UNIVERZITA PARDUBICE
DOPRAVNÍ FAKULTA JANA PERNERA

Diplomová práce

2007

Bc. Lukáš Zeman

UNIVERZITA PARDUBICE

DOPRAVNÍ FAKULTA JANA PERNERA

KATEDRA INFORMATIKY V DOPRAVĚ

TECHNOLOGIE A IMPLEMENTACE PARDUBICKÉ ČIPOVÉ KARTY A NÁVRH MOŽNOSTÍ VYUŽITÍ V INFORMAČNÍM PROSTŘEDÍ UNIVERZITY

DIPLOMOVÁ PRÁCE

AUTOR PRÁCE: Bc. Lukáš Zeman
VEDOUCÍ PRÁCE: Ing. Jana Holá, PhD.

2007

UNIVERSITY OF PARDUBICE

JAN PERNER TRANSPORT FACULTY

DEPARTMENT OF INFORMATICS IN TRANSPORT

TECHNOLOGY AND IMPLEMENTATION OF THE PARDUBICE CITYCARD AND THE PROPOSAL OF THE APPLICATION IN INFORMATIONAL ENVIRONMENT OF THE UNIVERSITY

THESIS

AUTHOR: Bc. Lukáš Zeman
SUPERVISOR: Ing. Jana Holá, PhD.

2007

Univerzita
Pardubice
Dopravní fakulta
Jana Pernera

Katedra: Katedra informatiky v dopravě

Akademický rok: 2006/2007

ZADÁNÍ DIPLOMOVÉ PRÁCE

Pro: **Bc. Lukáš Zeman**

Studijní program: **N3708 – Dopravní inženýrství a spoje**

Studijní obor: **1802T21 – Aplikovaná informatika v dopravě**

Název tématu: **Technologie a implementace Pardubické čipové karty a návrh možností využití v informačním prostředí univerzity**

Zásady pro zpracování:

1. Úvod (čipové karty, jejich funkčnost a obecné vlastnosti)
2. Přehled typů čipových karet na českém trhu
3. Popis Pardubické karty
4. Základní technologie Pardubické karty
5. Modely a využití karet jiných dopravců v ČR
6. Návrhy využití Pardubické karty v rámci UPa
7. Program pro základní komunikaci s kartou
8. Softwarové testování Pardubické karty

Seznam odborné literatury:

- JUŘÍK, P. Encyklopedie platebních karet. Praha : Grada, 2003. ISBN 80-247-0685-7.
- PŘÁDKA, M., KALA, J. Elektronické bankovnictví. Praha : Computer Press, 2000. ISBN 80-7226-328-5.
- Interní materiály firem EM TEST ČR, s. r. o. Vsetín a Mikroelektronika, s. r. o. Vysoké Mýto.
- Interní materiály Dopravního podniku města Pardubice, a. s. a Magistrátu města Pardubice.

Rozsah: 50 normostran

Vedoucí diplomové práce: **Ing. Jana Holá, Ph.D. (ÚEI UPa)**

Datum zadání práce: 15. 11. 2006

Termín odevzdání práce: 15. 5. 2007

L. S.

prof. Ing. Bohumil Culek, CSc.
děkan

prof. Ing. Karel Šotek, CSc.
vedoucí katedry

Prohlášení

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 20. 05. 2007

Lukáš Zeman

Abstrakt

Práce *Technologie a implementace pardubické čipové karty a návrh možností využití v informačním prostředí univerzity* se soustředí na problematiku využívání čipových karet, popisuje nejen situaci ve využívání karet v rámci integrovaného dopravního systému v Pardubicích, ale i v celé České republice, s ohledem na jednotlivé integrované dopravní systémy, možnosti a trendy. V práci je uveden princip nového odbavovacího systému v MHD, výhody a nevýhody jeho využití a návaznosti na případné využití v prostředí Univerzity Pardubice. Součástí práce je také aplikace, umožňující komunikaci mezi čtecím zařízením a čipovou kartou, která ověřuje možnost jednoduchého nasazení pro využití v univerzitním prostředí.

Cílem práce v teoretické části je podat přehled o dostupných čipových kartách na českém trhu, o novém odbavovacím systému a systému čipových karet pardubické MHD a možnostech dalšího rozvoje. Cílem implementační části práce je zkoumání technických parametrů Pardubické karty, včetně jejího testování z hlediska používaného software.

Nejdůležitějším závěrem celé práce je návrh na využití Pardubické čipové karty v informačním prostředí univerzity. Proto je součástí testování aplikace s názvem Read-Write-SC, sloužící ke komunikaci čipové karty pomocí čtecího zařízení s počítačem. Aplikace se nachází na přiloženém CD.

Abstract

The Thesis "*Technology and implementation of the Pardubice Citycard and the proposal of the application in informational environment of the University*", focuses on the usage of smart cards and describes not only the situation in exploitation of cards within the scope of the integrated traffic system in Pardubice, but also in all of Czech republic, with reference to individual integrated traffic systems, possibilities and trends. The principle of a new check-in system in a public transport as well as benefits and disadvantages of its usage and future possibilities of application in environment of the University of Pardubice are introduced in this thesis. As a part of the work is also an application, allowing communication among smart card reader and smart card that checks the possibility of simple setting for the usage in University environment.

The aim of the work in its theoretical part is to summarize all the available smart cards in Czech Republic, new check-in system and system of smart cards in the urban mass transportation in Pardubice and possibilities of its next expansion. The aim of the implementation part is the investigation of the technical parameters of the Pardubice Citycard, including its testing from the point of view of the used software.

The most important conclusion of the work is the proposal of usage of Pardubice Citycard in informational environment of the University. Therefore, the part of this work is the test application named Read-Write-SC, designed to communicate with smart cards using smart card reader connected to a personal computer. The application is enclosed on the CD.

Poděkování

Rád bych poděkoval především vedoucí práce Ing. Janě Holé, PhD. za všechny rady a připomínky při zpracování diplomové práce, Martinu Hodnému a Ing. Tomáši Pelikánovi z Dopravního podniku města Pardubic za poskytování informací a v neposlední řadě Ing. Olze Klápšťové. Zároveň chci poděkovat rodině, všem přátelům a především Mgr. Lucii Škarydové.

Obsah

Seznam ilustrací

Seznam tabulek

Seznam zkratek a značek

ACOS2	ACS Smart Card Operating Systems Version 2
ACS	Advanced Card Systems Ltd.
APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
ATM	Automated Teller Machine
AVS	Adress Verification Systém
CEPS	Common Electronic Purse Specifications
ČNB	Česká národní banka
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DPmČB	Dopravní podnik města České Budějovice
DPmP a.s.	Dopravní podnik města Pardubic a.s.
ECI	EuroCard International
EEPROM	Electrically Erasable Programmable Read Only Memory
EEPROM	Electrically Erasable PROM
EMV	Europay /MasterCard/VISA
ENIAC	Electronic Numerical Integrator and Computer
IBANCO	International BankAmericard Incorporated
ICA	Interbank Card Association
IDS	Integrovaný dopravní systém
ISIC	International Student Identity Card
JCCC	Joint Credit Card Company
kb	kilobite
kB	kilobyte
LAN	Local Area Network
MAC	Message authentication codes
MANIAC	Mathematical Analyse Numerical Integrator and Computer
Mb	Megabite
MB	MegaByte
MCU	Microcontroller Unit
NFC	Near Field Communications
P2P	Peer-to-peer (person-toperson)
PC	Personal Computer
PC	Personál Computer – osobní počítač
PDF	Portable Document Format. Formát pro popis dokumentů Adobe Acrobat.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMDP	Plzeňské městské dopravní podniky
POI	Point Of Interaction
R/O	Read-only
RAM	Random Access Memory
RF	Radio Frequency
RFID	Radio Frequency Identification
ROM	Read Only Memory
SC	Smart Card
SET	Secure Electronic Transaction
SPOM	Self Programable One-chip Microcomputer
SSL	Secure Sockets Layer
UMTS	Universal Mobile Telephone Standard
WAN	Wide Area Network
WDS	Wireless Distribution System
WSBA	Western States Bankcard Association

1 Úvod

Rozvoj využívání čipových karet jako bezkontaktních odbavovacích systémů a elektronických peněženek přináší nové a rychlejší možnosti nejen v dopravě, ale i ve službách města a regionu. S tímto rozvojem souvisí i integrace jednotlivých možností do uceleného systému služeb, které lze nabízet občanům i návštěvníkům města/regionu jako potenciálním zákazníkům. Jakmile takový systém bude vybudován, je vhodné jej rozšiřovat do nových oblastí. Vzhledem k tomu, že Dopravní podnik města Pardubic zavedl právě takový systém čipových karet a ve spolupráci s městem Pardubice a Pardubickým krajem dojde k jeho výraznému rozšiřování, je vhodné uvažovat o začlenění systému čipových karet Univerzity Pardubice do tohoto většího celku.

Teoretická část práce podává ucelený přehled o problematice využívání čipových karet. Je v ní uvedena historie karet – nejen čipových, ale i obecně platebních, zpracován přehled dostupných čipových karet na českém trhu, popsán právě zavedený odbavovací systém a systém čipových karet v Dopravním podniku města Pardubic a nastíněny možnosti dalšího využití nejen v dopravě.

V implementační části jsou testovány a následně popsány technické parametry Pardubické karty z hlediska používaného software, sepsány modely a využití podobných systémů u jiných dopravců v ČR podle jednotlivých integrovaných dopravních systémů. Dále jsou zpracovány návrhy využití Pardubické karty v univerzitním prostředí včetně dotazníkového průzkumu, provedeného na Univerzitě Pardubice mezi studenty a zaměstnanci. V poslední části je popis vytvořené aplikace s názvem Read-Write-SC pro PC, která umožňuje komunikovat s čipovou kartou přes dané čtecí zařízení. Tato aplikace je vytvořena pro konkrétní typ čtecího zařízení a čipové karty, po jednoduchých úpravách je rozšiřitelná na jakýkoliv typ karet, díky používaným standardům komunikace z normy ISO 7816. Aplikace je k vyzkoušení na přiloženém CD, kde jsou k dispozici i zdrojové kódy aplikace.

Práce vychází ze současného stavu poznatků, shrnuje možnosti dalšího rozšiřování čipových karet a bezkontaktních technologií obecně.

Význam práce tkví v ověření potenciální možnosti začlenění osobních čipových karet používaných studenty a zaměstnanci Univerzity Pardubice do širšího integrovaného systému služeb města Pardubic.

Poznámka

V celé práci jsou veškeré jednotky (Byty, bity apod.) psány ve formě zkratek, tedy *B* je Byte a *b* je *bite*. Kurzívou jsou psány pojmy, týkající se technické stránky čipových karet a proměnné používané ve vytvořené aplikaci. Části zdrojového kódu jsou psány stylem písma `Courier`.

2 Historie platebních karet

2.1 Předchůdci platebních karet – Amerika

Historie čipových karet sahá do poloviny dvacátého století, kdy byl vynalezen paměťový čip. Pokud není uvedeno jinak, je v této kapitole čerpáno z [1] a doplněno o vlastní poznatky. Samotná historie karet (myšleno platebních) ale sahá až do poloviny 19. století, kdy začíná v Americe docházet k masivnímu rozvoji obchodu a cestování. V té době pochopitelně ještě neexistovaly platební karty v dnešní podobě, využívány byly hlavně cestovní šeky a poštovní poukázky. Skutečnými předchůdci karet lze nazývat až kovové úvěrové známky z roku 1870 znázorněné na obrázku 1 vlevo, které byly dávány občanům, kteří v podstatě kupovali zboží „na dluh" a při placení pouze ukázali tuto známku. Ke skutečné platbě došlo například až na začátku nového měsíce za předchozí období. Tento způsob vytrval v různě pozměněných podobách až do druhé světové války.

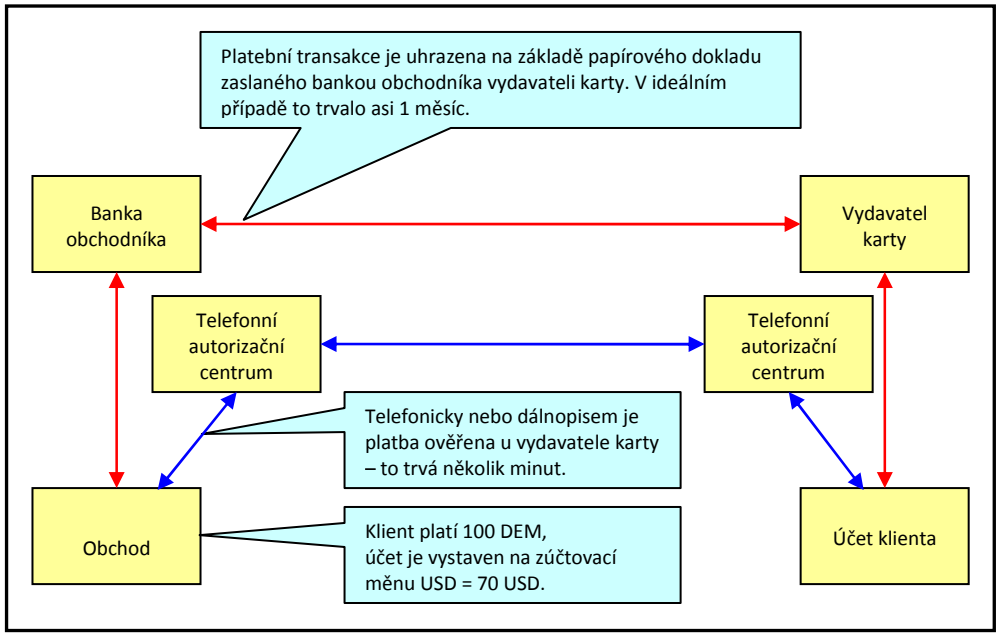
První platební kartu, která byla dostupná širší veřejnosti, vydala americká společnost Western Union Telegraph Company v roce 1914. Z počátku byly vydávány vybraným zákazníkům v době rostoucí konkurence a měly je přimět k častějšímu využívání služeb společnosti. Proto se tyto karty někdy nazývají věrnostní platební karty. Tento model v zápětí následovalo nespočet dalších společností. Logickým vyústěním byla dohoda mezi společnostmi o uznávání těchto karet mezi sebou. Okolo roku 1936 měla síť Retail Service Bureau asi 1000 obchodů. Nadějný rozvoj platebních karet přerušila 2. světová válka. Po jejím skončení se největšího rozšíření dostává úvěrové kartě leteckých společností, vystupující pod názvem Air Travel Card, která se 1. října 1948 stala první mezinárodně platnou kartou na světě. Další úspěšnou společností, vydávající předchůdce platebních karet, se stala společnost Diners Club, která začala v roce 1950 nejprve s restauracemi a později přidala i obchody. První platební kartu, podobající se těm dnešním, vydala v roce 1951 Franklin National Bank pod názvem Franklin Charge Plan. Mezi nejúspěšnější karty patří i karta Marine Midland Bank z Bufala, která se v roce 1962 stala nejúspěšnější Charge Card. Banka Marine Midland se později stala zakládajícím členem asociace MasterCard.

Do roku 1959 byly předchůdci platebních karet vždy jen z papíru. Právě v roce 1959 přišla společnost American Express s první plastovou kartou, která je zobrazena na obrázku 1 vpravo, kterou bylo těžší padělat, a zároveň díky imprinterům zrychlily placení.

Obr. 1: Vlevo – Charge Metal Coins – předchůdci karet; vpravo – první plastová karta – American Express [1]

Dokud byly karty papírové, musely se veškeré údaje přepisovat na účtenky ručně. To způsobovalo chyby při následném zaúčtování nákupů a zdržovalo to i při placení v obchodech. S příchodem plastových karet se mohl plně rozšířit systém tzv. imprinterů, který ve 40. letech vyvinulo několik amerických firem. Jednalo se o mechanické snímače, které přes kopírovací papír přetiskly na účtenku údaje vyražené na platebních kartách. Z počátku se tento systém využíval pro potisk obálek (první vyrobený přístroj je na obrázku 3 vlevo), vojenské štítky, poznávací značky a později právě i pro platební karty. Na účtenku se také otiskly údaje o obchodu, obchodník pak dopsal částku, datum a dal doklad podepsat klientovi. Jeho podpis musel být shodný s podpisovým vzorem na kartě.

Pokud placená částka překročila nastavený limit (obvykle 50–100 dolarů), musel obchodník požádat telefonicky o povolení transakce (autorizaci). To probíhalo telefonem či dálnopisem a úředníci vydavatele karty pak museli najít aktuální zůstatek klienta a rozhodnout, zda je možné nákup kartou povolit. To vše tedy trvalo minimálně několik minut. Pokud bylo vše v pořádku, předal obchodník jednu kopii účtenky klientovi, jednu si ponechal a originál zaslal bance. Ta pak jednou týdně či měsíčně uhradila obchodníkovi obdržené transakce, od nichž odečetla provizi. Potom odeslala účtenky a požadavek na úhradu transakcí vydavateli karet, který pak zaslal všechny účtenky doručené do konce měsíce spolu s jejich soupisem klientovi. Schéma autorizace a zúčtování je na následujícím obrázku 2.

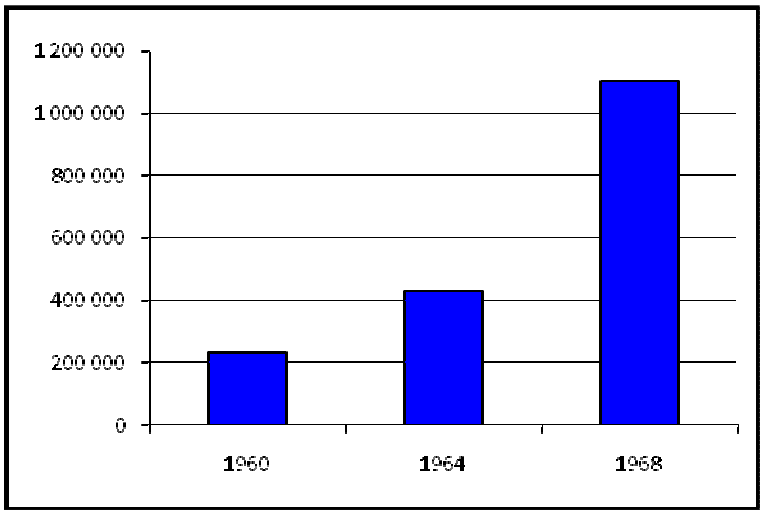


Obr. 2: Schéma autorizace a zúčtování v 60. a 70. letech [1]

V 50. letech se postupně začínají kreditní karty zavádět i různé banky. Jelikož každá banka chtěla mít svojí vlastní kartu a zároveň nechtěla spolupracovat s jinými bankami, končila většina těchto projektů ztrátově. „Pomáhal“ tomu i McFaddenův zákon z roku 1927, který zakazoval působit bankám v jiném městě (unijním státě), než ve kterém měly své sídlo. Tento zákon s různými úpravami platil až do 29. září 1995. První bankou, která přišla v roce 1958 s nabídkou kreditních karet, byla Bank of America a svůj produkt nazvala BankAmericard – obrázek 3 vpravo.

Obr. 3: Vlevo – přístroj Adressograph pro otisk údajů z karty; vpravo – BankAmericard – první bankovní karta [1]

Následující graf na obrázku 4 znázorňuje růst počtu aktivních karet BankAmericard.

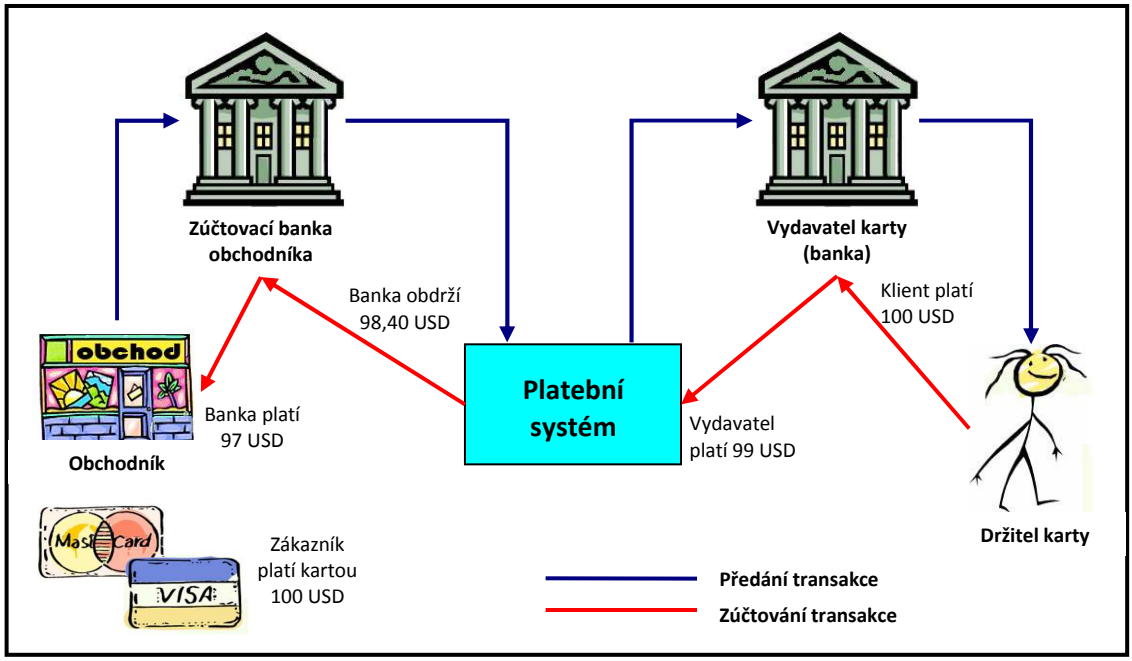


Obr. 4: Růst počtu aktivních karet BankAmericard [1]

2.2 Interchange Fee

Jedná se o systém poplatků, které jsou hrazeny zúčtovací bankou vydavateli karty na úhradu jeho nákladů a rizik souvisejících. Zaveden byl v 70. letech a stanovil určité procento z částky transakce – např. BankAmericard stanovila jeho výši v roce 1971 na 1,95 %.

Banka A byla povinna zajistit, aby jí nasmlouvaný obchodník přijal kartu vydanou bankou B, a banka A následně musela provést všechny potřebné operace k tomu, aby obchodník dostal zaplaceno a banka B jí zaplatila klientův nákup. Banka B (vydavatel karty) tedy původně obdržela od obchodníka celou dohodnutou provizi skrze banku A (zúčtovací banka), které nezůstalo nic. Proto byla dohodnuta Interchange Fee, která zajišťovala, že bance obchodníka (banka A) zůstala část provize. Obě banky tak získaly prostředky na pokrytí provozních nákladů a zisk. Vydavatel karty (banka B) měl navíc příjem z poplatků za vydání karty a případně z úroků. Celý systém znázorňuje obrázek 5.



Obr. 5: Schéma platby kartou (Interchange Fee) [1]

2.3 Začátky v Evropě

Pravděpodobně první kreditní kartu v Evropě vydala v roce 1951 ve Velké Británii společnost Finders Service, když se její majitel vrátil z Ameriky, kde ho inspirovaly příklady karet Diners Club a další. O jedenáct let později vytvořila první evropskou pobočku Diners Club. V roce 1965 se tato karta dostala do ČSSR a jednalo se o první zemi v sovětském bloku. V témže roce se v Evropě poprvé objevila plastová platební karta, kterou vydala britská National Provincial Bank a zároveň Westminster Bank vydala první mezinárodní platební kartu. O rok později, 29. června 1966 koupila Barclays Bank licenci BankAmericard, nasmlouvala 30 000 obchodníků a do konce roku vydala 1 milion karet nazvaných Barclaycard. Roku 1967 zavedla první bankomaty na světě „Cash Point". Do roku 1972 působila BankAmericard v 71 zemích a měla spojení s 15 000 bankami. Další přední britské banky nezůstaly pozadu a roku 1972 založily konkurenční kartu k BankAmericard – Access Card, provozovanou společným podnikem Joint Credit Card Company (JCCC). Během několika měsíců tuto kartu přijímalo přes 70 000 obchodníků a vydáno bylo 3 milióny karet.

Úspěch kreditních karet ve Spojených státech a jejich expanze do Evropy (hlavně Velké Británie) inspirovala evropské bankéře a hoteliéry. Spojením dvou evropských konkurenčních karet vznikla v roce 1965 karta EuroCard International (ECI). Tato karta měla silné zázemí ve švédské bankovní skupině Wallenberg s úzkými vazbami na královskou rodinu. V roce 1969 uzavřel ECI strategické partnerství s americkou asociací Interbank (Master Charge). V roce 1974 začíná ECI akceptovat britské karty Access Card (do té doby platily jen ve Velké Británii a Irské Republice). Jelikož EuroCard měla smluvní vztahy s Master Charge, došlo po roce k začlenění Access Card i do této, v té době již celosvětové, sítě. V roce 1988 koupil Master Charge (v té době již jako MasterCard) 12,25 % akcií EuroCard, čímž upevnil partnerské vztahy. Od té doby se v evropských obchodech objevuje dvojité logo MasterCard/EuroCard. K velkému rozšíření karet Access a díky integraci později i karet MasterCard přispěl velmi dobrý marketing, založený na přátelské reklamě. Z poslední doby jsou známé televizní spoty nazývané „priceless", tedy k „nezaplacení", kdy každý z těchto spotů končil slovy „Některé věci si za peníze nekoupíte. Na všechno ostatní je tady MasterCard". V minulosti proslavil tyto karty i Rowan Atkinson ve známé scénce Mr. Bean na svačině v parku, kdy po namazání chleba kreditní kartou Access využil slogan „I'am your flexible friend". V jiné scénce Mr. Bean v obchodním domě se zase chlubí zbrusu novou kartou American Express. Původní slogan karet Access a obrázky ze scének Mr. Beana jsou na obrázku 6.

Obr. 6: Slogan karty Access, My flexible friend a karta American Express ve scénkách Mr. Beana

2.4 VISA International

Začátkem 70. let, kdy dochází k rozšíření karty BankAmericard do celého světa, obzvláště do Evropy, začíná některým bankám vadit americký název této karty. Po složitých jednáních dochází v září 1974 v kanadském Vancouveru k založení mezinárodní asociace International BankAmericard Incorporated (IBANCO). Tato asociace začala hledat nový název pro své karty – název měl být krátký, graficky zpracovatelný, snadno zapamatovatelný, vyslovovaný ve všech řečech stejně, bez jakéhokoliv významu v žádném jazyce a registrovatelný jako obchodní značka.

Vymyšleno a testováno bylo několik set různých názvů, dvanácti členný tým nakonec vybral slovo VISA, které bylo v roce 1977 zavedeno jako nový název. Název BankAmericard zůstal jen jako název karet Bank of America. Logo karet VISA zůstalo oproti BankAmericard zatím téměř nezměněné. K výrazné změně došlo až po 28 letech od zavedení této značky – od 1. června 2006 musí mít všechny nově vyráběné karty nové logo a hologram přesunutý na zadní stranu po celé délce magnetického proužku. Vývoj karet VISA je na obrázku 7 vlevo.

2.5 MasterCard

I rozšíření karet Master Charge na všechny kontinenty vedlo vedení asociace k diskuzi o změně názvu i loga, aby lépe odpovídaly potřebám marketingu na světovém trhu. Ke změně došlo v roce 1979, kdy jméno Master Charge nahradilo slovo MasterCard. Úpravy se dotkly i loga, když se zmenšily oba kruhy a přestalo se používat logo „i“ asociace Interbank. Název banky, dosud tištěný typizovaným písmem, nahradilo logo banky. Tím skončilo období jednotného vzhledu karet a banky mohly lépe využívat svůj marketing. K další úpravě loga MasterCard došlo v roce 1990, kdy byly zavedeny jasnější odstíny červené a oranžové barvy a do průniku kotoučů bylo vloženo 22 vodorovných linek. K zatím poslední úpravě došlo v roce 1996, kdy bylo zvětšeno písmo, podloženo stínem a zmenšil se počet vodorovných linek. Pro označení obchodů a bankomatů byl zaveden modrý podklad. Postupný vývoj karet MasterCard ukazuje obrázek 7 vpravo. V roce 1987 vstupuje MasterCard jako první kartový systém do Číny. Vývoj kartových systémů od roku 1986 do roku 2004 je v tabulce v příloze A.

Obr. 7: Vlevo – postupný vývoj karet VISA; vpravo – vývoj karet MasterCard [1]

2.6 Střední a východní Evropa

Pro tuto oblast byl rozhodující rok 1989, kdy došlo k formálnímu pádu železné opony a evropský trh se tak rozšířil o zhruba 330 milionů lidí. V roce 1990 bylo sice v tomto regionu vydáno jen několik tisíc platebních karet, v roce 2005 to již ale bylo okolo 115 milionů, jak je vidět v tabulce 1. Zdejší banky se totiž poučily z chyb svých západních sousedů a přeskočily období šeků a záručních karet a investovaly tak přímo do bankomatů a debetních karet. Místním bankám pří získávání know-how a budování moderní infrastruktury velmi pomohl EuroCard (nyní MasterCard Europe). Na obrázku 8 je první platební karta Živnostenské banky z roku 1987 a první VISA karta z roku 1991, vydané v zemích RVHP.

Tab. 1: Situace ve střední a východní Evropě v roce 2005

Země	Počet obyvatel (mil.)	Počet karet (mil.)	Počet bankomatů	Počet obchodníků
Bělorusko	9,8	0,167	40	1 500
Bosna a Hercegovina	4	0,056	30	600
Bulharsko	7,8	3,4	2 107	9 820
Česká republika	10,5	6,5	2 850	55 000
Estonsko	1,4	1,3	779	11 113
Chorvatsko	4,4	6	1 787	43 000
Litva	2,3	1,7	882	15 503
Lotyšsko	3,5	2,7	1 012	13 556
Maďarsko	10,1	6,6	1 371	21 400
Makedonie	2,06	1,3	131	3 858
Moldávie	4,5	0,235	120	1 400
Polsko	38,4	16,9	8 100	110 000
Rumunsko	21,7	6,2	3 400	20 000
Rusko	144	35	25 000	65 000
Slovensko	5,4	3,4	1 590	14 748
Slovinsko	2	2,5	900	34 770
Srbsko	7,5	2,1	623	4 500
Ukrajina	48	15,6	9 469	82 128
Celkem	**327,36**	**111,658**	**60 191**	**507 896**

[1]

Obr. 8: První platební karta a první VISA karta v zemích RVHP [1]

2.7 Pokrokové technologie

2.7.1 Magnetický proužek

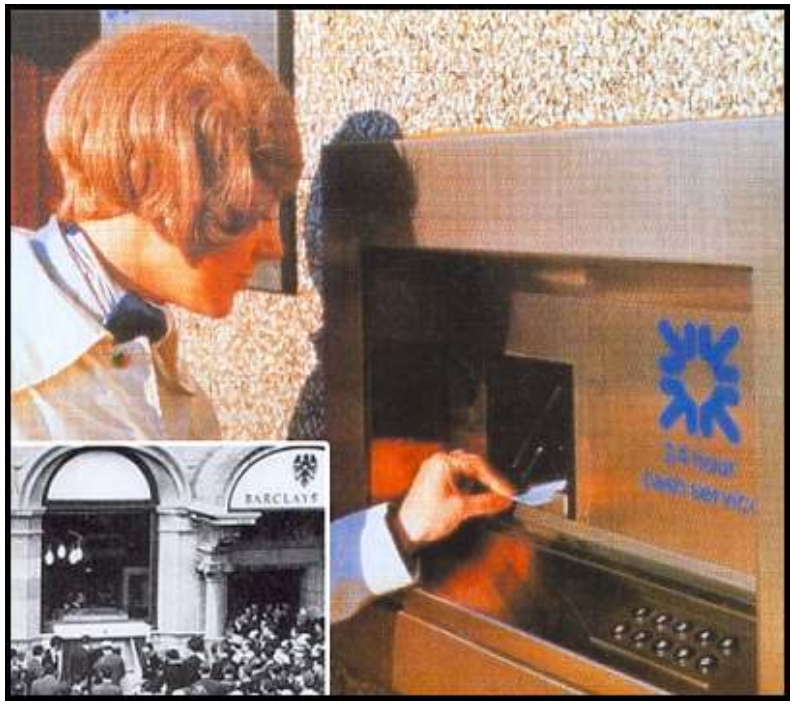
Magnetický záznam byl vynalezen již v roce 1878, o dvacet let později byl vyvinut magnetofonový pásek a v roce 1968 vyvinula společnost IBM technologii záznamu informací na magnetický proužek, který mohl být umístěn na kreditní kartu metodou zvanou Hot Stamping. Požadavek na jeho vývoj dala rada ředitelů bank již v roce 1966. IBM pochopila, že magnetický proužek je jednoduchou metodou pro identifikaci klientů a rozhodla se ji prosadit jako otevřený standard. Podařilo se jí získat spolupráci dalších výrobců a rovněž vyvinout a zavést potřebné normy. Po několika zkušebních projektech se v roce 1969 začal magnetický proužek používat na kartě Air Travel Card. V roce 1972 zavádí magnetické proužky BankAmericard a do dubna 1973 bylo již 85 % všech bankovních karet opatřeno tímto proužkem.

Magnetický proužek je definován normou ISO, ponechává však dostatek prostoru pro to, aby různé systémy využívaly některá definovaná pole podle svých potřeb. Magnetický proužek má tři záznamové stopy se specifickým účelem:

- Stopa 1: má 79 znaků, které obsahují číslo karty (až 18 číslic) a jméno klienta (až 26 alfanumerických znaků).
- Stopa 2: obsahuje 40 numerických znaků včetně čísla karty (až 19 číslic) – v bankovnictví se používá nejvíce.
- Stopa 3: na rozdíl od první a druhé stopy, které jsou určeny pouze pro čtení, může být záznam na této stopě přepisován – k tomu sloužilo až 107 alfanumerických znaků.

2.7.2 První bankomaty

Bankomaty (ATM) byly prvním počítačovým zařízením, které bylo obsluhováno laiky, a to v době, kdy lidé neměli žádné zkušenosti s používáním počítačů. Zároveň byly prvním komerčním zařízením, které využívalo šifrovací systémy. Vedou se spory, kdo je skutečně vynálezcem bankomatu. Britské banky tvrdí, že na myšlenku konstrukce zařízení na výplatu peněz přišel v roce 1965 Skot John Shepherd-Barron, který pracoval jako ředitel společnosti De la Rue Instruments, patřící k tiskárně cenin. S myšlenkou „cash machine“ přišel za ředitelem Barclays Bank, kterého to velmi zaujalo, a hned si jeden bankomat objednal. Vývoj – včetně testování – trval téměř tři roky a tak byl první peněžní automat zprovozněn 27. června 1967 v bance Barclays Bank v londýnské čtvrti Enfield – obrázek 9 (ve výřezu vlevo dole). Další bankomat, tentokrát od firmy Chubb, byl instalován u banky National Westminster Bank o měsíc později. Oba automaty vyplácely bankovky v hodnotě 10 liber po vložení děrného štítku a zadání PIN (Personal Identification Number) – obrázek 9. Pokyny k obsluze zobrazoval otočný válec s texty.



