Michal Palán[1]

Bezkontaktní čipové karty Českých drah

Klíčová slova: *bezkontaktní čipová karta, Radio Frequency Identification, RFID, contactless smartcard, Proximity Integrated Circuit Card, PICC, Modrá karta, In-karta, MIFARE, DESFire, šifrování dat, 3DES*

Bezkontaktní čipová karta

První elektronické karty byly vynalezeny kolem roku 1970. O prvenství se vedou spory mezi Němcem Jürgenem Dethloffem, Japoncem Kunitakou Arimurou a Francouzem Rolandem Morenem. K prvním masovému nasazení došlo až v roce 1983 ve Francii, šlo o telefonní kartu *Télécarte*. Zpočátku se ovšem jednalo pouze o velmi jednoduché kontaktní paměťové karty, které sloužily pouze k ukládání dat ve velmi omezeném rozsahu. Komunikaci s vnějším zařízením obstarávaly kovové kontakty vyvedené na povrch karty.
Koncem 80. let se objevily kontaktní čipové karty. Ty už kromě paměťových obvodů obsahovaly také integrovaný mikroprocesor, který umožňoval realizovat vyspělou komunikaci mezi kartou a čtecím zařízením a hlavně kryptograficky zabezpečenou komunikaci a přístup k uloženým datům. Stále se však jednalo o kontaktní kartu – pro práci s ní bylo nutné zasunout ji do čtecího zařízení.

Čip kartu integruje obsahuje tyto části:

- Rozhraní pro komunikaci se čtecím zařízením
- CPU (Central Processing Unit) – procesor. Původně osmibitový mikroprocesor založený na architektuře CISC s frekvencí 5 MHz, v případě modernějších typů již 32-bitový.
- Matematický koprocesor pro podporu kryptografických operací
- ROM (Read Only Memory) – paměť pouze pro čtení, obsahuje operační systém a základní programovou část. V současné době jej její rozsah 16 KB až 96 KB.
- EEPROM (Electrically Erasable Programmable Read Only Memory) – vícenásobně elektricky programovatelná a smazatelná paměť, obsahuje uživatelské programy a data. Velikost bývá do 72 kB.
- RAM (Random Access Memory) – paměť s volným přístupem, slouží pro běžnou činnost procesoru. Její velikost bývá překvapivě malá, typicky 256 bajtů. Důvodem je to, že struktura buňky na křemíkovém čipu pro tento typ paměti zabírá poměrně mnoho místa.

V polovině 90. let se začaly prosazovat bezkontaktní čipové karty (BČK), jež kromě čipu a paměti obsahují také integrovanou anténu a vysílač / přijímač. Čtecí zařízení kolem sebe neustále vytváří elektromagnetické pole. Jakmile se BČK ocitne v jeho blízkosti, v anténě se indukuje elektrický proud, sloužící k napájení čipu. Je-li intenzita dostatečná, čip se „probudí“ a začne komunikovat. Obrovskou výhodou tohoto principu je naprostá necitlivost na

[1] Ing. Michal Palán (1979). Absolvent magisterského studia na Univerzitě Pardubice, Dopravní fakultě Jana Pernera – obor technologie a řízení dopravy (2002), v současné době je posluchačem doktorandského studia téže školy. Pracuje na Generálním ředitelství Českých drah, odboru strategie a informatiky.

znečistění kontaktů (žádné tu nejsou) a poškození čipu elektrostatickým napětím. Nevýhodou je nutnost nižší spotřeby čipu (napájení je možné pouze elektromagnetickým polem), proto zpočátku měly tyto karty asi pětileté technologické zpoždění za kartami kontaktními.

Mluvíme-li o bezkontaktních čipech, používají se dva názvy pro různé typy zapouzdření:

- Karta – plastová karta s potiskem rozměrů běžné kreditní karty
- Tag – jakýkoliv jiný tvar, sloužící zejména k identifikaci osob či zboží (klíčenka, kruhové nebo obdélníkové pouzdro různých rozměrů, skleněný váleček pro identifikaci zvířat, samolepicí nálepka…)

Komunikace funguje na principu modulace elektromagnetického pole. Čipy pro RFID obecně využívají různé nosné frekvence:

- 125 kHz, , 134 kHz – první generace bezkontaktních karet s nízkou přenosovou rychlostí. Obsahují obvykle pouze jedinečné číslo čipu. Používají se pro jednoduché aplikace typu kontrola přístupu.
- 13,56 MHz – kmitočet používaný v současnosti pro hlavní rodinu karet určených jak pro náročné platební a bankovní aplikace, tak i pro bezkontaktní identifikaci zboží, výrobků, kontejnerů... Čtecí vzdálenost je od 10 cm (pro platební karty s procesory) až po 1 m (pro jednoduché identifikační čipy)
- Pásmo UHF 868 MHz (v Evropě) a 915 MHz (v USA) – Je využíváno zejména pro identifikaci kontejnerů a palet na větší vzdálenosti. Díky vysokému kmitočtu lze realizovat snadno směrovou anténu a tak dosáhnout čtecí vzdálenost 2 až 3 m. Nevýhodou jsou větší rozměry tagu a čtecí vlastnosti ovlivňuje i vlhkost.
- Mikrovlnné pásmo 2,45 a 5,6 GHz – je doménou zejména aktivních tagů (s vlastním napájecím zdrojem) pro dopravní aplikace. Tak lze identifikovat například vozidlo jedoucí rychlostí až 200 km/h na vzdálenost 15 m. Nejznámější aplikací je tarifní systém pro sledování průjezdu kamionů na dálnicích.

Zpočátku nebyly bezkontaktní čipové karty nijak standardizovány a každý výrobce prosazoval svoji technologii. Ke sjednocení došlo až v posledních letech, kdy vešly v platnost normy:

- ISO 15693 – norma pro karty a tagy určené zejména pro identifikaci osob a zboží na kmitočtu 13,56 MHz
- ISO 18000 – norma definuje zejména tagy sloužící jako náhrada dosud používaného čárového kódu na výrobcích (s různým kmitočtem)
- ISO 14443 – norma určená zejména pro identifikační a platební karty. Norma má 4 části. ISO 14443-1 stanovuje fyzikální charakteristiky karty, jako jsou její rozměry, odolnost vůči ultrafialovému a rentgenovému záření, mechanickému namáhání a odolnost vůči působení elektrického a magnetického pole. V části ISO 14443-2 jsou stanoveny parametry datového přenosu a část ISO 14443-3 uvádí, jak má komunikační zařízení (Proximity Coupling Device) pracovat v inicializační fázi komunikace s kartou (Proximity Integrated Circuit Card), jak postupovat, ocitne-li se v jeho dosahu více karet, a podobně. Konečně část ISO 14443-4 definuje komunikační protokoly.

Technologie MIFARE

Nejrozšířenější technologií platebních a bankovních karet na světě je v současnosti MIFARE rozvíjená společností Philips. Počátkem roku 2006 již ve světě fungovalo více než 500 milionů karet této rodiny a 5 milionů komunikačních zařízení. Jde o otevřenou architekturu,

takže výrobců karet je více než 50 a výrobců čteček přes 200. Výrobcem samotného čipu je u vyšších typů karet z bezpečnostních důvodů výhradně firma Philips.

Existuje celkem 6 typů karet standardu MIFARE:

- MIFARE Ultralight
- MIFARE Standard 1k
- MIFARE Standard 4k
- MIFARE DESFire
- MIFARE PROX
- MIFARE SmartMX

Základní technické parametry přehledně shrnuje následující tabulka:

	MIFARE Ultralight	MIFARE Standard 1k	MIFARE Standard 4k	MIFARE DESFire	MIFARE PROX	SmartMX
velikost paměti	64 B	1024 B	4096 B	4096 B	16384 B	73728 B
délka čísla karty	56 bitů	32 bitů	32 bitů	56 bitů	56 bitů	56 bitů
počet zápisů do paměti	1000	100.000	100.000	100.000	100.000	100.000
doba uchování dat	2 roky	10 let	10 let	10 let	10 let	10 let
doba vykonání typické transakce	31,4 ms	164 ms	164 ms	105 ms	105 ms	105 ms
elektronická peněženka	není	32 bitů, plný kredit	32 bitů, plný kredit	plný i omezený kredit	Uživatelsky programovatelná	Uživatelsky programovatelná
metoda šifrování dat	žádná	CRYPT1	CRYPT1	DES, 3DES AES*	DES, 3DES, RSA	DES, 3DES, RSA, ECC
počet aplikací	1	16	40	28		
vhodné použití	jednorázové jízdenky	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	e-ticketing, věrnostní programy, elektronická peněženka	e-business	e-business

