PAMETNA KARTICA

Aleksandar Jurišić, Department of Combinatorics and Optimization,
University of Waterloo, Waterloo, Canada, N2L 3G1 & Certicom Corp., Mississauga

Alenka Trojar, School of Business and Economics, Wilfrid Laurier, University Waterloo, Canada

Povzetek

Pametne kartice nudijo stopnjo varnosti, ki je potrebna, da računalniške mreže zares zaživijo, ter združijo telekomunikacije in računalnike. Po kratkem zgodovinskem pregledu razvoja kartic sledijo opisi treh pomnilnih kartic, ki pripomorejo k boljšemu razumevanju prednosti pametnih kartic. Z dvema primeroma so opisani vidiki varnosti in zaščite pametnih kartic. Seznanimo se tudi z osnovnimi komponentami in karakteristikami pametnih kartic. Sledi pregled sedanje uporabe pametne kartice in možnosti v prihodnosti.

Abstract

Smart cards provide the degree of security necessary to make computer networking truly viable. They unify telecommunications and computing. After a brief historical overview of the developement of cards, we survey three basic types of memory cards, in order to better understand the advantages of smart cards. The security aspects of smart cards are illustrated by two examples. Applications of smart cards are surveyed and a view for their future possibilities is given.

1. Uvod

Večina ljudi ima danes vsaj eno kreditno kartico. V mnogih deželah uporabljajo tudi telefonske kartice, kartice za avtomate, zdravstvene kartice in še mnoge druge. Današnja tehnologija lahko vse te kartice nadomesti s kartico, ki ima različne funkcije in zagotavlja veliko varnost lastniku ter računalnikom, s katerimi kartica komunicira. Taka kartica se imenuje pametna kartica (Smart Card) in se poskusno uporablja že po vsem svetu. Ima enako velikost kot običajna kreditna kartica in vsebuje eno ali več tiskanih vezij s funkcijami procesorja, pomnilnika in vhodno-izhodne enote. Pametna kartica nam bo omogočila, da bomo kmalu nosili računalnik kar v žepu. S temi lastnostmi bo pametna kartica postala pomembna možnost za varno shranjevanje ter izmenjavo podatkov in bo izboljšala varnost računalniških sistemov.

Osnovne funkcije pametnih kartic so:

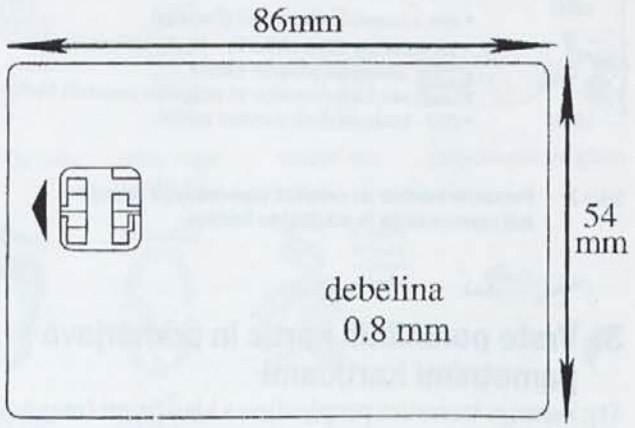
- prenašanje podatkov (pametna kartica omogoča varen način shranjevanja in prenašanja podatkov ter varen dostop do informacij)
- prepoznavanje lastnika kartice (pametna kartica prepozna lastnika in onemogoči, da bi kdo prevzel njegovo identiteto)
- nadomestilo za denar ter varno plačilno poslovanje.

Po kratkem zgodovinskem pregledu v 2. poglavju sledijo opisi treh pomnilnih kartic, ki pripomorejo k boljšemu razumevanju prednosti pametnih kartic. V 4. poglavju so opisane prednosti pametne kartice na področju varnosti in zaščite z dvema primeroma. V 5. poglavju pa se seznanimo z osnovnimi komponentami in karakteristikami pametnih kartic.

Tehnični del članka se zaključuje z opisom sistema pametne kartice. V 7. poglavju podajamo pregled mnogih načinov uporabe pametne kartice, v 8. pa njene možnosti v prihodnosti.

2. Kratka zgodovina

Desetletja so uporabljali papirnate kartice (vizitke) z imenom, priimkom in naslovom za osebno predstavitev



Slika 1: **Dimenzije kartice in lega kontaktov so določeni s standardom ISO 7816.**

in za krajša sporočila. Leta 1930 so se pojavile plastične kartice, ki jih je bančna industrija začela uporabljati kot kreditne kartice. Diner's Club in American Express sta predstavila prve take kartice v 50-ih letih. Leta 1967 so začeli plastičnim karticam dodajati magnetni trak. Kasnejši standardi pa so omogočili, da je uporaba magnetne kartice postala mednarodna.

Z razvojem računalnikov in komunikacijskih sistemov v zadnjih 20-ih letih je postala potreba po učinkovitem in varnem komuniciranju vedno nujnejša in pomembnejša. Konec 70-ih let je Francoz Moreno prijavil patent - čip, vgrajen v kreditno kartico. Tako pametno kartico je mogoče programirati za različne funkcije in jo usposobiti za kontrolo računalniškega povezovanja z zunanjo enoto. Sredi 80-ih let so v Angliji in ZDA razvili kontaktne in brezkontaktne pametne kartice in začeli razvijati njihove standarde. V svetu pametnih kartic pa je najbolj pomembna prav standardizacija. Kartice različnih proizvajalcev morajo biti usklajene za interakcijo z računalniki. V naslednjih petih, desetih letih pričakujemo nagel razvoj uporab pametne kartice, vse dokler ne bodo pametne kartice zares postale računalnik v našem žepu.

Slika 2: **Pametne kartice so rezultat vzporednega razvoja mikroprocesorja in magnetne kartice.**

3. Vrste pomnilnih kartic in primerjava s pametnimi karticami

Trg kartic je trenutno preplavljen s klasičnimi (magnetnimi) karticami ter različnimi novimi karticami. Da bi lažje razumeli prednosti pametne kartice in njeno potencialno tržišče, bomo najprej opisali značilosti pasivnih (pomnilnih) kartic, ki so trenutno najbolj v rabi.