Obr. 9: První bankomat v Barclays Bank (černobílý výřez) a druhý v National Westminster Bank [1]

Američané však tyto výše uvedené zařízení mezi bankomaty nepočítají. Podle nich se bankomaty začala zabývat v roce 1965 firma Diebold, výrobce trezorů a bankovní techniky. Vynález amerického bankomatu je ale přisuzován Donu Wetzelovi z Dallasu, kterého napadlo sestrojit automatického bankovníka při čekání ve frontě před pokladnou v bance. Wetzel byl viceprezidentem pro plánování produktů ve společnosti Docutel, zabývající se vývojem zařízení pro automatické třídění zavazadel na letištích. Patent přihlásil se svými kolegy v roce 1973. Jejich systém již nepoužíval děrné štítky, ale karty s magnetickým proužkem. Zajímavostí může

být fakt, že britská firma de la Rue Instruments v čele s Johnem Shepherd-Barronen svůj patent bankomatu nikdy nepřihlásila a to kvůli nutnosti uveřejnění kódovacích algoritmů a systémů při patentovém řízení. Tento krok podpořil rychlejší rozvoj bankomatů, nicméně umožnil konkurentům vyvíjet podobná zařízení.

Britské i americké první bankomaty byly drahé, pomalé a hlučné, byl však zázrak je vůbec vyrobit bez mikroelektroniky. Bankovky byly uloženy v obálkách s určitou sumou a musely se plnit ručně. Obálky s bankovkami se často zasekávaly. V roce 1973 vyvinul Docutel bankomat, který peníze nejen vydával, ale pomocí vhozu pro obálky také přijímal. Nazval ho Total Teller. Americké banky však tento název nepřijaly a začaly používat výraz, který se stal celosvětově známým – Automated Teller Machina (ATM).

2.7.3 Zavedení počítačových center

V roce 1970 uvedl Master Charge do provozu tři počítače IBM 360-40, které zajišťovaly autorizace transakcí. Přehled transakcí byl zasílaný klasickou poštou, což bylo velmi zdlouhavé. Master Charge ke zpracování transakcí zvolil decentralizovaný systém spojující dohromady 13 počítačových center nazvaný OmniSwitch. Tato centra třídila transakce, ale i varovala bezpečnostní pracovníky, pokud byla karta použita podezřelým způsobem. BankAmericard budoval vlastní systém nazvaný BASE I – ten pracoval tak, že když obchodník žádal autorizaci transakce, byl jeho hovor automaticky přepojen systémem na banku klienta. Zůstatek jeho účtu byl zaznamenán v počítači. Během několika sekund obdržel obchodník souhlas nebo nesouhlas s transakcí. Průměrná délka autorizace se tak zkrátila z 5 minut na 56 sekund a během prvního roku došlo k ušetření 30 miliónů dolarů. Ještě téhož roku byl zprovozněn i systém BASE II, který zabezpečoval clearing a zúčtování a po prvním roce provozu banky ušetřily 12 miliónu dolarů na poštovních nákladech.

2.7.4 Platební terminály

Nárůst počtu vydaných karet a provedených prodejních transakcí se projevil vzrůstem počtu papírových dokladů, které museli obchodníci vyplnit a zaslat bance k úhradě. Banky pak musely tyto doklady zpracovat a autorizovat. To vše vedlo k myšlence zkonstruovat platební terminál zjednodušující bezhotovostní placení. První generace terminálů byla založena na principu napsání potřebných informací na klávesnici. Autorizace byla provedena vytočením telefonního čísla příslušného centra platebního systému nebo ověřením proti databázi zablokovaných karet uložených v paměti terminálu. Druhá generace prováděla kontrolu platební transakce prostřednictvím záznamu finančního limitu, druhu použití a časové platnosti na magnetickém proužku a seznamu zakázaných a zablokovaných karet uloženém v platebním terminálu (on-line). Minimálně jednou denně se pak prováděl přenos dat o provedených transakcích do banky. Nejprve pomocí disket později přes telefonní a datové linky. Obrázek 10 ukazuje první funkční platební terminál z roku 1984, vyrobený společností Verifone.

Obr. 10: Verifone ZON Jr, první platební terminál z roku 1984 [1]

2.7.5 PIN a DES

Již první bankomatové karty, jež měly podobu plastových děrných štítků, používaly k ověření totožnosti klienta osobní identifikační kód PIN. Bezpečnost těchto karet byla však velmi primitivní – PIN byl zakódován v děrném štítku nebo magnetickém proužku karty. Jednoduché algoritmy výpočty PIN z čísla karty byly začátkem 70. let pro podvodníky jen krátkodobou překážkou. Proto již v roce 1965 vydal americký úřad pro normy podmínky pro vývoj šifry pro bezpečné používání osobních počítačů v úřadech federální vlády. V roce 1972 byly stanoveny podmínky pro přesnější šifrovací algoritmus, jež měl být:

- velmi bezpečný,
- dostupný všem uživatelům,
- přizpůsobitelný potřebám různých sektorů,
- levný,
- snadno ověřitelný.

Do vývoje se zapojili specialisté z FBI i britské MI5. Byla vyvinuta řada technologií, které však nebyly vhodné pro mezinárodní používání. Dne 27. 8. 1974 předložila nejvhodnější řešení společnost IBM. Její metoda měla název Lucifer a používala stejný klíč pro šifrování i dešifrování informací. Americký národní bezpečnostní úřad vyhodnotil jeho bezpečnost a navrhl zkrátit délku šifrovacího klíče ze 128 na 56 b (kvůli použití pro komerční účely). V lednu 1978 byl algoritmus zveřejněn a současně byl změněn jeho název na Data Encryption Standard – DES. Jak postupně rostl výkon počítačů, byla prodlužována délka šifrovacího klíče DES, aby se udržela vysoká bezpečnost této metody. V současné době se používá Triple DES (3DES) s délkou klíče 56 znaků, což poskytuje okolo 70 000 triliónů možných kombinací.

3 Čipové karty

3.1 Chytré karty

I tato kapitola čerpá převážně z [1], opět doplněno o vlastní poznatky. Nový typ karet by nemohl vzniknout bez rychlého rozvoje počítačů, které se začaly ve větší míře rozvíjet během druhé světové války. Ve 40. letech 20. století přišel Američan John von Neumann s tzv. Neumannovým schématem, které rozdělovalo počítač na několik částí se specifickou úlohou. Společně s ním se začala prosazovat binární (dvojková) soustava. V roce 1943 byl v USA za pomoci firmy IBM sestrojen první reléový počítač Mark I. O rok později sestrojili experti z University of Pennsylvania první plně elektronický číslicový počítač ENIAC – Electronic Numerical Integrator and Computer, vážící přes 30 tun. V roce 1945 sestrojil John von Neumann počítač MANIAC – Mathematical Analyse Numerical Integrator and Computer, který byl mimo jiné použit při vývoji vodíkové bomby. V padesátých létech vznikl počítač UNIVAC (obrázek 11 vlevo), který se stal až do 70. let standardem pro nevojenské aplikace. V druhé polovině 50. let byl zaveden systém programovací architektury – jazyky Fortran (1975), Cobol (1960) a Basic (1964). Převratnou novinkou byl vynález tranzistoru v roce 1948, který přinesl jeho autorům Nobelovu cenu. Díky němu pak začala éra miniaturizace a zlevňování.

3.1.1 Mikročip a vznik čipové karty

První mikročip byl komerčně nabídnut společností Intel 15. listopadu 1971 pod názvem Intel 4004. Obsahoval 2250 tranzistorů, měl takt 108 kHz a zpracoval 600 000 instrukcí za sekundu – obrázek 11 vpravo.

Obr. 11: Vlevo – Počítač UNIVAC z roku 1952; vpravo – Intel 4004 – první mikročip [1]

Myšlenka chytrých karet vznikla již koncem 60. let 20. století. Zabývalo se jí několik vynálezců z různých konců světa – například Jürgen Dethloff a Helmut Grottrupp z Německa si patentovali identifikační systém již v roce 1968. O dva roky později si v Japonsku patentoval čipové karty Kunitaka Arimura a v témže roce v USA J. K. Ellingboe z IBM patentoval elektronickou kreditní kartu pod názvem „Active Electric Card“. Obecně je ale za vynálezce čipových karet považován Francouz Roland Moreno, který tuto myšlenku dokázal prosadit do života. Ten nejprve přišel s myšlenkou prstenu, ve kterém byl implantován mikročip, pomocí kterého by se dalo platit v obchodech se speciálním snímačem. Tuto myšlenku dokonce zrealizoval a předvedl v září 1974 bankám. Bankéři však nebyli tímto typem nadšeni, kromě ředitele technického vývoje v bance Crédit Industrie et Commercial, který Morenovi poradil, aby pro tuto platební metodu použil spíše formát kreditní karty. Moreno se proto obrátil na společnost CII-Honywell Bull a společně s vedoucím vývojového centra této firmy, Michelem Ugonem, vyrobili prvním několik karet s mikročipem. V roce 1978 patentoval Michel Ugon první jednočipový mikroprocesor, označovaný jako SPOM – Self Programable One-chip Microcomputer. V témže roce rozhodla francouzská vláda, že čipová karta je francouzský vynález hodný zvláštní pozornosti a během 5 let investovala do jejich vývoje více než 85 milionů franků. V roce 1979 pak vyhlásili banky výběrové řízení na zkušební provoz těchto

karet a v roce 1981 spustily první projekty Caen, Lyonu a Blois, kde se zkoušely tři rozdílné technologie čipových karet navržené firmami Philips, Schlumberger a Bull CP8. V roce 1984 bylo oznámeno, že vítězem se stává technologie Bull CP8 s čipy od firem Motorola a Eurotechnique (Thomson). Současně s tím vydaly banky specifikace a standardy čipových karet francouzských bank.

3.1.2 MasterCard a VISA

EuroCard, Mastercard i VISA pozorně sledovaly vývoj a testování čipových karet. V roce 1985 uzavřel MasterCard se společností Bull CP8 smlouvu o testování v USA. VISA International provedla se stejnou společností studii o možnosti využití karet s mikroprocesorem, která ukázala, že čipové karty mohou zvýšit ochranu proti zneužití a snížit náklady.

3.1.3 Mondex a JavaCard

Karty Mondex, které vznikly ve Velké Británii v roce 1990, pracují s nejsilnější, flexibilní a bezpečnou platformou MULTOS. Jako jediná čipová karta v civilním sektoru dosáhla certifikace bezpečnosti na nejvyšší úrovni ITSEC E6. MULTOS je otevřená platforma, která umožňuje, aby v kartě bylo vedle sebe použito více nezávislých aplikací. Používá při tom bezpečnost založenou na algoritmu RSA, a proto vyžaduje výkonné čipy s koprocesorem, které jsou výrazně dražší než klasické čipové karty. Tyto karty lze ale také použít pro digitální podpis a přenos dat tohoto systému je bezpečný i při přenosu přes telefonní linky či Internet. Velkou výhodou této platformy je i jeho platformová nezávislost. Nové aplikace tak bez problémů fungují na starších čipových kartách a stejně tak starší aplikace na nových kartách. V těchto kartách lze využívat aplikace napsané v jazyce JavaCard, který vzešel z jazyka Java – produktu firmy Sun Microsystems z roku 1990. Jedná se o objektově orientovaný jazyk, jehož velikou předností je přenositelnost, umožňující použití stejné aplikace na různých platformách. Samotný jazyk JavaCard vyvinula společnost VISA International v roce 1996 a o rok později vydala jeho první specifikace. Aplikace psané v tomto jazyce pak mohou být kdykoli přidány do paměti čipové karty, stejně jako přepsány nebo smazány – a to přímo v zařízení, kde se karta právě nachází (např. platební terminál).

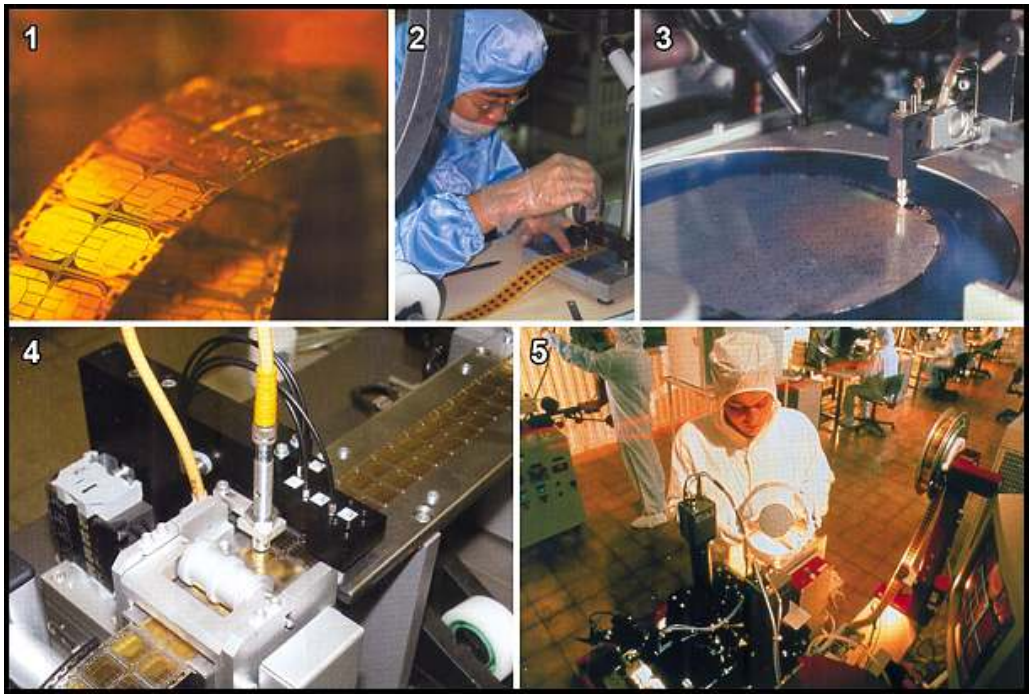
3.2 Realizace čipových karet

První čipovou kartu vyrobenou podle standardu EMV (Europay /MasterCard/VISA) vyvinula v roce 1995 rakouská firma Mikron GmbH (dnes součást koncernu Philips) pod označením Mifare. Tento typ se rychle rozšířil a v říjnu 1997 je jako první zavedly britské banky. Nejprve se mělo jednat o dvouletý zkušební provoz, díky vynikajícím výsledkům se však banky rozhodly do konce roku 2001 nahradit všech 104 miliónů platných platebních karet čipovými kartami. Původně banky nevyužívaly PIN u svých karet, počet zneužitých ztracených či odcizených karet však rostl, proto byl v roce 2002 PIN zaveden. V roce 1998 asociace MasterCard a VISA vydaly časový plán přechodu bank od magnetických na čipové karty. Důležitou součástí tohoto plánu je přesun odpovědnosti za zneužití karet na banky, které od ledna 2005 nepoužívají právě tuto technologii s čipem. V roce 2002 MasterCard představil novou kartu OneSMART MasterCard, do které je možné ukládat různé důvěrné informace – například rodná čísla, čísla účtů, hesla, e-mailové adresy, telefonní čísla apod.

3.3 Výroba

Samotné čipy vyrábí jen několik výrobců – např. Philips, STE, Hitachi. Základním materiálem jsou křemíkové krystaly o téměř 100% čistotě. Válce tohoto křemíku jsou rozřezány na plátky o síle 0,5 mm a průměru asi 18 cm. Technologií fotolitografie je v křemíku vytvořena struktura budoucího čipu. Každý plátek křemíku obsahuje několik tisíc čipů, které jsou diamantovým nožem rozřezány na jednotlivé části, tzv. dye. Po nezbytných testech jsou tyto dye umístěny na tištěný obvod a spojeny tenkými zlatými drátky se 6 nebo 8 kontakty modulu. Potom je čip opatřen ochranným lakem a je do něj nahrán firmware – tím je dokončena výroba mikromodulu. Následně

dochází k umístění mikromodulu do plastové karty a čip je předpersonalisován aplikací pro daný typ karty. V závěru procházejí čipy řadou testování. Během uskladnění v trezorech a jejich dopravy k zákazníkovi jsou čipy uzamčeny tajným transportním klíčem. Kartové centrum banky pak do paměti čipu a na magnetický proužek zaznamená potřebné údaje a na povrch karty jsou vyraženy či vytištěny základní údaje. Nakonec je karta finálně otestována a předána bance či zaslána klientovi. Různé části výroby jsou znázorněné na obrázku 12.



Obr. 12: Fáze výroby karet. 1 – Kontaktní plošky; 2 – Průběžná kontrola; 3 – Křemíková deska před rozřezáním; 4 – Vstupní kontrola čipu; 5 – Výroba čipů [1]

3.4 Elektronické peněženky

Obecně platí, že systém elektronických peněženek se využívá k placení částek do 30 dolarů. Na myšlenku elektronických peněženek přišly francouzské banky koncem 80. let 20. století, když úspěšně zavedly možnost platit ve veřejných telefonních automatech bankovními kartami. Princip elektronické peněženky spočívá v tom, že se do čipu karty zaznamená určitá finanční částka, která se placením snižuje a dobíjením zvyšuje. Zaplacená částka se zaznamená do samoobslužného terminálu a po daném časovém období se souhrn všech transakcí odešle ke zpracování do centrály. Peníze, které si klient do peněženky „nabil“, jsou evidovány v tzv. plovoucím účtu (float account).

Prvním celoplošným projektem elektronické peněženky byl dánský Danmont v roce 1992, následovaný portugalským SIBS (1995), belgickým Protonem (1996) a rakouskou peněženkou Quick (obrázek 13). Z počátku vyvíjely peněženky pouze velké banky a MasterCard i VISA stály stranou. Po krátkém čase bylo v provozu již 23 evropských a 49 mimoevropských systému, které však nebyly vzájemné kompatibilní. Po viditelných úspěších se do tohoto projektu postupně zapojily od roku 1994 i VISA, Europay a MasterCard. Až v roce 1998 se začalo jednat o vzájemné kompatibilitě těchto karet. Problémem bylo zaprvé to, že většina bank vyvíjela své systémy bez vazby na standard čipových karet EMV, který byl specifikován až v roce 1996, a zadruhé bylo potřeba zvýšit počet obchodů a dobíjecích terminálů, které musely být inoperatibilní.

Řešení spočívalo v rozdělení jednotlivých druhů elektronických peněženek podle použité technologie do tří federací: GeldKarte, Proton a Mondex (ten je sám o sobě velmi specifický – viz dále). V jejich rámci mělo být zajištěno vzájemné používání peněženek a v dalším kroku se mělo hledat řešení interoperability mezi federacemi. V březnu 1999 vydaly evropské banky standard

CEPS – Common Electronic Purse Specifications, který byl poprvé implementován v projektu Ducato v listopadu 2001.

Projekt Mondex britské banky National Westminster Bank umožňuje používat až pět měn současně, archivuje posledních 10 transakcí a jeho použití může být vázáno na zadání PIN. Dobíjení těchto karet je možné převodem z účtu, složením hotovosti v bance, telefonem, internetem nebo z jiné Mondex peněženky.

Ekonomika drobných plateb byla z počátku velmi nejistá, protože bylo třeba investovat do vydání čipových karet a vybudování potřebné infrastruktury platebních terminálů v prodejnách tisku, v parkovacích a prodejních automatech atd. Příjem elektronické peněženky přinášejí z poplatků za vydání karty, z transakčních poplatků u obchodníků a z úroků plovoucího účtu, kde jsou peníze evidovány od data nabití do data jejich použití k placení. Kromě toho poskytuje plocha karty značný prostor k pronájmu k reklamním účelům.

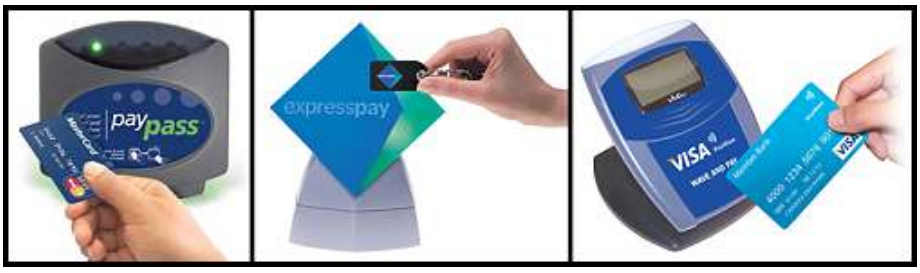
Obr. 13: Elektronické peněženky QUICK (1996) a Komerční Banka (1997) [1]

Specifickou oblastní elektronických peněženek jsou předplatní karty, které se nejčastěji využívají u telefonních automatů. V roce 1993 zavedla VISA bankomatovou kartu VISA Travel Money, kterou si může v bance zakoupit kdokoliv bez vlastnictví běžného účtu, stačí v bance uložit částku, kterou chce čerpat a ihned obdrží kartu a PIN. Na podobném principu fungují i Gift Card – dárkové karty.

3.4.1 Bezkontaktní placení – Proximity Payments

Jedná se o placení pomocí přiblížení bezkontaktní platební nebo předplatní karty či jiného identifikačního zařízení do blízkosti platebního zařízeni POI – Point Of Interaction. Využívá se především u placení v MHD, parkovacích automatech či mýtného pozemních komunikacích. Bezkontaktní karty využívají jako komunikační standard protokol Mifare firmy Philips nebo HID firmy Hughes.

Kromě různých lokálních platebních systémů začal od roku 2002 fungovat i systém MasterCard PayPass, kdy klient přiblíží svou platební kartu k terminálu s bezkontaktním snímačem a mezi ním a duálním čipem karty dojde ve zlomku sekundy k výměně potřebných informací. Toto řešení je vhodné zejména tam, kde je důležitá rychlost placení, protože se doba placení zkrátí až o 65 %. Na sklonku roku 2005 se MasterCard, VISA a American Express dohodly na společném protokolu pro bezkontaktní čipové karty, který je založen na technologii MasterCard PayPass (ISO/IEC 14448). VISA používá pro tuto technologii název Visa Contactless a American Express expresspay. Nejčastěji je tímto způsobem možné platit částky do 25 dolarů. Ukázka tří systémů je na obrázku 14.



Obr. 14: Tři systémy bezkontaktního placení – zleva: MasterCard PayPass, American Express expresspay a VISA Contactless [1]

3.4.2 M-commerce

M-commerce využívá placení pomocí mobilních telefonů, který se plně rozšiřuje až s nástupem sítí GSM třetí generace, nazývané 3G nebo UMTS. Telefony podporující tuto síť v sobě obsahují i funkci NFC – Near Field Communications, pomocí které lze platit bezkontaktně mobilními telefony u speciálních terminálů – stačí přiblížit mobilní telefon k terminálu a dojde k zaplacení potřebné částky – ukázka na obrázku 15 je z městské hromadné dopravy v německém Hanau. Tento způsob funguje na stejném principu jako bezkontaktní placení.

Obr. 15: Placení MHD v Hanau (D) pomocí mobilního telefonu Nokia 3220 [1]

3.5 Bezpečnost čipových karet

Mimo standardních způsobů, používaných nejen u platebních karet, tedy ověřování totožnosti držitele, ochrana osobních údajů, je u karet velké nebezpečí při padělání karty. Prvním ochranným prvkem se stala nutnost zadávat PIN, tedy 4–6 místné číslo. Další způsob ochrany karet je hologram, který zavedl MasterCard v roce 1983 a později ho následovaly všechny další organizace vydávající platební karty. Dalším opatřením proti zneužití, hlavně při platbách přes telefon či Internet, je systém ověření adresy příjemce služby AVS – Adress Verification System.

3.6 Další využití čipových karet (kobrandované a afinitní karty)

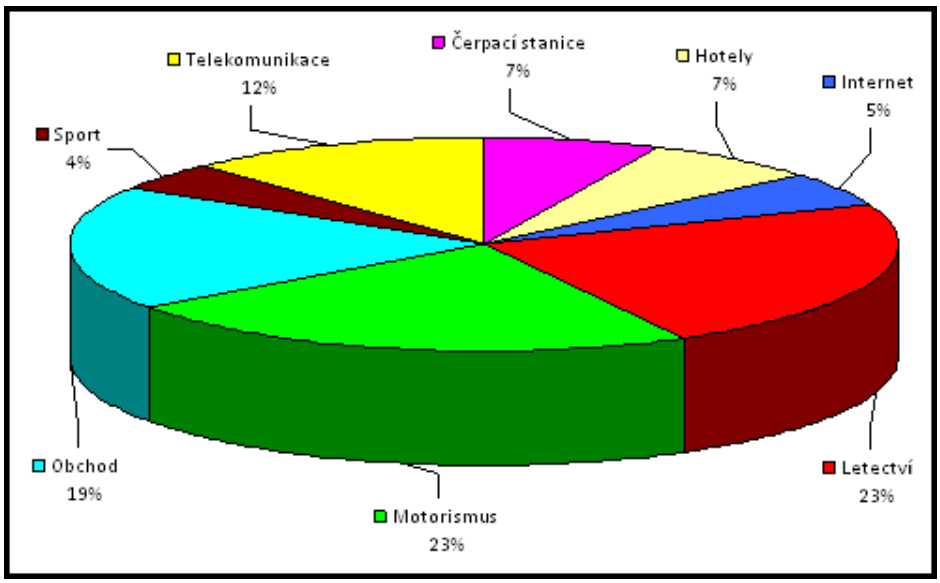
Začátkem 80. let hledaly americké banky na trhu s velkou konkurencí nástroje pro marketing ziskových segmentů. Jedním z nástrojů se staly tzv. Cobranded Cards a Affinity Cards, které jsou určené pro specifické klientské skupiny. První kobrandované karty vydala v roce 1986 americká Marine Midland Bank společně s Continental Airlines a o rok později Eastern Airlines pod značkou karet MasterCard.

Kobrandované a afinitní karty jsou příkladem strategické spolupráce mezi vydavatelem (emitentem) karty a dalšími partnery. Vydavatel karty získává pomocí těchto karet přímý nebo nepřímý přístup k databázi potenciálních klientů a nové distribuční kanály, zatímco partner těží z podpory technického a obchodního zázemí vydavatele (nejčastěji banky). Vydavatel karty

zajišťuje platební funkce a obvykle nabízí i své další (bankovní) služby. Partner poskytuje své služby, výhody nebo jiné speciální podmínky určené pro cílovou skupinu. Graf na obrázku 16 ukazuje nejčastější partnery kobrandovaných karet.

Výhody kobrandovaných karet lze rozdělit do tří skupin podle typu uživatele:

- Výhody pro partnera
  - zvýšení tržeb – preference služeb partnera díky vyšší kvalitě služeb (slevy, výhody,…)
  - zvýšení věhlasu značky – logo na kartě, reklama
  - snížení nákladů – provize od vydavatele za vydané karty, provedený obrat
  - lepšení komunikace – pravidelné výpisy ke kartě nebo účtu
- Výhody pro klienta
  - zvýhodněné podmínky – marketingové programy, slevy, výhody, věrnostní programy
  - příslušnost k firmě, status – propagování příslušnosti při každém použití karty
  - podpora zájmů cílové skupiny – provize pro svou organizaci
- Výhody pro vydavatele
  - nižší akviziční náklady – vyšší míra kladné odezvy mezi členy na nabídku vydavatele (banky), možnost předvýběru klientů
  - zvýšení příjmů – častější používání karty, menší náchylnost ke změnám firmy a vydavatele



Obr. 16: Nejčastější partneři u kobrandovaných karet [1]

Afinitní karty jsou takové karty, které vydávají banky nebo specializované organizace společně s nekomerčními subjekty, jako jsou zájmové či charitativní organizace apod. Jejich cílem je pro platební karty konkrétního vydavatele získat skupinu osob, které spojuje stejné povolání (lékaři, právníci, studenti, učitelé, atd.), společné zájmy (ochrana zvířat, přírody, charita, …) nebo členství v zájmových klubech (golf, tenis, atd.).

Mezi další speciální typy platebních karet lze zahrnout tyto typy:

- Corporate Card – tedy, karty které umožňují středním a velkým firmám řídit a sledovat náklady na dopravu, ubytování a další náklady spojené se služebními výdaji zaměstnanců a stanovit individuální finanční limity, analyzovat očekávané náklady a díky tomu lépe řídit cash-flow společnosti.
- Purchasing Card – karty snižující provozní náklady firmy zjednodušením procedur pro nákupy zboží a služeb v malých až středních kategoriích a snižují také náklady na zpracování faktur (až o 70 %).

- Distribution Card – tyto karty se používají k placení menších dodávek zboží mezi firmami – nahrazuje hotovost a šeky a zjednodušuje tak placení a zvyšuje bezpečnost.
- Procurement Card – cílem této karty je zajistit nákupy zboží a služeb v nižší cenové hladině pouze v určených obchodech nebo obchodních segmentech (letenky, kancelářské služby). Firma může toto omezení nastavit ke každé kartě individuálně.

Následující obrázek 17 představuje některé kobrandované a afinitní karty.

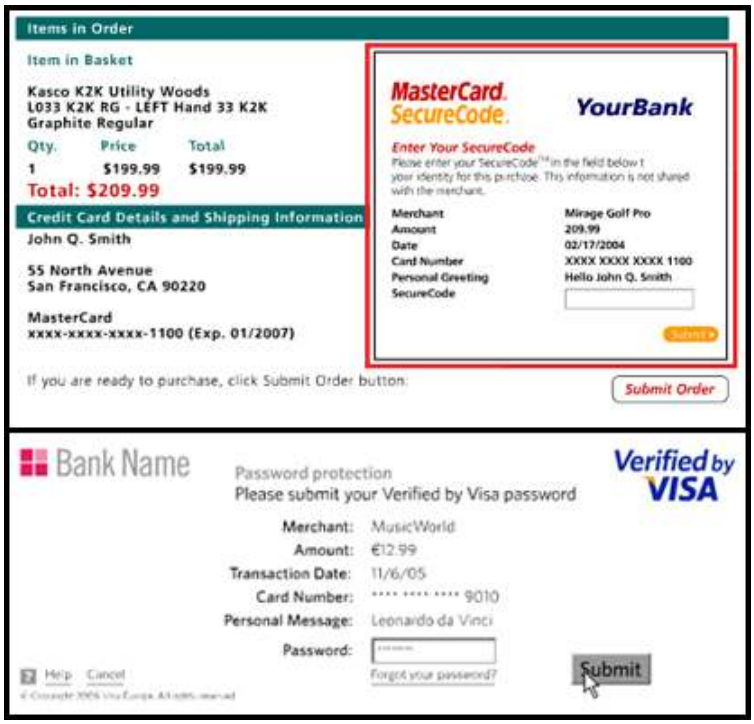
Obr. 17: 1 a 2 – Kobrandované karty; 3 – Afinitní karta; 4 – Corporate Card [1]

3.7 Budoucnost platebních karet

Způsoby prodeje zboží a služeb se neustále rozšiřují a dnes se kromě Internetu, mobilních telefonů a digitální televize rozvíjí také placení pomocí bezkontaktních čipových karet.

3.7.1 Internetové platby

Internet umožňuje největší a nejrychleji rostoucí způsob placení zboží „na dálku“. Pro bezpečné placení na Internetu bylo vyvinuto několik metod. Jako první se začal využívat protokol SSL – Secure Sockets Layer, který byl vyvinutý společností Netscape Communications v 90. letech. SSL sice zajišťuje bezpečné šifrování dat, ale neověřuje identitu zákazníka ani obchodníka, proto tedy existuje riziko, že podvodník použije číslo odcizené karty, nebo že podvodný obchodník zneužije čísla karet, použitých ve svém obchodě. Evropské banky vyvinuly v druhé polovině 90. let bezpečnější protokol SET – Secure Electronic Transaction, který se ale z důvodu velké nákladnosti a složitosti nerozšířil. Proto některé banky zavedly dočasná řešení jako například tzv. pseudočíslo, čili jednorázové či trvalé číslo, použitelné pouze pro placení přes Internet. Druhým způsobem bylo využití virtuální karty, kdy je klientovi přiděleno speciální číslo platební karty pro internetové obchodování. Kvalitní řešení přinesly až organizace VISA a MasterCard se svými metodami „Verified by VISA“ a „MasterCard SecureCode“ (obrázek 18). Oba systémy jsou založeny na tom, že se při placení kartou na Internetu objeví pop-up obrazovka zprostředkovaná zúčtovací bankou. Do ní klient doplní tajné heslo (ne PIN karty), které jde mimo obchodníka, který pouze obdrží od banky informaci o zaplacení.



Obr. 18: Ukázka systémů MasterCard SecureCode a Verified by VISA

3.7.2 P2P – osobní platby

Pojem P2P znamená peer-to-peer, v doslovném překladu tedy „rovný s rovným“. V počítačové terminologii se jedná o označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví klienti (uživatelé). V obchodním sektoru se tento pojem překládá jako person-to-person, čili „od osoby k osobě“. V případě platebních operací se pak jedná o placení za zboží či služby bez prostředníka, tedy přímo mezi dvěma osobami. Dříve se tento způsob využíval jen pro placení mezi lidmi, dnes je možné pomocí těchto systémů platit i obchodníkům či organizacím. Tyto operace lze provádět pomocí běžného účtu u banky, účtu u nebankovní společnosti nebo prostřednictvím platebních karet. Odesílatel může využít P2P služby některého z poskytovatelů (PayPal, CertaPay, FastPay, Western Union atd.) nebo prostřednictvím své banky, pokud tyto služby nabízí. V této době tyto služby začínají zavádět i MasterCard (MasterCard MoneySend) a VISA (VISA Direct) prostřednictvím svých členských bank.

4 Přehled typů čipových karet na českém trhu

4.1 Technické členění čipových karet

Čipové karty lze podle obecně rozdělit do kategorií podle použité paměti a podle nutnosti kontaktu se čtečkou karty, jak se uvádí v [2] a [3]. Z hlediska použité paměti se rozlišují:

- paměťové – RAM, ROM, EEPROM – používají se pro jednoduché aplikace
- paměťové se speciální logikou (ochrana PINem, čítače atd.)
- procesorové (Smart Card) – zvyšují ochranu proti podvodům – jsou založeny na standardu EMV pro vzájemnou kompatibilitu čipů a terminálů – viz kapitola 3.

