Bezpečnost magnetických karet a možnosti jejich využití v průmyslu komerční bezpečnosti

Security magnetic cards and the possibility of their use in commercial security industry

Bc. Marek Šimčík

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. Marek ŠIMČÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost maqnetických karet a možnosti jejich využití v průmyslu komerční bezpečnosti.**

Zásady pro vypracování:

1. **Proveďte průzkum informačních zdrojů k danému tématu a proveďte jeho literární rešerši.**
2. **Popište současný stav v oblasti technologií a použití magnetických karet a porovnejte je.**
3. **Navrhněte formou projektu vhodný nástroj pro zjišťování informací na magnetických kartách.**
4. **Realizujte zvolené řešení a toto diskutujte.**
5. **Vyslovte závěry týkající se bezpečnosti magnetických karet a vámi realizovaného projektu.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **REID, Robert N. Facility manager's guide to security: protecting your assets. 1st edition. Lilburn, Ga : The Fairmout Press, Inc., 2005. 315 s. ISBN 0-88173-479-9.**
2. **SNEHI, Jyoti. Computer Peripherals and Interfacing. 1st edition. New Delhi : Maxmi Publication (P) LTD., 2006. 123 s. ISBN 81-7008-929-8.**
3. **GUSTIN, Joseph F. Cyber terrorism: a guide for facility managers. 1st edition. Lilburn, Ga : The Fairmout Press, Inc., 2004. 233 s. ISBN 0-88173-442-X.**
4. **SCHNEIDER, Gary. Electronic Commerce. 1st edition. Boston : Course Technology, 2009. 630 s. ISBN 1-4239-0305-6.**
5. **KHOSROW-POUR, Mehdi. E-Commerce Security: Advice from Experts. 1st edition. Hershey : CyberTech Publishing, 2004. 110 s. ISBN 1-59140-240-7.**
6. **PARDOE, Terry D., SNYDER, Gordon, SNYDER, Gordon F. Network security. 1st edition. New York : ThomsonDelmar Learning, 2005. 461 s. ISBN 1-4018-82498.**
7. **HENDRY, Mike. Smart card security and applications. 2nd edition. Nordwood : Artech house,Inc., 2001. 220 s. ISBN 1-58053-156-3.**
8. **RANKL, Wolfgang, EFFING, Wolfgang. Smart card handbook. 3rd edition. West Sossex : John Wiley & sons, 2003. 943 s. ISBN 0-470-85668-8.**
9. **HADDAD, Aneace. A new way to pay: creating competitive advantage through the EMV smart card standard. 2nd edition. Aldershot : Gower Publishing Limited, 2005. 128 s. ISBN 0-556-08688-3.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

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

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce pojednává o bezpečnosti magnetických karet a jejich využití v komerční bezpečnosti. Seznamuje čtenáře s principem technologie magnetických karet a jejich složení. V logickém sledu čtenář získá informace, jak technologie pracuje a jaké nám přináší výhody. Práce porovnává současný stav v oblasti technologii a použití magnetických karet. V druhé části této práce je navržený vhodný nástroj pro zjišťování informací z magnetických karet. V závěru je popsána bezpečnost magnetických karet a výsledky navrženého projektu.

Klíčová slova: magnetická karta, karta s magnetickým proužkem

ABSTRACT

The thesis dissertates the theme of safety and security of magnetic cards and its use in commercial security. It acquaints the reader with the principles of technology of magnetic cards and their contents. The reader gains in logical order the information about how the technology works and what advantages it brings. The thesis describes the current situation in the field of technology and use of magnetic cards. In the second part of the work an appropriate tool for detecting information on magnetic cards is introduced. Safety and security of magnetic cards and the results of the proposed project are described in the conclusion.

Key words: magnetic card, card with a magnetic strip

Rád bych poděkoval vedoucímu mé diplomové práce doc. Mgr. Romanu Jaškovi, Ph.D. za cenné připomínky a rady při řešení problémů souvisejících s diplomovou prací. Dále bych chtěl poděkovat své přítelkyni, za podporu.

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

Plastové magnetické karty se staly součástí života každého z nás, od kreditních karet přes členské až po identifikační zaměstnanecké karty. Jejich standardní velikost, přenosnost a trvanlivost z nich činí perfektní prostředek pro použití v mnoha aplikacích.

Jak vůbec magnetické karty vznikly a proč? Velký význam měla bankovní sféra, která se snažila najít co nejvhodnější a nejbezpečnější řešení bezhotovostních plateb. První vznikly v roce 1914, byly z plechu a podobaly se vojenským štítkům, tzv. „metal money“. Další vývoj šel od cestovních šeků, přes kovové úvěrové mince a několik typů úvěrových karet, až po první magnetické platební karty. Zlom ve vývoji představuje použití magnetického proužku jako nosiče klientských dat. Za jeho rozšíření vděčíme zejména snadné výrobě, nízkým pořizovacím nákladům a flexibilitě.

Většina karet obsahuje z rubové strany magnetický proužek, který slouží pro uložení dat, která lze kdykoliv z pásky přečíst pomocí čtecího zařízení. Magnetický proužek byl vynalezen již v roce 1878, avšak až společnost IBM ho dokázala aplikovat tak, aby byl schopen nést statická data o klientovi. Přes počáteční nedokonalosti, jako lehkou padělatelnost, se časem podařilo magnetický proužek upravit tak, aby mohl bezpečně nést všechna nezbytná data o uživateli. První karta s magnetickým proužkem byla vydána v roce 1969, jednalo se o kartu Air Travel Card. O pouhé 4 roky později bylo již proužkem vybaveno plných 85% všech platebních karet.

V roce 1974 zavedla American Bankers Association normu, která definovala magnetický proužek pro bankovnictví. Tato norma se v roce 1974 stala základem mezinárodních norem ISO, které se používají dodnes.

V současnosti, kdy se na celém světě zvyšují nároky na bezpečnost, rychlost a přesnost, magnetické karty a magnetický proužek zaujímají důležité postavení. Nachází využití např. tam, kde je třeba kontrolovat a odbavovat velká množství cestujících (například letiště).

Budoucnost karet s magnetickým proužkem je otázkou. Pravděpodobně budou nahrazeny čipovými kartami, které jsou mnohem bezpečnější. Nicméně ještě neproběhla transformace na všech příjmových místech, proto většina karet je tzv. hybridních (nese proužek a čip).

I. TEORETICKÁ ČÁST

1 MAGNETICKÁ KARTA

Magnetická karta je prostředek identifikace a autorizace osob. Magnetické karty existují již od počátku sedmdesátých let, kdy byl magnetický proužek používán na papírových ID kartách, stejně jako na kreditních kartách. Technologie magnetického proužku je velmi rozšířená po celém světě, hlavně v USA kde zůstává dominantní technologií pro zpracování transakcí a kontrolu přístupu.[11]

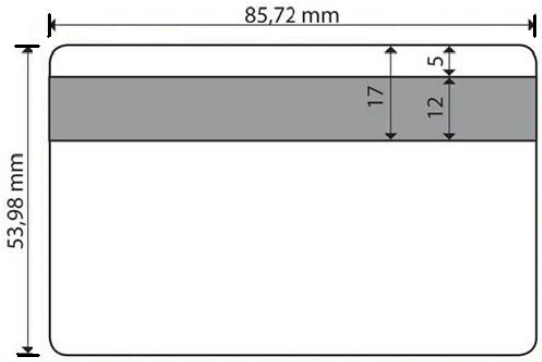
Magnetické karty jsou jedním z nejrozšířenějších zapisovatelných nosičů informace. Magnetický proužek umožňuje mnohonásobný zápis a čtení informace v digitální podobě (viz třetí stopa magnetického proužku).[16]

Magnetická karta se skládá ze samotné karty (většinou z PVC) a magnetického proužku.

Obr. 1 *Magnetická karta [23]*

1.1 Normy ISO pro magnetické karty

- **ČSN EN ISO/IEC 7810** - Identifikační karty - Fyzikální charakteristiky
- **ČSN ISO/IEC 7811-1** - Identifikační karty - Záznamová technika - Část 1: Reliéfní písmo
- **ČSN ISO/IEC 7811-2** - Identifikační karty - Záznamová technika - Část 2: Magnetický proužek s nízkou koercitivitou.
- **ČSN ISO/IEC 7811-6** - Identifikační karty - Záznamová technika - Část 6: Magnetický proužek - Vysoká koercitivita[11]
- **ČSN ISO/IEC 7812** - Identifikační karty – Identifikace vydavatelů karet
- **ČSN ISO/IEC 7813** - Identifikační karty - Karty pro finanční transakce.



Obr. 2 *Rozměry magnetické karty [21]*

1.2 Výrobní materiál karet

K výrobě plastových karet se používají syntetické hmoty jako PVC, ABS, PET, PVH nebo polykarbonáty. Typ materiálu je volen většinou s ohledem na účel, který plastová karta bude plnit. Jiný materiál bude vhodný pro kartu k jednorázovému použití, jiný pro platební kartu nebo kartu zaměstnance s poměrně velkou frekvencí používání.

Pro potisk v termotiskárnách jsou zpravidla použity karty z PVC. Polyvinylchlorid má velmi velkou schopnost absorbovat sublimované barvy, je proto ze jmenovaných karet pro termotisk nerozšířenějším materiálem. Naproti tomu PET nebo ABS jsou velmi odolné materiály s horší schopností absorpce. Bývají zpravidla použity pro karty, které budou potisknuty například ofsetem nebo Termo Re-Transferem.

Často se také setkáme s pojmem kompozitní karta (nebo PVH). Jedná se o kartu sendvičové konstrukce. Obě strany jsou opatřeny svrškem z PVC pro snadný potisk, jádro je pak tvořeno z PET- tedy z polyetylenu. Výsledkem je kompenzace teplotní nestálosti PVC. Kompozitní karty jsou odolnější zejména vůči vyšším teplotám (kolem 180°C), to je také důvod, proč lze pouze takové karty laminovat.[11]

1.2.1 PVC karty

Zajišťují vysokou kvalitu obrázků, střední pružnost a tepelnou odolnost. Tyto vlastnosti jsou důležité pro aplikace vyžadující potisk od kraje do kraje. PVC karty se používají především jako identifikační, návštěvní a věrnostní karty.[11]

1.2.2 ABS karty

Plastové karty mají maximální životnost a odolnost proti fyzikálním a chemickým vlivům. Karty z ABS plastu jsou používány zejména jako platební karty.[11]

1.2.3 PET karty

Vyznačují se vysokou kvalitou povrchové úpravy. Jsou velmi odolné vůči mechanickému namáhání při běžných teplotách. V mraze se jejich mechanické vlastnosti, stejně jako u PVC, zhoršují.[11]

1.2.4 Kompozitní karty

Karty jsou odolnější, protože se skládají z několika vrstev. Jádro tvoří polyester a povrch PVC (60% PVC a 40% polyester). Předpokládaná životnost materiálu je od 4 do 7 let v závislosti na použití. Tyto karty se používají v aplikacích vyžadujících dlouhou životnost potisku a velkou odolnost, jako např. přístupové karty a multifunkční identifikační karty. Pomocí laminace se zvyšuje životnost karty až na trojnásobek.[11]

1.2.5 PET-G karty

Pro výrobu plastových karet je zajímavý hlavně pro svou čirost. Průhledné magnetické karty s potiskem jsou velmi efektní a vhodné zejména pro věrnostní a reklamní aplikace.[11]

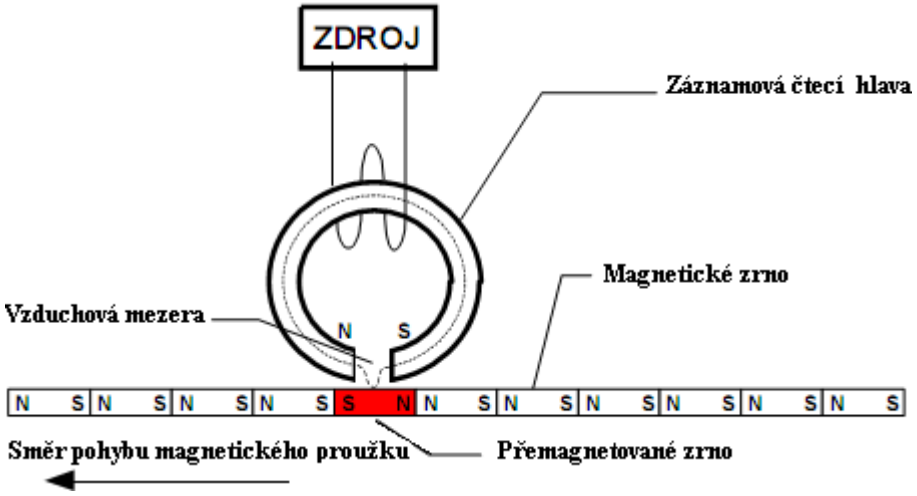
1.2.6 Papírové karty

Papírové magnetické karty mají jádro z papíru. Jejich povrchová úprava může být v provedení matném anebo lesklém (PVC laminace).

1.3 Princip magnetického záznamu

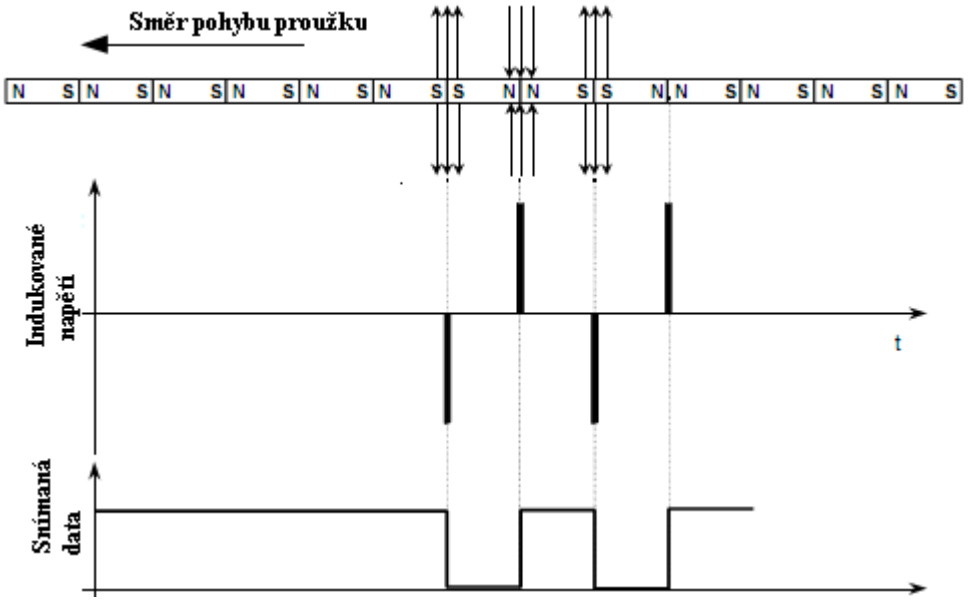
Princip záznamu informace je obdobný jako u magnetofonu. Magnetický proužek je pokryt vrstvou feromagnetického materiálu, který je tvořený velkým množstvím miniaturních magnetických zrn zalitých v pojivě, který je současně drží na podkladové ploše. Magnetické zrna tvoří miniaturní tyčové magnety. Hustota těchto miniaturních magnetů je přibližně 8 miliónů zrn na jeden centimetr délky proužku. Jako magnetický materiál jsou

používané oxidy železa nebo chrómu, případně upravené čisté železo (Fe2O3 , CrO2 , Fe). Magnetická vrstva se vyrábí tak, že po nanesení na podkladovou vrstvu se magnetická zrna externím magnetickým polem uspořádají rovnoběžně s magnetickou páskou po dobu tvrdnutí pojiva. Tyto magnetické částice jsou permanentní tyčové magnety se dvěma stabilními póly. Když je však umístíme do silného externího magnetického pole opačné polarity, dojde ke změně jejich magnetické polarity. Intenzita magnetického pole potřebná na změnu polarity, se nazývá koercitivní sila – koercitivita. Magnetická zrna se dodávají s různou koercitivitou. Na nevyužitém magnetickém proužku jsou magnetická zrna uspořádaná se stejnou polaritou, tím splynou a vypadají jako jeden tyčový magnet. Při vzniku rozhraní dvou pólů stejné polarity (například S–S nebo N-N), magnetické toky se budou odpuzovat, koncentrace magnetických siločar slouží jako rozhraní dvou pólů se stejnou polaritou. Zápis na magnetickou pásku spočívá ve vytvoření rozhraní dvou pólů stejné polarity, čtení proužku spočívá v detekci takových rozhraní. Při pohybu magnetického proužku v externím magnetickém poli dochází k magnetizaci aktivní vrstvy proužku. Po oddálení zdroje magnetického pole si zmagnetizovaný materiál ponechává malou část magnetického pole, tzv. zbytkový (remanentní) magnetismus. Při záznamu jsou jednotlivá zrna zmagnetována podle okamžité polarity a intenzity magnetického pole. V důsledku toho na pásce vznikají rozhraní dvou pólů se stejnou polaritou. Protože pro záznam informací pomocí magnetických kódů používáme binární kód, stačí dvě polarity magnetického pole při konstantní intenzitě. Na přepólování magnetických zrn proužku je třeba vnější magnetické pole. To se vytvoří cívkou, která mění polaritu magnetického pole v důsledku změn směru proudu protékajícího vinutím cívky. Cívka je navinutá na železném jádře prstenčitého tvaru se vzduchovou mezerou, do které je magnetické pole soustředěné. Pod vzduchovou mezerou se pohybuje magnetická páska. Když ve vzduchové mezeře vystavíme elementární magnety magnetického proužku silovému působení magnetického pole, polarizují se opačně než polarita magnetického pole v mezeře (dokud pole působí). Při pohybu proužku a záznamové hlavy proti sobě, dochází v závislosti na okamžité polaritě magnetického proudu k různému přemagnetování zrn a tím k záznamu informace.[10]



Obr. 3 *Přemagnetování magnetického zrna [10]*

Při mazání magnetického proužku, zdroj v cívce vytvoří magnetické pole o konstantní polaritě a celá páska se pohybuje vzduchovou mezerou. Tak se všechna magnetická zrna přemagnetizují pomocí magnetického pole stejné orientace, tím zanikne rozhraní se stejnou polaritou a jím způsobené magnetické toky.