Karty MIFARE PROX a SmartMX jsou vyspělé duální procesorové karty (s kontaktním i bezkontaktním rozhraním), jejichž funkce lze programovat v jazyce JAVA. Umožňují tak naprogramování složitých a velmi bezpečných aplikací s širokým spektrem použití, nejsou však tak vhodné pro utilitární využití pouze v dopravě. Proti nim hovoří vysoká výrobní náročnost, vysoká cena (asi osminásobná oproti MIFARE Standard 1K a pětinásobná oproti MIFARE DESFire) a komplikovanější vytváření softwaru.
Naproti tomu karta MIFARE Ultralight zvládá prakticky pouze jedinou aplikaci. Pro svou malou paměťovou kapacitu, velmi nízkou bezpečnost, krátkou trvanlivost a na druhé straně také nízkou cenu je vhodná pouze pro jednorázové, případně celodenní jízdenky.
Dopravci, kteří ve svých odbavovacích systémech chtějí využívat i další funkce (zejména elektronickou peněženku), volí téměř výhradně karty MIFARE Standard 1k, Standard 4k a DESFire. Každý čip má své jedinečné číslo naprogramované jeho výrobcem, které lze volně číst, ale nelze jej změnit. Přístup k datům na kartě lze zabezpečit použitím kryptografie.

Karty MIFARE DESFire

Karty MIFARE DESFire mají následující parametry.

Radiofrekvenční rozhraní

- bezkontaktní přenos dat, napájení elektromagnetickým polem (provoz bez baterií)
- provozní vzdálenost až 100 mm (v závislosti na geometrii antény a výkonu vysílače)
- provozní frekvence 13,56 MHz
- přenosová rychlost 106 kbit/s, 212 kbit/s nebo 424 kbit/s
- integrita dat: 4 Byte MAC (message authentication code), 16 bit CRC, parita, bitové kódování, bitový počet
- antikolizní vlastnosti (možnost práce více karet současně v poli antény)
- přenosový protokol dle ISO 14443-4

Stálá paměť

- 4 KB stálé (nonvolatilní, udržující si obsah i bez přítomnosti napájecího napětí) paměti, v nové verzi až 8 KB
- doba zápisu 2 ms na blok (1 ms mazání předchozích dat, 1 ms vlastní zápis)
- doba uchování dat 10 let
- trvanlivost 100 000 zapisovacích cyklů

Organizace stálé paměti

- flexibilní souborový systém (u starších typů karet se používaly paměťové bloky o pevné velikosti)
- až 28 zcela nezávislých aplikací na kartě
- až 16 souborů pro každou aplikaci
- až 14 kryptografických klíčů pro každou aplikaci

Bezpečnost

- 7-bajtové jedinečné číslo karty
- 3-kroková autentifikace (viz níže)
- hardwarově podporované šifrování algoritmy DES/3DES (v nové verzi i AES)
- zabezpečení dat 4-bajtovým MAC (Message authentication code)
- autentizace na aplikační úrovni

Výhody proti MIFARE Standard

- plně multiaplikační systém, každou z aplikací má její vlastník plně pod kontrolou
- větší paměť (dána lepším využitím paměti)
- výrazně rychlejší čtení a zápis
- předpoklad rozvoje do budoucna s kompatibilním protokolem ISO 14443-4
- významně dokonalejší kryptografické zabezpečení (3DES)

Každou nezávislou aplikaci na kartě reprezentuje její identifikátor AID o délce 3 byte (Application Identifier). Soubory mohou být pěti typů: standardní datový soubor, záložní datový soubor, hodnotový soubor se zálohou, soubor s lineárním záznamem a soubor cyklickým záznamem (oba se zálohou). Zálohou je automaticky vybaveno prvních 8 souborů každé aplikace, zbylých 8 je bez zálohy.

