STANJE I PERSPEKTIVE TEHNOLOGIJE PAMETNIH KARTICA

STATUS AND PERSPECTIVE OF THE SMART CARD TECHNOLOGY

Miodrag Peranović, dipl. oec., asistent
Ekonomski fakultet u Brčkom

Anstrakt. U članku se opisuje trenutno stanje i perspektive korišćenja pametnih kartica u bankarstvu, trgovini i drugim područjima. Poseban akcenat stavljen je na bezbjednost podataka. Pored toga u radu su predstavljeni finansijski pokazatelji na tržištu pametnih kartica kao i predviđanje prihoda u narednom vremenskom periodu.

Ključne riječi: pametna kartica, elektronski novac, sigurnosni protokol

Abstract. The article describes the current state and prospects of smart cards usage in banking, trade and other areas. Special emphasis is placed on the security of data. The paper also presents the financial parameters of the smart card market and revenue forecasting in the next period.

Key words: smart card, electronic funds, security protocol

UVOD

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja u kojem je osnovni cilj da se, bez obzira na prostornu distancu, brže i efikasnije povežu poslovni partneri i tokovi informacija. Model globalne organizacije zahtijeva novu koncepciju pristupa poslovanju banaka, o čemu svjedoče sve veća ulaganja u specijalizovanu, prema klijentu orijentisanu tehnologiju. Komunikacija postaje masovna, brza i jeftina, a mnogobrojni servisi na Internetu omogućavaju da poruke veoma brzo stignu u bilo koji dio svijeta.

Primjena informacione tehnologije omogućila je uvođenje sistema elektronskih plaćanja, čime je riješen problem sistema plaćanja papirnim dokumentima. Pokazalo se da uvođenje sistema elektronskih plaćanja znači mnogo više od zamjene papirnih dokumenata i njihovog fizičkog prenosa elektronskim putem, odnosno da efikasno i ekonomično korišćenje ove tehnologije zahtijeva reinženjering poslovnih procesa i međusobnih odnosa učesnika. Najveće tehnološko dostignuće u razvoju bankarstva je pojava elektronskog novca, a samim tim i elektronskog bankarstva.[1] Elektronski novac je u savremenoj interpretaciji informacija. Pojava elektronskog novca zasniva se na elektronskoj razmjeni podataka i sredstava (*EFT – Electronic Funds Transfer*) što je pojmovno određeno kao elektronsko bankarstvo. Novi platni sistem, zasnovan na digitalnom novcu, bio bi uspješniji ako bi ga prihvatio veliki broj korisnika. Prihvatanje zavisi od odnosa troškova i koristi strana koje učestvuju u novom platnom sistemu.

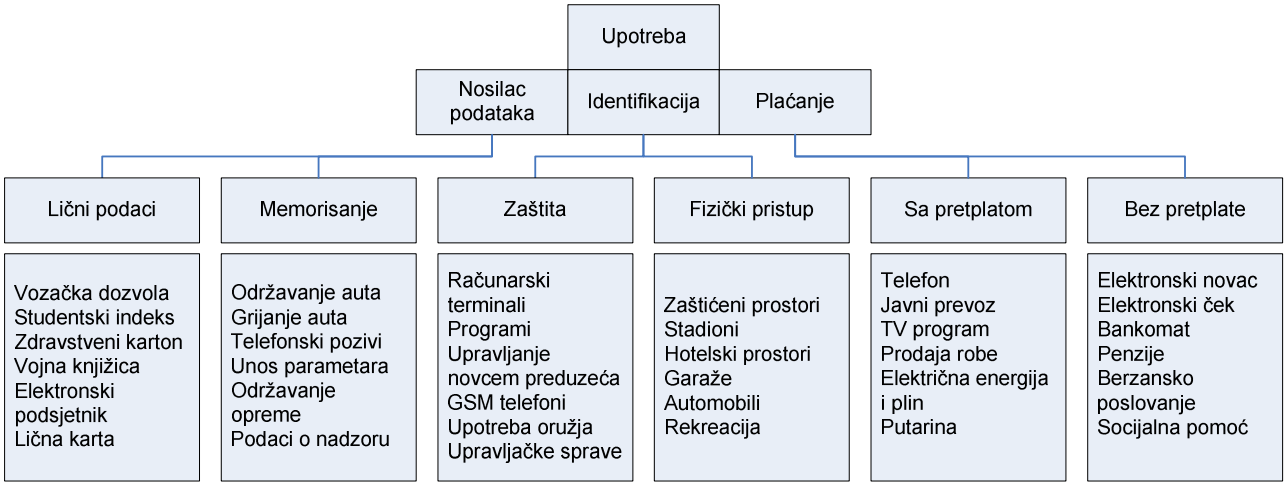
POJAM, RAZVOJ I PODRUČJA UPOTREBE PAMENTIH KARTICA

