popsaného je již snadné odvodit nejběžnější způsoby využívání plastových karet. Díky své přenositelnosti a schopnosti nést informace v grafické nebo digitální podobě jsou jedinečným prostředkem pro identifikaci, autorizaci či mobilní platby. Každý z nás se mnohdy i nevědomky účastní aplikací, kde se karty využívají. Používají se v hromadné dopravě jako průkaz o zaplacení jízdného, v zaměstnání pro kontrolu přístupu, v obchodech pro bezhotovostní platby či prokázání nároku na slevu. V posledních letech se také značně rozšířilo použití karet na místo klíčů od pokojů. Kartu dostane zákazník při registraci, většinou to bývá magnetická, a je předem aktivována na smluvenou dobu pobytu. Také sim-karta, kterou má každý z nás v mobilním GSM telefonu, je vlastně oříznutá kontaktní karta s čipem. Dalšími které většina z nás využívá je karta pojištěnce, řidičský průkaz a méně běžné klubové průkazy do fitness centra, či In-Karta jež poskytují České dráhy od roku 2006 svým zaměstnancům a zákazníkům je vlastně bezkontaktní čipová karty typu Mifare DESFire. Jak vidíme, karty jsou našimi pomocníky v každodenních činnostech tam, kde je vyžadováno ověření identity.

Plastové karty bez inteligence

- slevové (s konstantní slevou)
- klubové
- věrnostní
- zákaznické
- pojištěnecké
- reklamní
- losovací karty
- permanentky, VIP karty
- průkazy, vizitky

Plastové karty s inteligencí

Paměťové karty

- identifikační karty
- předplacené telefonní karty
- elektronická peněženka
- přístupové systémy
- karty zdravotních pojišťoven
- elektronické jízdné
- členské a klubové karty

Mikroprocesorové karty

- bankovní karty
- elektronické peněženky
- GSM karty
- zdravotnictví
- předplacené TV a satelit
- multifunkční karty

Výhody použití karty s kontaktním čipem

- velká rozšířenost systému a podpora řady výrobců
- vysoká bezpečnost
- možnost uložení značného množství dat
- možnost běhu více aplikací na jednom čipu

Výhody použití karty s kontaktním čipem

- bezkontaktní řešení
- vysoká bezpečnost a spolehlivost
- možnost uložení značného množství dat
- možnost běhu více aplikací na jednom čipu

4.1 Platební karty

4.1.1 Historie platebních karet

O příčinách vzniku a uvedení platebních karet na trh jsem se zmínil již v úvodu této práce, neboť právě ony byly prvními standardizovanými kartami té doby. První platební kartu na světě vydala v roce 1014 americká telefonní a telegrafní společnost Western Union Telegraph Company. Karta byla vyrobena z plechu a podobala se vojenských identifikačním štítkům. Western Union ji nabídla zdarma svým stálým zákazníkům, kterým umožňovala telefonovat a zasílat telegramy prostřednictvím svých poboček a uhradit je najednou na konci měsíce. Společnost tak svým zákazníkům poskytovala krátkodobý obchodní úvěr.

Důvodem, proč společnost Western Union začala vydávat tzv. „Identification Card“, byla snaha udržet si dobré klienty a přimět je k častějšímu používání jejich možností bezhotovostního placení. Proto se tyto karty nazývají věrnostní. První platební karty skutečně zvýšily tržby společnosti, protože bezhotovostní placení bylo mnohem pohodlnější než hotovost a pro klienta bylo snazší rovněž utratit více peněz. Uplatnila se tak mnohaletá zkušenost obchodníků, kteří již dávno zjistili, že když se dá zákazníkovi možnost zaplatit později nebo na splátky, koupí si více nebo dražší zboží.

Věrnostní a platební karty se staly jedním z prostředků konkurenčního boje, a proto je začaly nabízet i další společnosti. Krize amerického hospodářství v roce 1929 zastavila další rozvoj kreditních karet. Teprve koncem 30. let se situace začala měnit. Telekomunikační společnost AT&T zavedla „Bell System Credit Card“, která měla podpořit věrnost zákazníků. Její příklad následovaly další telegrafní a železniční společnosti a řada obchodních domů a hotelů.

Přes své nesporné výhody (bezhotovostní placení, stimulace ke spotřebě atd.) trpěly věrnostní platební karty jednou významnou nevýhodou, jejich použití bylo omezeno pouze na obchodní síť firmy, která kartu vydala. Tuto nevýhodu odstranila až Charge Card společnosti Diner Club International.

V historii platebních karet zaujímá stejně významné místo jako Western Union společnost Diner Club International. Byl-li rok 1914 rokem zrodu věrnostní platební karty, pak rok 1950 byl rokem vzniku univerzálně použitelné platební karty. Její zakladatelé Robert

McNamara a Ralph Schneider pozvali několik svých přátel do prvotřídní restaurace v New Yorku. Při placení však McNamara zjistil, že u sebe nemá žádné peníze. Díky tomu, že jej v restauraci dobře znali, mu byla nabídnuta možnost, aby zaplatil příště. Spojení této náhody s vrozenou podnikavostí obou pánů pak vedlo k myšlence založit klub, nazvaný příznačně „Diners Club“. Jeho úkolem se stalo vydávat svým členům úvěrové karty nazvané „Charge Card“ pro bezhotovostní placení u všech smluvních hotelů, restaurací a obchodů, které s klubem uzavřou smlouvu. Vznikla tak první víceúčelová úvěrová karta pro nákupy dražšího zboží a služeb – Travel and Entertainment Card (T&E Card). Klub bude obchodním partnerům ručit za závazky svých členů a bude jim proplácet předložené účty. Svým členům pak jednou za měsíc zašle výpis provedených transakcí, které klubu uhradí najednou do data splatnosti. A protože je karta univerzálně použitelná a přinese obchodnímu partnerovi zvýšení tržby, aniž by nesl riziko případné insolventnosti člena Diners Club, musí se podílet na nákladech. Byl proto zaveden poplatek (provize) z částky nákupu, hrazený příjemcem karty jejímu dodavateli ve výši 5%, a také byl poprvé zaveden roční poplatek za vydání a správu karty ve výši 5 amerických dolarů [10].

4.1.2 Historie bankovních karet

Koncem 40. let se začaly o platební karty zajímat i americké banky. Nejprve v roce 1947 zavedla newyorská banka Flatbush papírový doklad nazvaný „Charg-It“, který sloužil k placení v lokální síti obchodů. Podobnou službu pak zavedlo několik dalších amerických bank. Všechny karty tehdy sloužili k placení, nikoli k čerpání úvěru. První kreditní kartu vydala až v roce 1951 newyorská banka The Franclin International. Karta byla vydávána zdarma a klienti museli uhradit provedené nákupy do 30, 60 nebo 90 dnů.

Pravděpodobně první kartu v Evropě vydala v roce 1951 společnost Finders Service ve Velké Británii. Založil ji Donald McCullough po návratu ze své cesty po Spojených státech, kde ho inspirovaly příklady karet Diners Club a další. O jedenáct let později se Finders Service spojila se společností Credit Card Service a vytvořila pobočku Diners Club ve Velké Británii, jejichž karta se pak stala nejvýznamnější kartou typu Charge Card na britských ostrovech. Rozvoj platebních karet v západní Evropě nastal až v druhé polovině 20. století poté, co i konzervativní evropští bankéři usoudili, že karty jsou vhodným

produktem pro jejich klienty. Kolébkou platebních karet se stali mimo Velké Británie Švédsko a Francie.

V České republice jsou mezinárodní platební karty přijímány od roku 1969. Jako první byly karty Diners Club a American Express. Postupně byly do roku 1990 akceptovány ještě Eurocard/MasterCard, JCB, VISA, Air Plus a enRoute. Uzavírání smluv s obchodními místy, školení jejich personálu, autorizaci a zúčtování transakcí zajišťovala cestovní kancelář Čedok. První bankomatové karty vydaly Česká a Slovenská spořitelna v létě roku 1989. Jednalo se přibližně o 1000 zaměstnaneckých karet a 2 off-line bankomaty NCR). V roce 1988 vydala své první platební karty Živnostenská banka. Jednalo se o tzv. dispoziční karty k tuzexovým účtům, které sloužily k výběru odběrních poukazů PZO Tuzex v pobočkách ČSOB a SBČS a k bezhotovostnímu placení v prodejnách Tuzex. V roce 1991 navázala Živnobanka na tento projekt vydáním karet VISA Classic a o rok později VISA Business [11].

V roce 1990 otevřela v Praze svoji kancelář společnost American Express a převzala od Čedoku zajištění příjmu svých karet v obchodní síti. Svoji zprostředkovatelskou činnost pro ostatní systémy Čedok ukončil v červnu 1992 – převzaly ji členské banky VISA a Eurocard/MasterCard.

Platební karty jsou dnes jedním z nejdynamičtějších se rozvíjejících bankovních produktů. Dokumentuje to výrazný růst počtu platebních karet mezinárodních organizací. Již v letech 1997 až 2000 vzrostl počet jimi vydaných karet o 60% na 1,9 miliardy kusů. Tak vysokému tempu růstu i nasycení trhu, které přetrvává do dnes, mohou platebním kartám konkurovat jen mobilní telefony a růst využití internetu, tedy nové distribuční kanály, kde opět platební karty sehrají klíčovou roli. S rostoucím počtem majitelů karet rostly také požadavky na stanovení určitých jednotných pravidel. Příčinou vzniku národních a později mezinárodních bankovních asociací a společností pro platební karty byla nutnost zajistit:

- efektivní infrastrukturu
- jednotnou identifikaci vydavatele karty
- jednotné ověření a zpracování transakcí
- jednotná pravidla pro používání karet, reklamace atp.
- centrální marketing

4.1.3 Způsoby použití karty

Nejdříve se na platební karty zaznamenávaly reliéfním písmem a pomocí kopírovacího papíru a mechanického snímače s válečkem se pak otiskly na účtenku. Mechanický snímač (tzv. imprinter) byl dlouhou dobu nejrozšířenějším prostředkem pro provádění placení kartou. Odstranil ruční přepisování identifikačních údajů z karty a doplňování identifikace obchodníka, u kterých docházelo ke ztrátám a chybám. V sedmdesátých letech byl kopírovací papír nahrazen chemickým samopropisujícím papírem.

Jakmile technici přišli koncem 60. let s nápadem umístit na platební kartu magnetický pásek a použít ho pro záznam dat potřebných pro provedení transakce, otevřely se možnosti pro postupnou elektronizaci. Vzhledem k tomu, že v té době byl právě zkonstruován první bankomat, byl magnetický proužek používán pro výběr hotovosti. Bankomatové karty tak začaly dobývat svět. Teprve koncem 70. let se v USA objevily první platební terminály v obchodních domech, jejichž masový rozvoj nastal až v druhé polovině 80. let.

Nejprve byly platební karty použitelné pouze lokálně, později v rámci jednoho státu a od konce 60. let i mezinárodně. Prvními držiteli karet byli velmi dobří zákazníci s prověřenou finanční morálkou. Masové zavedení kreditních a zejména debetních karet v 70. – 80. letech způsobilo boom platebních karet. Přestaly být exkluzivní službou pro úzký segment zákazníků a staly se běžnou součástí života.

Systém platebních karet dnes tvoří:

- autorizační, clearingový a zúčtovací systém
- systém správy kare banky (Card Management Systém)
- platební karty
- bankomaty
- obchody (platební terminály)
- internetové obchody

Na samotném počátku historie univerzálních platebních karet se transakce autorizovaly z obchodu přímo u vydavatele karty, což trvalo 5 až 15 minut. Zúčtování se pak provádělo prostřednictvím mezinárodního platebního styku. Teprve začátkem 70. let MasterCard a

Visa vybudovaly první elektronické autorizační systémy využívající telex a automatizovaly clearing a zúčtování prostřednictvím výpočetních center. Tím se doba nutná pro autorizaci snížila na sekundy a zlevnilo se také mezibankovní zúčtování.

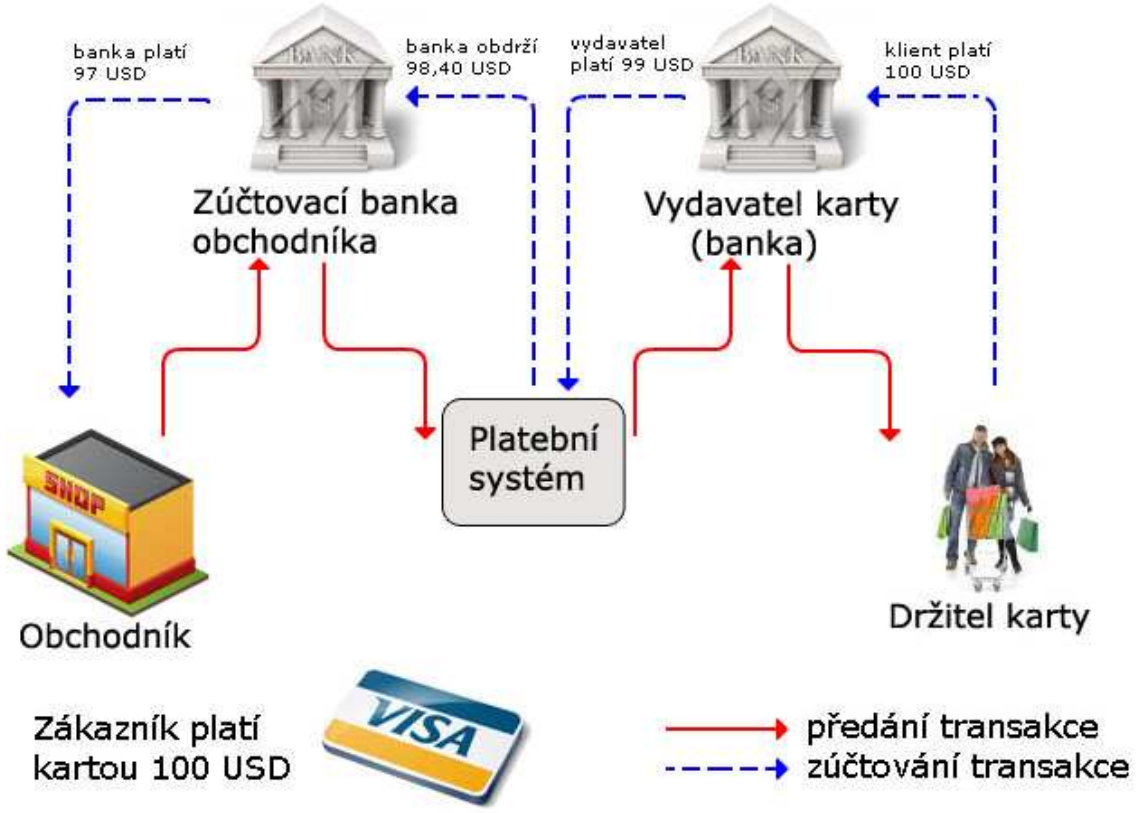
Platební karta vstupuje do tohoto systému v několika operacích:

- autorizace (ověření) transakce
- přenos transakce do centra platebního systému
- clearing (vzájemné vypořádání všech transakcí – pohledávek i závazků bank)
- zúčtování (úhrada výsledného salda mezi bankami)
- přenos transakce vydavateli karty (zúčtování s klientem, výpis)

Každý příjemce platebních karet (např. obchod) má stanoven tzv. autorizační limit (Floor limit). U transakcí překračujících jeho výši musí být provedena autorizace. Toto ověření se provádí telefonicky nebo automaticky, je-li obchodník vybaven platebním terminálem.

Autorizační centrum odešle do sítě platebního systému dotaz obsahující číslo karty, dobu platnosti, částku a další údaje. Podle čísla karty systém rozpozná jejího vydavatele a doplní dotaz o identifikaci banky. Banka ověří finanční krytí transakce zůstatkem na účtu, finančním nebo úvěrovém limitu klienta a odešle zpět potvrzení (autorizační kód) nebo odmítnutí transakce. Pokud je karta nahlášena jako odcizená nebo ztracená nebo si vydavatel přeje z jiných důvodů kartu zadržet (např. nedovolené přečerpání účtu klientem), předá příkaz kartu zadržet: Pick-up Card.

Celý proces autorizace od vstupu dotazu do sítě až po odeslání odpovědí bance trvá v průměru 2 sekundy, ale přenos výsledku až do bankomatu nebo platebního terminálu trvá déle (5-10 sekund). Pokud vydavatel karty neodpoví na autorizační dotaz do stanovené doby, proběhne ověření v centrále platebního systému: Dynamic Stand-in. V obou případech ověří centrála transakci na základě předem stanovených parametrů. V případě, že je přerušeno spojení s platebním systémem, proběhne záložní autorizace v lokálním spojovacím modulu: Down Option Parameters. Tím je zajištěna téměř 100% provozuschopnost platebních karet. Po obnovení spojení se odešlou zprávy o provedených záložních autorizacích do řídícího centra a vydavateli karty k provedení aktualizace dat.



Obr. 10. Průběh předávání transakce a jejího zúčtování [11]

Následujícím krokem v procesu zpracování platební transakce je clearing a zúčtování. Obchodník předává bance zprávu o provedené platební transakci v podobě papírového prodejního dokladu nebo elektronicky. Banka transakce zpracuje v systému zvaném Card Management Systém. Jeho výstupem jsou data pro zúčtování vlastních klientů a soubor dat určený pro vyrovnání s ostatními účastníky platebního systému.

Clearing těchto transakcí provádí centrální střediska VISA, Europay a MasterCard. Každý z vydavatelů pak denně obdrží informaci o sumě debetních a kreditních transakcí, které budou zúčtovány s jeho účtem. Tyto informace slouží k tomu, aby banky které jsou v převažující dlužnické pozici, mohly včas přesunout prostředky k úhradě na zúčtovací účet. Současně se zúčtováním odesílá centrála bankám detailní informace o jednotlivých transakcích, aby mohly zatížit účty svých klientů. Některé země provádějí clearing a zúčtování zvlášť pro tuzemské a mezinárodní transakce.

Clearingové a zúčtovací systémy zpracovávají i reklamace klientů a bank, jejichž hlavními příčinami jsou zejména chybně zúčtované a podvodné transakce. K chybnému zúčtování dochází zejména v případech, kdy zúčtovací banka odešle informaci o transakci duplicitně,

v jiné měně než byla prováděna nebo s chybně převzatou částkou. Současně provádí i bezpečnostní monitoring transakcí.

Jestliže autorizační, clearingový a zúčtovací systém tvoří kostru mezibankovních systémů platebních karet, pak jeho základem jsou informační systémy jednotlivých vydavatelů karet, provozovatelů bankomatů a zúčtovacích bank obchodníků. Tyto systémy se souhrnně nazývají systémy řízení platebních karet – Card Management Systém. Systém řízení platebních karet je provozně rozdělen do dvou vzájemně spolupracujících částí:

Front Office – tato část systému řízení platebních karet zabezpečuje on-line nebo off-line komunikaci s obchodní sítí banky (bankomaty a obchodníci akceptující karty) a mezibankovním systémem spolupracujících bank (na národní nebo mezinárodní úrovni), jako jsou např. EPSS a VISANet. Hlavní součástí Front Office jsou autorizační a bezpečnostní systém, komunikační modul a terminál management (řídí a monitoruje sítě bankomatů a platebních terminálů).

