Využití čipových karet v oblasti komerční bezpečnosti

The use of smart cards in the field of commercial security

Marek Dvořák

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Marek DVOŘÁK**
Osobní číslo:	**A08642**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Využití čipových karet v oblasti komerční bezpečnosti**

Zásady pro vypracování:

1. **Seznamte se s druhy karet, jejich oblasti použití, softwarovým vybavením a historií.**
2. **Navrhněte možnosti využití čipových karet v průmyslu komerční bezpečnosti. V práci se zaměřte na budoucí vývoj využití karet.**
3. **Proveďte analýzu současného stavu v používání karet pro docházkový systém v průmyslovém závodu Precheza a.s. Přerov. Udělejte návrh na zkvalitnění služeb a zabezpečení.**
4. **Zjistěte možnosti zneužití, zničení, a kopírování karet.**
5. **Porovnejte s jinými identifikačními systémy.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Rankl, W.; W. Effing (1997). Příručka čipové karty. John Wiley a synové. ISBN 0-471-96720-3.**
2. **MATTHEWS, Adam. Low Cost Attacks on Smart Cards The Electromagnetic Side-Channel. Next Generation Security Software Ltd. online. 2006 cit. 2009-11-17.**
3. **Introduction to Smart Cards cit. 25.4.2006.**
4. **OKsystem - Čipové karty online. 1999 cit. 2011-02-02. Čipové karty.**
5. **BERKES, Jem E. Side-Channel Monitoring of Contactless Java Cards. s.l., 2008.**

Vedoucí bakalářské práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce seznamuje čtenáře s chronologickým vývojem, a to od obyčejných karet k moderním čipovým kartám. Stručně seznamuje s možnými druhy karet a principy jejich funkce s hlubším zaměřením na čipové karty. Poukazuje na možnosti zneužití karet zabezpečení a právními postihy. Praktická část bakalářské práce je rozdělena do čtyř samostatných kapitol. První kapitola řeší analýzu používání karet pro docházkový systém v konkrétní firmě. Druhá kapitola seznamuje čtenáře s budoucím využitím karet. Další kapitola praktické části zahrnuje zkoušku fyzikální a elektrické odolnosti proti zničení karty. Poslední kapitola obsahuje porovnání s jinými identifikačními systémy. Závěr obsahuje shrnutí poznatků získaných při nastudování problematiky a při vlastní práci s kartou. Součástí práce jsou grafy obsažené v příloze P2 a vystihují výsledky veřejného mínění.

Klíčová slova: čipová karta, identifikační systém, riziko, bezpečnost, přístupový systém

ABSTRACT

Theoretical part of this paper discusses the chronological development of cards from the modest to modern smart cards. It describes several types of cards and its functionality, especially of chip cards. It refers to the possibility of misuse, security and legal action.

Practical part is divided in three independent chapters. First chapter analyzes the usage of cards for attendance system at particular company. The second chapter deal with future usage of cards. In the next chapter the card is tested against physical and electrical destruction. The last chapter compares other system for identification. This paper concludes with the knowledge gained through studying and using card. Annex P2 contains charts describing results of public opinion.

Keywords: smart card, identification system, risk, safety, access system

Poděkování:

Na tomto místě chci poděkovat panu doc. Mgr. Milanu Adámkovi, Ph.D. za odborné vedení a poskytnutí potřebné literatury při tvorbě této bakalářské práce. Dále děkuji vedoucím zaměstnancům závodu Precheza a.s. za vstřícné jednání a poskytnutí potřebných materiálů.

Marek Dvořák

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Svět se stává neustále rychlejším a nebezpečnějším. Tyto změny se nejvíce projevují v oblasti marketingu, informačních a bezpečnostních technologiích. Na tyto změny je třeba rychle reagovat, zvláště, když jde o zabezpečení informačních a identifikačních systémů, při dodržení vysokého standardu, spolehlivosti a jednoduchosti pro uživatele. Bylo třeba najít řešení, kde bude možné skloubit všechny tyto aspekty do jednoho výrobku a přitom by mohl člověk toto zařízení nosit v kapse. Bylo také třeba zohlednit, aby s tímto zařízením mohl pracovat kdokoli, od dítěte po důchodce. Zároveň musí být zajištěna odolnost vůči poškození běžným používáním. Výsledkem toho je čipová karta. Karty prošly od prvotního zrodu dlouhou řadou vylepšení a zabezpečení. Postupně zaplavily svět. Dnes už si stěží dokážeme představit život bez karet, které se staly nedílnou součástí peněženek většiny z nás.

Ovšem, každý klad má také svůj protiklad. Navzdory přínosu se ukazují i možnosti jejich zneužití, zejména pokud v kartách není implementována tolik potřebná ochrana, například v podobě bezpečnostních kódů nebo použití některé z kryptografických metod.

Systémy pracující s čipovými kartami nabízejí širokou škálu využití. Právě možnosti využití se staly inspirací pro zvolení tématu této práce.

I. TEORETICKÁ ČÁST

1 VÝROBA, VÝVOJ A DRUHOVÁ ROZMANITOST

1.1 Historie a postupný vývoj

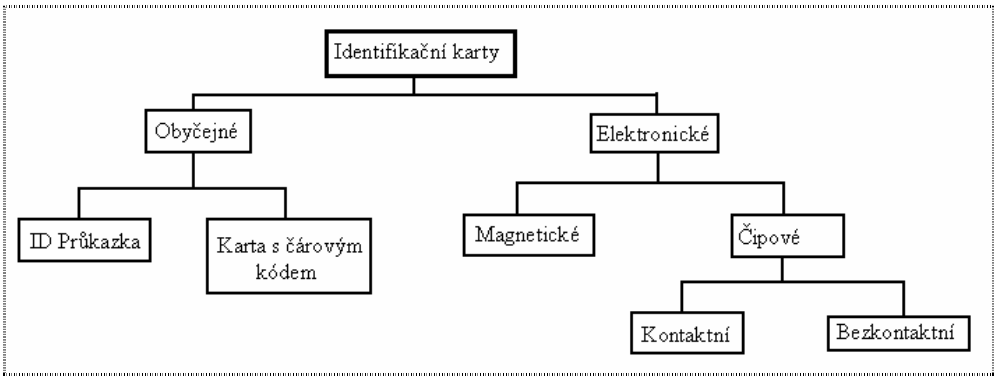
Historie dnešních platebních a bezpečnostních karet sahá až do 70. let 19. století, jako forma úvěrových šeků. Když americká telegrafní společnost Western union telegraph copany vydala v roce 1914 svým zákazníkům svoji historicky první platební kartu, vůbec netušila, jakou éru odstartovala. Vlastník jejich karty mohl využívat služeb bez přímého zaplacení a jednou měsíčně dostával poštou výpis svého účtu. Karty nadále začínají pronikat do letecké dopravy. V roce 1951 vydává Franklin National Bank of New York bankovní kreditní kartu, za kterou stojí firma VISA. Tyto karty ale obsahovaly jen údaje na nich vyražené. Roku 1971 je společností International Air Transportation Association (IATA) vyrobena karta s magnetickým páskem a první platební terminály. Nastává problémem s velmi jednoduchou možností kartu zkopírovat. Ve stejném roce si nechává japonský vynálezce Kunitaka Arimura registrovat vynález - čipovou kartu. Nemá ale možnost ovlivňovat budoucí vývoj a může působit jen v Japonsku. Navíc se stará spíše o usazení čipu do karty. O 3 roky později si nechává patentovat francouzský žurnalista Roland Moreno čipovou kartu se zataveným mikročipem, doplněnou o bezpečnostní PIN kód. Rok 1986 je velmi významný v historii karet zavedením normy ISO 7816 pro čipové karty. Koncem 80. let vyrobila firma Bull první kartu s mikroprocesorem. Technologie a zabezpečení již byly natolik vyspělé, že karty začaly pronikat do jiných oblastí, jako do zabezpečovacích systémů a prvků identifikace. Pro opravdu masové rozšíření bylo potřeba podrobit tyto systémy obrovskému bezpečnostnímu testu a návrhu pro nejvhodnější standard. K tomu byla sestavena skupina složená z asociací Karte Blue, Karte Verde a Francouzskou telekomunikační administrativou. Test proběhl na 100 000 kartách a 700 platebních terminálech. Výsledky dopadly dobře pro většinu testovaných karet. Společnost Carte Boncaire vybrala čipovou kartu Bull CP8. Začíná masové rozšíření, kdy Francií bylo v roce 1992 vydáno přes 21 milionů karet. Píše se rok 1996, společnosti MasterCard a VISA vydávají mezinárodní standard pro čipové karty.

Ve vývoji se pokračovalo velmi rychlým tempem a kromě otázky bezpečnosti se řešilo, jak urychlit a usnadnit princip čtení. Upustilo se od kontaktního čtení a přešlo se k bezkontaktnímu, kdy stačí kartu pouze přiložit. Komunikace probíhala bezdrátově,

pomocí elektromagnetických vln. Roku 2005 tyto společnosti vydávají standard pro bezkontaktní čipové karty (RFID karty). Dnes je svět doslova zaplaven miliardami různých typů plastových karet. [1] [2] [3] [4]

1.2 Přehled dnešních identifikačních karet

Dnes máme na výběr ze spousty typů karet, avšak každá je jinak vhodná pro naši oblast použití. Tomu odpovídá míra zabezpečení a cena. Základní dělení karet znázorňuje obr. 1. [5]



Obr. 1 Základní rozdělení identifikačních karet - blokové schéma. [5]

1.2.1 Embosovaná karta

Embosovaná karta má reliéf vystupující z povrchu nebo vrytý do povrchu karty. Takto vystouplý text bývá většinou zvýrazněn barvou. Tento proces se nazývá tipping. Karta obsahuje identifikační údaje v jakékoliv podobě, buďto jako číselný kód, nebo jiný text, který jednoznačně určuje jejího majitele. Pro vyšší bezpečnost bývá doplněna o bezpečnostní prvky, nejčastěji hologramy a 3D nálepky. Obvykle se s nimi setkáváme v podobě karty pojištěnce, různých druhů průkazek, moderních řidičských průkazů a podobně. Přesný standard pro identifikační kartu určuje norma ISO 7811-1. [6]

1.2.2 Optická karta

Karta je vhodná především tam, kde není vysoký nárok na nebezpečnost. Má na sobě vytištěn ojedinělý čárový kód typu EAN nebo jiné kódy. Čtečka při snímání pomocí infračervených diod rozlišuje tmavá a světlá místa kódu, která reprezentují logickou 1 a 0. Pořizovací náklady na kartu jsou minimální. Karta najde využití ve

stravovacích zařízeních, často se s ní setkáváme v obchodech v podobě věrnostní karty. [7]

1.2.3 Optická paměťová karta

Je to karta se zapuštěným paměťovým povrchem připomínajícím povrch CD nosiče. Dokáže pojmout až 3 MB dat, ale neumožňuje zápis. Svého rozšíření se dočkala v USA, kde od roku 1997 bylo vydáno kolem sedmi milionů těchto karet. [8]

1.2.4 Karta s magnetickým páskem

Karta se hojně rozšířila především kvůli velice nízkým pořizovacím nákladům. Byla populární při platbách v obchodech. Mnohé terminály však nevyžadovaly nutnost použití PIN kódu, stačil pouze podpisový vzor. Na první pohled ji poznáme podle černého podélného pruhu délky 85,6 mm a šířky 13 mm na rubové straně karty. Střed pásku leží 12 mm od okraje. Pásek obsahuje datové informace uložené ve 3 stopách, z nichž každá má standardizovanou šířku 2,794 mm. Pásky nejsou příliš odolné vůči okolnímu magnetickému poli. [9]

- 1. stopa na magnetickém pásku má kapacitu až 79 alfanumerických znaků a definovala ji společnost IATA (International Air Transportation Association) již v roce 1969
- 2. stopa může disponovat až čtyřiceti numerickými znaky od 0 po 9 a rovnítkem. Umožnilo použít kartu při online finančních transakcích.
- 3. stopa poskytuje až 107 numerických znaků na uložení informací pro banky, za účelem ověření PIN kódu. Vrstva funguje v režimu read/write, to znamená, že informace je možno přemazávat. Toho využijeme například při odečítání bankovního kreditu.

1.2.5 Hybridní karta

Hybridní karty mohou spojovat vlastnosti kontaktních i bezkontaktních. Pro tato dvě rozhraní používají jeden společný čip. Druhým příkladem hybridní karty je karta s magnetickým páskem doplněná o čip. Typickým příkladem je většina dnešních platebních karet. [5] [10]

1.3 Výroba potisku karet

Na karty se tiskne převážně průmyslovou tiskárnou, a to metodou nazývající se termotransferový tisk. Tato forma tisku se hodí na většinu plastových karet. Podle barvy rozlišujeme na sublimační (barevný) a monochromatický tisk.

Termotransferový tisk je digitální forma tisku o rozlišení 300 dpi a vyšším, takže mizí problém rozostřených okrajů. Princip tisku spočívá v přenosu barviva ze speciální jednorázové barvící pásky z tiskové hlavy přímo na povrch karty. K přenosu barvy je zapotřebí značného tepla. Umožňuje jak monochromatický tisk strojově čitelných kódů, tak i tvorbu fotografických obrázků třemi barvami. Barevný tisk využívá červenou, modrou a žlutou barvu. [11]

- Sublimační tisk dokáže tisknout různě velké barevné body, tím dosahuje vynikající kvality obrázků bez ostrých okrajů. Barviva pronikají až do části povrchu tištěné karty. Velikost barevného bodu je přímo úměrná vyvolanému teplu z tiskové hlavy. Výsledná barva je dána kombinací užitých dílčích barev.
- Monochromatický tisk nedokáže řídit hustotu ani velikost tiskového bodu, takže se bod vytiskne, nebo nevytiskne. Vykreslit spojitý obrázek je tedy nemožné, ale můžeme vytvořit iluzi spojitého polotónu jednotlivými inkoustovými tečkami procesem zvaným „dithering“. Je to v podstatě rastrování, které umí vytvořit jen ostrý text a grafiku. Hodí se především pro tisk bezpečnostních čárových kódů a grafik viditelných pod ultrafialovým světlem.