Pasivne ali pomnilne kartice se uporabljajo predvsem za shranjevanje podatkov. Delimo jih v tri skupine: magnetne kartice, optične kartice in kartice s čipom.

(a) Magnetne kartice

Zaradi vse večje potrebe po avtomatizaciji v bančništvu so plastični kartici dodali magnetni trak. Le-ta deluje podobno kot avdio trak za snemanje; nekateri trakovi imajo tudi bralni del (*read-only*), kar pomeni, da lahko podatke samo beremo, ne pa tudi spreminjamo. Kljub temu pa je varnost te kartice pomanjkljiva, saj je magnetni trak izredno lahko posneti in kartico ponarediti. Pomanjkljivost kartice je tudi majhen pomnilnik (manj kot 900 zlogov). Vseeno pa je magnetna kartica trenutno najbolj razširjena zaradi nizkih stroškov proizvodnje ter pomnilne zmogljivosti, ki povsem zadošča za preproste vrste uporabe.

(b) Optične kartice

Glavna značilnost optične kartice je, da vsebine kartice ne moremo izbrisati. Te kartice delujejo po načelu "enkrat zapiši, večkrat preberi" (*write-once read-many times*). Za branje in pisanje na kartico se uporabljajo laserji, ki izžgejo milijon drobnih luknjic v tanek list optičnega traku (mesto z luknjico ali brez nje predstavlja stanje bita). Optična kartica ima izredno veliko pomnilno zmogljivost, saj nanjo lahko spravimo že od 2 do 8 MB podatkov. Zaradi te lastnosti se je kartica izkazala predvsem v zdravstvu in netiskanih publikacijah (CD-ROM, Internet). V primerjavi s pametno kartico ima optična kartica prednost predvsem zaradi velikega pomnilnika in nizke cene.

(c) Kartice s čipom

Razlikujemo dve vrsti kartic s čipom, pomnilne kartice ter pametne kartice. Pomnilne kartice s čipom imajo običajno manj pomnilnika kot pametne kartice ter lahko izvajajo manjše logične operacije s pomočjo integriranih vezij. Vendar pa te kartice nimajo logike v smislu procesorja in jih zato ne moremo ponovno programirati. Kartice s čipom se uporabljajo predvsem kot telefonske kartice.

Zadnja novost na trgu kartic je kartica s čipom obsežnega pomnilnika (do 32MB). Združenje *The Personal Computer Memory Card Industry Association* (PCMCIA) je uvedlo standard izdelave kartic in sicer v velikosti kreditne kartice, z izjemo debeline. Uporabljajo se predvsem za povečanje pomnilnika v prenosnih računalnikih ter za prenos podatkov.

Novi materiali (plastika) in značilnosti (magnetni trak, površina na optičnih karticah, čipi) so izredno povečali trg kartic. Po nekaterih ocenah se uporablja že

tri milijarde različnih kartic. Prednost varnega komuniciranja dela kartico vse bolj konkurenčno za uporabo pri denarnih zadevah. Pametna kartica stane od manj kot 1 ameriški dolar do 20 dolarjev (USD), medtem ko stanejo optične kartice od 4 do 8 USD, magnetne kartice pa stanejo od 10 do 50 centov, glede na to, ali vsebujejo sliko, hologram. Čeprav je cena pametnih kartic višja od cen drugih kartic, so jih nekatere dežele (Anglija, Japonska, Francija, Nemčija) že pričele uvajati. Uporaba pametnih kartic raste in ta trend se bo verjetno še povečeval, ko se bodo zniževali stroški proizvodnje.

4. Zakaj pametne kartice

Ker večina ljudi še vedno uporablja magnetno kartico, bomo podrobneje razložili, zakaj bo pametna kartica nadomestila magnetno kartico. Za razliko od pametnih kartic so magnetne kartice povsem pasivne (uporabljajo se v glavnem za hranjenje podatkov). Magnetna kartica dopušča različne oblike zlorabe, na primer prekoračitev računa, saj se večina nakupov ne zapisuje takoj v glavnem računalniku (nepovezani sistemi se vedno bolj uveljavljajo). Tudi ponarejanje in kopiranje magnetnih kartic ni redek pojav. Metode so ponavadi zelo rafinirane. Mogoče je kopirati informacije z magnetnega traku na prazno kartico in nanjo vtisniti podatke z originalne kartice

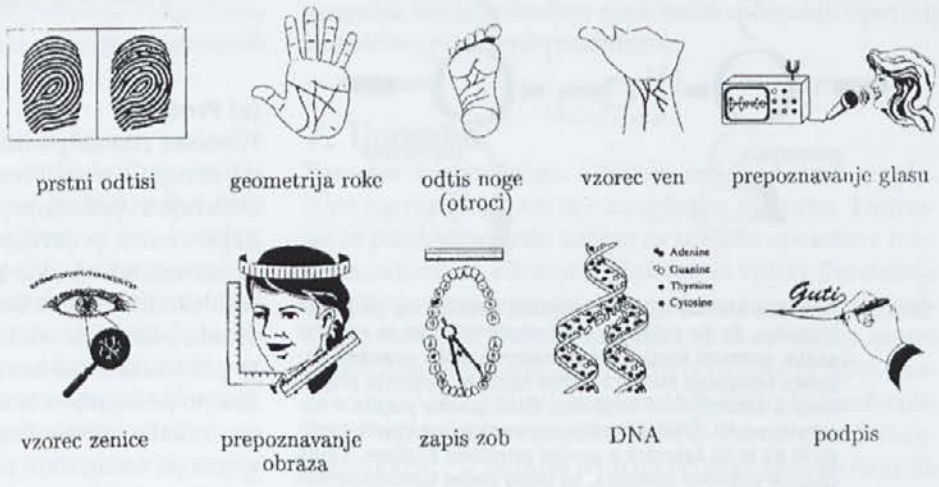
Kadar uporabljamo magnetno kartico v bankomatu, le-ta najprej "vpraša" lastnika kartice za geslo in ga pošlje glavnemu računalniku v banki skupaj z zakodiranim geslom z magnetnega traku. Računalnik zakodira še vtipkano geslo in opravi primerjavo. Geslo potuje po linijah nezaščiteno in tako lahko nekdo, ki prisluškuje povezavi med bankomatom in računalnikom ali pa ima dostop do gesel na glavnem računalniku v banki, geslo ukrade.

