Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Problematika vzájemné kompatibility městských čipových karet v ČR

Radomír Kozler

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Problematika vzájemné kompatibility městských čipových karet v ČR " jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28.4.2009 _____

Poděkování

Rád bych touto cestou poděkoval vedoucí bakalářské práce RNDr. Dagmaře Brechlerové, Ph.D. za odborné rady a pomoc, dále Mgr. Martinu Chvalovi a Zbyňku Proškovi, členům týmu Plzeňské karty za pomoc při získávání informací.

Problematika vzájemné kompatibility městských čipových karet v ČR

Broad issue of mutual city cards compatibility in the CR

Souhrn

Cílem této bakalářské práce je ozřejmit problematiku vzájemné kompatibility existujících městských čipových karet na území ČR. Základem pro práci je vyhodnocení možností vzájemné kompatibility na dvou úrovních a to ryze technické, tedy použitého hardwaru neboli typu karet, a v druhé úrovni na rovině aplikační, tedy použitých datových struktur a možnosti vzájemného sdílení jednotlivých aplikací na užívaných čipových kartách.
Na základě shrnutí poznatků o používané technologii a různých aplikací u fungujících nebo připravovaných projektů městských multifunkčních čipových karet přináší tato práce informace o používání těchto technologií v ČR a snaží se pro čtenáře ozřejmit klíčové body, které bude nutno vyřešit pro uznávání karet mezi jednotlivými systémy městských čipových karet.

Summary

At present city cards have been used in the Czech Republic. The aim of this bachelor work is to clarify the broad issue of their mutual compatibility. The work is based on the evaluation of possibilities of mutual compatibility at two levels: First, it is a purely technical level, i.e. the hardware (the card type), and second, an application level, i.e. applied data structures, and possibilities of sharing the pieces of applications already used.

Following the findings based on technology and various applications used in both current and prepared projects connected with multiple-function city cards, this work brings information on using the technologies in the Czech Republic and tries to clarify the crucial problems which must be solved before city cards become interactive in different systems.

Klíčová slova: čipová karta, Mifare, DESFire, elektronická peněženka, městská karta, multifunkční karta, kompatibilita.

Keywords: chip card, Mifare, DESFire, electronic wallet, city card, multitifunctional card, kompatibility.

Obsah

1. Cíl a metodika práce

V české republice se v posledních pěti letech zrodil nový fenomén, pro který se vžívá označení „městská čipová karta“. Pod tímto termínem rozumíme systém, který umožňuje držiteli takové karty zjednodušeným způsobem čerpat služby a to placené ze strany držitele, tak i hrazené například městem, zpravidla v urbanizovaném prostředí. Nelze však opominout další rozvíjející se trend, kterým je rozšíření těchto karet mimo území měst, která původně stála u jejich zřízení, do jejich okolí a celých krajů včetně všech výhod s tím přicházejících. Nově plánované systémy jako je Moravskoslezská nebo Karlovarská karta tak jsou již rovnou plánovány s celokrajskou působností a „sudičkou“ určující jejich budoucnost již nejsou orgány měst, ale krajské úřady.

V současné době jsou držiteli některé z těchto čipových karet již statisíce obyvatel České republiky. Významným způsobem se rozšiřuje jak území pokryté vydavateli jednotlivých čipových karet, tak spektrum služeb, které je za jejich pomoci možno užívat. Abychom zachovali vyváženost informací, musíme také zmínit, že se objevuje spektrum specifických služeb kde je umožněno v některých variantách užívat tyto služby pouze držiteli takové karty. Typickým příkladem je nákup roční časové jízdenky na MHD v Praze, kde je její pořízení podmíněno držením karty Open card.

Jednotlivé systémy však vznikají po republice jako samostatné technické projekty stavěné na míru podle jednotlivých zadání, bohužel však bez existence normy pro jejich tvorbu, či alespoň dodržení základních parametrů, které by do budoucna umožnili jejich vzájemné propojení. Tvůrci těchto systémů se velmi často ohánějí heslem „Jedna karta na všechno“, ale klapky na očích a i neexistence normativního předpisu způsobuje, že do budoucna bude propojení těchto systémů technicky, finančně, právně i organizačně velmi náročné. Parafrázované heslo „Jedna karta na všechno a v celé ČR“ tak je nyní spíše utopické a s každým dalším vytvořeným systémem se paradoxně spíše oddaluje, nežli blíží.

Svou bakalářskou práci jsem nazval Problematika kompatibility městských čipových karet v ČR. V první části se zabývám hardwarovou kompatibilitou uvedených systémů spolu s analýzou současného stavu. Druhá část se zabývá problematikou kompatibility na aplikační úrovni, s přihlédnutím k aplikaci uložené na kartě i jejímu protějšku na straně systému městské čipové karty nebo subjektů na projektu participujících.Na základě těchto údajů je v závěru uveden seznam klíčových bodů, které je nutno splnit, aby dva systémy městských čipových karet mohly vzájemně sdílet jeden datový nosič, tedy čipovou kartu a vzájemně si ji uznávat.

2. Technická kompatibilita

2.1. Úvod do problematiky

2.1.1. Popis technologie čipových karet

S postupující miniaturizací ve výpočetní technice se stále více využívá mikročipů k uchování specializovaných informací, mnohdy jednoúčelových, které jsou mikročipy nejen schopny bezpečně uchovávat, ale i velmi rychle a jednoduše opět poskytovat. Při velikosti čipů v řádech milimetrů i méně je možno tyto prvky zabudovat prakticky do jakéhokoli média, které může být původně určeno pro zcela jiné účely (propisovací tužky, peněženky, klíčenky, přívěsky, obal na zboží atd.). Jde jen o to, jakým způsobem se vlastní čip spojí se zařízením, které bude schopno zpracovat informace uložené v paměti čipu. Velmi výhodnou formou se ukázalo být zabudování mikročipu do plastové karty, kde velikost karty byla volena tak, aby nekladla přílišné prostorové nároky, ale zároveň byla dostatečně velká na to, aby mohla nést další vizuální informace, jak je uvedeno v literatuře [3]. Toto spojení je nazýváno čipová karta.

2.1.2. Druhy čipových karet

Pod pojmem čipová karta je převážně míněna plastová identifikační karta o rozměrech 85,6 x 54 x 0,76 mm (jak je stanoveno normou ISO/IEC 7810), ve které je zabudován elektronický mikročip (fyzikální vlastnosti tohoto čipu a jeho umístění podléhají pak normě ISO/IEC 7816). Čipové karty prošly dlouhodobým vývojem a mají za sebou úspěšnou praxi. V zásadě se dělí na paměťové a mikroprocesorové, dále na kontaktní (standardní) a bezkontaktní.

2.1.3. Druhy karet podle čipu

Paměťové karty mají čip pouze jako paměťovou buňku. Slouží jako médium pro bezpečné uložení informací. Přístup k těmto informacím může být ochráněn. Nenabízejí však kryptografické funkce a jejich nevýhodou je také to, že je lze zkopírovat.

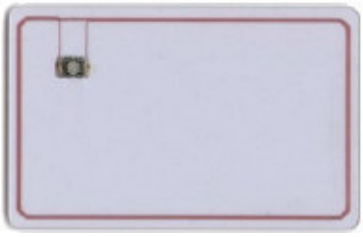
Mikroprocesorové karty jsou karty s aktivním procesorem a operačním systémem nabízejícím potřebné kryptografické, souborové a další funkce. Navíc mohou obsahovat nejrůznější bezpečnostní obvody apod.

2.1.4. Druhy karet podle rozhraní

Obrázek 1 Kontaktní čipová karta

Kontaktní čipová karta je karta, která má svůj čip propojen s výstupem na povrch karty. Tento výstup pak musí přijít do přímého kontaktu se zařízením na komunikaci s kartou. Výhodou tohoto druhu karty je bezpečnost a spolehlivost při komunikaci čtecího zařízení s kartou. Z tohoto důvodu také je kontaktní čip vyžadován např. pro karty s elektronickým podpisem. Nevýhodou této karty pak je, že užíváním dochází k opotřebení kontaktů a životnost karty je nižší. Také rychlost komunikace je nižší a operativnost z důvodů nutnosti zasunutí karty mezi kontakty horší.

Obrázek 2 Bezkontaktní čipová karta



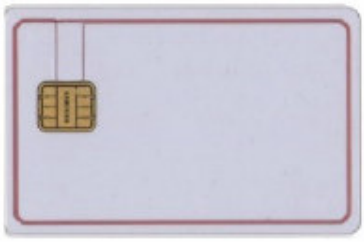
Bezkontaktní čipová karta komunikuje prostřednictvím elektromagnetických vln a není nutno ji zasouvat do čtečky. Karta má uvnitř plastu zalisovanou obvodovou spirálu (anténu), v níž se po přiložení do elektromagnetického pole čtečky indukuje napětí. Tím je pak napájen vlastní čip. Výhodou těchto karet je, že se nemusí zasouvat do čtečky, dokonce mohou pracovat i v ochranném pouzdře, což umožňuje opakované použití. Z toho důvodu jsou tyto karty vhodné pro masovou identifikaci a hojně jsou využívány u dopravních, docházkových a přístupových systémů. Výhodou je i to, že díky bezkontaktnímu pracovnímu režimu lze lépe ochránit čtecí zařízení proti povětrnostním vlivům nebo vandalství.

Kombinované karty sdružují výhody obou předchozích typů. Jde buď o karty hybridní, které v sobě mají umístěny dva oddělené čipy, z nichž jeden je bezkontaktní a druhý kontaktní,

Obrázek 3 Hybridní karta

nebo je to karta duální, která obsahuje pouze jediný čip, ale ten může komunikovat jak bezkontaktním, tak kontaktním způsobem.

Obrázek 4 Duální karta



Duální karty se v karetních systémech v ČR prakticky nevyskytují. Hybridní karty však poskytují skvělé možnosti kombinovaného využití dvou druhů čipů na jednom médiu. Při dodržení požadovaných parametrů jsou však v současné době jejich ceny relativně vysoké (řádově desetinásobek ceny standardní bezkontaktní čipové karty).

2.1.5. Výběr vhodné karty

Pro multifunkční použití čipové karty v městském prostředí je vhodné vybrat kartu, která na jedné straně zajistí dostatečnou bezpečnost jednotlivých operací, na druhé straně umožní opakované užívání karty v dlouhodobějším výhledu. Z tohoto hlediska je nejvhodnější pro městskou kartu využití mikroprocesorové bezkontaktní čipové karty. Kromě výše uvedených norem pro čipové karty se speciálně bezkontaktním kartám věnuje norma ISO/IEC 14443, která stanovuje základní vlastnosti – operační podmínky, komunikační vlastnosti, odolnost apod. Na světě nejrozšířenější v této skupině jsou karty s čipem firmy PHILIPS s typovým označením MIFARE.

2.1.6. MIFARE karty

MIFARE karty jsou vnímány jako průmyslový standard bezkontaktních a duálních karet. Již v roce 2000 byl podíl MIFARE karet více než 85% mezi všemi emitovanými bezkontaktními kartami na světě a v současnosti je užíváno přes 200 milionů karet základní řady MIFARE Standard.

MIFARE Standard je bezkontaktní karta s paměťovým čipem o kapacitě 1 kB, který pracuje na frekvenci 13,56 MHz. Čip je rozdělen do 16 sektorů, z nichž každý s výjimkou prvního, který nese informaci o výrobci a číslo karty, může být využit pro jinou aplikaci. Rychlost datového přenosu je 106 kbit/s, což v praxi znamená, že operace jsou prováděny řádově v desítkách milisekund. Životnost karty bývá udávána 10 let a čip by měl snést 100.000 zápisových operací. Jde o kartu s dostatečnou kapacitou i odolností a s dostupnými pořizovacími náklady (do 30,- Kč bez DPH za kartu). Bezpečnost dat na kartě je zajištěna tím, že ke každému sektoru na čipu existuje sada dvou druhů bezpečnostních klíčů (číselných kódů), z nichž jedny klíče jsou určeny pro čtení a druhé pro zápis. Vlastní data v paměti jsou pak ukládána šifrovaně a bez znalosti těchto klíčů nelze k datům přistoupit. Další sada bezpečnostních klíčů pak zajišťuje nedostupnost adresářové struktury čipu nežádoucím zařízením. Tato karta je pro své ideální vlastnosti nejrozšířenější ve stávajících karetních systémech. Firma PHILIPS vyvinula později rozšířenou podobu této karty s větší pamětí – 4 kB. Vlastnosti této karty jsou velmi podobné. K dispozici je na ní však 32 sektorů po 16 B nebo 8 sektorů po 256 B. Cena těchto karet je prakticky totožná s cenou karet 1 kB.