1.4 Materiály

Většina odolnějších plastových karet je vyráběna sendvičovým systémem z více vrstev spojených velkým tlakem. Přední a zadní strana je z polymerních materiálů typu PVC, PC nebo PET. Vnitřní část je vyrobena z ABS plastu. Levnější karty nejsou složeny z více vrstev, tím se ale podstatně snižuje jejich pružnost a často při nižších teplotách praskají. [12]

1.5 Rozměry karet

Standardizovaný rozměr karet stanovuje norma ČSN ISO/IEC 7810:2006. V dnešní době nejrozšířenější karty se odborně nazývají ID1. Jejich delší strana je rovna 85,6 mm s odchylkou ± 0,12 mm, kratší stana 54 mm s povolenou odchylkou ± 0,08 mm. Standardizovaná tloušťka je stanovena na 0,3, 0,5 a 0,76 mm. Karta s čipem může mít i tloušťku 0,81 až 0,84 mm. Méně užívané jsou karty označené ID-2 o rozměrech 105×74 mm a ID-3 o velikostech 125×88 mm. Pro SIM karty platí označení ID-000 a rozměry 25×15 mm. [13] [14]

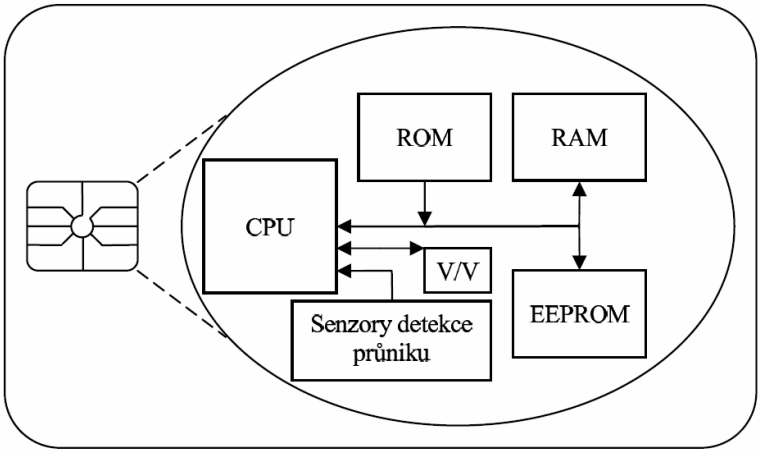
1.6 Norma ISO/IEC 7810

Norma se zabývá rozdělením identifikačních karet

- *Norma ISO/IEC 7810 - Fyzikální požadavky na plastovou identifikační kartu*
- *Norma ISO/IEC 7501 - Strojově čitelné cestovní dokumenty*
- *Norma ISO/IEC 7811 - Identifikační karty - Záznamová technika*
- *Norma ISO/IEC 7812 - Identifikace vydavatelů*
- *Norma ISO/IEC 7813 - Karty pro finanční transakce*
- *Norma ISO/IEC 7816 - Karty s integrovanými obvody s kontakty*
- *Norma ISO/IEC 10536 - Bezkontaktní karty s integrovanými obvody s těsnou vazbou.*
- *Norma ISO/IEC 14443 - Bezkontaktní karty s integrovanými obvody s vazbou na blízko*
- *Norma ISO/IEC 15693 - Bezkontaktní karty s integrovanými obvody s vazbou na dálku.*
- *ISO/IEC 11693 - Karty s optickou pamětí - Všeobecné charakteristiky*
- *ISO/IEC 11694 - Karty s optickou pamětí - Lineární metoda záznamu [14]*

2 ČIPOVÉ KARTY

Čipová karta je karta o rozměrech daných normou ČSN ISO/IEC 7810:2006, doplněná o vestavěný polovodičový mikročip (ICC – Integrated circuit chip), který je srdcem karty. V mikročipu jsou uloženy všechny informace a je implementována kryptografická ochrana. Moderní čipové karty mají v mikročipu implementován v podstatě celý počítač, protože obsahuje mikroprocesor, paměť, software a vstupně-výstupní zařízení. Dále mají moderní čipy spoustu bezpečnostních mechanismů, schopných čelit softwarovým útokům. Karty mohou komunikovat se čtecím zařízením buďto přes kontaktní plošky, nebo bezkontaktně. [15] [16]



Obr. 2 Architektura uvnitř čipu. [17]

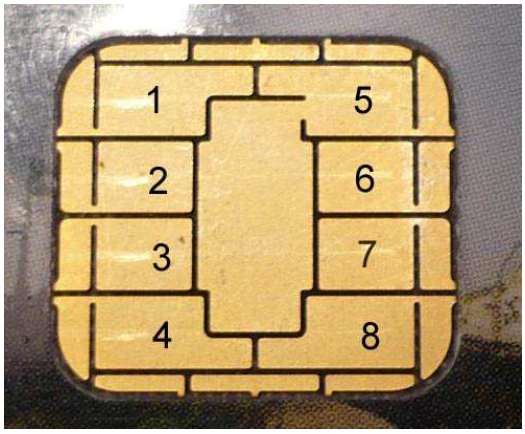
2.1 Rozdělení dle komunikace

2.1.1 Kontaktní karty

Kontaktní systém sestává z karty s vodivými kontakty a ze čtečky. Standardy pro čipové karty kontaktní přesně určuje mezinárodní norma ČSN ISO/EIC 7816. Kartu poznáme na první pohled tak, že jsou z lícové strany vidět elektrické vývody z čipu. Protože kartu nosí spousta lidí přímo u sebe v peněžence v nevhodných skladovacích podmínkách, bývají kontaktní plošky pozlaceny z důvodu ochrany proti korozi. Tyto elektrické kontakty mají ve většině případů stejný tvar. Obrazec z plošek tvoří 8 velkých elektricky aktivních ploch o rozměrech 13×12 mm. Přesné umístění čipu na kartě určuje norma ISO/IEC 7816-2. Kontakty zprostředkovávají napájení, přivádí externí taktovací signál a zprostředkovávají datovou komunikaci. Pro výměnu

informací musí být karta vsunuta do čtečky a kontakty musí být navzájem vodivě spojeny.

Rozšiřující možnosti komunikace specifikuje norma ISO/IEC 7816-12, podle níž dnes mohou karty komunikovat přes rozhraní USB. Tento standard musí karta podporovat. [18] [19]



Obr. 3 Vodivé kontakty z čipu na kartě s popisem kontaktů

Tab. 1 Význam čísel kontaktů [20]

Číslo kontaktu	Označení kontaktu	Popis kontaktu
1	VCC	napájení čipu napětím +5V
2	RST	reset
3	CLK	hodinový signál
4	AUX1	Záložní, zatím nevyužitý kontakt
5	GND	Zem, napětí 0V
6	VPP	Programovatelný vstup
7	I/O	Datový vstup a výstup pro sériovou komunikaci
8	AUX2	Záložní, zatím nevyužitý kontakt

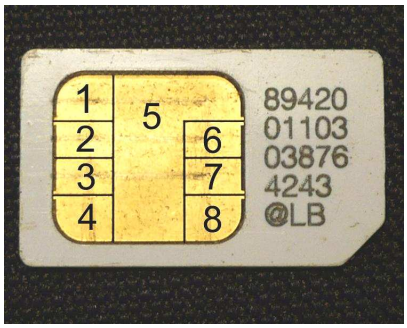
- Náhled části normy ČSN ISO/EIC 7816

ISO/IEC 7816 sestává z následujících částí pod společným názvem Identifikační karty – Karty s integrovanými obvody:

- *Část 1: Karty s kontakty - Fyzikální charakteristiky*
- *Část 2: Karty s kontakty - Rozměry a umístění kontaktů*
- *Část 3: Karty s kontakty - Elektrické rozhraní a protokoly přenosu*
- *Část 4: Organizace, bezpečnost a příkazy pro výměnu*
- *Část 5: Registrace poskytovatelů aplikací*
- *Část 6: Mezioborové datové prvky pro výměnu*
- *Část 7: Mezioborové příkazy pro strukturovaný kartový dotazovací jazyk*
- *Část 8: Příkazy pro bezpečnostní operace*
- *Část 9: Příkazy pro správu karet*
- *Část 10: Karty s kontakty - Elektronické signály a odpověď na reset pro synchronní karty*
- *Část 11: Ověřování osob biometrickými metodami*
- *Část 12: Karty s kontakty - Elektrické rozhraní USB a provozní procedury*
- *Část 13: Příkazy pro správu aplikací v multiaplikačním prostředí*
- *Část 15: Aplikace kryptografické informace [21]*

- SIM karta

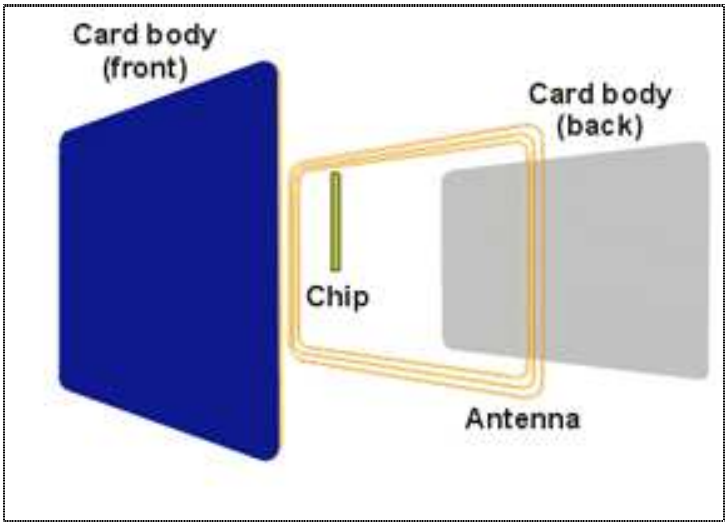
Je čipovou kontraktní kartou navrženou speciálně pro mobilní telefony. Nese v sobě informace o telefonním čísle, má vnitřní paměť a procesor. Bez ní je telefon zcela nepoužitelný. Jméno SIM značí (Subscriber Identity Module). Bylo tak učiněno s předpokladem, že mobilní telefony budou lidé často měnit a karta s číslem se bude pouze přesunovat. Samozřejmostí je zde vzájemná kompatibilita a možnost použít ji v jakémkoli GSM zařízení, podléhá však normě ISO 7816. Komunikuje přes protokol T=1 nebo T=0. Protokol je více popsán v části Komunikační protokoly na straně 21. Zapojení kontaktů je naprosto stejné jako u kreditní karty, viz tabulka 1 na str. 17. [19]



Obr. 4 Fotografie SIM karty s popisem kontaktů.

2.1.2 Bezkontaktní karty

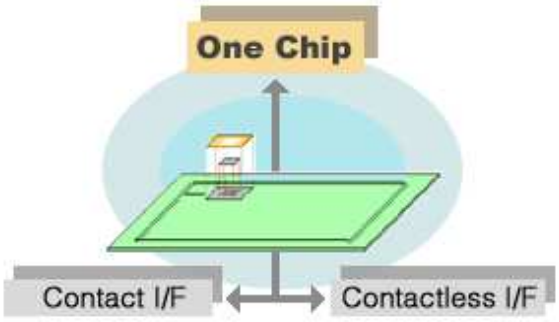
Kontaktní karta komunikuje bezdotykově. Pro vzájemný přenos informací je využito elektromagnetické indukce. Přenos funguje na radiových vlnách o modulovaných frekvencích 125 kHz nebo 13,56 MHz za předpokladu dostatečného přiblížení karty ke čtečce. Vzdálenost je závislá na vyzářeném výkonu a citlivosti čtečky a karty. Typická komunikace probíhá do vzdálenosti cca 15 cm. Karty jsou odborně nazývány RFID karty podle anglického Radio Frequency IDentification. V kartě je zalita anténa, tvořená několika závity tenkého drátu kvůli naindukování elektromagnetických vln, které pocházejí ze čtečky. Bezdrátovou komunikaci definuje čtyřdílný standard ISO/IEC 14443. Rychlost komunikace se dnes ustálila na 848 Kb/s. Vědcům se už podařilo dosáhnout přenosové rychlosti 5 Mbit/s. Přenosová rychlost má velký význam pro přesun velkých objemů dat. Většinou jsou bezkontaktní karty používány pro identifikaci osob, evidenci docházky atp. V tomto případě se jedná o malé přesuny dat, ale například ve spojení s biometrickým systémem je třeba přenášet větší objemy dat v krátkém čase. Pro budoucí vývoj bude otázka rychlosti druhý největší problém hned po otázce zabezpečení. [15] [22]



Obr. 5 Ilustrační obrázek čipové karty. [13]

2.1.3 Duální karty

Duální karta má jeden společný čip pro kontaktní a současně i bezkontaktní přenos informací. [13]



Obr. 6 Duální karta. [13]

2.2 Výčet obsažených vnitřních komponent

2.2.1 Paměť

Karty obsahují 3 typy pamětí. Každá má své výhody. Paměť typu ROM (Read-Only Memory) je pevně daná a data jsou do ní vepsána již přímo při výrobním procesu. Tato data již dále nelze měnit. Většinou obsahují číslo karty, jméno držitele atp. Hodí se na uložení operačního systému karty. Naproti tomu paměť EEPROM (Electrically-Eraseble-Programable-Memory) dokáže svůj obsah uložených dat měnit elektrickým proudem. Jsou v ní uložena aplikační data, měnící se v čase. Příkladem je odečet jednotek u telefonních karet. Kapacita se pohybuje od 2 kB do 74 kB. [20]

Paměť RAM (Random Access Memory). V této paměti jsou uloženy informace pouze pro běh funkcí potřebných k aktuálnímu početnímu výkonu. Je energeticky závislá, a proto neudrží data permanentně. Její velikost je typicky 256 bajtů. [21]

2.2.2 Procesor

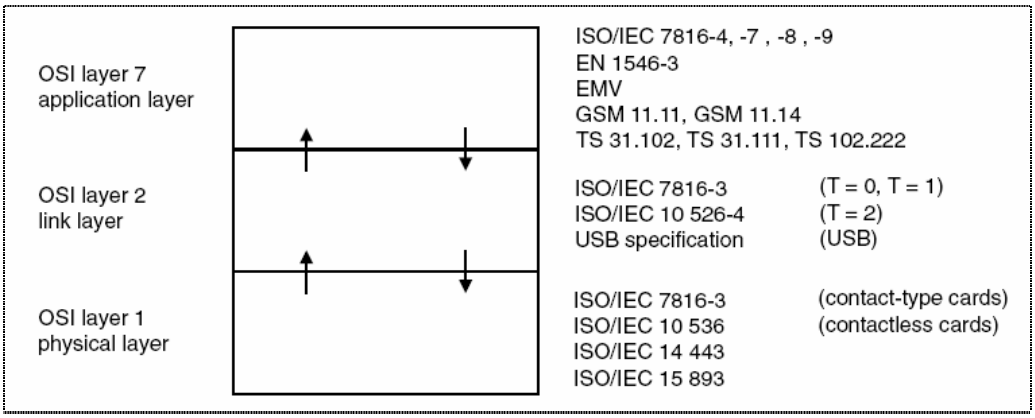
Procesor zpracovává početní úkony a odpovídá za jejich správné vykonání. Je mozkem karty a tvoří ho obvykle 8 bitový mikroprocesor, pracující na taktovací frekvenci 5 MHz. [20]