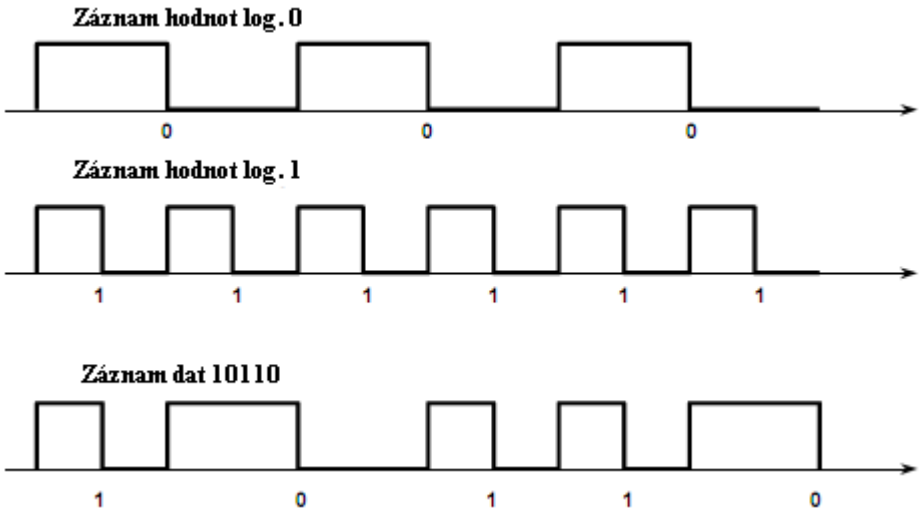
Obr. 4 *Čtení magnetického proužku[10]*

Čtení údajů zaznamenaných na magnetické pásce je obrácená činnost, ke které lze použít stejnou cívku. Při pohybu proužku pod vzduchovou mezerou vzniká v železném jádře proměnlivé magnetické pole. Ve vzduchové mezeře dochází ke změně magnetického pole, které vzniká na rozhraní stejných polarit indukovaných napětím v čtecí cívce. Po zesílení lze informaci zpracovat v dalších obvodech.

1.3.1 Kódování údajů

Významným krokem je kódování údajů, tj. způsob přiřazení změn magnetizace na pásce a jimi vyvolané elektrické signály logickým hodnotám (log.0 a log.1). Lze zapisovat informace do jedné a více stop.

F2F „frequency two frequency" někdy označované též jako „Aiken Biphase". Podstatou této kódovací techniky je záznam logických nul a jedniček v podobě napěťových impulzů, které se liší frekvencí. Frekvence logických jedniček je dvojnásobkem frekvence logických nul.



Obr. 5 *Kódování F2F [10]*

1.3.2 Magnetické kódy

Důležitým faktorem ovlivňujícím kapacitu magnetického proužku a bezpečnost údajů zapsaných na proužku, je způsob reprezentace alfanumerických znaků binárními symboly. Existuje velké množství různých možností. Americký národní institut pro standardy ANSI (American National Standards Institute) a Mezinárodní organizace pro standardy ISO (International Standards Organisation) zvolili 2 standardy, které jsou doporučené pro použití v magnetických kartách.

ANSI / ISO BCD datový formát

Jde o 5 bitový binárně kódovaný dekadický formát o 16 znacích, který se používá k zakódování 4 z 5 bitů. Pátý bit je paritní bit nepárové parity – doplňuje celkový počet bitů jednoho znaku na nepárový počet.

Datové bity				*Par. bit*	*Znak*	*Význam*
b1	*b2*	*b3*	*b4*	*b5*		
0	0	0	0	1	0 (0_H)	**Data**
1	0	0	0	0	1 (1_H)	**Data**
0	1	0	0	0	2 (2_H)	**Data**
1	1	0	0	1	3 (3_H)	**Data**
0	0	1	0	0	4 (4_H)	**Data**
1	0	1	0	1	5 (5_H)	**Data**
0	1	1	0	1	6 (6_H)	**Data**
1	1	1	0	0	7 (7_H)	**Data**
0	0	0	1	0	8 (8_H)	**Data**
1	0	0	1	1	9 (9_H)	**Data**
0	1	0	1	1	: (A_H)	**Řízení (Control)**
1	1	0	1	0	; (B_H)	**Začátek bloku (Start Sentinel)**
0	0	1	1	1	< (C_H)	**Řízení (Control)**
1	0	1	1	0	= (D_H)	**Oddělovač polí (Field Separator)**
0	1	1	1	0	> (E_H)	**Řízení (Control)**
1	1	1	1	1	? (F_H)	**Konec bloku (End Seninel)**

Tab. 1 *Kódování znaku datového formátu ANSI/ISO BCD [10]*

Při čtení dat magnetické karty se jako první čte vždy nejméně významný bit (b1). Z tabulky 1 je možné odvodit, že 16 znaková 5 bitová sada je tvořená 10 číslicemi reprezentujícími data, 3 znaky ohraničenými blokem dat (začátek stopy, konec stopy a oddělovač polí) a 3 řídícími znaky.

Záznam na magnetické pásce začíná řetězcem nulových impulzů, které mají význam v aktivování vlastního časování (tzv. self-clock ing) na synchronizaci a spuštění dekódování. Začátek stopy dat (Start Sentinel), který nese informaci o začátku 5 bitových skupin údajů. Blok dat je ukončený koncem stopy (End Sentinel), za kterým následuje tzv. „podélný“ kontrolní znak LRC (Longitudinal Redundancy Check). LRC znak je paritní kontrola součtu všech datových bitů b1, b2, b3 a b4 všech předcházejících znaků. LRC umožňuje zachytit skryté chyby, které se můžou vyskytnout v případě tzv. kompenzované chyby znaku. Dojde také ke změně 2 anebo vícerých bitů, takže se nezmění parita znaku. Záznam

je opět ukončený synchronizačními nulovými impulzy. Počáteční a zakončovací blok nulových impulzů má proměnlivou délku.

Začátek stopy, konec stopy a kontrolní znak LRC se označují souhrnným pojmem „Ohraničující znaky“ (Framing Characters) a na konci procesu čtení informace se tyto znaky z informace odstraní.

ANSI / ISO ALPHA datový formát

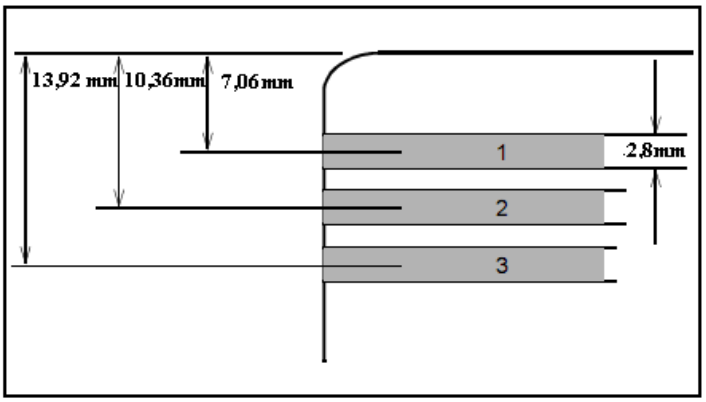
Na magnetickou pásku se můžou zapisovat i alfanumerické znaky. Druhý datový formát ANSI/ISO je proto označovaný jako o ALPHA (alfanumerický). Tento formát je tvořený 7 bitovou znakovou sadou, která umožňuje kódovat 64 znaků. Obdobně jako v předcházejícím kódu, informace o znaku nese 6 bitů. Sedmý bit je paritní bit nepárové parity. Z tabulky 2 je zřejmé, že 7 bitová znaková sada obsahuje 64 znaků, z toho 43 alfanumerických znaků, 3 znaky oddělených blokových dat (začátek stopy, konec stopy a oddělení) a 18 řídících anebo speciálních znaků. Obdobně jako při předcházejícím kódu se jako první čte vždy nejméně významný bit b1.

Data						P	Znak	Význam	Data						P	Znak	Význam
b1	b2	b3	b4	b5	b6	b7			b1	b2	b3	b4	b5	b6	b7		
0	0	0	0	0	0	1	medz (0_h)	Speciální	0	0	0	0	0	1	0	@ (20_h)	Speciální
1	0	0	0	0	0	0	! (1_h)	Speciální	1	0	0	0	0	1	1	A (21_h)	Data (písmeno)
0	1	0	0	0	0	0	" (2_h)	Speciální	0	1	0	0	0	1	1	B (22_h)	Data (písmeno)
1	1	0	0	0	0	1	# (3_h)	Speciální	1	1	0	0	0	1	0	C (23_h)	Data (písmeno)
0	0	1	0	0	0	0	$ (4_h)	Speciální	0	0	1	0	0	1	1	D (24_h)	Data (písmeno)
1	0	1	0	0	0	1	% (5_h)	Začátek bloku	1	0	1	0	0	1	0	E (25_h)	Data (písmeno)
0	1	1	0	0	0	1	& (6_h)	Speciální	0	1	1	0	0	1	0	F (26_h)	Data (písmeno)
1	1	1	0	0	0	0	' (7_h)	Speciální	1	1	1	0	0	1	1	G (27_h)	Data (písmeno)
0	0	0	1	0	0	0	((8_h)	Speciální	0	0	0	1	0	1	1	H (28_h)	Data (písmeno)
1	0	0	1	0	0	1	) (9_h)	Speciální	1	0	0	1	0	1	0	I (29_h)	Data (písmeno)
0	1	0	1	0	0	1	* (A_h)	Speciální	0	1	0	1	0	1	0	J ($2A_h$)	Data (písmeno)
1	1	0	1	0	0	0	+ (B_h)	Speciální	1	1	0	1	0	1	1	K ($2B_h$)	Data (písmeno)
0	0	1	1	0	0	1	, (C_h)	Speciální	0	0	1	1	0	1	0	L ($2C_h$)	Data (písmeno)
1	0	1	1	0	0	0	- (D_h)	Speciální	1	0	1	1	0	1	1	M ($2D_h$)	Data (písmeno)
0	1	1	1	0	0	0	. (E_h)	Speciální	0	1	1	1	0	1	1	N ($2E_h$)	Data (písmeno)
1	1	1	1	0	0	1	/ (F_h)	Speciální	1	1	1	1	0	1	0	O ($2F_h$)	Data (písmeno)
0	0	0	0	1	0	0	0 (10_h)	Data (číslo)	0	0	0	0	1	1	1	P (30_h)	Data (písmeno)
1	0	0	0	1	0	1	1 (11_h)	Data (číslo)	1	0	0	0	1	1	0	Q (31_h)	Data (písmeno)
0	1	0	0	1	0	1	2 (12_h)	Data (číslo)	0	1	0	0	1	1	0	R (32_h)	Data (písmeno)
1	1	0	0	1	0	0	3 (13_h)	Data (číslo)	1	1	0	0	1	1	1	S (33_h)	Data (písmeno)
0	0	1	0	1	0	1	4 (14_h)	Data (číslo)	0	0	1	0	1	1	0	T (34_h)	Data (písmeno)
1	0	1	0	1	0	0	5 (15_h)	Data (číslo)	1	0	1	0	1	1	1	U (35_h)	Data (písmeno)
0	1	1	0	1	0	0	6 (16_h)	Data (číslo)	0	1	1	0	1	1	1	V (36_h)	Data (písmeno)
1	1	1	0	1	0	1	7 (17_h)	Data (číslo)	1	1	1	0	1	1	0	W (37_h)	Data (písmeno)
0	0	0	1	1	0	1	8 (18_h)	Data (číslo)	0	0	0	1	1	1	0	X (38_h)	Data (písmeno)
1	0	0	1	1	0	0	9 (19_h)	Data (číslo)	1	0	0	1	1	1	1	Y (39_h)	Data (písmeno)
0	1	0	1	1	0	0	: ($1A_h$)	Speciální	0	1	0	1	1	1	1	Z ($3A_h$)	Data (písmeno)
1	1	0	1	1	0	1	; ($1B_h$)	Speciální	1	1	0	1	1	1	0	[($3B_h$)	Speciální
0	0	1	1	1	0	0	< ($1C_h$)	Speciální	0	0	1	1	1	1	1	\ ($3C_h$)	Speciální
1	0	1	1	1	0	1	= ($1D_h$)	Speciální	1	0	1	1	1	1	0	] ($3D_h$)	Speciální
0	1	1	1	1	0	1	> ($1E_h$)	Speciální	0	1	1	1	1	1	0	^ ($3E_h$)	Oddělovač polí
1	1	1	1	1	0	0	? ($1F_h$)	Konec bloku	1	1	1	1	1	1	1	_ ($3F_h$)	Speciální

Tab. 2 *Kódování znaků datového formátu ANSI/ISO ALPHA [10]*

1.4 Umístění dat na magnetické pásce

ANSI / ISO standard definuje tři standardní stopy, z kterých každá je určená na jiné účely. Tyto stopy jsou určené jen jejich polohou na magnetické pásce, protože konstrukčně je magnetická vrstva homogenní bez dělících mezer.



Obr. 6 *Umístění stop na magnetickém proužku*

Data jsou na pásce zapsané zleva doprava. V jednotlivých stopách se používají různé kódy s různou hustotou záznamu. Podle doporučení ANSI/ISO se používají následující kódy:

Stopa	Název	Hustota záznamu	Datový formát	Počet znaků
1	IATA	210 bpi	ALPHA	79
2	ABA	75 bpi	BCD	40
3	THRIFT	210 bpi	BCD	107

Tab. 3 *Rozdělení stop na magnetickém proužku*

1.4.1 První stopa

Byla definována již v roce 1969, je pojmenovaná podle Mezinárodní asociace letecké dopravy IATA (International Air transport Association). Obsahuje jméno držitele karty, číslo (označení) účtu a případně další volitelné údaje. Strukturu stopy znázorňuje tab. 4.

SS	FC	PAN	NAME	FS	Doplňkové	ES	LRC
Start Sentinel-Začátek stopy	Formát Code-Použitý formát kódu	Primary Account Number-Základní číslo účtu,max 19 znaků	Max. 26 Alfanumerických znaků	Field Separátor-Oddělovač polí	Datum vypršení platnosti, kódovací PIN, …	End Sentinel-Konec stopy	Longitudinál Redundancy Charakter-Longitudinál redundandní znak

Tab. 4 *Struktura 1. stopy magnetického proužku*

Americké banky přijaly tuto normu v roce 1970. První stopa má 79 znaků včetně SS, ES a LRC. Obsahují číslo karty (až 18 číslic) a jméno klienta (až 26 alfanumerických znaků), včetně SS, ES a LRC. PAN používané na kartách MasterCard má proměnlivou délku. Nejvíc má 16 znaků. Karty VISA používají 13 anebo 16 znaků včetně kontrolní číslice, vypočítané jako modul 10.

1.4.2 Druhá stopa

Pojmenovaná podle Americké bankovní asociace ABA (American Banking Association). Tato stopa je nejčastěji používaná v bankovnictví. ABA vytvořila standard stopy a všechny světové banky ho musí dodržovat. Tato stopa obsahuje 40 numerických znaků včetně čísla karty (až 19 číslic). Obsah stopy: účet držitele karty, zašifrovaný PIN a případně další volitelné údaje.

SS	PAN	FS	Doplňkové	ES	LRC
Start Sentinel-Začátek stopy	Primary Account Number-Základní číslo účtu,max 19 znaků	Field Separátor-Oddělovač polí	Datum vypršení platnosti, kódovací PIN, …	End Sentinel-Konec stopy	Longitudinál Redundancy Check

Tab. 5 *Struktura 2. stopy magnetického proužku*

1.4.3 Třetí stopa

Je podobná stopám 1 a 2, ale používá se zřídka. Na rozdíl od 1. a 2. stopy, které jsou určeny pouze pro čtení, může být záznam na 3. stopě přepisován. Dříve se používala zejména pro operace typu off-line, uskutečněných v bankomatech pomocí čtecího zařízení, které zapíše přímo na kartu aktuálně údaje o stavu účtu. Vzhledem k tomu, že bankomaty v současnosti pracují výhradně v režimu on- line, tato možnost ztratila význam. Na této stopě byl zaznamenán parametr, podle kterého bylo možné ověřit správnost kódu PIN. K záznamu potřebných informací, sloužilo až 107 numerických znaků (PIN, kód země, měnová jednotka, finanční limit a další).

1.5 Rozdělení magnetických karet podle proužků koercitivity magnetického proužku

Jak již bylo naznačeno v kapitole 1.4 (Princip magnetického proužku), magnetické karty se rozlišují podle koercivity.

1.5.1 Magnetická karta s proužkem HiCo (High Coercitivity)

Zkratka pro vysokou koercivitu. HiCo magnetické stopy určuje nejvyšší úroveň její odolnosti před poškozením rozptýleným magnetickým polem. Využití má v těžkých průmyslových provozech s vysokým stupněm elektromagnetického rušení. Kódovat karty s touto magnetickou stopou je mnohem náročnější než karty s magnetickou stopou LoCo, neboť kódování vyžaduje větší výkon. Magnetické karty HiCo jsou proto nepatrně nákladnější.[11]

1.5.2 Magnetická karta s proužkem LoCo (Low Coercivity)

Zkratka pro nízkou koercivitu. Je jednodušší na kódování a nepatrně levnější než karty s magnetickou stopou HiCo. Výběr typu magnetické stopy závisí na tom, jak bude karta

používána. Magnetickou kartu budeme moci použít v běžných kancelářských prostředích. Rozdíl mezi magnetickým proužkem HiCo a LoCo, lze poznat podle barvy. HiCo má barvu černou a LoCo hnědou.[11]

1.6 Detekce chyb při čtení z magnetické karty

Používají se dvě metody detekce. A to paritní bit a LRC (Longitudinal redundancy check). LRC je kód, který je používán při zápisu na kartu a při čtení z karty se kontroluje. LRC obsahuje kombinaci bitů, které tvoří celkový počet kódovaných a odpovídající bitové lokace všech znaků, včetně řídících znaků (start a konec stopy včetně LRC), přitom ignoruje paritu. Ke kontrole LRC se provede XOR na všechny kódové znaky. Výsledek musí být nula. Účelem těchto dvou metod je udělat detekci chyb více přesnou. Důvod je jednoduchý, při čtení znaku dojde ke dvěma chybám, ale výsledek parity bude jako by nepřečetl žádnou chybu. Proto se aplikuje LRC, aby bylo čtení označeno za chybné.