MIFARE Ultralight je zjednodušená obdoba Standard karty. Její čip má pouze poloviční kapacitu. Také materiálem pro výrobu karty nemusí být v tomto případě plast a karta z cenových důvodů může být zhotovena pouze z tvrzeného papíru. Protože se však tato karta příliš neujala a její výroba je spíše výjimkou, je cenový rozdíl oproti plastovým kartám, který měl původně vyvážit omezené vlastnosti, zanedbatelný. MIFARE DESFire je nová řada bezkontaktních karet firmy PHILIPS. Původem je osvědčená řada Standard, ale čip již obsahuje aktivní mikroprocesor a operace jen s pamětí jsou nahrazeny příkazy orientačně obdobnými příkazům BIOS počítače. Karty se vyrábí s kapacitou 2, 4 a 8 kB. Operační frekvence zůstala na 13,56 MHz, rychlost datového přenosu se však výrazně zvýšila (může dosahovat až 848 kbit/s). Také organizace dat již není omezena na pevně dané sektory, ale datová struktura odpovídá jednodušší formě souborového systému. Na kartě může být uloženo 28 různých aplikací a každá z nich může obsahovat až 32 souborů. Velikost každého souboru je definována v okamžiku jeho vytváření. U této karty je kladen vysoký důraz na bezpečnost prováděných operací i uložených dat. Kromě jiného tato karta umožňuje i funkce ověření pomocí PIN kódu. Cena karty DESFire 4 kB se pohybuje kolem 50,- Kč (bez DPH), cena karet DESFire 8 kB pak kolem 100,- Kč (bez DPH). Kompatibilita karet MIFARE je možná pouze zpětně – tedy na novějším zařízení lze číst karty staršího typu. Na čtečce karet MIFARE DESFire bude možno bez problémů číst a zpracovávat i karty MIFARE Standard.

Starší čtečky karet MIFARE Standard však nejsou schopny pracovat s novými DESFire kartami.

2.1.7. Bezpečnost systémů bezkontaktních čipových karet

Bezpečnost systémů bezkontaktních čipových karet musí odpovídat současným požadavkům. Hlavním cílem zabezpečení je, aby data ukládaná v paměti karty byla zabezpečena proti neoprávněnému vyčtení a neoprávněné modifikaci, a zároveň aby existovaly mechanismy kontrolující integritu a neporušenost uložených dat.

2.1.8. Přístupové klíče

Pod pojmem přístupový klíč bývá převážně rozuměno kódovací číslo, jehož prostřednictvím je aktivován proces práce s daty v paměti čipové karty. Čipy použité v čipových kartách mají vlastní logiku, která umožní ověřit oprávněnost přístupu k datům na základě zadaného přístupového klíče. Přístup k datům je povolen dle typu klíče na různé úrovni, která umožní akci, nebo kombinaci akcí na úrovni „čtení“, „zápis“, „snížení hodnoty číselných dat“, „navýšení hodnoty číselných dat“, nebo „změna přístupových oprávnění“. Přístupové klíče mají u různých mikroprocesorů různou délku a možnost použití. Karty MIFARE Standard používají 2 přístupové klíče o délce 48 bitů přiřaditelné ke každé aplikaci. MIFARE DESFire mohou využít až 14 různých uživatelsky definovatelných klíčů o délce 128 bitů, které se přiřazují jednotlivým souborům v aplikaci.

2.1.9. SAM moduly

Funkčnost přístupových klíčů je závislá kromě jiného na jejich utajení. Čtecí zařízení pracující s pamětí čipové karty musí mít přístupové klíče k dispozici. To lze zajistit tak, že do zařízení vloží klíče přímo výrobce. Není však z bezpečnostního hlediska žádoucí sdělovat každému výrobci zařízení kompletní klíčové sady. Vhodnějším řešením je proto využití tzv. SAM modulů (Secure Access Module), v kterých jsou sady přístupových klíčů uloženy. Jde o kontaktní čipové karty dle standardu ISO 7816 (obdoba SIM karty v mobilním telefonu), které jsou konstruovány tak, aby do nich bylo možno přístupové klíče uložit, ale nebylo možno je vyčíst. Čtecí zařízení pak při načítání karty využívá přímo SAM modul k navázání spojení s čipem karty. SAM modul může obsahovat kromě klíčů také algoritmy elektronických podpisů, kryptování dat apod. SAM moduly lze použít jak pro vozidlové odbavovací systémy jednotlivých dopravců, tak i pro místa akceptující platby z elektronické peněženky.

2.1.10. Digitální podpis

Digitální podpis, který zajišťuje nepopiratelnost a integritu dat, je zpravidla řešen jako kontrolní součet paměťových buněk čipové karty, jež obsahují data. S ukládanými daty je proveden speciální algoritmus, jehož výsledek se uloží na kartu do určeného datového prostoru. Při následném čtení dat je pak proveden výpočet stejným algoritmem, a pokud vyjde správný výsledek, má se za to, že data nebyla neoprávněně modifikována, ani nevznikla chyba při jejich ukládání, jak je uvedeno v literatuře [1].

2.1.11. Kryptování dat

Data ukládaná do paměti čipové karty mohou být kryptována (šifrována). Jde o rozšiřující bezpečnostní prvek, který zajistí, že i v případě prolomení přístupových klíčů nebude možno pracovat s daty na kartě bez znalosti dešifrovací procedury. U karet MIFARE Standard může kryptografickou funkci plnit SAM modul.

2.1.12. Městská karta v ČR

Městská čipová karta na sobě má zpravidla vytištěny markanty jednoznačně identifikující jejího držitele, nejpoužívanější je jméno a příjmení, fotografie a dále číslo karty jedinečné pro daný systém. To je takzvaný nepřenosný typ karty, v systému evidovaný na jejího držitele. Vedle těchto karet existují zpravidla ve všech systémech karty přenosné, kde jediným markantem je jedinečné číslo karty v systému, který ji vydal.

Lze říci, že všechny karty používané v systémech městských čipových karet mají prapůvod u výrobce Philips Semiconductors. Dnes se jedná o společnost NXP která projekt výroby a rozvoje těchto karet převzala. Jedná se technologicky o dva standardy, které se dále dělí. Je to jednak Mifare Standard podle ISO/ IEC 14443 typ A a dále typ DESfire. V obou případech jde o velmi cenově výhodné karty vhodné pro nasazení v dopravních a městských systémech. Je třeba zdůraznit, že pro potřeby této práce se zabýváme pouze typy v současné době aktivně používanými v pro nás relevantních systémech na našem území. Škála typů bezkontaktních karet je daleko širší, a to i v portfoliu firmy NXP. Tyto karty si však svoji cestu na český trh nenašly buď z důvodů cenových, nebo technologických.

2.2. Karty Mifare standard 1kByte a 4kByte

Karty s čipem Philips Mifare standard svým rozšířením více než 200 milionů karet pokrývají cca 80% trhu s bezkontaktními kartami a byly použity ve velkých projektech v oblasti veřejné dopravy v metropolích jako Soul, Londýn, Beijing, apod. V ČR jsou základem pro systém Plzeňské karty a pro systém Karty integrované dopravy a služeb měst Mostu a Litvínova, dále

pro širokou škálu dopravců v linkové dopravě, například pro systém integrované dopravy Středočeského kraje.

Každá karta má jednoznačné nesmazatelné identifikační číslo dané výrobcem (4 bytes – přes 4 miliardy kombinací), kterým bude v celém systému identifikována. V paměti karty jsou kromě dalších dat uložena základní data o držiteli.

Fotografie, jméno a příjmení držitele karty jsou v případě personifikovaných karet natištěny na kartě a to nesmazatelným způsobem.

Karty umožňují až 100 000 cyklů záznamů a bezkontaktní způsob transakce, kdy stačí kartu pouze přiblížit ke čtecímu zařízení, zabezpečuje její vysokou životnost. Tím je možno její pořizovací hodnotu rozpočítat na delší časové období.

Karta je optimalizována pro potřeby co nejrychlejšího odbavení a celá transakce může být kratší než 100 ms.

Disponují paměťovým prostorem 1 kByte nebo 4kByte, který je rozdělen do zabezpečených sektorů a umožňuje tak snadnou implementaci více aplikací, včetně elektronické peněženky. Šifrovaný bezkontaktní přístup (čtení i zápis) k jednotlivým sektorům je zabezpečen dvěma různými klíči a u každého klíče lze nadefinovat povolené operace s daty v jednotlivých blocích.

Vnitřní architektura karet

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 VF modulátor a demodulátor, zdroj kmitočtu a napěťový regulátor.

V bloku označeném Digital Control Unit je mikroprocesorová jednotka se speciálními obvody:

- pro řešení kolizí při detekci více karet v dosahu jednoho přijímače (Anticollision)
- třístupňovou bezpečnostní autentizaci karty (Authentication)
- kryptografickým procesorem, který zrychluje šifrovací operace (Crypto)
- jádro mikroprocesoru a jednotka pro podporu aritmetických operací (Control &ALU), které se využívají pro funkce elektronické peněženky
- rozhraní na elektricky přepisovatelnou paměť

Blok elektronicky přepisovatelné 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.

Tabulka 1 Základní parametry Mifare Standard 1kByte a 4kByte

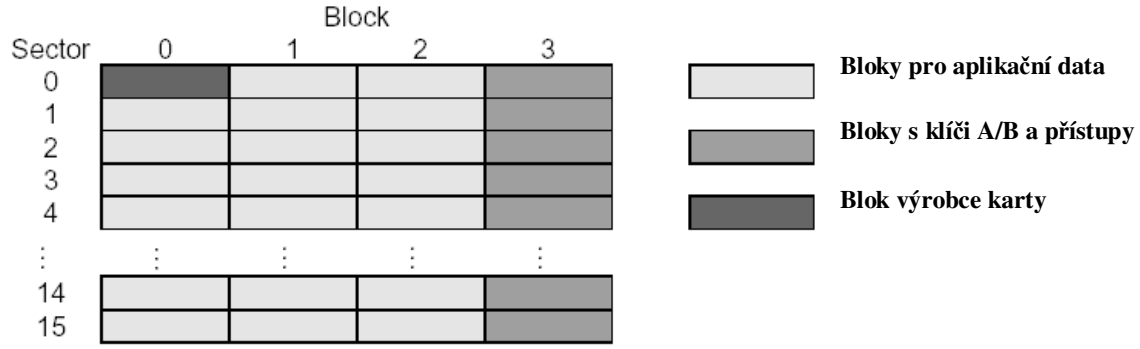
Čip	Philips Semiconductors Mifare Standard
Norma	ISO 14443-2 type A
Provozní frekvence	13,56 MHz
Přenosová rychlost	106 kBaud
Paměť	1 kByt EEPROM - 16 sektorů po 4 blocích nebo 4kByt EEPROM - 32 sektorů po 4 blocích a 8 sektorů po 16 blocích
Rozměry	85,6 x 54,0 x 0,76 mm - ISO 7816/ ISO 7810 ID-1
Provozní teplota	-20°C až + 50°C
Teplota skladování	-20°C až + 50°C
Materiál	PVC (alternativně polykarbonát)
Povrch	bílý, matný
Provozní vzdálenost	až 100 mm
Počet záznamů	100 000 cyklů
Zachování záznamů v paměti	10 let
Napájení	bezkontaktní přenos energie

Zdroj(http://mifare.net/products/smartcardics/mifare_standard1k.asp)

2.2.1. Rozdělení paměti Mifare Standard 1kByte

Karta má interní elektronicky přepisovatelnou pamět EEPROM rozdělenou do 16 sektorů po 4 blocích a do každého bloku je možné uložit 16 znaků. Z každého sektoru jsou nicméně pro vlastní aplikační data použitelné pouze 3 bloky. Poslední čtvrtý sektor je vždy rezervován pro uložení přístupových klíčů A a B spolu s informacemi definující povolené operace s daty v jednotlivých blocích(tabulky byly zpracovány s využitím datasheetů pro verzi 4 kByte) :

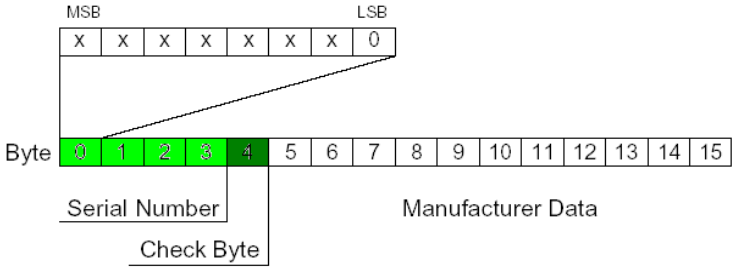
Obrázek 5 Rozdělení paměti na kartě do sektorů a bloků



Zdroj(http://www.ibtechnology.co.uk/PDF/Mifare_classic4k.pdf)

Blok výrobce karty – Sektor 0 má první blok (blok 0) vyhrazen pro údaje výrobce. Struktura 16 bytů tohoto bloku je uvedena na následujícím obrázku:

Obrázek 6 Struktura prvního bloku nultého sektoru



Zdroj(http://www.ibtechnology.co.uk/PDF/Mifare_classic4k.pdf)

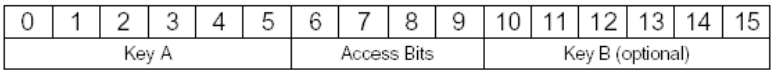
V prvních 4 bytech je uvedeno unikátní sériové číslo karty. Pro kontrolu následuje kontrolní součet tohoto čísla. Ostatních 11 bytů je specifických podle konkrétního výrobce.