2.3 Rozdělení dle operačních systémů

Podle vlastností operačního systému lze dělit čipové karty na statické a dynamické. Statické karty jsou schopny číst, zapisovat a pracovat s daty. Mezi tyto karty patří většina dnešních platebních karet a SIM karty. Na rozdíl od statických, karty dynamické mohou i měnit programový kód, díky němuž se kompletně mění chování karty. V dnešní době sem patří JavaCards a MULTOS. [20]

2.4 Komunikační protokoly

Proces komunikace mezi čtečkou a kartou probíhá podle předem stanovených protokolů na základě mezinárodní normy ISO/EIC 7816. Komunikační protokol se dělí do více subvrstev, a to na fyzickou, linkovou a aplikační vrstvu. Toto rozdělení znázorňuje model OSI na obr. 4. Bližší specifikace popisuje standard ISO/IEC 7816-3 pro karty kontaktní a ISO/IEC 14 443 pro karty bezkontaktní. [13] [20]



Obr. 7 Blokové schéma komunikačního procesu. [20]

2.4.1 Fyzická vrstva

Vrstva musí splňovat normu ISO/IEC 7816-1 představující fyzikální vlastnosti karty jako jsou ohebnost, odolnost vůči EMV atd. Také musí splňovat normu ISO/IEC 7816-2 zabývající se umístěním čipu na kartě. [22]

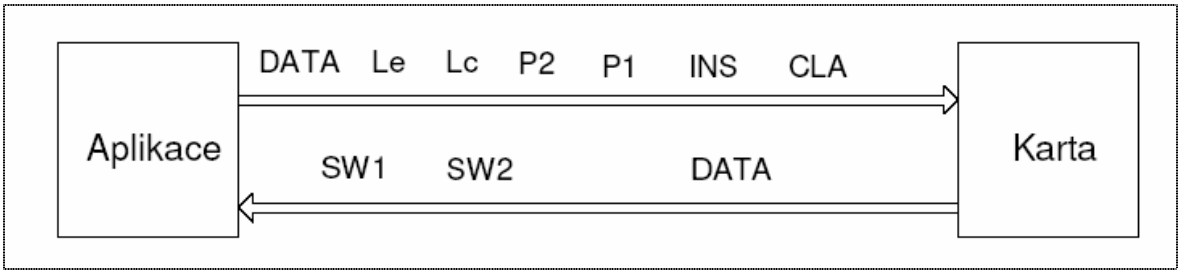
2.4.2 Linková vrstva

Na úrovni linkové vrstvy jsou definovány přenosové protokoly, označující se T=x, kde písmeno T značí pojem Transmission protocol a písmeno x symbolizuje verzi transportního protokolu. Kontaktní karty označují revize 0 až 2, bezkontaktní využívají protokol T=CL.

- **Protokol T=0** je určen pro transport dat v asynchronním režimu v poloduplexním režimu. Řídí se standardy ISO/IEC 7816-3, GSM a EMV. Nedokáže řetězit bloky, má paritní bit, ale nedokáže detekovat chyby. Zabírá v paměti 300 bajtů. [13]
- **Protokol T=1** je transportní protokol pracující v poloduplexním asynchronním režimu orientovaném blokově. Data jsou posílána v bloku a tyto bloky dále mohou tvořit řetězce. Blok dat se skládá ze tří částí: Prolgue field, Epilog field a Information field. Kromě normy ISO/IEC 78169-3 se řídí i standardem pro EMV a podporuje řetězení bloků. Je doplněn o detekci chybových kódů. V paměti zabírá 1100 bajtů. [13]
- **Protokol T=CL** je transportním protokolem pro komunikaci bezkontaktních čipových karet. [13]

2.4.3 Aplikační vrstva

Aplikační vrstva je zvaná APDU (applications prococols data units). APDU rozhraní eliminuje kompatibilitu různých typů čipových karet. Protokol je standardizován v modelu OSI jako mezinárodní datová jednotka. Protokol je nezávislý na své linkové subvrstvě. Rozlišuje příkazy a odpovědi karty. Struktura APDU je znázorněna na obr. 8 [13]

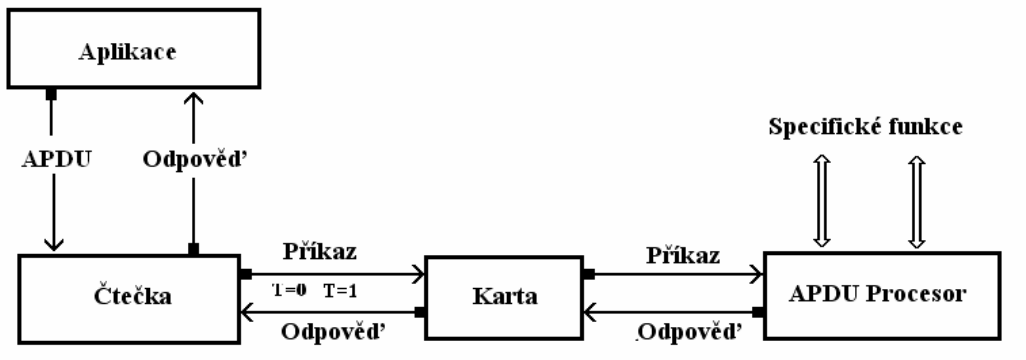


Obr. 8 Blokové schéma protokolu APDU. [20]

- **Příkaz APDU** je složen z následujícího datového slova
  - *CLA (1 bajt) Toto povinné pole slouží pro identifikaci instrukční třídy,*
  - *INS (1 bajt) Povinné pole, označuje konkrétní instrukci z instrukční třídy definovanou CLA*
  - *P1 (1 bajt) Toto pole definuje parametr 1*
  - *P2 (1 bajt) Toto pole definuje parametr 2*
  - *LC (1 bajt) Nepovinné pole určuje počet bajtů v datovém poli*
  - *Datové pole (proměnný počet, LC bajtů) Nepovinné pole příkazu, obsahuje data*
  - *Le (1 bajt) Volitelné pole specifikuje maximální počet bajtů očekávané odpověd*
  - *SW1 (1 bajt) Povinné pole obsahující stavové informace (status word),*
  - *SW2 (1 bajt) Podobně jako SW1 [20]*

Tab. 2 Základní příkazy pole CLA a INS [20]

Příkazy	Popis funkce
SELECT	otvírá soubor nebo adresář
UPDATE	mění obsah souboru
AUTHENTICATE	autentizuje kartu vůči okolnímu prostředí
READ	čte soubor
VERIFY	zjišťuje, zda je PIN správný



Obr. 9 Schéma komunikace. [13]

3 BEZPEČNOST ČIPOVÝCH KARET

Čipové karty jsou velice dobře zabezpečeny proti potenciálnímu úniku uložených dat, avšak žádný systém nedokáže být absolutně odolný ve všech směrech. Tedy i karta čipová má jisté nedostatky v ochraně. Útočníci se snaží přijít na bezpečnostní „díry“ na základě zkušeností a s použitím technického vybavení. Bezpečnost karty se dá rozdělit do více oblastí, a to na fyzickou bezpečnost chránící před mechanickými útoky, softwarovou bezpečnost a bezpečnost dalších periferií, jako jsou čtečky a terminály. Zabezpečení vždy „pokulhává“ vinou nejslabšího článku celého řetězce. Pro útočníky jsou karty populárním cílem zejména kvůli získání mnohdy finančně vysoko ohodnocených informací. [22] [24]

3.1 Útoky na čipové karty a možnosti prolomení bezpečnostních kódů

3.1.1 Fyzické útoky

Tyto útoky vycházejí ze zkoumání struktury čipu a provádí s ním reverzní funkce. Využívá analýzy a modifikace hardwaru, užitím kvalitního a výkonového laboratorního vybavení jako jsou speciální sondy. Útočník se nejprve musí dostat k čipu. To provede odstraněním plastového obalu mechanickou nebo chemickou cestou. K odkrytému čipu připojí tenké elektrické vodiče k datové sběrnici. Má možnost pozorovat elektronovým mikroskopem chování paměťové buňky. Práci mu může usnadnit pouhé snížení taktovací frekvence čipu. Proti těmto útokům jsou už dnes čipy chráněny bezpečnostní pasivní vrstvou, ochrannou mřížkou nebo světlo citlivými detektory. [23] [24]

3.1.2 Logické útoky

Útok využije skryté chyby, která se může náhodně objevit při normálním provozu na komunikačním kanálu, přes který se vyměňují všechny informace. Při bezpečnostním testování k chybě totiž ani nemuselo dojít. Jde o jednoduchou nedestruktivní metodu. Patří sem skenování příkazů, skenování souborového systému a kryptografická analýza se zneužitím protokolu. [20] [24]

3.1.3 Útoky postranními kanály

Protože se čipové karty obtížně sabotují, přešlo se ke zkoumání jednotlivých děr, metodou zvanou postranní kanál. Není to forma chování celé kryptoanalýzy, ale zabýváme se konkrétními chybami, při kterých může uniknout nějaká část dat, z nichž lze prolomit bezpečnostní kódy a provést cílený útok. [20]

Kryptografický algoritmus se zpravidla dělí na dvě odvětví. Jedna část se zabývá matematickým modelem. Druhá pojednává o implementaci běžících procesů a jejich zkompletování před průchodem na procesor. [20] [24]

Útočník může využít chyby ve špatném šifrovacím algoritmu, nebo může útočník zdvojit blok tím, že pošle dva bloky za sebou. Pokud si toho kryptografický algoritmus nevšimne, může se tak stát, že místo požadované částky 100 Kč se přibalí k tomuto další dvě nuly a dostaneme tím transakci 10 000 Kč. [20]

- Chybový postranní kanál

Tento typ útoku využívá dočasných nebo permanentních chyb k ovlivnění chování. U dočasné chyby se zařízení na chvíli vyruší a jeden konkrétní výpočet proběhne nesprávným způsobem. Naproti tomu u permanentního se blokuje celá paměťová buňka nějakým znakem a znemožní na delší dobu správnou funkci. Chybový postranní kanál nemůže hardwarově zničit zařízení. [20]

- Metoda vynucení chyby

Karta přechází do chybových stavů díky několika možným způsobům. Prvním je způsob vynucení chyby. Spočívá ve vystavení karty cizímu intenzivnímu elektromagnetickému poli. Karty mají v sobě implementovánu ochranu a přejdou do vlastní vytvořené chyby. Této chyby útočník využije. Dalším často používaným způsobem je změna napájecího napětí minimálně o 15%, protože karty jsou podle mezinárodního standardu ISO stavěny na povolený výkyv napětí o 10%. Přivedením přepětí nebo podpětí generujeme v kartě chybový stav. Hojně využívanou je změna taktovací frekvence. Karta opět na základě normy pracuje s určitou tolerancí. Změnou frekvence opět docílíme vytvoření vlastní chyby v kartě. Poslední metodou je veliký výkyv teploty, kterého se v praxi moc nevyužívá, ale lze opět takto dostat kartu na zkoumání chyby.

- Výkonový postranní kanál

Zkoumá energii spotřebovanou při operaci. Karta si pro sebe vytváří výkonovou analýzu zvanou SPA. Z ní je možno vydedukovat množství energie vynaložené na provedení úkonu. Získané informace pak útočník porovnává s časovou vynucenou chybou. [20]

- Elektromagnetický postranní kanál

Při práci polovodičového čipu vzniká kolem něj elektromagnetické pole. Pomocí cívky měříme vyzařované elektromagnetické pole, následně jej budeme zaznamenávat a při útoku tyto poznatky využijeme. [20]

- Časový postranní kanál

Metoda měří čas potřebný pro kryptografické zařízení. Čas se vztahuje k běhu algoritmu a taktovací frekvenci, podle těchto získaných informací už lze sestavit přibližný model tajného klíče. [20]

3.2 Možnosti kopírování

Čipovou kartu bylo možné zkopírovat kvůli nedostatečnému kryptografickému zabezpečení. K vyrobení kopie stačil vlastní hackerský software, čtečka RFID karet a speciální hardwarové zařízení zvané transmitter, kterým je v postatě malý přenosný počítač. Z transmitteru se později data nakopírují do počítače, v němž dojde ke kryptografickému odkódování. Poslední součástkou je anténa připojená k transmitteru. Pomocí těchto zařízení lze mít za několik minut kopii karty. [25]

Moderní čipové karty, zabezpečené nejnovějšími kryptografickými algoritmy, jsou už opravdu bezpečné. Musejí podléhat normě FIPS 140 – 1 level 2. Tyto čipové karty dosud není možné kopírovat. Podle dostupných informací z internetu a odborných publikací nebyl zjištěn jediný úspěšný pokus o zkopírování těchto dosud „bezpečných“ karet. S nárůstem používaných karet je pouze otázkou času, kdy nějaký „hacker“ za pomocí speciálních technik dokáže toto zabezpečení prolomit a zhotovit kopii čipové karty. [26]

3.3 Možnost zneužití karet

V drtivé většině zneužití dobře zabezpečené karty s čipem jde o pochybení lidského faktoru, nebo o bezpečnostní díru mezi čtečkou a nadřazeným systémem. Vlastní karta je relativně bezpečná. Další riziko představuje krádež platební karty nedoplněné o bezpečnostní PIN kód. Lze jednoduše zneužít například kartu pro neoprávněný vstup přes turniket, kde není ochrana doplněna dalším ochranným prvkem jako například zadání PIN kódu nebo biometrickou ochranou. Kradenou kartu lze snadno zneužít k platbě přes internet. [27]

3.4 Možnosti zničení čipových karet

Mikročip, obsažený v kontaktní čipové kartě je polovodičový čip s miliony tranzistory typu CMOS a ty jsou, jak je obecně známo náchylné na statickou elektřinu. Sice jsou obvody chráněny proti zničení tímto nebezpečně vysokým napětím, ale jakási míra nebezpečí zde je.

Pro RFID karty představuje riziko vysoká hodnota okolního elektromagnetického vlnění. Kartu dokáže zcela bezpečně zničit elektromagnetické pole v mikrovlnné troubě nebo různé elektromagnetické zbraně. Mobilní telefon by neměl na základě elektromagnetické kompatibility kartu znehodnotit.

3.4.1 Možnosti ochrany

Karty mnohdy obsahují citlivá data, přístup k citlivým datům, k majetku nebo umožňují přístup do prostor s oprávněnými osobami u přístupových systémů. Proto je třeba karty chránit před zneužitím. Rozhodně preferovat čipové karty před kartami s magnetickým páskem. [28]

3.4.2 Personální ochrana

Největší riziko představuje vyzrazení PIN (Personál Identification Number) kódu. Spousta lidí si neuvědomuje riziko ztráty karty a z pocitu, že mohou někdy zapomenout PIN kód, tak si ho zapíšou na kartu, nebo ho nosí napsaný na papírku společně s ostatními doklady, čímž si zadělávají na problém vykradení konta. [28]

Lidé si také myslí, že moderní karty jsou bezpečné a dají je do rukou pochybným prodejcům, kteří mohou zhotovit plagiát magnetického pásku. Při platbě přes internet musíme dávat pozor na podvodné stránky.