Data se mezi kartou a čtečkou mohou přenášet ve 3 režimech: nezašifrovaně, nezašifrovaně se zašifrovaným autentizačním kódem (MAC) a zašifrovaně. Přístup k datům je možný na aplikační úrovni. Pro každou aplikaci lze stanovit až 14 různých klíčů, které mohou různým subjektům zajistit různý stupeň přístupu k datům. Pro každý klíč pak lze stanovit jedno ze čtyř oprávnění: čtení dat, zápis dat, čtení i zápis a změna oprávnění k přístupu.
Kromě těchto klíčů existuje pro každou aplikaci ještě tzv. master klíč (Application Master Key), který je vždy vyžadován pro operace změny nastavení přístupových práv aplikace a změny master klíče aplikace. Dále jeho znalostí mohou být podmíněný některé další operace, jako vytvoření a zrušení souboru, čtení seznamu souborů a čtení přístupových práv aplikace.
Třetím typem klíče je master klíč karty (PICC Master Key). Ten je nezbytný pro formátování karty, změnu nastavení přístupových práv ke kartě a ke změně master klíče karty. Navíc může být vyžadován pro další operace, jakými jsou vytvoření a zrušení aplikace, čtení seznamu aplikací a čtení přístupových práv karty.
Autentizace je proces, který proběhne na začátku komunikace karty se čtečkou. Při této proceduře se čtecí zařízení a karta navzájem ujistí, že je jim známa hodnota tajného klíče, aniž by si hodnotu tohoto klíče navzájem posílaly. Vedlejším produktem tohoto procesu je hodnota tzv. *session key* (klíč platný pouze pro tuto jednu komunikaci), který se poté využije pro šifrování přenášených dat.

Projekt Modrá karta

České dráhy zahájily svůj projekt Modrá karta jako reakci na stále silnější prosazování čipových karet v české veřejné dopravě. Projekt byl rozdělen do dvou etap – zaměstnanecké a zákaznické. V první etapě šlo především o nahrazení stávajícího jízdního dokladu pro zaměstnance a jejich rodinné příslušníky – železniční průkazky – za nový typ jízdního dokladu, jehož nosičem je čipová karta. Postupně se vyvíjejí a uvádějí do provozu také další aplikace – služební průkaz, přístupy do budov, přístup k tiskárnám a kopírovací technice a další.
V zákaznické etapě jde jednak o nahrazení slevových průkazů ČD bezkontaktními kartami (karta Z, junior pas, senior pas) a jednak o nabídku nových produktů. Prvním z nich je roční síťová jízdenka na první vozovou třídu In-gold.
Jako nosič byla zvolen typ MIFARE DESFire. Cílem je, aby čipová karta ČD umožňovala cestujícím nahrání aplikací jiných dopravců. Jediná karta by tak sloužila k cestování v různých dopravních prostředcích s různými dopravci.
České dráhy za tím účelem v roce 2004 iniciovaly proces stanovení standardů odbavovacího systému ve veřejné osobní dopravě založeného na využití bezkontaktních čipových karet jako media pro společný elektronický jízdní doklad a pro sdílené bezhotovostní platby. Tyto standardy se uvádějí pod názvem Národní dopravní karta.

Závěr

Bezkontaktní čipové karty se v posledních letech masově nasazují nejen v dopravě, ale pronikají i do jiných oblastí. V České republice se od jednoúčelového nasazení u autobusových dopravců jako elektronické peněženky (přesněji předplaceného kreditu jízdného) přechází k multiaplikačním městským a regionálním kartám. Pozornost si získávají otevřené systémy založené na přijímání karty různými subjekty, což je atraktivní pro uživatele, který tak nepotřebuje nosit několik různých karet. Čipová karta se postupně stává univerzálním dokladem.

V dopravě si získávají oblibu jednoduchostí, rychlostí použití a pestřejší nabídkou slev a výhod. Pro dopravce jsou zajímavé možnosti získávání podrobnějších informací o využívání jednotlivých spojů a struktuře jejich cestujících.

Literatura

[1] *MIFARE DESFire, Contactless Multiapplication IC with DES and 3DES Security, MF3 IC D40*, Philips Semiconductors, Eindhoven 2004.

[2] Rankl, W. – Effing, W. *Smart Card Handbook*, John Wiley & Sons, 2000. ISBN 0471988758

[3] Introduction to Smart Cards <http://sumitdhar.blogspot.com/2004/11/introduction-to-smart-cards.html> [cit. 25.4.2006]

[4] MIFARE – contactless smart card ICs <http://www.semiconductors.philips.com/products/identification/mifare/index.html> [cit. 25.4.2006]

[5] *Standardy bezkontaktní čipové karty*, PVT Prokom a.s., Praha 2004.

Praha, květen 2006

Lektoroval: Ing. Kolčava
COMINFO Zlín