Podle toho, zda je kartu možné použít přímo zasunutím do čtečky nebo zda stačí přiblížení k čtecímu zařízení na vzdálenost několika centimetrů, se rozlišují tyto karty (obrázek 19):

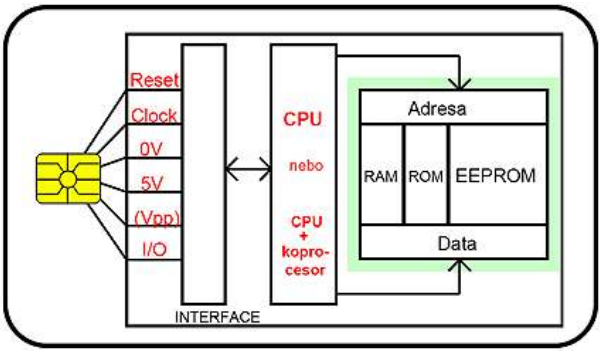
- Kontaktní – u těchto karet je nutný kontakt se čtečkou. Jedná se o ideální technologii pro logický přístup, velkou výhodou je potom velmi nízká cena čtecích zařízení a vysoká míra bezpečnosti. Nevýhodou potom je ale často nižší čtecí rychlosti než u bezkontaktních technologií (standard: 9,6 kb/s, běžné maximum: 115 kb/s, bezkontaktní: až 423 kb/s), proto nedosahuje rychlosti odbavení a dalších výhod bezkontaktních technologií. Typickými představiteli této kategorie jsou procesorové karty s vlastním operačním systémem a případně s možností aplikací umístěných přímo na kartě. Problematická je i standardizace vzhledem k velkému množství technologií a vrstev a k velkému počtu dostupných a navzájem nekompatibilních produktů
- Bezkontaktní – tyto karty nemůžou používat externí zdroj energie. Jedná se o ideální technologii pro fyzický přístup, kde je požadována vysoká rychlost odbavení. Operace s kartou však mohou být prováděny bez vědomí uživatele. Většina produktů má na straně karty velmi omezenou funkcionalitu – většina inteligence je v řídicích systémech, proto u nich převažuje poměrně nízká míra bezpečnosti. Čtecí zařízení těchto karet jsou v porovnání s kontaktní technologií mnohem dražší.
- Hybridní karty kombinují výhody (a nevýhody) bezkontaktních a kontaktních karet. Nelze však sdílet informace mezi kontaktní a bezkontaktní částí. Technologie výroby je ale dlouhodobě ověřená a proto nejsou provozní problémy. Vzhledem k ceně je funkčnost bezkontaktní části omezena na bezvýznamový identifikátor nebo zabezpečené paměťové médium a s tím souvisí nízká bezpečnost funkcionality realizované přes bezkontaktní rozhraní. Cena karty je typicky součtem ceny za kontaktní a bezkontaktní část. Lze kombinovat i více bezkontaktních technologií v jedné kartě, navíc s kontaktní technologií nebo i magnetickým proužkem.
- Duální karty kombinují výhody bezkontaktních a kontaktních karet a při tom eliminují většinu výše uvedených nevýhod. Obsahují výkonný procesor a podporují kryptografické funkce a jednotnou funkcionalitu přes kontaktní a bezkontaktní rozhraní. Nevýhodou je vyšší cena karty (duální čip + vyšší cena za tělo, anténu a zpracování karty)

Obr. 19: 1 – Bezkontaktní karta; 2 – Kontaktní karta; 3 – Hybridní karta; 4 – Duální karta [3]

Jak bylo řečeno, hybridní a duální karty spojují technologii kontaktních a bezkontaktních karet, proto v následujícím přehledu jsou uváděny pouze kontaktní a bezkontaktní technologie.

4.1.1 Kontaktní technologie

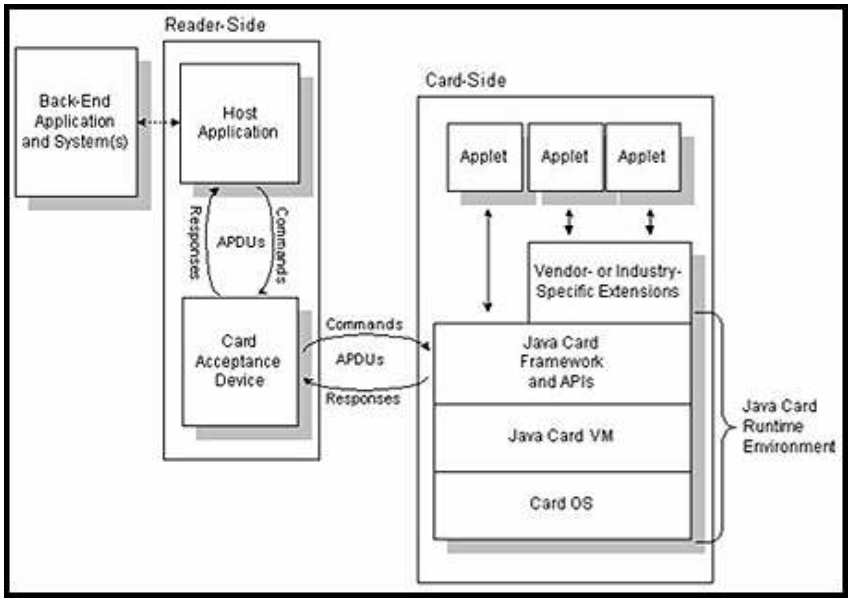
Paměti a nereverzibilní čítače mají různou úroveň bezpečnosti, procesory jsou bez podpory PKI – Public Key Infrastructure. Mají zapisovatelnou paměť o velikosti 4–72 kB, případně i procesory s podporou PKI a zapisovatelnou pamětí o velikosti 8–128 kB. Tento typ technologie může mít odlišné velikosti a technologie pamětí (EEPROM, Flash, ROM). Na obrázku 20 je schematické znázornění kontaktní čipové karty. [3]



Obr. 20: Schéma kontaktní čipové karty [2]

Kontaktní čipové karty lze dále kategorizovat na karty:

- s pevnou funkcionalitou – jsou orientovány na bezpečné uložení dat v systému souborů, mají pevnou množinu operací s daty, případně volitelně včetně podpory PKI. Stejná funkcionalita bývá realizována odlišným způsobem. Jednotlivé systémy mají mezi sebou jen velmi malou slučitelnost.
- programovatelné – k jejich programování se používají jazyky C, MEL nebo Java (dříve i Basic) – nativní kód procesoru nebo interpretace je pomocí virtuálního stroje. Nejdál v podpoře skutečně multiplikační karty s možností instalace aplikací různých vydavatelů a možností řízeně sdílet data přes aplikační firewall jsou JavaCard a MULTOS. JavaCard (schéma na obrázku 21) s rozšířeními GlobalPlatform/OpenPlatform je nejuniverzálnější a nejrychleji rostoucí dostupná technologie, používaná od veřejné správy přes bankovnictví až po aplikace pro velké obchodní společnosti.



Obr. 21: Schéma funkčnosti JavaCard – vlevo čtecí zařízení, vpravo karta s rozhraním JavaCard [2]

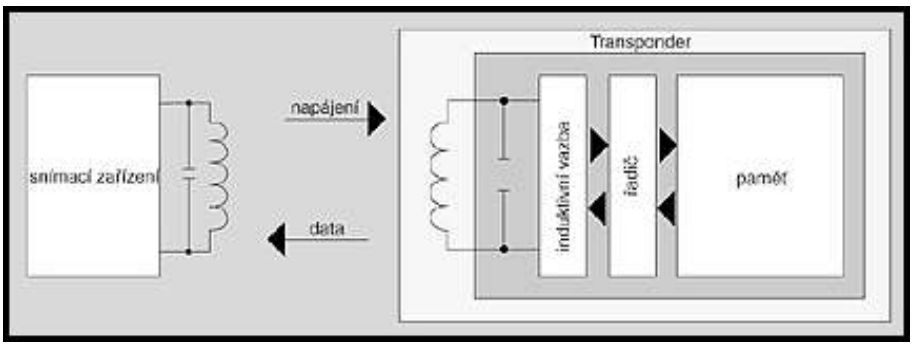
Bezpečnost kontaktních karet je na solidní úrovni, i když produkty jednotlivých výrobců mohou mít odlišnou míru a mechanismy ochrany bezpečnosti a integrity dat v kartě. Dobře řešená je u tohoto typu aktivní obrana proti známým útokům. Aplikační zabezpečení je řešeno přístupovými právy – všechny přístupy do paměti jsou kontrolovány mikroprocesorem, čtení a zápis probíhá pomocí kryptografického klíče a karta se autentizuje PINem držitele karty. PIN se nepřenáší po komunikačních linkách, po několikanásobném nesprávném zadání se karta zablokuje. Z hlediska zabezpečení čipu nelze mazat ani modifikovat ROM. Čip je chráněn proti přímému fyzickému útoku, rentgenování i mazání pomocí UV paprsků, dále nelze čip duplikovat a při útoku sondou dojde k jeho automatickému smazání (tzv. probing). Hlavní výrobci čipů pro kontaktní karty jsou Infineon, Philips (P8WE, SmartMX, SmartXA), STM, Atmel, Renesas, Samsung a Emosyn.

4.1.2 Bezkontaktní technologie

Přenos dat probíhá bez potřeby galvanického propojení kontaktů snímače na vývody karty. Bezkontaktní čipy mohou být hermeticky uzavřeny v plastikovém obalu, jsou necitlivé na oxidaci kontaktů, prach, špínu, vlhkost, rázy, vibrace a mají vysokou životnost. Mohou být používány v těžších a náročnějších podmínkách, než kontaktní karty. Významnou výhodou v porovnání s kontaktními kartami je téměř úplné vyloučení možnosti úmyslného poškození funkce karty vzhledem k tomu, že neexistují žádné vnější vývody. Karty jsou pasivní a nemají tedy vlastní zdroj energie pro zajištění funkcí karty, energii pro svůj provoz získávají přes indukční vazbu s vysílačem snímacího zařízení.

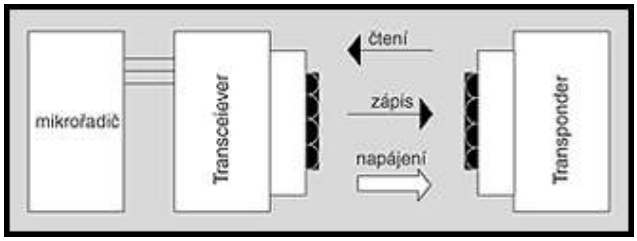
Tuto technologii implementují různí výrobci na různých frekvencích, nejčastěji se však využívá frekvence 125 kHz a/nebo 13,56 MHz. Následující přehled mapuje stav bezkontaktních čipových karet na českém trhu, čerpáno bylo převážně z [2], [3], [4] a [5]:

- UNIQUE H4102 a ZOODIAC H4105 od firmy EM-Microelectronic pracují na frekvenci 125 kHz resp. 134 kHz. Jedná se o R/O čipy (read-only) se 64 (resp. 128) bitovým kódem. Informace je do čipu zapsána laserem při výrobě a výrobce garantuje, že nevyrobí dva čipy se shodným kódem. Přenosová rychlost se pohybuje kolem 50 kBd. Základní princip komunikace je na obrázku 22. Čip bývá nejčastěji umístěn v plastové kartě klasických rozměrů, může však být umístěn v podstatě do čehokoliv. Dosah identifikačního čipu závisí hlavně na konstrukci vysílací antény, jejím tvaru a dále pak na velikosti elektromagnetického pole čtečky a její citlivosti. Tyto identifikátory nacházejí nejčastější využití při kontrole docházky, v přístupových systémech, při automatické identifikaci materiálu nebo zboží na skladu, označování zakázek (čistírny, odvoz odpadu, opravny, oběh vratných obalů), při ochraně zboží proti krádeži v obchodních domech, označování značkového zboží pro odlišení od padělku (parfémy, koňak, oděvy) atd. Čip UNIQUE H4102 využívá v tuto chvíli Univerzita Pardubice – viz dále v kapitole 8.



Obr. 22: Základní princip komunikace čipu UNIQUE [3]

- Čipy Q5 firmy SOKYMAT – umožňuje čtení i zápis (read-write – R/W) a je navržen pro frekvence v rozsahu 100–150 kHz. Z důvodu zachování kompatibility a dodržení standardů RFID se tento čip nejvíce využívá na frekvenci 125 kHz. Čip je vybaven 264 bitovou pamětí EEPROM pro ukládání uživatelských dat. Stejně jako předchozí varianta, i tato se dá umístit do libovolného obalu. S čipem Q5 spolupracují v módu čtení všechny standardizované čtečky na frekvenci 125 kHz. Pro zápis je nutné použít čtečku RFID, která je vybavena funkcí zápisu do identifikátorů na frekvenci 125 kHz. Obrázek 23 ukazuje princip komunikace čipu Q5.



Obr. 23: Základní princip komunikace čipu Q5 [3]

- Hitag 1 a 2 – výrobcem těchto čipů je společnost Philips, jedná se o R/W čip se 2048 (Hitag 1) resp. 265 (Hitag 2) bitovou pamětí pracující na frekvenci 125 kHz. Má antikoliznía kryptovací vlastnosti. Ochranu pro čtení i zápis lze uskutečnit zadáním hesla. Hitag 1 je kódován systémem AC/Manchester, Hitag 2 pomocí Biphase/Manchaster.
- TITAN od firmy EM-Microelectronic je určený pro R/W aplikace. Na čipu je 1 kb paměti EEPROM, která je přepisovatelná uživatelem. Paměť je zabezpečena heslem o délce 32 b pro ochranu zápisu i čtení. Čip pracuje ve frekvenčním rozsahu od 100 kHz do 150 kHz.
- Mifare (Philips) je přepisovatelný čip o různých velikostech, který pracuje na frekvenci 13,56 MHz. Operační dosah má až 10 cm. Obsahuje antikolizní funkce a její bezpečnost je na velmi vysoké úrovni. Norma pro tento čip je ISO 14443 Part 1 až 3 a jsou k dispozici dvě verze modulace – Type A a Type B. Konkrétní typ Mifare čipu je použit v novém odbavovacím systému DPmP a.s. a proto je čip popsán dále.
  - Mifare Ultralight – bezvýznamový identifikátor a 512 b nechráněné paměti.
  - Mifare Standard – bezvýznamový identifikátor, 1 kB nebo 4 kB paměti s ochranou a autentizací, základní funkce pro autonomní platební funkce, fyzická adresace, přenosová rychlost 106 kBd. Mifare Standard je občas nazývána též Mifare Classic.
  - Mifare DESFire – vyšší a standardní bezpečnost (3DES namísto proprietárního Crypt1), 4kB paměť, vyšší přenosové rychlosti (423 kb/s), logická organizace dat v souborovém systému a podpora vícefunkční karty; není kompatibilní s Mifare Standard (ISO 14443 Part 4). Procesor je s pevným jednoduchým OS bez PKI. Technologie DESFire byla americkou vládou a agenturou NASA vybrána pro zabezpečení přístupu do objektů, pro jízdenkový systém byla zvolena v americkém Seattlu a v norském Oslu; jako elektronická vstupenka byla využita na stadionu 1. FC Köln při mistrovství světa v kopané v roce 2006.
  - Mifare ProX – procesor pro čipovou kartu s duálním rozhraním (ISO 14443 Type A Part 1-4) a volitelnou emulací Mifare Standard
  - Mifare SmartMX – výkonnější procesor pro čipovou kartu s trojím rozhraním (kontaktní ISO 7816, USB, bezkontaktní ISO 14443 Type A Part 1-4) a volitelnou emulací Mifare Standard
- I-Code (Philips) – R/W čip se sériovým 64 bitovým číslem a 384 bitovou uživatelskou pamětí, pracovní teplotní rozsah 70°C, krátkodobý teplotní výkyv může být až ke 180°C. Obsahuje antikolizní funkce a stejně jako Mifare má operační dosah kolem 10 cm.
- TEMIC 5554 (5557) – výrobcem je firma Atmel. Jedná se o přepisovatelný čip s pracovní frekvencí 125 kHz. Čtecí vzdálenost je do 10 cm a paměť čipu 264 resp. 330 B.
- iClass jsou bezkontaktní R/W čipy společnosti HID. Na trhu jsou dva typy – 2 kb (256 B) a 16 kb (2 kB). Oba pracují na frekvenci 13,56 MHz. Poskytují vysokorychlostní a spolehlivou komunikaci s velmi dobrou integritou dat. Komunikace mezi kartou a čtečkou je

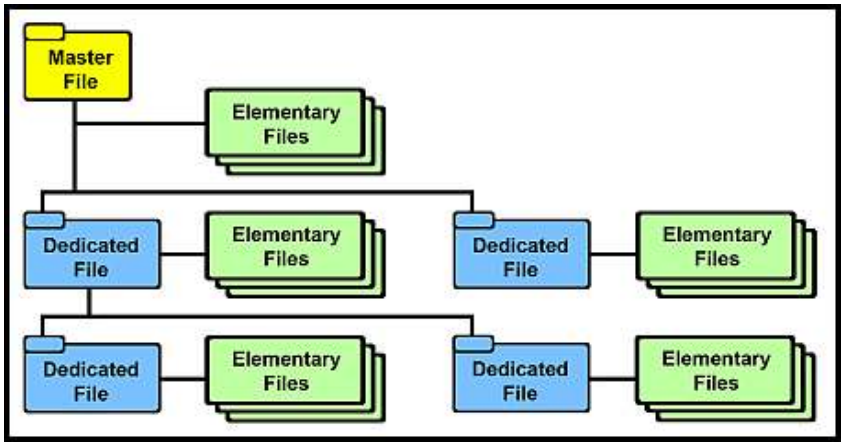
zabezpečena vzájemným ověřováním, šifrovaným přenosem dat a 64 bitovými diverzifikovanými klíči pro čtení a zápis.

- Čipy Cotag společnosti Bewator jsou na trhu buď jako aktivní nebo pasivní. Aktivní znamená, že karty s tímto čipem (označení 928) mají v sobě baterii a tím zvýšený operační dosah až na jeden metr. Problémem je omezená životnost, daná životností baterie. Dokáží spolupracovat s technologiemi Mifare i Hitag. Pasivní varianta neobsahuje baterii, proto je její životnost v podstatě neomezená. Její dosah je klasických 10 cm, v případě použití se speciální čtečkou může být dosah až 30 cm. Jak pasivní tak i aktivní karty pracují na frekvenci 132 kHz.
- Legic MIM256 a MIM1024 – R/W čipy s frekvencí 13,56 Mhz. Komunikace není založena na žádné normě ISO, paměť není segmentována – lze ji rozdělit kódováním. Bezpečnost je na velmi vysoké úrovni díky unikátnímu autorizačnímu konceptu. Čip je chráněn proti měnícím se vlivům různých aplikací. Oba typy mají dosah do 70 cm, MIM256 má celkovou kapacitu 256 B, použitelnou pak 234 B a MIM1024 má z celkové kapacity 1024 B použitelných 1002 B.
- Infineon R/W čipy pracují buď přímo s technologií Mifare nebo ji trochu pozměňují, přičemž specifikace v základech zůstávají stejné – frekvence 13,56 MHz, rychlost 106 kBd, operační vzdálenost 10 cm (u některých typů až 1,5 m), velikosti podle typu karty (řádově B až kB).
- Indala (dříve Motorola, dnes HID) jsou čipy pracující s frekvencí 125 kHz (R/O technologie) nebo 13,56 MHz – read-write. Oba typy mají neomezenou životnost a s tím spojenou doživotní záruku proti poškození.
- TIRIS jsou čipy od Texas Instruments a existují v několika verzích – buď jen R/O nebo R/W. Jedna z největších předností systému TIRIS je extrémně velká čtecí vzdálenost při zachování vysoké spolehlivosti čtení. Čtecí vzdálenost je závislá na mnoha kritériích, standardně je čtecí vzdálenost kolem 1m. TIRIS používá k zabezpečení přenosu dat 16 bitový CRC algoritmus (CRC-CCITT), který zajišťuje, že budou přenášena jen platná data. V případech, že intenzita elektromagnetického pole není dost silná ke spolehlivému přenosu dat, čtečka odpovídá příznaky NO READ nebo INVALID. Tyto čipy pracují s frekvencí 13,56 MHz.

4.2 Stromová struktura souborů na čipové kartě

Stromová struktura čipových karet je obdobná strukturám běžných operačních systémů (obrázek 24) – vrcholová úroveň je kořenový adresář (Master File), následují podadresáře Dedicated File a datové souboru Elementary File. [6] Přístupová práva jsou následující:

- ALW = vždy,
- NEV = nikdy,
- PRO = chráněný, je potřeba správný klíč,
- ENC = šifrovaný – jedná se o rozšíření práva PRO.



Obr. 24: Stromová struktura čipových karet [6]

5 Pardubická karta

5.1 Modernizace odbavovacího systému v MHD

Dopravní podnik města Pardubic a.s. v průběhu léta a podzimu 2006 nahradil mechanický odbavovací systém moderním, perspektivním a univerzálním systémem, který je založen na odbavování cestujících prostřednictvím bezkontaktních čipových karet. S modernizací tohoto systému souvisela i modernizace prodejních zařízení a přepravní kontrola.

Příprava celého projektu se rozeběhla v roce 1998, kdy byly zpracovány studie a průzkumy, které se staly součástí konečného projektu. Ten byl prostřednictvím Ministerstva pro místní rozvoj předán do výběru k financování ze Strukturálních fondů EU, kde byl také schválen, a byla poskytnuta dotace ve výši 18 miliónů Kč. Zbylých 6 miliónů Kč hradí Statutární město Pardubice ze svých fondů. V této kapitole je čerpáno z [7], [8] a vlastních poznatků.

5.2 Popis Pardubické karty

Pardubická karta je koncipována jako bezkontaktní paměťová čipová karta typu Mifare Standard, která slouží jako elektronický nosič jízdného a může být využívána v souladu s obchodními podmínkami i u dalších smluvních partnerů DPmP a.s. Při vybírání technologie byl brán ohled na budoucí širší využití čipové karty v rámci města resp. celého regionu.

Pardubická karta v sobě obsahuje dvě základní funkce – časové jízdné a elektronickou peněženku pro platby jednotlivého jízdného. Nahrazuje papírové časové jízdenky, které se na kartu ukládají. Do budoucna bude možné Pardubickou kartu využít k úhradě nejrůznějších služeb a akcí – např. parkovného, vstupného na společenské, kulturní a sportovní akce apod. Další výhodou Pardubické karty v budoucnu bude úhrada jízdného v rámci integrovaného dopravního systému za účasti dalších dopravců v regionu. Životnost karty je výrobcem garantována na 5 let a majitelem karty je DPmP a.s.

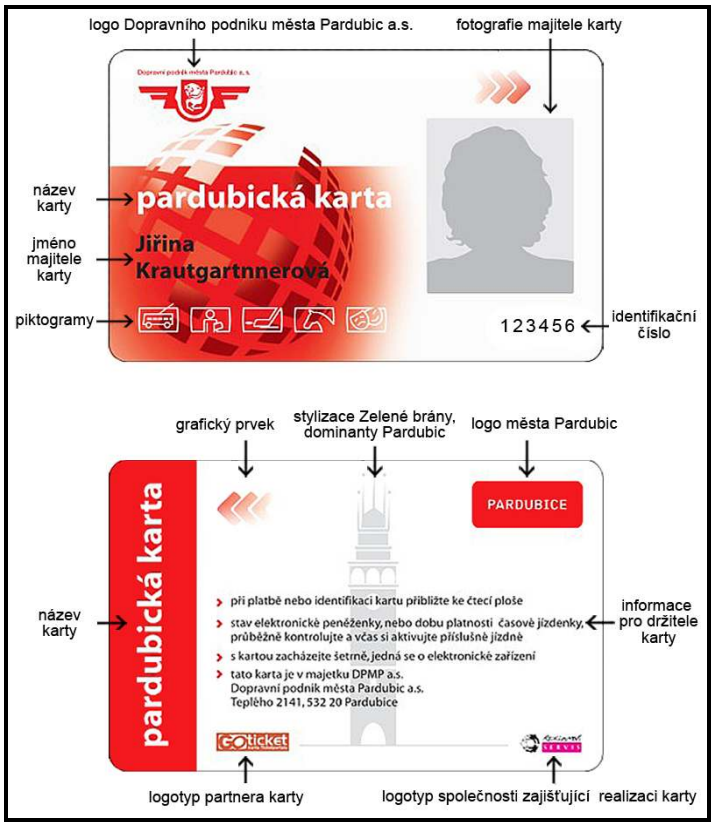
Jízdné je ukládáno v elektronické podobě do elektronického čipu – procesoru, který slouží jako paměť. Její část je využívána jako nosič předplatného časového jízdného a část jako tzv. elektronická peněženka, ve které se ukládají veškeré operace související s uložením finanční hotovosti a jejího postupného čerpání, tedy úhrady za jízdné. Pro získání Pardubické karty je nutno vyplnit „Žádost o vydání Pardubické karty“, která je zdarma k dispozici ve všech předprodejních místech DPmP a.s., na internetových stránkách www.dpmp.cz ke stažení ve formátu PDF, v městském informačním centru a na vrátnici DPmP a.s.

Karta je distribuována ve třech variantách:

- personalizované pro konkrétního uživatele (nepřenosné) – fungují jako elektronická peněženka a zároveň jako nepřenosné časové jízdné. Na kartě je uvedeno jméno, příjmení a fotografie uživatele – obrázek 25. Personalizované karty se dále dělí na:
  - občanské – základní typ, pro libovolné cestující – nezlevněné nepřenosné časové jízdné,
  - občanské zlevněné – pro osoby od 6 do 15 let,
  - žákovské – určené pro žáky ve věku do 16 let po předložení potvrzení o denním studiu,
  - studentské – karty pro studenty od 16 do 26 let po předložení potvrzení o studiu,
  - seniorské – pro seniory nad 65 let po předložení průkazu totožnosti a ověření věku,
  - organizace – karty určené pro firmy a organizace,
  - zaměstnanec – pouze pro zaměstnance DPmP a.s. a jeho rodinné příslušníky,
- nepersonalizované (přenosné, anonymní) – fungují jako elektronická peněženka a časové jízdné přenosné, na kartě není uveden žádný údaj o uživateli karty. Tuto kartu lze dodatečně personalizovat, pokud není mechanicky poškozená,
- zaměstnanecké karty – určené pro obsluhu odbavovacích zařízení (řidič, předprodej, revizor, servis, …).

Požádat o Pardubickou kartu může každý občan bez rozdílu bydliště nebo organizace bez rozdílu sídla firmy. Pro každý typ karty jsou stanoveny samostatné podmínky pro pořízení a používání.

Při pořízení personifikované Pardubické karty je třeba vyplnit Žádost o vydání Pardubické karty, která je zároveň smlouvou mezi uživatelem karty a DPmP a.s. Případný uživatel se dále musí seznámit s Podmínkami pro vydávání a používaní Pardubické karty a podpisem potvrdit souhlas s nimi. Tyto „Podmínky“ jsou součásti žádosti o kartu a obsahují informace o právech a povinnostech uživatele karty i jejího vydavatele. Manipulační poplatek za vystavení karty je 130 Kč.



Obr. 25: Pardubická karta – personalizovaná (přední a zadní strana) [7]

5.3 Používání karty

Pardubickou kartu je možné dobíjet v předprodejních místech DPmP a.s. a zároveň ve vybraných jízdenkových automatech. Karta nesmí být dlouhodobě vystavena vlivům extrémních teplot (pod -10°C a nad 40°C), působení střídavého elektrického nebo magnetického pole a statického elektrického nebo magnetického pole mimo běžný rozsah. Karta nesmí být rovněž jakýmkoliv způsobem ohýbaná, lámaná či jinak povrchově a mechanicky poškozována. Za platnou kartu používanou v odbavovacím systému je považována nepoškozená karta a to bez jakýchkoliv neautorizovaných zásahů do její funkčnosti. Kartu je doporučeno nosit v pouzdře, které je vydáno s kartou – použití je možné i bez vyjmutí karty z pouzdra. Karta by měla fungovat i v případě uložení v dokladovém pouzdře nebo peněžence. Při dodržení výše uvedených pravidel je životnost karty výrobcem stanovena na 5 let ode dne vydání.

Blokování karty

V případě ztráty nebo odcizení je možné kartu zablokovat:

- osobně uživatelem karty v kterémkoliv předprodejním středisku po vyplnění žádosti a prokázání své totožnosti,
- telefonicky po nahlášení hesla, pokud jej uživatel karty uvedl na žádosti o vystavení karty, v opačném případě nebude blokace touto formou provedena.

Zablokováním karty se zabrání čerpání prostředků z elektronické peněženky a zneužití časové jízdenky. Cestujícímu bude vystavena karta nová a bude mu na ni převeden zůstatek z původní karty. Uživatel může dodatečně zrušit blokaci karty za manipulační poplatek, pokud již nepožádal o vystavení karty nové.

Běžné cestování

Cestující s platnou časovou jízdenkou se v denním provozu nemusí při nástupu do vozidla jakýmikoliv dveřmi odbavovat. Cestující předkládá kartu jen při přepravní kontrole. Odbavení probíhá pouze v případě dokupovaných jízdenek pro spolucestující. V provozu, kdy je zaveden nástup předními dveřmi je nutné odbavení všech cestujících u terminálu umístěném v přední části vozidla u kabiny řidiče. Cestující s kartou a s vloženou hotovostí na elektronické peněžence je odbaven terminálem při nástupu do vozidla přiložením karty do čtecí zóny terminálu. Při výstupu z vozidla se cestující opět odbaví u terminálu opětovným přiložením karty do čtecí zóny. Označením výstupu je vypočtena cena za skutečnou provedenou přepravu. Podle druhu karty bude peněženka předdefinována jako zlevněná nebo nezlevněná.

Přestupování

Pokud cestující přestoupí a ve druhém spoji označí kartou nástup do 30 minut od prvního odbavení ve vozidle, má nárok na zlevněný přestup s 50% slevou. Cestující může dále svou elektronickou peněženkou na kartě uhradit jízdné pro 2 spolucestující – tlačítkem na dotykové obrazovce kteréhokoliv čtecího zařízení zvolí nákup dalších jízdenek – viz obrázek 34. Pro potřeby hromadné úhrady jízdného (např. školy) je možné využít platbu z karty přímo u řidiče vozidla. Cestující je povinen v takovém případě nahlásit řidiči vozidla počet a druhy požadovaných jízdních dokladů a příslušné tarifní pásmo, ve kterém se bude skupina osob pohybovat.

Doklad o zaplacení, kontrola a převod karty

Pokud cestující potřebuje doklad o zaplacení jednotlivého jízdného, musí nastoupit předními dveřmi, na dotykové obrazovce zvolit „TISK“, přiblížit kartu ke snímači a odebrat doklad z tiskárny. Každý uživatel karty si může na obrazovce kteréhokoliv čtecího zařízení kdykoliv zkontrolovat stav karty – tj. platnost časové jízdenky, zůstatek prostředků na elektronické peněžence a další údaje – po stisku políčka „Info“ na dotykové obrazovce a přiblížení karty ke snímači (obrázek 34). Majitel Pardubické karty se může rozhodnout pro převod obsahu karty na kartu jinou. Takto může být převedena hotovost v elektronické peněžence nebo předplatné časové jízdné. Takový převod je možné provést ve všech předprodejních střediscích Dopravního podniku a to bez udání důvodu za podmínek, které nebudou v rozporu s tarifními a Smluvními přepravními podmínkami.

5.4 Budoucnost Pardubické karty

1. června 2007 bylo zavedeno vzájemné uznávání čipových karet v Pardubicích a Hradci Králové. V první fázi se uznávají pouze elektronické peněženky, do budoucnosti se počítá s možností mít na jedné kartě předplacené jízdenky pro jeden či druhý dopravní podnik. Od podzimu 2007 se začne testovat placení parkovného v Pardubicích, plný provoz tohoto systému by měl být spuštěn ještě v prosinci 2007. Koncem roku se spustí pilotní projekt integrace Pardubické karty do základních a středních škol, kdy bude nejprve vybráno několik škol, na kterých se bude systém testovat. Po úspěšném otestování by k plnému provozu mohlo dojít během roku 2008. Výhodou zavedení Pardubické karty na školách by byla možnost kontroly docházky žáků a studentů středních škol – například zasláním automatického e-mailu či SMS zprávy rodičům, pokud se žák/student střední školy nedostaví do určité hodiny do školy). Další fáze je možnost rezervace do sportovních a kulturních zařízení, případně poskytnutí aplikačního prostoru karty dalším, soukromým, subjektům, se plánuje také během let 2008 a 2009. DPmP a.s. se nebrání poskytnutí karet firmám, které by projevily zájem zavést například prezenční systém na principu Pardubické karty. V budoucnu by byl prostor pro spolupráci s bankovními ústavy, nutností by ale pak byla změna karet (DESFire, procesorová apod.)

6 Softwarové testování Pardubické karty

6.1 Systém BackOffice

BackOffice je systém plnohodnotného zajištění všech operací, nutných k provozu systému – vydávání a správy čipových karet, předprodeje, odbavování, revizorské kontroly a zpracování statistických informací z provozu odbavovacího a revizorského systému.

BackOffice je složen z několika základních částí (pracovišť). Centrem systému je server WinADO[1], který slouží jako úložiště dat a je hlavní operační jednotkou, k níž jsou pomocí komunikační infrastruktury připojena jednotlivá pracoviště (PC v podobě klientského počítače WinADO či přímo zařízení firmy EM TEST ČR spol. s r.o.) – celý systém je znázorněn v příloze B. [8]

Základní dělení klientů systému WinADO:

- personalizační pracoviště – slouží k personalizaci bezkontaktních čipových karet. Pracoviště je vybaveno vhodným zařízením – čtečkou čipových karet a odpovídajícím softwarem na obslužném PC,
- předprodejní pracoviště – pracoviště pro možnost plnění elektronických peněženek a prodej časových jízdenek, pracoviště musí být taktéž vybaveno čtečkou a obslužným PC – v praxi bývá sloučeno s personalizačním pracovištěm,
- revizorské pracoviště – slouží k vyčítání a aktualizaci revizorských čteček a pro zpětnou kontrolu stavu účtů, zablokovaných karet, apod.,
- pracoviště pro přípravu vstupních dat – slouží k zavádění jízdních řádů, tvorbě tarifního systému, turnusů a k ostatním aktivitám přímo souvisejících s provozem dopravy, včetně tvorby výstupních sestav ze systému,
- pracoviště osobní pokladny – pro zavádění a zpracování odpočtů z jednotlivých zařízení (palubní počítače umístěné ve vozidlech a předprodejní aplikace),
- palubní počítač – umístěný v jednotlivých vozech, který zasílá statistiku vydaných jízdenek na server a přijímá změny v jízdních řádech, v tarifním systému, v textech světelných tabulí, v turnusech, v seznamu blokovaných karet apod.