Další z možností je pojištění karty proti neoprávněnému zneužití nebo ztrátě. [25] [26]

3.4.3 Technická ochrana

Jedním z možných řešení, o kterém byla rozvinuta diskuse na serveru idnes.cz je pokusit se poškodit magnetický pásek u hybridní karty. Pak bude možno takovou platební kartou platit pouze přes terminál se čtením čipových karet. Toto řešení má úskalí z právního hlediska, protože majitelem karty je banka.

Další možnosti se nabízejí u bank, které poskytují uzamčení a odemčení platební karty, a to posláním SMS z registrovaného telefonního čísla. [29]

4 PRÁVNÍ ODPOVĚDNOST

4.1.1 Padělání platební karty

Na rozdíl od neoprávněného držení jde o promyšlenou činnost s užitím dobrého technického vybavení a znalostí. Stává se trestným činem a vztahuje se na něj stejný zákon jako v případě padělání bankovek, podle § 140 odstavce 2) TZ , který zní následovně: [30]

Dle § 140 trestního zákona tento trestný čin spáchá:

1. kdo sobě nebo jinému opatří padělané nebo pozměněné peníze (platební kartu), nebo kdo takové peníze (platební kartu) přechovává (§ 140 odst. 1 tr. zákona), nebo

2. kdo padělá nebo pozmění peníze (platební kartu) v úmyslu udat je jako pravé nebo platné, anebo jako peníze vyšší hodnoty (což u platebních karet nepřipadá v úvahu), nebo kdo padělané nebo pozměněné peníze (platební kartu) udá jako pravé (§ 140 odst. 2 tr. zákona).

4.1.2 Zneužití, neoprávněné držení a padělání identifikačních karet

Bohužel na toto nepamatuje zákon jako v případě kreditních karet, lze se ale podle dostupných informací řídit následujícími zákony: [30]

§ 249 Neoprávněné užívání cizí věci

(1) *Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu jich přechodně užívat, nebo kdo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takových věcí, které mu byly svěřeny, přechodně užívá, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo zákazem činnosti.* (2) *Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 značnou škodu nebo jiný zvlášť závažný následek.* [30]

§ 247 Krádež

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a

a) způsobí tak škodu nikoli nepatrnou,

b) čin spáchá vloupáním,

c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,

d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo

e) byl za takový čin v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu nikoli malou.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) způsobí-li takovým činem značnou škodu nebo jiný zvlášť závažný následek.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsah. [30]

5 SOFTWAROVÉ VYBAVENÍ SYTÉMŮ

Softwaru je dnes celá řada a firmy si převážně nechávají software tzv. „ušít na míru“ podle svých potřeb.

Podle druhu použitého softwaru rozlišujeme systémy autonomní a heteronomní. Autonomní systém má v sobě zaimplementovánu databázi a funguje jako samostatný celek. Terminály heteronomního systému pracují převážně autonomně, ale poskytují nadřazenému systému data. Tato data se ukládají a mohou být použity pro výpočet mezd apod. Další důležitou částí systému je uživatelský program, přes který probíhá veškerá komunikace uživatele se systémem. Většinou komunikace probíhá přes klávesnici a grafický displej. Uživatel si zde v menu vybere z nabízených možností. Například si může zvolit druh odchodu. [31]

6 ČTEČKY A TERMINÁLY

6.1 Čtečka

Pojem čtečka značí pouze zařízení schopné identifikovat kartu, číst a popřípadě zapisovat data. Podle typu komunikace mají čtečky v sobě implementovánu elektroniku pro dešifrování a přenos dat. Pro bezkontaktní čtení (RFID) je zde i elektronika pro bezdrátovou komunikaci. Zařízení samo o sobě nesplňuje žádnou funkci. Čtečky jsou vždy součástí nějakého systému. [32]

6.2 Terminál

Slovo terminál je v překladu do českého jazyka překladiště nebo konečná stanice. Pojmem terminál v přístupových systémech je chápán jako kompletní zařízení složené z čtečky, softwaru, uživatelského rozhraní, akčního členu a případné propojení s nadřazeným systémem. Většinou bývá uživatelský software, displej a čtecí zařízení implementováno do jednoho funkčního celku. Pro funkci kontroly vstupu stačí do zařízení nahrát databázi karet a připojit akční člen – nejčastěji otočný turniket. [33]

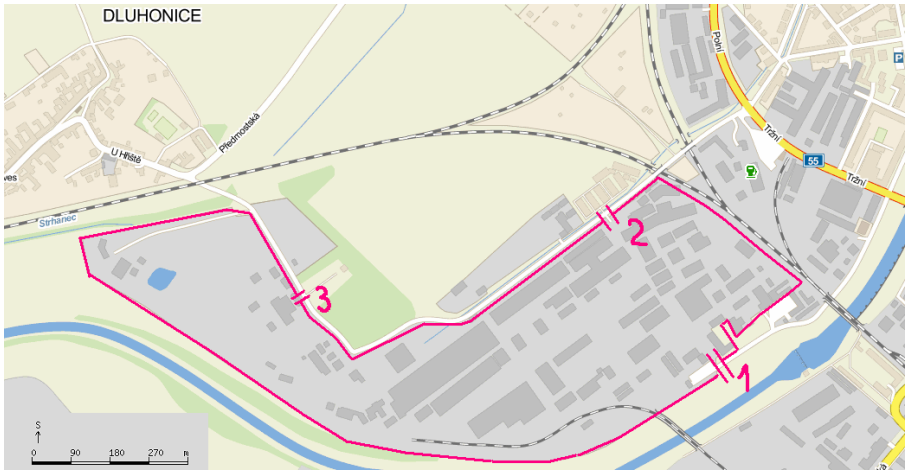
II. PRAKTICKÁ ČÁST

7 ZABEZEPEČENÍ PRŮMYSLOVÉHO ZÁVODU PŘÍSTUPOVÝM SYSTÉMEM

7.1 Seznámení s problematikou

Každý člověk chce svůj majetek hlídat, nebo pod ním mít co nejlepší kontrolu. Přitom ale nechce být omezován a snaží se najít vhodnou alternativu, jak tento problém vyřešit. V teoretické části bylo uvedeno, že čipové karty jsou odolné, spolehlivé a cenově dostupné. Celý systém se pak v kombinaci s vhodným softwarem stává multifunkčním, s velkým potenciálem využití a možností provázání jednotlivých složek systému.

Tyto informace získali i vedoucí zaměstnanci průmyslového závodu Precheza a.s. Přerov. Snažili se o zavedení kontroly vstupu s možností provázání na mzdový systém. Na začátku návrhu byla postavena všechna pro a proti. Především bylo třeba zohlednit, zda provoz systému uspoří v celkové míře finanční prostředky, zvýší bezpečnost a přehlednost. Výsledek byl pozitivní. Vlastní realizaci pak provedla Zlínská firma ComInfo®. Od ledna 2011 je systém plně funkční. Plnou vahou nahrazuje zastaralý „píchačkový“ systém. Střežen je rozsáhlý areál o celkové rozloze 35,5 ha, v němž se kromě vlastní firmy nachází i dalších 12 malých firem. Areál znázorňuje obr. 10. Čísla na obrázku vyznačují místa kontrolovaných vstupů a výstupů. Jelikož samotný systém není úplně dokonalý, je samozřejmostí pravidelný dohled a perfektní fungování fyzické ostrahy.



Obr. 10 Rozloha areálu s vyznačením vrátnic. [34]

7.2 Obecné seznámení se systémem

Celý systém se je tvořen vstupními branami, otočnými turnikety, mobilními a pevnými čtečkami RFID, terminálem s dotykovým LCD displejem, komunikačním rozhraním, záložními zdroji, RFID kartami a softwarem.

Tab. 3 Soupis jednotlivých komponent.

P.č.	Obj. kód	Typ	Položka - popis	kusů
Dodávka hardware				
	obj. číslo	označení	popis	kusů
1	51A90000504000	REI ST	Snímač identifikačních karet, grafický display s LED podsvitem	6
2	51000000040000	REI KP	klávesnice Passport	6
3	550G0000040000	REI-MF1	čtecí hlava REI MIFARE	6
4	51000000003000	ET	rozhraní ETHERNET	6
5	219000000	KPN-12	Napájecí zdroj 12V, 1,8 A, -20 až +50 st.C, 207x110x237 mm	6
6	24701400	AKU	Akumulátor 12V 6,5 Ah	6
7	25000400	Mifare Ultralight	bílá ISO karta bez potisku, přepisovatelná	850
8	25000410	BAR-ST	Tří-ramenný otočný turniket	4
9	25000401	ENCO	Enkodér pro karty MIFARE, USB, napájení z portu USB	1
Dodávka software				
9	71000011	STRUKTURA	Administrace uživatelů	1
10	71000012	CARDS	Správa karet	1
11	71001150	PASSPORT	Základní modul systému docházky, licence na kartu	600
12	71001152	PŘEHLEDY	Denní přehledy přítomnosti, licence na kartu	600
13	71001153	INFO	Zobrazení informace o docházce na snímačích, licence na kartu	600
14	71001154	STATISTIKY	Statistiky a dlouhodobé přehledy, licence na kartu	600
15	71001156	CARDPAY	Správa účtů licence na strávníka	1
16	71001155	MZDY	Standardní spojovací soubory se mzdovým softwarem, licence na k	600
17		Intranet server	Licence na instalaci	1

7.3 Systém kontroly vstupu

Uživatel projde vstupní branou a dojde k turniketu. Při obyčejném každodenním vstupu si nemusí měnit žádné údaje, pouze přiloží kartu. Po úspěšném identifikování v centrální databázi dojde k protočení turniketu. Poté se zapíše do databáze čas a druh příchodu nebo odchodu. Uživatel si může zvolit druh odchodu přímo na snímači karet doplněném o grafický LCD displej, který je instalován na všech třech vrátnicích. Zde je 7 různých nabídek druhů příchodu nebo odchodu. Příchody s odchody se vždy párují.

Pokud bude při odchodu na dovolenou opomněno zadání dovolené, pak při příchodu z dovolené se musí zadat.

Vjezd automobilů do areálu a.s. je také podřízen kontrole čipovými kartami. Pracovníci fyzické ostrahy disponují mobilní čtečkou karet. Každý řidič automobilu musí mít kartu, která identifikuje daný automobil. Pouze v případě mimořádné návštěvy se vydává přenosná karta s papírovou povolenkou.

Kontrola vstupu je kromě tohoto technického vybavení doplněna trvalou přítomností fyzické ostrahy, protože zábradlí i turniket sahají pouze do výše jednoho metru od země. Tvoří tedy pouze psychickou bariéru.

Obr. 11 Vstupní terminál do areálu Prechezy.

7.4 Hardwarové vybavení

7.4.1 Karty

Karta má standardní velikost jako platební karta podle normy ISO/IEC 7810 a vyhovuje standardům elektromagnetické kompatibility. Komunikuje na nosné frekvenci 13,56 MHz. Karta je vložena v ochranném obalu z tvrdého PVC plastu. Potisk karty je barevný. Obsahuje logo firmy, jméno, příjmení, osobní číslo, číslo karty a fotografii o rozměrech 45×34 mm. Podobu karty znázorňuje obr. 12.

Obr. 12 Detail karty.

7.4.2 Čtečky a terminály

Používány jsou pevné i mobilní čtecí hlavy, schopné komunikace s kartami na radiových frekvencích 13,56 MHz a 125 kHz.

Na vrátnicích je nainstalováno celkem 6 kusů pevných multifunkčních terminálů s obchodním označením REA:TOUCH. Terminál se vyznačuje moderním kompaktním designem, grafickým dotykovým displejem o úhlopříčce 7 palců s rozlišením 800×480 obrazových bodů. Podporuje připojení mnoha externích zařízení, z nichž je využíván pouze turniket. Terminál lze umístit pouze v zastřešených prostorách, protože má krytí vůči povětrnostním podmínkám pouze IP42. Program uživatelského rozhraní je velmi dobře propracován. Uživatel si může zvolit ze sedmi druhů příchodu nebo odchodu prostřednictvím dotykového displeje. Po zvolení pouze přiloží kartu. Terminály disponují rozhraním ethernet pro svou vzájemnou komunikaci. V podniku využívají vnitřní podnikové sítě o přenosové rychlosti 100 megabit za sekundu. Terminál je napájen 24 V stejnosměrného napětí, ale lze použít alternativně i napájení PoE. [33] [34]

Obr. 13 Terminál REA::TOUCH. [36]

Dále je instalováno 6 kusu čtecích hlav označených v katalogu jako REI MIFARE. Kvůli absenci displeje není možno měnit druh příchodu nebo odchodu. Ten se automaticky páruje s předchozím. Čtečky mají podstatně menší rozměry a mohou být díky krytí IP 67 použity i ve venkovních prostorách. Dva kusy REI MIFARE jsou na hlavní vrátnici k použití druhého turniketu. Další dva jsou na vrátnici ZOK a při vjezdu na hlídané podnikové parkoviště.

7.4.3 Turnikety

Použit je tříramenný trnový turniket, obchodně značený jako BAR-ST. Vyniká elegantním designem a spolehlivým provozem. V turniketu je pohonná jednotka s funkcí Fail-safe. Tato funkce otevírá turniket pro volný průchod v případě výpadku energie. V případě výpadku energie je provozu schopný ještě 6 hodin díky záložnímu olověnému akumulátoru. Mechanicky turniket dovoluje oboustranný průchod a kapacita průchodnosti se pohybuje v rozmezí 15 až 30 osob za minutu. Turniket je řízen signálem se sériovým přenosem dat RS485 z terminálu. Turniket je napájen 12 V DC s klidovým odběrem 12,5 W, s nárůstem na 15 W při průchodu. [35]

7.5 Softwarové vybavení

7.5.1 Zpracování uživatelského menu

Uživatelské menu je velice přehledně zpracováno. Užíváno je šest standardních voleb, doplněných o sedmé programovatelné tlačítko, pojmenované jako služební pochůzka. Výchozím bodem je položka s číslem 1, kterou není třeba zadávat a značí každodenní příchod a odchod. Zaměstnanec si na dotykové obrazovce dále může zvolit ze sedmi položek pro změnu. V tu chvíli se na displeji zobrazí: „Přiložte kartu“. Pokud do 10 sekund nedojede k přiložení karty, systém automaticky navrátí volbu číslo 1. Pokud pracovník omylem zvolil nesprávný druh přerušení pracovní doby, může učinit opravu do 59 vteřin. Zadání jiného druhu páruje se páruje, takže stačí zadat pouze jedenkrát, buď při odchodu nebo příchodu. [36]

- **Popis položek menu**
  - Položka č. 1 registruje počet odpracovaných hodin. Je automaticky zvolena jako výchozí.
  - Položka č. 2 je služební cesta, je to placená forma pracovní nepřítomnosti, sloužící k odjezdu z areálu za účelem prezentace firmy, externího školení nebo nákupu zboží.
  - Položka č. 3 funguje jako odchod na oběd.
  - Položka č. 4 značí odchod k lékaři.
  - Položka č. 5 značí placenou dovolenou.
  - Položka č. 6 značí nepřítomnost zapříčiněnou nemocí zaměstnance.
  - Položka č. 7 značí odchod na oddělené pracoviště vně areálu.

