Portál pre odborné publikovanie ISSN 1338-0087

Čipové karty a jejich využití

Seidl Jaromír · Informačné technológie

22.09.2014

Práce se zabývá základním technologickým a bezpečnostním principům čipových karet, jejich rozdělení a technickým vlastnostem čipu. Odborný článek je zaměřený na využití čipových karet v jejich základních aplikacích. Každý čip na procesorové kartě si lze zjednodušeně představit jako jakýsi minipočítač s vlastním procesorem, operačním systémem, pamětí, oblastmi pro ukládání dat, kanály pro komunikaci s I/O zařízeními.

Úvod

Na celém světě existuje několik miliard čipových karet, které nacházejí uplatnění v mnoha oblastech využití. K jednodušším aplikacím čipových karet lze zařadit například předplacenou telefonní kartu s pamětí a pevnou logikou. Na druhé straně existují čipové karty pro aplikace k elektronickému podpisu, které vyžadují vysokou úroveň zabezpečení dat. Mezi nejrozšířenější aplikace čipových karet patří platební karty, které se využívají nejen v oblasti bankovnictví, ale i jako platební prostředek v obchodech či v oblasti služeb. V současnosti se z důvodu vyšší bezpečnosti postupně přechází z karet s magnetickým proužkem na karty čipové. K nejrozšířenějším aplikacím čipových karet patří také čipové SIM karty v mobilních telefonech. Z hlediska potřeby zabezpečit komunikaci budou zajímavé především různé varianty procesorových karet. Každý čip na procesorové kartě si lze zjednodušeně představit jako minipočítač s vlastním procesorem, operačním systémem, pamětí, oblastmi pro ukládání dat, kanály pro komunikaci s I/O zařízeními.

První zmínka o využití karet s “autentizací” pro bankovní operace se objevila v utopickém románu Looking Backward v roce 1887, jehož autorem byl americký autor Edward Bellamy. Praktický pokus o zavedení kreditní karty bez čipu a magnetického pásku proběhl roku 1958. Teprve v letech 1968 a 1969 němečtí elektroinženýři Helmut Gröttrup a Jürgen Dethloff společně vyplnili patenty na automatickou čipovou kartu. Následný zásadní patent pro čipové karty s mikroprocesorem a pamětí patentoval Jürgen Dethloff v roce 1978. Koncept samotné paměťové karty je připisován francouzskému vynálezci Rolandu Morenovi, na jehož podkladě byl v laboratořích Honeywell vytvořen první mikroprocesorová čipová karta. Ta byla roku 1978 patentována a dala tak potřebný základ architektury čipu. O tři roky později použila technologii firma Motorola v kartě s označením “CP8”. Karta “CP8” se stala důležitou pro vývoj současných karet založených na systému veřejného klíče (PKI).

Největší nárůst v používání čipových karet přišel v roce 1990 se zavedením SIM karet používaných v GSM mobilních zařízeních. S rozšířením mobilních telefonů v Evropě se čipové karty stávaly samozřejmostí. Další rozvoj v bankovnictví, když mezinárodní platební systémy MasterCard, Visa a Europay v roce 1993 podepsaly smlouvu na spolupráci při vývoji specifikace pro čipové karty pro platbu s kreditní a debetní kartou. První verze systémů EMV (Europay, MasterCard, Visa) byla spuštěna v roce 1994. Ve většině vyspělých zemí došlo od konce devadesátých let až dodnes k výraznému pokroku v používání EMV kompatibilních zařízení v maloobchodních prodejnách a při vydávání debetních a kreditních karet odpovídajících specifikaci EMV. [1]

1. Čipové karty

Čipová karta je moderním platebním prostředkem. Co to vlastně je čipová karta? Čipová karta je technické zařízení podobné bankovní kartě, ze kterého je možné číst údaje i údaje do něho zapisovat. Do čipové karty se vloží Vaše osobní údaje, které budou sloužit k identifikaci držitele karty. Základní rozdělení čipové karty na kontaktní a bezkontaktní. Bezkontaktní karty, jejichž fyzické vlastnosti předepisuje norma ČSN ISO/IEC 14443-x, se používají zejména v systémech kontroly a evidence vstupů, docházkových systémech, a systémech pro odbavení cestujících v hromadné dopravě. Třída bezkontaktních karet není pro účely zabezpečení dat příliš zajímavá. Zajímavou se však může stát v kombinaci s kontaktním čipem v jedné kartě (tzv. duální čipové karty). Přestože vzhled všech kontaktních čipových karet je na první pohled téměř shodný, společným základem jsou pouze pravidla definovaná základní sadou norem ISO/IEC 7816-1, -2, -3, -4, resp. jejich českých ekvivalentů ČSN EN 27816-1, -2, -3, -4. Podle základních technických charakteristik se kontaktní čipové karty dělí:

- karty ryze paměťové,
- karty s chráněnou pamětí,
- standardní procesorové karty,
- procesorové karty s přídavnými kryptokoprocesory.