Jednotlivá pracoviště jsou rozdělena pro přehlednost podle hlavní náplně práce, v praxi je možné vykonávat všechny operace na kterémkoliv klientu (mimo palubní počítač), pokud to dovolí přístupová práva a potřebný hardware. [8]

6.2 Systém WinADO

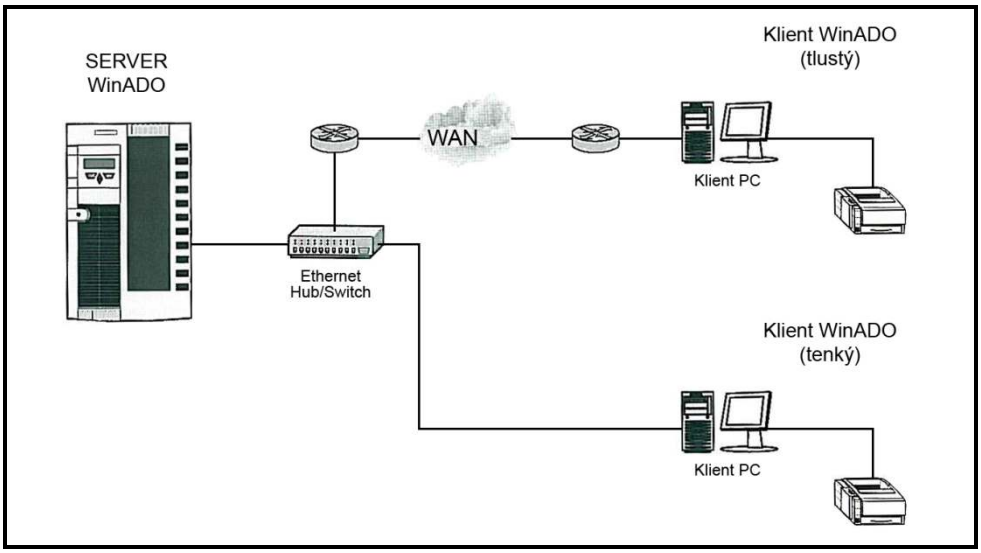
Server WinADO je vybaven serverovým operačním systémem od společnosti Microsoft a databázovým strojem MS SQL2000[2]. Server je úložištěm všech dat a programového vybavení systému WinADO.

Klient systému WinADO je počítač, kterému je umožněno spuštění klientské aplikace WinADO a využívání funkcí systému dle nastavených uživatelských práv přihlášeného uživatele. Klienti se dělí na dva základní typy – obrázek 26:

- tenký klient WinADO – počítač s operačním systémem MS Windows 98 SE a vyšším s konektivitou a dostatečnými přístupovými právy na server WinADO, ze kterého spouští aplikaci WinADO. Tenký klient se využívá v rámci sítí s dostatečnou propustností (např. LAN). Výhodou tohoto klienta jsou menší nároky na administraci aplikační části systému WinADO.

[1] Software založený na architektuře klient/server – skládá se z databázového serveru a klientských PC.
[2] Relační databázový systém firmy Microsoft.

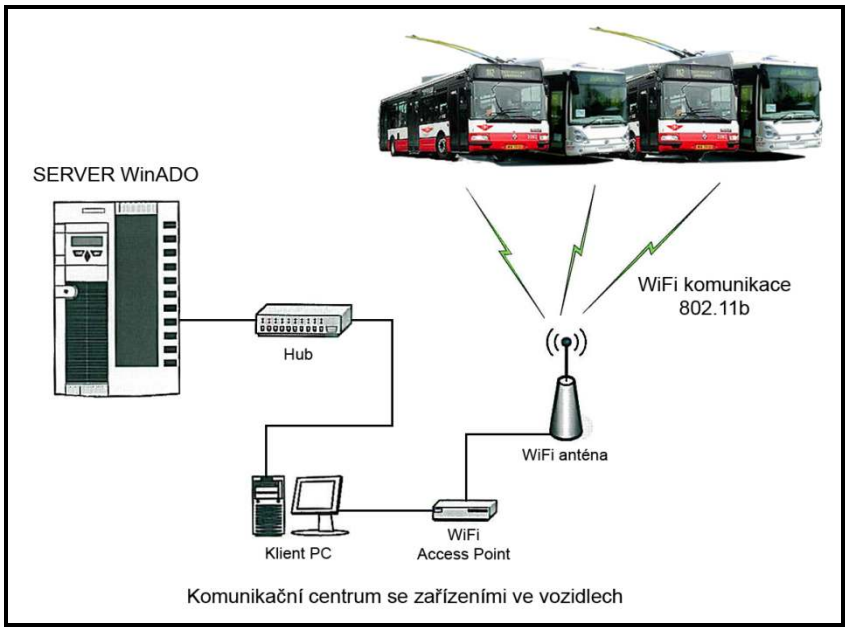
- tlustý klient WinADO – počítač s operačním systémem MS Windows 98 SE a vyšším s konektivitou a dostatečnými přístupovými právy na server WinADO. Tlustý klient spouští aplikaci z lokálního disku a se serverem komunikuje pouze na datové úrovni. Tlustý klient se využívá v rámci sítí s nižší prostupností (např. WAN). Nevýhodou tohoto klienta jsou vyšší nároky na administraci aplikační části systému WinADO.



Obr. 26: Blokové schéma WinADO – server – klient [8]

Jednotlivá pracoviště DPmP a.s. jsou podle umístění rozdělena na tenkého a tlustého klienta – pracoviště, umístěná přímo v areálu Dopravního podniku města Pardubic a.s., jsou spojeny pomocí lokální sítě LAN a tudíž považovány za tenké klienty, dislokované pracoviště potom spojuje síť WAN (tlustý klient).

Samostatným článkem v systému jsou potom jednotlivé vozy – trolejbusy a autobusy. Ty obsluhuje pracoviště se standardním klientem systému WinADO, který je však rozšířen o další síťovou kartu, ke které je připojen WiFi AccessPoint. Na klientském počítači je instalován softwarový firewall, který chrání síť před napadením případnými útočníky přes WiFi komunikaci. K AccessPointu je připojena anténa s patřičnou charakteristikou, aby umožnila pokrytí požadovaného prostoru pro komunikaci se zařízeními v odstavených vozidlech – celý tento systém je znázorněn na obrázku 27. [8]



Obr. 27: Blokové schéma komunikace s vozidly [8]

Prostory vozového parku DPmP a.s., ve kterých se nacházejí vozy, jsou pokryty WiFi signálem. Když přijede vůz do areálu pokrytého signálem WiFi, načtou se přes tuto technologii ze zařízení vozidel statistiky o daném turnusu a do těchto zařízení se nahrávají potřebná nová data. Optimální pokrytí areálu DPmP a.s. zabezpečuje celkem pět přístupových bodů, které jsou propojeny STP kabelem 24GW nebo v nepřístupných místech (z důvodu křížení elektrického vedení) WDS (Wireless Distribution System) režimem do lokální sítě. Komunikace mezi WiFi zařízeními probíhá v šifrované podobě, tudíž je dostatečně zabezpečená před průnikem nežádoucí třetí strany do interní sítě.

6.3 Základní technologie Pardubické karty

V této části je čerpáno z [8], doplněno o vlastní poznatky. DPmP a.s. používá ve spolupráci s firmou EM TEST ČR spol. s r.o. čipovou kartu Mifare® Standard 4k[3] s pamětí EEPROM 4kB. Tento typ karty umožňuje široké použití při úhradě za poskytování služeb u různých dopravců a jiných subjektů v regionu, kontrolu a zajišťování evidence, realizace dopravních průzkumů, řešení různých aktivit a přístupových práv držitele. Postupné rozšiřování o další aktivity nevyžaduje fyzickou výměnu karty.

Uvedená karta disponuje paměťovým prostorem 4kB, který je rozdělen do 32+8 zabezpečených sektorů a umožňuje tak snadnou implementaci více aplikací, včetně elektronické peněženky. Šifrovaný bezkontaktní přístup k jednotlivým sektorům je zabezpečen dvěma různými klíči a u každého klíče lze nadefinovat povolené operace s daty v jednotlivých blocích. Každá karta má jednoznačné nesmazatelné identifikační číslo dané výrobcem (4 B = přes 4 miliardy kombinací), kterým je v celém systému identifikována. V paměti karty jsou uložena i data o držiteli. Karta je optimalizována pro co nejrychlejší odbavení a celá transakce může být kratší než 100 milisekund. Na jednu čipovou Mifare kartu je možné umístit více aplikací – za aplikaci se považuje definovaná funkčnost nevyžadující přímou spolupráci s jinou aplikací. Výrobce garantuje životnost 100 000 cyklů záznamů. Bezkontaktní čipové karty Mifare mají několik nezávislých částí (sektorů) se samotným přístupem pro čtení i zápis. To umožňuje, aby na kartu mělo přístup více nezávislých subjektů. Následující tabulka 2 ukazuje přehled parametrů použité čipové karty Mifare.

Tab. 2: Technické parametry čipové karty Mifare Standard 4k

Typ přenosu dat		bezkontaktní
Frekvence přenosu		13.65 MHz
Rychlost přenosu dat (čtení/zápis)		106 kBaud
Doba transakce		menší než 100 ms
Paměť karty	Celková	4 096 B
	použitelná	3 440 B
Rozdělení paměťového prostoru		32 sektorů se 4 bloky po 16 B, 8 sektorů po 256 B
Počet záznamů		minimálně 100 000 zápisů
Zachování záznamů		minimálně 10 let
Provozní vzdálenost		až 100 mm
Rozměr		85,6 x 54 x 0,76 mm
Materiál		PVC
Barva		bílá, matná
Napájení		indukční
Provozní teplota		-25 až +70 °C
Skladovací teplota		-55 až +125 °C

[8]

[3] Toto je obchodní označení karty, skutečný název karty je Mifare Standard 4 Kyte Card IC MF1 IC S70.

6.3.1 Vnitřní architektura karty

V kartě je po obvodě zabudována smyčka antény, která je připojena na vysokofrekvenční obvody (RF-Interface), které fyzicky zabezpečují bezkontaktní přenos mezi kartou a čtecím zařízením. Součástí je RF (Radio Frequency) modulátor a demodulátor, zdroj kmitočtu a napěťový regulátor. V bloku označeném Digital Control Unit je mikroprocesorová jednotka se speciálními obvody:

- Anticollision – pro řešení kolizí při detekci více karet v dosahu jednoho přijímače,
- Authentication – třístupňová bezpečnostní autentizace karty,
- Crypto – kryptografický procesor, který zrychluje šifrovací operace,
- Control&ALU – jádro mikroprocesoru a jednotka pro podporu aritmetických operací , které se využívají pro funkce elektronické peněženky,
- rozhraní na elektronicky přepisovatelnou paměť.

Blok elektronicky přepisovatelé paměti (EEPROM) slouží k uložení aplikačních dat a pro konfigurační data včetně přístupových klíčů. Karta neobsahuje vlastní zdroj energie – pro provoz se používá energie indukovaná do cívky karty z vysílače, obsaženém v čtecím zařízení. V kartě jsou dále vestavěny bezpečnostní prvky, které umožňují ochranu dat uložených na kartě i při přenosu mezi kartou a čtecím zařízením:

- vzájemná 3 stupňová autentizace mezi kartou a čtečkou pro přístup k datům do jednotlivých sektorů (ISO 9798-2),
- šifrování přenášených dat s ochranou proti zneužití odposlechnutých autentizačních dat karty jejich zopakováním při podvodné autentizaci,
- pár klíčů pro každý ze 40 sektorů umožňuje provozovat velký počet nezávislých aplikací, kdy data jedné z nich nejsou přístupná ostatním,
- unikátní sériové číslo každé karty,
- transportní klíč omezuje přístup do pamětí karty při transportu od výrobce čipu pouze na oprávněné odběratele, vybavené odpovídajícím klíčem.

6.3.2 Integrita dat

Integrita dat při přenosu je zajištěna následujícím způsobem:

- kontrolní suma 16 b pro každý blok,
- paritní bit pro každý byte,
- kontrola počtu bitů,
- kódování bitů pro rozlišení 0 a 1,
- monitorování přenosového kanálu (protokol, analýza toku bitů).

6.3.3 Zpracování transakcí

Elektronické obvody karty se aktivují, pokud se dostane do účinného dosahu antény čtecího/zapisovacího (dále jen čtecího) zařízení a indukovaná energie dostačuje pro jejich provoz. Karta odpoví na „výzvu“ čtecího zařízení, které vyhodnotí, kolik odpovědí dostalo, tj. kolik karet je v dosahu. „Antikolizní mechanismus“ vyhodnotí podle unikátního čísla karty jednu z karet a tu osloví, pošle jí příkaz „výběr“. Ostatní karty pozastaví a tyto musí čekat na další „výzvu“. S vybranou kartou zahájí čtecí zařízení třístupňovou autentizaci, která se vztahuje přímo ke konkrétnímu sektoru karty. Po úspěšné autentizaci následují čtecí/zapisovací nebo inkrementální/dekrementální operace. Tyto operace nevyžadují další autentizaci, pokud se vztahují ke stejnému sektoru. Po ukončení všech požadovaných operací je karta pozastavena a čtecí zařízení opět vysílá „výzvu“. Toto se odehrává v řádech desetin sekundy.

6.3.4 Bezpečnost systému při použití Mifare karet

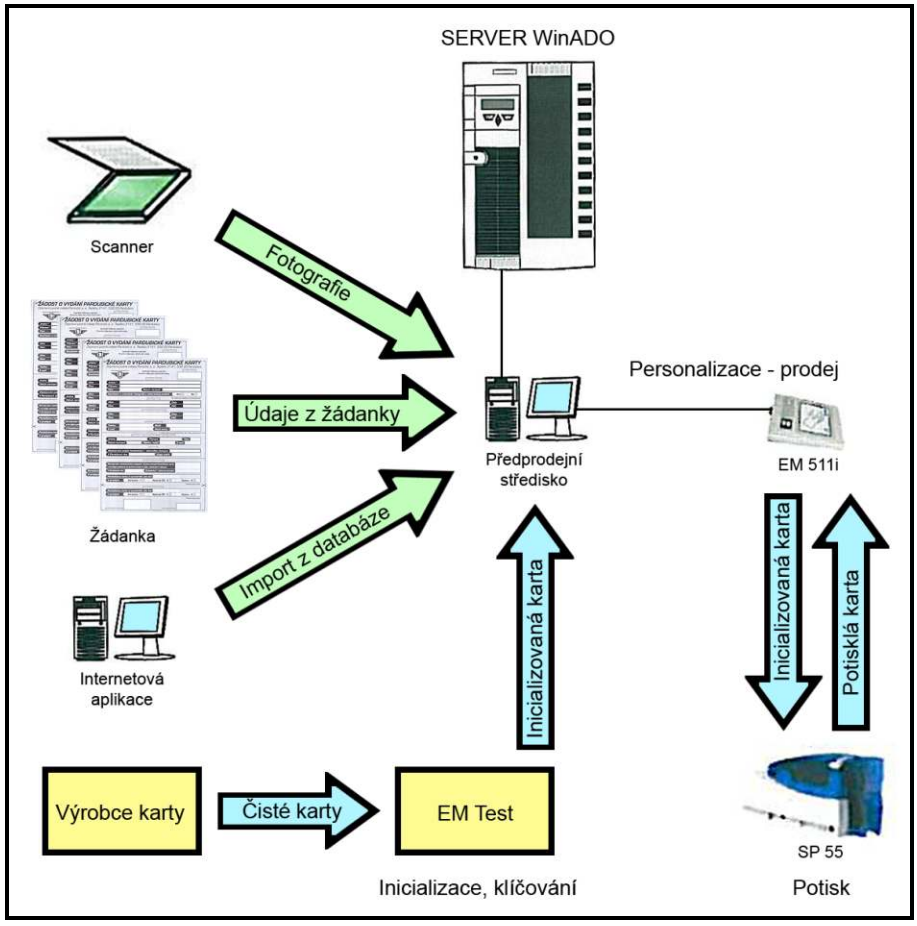
Bezpečnost systému je při použití karet Mifare v současné době na technicky možné úrovni, neboť tyto karty jsou chráněny kryptoprocesorem (bezpečnostní logika, založená na propracovaném systému přístupových hesel a šifrování dat podle standardu Mifare Crypto). Systém EM TEST však používá i další ochranu, založenou na kódování údajů na kartě a současné podvojné registraci údajů, kdy se pohyb na čipové kartě zaznamenává i v terminálu a tyto údaje se pak vyhodnotí přes obslužný software. V jednotlivých čtecích zařízeních (terminálech) pak lze zablokovat karty, na nichž by byl zaznamenán nežádoucí pohyb.

6.4 Životní cyklus karty

Dříve než se karta začne používat jako Pardubická karta, musí projít následujícími kroky:

- inicializace karty pro dopravní aplikaci včetně nahrání odpovídajících klíčů pro DPmP a.s.,
- potisk karty,
- personalizace karty (pouze u nepřenosných karet).

Uvedené operace jsou prováděny ve dvou úrovních v závislosti na počtu požadavků na Pardubickou kartu. První úroveň je optimalizována na skokový nárůst požadavku na kartu a probíhá například při nasazení nového odbavovacího systému. Předpokládaný skokový nárůst požadavků při nasazení systému je 20 – 30 tisíc kusů karet. Po odeznění vlny žádostí o kartu je k dispozici druhá úroveň systému znázorněná na obrázku 28, která je optimalizována na řádově desítky požadavků denně. Tyto úrovně se mohou vzájemně prolínat v závislosti na požadavcích na karty ze strany uživatelů.



Obr. 28: Životní cyklus karty při průběžných požadavcích [8]

6.5 Statistické výstupy

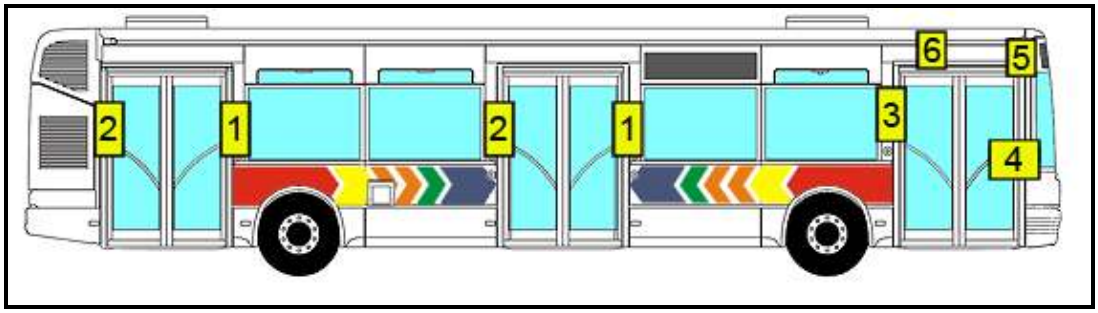
Systém WinADO umožňuje na základě statistiky vyčtené z odbavovacích zařízení ve vozidlech a z předprodejní aplikace provádět statistické výstupy (přehledy). Standardní dělení těchto výstupů je následující:

- statistické výstupy z odbavovacích zařízení včetně předprodejní aplikace,
- statistické výstupy z pohybu na čipové kartě.

Výstupy jsou realizovány ve formě tabulek. Díky použité technologii postupného vnořování je možnost u každého zobrazeného řádku získat podrobnější informace. V některých případech je možné zvolit různé formy zobrazení podrobnějších informací vybraného řádku. Zobrazené výstupy je možné vytisknout, exportovat, případně pomocí schránky systému zkopírovat do jiné aplikace. U všech výstupů je možnost různého nastavení – například výběr zobrazených sloupců, nastavení omezení zobrazených dat (podle tarifu, období, měny, linky, turnusů atd.). Jednotlivá nastavení je možné ukládat do tzv. profilů jednotlivých uživatelů. V detailním výpisu jedné jízdy lze zobrazit přesné informace o jízdě – jméno řidiče, linka spoje, číslo kasy, cena jízdy, zůstatek na kartě, tarif, nástupní a výstupní zastávky atd. V příloze C je vlevo ukázka aplikace s výstupy podle držitelů čipových karet – konkrétně se jedná o testovací čipovou kartu číslo 800382, která byla zapůjčena na testování. V uvedené příloze je pak výpis jízd absolvovaných počátkem prosince 2006, včetně podrobného přehledu o době jízdy, zůstatku, použitého zařízení apod. V pravé části přílohy C je potom opis lístku jedné konkrétní jízdy s číslem 1606, konkrétně na lince 13 ze zastávky Polabiny, Sluneční na zastávku U Grandu.

6.6 Realizace

Montáž čtecích zařízení do vozidel DPmP a.s. probíhala během léta 2006. Do každého vozidla (autobus i trolejbus) bylo montováno zařízení pro identifikaci čipových karet, kombinované zařízení umožňující tisk dokladů, řídící jednotku odbavovacího systému a případně i zobrazovač času/zastávky. Schematické znázornění přístrojů ve vozidle ukazuje obrázek 29.



Obr. 29: Rozmístění čtecích zařízení ve vozidle. 1 – Kombinované zařízení pro identifikaci čipových karet a označení papírového jízdního dokladu; 2 – Zařízení pro identifikaci čipových karet; 3 – Elektronický označovač papírového jízdního dokladu; 4 – Kombinované zařízení pro identifikaci čipových karet a výdej papírového jízdního dokladu; 5 – Řídící jednotka odbavovacího systému; 6 – Zobrazovač času a zastávky [8]

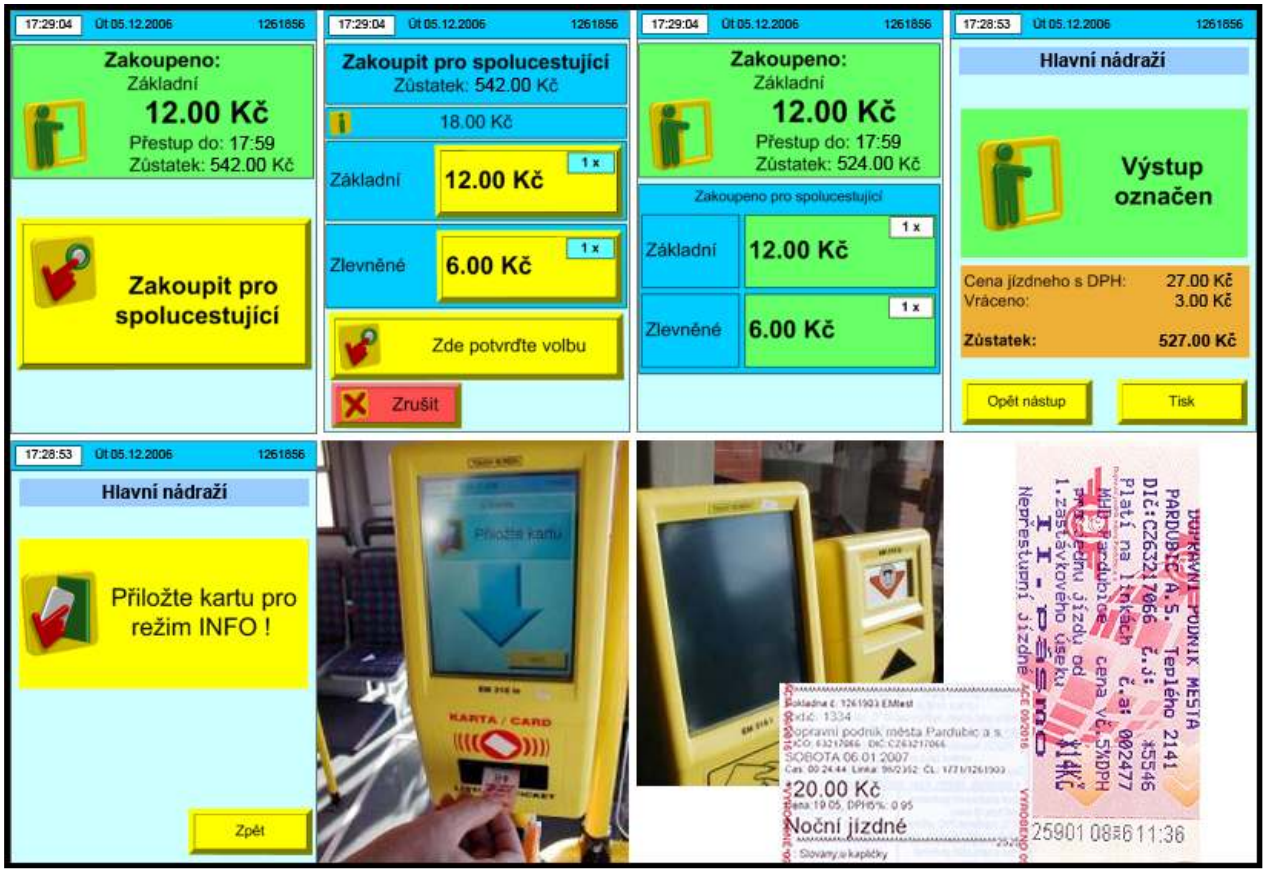
Montáž spočívala v natažení síťových a napájecích kabelů skrz celé vozidlo nad okny a jejich protažení do jednotlivých madel, na které byly poté přimontovány držáky čtecích zařízení. V pojistkové skříni vozidla byly provedeny nezbytné úpravy, byl namontován palubní počítač, přijímač GPS a WiFi rozhraní pro komunikaci se serverem v depu. Po montáži přišla fáze tetování, kdy se v každém voze otestovala funkčnost jednotlivých čteček z hlediska správného sesíťování a komunikace. Za jeden pracovní den se podle počtu pracovníků upravily 2 až 4 autobusy (trolejbusy). Následující obrázky 30-33 jsou fotografie z realizace v DPmP a.s. během července a srpna 2006.

Obr. 30: Síťování autobusu Karosa B731

Obr. 31: Elektrická skříň a palubní počítač

Obr. 32: Příprava pro držáky čtecích zařízení

Obr. 33: Namontované držáky a celkový pohled na testovací čtecí zařízení



Obr. 34: Obrazovky z provozu čtecích zařízení po přiložení karty a papírové jízdenky (vytisknutá na palubní tiskárně a z předprodejního automatu)

7 Modely a využití karet jiných dopravců v ČR

7.1 Integrovaný dopravní systém

V dnešní době již většina významných dopravců v ČR využívá výhod a předností čipových karet. Tito jednotliví dopravci jsou často sdruženi v takzvaných integrovaných dopravních systémech – IDS. IDS je systém dopravní obsluhy určitého uceleného území veřejnou dopravou zahrnující více druhů dopravy (např. městskou, regionální, železniční apod.) nebo linky více dopravců, jestliže jsou cestující v rámci tohoto systému přepravováni podle jednotných přepravních a tarifních podmínek.

Doprava bývá v rámci IDS zajišťována různými dopravními prostředky: železnicí, metrem, tramvajemi, trolejbusy, autobusy, lanovkami nebo plavidly. Na dopravě v rámci IDS se mohou účastnit různí dopravci, přičemž jízdní řády jednotlivých linek v rámci IDS by měly být optimalizovány, a to bez ohledu na to, který dopravce dotyčnou linku provozuje.

V současné době se v českých IDS používá zejména zónový nebo pásmový tarif. To znamená, že území s integrovaným dopravním systémem se člení na jednotlivé zóny (pokud mají tvar soustředných kruhů, resp. mezikruží čili prstenců, označují se jako pásma). Pásmové rozdělení území IDS je výhodnější v případě menšího území s jednou městskou aglomerací uprostřed, u kterého v okrajových částech převládají radiální přepravní proudy. Rozdělení na zóny je vhodnější v území s více regionálními centry a větším podílem mezizónové přepravy. V tabulce 3 je přehled krajů České republiky a jejich integrovaných systémů, které jsou v dalších podkapitolách popsány z hlediska využívání čipových karet.

Tab. 3: Integrované dopravní systémy v ČR

Kraj	Název IDS	Zkratka
Středočeský kraj a Hlavní město Praha	Pražská integrovaná doprava	PID
	Středočeská integrovaná doprava	SID
Jihočeský	Českobudějovická integrovaná doprava	IDS ČB
	IDS Tábor – Sezimovo Ústí – Planá nad Lužnicí	IDS TA
Plzeňský	Integrovaná doprava Plzeňska	IDP
Karlovarský	Integrovaná doprava Karlovarského kraje	IDOK
Liberecký	Integrovaný dopravní systém Libereckého kraje	IDS LK
	Jablonecký regionální integrovaný systém	JARIS
Pardubický a Královéhradecký	Východočeský dopravní integrovaný systém	VYDIS
	Integrovaná regionální doprava Broumovsko, Poličsko, Hronovsko a Náchod	IDEKO IREDO
Jihomoravský	Integrovaný dopravní systém Jihomoravského kraje	IDS JMK
Olomoucký	Integrovaný dopravní systém Olomouckého kraje	IDSOK
Zlínský	Zlínská integrovaná doprava	ZID
Moravskoslezský	Ostravský dopravní integrovaný systém	ODIS
Vysočina / Ústecký	Nemají / Na počátku	–

[9]

V následujícím přehledu jsou uvedeny významní dopravci v jednotlivých regionech, případně funkce integrovaného systému, převážně s důrazem na používaný odbavovací systém a čipové karty a jejich vzájemnou akceptaci. Technické specifikace jednotlivých karet jsou uvedeny v kapitole 4, proto zde jsou uváděny pouze stručné informace.

7.2 Hlavní město Praha

Pražská integrovaná doprava (PID) se z části prolíná se Středočeskou integrovanou dopravou (viz dále) a díky vzniku již v roce 1992 patří mezi nejstarší v republice. Oba systémy používají karty Mifare Standard, případně novější Mifare DESFire – oba tyto systémy fungují vedle sebe. V polovině dubna 2007 došlo ke spuštění projektu OPENCARD, tedy čipové karty pro obyvatele a návštěvníky Prahy. Karta OPENCARD se postupně rozšíří do několika oblastí, vedle hrazení parkovného v zónách placeného stání bude tato karta sloužit pro služby městské knihovny,

zabezpečený přístup na informační portál Prahy, úhrada vstupu do kulturních a sportovních zařízení a na společenské akce (koncerty, divadla, galerie, muzea, kina, bazény apod.), vstup do památkových objektů, hrazení obecních poplatků, používání městské hromadné dopravy a integrovaného dopravního systému, atd. Z počátku bude pro uživatele pouze karta vydávaná na jméno (vázána na konkrétní fyzickou osobu). Do budoucna je plánován vznik nepersonalizované karty, která bude sloužit zejména turistům a návštěvníkům Prahy. [10] Jedná se o hybridní karty, tedy o kombinaci kontaktní a bezkontaktní části (viz kapitola 4.1). Bezkontaktní čip je Mifare Standard 4k. Dodavatelů systému je více, hlavní část software kartového centra dodala společnost HAGUESS, a.s.

7.3 Středočeský kraj (SID)

Středočeská integrovaná doprava (SID) zahrnuje Kladenskou integrovanou dopravu (KLID), Integrovanou dopravu Berounska (IDB), Integrovanou dopravu Benešovska a Integrovanou dopravu okresu Kutná Hora (IDS KH). Dopravce, spadající do SID, musí mít odbavovací zařízení, která cestujícím umožňují používat bezkontaktní čipovou kartu s elektronickou peněženkou a elektronickými kupóny ve formátu bezkontaktní čipové karty technologie Mifare Standard, kterou postupně nahrazuje novější a bezpečnější Mifare DESFire. Vydávání karet u jednotlivých dopravců je na vzájemné dohodě, své karty může vydávat jakýkoliv dopravce, který zároveň může zprostředkovávat vydávání i karet jiných dopravců, spadajících do SID. Dopravce musí mít vybudován funkční systém přenosu dat z odbavovacích zařízení na svoje určené pracoviště. Způsob přenosu není určen – může se jednat o technologie PCMCIA, GPRS, WiFi atd. Dopravce musí mít dále vybudován systém předávání dat do clearingového centra z určeného pracoviště. V případě, že dopravce vydává bezkontaktní čipovou kartu s elektronickou peněženkou, kterou akceptují i jiní dopravci, musí mít povolení ČNB k vydávání elektronických peněz podle zákona č. 124/2002 Sb., o platebním styku, v platném znění. Nový účastník clearingu musí s ostatními účastníky clearingu uzavřít příkazní smlouvy na dobíjení elektronických peněženek na bezkontaktní čipové kartě a vzájemné smlouvy o akceptaci elektronických peněženek na bezkontaktní čipové kartě, zároveň musí mít uzavřenou smlouvu s ČSAD SVT Praha s.r.o. (pověřený provozovatel clearingu) o využívání služeb clearingového centra. [11]

7.4 Jihočeský kraj (IDS ČB a IDS TA)

Jihočeský kraj má v tuto chvíli dvě skupiny integrovaných systémů – první funguje v okolí Českých Budějovic jako Českobudějovická integrovaná doprava a druhá v okolí Tábora pod názvem IDS Tábor – Sezimovo Ústí – Planá nad Lužnicí. Jihočeský krajský úřad nyní dokončuje projekt souhrnného IDS pro celý kraj. Jednotliví dopravci proto čekají, jak celá situace dopadne a až na výjimky čipové karty nepoužívají. Dle vyjádření Dopravního podniku města Českých Budějovic je připravován projekt na zavedení karet v rozsahu podobném jako v Plzni, Pardubicích či Hradci Králové, tedy v podobě metropolitní karty s využitím v MHD, knihovnách, školách atd. Konkrétní technologie však ještě nebyla zvolena, DPmČB, a.s. v tuto chvílí získává informace a zkušenosti z míst, kde již podobný systém funguje.

Společnost COMETT PLUS, spol. s r.o. zajišťuje v regionu Tábor – Sezimovo Ústí a Planá nad Lužnicí pravidelnou autobusovou a městskou hromadnou dopravu. V pravidelné autobusové dopravě se zavedení čipových karet bude řídit požadavky chystaného IDS Jihočeského kraje, v případě MHD Tábor je situace obdobná s tím, že je snaha, aby případná čipová karta sloužila i pro potřeby měst Tábor, Sezimovo Ústí a Planá nad Lužnicí.

V tuto chvíli se v těchto městech používá odbavovací systém od firmy R&G Mielec Polsko, proto by byla snaha tento stávající systém pouze rozšířit o čtečky čipových karet.