1.7 Snímače magnetických kódů (tzv. čtečka)

Čtecí zařízení pro magnetické karty může být konstruováno jako statické. Čtecí hlava je pevná a pohybuje se karta v drážce čtečky. Pohyb karty je zpravidla ruční. To má za následek různé rychlosti pohybu karty ve snímači, proto se používají převážně jako čtecí. Druhý typ snímačů dělá pohyb čtecí hlavy pomocí krokového motoru, přitom se snímaná karta nepohybuje.

Obr. 7 *Z leva: IBM štěrbinová čtečka na dotykový displej, IBM štěrbinová čtečka, Čtecí hlava magnetického proužku*

1.8 Personalizace magnetických karet

Abyste mohli určit, komu plastová karta náleží (firma), není nic jednoduššího než opatřit kartu některým s personalizačních prvků. Znamená to, že kromě vlastního viditelného popisu karty (číslo karty, …), je ještě na její magnetický proužek (zpravidla na 2. stopu) zaznamenán kód, který jednoznačně identifikuje jak vlastního zaměstnance, tak vydavatele karty (organizaci). V kapitole jsou použity především zdroje 28, 17, 11.

1.8.1 Digitální tisk

Je způsob personalizace na archu (arch obsahuje několik karet), personalizované údaje se tisknou na danou kartu, design je všem společný. Dále se karta překryje silnou laminační folií a následně výsekem plastu na rozměr karty. Zápis je možný pomocí alfanumerických znaků nebo plnobarevný tisk.[28]

1.8.2 Termoprint

Termoprint je technika personalizace plastové karty, kterou je možné nanášet přímo na plastovou kartu nejrůznější personifikační prvky (fotografie, loga, identifikační čísla, čárové kódy apod.). Zápis je opět možný pomocí alfanumerických znaků a plnobarevného tisku.[28]

1.8.3 Re-transfer

Je způsob personalizace jednotlivých karet, personalizované údaje se tisknou na laminační fólii reverzním tiskem, následně se laminují tyto fólie na kartu. Zápis je možný pomocí alfanumerických znaků a plnobarevného tisku.[28]

1.8.4 Laserové gravírování

Je personalizace jednotlivých karet, gravíruje se laserem nebo diamantem. V případě laserového gravírování se využívá velmi slabého laserového paprsku, personalizované údaje vpalují přímo na povrch karty, tak aby se nepoškodila plastová karta. Umožňuje vypalovat alfanumerické znaky, obrázky v odstínech šedi. Gravírování diamantem se u plastu až tak často nevyužívá, avšak touto technologií mohou vzniknout velmi poutavé rytiny do plastové karty sloužící k personalizaci.[28]

1.8.5 Embossing

Vystouplé písmo je technologie, kterou je možné na plastové karty tisknout několikařádkové informace (jméno, adresa, tel. čísla, apod.). Doplňkem embossingu je tipping plastových karet, barevné zvýraznění vrcholů znaků (pokrytí barevnou fólií). Nejčastěji používané barvy jsou černá, stříbrná a zlatá, lze však použít i jiné odstíny barev a to v lesklém i matném provedení. Alfanumerické znaky jsou o velikosti 0,3 mm a 0,5 mm, na jeden řádek se vejde 29 znaků.[28]

Obr. 8 *Embossováná karta*

1.8.6 Ident

Ident je technologie personifikace plastové karty obdobná embossingu, ale výsledkem aplikace je vtlačené písmo.[17]

1.9 Personifikace magnetických karet

Pro určení komu plastová karta náleží (osobu), je možné opatřit kartu některým z personifikačních prvků. Znamená to: viditelný popis karty (osobní číslo, fotografie,…). Personifikovaná karta se díky těmto prvkům stává takzvanou kartou osobní.[15]

1.9.1 Fotografie uživatele

Fotografii na kartu s magnetickým proužkem je možné nanést více způsoby. Musí splňovat svými rozměry ISO normu.

Nejpraktičtější je tzv. laminace za studena. Kompletace magnetické karty spočívá v usazení standardizovaných podobenek (25x32 mm) do předem připravených okének karty a jejich následném přelepení průhlednou, dále neoddělitelnou fólií. Tento proces je možné realizovat i u vydavatele, není-li požadována nějaká další personifikace. Výhodou tohoto způsobu vydávání je operativnost a možnost přípravy karet přímo u vydavatele.

Další způsob implantace fotografie na kartu je laminace při vlastní výrobě karet (tzv. laminace za tepla). Tento proces vyžaduje, aby vydavatel odevzdal předem do výroby fotografie všech držitelů karet. Ty jsou potom tepelným procesem zataveny do vlastního PVC nosiče.

Nejnovější způsob přenášení fotografie je tzv. termoprint, který může být jak jednobarevný, tak i vícebarevný. Většinou se kvalitativně s výše uvedenými způsoby nedá srovnávat. Jeho výhodou je flexibilita a rychlost vydávání karet.

Rovněž jsou možné alternativní způsoby přenosu fotografie na vlastní nosič. Buď gravírováním pevně nanesené vrstvy, nebo vypalováním.

1.9.2 Podpisové pole

Některé magnetické karty mají pole pro dodatečný popis karty, např. podpis majitele. Podpisové pole se tiskne v různých velikostech, sítotiskovou průsvitnou barvou s možností podtisku. U bankovních karet bývá podpisové pole ze zadní strany.[28]

1.9.3 Tisk osobního čísla

Osobní číslo je jednoznačným identifikátorem zaměstnance (policie-služební číslo).

1.10 Ochranné a bezpečnostní prvky karet s magnetickým proužkem

Pro ochranu plastových karet se používají různé typy materiálů. Overlaye, holografické a ochranné laminovací materiály zajistí kartě trvanlivost a ochranu podle požadavků uživatele.

Materiál	**Životnost karty**	**Stálost**	**Zabezpečení**
Overlay	až 2 roky	minimáln	
Overlay s hologramem	až 2 roky	minimáln	Vizuální
Průhledná laminace	až 5 let	vysoká	
Laminace s hologramem	až 5 let	vysoká	Vizuální

Tab. 6 *Životnost materiálů*

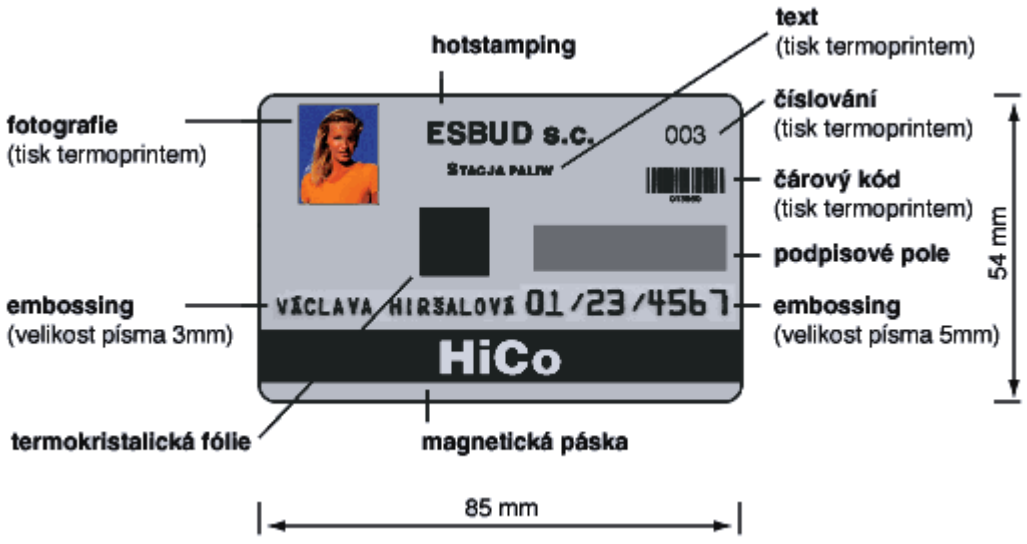
Karta musí zaručovat životnost karty (počet protažení karty snímačem), která u výrobců s certifikací nesmí být nižší než 10 000.[12]

Dále trvanlivost karty určuje, jak dobře dokáže odolávat různým formám zátěže okolního prostředí. To zahrnuje odolnost proti oděru (např. při průchodu čtečkou magnetické stopy či čárového kódu), ochranu proti vyblednutí barev na slunci a odolnost proti poškození vodou či chemikáliemi.

Musí být zabezpečená proti manipulaci, pozměňování a/nebo padělání. Při použití ochranných materiálů, jako jsou lamináty, může být karta vytvořena tak, aby byly eliminovány potenciální manipulace a úpravy.

Zabezpečení karty znamená, že u karty může být zkontrolována její pravost. Tato technika používá overlaye nebo lamináty s holografickým obrázkem.[11]

S již vydanou kartou jakéhokoliv provedení je třeba zacházet jako s ceninou. Proto je nutné toto médium chránit proti možnému padělání. Běžné způsoby ochrany jsou stejné jako u cenin, tzn. vodoznak, vlepení hologramu (trojrozměrný symbol vytvořený speciální laserovou technologií), vlepení speciálního drátku do nosiče PVC apod. Tyto přídavné zabezpečovací metody je možné kontrolovat buď jednoduše opticky, nebo za pomoci speciálních zařízení.[12]



Obr. 9 *Ochranné prvky magnetické karty [15]*

1.10.1 Scratch (stírací) pole

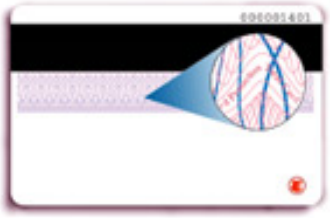
Je speciální fólie, která slouží pro zakrytí tištěných údajů na kartě, které se stávají čitelnými až po odstranění této fólie z karty. Má využití zejména u předplacených telefonních karet.[28]

1.10.2 Hotstamping

Jsou různobarevné metalické fólie, které se za vysokého tepla vyrazí na kartu.

1.10.3 Giloš

Geometricky přesný motiv je tvořený průnikem jedné nebo více křivek s definovaným průběhem, zakřivením a hustotou. Tisk gilošů je technologicky náročná záležitost a lze se s ním setkat např. u bankovek, cenin, kolků ale i předtisknutých plastových karet.[11]



Obr. 10 *Ochranný prvek karet- Giloš*

1.10.4 Hologram

Je nejefektivnější, ale také nejnákladnější ochranný prvek na kartě (vytvořený speciální laserovou technologií). Zrcadlové hologramy umožňují trojrozměrný dojem a prostorovou hloubku. Představuje vysoký stupeň zabezpečení, pravost karty lze jednoduše ověřit jejím pootočením.

Obr. 11 *Hologram*

1.10.5 Tisk sériových čísel

Jsou-li karty v sériích opatřeny jednoznačným číslem, je jejich padělání nebo pozměňování ztíženo.

Obr. 12 Sériové číslo

1.10.6 Mikrotisk

Jsou to velmi malá písmena a číslice viditelná pod lupou. Při použití jakékoliv kopírky nebo skeneru se tento ochranný prvek nezobrazí. Většinou jej není možné tisknout ani pomocí termosublimačních tiskáren na plastové karty.

Obr. 13 *Mikrotisk*

1.10.7 Opacitní značky

Jsou objekty na povrchu těla karty s odlišnou schopností propouštět nebo odrážet světlo.

Obr. 14 *Opacitní značka*

1.10.8 Nalepení termokrystalické fólie

Nalepením termokrystalické fólie se rozumí nalepení této fólie na kartu. Fólie reaguje na teplotu prstu různorodým zabarvením. Tyto fólie lze použít k měření stresu, nebo jako teploměr.

1.10.9 Bezpečnostní prvky aplikovatelné termotiskárnou

UV barvy

Používají se jednobarevné a vícebarevné barvící proužku s UV barvou. UV barva je viditelná pouze v UV spektru, k jejímu prohlížení je třeba zdroje UV světla, např. zkoušečka bankovek, černé zářivkové trubice na diskotékách

Obr. 15 *Tisk UV barvou* [11]

Tisk „šedé na šedou“

Pomocí některých tiskáren lze tisknout na světlé šedé pozadí tmavší šedý text nebo grafiku, pro většinu tiskáren plastových karet je tento tisk nemožný.

Obr. 16 *Tisk šedá na šedou* [11]

Laminační proužky s hologramem

Ochranná vrstva je aplikovatelná pouze pomocí laminátoru. Vrstva může obsahovat tisknuté a nalepené hologramy nebo může být jen čirá.

Obr. 17 *Laminační proužek s hologramem*

1.11 Ochrana dat zapsaných na magnetickém proužku

Jediná ochrana pro data na kartě je šifrování dat. Data můžeme šifrovat buď šiframi symetrickými, nebo asymetrickými.

1.11.1 Symetrické šifrování

Symetrické šifrování je založeno na principu jednoho klíče. Tím lze zprávu zašifrovat i odšifrovat. Příkladem symetrického klíče je DES (Data Encryption Standard). Symetrické kódy mají jako hlavní výhodu rychlost algoritmu. Na druhou stranu je nutné, aby se příjemce i odesílatel dohodli na jednom klíči, který budou znát pouze oni dva. Rizikem je tedy distribuce klíče - jak dostat klíč k příjemci, aniž by se ho chopil někdo nepovolaný? Nejbezpečnější je použít jinou cestu předání, než je cesta šifrované zprávy. Rizikem je prozrazení klíče, protože jsou odkryta jím zašifrovaná dat.

Např.: Klíč = 4
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EFGHIJKLMNOPQRSTUVWXYZABCD

Tedy AHOJ = EMSN

Nejznámější typy symetrického šifrování: DES, 3DES.

DES - Data Encryption Standard

DES byl vyvinut v IBM v polovině sedmdesátých let. Roku 1974 byl představen systém "Lucifer" (přejmenován na DEA) a v roce 1976 byl oficiálně přijat jako standard pod názvem DES. DES kryptuje text po 64bitových blocích. Klíč je 64bitový, ale pouze 56bitů je použito pro kódování. Zbylých 8 je kontrolní součet. Přesto, že DES je dobře navrhnutý, jeho 56bitový klíč je slabý vzhledem k dnešním potřebám a standardům. Proto byl vylepšen a zaveden tzv. Triple-DES. Triple-DES je DES, který aplikuje na stejný blok dat 3 klíče. Triple DES je tedy 168bitový.

1.11.2 Asymetrické šifrování

Asymetrické šifrování (kryptografie veřejného klíče), je metoda vyvinuta Whitfieldem Diffiem a Martinem Hellmanem v roce 1975.

Asymetrická kryptografie pracuje s dvojicí klíčů (keypair). Jeden z klíčů (veřejný), se užívá k zašifrování dat a je možné jej zveřejnit. Druhý z klíčů (privátní), je určen k dešifrování. Musí být pečlivě chráněn a musí jej znát pouze jeho majitel. Dvojice privátní/veřejný klíč je navržena tak, že z klíče veřejného není možné žádným způsobem odvodit ani spočítat klíč privátní. To zaručuje, že pouze držitel privátního klíče může zašifrovanou zprávu dešifrovat a získat její obsah.

Výměna zabezpečené (zašifrované) zprávy mezi odesílatelem a příjemcem vypadá následovně: odesílatel zašifruje data veřejným klíčem příjemce a odešle je na adresu příjemce. Příjemce vezme svůj privátní klíč a zprávu rozšifruje.

Hlavní výhodou asymetrického šifrování je, že soukromé klíče jsou pouze u jejich majitelů a vně se pohybují pouze veřejné klíče.

RSA

Algoritmus RSA je pojmenován podle počátečních písmen příjmení jeho autorů: Rivest, Shamir a Adleman. Vypracován byl v roce 1977 a je založen na neschopnosti lidského pokolení vymyslet rychlý algoritmus pro rozklad čísla na jeho prvočinitele. RSA je asymetrická šifra. Pokud tedy máme jen jeden klíč, můžeme buď šifrovat, nebo dešifrovat,

ale ne obojí najednou. RSA patří do skupiny šifer s veřejným klíčem. RSA používá tzv. modulární Aritmetiku. Algoritmus RSA je (zatím) velmi bezpečný, jelikož není znám žádný dostatečně rychlý postup na faktorizaci vysokého čísla. Ovšem nelze dokázat, že takovýto algoritmus neexistuje.

1.12 Výhody a nevýhody magnetických karet

Co se týče výhod a nevýhod magnetických karet, názory autorů se liší. Je to způsobeno aktuálností literatury, případně pojetím dané technologie. Proto uvádím jen ty výhody, které jsou v současnosti aktuální.

Výhody	Nevýhody
Nízká cena	Omezená kapacita dat – dáno délkou proužku (max. 1288 bitů dat)
Snadná identifikace	Nelze číst na dálku potřebuje kontakt
Životnost karty po povrchové úpravě	Karta s pamětí bez vlastní inteligence, s nejnižším stupněm ochrany
Data na 3. vrstvě mohou být změněna	Nedůvěryhodná dat-lehce kopírovatelná.
Imunita vůči kontaktním nečistotám	Snadná zničitelnost, možnost poškození magnetického proužku. Jestliže kartu ponecháme v blízkosti silného magnetického pole, znehodnotíte ji.
Žádná pohyblivé části	Neumí ověřit komunikační prostředí
Dobře zavedené standardy	Závislost na agresivitě prostředí (vlhkost, kyselost, …), odkrytá čtecí hlava
Potřeba hardwaru pro čtení případně zápis dat.	
Lze využít stopy (max 3.) pro různé aplikace	

Tab. 7 *Výhody a nevýhody magnetických karet*

2 POUŽITÍ MAGNETICKÝCH KARET V KOMERČNÍ BEZPEČNOSTI

Jak jsem již zmínil v úvodu, karty s magnetickým proužkem mají široké spektrum využití.

S magnetickou kartou se setkáváme jako:

- kartou kontroly vstupu - karty pro vstup a vjezd i jako součást zabezpečení a sběru dat v objektech (docházkový systém);
- identifikační kartou - především jako průkazy s ochrannými prvky a identifikací držitele;
- hotelové klíče - otevírání dveřních zámků, trezorů;
- kartou stravovacího systémů - použití např. ve školních jídelnách;
- bankovní kartou, karta pro platební sektor - kreditní karty, debetní karty.

V této kapitole jsem použil nabídky systémů od firmy Z-Ware, Entry systems, JSH, Bedex.