Obr. 14 Volba druhu nepřítomnosti. [36]

- **Informace o odpracované době**

Zaměstnanec má možnost nahlédnout na základní informace o stavu odpracovaných hodin stiskem klávesy Info a přiložením karty do 5 sekund od zadání. Následně se na displeji objeví stav celkových odpracovaných hodin, rozdíl vůči obvyklému fondu, počet odpracovaných směn a všechny ostatní příchody nebo odchody mimo položku číslo 1 – pracovní dobu. V jednotlivých položkách lze listovat tlačítky se symbolem šipky nahoru a šipky dolů. [36]

7.5.2 Software pro evidenci docházky

Evidence docházky je zpracovávána programem PASSPORT. Ten je vlastním produktem firmy ComInfo. Program PASSPORT umí evidovat docházku, zpracovat surová data pro mzdovou účtárnu a počítat utracenou finanční částku v podnikové kantýně. Jelikož firma Precheza a.s. je rozsáhlý podnik, využívá ještě doplnění systému o program WATT. Tento program je intranetovou nadstavbou a umožňuje získání různých podrobných výpisů. Pro usnadnění orientace slouží šedesáti stránkový manuál s obrázky.

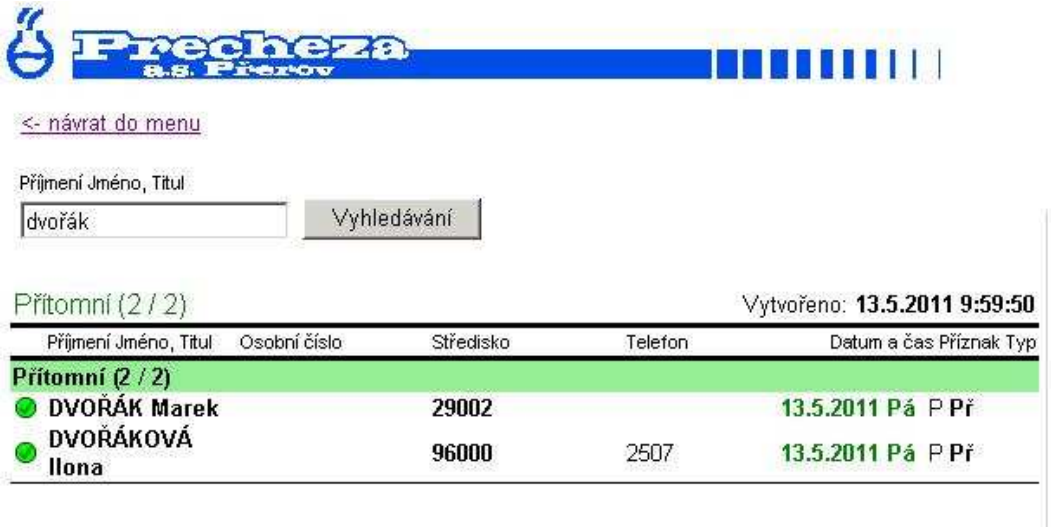
- **Funkce programu PASSPORT**

Pracovní doba se vypočítává programem PASSPORT2.0. Cílem je vyhodnotit a zpracovat primární data produkovaná ve snímačích. Běh výpočtu se řídí podle zadaných kritérií, mezi které patří model pracovní doby, časová kategorie a mzdová složka. Program běží takzvaně „na pozadí“ a pracuje autonomně. Program umí komunikovat s programem WATT. [37]

- **Funkce programu WATT**

Program běží v podnikové síti intranet a jeho prohlížení je možné přes jakýkoli internetový prohlížeč. Pro správnou funkci musí mít počítač nainstalovánu platformu Java. Bez hesla se mohou zaměstnanci dostat pouze na přítomnost. Další funkce se odemykají až po přihlášení. [37]

- **Základní využívané funkce programu WATT**
  - Přítomnost
  - Seznam osob
  - Editace docházky
  - Editace mzdové složky
  - Schválení práce navíc
  - Přehled docházky za určité období
- **Další, nevyužívané funkce programu WATT**
  - Docházková fotografie



Obr. 15 Ukázka vyhledání údaje o přítomnosti zaměstnance

7.6 Režimová opatření

Systém kontroly vstupu sám o sobě není bezpečný. Pokud by došlo k odcizení karty, mohl by se neoprávněně dostat do objektu téměř kdokoli. Toto riziko je sníženo na minimum díky pohotové fyzické ostraze, která namátkově kontroluje totožnost zaměstnance fotografie vytištěné na čipové kartě. Rovněž funguje kontrola příručních zavazadel, zde je zmenšeno riziko vnesení nebo vynesení věcí schovaných v zavazadlech.

7.7 Návrhy a nedostatky

7.7.1 Nedostatky

I přes velmi dobrou práci fyzické ostrahy by bylo dobré kontrolu vstupu doplnit kamerovým systémem CCTV, a to s možností záznamu. Kontrola zavazadel by se dala vyřešit rentgenovým detektorem, ale po zvážení rizik a pořizovací ceny je tento návrh příliš nadnesený i vzhledem k charakteristice střeženého objektu.

Při vjezdu na hlídané parkoviště je čtecí hlava vzdálena příliš daleko a uživatel má velký problém přiblížit kartu dostatečně blízko. Dalším malým nedostatkem v parkování je absence funkce antipassback. To by sice nevadilo, ale zaměstnanci často riskují a na zvednuté závoře projedou někdy i druhým automobilem bez přiložení karty. Je jen otázkou času, kdy na někoho závora spadne. Antipassback by mohl tomuto částečně zabránit.

Při dalším zkoumání byly objeveny už jen malé nedostatky, které není potřebné bezodkladně řešit. Například nikdo nepozná, jak dlouho se zaměstnanec zdržel na obědě a kdy skutečně dorazil na místo svého pracoviště.

7.7.2 Doplnění služeb

Za zmínku stojí instalace tiskárny v každé větší budově, s instalací čtecí hlavy REI MIFARE, s možností veřejného tisku za poplatek. Dále by bylo dobré přidat na hlavní vrátnici terminál pro zjištění útraty v podnikové kantýně, s možností náhledu historie plateb. Stav sice jde kontrolovat na počítači připojeném do podnikové sítě intranet, ale ne všichni zaměstnanci mají k počítačům přístup.

8 VYUŽITÍ KARET V BUDOUCNOSTI

Čipové karty začínají být velice populární. Je naprosto jasné, že v budoucnosti bude provedena spousta změn. Budoucnost se nedotkne pouze samotných karet, ale především různých modifikací karet v podobě hodinek, samolepících pásků a jiných pouzder, v nichž jsou zalisovány čipy a cívka. Dojde k miniaturizaci. Rozšíření poroste asi stejným tempem jako dodnes. Dá se čekat postupné snižování ceny čipu díky masové výrobě. Rychlý vývoj zasáhne bezpečnostní a zábavní průmysl. [38]

8.1 Čipové karty v hromadné dopravě

Hromadná doprava dnes zažívá velký odliv zákazníků, a to především kvůli vysokým nákladům. Největší problém je v provázanosti jednotlivých druhů dopravy a nutnosti kupovat si lístek. Pro budoucí rozvoj a přilákání zákazníků k tomuto způsobu dopravy bude nutné provést integraci jednotlivých složek systému. Toho lze docílit využitím čipových karet. Předseda Výboru pro dopravu zastupitelstva hl. m. Prahy Petr Hána tvrdí, že bude nutné sloučit všechny druhy dopravy. Podle propočtů dojde k úspoře několika desítek milionů korun. Kontrola jízdenek by probíhala za použití mobilních čteček pracujících online. Zatím takto fungující systém funguje na principu předplacených karet. Otázka platby přímo z účtu bez nutnosti dobíjet „kredit“ nebo ověření identity zatím není dořešena. Pro další budoucí vývoj se dá počítat se zaimplementováním do jedné multifunkční karty nebo s využitím mobilního telefonu. [39]

8.2 Budoucnost čipů v zábavním průmyslu

Čipy mohou být umístěny prakticky v jakýchkoliv pouzdrech, toho je už dnes využíváno například v plaveckých areálech. Vše bude otázkou součinnosti poskytovatelů služeb. Čím širší bude okruh využití, tím lépe pro uživatele. Pokud se povede tuto myšlenku realizovat, budeme moci mít jeden čip, umístěný například v hodinkách. Pro vstup a využívání služeb ve všech zábavních střediscích, hotelích apod. Finančně by systém fungoval buď stržením částky z účtu, nebo formou předplacení přes internetové bankovnictví. [40]

8.3 Budoucnost platební sféry

V nejbližší budoucnosti, řádově několika málo let, budou vydavatelé bankovních kreditních karet úplně upouštět od hybridních karet s málo bezpečným magnetickým páskem. Papírové peníze budou v budoucnu splňovat svou funkci jako dnes, ale ve velmi omezeném rozsahu. Po dořešení otázky zrychlení běhu transakcí lidé budou platit penězi pouze drobné nákupy a platby. Stále více obchodníků bude přecházet na moderní způsob platby – čipovou kartou. Vizí obchodních řetězců bude implementovat do čipové platební karty tzv. věrnostní karty. Zákazník by poté mohl přes internetové bankovnictví dokonce vidět seznam nakoupeného zboží i nabídku slev u různých obchodníků na základě věrnosti. [41]

Platební karty se pak někdy v budoucnu stanou pouze součástí jedné karty, která možná nahradí všechny jiné karty, které dosud používáme jednotlivě. Naprostou novinkou bude placení prostřednictvím mobilního telefonu. [42]

8.4 Multifunkční karta

Navrhovaný systém by měl v sobě implementovány osobní identifikační doklady, řidičský průkaz, zdravotní průkaz, kreditní kartu, elektronickou jízdenku apod. Již dnes není problémem tuto kartu vyrobit. Problémem k řešení do budoucna je otázka zabezpečení. Určitá osoba se smí dostat pouze k určitým datům, nikoli ke všem údajům uloženým v kartě. Dalším problémem je globalizace. [43]

8.5 Technologie NFC

Tato technologie představuje moderní systém placení nebo identifikace. Je stejně bezpečnou formou identifikace jako při použití čipové karty. Jedná se o bezkontaktní přenos informací po radiových vlnách mezi mobilním telefonem a terminálem. Technologie byla navržena a testována už v roce 2008. K masovému rozšíření doposud nedošlo. Komunikace probíhá na radiových vlnách na frekvenci 13,56 MHz. Dá se čekat, že tato technologie brzy vytlačí klasické plastové čipové karty.

Nevýhodou je omezení uživatele na funkčnost mobilního telefonu. V případě vybití baterie mobilu se můžete snadno dostat do problému. Na toto budou muset

pamatovat výrobci telefonů a doplnit telefon záložním zdrojem energie pro případ nouze. [44]

9 ZKOUŠKA FYZICKÉ A ELEKTRICKÉ ODOLNOSTI

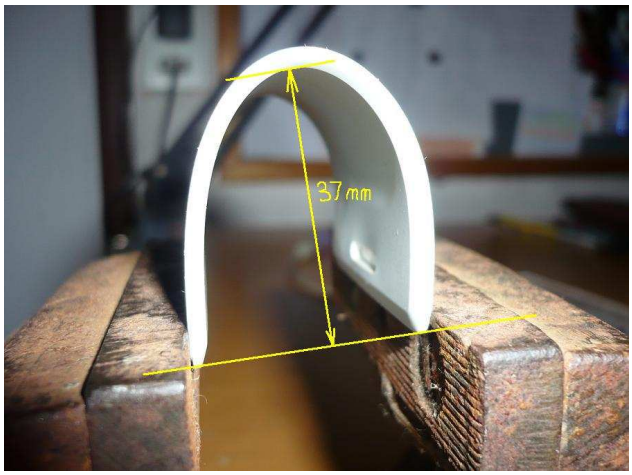
V této části bylo zjišťováno, do jaké míry dokáží karty odolávat fyzickým a elektrickým útokům. K testům byla použita RFID karta od firmy Motorola a čtečka KIF 1 od firmy Duha systém.

9.1 Odolnost mechanická

Zkouška mechanické pevnosti byla prováděna podélným ohybem a postupným měřením průhybu pomocí posuvného měřidla. Tento druh namáhání definuje norma ISO/IEC 7816-1, podle které karty musejí vydržet bez jakéhokoliv poškození průhyb 20 mm. [14]

Testovaná karta je vyrobena z odolného ABS plastu a je opatřena PVC fólií, která by měla podle informací napsaných v teoretické části, viz str. 17, podstatně zvýšit pevnost. To se stalo pravdou.

Při testování byla karta chycena do strojního svěráku a postupně prohýbána. Měřený průhyb dosáhl maximální hodnoty 37 mm. Tento stav dokazuje obr. 15. Přiblížením čtečky v tomto okamžiku bylo ověřeno, že je karta stále funkční. Dále byla karta uchycena do svěráku v místě ohybu. Následným přitahováním konečně došlo k prasknutí karty, ale díky kujnosti mědi nedošlo k přetržení tenkých drátků závitů antény, tudíž karta funguje i po takovéto razantní destrukci.



Obr. 16 Naměřený podélný průhyb karty.

Obr. 17 Zlom karty.

9.2 Odolnost elektrická

Při provádění zkoušky na elektromagnetickou odolnost bylo využito běžně dostupných prostředků v domácnosti a měřících přístrojů. Podle normy ISO musí karty splňovat požadavky na EMC.

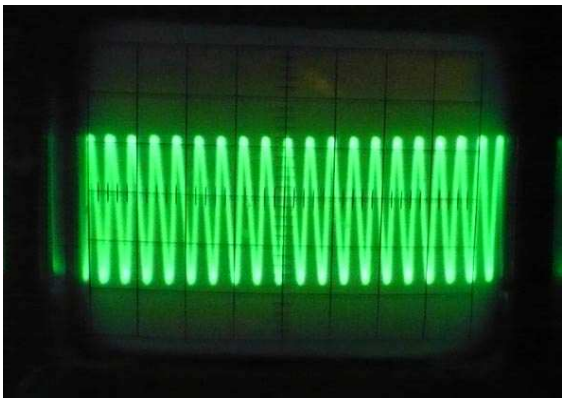
Obr. 18 Detail obnaženého čipu.