Bloky MAD – Sektor 0 má dále blok 1 a 2 vyhrazen pro vytvoření adresářové struktury (viz další kapitola)

Bloky pro aplikační data – u každého bloku lze z aplikačního hlediska nastavit dva typy chování. Jednak prostý zápis/čtení 16 bytů dat např. pro uložení identifikačních dat uživatele nebo pro uložení časového kupónu. Pro účely např. elektronické peněženky lze nastavit u vybraných bloků tzv.inkrementální/dekrementální mód, kdy karta dostane informaci o kolik má údaj v daném bloku zvýšit nebo snížit. Nastavení typu se provádí ve čtvrtém bloku sektoru (viz. obrázek 7).

Bloky s klíči A/B a řízení přístupů – rozložení dat v čtvrtém bloku, který je u všech sektorů rezervován pro uložení přístupových klíčů A a B spolu s informacemi definujícími povolené operace s daty v jednotlivých blocích.

Obrázek 7 Rozložení přístupových klíčů



Zdroj(http://www.ibtechnology.co.uk/PDF/Mifare_classic4k.pdf)

Bitové pole „Access Bits“ určuje pro jednotlivé aplikační bloky 0 až 2 jednak základní typ chování bloku (prostý zápis/čtení nebo Inkrement/Dekrement operace). Dále definuje jaký klíč (A nebo B) je třeba k provedení čtecí a nebo zapisovací operace a zda jsou takové operace povolené.

2.2.2. Rozdělení paměti Mifare Standard 4kByte

Rozdělení paměti na této kartě je prakticky stejné jako u předcházejícího typu a to z důvodu vzájemné kompatibility. Prakticky jediný rozdíl je v tom, že větší paměťový prostor je organizován v 32 sektorech se 4 bloky a 8 sektorech s 16 bloky (1 blok = 16 bytes).

2.2.3. Specifikace adresářových struktur

Struktura karet má být správně nadefinována podle specifikace MAD – Mifare Application Directory. Podobně jako u disket a pevných disků je na začátku karty (Sektor 0, Blok 1 a 2) zavedena adresářová struktura, která spravuje přidělování a odebírání sektorů karty pro jednotlivé aplikace. Aplikace se mohou obracet na kartu s požadavkem na transakci, aniž by znaly konkrétní umístění aplikace v sektorech. Podobně jako na discích se aplikace podívají do MAD adresáře karty a podle identifikátoru karty naleznou potřebné sektory. Toto je velmi výhodné, pokud očekáváme různý počet aplikací na jedné kartě u jednotlivých uživatelů a nahrávaných na kartu v různém pořadí. Aplikacím to velmi zjednoduší komunikaci s kartou a prohlédávání všech sektorů.

Existují dvě verze struktur Mifare karty dle specifikace MAD (verze 1 pro karty 1kB, verze 2 pro karty 4kB). Verze jsou navzájem kompatibilní. Následující seznam popisuje základní vlastnosti MAD struktury:

- dynamické rozmístění jedné nebo několika aplikací na kartě
- označení nevyužitých sektorů (sektorů, k nimž nejsou známy klíče, např. po vymazání aplikace z MAD)

- centrálně mezinárodně přidělované AID (identifikační číslo aplikace), zdarma po odeslání registračního formuláře aplikace
- čtení MAD struktury je povoleno obecně známým klíčem A, tedy seznam aplikací a verzi struktury MAD na kartě si můžou přečíst všichni
- zápis do MAD, zejména přidělování sektorů aplikacím, je umožněno klíčem B a je plně v režii vydavatele karty
- základní údaje o držiteli karty (jméno, příjmení, specifický údaj vydavatele karty) jsou společné všem aplikacím
- čtení údajů o držiteli karty je možné buď pomocí všeobecně známých klíčů A, nebo pomocí neveřejných klíčů (A nebo B), které vydavatel karty zveřejní jen provozovatelům aplikací na dané kartě
- místo na kartě vyhrazené pro jednu aplikaci nemusí být souvislé, může vyplňovat volné místo po jiných aplikacích
- vlastník Info sektoru dle MAD struktury je považován za vydavatele karty. Podle AID přiřazeného tomuto sektoru je možno zjistit u organizace přidělující AID kontaktní údaje na vydavatele. Vydavatel karty by měl mít zaregistrovánu alespoň jednu aplikaci.

V bloku 3 sektoru 0 je uložena informace o použití a nastavení MAD struktury pro konkrétní kartu.

Rozložení MAD v blocích 1 a 2 je uvedeno na následujícím obrázku ze standardu Mifare:

Obrázek 8 Rozložení MAD v blocích 1 a 2

byte 14		byte 12		byte 10		byte 8		byte 6		byte 4		byte 2		byte 0	
m	a	n	u	f	a	c	t	u	r	e	r	c	o	d	e
AID sector	for 7	AID sector	for 6	AID sector	for 5	AID sector	for 4	AID sector	for 3	AID sector	for 2	AID sector	for 1	infc	CRC
AID sector	for $F	AID sector	for $E	AID sector	for $D	AID sector	for $C	AID sector	for $B	AID sector	for $A	AID sector	for 9	AID sector	for 8
s	e	c	t	o	r		t	r	a	i	l	e	r		0

Zdroj(http://www.ibtechnology.co.uk/PDF/Mifare_classic4k.pdf)

Spolu s kontrolním součtem a Info bytem je v něm vidět možnost rozložení AID pro různé sektory. Například, pokud aplikace požaduje z karty údaje o držiteli, zadá AID 0x0004 a v MAD získá adresu konkrétního sektoru, kde je tato aplikace uložena.

2.2.4. Bezpečnostní prvky karet

V kartách jsou 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 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 paměti karty při transportu od výrobce čipu pouze na oprávněné odběratele, vybavené odpovídajícím klíčem

Integrita dat při přenosu je zajištěna následujícím způsobem:

- kontrolní suma 16 bitů 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)

2.3. Karty DESfire 4kByte a 8kByte

Karty tohoto typu jsou technickými nástupci karet Mifare. Jedná se o shodného výrobce a snahu posílit jak užitné vlastnosti, tak bezpečnost řešení. V případě DESfire karty se jedná o procesorovou bezkontaktní kartu vybavenou zabezpečovacím 3DES algoritmem. Odsud pramení první část názvu. Druhá část názvu v sobě obsahuje anglické slovo FIRE a je zkratkou pro čtyři slova – Fast (rychlá), Innovative (inovační,progresivní), Reliable(spolehlivá) a sEcure (bezpečná). V ČR postupně nahrazují dožívající systémy založené na kratách Mifare zpravidla ještě s proprietární strukturou nebo, a to nejčastěji, tvoří základ pro nově budované systémy kde investoři příznivě vyhodnotili marketingově dobře podané výhody standardu DESfire. Dva nejmasivnější systémy v naší republice jsou zcela jistě IN- karta Českých drah a pražská OPEN- CARD. Dále je například používána v systému Liberecké OPUS- CARD (už sám název napovídá o budoucí snaze vydavatele dosáhnout kompatibility s kartou pražskou, dále například dopravce CONNEX Morava, plánovaná Moravskoslezská karta atd.

Každá karta má jednoznačné nesmazatelné identifikační číslo dané výrobcem o délce 56 bitů, kterým je v systémech, které ji akceptují identifikována. V paměti karty jsou stejně jako u standardu MIFARE uložena základní data o držiteli.

Fotografie, jméno a příjmení držitele karty je v případě personifikované karty opět natištěno přímo na její plastové tělo buď specializovanými tiskárnami u vydavatele karty, nebo jako v případě Českých drah ve státní tiskárně cenin.
Karty opět umožňují až 100 000 cyklů záznamů a bezkontaktní způsob transakce.
Přestože je snaha optimalizovat procesy uvnitř karty a dosáhnout s kartou co nejrychlejší transakce, projevilo se složitější a bezpečnější šifrování jak na straně karty, tak na straně čtecích zařízení mírným nárůstem transakční doby, kdy je již udáváno na jednu transakci 105 ms.. I tato délka je v optimalizované sestavě čtecího zařízení. Nevhodným použitím SAM modulů s JAVA appletem už bylo prokázáno, že transakční doba se v tomto případě může prodloužit až o násobky udávané doby. Reálným nebezpečím se pak stává takzvané „utržení transakce“ kdy je karta během probíhající transakce oddálena od čtecího zařízení a transakce je v důsledku toho přerušena.
Karty DESFire disponují paměťovým prostorem 4kByte nebo 8kByte, kde již není použito rozdělení do sektorů jako u předchozího typu MIFARE, ale operace s pamětí jsou nahrazeny příkazy obdobnými příkazům BIOS běžného PC. Aplikace jsou tedy na kartu ukládány „souborově“, kdy každý soubor zabere potřebné místo v paměti. V důsledku této úpravy klesla využitelnost paměti asi o 20% oproti typu MIFARE standard.
Šifrovaný bezkontaktní přístup (čtení i zápis) k jednotlivým aplikacím je zabezpečen až 14 různými klíči pro jednu aplikaci, opět s možností volit rozdílný klíč pro čtení z aplikace a rozdílný pro zápis hodnot do aplikace. Za použití takzvaného master klíče je možno omezit prostor pro jednotlivé aplikace z důvodu řízení využití prostoru na kartě. Vydavatelem karty je pak předán příslušný klíč provozovateli aplikace, který si za pomoci tohoto klíče obhospodařuje jemu přidělený prostor na kartě a řídí i klíčové hospodářství ve vztahu k této aplikaci.
Vnitřní architektura karet
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 VF modulátor a demodulátor, zdroj kmitočtu a napěťový regulátor.

V bloku označeném Digital Control Unit je mikroprocesorová jednotka se speciálními obvody:

- pro řešení kolizí při detekci více karet v dosahu jednoho přijímače (Anticollision)
- třístupňovou bezpečnostní autentizaci karty (Authentication)
- jádro mikroprocesoru a jednotku pro podporu aritmetických operací (Control &ALU), které se využívají pro funkce elektronické peněženky
- rozhraní na elektricky přepisovatelnou paměť

Blok elektronicky přepisovatelné 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.

Tabulka 2 Základní parametry Mifare DESFire

Čip	Philips Semiconductors Mifare DESFire
Norma	ISO 14443-2 type A(plná kompatibilita s komunikačním kanálem) ISO 1443 Part 1 až 4
Provozní frekvence	13,56 MHz
Přenosová rychlost	106 kkbit/s – 424 kbit/s
Paměť	8 kByt EEPROM nebo 4kByt EEPROM (souborový systém)
Rozměry	85,6 x 54,0 x 0,76 mm – ISO 7816/ ISO 7810 ID-1
Provozní teplota	-20°C až + 50°C
Teplota skladování	-20°C až + 50°C
Materiál	PVC (alternativně polykarbonát)
Povrch	bílý, matný
Provozní vzdálenost	až 100 mm
Počet záznamů	100 000 cyklů
Zachování záznamů v paměti	10 let
Napájení	bezkontaktní přenos energie

Zdroj(http://mifare.net/downloads/MIFARE%20DESFire_low%20resolution.pdf)

2.3.1. Rozdělení paměti Mifare DESFire

Karta má interní elektronicky přepisovatelnou paměť EEPROM 4kByte nebo 8kByte. Tato paměť je organizována souborově. Stejně jako u předchozí MIFARE Standard je část paměti rezervována pro údaje výrobce a vydavatele karty. Rezervován je i prostor pro uložení přístupových klíčů. Vzhledem ke změněné organizaci paměti klesla i její využitelnost a to zhruba o dvacet % oproti sektorovému uspořádání.