Back Office – je vlastním srdcem systému platebních karet. Na jeho konstrukci a variabilitě závisejí možnosti vydavatele v oblasti nabízených platebních karet (druhy karet, doplňkové služby, druhy poplatků a způsob zúčtování) a služeb obchodníkům. Celý tento systém se dělí do několika základních modulů, které jsou vzájemně provázány:

- **zúčtovací systém** provádí zúčtování transakcí vlastních klientů a cizích klientů (držitelé karet) ve prospěch vlastních bankomatů, pokladen poboček a obchodníků,
- **modul platebních karet** obsahuje informace o držitelích platebních karet, parametry produktů, seznam transakcí, které klient provedl, kurzovní lístek, atd.,
- **obchodní modul** obsahuje název a adresu obchodních míst, kategorii obchodu (hotel, obchod, atp.), výše poplatků, seznam všech transakcí, které byly v daném obchodním místě provedeny.
-

Systém řízení platebních karet je pro svou provázanost na účetní, informační a bezpečnostní systém banky a mezibankovní autorizační, clearingový a zúčtovací systém jednou z nejsložitějších bankovních technologií. Proto připojení každého takového systému do sítí MasterCard a Visa je spojeno s jeho certifikací.

4.1.4 Placení v obchodní síti

První platební karty používaly k provedení transakce karty s reliéfním písmem. K otisku údajů na kartě na účtenku více jak 50 let sloužil mechanický snímač. Účtenky byly 3-4 listé, nejčastěji ze samokopírujícího papíru. Nárůst počtu vydaných karet a provedených prodejních transakcí se projevil vzrůstem počtu papírových dokladů, které museli obchodníci vyplnit a zaslat bance nebo společnosti k úhradě. Velké množství transakcí muselo být telefonicky autorizováno. Přičteme-li k tomu nutnost zpracovat prodejní doklady a autorizace v bankách, není divu, že již ve druhé polovině 70. let byly zkonstruovány první elektronické platební terminály nazývané EFTPOS, které bezhotovostní operace zjednodušily.

První terminály byly založeny na principu kontroly platební transakce prostřednictvím záznamu finančního limitu, druhu použití a časové platnosti na magnetickém proužku karty a seznamu zakázaných a zablokovaných karet uloženém v platebním terminálu (off-line). Jednou nebo vícekrát týdně (nyní již denně) se pak prováděl přenos dat o provedených transakcích do banky nebo jiného zúčtovacího místa. Nejprve k tomu byly používány diskety, později telefonní a datové linky.V polovině 80. let se začaly používat první terminály pracující nepřetržitě v režimu on-line. Ověření každé transakce probíhá v reálném čase v autorizační centrále karetního systému, a to včetně kódu PIN je-li použit pro verifikaci držitele karty. Kombinací obou výše popsaných postupů ověřování jsou terminály pracující ve smíšeném režimu semi on-line. Toto řešení šetří čas a telekomunikační náklady. Zvláštním druhem terminálu jsou samoobslužné prodejní, telefonní a parkovací automaty.

4.1.5 Výběry hotovosti

S myšlenkou konstrukce zařízení na výplatu peněz přišel v roce 1965 Skot John Shepard Baron. Nebyl totiž spokojen s časově omezenými úředními hodinami bank a přemýšlel proto o způsobu jak zařídit, aby mohl klient získat hotovost prakticky kdykoliv. Poté to trvalo však ještě několik let, než byl první prototyp bankomatu uveden do provozu. Nicméně technika v té době nebyla příliš dokonalá, a také chyběly zkušenosti. První bankomaty v 60. letech byly velmi jednoduché a sloužily jen klientům pobočky nebo banky, která jej provozovala. Neměly obrazovku a k identifikaci klienta sloužily děrné štítky, které bankomat po transakci zadržel a klienti je obdrželi poštou s měsíčním výpisem

z účtu. I přes svou jednoduchost byl tento systém u klientů oblíben. Nízkou úroveň zabezpečení prvních bankomatů brzy odhalili podvodníci, kteří začali ve velkém vyrábět padělky děrných štítků. Začátkem 70. let se objevily první karty s magnetickým proužkem, které rychle nahradily nezabezpečené děrné štítky. K ověření totožnosti klientů byly zavedeny kódy PIN. Pro záznam údajů na magnetický proužek byly použity šifrovací metody, na jejichž konstrukci se podíleli specialisté britské armády a tajné služby MI5. V roce 1979 vyvinula společnost IBM technologii šifrování DES, která se od roku 1980 používá pro generování a ověřování PIN. Počet bankomatů roste ročně přibližně o 15-20 %, zejména díky rozvoji platebních karet v Jižní Americe, Asii a Evropě. Vzhledem ke složitosti technologie bankomatů se jejich výrobou zabývá jen asi deset firem. Největšími dodavateli bankomatů v Evropě jsou společnosti NCR, Siemens-Nixdorf, IBM a Bull, které dohromady kontrolují asi 2/3 trhu. Bankomat se skládá ze tří částí:

- trezor s kazetami bankovek a bezpečnostním a spojovacím modulem
- operátorská část sloužící k řízení bankomatu (PC, operátorská klávesnice a tiskárna)
- provozní část skládající se z transportního a počítacího systému, tiskárny, obrazovky, klávesnice, snímače platebních karet, případně i dalších modulů

Bankomat se dělí na dvě skupiny:

Off-line bankomaty již patří do historie. Pro ověřování transakcí používaly údaje zaznamenané na magnetickém proužku karty. Zde byla uvedena identifikace klienta, zakódovaný PIN a finanční limit a disponibilní limit karty, který se snižoval každou transakcí. Uplynul-li od data poslední transakce stanovený časový úsek (např. 48 hodin), bankomat při příští transakci disponibilní limit zvýšil na úroveň finančnímu limitu a klient mohl čerpat opět celou částku. Aby se zabránilo většímu přečerpání běžných účtů a zneužití ztracených karet, byly v bankomatu databáze dočasně zakázaných karet (přečerpaný účet) a ztracených karet. Tyto údaje se pravidelně aktualizovaly pomocí diskety nebo dálkově pomocí modemu. Stejným způsobem se přenášela data o provedených transakcích do bankovního systému. Tímto způsobem pracovaly např. první bankomaty České spořitelny v letech 1989-94.

Dnes se téměř výhradně používají **on-line bankomaty**, které jsou napojeny prostřednictvím datové sítě do autorizačního centra a ověřují prováděnou transakci v reálném čase (on-line) přímo u vydavatele karty. Transakce jsou ověřeny během pár sekund. U tohoto postupu není na magnetickém proužku zaznamenán ani PIN, ani finanční limit karty.

Jednoúčelové bankomaty slouží pouze k vyplácení hotovosti, zatímco víceúčelové bankomaty mohou poskytovat i další služby, např. výpis účtu, příjem vkladů hotovosti, směnárenské operace, atp. V posledních letech se také rozšířilo využití bankomatů pro dobíjení předplatných kupónů telefonů GSM, či platbu peněžních složenek.

4.1.6 Rozdělení platebních karet

V průběhu své historie se platební karty rozdělily na řadu druhů, které veřejnosti většinou splývají do názvů kreditní, nebo platební karta. Karty dělíme do několika skupin podle kritérií, která pak mohou být na skutečné kartě i kombinované.

Obr. 11. Rozdělení platebních karet

Platební karta je druhem identifikačních dokladů, jejíž rozměry a fyzikální vlastnosti stanovuje norma pro identifikační karty ISO 3554 na 85,6 x 54,0 x 0,76 mm. Karta je

vyrobena z třívrstvého PVC, který musí být mj. schopen vyrovnat deformace vzniklé při běžném používání. Je netoxický, a odolný vůči chemickým vlivům.

Druh záznamu na kartě je jedním z faktorů ovlivňujících způsoby možného použití karty.

- **reliéfní záznam** slouží pro transakce s použitím mechanického snímače
- **magnetický záznam** se u platebních karet objevil až začátkem 70. let, umožnil u karet zavést službu výplaty hotovosti z bankomatů a později elektronické placení
- **čipové karty** k záznamu dat využívají paměťový čip nebo mikroprocesor (viz kapitola 3.2)
- **laserové karty** jsou založeny na principu záznamu dat na kompaktním disku, poprvé byl tento prácím u karet testován v polovině 80. let v USA, paměť těchto karet je velmi vysoká (jednotky MB), ale v bankovnictví se nepoužívají.

Tištěné údaje

Pro použití v mechanických snímačích (implenterech) se na kartu vyrazí nezbytné identifikační údaje a to písmem OCR 7B velikosti 3,63 mm. Pro ně je určena dolní polovina přední části karty, kterou norma dělí na tři řádky:

1) **Account numer Line** – obsahuje číslo karty. První dvě číslice určují druh karty, např. MasterCard začíná vždy číslicí 5, VISA číslicí 4. Za nimi následuje identifikace vydavatele karty (zpravidla 5 znaků), přidělovaná orgány ISO. Zbývajících 8 až 13 míst je určeno pro identifikaci konkrétního klienta.
2) **Valid Data Lane** – uvádí se v ní období platnosti karty (měsíc a rok), a to buď v podobě uvádějící začátek i konec platnosti, nebo jen konec platnosti. Navíc je v této oblasti u karet MasterCard čtyřmístné identifikační číslo banky (ICA).
3) **Třetí řádek** – je určen pro jméno držitele karty s maximálním počtem znaků 27.
4) **Čtvrtý řádek** – obsahuje u služebních karet jméno společnosti, k jejímuž účtu je karta vydána

V řádku čísla karty musí být uvedeno šestimístné identifikační číslo vydavatele karty (Issuer Identification Number – IIN), které je organizaci přiděleno podle normy ISO/IEC 7812 -1,2.

Pro karty určené pouze k elektronickým transakcím (bankomaty, platební terminály) se v posledních letech nahrazuje reliéfní písmo hladkým tiskem.

Obr. 12. Přední strana platební karty [15]

Na obrázku č. 12 jsou vyznačeny základní údaje přední strany platební karty:

1) logo banky
2) EMV čip
3) číslo karty
4) hologram
5) logo vydavatele karty
6) datum platnosti
7) jméno majitele

Zadní strana karty pak obsahuje:

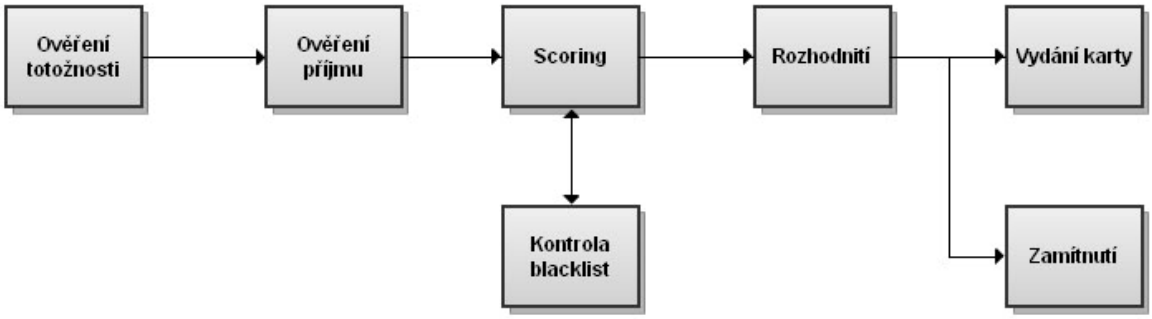
1) magnetický proužek – mývá 2 až 3 stopy záznamu identifikačních údajů. Celkem může být zaznamenáno až 1288 bitů.
2) podpisový proužek – je určen pro záznam podpisového vzoru držitele karty

Charge Card

Tato karta odstraňuje nutnost obstarávat si např. před služební cestou nebo nákupem hotovost, nebo šeky a umožňuje tak hradit bez problémů i nepředvídané výdaje, nebo zakoupit zboží, které zákazník původně neplánoval. Mezi majitelem účtu a vydavatelem karty může být uzavřena dohoda o automatickém inkasu z jeho účtu.

Podmínkou pro vydání této karty je důvěryhodnost klienta založená na jeho dobré znalosti bankou nebo na vyhodnocení scoringem. Scoring je metoda řízení rizika založená na

statistickém odhadu pravděpodobnosti, že hodnocená skutečnost nastane (v tomto případě klient bude splácet úvěr). Žádost o vydání karty obsahuje řadu údajů, ke kterým je přiřazeno určité bodové hodnocení. Součet těchto bodů udává tzv. skóre a je obrazem úvěrového rizika daného klienta. Bodové hodnocení, vzájemné vazby některých údajů a hranice pro přijetí, nebo zamítnutí žádosti jsou důvěrným know-how každé banky a zná je jen nejužší okruh zasvěcených. Pro úspěch scoringu je třeba zajistit dostatečně velké množství žádostí, co nejdelší časové období a také homogenní data.



Obr. 13. Zpracování žádosti o úvěrovou kartu

Kreditní karty

Jedná se o nástroj čerpání spotřebního úvěru čerpaného prostřednictvím revolvingového úvěrového účtu. Na rozdíl od Charge Card může být čerpaný úvěr u kreditních karet splácen po částech nebo najednou. Vždy je stanovena minimální výše splátky úvěru. I zde se poskytuje bezúročné období pro nákupy kartou. Úvěr nebývá zajištěn, proto jsou úvěrové karty nabízeny jen dobře známým klientům nebo na základě scoringu. Na základě ohodnocení bonity klienta, je mu pak stanoven úvěrový limit.

Debetní karty

Rozvoj výpočetní techniky a telekomunikací přinesl v 70. letech vznik debetních karet spojených s běžným účtem klienta. Do té doby byly platební karty vydávány bez přímé vazby na účet. Možnosti ověřit, zda právě prováděnou transakcí klient nepřekračuje zůstatek na účtu nebo povolený úvěrový limit, byla hlavní příčinou rozšíření bankomatových karet. Velký vliv na rozšíření karet mezi klienty měla správná taktika peněžních ústavů, tedy vědět jaký typ platebních karet přiřadit určitým skupinám obyvatelstva.

4.1.7 EMV

EMV je standard pro součinnost čipových karet a zařízení jež jsou schopny je přijmout, tedy platebních terminálů a bankomatů. Tato zkratka se skládá z prvních písmen tří společností, jež stály u zrodu tohoto standardu a spolupracovaly na jeho vývoji. Byly to Europay, MasterCard a Visa v roce 1994. V současné době jsou členy společnosti EMVCo, jež vlastní tento standard, také JCB a American Express.

EMV specifikuje požadavky na interoperabilitu mezi více aplikacemi čipu a interoperabilitou mezi čipem a terminálem. Tato kooperace je základem pro globální rozšíření čipových karet. Standard EMV má celkem 3 úrovně.:

1. úroveň – elektromagnetické charakteristiky, interface a přenosový protokol

2. úroveň – výběr aplikace čipu (definují jednotlivé systémy)

3. úroveň – specifikace pro implementaci v jednotlivých bankách nebo zemích

V roce 2009 bylo na celém světe již přes 944 milionů čipových platebních karet splňující EMV. Pokud chceme používat takové zařízení, ať už se jedná o novou platební kartu, nebo platební terminál v obchodě, musí splňovat EMV certifikaci pro používání v dané zemi.

EMV level 1 se zaobírá fyzickým elektrickým a přenosovým rozhraním,

EMV level 2 se zaobírá výběrem platebních aplikací a zpracováním finančních transakcí

V praxi to většinou bývá tak, že výrobce zařízení zařídí certifikaci úrovně EMV level 1 před uvedením na trh. Zákazník pak pro konkrétní aplikaci a použití žádá u své smluvní banky o certifikaci EMV level 2.

Výhody EMV kontaktních a bezkontaktních karet:

- zvýšená ochrana proti padělání karet, jež spoléhají pouze na data zakódovaná v magnetickém proužku na zadní straně karty
- unikátní digitální pečeť nebo podpis přímo v čipu zaručuje autenticitu při off-line používání a předchází tak zneužití falešných platebních karet
- mohou být použity pro zabezpečené platební transakce, chrání držitele karty, obchodníky proti zneužití karet pomocí jedinečných přenosových on-line kryptogramů
- poskytuje rozšíření metod pro ověření držitele karty
- jsou schopny uložit mnohem více informací než běžné magnetické karty

4.2 Budoucnost karet

Všeobecně se očekává nárůst počtu karet v předplatitelských a platebních systémech vedoucí až k radikálnímu omezení jak kovových, tak papírových peněz ve vyspělých zemích světa. Novinkou, která má ulehčit obchodníkům práci a zákazníkům čas, je bezkontaktní technologie PayPass. Předpokládá se, že první velcí obchodníci ji začnou používat už ve druhé polovině letošního roku. PayPass umožní jednoduché odbavení plateb – v případě nákupu do 500 korun, nebude nutné zadávat PIN, postačí kartu pouze přiložit ke speciální čtečce a je zaplaceno. Ovšem proti rozšíření bezkontaktních platebních karet je několik aspektu jako jsou bankovní poplatky za bezhotovostní platby ve výši 2 až 3 % snižující již tak nízkou marži obchodníků s potravinami. Bude tedy nutné aby se od těchto poplatků upustilo, popř. se snížili na minimum, aby drobný prodej neposunul do záporné marže. Další velká inovace která se k nám blíží je služba „Square“. Obchodník při ní již nebude potřebovat pokladnu, ale postačí mu obyčejný telefon a adaptér.

Názor odborníků na toto téma je vesměs jednoznačný, bezhotovostní platby budou i v budoucnu nadále posilovat. Je totiž velký obecný zájem na tom aby se zrychlil proces odbavení zákazníků – např. využitím karet s RF čipy. Z hlediska technologie čipových karet je vyvíjen tlak na výrobce aby se zvýšila bezpečnost bezkontaktních karet alespoň na úroveň těch kontaktních. Je to jedno z mála negativ jež brzdí ještě většímu rozvoji, i když jejich cena stále klesá.

Obecným trendem informačních a komunikačních technologií je také mobilita. V České republice byl aktuálně spuštěn projekt, jež umožní řidičům platit na místě pokuty za spáchané dopravní přestupky. Evropskou jedničkou v tomto směru je firma Ingenico, která nalezla mezeru na trhu a přišla se zařízením které kombinuje klasické PDA s platebním terminálem a termotiskárnou. Toto zařízení je schopné číst magnetické, kontaktní i bezkontaktní karty, provozovat webové aplikace aj.

Obr. 14. Ingenico IPA280 [23]

5 ZABEZPEČENÍ DAT NA KARTĚ

Dosud se práce zaobírala plastovými kartami jakožto nosiči informací. Stejně jako je tomu jinde, tak i v této oblasti je bezpečnost dat, která karta přenáší ať už v grafické či digitální podobě, velmi důležitá.

Pokud se bavíme o bezpečnosti v souvislosti s plastovými kartami, lze rozdělit rizikové faktory do tří skupin:

- integrita – hrozba nežádoucí modifikace informací
- autenticita – hrozba neoprávněného využívání služeb
- utajení – hrozba prozrazení důvěrných informací

5.1 Grafické ochranné prvky

Jelikož jsou karty samy o sobě přenosné, je vše co je na kartě vytištěno či vyryto, dostupné jak držiteli karty, tak i dalším osobám, jež s nimi mohou přijít za různých okolností do styku. Je tedy zřejmé že v těchto případech mohou složit jen jako nástroj k prokázání oprávnění držitele. Proto musí být karty zabezpečeny proti manipulaci, pozměňování či padělání.