Na úvod kapitoly bych vysvětlil základní pojmy:

Identifikace: používají se 4 třídy identifikace (0 – 3)

- **Třída identifikace 0** - žádná přímá identifikace. Je založena na prostém požadavku o přístup bez identity uživatele (tlačítko, kontakt, detektor pohybu aj.)
- **Třída identifikace 1** - informace jsou uložené v paměti, používají se hesla, osobní identifikační čísla aj.
- **Třída identifikace 2** – má identifikační prvek nebo biometrický. Používá identifikační prvky karet, fyzické klíče, otisk prstů aj.
- **Třída identifikace 3** - identifikační prvek nebo biometrie jsou spolu s informací uloženy v paměti. Je založena na používání kombinace identifikačního prvku nebo biometrie a informace uložené v paměti.

2.1 Přístupové systémy

Jednoznačně identifikují zaměstnance pomocí přístupové magnetické karty. Údaj je následně vyhodnocen a podle přístupových práv je umožněn průchod dveřmi, turniketem, bránou, závorou, brankou, atd. Průchody se dále zaznamenávají v uživatelském SW, kde jsou kdykoli k nahlédnutí.

Obr. 18 *Přístupový systém osob*

Proč zavádíme přístupové systémy:

- zavedením přístupových systémů se omezí volný a nekontrolovatelný pohyb osob v určitých prostorách objektů;
- pohyb osob je možno omezit v čase;
- nahradí mnoho klíčů jednou kartou nebo čipem;
- zvýší komfort ovládání;
- zvýší konkurenceschopnost (např. ovládání hotelových pokojů, vstupy do fitcenter, klubů, výtahů);
- umožní přístup pouze vybraným skupinám;

- je možno stanovit sazbu za pobyt v určitých prostorách;
- omezí se pohybu vozidel v areálu.

2.1.1 Klasifikace přístupů uživatelů

Třída přístupu A

Tato třída platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr ani ukládání přístupové transakce. Transakce je událost, která odpovídá uvolněním přístupového místa poté, co byla rozpoznána identita uživatele.

Třída přístupu B

Tato třída platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřídu, která se vztahuje na místo přístupu zahrnující časové filtry, ale bez funkcí ukládání dat (uvolnění přístupového místa poté, co byla rozpoznána identita uživatele).

2.1.2 Základní části přístupového systému

- Řídící jednotka:

Obr. 19 Řídící jednotka

- Čtecí zařízení - čtečka magnetických karet

Obr. 20 *Čtečka magnetických karet*

- Dveřní terminál - využívá se hlavně ke zvýšení komunikační vzdálenosti mezi řídící jednotkou a vlastním čtecím zařízením a dále pak k rozšíření počtu čteček připojitelných k jednotce.
- Akční členy - prvky, které umožňují vstup identifikovaných osob s právem přístupu do hlídaného prostoru přístupovým systémem. Příkladem jsou turnikety, elektromagnetické zámky, závory, atd.
- Záložní zdroj - zařízení sloužící k vlastnímu elektro-mechanickému odblokování dveří a jejich následnému otevření. V převážné většině případů se používá stejnosměrný 12ti voltový nízkoodběrový zámek. Má to velkou výhodu v jednoduchosti zálohy napájení a ušetření elektrické energie v případě většího počtu dveří.

2.1.3 Hotelové systémy

Hotelový systém může kombinovat např. řízení přístupů do budovy (místnosti) pomocí magnetických a čipových karet, pokojové trezory, evidenci pohybu zaměstnanců.

Kartové systémy hotelových zámků

Například hotelový kartový systém HT 24 od firmy Onity, dodávaný firmou Entry Systems. Systém je založen na použití počítače pro rozhraní Ethernet, protokol TCP/IP. Poskytuje možnost nakonfigurování až 5000 originálních uživatelských karet s označením konkrétního uživatele. Dále poskytuje podporu úplného rozvrhu směn zaměstnanců. A audit posledních 100 otevření. Všechny zadlabací zámky Onity jsou panikové tzn., umožňují okamžité opuštění uzamčeného pokoje pouhým stisknutím vnitřní kliky. Funkce, Auto-deadbolt“ navíc umožňuje automatické uzamčení, ke kterému dochází ihned po zavření dveří.

Obr. 21 *Zadlabávací zámky kartového systému Onity HT 24*

Hotelové trezory

Příkladem hotelového trezoru ovládaného hotelovou kartou nebo platební kartou hosta. Tato služba hoteliérů je především ochranou hostů před krádeží a zaměstnanců hotelů před zbytečnými obviněními. Pro příklad v české republice je dodavatelem hotelových trezorů ovládaných magnetickou kartou firma Entry Systems, která dodává trezory značka Onity s označením OS600. Trezor je s rozhraním pro magnetickou kartu s PIN kódem a auditem otevření. Tento jednoduše ovladatelný trezor využívá čtyřmístného kódu ve spojení s pokojovou kartou a zvýšenou bezpečnost dále zaručuje také díky auditu otevření a kódu "Non-resident Master Code". Jako dalšího zahraničního výrobce bych jmenoval Londýnskou firmu JSH Security Marketing.

Obr.22 *Trezor Onity-OS600*

Obr. 23 *Trezor JSH model205*

2.1.4 Parkovací a vjezdové systémy

Systém slouží pro sledování vjezdů a výjezdů vozidel spojené s ovládáním závory či automatických vrat, případně provoz parkoviště. Vjezdy a výjezdy lze povolit na základě identifikace kartou řidiče nebo vozidla na snímacím stojanu, umístěném častou závory.

Po identifikaci proběhne ověření povolení vjezdu a současně, zda je k dispozici volné parkovací místo (často informační tabule). V případě kladného vyhodnocení je vjezd povolen a závora se automaticky zvedne.

Výhody parkovacího systému:

- sledování služebních vozidel;
- kontrola automobilů externích, případně spolupracujících firem;
- možnost povolení vjezdu návštěv;

možnost krátkodobého vjezdu či výjezdu [15]

Obr. 24 *Parkovací systém - Obchodní dům IT Vrchlabí*

2.1.5 Elektronické vstupenky

Papírové vstupenky na koncerty a představení mohou být opatřeny magnetickým proužkem pro kontrolu pravosti. Pokud se jedná o plastové permanentky, bývají zabezpečeny čárovým kódem. U lépe chráněných je systém vstupenek opatřený interním čipem (R/O nebo R/W), který je stoprocentní ochranou proti pokusům o falšování.

2.2 Docházkové systémy

V kapitole čerpal především ze zdroje 15. Docházkový systém jednoznačně identifikuje zaměstnance pomocí karty, čipu, popřípadě biometrických údajů. Docházkový terminál zaznamenává jednotlivé průchody a vlastní uživatelský software je zpracuje a upraví. Konečné výsledky je pak možno přímo importovat do mzdového programu. Zavedení docházkového systému umožní nahradit tzv. píchací hodiny, docházkové sešity a knihy docházky. Slouží k automatickému snímání a evidenci příchodů, odchodů zaměstnanců, přerušení pracovní doby s následným informačním výstupem pro další využití. Odstraní ruční vyhodnocování podkladů a píchacích karet mistrům, vedoucím pracovníkům a mzdovým účetním. Umožní vedoucím pracovníkům okamžitý přehled o svých podřízených pracovnících. Zlepší využití efektivní pracovní doby pracovníků. Identifikace pracovníků je automatizovaná a provádí se magnetickými kartami. Základem docházkového systému je docházkový terminál umístěný na vrátnici, v provozu nebo jiném místě, kde nemůže být poškozen vandaly. Bývá pod dohledem obsluhy nebo kamery. Na docházkovém terminálu je možno zadávat příchod, odchod, služební cestu, služební pochůzku, oběd, nemoc, paragraf, OČR, návštěvu lékaře, náhradní volno, dovolenou a ostatní dle požadavku organizace.

Obr. 25 *Displej docházkového terminálu*

Terminál může být propojen s docházkovým softwarem několika způsoby. Nejčastěji je využíváno sériové rozhraní RS-232, RS-485 a dnes asi nejrozšířenější komunikace po síti (TCP/IP – Ethernet). Nově je nyní možno komunikovat i bezdrátově přes Wi-Fi.

2.2.1 Členění z hlediska způsobu připojení docházkového terminálu s docházkovým softwarem

On-line připojení umožňuje stálé propojení docházkového terminálu a stanice, s průběžným přenosem dat oběma směry (každý průchod terminálem automaticky po zaznamenání odešle ke zpracování).

Off-line připojení dává dočasné spojení terminálu a stanice (přenos dat oběma směry jen po dobu připojení, např. modemem, pomocí diskety nebo přenosného počítače).

On-line Ethernet je docházkový terminál, který komunikuje s PC pomocí Ethernet rozhraní přes protokol TCP/IP. Každý terminál má poté svoji specifickou IP adresu.

On-line Wi-Fi pomocí Wi-Fi modulu připojuje docházkový terminál k Access Pointu nebo klasické Wi-Fi kartě v jakémkoli PC v síti. Terminál má v této variantě opět svoji specifickou IP adresu a komunikuje přes rozhraní TCP/IP.

Komunikace v docházkovém systému probíhá oboustranně (do terminálu – nové osoby, bilance, časové zóny, systémové konfigurace, atd. a z terminálu nové průchody). Všechna data jsou zpracována, přepočítána a uložena docházkovým SW. Pověření pracovníci si poté dle svých přístupových práv prohlížejí či upravují údaje. Buď o všech, nebo pouze o svých podřízených. Úpravy probíhají pomocí klientského software nebo přes webové rozhraní, např. z domova. Docházkový systém je možno rozšířit o přístupové terminály, pomocí nichž se mohou evidovat průchody jednotlivými prostorami, omezit přístupy personálně i v čase. K docházkovému systému mohou být také připojeny turnikety, pomocí nichž se opět vymezí pohyb osob.

Docházkový systém se skládá:

- Docházkový terminál - mozek celého systému

Obr. 26 *Docházkové terminály (z leva) REX a i-REX*

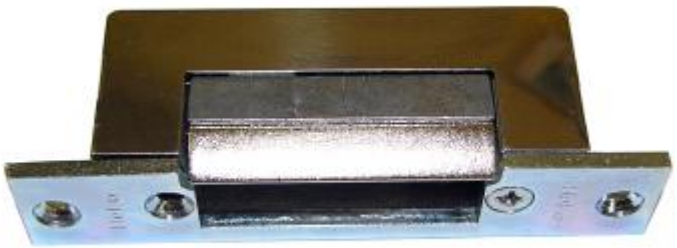
- Dveřní terminál - slouží k rozšíření systému o další vstupní místa. Na základní desce dveřního terminálu jsou svorky, určené pro připojení čteček karet z obou stran dveří a výstupní svorka pro akční členy, jako jsou nízkoodběrový elektromagnetický zámek nebo turnikety. A samozřejmě nesmíme zapomenout na svorky pro sběrnici.

Obr. 27 *Dveřní terminál*

- Vstupní zařízení – čtečky magnetických karet.

Obr. 28 *Čtečka magnetických karet*

- Akční členy - elektromagnetické zámky, turnikety – umožňují nám propustit osoby do objektu.



Obr. 29 *Akční členy*

- Záložní zdroj- Při výpadku elektrické energie napájení zabezpečí záložní zdroj. Doba zálohy se pohybuje podle typu zdroje a dané aplikace od 5 do 24 hodin. Zdroje používáme převážně spínané, které se vyznačují nezanedbatelnou úsporou spotřebované energie. Zdroj se skládá ze síťového napáječe s atestem, elektroniky pro stabilizaci napětí a dobíjení baterie, informačních LED diod, pojistky a záložní baterie. Baterie je 12ti voltová a kapacita se volí podle odběru dané aplikace. V případě větších odběrů lze též použít baterie dvě, případně bateripack. Uložená

data o průchodech jsou v terminálu v zálohované paměti. Velikosti paměti 32KB až 512 KB, což znamená přibližně 4000 až 64000 průchodů.

Obr. 30 *Záložní zdroj*

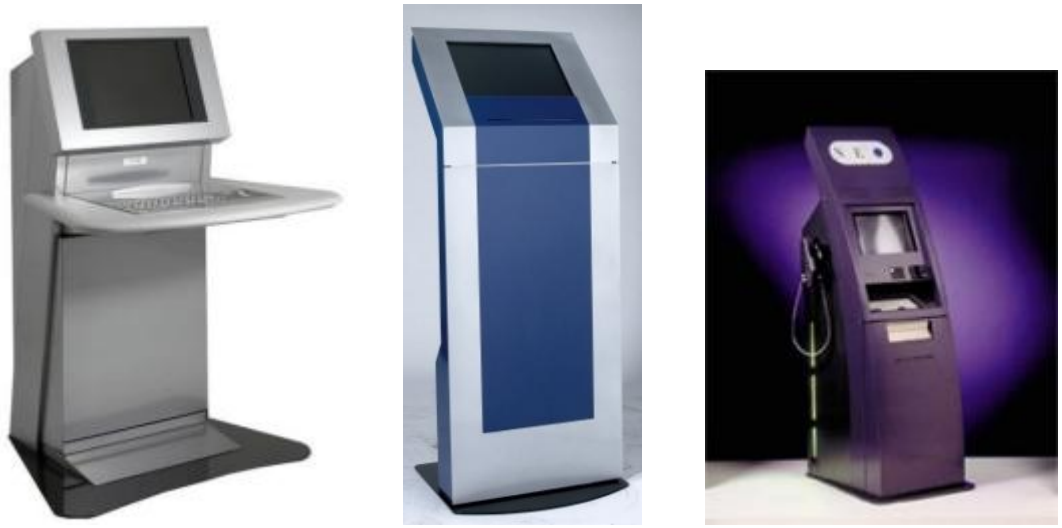
2.2.2 Stravovací systémy

Modifikací docházkového systému jsou stravovací systémy zabezpečující služby pro provoz hromadného stravování. Systém pokrývá problematiku zajištění distribuce stravy včetně vyúčtování stravy mezi jídelnou a podniky. Systém zároveň vytváří podklady pro vyúčtování odebrané stravy s ohledem na pravidla dotování pro zaměstnance ve mzdách. Použitím stravovacího systému zabráníme čerpání neoprávněných příspěvků zaměstnavatele na stravu, zjednodušíme objednání a výdej stravy strávníkům. Výstupy systému umožňují provádět kvalifikovaná rozhodnutí podle přesných a obsáhlých informací.[15]

2.3 Samoobslužné kiosky

Samoobslužné kiosky se dávají tam, kde je potřeba se informovat bez obsluhy. Kiosky jsou vybavené proti vandalství odolnou dotykovou tlačítkovou klávesnicí nebo dotykovým displejem bez klávesnice. Vybavují se jimi místa, kde je vyžadován terminál pro snadné užívání v sedící nebo stojící pozici a umožňuje přístup i vozíčkářům. Samoobslužné kiosky nabízí vysokou úroveň přizpůsobivosti a robustnosti. Kiosky jsou modulární konstrukce, kterou lze vybavit dotykovou obrazovkou, A4 nebo pokladní tiskárnou, scannerem,

motorizovanou vysouvací čtečkou karet magnetické karty/čipové karty karty, stereo sluchátky a reproduktory.



Obr. 31 *Samoobslužné kiosky*

2.4 Bankovní karta

S magnetickým proužkem se na bankovních kartách setkáváme již přes půl století. S postupem technologii stále dopředu máme u sebe každý minimálně jednu kartu, která obsahuje magnetický proužek, ale i čip (kontaktní nebo bezkontaktní). Platební karty v Evropě plní standardy EMV, a jsou vydávány jako karty hybridní. Pouze čipové karty se v Evropě nevyskytují. Platební standardy EMV je zkratka složena z počátečních názvů asociací Europay, MasterCard a Visa, které stály u zrodu myšlenky čipové platební karty a definovaly standardy toho, jak má taková platební karta fungovat. Vzhledem k množství platebních karet a množství akceptačních zařízení nemůže změna na čipovou technologii proběhnout jednorázově, jako velký třesk. Právě postupnost, tzv. migrace na EMV, si vyžádala kombinaci staré a nové technologie a tedy hybridní karty. Díky magnetickému proužku se svojí čipovou kartou zaplatíte či vyberete peníze i tam, kde bankomat nebo terminál s čipovou kartou zatím nepracuje.

U bankovních karet se používají pouze první dvě stopy magnetického proužku. Na obou stopách je datový prvek, který využívá bezpečného kryptografického procesu k ochraně integrity dat v proužku a odhaluje jakékoliv pozměnění nebo padělání (samozřejmě ne při kopírování). Označován zkratkami CVC, CVV. Zkratka CVC - Card Verification Code

toto označení používá společnost MasterCard nebo CVV - Card Verification Value toto označení používá společnost VISA. Třetí Stopa je nevyužitá, používala se pro výběr hotovostí nebo plateb za zboží, které byli v režimu off-line (nebyli připojeny přímo do banky). Na tuto stopu se ukládal zůstatek limitu karty, datum pro obnovení limitu a v šifrované formě PIN.

Obr. 32 *Bankovní platební karta e-Banky*

2.4.1 Zabezpečení platby kartou bez fyzické přítomnosti karty

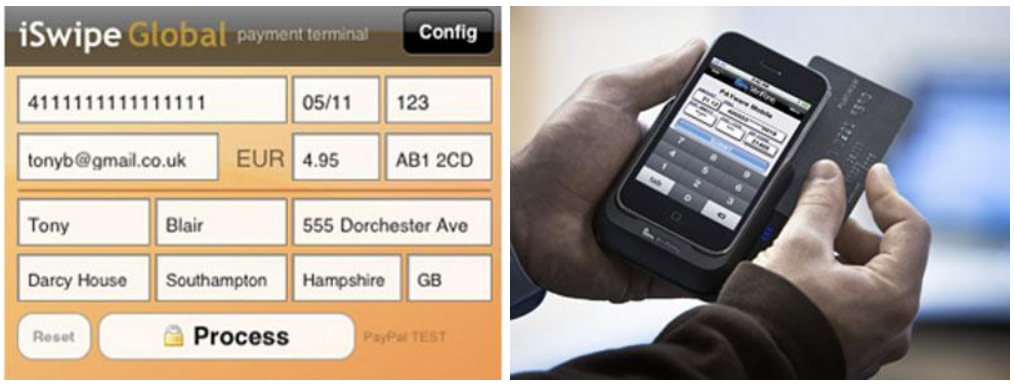
Platby přes Internet nejsou problém, otázkou je jejich bezpečnost. Přenos citlivých informací přes nebezpečné médium se vyřešilo používáním zabezpečených protokolů, nejběžnější je SSL. Nejvyšší stupeň zabezpečení poskytuje protokol 3D Security reprezentovaný pod značkami CVC2 (Card Verification Code toto označení používá společnost MasterCard) nebo CVV2 (Card Verification Value toto označení používá společnost VISA). Pokud internetový obchod používá tuto formu zabezpečení, dostanou se údaje o platební kartě pouze bance, se kterou má obchodník uzavřenou smlouvu. Samotný obchodník pak dostane údaje týkající se pouze objednávky. Jedná se tedy o nejbezpečnější placení kartou na internetu.