2.3.2. 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. Čtecí zařízení vyhodnotí kolik odpovědí dostalo, tj. kolik karet je v dosahu. „Antikolizní mechanismus“ vyhodnotí podle unikátního čísla karty jednu z karet a tu osloví, pošle ji příkaz „Výběr“. Ostatní karty pozastaví a tyto musí čekat až na další „Výzvu“. S vybranou kartou zahájí čtecí zařízení 3 stupňovou „Autentizaci“. Tato autentizace se vztahuje přímo ke konkrétní aplikaci(sektoru) karty.

- Po úspěšné autentizaci následují čtecí/zapisovací nebo inkrementální/dekrementální operace. Tyto operace nevyžadují další autentizaci pokud se vztahují ke stejné aplikaci (sektoru) karty. Po ukončení všech požadovaných operací je karta pozastavena a čtecí zařízení opět vysílá „Výzvu“. Toto se odehrává v řádech desetin vteřiny.

2.4. Vzájemné srovnání HW kompatibility

Na tomto místě je třeba udělat souhrn a vyhodnocení z předchozích stránek a vybrat parametry, které zásadním způsobem ovlivňují možnost vzájemné kompatibility po hardwarové stránce:

2.4.1. Typ karty

V předchozích kapitolách bylo konstatováno, že v České republice se užívají v systémech Městských čipových karet a u velkých dopravců dva základní typy karet, viz, příloha č.1. Obě karty jsou podle typu rozhraní bezkontaktní čipové karty a to navíc od stejného výrobce. Následující tabulka srovnává tyto dva typy po hardwarové stránce.

Tabulka 3 Srovnání Mifare Standard a Mifare DESFire

Čip	Philips Semiconductors Mifare Standard	Philips Semiconductors Mifare DESFire
Norma	ISO 14443-2 type A	ISO 14443-2 type A(plná kompatibilita s komunikačním kanálem) ISO 1443 Part 1 až 4
Provozní frekvence	13,56 MHz	13,56 MHz
Přenosová rychlost	106 kBaud	106 kkbit/s – 424 kbit/s
Paměť	1 kByt EEPROM - šestnáct sektorů po 4 blocích nebo 4kByt EEPROM nebo 4kByt EEPROM - 32 sektorů po 4 blocích a 8 sektorů po 16 blocích	8 kByt EEPROM nebo 4kByt EEPROM (souborový systém)
Rozměry	85,6 x 54,0 x 0,76 mm - ISO 7816/ ISO 7810 ID-1	85,6 x 54,0 x 0,76 mm - ISO 7816/ ISO 7810 ID-1
Provozní teplota	-20°C až + 50°C	-20°C až + 50°C
Teplota skladování	-20°C až + 50°C	-20°C až + 50°C
Materiál	PVC (alternativně polykarbonát)	PVC (alternativně polykarbonát)
Povrch	bílý, matný	bílý, matný
Provozní vzdálenost	až 100 mm	až 100 mm
Počet záznamů	100 000 cyklů	100 000 cyklů
Zachování záznamů v paměti	10 let	10 let
Napájení	bezkontaktní přenos energie	bezkontaktní přenos energie

Z tabulky je zřejmé, že typy se liší zejména:

- druhem použitého čipu
- přenosovou rychlostí
- organizací vnitřní paměti

Výrobce u těchto dvou typů karet MIFARE deklaruje takzvanou zpětnou kompatibilitu - tedy na novějším zařízení lze číst karty staršího typu.

Je tedy zřejmé, že pro dosažení vzájemné kompatibility systémů městských čipových karet je klíčové, aby byla navzájem kompatibilní čtecí zařízení těchto karet. Na čtečce karet MIFARE DESFire bude možno bez problémů číst a zpracovávat i karty MIFARE Standard. Starší čtečky karet MIFARE Standard však nejsou schopny pracovat s novými DESFire kartami.

Všichni provozovatelé takových systémů musí mít uvedenou skutečnost neustále na paměti. Pokud jde o novější systémy, nevzniká žádný problém a pořizované čtečky na karty DESFire jsou kompatibilní s ostatními systémy v ČR. Daleko horší situace je u systémů, které jsou dosud provozovány na kartách MIFARE Standard. Tam pro dosažení vzájemné kompatibility je bezpodmínečně nutné pořizovat všechna nová zařízení na standardu DESFire tak, aby při přechodu na modernější kartu nebylo v budoucnu nutné tato zařízení vyměňovat.

3. Aplikační kompatibilita

3.1. Úvod do problematiky

Tato kapitola si klade za cíl zmapovat problematiku aplikací na používaných městských čipových kartách v ČR a vzhledem k tomu, že taková aplikace přináší spotřebitelský užitek pouze v interakci s návaznými aplikacemi, ozřejmit i jejich fungování a vztahy. Systémy městských čipových karet využívají dvou základních principů. Jedním je využití jedinečného ID karty, které je spřaženo v systému s osobními daty držitele karty. Na vlastní čipové kartě pak neleží žádná aplikace a všechna data jsou držena a zpracovávána v systému využívajícím toto ID. Používá se pro něj označení „identifikační funkce karty".

Druhý princip je sofistikovanější a využívá datový prostor na kartě k uložení různých informací. Typickým příkladem takového využití je elektronická peněženka. Dochází k rozsáhlé komunikaci s vnitřním čipem karty, čtení, zápisu a to s sebou přináší rozsáhlejší možnosti využití, ale současně i větší nároky na obslužný software i samotné čtečky těchto karet.

3.2. Popis způsobů využití městských čipových karet

3.2.1. Využití bezkontaktních čipových karet v dopravě

Doprava je základní oblastí využitelnosti technologie čipových karet. Tento fakt dokazuje praxe tím, že čipové technologie do dopravy zavádějí nejen města jako službu občanům, ale zavádějí je i soukromí dopravci, u kterých vedle zkvalitňování služeb hraje značnou roli i otázka efektivity systému. Důvodů, proč právě doprava je pro čipové technologie vhodná, je několik:

- paměť karty je jednoduše a vícenásobně přepisovatelná a poskytuje dostatečnou kapacitu pro uložení potřebných informací pro poskytování přepravních služeb (uložení jízdenek s dlouhodobou platností, uložení záznamů o nároku na slevu apod.)
- cena jízdného se pohybuje v oblasti mikroplateb (tedy částek v řádu korun nebo maximálně několika desítek korun)
- doprava je užívána širokou základnou zákazníků, a tedy poskytuje prostor pro získání významného počtu uživatelů karetního systému
- uložením dat v paměti karty jsou potřebné informace k dispozici i u zařízení, která nejsou on-line napojena na systém (autobusy pohybující se mimo dosah počítačové sítě)
- technologie poskytuje vysokou míru zabezpečení dat

- technologie umožňuje urychlení a zjednodušení odbavení
- systémy související s využíváním čipových technologií poskytují významná statistická data pro možnost optimalizace dopravních služeb

Oblast dopravy bývá pokryta dvěma základními dopravními aplikacemi – využitím paměťové funkce karty převážně pro uložení dlouhodobých časových jízdenek a využitím platební funkce karty (elektronické peněženky).

3.2.2. Elektronická peněženka v dopravě

Elektronická peněženka je nejrozšířenější aplikací užívanou u dopravců. Její přidaná hodnota je dána především s ohledem na cenu jednotlivého jízdného, kdy pro platbu jízdenky cestující převážně potřebuje drobné mince. Výhodnější, než je manipulace s mincemi, je uložit na elektronickou peněženku přiměřený obnos a čerpat jej delší dobu. Jelikož je manipulace s hotovostí méně komfortní i pro řidiče vozidel hromadné přepravy osob, je často podporováno používání elektronické peněženky i tím, že dopravce poskytuje na jízdenky placené elektronicky slevu.

Aby držitel karty využíval svou elektronickou peněženku, je pro něj důležité, aby měl k dispozici jednoduchý a dobře dostupný způsob jejího nabíjení. Z toho důvodu je vyžadováno, aby ve vozech jednotlivých dopravců nebylo možno kartou jen zaplatit, ale aby zde byla též možnost nabíjení elektronické peněženky.

3.2.3. Čipová karta v dopravě jako nosič informace

Prakticky všechny MHD poskytují možnost zakoupit dlouhodobou časovou jízdenku. Časové jízdenky jsou zakotveny v tarifních podmínkách jednotlivých dopravců. Čipová karta, kterou její držitel lehce uloží do kapsy nebo do peněženky je ideální médium pro uchování záznamu o zakoupení dlouhodobé časové jízdenky. Informace uložené na kartě zpravidla obsahují údaj o intervalu časové platnosti (od kdy do kdy), lokální vymezení (např. platnost pro určitou oblast/tarifní zónu) a nároků na slevu (žákovské apod.). Data z karty jsou pak přečtena zařízením u řidiče ve voze příslušného dopravce a na jejich základě zařízení vyhodnotí, zda cestující má nárok na bezplatnou (resp. určitým způsobem zvýhodněnou) přepravu.

Výhodou využití karet pro uložení dlouhodobé časové jízdenky je pro držitele karty jednak možnost dlouhodobějšího plánování (elektronicky lze uložit informaci na kartě s libovolným předstihem a libovolnou platností, pokud to povolují nastavená pravidla), jednak uchránění vynaložených prostředků v případě ztráty (záznam o prodeji předplatného je uložen v systému, a lze jej tedy opakovaně uložit na duplikát ztracené karty).

Výhodou užití paměťových karet pro dopravce jsou jednak využitelná statistická data, jednak kvalitnější možnost kontroly nároků na poskytované slevy a rovněž možnost rozložení odbavování držitelů karet v čase – efektivnější využití odbavovacích míst (cestující nemusí nakupovat předplatné jen na přelomu měsíců, ale mohou navštívit přepážku v předstihu i týdnů).

Někteří dopravci využívají paměťové funkce čipových karet k dočasnému uchování informace o možné slevě. Princip spočívá v tom, že při platbě z elektronické peněženky je na kartu uložen záznam o čase nákupu jízdenky. V případě, že držitel karty nastoupí do jiného vozu téhož dopravce (případně dopravce v rámci integrovaného dopravního systému) do určité doby, je mu poskytnuta určitá sleva na nově zakupovanou jízdenku.

Karta může též sloužit jako nosič informace o nároku na slevu. Předpokladem je, že na kartě jsou uložena základní data o držiteli (jméno, příjmení a datum narození). Strojek dopravce pak dokáže podle data narození určit, zda držitel karty má, či nemá nárok na slevu pramenící z věku (žákovskou, důchodcovskou apod.).

Nárok na slevu pro jednotlivé jízdné lze odvodit i v případě kombinovaného využívání dlouhodobého předplatného a jednotlivého jízdného (např. v případě více tarifních pásem). Jestliže držitel karty cestuje v pásmu, kde nemá zakoupeno dlouhodobé předplatné, ale v jiném tarifním pásmu má předplatné s poskytnutou slevou, lze podle druhu uloženého předplatného odvodit nárok na slevu i při koupi jednotlivého jízdného. Strojek dopravce v takovém případě zkontroluje záznamy o kuponech na kartě, a jestliže nalezne slevový kupon, nabídne slevu i při koupi jednotlivé jízdenky. Čipová karta je paměťové médium a jako takové může uchovávat jakoukoli informaci. Slevové nároky je tedy možno ukládat přímo do paměti karty. V takovém případě je však nutno stanovit dostatečně univerzální pravidla pro záznam slevového nároku včetně způsobu prokazování, aby tyto záznamy nemusely být ukládány pro každého dopravce zvlášť. Bez takto stanovených pravidel nelze predikovat technické řešení podobného druhu poskytování slevy.

Paměťová funkce čipových karet je využívána i při ukládání krátkodobé přestupní jízdenky. Pod pojmem krátkodobá přestupní jízdenka je rozuměn mezistupeň mezi dlouhodobým časovým předplatným a jednorázovou jízdenkou. Zákazníkem pro tyto jízdenky je cestující, který hodlá čerpat přepravní službu více poskytovatelů (dopravců) v rámci limitovaného časového úseku (jedné cesty) - např. využije linkový autobus jednoho dopravce a následně městskou hromadnou dopravu. Karta jako nosič krátkodobé přestupní jízdenky může fungovat ve dvou variantách. Varianty nejsou mezi sebou příliš kombinovány, protože jejich kombinace dává prostor k zneužití systému.