9.2.1 Měření elektrických vlastností karty

Smyslem měření bylo zjistit, zda mohou být čipy ohroženy naindukováním nežádoucích napětí z přístrojů používaných v domácnosti (EMC). Měření bylo prováděno na vypreparované cívce a čipu s pomocí milivoltmetru a osciloskopu. Cívka byla položena na čtečku. Nejprve byla změřena frekvence a velikost výstupního napětí na cívce. Multimetrem změřená frekvence činila 125 kHz a napětí 2,5 V. Hodnota frekvence se shoduje s hodnotou danou normou ISO/IEC 7816. Ověření správnosti měření bylo provedeno na osciloskopu. Po přepočítání dílků na obrazovce a odečtením nastavené periody se měření shoduje.

S rostoucí vzdáleností klesá hodnota indukovaného napětí z 2,5 V na nejmenší změřenou hodnotu 50 mV ve vzdálenosti 1,1 m.

Spojením čipu s cívkou bylo sledováno, jakého minimálního naindukovaného napětí je zapotřebí pro vzájemnou komunikaci. Čtečka přečetla kartu ve vzdálenosti 10 cm. Naindukované střídavé napětí dosáhlo hodnoty 1,9 V a vykreslilo pravidelnou sinusovku. V okamžiku komunikace nastal malý zákmit.



Obr. 19 Detail nosné frekvence 125 kHz.

Měření dále pokračovalo záměnou čtečky za mobilní telefon. Naměřené napětí dosáhlo pouze hodnoty 50 mV. Takto malá hodnota nemůže ohrozit kartu. Měření ale není přesné, protože mobilní telefon pracuje na modulované frekvenci 800 MHz a 1,8 GHz. Daný měřicí přístroj nedokáže měřit v takovémto rozsahu. Toto zjištění vůbec nevadí, protože karta se také nedokáže přizpůsobit takové vysoké frekvenci díky frekvenční zádrži. Dalším aspektem je konstrukce antény (cívky). Cívka totiž indukuje největší napětí pro frekvence kolem 125 kHz. Jiné frekvence tlumí.

9.2.2 Zkouška odolnosti na elektrostatický náboj

Tento test byl prováděn vpuštěním elektrostatického náboje z piezoelektrického zapalovače o přibližném elektrostatickém napětí 5 kV. Na připojenou cívku byl ve třech pokusech přiveden statický náboj. Ani jednou nedošlo k nevratnému zničení čipu. Cívku tvoří hodně závitů, takže je možné, že se náboj probil do středu navinutého drátu a napětí se rychle utlumilo. Po odpojení cívky byl elektrický náboj přiveden přímo na kontakt čipu. Po prvním zásahu se povedlo čip zničit.

10 POROVNÁNÍ S JINÝMI SYSTÉMY

10.1 Porovnání s biometrickými systémy

Biometrický systém je sám o sobě bezpečný a nabízí velkou škálu možností sledování rozdílností jedinců. Navzdory přínosu se problematika kontroly biometrickými systémy potýká s kritikou zneužití osobních dat. Naproti tomu čipový identifikační systém je bezpečný jen za předpokladu ověření PINU. Hlavním rozdílem systémů je v tom, že čtečka načte kartu a jednoznačně ji identifikuje. Biometrické systémy jsou postaveny na principu porovnávání.

10.1.1 Čip vs. DNA

Metoda ověření DNA je jedna z nejspolehlivějších, protože bylo dokázáno, že je téměř mizivá šance, aby měli dva lidé stejnou DNA. Nevýhodou je zdlouhavý proces zjištění a porovnání DNA.

10.1.2 Čip vs. otisk prstu

Otisk prstu je v oblasti kontroly vstupu bezpečnější než čipové karty. S velkou výhodou se používá tam, kde je třeba chránit větší majetek a není kladen důraz na čistotu. Systém se nehodí pro kontrolu vstupu zaměstnanců pracujících holýma rukama s abrazivním materiálem. Levnější detektory mají kapacitu omezenu na 300 vzorků otisků. U čipových karet je kapacita téměř neomezená. [45]

10.1.3 Čip vs. Duhovka a sítnice

Z pohledu úspěšnosti je tato metoda vynikajícím řešením pro zabezpečení, pro velmi nízkou pravděpodobnost chyby. Úspěšnost detekce se velkou měrou snižuje při různých onemocněních oka. Je mnohem bezpečnější metodou kontroly jako čipová karta. [45]

10.2 Porovnání s fyzickou ostrahou

Fyzická ostraha je relativně dobrá, ale v případě přestrojení pachatele pracovník ostrahy nepozná na základě fotografie, zda se jedná o osobu neoprávněnou ke vstupu. Až identifikace čipem za podmínky zadání PINU je plnohodnotná.

ZÁVĚR

Karty mají za sebou od svého prvotního zrodu již celé století neustálého vývoje, především díky oblíbenosti v používání veřejností. Vývoj zaměstnal celou řadu vědců, analytiků a bezpečnostních inženýrů. Vždy byla na prvním místě ochrana dat uložených na kartě, nebo opatření proti neoprávněnému užití. S postupem času a zdokonalováním techniky se objevovaly nové technologie výroby a posléze se upouštělo od starších typů karet. Tak se přešlo z papírové kartičky s natištěnými údaji k moderním čipovým kartám. Pro sjednocení a globalizaci byly vydány mezinárodní certifikáty, jimiž se výrobci musí řídit.

Dnes karty s oblibou používá spousta lidí, protože jsou cenově dostupné a nabízí komfortní použití a dobré zabezpečení dat. I přes vysokou bezpečnost jsou známy metody, jimiž lze prolomit bezpečnost. Po technické stránce jsou to útoky postranními kanály, které využívají chyby v běžícím procesu. Na základě informací z chybových hlášek je možné získat důležité informace z karty. Druhým velikým problémem je vlastní neopatrnost držitelů karet. Uživatelé často podceňují ochranu svých karet. Z hlediska právní odpovědnosti myslí zákony České republiky na ochranu karet trestním zákonem, zákonem o neoprávněném užívání cizí věci a krádeže. Čipové karty samy o sobě nemají žádný význam. Potřebují ke své plnohodnotné funkci obslužný software a čtecí terminál. Softwaru a hardwaru je dnes k dostání nepřeberné množství.

Praktická část práce je zaměřená na analýzu využití čipových karet v podniku Precheza a.s. a seznámila nás s používaným systémem od firmy ComInfo. Dále se zaměřením na rozsah využití a popsala jednotlivé technické prvky systému. Další část se zabývala softwarem pro zajištění správného fungování jak pro docházkový systém, tak při zajištění bezpečnosti. Při zkoumání bylo zjištěno, že systém funguje podle teoretických předpokladů, a nedostatky v podobě absence kamerového systému, automatického systému kontroly zavazadel a špatné funkce parkovacího systému. Nebyly zjištěny další závažné nedostatky.

Budoucí vývoj karet bude velmi rozmanitý. Umožní bezproblémové cestování hromadnou dopravou, zrychlí se platby v obchodech. Možný je ale také přechod od technologie čipových karet na bezdrátovou technologii NFC. Tato technologie umožní komunikovat s terminálem prostřednictvím mobilního telefonu.

V deváté kapitole byla popsána vlastní studie chování karty od firmy Motorola. Test zahrnoval zkoušku na mechanickou a elektronikou odolnost. Výsledky testu odpovídají normám.

Poslední část srovnává praktické využití karet proti biometrickým systémům. Porovnáním nebylo dosaženo relevantních výsledků, protože jednotlivé systémy jsou odlišné a každý má jiné výhody a nevýhody.

Z grafů vyplývá, že alespoň nějakou platební či úvěrovou kartu využívá 90 % dotázaných. O budoucnosti karet toho příliš nevědí a polovina dotázaných by nechtěla multifunkční kartu. Bezpečnosti platebních karet věří 70 % dotázaných. Na tyto dotazy odpovědělo deset studentů, dvanáct důchodců a osm pracujících.

Práce nemohla do úplných detailů popsat celou problematiku, protože čipové karty nabízejí obrovský potenciál využití. Systém zabezpečení je složitý a velice obsáhlý.

ZÁVĚR V ANGLIČTINĚ

The cards have taken a huge effort of keeping itself in development almost a whole century thanks to the public popularity. The development itself took a lot of time of many scientists, analysts and security engineers. Secured data and unauthorized use protection have always been in the first place. With the time going forward many producers have improved manufacturing technology to progressively substitute old types of cards with new ones. That is how paper cards with printed dates have been replaced with modern chip cards. International certificates have been created for the globalization and unification and the manufacturers must follow their lead.

Lots of people like using cards in these days, because they are cheap, easy to use and offer good security. Despite all security elements there are known methods how to hack the security. On the technical side these are side channel attacks, which use errors in running process. Based on information gained from error logs one can manage to steal important data from the chip card. Other big issue comes with the card holder's carelessness. The users usually underestimate protecting their cards. Terms of legal responsibility in Czech Republic is held by the criminal law, the law on unauthorized use and theft. Chip cards themselves have no meaning. They need a utility software and a reading terminal to operate at full service. There is plenty of software and hardware available to purchase in these days.

The practical part of this thesis is focused on an analysis of usage of chip cards in Precheza a.s. company introduced the system developed by ComInfo company. Meanwhile I am focused on the range of applications and description of individual technical system elements. Software attendance system took next part in my examination whether the whole system works properly. After a while of research I have found that all aspects works fine as expected. No lacks have been found up to the missing CCTV system, automatic luggage control and bad parking system.

Chip cards are facing a bright and multiple future enabling traveling within public transportation without any problems, speeding up payments at stores. There is also a possibility of having the technology replaced by a wireless NFC technology. This technology allows to communicate with the terminal using just a cellular phone.

In the ninth chapter there is description of study of Motorola's card behavior. The test involves a mechanical and electrical endurance. The results conform to the standard.

The last chapter compares practical card use with biometric systems. Individual systems differs and that is why I could not come up with relevant results. Both have its advantages and disadvantages.

As you can see in the graphs, at least one credit or debit card is used by ninety percent of the respondents. They do not know much about the upcoming future and half of them is not interested in multipurpose card. Seventy percent of the respondents believe their cards are secure enough. The respondents consist of ten students, twelve retired and eight employees.

This thesis could not cover all details, because chip cards offer a huge potential of utilization. The security system is complicated and very extensive.

SEZNAM POUŽITÉ LITERATURY

[1] *Jak vznikly čipové karty - iDNES.cz* [online]. 2006-02-04 [cit. 2011-03-23]. Jak vznikly čipové karty. Dostupné z WWW: <http://finance.idnes.cz/jak-vznikly-cipove-karty-0xy-/bank.asp?c=A060201_151019_fi_osobni_zal>.

[2] *Bankovnictvi.iHNed.cz* [online]. 2010-09-06 [cit. 2011-03-08]. Svět platebních karet se mění před očima. Dostupné z WWW: <http://bankovnictvi.ihned.cz/c1-46449170-svet-platebnich-karet-se-meni-pred-ocima>.

[3] Historie, současnost a budoucnost čipových karet. In *Čipové karty* [online]. Ostrava: VŠB-TU Ostrava, 2005-10-07 [cit. 2011-03-24]. Dostupné z WWW: <http://homel.vsb.cz/~nav79/cipkart/cphisobu.htm>.

[4] *JUŘÍK, P.:* Encyklopedie platebních karet – Historie, současnost a budoucnost peněz a platebních karet, *1. vydání, Praha: Grada Publishing, spol. s.r.o., 2003. 312 s. ISBN 80-247-0685-7*

[5] JUŘÍK, P.: *Svět platebních a identifikačních karet*, 1. vydání, Praha: *Grada Publishing, spol. s.r.o1999. 248 s. ISBN 80-7169-759-1*.

[6] *Embosovaná karta* [online]. 2009 [cit. 2011-04-08]. Embosovaná karta. Dostupné z WWW: <http://embosovana-karta.webnode.cz/>.

[7] *Laminovaná optická karta VIS - Produktový katalog TOP kontakt* [online]. Internet Trading, s.r.o., 2011 [cit. 2011-04-12]. Laminovaná optická karta VIS. Dostupné z WWW: <http://produkty.topkontakt.idnes.cz/p/laminovana-opticka-karta-vis/450530/>.

[8] ČERVENKA, Pavel. *Studie RFID čipů a bezkontaktních čipových karet se zaměřením na bezpečnostní prvky* [online]. Praha: ČVUT FEL, 2008. 57 s. Bakalářská práce. České vysoké učení technické - fakulta elektrotechnická. Dostupné z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/cervepe1_2008bach.pdf>.

[9] *SOOM.cz - Bezpečnost magnetických karet* [online]. 2011 [cit. 2011-03-22]. Bezpečnost magnetických karet. Dostupné z WWW: <http://www.soom.cz/index.php?name=articles/show&aid=427>.

[10] ŠPATENKA, Martin. *Aplikace pro prohlížení záznamů na paměťové kartě řidiče* [online]. Pardubice: Univerzita Pardubice, 2010. 75 s. Diplomová práce. Univerzita Pardubice - Dopravní fakulta Jana Pernera. Dostupné z WWW: <http://dspace.upce.cz/bitstream/10195/36612/1/SpatenkaM_AplikaceProhlizeni_VP_2010.pdf>

[11] DOLEŽAL, Ivan. *Svět tisku - Zajímavé možnosti termotransferového potisku* [online]. 2003-10 [cit. 2011-05-02]. Svět tisku. Dostupné z WWW: <http://www.svettisku.cz/buxus/generate_page.php?page_id=209>.

[12] *Plastové karty - MCARD.cz* [online]. 1999 [cit. 2011-05-03]. Plastové karty. Dostupné z WWW: <http://www.mcard.cz/plastove-karty>

[13] SILNÝ, Martin. *Čipové karty - demonstrativní aplikace* [online]. Praha, 2007-08. 54 s. Bakalářská práce. České vysoké učení technické - fakulta elektrotechnická. Dostupné z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/silnym1_2007bach.pdf>.

[14] *Identifikační karty - Fyzikální charakteristiky* [online]. ČSN ISO/IEC 7810. Český normalizační institut, 2004, 2004-04 [cit. 2011-05-10]. Česká technická norma. Dostupné z WWW: <http://nahledy.normy.biz/nahled.php?i=70891>.

[15] *OKsystem - Technologie čipových karet* [online]. 2011 [cit. 2011-05-01]. Technologie čipových karet. Dostupné z WWW: <http://www.oksystem.cz/o-nas/servis-pro-novinare/napsali-o-nas/2005/07-business-world>.