7.5 Plzeňský kraj (IDP)

V Integrovaném Systému Plzeňska se využívá projekt Plzeňské karty, který patří mezi první bezkontaktní čipové karty v celém regionu. Využívá se čipová karta CMC1 francouzské společnosti ASK s čipem Philips Semiconductors Mifare Standard podle ISO/ IEC 14443 typ A, který disponuje paměťovým prostorem 1 kB. Primárně je Plzeňská karta určena pro placení jízdného v IDP, sekundárně s ní pak lze platit v různých městských a regionálních organizacích, jako je například plzeňské Divadlo J. K. Tyla, zoologická a botanická zahrada Plzeň a další. Elektronickou peněženku je možné nabít až do výše 4000 Kč a je v prodeji nejen v prodejnách PMDP v Plzni, ale také ve vybraných informačních centrech, v prodejnách novin a tabáku, vybraných hotelích a dalších místech. Uživatelská obsluha je realizována pomocí samoobslužného terminálu Cardman. Jako první v České republice je možné Plzeňskou kartu používat jako studentskou kartu typu ISIC. Tato karta je vydávána studentům starších 14 let středního odborného učiliště, střední, vyšší odborné nebo vysoké školy uznané Ministerstvem školství, mládeže a tělovýchovy ČR. Licence ISIC je vydávána vždy na jeden rok. Plzeňská karta ISIC pak na označených místech slouží jako identifikační, přístupový, platební a bezpečnostní nástroj pro oblast služeb města Plzně a pro komerční služby v rozsahu definovaném vydavatelem. Dále lze tuto kartu využívat jako elektronickou peněženku např. k úhradě za nákup zboží a služeb u PMDP a dalších smluvních partnerů. Další typy Plzeňské karty jsou ITIC (pro učitele), SCHOLAR (pro žáky základních škol) a IYTC (ALIVE – průkaz mládeže). V případě poškození, ztráty, odcizení či jakýchkoliv nesrovnalostí všech typů Plzeňské karty se toto řeší přímo s PMDP. [12]

7.6 Karlovarský kraj (IDOK)

Integrovaná doprava Karlovarského kraje používá odbavovací systém a čipové karty společnosti EM TEST ČR spol. s r.o. Karty jsou typu Mifare Standard s paměťovým prostorem 1 kB. Všichni dopravci v rámci celého IDOK používají stejný typ karet a odbavovacího zařízení. Mezi významné členy IDOK patří LIGNETA autobusy s.r.o., Autobusy Karlovy Vary, a.s., Dopravní podnik Karlovy Vary, a.s., Viamont a.s. a České dráhy, a.s. Pouze jeden z dopravců provozujících příměstskou autobusovou dopravu (Věra Havlovičová) používá odbavovací systém společnosti Mikroelektronika spol. s r.o.

7.7 Liberecký kraj (IDS LK a JARIS)

Část následujícího textu je z [13], zbytek je z vyjádření koordinátora Libereckého kraje KORID LK. Na příměstské dopravě v Libereckém kraji, která je provozována ČSAD Česká Lípa a.s., ČSAD Liberec, a.s., ČSAD Jablonec nad Nisou a.s. a ČSAD Semily, a.s. se používají bezkontaktní čipové karty Mifare Standard 1k – dodavatelem čipových karet a odbavovacího zařízení je firma EM TEST ČR spol. s r.o. Karta se využívá se jako elektronická peněženka s možností předvolby 4 linek a se slevou 10. jízdy zdarma během 15 dnů. Na platbu čipovou kartou se poskytuje sleva ve výši 5 % z jízdného placeném v hotovosti. Tyto slevy neplatí pro žáky a studenty, kterým je již sleva poskytnuta. Na další jinou funkci není čipová karta prozatím určena. Kromě výše uvedených dopravců využívá tuto kartu i Dopravní podnik Mladá Boleslav, s.r.o. a Transcentrum bus, s.r.o. Všichni výše uvedení dopravci mají navzájem uzavřeny smlouvy o uznávání čipových karet a vzájemném zúčtování. Společnost Vett a.s. Zákupy provozuje MHD v České Lípě a používá stejný standard, tedy Mifare Standard 1k, ale pouze pro potřeby své MHD – využívána je jako elektronická peněženka a personifikovaná předplatní jízdenka. IDS LK je zatím v přípravě, základem bude modernizace odbavovacího systému v autobusové dopravě modernějším systémem založeným již na bázi procesoru Intel.

V rámci MHD v Liberci je používána tzv. Liberecká městská karta standardu Mifare Standard 4k a strukturou MAD, která zatím slouží jako předplatní jízdenka a v budoucnu bude sloužit i jako elektronická peněženka. Dodavateli jsou společnosti Mikroelektronika spol. s r.o. a firma Apex spol. s r.o. Kromě dopravní funkce umožňuje i další aplikace:

- identifikace v systému Slevy v kapse (kulturní památky, sport, restaurace, …),
- rezervace vstupenek přes internet,
- docházkové systémy a stravovací systémy,
- vstup do radnice.

Primárně je projekt Liberecké městské karty zaměřen na občany města Liberec a na poskytování služeb na jeho území. Počítá se však i s tím, že se připojí další města a obce, dokonce i libovolné instituce z ČR a příhraničí, pro které bude podobná služba efektivní. Budovaná infrastruktura ve formě Kartového centra je dostatečně dimenzovaná a variabilní.

V budoucnu, po modernizaci odbavovacího zařízení v příměstské dopravě, bude jednotná platforma Mifare Standard 4k se strukturou MAD, kterou budou používat všichni zúčastnění dopravci v IDS na území Libereckého kraje. Souběžně však budou do konce životnosti platit současné ČK Mifare Standard 1k, u kterých však bude muset být změněna struktura na MAD.

7.8 Pardubický a Hradecký kraj (VYDIS a IREDO)

7.8.1 VYDIS a nový IDS Pardubického kraje

V současné době existuje v Pardubickém kraji pouze systém VYDIS – Východočeský Dopravní Integrovaný Systém, který zahrnuje železniční dopravu od Chvaletic po Holice, resp. do Chrudimi, a také na trati Pardubice-Hradec Králové-Jaroměř, včetně městské dopravy v obou krajských městech. Tento systém nevyužívá žádný typ čipových karet. V současnosti se pracuje na novém IDS, který by měl obsahovat kromě železniční a městské dopravy i linkovou autobusovou dopravu. Koordinátorem projektu je oddělení dopravní obslužnosti Odboru dopravy a silničního hospodářství Krajského úřadu Pardubického kraje. S novým systémem se očekává i nový, vhodně zvolený tarifní systém a použitelnost jednoho dokladu během celé přepravy zákazníka. Počítá se i s jistým „průnikem“ okolních integrovaných systémů – jak Královéhradeckého kraje (IREDO), tak i Jihomoravského kraje (IDS MK) do kraje Pardubického a naopak.

Pokud by zavedení IDS Pardubického kraje trvalo nepřiměřeně dlouhou dobu, je možná alternativa, kdy dojde ke spolupráci mezi DPmP a.s., Connex Východní Čechy a.s. a ČSAD Ústí nad Orlicí, jakožto mezi největšími dopravci v Pardubickém kraji. Každý z těchto dopravců používá svůj systém, všechny však pracují se standardem Mifare, proto není problém zajistit vzájemnou akceptaci bez nutnosti sdělování vlastních bezpečnostních klíčů. Spojením těchto tří subjektů by došlo k nárůstu používaných bezkontaktních čipových karet v Pardubickém kraji na necelých 180 000 (DPmP má v květnu 2007 vydáno 50 000 bezkontaktních čipových karet). Stranou zůstávají České Dráhy, které však prozatím s těmito zmíněnými dopravci nemají tendenci spolupracovat – zaprvé proto, že mají systém čipových karet na bázi Mifare DESFire a zadruhé protože nesouhlasí s rozdělováním vybraných financí za přepravu podle skutečně ujeté vzdáleností daným dopravcem – České dráhy v tuto chvíli nemají systém check-in – check-out, tedy systém přihlášení při vstupu do vozidla a odhlášení při výstupu (tímto systémem je velmi přesně měřitelný pohyb osob u daného dopravce). České dráhy preferují poměrný (matematický) systém přerozdělování vybraných finančních částek podle předem daného poměru, který je ovšem nevýhodný pro zbylé tři majoritní dopravce v Pardubickém kraji.

Jak již bylo zmíněno v kapitole 5.4, od 1. června 2007 bylo zavedeno vzájemné uznávání čipových karet v Pardubicích a Hradci Králové, které je, díky téměř totožným systémům odbavování cestujících, možné provozovat nezávisle na IDS.

7.8.2 IREDO – Královéhradecký kraj

Integrovaný dopravní systém IREDO je provozován v Královéhradeckém kraji, ve dvou oblastech, přičemž obě jsou napojeny železnicí až do Hradce Králové:

- Náchodsko – zahrnující okolí Broumova, Police, Hronova, Náchoda, Červeného Kostelce, České Skalice a Trutnova.
- Rychnovsko – zahrnující okolí Rychnova nad Kněžnou, Kostelce nad Orlicí, Dobrušky a Žamberka.

Do IDS IREDO je zapojena veřejná linková autobusová doprava a železniční doprava uvedených regionů v plné dopravní a tarifní integraci v systému řízeném organizátorem, kterým je královéhradecká společnost OREDO, s.r.o., zastupující v oblasti zajišťování dopravní obslužnosti Královéhradecký kraj. U vybraných dopravců je možno použít k platbě jízdného čipovou kartu dle zásad vyhlášených jejím vydavatelem.

Přímo v Hradci Králové provozuje systém čipových karet Dopravní podnik města Hradce Králové. Celý systém pochází od firmy EM TEST ČR spol. s r.o. a je téměř totožný se systémem DPmP a.s., který je popsán v kapitole 6. I zde se uvažuje o zpřístupnění karty pro širší využití v rámci města či regionu.

Další významnou společností v regionu je OSNADO spol. s r.o. (bývalá ČSAD Trutnov), sídlící ve Svobodě nad Úpou a obsluhující hlavně severní oblast Královéhradeckého kraje. Vedle pravidelné linkové dopravy zajišťuje tato společnost i městskou hromadnou dopravu v Trutnově a Dvoře Králové. Ve všech případech používá tento dopravce zařízení od společnosti EM TEST ČR spol. s r.o. a emitované karty jsou Mifare Standard 4k, tedy opět se jedná o systém používaný DPmP, a.s., popsaný v kapitole 6. V této době se připravuje zapojení do clearingu, který funguje v Libereckém kraji (ČSAD Semily, ČSAD Liberec, ČSAD Jablonec nad Nisou a další). Čipové karty OSNADO používají v několika mutacích v podobě ISIC/ITIC některé střední školy i ve vlastních docházkových a přístupových systémech, či systémech ke stravování ve škole. V případě placení čipovou kartou (elektronickou peněženkou) na linkových tratích je poskytována sleva v podobě 5 % z ceny jízdného. Na nepřenosnou dopravní kartu lze také nadefinovat až osm pravidelných úseků volby uživatele (tzv. komerční úseky). Tyto úseky je možno nadefinovat jak v předprodejním místě, tak i přímo ve vozidle u řidiče a dále je využívat pro různé slevové akce. Do budoucna se s touto čipovou kartou počítá v rámci celého IDS Královéhradeckého kraje.

7.9 Jihomoravský kraj (IDS JM)

V jihomoravském kraji se žádné čipové karty nevyužívají z důvodu neexistence jednotného, standardizovaného, celostátně uznávaného a především funkčního systému čipových karet. Pouze zde dožívají systémy, které si zavedlo několik dopravců před integrací. Obvykle se jedná o systém Mifare Standard a zařízení pocházející od firmy Mikroelektronika spol. s r.o. Tyto čipové karty je možné použít pouze u dopravce, který je vydal, případně u dalších, se kterými má uzavřené smlouvy o uznávání karet. V některých případech (Hodonín, Břeclav, Blansko) lze kartu použít jako elektronickou peněženku na území města. Koordinátor kraje (KORDIS JMK, spol. s r. o.) se ale tyto systémy snaží utlumovat. Z uvedených důvodů se na používané karty nevztahují žádné slevy na jízdném ani další výhody. Myšlenkou čipových karet se začne IDS JM zabývat až budou splněny podmínky standardizovaného funkčního systému.

7.10 Olomoucký kraj (IDSOK)

Integrovaný dopravní systém Olomouckého kraje zatím čipové karty v masivnějším měřítku nevyužívá. V autobusové dopravě je odbavování cestujících zajišťováno technikou Mifare od dodavatele Mikroelektronika spol. s r.o. V současné době běží u dopravce Connex Morava, a. s. zkušební provoz užití čipových karet pro zaměstnance. Výhledově by s ohledem na budovaný IDSOK připadalo v úvahu vytvoření "Karty Olomouckého kraje" pro potřeby odbavování cestujících. Veřejnosti byl systém jízdních výhod nabídnut již se vznikem IDSOK a celá problematika aplikace čipových karet se tím stala složitější.

7.11 Zlínský kraj (ZID)

Zlínská integrovaná doprava je zatím ve fázi dokončování. Hlavní dopravní společnost tohoto regionu, Zlín-Otrokovice, s.r.o., nevyužívá v současné době žádný typ odbavení cestujících čipovou kartou. O zavedení systému však uvažují a již byla dvakrát vypsána výběrová řízení, která byla ale zrušena kvůli neschopnosti uchazečů splnit požadovanou míru na kompatibilitu systému v rámci budovaného IDS. Do budoucna je plánován odbavovací systém minimálně na úrovni Mifare Standard 4k, v lepším případě rovnou Mifare DESFire, který využívají České Dráhy, a.s. ve své "IN" kartě (viz dále).

Odbavovací systém firmy EM TEST ČR spol. s r.o. a čipové karty Mifare Standard 1k. Používají v tomto kraji následující dopravci:

- ČSAD Vsetín
- ČSAD Uherské Hradiště
- Krodos Uherské Hradiště
- HousaCar Zlín

Connex Morava používá, stejně jako v jiných krajích ČR, kde Connex působí, odbavovací systém firmy Mikroelektronika spol. s r.o. a čipové karty Mifare Standard 4k

Z krajského úřadu, resp. koordinátora IDS, je kladen velký důraz na uznávání již vydaných a nově emitovaných karet navzájem mezi dopravci, stejně jako přidávání aplikací jednoho dopravce na již emitované karty ostatních dopravců (model „jeden cestující = jedna čipová karta).

7.12 Moravskoslezský kraj (ODIS)

Ostravský dopravní integrovaný systém v současné době čipové karty nevyužívá, ve fázi příprav je však několik variant. Jednotná čipová karta se nejpravděpodobněji bude nazývat MSKarta – Moravskoslezská regionální karta. Jednotliví dopravci v Moravskoslezském kraji (ČSAD Karviná, Havířov, Frýdek-Místek, BUS Slezsko,TQM Opava a Městský dopravní podnik) používají čipové karty Mifare Standard 1k dodané společností EM TEST ČR spol. s r.o. a společnost Connex Morava má připravenu technologii na výdej čipových karet Mifare DESFire. Identickou technologii využívají České dráhy. Objem čipových karet využívaných v regionu je zhruba 200 tisíc kusů. K vzájemnému uznávání karet dochází u ČSAD Havířov, ČSAD Karviná a ČSAD Frýdek Místek a dále ve skupině TQM a Městském dopravním podniku Opava. [14]

7.13 Ústecký kraj

Společnost IDS Ústeckého kraje, a.s. založil v roce 2003 Ústecký kraj jako koordinátora dopravní obslužnosti a integrovaného dopravního systému veřejné osobní dopravy Ústeckého kraje. I když v tomto kraji integrovaná doprava dosud není, existují její předpoklady v oblasti Chomutovska, Mostecka, Teplicka, Ústecka a Děčínska, které jsou intenzivně obsluhovány městskými dopravními systémy a propojeny páteřními železničními tratěmi. V tuto chvíli používají dopravci v kraji různé typy karet a každý má svůj systém, který si navzájem neakceptují.

Dopravní Podnik Teplice, s.r.o. používá čipové karty Mifare Standard a odbavovací systém dodaný společností EM TEST ČR spol. s r.o. Dopravní podnik města Děčína, a.s. používá kontaktní čipové karty pracující na zařízeních od firmy Mikroelektronika spol. s r.o. Jak již bylo uvedeno, i tento systém je platný pouze pro město Děčín v městské autobusové dopravě a v linkové dopravě v oblastech Děčín východ a Děčín západ. Jelikož tento typ kontaktní karty neumožňuje z kapacitního důvodu nést v sobě další informaci, není možné jej využívat pro další aktivity kromě jízdného. V horizontu pěti let DPmD, a.s. však neplánuje obnovu svého systému, protože přesto, že obnova odbavovacího zařízení proběhla v roce 2004, karty zůstaly cestujícím původní z roku 1997. Dopravní Podnik měst Mostu a Litvínova, a.s. pro odbavení cestujících používá čipové karty Mifare Standard 4K. Systém je dodaný firmou Mikroelektronika spol. s r.o.

7.14 Kraj Vysočina

V kraji Vysočina v této chvíli neexistuje žádný integrovaný dopravní systém. Krajský úřad zatím analyzuje možnosti a zkušenosti k jeho zavedení s pomocí jihomoravského organizátora, firmou Kordis, a s východočeským organizátorem OREDO. Na vysočině totiž neexistuje jedno velké spádové centrum, jako v jiných krajích (Plzeň, Brno, Pardubice atd.), ale takových center je v kraji Vysočina pět – Jihlava, Třebíč, Žďár nad Sázavou, Havlíčkův Brod a Pelhřimov. Všechna města jsou od sebe poměrně dost vzdálena a každé tvoří jakousi přirozenou spádovou oblast. Propojit tato města integrovaným dopravním systémem proto není jednoduché. Krajský úřad předpokládá, že IDS by začal fungovat nejprve v jednom okrese, nejpravděpodobněji ve Žďáru nad Sázavou, ostatní místa by se postupně připojila. Nádraží ČD ve Žďáru nad Sázavou má optimální polohu, neboť na něj přímo navazuje tamější terminál veřejné linkové i městské autobusové dopravy. Studie, která ve Žďáru nad Sázavou proběhla, ukázala, že zavedení IDS by tomuto regionu prospělo. Krajské město Jihlava má poněkud komplikovanou dopravní situaci, protože hlavní nádraží je od autobusového vzdáleno přes deset minut pěší chůze [15]. Co se týká čipových karet, používaných v tomto regionu, jednotlivý dopravci používají své systémy, nejčastěji dodané opět firmami Mikroelektronika spol. s r.o. nebo EM TEST ČR spol. s r.o., použité čipy jsou nejčastěji Mifare Standard 1k a 4k.

7.15 České Dráhy – In-karta

České dráhy poprvé uvažovaly o zavedení karetního programu již v roce 2002, projekt Národní dopravní karty se začal realizovat od roku 2004 pod názvem In-karta. Ukázka této karty je na obrázku 35. Na rozdíl od ostatních operátorů, kteří zpravidla poptávají dodávku komplexního systému s čipovými kartami, doplňuje projekt čipové In-karty Českých drah nový on-line odbavovací systém PARIS založený na webových službách. In-karta splní tři základní úkoly:

- Nabídne systém obchodních nabídek ČD v nové elektronické podobě – např. digitální forma kilometrické banky nebo předplatních jízdenek.
- Systém umožní poskytovat klientům další služby a výhody – např. věrnostní program.
- Přispěje ke získání přesnějších statistických údajů o přepravě cestujících.

In-karta se využívá i jako elektronická jízdenka a peněženka vhodné pro rychlou úhradu drobných plateb při cestách na kratší vzdálenosti, kde dosavadní bankovní karetní systémy nejsou dostatečně efektivní a pružné. Postupně dochází k začleňování této karty do jednotlivých integrovaných dopravních systémů. Jako elektronickou peněženku ji lze využít k placení ve vybraných obchodech. Zároveň lze pomocí této karty uskutečňovat některé operace prostřednictvím Internetu – nákup jízdenek, rezervace atp.

Pro realizaci projektu In-karty Českých drah byla zvolena technologická platforma Mifare DESFire, která umožňuje jak integraci již existujících systémů bezkontaktních čipových karet, tak i další rozvoj multifunkčních inteligentních kartových systémů pro použití ve veřejné dopravě, pro řízení přístupů a docházky, pro osobní identifikaci či pro elektronickou peněženku [16]. Nevýhodou je neexistence systému check-in – check-out (viz kapitola 7.8.1).

Obr. 35: Čipová In-karta Českých drah [16]

7.16 Connex

Společnost Connex je součástí nadnárodní akciové společnosti Veolia Environnement, resp. její dopravní odnože Veolia Transport. V České republice má celkem již devět dceřiných společností, které jsou uvedené v následujícím seznamu [17]:

- Connex Morava a.s.
- Železnice Desná
- Connex Východní Čechy a.s.
- Connex Praha s.r.o.
- BUS Slezsko s.r.o
- Connex Příbram s.r.o.
- MAD Kolín s.r.o.
- Connex Česká Železniční s.r.o
- DOPRAVNÍ PODNIK TEPLICE, s.r.o.

Hlavní činností je linková autobusová doprava (provozuje přes 600 pravidelných příměstských a městských linek), vedle ní pak provozuje i železniční dopravu (dvě železniční tratě se sedmi vlakovými soupravami). Jednotlivé části Connexu používají převážně systém čipových karet od společnosti Mikroelektronika spol. s r.o. a karty typu Mifare Standard 1k, některé v tuto chvíli přecházejí na Mifare Standard 4k.

8 Návrhy využití Pardubické karty v rámci UPa

8.1 Aktuální stav na Univerzitě Pardubice

Univerzita Pardubice v tuto chvíli využívá čipové karty dodané firmou Elatec s čipem H4102 s obchodním názvem UNIQUE. Jde o R/O (read only) čip s jedinečným 64 b kódem vyráběný firmou EM-Microelectronic. Tento čip nese informaci o délce 64 b, z čehož je 9 b hlavička (synchronizační bity), dále 40 datových bitů v Manchester kódu, 14 paritních bitů a 1 stop bit. Informace je vložena do čipu laserem při výrobě a výrobce garantuje, že nevyrobí dva čipy se shodným kódem. Rezonanční frekvence čipu je 125 kHz a přenosová rychlost se pohybuje kolem 50 kBd. Čip je zabudován do bezkontaktní plastové karty o velikosti platební karty dle ISO 7816-1.

Tento typ karet může být vybaven i magnetickým proužkem, Univerzita Pardubice však používá pouze karty s čipem. Čip je napájen z elektromagnetického pole čtečky, proto nevyžaduje vlastní zdroj napájení a čtecí vzdálenost je maximálně 10 až 15 cm. [18]

Vzhledem k tomu, že se stále více rozšiřují systémy bezkontaktního odbavování a placení v dopravních systémech, městech i krajích, je vhodné integrovat více služeb do jednoho média – v tomto případě bezkontaktní čipové karty. Proto je vhodné uvažovat o zakomponování Pardubické karty do univerzitního systému. Jelikož jsou ale oba tyto systémy navzájem nekompatibilní, bylo by potřeba provést na univerzitě určité změny, vedoucí k symbióze obou systémů. Nekompatibilita obou systémů je dána tím, že karta Univerzity Pardubice v sobě nese pouze číselný údaj, který je jednoznačně spjatý s konkrétní osobou, a veškeré další operace jsou provozovány na serverech univerzity. Do karty UPa tedy není možné uložit žádné jiné informace.

8.2 Možnosti rozšíření univerzitního systému

Jak již bylo uvedeno v kapitole 5.4, chystá se DPmP a.s. ve spolupráci s dalšími subjekty rozšířit působnost karty i mimo dopravu. Pardubická karta se tedy stane multifunkční čipovou kartou, kterou bude možné využívat jako platební a zároveň jako identifikační kartu. Z toho plynou výhody jak pro uživatele i poskytovatele služeb, tak i pro město a Pardubický region. Tyto výhody, rozdělené v následujícím seznamu do tří částí, lze samozřejmě převést i na univerzitní prostředí.

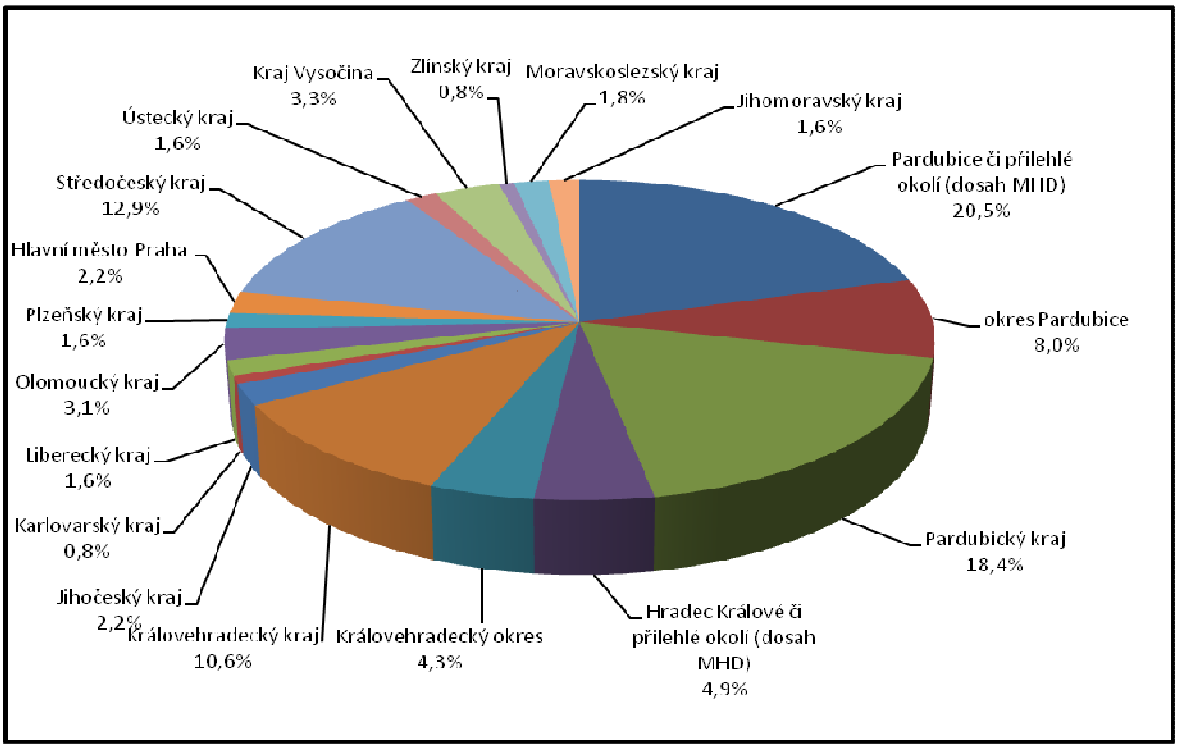
- Výhody pro uživatele:
  - bezhotovostní placení,
  - univerzální karta pro více služeb,
  - možnost využívání výhod a slev při používání karty,
  - zvýhodnění majitelů karet,
  - rychlejší a levnější platební styk v menších částkách.
- Výhody pro poskytovatele služeb:
  - jednoduché a pohodlné poskytování služeb,
  - omezení manipulace s hotovostí,
  - možnost samoobslužných plateb,
  - možnost přímého marketingu, průzkumů apod.,
  - regionální provázání se zákazníky,
  - systém výhod, výher atd. pro majitele karty.
- Výhody pro město/region:
  - zvýšení prestiže města,
  - vyšší ztotožnění občanů s městem/regionem,
  - speciální akce města/regionu,
  - propagace města/regionu,
  - sjednocení služeb.

V univerzitním prostředí by se Pardubická karta dala využít v několika oblastech, které jsou uvedeny v následujícím přehledu:

- studentská (zaměstnanecká) karta:
  - identifikace studenta/zaměstnance,
  - přístup do učeben,
  - přístup na koleje,
  - přístup do knihovny,
  - rezervace a vypůjčování titulů v knihovně,
  - rezervace jídel v menze,
  - rozesílání informací určitým skupinám uživatelů,
- ISIC/ITIC karta:
- elektronická peněženka k placení služeb,
  - platby za služby školy,
  - platby v menze,
  - platby v knihovně (pokuty),
  - platby na kolejích,
- elektronická peněženka k placení doplňkových služeb na univerzitě:
  - automaty na kávu, občerstvení, apod.,
  - prodejny občerstvení,
  - telefonní automaty.

8.3 Průzkum na Univerzitě Pardubice

V průběhu března a dubna 2007 byl proveden dotazníkový průzkum mezi studenty a zaměstnanci Univerzity Pardubice, který si kladl za cíl zodpovědět otázku, zda by byl zájem o použití Pardubické karty na univerzitě, případně jaké služby by byly preferovány. Jeden z vyplněných dotazníků je uveden v příloze D. Dotazník byl rozšířen mezi studenty a zaměstnance Univerzity Pardubice jak v elektronické podobě, tak v podobě tištěné. Byla snaha zasáhnout všechny fakulty a ústavy Univerzity Pardubice, což se povedlo s výjimkou Fakulty restaurování, která sídlí v Litomyšli a je tedy mimo sledovaný záměr, a Fakulty zdravotnických studií, ze které se nevrátil ani jeden dotazník. Největší poměrný počet respondentů byl z Filozofické fakulty, následovaný Ústavem elektrotechniky a informatiky a Dopravní fakultou Jana Pernera.

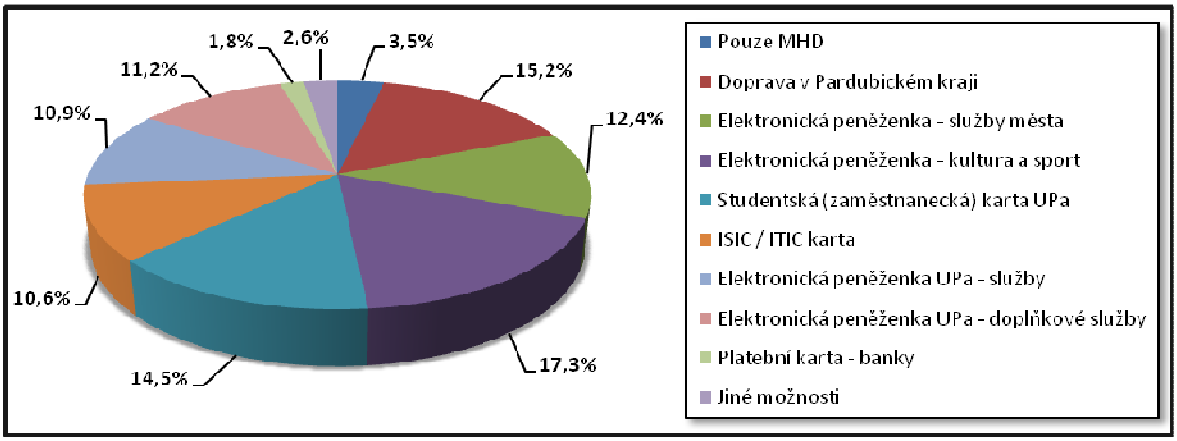


Obr. 36: Původ respondentů

Z celkového počtu 511 dotazníků byl poměr zaměstnanců a studentů 17 % ku 83 %. Graf na obrázku 36 ukazuje poměrné zastoupení oblastí, kde bydlí jednotliví respondenti. Z hlediska věkové struktury respondentů jich nejvíce, tedy 69 %, je ze skupiny 20-23 let, 10 % je mladších 20 let, 12 % respondentů spadá do věkové skupiny 24-26 let a zbylých 10 % je starších než 26 let.

Lehce přes 90 % dotazovaných projekt Pardubické karty zná. Přes 50 % respondentů by uvítalo širší využití Pardubické karty, necelých 16 % potom nevidí potřebu kartu rozšiřovat do jiných oblastí než je MHD a zhruba 25 % dotazovaných kartu nemá a ani neuvažuje o jejím pořízení i v případě rozšíření její působnosti mimo oblast MHD. Graf na obrázku 37 představuje jednotlivé možnosti využití Pardubické karty mimo oblast MHD včetně procentuálního zastoupení, co by respondenti preferovali. V dotazníku bylo možné zaškrtnout více možností, proto je velikost vzorku dat tohoto grafu 1781. Jednotlivé oblasti grafu představují možnosti využití Pardubické karty, uvedené v následujícím seznamu:

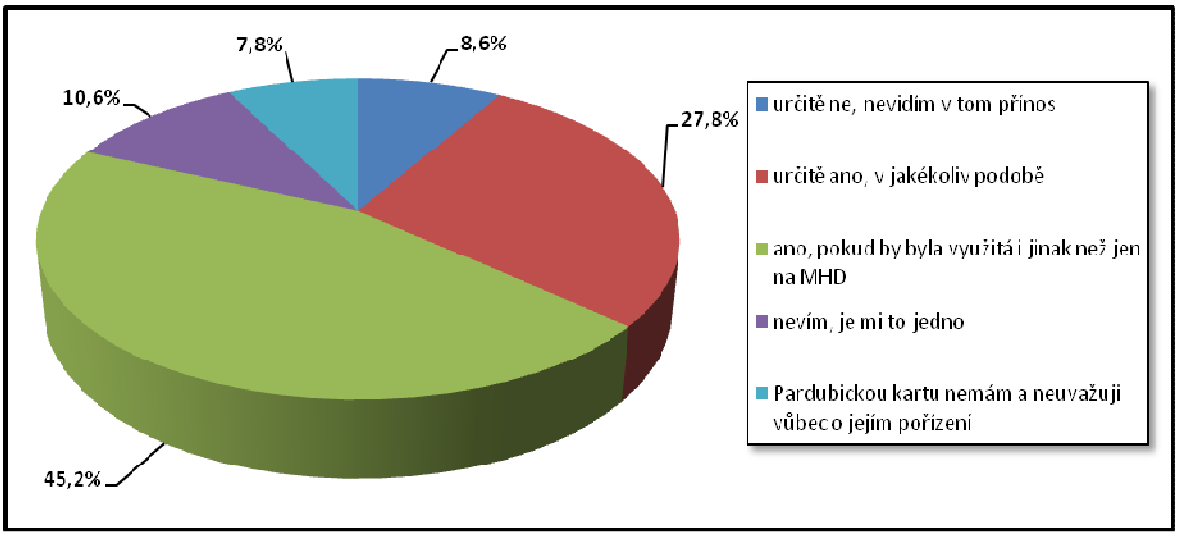
- pouze MHD – 3,5 %,
- doprava v rámci Pardubického kraje – 15,5 %,
- elektronická peněženka k placení služeb města (parkovné, pokuty městské policie, půjčovna bicyklů, přístup k informačním systémům města/regionu apod.) – 12,4 %,
- elektronická peněženka k rezervování a placení vstupenek do kulturních, sportovních a zábavních zařízení (divadla, kina, ČEZ aréna, tenis, bowling, squash, závodiště, plavecký areál, atd.) – 17,3 %,
- studentská (zaměstnanecká) karta (identifikace studenta/zaměstnance – přístup do učeben, přístup na koleje, knihovna, rezervace do menzy, apod.) – 14,5 %,
- ISIC/ITIC karta – 10,6 %,
- elektronická peněženka k placení služeb na území školy (služby školy, jídla v menze, platby v knihovně (pokuty apod.), platby na kolejích) – 10,9 %,
- elektronická peněženka k placení doplňkových služeb na Univerzitě (automaty na kávu, občerstvení, bagety, jídlo, bufet, apod.) – 11,2 %,
- klasická platební karta (MasterCard, Maestro, Visa, Visa Elektron) vybraných bank (KB, ČS, ČSOB, GE, E-banka, atd.) – 1,8 %,
- jiný způsob využití – zde mohli uživatelé uvádět své návrhy – vyskytly se zde pouze tři typy dalšího využití – 2,6 %:
  - krajská knihovna – tuto volbu uvedlo 14 respondentů,
  - MHD Hradec Králové – 31 respondentů,
  - otvírání lahvových piv – 1 osoba.