Karty lze opatřit těmito grafickými prvky:

- hoststamping – jak již bylo zmíněno v kapitole 2, jedná se o technologii horké ražby, pomocí které se za vysoké teploty "vtiskne" speciální metalická fólie různých barev do těla karty, tímto způsobem se vytváří například hologramy a speciální loga. Hologramy lze samozřejmě i tisknout či lepit. Poté je vhodné je překrýt laminační ochrannou vrstvou.

Obr. 15. Struktura karty s hologramem [12]

- UV barvy – karty lze potisknout speciálními ultrafialovými barvami, které jsou viditelné zase pouze v UV spektru, tzn. že k jejímu prohlížení je zapotřebí zdroj ultrafialového záření, podobně je tomu u ověřování bankovek
- „tisk šedé na černou“ – jelikož je pro naprostou většinou tiskáren nemožné tisknout na světle šedé pozadí tmavší šedý text či grafiku, lze i tuto metodu považovat za ochrannou
- mikrotisk – je metoda podobná předchozí, vytištěné znaky jsou natolik miniaturní, že jsou viditelné pouze pod lupou, při použití jakékoliv kopírky či skeneru se tento ochranný prvek nezobrazí, většinou je není možné tisknout ani pomocí termosublimačních tiskáren, z hlediska padělání karet se jedná o dostatečnou záruku proti kopírování
- Čárový kód – jedná se asi o nejprimitivnější metodu, pokud lze vůbec skrytí informací v čárovém kódu považovat za druh zabezpečení, neboť i QR (druh 2D kódu) umějí přečíst i novější mobilní telefony
- překrytý čárový kód – jedná se o metodu, jež zabrání kopírování čárového kódu, ten je přetištěn černou barvou složenou z YMC barev, překrytý čárový kód pak nelze zkopírovat, resp ofotit, a nelze jej ani přečíst laserovými či CCD snímači čárových kódů, toto je možné pouze infračerveným snímačem
- Guilloche (Giloš) – je geometricky přesný motiv tvořený průnikem jedné nebo více křivek s přesně definovaným průběhem, zakřivením a hustotou. Tisk gilošů je technologicky náročná záležitost a lze se s ním setkat např. u bankovek a cenin
- opacitní značky – aplikují se již při výrobě karty nebo při aplikaci laminačních vrstev, jsou to objekty s odlišnou schopností propouštět nebo odrážet světlo
- laser engraving (laserové rytí) – je moderní způsob rytí grafického designu do povrchu karty, na rozdíl od běžného gravírování nedochází zde k přímému styku s materiálem karty, využívá se laserový paprsek pomocí kterého se odstraní speciální vrstva z povrchu
- CLI/MLI – jedná se podobně jako v předchozím případě o úpravu povrchu pomocí laseru, Changeable Laser Imager a Multiple Laser Image jsou pomocí specializované technologie integrovány do průhledné povrchové vrstvy na kartě a tvoří tzv. „živý obraz“. Do něj mohou být právě pomocí laseru vyryty dva obrazce ve dvou různých úhlech
- kinegram – je tvořen malými mikroskopickými oblastmi jež mají schopnost lámat

světelné paprsky, při pohledu na kinegram z různých úhlů jsou viditelné rozdílné obrazce

5.2 Bezpečnost čipových karet

Zabezpečení čipových karet (bavíme-li se o aktuálně využívaných typech) nesoucích informace je úzce spojeno s kryptografií. Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

Tato věda se po staletí vyvíjela k větší složitosti zároveň s lidskou civilizací a mnohokrát ovlivnila také běh dějin. Zejména utajení či vyzrazení strategických vojenských informací může mít zásadní vliv, stejně tak prozrazení politických intrik, přípravy atentátů nebo informací o bankovním přístupu, to vše může úzce záviset na bezpečném přenosu informací a na schopnostech útočníka šifru rozbít [1].

Podstatou kryptografie jsou důležité faktory jako je utajení klíče, síla algoritmu, dostatečné délky klíče a na obtížnosti extrakce klíče ze zpráv. Klasické kryptografické algoritmy fungují na principech:

- transpozice – změna pořadí znaků ve zprávě
- substituce – záměna znaků
- abecední substituce

Tyto algoritmy jsou v současné době již velmi snadno zlomitelné, zvláště při využití moderních počítačů a jazykové statistiky. Nyní se pro utajení informací nejen na čipových kartách používají dva typy algoritmů:

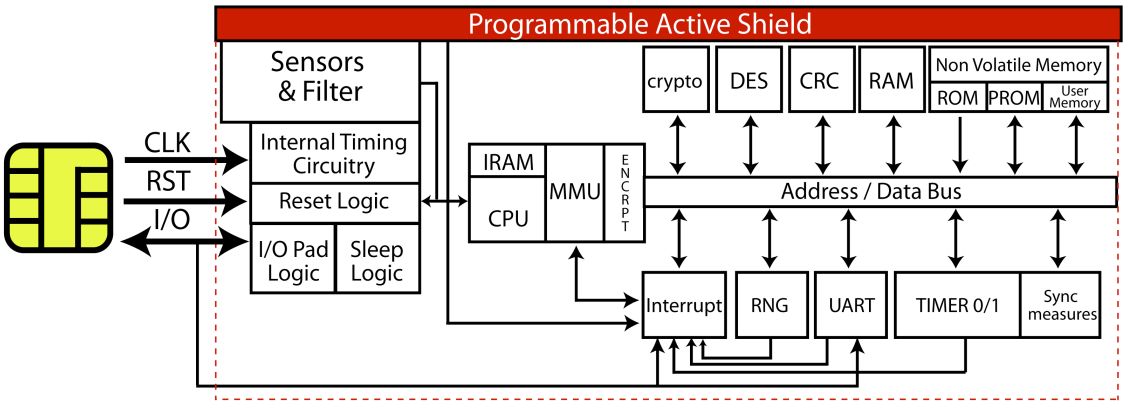
- opakovaná permutace a substituce bitů (symetrické šifry) – DES, 3-DES, IDEA, RC2, RC5, GOST, Blowfish, Twofish
- matematické výpočty (asymetrické šifry) – RSA, Rabin, ElGamal, eliptické křivky,

Asymetrická kryptografie je založena na tzv. jednocestných funkcích, což jsou operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, z výstupu je však velmi obtížné nalézt vstup. Oproti tomu symetrická šifra, někdy též nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování

jediný klíč. Velkou nevýhodou je nutnost sdílení tajného klíče, což v praxi znamená, že se odesílatel a příjemce tajné zprávy musí předem domluvit na tajném klíči.

Se stoupajícími počty útoků se samozřejmě musela zdokonalovat také architektura bezpečnostních mikrořadičů. Běžná karta v současné době disponuje již vyspělou technologií.

- nepřístupné vnitřní časovací obvody (ITC) – jsou využívány pro kryptografické a bezpečnostní operace,
- procesor (CPU) –stará se o proprietární časování, aby ztížil případnému útočníkovi určit, které operace právě integrovaný obvod (dále jen IC) provádí,
- programovatelný aktivní štít (PAS) – pokrývá celý IC, je vybaven signální vrstvou, jež detekuje pokusy o sondáž, ovládnutí interních modulů,
- modul správy paměti (MMU) – je volitelná komponenta, jež vytváří skutečný hardwarový firewall uvnitř IC,
- modul kryptace paměťové a procesorové sběrnice (ENCRPT) – šifruje a dešifruje data uložená v pamětích pomocí klíčů a proprietárních symetrických algoritmů, stará se o to, aby sběrnice spojující RAM a procesor mohla být šifrována po každém resetování čipu,
- šifrovací koprocesory – jsou přídavné koprocesory jež vykonávají symetrické a asymetrické šifrování,
- DES modul – provádí výpočty DES a 3-DES algoritmů,
- CRC modul – ověřuje integritu dat, zda nedošlo k chybám a změnám během přenosu, čtení a zápisu dat,
- paměti (P)ROM – slouží k uložení dat při výrobě karty, data jsou samozřejmě šifrovaná, aby nebylo možné je číst jako prostý text, pokud jsou extrahovány z IC,
- kryptace datové sběrnice – veškerá data přenášená sběrnicí jsou šifrována, je možné také měnit jednotlivé adresy sběrnice, aby adresové schéma nebylo pro útočníka srozumitelné,
- generátor náhodných čísel (RNG) – vysoce kvalitní generátor je základem mnoha kryptografických algoritmů, jeho pomocí je vygenerován náhodný klíč, jež se používá při vzájemné autentizaci a šifrování,



Obr. 16. Komponenty bezpečnostního mikrořadiče [16]

Software čipových karet

Charakteristiky tradičních (zastaralých) karet:

- jedna karta = jedna funkce
- software uložen pouze v ROM, tzn nelze jej aktualizovat
- proprietární software vytvořený výrobcem
- používané programovací jazyky C, Assembler

Charakteristiky moderních karet:

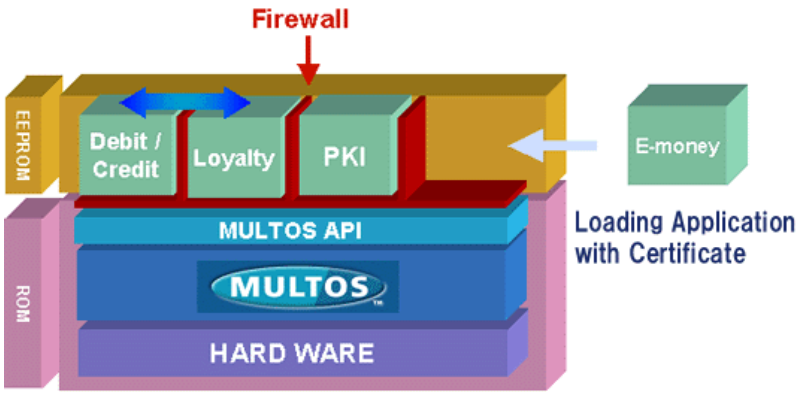
- více aplikací na jedné kartě s řízeným sdílením informací
- software může vyvíjet a nahrávat nejen výrobce
- vývoj aplikací v jazycích Java oproti standardnímu API

MULTOS

Pod touto zkratkou se skrývá zatím nejdokonalejší multiaplikační operační systém čipových karet. Skládá se ze dvou základních unikátních technologií, jež vytváří na kartě virtuální zařízení, které je schopno bezpečně vykonávat veškeré aplikace a STEP (Secure Trusted Environment Provisioning) technologie, jež zaručují, že veškeré operace prováděné systémem budou zcela řízeny uživatelem .

Platforma MULTOS se řídí několika důležitými pravidly:

1) veškeré aplikace, resp. kódy mohou být nahrány do karty, nebo odstraněny pouze se svolením držitele karty, k tomu se využívají certifikáty a šifrovací autorita
2) aplikace musí být striktně odděleny od všech ostatních, nemohou tedy manipulovat s daty jiných aplikací, o toto se stará firewall, jež dohlíží na jejich vykonávání, pokud se jedna aplikace pokusí neoprávněně číst z cizího paměťového prostoru, MULTOS okamžitě detekuje toto narušení a běh aplikace ukončí
3) nahrávání a mazání aplikací nesmí mít žádný vliv na kód a data již existujících aplikací, to je zajištěno alokací vlastního paměťového prostoru, rovněž je zabráněno následnému rozšiřování již přidělené paměti, jako to dělají např. Java-Karty, riskoval by se tím útok na cizí data
4) proces nahrávání aplikace musí být schopný garantovat autenticitu, integritu a utajení dat, MULTOS používá asymetrické šifry pro zakódování nahrávaných aplikací třetí strany za použití veřejného klíče dané karty, nahrání aplikace tedy nevyžaduje přenos zabezpečeným kanálem, MULTOS poté dešifruje data aplikace svým unikátním privátním klíčem, tento způsob nahrání dat do karty je patentován.



Obr. 17. MULTOS architektura [17]

Čipové karty se stávají častým cílem útočníků z několika prostých důvodů. Úspěšné útoky umožňují zneužití prostředků či informací a jsou finančně vysoko ceněné. Dalším důvodem je snadné obstarání pokusných vzorků pro otestování útoků, neboť čipové karty jsou levné a všeobecně přístupné. Útočník je také může snadno přenést do vlastního prostředí a v bezpečí podrobit sérii požadovaných útoků.

Rozeznáváme 3 skupiny útoků na data v čipových kartách:

- fyzické
- logické
- postranní

5.2.1 Interní fyzické útoky

Všechny funkce čipové karty jsou realizované na jednom čipu, jež je možné potřebně zkoumat. K tomu je samozřejmě nutností mít k dispozici kvalitně vybavenou laboratoř s výkonným technickým vybavením. Při takovýchto útocích se provádí především analýza a samotná modifikace hardwaru.

Rozpouštědla, leptavé látky, napouštění

Leptáním je možné odstranit vrchní ochrannou vrstvu na čipu karty. Na povrchu čipu je možné rozpoznat funkční bloky a podrobit jej optické, nebo elektrické analýze. V případě použití epoxidové pryskyřice je odstranění mnohem snazší, než při použití kovových a silikonových vrstev, jejichž odstranění vyžaduje agresivní nebezpečné chemikálie. Takovýto útok ztěžuje v dnešní době rozšířené používání vícevrstvých čipů.

Napouštění je speciální technika, jež využívá rozdíly v rychlosti leptání na odhalení jedniček a nul v některých typech pamětí ROM.

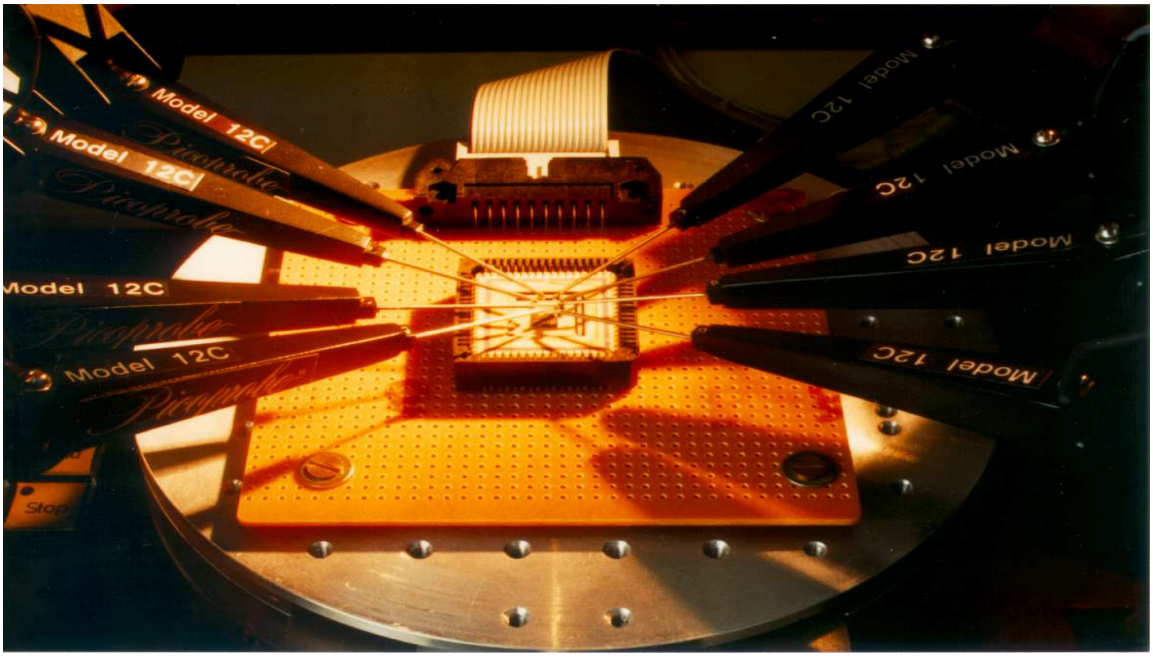
Obr. 18. Čip odkrytý leptáním [9]

Rastrovací elektronový mikroskop

Pokud se podaří čip odkrýt a nepoškodit jej, existuje pak množství způsobů odhalení obsahu aktivních RAM pamětí pomocí kontrastu napětí.

Sondáž

Tento způsob spočívá v umístění tenkých jehel na klíčová místa v čipu, kde je pak možné odposlechnout, popřípadě modifikovat komunikace po vnitřní sběrnici. Nutnou podmínkou k tomuto je samozřejmě zachování čipu ve funkčním stavu.



Obr. 19. Sondování pomocí osmi jehel *[18]*

Zaostřený iontový svazek (Focused Ion Beam - FIB)

Na rozdíl od elektronového mikroskopu působí proudem iontů. Odhaluje detaily a je dokonce schopný vytvářet změny v obvodě. Přidáním různých plynů k iontovému paprsku je možné nanést materiál, který vytváří linky, izolátory, nebo dokonce polovodiče. Touto technikou je možná tvorba tunelů ve vícevrstvých obvodech. Linky, které jsou příliš tenké a křehké pro sondy, mohou být pomocí FIB rozšířené a prodloužené.

Ochrana před fyzickými útoky

- Velikost čipu – zmenšením na úroveň menší než 200nm je znemožněna analýza pomocí optického mikroskopu a stejně tak je poté čip příliš malý na zkoumání sondami. Analýza je v tomto případě možná jen pomocí sofistikovaných elektronových mikroskopů a FIB,
- vícevrstvé čipy – citlivá data jsou zpracovávána ve vnitřních vrstvách čipu do kterých je obtížné proniknout,
- ochranná vrstva – na vrchní vrstvě je nanesená ochranná síť, která v případě svého narušení způsobí vypnutí čipu a vymazání paměti, což znemožňuje analýzu čipů v aktivním stavu,
- senzory – signály měřící proměnné prostředí jako je světlo, teplo, napětí či frekvenci hodin způsobí vypnutí čipu v případě, že se měřené hodnoty dostanou mimo stanovené meze,
- kódování vnitřní sběrnice – útočník pokoušející se interpretovat data na sběrnici musí předtím realizovat úplné reverzní inženýrství logiky kodéru,
- sjednocená logika – funkční bloky nejsou rozdělené do sekcí, ale smíchané dohromady. Tato technologie se používá většinou jen v drahých pokročilých zařízeních. Sektor standardních levných karet, stále čeká na masové zavedení této technologie.

5.2.2 Logické útoky

Čipové karty mají jeden komunikační kanál, přes který probíhá výměna informací se čtecím zařízením. Jsou funkcionálně podobné malým počítačům, neboť podporují velké množství příkazů vložených různými výrobci. Kvůli takovéto komplexnosti se může stát, že se vyskytne chyba, která se neprojeví při běžném používání, ani při bezpečnostních testech. Logické útoky zneužívají této chyby, aby zmátli čipovou kartu a získali tajné informace, nebo je pozměnili. Společným jmenovatelem této třídy útoků je nedestruktivní povaha, snadnost reprodukce a získání prostředků (karty, čtečky, PC, manuály, standardy). I proti různým technikám logických útoků existují způsoby ochrany.

Skenování příkazů (skryté příkazy)

I když čipové karty na běžné užívání potřebují jen několik příkazů, jsou schopny jich technicky rozlišit více než 65000. Některé příkazy mohou na čipu karty zůstat aktivní z doby testování nebo předcházejících aplikací. Takovéto příkazy pak mohou představovat hrozbu a vést k úniku či změně chráněných dat.