- cestující si zakoupí krátkodobý přestupní lístek prostřednictvím čipové karty. Na kartu je proveden záznam o době platnosti, tj. od kdy do kdy je cestující oprávněn cestovat příslušnou linkou nebo v příslušném tarifním pásmu v rámci krátkodobé přestupní jízdenky. Taková jízdenka může být nahrána na kartu jedna nebo i několik dle zadání tarifních podmínek. Nákup jízdenky probíhá platbou z elektronické peněženky. Na žádost cestujícího je nutno vydat daňový doklad, ale ten neslouží jako jízdenka. Cestující se prokazuje přiložením karty ke strojku v době nástupu do vozu (při přestupu) u řidiče nebo přepravní kontrole, která je vybavena čtečkou čipových karet.
- karta slouží jako elektronická peněženka a jízdním dokladem je vždy vytištěný papírový lístek s údaji o čase platnosti a tarifním pásmu. Na kartě se uchovává v transakčním logu (paměťový prostor pro záznam o provedených platbách z EP) záznam o provedené transakci, ale pro prokázání se vůči přepravní kontrole slouží papírový jízdní doklad.

Výhodou první varianty je kompletní kontrola jak nad pohybem cestujícího (data pro případnou optimalizaci dopravních služeb), tak kontrola nad provedenými úkony dopravce – možnost rozúčtování provedených přepravních úkonů mezi jednotlivé dopravce. Nevýhodou je, že přestupní jízdenka je vázána na kartu (z karty nelze koupit přestupní jízdenku pro spolucestující, kteří chtějí cestovat jinam, než držitel karty).

Výhodou druhé varianty je jednoduchost řešení i možnost nákupu přestupních jízdenek pro spolucestující. Tato varianta má však celou řadu nevýhod - neprůhledný způsob evidence a rozúčtování dopravních úkonů, možnost falsifikace tištěných přestupních jízdenek, chybějící statistická data při přestupu atd.

3.2.4. Využití bezkontaktních čipových karet u samoobslužných zařízení

Vlastnosti bezkontaktních čipových karet jsou ideální pro použití u samoobslužných zařízení. Příkladem takových zařízení jsou parkovací automaty či nápojové nebo stravovací automaty. Výhodou je, že potřebné informace, jež jsou pro samoobslužné zařízení zapotřebí, jsou umístěny přímo v paměti karty, a tedy se zařízení nemusí složitě napojovat na žádný centrální systém při každé operaci, ale postačí dávkové odesílání dat v pravidelných intervalech.

3.2.5. Parkovací automaty

Použití bezkontaktních čipových karet v parkovacích automatech se nabízí jako jedna z nejpřirozenějších forem využití kartového systému. V případě použití části automatů používajících výhradně platby elektronickou peněženkou odpadá nutnost výběru hotovosti z těchto automatů a snižuje se významně i riziko napadení těchto automatů z důvodu krádeže hotovosti. Pro uživatele odpadá nutnost nosit po kapsách drobné nutné pro úhradu v

mincovním parkovacím automatu. Příkladem je zčásti Praha, kde ale není využit způsob zpoplatnění prostřednictvím klasické elektronické peněženky, ale nákupem jisté formy předplatného.

3.2.6. Využití bezkontaktních čipových karet v kultuře a sportu

Vedle dopravy a samoobslužných zařízení je oblast kultury a sportu dalším vhodným místem pro využití čipových technologií. Prolíná se zde potřeba identifikace klienta s placením částek ve výši odpovídající hodnotám vhodným pro uplatnění elektronické peněženky. Navíc lze využít paměťový prostor k uložení informací o předplatném (abonentkách nebo permanentkách).

3.2.7. Využití elektronické peněženky

Oblast kultury, a především pak oblast sportu, je velmi vhodná pro využití elektronické peněženky. Jedním z důvodů je výše plateb, které probíhají v jednotlivých zařízeních (platby v řádu několika desítek korun), druhým pak tendence uživatelů těchto zařízení nenosit na sportoviště peněženku, která může být odcizena. Výhodou v tomto směru je i odolnost čipových karet proti vlhkosti.

3.2.8. Poskytování slev

Čipové karty lze využít v oblasti kultury a sportu pro poskytování slev. Tyto slevy mohou být vázány jednak na zařazení do určité skupiny dle dispozic držitele (věk, snížená pracovní schopnost apod.), jednak na „váženost“ klienta (věrnostní slevy, slevy pro zaměstnance, rezidenty města apod.). Informace o nároku na slevu může být uložena v paměti karty. Vzhledem k různorodosti poskytovatelů služeb v kultuře a sportu však tuto variantu nelze doporučit. Čip karty by byl v takovém případě zaplněn jednoúčelovými daty na úkor smysluplnějšího využití datového prostoru. Pro účel poskytování slev u jednotlivých subjektů je lépe využít pouze identifikační funkci karty a potřebná data o držiteli uložit v interních systémech poskytovatele služby. Samozřejmě lze využít dat, která již na kartách uložena jsou. U slev vázaných na věk držitele lze využít údaje o datu narození. Je-li struktura poskytovaných slev u subjektu nabízejícího službu identická se slevami poskytovanými v dopravě, lze rovněž využít informaci o zakoupeném předplatném kuponu (jestliže se držitel karty musel prokázat při koupi předplatného potvrzením o nároku na slevu, může být platný kupon na kartě akceptován jako potvrzení stejné hodnoty).

3.2.9. Rezervační systémy

V kultuře jsou běžně využívány systémy pro rezervaci vstupenek na jednotlivá představení. Jelikož karta jednoznačně identifikuje svého držitele, lze při vyzvednutí rezervovaných vstupenek této vlastnosti karty využít. Výhodou v takovém případě je pro provozovatele rezervačního systému, že jednotlivé rezervace jsou provedeny s vyšší mírou provázanosti na zákazníka, a lze tak více eliminovat možnost zneužití systému (např. rezervace vstupenek bez snahy o jejich zakoupení).

Rezervační systémy lze velmi dobře kombinovat se systémem platby elektronickou peněženkou.

3.2.10. Využití bezkontaktních čipových karet v oblasti školství

Využitelnost čipové karty ve školství je třeba hledat v aplikacích, u kterých karta funguje jako zjednodušující prvek. Vhodnými aplikacemi jsou:

- stravovací systémy – školní stravování je maximálně vhodné pro použití čipové karty. Lze ji využít pro identifikaci strávníka, kdy strávník se již při objednávání stravy na příslušný den identifikuje vůči systému svojí kartou, a následně při odběru stravy se opět prokáže svojí kartou a je mu vydána objednaná strava. Školy se tak zbavují složité manipulace se stravenkami a mají neustálý přehled jak o stavu objednávek, tak o stavu vydaných jídel. Většina školních jídelen v republice již však systém stravenek opustila a využívají obdobné systémy tak, jak je popsán výše jen s tím rozdílem, že jako identifikátor strávníka vůči systému používají např. kartičky s čárovým kódem nebo formu čipového přívěsku. To nahrává snadnému zavedení čipové karty do školních jídelen, kdy se ke stávajícím čtečkám jen přidají čtečky čipových karet a s minimálními náklady tak vzniká duální systém, který umožní identifikaci oběma typy médií. Další značnou přidanou hodnotu pro tento sektor je možnost využití elektronické peněženky, kdy si strávník může platit stravné přímo pomocí elektronické peněženky.
- přístupové, docházkové systémy – školství je pro aplikaci přístupových systémů zvláště vhodné. Větší školy mají někdy i větší počet využívaných vchodů. K těmto vchodům pak lze umístit čtečky čipové karty a reversní elektrický zámek. Přístup do školy pak lze nadefinovat pro všechny žáky školy a její zaměstnance. Samozřejmostí je možnost nadefinování přístupových časů – žák pak má možnost přístupu pouze v době vyučování, pro pedagogy a ostatní pracovníky je toto oprávnění rozšířeno např. dle instrukcí ředitele školy. Takto lze samozřejmě aplikovat přístupový systém i do větší hloubky, tj. na dveře kabinetů, dveře mezi různými částmi školy, vstup do specializovaných učeben, školní tělocvičny, atd. Lze takto ošetřit například i přístup cizích strávníků do prostor školních stravovacích zařízení,

kdy jednotlivé zámky umožní strávníkovi přístup pouze do prostor jídelny, a strávník tak nemůže vstoupit do jiných částí školy. Stejné čtečky, které jsou používány u přístupových systémů, je možno použít i pro docházkový systém, za pomoci kterého lze evidovat aktuální přítomnost a docházku žactva i personálu. Docházkový systém lze pak snadno propojit se mzdovým softwarem, speciálním školním softwarem pro hodnocení a docházku žáků, vyhodnotit zda už všichni opustili budovu a může dojít k jejímu uzamčení a podobně.

- školní bufety, stravovací a nápojové automaty – platbu z elektronické peněženky lze akceptovat i ve stravovacích a nápojových automatech. Pro žáky tak odpadá nutnost mít u sebe příslušnou hotovost, navíc v drobných mincích. Nepřítomnost hotovosti snižuje riziko drobných krádeží, a zvyšuje možnost kontroly ze strany rodičů o tom, kde jejich dítě peníze utratilo. Standardním prvkem systému zúčtování totiž je i možnost uživatelské kontroly provedených transakcí s jednotlivou kartou. Přijímat platbu z elektronické peněženky může i školní bufet, se stejnými výhodami, jaké jsou popsány u stravovacích a nápojových automatů.
- Elektronická škola – takto lze nazvat systém, kdy karta je plně integrována do systémů školy a lze nasadit aplikace, jež jsou velmi atraktivní z uživatelského hlediska. Dítě přijede do školy MHD (s čipovou kartou jako průkazkou), následně mu stejná karta umožní vstup do školy a zaregistruje ho mezi přítomné žáky. Před začátkem hodiny si z elektronické peněženky zakoupí občerstvení. Pedagog při příchodu do hodiny pohledem na monitor, kde mu červeně svítí na schématu třídy absentující žáci, zkontroluje docházku. Známky jsou zaznamenávány do počítače na účet žáka. V době oběda si žák vyzvedne pomocí čipové karty objednanou stravu. Odtud odejde do tělocvičny, kam ho elektronický zámek vpustí, protože v systému je nastaveno, že jeho třída má tuto hodinu tělocvik a všichni žáci třídy mají povolen vstup do tělocvičny. Před odchodem ze školy si ve školní knihovně vypůjčí za pomoci své čipové karty potřebnou literaturu. Při odchodu ze školy se odhlásí přiložením karty ze systému a odjede MHD opět domů. Rodič si za pomoci osobního hesla přes internet může ráno zkontrolovat, zda dítě dorazilo do školy, jaké má známky, zda si vyzvedlo oběd, atd.

3.2.11. Využití bezkontaktních čipových karet v identifikačních systémech

Model využití městských a regionálních čipových karet v identifikačních systémech různých subjektů poskytuje jejich provozovatelům celou řadu výhod, jak je uvedeno v literatuře [3]. Provozovatelé nemusí vydávat vlastní karty a odpadá tedy pořizování potřebné techniky pro vybavení kartového centra pro každý subjekt zvlášť. Uživatelům systému odpadne nutnost vlastnit několik různých karet. Čipová karta na sobě mívá vytištěnu fotografii držitele, jméno a příjmení. Těmito údaji je držitel dostatečně přesně identifikován. Kdyby ani tato data

nestačila, lze je doplnit datem narození případně dalšími údaji, které jsou uloženy v čipu karty.

3.2.12. Systémy přístupové kontroly

Kontrola přístupu pomocí čipové karty jako identifikátoru klade důraz na dokonalou technickou identifikaci osoby před povolením přístupu k prostorám nebo použití technického zařízení. Identifikace osoby kartou může být ještě doplněna prvkem biometrického parametru osoby (otisk prstu, vzorek sítnice,…) nebo požadavkem na zadání PIN (s těmito údaji se však zpravidla nepočítá na kartě a příslušný systém je musí mít uloženy ve vlastních databázích). Při přístupové kontrole bývá důsledně řešena mechanická zábrana vstupu: bezpečnostní provedení turniketů, systém propojených dvojích dveří, apod. Za pozornost stojí možnosti nastavení parametrů systému, přidělení přístupových práv a jejich operativní změny. Pomocí těchto systémů lze ovládat jak motorovou vložku, elektronického vrátného tak i závory, garážová vrata a turniketové závory (například lyžařských vleků).

3.2.13. Systém vstupní kontroly a docházkový systém

Vstupní kontrola znamená kontrolu přicházejících osob do objektu nebo areálu na základě předložení identifikačního průkazu – v tomto případě čipové karty. Vstupní prostor je obvykle kombinován se systémem přístupové kontroly a bývá vybaven dalšími technickými prostředky – turnikety, dveře s elektrickým zámkem, vrata nebo závory. Systém vstupní kontroly prověřuje oprávněnost ke vstupu, především ale eviduje a archivuje údaje (aktuální i historické) o příchodech, odchodech či přítomnosti osob ve vymezeném prostoru. Evidence pracovní doby je nadstavbou systémů vstupní kontroly z pohledu právních předpisů a firemních požadavků na kontrolu pracovní doby. Navazuje na organizaci a přípravu mzdové agendy a programové vybavení je provedeno v různém rozsahu od prosté evidence pracovní doby (příchody, odchody, bilance), až po podklady pro výpočet mezd (rozlišení standardních a nestandardních příchodů a odchodů z pohledu začlenění do pracovní doby).