Obr. 37: Preferované možnosti využití Pardubické karty v jiných oblastech

Na otázku číslo 4 odpovědělo 56 % dotazovaných, že stávající univerzitní kartový systém považují za dostačující, 21 % za velmi dobrý, 19 % by uvítalo nějakou změnu a pouze 4 % respondentů ho považuje za nedostačující. Graf na obrázku 38 pak uvádí postoj dotazovaných k integraci karet, kdy by došlo ke sloučení studentské/zaměstnanecké a Pardubické karty tak, že by ve finále existovala pouze jedna univerzální karta „na všechno“. Z něj je patrné, že převážná většina, přes

72 %, dotazovaných by tento způsob integrace uvítala, pouze 17 % je proti podobné integraci a skoro 11 % dotazovaných není rozhodnutých, zda by bylo lepší mít jednu kartu nebo nechat stávající systém.



Obr. 38: Spojení studentské a Pardubické karty do jedné univerzální čipové karty

8.4 Závěry průzkumu

Většina dotazovaných by uvítala rozšíření stávající studentské karty o další možnosti, jako je například bezhotovostní placení. Tato změna by si vyžádala větší zásah do stávajícího univerzitního systému čipových karet. Vzhledem k tomu, že DPmP a.s. má vydaných již přes 50 000 karet, v kombinaci s DPmHK a.s. přes 110 000 a po připojení společností Connex Východní Čechy a.s. a ČSAD Ústí nad Orlicí se bude počet vydaných karet blížit hodnotě 250 000, nehodlá ustupovat Univerzitě Pardubice v otázce změny či přizpůsobení svých zařízení a systému univerzitním potřebám, proto by veškeré změny byly nutné provádět pouze na UPa s ohledem na kompatibilitu s výše uvedenými společnostmi. Výhodou je, že systém Dopravního podniku je nový, proto se neočekává v příštích minimálně 5-10 letech jeho nahrazení. Dle vyjádření DPmP a.s. by mohlo dojít v budoucnu pouze k přechodu z čipových karet typu Mifare Standard 4k na Mifare DESFire, což by znamenalo pouze výměnu čipových karet uživatelů. Stávající čtecí a komunikační zařízení jsou po nahrání novějšího firmware schopny akceptovat karty typu DESFire, proto není nutná jejich výměna.

Vedle výše uvedených faktů je třeba ještě přihlédnout k tomu, že jediným emitentem Pardubické karty je DPmP a.s., čili veškeré operace, týkající se finanční stránky jdou přes jeho zúčtovací centrum. Na jednu stranu to může být výhoda vzhledem k tomu, že pro vedení elektronické peněženky je nutné povolení od ČNB, které by Univerzita nemusela získávat, na druhou stranu by bylo nutné vyřešit podmínky, za kterých by DPmP a.s. finanční stránku univerzitě spravoval.

Další spornou otázkou by mohlo být řešení zabavené karty ze strany jiného subjektu, než je Univerzita Pardubice. Když by došlo k zabavení karty například revizorem Dopravního podniku města Pardubic, jak by se řešila situace, kdy by se student nedostal do učebny, do knihovny, nemohl jít na oběd apod. V rámci Dopravního podniku mají sice tuto situaci vyřešenu, otázkou je, jestli by tento styl byl použitelný i u externích subjektů.

Vedle těchto technických věcí by bylo potřeba vyřešit i design karty – jestli by se karta koncipovala jako oboustranná, kde z jedné strany by byly údaje Dopravního podniku města Pardubic a z druhé strany Univerzity Pardubice, či zda by se hledalo kompromisní řešení. DPmP a.s., Univerzita Pardubice i vydavatel karty ISIC mají své standardy pro grafické ztvárnění karet, proto i tuto fázi by musel předcházet důkladný rozbor možností.

Poslední věcí, která by byla potřeba vyřešit je poskytování osobních údajů dalším subjektům, zapojených do projektu Pardubické karty. Byl by potřeba vybudovat nějaký aparát, který by zajišťoval ochranu osobních údajů pro jednotlivé aplikace v kartě – pokud student/zaměstnanec UPa nedá souhlas jinému subjektu, aby tento nemohl používat jeho osobní údaje, uložené v kartě. Ne všichni uživatelé z řad Univerzity Pardubice by zajisté chtěli využívat Pardubickou kartu například pro sportovní účely, zatímco komerční poskytovatelé služeb, spojených s Pardubickou kartou by mohli posílat své reklamní nabídky všem majitelům Pardubické karty bez výjimky.

Obecně by se dalo doporučit sloučení obou karet, předtím je ale nutné vyřešit mnoho problémů, které byly nastíněny výše. Z důvodu výměny stávajícího systému za nový je velmi vážným problémem i finanční otázka této případné změny. Zároveň si je třeba uvědomit, že nějaký čas by musely fungovat oba systémy souběžně. Z provedeného dotazníkového výzkumu vyplývá, že by převážná většina studentů i zaměstnanců byla pro takovouto změnu. Vedle tohoto systému bezkontaktních čipových karet je ale na zvážení varianta biometrických prvků. Tato technologie je ale stále ve fázi rozvoje a proto není zatím běžně dostupná.

9 Aplikace pro základní komunikaci s kartou

9.1 Použité čtecí zařízení

V této kapitole je čerpáno převážně z [19] a [20], doplněno o vlastní poznatky a zkušenosti. Použitá čtečka je typ ACR38U-SPC[4] Smart Card Reader/Writer od společnosti ACS, Advanced Card Systems Ltd. Jedná se o nenákladné univerzální čtecí/zapisovací zařízení pro komunikaci mezi počítačem a čipovou kartou. Různé typy karet používají různé příkazy a komunikační protokoly, typ ACR38 proto používá jednotné rozhraní od počítače ke kartě pro různé druhy čipových karet. ACR38 se připojuje k počítači pomocí rozhraní USB 2.0, přijímá příkazy z počítače, přenáší specifické funkce na kartu a vrací požadovaná data nebo informace o stavu. Čtečka podporuje typy karet uvedené v následujícím seznamu:

- MCU karty (karty s procesorem):
  - s protokolem T=0 a T=1,
- čipové karty (Memory-based cards) standardu ISO-7816 Class A, B a C (5V, 3V, 1.8V):
  - karty obsahující sběrnici s protokolem I2C,
  - Atmel: AT24C01 / 02 / 04 / 08 / 16 / 32 / 64 / 128 / 256 / 512 / 1024,
  - SGS-Thomson: ST14C02C, ST14C04C,
  - Gemplus: GFM1K, GFM2K, GFM4K, GFM8K,
- SLE4432/4442 intelligent 256 B EEPROM s funkcí ochrany proti zápisu,
- SLE4418/4428 intelligent 1 kB EEPROM s funkcí ochrany proti zápisu,
- secure memory cards – AT88SC153, AT88SC1608,
- SLE4406/4436/5536 '104' type EEPROM SLE4406, SLE4436, SLE5536.

Typické použití tohoto zařízení je pro internetové bankovnictví, nakupování po Internetu, kontrola přístupu k síti, blokování software, digitální podpis, identifikaci, hraní her apod. Čtecí zařízení je znázorněno na obrázku 39.

Obr. 39: Čtecí zařízení ACR38U-SPC včetně testovací karty ACOS2

9.2 Komunikační protokol

Při standardní činnosti funguje ACR38 v podřízeném módu (slave) s ohledem na komunikaci mezi počítačem a čtečkou. Komunikace je zajišťována formou úspěšných výměn dotaz-odpověď. Počítač přenáší příkazy do čtečky a přijímá odpovědi po vykonání daného příkazu. Další příkaz může být přenášen až po přijetí odpovědi na předchozí příkaz. Pouze dva příkazy lze přenášet bez předchozí odpovědi – tzv. Reset Message a Card Status Message, tedy zprávy o obnovení čtečky a stavu karty.

[4] SPC – Space Ship Casing – označení designu čtečky pro klasické čipové karty standardních rozměrů, písmeno U znamená, že se čtečka připojuje přes rozhraní USB

Příkaz pro čtečku

Standardní příkaz posílaný čtečce se skládá ze šesti bytů protokolu a proměnného počtu bytů ve formě čísla a má strukturu v následující tabulce 4.

Tab. 4: Struktura standardního příkazu posílaného čtecímu zařízení

Byte	1	2	3	4	5 …	N+4 (N>0)
	Hlavička	Instrukce	Délka dat = N		Data	
	01_H		Délka dat N			

[19]

- Hlavička (Header) – vždy 01_H – indikuje začátek příkazu.
- Instrukce (Instruction) – kód příkazů, které se posílají do čtečky ACR38.
- Délka dat (Data Length) – počet bytů dat – kódován ve 2 B – první (MSB) a druhý (LSB) byte reprezentují délku dat N.
- Data – data, přenášené příkazem – například u příkazu READ představují data začátek adresy a počet bytů ke čtení. Data mohou být reprezentována hodnotami, které se mají zapsat do karty apod.

Odpověď z čtečky

Odpověď z ACR38 závisí na předchozím příkazu, který byl čtečkou přijat bez chyby. Odpověď se standardně skládá ze tří bytů protokolu, dvou bytů stavu a proměnného počtu bytů. Struktura odpovědi je opět v následující tabulce 5.

Tab. 5: Struktura odpovědi ze čtecího zařízení

Byte	1	2	3	4	5 …	N+4 (N>0)
	Hlavička	Stav	Délka dat = N		Data	
	01_H		Délka dat N			

[19]

- Hlavička a Délka dat jsou totožné jako u příkazu pro čtečku – viz výše.
- Stav (Status) – udává vykonání příkazu – 00_H = zpráva a úspěšném provedení příkazu. Jiné hodnoty znamenají chybu, nebo informaci, že příkaz nemůže být proveden – viz následující tabulka 6.
- Data – data obsažená v příkazu – například pro příkaz READ_DATA obsahují obsah adresy paměti karty, ze které se čte. Data mohou být reprezentována hodnotami, které se čtou z karty a/nebo informacemi o stavu.

Tab. 6: Stavové informace přijímané z čtečky

Kód stavu	Stav
00	OK – příkaz úspěšně proveden
F4	SLOTERROT_PROCEDURE_BYTE_CONFLICT
F6	SLOTERROR_BAD_LENGTH
F7	SLOTERROR_BAD_FIDI
F8	SLOTERROR_BAD_ATR_TS
F9	SLOTERROR_ICC_NOT_POWERED_UP
FA	SLOTERROR_ICC_NOT_INSERTED
FB	SLOTERROR_HW_ERROR
FC	SLOTERROR_XFE_OVERRUN
FD	SLOTERROR_XFE_PARITY_ERROR
FE	SLOTERROR_ICC_MUTE
FF	SLOTERROR_CMD_ABORTED

[19]

Zprávy o stavu karty

Když dojde k zasunutí či vysunutí karty do/z čtečky ve chvíli, kdy je čtečka nečinná (neprovádí se žádný příkaz), čtečka přenese tzv. Card Status Message, tedy zprávu o stavu karty, kterým oznámí počítači změnu stavu vložení. Tato informace je přenesena pouze jednou, když dojde k vložení či vysunutí karty. Čtečka neočekává žádný signál od počítače, po přenesení této informace čtečka dále očekává další příkazy. Tyto zprávy mají strukturu a obsah uvedené v tabulce 7 (vložení karty) a v tabulce 8 (vysunutí karty).

Tab. 7: Vložení karty

Byte	1	2	3	4
	Hlavička	Stav	Délka dat = N	
	01_H	$C1_H$	00_H	00_H

[19]

Tab. 8: Vysunutí karty

Byte	1	2	3	4
	Hlavička	Stav	Délka dat = N	
	01_H	$C0_H$	00_H	00_H

[19]

9.3 Použitá čipová karta

Čipová karta zvolená pro vytvořenou aplikaci – na obrázku 40 – je mikroprocesorová (MCU) karta ACOS2 (ACS Smart Card Operating Systems Version 2) s následujícími vlastnostmi:

- EEPROM pro uživatelská data: 1 kB, 8 kB,
- vyhovuje standardu ISO-7816-1/2/3, T=0,
- DES, 3DES a MAC[5] (Message Authentication Codes) kapacita zajišťuje velmi vysokou míru bezpečnosti uložených dat,
- vzájemná autentifikace[6] (mutual authentication) s náhodným číslem a přiřazeným párovým klíčem,
- pět bezpečnostních kódů, Issuer Code a PIN pro přístup k datům, uložených na kartě a pro provádění příkazů (READ, WRITE atd.),
- emitentem definovaná oblast souborů pro vyhovující a výkonnou správu paměti,
- určená zabezpečená struktura dat pro platební aplikace.

Obr. 40: Použitá čipová karta ACOS2

9.3.1 Životní cyklus čipu

Během celého životního cyklu čipové karty se rozlišují tři fáze a dva různé operační módy – stupeň výroby, stupeň personalizace, uživatelský stupeň a uživatelský stupeň v módu emitenta. Karta je pokaždé v jednom z těchto čtyř stupňů.

[5] Algoritmus pro generování kryptografických kontrolních součtů.
[6] Proces, ve kterém karta a čtecí zařízení ověří pravost svého protějšku.

Stupeň výroby (manufacturing stage)

V této fázi je jakýkoliv zápis do interních datových souborů (internal dala files) či čtení z bezpečnostních souborů podmíněn úspěšných zadání kódu emitenta (Issuer Code – IC). Inicializační IC kód je naprogramován v mikroprocesoru ACOS2 během výroby čipu. Všechny příkazy karty jsou dostupné, ačkoli některé z nich (například autentifikace) nebudou dávat rozumné výsledky, dokud nebudou požadovaná data naprogramována na kartu. Během stupně výroby jsou do EEPROM paměti karty zapsána následující data:

- výrobní soubor – obsahuje dva záznamy, každý o 8 B, tento soubor je zapsán pouze při výrobě, dále slouží pouze ke čtení a obsahuje data, která jsou jedinečná pro každou kartu – sériové číslo karty, identifikaci výrobce apod.,
- IC kód pro personalizační stupeň – IC kód je nezbytný pro povolení zápisu během personalizačního stupně,
- pojistka výrobce – nevratná změna z výrobního stupně na stupeň personalizace, jeden bit v 16 B výrobním souboru.

Stupeň personalizace (personalization stage)

K personalizaci dochází ve chvíli ukončení stupně výroby a trvá, dokud není přiřazen personalizační bit v paměti EEPROM. Jakmile dojde k naprogramování personalizačního bitu a tím k ukončení fáze personalizace, je možné se do ní vrátit znovu v módu emitenta (Issuer Mode) provedením příkazu CLEAR CARD, který fyzicky vymaže EEPROM paměť kromě části, kde jsou informace o výrobci karty a vrátí kartu do stavu před naprogramováním personalizačního bitu. Během stupně personalizace jsou dostupné příkazy pro čtení i zápis jen po správném uvedení IC kódu. Během tohoto stupně jsou do paměti karty zapsána následující položky:

- personalizační soubor obsahuje tři záznamy, každý o velikosti 4 B a obsahuje data unikátní pro každou kartu, jako například identifikace emitenta, kód karty atd., po dokončení této fáze je tento soubor určen pouze ke čtení,
- bezpečnostní (tajné) kódy a klíče,
- definice bloků soborů pro uživatelská data,
- datovou strukturu pro účetní položky,
- personalizační bit – oznámení o změně stavu z personalizačního stupně do stupně uživatelského.

Uživatelský stupeň (user stage)

Tento stupeň určuje normální stav karty. Začíná při ukončení předchozího personalizačního stupně a trvá do chvíle, kdy dojde k uložení kódu emitenta na kartu. Předání kódu emitenta na kartu změní operační mód do módu emitenta. Tento mód umožňuje přístup k určitým částem paměti, která je jinak nepřístupná.

9.3.2 EEPROM paměť – rozdělení

Oblast EEPROM paměti s velikostí 8 kB je rozdělena do dvou základních oblastí – vnitřní paměť a uživatelská paměť. Vnitřní paměť se používá pro ukládání konfigurací a je využívána operačním systémem karty k řízení potřebných funkcí. Uživatelská paměť slouží u ukládání dat různých uživatelských aplikací.

Datové soubory

Přístup do obou výše zmíněných částí paměti v podstatě znamená přístup k datovým souborům a záznamům dat. Datové soubory jsou nejmenší entity, které mohou být přiřazeny k ovládání čtení a zápisu dat uložených v EEPROM paměti a skládají se ze záznamů dat. Záznamy dat jsou nejmenší možné jednotky dat, které mohou být adresované v datovém souboru. Každý soubor dat obsahuje N datových záznamů (maximálně 255). Při operaci se

záznamem (čtení nebo zápis) se musí specifikovat číslo záznamu. Délka záznamu se může lišit pro různé soubory, vždy je ale spjatá s konkrétním souborem.

Struktury souborů interních datových souborů (velikost souboru, identifikátor souboru, délka záznamu, atributy bezpečnosti) jsou definovány operačním systémem a nemohou být měněny. Struktura souboru pro uživatelská data je stanovena v personalizační části karty. Struktura souborů se vytvoří po naprogramování parametru N_OF_FILE v personalizačním stupni. Přístup ke všem souborům je možný pouze pomocí příkazů WRITE a READ. Operační systém neudržuje informace o tom, jaké záznamy jsou zapisovány pomocí příkazu WRITE. Data vrácená z karty jako odpověď na příkaz READ jsou aktuálně čtena z EEPROM paměti bez ohledu na to, zda byla data vůbec zapsána. Každý soubor je identifikován pomocí dvoubytového tzv. souborového identifikátoru (File Identifier), který je přiřazen během definice v personalizačním stupni danému souboru. Operační systém nevykonává revizi jedinečnosti každého souborového identifikátoru. V případě přiřazení již použitého identifikátoru, může dojít k chybné funkci karty. Hodnota FF_H prvního bytu souborového identifikátoru je použita pro interní datové soubory a nemůže být použita pro uživatelské datové soubory. Před příkazy WRITE nebo READ musí být nejprve soubor otevřen pomocí příkazu SELECT FILE. V daném čase může být otevřen pouze jeden soubor.

Kontrola přístupu k datovým souborům

Ke každému datovému souboru jsou přiřazeny dva bezpečnostní atributy. Tyto atributy definují bezpečnostní podmínky, které je nutné splnit, aby byla povolena příslušná operace. Prvním atributem je *bezpečnostní atribut čtení*, který kontroluje přístup při čtení pomocí příkazu READ – pokud není splněn, není možné z datového souboru číst. Druhým atributem je *bezpečnostní atribut zápisu* – tento kontroluje přístup při zápisu pomocí příkazu WRITE, stejně jako u atributu READ. Ani v tomto případě, pokud nedojde ke splnění podmínek, není příkazu WRITE umožněno zapisovat do datového souboru. Tyto atributy určují, jaký aplikační kód (Application Code 1–5), kód emitenta (Issuer Code – IC) či PIN musí být úspěšně odeslán kartě, aby byla povolena požadovaná operace.

Interní datové soubory

Atributy interních datových souborů jsou definovány v operačním systému karty a nemohou být měněny. Bezpečnostní atributy ale závisí na stupni životního cyklu karty. Definice interních datových souborů je v následujícím přehledu v tabulce 9.

Tab. 9: Definice interních datových souborů

		Bezpečnostní atributy souboru			Organizace záznamu
Oblast paměti	**ID interního souboru**	**Výrobní stupeň**	**Personalizační stupeň**	**Uživatelský stupeň**	
MCU-ID soubor	FF 00_H	R: přístupný W: nepřístupný	R: přístupný W: nepřístupný	R: přístupný W: nepřístupný	2x 8 B
Výrobní soubor	FF 01_H	R: přístupný W: IC kód	R: přístupný W: nepřístupný	R: přístupný W: nepřístupný	2x 8 B
Personalizační soubor	FF 02_H	R: přístupný W: IC kód	R: přístupný W: IC kód	R: přístupný W: nepřístupný	3x 4 B
Bezpečnostní soubor	FF 03_H	R: IC kód W: IC kód	R: IC kód W: IC kód	R: nepřístupný W: IC kód	12x 8 B
Uživatelský soubor	FF 04_H	R: přístupný W: IC kód	R: přístupný W: IC kód	R: přístupný W: IC kód	N_OF_FILE x 6 B
Soubor s účtem	FF 05_H	R: přístupný W: IC kód	R: přístupný W: IC kód	R: IC kód W: IC kód	8x 4 B
Bezpečnostní soubor pro účet	FF 06_H	R: přístupný W: IC kód	R: přístupný W: IC kód	R: nepřístupný W: IC	4x 8 B
Oblast souborů pro uživatelská data	ID souborů: xx yy_H xx ≠ FF_H	Závisí na definici souborů			

[20]

Uživatelské datové soubory

Uživatelské datové soubory jsou alokovány a definovány v personalizačním stupni. Data uložená v této oblasti jsou dostupná pro čtení i zápis jen po úspěšném splnění bezpečnostních podmínek. Tyto soubory mohou obsahovat až 255 záznamů, každý o maximální délce 32 B.

Dostupný paměťový prostor pro uživatelské datové soubory závisí na tom, zda je požadována struktura dat pro účet. Pokud je účet požadován, je omezen paměťový prostor uživatelských soborů na 64 nebo 96 B, v závislosti na vybraném šifrování účtu (DES nebo Triple DES). S ohledem na maximální flexibilitu není velikost paměti pro datové uživatelské soubory určena pevně. Velikost uživatelských datových souborů se počítá jako počet záznamů násobený délkou záznamu v B, zaokrouhlený na následující vyšší násobek 4 B. Množství paměťového prostoru obsazeného všemi datovými uživatelskými soubory je součet velikostí individuálních souborů.

Definiční blok uživatelského souboru

Každý uživatelský datový soubor je popsán v asociovaném bloku definičních souborů, které obsahují identifikátor souboru, délku záznamu, délku souboru a bezpečnostní atributy. Každý blok definičního souboru zahrnuje 6 B, které jsou schematicky zobrazené v tabulce 10.

Tab. 10: 6 B definičního bloku

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5 / 6
Délka záznamu	Počet záznamů	Bezpečnostní atribut čtení	Bezpečnostní atribut zápisu	Identifikátor souboru

[20]

Všechny bloky definičních souborů jsou uloženy ve správci uživatelských souborů (User File Management File), po jehož vybrání příkazem SELECT FILE mohou být čteny pomocí READ příkazu. Počet záznamů v tomto správci je dán hodnotou parametru N_OF_FILE.

Alokace uživatelského souboru

Pro alokaci uživatelských datových souborů na nové kartě slouží kroky uvedené v následujícím seznamu. Jak již bylo uvedeno, před těmito kroky musí být kartě poslán IC kód.

1) Příkaz SELECT FILE s identifikátorem souboru ID = FF 02 – slouží k vybrání personalizačního souboru.
2) Zapsání počtu budoucích uživatelských datových souborů – parametr N_OF_FILE – 3 B prvního záznamu personalizačního souboru – alokuje požadovaný prostor ve správci uživatelských souborů (User File Management File).
3) Příkaz SELECT FILE s identifikátorem souboru ID = FF 04 – slouží k vybrání uživatelského souboru správce souborů.
4) Zapsání N_OF_FILE souboru definičních bloků do správce pomocí příkazu WRITE. Zapíše jednou 6 B do každého definičního bloku soboru.
5) Po splnění předchozích čtyř kroků mohou být uživatelské datové soubory vybrány a je možné z nich číst resp. do nich zapisovat.

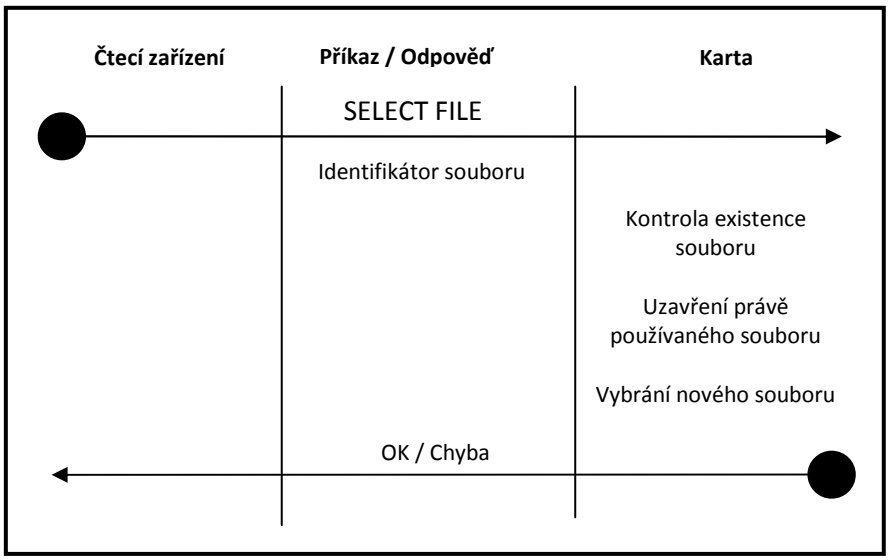
9.3.3 Přístup k datovým souborům

Následující body jsou shodné pro interní datové soubory i pro uživatelské datové soubory.

SELECT FILE

Příkaz SELECT FILE může být použit kdykoliv, kdy je ho potřeba. Specifikovaný soubor – pokud existuje – bude vybrán a předchozí soubor – pokud nějaký byl – bude uzavřen. Pokud požadovaný soubor neexistuje, karta vrátí chybový kód a ke změně souboru nedojde. Bezpečnostní podmínky specifikované pro nově vybraný soubor nejsou při tomto příkazu kontrolovány a vzájemná autentifikace není nutná – nemusí být splněna před provedením

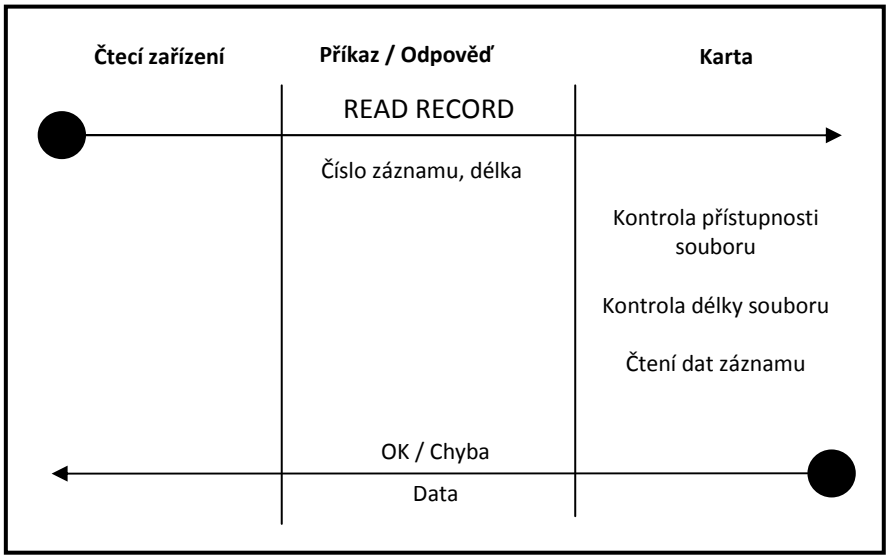
příkazu SELECT FILE. Po resetu karty není vybrán žádný soubor. Příkaz SELECT FILE je znárodněn na schématu na obrázku 41.



Obr. 41: Schéma příkazu SELECT FILE [20]

READ RECORD

Příkaz READ RECORD pro čtení záznamu může být proveden až po příkazu SELECT FILE. Nejprve dojde ke zkontrolování bezpečnostních podmínek a v případě jejich úspěšného splnění dojde k provedení příkazu. Příkaz READ RECORD může číst data jen z jednoho záznamu – počet bytů k přečtení je specifikován ve formátu příkazu. Maximální počet bytů ke čtení je stejný, jako je délka záznamu. Jestliže je počet čtených bytů (N) menší než délka záznamu, karta vrátí prvních N bytů. Schéma příkazu READ RECORD je na následujícím obrázku 42.



Obr. 42: Schéma příkazu READ RECORD [20]

WRITE RECORD

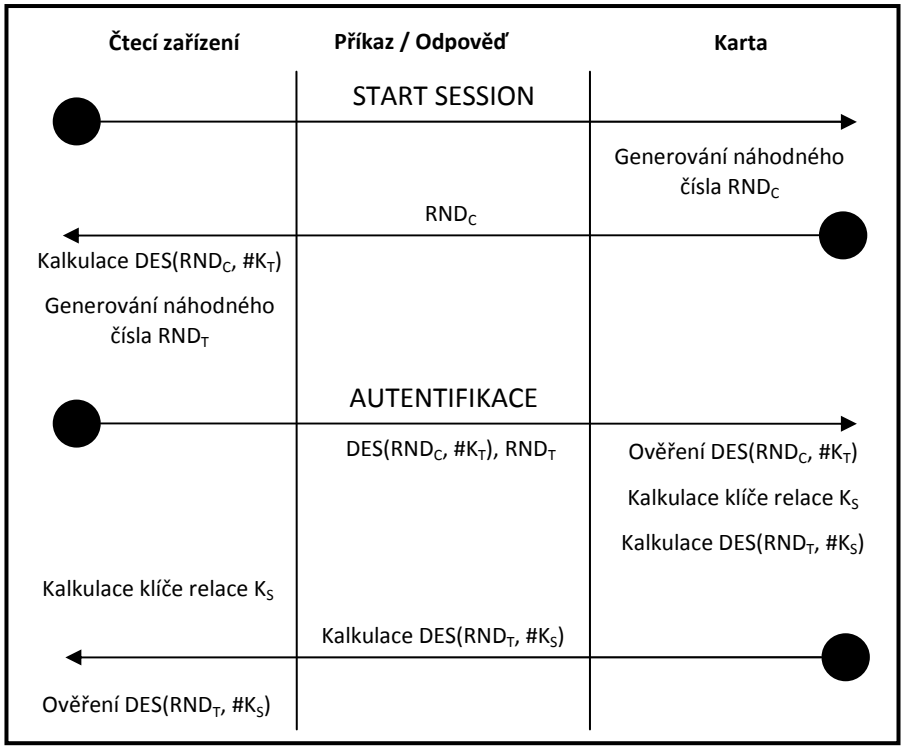
Stejně jako u předchozího příkaz READ, i u tohoto WRITE RECORD je potřeba nejprve provést příkaz SELECT FILE a dodržet bezpečnostní podmínky. Počet bytů k zapsání je specifikován v příkazu. Maximální počet bytů k zapsání je stejný jako délka záznamu. Pokud je počet bytů k zapsání (N) menší než délka záznamu, dojde k přepsání prvních N bytů novými daty. Schéma příkazu WRITE RECORD je téměř totožné s obrázkem 42, jen s rozdílem, že nedochází ke čtení záznamu, ale k jeho zápisu a vedle čísla záznamu není délka, ale zapisovaná data.

9.3.4 Bezpečnost

Operační systém čipové karty ACOS2 poskytuje následující bezpečnostní mechanismy:

- DES a MAC kalkulace,
- vzájemná autentifikace a klíč relace (Session Key) založený na náhodných číslech,
- tajné kódy,
- bezpečné zpracování transakce účtu.

DES, Data Encryption Standard je v podstatě DEA algoritmus (Data Encryption Algorithm) pro šifrování a dešifrování dat, který je specifikován standardem ANSI X3.93. MAC je založen na algoritmu pro generování kryptografických kontrolních součtů a popsán standardem ANSI X3.93. Vzájemná autentifikace je proces, ve kterém karta a čtecí zařízení ověří pravost svého protějšku pomocí tajných klíčů, jejichž výměna je zajištěna bezpečnou cestou s použitím náhodných čísel a DES šifrování. Klíč relace je výsledek úspěšného vykonání vzájemné autentifikace a používá se pro šifrování a dešifrování dat během relace. Relace je definována jako čas mezi úspěšným provedením procedury vzájemné autentifikace a resetováním karty nebo vykonáním nového příkazu START SESSION. Tajné kódy (Secret Codes) a PIN kód jsou používány pro selektivní umožnění přístupu k datům uložených v kartě a vlastnostem a funkcím poskytovaných kartou – například příkazy READ a WRITE. Zpracování transakce účtu poskytuje mechanismus pro bezpečnou a prověřenou manipulaci s daty v datové struktuře účtu, obzvláště v hodnotě zůstatku. Následující schéma na obrázku 43 ukazuje proces vzájemné autentifikace.



Obr. 43: Schéma procesu vzájemné autentifikace [20]

Poznámky ke schématu:

- DES může být 1DES nebo 3DES,
- kalkulace klíče relace K_S záleží na vybraném šifrování,
- RND_C – osmi bytové náhodné číslo generované kartou,
- RND_T – osmi bytové náhodné číslo generované čtecím zařízením,
- K_C – číslo karty,
- K_T – číslo terminálu,
- K_S – číslo relace.

9.3.5 Tajné kódy

Tajné kódy uložené na kartě se používají pro omezení přístupu k uloženým datům v uživatelských datových souborech a k některým příkazům poskytovaných kartou. Tajné kódy musí být předkládány kartě v pořadí, v jakém je schopná číst či zapisovat data z/do uživatelských datových souborů nebo vykonávat některé přednostní příkazy. Jak již bylo uvedeno, karta typu ACOS2 poskytuje následující tajné kódy:

- pět Aplikačních kódů (Application Code – AC),
- jeden kód emitenta (Issuer Code – IC),
- jeden PIN kód.

Aplikační kódy (AC)

Pět aplikačních kódů AC1-AC5 je k dispozici pro řízení přístupu k datům uloženým v datových souborech. Každý aplikační kód má délku 8 B. Volba bitu v bezpečnostním registru v personalizačním souboru specifikuje pro každý kód, zda tento musí být předložen kartě v šifrované či nešifrované podobě s aktuálním klíčem relace.

Kód emitenta (IC)

IC kód je poskytován k řízení přístupu k datovým souborům a přednostním příkazům karty. Jeho délka je 8 B. Stejně jako v předchozím případě, i zde je potřeba specifikovat, zda má být v šifrované či nešifrované podobě.

PIN kód

PIN je využíván k řízení přístupu k datovým souborům, je dlouhý 8 B a kartě je prezentován příkazem SUBMIT CODE. V závislosti na odpovídající volbě bitu PIN_DES v bezpečnostním registru je PIN šifrován algoritmem DES s aktuálním klíčem relace před tím, než je uložen na kartu. PIN kód může být změněn příkazem CHANGE PIN, jestliže je nastavena volba bitu PIN_ALT v registru. V závislosti na použití šifrování DES je nový kód buď zašifrován stejným algoritmem, nebo ponechán nešifrovaný.