[16] RAKL, Wolfgang; EFFING, Wolfgang. *Příručka čipové karty*. 3. [s.l.] : John Wiley a synové, 1997. 420 s. ISBN 0-471-96720-3.

[17] KRHOVJÁK, Jan. *Analýza útoků na aplikační programovací rozhraní pro hardwarová bezpečnostní zařízení* [online]. Brno: Masarykova univerzita v Brně, 2004-09-15. 82 s. Oborová práce. Masarykova univerzita - Fakulta informatiky. Dostupné z WWW: <http://www.fi.muni.cz/~xkrhovj/apinf/SDIPR/DP_upravena_v1.pdf>.

[18] *Dhar's Blog: Introduction to Smart Cards* [online]. 2004-11-16 [cit. 2011-05-02]. Dhar's Blog. Dostupné z WWW: <http://sumitdhar.blogspot.com/2004/11/introduction-to-smart-cards.html>.

[19] NÁVRAT, Lubomír, et al. *Čipové karty - Typy karet* [online]. 2005-10-07 [cit. 2011-05-03]. Typy čipových karet. Dostupné z WWW: <http://homel.vsb.cz/~nav79/cipkart/cptypy.htm>.

[20] MATĚJKA, Jiří. *ÚTOKY POSTRANNÍMI KANÁLY NA CIPOVÉ KARTY* [online]. Brno, 2010. 88 s. Diplomová práce. Vysoké učení technické v Brně. Dostupné z WWW: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=28101

[21] Český normalizační institut. *ČSN ISO/IEC 7816-1 (369205) - Náhled normy* [online]. 2003 [cit. 2011-05-02]. Česká technická norma. Dostupné z WWW: <http://nahledy.normy.biz/nahled.php?i=69219>.

[22] MATTHEWS, Adam. Low Cost Attacks on Smart Cards The Electromagnetic Side-Channel. *Next Generation Security Software Ltd* [online]. 2006-09, 1, [cit. 2011-04-20]. Dostupný z WWW: <http://www.google.cz/url?sa=t&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fwww.nccgroup.com%2FLibraries%2FDocument_Downloads%2F09_06_Low_Cost_Attacks_on_Smart_Cards_-_The_Electromagnetic_Side-Channel_sflb.sflb.ashx&rct=j&q=MATTHEWS%2C%20Adam.%20Low%20Cost%20Attacks%20on%20Smart%20Cards&ei=26XGTayJAYL1sgaOoJD_Dg&usg=AFQjCNEnmcFWECCjYDNkL343PLszLK6lzA&cad=rja>.

[23] BERKELS, Jem. *Side-Channel Monitoring of Contactless Java Cards* [online]. Ontario, Canada, 2008. 79 s. Diplomová práce. University of Waterloo. Dostupné z WWW: <http://www.sysdesign.ca/archive/jb-thesis-final-electronic.pdf>.

[24] *Jsou čipové karty bezpečné? - Lupa.cz* [online]. 2006-03-27 [cit. 2011-05-04]. Jsou čipové karty bezpečné. Dostupné z WWW: <http://www.lupa.cz/clanky/jsou-cipove-karty-bezpecne/>.

[25] BELLA, Tomáš; ULEJ, Tomáš. *Čipové karty je ľahké prečítať | Téma | pocitace.sme.sk* [online]. Petit Press, 2009-10-27 [cit. 2011-05-06]. Čipové karty je ľahké prečítať. Dostupné z WWW: <http://pocitace.sme.sk/c/5080757/cipove-karty-je-lahke-precitat.html>.

[26] TENORA, Lukáš. *KRYPTOGRAFICKÉ MODULY PRO ZABEZPECENÍ SÍTÍ* [online]. Brno: VUT Brno, 2008. 63 s. Bakalářská práce. Vysoké učení technické v Brně - Fakulta Elektrotechniky a komunikačních technologií. Dostupné z WWW: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=9383&lang=0>.

[27] TŮMOVÁ, Věra. *Češi stále u karet i účtů podceňují ochranu hesel a PIN: Platební karty | Zprávy: ZLATÁ KORUNA* [online]. 2009-01-19 [cit. 2011-05-09]. Češi stále u karet i účtů podceňují ochranu hesel a PIN. Dostupné z WWW: <http://www.zlatakoruna.info/clanky/39-10-platebni-karty/17743-cesi-stale-u-karet-i-uctu-podcenuji-ochranu-hesel-a-pin>.

[28] TŮMOVÁ, Věra. *Má smysl pojistit bezpečnou kartu s čipem? - Peníze.cz* [online]. 2007-10-16 [cit. 2011-04-09]. Má smysl pojistit bezpečnou kartu s čipem?. Dostupné z WWW: <http://www.penize.cz/platebni-karty/29441-ma-smysl-pojistit-bezpecnou-kartu-s-cipem>.

[29] CHVÁTA, Dalibor. *Čipová karta s domácí úpravou pro lepší bezpečnost - Měšec.cz* [online]. 2008-02-20 [cit. 2011-04-09]. Čipová karta s domácí úpravou pro lepší bezpečnost. Dostupné z WWW: <http://www.mesec.cz/clanky/cipova-karta-s-domaci-upravou-pro-lepsi-bezpecnost/>.

[30] *Trestní zákon - Část II. - Hlava IX. - Trestné činy proti majetku* [online]. 2008 [cit. 2011-03-03]. Zákon č. 140/1961 Sb., trestní zákon. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/trestni_zakon/cast2h9.aspx#>.

[31] GREEN Center s.r.o. *Autonomní systémy* [online]. 2008 [cit. 2011-05-19]. Autonomní systémy. Dostupné z WWW: <http://www.green.cz/stranka-autonomni-systemy-8>.

[32] GEDIP, s.r.o. *Čtecí hlavy RFID* [online]. 2011 [cit. 2011-05-09]. Čtecí hlavy RFID. Dostupné z WWW: <http://www.cominfo.cz/cz/kategorie/cteci-hlavy-rfid.aspx>.

[33] GEDIP, s.r.o. *Terminál REA* [online]. 2011 [cit. 2011-05-09]. Terminál REA. Dostupné z WWW:<http://www.cominfo.cz/cz/kategorie/cteci-hlavy-rfid.aspxhttp://www.cominfo.cz/cz/kategorie/terminal-rea.aspx>.

[34] *Mapy.cz* [online].NAVTEQ, 2010 [cit. 2011-05-02]. Mapy.cz. Dostupné z WWW: <http://www.mapy.cz/#mm=ZP@x=140030528@y=133774016@z=14>.

[35] ComInfo. *Turniket BAR - ST* [online]. 2010 [cit. 2011-05-16]. Turniket BAR - ST. Dostupné z WWW: <http://www.cominfo.cz/cz/produkt/176-tur-turniket-bar--st.aspx>.

[36] Metodika obsluhy snímače bezkontaktních identifikačních karet: REA::Touch. In ComInfo. *Metodika obsluhy snímače bezkontaktních identifikačních karet*. Zlín: ComInfo, 2010-09-07. s. 7.

[37] ComInfo a.s. Uživatelská dokumentace: Watt. *Uživatelská dokumentace* [online]. 2003, 1, [cit. 2011-05-16]. Dostupný z WWW: <https://watt.ukf.sk/doc/manual_user.pdf>.

[38] *Čipové karty už nejsou jen čipové karty* [online]. 2011, 2011-04-21 [cit. 2011-05-06]. Čipové technologie nejsou jen čipové karty. Dostupné z WWW: <http://bankovnictvi.ihned.cz/c1-51620120-cipove-technologie-nejsou-jen-cipove-karty>.

[39] Ekolist.cz. *Jaká je budoucnost hromadné dopravy? Zřejmě v čipových kartách - Ekolist.cz* [online]. Ekolist.cz [cit. 2011-05-05]. Jaká je budoucnost hromadné dopravy? Zřejmě v čipových kartách. Dostupné z WWW: <http://ekolist.cz/cz/zpravodajstvi/zpravy/jaka-je-budoucnost-hromadne-dopravy-zrejme-v-cipovych-kartach>.

[40] *Trh Zábavy* [online]. 2005-06 [cit. 2011-05-01]. Trh zábavy. Dostupné z WWW: <http://www.trhzabavy.cz/_0506/050612sz.php>.

[41] ROSLEROVÁ, Andrea. *Budoucnost patří bezhotovostním platbám, shodují se odborníci z expertního týmu* [online]. 2010-04-13 [cit. 2011-05-05]. Budoucnost patří bezhotovostním platbám, shodují se odborníci z expertního týmu. Dostupné z WWW:<http://www.retailinfo.cz/magazin/clanky/budoucnost-patri-bezhotovostnim-platbam-shoduji-se-odbornici-z-expertniho-tymu>.

[42] KUBÍK, Tomáš. *Bezkontaktní mobilní platby v ČR: pilotní projekt odstartuje již v polovině roku* [online]. 2011-03-24 [cit. 2011-05-19]. Bezkontaktní mobilní platby v ČR: pilotní projekt odstartuje již v polovině roku. Dostupné z WWW: <http://bankovnipoplatky.com/bezkontaktni-mobilni-platby-v-cr-pilotni-projekt-odstartuje-jiz-v-polovine-roku-13988.html>.

[43] KRAUS, Vojtěch. *NFC technologie budoucnosti již brzy?* [online]. 2011-01-28 [cit. 2011-04-09]. NFC technologie budoucnosti již brzy?. Dostupné z WWW: <http://jablickar.cz/nfc-technologie-budoucnosti-jiz-brzy/>.

[44] ČTK. *Telefon se stane peněženkou, tvrdí Nokia a mobilní operátoři - iDNES.cz* [online]. 2007-04-28 [cit. 2011-05-03]. Telefon se stane peněženkou, tvrdí nokia a mobilní operátoři. Dostupné z WWW: <http://mobil.idnes.cz/telefon-se-stane-penezenkou-tvrdi-nokia-a-mobilni-operatori-plp-/mob_tech.aspx?c=A070427_003306_mob_tech_ada>.

[45] BENEŠ, R. *Autentizační metody založené na biometrických informacích* [online].Vysokké učení techniké v Brně, 2010-11-18 [cit. 2011-05-08]. Autentizační metody založené na biometrických informacích. Dostupné z WWW: <http://magazin.specialista.info/view.php?cisloclanku=2005100402>.

[46] KRČÁL, Martin. *Citace 2.0 - vše o citování literatury a dokumentů (http://www.citace.com)* [online]. 2009 [cit. 2011-05-21]. Citace.com - generátor citací. Dostupné z WWW: <http://citace.com/index.php>.

Seznam použitých symbolů a zkratek

3D	Plochý obraz jevící se, jako by se jednalo o trojrozměrný předmět.
ABS	Význam třetí zkratky.
ACCESS	Systém kontroly vstupu.
AES	Symetrický blokově orientovaný algoritmus (*Advanced Encryption standard*)
Antipassback	Funkce přístupového systému, neumožnit opakovaný vstup
APDU	Aplikační protokol pro čipové karty (*Applications protocols data units)*
AUX	Vstup externího napájení
CCTV	Uzavřený televizní okruh *(close circuit television)*
CLA	Instrukční třída protokolu APDU
CMOS	Polovodičová součástka *(Complementary Metal-Oxide-Semiconductor)*
CPU	Centrální procesorová jednotka *(Central Processing Unit)*
ČSN	Označení českých technických norem
DNA	Deoxyribonukleová kyselina *(Deoxyribonucleic acid)*
dpi	Počet obrazových bodů na délku 1 palec *(dots per inch)*
EAN	Čárový kód složený z černých a bílých pruhů
EEPROM	Elektronicky přepisovatelná paměť
EMC	Elektromagnetická kompatibilita *(Electromagnetic kompatibility)*
EMV	Standard pro čipové karty *(Europay Mastercard and Visa)*
FIPS	Program pro přenos dat v APDU protokolu *(Fully Interactive Partition Splitter)*

GND	Zemnící kontakt o referenčním napětí 0 V *(ground)*
ha	Jednotka plochy čtverce o straně délky 100 m *(hektar)*
Hz	Jednotka frekvence. Představuje jeden kmit za jednu sekundu
I/O	Vstupní a výstupní rozhraní *(input/output)*
IATA	Mezinárodní asociace leteckých dopravců *(International Air Transportation Association)*
ICC	Integrovaný obvod *(Integrated circuit chip)*
IEC	Mezinárodní elektrotechnická komise (International Electrotechnical Commision)
IPXX	Krytí elektrických přístrojů. Písmeno x reprezentuje číslici značící stupeň krytí.
ISO	International Organization for Standardization
kB	Jednotka datového objemu *(kilobyte)*
LCD	Zobrazovací displej na bázi tekutých krystalů *(Liquid crystal display)*
NFC	Technologie bezdrátového přenosu mobilním telefonem (Near Field Communication)
OSI	Spojení otevřených systémů *(Open Systems Interconnection)*
PIN	Osobní identifikační číslo *(Presonal Identification Number)*
PoE	Napájení po ethernetovém vedení (Power ower Ethernet)
PVC	Druh plastu – polyvinylchlorid *(polyvinyl chloride)*
RFID	Identifikace prostřednictvím radiových vln (Radio
ROM	Pevná paměť *(Read-Only Memory)*
RS485	Sériové komunikační rozhraní přenosu dat
SIM	Účastnický identifikační modul (Subscriber Identitiy Module)
SMS	Krátká textová zpráva (Short message service)

SPA	Prostá výkonová analýza (Simple power analysis)
TZ	Trestní zákon
USB	Univerzální sériové rozhraní
UTP	Nestíněná kroucený dvojlinka *(Unshielded twister pair)*
V	Jednotka elektrického napětí *(volt)*
VCC	Kontakt napájení
VISA	Asociace vydávající platební karty *(Visa International Service Association)*
VPP	Programovatelný vstup

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: SEZNAM POUŽITÝCH POMŮCEK A ZAŘÍZENÍ

1. digitální fotoaparát LUMIX DMC FX-10
2. čtečka RFID karet KIF 1 /INDALA od firmy Duha systém
3. strojní svěrák YORK 80
4. 2 kusy RFID karet Motorola
5. mobilní telefon Sony Ericsson k700i
6. multimetr Metex M-3270
7. osciloskop 3M

PŘÍLOHA P II: DOTAZNÍK VEŘEJNÉHO MÍNĚNÍ

„Dobrý den, mohl(a) byste mi prosím věnovat krátkou chvíli vašeho volného času na pár otázek na téma identifikační karty?“

☐ ano ☐ ne

1) „Vlastníte, nebo používáte nějaké karty, jako například karty do nákupních center, platební karty nebo jiné identifikační doklady? “

   ☐ mám pouze osobní doklady

   ☐ osobní doklady a platební kartu

   ☐ mám více platebních a jiných karet

2) „Víte, že v nedávné budoucnosti bude možné mít jen jednu kartu na vše?“

   ☐ ano ☐ ne

3) „Vyhovovalo by vám, kdyby byla jen jedna karta místo vašich všech ostatních karet, nebo dokladů?“

   ☐ ano ☐ ne

4) „Při sjednocení karet by mohlo dojít k neoprávněnému zneužití citlivých údajů. Myslíte si, že jsou moderní čipové karty bezpečné?