Pametna kartica ima dve značilnosti, ki onemogočata zgoraj omenjene zlorabe in ponarejanje. Ena od teh je obstojni pomnilnik, ki se ga ne da spreminjati in se ohrani tudi po prekinitvi napajanja. Ta pomnilnik lahko vsebuje tudi podatke, ki so bili zapisani po tem, ko je bila kartica izdana, in lahko zabeleži vsako transakcijo. S tem preprečuje lastniku, da bi prekoračil svoj limit. Druga značilnost pa je, da procesor kartice nadzira vse interakcije med raznimi zunanjimi napravami, ki berejo kartico in pišejo nanjo, in pomnilnikom pametne kartice. Ta je oblikovan tako, da so določeni deli pomnilnika fizično in logično dostopni le izdajatelju kartice.

Naslednja dva primera kažeta, zakaj sta omenjeni značilnosti tako pomembni za zagotovljanje varnosti pri prepoznavanju. Le-to se opravlja v dveh delih: najprej se mora kartica prepričati, da jo uporablja njen lastnik, nato pa komunicira (varno) z glavnim računalnikom.

Oglejmo si bolj podrobno, kako lahko lastnik dokaže svojo identiteto kartici. Recimo, da podjetje hrani podatke v glavnem računalniku, do katerega je možen dostop s pametnimi karticami. Le-te so izdali zaposlenim, ki imajo dovoljenje za dostop do računalniškega sistema. Vsaka kartica je programirana z edinstvenimi informacijami, kot je na primer osebna prepoznavna številka PIN *(personal identification number)*. Prepoznavna številka je zakodirana z enosmerno transformacijo *(hash function)* in shranjena v posebnem delu pomnilnika (v tajnem področju - *secret zone*), ki ga ni mogoče brati. Ko zaposleni želi dostop do računalniškega sistema, mora vstaviti kartico v vhodno-izhodno enoto in vtipkati PIN. Procesor pametne kartice izvede enosmerno transformacijo vtipkane številke ter jo primerja s shranjeno prepoznavno številko v tajnem področju. Ta primerjava poteka v procesorju kartice. Pomembno je, da PIN ne potuje prek nezanesljivih linij in se ne vpisuje v delovni pomnilnik glavnega računalnika (ki bi ga lahko kdo opazoval). Če pametna kartica potrdi, da se prepoznavni številki ujemata, se prične drugi del prepoznavanja, ko pametna kartica komunicira z glavnim računalnikom in omogoči zaposlenemu dostop do računalniškega sistema.

Čeprav se osebna prepoznavna številka lokalno preverja, njena dolžina (štiri številke) ne zadostuje za varnost. To pomanjkljivost poskušajo odpraviti z omejitvijo števila poskusov vnašanja gesla ali pa z dodatnim preverjanjem, na primer prstnih odtisov, geometrije roke, podpisa, vzorca zenice, s prepoznavanjem glasu itd. (glej sliko 3).



Slika 3: **Biometrični testi**

Sedaj pa si podrobneje oglejmo še drugi del prepoznavanja. Ko smo uspešno opravili prvi del prepoznavanja in je kartica prepričana, da jo zares uporablja njen lastnik, prične kartica komunicirati z glavnim računalnikom. To lahko ponazorimo s hipotetično situacijo:

Temno je kot v rogu in po opravljeni diverziji v sovražnem taboru se vohun vrača v grad. Bližajoč se vratom, zasliši šepetajoč glas:

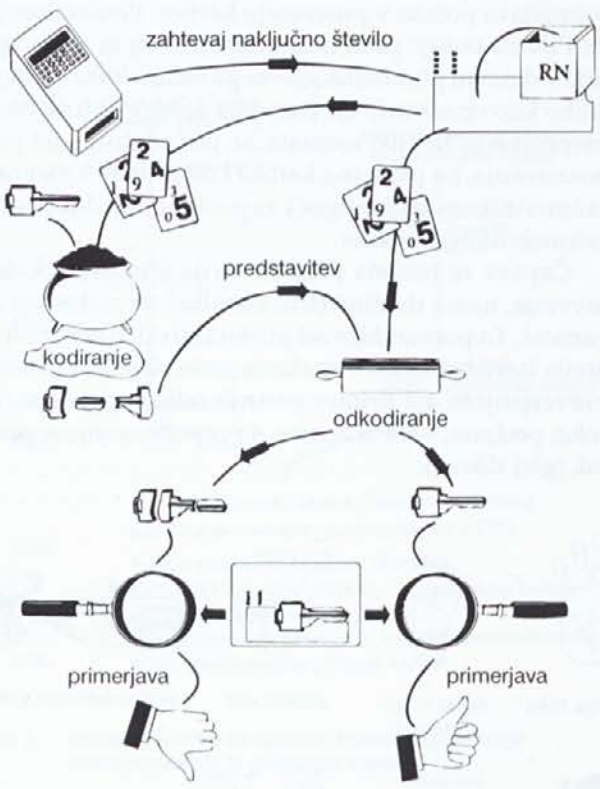
"Geslo ali streljam!"

Ali šepeta prijatelj ali sovražnik?

Kako lahko vohun prepriča stražarja, da pozna geslo, ne da bi ga pri tem izdal morebitnemu sovražniku-prisluškovalcu? McGeoch [17].

Vohunova dilema je vsakdanji problem v telekomunikacijah. Kadar kartica v bankomatu komunicira z banko, morata biti oba prepričana o pristnosti drug drugega. Iz tega sledi, da morajo biti elektronska gesla taka, da jih ni mogoče ponarediti in da ne koristijo prisluškovalcu. Ena od metod za varno izmenjavo gesel v tem kontekstu se imenuje dokaz brez znanja *(zero-knowledge proof)*, kar pomeni, da dokažeš (z odgovori na serijo vprašanj), da poznaš svoje geslo, a pri tem ne izdaš niti en sam bit gesla. Glej [17], [13] in [20].