9.4 Použité vývojové prostředí

Aplikace s názvem Read-Write-SC (SC je zkratka Smart Card) je vytvořena jako standardní formulářová aplikace operačního systému Windows v jazyku C# v prostředí .NET Framework 2.0. K volbě tohoto jazyka a prostředí přispěly jeho následující vlastnosti:

- prostředí .NET umožňuje vytvářet jakékoliv aplikace pro operační systém Windows,
- C# plně podporuje třídy a objektově orientované programování včetně implementace a dědění, virtuálních funkcí a přetěžování operátorů,
- obsahuje konzistentní a dobře definovanou množinu základních typů,
- automaticky čistí dynamicky přidělovanou paměť pomocí Garbage Collectoru,
- automaticky se používají ukazatele a reference.

Aplikace byla naprogramována pomocí produktu Microsoft Visual C# 2005 Express, která je volně ke stažení z [21]. Při vývoji aplikace bylo čerpáno z vlastních zkušeností, nápovědy Microsoft Visual C# 2005, [22] a [23].

Aplikace je určena pro terminál, reprezentovaný klasickým počítačem PC, a je v ní využívána knihovna *winscard.dll*, která je standardní součástí operačního systému Microsoft Windows a pomocí které dochází ke hardwarové komunikaci mezi kartou, čtecím zařízením a počítačem. Využívá se v ní protokolu APDU – Application Protocol Data Unit, který obsahuje buď příkaz (od čtečky do karty) nebo odpověď (od karty do čtečky). Tento protokol je definován standardem ISO 7816. Karta nikdy není iniciátor komunikace, vždy je pasivní. Čeká na příkaz od terminálu,

jakmile ho dostane, zpracuje ho a odpoví. Příkaz obsahuje položky uvedené v následujícím seznamu [24]:

- příkazové APDU:
  - povinné hlavičky:
  - CLA – Class byte – je používán pro identifikaci aplikace,
  - INS – Instruction byte – tento byte identifikuje instrukční kód,
  - P1-P2 (Parameter bytes) jsou další specifikace APDU příkazu,
  - podmíněné tělo:
    - Lc – udává počet bytů v poli pro data APDU příkazu,
  - pole pro data:
    - Le – udává maximální počet bytů v poli dat v odpovědi,
- APDU odpověď:
  - tělo - pole pro data,
  - povinný dodatek – SW1, SW2 – Status bytes – udávají stav, s jakým proběhl příkaz.

9.5 Rozsah aplikace

Vytvořená aplikace komunikuje pomocí čtečky čipových karet s čipovou kartou standardu ACOS2. V rámci aplikace lze nastavit v uživatelské části karty tři typy podadresářů, se kterými lze potom pracovat – zapisovat od nich zadaná data daného rozsahu a uložená data z nich číst. Karta má kapacitu i pro účetní údaje (viz výše v popisu karty), proto by nebyl problém do aplikace přidat část, která by sloužila jako elektronická peněženka. V podstatě by se jednalo jen o přidání několika metod, které by předávaly potřebná data. V případě peněžních operací by bylo vhodné i zajistit DES nebo 3DES šifrování, které tato karta také podporuje. Samotná aplikace funguje v podstatě jako terminál, který může běžet na počítači, který řídí nějaké zařízení (zámek, odečet z účtu apod.). Pro tuto práci byla vytvořena pouze základní komunikace mezi čtečkou, kartou a počítačem – posílání příkazů na kartu (zápis) a příjem informací z karty (čtení).

9.6 Popis aplikace

Jak již bylo uvedeno, je v aplikaci využívána knihovna systému Windows *winscard.dll*. Ta je potom v aplikaci vyžívána modulem *ModWinsCard.cs*, která byla dodána výrobcem čtecího zařízení a zajišťuje rozhraní mezi samotnou aplikací a hardwarovou komunikací s knihovnou. Jsou v něm definovány typové konstanty, rozsahy paměti, protokoly a prototypy metod, což jsou metody deklarované v externím souboru, v tomto případě právě v knihovně *winscard.dll* – příkladem může být externí metoda sloužící k odpojení karty – metoda má následující podobu[7]:

```
[DllImport("winscard.dll")]
public static extern int SCardDisconnect(int hCard, int Disposition).
```

Vlastní využití tohoto modulu je potom přímo ve zdrojovém kódu formuláře.

Vykonání přenosu

Mezi nejdůležitější metody této aplikace patří metoda

```
VykonejPrenosAPDU(ref APDURec apdu),
```

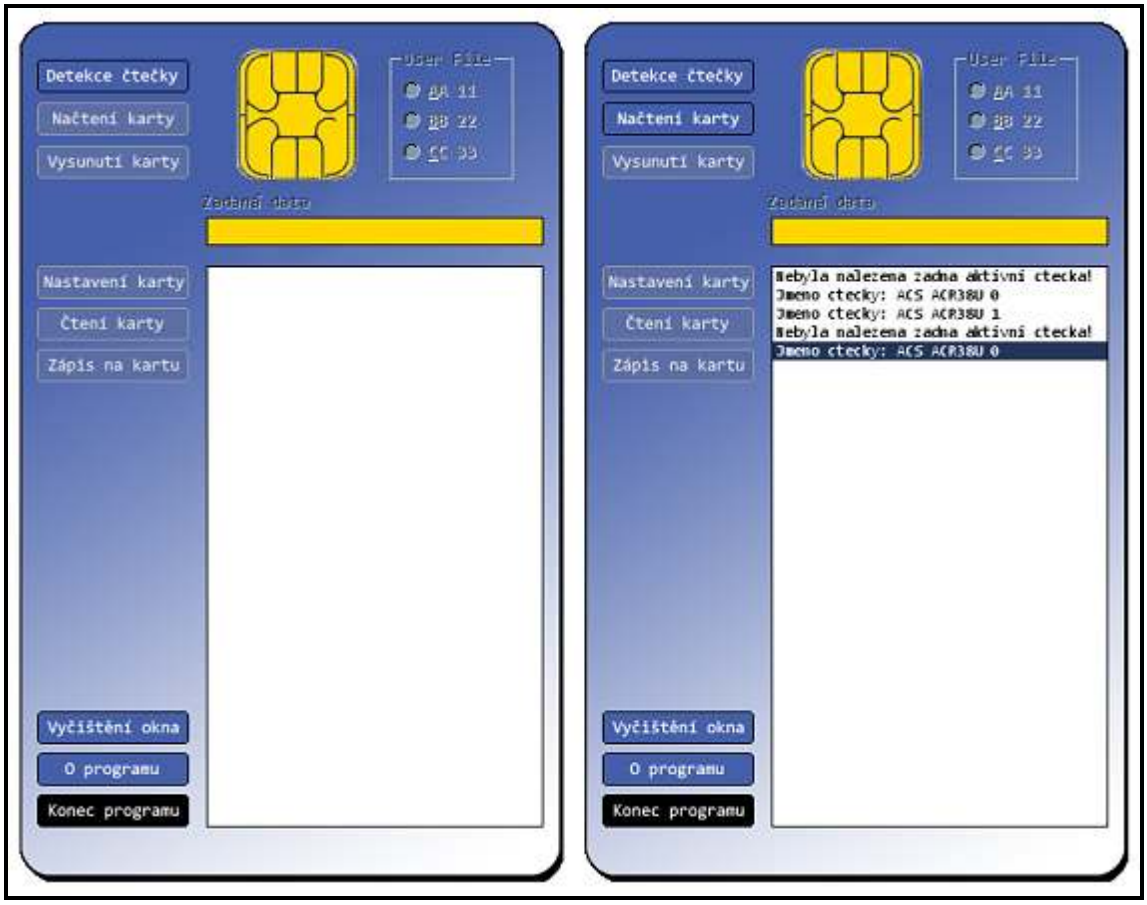
která má jako parametr záznam *apdu*, který obsahuje všechny potřebné části protokolu APDU. Z jejího názvu je patrné, že zajišťuje přenos informací mezi samotnou aplikací a modulem *ModWinsCard.cs* a to pomocí metody `SCardTransmit`, která má parametry *hNactenaKarta, PosliZadost, BufferOdeslany, DelkaBuffOdesl, BufferPrijaty a DelkaBuffPrijat,* ve kterých jsou uloženy potřebné části záznamu *apdu* a pomocí kterých dojde k poslání příkazů kartě. Tato metoda vrací kód čtečky. Pokud je 0, došlo ke správnému navázání spojení, což se ověří pomocí parametru *SCARD_S_SUCCESS* v třídě *ModWinsCard*. Z parametru *DelkaBuffOdesl* je potom zjištěn

[7] Jak bylo uvedeno již na začátku, části textu, převzaté přímo ze zdrojového kódu, jsou uváděny písmem Courier.

kód operace a specifický kód stavu (viz dále u jednotlivých operací). Pro jednodušší orientaci v kódech byla vytvořena metoda `UrciZKoduOperaci(string Kod)`, která převádí číselné kódy do textové podoby. Zmiňované kódy stavů i operací jsou v příloze E – kódy stavů v tabulce 1, kódy operací v tabulce 2.

Detekce čtečky

Po spuštění aplikace dojde k zobrazení formuláře, který je znázorněn na obrázku 44 vlevo. Formulář obsahuje osm tlačítek, z toho po startu jsou aktivní pouze čtyři. Po stisknutí tlačítka „Detekce čtečky“ dojde ke zjištění, zda je k počítači připojena čtečka čipových karet – pokud ano, je do pole s informacemi vypsán název čtečky, pokud ne, je vypsána informace o nenalezení aktivní čtečky. V případě, že je k počítači připojeno více čteček najednou, je jako aktivní rozpoznána ta, která byla připojena dříve. Po odpojení jedné z více čteček dojde k detekování další v pořadí připojení – viz výpisy v informačním okně na obrázku 44 vpravo – nejprve není připojená žádná čtečka, poté je připojena čtečka ACR38U-SPC a vzápětí vedle ní i ACR38T-IBS[8], následně obě odpojeny a opět zapojena pouze ACR38U-SPC. Po úspěšné detekci čtečky dojde k aktivování tlačítka „Načtení karty“.



Obr. 44: Formulář aplikace – vlevo ihned po startu; vpravo po připojení žádné, jedné a dvou čteček

Detekování čtečky je zajištěno zavoláním metody `SCardEstablishContext` z třídy `ModWinsCard`, která zajistí spojení s čtečkou a vrací kód čtečky. Jak již bylo uvedeno v části „Vykonání přenosu“, i zde je tento kód 0, pokud došlo ke správnému navázání spojení, což se opět ověří pomocí parametru *SCARD_S_SUCCESS* v třídě *ModWinsCard*. Následně dojde ke zjištění aktivních čteček připojených k počítači pomocí metody

```
SCardListReaders(this.hSpojeni, tmp,ref SeznamCtecek, ref pcchReaders).
```

[8] ACR38T-IBS čtečka čipových karet velikosti SIM karty, IBS je označení designu čtečky – Ice Bar Casing.

Z jejího parametru `SeznamCtecek` je zjištěn název čtečky (jak již bylo uvedeno, zvolí se první čtečka v seznamu, tedy ta, která byla k počítači připojena dříve). Do informačního okna je pak vypsán chybový stav či jméno čtečky.

Načtení karty

Po úspěšné detekci připojené čtečky a stisku tlačítka „Načíst kartu“ dojde pomocí metody `SCardConnect` k připojení vložené karty, úspěšnost vložení je opět porovnána s parametrem *SCARD_S_SUCCESS*. Uživatel je opět následně informován o úspěšném či neúspěšném načtení karty – viz obrázek 45 vlevo (společně s vysunutím). Po úspěšném načtení karty dojde k aktivování všech ostatních komponent kromě pole pro zadávání dat k zapsání na kartu.

Vysunutí karty

Vysunutí karty je zajištěno operací `SCardDisconnect`, která zajistí korektní odpojení karty ze čtečky včetně přerušení napájení čipu (*SCARD_UNPOWER_CARD*). Toto je zajišťováno třídou *ModWinsCard*, resp. knihovnou *winscard.dll*. Uživatel je informován o úspěšném či neúspěšném odpojení informací v informačním okně – viz obrázek 45 vlevo. Po odpojení karty dojde k deaktivování tlačítek spojených s operacemi na kartě.

Nastavení karty

V tuto chvíli může uživatel na kartě vytvořit tři uživatelské soubory v uživatelské části karty pomocí tlačítka „Nastavení karty“. Pro jednoduchost a názorné ukázání nastavování karty jsou implicitně nastaveny tři soubory s identifikátory *AA 11*, *BB 22* a *CC 33*, první o velikosti 4 B, druhý 8 B a třetí 16 B. V první fázi vytváření uživatelských souborů je potřeba kartě poslat IC kód, jak je uvedeno již v kapitole 9.3.2. K tomu slouží metoda

`DejIssuerCode().`

Pomocí ní je do parametrů záznamu *apdu* přidána požadovaná operace, konkrétně SUBMIT CODE, která má tvar v tabulce 11.

Tab. 11: SUBMIT CODE – složení příkazu

CLA	INS	P1	P2	P3	DATA
80	20	Číslo kódu	00	08	Kód

[20]

Čísla kódu jsou v kartě reprezentována číslicemi 1-5 pro kódy AC1-AC5, 6 pro PIN kód a číslem 7 pro IC kód. Více o těchto kódech je v kapitole 9.3.2 a 9.3.5. Kód je osmibytový kód, který záleží na zvoleném typu (AC, PIN, IC). V této aplikaci je využíván pouze IC kód, na pozici *apdu.P1* je tedy hodnota 07. Jelikož se jedná o testovací kartu, je jejich IC kód nastaven na hodnotu „ACOSTEST“, která je reprezentována následujícími hexadecimálními čísly:

A	***C***	***O***	***S***	***T***	***E***	***S***	***T***
41	43	4F	53	54	45	53	54

Odpověď karty na tento příkaz je ve formě stavových kódů 63 Cn, 69 83 nebo 69 85. Význam kódů je uveden v tabulce v příloze E v tabulce 1.

Záznam *apdu* je potom předán jako parametr metodě `VykonejPrenosAPDU`, jež je popsána výše. Po úspěšném ověření IC kódu dojde k vybrání personalizačního souboru, ve kterém bude možné vytvořit uživatelské soubory – viz kapitola 9.3.2. Vybrání souboru je zajištěno metodou

`VyberSoubor(byte MaxAdresa, byte MinAdresa),`

Její parametry *MaxAdresa* a *MinAdresa* představují požadovanou oblast na kartě, v případě vybírání uživatelského souboru to je FF pro *MaxAdresa* a 02 pro *MinAdresa*. Soubor je vybrán pomocí operace SELECT FILE, který je uveden v tabulce 12.

Tab. 12: SELECT FILE – složení příkazu

CLA	INS	P1	P2	P3	DATA
80	A4	00	00	00	ID souboru

[20]

ID souboru je v tomto případě FF 02. Karta na tento příkaz odpoví stavovými kódy 6A 82 či 91 XX, jejichž význam je uveden v příloze E v tabulce 1. Samotný přenos je opět vykonán metodou `VykonejPrenosAPDU`.

V personalizačním souboru FF 02 je potom alokována oblast dat o požadované velikosti (v tomto případě pro 3 uživatelské soubory). Toto je provedeno metodou

`ZapisZaznam(int caseType, byte CisloZaznamu, byte MaxDelka, byte DelkaDat, ref byte[] ApduIn),`

která využívá operaci WRITE RECORD. Složení příkazu této operace je uvedeno v tabulce 13.

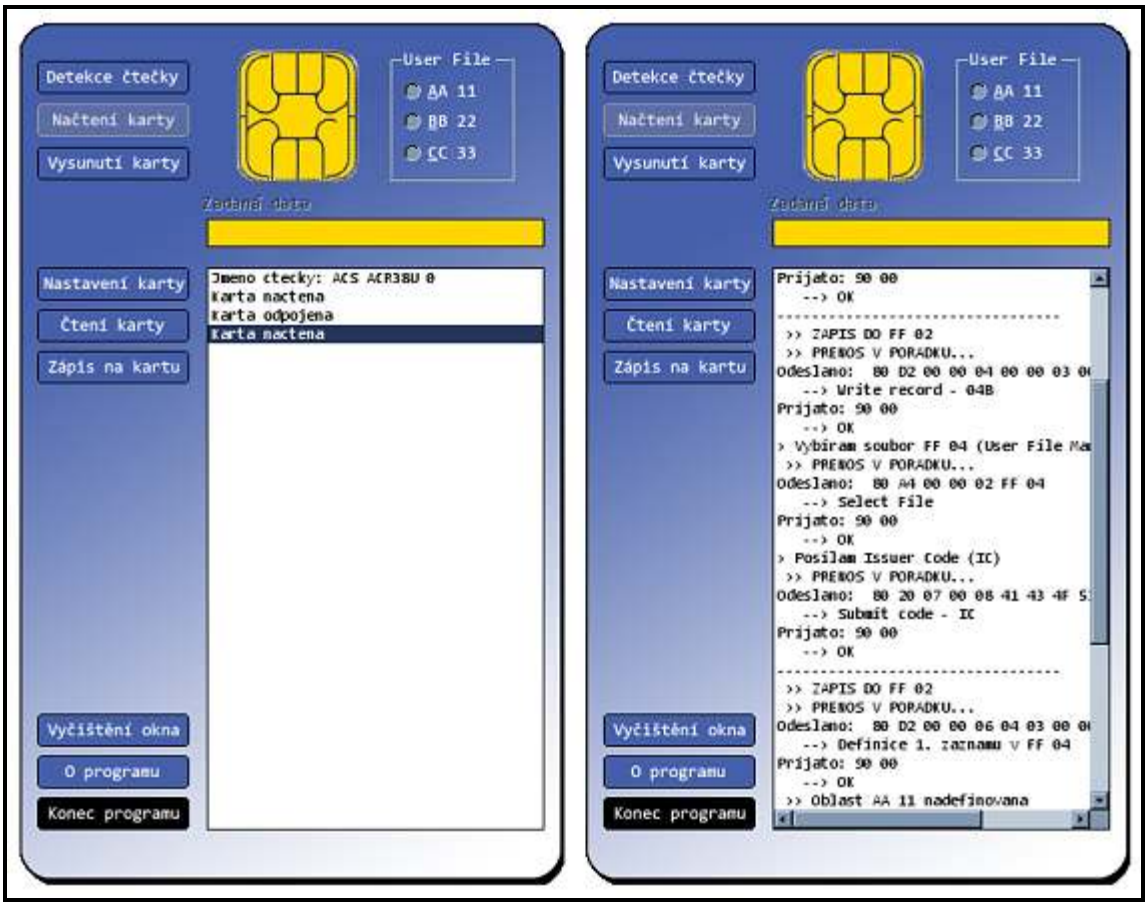
Tab. 13: WRITE RECORD – složení příkazu

CLA	INS	P1	P2	P3	DATA
80	D2	Číslo záznamu	00	Délka	Byte 1 … Byte N

[20]

Číslo záznamu je logické číslo záznamu, který se má číst, *Délka* je počet datových bytů, které se zapíší do záznamu, který je identifikován *Číslem záznamu*. *Byte 1 … Byte N* jsou datové byty, které se uloží do prvního bytu *Délky* záznamu. Odpovědí z karty jsou opět stavové kódy, v tomto případě 69 82, 6A 83, 67 00, 68 85 – viz příloha E – tabulka 1. Přenos je opět vykonán metodou `VykonejPrenosAPDU`.

V personalizačním souboru dojde následně k vybrání správce uživatelských souborů. Postup je stejný jako v případě vybrání personalizačního souboru s rozdílem ID souboru, který je u tohoto typu FF 04.

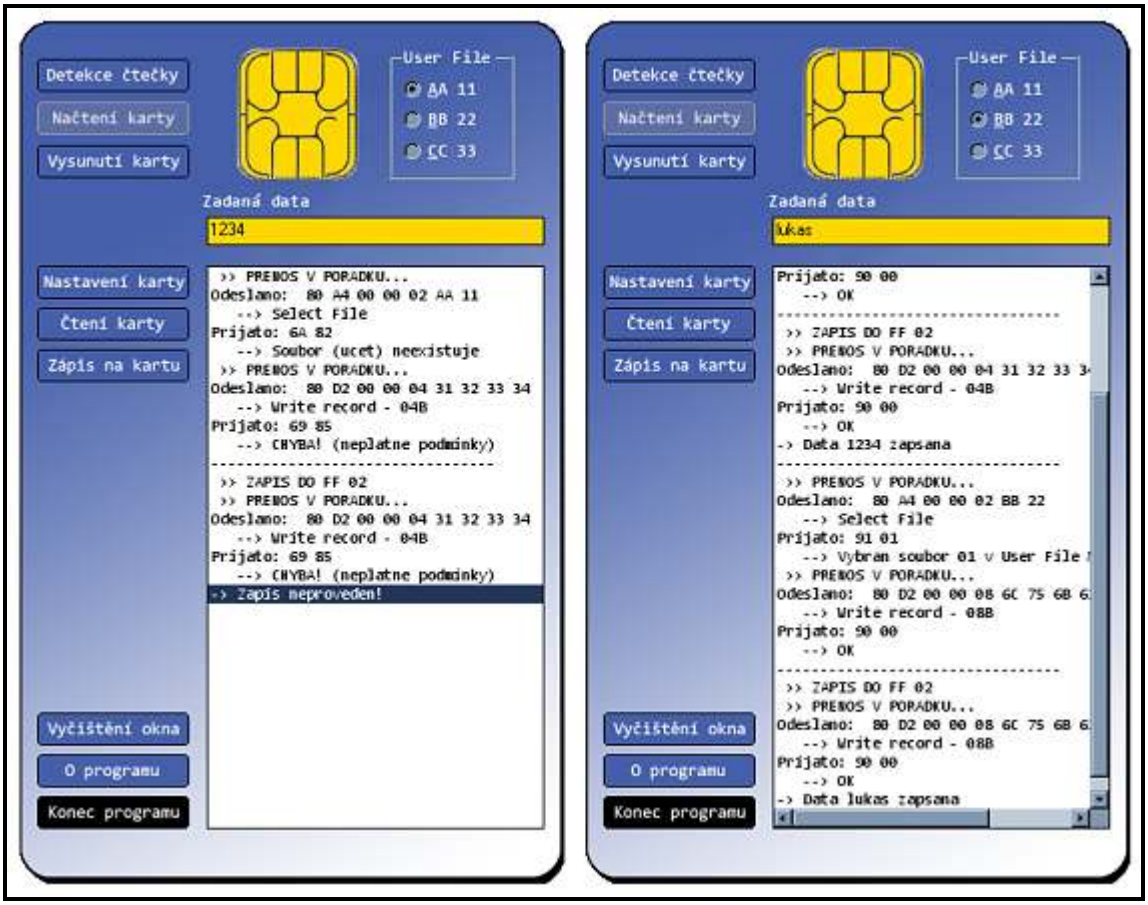


Obr. 45: Levé okno – Načtení a vysunutí karty; Pravé okno – Nastavení karty (část výpisu)

Jak bylo uvedeno již v kapitole 9.3.2, je nutné před dalším zapisováním na kartu opět ověřit IC kód, proto je opět volána metoda `DejIssuerCode()`. Po této operaci se nadefinují již konkrétní uživatelské soubory *AA 11*, *BB 22* a *CC 33* o daných velikostí. K definici těchto souborů se používá proměnná *tmpPole*, která je prezentovaná jako pole bytů. Po definici každé ze tří oblastí je zavolána opět metoda `ZapisZaznam`() a úspěšné vytvoření uživatelských souborů je ověřeno parametrem *SCARD_S_SUCCESS*. Do informačního okna jsou postupně vypisovány informace o požadovaných a proběhlých operací, včetně odpovědí karty – informační okno je možné vidět na obrázku 45 vpravo. Po úspěšném vytvoření uživatelských souborů se na formuláři zpřístupní pole přepínačů mezi těmito soubory. Nastavení karty lze provádět kdykoliv, v případě že karta je již nastavena a obsahuje v daných sektorech nějaká data, nedojde k jejich přepsání.

Zápis na kartu

Zápis na kartu je povolen po úspěšném načtení karty. Pokud ale uživatel nezvolí předdefinovaný uživatelský soubor v přepínači *User File*, nedojde k možnosti zadání požadovaných dat do okna nad informačním oknem a po stisku tlačítka „Zápis na kartu“ se do informačního okna vypíší chybové stavy – viz obrázek 46 vlevo. K podobné situaci dojde v případě, že karta nebude nastavena a uživatel na ní bude zkoušet zapsat data (do neexistujících uživatelských souborů). Při výběru jednoho ze tří předdefinovaných uživatelských souborů se, po najetí myší na přepínač, uživateli zobrazí informace o daném souboru, konkrétně o jeho velikosti, která je potom určující pro zadávaná data. Po výběru uživatelského souboru (již bylo uvedeno, že soubor *AA 11* umožňuje uložit 4 B dat, soubor *BB 22* data o velikosti 8 B a soubor *CC 33* 16 B velká data) se zaktivuje textové pole pro zadání dat. Podle zvoleného předdefinovaného uživatelského souboru lze zadat data o maximální velikosti, kterou umožňuje zvolený soubor.



Obr. 46: Levé okno – chybný zápis (neexistující uživatelské soubory); Pravé okno – úspěšný zápis číslic *1234* a slova *lukas* po převodu do ASCII kódu a hexadecimální podoby

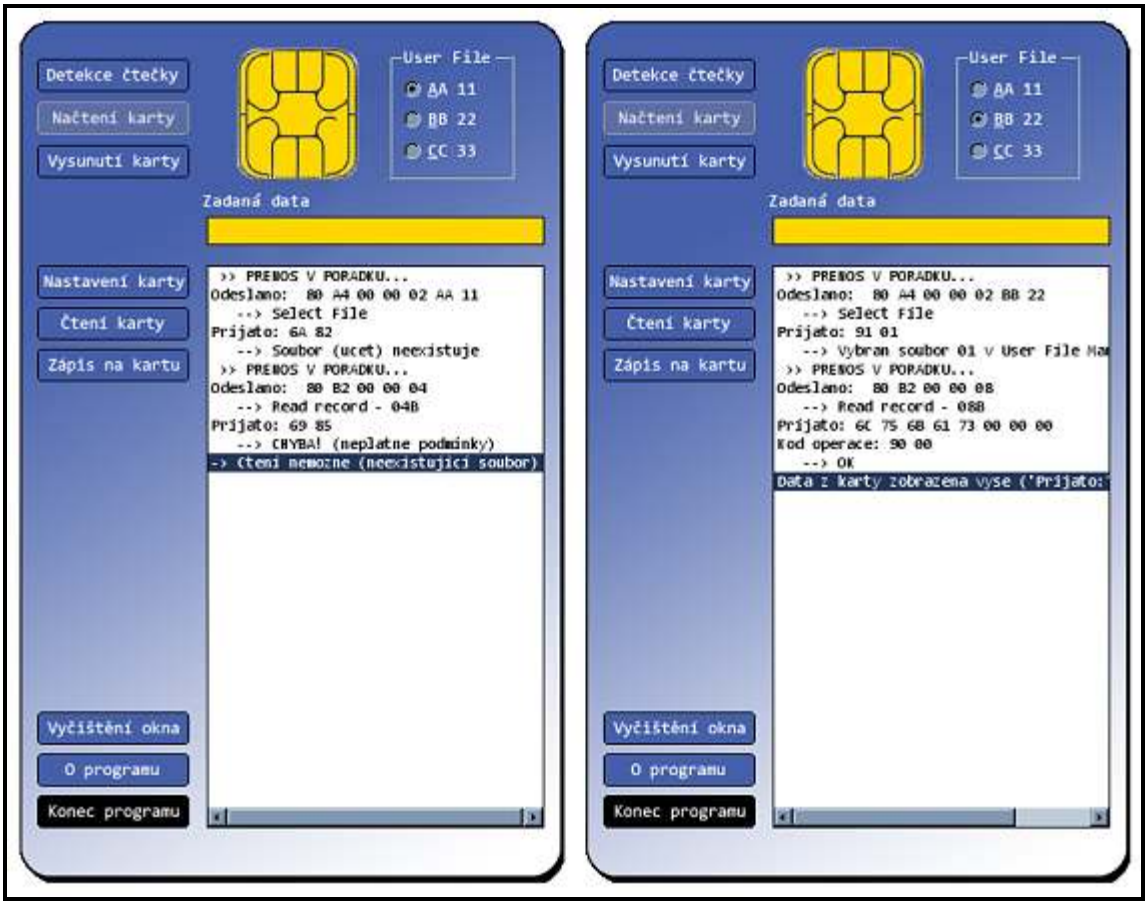
Po zadání dat a stisku tlačítka „Zápis na kartu“ dojde nejprve k výběru zvoleného souboru metodou `VyberSoubor(MaxAdresa, MinAdresa)`, kde *MaxAdresa* a *MinAdresa* jsou identifikátory zvoleného uživatelského souboru (např. AA 11). Tato metoda je více popsána v části *Nastavení karty*. K zapsání lze zadávat jakákoliv data, k jednotlivé znaky jsou totiž převedeny do ASCII[9] kódu metodou

```
Asc(string character).
```

K samotnému zapsání na kartu dojde pomocí metody `ZapisZaznam()`, která je popsána výše. Do informačního okna aplikace jsou vypsány informace o proběhlých operacích, včetně jejich úspěšnosti či neúspěšnosti – úspěšný zápis dat „1234“ do souboru *AA 11* a dat „lukas“ resp. Jejich konverzi do ASCII kódu a následně do hexadecimální podoby (6C 75 6B 61 73) do souboru *BB 22* ukazuje obrázek 46 vpravo. Příklad převodu je v kapitole 9.7 – Ověření funkčnosti aplikace. Tabulka ASCII kódů je v příloze F.

Čtení z karty

Po načtení karty je z ní možné ihned číst. Před čtením je nutné vybrat jeden z předdefinovaných uživatelských souborů. Pokud se tak nebude učiněno, dojde k vypsání chybové hlášky o neexistenci souboru. Stejný chybový stav nastane i v případě, když bude vložena nová, ještě nenastavená karta – obrázek 47 vlevo.



Obr. 47: Levé okno – neúspěšné čtení (nenastavená karta); Pravé okno – přečtení slova *lukas* z *BB 22*

Pokud uživatel vybere jeden ze souborů a stiskne tlačítko „Čtení karty“, dojde nejprve ke zkontrolování vybraného uživatelského souboru, dále pak k jeho vybrání opět metodou `VyberSoubor()` (viz výše v části *Nastavení karty*) a zvolený soubor je přečten metodou

[9] ASCII - American Standard Code for Information Interchange (americký standardní kód pro výměnu informací) – jedná se o kódovou tabulku definující znaky používané v informatice – viz příloha F.

`CtiZaznam(byte CisloZaznamu, byte DelkaDat).`

Tato metoda využívá operaci READ RECORD. Složení příkazu operace je uvedeno v tabulce 14.

Tab. 14: READ RECORD – složení příkazu

CLA	INS	P1	P2	P3
80	B2	Číslo záznamu	00	Délka

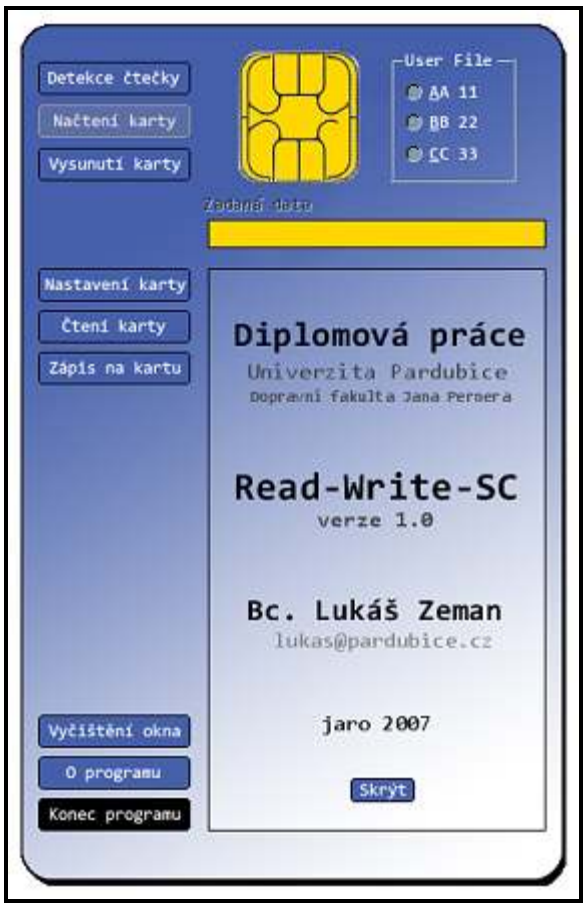
[20]

Číslo záznamu je logické číslo záznamu, který se má číst, *Délka* je počet datových bytů, které se zapíší do záznamu, který je identifikován *Číslem záznamu*. Odpovědí z karty jsou opět stavové kódy, v tomto případě 69 82, 6A 83, 67 00 a 69 85 – významy těchto kódů opět viz příloha E.

Metoda `CtiZaznam()` nadefinuje záznam *apdu* zmiňovaný již výše a do jeho parametru P3 uloží délku dat, která je požadována k přečtení. Délka dat je určena délkou uživatelského souboru, který se vybere v přepínači „User File“. Záznam *apdu* je předán výše popsané metodě `VykonejPrenosAPDU()`, která zajistí přenos. Do informačního okna jsou následně vypsána přečtená data a informace o úspěšném či neúspěšném dokončení operace. Čtení z uživatelského souboru *BB 22*, do kterého bylo předtím zapsáno slovo „lukas“ je ukázáno na obrázku 47 vpravo.

Zbývající akce s formulářem

Poslední tři tlačítka na formuláři je „Vyčištění okna“, po jehož stisku dojde k vymazání stávajícího obsahu v informačním okně, dále pak „O programu“, které zobrazí v informačním okně informace o této aplikaci – viz obrázek 48. Po opětovném stisku tlačítka „O programu“ (či po stisku tlačítka „Skrýt“ v informacích) dojde ke skrytí informací o aplikaci a zobrazí se původní obsah informačního okna. Posledním tlačítkem „Konec programu“ se aplikace ukončí – před samotným ukončením celé aplikace dojde ještě k vysunutí a odpojení karty pomocí metod `SCardReleaseContext` a `SCardDisconnect (SCARD_UNPOWER_CARD)`.