3.2.14. Systémy kontroly vjezdu

Systémy kontroly vjezdu a parkovací systémy využívají identifikačních možností karty pro řízení vjezdu pro auta. Identifikátor – karta - může být přiřazen řidiči nebo autu, případně je kontrolováno obojí. Mechanickou zábranou jsou automatické závory (nebo vrata) ovládané systémem. Parkovací systémy kromě kontroly vjezdu a výjezdu evidují čas příjezdu a odjezdu, obsazenost parkovacích míst. Samozřejmostí by měla být možnost úhrady parkovného z elektronické peněženky.

3.2.15. Knihovní systémy

Využití čipové karty jako průkazu čtenáře poskytuje hned několik výhod. Karta je personifikována fotografií, a tedy hůře zneužitelná, čtenáři postačuje jedna karta pro dopravu i pro vypůjčení knih, z elektronické peněženky karty lze hradit všechny poplatky spojené s knihovními službami bezhotovostně.

3.2.16. Využití čipových karet v oblasti veřejné správy a E-GOVERNMENTU

Významnou vlastností čipových karet v oblasti veřejné správy a tzv. E-GOVERNMENTU je možnost rychlé a jednoznačné identifikace držitele karty. V této oblasti však nebývá dostatečné se prokázat prostým přiložením bezkontaktní karty na čtečku, ale je nutno tuto identifikaci doplnit o zadávání PIN nebo jinou další autorizací. Stávající normy rovněž v některých případech vyžadují kontaktní spojení čtecího zařízení s čipem karty, a tedy nelze akceptovat bezkontaktní čipovou kartu, jak je uvedeno v literatuře [1]. Pro tyto případy existuje řešení v podobě hybridních čipových karet.

3.2.17. Karta jako identifikátor občana (např. pro rychlý přístup k jeho dokumentaci)

Každá bezkontaktní čipová karta má svoje jedinečné ID (identifikační číslo). Z karty lze dále při znalosti čtecích klíčů načíst další údaje o držiteli. Pokud by se už ve vyvolávacím systému občan identifikoval svojí čipovou kartou, pak úředník, který ho bude odbavovat, již dopředu ví, kdo se ocitne na druhé straně jednacího stolu. Současně počítačový systém dopředu připraví a upozorní úředníka na agendu, kterou má občan na úřadě v běhu. Tento proces přispěje ke zrychlení odbavení a zároveň výrazně zvyšuje komfort pro občana.

3.2.18. Karta v přístupovém systému občan – úředník

Při použití bezkontaktní čipové karty ve vyvolávacím systému lze nastavit elektronické zámky tak, že občan, který se ve vyvolávacím systému identifikoval za pomoci čipové karty, projde soustavou elektrických zámků pouze k úředníkovi, u nějž je připravena k vyřízení jeho agenda. Zamezí se tak nekontrolovanému pohybu osob po úřadě, a tím se sníží například i riziko drobných krádeží.

3.2.19. Karta jako elektronická peněženka pro poplatky přímo u úředníka

Elektronická peněženka čipové karty může sloužit i pro placení drobných správních poplatků přímo u úředníka. Odpadá tím manipulace s hotovostí a značně se zvyšuje komfort pro občana.

3.2.20. Využití bezkontaktních čipových karet v oblasti turistického ruchu

Funkce čipových karet v oblasti turistického ruchu může být standardní, nebo specializovaná. Standardními funkcemi jsou např. využití elektronické peněženky na kartě, využití karty v dopravě jako nosič dlouhodobého předplatného či přestupní jízdenky apod. Specializované funkce jsou takové, které karta plní pouze v daném oboru.

3.2.21. Standardní funkce karet v turistickém ruchu

Každá karta, která je zavedena do centrálního systému, může plnit všechny úkoly, které systém s kartou dokáže provozovat. Zvláštností je pouze způsob distribuce karet a poskytování záruk. Jestliže má být karta dána k dispozici krátkodobému jednorázovému uživateli (turistovi), je nutno zkrátit na minimum cestu karty k zákazníkovi – není vhodné nutit tyto zákazníky absolvovat kompletní proceduru vyplňování žádosti o kartu apod. Vhodnější je připravit kartu s již nastavenými funkcemi a v bezpečném obalu ji nabízet v síti prodejen s co nejdelší otevírací dobou a co nejlepší dostupností (vhodná je např. síť trafik). Karta v takovém případě není přidělena zákazníkovi na jméno (nenese identifikační prvky držitele), a tedy i její použití je omezeno jen na takové funkce, které nevyžadují plnou identifikaci klienta (např. elektronická peněženka).

3.2.22. Turistická karta

Turistické karty jsou ve větších městech nebo regionech prostředkem k posílení a podpoře turistického ruchu. Jejich úkolem je podat návštěvníkům města a regionu potřebné informace o místech vhodných k návštěvě, o otevíracích dobách a cenách. Pro motivaci turistů k návštěvě určitých míst nebo čerpání služeb bývá k dispozici soubor slevových kuponů. Návštěvníkovi je prostřednictvím Turistické karty dáván podnět k delšímu setrvání v regionu či díky zpříjemnění pobytu důvod k návratu do regionu.

3.2.23. Kobrendované karty

Pod pojmem „kobrendovaná karta“ je rozuměno funkční spojení dvou druhů karet. Většinou se toto spojení týká dvou druhů karet (převážně různých vydavatelů), z nichž každá má stěžejní funkcionality postaveny na jiném prvku – např. karta s čistě vizuální identifikační funkcí a karta čipová s primárními funkcemi uloženými v čipu karty. Spojením těchto karet do jedné vznikne nový produkt, který poskytuje plnohodnotné služby obou druhů karet současně.

S emisemi kobrendovaných karet jsou většinou spojeny dvě komplikace

– problematika vydavatele karty – jeden z vydavatelů původně oddělených karet ztrácí plnou kontrolu nad svým vlastním produktem

– problematika poskytování záruky – jak se zachovat ke kartě, jejíž jedna část je plně funkční, zatímco druhá nefunguje

3.3. Popis základního systému městské čipové karty

Aby systém městské čipové karty mohl začít fungovat musí být vytvořen systém, který bude schopen kartu vyrobit (naprogramovat, napersonifikovat). Tím je takzvané Kartové centrum. Úkolem tohoto centra je vedle vlastní výroby karet také uchovávat informace o jednotlivých držitelích karty, archivovat žádosti o karty, zhotovovat duplikáty karet v případě ztráty nebo nefunkčnosti, vytvářet seznam zakázaných karet (BlackList) apod. Abychom mohli začít uvažovat nad vzájemným propojením dvou nebo více systémů městských karet je nutné zhruba definovat popis takového fungování jednotlivého systému.

3.3.1. Popis Kartového centra

Základem Kartového centra je databázový systém, v němž jsou všichni držitelé karet registrováni společně s informacemi o veškerých vydaných kartách, které byly v systému vytvořeny. Nad daty centra funguje aplikace, která zajistí potisk karet na speciálních tiskárnách. Zároveň tato aplikace zajistí naformátování potřebných paměťových oblastí v čipu karty a nastavení elektronických bezpečnostních prvků. Systém Kartového centra dále vytváří účetní a statistické sestavy, které slouží ke kontrolním nebo optimalizačním procesům.

3.3.2. Odbavovací systém Kartového centra

Odbavovací systém může být buď samostatná aplikace, nebo součást Kartového centra. Jeho úkolem je provádět základní operace jaké bývají po kartě vyžadovány – nahrávání časových jízdenek, nabíjení elektronické peněženky na kartě, případně práce s dalšími aplikacemi, jsou-li na Kartě uloženy. Vzhledem k tomu, že odbavovací systém využívá databází Kartového centra, využívá se spojení obou systémů do jednoho. Výhoda tohoto řešení je i v tom, že je spravována pouze jedna aplikace pro výrobu i práci s kartami.

3.3.3. Vybavení modelového Kartového centra městské karty

Kartové centrum může být tvořeno tvořeno několika základními prvky:

- datová a systémová základna
- personifikační pracoviště
- archiv žádostí

Datová a systémová základna je společná pro celý systém městské čipové karty, proto musí být dimenzována na předpokládanou kapacitu klientů. Zde je uloženo vlastní programové jádro celého karetního systému a datové úložiště pro uchování dat o klientech systému a kartách, které jsou těmto klientům přiřazeny. Vybavení této modelové základny může být například takovéto:

- aplikační server
- HW – výkonný server
- operační systém
- aplikační SW
- primární databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém
- sekundární databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém

Duplicita databázových serverů, které jsou propojeny replikačním systémem zajišťujícím synchronizaci databází na obou serverech v reálném čase, je doporučováno z důvodu vysokého důrazu na zabezpečení dat v systému, jak je uvedeno v literatuře [2].

Personifikační pracoviště je místo, kde probíhá vlastní výroba karet podle požadavků zákazníků na žádosti o výrobu karty. Toto pracoviště může být buď řešeno jednoúčelově – budou se zde karty pouze vyrábět, nebo může být kombinováno s odbavovací přepážkou, což umožní nabízet speciální služby – např. výroba karty na počkání apod. Kombinované řešení navíc využívá pracovní síly obsluhy pracoviště efektivněji.

Vybavení personifikačního pracoviště :

- PC (+operační a antivirový systém)
- licence programu odbavovacího systému
- tiskárna daňových dokladů
- čtečka čipových karet
- UPS
- pokladní zásuvka pro uschování operativní hotovosti
- tiskárna pro potisk BČK
- scanner pro snímání fotografií ze žádosti

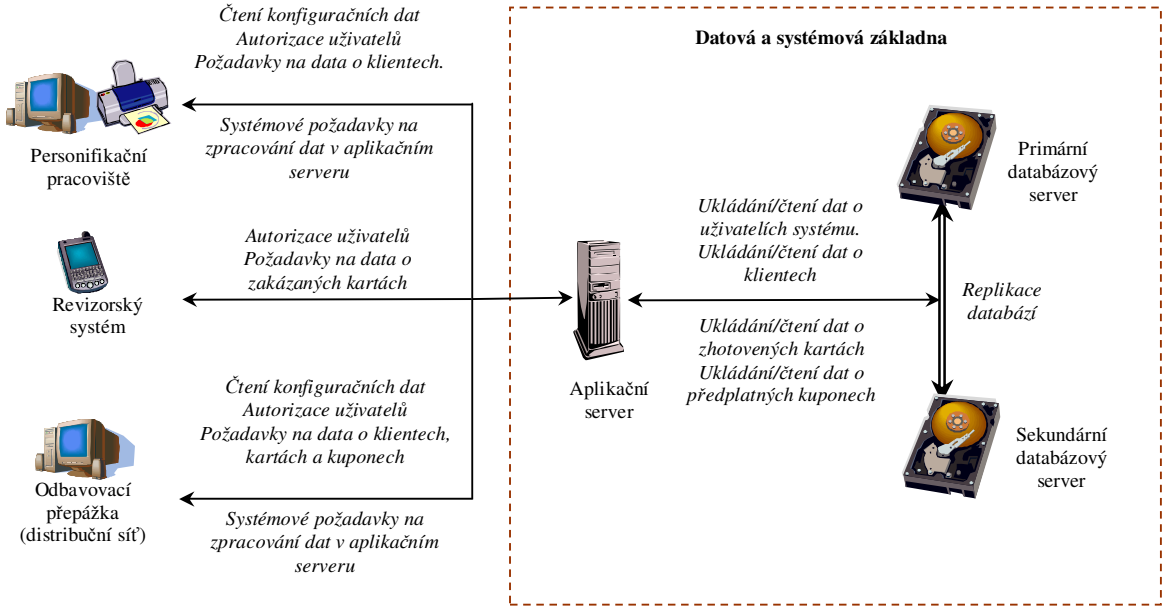
V místě personifikačních pracovišť pak je předpokládáno sdílené vybavení:

- tiskárna pro tisk pokladních uzávěrek
- kopírka

Kartové centrum může obsahovat buď jedno masivní personifikační pracoviště, které bude řešit veškerou výrobu karet pro systém městské čipové karty, nebo může být zbudována síť personifikačních pracovišť tak, aby např. každá větší čtvrť měla jedno personifikační pracoviště (a tedy místo, kde bude možno karty vyrábět na počkání).