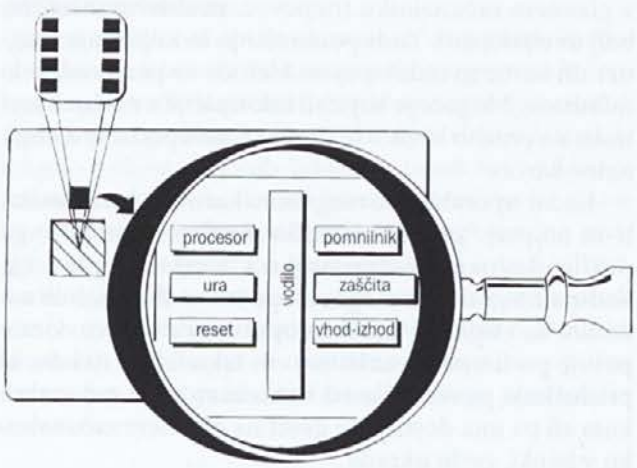
Glede na pomembnost podatkov, ki jih varujemo, se odločimo za ustrezno obliko zaščite. Geslo oziroma PIN pomeni osnovno zaščito, DES *(Data Encryption Standard)* [5], [25] nudi srednji, shema javnih ključev *(Public Key Scheme - PKS)* [12], [8], [9, Ch.13,14], [15] pa visok nivo zaščite



Slika 4: **Pametna kartica ustvari naključno število, ter ga pošlje čitalniku. Ta ga zakodira s privatnim ključem in rezultat pošlje pametni kartici. Če pametna kartica uspešno dekodira naključno število z javnim ključem, potem je prepričana o avtentičnosti čitalnika. Enak proces poteka v nasprotni smeri. Čitalnik pošlje novo naključno število kartici, ki ga le-ta zakodira s svojim privatnim ključem. Če ga čitalnik uspešno dekodira, se lahko začne komunikacijski proces.**

5. Sestavine in vrste pametnih kartic

Mikroračunalnik pametne kartice je majhen računalnik, ki vsebuje vse tri osnovne mikroračunalniške sestavine: procesor, pomnilnik in vhodno-izhodno enoto (ne vsebuje pa vseh integriranih vezij kot osebni računalnik).



Slika 5: **Mikročunalnik pametne kartice ima površino največ 5 mm x 5 mm, sicer bi ga lahko prožnost kartice poškodovala.**

(a) Procesor

Procesor naredi pametno kartico "pametno", različno od drugih kartic. Procesor ima dve osnovni funkciji: obdeluje in prikazuje podatke. Trenutno so v rabi 8-bitni procesorji, pojavljajo pa se tudi že 16-bitni. Operacijski sistem odloča, kje bodo shranjeni podatki in v kakšnih okoliščinah se bo izvedel prenos informacij prek vhodno-izhodne enote. Kartica poskrbi za samouničenje pri vsakem nenormalnem stanju (segrevanje ali fizično poseganje v notranjost kartice zaznavajo varnostna stikala - *temper resistent switches)*. Uporabniški programi pa omogočajo prepoznavanje, varnost poslovanja itd.

Nekatere vrste pametnih kartic vsebujejo tudi kripto-koprocesorje za hitro kodiranje ali dekodiranje oziroma za izdelavo digitalnih podpisov (*digital signatures*), ki overovljajo poslovne informacije ali pa potrjujejo njihovo identiteto. Več o tem si lahko preberete v [2] in [4].

(b) Pomnilnik

Pomnilnik je lahko obstojen (*non-volatile*) ali začasen (*volatile*), glede na to, ali se podatki ohranijo ali izgubijo po prekinitvi napajanja, oziroma ko računalnik ugasnemo. Pametna kartica mora imeti obstojen pomnilnik, ki hrani podatke, kot so ime nosilca kartice, in uporabniške programe itd. Imeti mora tudi pomnilnik, kamor se vpisujejo sprotne informacije, na primer stanje po pravkar opravljenem poslu.

Na splošno ima pametna kartica tri vrste pomnilnika:

- bralni pomnilnik (ROM) - za shranitev operacijskega sistema
- bralno-pisalni pomnilnik (RAM) - za začasno shranjevanje podatkov
- programabilni bralni pomnilnik (PROM), ki ga lahko delimo v izbrisljivi programabilni bralni pomnilnik (EPROM) ali v električno izbrisljivi programabilni bralni pomnilnik (EEPROM).

EPROM se lahko uporablja v pametni kartici za trajno shranjevanje zapisov skozi njeno življenjsko dobo. EPROM ji omogoča večjo pomnilno zmogljivost kot drugi pomnilniki, vendar pa je podatke mogoče le zapisovati in ne brisati, tako da se pomnilnik po določenem času napolni in kartici se izteče življenjska doba. Prve pametne kartice so imele EPROM, sedaj pa se vse bolj uveljavlja uporaba EEPROM-a s kapaciteto od 100 zlogov do 64KB. EEPROM se uporablja za shranjevanje programov in podatkov, ki se periodično spreminjanjo. Ker se EEPROM lahko izbriše z elektronskim signalom, kartica ne zapade, ko je pomnilnik poln. EEPROM ima manjšo pomnilno kapaciteto in je dražji kot drugi tipi pomnilnika ter potrebuje več integriranega vezja. Zaradi tega ni ustrezen za shranjevanje zapisov posameznih poslov.

PROM je razdeljen v tri področja. V tajnem področju (*secret zone*) so lahko shranjeni podatki, ki jih uporablja samo procesor, na primer lastnikovo geslo, kreditni limit itd. Drugi podatki, na primer priimek in ime lastnika, naslov, so shranjeni v odprtem področju (*open zone*), in jih lahko preberemo z različnimi čitalniki, a jih ne moremo spreminjati. Delovno področje (*working zone*) vsebuje zapis podatkov, ki se nanašajo na funkcijo kartice in jih je potrebno spreminjati (na primer zapisi nakupov). V delovnem področju se lahko piše (in bere) samo pri določenih pogojih, na primer če je kartica v čitalniku oziroma blagajni pri pooblaščenem prodajalcu.