Z pohledu způsobu úpravy aplikačních profilů podle požadavků zákazníků, popř. vytváření specifických aplikací, je možné procesorové karty ještě členit na karty s proprietárními operačními systémy a karty na bázi otevřených platforem (Open Platform: Java Card, Multos, Windows for Smart Cards). [2] Zejména v posledních pěti letech nastal v celosvětovém měřítku skutečně masivní rozvoj v aplikačním využívání čipových karet. Přestože se ani tomuto oboru nevyhnul určitý dílčí otřes, který v prvních letech nového milénia poznamenal téměř všechny oblasti informatiky a „nové ekonomiky„, trh čipových karet je už v současné době opět na vzestupu a v období přechodu z fáze formujícího se trhu (emerging market) do fáze trhu plně rozvinutého.

2. Vzhled karty

Kreditní karta je vyrobená z plastu, lépe řečeno z třívrstvého PVC a musí být netoxický, odolný vůči chemickým vlivům při běžném používání apod. Musí splňovat standardní rozměry (85,6 x 54,0 x 0,76 mm), které stanoví mezinárodní norma ISO 3554. Pro použití v mechanických snímačích se na kartu vyrazí nezbytné identifikační údaje písmenem OCR 7B velikosti 3,63 mm. Na přední straně kreditní karty jsou

zobrazeny vydavatel platební karty, platnost platební karty, číslo karty, jméno držitele, a čip. Platnost platební karty je uváděná stylem měsíc a rok, buď jako začátek i konec platnosti nebo pouze konec platnosti.

Je důležitá z hlediska použitelnosti karty, neboť karty s prošlou platností jsou automaticky zablokovány. Číslo karty obsahuje 12 až 19místné číslo karty. První dvě čísla určují oblast použití karty, např. Master Card začínají číslicí 5, VISA číslicí 4, národní systémy číslicí 9. Následujících 5 znaků je identifikace vydavatele karty, přidělována orgány ISO. Zbylých 8 až 13 míst je pro identifikaci konkrétního kartového produktu vydavatele a klienta. Jméno držitele držitelem je obvykle majitel účtu, ke kterému se karta vztahuje nebo jím může být i osoba oprávněná disponovat s prostředky. Maximální počet znaků může být 27. Čip slouží k záznamu dat. Je bezpečnější než magnetický proužek. V současnosti jsou karty v České republice vydávány s vestavěným magnetickým proužkem i čipem, tzv. hybridní karty. V budoucnosti by však čipová technologie magnetické proužky nahradit. [2]

Obr. 1 Rozmístění znaků a čísel na platební kartě

U některých karet se můžeme také setkat s hologramem (ochrana karty proti padělání, trojrozměrný obraz měnící při natáčení proti světlu svou barvu i tvar, jeho výroba je technicky i finančně náročná). Na zadní straně se nachází Magnetický proužek, který obsahuje tzv. servisní kódy, které definují základní vlastnosti karty, může mít dvě až tři záznamové stopy. Druhým údajem na zadní straně je podpisový proužek sloužící k zaznamenání podpisového vzoru, který je vyroben ze speciálního papíru citlivého na gumování a chemické látky, schopného odhalit jakoukoli změnu původního podpisu. Zajišťuje ochranu proti padělání, používá se ceninový tisk, případně i vlákna a barvy

citlivé na infračervené světlo.

3. Důvody pro zavedení čipových karet v bankovnictví

Úspora provozních nákladů u magnetických karet jsou významnou položkou provozních nákladů telekomunikační a autorizační poplatky. Důvodem je skutečnost, že na magnetickém proužku karty nelze bezpečně zaznamenat PIN kód klienta ani finanční částku, kterou může disponovat. Tyto údaje jsou uloženy v bankovních autorizačních centrálách, kde se provádí on-line ověření požadovaných transakcí. Čipové karty mají důvěrné data uloženy přímo v paměti mikroprocesoru, tím se sníží potřeba on-line autorizací a s nimi spojených telekomunikačních poplatků přibližně o 80 – 90 %. V České republice je velkou překážkou celoplošného rozšíření platebních karet nedostatečná kvalita a vysoké ceny telekomunikací. Čipové karty mohou tento problém z větší části vyřešit. [3]