2.4.2 Platby přes mobilní telefon se čtečkou magnetických karet

K mobilnímu telefonu iPhone od společnosti Aplle můžeme připojit čtečku magnetických karet. Čtečka se připojí do sluchátka. Pracuje se speciálním softwarem na transakce s kreditní kartou včetně digitálních podpisů.

Obr. 33 *Mobilní telefon iPhone od firmy Aplle s připojenou čtečkou karet.*

Telefony od firmy Aplle iPhone 3G nebo iPhone 3GS, modifikované firmou Mophie, umožňuje přijímat a posílat platby. Mobilní telefon obsahuje čtečku magnetických karet přímo v těle telefonu. Bezpečnost je zaručena, díky okamžitému šifrování dat z karty. Nikde se data neukládají.



Obr. 34 *Mobilní telefon iPhone od firmy Aplle s integrovanou čtečkou magnetických karet.*

2.5 SROVNÁNÍ S JINÝMI SYSTÉMY

Vedle magnetických karet existují i další prostředky identifikace. Mezi nejznámější patří optické systémy, čipové systémy (kontaktní, bezkontaktní), v neposlední řadě biometrické systémy. Pokusíme se o srovnání jejich vlastností a aplikačního nasazení.

2.5.1 Karty s čárkovým kódem

Neumí ověřit identitu okolí, se kterým komunikuje (osoby, technické nebo programové prostředky). Aktualizace údajů čárového kódu není možná. Ochrana dat před zneužitím šifrování možná je. Kód je možné kopírovat, stačí kopírka na 1D a 2D kódy. Přístup k datům je možný jen pro oprávněné držitele, a jen v případě šifrovaní dat média. Čtení karty s čárovým kódem je bezkontaktní ze vzdálenosti do jednoho metru (dražší řešení). Cena média s čárovým kódem je nižší než u magnetických karet. Umožňuje bezpečně a dlouhodobě uchovávat údaje na identifikačním mediu. Spolehlivost čtení bývá vysoká. Datová kapacita identifikačního media může být až několikanásobně vyšší. Velkou nevýhodou je nutnost umístění snímače tak, aby byl dobře a volně přístupný pro vložení karty, tím je i volně přístupný vandalům. Nevýhodný je i samotný fakt, že při každém průchodu či příjezdu, musíme vytahovat kartu. Automatická identifikace je umožněna v případě umístění čárového kódu na stejné viditelné místo.

2.5.2 Čipové karty kontaktní

Umožňuje inteligentní rozhodování, bezpečně a dlouhodobě uchovávat údaje. I ověřit identitu okolí, se kterým komunikuje (osoby, technické nebo programové prostředky). Podporuje kryptografické operace (elektronický podpis). Umožňuje aktualizace již zapsaných údajů i ochranu dat před zneužitím šifrováním. Vyloučení neoprávněného přístupu do chráněné oblasti paměti. Není možné kopírování údajů v paměti. Přístup k datům je jen pro oprávněné držitele. Rozlišuje úrovně přístupu pro různé držitele. Čipové karty mohou obsahovat jednu nebo několik aplikací. O tom kolik aplikací bude a v jakém rozsahu, je nutné rozhodnout od počátku přípravy technického vybavení karty. Aplikace pak lze přidávat postupně. Pro zajištění efektivnosti využití jsou aplikace ukládány vedle sebe na tomtéž čipu. Při několikanásobném zadání špatného pinu se karta zablokuje. K samozničení čipu dochází při výrobě duplikátů. Každý čip má své nezaměnitelné výrobní číslo. Cena čipové karty je vyšší.

Spolehlivost čtení z čipu bývá velmi často střední. Čipová karta se čte kontaktně, tím vzniká mechanické opotřebení čipové karty i čtečky. Datová kapacita identifikačního media je několikanásobně vyšší. Velkou nevýhodou je nutnost umístění snímače tak, aby byl dobře a volně přístupný pro vložení karty a tedy je i volně přístupný vandalům. Při každém průchodu či příjezdu musíme vytahovat kartu a protahovat ji snímačem.

Automatická identifikace není možná. Využití je daleko větší než u magnetických karet (SIM karta, bankovní karta, atd.). Nevýhoda je potenciální šíření virů nebo červů.

2.5.3 Čipové karty bezkontaktní

Má téměř ty samé vlastnosti, jako čipové karty kontaktní. Čipové karty bezkontaktní nemají kontakt se čtečkou. Z toho plyne, že karta se neopotřebovává čtením ani zápisem. Spolehlivost čtení z čipu bývá vysoká. Pracuje na radiofrekvenčním principu. Má dosah do 10 metrů. Výhoda je, že nemusíte při každém průchodu vytahovat kartu, ale čtečka ji načte i přes oděv nebo tašku. Další výhoda je možnost automatické identifikace, objekt může jet rychlostí až 3 m/s a bude identifikován. Nevýhody karet jsou nemožnost embosování., možnost sledování pohybu osob. A jako každý radiový kmitočet je tu možnost odposlechu.

2.5.4 Biometrie

Biometrie využívá specifických charakteristik člověka, jako jsou otisky prstů, oční sítnice, oční duhovka, hlas, podpis, tvář, krevní řečiště ruky a kůže. Biometrická identifikace je mnohem bezpečnější a uživatelsky pohodlnější. Výhody biometrie jsou neoklamatelnost (ale ne na 100 %), nulové provozní náklady (žádná režie spojená s identifikačními médii - karty), rychlost, praktičnost (není co nosit ani ztrácet), spolehlivost (osvědčené technologie). Cena je příznivá ve vztahu k bezpečnosti a neexistujícím dodatečným nákladům. Nevýhoda je nemožnost uložení dat. Neuniverzálnost, předpokládá se u každé osoby, že má daný rys. Šum v získaných datech způsobí špína na snímačích, špatné světlo vede až k odmítnutí povoleného uživatele. Dada nasnímaná se mohou značně lišit od dat v databázi (jiný úhel hlavy). Dalším rizikem je možnost oklamat fotkou obličeje, otisk prstu razítkem (záleží na snímači).

II. PRAKTICKÁ ČÁST

3 NÁSTROJ PRO ZJIŠŤOVÁNÍ INFORMACÍ NA MAGNETICKÝCH KARTÁCH

Z předchozích kapitol víme, jakým způsobem jsou data na magnetické kartě zaznamenána.

3.1 Zadání úkolů projektu

- Pro zjištění informací na magnetických kartách použijeme čtečku magnetických karet.
- Popíšeme instalaci softwaru.
- Popíšeme software ke zjišťování informací z magnetických karet (dodávaný se čtečkou).
- Zjistíme všechny dostupné informací z magnetických karet.
- Vyzkoušíme destruktivní metody pro bezpečnost dat na kartách.

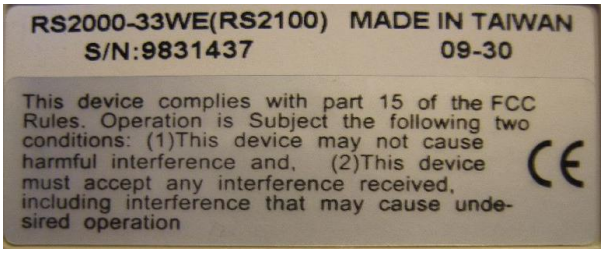
3.2 Realizace projektu

Pro realizaci projektu jsem zakoupil čtečku magnetických karet od firmy Vikintek, typ RS2000-33WE.

3.2.1 Parametry čtečky

Čtečka magnetických karet má tyto vlastnosti:

Čtení 1. - 3. stopy magnetického proužku, nízká a vysoká coervicita karty(300 až 4000Oe), formát záznamu je ISO 7811, velikost čtečky je 90mm x 34mm x 28mm, spotřeba energie 5,5 mA, typy rozhraní jsou RS-232, snímá od 12,5 cm/sec. do 125 cm/sec., čte obousměrně, operační teplota je 5°C až 55°C, skladovací teplota -30°C až 65°C, relativní vlhkost je 0 až 95%, nekondenzující, životnost čtecí hlavy je 500.000 průchodů.



Obr. 35 *Přístrojový štítek RS2000-33WE*

Obr. 36 *Čtečka RS2000-33WE s konektorem Canon 9M*

3.2.2 Instalace softwaru

Abychom mohly používat čtečku, musíme nainstalovat software a ovladače.

Postup instalace:

Po spuštění autorunu se ukáže nabídka s možnostmi instalace software pro různé typy čteček s různými rozhranními. My vybereme typ RS2100 .

Obr. 37 *Instalace krok 1*

Po výběru začne probíhat samotná instalace. Ocitneme se v nastavení instalačního programu, který nás upozorňuje, že při instalaci nemůžeme instalovat ani aktualizovat,

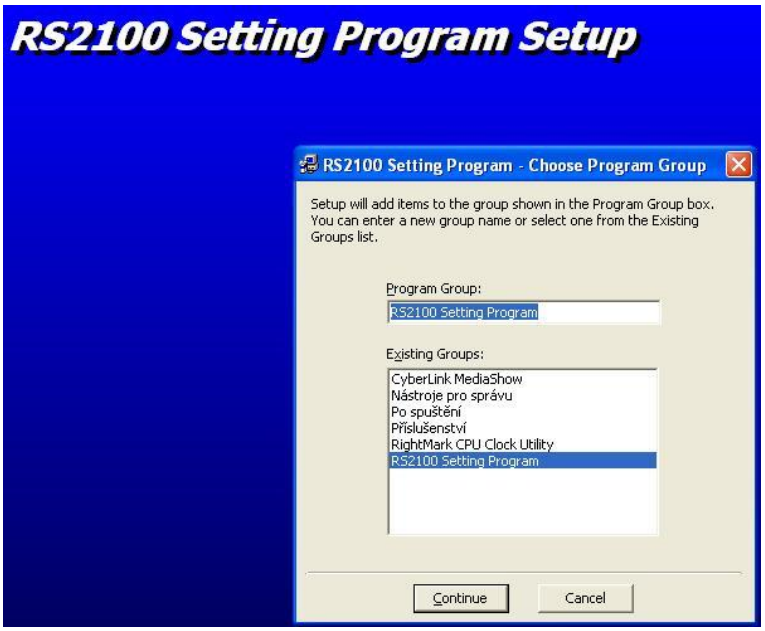
jestliže jsou data (soubory) používány. Před instalací doporučujeme zavřít běžící aplikace. Potvrdíme OK.

Obr. 38 *Instalace krok 2*

Instalační program nás dále vyzívá, abychom pro instalaci klikli na tlačítko níže. Upozorňuje nás, že při kliknutí na tlačítko instalovat, bude program nainstalován do níže určeného adresáře. Pro změnu adresáře můžeme využít tlačítko Change Directory. Klikneme na tlačítko instalace.

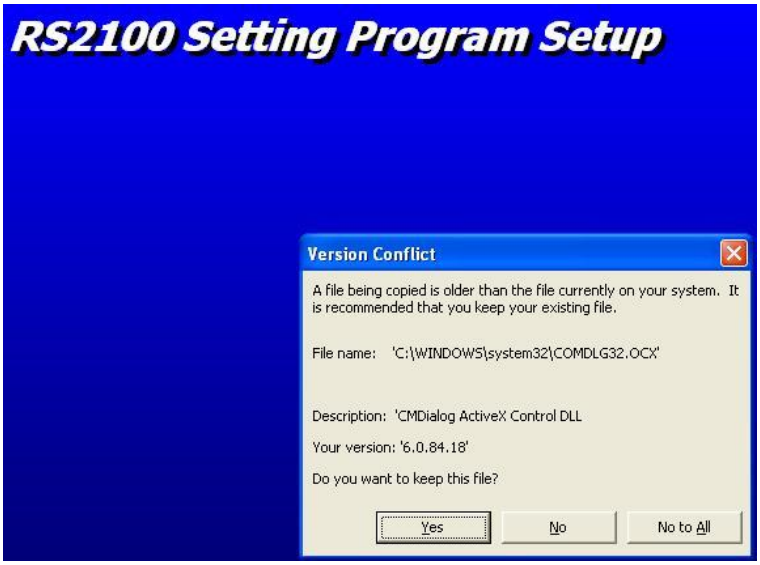
Obr. 39 *Instalace krok 3*

V dalším kroku se instalační program ptá, jak chceme pojmenovat skupinu v nabídce start. Do nabídky Start-Programy můžeme zadat nový název skupiny, nebo vybrat ze stávajících v seznamu. Klikneme na Continue.



Obr. 40 *Instalace krok 4*

Instalace může přinést komplikace ve smyslu, soubor který mám v počítači je novější než soubor v instalačním programu. Doporučuje, abychom ponechali stávající soubor.



Obr. 41 *Instalace krok 4-1*

V posledním kroku nás informuje, že nastavení je kompletní a instalace proběhla úspěšně.

Obr. 42 *Instalace krok 5*

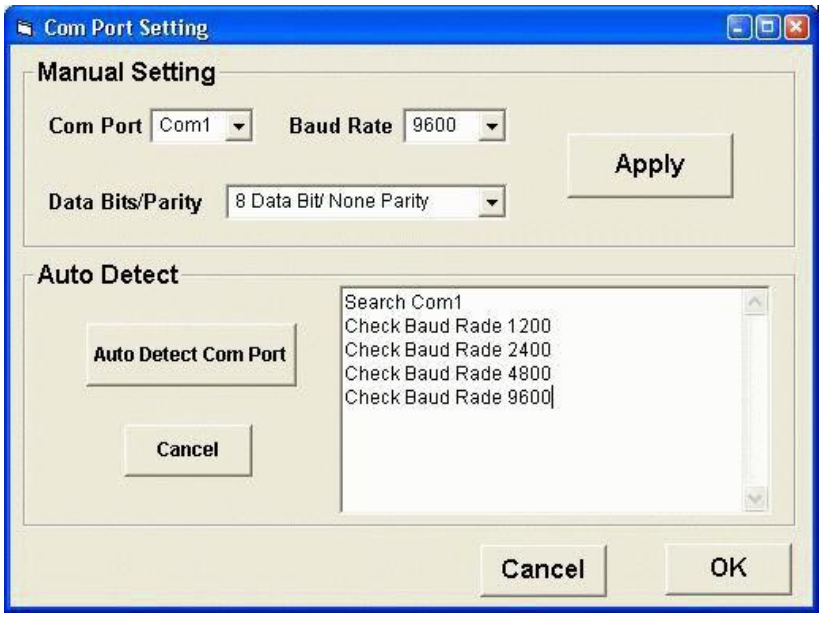
3.2.3 Nastavení software RS2100 Setup Program- Detekce a nastavení hardwaru

Nyní můžeme program RS2100 Setup Program spustit.

Obr. 43 *Software RS2100 Setup Program*

Máme spuštěný program, musíme pro správnou funkci zařízení spárovat čtečku připojenou do portu Com1 s programem. Klikneme v hlavní programové nabídce na položku ComPort(C) a vybereme v nabídce Auto Detect (automatická detekce). V Okně Com Port

Setting klikneme na tlačítko Auto Detect Com Port. Nám se povedlo detekovat čtečku na portu Com1 s maximální přenosovou rychlostí 9600 baud. Přenosová rychlost 9600 Baud znamená, že za 1s můžeme poslat maximálně 9600/10=960 bajtů (číslo 10 odpovídá jednomu start bitu, 8 datovým bitům a jednomu stop bitu).



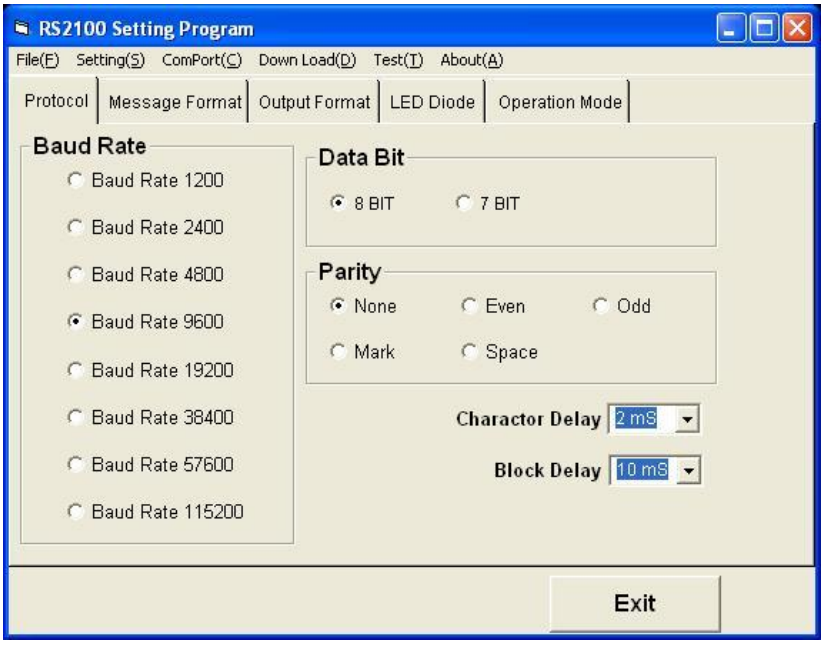
Obr. 44 *Autodetekce čtečky*

3.2.4 Nastavení software RS2100 Setup Program- Nastavení parametrů čtečky

Nastavení čtečky je možno buď uložit, nebo načíst souborem s příponou "set". Klikneme v hlavní nabídce na "Setting (S)". Otevřou se záložky:

Protokol

- Výchozí nastavení: Přenosová rychlost: 9600, Parita: Žádná, Data bit: 8
- Charakter Delay - je zpoždění před odesláním dalších znaků do počítače. Lze to použit, když je váš software pomalý při zpracování klávesnicových dat. Můžeme volit v rozmezí od 1 ms do 100ms.
- Blok Delay - je zpoždění před odesláním dalšího bloku dat do počítače. Lze to použit, když je váš software pomalý při zpracování klávesnicových dat. Můžeme volit v rozmezí od 0 ms do 990 ms.