Revizorský systém je zmíněn z toho důvodu, že základem pro systémy městských čipových karet je dopravní aplikace pro použití v MHD. Tento systém je tak nutnou nadstavbou a slouží jako support pro odbavení cestujících v MHD.

Obrázek 9 Modelové schéma řešení Kartového centra a odbavovacího systému městské čipové karty



Z výše uvedeného plyne, že pro vzájemné uznávání karet by dva takové systémy musely u všech zařízení, u kterých by k používání cizích karet docházelo, zajistit minimálně:

- HW kompatibilitu čteček čipových karet
- Odesílání dat o práci s cizí kartou mateřskému vydavateli a to přímo, či přes Datovou a systémovou základnu vlastního Kartového centra.

3.3.4. Zúčtovací centrum městské čipové karty

Jednou z nejdůležitějších aplikací v systémech městských čipových karet je elektronická peněženka. Zúčtovací centrum je databázový systém, který shromažďuje data o použití elektronické peněženky u jednotlivých partnerů, provádí potřebné kontrolní algoritmy a v dohodnutých termínech vyhodnocuje stav vzájemných pohledávek mezi jednotlivými subjekty zúčtování. Pro vyrovnání vzájemných pohledávek připravuje zúčtovací centrum potřebné doklady. V systému městské čipové karty se zpravidla vyskytuje více subjektů s různými odbavovacími a pokladními systémy a je nutno zajistit jednotný způsob předávání dat včetně definice struktury datových souborů. Předávání dat musí být zabezpečené proti neoprávněnému odečtení nebo modifikaci zasílaných souborů s jednoznačným kontrolním mechanismem informujícím zúčastněné subjekty o úspěšnosti přenosu a zpracování datových souborů, jak je uvedeno v literatuře [2] .

3.3.5. Přístup k datům v Zúčtovacím centru městské čipové karty

Každý subjekt zúčastněný v systému akceptace elektronických peněz systému městské čipové karty musí mít možnost nahlížet do dat uložených v zúčtovacím centru, pokud byla tato data pořízena na jeho provozovnách. Důvodem je možnost kontroly správnosti zúčtovacích procesů. Vydavatel elektronických peněz na městské čipové kartě musí mít absolutní přehled o všech transakcích, které jsou s jeho elektronickými penězi prováděny, a to proto, aby byl schopen řešit reklamace při práci s elektronickou peněženkou. Proto musí zúčtovací centrum umožňovat i kompletní přístup k datům na úrovni čtení.

3.3.6. Kontrolní mechanismy Zúčtovacího centra městské čipové karty

Zúčtovací centrum musí provádět kontrolní procedury, které budou hlídat bezpečnost celého systému. Mezi kontrolní procedury patří např.:

- vyhodnocení úspěšnosti přenosu a zpracování importních datových souborů od jednotlivých subjektů zúčtování
- prověření integrity dat
- kontrola návaznosti jednotlivých transakcí s elektronickou peněženkou
- kontrola původu vstupních dat
- kontrola souladu systému s legislativou (hlídání stanovených limitů)

3.3.7. Vybavení modelového Zúčtovacího centra městské čipové karty

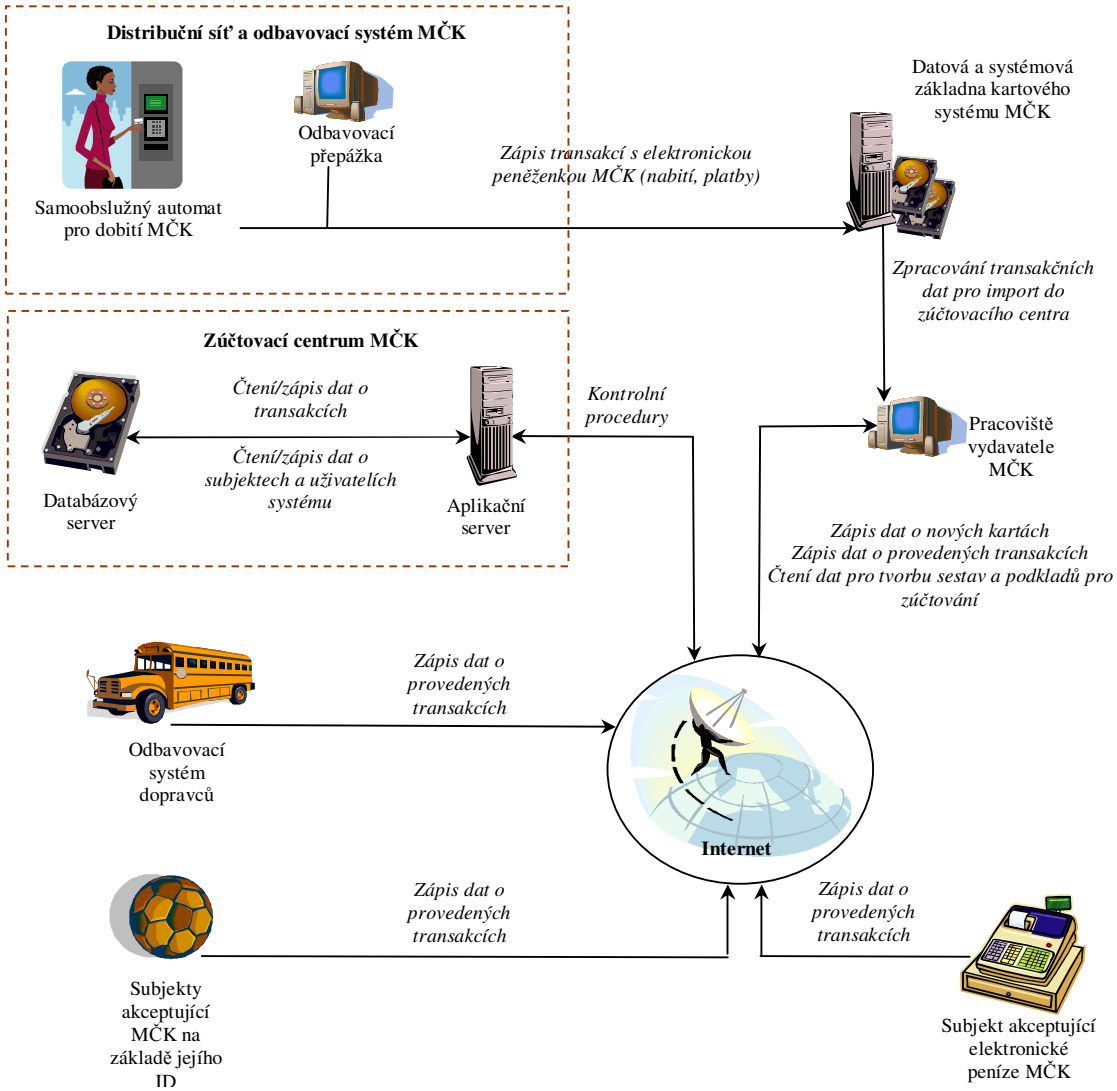
- aplikační server
- HW – výkonný server
- operační systém
- aplikační SW
- databázový server
- HW – výkonný server s kvalitním zálohovacím zařízením
- operační systém
- databázový systém
- zálohovací systém

Z důvodu zabezpečení proti ztrátě dat může být i u Zúčtovacího centra systému městské čipové karty vybudována redundantní replikace dat na sekundární datový server. Vzhledem k tomu, že veškerá data do centra budou dodávána jednotlivými subjekty ve formě importních souborů, není tento systém tak náchylný na ztrátu dat, jako odbavovací systém a Kartové centrum, a tedy duplicita dat není pro takový systém nezbytná .

3.3.8. Zúčtování předplatních kuponů

Pro přesnější rozdělení tržeb z prodeje předplatních kuponů – časových jízdenek - mezi jednotlivé dopravce může být zúčtovacím centrem vyhodnocováno i využívání těchto jízdenek. Zavedení tohoto způsobu rozdělování tržeb závisí na dohodnutém tarifním systému a na sjednaných smlouvách mezi dopravci a koordinátory integrovaných dopravních systémů.

Obrázek 10 Schéma zúčtování v systému městské čipové karty



Z výše uvedeného plyne, že pro vzájemné uznávání karet by dva takové systémy musely u všech subjektů u kterých by k používání karet v aplikaci elektronická peněženka docházelo, zajistit minimálně:

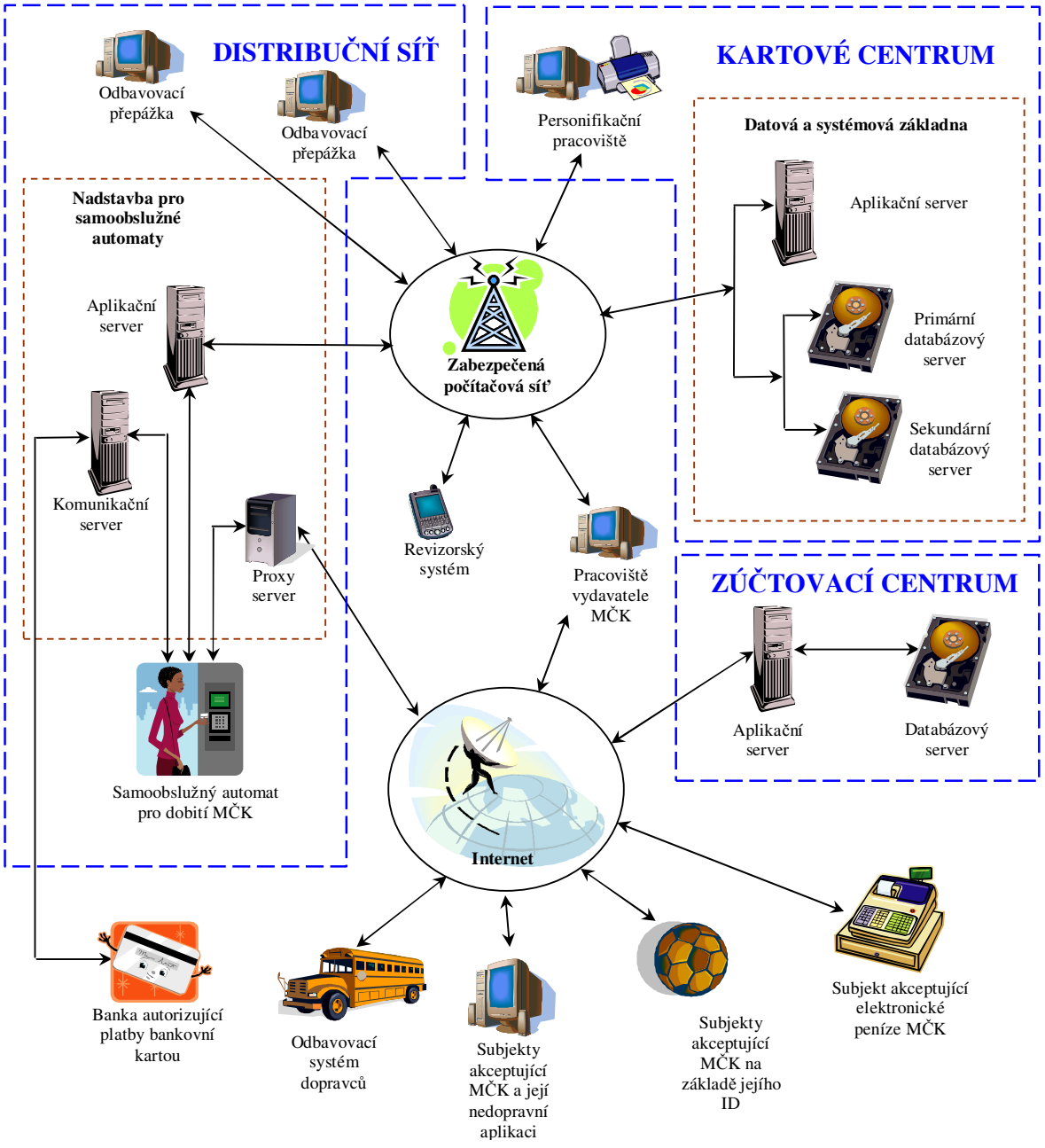
- HW kompatibilitu čteček čipových karet

- Odesílání dat o transakcích s elektronickou peněženkou mateřskému zúčtovacímu centru

3.3.9. Celkové schéma modelového systému městské čipové karty

Toto schéma znázorňuje celkový model systému městské čipové karty. Pro zajímavost je do něj vřazeno i schéma funkce dobíjení městských čipových karet v samoobslužných automatech pomocí bankovní karty s její autorizací např. přes Global Payment prostřednictvím jedné smluvní banky.