- Ochrana proti podvodům – čipové karty díky svému technickému řešení nabízí větší aktivní i pasivní ochranu proti výrobě padělků, proti zneužití karty neoprávněnou osobou a podvodným duplicitním transakcím. V paměti karty můžou být bezpečně uloženy informace o klientovi, např. PIN klienta, digitalizovaný podpis, fotografie a jiné.
- Úvěrový management – vydavatel karty může do paměti čipové karty uložit transakční, denní i týdenní finanční limity transakcí, které nemusí být ověřeny v reálném čase spojením s bankou. Během on-line transakce (např. v bankomatu) je možné tento limit kdykoli změnit podle finanční situace majitele karty.
- Doplňkové služby – přinášejí vyšší užitek bankám i uživatelům karet. Paměť karty umožní její souběžné použití pro bankovní i nebankovní aplikace (např. bonusy obchodních domů, identifikace zdravotních pojišťoven)

4. Typy platebních karet dle použití

Platební karty dle použití rozdělujeme na elektronickou, embosovanou a čipovou kartu (smart card). Prvotním a nejzákladnější kartou je karta s magnetickým pruhem, tj. karta elektronická. Elektronická karta s magnetickým pruhem, používá se v bankomatech a v místech vybavených elektronickým platebním terminálem. Poplatky za elektronickou kartu jsou zpravidla nižší než poplatky u karet embosovaných. Při transakci musíme zadávat čtyřmístný PIN. Elektronická karta je v ČR nejrozšířenější. Druhým typem je karta embosovaná. Tato platební karta s plasticky vyraženými údaji (jméno držitele, číslo karty atd. z karty vystupují) má větší uplatnění než karty elektronické, lze ji použít u prodejců s mechanickou (imprinterem – snímač používaný k otisku veškerých údajů z karty) nebo elektronickou čtečkou a také při platbě přes internet a v zahraničí.

Při transakci musíme zadávat PIN nebo stačí účtenku podepsat a obsluha podpis zkontroluje s podpisovým vzorem na zadní straně karty. Způsob ověřování se provádí dle zařízení, jež mají prodejci k dispozici. Pro výběr hotovosti je vždy nutné zadat PIN. Nejbezpečnější kartou je karta čipová nebo taky nazývaná jako smart card, která vyžaduje zadání PIN kódu při každé platbě. V poslední době se hodně rozšiřuje. Můžeme ji použít na více funkcí (např. karta na stravování, do knihovny, telefonní karta) a může se na ní nacházet více informací (např. zdravotní údaje pro případ nehody). Dělí se na paměťovou, paměťovou s autentizací logikou a na modernější

mikroprocesorovou kartu. Tyto tři druhy se od sebe liší použitou technologií, stupněm bezpečnosti, flexibilitou, počtem aplikací a výrobní cenou. [3]

4.1 Druhy karet z hlediska teritoria možného užití

V praxi jsou využity z hlediska možného využití na karty tuzemské a mezinárodní. Tuzemské karty používají se pouze na území daného státu. Jsou s nimi obvykle spojeny nižší poplatky i nižší nároky na bonitu klienta. Tyto karty se využívají také i v případech, kdy je tuzemská měna nesměnitelná. Rozdílem mezi tuzemskou a mezinárodní kartou je zejména ve využití karty, kde mezinárodní lze použít i v zahraničí, umožňují platit v zahraničí s lepším směnným kurzem, než kdybychom si měnili peníze ve směnárně a bez směnárenských poplatků. Obvykle je v této kartě zahrnuté cestovní a úrazové pojištění. U mezinárodních kreditních karet jsou poplatky vyšší než u karet domácích.

4.2 Rozdělení karet podle typu

Zvláštní skupinu bankovních platebních karet tvoří co-branded a affinity karty, které jsou vydávány ve spolupráci s další institucí. Banka chce získat vydáváním těchto karet nové klienty a spolupracující instituce chtějí získat provize z plateb provedených těmito kartami nebo zvýšit věrnost svých zákazníků.

Tabulka 1: Rozdělení karet podle typu

Typ	MasterCard	Visa
elektronická	Maestro	Electron
embosovaná	Standard	Classic
zlatá	Gold	Gold

Vývoj ukazuje, že co-branded a affinity karty mají vyšší frekvenci používání než je tomu u ostatních karet. Co-brandové platební karty – vznikají ve spolupráci vydavatele s nějakou společností z komerční sféry (např. mobilní operátoři, obchodní řetězce, letecké společnosti a další). Při platbě kartou získává držitel nějaké výhody, slevy či bonusové body. Tato platební karta přináší výhody všem zúčastněným (bance, držiteli i obchodním partnerům). Někdy je potřeba pro získání karty splnit určité podmínky jako je například členství v určité organizaci nebo uzavření smlouvy s obchodními partnery.