(c) Vhodno-izhodna enota

Vmesnike pametne kartice delimo na kontaktne in brezkontaktne.

Kontaktna kartica se napaja in komunicira prek kovinskih kontaktov. Brezkontaktna kartica pa nima neposrednega kontakta in je ni potrebno nikamor vložiti. Podatke in energijo prenaša na več načinov, na primer z induktivnim sklopom, z optičnim sklopom zmogljivosti, z mikrovalovnim sklopom itd., in glede na to deluje na razdalji 1 mm ali pa nekaj metrov (na primer na avtocesti čitalnik zazna brezkontaktno kartico v avtu, ki vozi do 100 km na uro). Brezkontaktna kartica ima številne prednosti pred kontaktno kartico, saj je zanesljivejša, njena življenjska doba je daljša ter omogoča hitrejšo in bolj enostavno uporabo. Čitalna naprava nima reže, tako je manj možnosti za vandalizem (na primer lepilo, žvečilni gumi v reži).

6. Sistem pametne kartice

Sistem pametne kartice lahko vsebuje pisalno-čitalno enoto (*writer-reader unit - WRU*), tiskalnik in osebni računalnik.

Oglejmo si primer, ko se pametna kartica uporablja kot kreditna kartica (potovalni ček) in komunicira s čitalnikom v trenutku prodaje. Kaj se dogaja v čitalniku kartice? Lastnik vloži svojo pametno kartico v čitalnik, vtipka PIN, kartica in čitalnik pa preverita avtentičnost drug drugega. Kupec potrdi vrednost nakupa, čitalnik pa sporoči kartici, naj zabeleži nakup in zmanjša svojo vrednost za ceno prodanega blaga. Ko je transakcija zaključena, čitalnik izvrže kartico.

Čitalniki v trgovinah se občasno povezujejo z glavnim računalnikom v banki, da mu sporočajo opravljene transakcije in obnovijo seznam ukradenih kartic. Čitalnik pametne kartice imamo lahko tudi doma, kjer ga povežemo z računalnikom, tiskalnikom ali televizorjem, da si ogledamo tekoče podatke o opravljenih nakupih in stanje našega računa v banki. Sistem pametne kartice poveča prilagodljivost in varnost v mnogih primerih uporabe, ker je sposoben zapletenih računskih operacij in zaščite spravljenih podatkov.

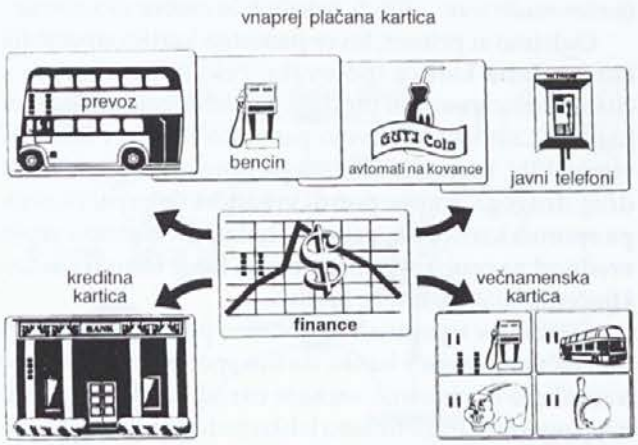
7. Uporaba

Pametne kartice lahko v širšem smislu delimo na plačilne kartice in na kartice za splošno uporabo. Trenutno so predvsem v rabi kartice za splošno uporabo v telekomunikacijah, zdravstvu, šolstvu in vojski. Precejšnje investicije v bankomate in že vpeljana uporaba magnetnih kartic v plačilne namene sta vsekakor vzroka za trenutno neenakomerno porazdeljeno tržišče (v ZDA imajo sedaj 13.000 čitalnikov pametnih kartic in kar 5 milijonov naprav za magnetne kartice). Porast zlorab magnetne kartice v zadnjih letih pa bo prav gotovo nagnila tehtnico v prid pametni kartici.

(a) Plačilne kartice

Za plačevanje se pogosto uporablja vnaprej plačana kartica (*prepaid card*). S tako kartico lahko plačamo toliko zneskov, kolikor denarja smo položili nanjo, in je zlasti uporabna za nepovezane sisteme (*off-line*). Vnaprej plačano kartico uporabljamo predvsem za plačevanje avtomatov (običajno na kovance), kot so javni telefon, fotokopirni in pralni stroj, parkirna ura, prodaja hrane in pijače. Raje uporabljamo nepovezane sisteme, saj so hitri in poceni. Čeprav so zneski plačila majhni, je pretok denarja velik, plačevanje pa izredno poenostavljeno. Državne banke pa opozarjajo, da gre v teh primerih za novo metodo tiskanja denarja brez ustaljenih določil, kdo garantira za izdano vrednost.

Pametne kartice se bodo kmalu uporabljale kot nadomestilo za denar in čeke, se pravi, da bomo namesto gotovine uporabljali elektronsko gotovino, namesto papirnatega čeka pa elektronski ček ali elektronski potovalni ček (vnaprej položen denar je mogoče porabiti v katerikoli valuti). Pametna kartica bo v resnici postala elektronska denarnica in bo zagotavljala tudi kreditno sposobnost.



Slika 6: **Plačilne, kreditne in večnamenske kartice, ki se uporabljajo na področju financ.**

Slika 7: **Področja v zdravstvu, kjer se uporabljajo pametne kartice**

(b) Uporaba v zdravstvu

V zdravstvu nudijo pametne kartice celo paleto storitev, na primer prepoznavanje, vodenje administracije, kot so zapisi o izdanih receptih, boleznih, cepljenjih, pregledih, plačevanju, skratka vse zdravstvene informacije o lastniku kartice, njegovih zdravnikih (v urgentnih primerih) ter komunikacijo med zdravniki, pri tem pa ohranijo zasebnost podatkov. Poenostavljajo administracijo in omogočajo geografsko mobilnost (na primer bolnikom, ki potrebujejo dializo). Problem povzroča samo nezadosten pomnilnik, ki pa se ga da bolje izkoristiti z uporabo mednarodno uveljavljenih kratic za diagnoze, zdravila in podobno.