Pametna kartica je pravi računar, naravno bez monitora i tastature, iako postoje neke kartice sa malim ekranom od tekućeg kristala, pa čak i tastaturom za unos šifre pametne kartice. Prvi prijedlozi za upotrebu pametnih kartica su sigurnost sačuvanih informacija na kartici i zaštita podataka drugih računarskih sistema. Zato je oprema na pametnoj kartici pripremljena i optimizovana upravo za te podatke. Naravno, to ne ide bez upotrebe odgovarajućih kriptosistema za zaštitu podataka. Sigurnost ne zavisi od pojedinog mikroprocesora i algoritma koje izvodi operativni sistem. Treba omogućiti sigurnu upotrebu pametne kartice, te dobro poznavati principe planiranja koje upotrebljavaju proizvođači pametnih kartica. Pametne kartice su rezultat paralelnog razvoja mikroprocesora i magnetne kartice. Pametna kartica je plastična kartica koja izgledom podsjeća na običnu kreditnu ili debitnu karticu s tim da posjeduje jedan detalj koji je odvaja od njih, a to je integrisano kolo ili čip, na kome se nalaze procesor i memorija. Na čipu se na siguran način mogu čuvati određeni podaci.

[1] *Stankić, R., Krsmanović, B., Elektronsko poslovanje, Fakultet spoljne trgovina, Bijeljina, 2007., str. 93.*

Najveća snaga *Smart Card* tehnologije jeste u raznovrsnosti mogućih primjena. Zahvaljujući inteligenciji kartice, moguće je razviti raznovrsne sigurnosne aplikacije u oblastima kao što su: zaštita pristupa računaru ili mreži, identifikacija, mobilna telefonija, elekronski novac, vozačka dozvola, zdravstveni karton, zaštita podataka, digitalni potpis, zaštita autorskih prava, elektronska trgovina itd.

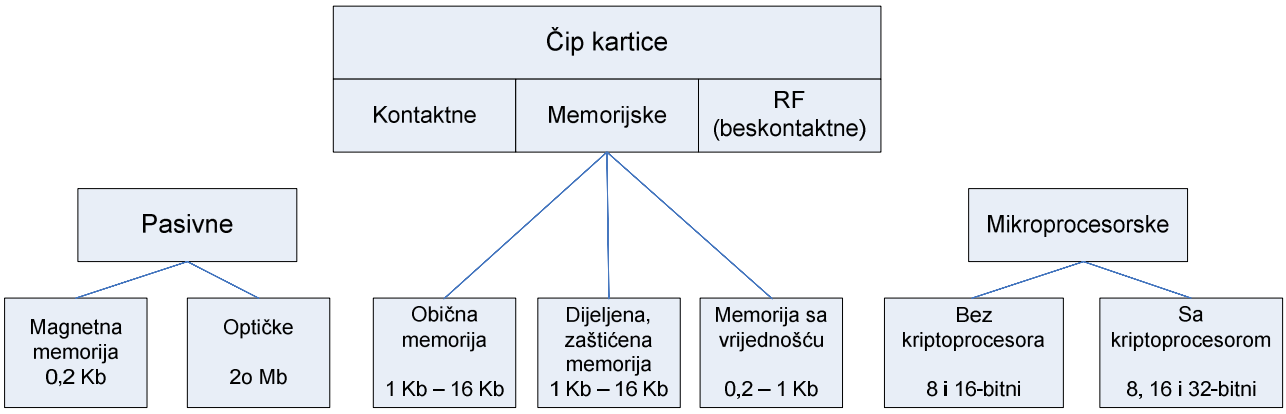
Slika 1: Područja upotrebe pametnih kartica



Izvor: http://www.smartcardstrends.com

U toku razvoja došlo je do stvaranja različitih vrsta pametnih kartica, na osnovu veličine memorije, količini podataka, stepenu sigurnosti i sl. Osnovna podjela je na tri vrste i to: pasivne, memorijske i mikroprocesorske kartice.

Slika 2: Podjela kartica sa čipom



Izvor: http://www.smartcardbasics.com

Kartice sa čipom mogu se podijeliti u tri grupe, i to: kontaktne, beskontaktne i kombinovane. Svaku od ovih grupa možemo dalje razdijeliti s obzirom na veličinu i tip memorije te prisutnost procesora. Procesor daje kartici pravu «pamet». Memorijske kartice, strogo gledano, nisu pametne kartice, a ime pametna kartica se često koristi za sve kartice sa čipom.

Pasivne kartice ne sadrže čip; one su preteča savremenih pametnih kartica. Trenutno su najraširenije kartice sa magnetnom trakom na zadnjoj strani. Koriste se u bankarstvu za ograničavanje pristupa. Magnetna traka na zadnjoj strani može sačuvati samo oko 200 bajta podataka.