Opatření:

- omezení dostupnosti příkazů
- omezení a kontrola zavádění příkazů
- řízení životního cyklu

Skenování souborového systému

V případě, že má soubor větší přístupová práva, než-li je potřebné, vzniká bezpečnostní riziko a při přístupu vícero oddělených aplikací naráz na jeden soubor může dojít ke zmatení operačního systému a přidělení nekorektních přístupových práv.

Opatření:

- omezení přístupu k souborům
- test mechanismu přístupu (PIN)

Neplatné požadavky / přetečení zásobníku

Všechny používané příkazy mají určitý počet platných parametrů. Ovšem nepovolená hodnota tohoto parametru může vést namísto požadovaného odmítnutí k nesprávné interpretaci a nežádoucím efektům. Příkladem může být příkaz ke čtení souboru, kde díky špatně zadané délce ofsetu může být překročena skutečná velikost souboru.

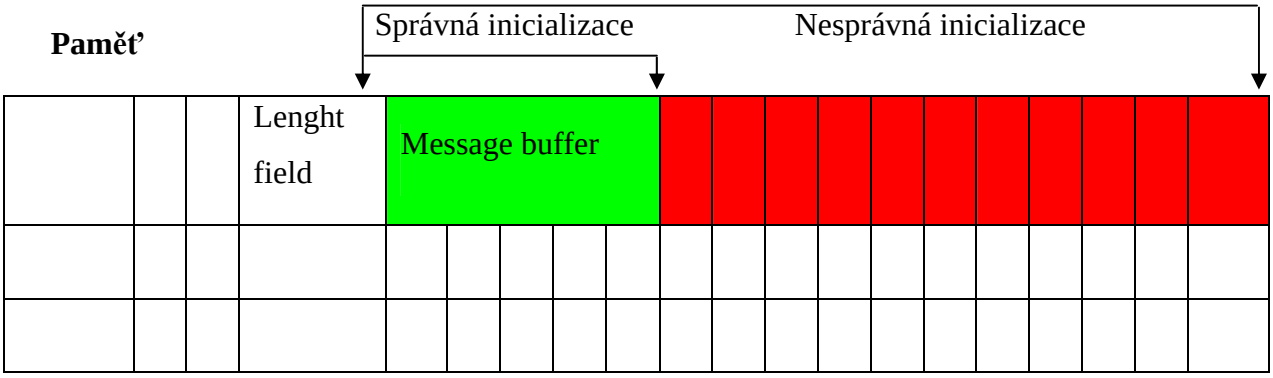
Opatření:

- zamezení chybného přístupu
- ověřování shody

Kryptografická analýza a zneužití protokolu

Výměna informací mezi terminálem a čipovou kartou je řízena komunikačním protokolem, který kontroluje tok dat a ošetřuje chyby. Posláním zprávy, která neodpovídá aktuálnímu stavu komunikace, je možné zmást čipovou kartu a dostat se ke chráněným informacím.

Příkladem je chyba v implementaci funkce zotavení se z chybového stavu. Čipová karta si udržuje v RAM malý buffer, do kterého ukládá výsledky operací. Někdy se zde nachází i délka pole dat připravených na odeslání. V případě, že zpráva nebyla předtím korektně doručená, může příjemce požádat o znovu-přenesení. Pokud ovšem nebyla původně žádná zpráva odeslaná, pak se při nesprávné implementaci karta pokusí zprávu znovu odeslat. Při tom samozřejmě použije pole uvedené délky, jež není správně inicializované, a příjemce dostane část paměti nebo dokonce její celý obsah i s chráněnými daty.



Obr. 20. Rozložení paměti v čipu

U proprietárních šifrovacích protokolů není možné veřejné testování a upozornění na chyby. Mohou tedy obsahovat chyby, které jsou v případě úniku struktury protokolu zneužitelné.

Obecně se způsoby ochrany před logickými útoky musí řídit několika pravidly:

1. strukturovaný návrh
2. formální verifikace
3. testování
4. standardizace rozhraní a aplikací
5. používání testovacích laboratoří

Softwarová analýza

Na následujících řádcích zdrojového kódu v jazyku Java si můžete všimnout, jak je snadné stažení veškerého obsahu paměti z karty. Využije se při tom protokolu APDU, což je komunikační protokol mezi čipovou kartou a čtecím zařízením.

```
1 class MaliciousCardlet
2       {
3        public void process(APDU a)
4               {
5                for (short i = 0; i <= 0xFFF8; i += 2)
6                       {
7                        byte [] b = (byte []) i;
8                        send_byte((byte) (b.length >> 8));
9                        send_byte((byte) (b.length & 0xFF));
10                      }
11              }
12      }
```

Samozřejmě, že neověřený kód není vykonáván přímo v HW, ale skrze softwarově izolovanou vrstvu, tzv. sandbox. API zabezpečující prostředí pro vykonávání ověřených aplikací poskytuje řízený přístup k systémovým prostředkům. Oproti tomu neověřené aplikace jsou vykonávány bezpečnostním virtuálním zařízením. Obě metody mají přiřazeny sadu privilegií a schopností, což závisí na zavaděči, který je použit k nahrání kódu. Systémový kód má veškerá oprávnění, oproti tomu webový aplet má oprávnění velmi omezená.

5.2.3 Postraní útoky

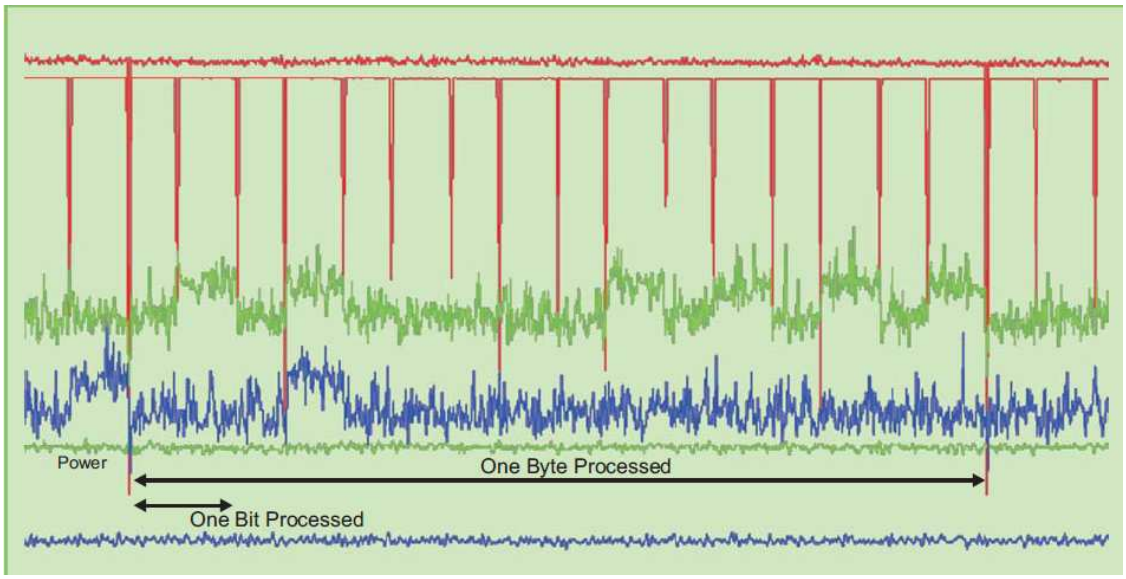
Využívají fyzikální fenomény na analýzu, či modifikaci chování čipové karty.

Například měřením spotřeby energie je možné odhalit detaily o zpracovávaných datech. Umožňuje to skutečnost, že tranzistory na čipu protéká během činnosti elektrický proud a množství spotřebované energie závisí na určitém probíhajícím procesu.

Dalším jednoduchým nepřímým způsobem je odhadnutí, kdy se požadovaná data právě zpracovávají na základě předpokladu, že se úlohy na čipu vykonávají v pravidelných stanovených cyklech.

Diferenciální analýza spotřeby energie – odhalení klíče algoritmu DES

Spotřeba energie není samozřejmě konstantní, stále se mění a projevují se v ní pravidelné vzory v závislosti na právě zpracovávaných datech. Algoritmu DES trvá zašifrování vstupních dat přesně 16 cyklů. Je tedy možné identifikovat 16 opakujících se vzorů v charakteristice spotřeby energie. Viz obr .



Obr. 21. Analýza algoritmu DES [19]

Útočník potřebuje znát pouze vstup, nebo výstup algoritmu. Protože zpracování bitu ‘1’ spotřebuje více energie, než zpracování bitu ‘0’ a naopak. Je tedy možné tímto způsobem odhadnout klíč používaný algoritmem DES [18].

Ochrana před útoky postranní analýzou

Hardwarová opatření:

- snížení spotřeby energie, tlumení EMG záření (např. metalickým krytím)
- zvýšení šumu vykonáváním náhodných procesů
- změna časování, proměnná frekvence hodin

Softwarová opatření:

- redukce relevantních signálů náhodným řazením procesů
- přidání časového šumu náhodným zpožděním, více-cestné vykonávání algoritmu
- eliminace časových závislostí
- plnění pomocných proměnných náhodnými hodnotami

Opatření na úrovni aplikací:

- omezení počtu pokusů o průnik (např. zadávání PINu)
- omezená kontrola a viditelnost vstupu a výstupu šifrovacích algoritmů

Způsoby nebezpečné manipulace:

- napětím – obvodu jsou vnucovány výkyvy napětí mimo obvyklé pracovní meze a je zkoumaná změna chování, kterou mohou způsobit,
- EMG zářením – silný elektromagnetický impuls může indukovat signály, jež mohou poškodit čip nebo vyvolat nestandardní chování,
- teplotou – sledování změn chování změnou teploty mimo pracovní meze,
- světlem a RTG paprsky – zde se využívá citlivosti polovodičů na světlo.

Vhodná opatření:

- použití senzorů pro napájecí napětí, světlo a teplotu,
- dvojitá implementace (pro ověřování),
- kontrola platnosti běhu programu.

5.2.4 Hrozby bezkontaktních čipových karet

Mimo výše zmíněných hrozeb existují samozřejmě také hrozby specifické pouze pro bezkontaktní čipové karty.

Takzvané „Man-in-the-middle“ útoky jsou způsoby odposlechu dat během běžného přenosu, přičemž si držitel karty nemusí být ničeho vědom. Ochranou by v tomto případě mělo být dostatečné šifrování spojení a vzájemná autentizace.

Na rozdíl od kontaktních čipových karet existuje mnohem větší riziko přerušení operace při vzdálení se z dosahu EMG pole. Vykonávané transakce mohou zůstat nedokončené, což může znamenat velké bezpečnostní riziko. Ovšem toto závisí na platformě systému. Vhodnými opatřeními v tomto případě bude bezpečné ukončování operací a backtracking. Při zápisu dat do bezkontaktní karty jsou nejprve uložena do mezipaměti (bufferu) a až poté do konkrétního bloku. Po úspěšném dokončení karta odešle tuto informaci do čtecího zařízení. Pokud ji ale neobdrží, považuje proces zápisu za nezdařilý.

Nejvýznamnějším rozdílem oproti kontaktním čipovým kartám je to, že uživatel nemusí ani vědět, že se na kartě provádějí nějaké operace či transakce. V tomto případě totiž nejsou k přenosu dat nutné klasické dotykové čtečky, ale stačí být v dosahu příslušného pole. Ovšem takovéto riziko je čistě teoretické. K tomu aby útočník chtěl číst data z karty na větší vzdálenost, musel by použít čtecí zařízení s vysoce výkonnou anténou. Takovémuto riziku se dá předcházet například vyžadováním interakce uživatele karty při autentizaci, nebo speciálním odstíněným pouzdrem. atp. Je zřejmé, že jedině kombinací různých prvků včetně interakce lze dosáhnout zabezpečení

Některé typy karet mají implementované kontaktní i bezkontaktní rozhraní, které využívá jeden čip. V takovém případě je možné, že útočník vytvoří komunikační tunel pomocí jednoho rozhraní a posléze se přepne na druhé, méně zabezpečené.

5.2.5 Rozšíření čipových karet

Jak již bylo řečeno, nejvyšší stupeň zabezpečení lze dosáhnout pouze kombinací různých prvků, a to neplatí nejen pro karty. Biometrické systémy, jež jsou schopny na základě unikátnosti získaných vlastností identifikovat uživatele. Nabízí se proto skvělá kombinace karty, v jejímž čipu jsou uloženy biometrické údaje držitele. V praxi to funguje tak, že uživatel se nejprve autentizuje kartou popř. PINem a poté ještě některým z biometrických

údajů např. otiskem prstu. Z toho plyne, že i ukradená karta s prolomeným heslem je útočníkovi k ničemu, neboť nedisponuje biometrickými vlastnostmi jako pravý majitel karty. Typickými aplikacemi kde se takovéto kombinace používají jsou různé typy ověřování přístupů či totožnosti ve střežených objektech.

II. PRAKTICKÁ ČÁST

6 PRAKTICKÉ TESTY KARET

V této části práce budou popsány testy s plastovými kartami, které jsem provedl za účelem podrobného zdokumentování a ověření doposud popisovaných teoretických informací.

6.1 Potisk plastové karty

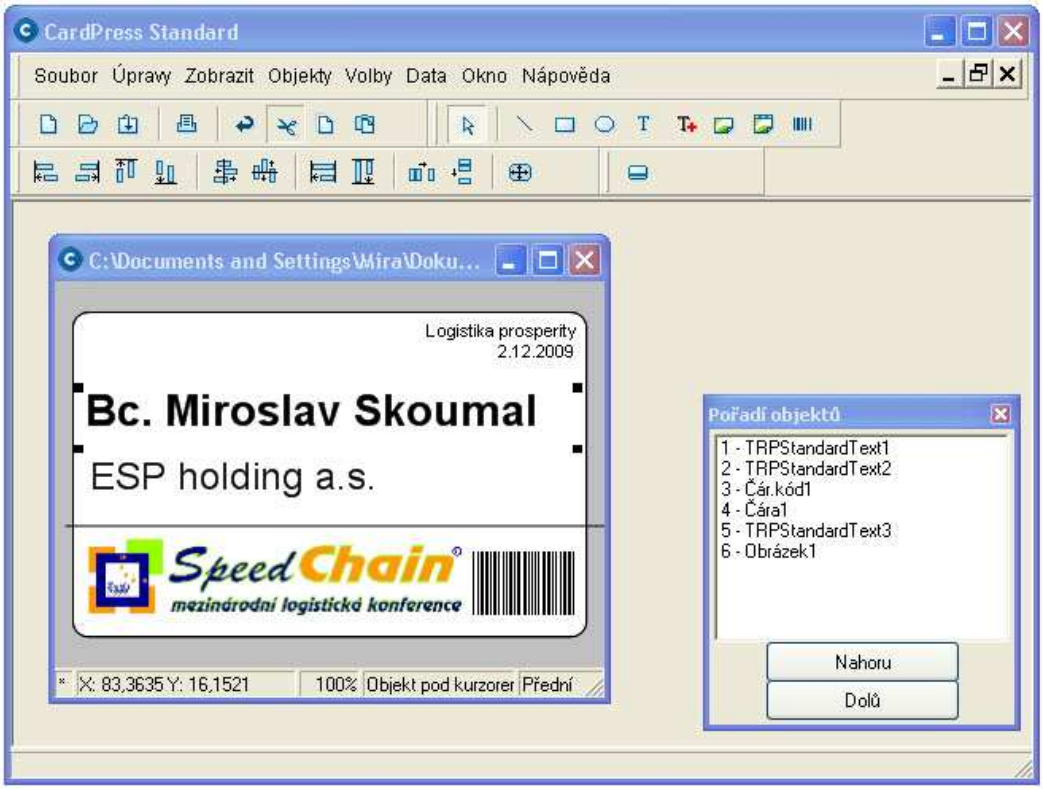
Pro testovací tisk jsem se rozhodl použít retransférovou tiskárnu plastových karet EDISECURE XID 560ie. Tato tiskárna je navržena zvlášť pro použití v průmyslu. Poskytuje téměř tak kvalitní potisk, jaký bychom získali offsetem, a to i na nerovnoměrném povrchu karet. Mezi hlavní výhody patří schopnost potisku karty po celé ploše a použití barevných kazet pro snadné doplňování spotřebního materiálu. Interní posuvný mechanismus umožňuje tisk po obou stranách karty bez ohledu na umístění magnetické stopy nebo kontaktního pole. Tiskárna je také schopna kódovat čipové karty a umožňuje jednostrannou laminaci. Tato tiskárna patří mezi nejrychlejší na trhu, čemuž odpovídá také cena přesahující 100 000,- Kč.

Obr. 22. EdiSecure 560ie [20]

K tisku je samozřejmě zapotřebí také příslušný software. Použil jsem aplikaci CardPress, jež byla vyvinuta pro tiskárny plastových karet Zebra, Evolis a EdiSecure firmou PaSCom s.r.o. Tento software umožňuje velmi jednoduchý návrh, zpracování dat i potisk karet. Obsahuje vektorový grafický editor pro tvorbu grafických prvků. Je schopen spolupracovat se všemi běžnými databázovými systémy MS Access, Oracle, SQL, Paradox, Informix, FoxPro, atd. Umožňuje kódování Mifare karet a podporuje také biometrické systémy.

Po instalaci aplikace CardPress jsem vytvořil databázi osob, jež obsahovala atributy jako jméno, příjmení, titul, firma a unikátní ID. Při spuštění se automaticky vytvoří design prázdné karty předdefinované velikosti. Postupně jsem na kartu vložil prvky textové pole, čárový kód, čára a obrázek. V okně nazvaném „Pořadí objektů“ jsou zobrazeny veškeré

objekty, které jsou v návrhu umístěny. Čárový kód obsahuje pouze unikátní ID z databáze osob. V panelu nástrojů lze nalézt funkce pro standardní zarovnání objektů a některé grafické prvky.