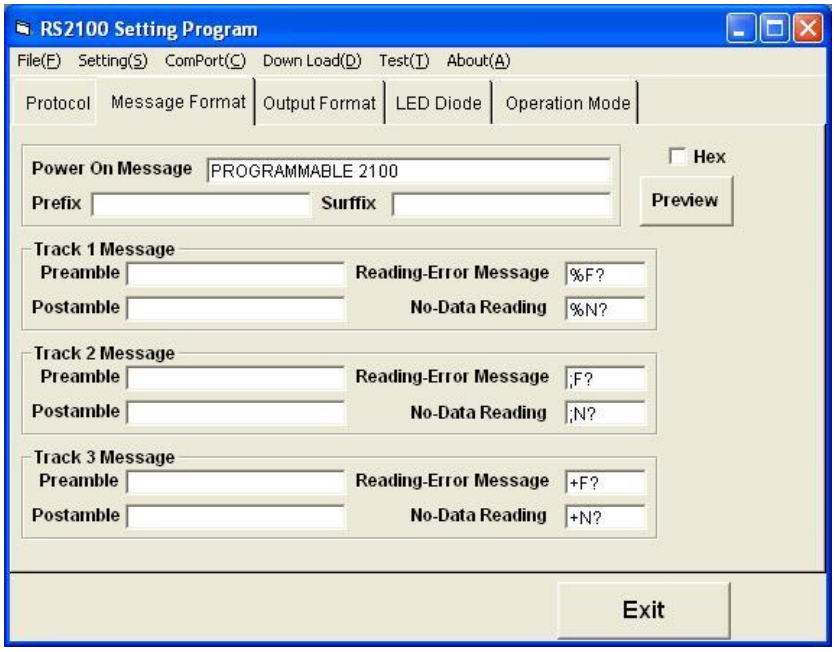
Obr. 45 *Záložka protokol*

Message Format

- Zpráva může být definována řetězcem ASCII nebo HEX znaků.
- Power-On message(úvodní zpráva) má až 17 znaků, lze ji definovat. Výchozí hodnota je PROGRAMMABLE 2100.
- Prefix (znaky přidané na začátek stopy dat), Suffix(znaky přidané na konec stopy dat), Preamble (znaky přidané na začátek stopy bloku dat), Postamble message (znaky přidané na konec stopy bloku dat), lze definovat až 9 znaky.
- Reading-Error, No-Data Reading message, lze definovat až 3 znaky.
- Preview - klikněte na Preview, zobrazí se náhled zprávy a výstupní formát (jak bude vypadat).

Příklad:

<Prefix Message><Preamble Message><Data Block 1><Postamble message><Preamble Message><Data Block 2><Postamble message><Preamble Message><Data Block 3> <Postamble message><Suffix Message>.



Obr. 46 *Message Format*

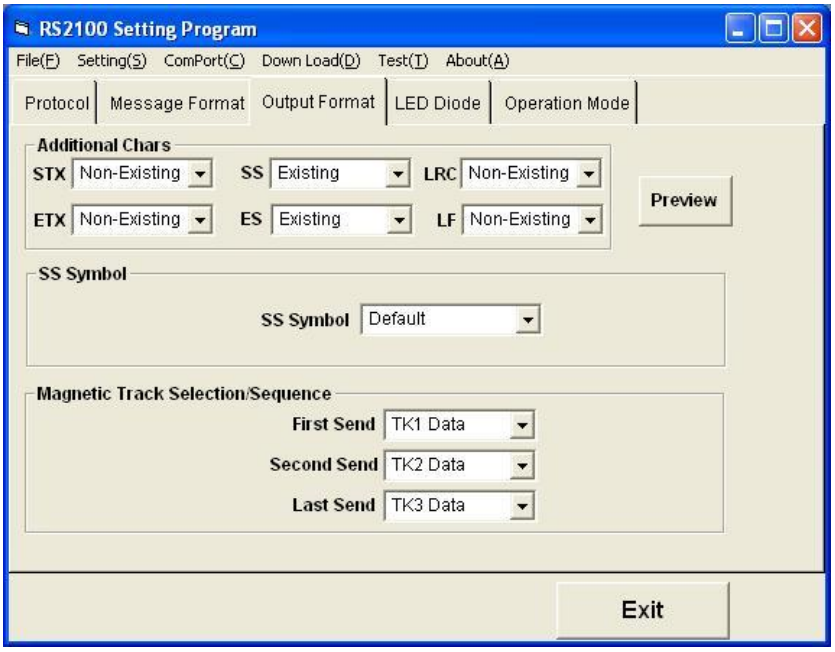
Output Format

- Additional Chars (přídavné znaky) - STX (začátek textu), ETX (konec textu), SS (začátek stopy), ES (konec stopy), LRC(langitudiální redundanční znak), LF (redundantní znak), je možno zvolit Exist nebo Non-Exist
- SS Symbol – máme na výběr ze dvou typů startovacích symbolů podle ISO.

SS		ES	Popis
Default	Originál		
%	%	?	1.stopa
;	;	?	2.stopa
+	;	?	3.stopa-ISO
#	%	?	3.stopa-AAMVA
!	!	?	3.stopa-CA DMV

Tab. 8 *Znak SS pro stopu*

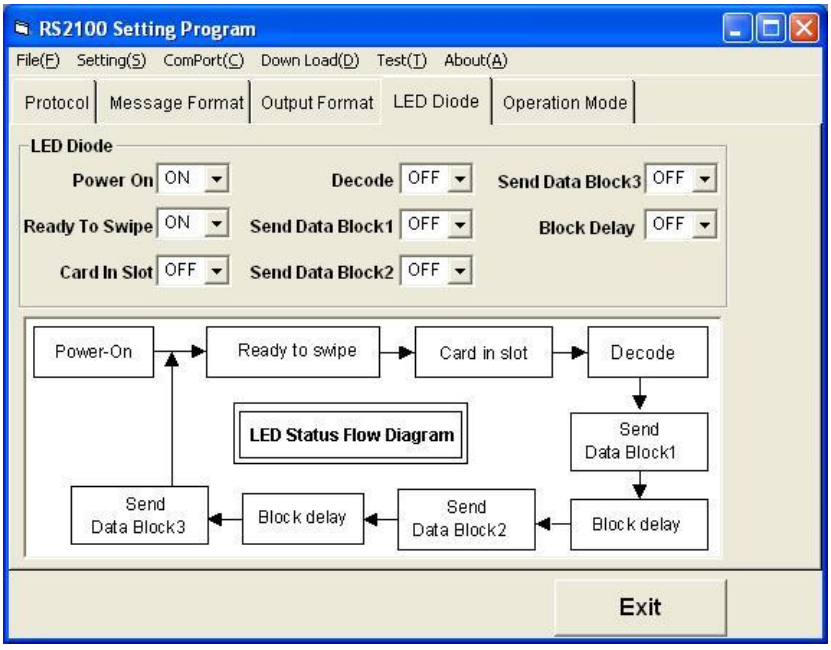
- Magnetic Track Selection / Sequence (pořadí stop) - díky této oblasti nastavení můžeme posloupnost načtení stop měnit nebo i některou stopu vynechat.



Obr. 47 *Output Formát*

LED Diode

Nastavení nám umožňuje určit, při jaké činnosti bude led dioda svítit a při jaké svítit nebude.

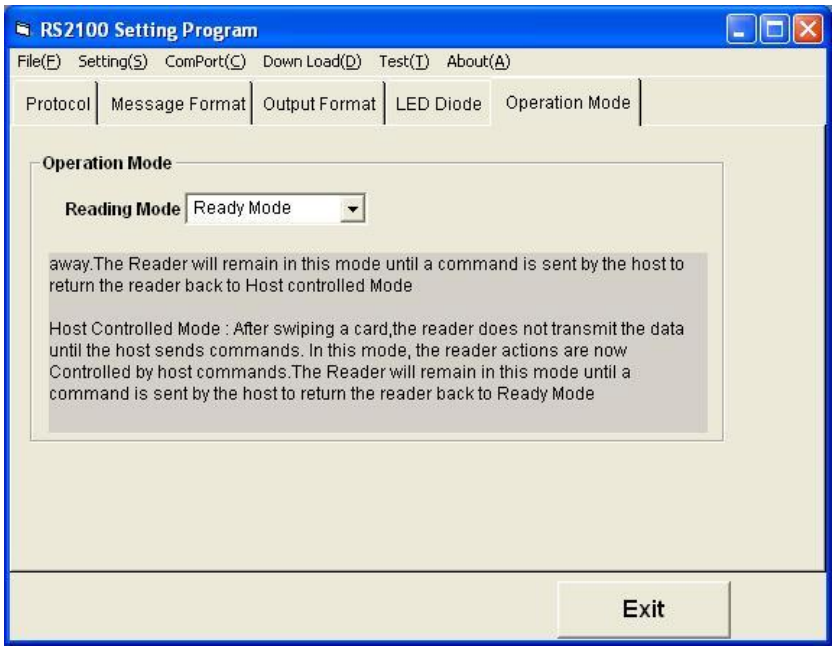


Obr. 48 *LED Diode*

Operation Mode

Existují dva druhy modů:

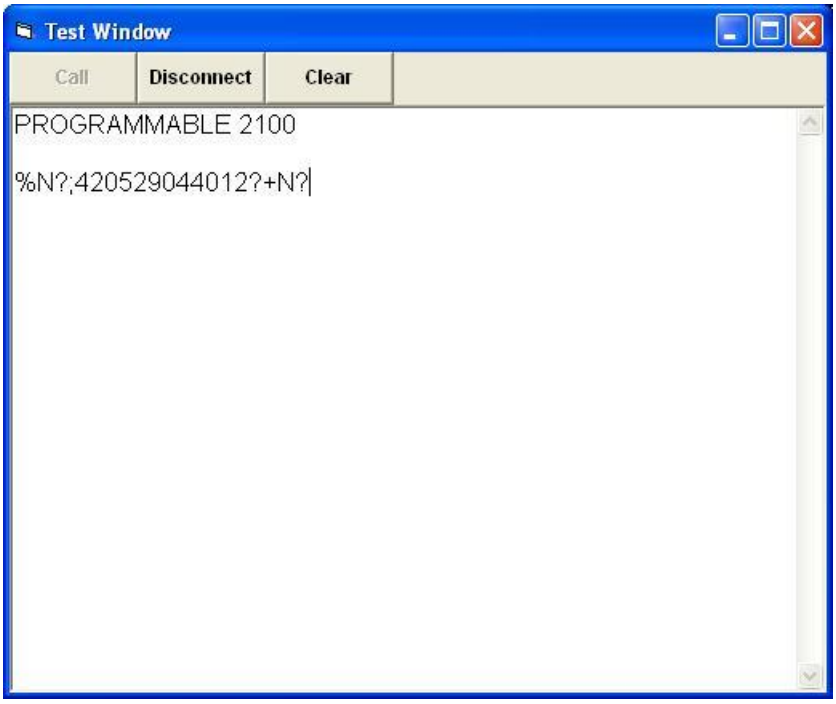
- Ready Mode (výchozí) - čtečka odesílá data do počítače ihned, jakmile magnetická karta projde čtečkou. Jinými slovy, čtečka je vždy připravena magnetickou kartu přijmout.
- Command Mode- po průchodu karty čtečkou se data nepřenáší do počítače (zůstává nečinná). Řídí se pouze příkazy z počítače. Čtečka v tomto režimu zůstává, dokud není změněn její operační mód na Ready Mode.



Obr. 49 *Operation Mode*

3.2.5 Testování čtečky RS2000-33WE(RS2100)

Pro ověření funkčnosti klikneme v hlavní nabídce na položku “Test (T)“. Na čtečce se rozsvítí, zelená led dioda. Což znamená, že čtečka je připravená k provozu. Protáhneme-li kartu s nějakými numerickými nebo alfanumerickými znaky, budou zobrazeny v testovacím okně takto:



Obr. 50

Začátek první stopy '%', a konec první stopy '?'.

Začátek druhé stopy ';', konec druhé stopy '?'.

Začátek třetí stopy ‘+’, '#' (AAMVA), '!' (CA DMV), konec třetí stopy '?'.

Tímto je celé nastavení softwaru ukončeno a můžeme se pustit do testování magnetických karet.

3.2.6 Zjišťování informací z magnetických karet

Karta číslo 1

Obr. 51 *Karta č. 1*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B5264479513807772^CHLUPAC/ALES^0809121000000155874200000000000?
2.stopa	;5264479513807772=08091210000001558742?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
52644795138077	Číslo karty
^	Oddělovač
CHLUPAC/ALES	Příjmení/Jméno
^	Oddělovač
0809	Datum platnosti (09/2008)
121	Servisní kód MasterCard
000000	Výplň
1558742	Nepodařilo se zjistit
00000000000	Výplň
?	Konec
Popis 2. stopy	
;	Začátek stopy
52644795138077	Číslo karty
=	Oddělovač
0809	Datum platnosti (09/2008)
121	Servisní kód MasterCard

000000	Výplň
1558742	Nepodařilo se zjistit
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 9 *Karta č.1*

Karta číslo 2

Obr. 52 *Karta č. 2*

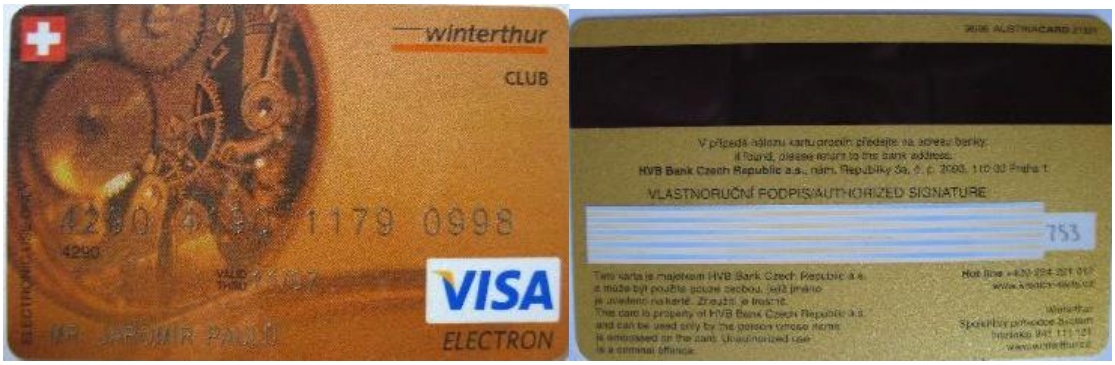
Po protažení čtečkou jsme zjistili následující data:

1.stopa	%N?
2.stopa	;7004320612140921 8=3462?
3.stopa	+N?
Popis 1.stopy	
%	Začátek stopy
N	Žádná data
?	Konec stopy
Popis 2.stopy	
	Začátek stopy
7004320612140921	Číslo karty
=	Oddělovač
3462	Zákaznický číslo
?	Konec stopy
Popis 3.stopy	
%	Začátek stopy

N	Žádná data
?	Konec stopy

Tab. 10 *Karta č.2*

Karta číslo 3



Obr. 53 *Karta č. 3*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B4290419011790998^PAULU/JAROMIR.MR ^07111211453700000000000 793000000?
2.stopa	;4290419011790998=07111211453779300000?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
4290419011790998	Číslo karty
^	Oddělovač
PAULU/JAROMIR.MR	Příjmení/Jméno
^	Oddělovač
0711	Datum platnosti (11/2007)
121	Servisní kód VISA
1	PVKI: Indikátor čísla PIN
4537	PVV: PIN
0000000000	Výplň
793	CVV: Ověřovací kód karty
000000	Výplň
?	Konec stopy
Popis 2. stopy	

;	Začátek stopy
4290419011790998	Číslo karty
=	Oddělovač
0711	Datum platnosti (11/2007)
121	Servisní kód VISA
1	PVKI: Indikátor čísla PIN
4537	PVV: PIN
793	CVV: Ověřovací kód karty
00000	Výplň
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 11 *Karta č. 3*

Karta číslo 4

Obr. 54 *Karta č. 4*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B5435541700121814^PAULU/JAROMIR^0406101 0865103073453000000000000000000000000?
2.stopa	;5435541700121814=04061010865103073453?
3.stopa	+N?
Popis 1.stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
5435541700121814	Číslo karty

^	Oddělovač
PAULU/JAROMIR	Příjmení/Jméno
^	Oddělovač
0406	Datum platnosti (06/2004)
101	Servisní kód MasterCard
0865103073453	Nepodařilo se zjistit
00000000000000000000	Výplň
?	Konec stopy
Popis 2.stopy	
;	Začátek stopy
5435541700121814	Číslo karty
=	Oddělovač
0406	Datum platnosti (06/2004)
101	Servisní kód MasterCard
0865103073453	Nepodařilo se zjistit
?	Konec stopy
Popis 3.stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 12 *Karta č. 4*

Karta číslo 5

Obr. 55 *Karta č. 5*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B5435543700597340^JAROMIR/PAULU^10021010642303 28312900000000000?