Obrázek 11 Schéma celkového řešení systému městské čipové karty



Z výše uvedeného plyne, že pro vzájemné uznávání karet by dva takové systémy musely u všech subjektů u kterých by k používání karet v aplikaci elektronická peněženka docházelo, musely zajistit minimálně:

- HW kompatibilitu čteček čipových karet
- Odesílání dat o práci s cizí kartou mateřskému vydavateli a to přímo, či přes Datovou a systémovou základnu vlastního Kartového centra.

- Odesílání dat o transakcích s elektronickou peněženkou mateřskému zúčtovacímu centru

3.3.10. Modelový případ rozložení aplikací na MČK

Tabulka je příkladem možného rozdělení aplikací v datovém prostoru MČK. Cílem je ujasnit jaká data musí být zpřístupněna kompatibilním systémům, aby mohla s neznámou MČK plnohodnotně pracovat. Pro příklad byla použita karta MIFARE standard 1kBYTE se strukturou MAD.

Tabulka 4 Modelové rozložení aplikací na městské čipové kartě

Číslo sektoru	Číslo bloku	Popis	Klíče
0.	0	Sériové číslo karty, kód výrobce a další doplňující údaje.	A0, B0
	1,2	MAD Struktura (mapa rozmístění aplikací do sektorů na kartě)	
1.	0,1,2	**Údaje o držiteli karty**	A1, B1
2.	0,1,2	**Aplikace abonentní předplatné** **1. Kupón**	A2, B2
3.	0,1,2	**Aplikace abonentní předplatné** **2. Kupón**	A2, B2
4.	0,1,2	**Aplikace elektronická peněženka** (1. sektor)	A3, B3
5.	0,1,2	**Aplikace elektronická peněženka** (2. sektor)	A3, B3
6.	0,1,2	**Aplikace elektronická peněženka** (3. Sektor)	A3, B3
7.	0,1,2	**Aplikace elektronická peněženka** (4. Sektor)	A3, B3
8.	0,1,2	**Aplikace předplatné v MHD** **3. Kupón**	A4, B4
9.	0,1,2	**Aplikace předplatné v MHD** **4. Kupón**	A4, B4
10.	0,1,2	**Aplikace předplatné integrovaného dopravního systému** **5. Kupón**	A5, B5
11.	0,1,2	**Aplikace předplatné integrovaného dopravního systému** **6. Kupón**	A5, B5
12.	0,1,2	**Volné místo**	A20, B20
13.	0,1,2	**Volné místo**	A20, B20
14.	0,1,2	**Volné místo**	A20, B20
15.	0,1,2	**Volné místo**	A20, B20

V nultém a prvním sektoru pak mohou být uloženy například tyto údaje:

1. Jedinečné ID karty
2. Jedinečné ID vydavatele karty
3. Jméno a příjmení držitele karty
4. Datum narození držitele karty
5. Jedinečné ID jednotlivých aplikací
6. Platnost karty
7. Jednoznačná Identifikace rozlišení typu karty

Aplikace elektronická peněženka pak může obsahovat například tato data:

1. Aktuální stav peněženky
2. Log obsahující čtyři poslední transakce
3. Záloha elektronické peněženky

Aplikace abonentní předplatné pak může obsahovat například tato data:

1. Označení např. divadla pro které předplatné platí
2. Datum od kdy předplatné platí
3. Datum do kdy předplatné platí
4. Typ předplatného (plnocenné, dětské, důchodce atp.)
6. Na této modelové kartě mohou být uložena dvě taková předplatná

Aplikace předplatné MHD pak může obsahovat například tato data:

1. Označení zóny (územní platnost)
2. Datum od kdy předplatné platí
3. Datum do kdy předplatné platí
4. Typ předplatného (plnocenné, dětské, důchodce atp.)
5. Typ předplatného (jednoznačné ID tarifu neboli předplatného)
6. Na této modelové kartě mohou být uložena dvě taková předplatná s různými daty platnosti a různou územní platností

Aplikace předplatné integrovaného dopravního systému pak může obsahovat například tato data:

1. Označení zóny (územní platnost)

2. Datum od kdy předplatné platí
3. Datum do kdy předplatné platí
4. Typ předplatného (plnocenné, dětské, důchodce atp.)
5. Typ předplatného (jednoznačné ID tarifu neboli předplatného)
6. Na této modelové kartě mohou být uložena dvě taková předplatná s různými daty platnosti a různou územní platností

Z tabulky plyne, že pro práci s aplikacemi na kartě je nutné znát:

- Přístupové klíče k aplikaci
- Strukturu aplikace
- Strukturu karty
- Logiku aplikace, aby mohla být správně obsloužena (zapsáno na správné místo, dobře vyhodnocen nárok na slevu)

Druhou možností je povolit druhému vydavateli umístění jeho vlastní aplikace na cizí kartě. Vydavatel tak pracuje s vlastní důvěrně známou aplikací včetně vlastních přístupových klíčů a nemusí obslužný SW na své straně prakticky nijak přizpůsobovat. Nevýhodou je obsazení dalšího omezeného prostoru na kartě aplikací s často prakticky identickým účelem.

4. Závěr

Cílem této práce bylo pokusit se definovat klíčové body z pohledu hardwaru a softwaru, které by bylo nutno vyřešit, aby dva systémy městských čipových karet mohly svoje karty navzájem mezi sebou uznávat.

Důvodem pro takové uznávání je pohodlí uživatele. Pokud by mohlo docházet k přenosu karet mezi dvěma takovými systémy, uživatel by svoji kartu se stejným komfortem použil v Praze, Plzni nebo Brně bez zvýšených nákladů na pořizování dalších, technicky prakticky identických karet. V praxi by to znamenalo, že se svojí pražskou OPEN CARD v kapse, kde má nahraný roční kupon opravňující ho k cestování metrem a pražskou MHD vůbec, docestuje autem do Brna, tady vystoupí, zaplatí z elektronické peněženky za parkovné v parkovacím automatu, v tramvaji si zakoupí z téže elektronické peněženky jednodenní jízdné pro celou rodinu, které je mu v elektronické podobě zaznamenáno na tutéž kartu a navštíví místní autodrom, kde mu jako vstupenka poslouží opět OPEN CARD, na jejíž ID byla tato vstupenka zakoupena pomocí e-shopu již v Praze. Takto sofistikovaný systém má již dnes například projekt Plzeňské karty. Proto se tato práce snaží zjistit, které parametry by bylo nutno sdílet nad množinou vydaných karet mezi dvěma, případně více různými vydavateli takových karet a zda je to vůbec technicky možné.

Práce vychází z informací mezi odbornou veřejností obecně známých, veřejně dostupných zdrojů na internetu jak o používané technologii, tak o jednotlivých karetních systémech, které jako technologické projekty zpravidla mají vlastní internetové stránky. Dále byla využita odborná literatura a v neposlední řadě informace získané od týmu pracovníků projektu Plzeňská karta.

Problematika byla dekomponována na dva základní prvky a to hardwarovou kompatibilitu a kompatibilitu softwarovou. Cílem nebylo zabřednout do technického detailu, ale podívat se na problém shora a nalézt klíčové prvky spíše z roviny systémové integrace. Pro řešení, které by mělo v budoucnu propojit celé existující systémy a dát pravidla pro rozvoj nových, je takový nadhled nutný a doufám, že se ho pod vedením vedoucí bakalářské práce podařilo udržet.

Provedená analýza z dostupných zdrojů ukázala, že systémy městských čipových karet v ČR jsou i nadále na vzestupu, a to s trendem obsluhovat jednou čipovou kartou co nejvíce systémů a zařízení.

Z pohledu hardwarové kompatibility bylo zjištěno, že v České republice se užívají v systémech městských čipových karet a u velkých dopravců dva základní typy karet. Obě karty jsou podle typu rozhraní bezkontaktní čipové karty a to navíc od stejného výrobce. Jedná se o karty Mifare Standard a Mifare DESFire výrobce Philips Semiconductors. Výrobce u těchto dvou typů karet MIFARE deklaruje takzvanou zpětnou kompatibilitu - tedy na novějším zařízení lze číst karty staršího typu.

Je tedy zřejmé, že pro dosažení vzájemné hardwarové kompatibility systémů městských čipových karet je klíčové, aby byla navzájem kompatibilní čtecí zařízení těchto karet.

Pro identifikaci klíčových bodů softwarové kompatibility bylo zjišťováno, za jakých podmínek lze navzájem sdílet aplikace uložené na čipové kartě. Pro takové sdílení je pak třeba znát minimálně následující skutečnosti:

- Přístupové klíče k aplikaci
- Strukturu aplikace
- Strukturu karty
- Logiku aplikace, aby mohla být správně obsloužena (zapsáno na správné místo, dobře vyhodnocen nárok na slevu)

Druhou možností je povolit druhému vydavateli umístění jeho vlastní aplikace na cizí kartě. Vydavatel tak pracuje s vlastní důvěrně známou aplikací včetně vlastních přístupových klíčů a nemusí obslužný SW na své straně prakticky nijak přizpůsobovat. Nevýhodou je obsazení dalšího omezeného prostoru na kartě aplikací s často prakticky identickým účelem.

Na základě provedených zjištění bylo konstatováno, že neexistují významné technické bariéry pro vzájemné uznávání čipových karet mezi jednotlivými systémy různých vydavatelů těchto karet. Bude však nutno vyřešit jednotnou podobu aplikací a dále problematiku předávání přístupových klíčů k těmto aplikacím, případně k volnému paměťovému prostoru.

Vzájemnému sdílení karet na bázi prostého ID pak nebrání vůbec nic, kromě typu použité čtečky.

5. Seznam literatury:

1. DOSTÁLEK, L. – VOHNOUTOVÁ, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1.vydání. Brno. Computer Press. 2006. 534 s. ISBN 80-251-0828-7
2. RODRYČOVÁ, D. – STAŠA P. Bezpečnost informací jako podmínka prosperity firmy. Grada Publishing. 2000. 143 s. ISBN 80-7169-144-5
3. RANKL, W. EFFING, W. Smart Card Handbook, 3rd edition, New York, John Wiley &
Sons, 2003, ISBN 0470856688

Internetové zdroje:

1. Mifare 1k. [cit. dne: 25.3.2009.]
dostupné z:http://mifare.net/products/smartcardics/mifare_standard1k.asp
2. Mifare 1k. [cit. dne: 25.3.2009.]
dostupné z:http://mifare.net/products/smartcardics/mifare_standard1k.asp
3. Mifare 1k. [cit. dne: 25.3.2009.]
dostupné z:http://mifare.net/products/smartcardics/mifare_standard1k.asp

6. Seznam zkratek:

Zkratka	Význam
ID	identifikační prvek (např. číslo)
PIN	osobní identifikační číslo (Personal Identification Number)
SAM	Secure Access Module
HW	hardware
SW	software
MČK	městská čipová karta
MAD	Mifare Application Directory
BlackList	seznam zakázaných - blokovaných karet v systému
EP	elektronická peněženka

7. Seznam obrázků:

8. Seznam tabulek:

9. Přílohy

Příloha 1 Kartové projekty v ČR – typ karty a její využití

Název karty	vydavatel karty	technický standard karty	aplikace na kartě	aplikace na kartě	použití na základě ID karty	poznámka
Plzeňská karta	Plzeňské městské dopravní podniky a.s.	Mifare Standard 1k	Předplatné IDS	Elektronická peněženka	čtenářský průkaz, stravné na školách, kopírování, identifikační a docházkové systémy, rezervační systém Plzeňská vstupenka, přístupové systémy.	
Open card	Hlavní město Praha	MIFARE DESFire 4k	Předplatné IDS	kupóny na parkování	čtenářský průkaz, přístup k evidenci dopravních přestupků	
Opus card	Liberecká IS, a.s.	MIFARE DESFire 4k	Předplatné MHD		Benefit program, čtenářský průkaz, rezervační systém e-vstupenka	
IN-karta	České dráhy a.s.	MIFARE DESFire 4k	Předplatné na tratích ČD	Slevový průkaz na tratích ČD		
Karta integrované dopravy a služeb	Dopravní podnik měst Mostu a Litvínova a.s.	Mifare Standard 4k	Předplatné IDS	Elektronická peněženka v dopravě	bonusový program	
Městská karta	Dopravní podnik města Hradce Králové, a.s.	Mifare Standard 4k	Předplatné pro dopravu	Elektronická peněženka v dopravě		formátováno pouze 1k
Pardubická karta	Dopravní podnik města Pardubic a.s.	Mifare Standard 4k	Předplatné pro dopravu	Elektronická peněženka v dopravě		