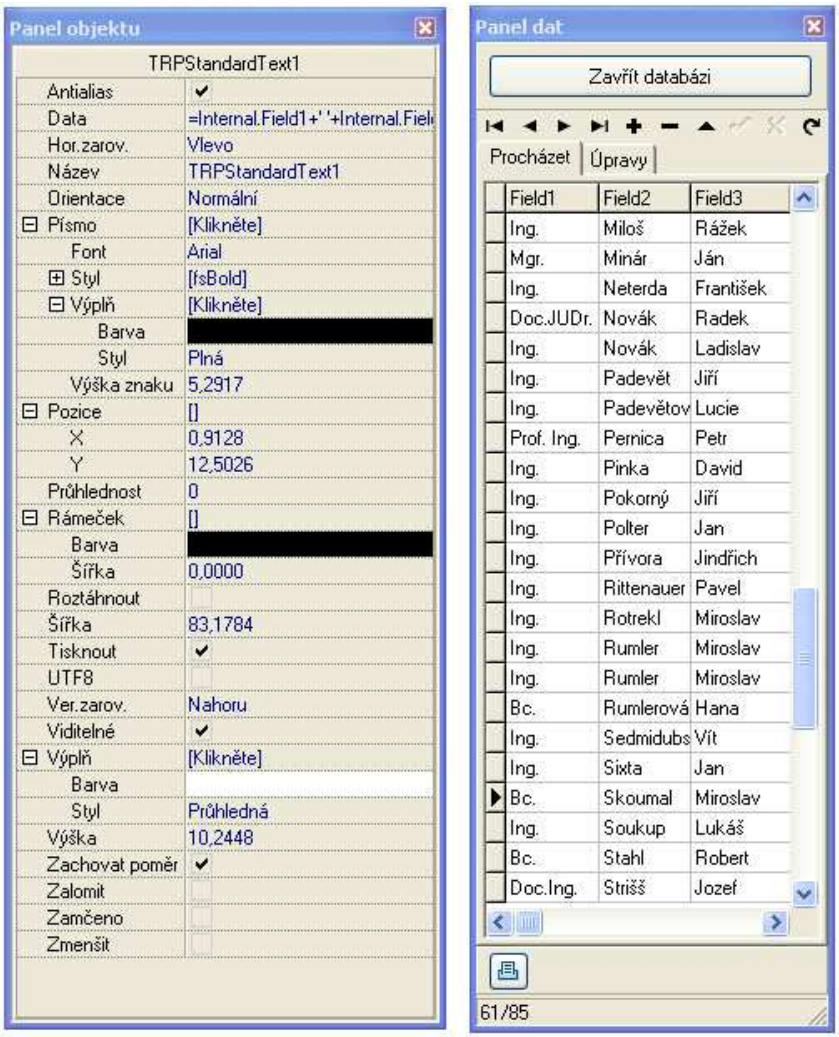
Obr. 23. Hlavní návrhové okno programu CardPress

Grafický design karty jsem propojil s vytvořenou databází a skrze okno „Návrhář dat“ se do jednotlivých textových polí automaticky vložily konkrétní údaje.

Obr. 24. Dialogové okno „Návrhář dat“

Jak je vidět z tohoto dialogového okna, textové pole čte informace z databáze celkem ze čtyř sloupců (Field 1 až 4). První sloupec obsahuje titul před jménem, druhý sloupec příjmení, třetí sloupec křestní jméno a poslední čtvrtý sloupec titul uváděný za jménem. Za upozornění stojí, že pomocí „Návrháře dat“ lze snadno měnit pořadí textových buněk, které jsou vkládány do textového pole na kartě. Konkrétně v tomto případě jsem prohodil sloupce 2 a 3, protože v databázi mám uvedeno nejdříve příjmení až pak jméno a na kartě požaduji obrácené pořadí.

Stejně jako jiné podobné programy pro návrh designu nabízí i CardPress nástroje pro formátování grafických a textových prvků. Je možné vybírat z podobných textových atributů, jaké nabízí např. MS Word. V databázovém okně je možné upravovat atributy a přidávat záznamy, popř. načíst již existující databázi podporovaného typu. Práce s programem je snadná a pro běžného uživatele intuitivně ovladatelná.



Obr. 25. Dialogová okna pro formátování textu a úpravy databáze.

Na následujícím obrázku je vidět výsledek mého návrhu. Karta byla vytištěna během cca 40ti sekund. Vzhledem k tomu, že v návrhu bylo plnobarevné logo, je to čas velmi dobrý. Kompletní databáze 85 osob byla vytištěna za méně než 1 hodinu.

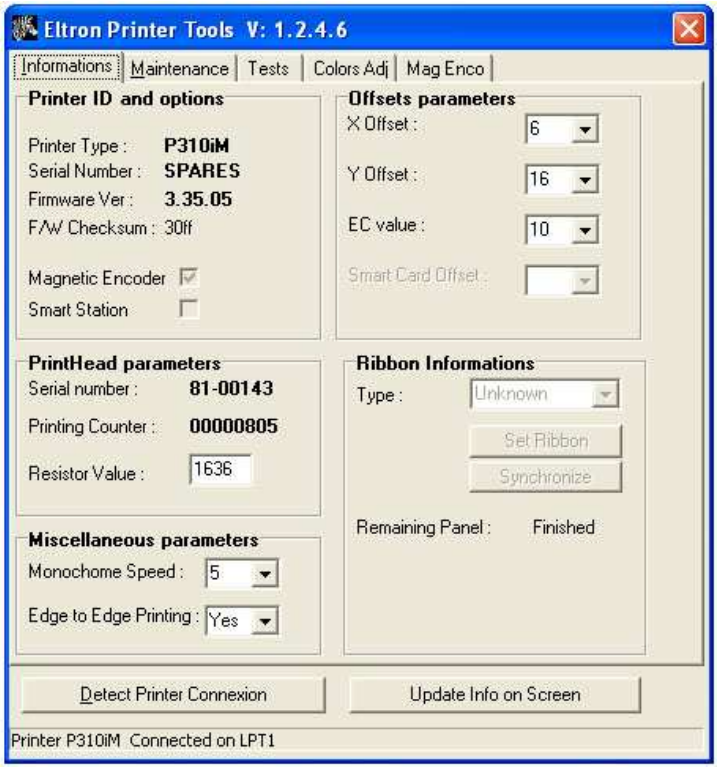
Obr. 26. Karta potištěná s využitím sw CardPress

6.2 Kódování a čtení magnetických karet

Pro testování zápisu a čtení magnetických karet jsem se rozhodl použít opět jiný typ tiskárny a to Eltron P310iM. Společnost Eltron spadá pod celosvětově největšího výrobce a distributora tiskáren plastových karet a čárových kódů Zebra. Aby tiskárna byla schopna kódovat, popř. číst data na magnetickém proužku, musí obsahovat speciální magnetickou hlavu. Tyto hlavy se dodávají v několika variantách, takže jsou schopny zapisovat a číst všechny nebo jen jednu stopu magnetického záznamu. Písmeno „M“ v názvu tiskárny znamená, že je schopna kódovat a číst karty s magnetickým proužkem.

Obr. 27. Tiskárna Eltron P310iM [21]

Součástí balení tiskárny je CD s ovladači a softwarem pro diagnostiku a kódování karet. Program Eltron Printer Tools nám ukazuje po načtení informací, jaké zařízení máme připojeno k PC. V první záložce je možné vidět aktuální firmware a celkový počet potištěných karet (tato informace je uložena v paměti mainboardu). Stejně jako u jiných zařízení je možné nastavit rychlost tisku. Někteří zákazníci vyžadují rychlejší zhotovení karty, samozřejmě na úkor kvality. Také lze nastavit offsetové parametry, tedy pozice potisku. Tato tiskárna na rozdíl od výše zmíněné EdiSecure neumí potisknout celý povrch karty a zanechává nepatrné okraje.

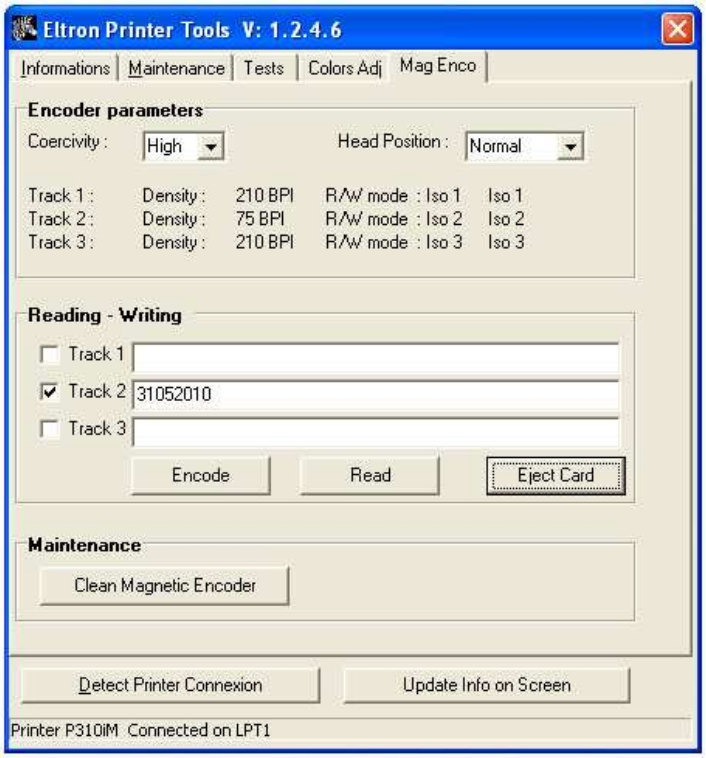


Obr. 28. Eltron Pointer Tools

V záložce Tests jsou veškeré testovací funkce potřebné ke kontrole funkčnosti důležitých částí tiskárny, jako je pohyb tiskové hlavy nahoru a dolů, posun nosných válečků, pohyb krokovacího motoru, kontrola všech senzorů a také teplota.

V posledním okně je nastavení kodéru magnetických karet. Uživatel si může zvolit ze dvou základních typů LowCo a HighCo, a také stopu magnetického proužku, do kterého chce zapisovat údaje. Na následujícím obrázku je patrné, že jsem použil karty s vysokou koercivitou. Zvolil jsem druhou stopu, do které je možno zapisovat pouze číselné údaje, a pomocí kodéru zapsal na kartu aktuální datum.

Zápis i čtení v této tiskárně trvá jen několik sekund. Pokud má uživatel k dispozici nestandardní kartu, která má magnetický proužek umístěn na jiném místě, než-li je běžné, tato aplikace mu umožňuje změnit polohu hlavy. Informuje nás také o tom, že hustota záznamu dat 1. a 3. stopy je 210 bitů na palec a 2. stopy jen 75 bitů na palec.

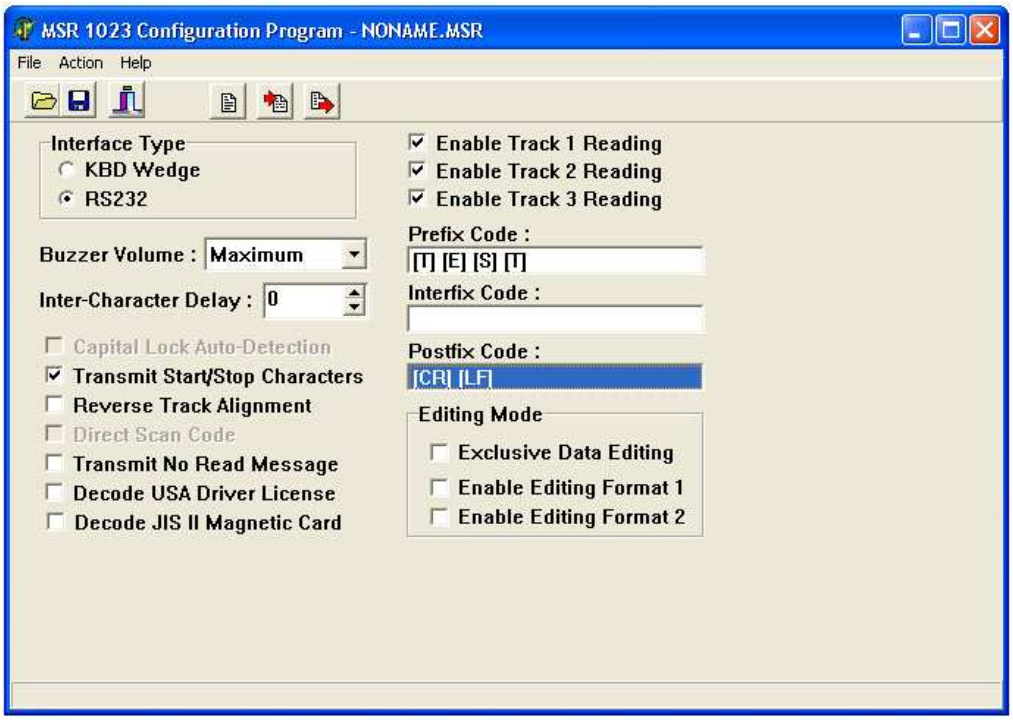


Obr. 29. Čtení a zápis dat na magnetickou kartu

Samozřejmě tiskárny nejsou jediným zařízením schopným číst magnetické karty. Již dosti běžným vybavením obchodů či klubů se staly přenosné stolní čtečky. Jedním z důvodů je také relativně nízká cena. Pro tento test jsem zvolil zařízení Cipherlab MSR 1023 jež se dá pořídit za cenu lehce převyšující 2000,-Kč. Firma Cipherlab se zabývá mimo jiné také výrobou snímačů čárových kódů. MSR zkratka zde tedy znamená Magnetic Stripe Reader.

Obr. 30. Cipherlab MSR 1023 [22]

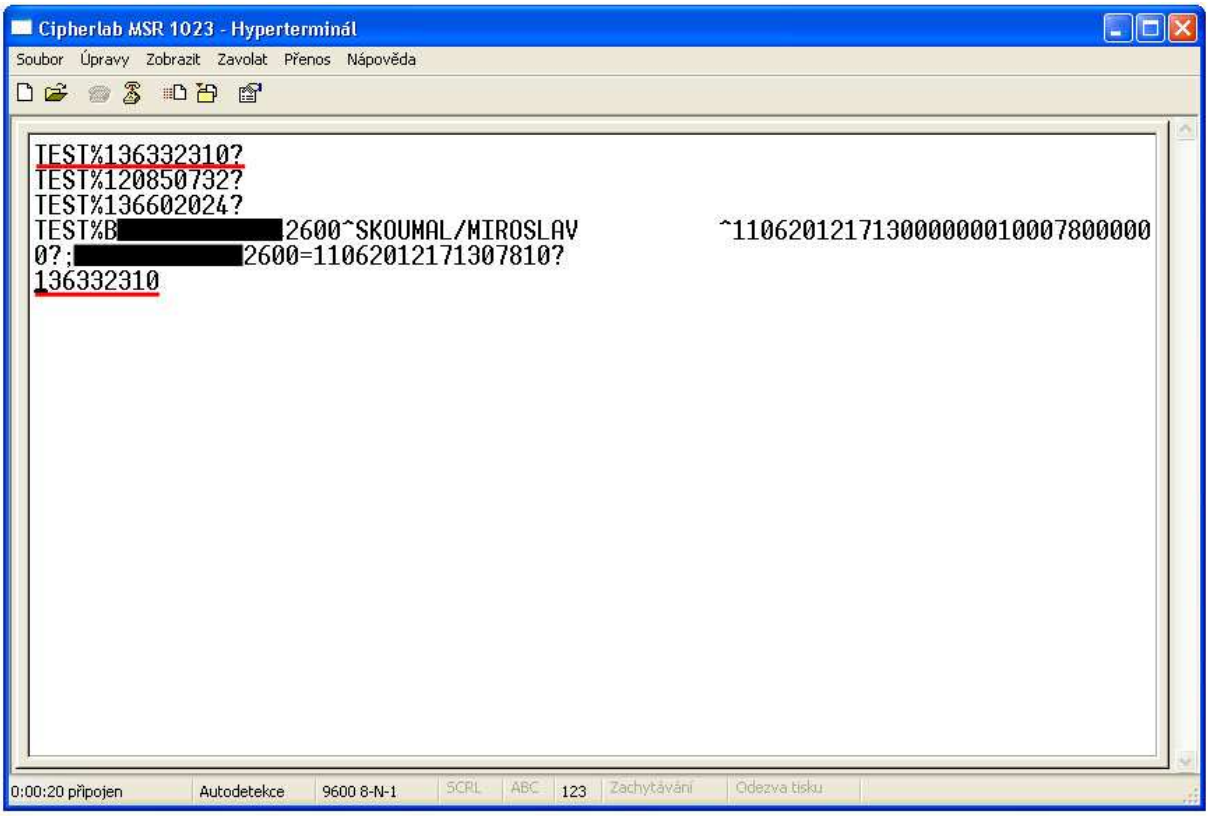
K této čtečce jsou standardně dodávány komunikační kabely PS2 a RS232. Na spodní straně zařízení nalezneme 9 nastavovacích jumperů, s jejichž pomocí se nastaví jedno ze dvou komunikačních rozhraní. V případě PS2 se volí typ klávesnice a v případě sériové komunikace rychlost přenosu, parita a bitový tok. Abych mohl použít aplikaci určenou ke konfiguraci této čtečky, bylo nutné použít sériovou komunikaci. Jumpery byly tedy nastaveny na následující hodnoty: 111110001. Toto nastavení odpovídá standardnímu nastavení komunikace RS232 portu, tedy 9600 b/s, 8 Data bits, žádná parita, 1 stop bit a bez řízení toku. Součástí balení je také tzv. konfigurační karta, která uvede čtečku do nastavovacího módu. Program určený k nastavení základních funkcí je pak již schopný se spojit se zařízením Cipherlab.



Obr. 31. Konfigurační program ke čtečce magnetických karet Cipherlab 1023

Z obrázku výše je zřejmé, že lze nastavit jen několik základních funkcí. Prvně se tedy musí zvolit typ rozhraní, poté je možno stáhnout z čtečky uloženou konfiguraci. Je možné zvolit, které stopy magnetického proužku se mají číst, zda se mají přenášet a zobrazovat uvozovací a ukončovací znaky. Pro účely testování jsem nastavil čtyř-písmenný prefix „TEST“ a postfix v podobě enteru, který je v tomto případě složen ze dvou ascii znaků CarriageReturn (návrat kursoru na začátek řádku) a LineFeed (posun na další řádek). Tento postfix je vhodný také z toho důvodu, že snímaná data budu zachytávat v aplikaci HyperTerminál, která neumí automaticky odřádkovat.

Po nahrání upraveného nastavení zpět do čtečky se tato vrátí automaticky zpět z konfiguračního módu. Poté je možno se programem HyperTerminál připojit na sériový port a zachytávat na něm data z čtečky.



Obr. 32. Data zachycená na sériovém portu z čtečky Cipherlab 1023

Na prvním a posledním řádku jsou zvýrazněny data přečtené ze stejné magnetické karty, s tím rozdílem, že v prvním případě byly zobrazeny uvozovací a ukončovací znaky a nastavený prefix. Tyto znaky (v angličtině nazývány Start/Stop Characters) jsou odlišné pro první a druhou, resp. třetí stopu. Jak je tomu přesně, můžeme vidět v následující tabulce:

	Start	**Stop**
ISO Track 1	**%**	**?**
ISO Track 2	**;**	**?**
ISO Track 3	**;**	**?**

Tab. 3. Start/Stop znaky

Z tabulky je tedy zřejmé že jsem pomocí čtečky Cipherlab přečetl první stopu magnetických karet. Zkusil jsem také přečíst platební kartu a zjistil, že jsou na ni uložené

informace první a druhé stopě. Z těchto informací lze vyčíst číslo karty, její typ (Visa / MasterCard) jméno banky (2600 je kód České spořitelny), jméno držitele, či její platnost.

6.3 Čtení RFID karet

Pro testování bezkontaktních karet jsem zvolil běžně dostupnou čtečku Promag 340 RFID. Toto zařízení disponuje duálním rozhraním pro 125 kHz a 13,56 MHz, je tedy schopné číst nejen běžné čipové karty typu Mifare, ale také identifikační RFID tagy, jež právě pracují na frekvenci 125 kHz. Pro testy jsem vybral několik karet typu Mifare 1K, průkaz studenta UTB, In-Kartu pro zákazníky Českých drah a tag ve tvaru přívěsku, který se používá v docházkovém systému.