2.stopa	;5435543700597340=10021010642303283129?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
543554370059734	Číslo karty
^	Oddělovač
JAROMIR/PAULU	Jméno/Příjmení
^	Oddělovač
1002	Datum platnosti (02/2010)
101	Servisní kód MasterCard
0642303283129	Nepodařilo se zjistit
00000000000	Výplň
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy
543554370059734	Číslo karty
=	Oddělovač
1002	Datum platnosti (02/2010)
101	Servisní kód MasterCard
0642303283129	Nepodařilo se zjistit
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 13 *Karta č. 5*

Karta číslo 6

Obr. 56 *Karta č. 6*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%N?
2.stopa	;360137848?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
N	Žádná data
?	Konec stopy
Popis 2.stopy	
;	Začátek stopy
360137848	Číslo karty
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 14 *Karta č. 6*

Karta číslo 7

Obr. 57 *Karta č. 7*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%N?
2.stopa	;360137839?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
N	Žádná data
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy
360137839	Číslo karty
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 15 *Karta č. 7*

Karta číslo 8

Obr. 58 *Karta č. 8*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B6763690015829544^VONDROUS/ONDREJ^0801121082440022495800 00000000?
2.stopa	;6763690015829544=08011210824400224958?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
6763690015829544	Číslo karty
^	Oddělovač
VONDROUS/ONDREJ	Příjmení/Jméno
^	Oddělovač
0801	Datum platnosti (01/2008)
121	Servisní kód MasterCard
0824400224958	Nepodařilo se zjistit
0000000000	Výplň
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy
6763690015829544	Číslo karty
=	Oddělovač
1002	Datum platnosti (01/2008)
121	Servisní kód MasterCard
0824400224958	Nepodařilo se zjistit
?	Konec stopy
Popis 3. stopy	

+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 16 *Karta č. 8*

Karta číslo 9

Obr. 59 *Karta č. 9*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B5577110162288699^PAULU/JAROMIR^090652100000064 3061100000000000?
2.stopa	;5577110162288699=09065210000006430611?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
5577110162288699	Číslo karty
^	Oddělovač
PAULU/JAROMIR	Příjmení/Jméno
^	Oddělovač
0906	Datum platnosti (06/2009)
521	Servisní kód VISA Electron
000000	Výplň
06430611	Nepodařilo se zjistit
00000000000	Výplň
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy

5577110162288699	Číslo karty
=	Oddělovač
0906	Datum platnosti (06/2009)
521	Servisní kód
00000	Výplň
06430611	Nepodařilo se zjistit
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 17 *Karta č. 9*

Karta číslo 10

Obr. 60 *Karta č. 10*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%N?
2.stopa	;420529044012?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
N	Žádná data
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy
420529044	Číslo karty
012	Nepodařilo se zjistit (pravděpodobně ověření)

?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 18 *Karta č. 10*

Karta číslo 11

Obr. 61 *Karta č. 11*

Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B4729430019461889^VONDROUS/ONDREJ^1004 2011744100495000000??
2.stopa	;4729430019461889=10042011744149506682?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
4729430019461889	Číslo karty
^	Oddělovač
VONDROUS/ONDREJ	Příjmení/Jméno
^	Oddělovač
1004	Datum platnosti (04/2010)
2011744100495	Nepodařilo se zjistit
00000	Výplň
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy

4729430019461889	Číslo karty
=	Oddělovač
1004	Datum platnosti (04/2010)
2011744149506682	Nepodařilo se zjistit
00000	Výplň
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 19 *Karta č. 11*

Karta číslo 12

Obr. 62 *Karta č. 12*

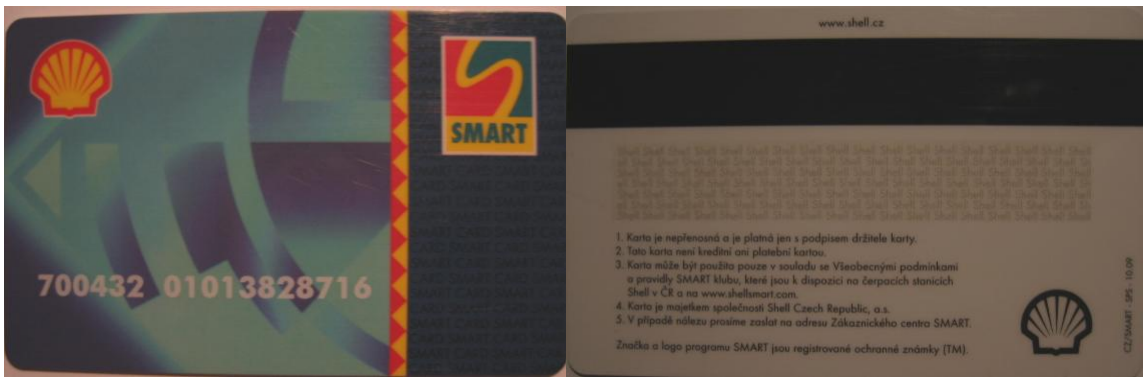
Po protažení čtečkou jsme zjistili následující data:

1.stopa	%B4407522220391993^PAULU/LADA^1104 2061001700723000000?
2.stopa	;4407522220391993=11042061001772302995?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
B	Formát (pro platební karty "B")
4407522220391993	Číslo karty
^	Oddělovač
PAULU/LADA	Příjmení/Jméno
^	Oddělovač
1104	Datum platnosti (04/2011)

20610017007230	Nepodařilo se zjistit
00000	Výplň
?	Konec stopy
Popis 2. stopy	
;	Začátek stopy
4407522220391993	Číslo karty
=	Oddělovač
1104	Datum platnosti (04/2011)
2061001772302995	Nepodařilo se zjistit
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 20 *Karta č. 12*

Karta číslo 13



Obr. 63 *Karta č. 13*

Po protažení čtečkou jsme zjistili následující data:

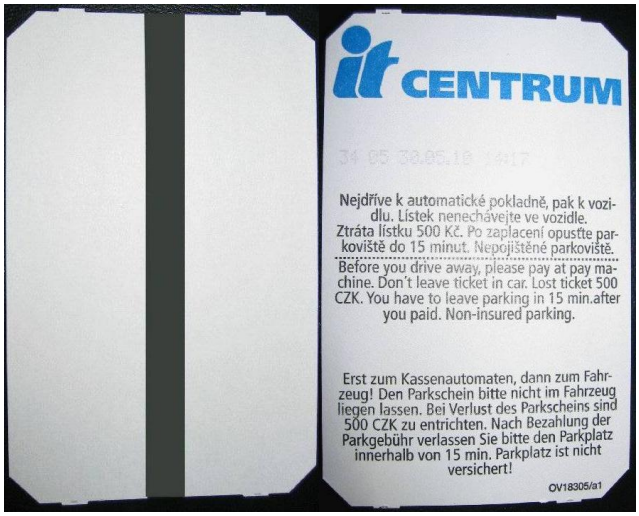
1.stopa	%N?
2.stopa	70043201013828716=?
3.stopa	+N?
Popis 1. stopy	
%	Začátek stopy
N	Žádná data
?	Konec stopy
Popis 2. stopy	

;	Začátek stopy
70043201013828716	Číslo karty
=	Oddělovač
?	Konec stopy
Popis 3. stopy	
+	Začátek stopy
N	Žádná data
?	Konec stopy

Tab. 21 *Karta č. 13*

Karta číslo 14

Karta je z parkovacího systému v obchodním domě IT Centrum, Vrchlabí. Z karty se mi nepodařilo přečíst žádná data. Příčina je v umístění magnetického proužku. Zkoušel jsem kartu různě přehýbat, aby se dostal magnetický proužek na čtecí hlavu, ale bez úspěchu.



Obr. 64 *Karta č. 14*

Vyhodnocení

Zjišťování informací na magnetických kartách je bezproblémově proveditelné. Během pokusů jsem měl 2 krát špatně načtenou stopu. Jednalo se v obou případech o chybu dat na 2. stopě magnetického proužku. Tímto označuji magnetické karty z pohledu spolehlivosti čtení za spolehlivé.

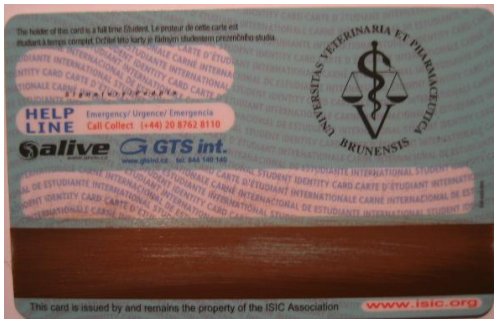
3.2.7 Zkoušky odolnosti magnetického proužku na kartě

Pro destruktivní i nedestruktivní zkoušku jsem vybral několik karet náhodně.

Pokus č. 1 - zkouška odolnosti karty opotřebením

Opotřebení jsem simuloval smilkovým papírem. Na pokus jsem použil kartu číslo 10. Pokus jsem rozdělil do dvou částí.

V první části jsem obrousil vrstvu na magnetickém proužku jen trochu, jak ze zřejmé z obrázku.



Obr. 65 *Odolnost – opotřebení*

Výsledek - data na magnetické kartě byla beze změny, karta byla v pořádku.

Při dalším broušení, kterému byla magnetická karta podstoupena, byla výsledkem absolutní ztráta dat.

Obr. 66 *Odolnost – opotřebení 1*

Pokus č. 2 - zkouška odolnosti karty proti magnetu na pouzdrech

Pouzdrem je myšleno pouzdro na mobilní telefon, kabelky, obaly na brýle, pouzdra na notebooky.

V první části zkoušky jsem byl opatrný, protože jsem se bál zničit kartu hned na první pokus. Proto jsem pomalu přejel jen horní částí magnetického pouzdra od mobilního telefonu. Pro pokus jsem použil karty číslo 8 a 11.

Obr. 67 *Odolnost – pouzdro na mobil*

Výsledek - data na magnetické kartě byla beze změny. Karta byla v pořádku.

V další části pokusu jsem přiložil magnetickou kartu přímo k magnetu.

Obr. 68 *Odolnost – pouzdro na mobil 1*

Výsledek - data na magnetické kartě byla beze změny. Karta byla v pořádku.

Pokus č. 3 - zkouška odolnosti karty proti magnetu

Pro pokus se mi povedlo získat velký magnet. Na pokus jsem použil kartu číslo 11.

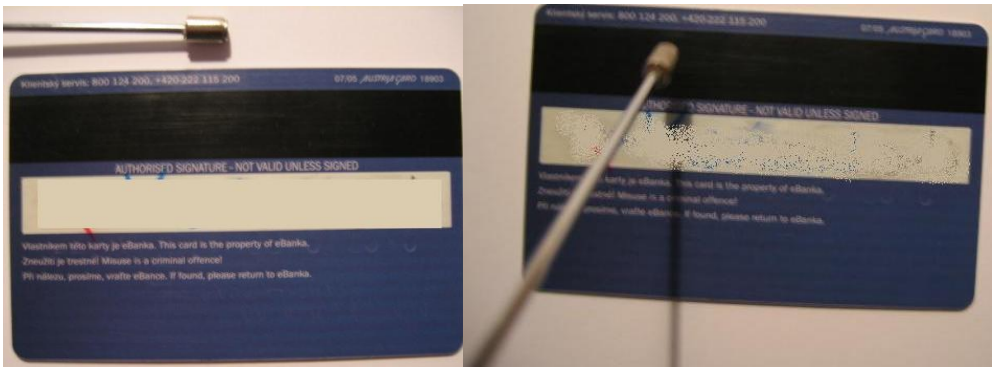
Obr. 69 *Odolnost – magnet*

Výsledek - data na magnetické kartě byli beze změny. Karta byla v pořádku.

Pokus č. 4 - zkouška odolnosti karty proti neodymovému magnetu

Opět jsem postupoval dvoufázově. Na pokus jsem použil kartu číslo 8.

Při prvním pokusu jsem neodymovým magnetem přejel, vlnitým pohybem, po magnetickém proužku.



Obr. 70 *Odolnost – neodymový magnet*

Výsledek - data na magnetické kartě byla beze změny, karta byla v pořádku.

Ve druhé části pokusu jsem projížděl po magnetickém proužku všemi směry.

Výsledek - data na magnetické kartě byla nenávratně znehodnocena.

Pokus č. 5 - zkouška odolnosti karty s obalem proti neodymovému magnetu

Při pokusu jsem důkladně přejížděl přes magnetický proužek po kartě v obalu. K pokusu jsem použil kartu číslo 11.

Obr. 71 *Odolnost – neodymový magnet (karta v obalu)*

Výsledek - data na magnetické kartě byla beze změny, karta byla v pořádku.

Pokus č. 6 - závislost průtahové rychlosti karty na množství přečtených dat čtečkou

Pokus měl myšlenku, že když čtečka kartu nepřečte, tak ne vždy je chyba na čtecím zařízení. Postupoval jsem rychlostí nižší, než je deklarovaná rychlost pro čtení (10 cm/s). Při pokusu byly použity karty číslo 8, 11, 12.

Výsledek - při pokusu jsem zjistil, že první stopa je čitelná vždy, druhá stopa ve všech případech vykazovala chybu (tedy " ;F? "). V neposlední řadě třetí stopa vykazovala, že je stále prázdná(tedy " ;N? "), tím usuzuji, že by ji bylo možné přečíst (v případě zapsaných dat na třetí vrstvě).

Vyhodnocení

Pokus č. 1, který jsem provedl na magnetických kartách, kde jsem zkoumal jejich odolnost proti opotřebení. Pokus byl zajímavý a překvapil mě, že při první části pokusu byla karta čitelná v plném rozsahu, i když místy nebyl vidět vůbec proužek. Jediné možné vysvětlení, které mně napadlo je, že jsem nepoškodil tu část karty, kde data byla zapsána. V druhé části pokusu jsem proužek úplně znehodnotil.

Další část pokusů jsem orientoval do oblasti, před kterou varovala většina literárních zdrojů, a sice zničení uložených dat na magnetickém proužku při přiblížení magnetu. Pokus č. 2 byl uskutečněn na běžně užívaných doplňcích, jakou jsou pouzdra na mobil, pouzdro na brýle, taška na notebook, atd. Tyto pokusy dopadly pro magnetické karty velice úspěšně. Data na magnetickém proužku byla kompletní. Tímto vyvozuji závěr, že magnetickým kartám neškodí námi běžně nošené doplňky (např. pouzdro na mobil).

Pokus č. 3 jsem provedl s velkým magnetem užívaným ve veterinární medicíně, při podezření na cizí těleso v předžaludcích krav. Pokus byl opět úspěšný pro magnetické karty a magnetický proužek byl nepoškozený.

Pokus č. 4 byl proveden s neodymovým magnetem. V první části pokusu jsem projel neodymovým magnetem po magnetickém proužku vlnitým pohybem, data na proužku byla v pořádku. V druhé části pokusu jsem opět projížděl neodymovým magnetem tentokrát důkladně a všemi směry. Výsledek byl, že data na magnetickém proužku byla poškozená. To ukazuje, že proti mírnému vystavení neodymovému magnetu jsou data na kartě odolná, ale při intenzivnějším vystavení se data ztrácí.

Pokus č. 5 byl opět provedený s neodymovým magnetem, akorát karta byla uložená v obalu originálně dodávaném s kartou. Místem magnetického proužku jsem projížděl magnetem důkladně a všemi směry. Výsledek byl, že data uložená na magnetické kartě byla v pořádku, což ukazuje na funkčnost originálních obalů.

Pokus č. 6 jsem zaměřil na ovlivnění rychlosti průchodu karty čtečkou na čtení dat. Čtečka, má udávanou průchodovou rychlost od 10 cm/s, četla i pod touto rychlostí. Spolehlivě přečetla 1. a 3. stopu. Kdežto 2. stopa vykazovala poškození u všech třech testovaných karet.

3.3 Podvody s magnetickou kartou

Závěrem bych se jen orientačně zmínil o podvodech a zneužívání magnetických karet, zejména v bankovní sféře. V této kapitole jsem čerpal především ze zdroje 25.

3.3.1 Podvody s přítomností karty

Karta je fyzicky přítomna u podvodu a je nástrojem identifikace.

Podvod y se ztracenou nebo zcizenou kartou

Podvody se ztracenou nebo zcizenou kartou, jsou podvody provedené pomocí originální platební karty, která se dostala mimo fyzickou kontrolu oprávněného držitele. Podvodník se snaží použít nalezenou nebo ukradenou kartu jako oprávněný držitel karty. V některých případech se podvodník ani nesnaží věrohodně napodobit podpis. Může také využívat ukradených a pozměněných nebo přímo padělaných osobních dokladů. Pro vyšetřování podvodu při ztrátě karty je výhodné mít k dispozici fotokopii přední i zadní strany karty. Jsou též případy podvodného zadržení platební karty, a to buď cíleným nevrácením karty obchodníkem, který ji může dále postoupit do řetězce podvodníků. Další případem podvodného zadržení platební karty je umístěním zařízení před či přímo do čtečky bankomatu, které kartu zadrží (tzv. libanonská smyčka). Většina z těchto podvodů v této kategorii se uskuteční u obchodníků dříve, než je nahlášena ztráta karty držitelem. Zneužití ztracené či zcizené karty patří v České republice mezi nejčastější kartové podvody.

Podvody s padělanou kartou

Padělaná karta je taková karta, která byla vyrobena a personalizována bez souhlasu vydavatele. Případně taková karta, která byla právoplatně vydána, ale později byla vizuálně upravena nebo byla pozměněna její elektronická data. Jedním ze způsobů padělání magnetických karet je tzv. SKIMMING. Skimming je postup, při kterém jsou originální data z magnetického proužku karty zkopírovány na jinou kartu. Bez vědomí právoplatného držitele karty. V prvním kroku se data zkopírují a ve druhém se nahrají na novou, padělanou kartu. Celé kopírování je provedeno elektronicky. V případě organizované skupiny, může pachatel či pachatelé zaplatit Vaší kartou kdekoliv na světě do několika minut od krádeže originálních údajů. Okradený zjistí, že byl podveden, až na výpisu z účtu. A to je prvotní impulz pro zablokování karty.
Zkopírování údajů z magnetického proužku se nejčastěji děje:

1) u obchodníků, kde nepoctivý pracovník obchodní společnosti zkopíruje obsah magnetického proužku před vrácením karty zákazníkovi, a poté získaná data využije nebo předá dále k výrobě padělané karty;
2) u bankomatu, kde podvodníci umístí speciální kopírovací zařízení, které zkopíruje všechna data z magnetického proužku karty.

Tento druh podvodu je na území České republiky na ústupu díky přechodu na hybridní karty. Z dosavadních zkušeností vyplývá, že ke zkopírování údajů z magnetického proužku karty dochází nejčastěji u bankomatů, v barech, restauracích, u čerpacích stanic a někdy i v hotelech. Banky a vydávající instituce mají k dispozici řadu možností, jak čelit podvodům padělanou kartou:

1) zavedení čipových karet - po zavedení čipových karet lze očekávat pokles výskytu podvodů s padělanou kartou, protože čip zamezí kopírování údajů;
2) inteligentní počítačové programy, které mohou sledovat chování platební karty a rozpoznat neobvyklé typy transakcí.