Co-brandovou kreditní kartu má například v nabídce Komerční banka. Ta nabízí ve spolupráci s mobilním operátorem T-Mobile kartu T-Mobile bonus. Držitelem karty je zákazník T-Mobile, a používáním této karty získává různé výhody v podobě volných minut volání, SMS, mobilních telefonů, slev u vybraných obchodníků a další. Držitelem karty přitom nemusí být klient Komerční banky. S mobilním operátorem spolupracuje také Citibank. Tato banka s O2 nabízí kreditní kartu, díky které lze získat slevy na služby O2 a další slevy u vybraných partnerů. UniCredit Bank má v nabídce co-brandové kreditní karty ve spolupráci s penzijním fondem AXA, pojišťovnou Generali, ČSA, Škodou Auto a jinými značkami. [5]

Obr.2 Co-branded Card

4.3 Affinity karty

Affinity jsou karty vydávané bankami nebo specializovanými organizacemi společně s nekomerčními subjekty, jako jsou např. profesní sdružení, charitativní organizace nebo nadace. Jejich cílem je pro platební karty konkrétního vydavatele získat skupinu osob, které spojuje společné povolání (lékaři, právníci ap.), společné zájmy (ochrana zvířat, ochrana přírody, charitativní činnost aj.) nebo členství v zájmových klubech (např. sportovních). Aby byl kartový program úspěšný, musí členům cílové skupiny přinést zvláštní hodnotu navíc. Příklad Affinity Card: Cary for the Wild – Elephant Relocation Project Eurocard/MasterCard. Tento projekt Bank of Scotland přinesl během prvního roku 250 000 GBP, které byly použity na záchranu 500 slonů v Zimbabwe jejich přemístěním do oblasti s vhodnějšími životními podmínkami. V České republice Affinity Card nabízí Raiffeisenbank, z každé platby přispívá do fondu National Geographic. [6]

Obr.3 Affinity Card

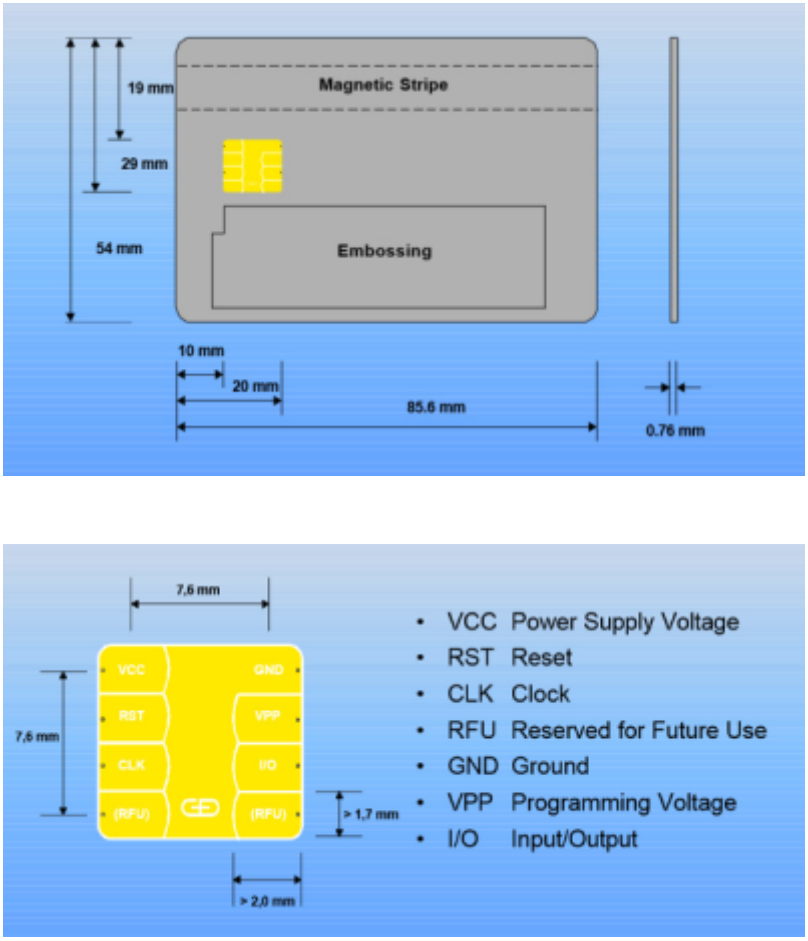
4.4 Technické parametry bezkontaktního čipu