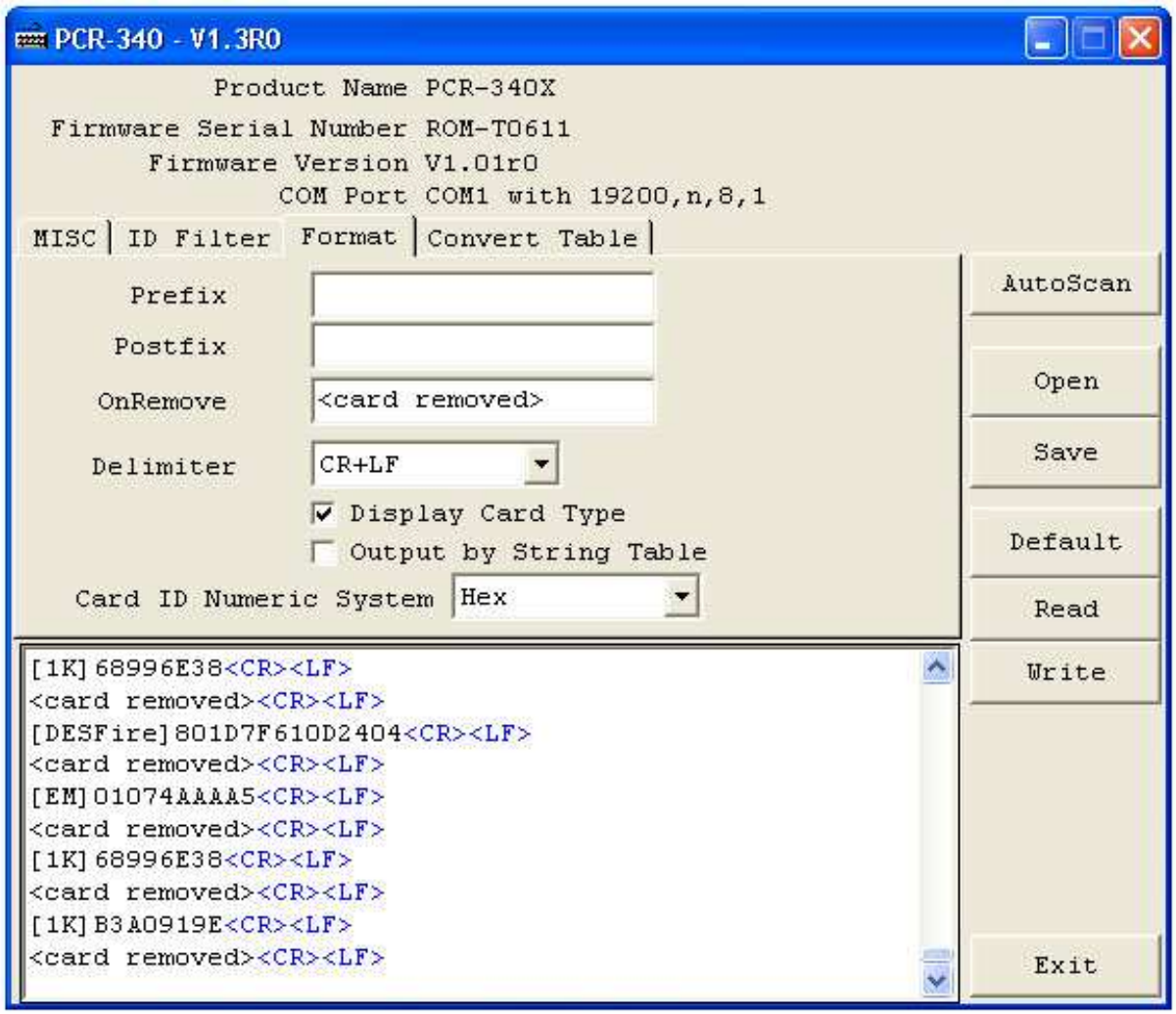
Obr. 33. Bezkontaktní RFID čtečka Promag 340.

Toto RFID čtečku je možné připojit k počítači několika způsoby. Lze využít sériový port, USB, nebo PS2. Připojil jsem tedy zařízení k sériovému portu počítače, který byl nastaven standardně, pouze s vyšší přenosovou rychlostí 19200 b/s. V základním balení je dodáván software, který slouží k nastavení základních vlastností, podobně jako tomu bylo u Cipherlabu. Toto zařízení se dá na českém trhu koupit za cenu okolo 4000,- Kč.

I když Promag 340 umí pouze přečíst sériové číslo karty, dá se vhodně upraveným způsobem použít jako elektronický zámek. Přiložená karta pak funguje jako klíč, díky kterému se uživatel snadno přihlásí do systému a je mu umožněna práce např. v pokladním systému nebo je mu povolen vstup do místnosti.

Cílem mého pokusu bylo zjistit přesný typ všech karet, respektive tagu. Odhadoval jsem že In-Karta bude disponovat nejlepšími parametry, naopak studentský průkaz, jelikož se v jeho případě nejedná o žádnou komerční zabezpečenou aplikace, bude 125 kHz karta.

Na následujícím obrázku je vidět, že v konfiguračním programu lze podobně jako v předchozím případě nastavit prefix a postfix, oddělovač dat a také nám umožňuje zobrazovat upozornění o tom, že karta byla odstraněna z dosahu snímače.



Obr. 34. Prostředí ovládacího programu k zařízení Promag 340.

Nejdříve jsem testoval běžnou kartu Mifare 1k, pak následovala In-Karta Českých drah, studentský průkaz UTB a opět Mifare ovšem tato již neobsahovala čip NXP Semiconductors od firmy Philips, ale levnější variantu čínské výroby čip FUDAN

Microelectronics. Jak je vidět uživatelský software zobrazuje SN a typ karty. Výsledky byly následující.

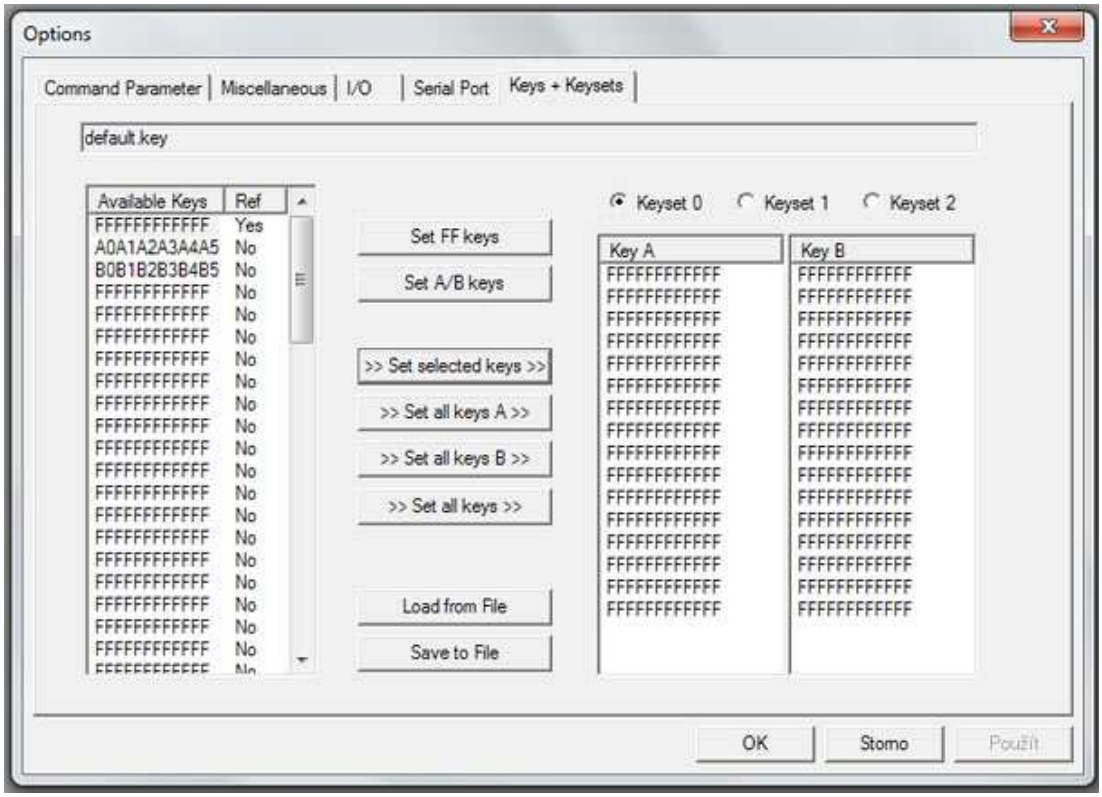
- Běžná Mifare karta – typ 1k, cenově dostupná s nízkou úrovní zabezpečení
- In-Karta – typ Mifare Desfire 4k, větší paměť, rychlejší přenos, vyšší stupeň ochrany
- Průkaz studenta UTB – 125 kHz RFID karta
- Tag (klíčenka) – 125 kHz RFID čip

6.4 Kódování a čtení bezkontaktních karet

K tomuto pokusu jsem si zapůjčil zařízení firmy Pascom s.r.o., které umí číst a zapisovat informace do bezkontaktních čipových karet, jejichž nosná vlna nesoucí informace funguje na 13,56 MHz. V reálném provozu tato čtečka slouží k zaznamenávání informací o provedené práci a změnách na vysokozdvižných vozících Still. Pracovník na začátku své směny zasune kartu do zapisovacího zařízení, jež je připevněno přímo k vozíku a po skončení pracovní doby kartu vyjme a předá pověřenému pracovníkovi jež pomocí tohoto zařízení stáhne veškeré informace o činnosti uživatele. Mimo jiné, také karta v tomto případě slouží jako bezpečnostní klíč, bez něhož není možné vysokozdvižný vozík nastartovat.

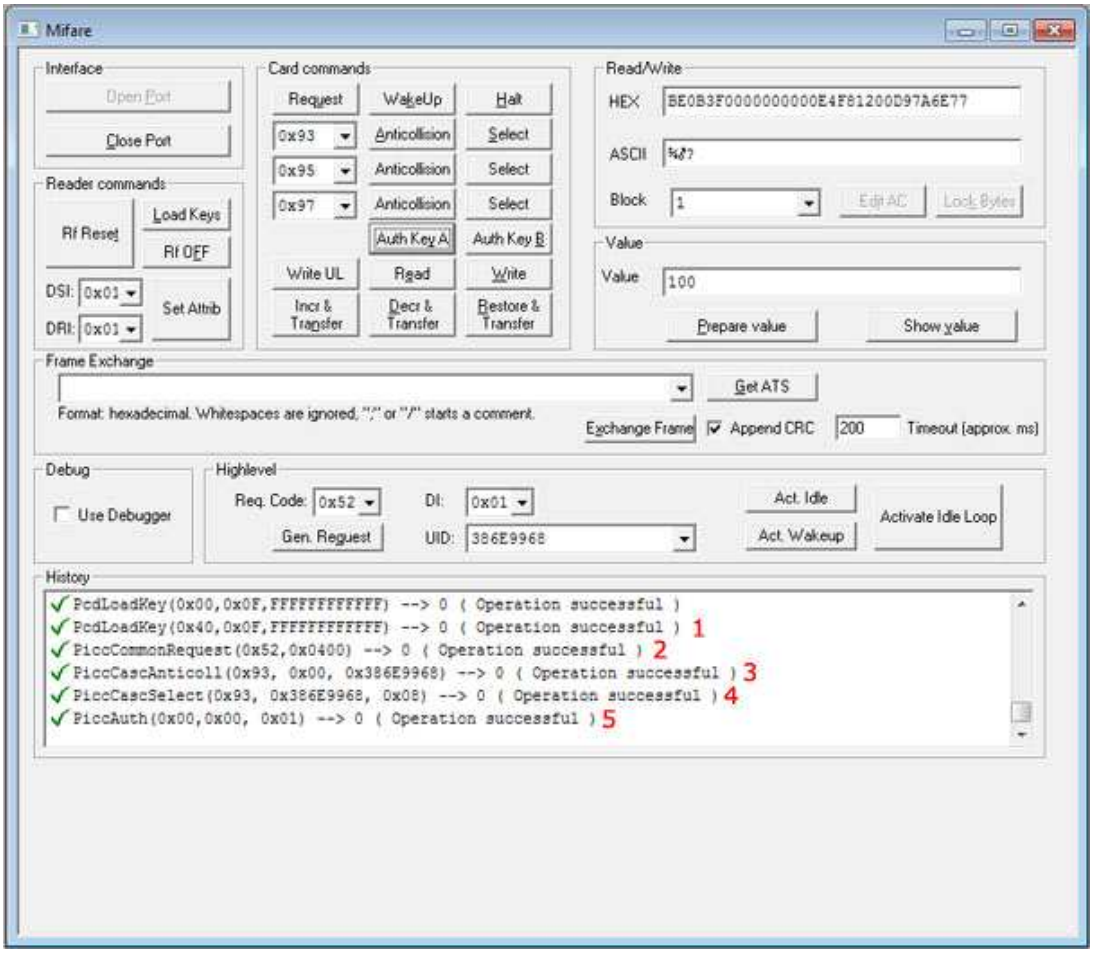
Obr. 35. Zařízení pro zápis a čtení Mifare karet.

Tato čtečka disponuje běžným konektorem USB, takže je možné ji propojit pomocí klasického USB (A/B) kabelu. Jelikož koncový zákazník využívající toto zařízení používá webovou aplikaci jež podléhá licenční smlouvě, rozhodl jsem se otestovat jej za pomocí volně dostupného programu MifareWND. Tento program, jak bude dále popsáno, umožňuje provádět s kartami veškeré operace. Čtení a zápis nemusí probíhat automaticky, takže je pouze na uživateli, co se rozhodne s kartou provádět. Mým cílem bylo vyzkoušet si krok za krokem procedury jež v běžných aplikacích, kde se bezkontaktní karty používají, provádějí automatizovaně. Zajímalo mne jak je možné, že v praxi ve většině případů není nutná žádná spoluúčast držitele karty k tomu, aby se autentizoval a veškerá komunikace mezi kartou a čtecím zařízením probíhá bez dalšího vnějšího zásahu, a to včetně ověření pravosti karty až po přenos dat a jejich zapsání do paměti. Měl jsem opět k dispozici několik běžně dostupných karet Mifare Classic 1k a Mifare Classic 4k. Rozdíl mezi těmito dvěma typy je ve velikosti a organizaci paměti. Tím pádem se také liší maximální počet aplikací, k nimž mohou karty sloužit. Jak jsem se později na vlastní oči přesvědčil, bezkontaktní karta Mifare disponuje 1kB paměti, která je v EEPROM organizována v 16 sektorech a z nichž každý se dále dělí na 4 bloky o velikosti 16 bytů. U typu Mifare 4k je to poněkud odlišné. Jak je již z názvu patrné disponuje 4 kB paměti, která je organizována ve 40 sektorech. Prvních 32 sektorů se opět dělí na 4 bloky po 16 bytech a zbylých 8 sektorů na 16 bloků po 16 bytech. Mimo standardních nástrojů a nastavení, kteréžto podobné čtečky mývají je nutné před započetím samotné komunikace nastavit autentizační klíče.



Obr. 36. Nastavení autentizačních klíčů.

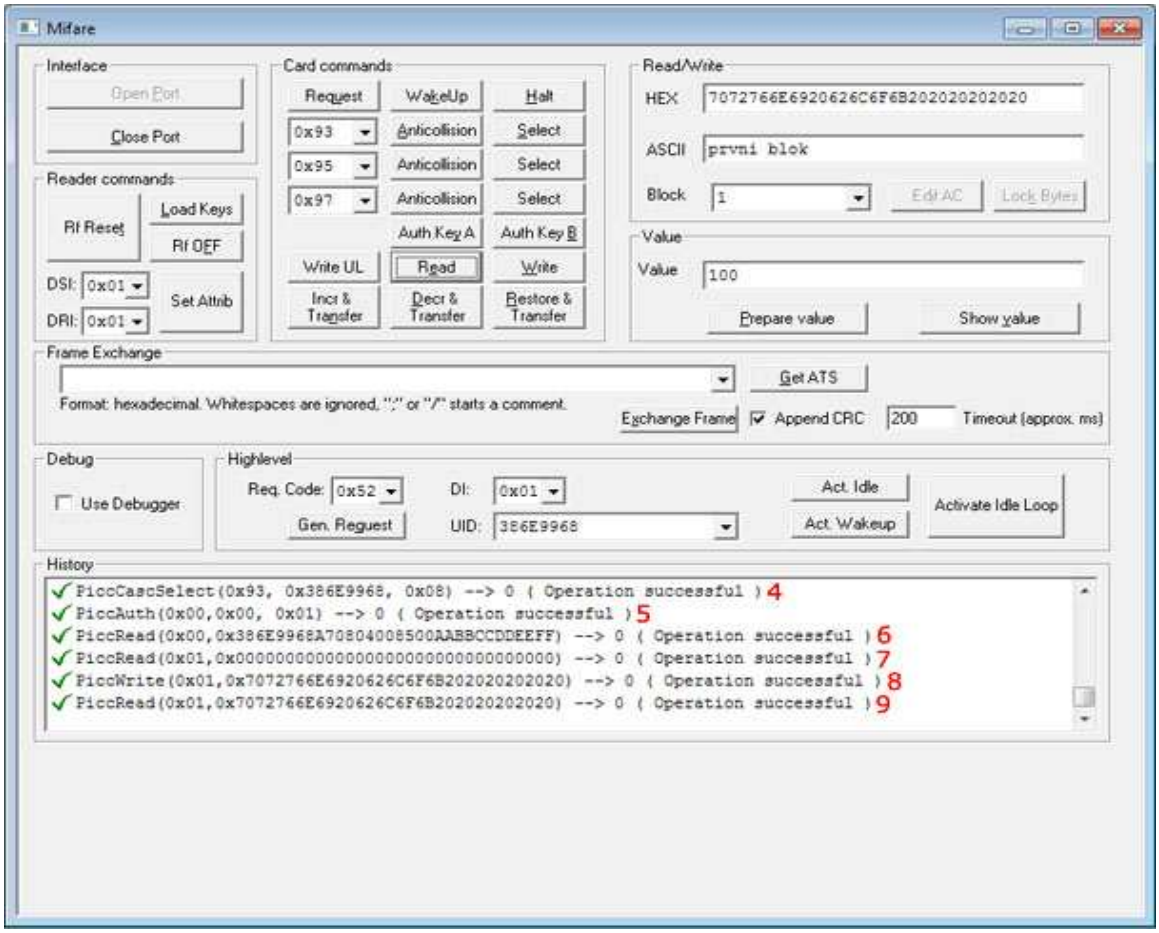
Pomocí autentizačního klíče je uživateli povoleno číst a zapisovat do určitého sektoru. To znamená že, pro každý sektor lze nastavit unikátní klíč. Jak vidíme na obrázku tak se nastavují dva klíče A a B. Ty lze nastavit tak, že první slouží k autorizaci pro čtení a druhý pro zápis do paměti. Z toho vyplívá, že nejvíce rozšířená karta Mifare 1k může mít až 32 unikátních klíčů. Takováto ochrana je dobrá především k tomu, aby se logicky oddělili činnosti čtení a zápisu. Můžeme takto nastavit kartu a do programu jež se stará o komunikaci uložíme pouze klíč A. Tím zaručíme, že uživatel bude moci z jemu přidělených sektorů pouze číst. Tato karta tedy může nést data až pro 15 různých aplikací, které se navzájem neovlivňují, samozřejmě při dodržení stanovených bezpečnostních pravidel. Jedním z nich je změna defaultních klíčů. Z praxe bych to přirovnal např. ke změně defaultního hesla na routeru či access pointu. Ve chvíli, kdy zakoupíte od výrobce či distributora zcela novou kartu, jsou všechny klíče přednastaveny na „FFFFFFFFFFFF“. Ověřil jsem si tedy, že všechny klíče jsou nastaveny na tuto hodnotu a pokračoval dál v hlavním okně programu MifareWND.