(c) Uporaba v šolstvu - na univerzah

Zapis na pametni kartici vsebuje informacije o študentu, tako akademske kot administrativne. Hkrati pa kartica omogoča prepoznavanje in vstop v knjižnice, laboratorije, športne ter druge objekte. Ker je univerza svet v malem, se je študentska pametna kartica prva približala večnamenski kartici, s tremi glavnimi funkcijami, te pa so podatkovna baza, nadzor dostopa in elektronska denarnica.

Slika 8: **Uporaba pametnih kartic na univerzi**

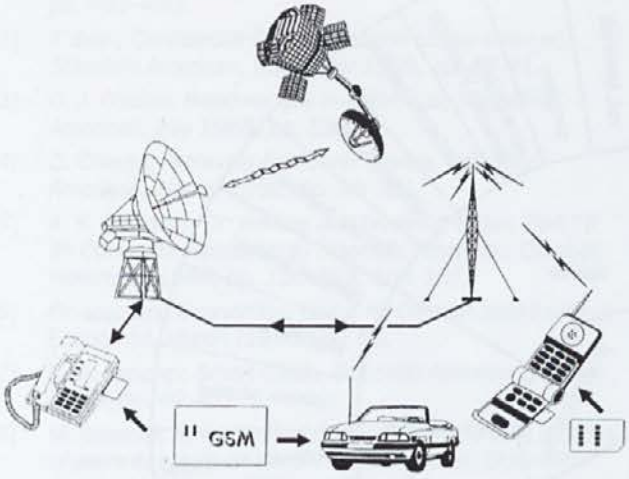
(d) Uporaba v telekomunikacijah

Javni telefoni so daleč največji uporabniki kartic s čipom. Večina telefonskih kartic so vnaprej plačane kartice (*prepaid cards*) in zaenkrat nimajo procesorja, marveč le nekaj logike v obliki integriranega vezja, z ne več kot 100 zlogov pomnilnika. So izredno zanesljive in poceni. Lahko hranijo tudi izbrane telefonske številke in omogočajo hitro klicanje teh številk (*speed dialing*).

Nekatera telefonska podjetja pa že nudijo telefone s pametnimi karticami.

Danes je mogoče dobiti številke, ki niso vezane na telefonski priključek, marveč na pametno kartico, že v 85-ih državah. V tem primeru je pametna kartica v bistvu sledni telefon" (*follow-me phone*), kar pomeni, da kjerkoli vložimo pametno kartico v telefon in vtipkamo osebno prepoznavno številko, lahko sprejmemo telefonski klic ali pa kličemo sami. Telefon je lahko osebna last ali pa je na razpolago v taksijih, letalih, ladjah, v sposojenih avtomobilih, javnih govorilnicah itd.

Ta sistem se je začel razvijati leta 1987 in se imenuje GSM *(Global System for Mobile Communications)*. Gre za mednarodni mobilni telefonski sistem, ki temelji na digitalnem prenosu in značilostih pametne kartice. Ima že prek 10 milijonov naročnikov in se bo kmalu razširil po vsem svetu. Uporabnikova kartica potrjuje njegovo identiteto *(Subscriber Identity Module - SIM)*. Ko kartico vložimo v telefon, GSM uporabi podatke na kartici in prepoznavno številko za preverjanje naročnikove identitete, klic pa se obračuna v matični državi. Hkrati lahko pametna kartica omogoča tudi šifriran prenos in s tem preprečuje prisluškovanje.



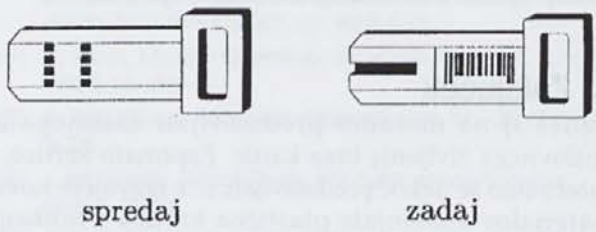
Slika 9: **GSM *(Globalni sistem za prenosno komuniciranje)***

(e) Varovanje podatkov in računalniškega sistema

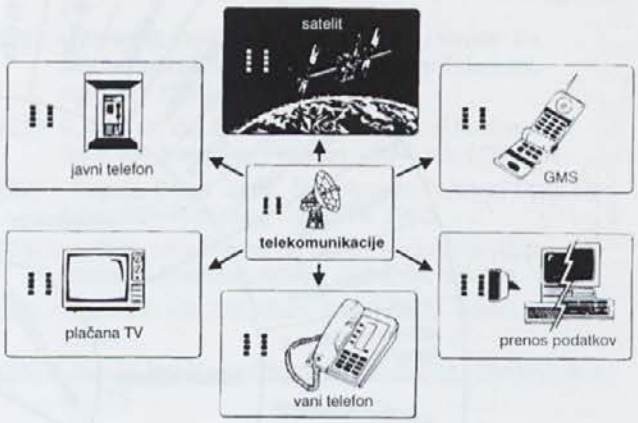
Pametne kartice se lahko uporabljajo kot varnostna ključavnica za računalnike in diske. Če ne vtipkamo pravilnega gesla ali če pametna kartica ni prisotna, se tipkovnica oziroma sistem zaklene. Informacije na disku ali pa kakšnem drugem podatkovnem mediju je moč zakodirati s ključem, ki je bil dodeljen lastniku in spravljen v pametni kartici. Podobno se lahko zaščiti tudi komunikacija med različnimi računalniki.

(f) Plačani televizijski programi

Določene televizijske programe je treba posebej plačati in so zakodirani. Če jih hočemo gledati, moramo plačati naročnino ter dobiti posebno napravo, ki zna program odkodirati. Da pa ne bi prišlo do ponarejanja teh naprav (predvsem kadar je na voljo samo enosmerna komunikacija od televizijskega podjetja do gledalca), je dobro uvesti gesla in jih pogosto zamenjevati, same naprave pa opremljati z ustreznimi kodami. Ta problem se da enostavno rešiti s pametno kartico, saj je veliko lažje menjavati gesla na kartici ali pa kartice kot pa same kodirne naprave.