3.3.2 Podvody bez přítomnosti karty

Podvody bez přítomnosti karty jsou takové podvody, při kterých není fyzicky přítomna karta nebo držitel karty v místě prodeje. Podvodníci využívají podvodně získaná data o platební kartě k provedení nákupu prostřednictvím písemné, telefonní, faxové nebo

internetové objednávky. Podvody bez přítomnosti karty se staly oblíbenými po rozšíření faxu, kde autentizačním prvkem objednávky byl obvykle podpis klienta. Po rozšíření internetu se k objednávkám začal používat i tento způsob komunikace, ovšem bez autentizace podpisem. Bezhotovostní platby tohoto typu se staly u zákazníků velmi oblíbené a pohodlné. Obchodník nemá možnost fyzicky zkontrolovat kartu ani identitu držitele karty, míra rizika zneužití je vyšší než u běžných transakcí. Podvodníci obvykle data o kartě získávají ze zahozených nebo zkopírovaných potvrzení o transakcích, jejich podvodným vyžádáním např. e-mailem (phishing), z fiktivních internetových obchodů, vykrádáním databází s údaji o provedených transakcích (database hacking), apod. Stejně jako u podvodu padělanou kartou se právoplatný držitel karty o podvodu nedozví, dokud neobdrží výpisu z účtu.

Banky a vydávající instituce mají k dispozici řadu možností, jak čelit podvodům bez fyzické přítomnosti karty:

1) v souladu s pravidly kartových asociací se na karty s magnetickým proužkem tiskne třímístný kontrolní kód (CVV2 nebo CVC2) do podpisového proužku na zadní straně karty, který je při platbě bez přítomnosti karty obchodníkem požadován jako autentizace skutečnosti, že klient má kartu ve svém držení. Kód je jedinečně propojen s každou jednotlivou plastovou kartou a spojuje s ní číslo karty účtu (PAN);

2) zavedení nového prvku autentizace pro bezpečné platby - technologie 3D Secure, která umožní autentizaci držitele karty anebo obchodní společnosti;

3) rozšíření výhradně čipových karet při provádění plateb na internetu - k provádění plateb po internetu bude zapotřebí čtečka čipové karty připojená k počítači, ze kterého je transakce prováděna; tato čtečka zprostředkuje autentizaci oprávněného držitele karty;

4) využívání inteligentních počítačových programů, které mohou sledovat chování platební karty a rozpoznat neobvyklé typy transakcí, resp. upozornit na četnější výskyt transakcí bez přítomnosti karty na jednotlivé kartě nebo u konkrétní obchodní společnosti.

Někteří vydavatelé karet nabízejí další způsoby ochrany před podvody bez přítomnosti karty:

a) úplný zákaz transakcí bez přítomnosti karty

b) omezení maximální výše transakcí bez přítomnosti karty

c) umožnění platby bez přítomnosti karty jen na vyžádání (dočasné odblokování na základě žádosti držitele karty a následné zablokování)

d) vydání virtuální karty se sníženými limity, která je určena pouze pro platby bez přítomnosti karty [25]

3.3.3 Podvody kartou ztracenou v poště

Podvod je založen na zcizení karty během přepravy od vydavatele karty před tím, než ji mohl převzít právoplatný držitel karty, a jejím následném zneužití neoprávněným držitelem. Předcházet tomuto podvodu může držitel karty, který očekával zásilku, která nedorazila, měl by kontaktovat vydavatele karty a tím přispěje k včasnému odhalení. Ztracení zásilky s platební kartou dochází pouze ojediněle. Banky využívají řadu opatření, která snižují riziko zneužití takto zcizené karty:

- Základním opatřením proti případnému zneužití zasílané karty, je odesílání platební karty v neaktivním stavu (tj. není povolena autorizace plateb). Držitel karty po jejím obdržení musí provést aktivaci dle pokynů vydavatele karty.
- Dalším důležitým opatřením ze strany vydavatele je časově oddělené zaslání platební karty a PINu ve dvou samostatných zásilkách.
- Vydavatelé zavádějí takový způsob zasílání karet a jejich následného monitoringu, aby umožnili včasné odhalení nedoručené zásilky či případného zneužití karty.

3.3.4 Podvody se zcizenou identitou

K podvodu se zcizenou identitou dochází použitím podvodně získaných osobních údajů. K využití zcizené identity může dojít dvěma způsoby:

- podvodná žádost o kartu - podvodník může s pomocí zcizených nebo padělaných osobních dokladů požádat o otevření účtu a vydání karty;
- převzetí účtu - podvodník předstírá, že je skutečným držitelem karty a pokouší se podvést banku nebo kartovou společnost. Může také požádat banku o změnu parametrů karty nebo účtu (např. adresy) a následně o vydání nové karty.

Ve světě četnost zcizování identity v poslední době narůstá. V České republice se zatím tento druh podvodu prakticky nevyskytuje.

ZÁVĚR

Cílem této práce bylo navrhnout vhodný nástroj na zjišťování informací na magnetických kartách, zhodnotit bezpečnost magnetických karet a jejich využití v komerční bezpečnosti. V teoretické části práce jsem udělal náhled na technologii, princip uložení dat na magnetických kartách a jejich využití v komerční bezpečnosti. V praktické části jsem zjišťoval informace na magnetických kartách pomocí čtečky magnetických karet od firmy Vikintek, typ RS2000-33WE a následně provedl analýzu uložených dat na magnetickém proužku. Zjišťování informací probíhala bezproblémově, proto označuji magnetické karty s pohledu zjišťování informací jako spolehlivé. Dále jsem popsal instalaci a nastavení softwaru pro čtení magnetických karet. Ověřil jsem, že bezpečnost uchování dat na magnetické kartě není ohrožena běžně používanými magnety (jako jsou magnety kabelek či mobilních telefonů). Zkoušel jsem účinky na data uložená na kartě neodymovým magnetem i přímý styk s magnetickým proužkem, který se ukázal jako destruktivní. Jako ochrana proti zničení se osvědčil obal, který vydavatel karet ke kartám přikládá.

Bezpečnosti magnetických karet, již princip nám naznačuje, že magnetický proužek nemá aktivní zabezpečení (např. PIN). Kdokoliv, kdo vlastní čtečku magnetických karet, může zjistit informace na ní uložené. Abychom ochránili data uložená na kartě, používáme šifrovací algoritmy. Tím znemožníme útočníkovy zjištění pravých informací uložených na kartě.

Přínosem mé práce je ucelený pohled na problematiku magnetických karet a jejich využití. Pro používání jako členských karet nebo karet parkovacích se jeví jako vhodné. Naopak pro bankovní sféru se jeví jako nevhodné pro možnost snadného podvodu. Nejčastější zneužití magnetických karet je jejich zkopírování, které je velmi snadné. Jestliže se tedy útočník dostane, byť jen na vteřinu, ke kartě je schopen kartu okopírovat. Potom si nemůžete být jisti, že vaši kartu nezneužije. I když jako ochrana před zneužitím slouží vzor podpisu na rubu karty, ale sami si vzpomeňte, kdy po vás prodavač při placení magnetickou kartou, zkontroloval podpis. Jednoduchá kopírovatelnost magnetických karet je již dlouhou dobu veřejně známa a proto se karty s magnetickou páskou začínají pomalu nahrazovat čipovými kartami, které nabízí daleko lepší ochranu proti přečtení uložených dat.

Vydavatelé karet proto začaly emitovat karty hybridní, tedy s magnetickým proužkem a čipem. To však nevyřešilo problém s magnetickým proužkem. Některé země umožňují tzv. "fall-back". To znamená, že při poškození čipu na hybridní kartě se data čtou z magnetického proužku. Tím se degraduje technologie hybridních karet a nahrává útočníkům. Česká republika "fall-back" neumožňuje.

Jak jsem se zmínil výše, magnetické karty se začali nahrazovat čipovými. Příkladem úspěšné bezkontaktní čipové multifunkční karty je projekt hlavního města Prahy - Opencard. Umožňuje jednodušší přístup k městským službám, jako jsou: průkaz integrované dopravy, čtenářský průkaz, placení parkovného, přihlášení k portálu hl. města Prahy (dopravní přestupky), slevová karta (na kulturu, sport, gastronomii a volnočasové aktivity). Díky bezkontaktnímu přenosu dat nemusíme vytahovat peněženku pro přečtení. Karta může být opatřena kontaktní čipovou částí, která umožňuje uložení elektronického certifikátu (elektronický podpis). Magnetické karty nemůžeme použít pro takové aplikace z důvodů bezpečnosti uložených dat, extremní náročnosti na opotřebení karty a z nemalé části z pohodlnosti.

Magnetické karty jsou v oběhu již několik desítek let, přesto se stále používají a používat budou, díky jejich nízké pořizovací ceně (minimálně v parkovacích a vjezdových systémech), velkému objemu vydaných magnetických karet a velkému objemu čtecích terminálů ve světě.

CONCLUSION

The goal of this thesis is to propose an appropriate tool for detecting information on magnetic cards and to evaluate the safety and security of magnetic cards and their usage in active safety. In the theoretical part I presented an overview of technology and the principles of storing data on a magnetic card and their use in commercial security. In the practical part I explored information about magnetic card. I used scanner of firm Vikintek type RS2000-33WE. Reading of in formations wasn´t a problem. I mean magnetic cards in terms of reading information as safe. I descriptioned installations and configuration of software for reading of magnetic cards. I verified, that the safety of storing the data on a magnetic part is not jeopardized by commonly used magnets such as those on handbags or in mobile phones. I examined the effects on the data stored on a card using a neodymium magnet and direct contact with the magnetic strip, which showed as destructive. As a protection the cover provided with the card proved effective.

Safety of magnetic cards is concerned, the principle itself shows that the magnetic strip does not provide an active protection (for example PIN code). Anyone, who owns a magnetic card reading device, can gain data stored on a card. To protect the data stored we use encryption algorithms. With this we disable the attacker to gain the real information from the card.

Contribution of my work is a comprehensive view at the issue of magnetic cards and their use. For use as cards or membership cards parking, it seems appropriate. Conversely for the banking sector appears to be inappropriate for an easy fraud.The most often abuse of magnetic cards is their copying, which is very simple. If the attacker has an opportunity to get to a card even just for only one second, they are able to copy it. Then you cannot be sure that they will not abuse it. It is true that there is a signature field on your card as a safety feature, but try to recollect when a shopkeeper checked your signature against the card template. Easy ability to copy magnetic cards has been generally known for a long time and therefore are the magnetic cars being slowly replaced with smart cards that provide much better protection against reading the stored data.

Issuers of cards have started to emit hybrid cards: with both magnetic strips and chips. That, however, did not solve the problem with magnetic strips. Some countries enable so called "fall-back". That means that when a chip is damaged on a hybrid card the data from

the card is read from the magnetic strip. By this the technology of hybrid cards is degraded and it is a great advantage for the attackers. The Czech Republic does not allow "fall-back".

As mentioned above, magnetic cards have started to be replaced by smart cards. A good example of non contact chip multifunction card is the Prague project "Open card". It enables an easier access to the city services such as public transport, library card, payments of parking, log-in into the Prague portal (traffic offences), discount card (culture events, sport, activities for free time). Thanks to the non contact data transfer we do not need to take out our purse for reading the card. The card can contain a contact chip part that enables storing an electronic certificate (electronic signature). Magnetic cards cannot be used for such applications due to insufficient protection of stored data, extreme demand on wear of the card and, of course, comfort.

Magnetic cards have been in use for tens of years but are still used and so they will be thanks to their low acquisition price (at least in parking and entering systems), a huge amount of already issued cards and large number of reading terminals all over the world.

SEZNAM POUŽITÉ LITERATURY

[1] REID, Robert N. Facility manager's guide to security: protecting your assets. 1st edition. Lilburn, Ga : The Fairmout Press, Inc., 2005. 315 s. ISBN 0-88173-479-9.

[2] SNEHI, Jyoti. Computer Peripherals and Interfacing. 1st edition. New Delhi : Maxmi Publication (P) LTD., 2006. 123 s. ISBN 81-7008-929-8.

[3] GUSTIN, Joseph F. Cyber terrorism: a guide for facility managers. 1st edition. Lilburn, Ga : The Fairmout Press, Inc., 2004. 233 s. ISBN 0-88173-442-X.

[4] KHOSROW-POUR, Mehdi. E-Commerce Security: Advice from Experts. 1st edition. Hershey : CyberTech Publishing, 2004. 110 s. ISBN 1-59140-240-7.

[5] PARDOE, Terry D., SNYDER, Gordon, SNYDER, Gordon F. Network security. 1st edition. New York : ThomsonDelmar Learning, 2005. 461 s. ISBN 1-4018-82498.

[6] HENDRY, Mike. Smart card security and applications. 2nd edition. Nordwood : Artech house,Inc., 2001. 220 s. ISBN 1-58053-156-3.

[7] RANKL, Wolfgang, EFFING, Wolfgang. Smart card handbook. 3rd edition. West Sossex : John Wiley & sons, 2003. 943 s. ISBN 0-470-85668-8.

[8] HADDAD, Aneace. A new way to pay: creating competitive advantage through the EMV smart card standard. 2nd edition. Aldershot : Gower Publishing Limited, 2005. 128 s. ISBN 0-556-08688-3.

[9] THORNTON, Frank, et al. RFID security. Rockland : Syngress Publishing, Inc., 2006. 220 s. ISBN 1-59749-047-4.

[10] ING. NAGI, Petr. *Použitie automatickej identifikácie na ochranu objektov*. Žilina, 40 s. Oborová práce. Žilinská univerzita. Dostupné z WWW: <www.fel.uniza.sk/~nagy/BS/PDF/Aut_ID.pdf>.

[11] *CardHouse s.r.o.[*online]. 2001-2009 [cit. 2010-05-24]. Identifikace osob komplexně. Dostupné z WWW: <www.cardhouse.cz>.

[12] *IMA s.r.o.[*online]. 2007 [cit. 2010-05-24]. Identifikace osob komplexně. Dostupné z WWW: <www.ima.cz>.

[13] *Pandarton.cz* [online]. 2008-11-4 [cit. 2010-05-25]. Karty s magnetickým pruhem. Dostupné z WWW: <www.pandatron.cz/?535&karty_s_magnetickym_ pruhem>.

[14] *ID Standard* [online]. 2004-2010 [cit. 2010-05-24]. ID standard. Dostupné z WWW: <www.idstandard.cz>.

[15] *M Card* [online].[cit. 2010-05-25].Výroba a prodej plastových karet. Dostupné z WWW: <www.mcard.cz>.

[16] DafiCard [online]. 2009-2010 [cit. 2010-05-25]. Dafikard, dodavatel a výrobce plastových karet. Dostupné z WWW: <www.daficard.cz>.

[17] Clever Card [online]. 2009 [cit. 2010-05-25]. Výroba plastových karet. Dostupné z WWW: <www.clevercard.cz>.

[18] Business centre [online]. 2008-2010 [cit. 2010-05-25]. Slovní pojmů. Dostupné z WWW: <www. business.center.cz>.

[19] Inplastor [online]. 2008-2010 [cit. 2010-05-25]. Plastové karty. Dostupné z WWW: <www. www.inplastor.at >.

[20] Robinco CS[online]. 2010 [cit. 2010-05-25]. Plastové karty Robinco CS. Dostupné z WWW: <www. plastovekartyrobinco.cz >.

[21] BestaPrint[online].[cit. 2010-05-25]. Plastové karty. Dostupné z WWW: <www. bestaprint.cz >.

[22] ERRINGTON, Andrew m. Credit Card reader Using a PIC12C509. *Microchip* [online]. 2002, [cit. 2010-05-28]. Dostupný z WWW: <http://ww1.microchip.com/downloads/en/AppNotes/00727a.pdf>.

[23] B&C Data Systems[online]. 1996-2010.[cit. 2010-05-25]. Magnetic Card Encoding. Dostupné z WWW: <www.bcdata.com/encoding.html>.

[24] ČELUSTKA, Emil Čelustka. *E-komerce.cz* [online]. 13.4.2002 [cit. 2010-05-29]. Stopařův průvodce světem platebních karet 2. Dostupné z WWW: <http://www.e-komerce.cz/ec/ec.nsf/0/ c816f9ff4a5be4c6c1256b270068d3eb>.

[25] *SBK platební karty* [online]. 2010 [cit. 2010-05-29]. SBK bezpečnostní výbor. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/media_bezpecnost.html>.

[26] *Soom.cz* [online]. 15.8.2007 [cit. 2010-05-29]. Bezpečnost magnetických karet. Dostupné z WWW: <http://www.soom.cz/index.php?name=articles/show&aid=427>.

[27] Historie platebních karet. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 19. 2. 2010 [cit. 2010-05-29]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Historie_platebn%C3%ADch_karet#Magnetick.C3.BD_prou.C5.BEek>.

[28] *Státní tiskárna cenin* [online]. 2010 [cit. 2010-06-01]. Karty. Dostupné z WWW: <http://karty.stc.cz/>.

[29] ŠIMČÍK, Marek. *Technologie datové bezpečnosti vnitřních sítí*. Zlín, 2008. 57 s. Bakalářská práce. UTB Zlín.

[30] MORAVEC, Ondřej. Čipové karty a vše o nich. *FinExpert.cz* [online]. 30.5.2006, [cit. 2010-06-02]. Dostupný z WWW: <http://www.finexpert.cz/Autori/Cipove-karty-a-vse-o-nich/sc-48-sr-1-a-16871/default.aspx>.

[31] Z-Ware [online]. 2009-2010 [cit. 2010-05-25].Z-WARE. Dostupné z WWW: < www.z-ware.cz >.

[32] JSH Security Marketing[online].[cit. 2010-05-25].State-of-the-art Elektronic Safe. Dostupné z WWW: < www.jsh.co.uk >.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAMVA	The American Association of Motor Vehicle Administrators - Americká asociace pro motorová vozidla
CA DMV	California Department of Motor Vehicles - Kalifornské oddělení motorových vozidel
CVC/CVC2	Card Verification Code/2 (MasterCard) - Ověřovací kód karty
CVV/CVV2	Card Verification Value/2 (VISA) - Ověřovací kód karty
PVKI	PIN Verification Key Indikator - Indikátor čísla pinu
PVV	PIN Verification Value - Zakódovaný PIN číslem menším než 9, trojicí klíčů, 3 x DES

SEZNAM OBRÁZKŮ

SEZNAM TABULEK