Obr. 37. Aplikace Mifare WND

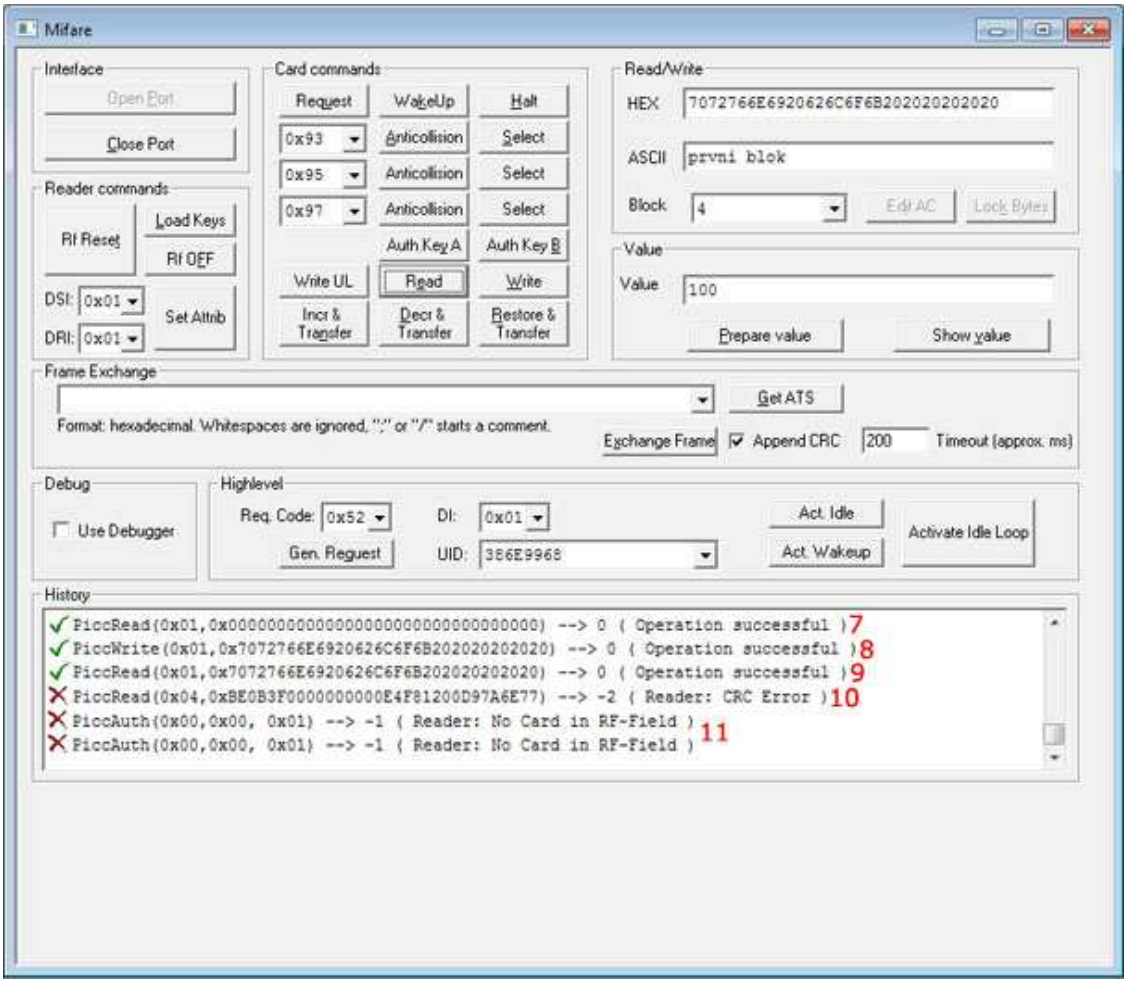
Vytvořené klíče jsem uložil a pomocí tlačítka **Load Keys** nahrál do paměti programu (1). Abych se dostal k datům uloženým na kartě v určitém sektoru musím se tedy nejprve autentifikovat. Samozřejmě nemohu přes čtecí zařízení vyslat do okolí nějaký klíč, aniž bych měl jistotu že se v blízkosti čtečky nachází nějaká karta. K tomuto účelu slouží funkce **Request** (2). Ta vyšle do okolí signál a čeká na odezvu, která by znamenala že se v okolí nachází kompatibilní karta. Ta se nabije pomocí EMG pole generovaným čtečkou a odešle odpověď jež říká „ano jsem tady a připravena ke komunikaci“. Ovšem co se může stát, že se v okolí čtecího zařízení nachází několik kompatibilních karet a všechny odešlou své odpovědi. V praxi tento případ může nastat např. když uživatel má schovanou kartu v peněžence spolu s jinými a přiloží ji k elektronickému zámku. V takovém případě nemůže zařízení komunikovat se všemi najednou, ale musí určit pořadí v jakém jednotlivé karty zkontaktuje. K tomuto slouží funkce **Anticollision** (3). Tím jsem vybral jednu z karet a jako návratová hodnota se zobrazilo její sériové číslo 386E9968. Pokud jsem si jist že je to právě ta karta se kterou chci navázat spojení odešlu příkaz **Select** (4), kterým určím, že

pouze s ní chci komunikovat. Nyní si již mohu zvolit konkrétní blok paměti a odeslat auentizační klíč (5). Jelikož jsem nastavil všechny na stejnou hodnotu stačí odeslat klíč A.



Obr. 38. Čtení a zápis do bloků v paměti Mifare 1k.

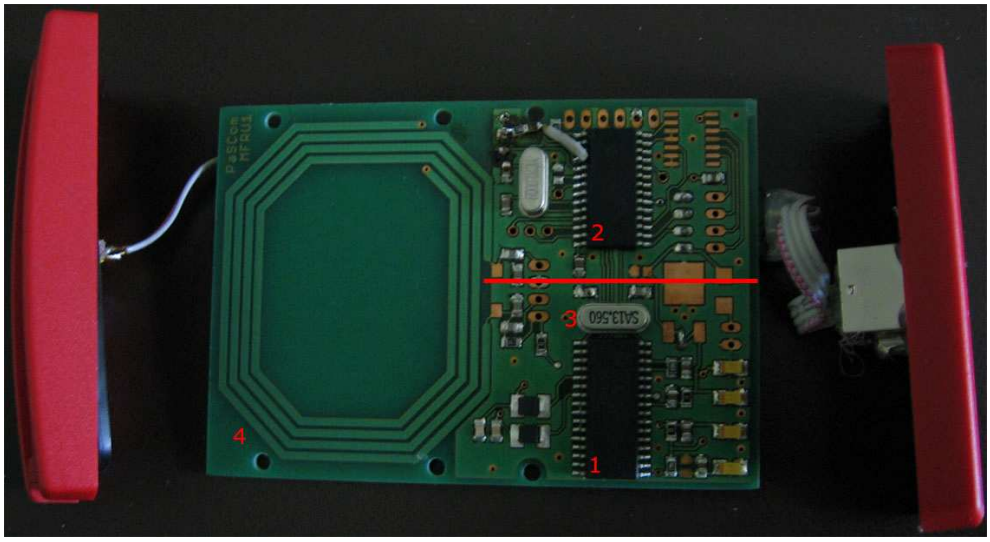
Jakmile jsem se již autentizoval, karta mne nechá abych přečetl pomocí příkazu **Read** obsah paměti nultého bloku(6). V tomto bloku se nachází sériové číslo karty a další údaje, které se sice zobrazí, ale jejich hodnota je ve skutečnosti jiná. Nultý blok je určen pouze pro čtení a není možné do něj zapisovat. Program oznámí že uložení dat proběhlo v pořádku, nicméně údaje se nezmění. Proto zvolím pro můj test blok č. 1. Jak je vidět na předchozím obrázku tak zbylá paměť je prázdná, tzn. obsahuje nuly (7). Rozhodl jsem se tuto hodnotu změnit a zapsal v ascii test „první blok“ a uložil do paměti příkazem **Write**. Program Mifare WND tak jak je nyní nastavený doplnil zbylé místo v paměťovém bloku mezerami (9).



Obr. 39. Nezdařený pokus o čtení z bloku paměti.

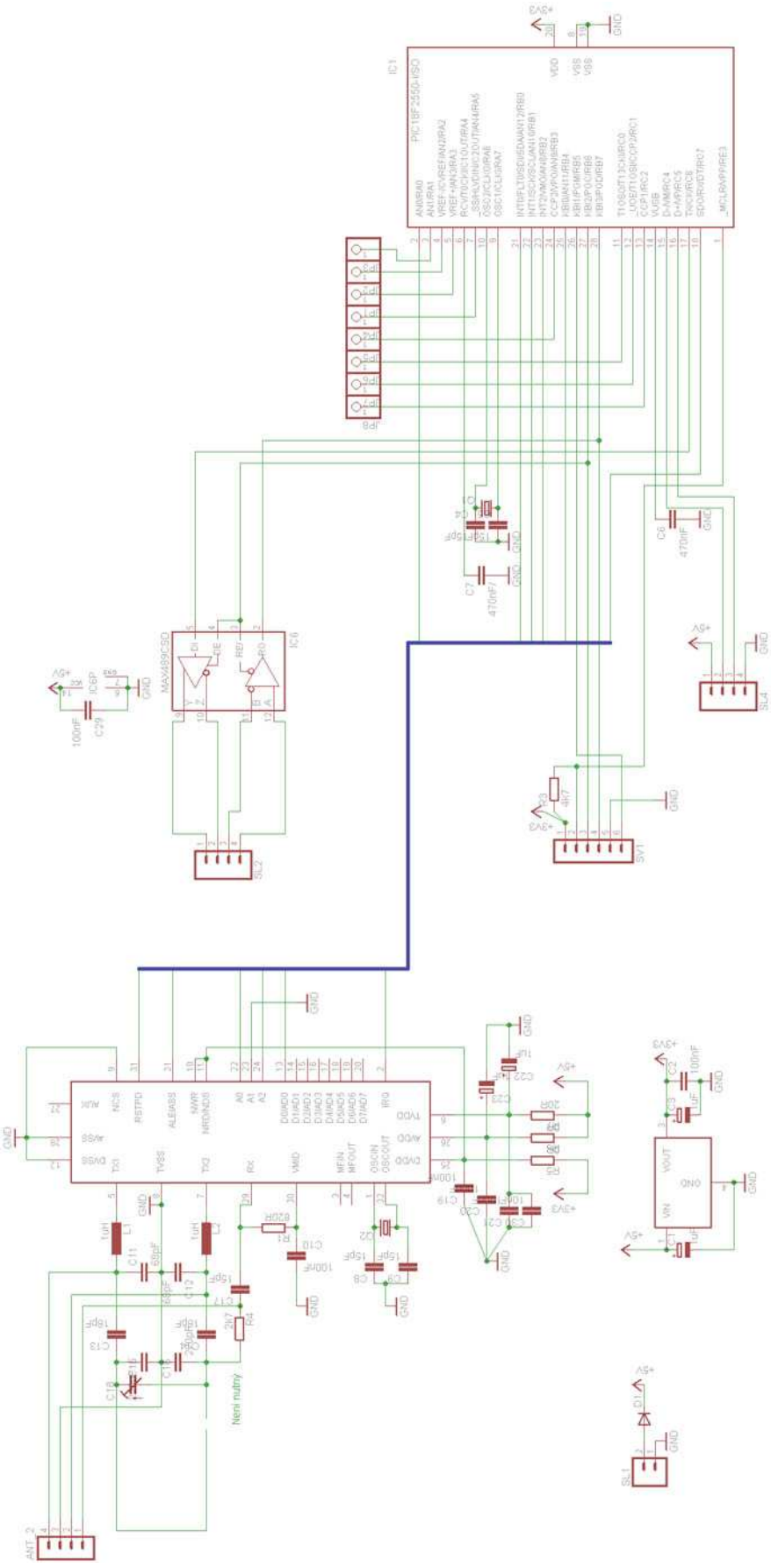
Co se ovšem stane pokud se pokusím číst jiné bloky paměti? Z toho co jsem již popisoval výše je to zřejmé. Jelikož jsem se autentizoval klíčem pro první blok, karta přijala mou autorizace pouze i pro ostatní bloky ve stejném sektoru. Když sem se tedy pokusil číst data z bloku č. 4 který již spadá do druhého sektoru, akce se nezdařila (10). Pokud bych chtěl pokračovat dále v komunikaci s kartou, musel bych se opětovně autentifikovat klíčem pro příslušný sektor. Při odstranění karty z dosahu radio-frekvenčního pole čtečky a pokusu o další komunikaci dojde k chybě jež je oznámena (11) a pro započetí nové komunikace se musí celý proces autentifikace opakovat. Jak jsem se již zmínil, pokud jsou v dosahu zařízení dvě a více karet, musí uživatel zvolit příslušnou kartu s kterou chce komunikovat. Pomocí příkazu **Halt** je možné danou kartu „uspat“ a později se k ní vrátit a oživit ji příkazem **WakeUp**. Každý z bloků může obsahovat také peněžní hodnotu (Value) která je reprezentována 4 Bytovou proměnnou typu integer.

Nyní když jsem viděl a mohl si také nasimulovat jednotlivé kroky které v reálných aplikacích probíhají automaticky, resp. jsou řízeny provazově, mne zajímalo co je vlastně potřebné k tomu, aby člověk mohl sestrojit podobné zařízení pro komunikaci s bezkontaktními čipovými kartami.



Obr. 40. Odkryté zařízení pro zápis a čtení Mifare karet.

Celé zařízení se dá rozepět na tři hlavní části. Na obrázku výše je číslem (1) označen mikroprocesor Philips CL RC632 jež obstarává jednu z nejdůležitějších činností a to je komunikace s čipem karty. Nad ním se nachází krystal (3) který určuje frekvenci nosné vlny, v tomto případě tedy 13,56 MHz. První hlavní částí tohoto zapojení je tedy modulátor signálu, na obrázku pod čarou. Na druhé polovině plošného spoje je umístěn osmibitový mikrořadič PIC 18F2550 (2) od firmy Microchip, který se stará o komunikaci mezi počítačem a mikroprocesorem Philips. Ten mimo jiné umí komunikovat se sběrnicí USB 2.0 při plné rychlosti, tj. 12 Mbit/s při pracovní frekvenci 48 MHz. Poslední důležitou částí je anténa (4).



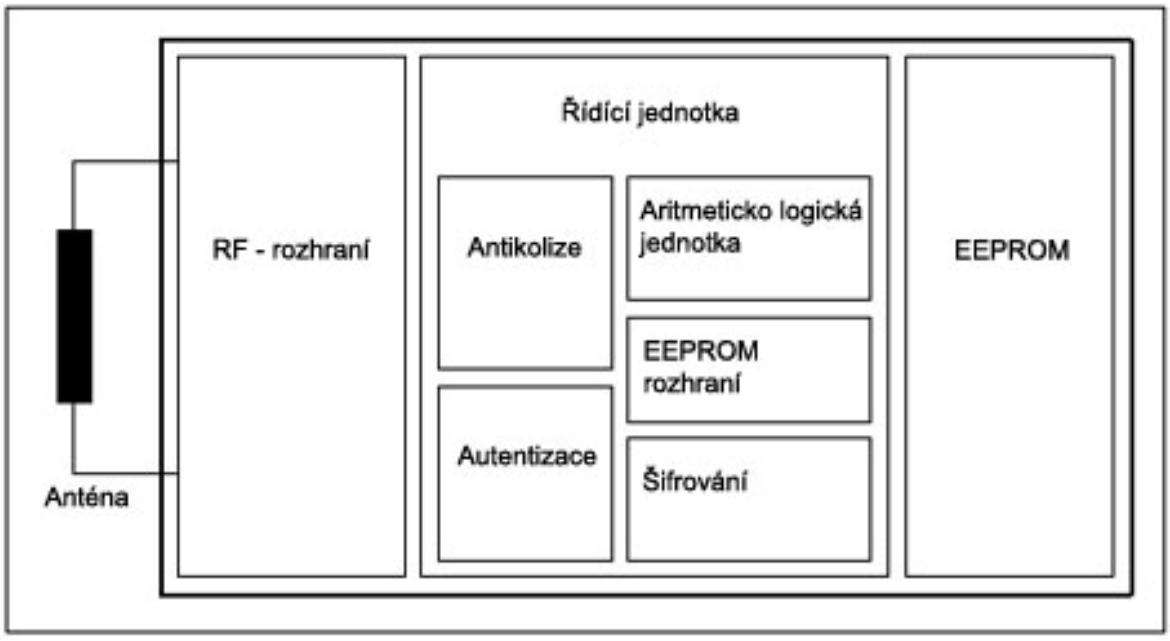
Obr. 41. Schéma elektronického zapojení Mifare kodéru

6.5 Rozbor funkčnosti Mifare karet

Jelikož jsou Karty Mifare v současné době nejrozšířenějším typem bezkontaktních čipových karet a věnoval jsem jim velký prostor i v praktické části této práce, bylo by dobré abych ji ještě rozšířil o více konkrétních informací.

Mifare 1k, které jsem použil pro své testování, obsahují čip Mifare MF1 IC S50 vyrobený společností Philips tak, aby fungoval v souladu s normou ISO/IEC 14443A. Anténa spojená s tímto čipem, funguje podobným způsobem jako běžné cívky. Karta nemusí obsahovat žádný zdroj energie. Ta je získána pomocí antény RF signálu vysílaného kompatibilním zařízením. Maximální rychlost přenosu informací je u tohoto typu 106 kbit/s při vzdálenosti do 10cm od zdroje signálu. Tato vzdálenost závisí na zvolené geometrii antény.