Slika 10: **Za plačane televizijske programe (pay-TV) se običajno uporablja pametna kartica v obliki ključa.**



Slika 11: **Uporaba pametne kartice v telekomunikacijah in uporabniški elektroniki**

(g) Uporaba v vojski

Pametna kartica ima izredno pomembno vlogo v vojski, saj med drugim omogoča nadziranje gibanja, dostop do raznih objektov, uporabo orožja ter zagotavlja tajnost komunikacij.

(h) Druge vrste uporabe

Pametne kartice se uporabljajo na različnih področjih, tudi v transportu, hotelih, pri športu, na razstaviščih, črpalkah

in še marsikje. Kartica lahko vsebuje zapis podatkov ali rezultatov, na primer na borzi. V Angliji so nadomestili vstavljanje kovancev v posebne merilnike za uporabo kurjave in elektrike z vnaprej plačano pametno kartico.

Pametne kartice postajajo vse bolj popularne na vseh koncih sveta. Tako so jih s pridom uporabljali tudi na olimpijskih igrah v Atlanti leta 1996. Vsak športnik je dobil svojo pametno kartico, ki jo je uporabljal za prepoznavanje, kot elektronsko denarnico in za dostop v razne objekte. Več kot milijon vnaprej plačanih kartic so uporabljali v tisočih trgovinah.

Obstajajo tudi druge možnosti uporabe pametne kartice, ki pa zaenkrat se niso tako razširjene, na primer za dostop v zabavišče, kino, gledališče, kot potni list itd.

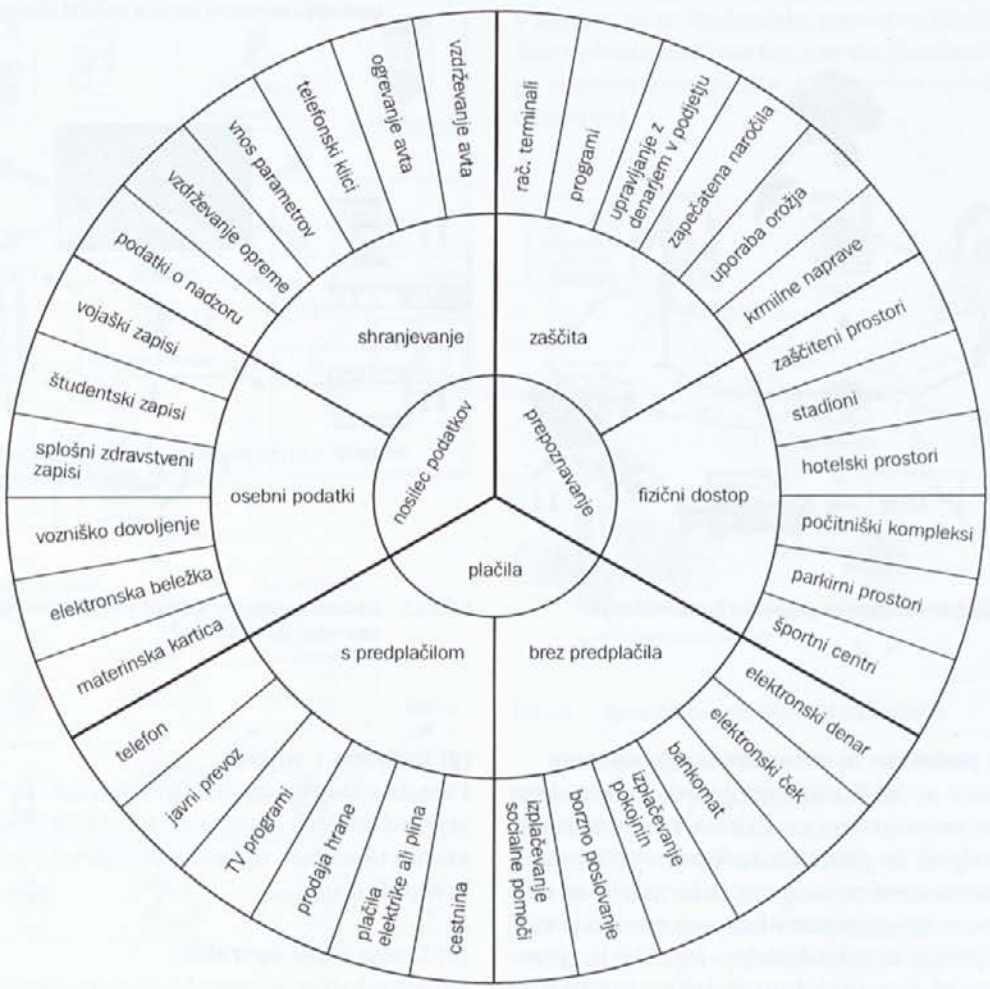
8. Zaključek

Danes si ne moremo predstavljati osebnega in poslovnega življenja brez kartic. Papirnato kartico, s katero smo se nekoč predstavljali, je z razvojem novih materialov zamenjala plastična kartica s funkcijo kreditne kartice. Bančna industrija je zaradi potrebe po avtomatizaciji dodala plastični kartici magnetni trak. Premajhen pomnilnik in nezadostna varnost sta glavni pomanjkljivosti magnetne kartice. Precej večjo pomnilno zmogljivost ima optična kartica, največjo zaščito pa nam nudi pametna kartica. Pametna kartica nam omogoča predplačila, brezgotovinsko poslovanje, dostop do objektov, bazo osebnih in drugih podatkov ter zaščito le-teh, predvsem pa onemogoča zlorabo in kriminal ter poenostavlja administracijo.

Nadomestila bo kovance, bančne izpiske, čeke, identifikacijske dokumente, transportne karte, zdravstvene recepte, kreditne kartice, ključe itd, glej sliko 12.