Existují dva základní typy provedení čipové karty podle způsobu přenosu informace mezi kartou a čtecím zařízením. Bezkontaktní karta obsahuje pouze bezkontaktní čip. Zabudovaný mikroprocesor spolu s karetním operačním systémem nabízí mimo jiné i

bezpečnostní funkce prostřednictvím integrovaných kryptografických algoritmů, jako např. DES, 3DES, RSA atd. Vhodné pro všechny typy aplikací, které vyžadují inteligentní karty (platební aplikace, kombinované věrnostní systémy, PKI systémy).

Proximity Card (ISO 14443)

- f= 13,56MHz, L=0-10cm
- Paměťové i procesorové karty s kryptografií
- Přenosová rychlost 106-424 kbit/s
- Antikolizní systém
- Vicinity Card (ISO 15693) Special Tag (ISO 18000)
- f=13,56MHz,900 MHz 2,45GHz (směrové antény)
- L=cca1.5m u směrových antén 10m
- Obsahují pouze ID číslo bez podpory kryptografie



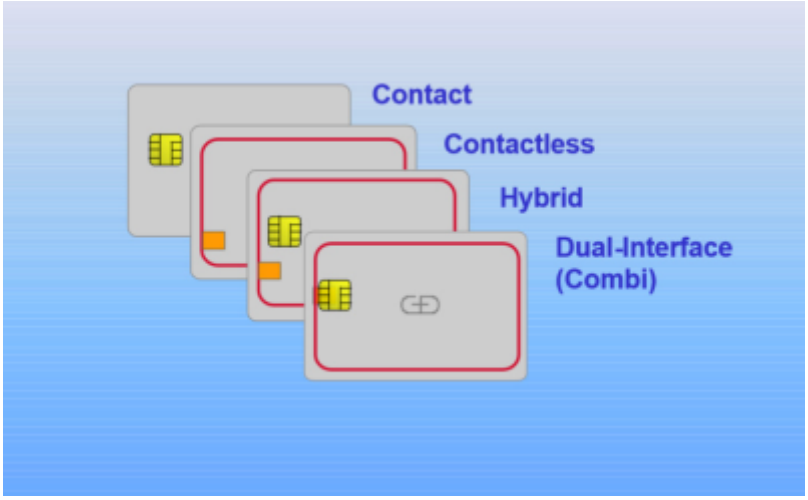
Obr. 4 Rozmístění čipové karty & čip

Závěr

Karty s kontaktním čipem se často kombinují s jinými druhy personalizačních prvků jako je např. magnetický proužek nebo tisk personifikační číselné řady. Možností nabízejí kontaktní čipové karty mnoho, v zásadě je však nutné pro stanovení cenové nabídky specifikovat typ čipu i další požadavky podle předpokládané využitelnosti karet. Karty kontaktní bývají také vyráběny zároveň s čipem bezkontaktním. – viz níže (duální a hybridní karty). S kontaktními čipovými kartami se setkáváme především v bankovním sektoru, kde bývají kombinovány právě s magnetickými pruhy, v

hotelových systémech, jako telefonní karty, aj. Co je třeba k realizaci zabezpečení prostřednictvím čipové karty:

- čipová karta PKI s implementovanou kryptografií,
- vhodná čtečka čipových karet (nejlépe PC/SC) s libovolným rozhraním pro připojení k PC,
- programové vybavení pro integraci čipové karty do hostitelského systému,
- programová podpora pro správu čipové karty



Obr. 5 Přehled čipových karet

Literatura

1. TRENT. A Fascinating Look At Edward Bellamy, Inventor Of The Credit Card, [online]. 2007-02-16, www.thesimpledollar.com
2. BUČKOVÁ, Veronika. Jaké výhody přináší kreditní karty?
3. Pramen: DVOŘÁK, Petr. Bankovnictví pro bankéře a klienty. Bankovnictví [online]. [cit. 2. červen 2012]
4. PIJÁK, Michal. Platební karta – jakou vybrat? Card [online]. [cit. 3.brezna 2014]
5. Zdroj: Affinity Card [online]. [cit. 25. února 2010] Dostupné z: http://www.ruffedgrousesociety.org/Affinity-Card
6. Zdroj: T-Mobile Bonus kreditní karta [online]. [cit. 1. března 2010] Dostupné z: http://www.kb.cz/cs/seg/seg1/products/tmobile_bonus_card.shtm