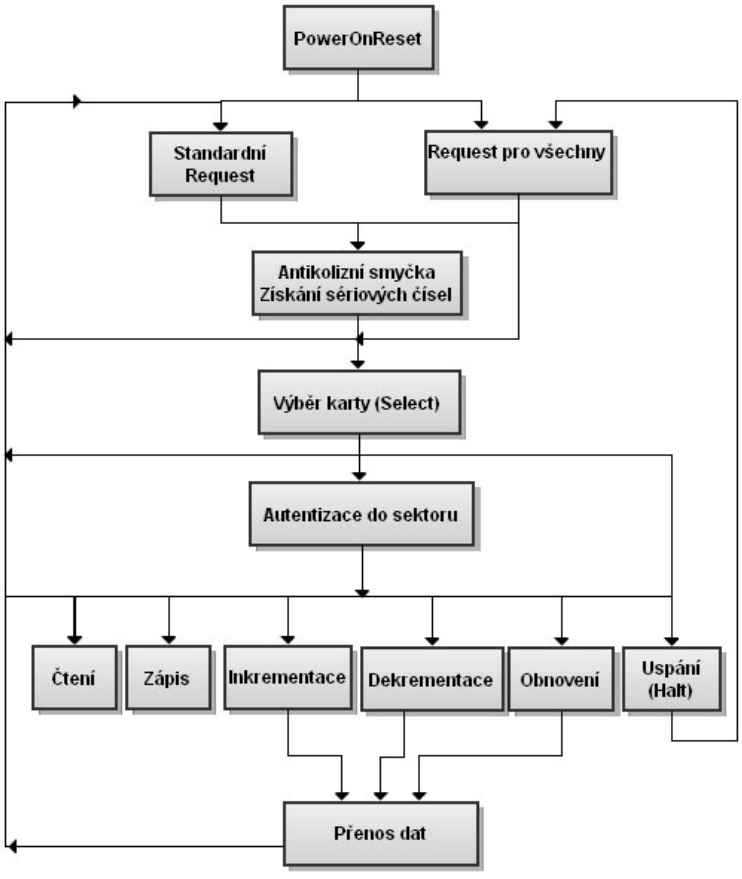
Pracovní frekvence je 13,56 MHz, přičemž běžná výměna informací s kompatibilním zařízením netrvá déle než 100 ms. Společnost Philips zaručuje pro tyto své výrobky záruku 10 let na uchování dat a až 100 000 pracovních cyklů. Z celkové paměti 1 kByte uložené v EEPROM je uživatelům k dispozici 768 Bytů. Jak jsem již popisoval výše, pro čtení a zápis do každého sektoru je možné zvolit 48 bitové klíče A/B. Z toho vyplívá že 2^{48} je dostatečně složitým klíčem, nemůže tedy v reálném čase dojít k jeho prolomení útokem hrubou silou.



Obr. 42. Schéma logického rozmístění součástí karty

Z obrázku je zřejmé, že čip MF1 IC S50 se skládá z 1kBytové paměti, radio-frekvenčního rozhraní a řídící jednotky, která se ovládá jednotlivé funkce čipu, jako je kryptace dat atp.

- RF-rozhraní se skládá z modulátoru / demodulátoru signálu, usměrňovače, generátoru časových cyklů, regulátoru napětí a resetovaní a power-on-reset jednotky která začíná každou komunikaci
- Antikolize zajišťuje schopnost výběru a operací s více kartami
- Autentizace – pro čtení nebo zápis do každého bloku je možné zvolit unikátní klíč, který slouží k autentizaci uživatele do paměti požadované aplikace
- ALU – řídí inkrementaci a dekrementaci dat uložených v redundantním formátu
- EEPROM rozhraní – slouží k přístupu do paměti čipu
- Šifrování – používá se odzkoušená 56 bitová proudová šifra Crypto1
- EEPROM – 1 kByte paměti je rozdělen do 16 sektorů, a každý z nich se dělí na 4 bloky o velikosti 16 Bytů,



Obr. 43. Přenosová sekvence

Na obrázku č. 38 jsou znázorněny všechny procesy nutné k uskutečnění přenosu dat tak, jak jsem je v posledním pokusu zkoušel manuálně a trvají ve skutečnosti jen velmi krátkou dobu. Identifikace karty v okolí a její vybrání včetně antikolize trvá 4 ms, pak se během 2 ms provede autentizační procedura a nakonec zápis dat do bloku 6 ms, popř. čtení za 2,5 ms.

Organizace paměti.

Jak jsem již několikrát zmínil, paměť Mifare karet se dělí na sektory a ty pak dále na bloky. Pro lepší pochopení organizace dat v paměti je dobré to zobrazit graficky.

		Čísla Bytů uvnitř bloku															
Sektor	Blok	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Obsah
15	3	Klíč A						Přístup. bity				Klíč B						Trailer sektor 15
	2																	Data
	1																	Data
	0																	Data
14	3	Klíč A						Přístup. bity				Klíč B						Trailer sektor 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Klíč A						Přístup. bity				Klíč B						Trailer sektor 1
	2																	Data
	1																	Data
	0																	Data
0	3	Klíč A						Přístup. bity				Klíč B						Trailer sektor 0
	2																	Data
	1																	Data
	0																	(nultý) blok výrobce

Obr. 44. Organizace paměti EEPROM karty Mifare 1k

Nultý blok obsahuje neměnné údaje jako sériové číslo karty, kontrolní bit a další data výrobce. Do tohoto bloku jsou informace zapsány při výrobě a pak je již nelze nikdy přepsat. Každý sektor obsahuje tři 16 bytové bloky pro ukládání dat. Tyto datové bloky mohou být konfigurovány pomocí tzv. přístupových bitů. Lze je nastavit dvojím způsobem. Buď jako běžné bloky určené pro čtení / zápis dat, nebo jako 4 bytové „value“

bloky. Druhý způsob se používá především v různých elektronických aplikacích, kde lze hodnoty upravovat pouze pomocí příkazů „increment“ a „decrement“. Poslední čtvrtý blok v každém sektoru se nazývá „trailer“ a obsahuje dva přístupové klíče a podmínky programového přístupu do celého sektoru – tedy výše popsané přístupové bity. Pokud se uživatel pokusí přečíst data z trailer bloku, vrátí se mu pouze logická 0. Autentizační klíč A je povinný, nicméně klíč B je volitelný a v případě jeho nenastavení lze posledních 6 bytů traileru použít k uložení dalších dat.

Mifare 1k obsahuje 16 samostatných sektorů a dá se tedy použít až v 15 různých aplikacích (nultý sektor nelze použít). V takovýchto případech se musí řídit pravidly MAD (Mifare Aplication Direktory). V české republice je asi nejznámějším příkladem takovéhoto použití pražská Open Card. Nultý sektor takové multiaplikační karty obsahuje údaje o všech uložených datech a při přečtení těchto informací systém zjistí do kterého sektoru šáhnout pro data požadovaná danou aplikací. Z toho vyplívá, že je nutné nastavit pro nultý sektor klíč A pouze pro čtení jako veřejný na hodnotu „a0a1a2a3a4a5“. Klíč B jež pak umožňuje zápis a měl by utajený pouze v rámci společností jež provozují kartu ve svých aplikacích. Z důvodů bezpečnosti by data identifikačních a manipulačních algoritmů měla používat pouze nepřímé adresování za pomoci pointerů sektorů, které ovšem nesmí být součástí datové struktury MAD.

Na závěr praktické části uvádím přehled současných typů Mifare karet velikosti pamětí.

Mifare	**Ultralight**	**1k**	**4k**	**Plus**	**DesFire**	**Pro X**	**SmartMX**
přenosová rychlost [kbit/s]	106	106	106	848	424	424	424
velikost paměti	512 bit	1 kbyte	4 kbyte	2-4 kbyte	4 kbyte	8-16 kbyte	200 kbyte

Tab. 4. Typy Mifare karet

ZÁVĚR

Cílem této práce bylo zmapovat a detailně popsat plastové karty sloužící k identifikaci jakožto HW tokeny nebo k bezhotovostním platbám a celé řadě dalších účelů. Postupnou analýzou jednotlivých technologií souvisejících s touto tématikou jsem vyhodnotil jejich výhody a upozornil také na slabá místa. Popis tak složité technologie, jakou jsou čipové karty, není snadný úkol, bylo důležité neopomenout veškeré důležité detaily, ať už se jedná o materiál, ze kterých se plastové karty vyrábějí, nebo komunikační protokol mezi čipem a terminálem.

Identifikační karty jsou našimi užitečnými pomocníky v reálných aplikacích tam, kde se požaduje určitý stupeň zabezpečení. Domnívám se, že naprostá většina z nás nosí při sobě minimálně jednu kartu, kterou využívá k platbám za objednané zboží z internetu, nebo aby prokázal v případě potřeby svou identitu či organizaci, ke které patří. Čipové karty zažívají v posledních letech tak obrovský rozmach, který je srovnatelný snad jen s rozšířením mobilních telefonů před několika lety. Multifunkční karty jsou technologií, která ulehčuje lidem práci, šetří jim čas i peníze, ale v nepravých rukách mohou způsobit velké ztráty, a to nejen finanční. Proto je zabezpečení informací, jejichž jsou veškeré druhy karet nositeli, tak důležité. Velkou část práce jsem věnoval popisu možných rizik v souvislosti s používáním karet a samozřejmě také uvedl způsoby ochrany před těmito hrozbami. Jelikož jsou informace uložené na kartě velmi důležité, je rovněž žádoucí, aby byly dostatečně chráněné. Nepřejeme si, aby cizí lidé měli přístup do našeho hotelového pokoje, aby využíval našich předplacených služeb ve fitnes či jiných společenských klubech. A asi vrcholem bezpečnostního rizika je možné zneužití platebních karet.

V praktické části jsem se snažil otestovat technologie úzce související s naším životem. Stále více zákazníků si pořizuje tiskárny plastových karet včetně kodérů čipových karet, namísto zakázkové výroby a potisku. Napomáhají tomu klesající ceny zařízení k tomu potřebných. Nyní si již může každý člověk s dostatkem peněz a znalostí za pomocí tiskáren a terminálu resp. R/W zařízení vytvořit vlastní aplikaci, kde využije veškeré finesy technologie čipových karet. Záleží pouze na našich požadavcích, moderní identifikační a komunikační technologie se stále zdokonalují a plastové karty ať už s inteligencí nebo bez jsou toho důkazem. Před sto lety nám sloužily jako pouhé vizitky, nyní je využíváme nejen jako prostředek identifikace ale i mobilních plateb.

CONCLUSION

Tendency of this thesis was mapped and described in detail plastic cards serving to identification, as a hardware token or to credits transfers and quite a few of other purposes. With sequential analysis of individual technology reletad with this theme evaluated I benefits and drawed attention to weak points. Description so complicated technology as are smart cards is not easy imposition, don´t miss out important details was importent, whether is material, from which are plastic cards producing, or communications protocol between chip and terminal.

Identification cards are our useful helpers in real applications there, where is desired especial factor of security. I think, that absolute majority of us carry by herself minimally one card, which make use of payments of goods on order on internet, or proof of identity in case of need or belonging to organization. Chip cards digest of late years so huge boom, which is perhaps comparable with expansion of cell phones some years ago. Multifunction cards are technologies, which salving people work, spare time and money, but can make big losses and not financial only in wrongly hands. This is why is of information security, which is all kinds of cards for owner, so important. A great deal of thesis I bestowed description of possible risks in connection with using cards and of course introduced way of shelter from this threats. Since information saved on card are very important, is desirable to sufficient security too. We don´t wish, that strange people have acces to our hotel room, make use of our subscription services in fitness or in others social clubs and perhaps top of security risk is possible improper use of payment cards.

In practically part I tried to test technology, which closely have connection with our life. More and more customers buy printers plastic cards including coder chip cards, instead custom manufacturing and printing, falling prices arrangement, which is needed for it, advance that.

Now can everyone, who has enough money and knowledge, with the help of printer and terminal, resp. R/W device, create own application, where make of all benefits technology of chip cards.

It depends on our requirements only, modern idetification and communication technology are always innovating and plastic card – with or without inteligence – are proof of this. Hundred years ago served us like business cards only, now we make use of it like means of identification, but also mobile payments.

SEZNAM POUŽITÉ LITERATURY

[1] Wikipedia [online], Dostupné z WWW: <http://en.wikipedia.org/wiki/Smart_card>

[2] What is a smart card [online], Dostupné z WWW:
<http://computer.howstuffworks.com/question332.htm>

[3] Handschuh, H. Dr.: Contactless technology security issues, security Technologies department Gemplus, Information Security Bulletin, April 2004, [online], Dostupné z WWW: <http://www.chi-publishing.com/samples/ISB0903HH.pdf>

[4] Schneier,B., Shostack,A.: Modeling security threats for smart cards, [online], Dostupné z WWW: <http://www.schneier.com/paper-smart-card-threats.html>

[5] Payment card industry (PCI) Data security standard, [online], Dostupné z WWW:
<https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>

[6] Smart card alliance: Contactless technology for secure physical access: Technology and standard choices, [online], Dostupné z WWW:
<http://www2.cnipa.gov.it/site/_contentfiles/01379900/1379995_Contactless_Technology_Report.pdf>

[7] Clarke R.: Smart card technical issues, [online], Dostupné z WWW:
<http://www.anu.edu.au/people/Roger.Clarke/DV/SCTISK2.html>

[8] ČSN ISO/IEC 7816. *Identifikační karty - Karty s integrovanými obvody s kontakty*. Praha : Český normalizační institut, 2003. 75 s.

[9] Witteman M., Advances in Smartcard Security, Information Security Bulletin, July, 2002, [online], Dostupné z WWW:
<http://www.riscure.com/1_general/articles/ISB0707MW.pdf>

[10] JUŘÍK, Pavel. Platební karty : Velká encyklopedie 1870-2006. [s.l.] : Grada, 2009. 296 s. ISBN 80-247-1381-0.

[11] JUŘÍK, Pavel. Svět platebních a identifikačních karet. 2. dopl. vyd. [s.l.] : Grada, 2001. 184 s. ISBN 80-247-0195-2.

[12] *Cardhouse.cz* [online]. 2009 [cit. 2010-04-10]. Identifikace osob komplexně. Dostupné z WWW: <http://cardhouse.cz/>.

[13] *Cardacc.com* [online]. 2010 [cit. 2010-04-11]. Kantech proximity access card and tags. Dostupné z WWW: <http://www.cardacc.com/kantech-cards.htm>.

[14] *Rfidportal.cz* [online]. 2009 [cit. 2010-04-10]. RFID portál. Dostupné z WWW: <http://www.rfidportal.cz/index.php?page=rfid_obecne>.

[15] *Mastercard.com* [online]. 2010 [cit. 2010-04-15]. Credit Card Processing. Dostupné z WWW: <http://www.mastercard.com/au/personal/en/education/chipcard.html>.

[16] *Smartcardalliance.org* [online]. 2010 [cit. 2010-04-20]. Smart Card Alliance. Dostupné z WWW: <http://www.smartcardalliance.org/pages/newsletter-200907-feature?issue=200907>.

[17] *Hitachi.co.jp* [online]. 2010 [cit. 2010-04-20]. Hitachi Smart Card System Solution. Dostupné z WWW: <http://www.hitachi.co.jp/Div/smartcard/english/multos.html>.

[18] *Blackhat.com* [online]. 2001 [cit. 2010-04-22]. Everything you always wanted to know about Smart Cards. Dostupné z WWW: <http://www.blackhat.com/presentations/bh-europe-01/marc-witteman/bh-europe-01-witteman.ppt>.

[19] *Cristal.inria.fr* [online]. 2006 [cit. 2010-05-15]. Smart card security from a programming language and static analysis perspective. Dostupné z WWW: <http://cristal.inria.fr/~xleroy/talks/language-security-etaps03.pdf>.

[20] *Edisecure.com* [online]. 2010 [cit. 2010-04-30]. Digital Identification Solution. Dostupné z WWW: <http://edisecure.com/page/view/key/xid-560ie>.

[21] *Zebra.com* [online]. 2010 [cit. 2010-06-04]. Card Printers. Dostupné z WWW: <http://www.zebra.com/id/zebra/na/en/index/products/printers/card.html>.

[22] *Thebarcodewarehouse.co.uk* [online]. 2007 [cit. 2010-06-04]. Barcode hardware. Dostupné z WWW: <http://www.thebarcodewarehouse.co.uk/Products/cipherlab-1023.aspx>.

[23] *Ingenico-us.com* [online]. 2010 [cit. 2010-05-20]. Beyond Payment. Dostupné z WWW: <http://www.ingenico-us.com/ >.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Triple Data Encription Standard.
ABS	Acrylonitril Butadien Styren
APDU	Application Protocol Data Unit.
API	Application Programming Interface
CLA	CLAse of instruction
CLI	Changeable Laser Imager
CLK	CLocK
Co	Coercivity
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFTPOS	Electronic Funds Transfer at Point of Sale
FIB	Focused Ion Beam
IIN	Issuer Identification Numer
ISO	International Organization for Standardization
ITC	Internal Timing Circuit
JCB	Japan Credit Burelu
MLI	Multiple Laser Image
MMU	Memory Management Unit
MSR	Magnetic Stripe Leader
MULTOS	MULTi-application smart card Operating Systém
PET	PolyEThylen
PVC	Polvinylchlorid
RCx	Rivest Cipher
STEP	Secure Trusted Environment Provisioning

SEZNAM OBRÁZKŮ

Obr. 1. Obchodní vizitka z roku 1895 [10] 12
Obr. 2. Princip termotransféru barvy [12] 15
Obr. 3. Karta s magnetickým pruhem[13] 19
Obr. 4. Kontaktní plošky čipové karty [1] 23
Obr. 5. Struktura čipové karty 24
Obr. 6. kontaktní čipová karta [12] 26
Obr. 7. Princip bezdotykové komunikace 27
Obr. 8. Hybridní karta [12] 27
Obr. 9. Aktivace protokolu karty s vazbou na blízko typu A [12] 32
Obr. 10. Průběh předávání transakce a jejího zúčtování [11] 40
Obr. 11. Rozdělení platebních karet 44
Obr. 12. Přední strana platební karty [15] 46
Obr. 13. Zpracování žádosti o úvěrovou kartu 47
Obr. 14. Ingenico IPA280 [23] 49
Obr. 15. Struktura karty s hologramem [12] 50
Obr. 16. Komponenty bezpečnostního mikrořadiče [16] 54
Obr. 17. MULTOS architektura [17] 55
Obr. 18. Čip odkrytý leptáním [9] 56
Obr. 19. Sondování pomocí osmi jehel *[18]* 57
Obr. 20. Rozložení paměti v čipu 60
Obr. 21. Analýza algoritmu DES [19] 62
Obr. 22. EdiSecure 560ie [20] 67
Obr. 23. Hlavní návrhové okno programu CardPress 68
Obr. 24. Dialogové okno „Návrhář dat“ 68
Obr. 25. Dialogová okna pro formátování textu a úpravy databáze. 69
Obr. 26. Karta potištěná s využitím sw CardPress 70
Obr. 27. Tiskárna Eltron P310iM [21] 70
Obr. 28. Eltron Pointer Tools 71
Obr. 29. Čtení a zápis dat na magnetickou kartu 72
Obr. 30. Cipherlab MSR 1023 [22] 72
Obr. 31. Konfigurační program ke čtečce magnetických karet Cipherlab 1023 73

Obr. 32. Data zachycená na sériovém portu z čtečky Cipherlab 1023 74
Obr. 33. Bezkontaktní RFID čtečka Promag 340. 75
Obr. 34. Prostředí ovládacího programu k zařízení Promag 340. 76
Obr. 35. Zařízení pro zápis a čtení Mifare karet. 77
Obr. 36. Nastavení autentizačních klíčů. 79
Obr. 37. Aplikace Mifare WND 80
Obr. 38. Čtení a zápis do bloků v paměti Mifare 1k. 81
Obr. 39. Nezdařený pokus o čtení z bloku paměti. 82
Obr. 40. Odkryté zařízení pro zápis a čtení Mifare karet. 83
Obr. 41. Schéma elektronického zapojení Mifare kodéru 84
Obr. 42. Schéma logického rozmístění součástí karty 85
Obr. 43. Přenosová sekvence 86
Obr. 44. Organizace paměti EEPROM karty Mifare 1k 87

SEZNAM TABULEK

Tab. 1. Kontaktní plošky čipové karty 23
Tab. 2. Struktura příkazu APDU 30
Tab. 3. Start/Stop znaky 74
Tab. 4.Typy Mifare karet 88