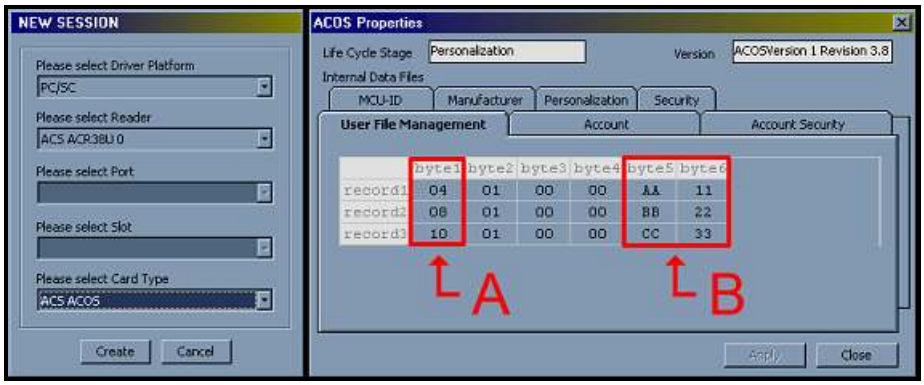


Obr. 48: Zobrazení informací o aplikaci

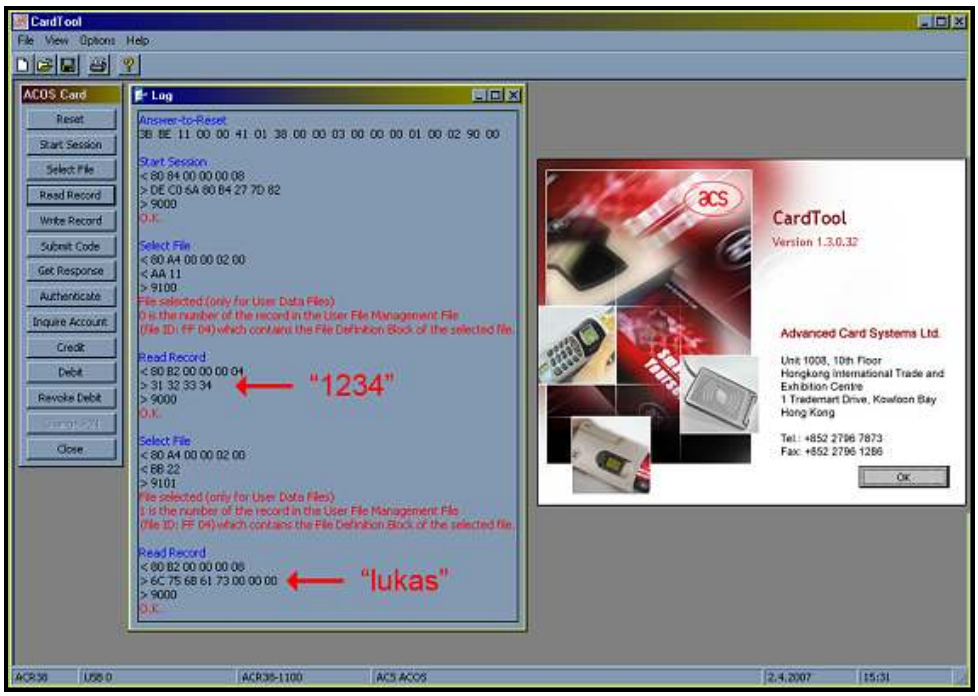
9.7 Ověření funkčnosti aplikace

K ověření funkčnosti vytvořené aplikace byla použita aplikace CardTool v.1.3.0.32, která byla dodána se čtecím zařízením a čipovou kartou společností ACS. CardTool je aplikace, která umožňuje posílat příkazy jakémukoliv čtecímu zařízení a pomocí něj komunikovat s vloženou čipovou kartou.

V první fázi dojde k nastavení připojené čtečky a vložené čipové karty (obrázek 49 vlevo), následně k nastavení aplikace pro tento typ a zahájení relace. Poté je již možné pracovat s kartou. Obrázek 49 vpravo ukazuje vlastnosti vložené karty ACOS2, konkrétně je zobrazena záložka „User File Management“, kde jsou vidět všechny tři soubory, vytvořené aplikací. Příkazem „Select File“ je vybrán uživatelsky vytvořený soubor AA 11 a poté z něj přečten záznam o velikosti 4 B – v okně se zprávami je vidět skutečně výstup 1 2 3 4, který byl zapsán uživatelem – ve skutečnosti je zobrazeno 31 32 33 34, což je způsobeno již zmiňovaným převodem zadaných čísel do ACSII kódu, který je poté převeden do šestnáctkové soustavy – číslice 1 má ASCII kód 49, který po převedení do šestnáctkové soustavy má hodnotu 31. Poté je zvolen další soubor, BB 22, a postup se opakuje – výsledkem je posloupnost čísel 6C 75 6B 61 73, což je slovo „lukas“ opět nejprve znak po znaku převedené do ASCII kódu a následně do hexadecimální podoby (písmeno „k“ má ASCII kód 107 a číslo 107 je v šestnáctkové soustavě reprezentováno jako „6B“. Výstup testovací aplikace je na obrázku 50, tabulka ASCII kódů v příloze F.



Obr. 49: Aplikace CardTool – Levá část – nastavení čtečky a typu karty; Pravá část – Správce souborů – A = hexadecimální velikost souborů, B = tři uživatelské soubory



Obr. 50: Aplikace CardTool – Informační okno se zprávami o operacích s kartou

10 Závěr

V teoretické části byly představeny čipové karty z hlediska jejich historie a vývoje. Jelikož na českém trhu figuruje řada typů čipových karet, byl jejich počet zúžen pouze na bezkontaktní technologii, která je z hlediska Pardubické čipové karty důležitá. Společnosti, zabývající se touto problematikou distribuují na českém trhu patnáct typů bezkontaktních čipů, z nichž mezi nejpoužívanější a nejrozšířenější patří čipy společnosti Philips pod obchodním označením Mifare. Tento typ využívají téměř všichni dopravci v České republice, včetně Dopravního podniku města Pardubic v jejich, již zmíněné, Pardubické kartě. Nový odbavovací systém DPmP, a.s., respektive použití bezkontaktní čipové karty s funkcí elektronické peněženky, je velkým přínosem pro rozvoj města i regionu a skrývá se v nich velký potenciál pro budoucí využití pro služby nejen města, ale i regionu a soukromých společností.

Implementační část představila sofistikovaný software k zajišťování všech operací, které jsou nutné k provozu systému čipových karet. Pomocí tohoto software lze účelně sledovat pohyb osob a využívání čipových karet v jednotlivých oblastech zájmu, zpracovávat statistické informace z provozu, ale i jednoduše nastavovat tarifní zóny pro konkrétní uživatele.

Jelikož je tendence sdružovat jednotlivé dopravce v daném regionu do integrovaných dopravních systémů, ve kterých se sbíhají různé typy doprav, byla jedna oblast implementační části práce zaměřena na tyto integrované dopravní systémy v jednotlivých krajích České republiky. V každém kraji existuje koordinátor takového systému, který má na starost přípravu, realizace a provozování daného IDS a koordinaci základní dopravní obslužnosti na území určitého kraje. Jednotlivý koordinátoři či zástupci významných dopravců v daných krajích byli kontaktováni a jejich vyjádření o aktuálním stavu s důrazem na oblast odbavovacího zařízení resp. použitých čipových karet, posloužily jako významné zdroje v této části práce.

Další částí bylo případné rozšíření univerzitního systému čipových karet o možnosti elektronické peněženky a s tím související možnou integraci Pardubické karty na univerzitu. Pro tento případ byly navrženy oblasti, kterých by se toto rozšíření mohlo týkat, a zároveň byl vytvořen dotazník, který byl elektronicky i tištěnou formou distribuován mezi studenty a zaměstnance Univerzity Pardubice. Dotazník se týkal především otázek spokojenosti se stávajícím systémem a možnostmi rozšíření systému o navržené oblasti. Z výsledků je pak patrné, že převážná většina dotazovaných by integraci s Pardubickou kartou, a s tím související rozvoj služeb, uvítala. Před případnou integrací je ale potřeba vyřešit mnoho problémů, které jsou v této práci popsány. Jejich řešení by mohlo být dobrým tématem pro další diplomové práce.

Poslední částí této práce je vytvořená aplikace s názvem Read-Write-SC, která umožňuje komunikovat čipové kartě s klasickým stolním počítačem s operačním systémem Windows přes čtecí zařízení. Stolní počítač typu PC s operačním systémem Windows zastupuje terminál, na kterém je aplikace spuštěna a se kterým čipová karta začne komunikovat ve chvíli vložení do čtecího zařízení (v případě použití bezkontaktní čipové karty je tímto okamžikem přiblížení karty ke čtecímu zařízení). Aplikace byla vytvořena z důvodu ověření nenáročnosti takovéto komunikace i s ohledem na její bezpečnost. Pro vývoj a testování byl použit konkrétní typ čipové karty a čtecího zařízení, uvedený v dané části práce, po jednoduchých úpravách je však tato aplikace rozšiřitelná na jakýkoliv typ karet, díky používaným standardům komunikace z normy ISO 7816. Aplikace je k vyzkoušení na přiloženém CD, kde jsou k dispozici i zdrojové kódy aplikace.

Soupis bibliografických citací

[1] JUŘÍK, P. *Encyklopedie platebních karet*. Praha: Grada, 2003. ISBN 80-247-0685-7.

[2] PŮLPÁN, R. Bezkontaktní karty dobývají svět. *Sdělovací technika*. Praha: 2002, roč. 50., č. 6,. s. 20

[3] NOVÁK, P. *Aspekty využití bezkontaktních, kontaktních, hybridních a duálních čipových karet ve školství*. Seminář Technické, obchodní a právní řešení v oblasti identifikačních karet a PKI [online]. 2004, [cit. duben 2007]. Dostupný z WWW: <http://www.cesnet.cz/doc/seminare/20040616/acg-novak.ppt> .

[4] *M CARD – plastové karty, bezkontaktní karty, čipové karty, magnetické karty* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.mcard.cz/bezkontaktni.html>.

[5] *Elatec – RFID čipy* [online]. [cit. únor 2007]. Dostupný z WWW: <http://www.elatec.cz/rfid/chips.php>.

[6] HANÁČEK, P., MATYÁŠ, V. *Čipová karta v informačních systémech* [online]. 2003, [cit. Duben 2007]. Dostupný z WWW: <www.datakon.cz/datakon03/d03_tut_hanacek.pdf>.

[7] *Pardubická karta*. Pardubice: Dopravní podnik města Pardubic a.s., www.dpmp.cz

[8] *Zavedení odbavovacího systému MHD v Pardubicích*. Vsetín: EM TEST ČR spol. s.r.o. www.emtest.biz

[9] *Wikipedia.org: Integrovaný dopravní systém* [on-line]. [cit. duben 2007]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Integrovan%C3%BD_dopravn%C3%AD_syst%C3%A9m>.

[10] *Opencard.cz* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.opencard.cz>.

[11] *Středočeský kraj: Středočeská integrovaná doprava* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.kr-stredocesky.cz/doprava/stredoceska-integrovana-doprava>.

[12] *Plzeňská karta* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.plzenskakarta.cz>.

[13] *Citycard.cz Liberec* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.citycard.cz>.

[14] *České dráhy, a.s. – IDS – příměstská doprava* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.cd.cz/index.php?action=section&id=17318>.

[15] HARÁK, M. Integrovaný dopravní systém bude zaveden i v kraji Vysočina. *ŽELEZNIČÁŘ – Týdeník Českých drah* [online]. Květen 2005, č. 36 [cit. duben 2007]. Dostupný z WWW: <http://www.cd.cz/static/old/NEW/TCD2005/5_36ids.htm>.

[16] *In-karta* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.inkarta.cz>.

[17] *Veolia Transport Česká republika* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.connex.cz/PortalPage____11153.aspx>

[18] *Elatec – RFID – Unique – EM4102* [online]. [cit. duben 2007]. Dostupný z WWW: <http://www.elatec.cz/rfid/unique.php>.

[19] ACR38 USB Smart Card Reader/Writer Reference Manual – version 1.9. Hong Kong: Advanced Card Systems Ltd. February 2006.

[20] *ACOS2 Smart Card Reference Manual – version 2.3*. Hong Kong: Advanced Card Systems Ltd. April 2006.

[21] *Visual Studio Express: Visual C# – Easy to Use* [online]. [cit duben 2007]. Dostupný z WWW: <http://msdn.microsoft.com/vstudio/express/visualcsharp/default.aspx>.

[22] *Visual C# online help* [online]. [cit. duben 2007]. Dostupný z WWW: <http://msdn2.microsoft.com/en-us/library/kx37x362(VS.80).aspx>

[23] ROBINSON, S., ALLEN, S. K. C# *Programujeme profesionálně*. 1. vyd. Brno: Computer Press, 2003. 1130s. ISBN: 80-251-0085-5.

[24] FERENC, J. *Odběrová analýza průběhu ověřování PINu na kryptografické čipové kartě*. Brno 2006. Bakalářská práce na Masarykově Univerzitě na Fakultě informatiky. Vedoucí bakalářské práce Mgr. Petr Švenda.

[25] PŘÁDKA, M., KALA, J. *Elektronické bankovnictví*. Praha: Computer Press, 2000. ISBN 80-7226-328-5.

[26] ASCII tabulka [online]. [cit. duben 2007]. Dostupně z WWW: <http://www.labo.cz/mft/matasciit.htm>.

[27] BOLDIŠ, P. *Bibliografické citace dokumentů podle ČSN ISO 690 a ČSN ISO 690-2: Část 1 – Citace: metodika a obecná pravidla* [online]. Verze 3.3. c1999–2004, poslední aktualizace 11. 11. 2004. [cit. duben 2007]. Dostupný z WWW: <http://www.boldis.cz/citace/citace1.pdf>.

[28] BOLDIŠ, P. Bibliografické citace dokumentů podle ČSN ISO 690 a ČSN ISO 690-2: část 2 – Modely a příklady citací u jednotlivých typů dokumentů [online]. Verze 3.0. c1999–2004, poslední aktualizace 11. 11. 2004. [cit. duben 2007]. Dostupný z WWW: <http://www.boldis.cz/citace/citace2.pdf>.

Přílohy

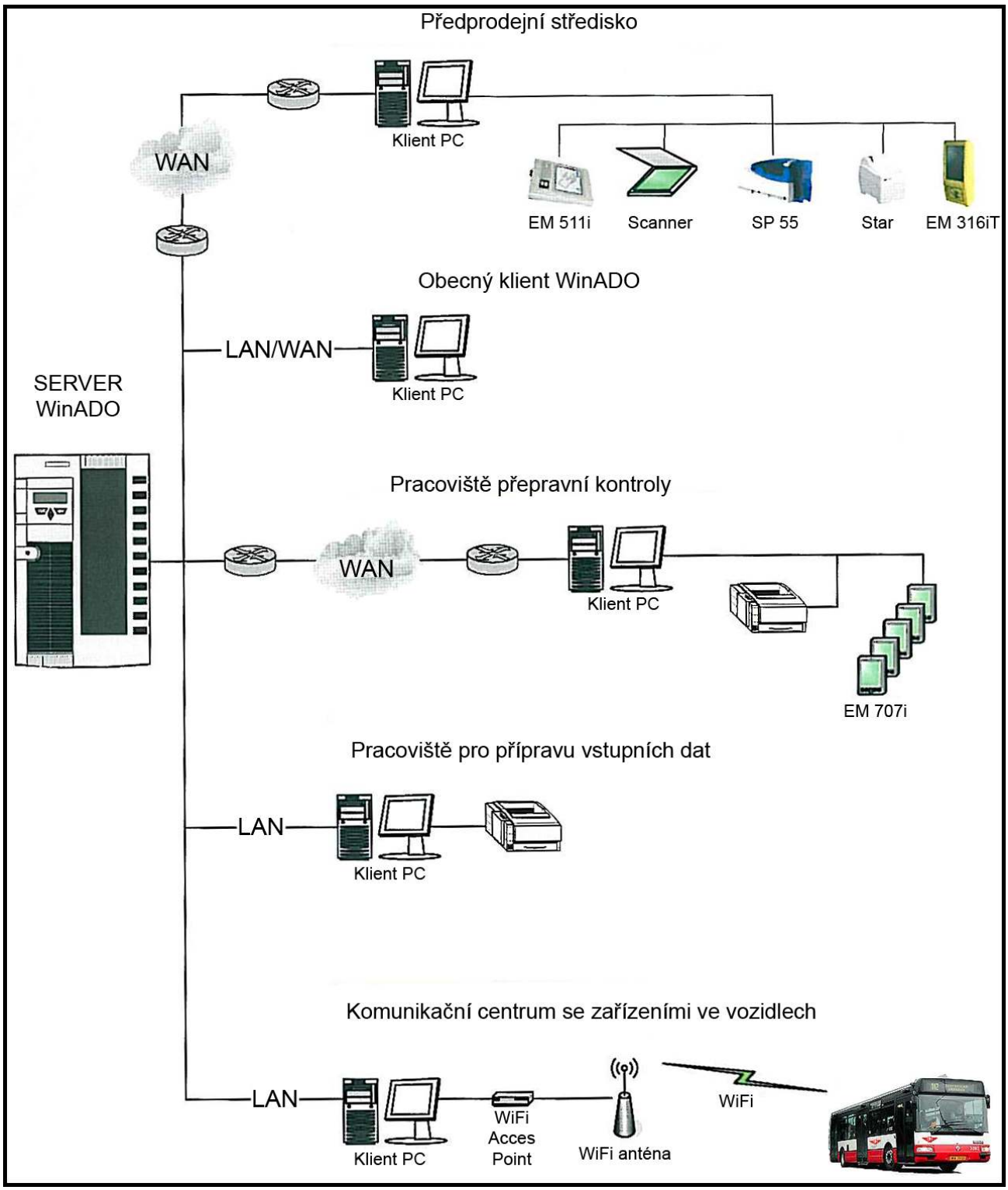
Příloha A

Vývoj kartových systémů od roku 1986 do roku 2004 [1]

	Počet karet (mil.)					Obrat (mld. USD)					Počet bankomatů (tis.)				
	1986	1990	2000	2002	2004	1986	1990	2000	2002	2004	1986	1990	2000	2002	2004
American Express	26	36,7	51,7	57,3	65	64	111	297	-	416	0	40	400	500	550
Diners Club	6,5	6,9	8	-	8,5	9	16	35	-	33	0	0	331	780	950
EuroCard / MasterCard	132	161	810	1095	1242	96	200	865	1142	2858	0	45	604	821	1010
JCB	7,6	18,5	36	48,4	52	3,4	11	42	43	52	0	0	0	0	0
VISA	145	255	1079	1215	1230	135	348	1854	2475	3423	0	62	550	810	950

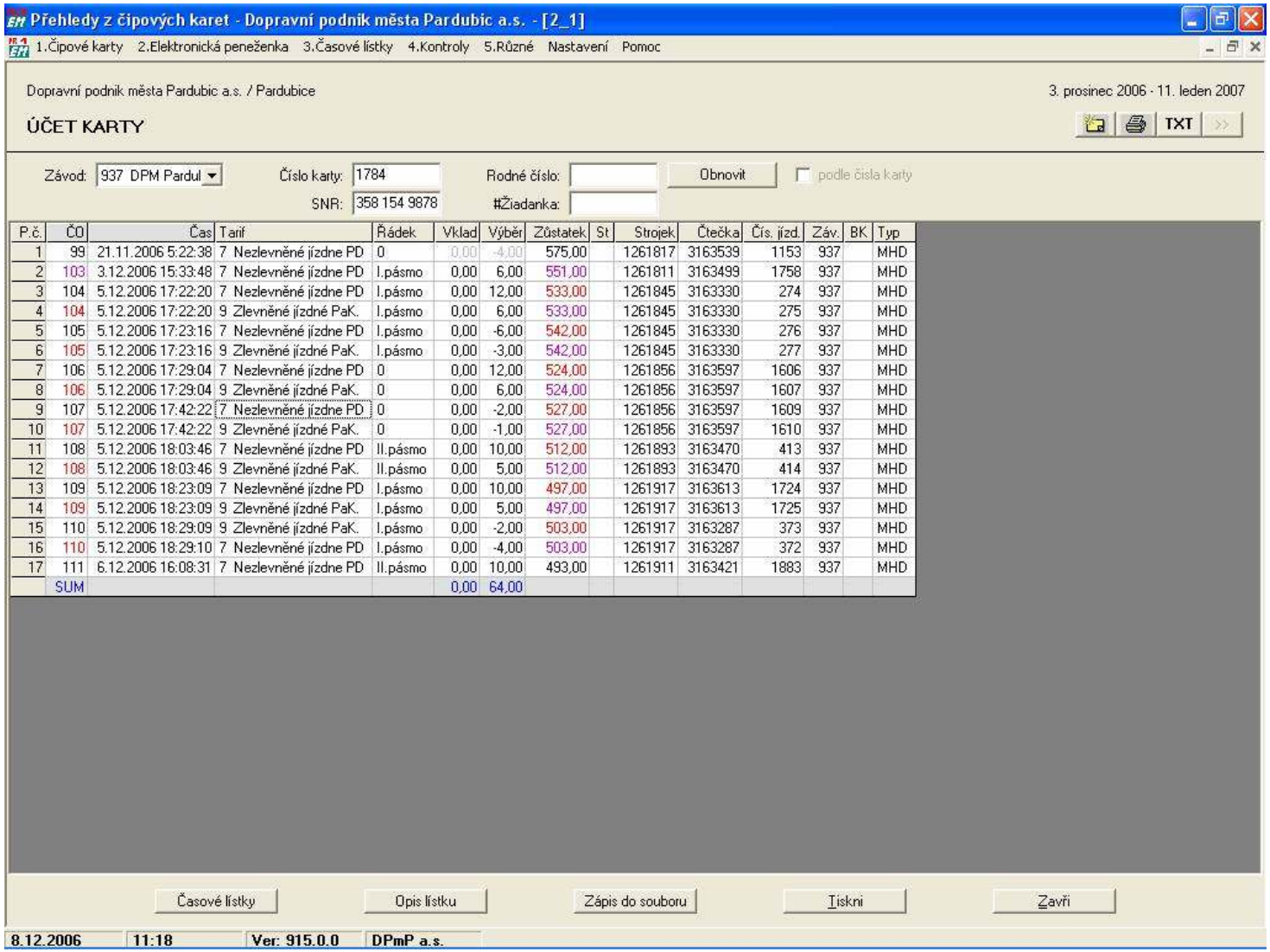
Příloha B

Blokové schéma systému WinADO - celkový pohled [8]



Příloha C

Systém WinADO - ukázka aplikace s výstupy čipové karty číslo 800382 (testovací jízdy z prosince 2006) a Opis lístku 1606



Opis lístku 1606

Firma	Dopravní podnik města Pardubic a.s.		
IČO	63217066	**DIČ**	CZ63217066
Řidič	Rabatin Evžen		
Datum	úterý	5.12.2006	
Linka	13	**Spoj**	1728
Kasa	1261856	**Kód spoje**	0
Číslo	1606	**Čas**	17:42:22
Číslo výstup	1609	**Čas výstup**	17:42:22
Cena	20,00 Kč		
Bez DPH	19,00 Kč	**DPH 5%**	1,00 Kč
Karta	1784	**Zůstatek**	524,00 Kč
SNR	358 154 9878		
Tarif	Nezlevněné jízdne PD		
Nástupní zast.	Polabiny,Sluneční		
Výstupní zast.	U Grandu		

Příloha D

Dotazník – Využití Pardubické karty na Univerzitě Pardubice

Pardubická karta je bezkontaktní čipová karta, která slouží jako elektronický nosič jízdného, buď ve formě časových jízdenek, nebo ve formě elektronické peněženky, ze které je možné platit za jednotlivé jízdy. Do budoucna je snaha rozšířit Pardubickou kartu mimo oblast MHD.

Není-li uvedeno jinak, zaškrtněte pouze jednu odpověď. V elektronické podobě zabarvěte vhodnou odpověď (odpovědi).

1) Projekt Pardubická karta

- ☐ znám
- ☐ slyším poprvé

2) Pardubickou kartu

- ☐ mám a takto mi vyhovuje
- ☐ mám ale uvítal/a bych širší využití
- ☐ zatím nemám, ale budu mít
- ☐ nemám a nepotřebuji
- ☐ nemám, ale zařídil/a bych si ji, pokud by ji bylo možné použít jinde než MHD
- ☐ nemám, ale zařídil/a bych si ji, pokud by ji bylo možné použít na Univerzitě
- ☐ nevím

3) Pardubickou kartu bych využíval/a (možné zaškrtnout více možností):

- ☐ pouze na MHD
- ☐ na dopravu v rámci Pardubického kraje
- ☐ jako elektronickou peněženku k placení služeb města (parkovné, pokuty měst. policie, půjčovna kol, ...)
- ☐ jako elektronickou peněženku k rezervování a placení vstupenek do kulturních, sportovních a zábavních zařízení (divadla, kina, ČEZ aréna, tenis, bowling, squash, plavecký areál, závodiště, ...)
- ☐ jako studentskou (zaměstnaneckou) kartu (identifikace studenta/zaměstnance - knihovna, přístup do učeben, přístup na koleje, rezervace do menzy...)
- ☐ jako ISIC (ITIC) kartu
- ☐ jako elektronickou peněženku k placení služeb na území školy (obědy (menza), knihovna, koleje)
- ☐ jako elektronickou peněženku k placení doplňkových služeb na Univerzitě (automaty na kávu, občerstvení, bagety, jídlo, bufet, ...)
- ☐ jako klasickou platební kartu (MasterCard, Maestro, Visa, Visa Elektron) vybraných bank (KB, ČS, ČSOB, GE, E-banka, ...)
- ☐ jiný způsob využití (doplňte): _____

4) Stávající univerzitní systém karet (přístup do knihovny, místností, obědy, …) považuji za:

- ☐ velmi dobrý
- ☐ dostačující
- ☐ nedostačující
- ☐ uvítal/a bych změny

5) Spojení studentské karty s Pardubickou kartou – ve finále jedna karta na „všechno“:

- ☐ určitě **ne**, nevidím v tom přínos
- ☐ určitě **ano**, v jakékoliv podobě
- ☐ ano, pokud by byla, kromě MHD a studentské karty, využitá i jako alespoň jedna z možností v bodě 3)
- ☐ nevím, je mi to jedno
- ☐ Pardubickou kartu nemám a neuvažuji vůbec o jejím pořízení

A) Jsem

☐ student UPCE ☐ zaměstnanec UPCE

B) Jsem

☐ muž ☐ žena

C) Jsem z

☐ Pardubic či přilehlého okolí (dosažitelného MHD)

☐ okresu Pardubice

☐ Pardubického kraje (Přelouč, Chrudim, Holice, Hlinsko, Vysoké Mýto, Svitavy, Litomyšl, Česká Třebová, Polička, Ústí nad Orlicí, Vamberk, Lanškroun, Králíky)**

☐ Hradce Králové či přilehlého okolí (dosažitelného MHD)

☐ Královehradeckého okresu

☐ Královehradeckého kraje

☐ Jiného kraje ČR - uveďte _____ (město _____)

D) Je mi

☐ méně než 20 ☐ 24 - 26

☐ 20 - 23 ☐ více než 26

E) Studuji

☐ bakalářské studium (uveďte ročník _____2._____)

☐ navazující magisterské studium (uveďte ročník _____)

☐ postgraduální studium (uveďte ročník _____)

F) Studuji formou

☐ prezenčního denního studia

☐ kombinovaného (dálkového) studia

G) Studuji

☐ Chemicko-technologickou fakultu ☐ Fakultu restaurování

☐ Dopravní fakultu Jana Pernera ☐ Fakultu zdravotnických studií

☐ Fakultu ekonomicko.správní ☐ Ústav elektrotechniky a informatiky

☐ Filozofickou fakultu

H) V případě dokončení bakalářského stupně CHCI pokračovat magisterským stupněm

☐ ANO zde v Pardubicích ☐ NE

☐ ANO jinde v ČR ☐ NEVÍM

☐ ANO v zahraničí

I) V případě dokončení magisterského stupně CHCI pokračovat postgraduálním stupněm

☐ ANO zde v Pardubicích ☐ NE

☐ ANO jinde v ČR ☐ NEVÍM

☐ ANO v zahraničí

J) Bydlím

☐ v dosahu MHD (denně dojíždím)

☐ mimo dosah MHD (denně dojíždím - Bus/Vlak/Oboje/Jinak*)

☐ na kolejích v Pardubicích

☐ na privátu v Pardubicích

*** nehodící se škrtnete** ****zaškrtnete správnou odpověď**

Příloha E

Stavové kódy a kódy operací [20]

Tab. 1: Stavové kódy

Kód	Popis
90 00	OK
91 nn	Vybrán soubor nn v User File Management File
61 nn	OK - Pošli GET RESPONSE s *Le = nn* pro získání odpovědi (dat)
62 81	Pravděpodobně poškozená data
63 Cn	Nesprávný klíč, *n* značí počet zbyvajících pokusů
67 00	Špatné *P3* - specifikovaná délka je větší než délka záznamu nebo větší než 32
69 66	Příkaz nedostupný
69 82	Nepřijatý kód (Secret Code / Issuer Code / PIN)
69 83	Autentifikace neúspěšná (klíč uzamčen)
69 85	Chyba - neplatné podmínky
69 F0	Nekonsistentní data (na účtu)
6A 82	Soubor (účet) neexistuje
6A 83	Záznam nenalezen - soubor příliš krátky
6A 86	Nepsravné *P1 - P2*
6B 20	Nesprávná částka (částa příliš velká)
6C nn	Pošli GET RESPONSE s *P3 = nn* pro získání odpovědi (dat)
6D 00	Neznámý INS
6E 00	Nesprávný CLA
6F 10	Další transkace nemožné - počítadlo transakcí účtu na maximu

Tab. 2: Vybrané kódy operací

Kód	Popis Popis	Kód	Popis
80 84 00 00 08	Start session	80 D2 00 00 04	Write record - 04B
		80 D2 00 00 08	Write record - 08B
80 82 00 00 10	Authenticate	80 D2 00 00 10	Write record - 16B
80 C0 00 00 08	Get response		
		80 D2 00 00 06	Definice 1. zaznamu v FF 04
80 20 01 00 08	Submit code - AC1	80 D2 01 00 06	Definice 2. zaznamu v FF 04
80 20 02 00 08	Submit code - AC2	80 D2 02 00 06	Definice 3. zaznamu v FF 04
80 20 03 00 08	Submit code - AC3		
80 20 04 00 08	Submit code - AC4	80 E2 00 00 0B	Credit
80 20 05 00 08	Submit code - AC5	80 E6 00 00 0B	Debit
80 20 06 00 08	Submit code - PIN	80 E8 00 00 04	Revoke Debit
80 20 07 00 08	Submit code - IC		
		80 E4 00 00 04	Inquire Account
80 A4 00 00 02	Select File	80 C0 00 00 19	Get response (Inquire Account)
80 B2 00 00 04	Read record - 04B	80 24 00 00 08	Change PIN
80 B2 00 00 08	Read record - 08B		
80 B2 00 00 10	Read record - 16B		

Příloha F

Tabulka ASCII kódů [26]

Kód	Význam znaku	Kód	Význam znaku
9	tabulátor	13	návrat vozíku - Carriage Return (CR)
10	posuv o řádek - Line Feed (LF)	27	Escape
12	posuv o stránku - Form Feed (FF)	32	mezera

Kód	Znak	Kód	Znak	Kód	Znak	Kód	Znak	Kód	Znak	Kód	Znak	Kód	Znak	Kód	Znak
32		60	<	88	X	116	t	144	□	172	¬	200	Č	228	ä
33	!	61	=	89	Y	117	u	145	‘	173		201	É	229	Í
34	"	62	>	90	Z	118	v	146	’	174	®	202	Ę	230	ć
35	#	63	?	91	[	119	w	147	“	175	Ż	203	Ë	231	ç
36	$	64	@	92	\	120	x	148	”	176	°	204	Ě	232	č
37	%	65	A	93	]	121	y	149	•	177	±	205	Í	233	é
38	&	66	B	94	^	122	z	150	–	178	˛	206	Î	234	ę
39	'	67	C	95	_	123	{	151	—	179	ł	207	Ď	235	ë
40	(	68	D	96	`	124	|	152	□	180	´	208	Đ	236	ě
41	)	69	E	97	a	125	}	153	™	181	µ	209	Ń	237	í
42	*	70	F	98	b	126	~	154	š	182	¶	210	Ň	238	î
43	+	71	G	99	c	127		155	›	183	·	211	Ó	239	ď
44	,	72	H	100	d	128	€	156	ś	184	¸	212	Ô	240	đ
45	-	73	I	101	e	129	□	157	ť	185	ą	213	Ő	241	ń
46	.	74	J	102	f	130	‚	158	ž	186	ş	214	Ö	242	ň
47	/	75	K	103	g	131	□	159	ź	187	»	215	×	243	ó
48	0	76	L	104	h	132	„	160		188	Ľ	216	Ř	244	ô
49	1	77	M	105	i	133	…	161	ˇ	189	˝	217	Ů	245	ő
50	2	78	N	106	j	134	†	162	˘	190	ľ	218	Ú	246	ö
51	3	79	O	107	k	135	‡	163	Ł	191	ż	219	Ű	247	÷
52	4	80	P	108	l	136	□	164	¤	192	Ŕ	220	Ü	248	ř
53	5	81	Q	109	m	137	‰	165	Ą	193	Á	221	Ý	249	ů
54	6	82	R	110	n	138	Š	166	¦	194	Â	222	Ţ	250	ú
55	7	83	S	111	o	139	‹	167	§	195	Ă	223	ß	251	ű
56	8	84	T	112	p	140	Ś	168	¨	196	Ä	224	ŕ	252	ü
57	9	85	U	113	q	141	Ť	169	©	197	Ĺ	225	á	253	ý
58	:	86	V	114	r	142	Ž	170	Ş	198	Ć	226	â	254	ţ
59	;	87	W	115	s	143	Ź	171	«	199	Ç	227	ă	255	˙

Údaje pro knihovnickou databázi

Název práce	Technologie a implementace pardubické čipové karty a návrh možností využití v informačním prostředí univerzity
Autor práce	Bc. Lukáš Zeman
Obor	Informatika
Rok obhajoby	2007
Vedoucí práce	Ing. Jana Holá, PhD.
Anotace	Cílem diplomové práce je popis principu nového odbavovacího systému v MHD v Pardubicích a výhody a nevýhody jeho využití a návazností na případné využití v prostředí Univerzity Pardubice. Součástí práce je aplikace, umožňující komunikaci mezi čtecím zařízením a čipovou kartou. V teoretické části je podaný přehled o novém odbavovacím systému pardubické MHD, v implementační části práce je návrh využití Pardubické čipové karty v informačním prostředí univerzity a možnost vyzkoušení komunikaci čipové karty pomocí čtecího zařízení s počítačem pomocí vytvořené aplikace s názvem Read-Write-SC.
Klíčová slova	informatika, doprava, čipová, karta, MHD Pardubice, Dopravní podnik, čipová karta, smart card, aplikace, odbavovací systém, čtecí zařízení