Pametna kartica je računalnik v žepu, njen razvoj in možnosti pa še zdaleč niso zaključene. Na Japonskem in v ZDA so izoblikovali pametno kartico s tipkovnico in majhnim zaslonom (super pametna kartica - *Super Smart Card*), razvita pa je bila tudi že tako imenovana kombinirana kartica (*Combi Card ali Hybrid Card*), ki ima lastnosti kontaktne in brezkontaktne kartice.

Pred kratkim so se Europay, Mastercard in Visa



Slika 12: **Področja uporabe pametnih kartic**

(EMV) dogovorili za skupno specifikacijo pametne kartice, ki določa osnovne protokole za komunikacijo med kartico in čitalnikom. Ta se ravna po standardu RS-232 za komunikacijo med osebnim računalnikom in modemom.

Specifikacija je dovolj splošna, da lahko izmenjamo katero koli informacijo med računalnikom in programom. To pa je osnova za večnamensko pametno kartico (*Multipurpose Smart Card*). Glavni prozvajalci pametne kartice (Gemplus,Thompson - Francija, Philips - Nizozemska, Motorola - ZDA, Mondex - Anglija, Siemens - Nemčija) so dosegli prvo stopnjo njene tehnične zrelosti. Pomnilna zmogljivost ni več zavirajoč dejavnik, pojavljajo pa se nove dileme, kot so izbira med nivojem zaščite ter ceno kartice, katere informacije zaščititi in komu omogočiti dostop do njih. Prihodnost pametne kartice je odvisna tudi od potreb po zasebnosti, od gospodarskih in političnih razmer, od programskih možnosti in od drugih vplivov. Skratka, pametna kartica je tu in njene možnosti je treba izrabiti

Literatura:

[1] *S. Bassein, A Sampler of Randomneš, Scientific American, American Math. Monthly, June-July (1996), pp. 483-490.*

[2] *T. Beth, Confidental Communication on the Internet, Scientific American, December 1995, pp. 87-91.*

[3] *G. J. Chaitin, Randomness in Arithmetic, Scientific American, July 1988, pp. 52-57.*

[4] *D. Chaum, Achieving Electronic Privacy, Scientific American, August 1992, pp. 96-101.*

[5] *A. K. Dewdney, On making and breaking codes, Part I,II (in Computer Recreations) Scientific American, October, November 1988, pp. 120-123, 104-107.*

[6] *Finance and Economics: Going for Olympic gold cards Economist, March (1996), 67-68.*

[7] *C. H. Fancher, Smart Cards, Scientific American, August 1996, pp. 40-45.*

[8] *M. Gardner, A new kind of cipher that would take millions of years to break, (in Mathematical games),Scientific American, August 1977, pp. 120-124.*

[9] *M. Gardner, Penrose tiles to trapdoor Ciphers. W.H. Freeman and Company 1989.*

[10] *M.E. Haykin and R.B.J. Warnar, Smart Card Technology: New Methods for Computer Ačeš Control, NIST, Special Publication 500-157, 1988.*

[11] *P.L. Hawkes, D.W. Davies and W.L. Price (eds.), Integrated Circuit Cards Tags and Tokens, BSP Professional Books,1990.*

[12] *M. E. Hellman The Mathematics of Public-Key Cryptography, Scientific American, August 1979, pp. 146-158.*

[13] *Jean-Jacques, Myriam, Maurier and Michael Quisquater, Louis, Marie-Annick, Gaid, Anna, Gwenole, and Soazig Guillou (in collaboration with T. Berson, for the English version), How to Explain Zero-Knowledge Protocols to Your Children, Advances in Cryptology - Crypto' 89, Lecture Notes in Computer Science 435, Springer-Verlag Berlin, New York (1990), pp. 628-631.*

[14] *D. Kahn, Modern Cryptology, Scientific American, July 1966, pp. 38-46.*

[15] *B. Magajna, O tajnopisih, Obzornik mat. fiz., 38 (1991), 9-18.*

[16] *J. McCrindle, Smart Cards. IFS Publications/Springer-Verlag, 1990.*

[17] *C.C. McGeoch, Zero-knowledge proofs, American Math. Monthly, Aug.-Sep. (1993), pp. 682-685.*

[18] *R. McIvor, Smart Cards, Scientific American, November 1985, pp. 152-159.*

[19] *D. Naccache, D. M'Raihi, Gemplus, Cryptographic Smart Cards, IEEE Micro, Vol. 16, No. 3, June 1996, pp. 14-24.*

[20] *I. Steward, Proof of Purchase on the Internet (in Mathematical Recreations), Scientific American, October? 1995, two pages.*

[21] *G. Stix, Dr. Big Brother (in Science and Business), Scientific American, February 1994, pp. 108-110.*

[22] *J. Svigals, Smart Cards, The Ultimate Personal Computer. Macmillan Publishing Company, 1985.*

[23] *P. Wallich, Wire Pirates (in Trends in Communication) Scientific American, March 1994, pp. 90-101.*

[24] *J.L. Zoreda and J.M. Oton, Smart Cards. Artech house, 1994.*

[25] *J. Zupan, Nekaj o kriptografskih metodah, Obzornik mat. fiz., 25*

◆

Aleksandar Jurišić je diplomiral leta 1987 pri prof. Vrabcu (Uporaba topologije v kombinatoriki) na Fakulteti za matematiko, teoretična smer. Po letu dni magistrskega študija (mentor prof. Pisanski, teorija grafov) na domači univerzi je leta 1988 odšel nadaljevat študij na Department of Combinatorics and Optimization, University of Waterloo, Kanada, kjer je pod mentorstvom prof. Godsila (algebraična kombinatorika) 1990. leta magistriral, 1995. pa doktoriral (Antipodal covers). Trenutno opravlja postdoktorski študij iz kriptografije na Department of Combinatorics and Optimization, University of Waterloo in Certicom Corp., Mississauga.

Alenka Trojar je diplomirala leta 1988 na Ekonomski Fakulteti na plansko-analitski smeri in se zaposlila v Intertradu. Leta 1993 je odšla v Kanado, kjer je 1995. končala program Diploma in Accounting na School of Business and Economics, Wilfrid Laurier University. Sedaj vodi zastopniško podjetje Amoebius.

◆