   ☐ ano ☐ ne

5) „Nebojíte se například používat platební karty k placení v obchodech?“

   ☐ myslím si že jsou bezpečné a nebojím se je používat k placení

   ☐ kartu používám pouze k výběru z bankomatu

6) „Víte, že skutečným majitelem vaší platební karty je banka a vy jste pouze držitelem?“

   ☐ ano ☐ ne

7) „Povedlo se vám někdy nějak zničit kartu?“

   ☐ ne, nepodařilo

   ☐ ano, zlomila se

   ☐ ano, došlo k přemazání magnetického pásku

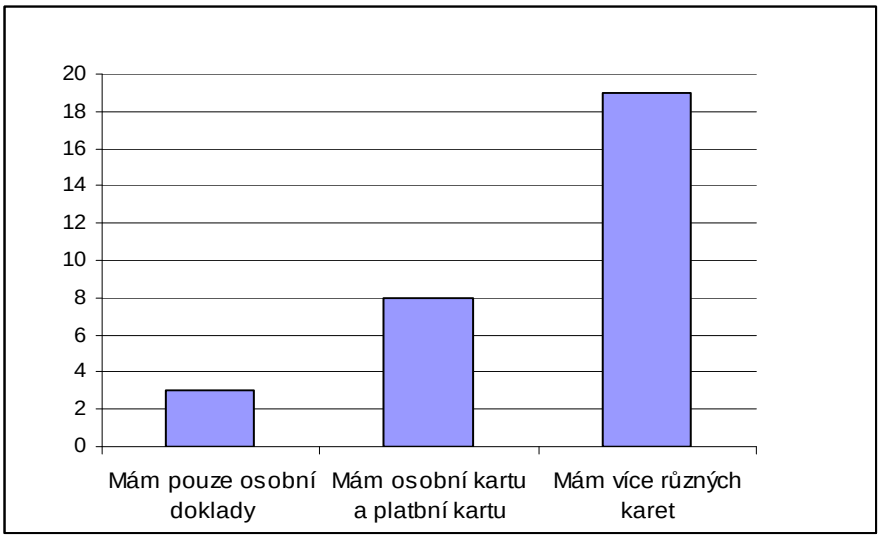
   ☐ ano, zde uvedenou příčinou……
   …… …..

8) „Můžete mi prosím sdělit, zda jste student, důchodce nebo pracující?“

   ☐ důchodce ☐ student ☐ pracující

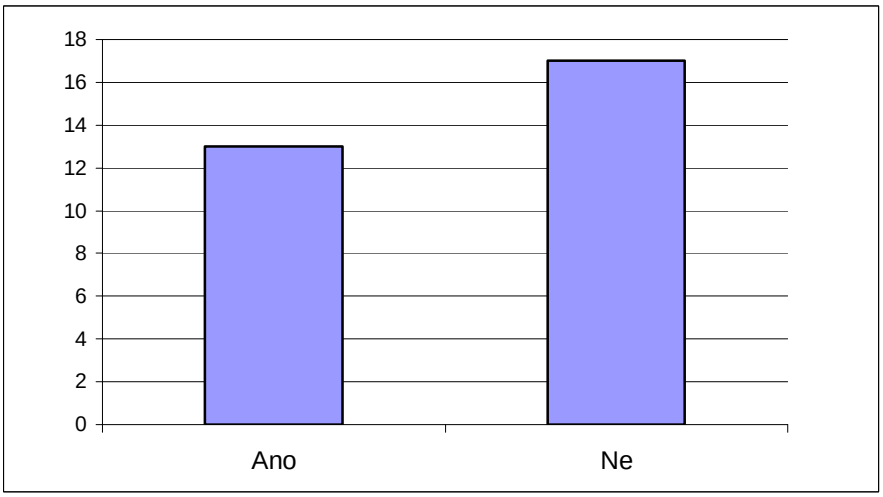
„Děkuji za váš čas, Nashledanou

1) „Vlastníte, nebo používáte nějaké karty, jako například karty do nákupních center, platební karty nebo jiné identifikační doklady? “



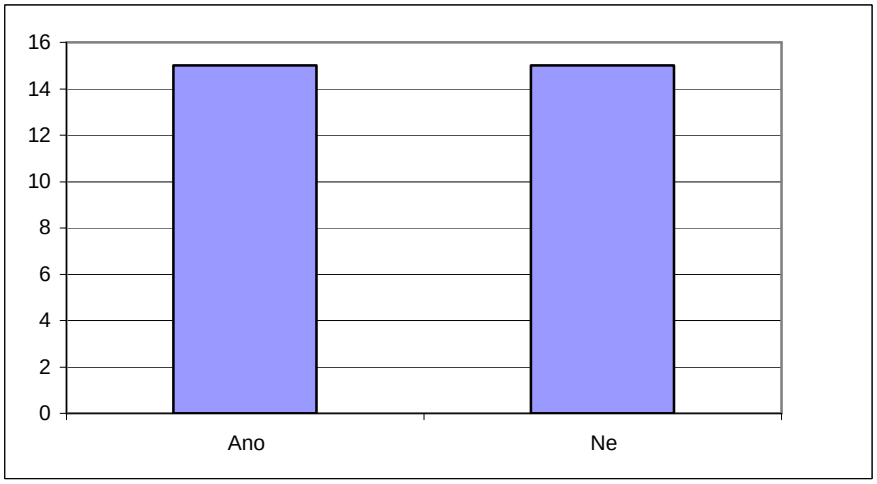
Graf 1 Výsledky odpovědí na 1. otázku

2) „Víte, že v nedávné budoucnosti bude možné mít jen jednu kartu na vše?“



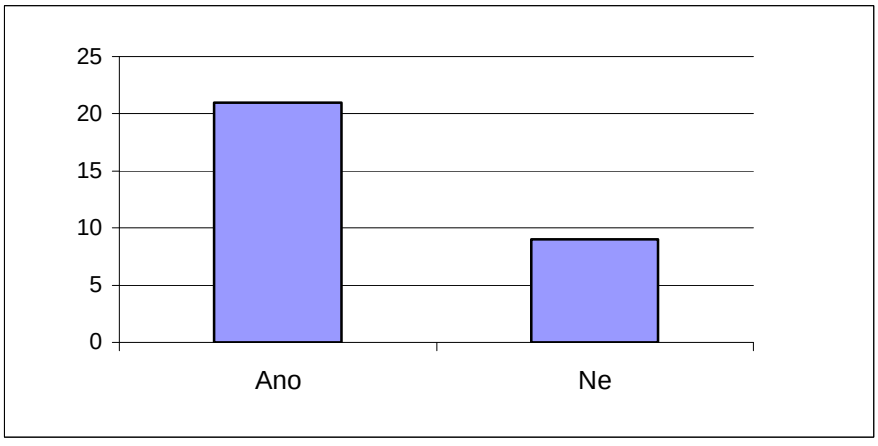
Graf 2 Výsledky odpovědí na 2. otázku

3) „Vyhovovalo by vám, kdyby byla jen jedna karta místo vašich všech ostatních karet, nebo dokladů?“



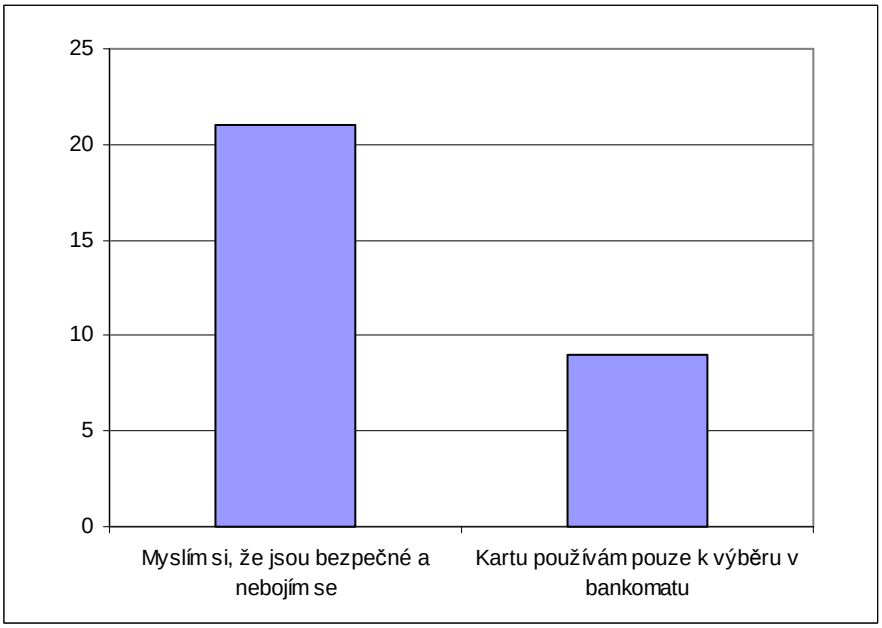
Graf 3 Výsledky odpovědí na 3. otázku

4) „Při sjednocení karet by mohlo dojít k neoprávněnému zneužití citlivých údajů. Myslíte si, že jsou moderní čipové karty bezpečné?



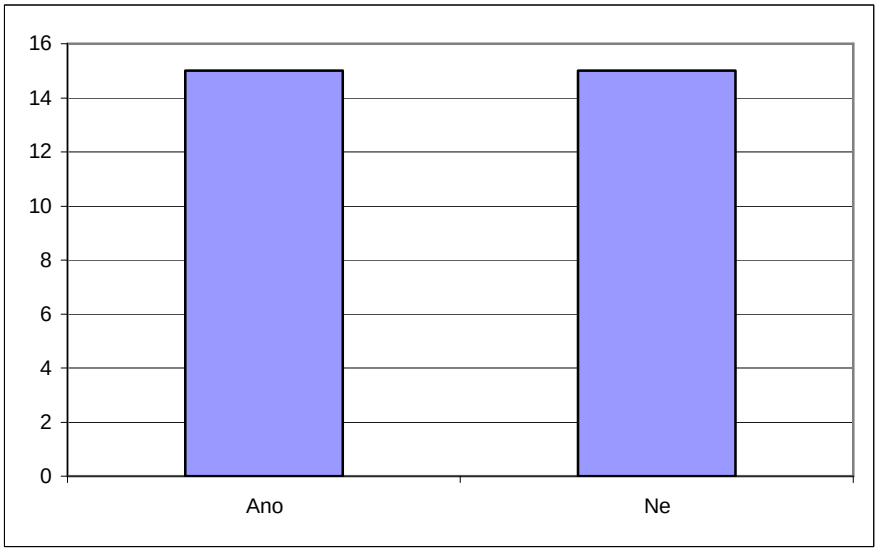
Graf 4 Výsledky odpovědí na 4. otázku

5) „Nebojíte se například používat platební karty k placení v obchodech?“



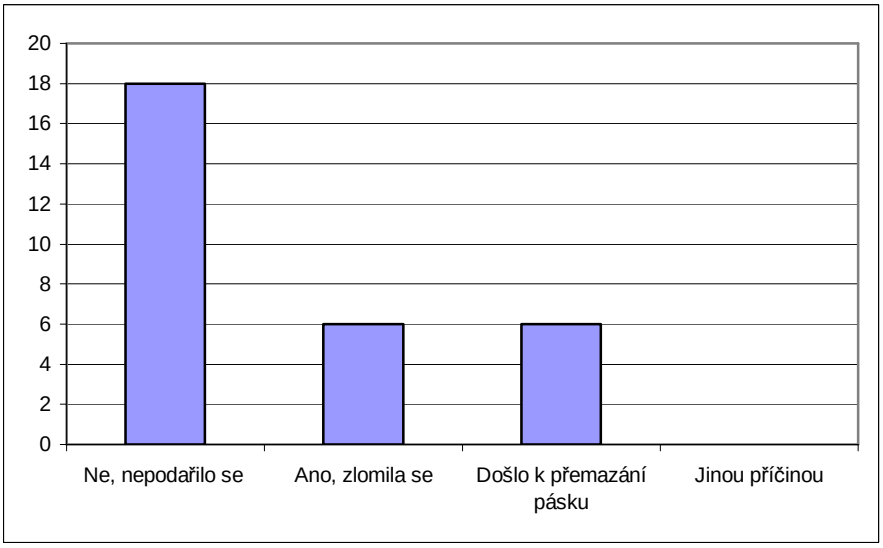
Graf 5 Výsledky odpovědí na 5. otázku

6) „Víte, že skutečným majitelem vaší platební karty je banka a vy jste pouze držitelem?“



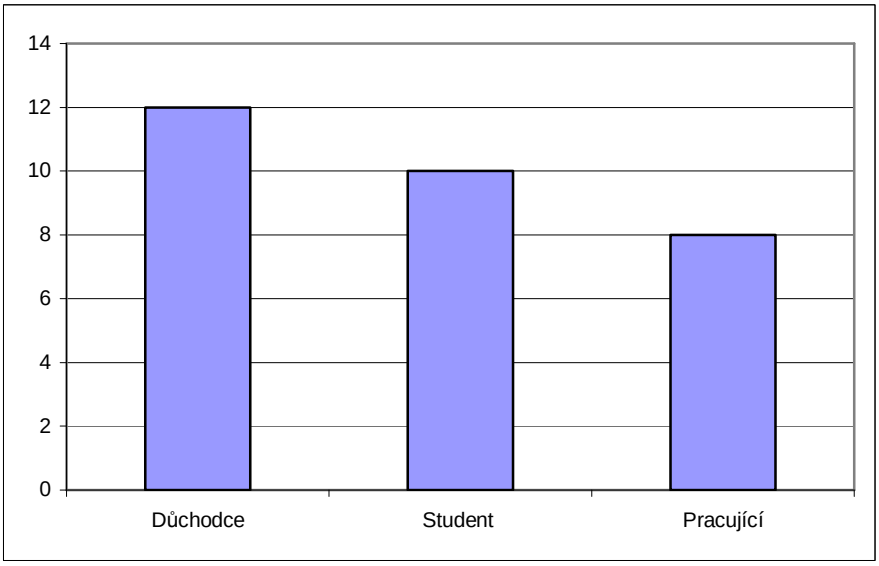
Graf 6 Výsledky odpovědí na 6. otázku

7) „Povedlo se vám někdy nějak zničit kartu?“



Graf 7 Výsledky odpovědí na 7. otázku

8) „Můžete mi prosím sdělit, zda jste student, důchodce nebo pracující?“



Graf 8 Výsledky odpovědí na 8. otázku