Memorijske kartice nemaju vlastiti procesor i zato ne mogu dinamički obrađivati podatke. S obzirom na vrstu memorije razlikuju se tri tipa memorijskih pametnih kartica: kartice sa običnom memorijom, sa zaštićenom ili dijeljenom memorijom i sa memorisanom vrijednošću.

Kartice sa običnom memorijom su namijenjene uglavnom memorisanju podataka. Imaju najnižu cijenu po bitu memorisane informacije. Pojavljuju se kao kartice sa čipom i memorijom *EEPROM* ili kao kartice sa memorijom *flash*.

Kartice sa zaštićenom ili dijeljenom memorijom imaju ugrađene jednostavne logične veze kojima nadgledaju pristup podacima. Moguće je određene dijelove memorije zaštititi od pisanja i brisanja, što se obično postiže šiframa ili sistematskim ključevima. Upotrebljive su, prije svega, tamo gdje nije potrebna visoka sigurnost podataka, npr. za kontrolu pristupa sa *PIN*-om ili kao kartice za razne pogodnosti.

Kartice sa memorisanom vrijednošću su namijenjene memorisanju vrijednosti ili žetona za jednokratnu ili višekratnu upotrebu. Tipičan primjer takvih kartica su telefonske kartice.

Mikroprocesorske kartice: Za ove kartice može se reći su pametne. Obično sadrže procesor, ulazno-izlaznu jedinicu, te više vrsta memorija. Trenutno se upotrebljavaju 8, 16, 32-bitni procesori, u prosjeku imaju 64 kB *ROM*-a, 16 do 32kB *EEPROM*-a, te 3kB *RAM*-a, a ulazno-izlazna jedinica dostiže prenose 9,6-115 *kbita* u sekundi (pri čemu je moguć samo polovičan dupleksni način). Po računarskoj moći su uporedive sa prvim računarom *IBM-XT*, kartice sa kriptokoprocesorom u nekim operacijama premašuju za 50 *MHz* računar 486. To danas, inače, nije puno, ali moramo znati da je veličina čipa na kartici ograničena na 25mm² (inače bi se mogao čip zbog savijanja kartice oštetiti). Pri tome procesor mora dijeliti prostor još sa memorijom, vodilicom, ulazno-izlaznom jedinicom, te najčešće još i sa generatorom slučajnih brojeva. Ćelije *ROM*-a mogu se samo čitati. Većina proizvođača garantuje pohranjivanje podataka u *EEPROM*-u do 10 godina. Nakon navedenog vremenskog perioda, zbog konstrukcije *EEPROM* ćelije, može se desiti da memorija ne čuva vrijednosti koje su bile u nju upisane. Na osnovu navedenog neophodno je podatke obnavljati ako ih je potrebno čuvati više od 10 godina.[2]

PAMETNE KARTICE U ELEKTRONSKOM POSLOVANJU

Razvoj tehnologija sistema elektronskog plaćanja je najdinamičniji između organizacija (Business to Business - *B2B* poslovanje). Transakcije u *B2B* poslovanju su složenije od transakcija u trgovini sa krajnjim kupcima (*Business to Business - B2C* trgovina) i zahtijevaju opširnije računovodstvene i finansijske evidencije. U *B2B* poslovanju mnoge operacije su komplikovanije, podložne pregovaranju, kompromisima, koji su ponekad u suprotnosti sa ekonomskim zakonima i logikom. Zato ne postoji jedinstven i opšteprihvaćen sistem elektronskog plaćanja u *B2B* poslovanju. Umjesto toga upotrebljava se mnoštvo drugih metoda. Tako, na primjer, usluge elektronskog plaćanja u *B2B* poslovanju nudi veći broj asocijacija kao svoja izvorna, autorska rješenja od kojih su neke: *Paymentech, TradeCard, Clareon, eCredit, eTime, Capital, SubmitOrder.com, ViaPay*. Na cjelokupnom tržištu, tržište pametnih kartica zauzima izuzetno visok značaj prema iznosu prometovanih sredstava. Najbolji primjer jeste tržiše Hong Kong-a. Prema istraživanju VDC marketinške kuće, prihod po osnovu pametnih kartica u Hong Kongu za 2008., 2009. godinu kao i predviđanja za 2010. godinu prikazani su na slici 3, dok se do kraja 2013. godine predviđa porast od preko 26% u odnosu na 2010. godinu.[3]

Da bi neki sistem elektronskog plaćanja odgovarao poslovanju organizacije, potrebno je da zadovoljava određene uslove:

1. da prodavcu omogući pouzdano utvrđivanje finansijske sposobnosti i kredibiliteta kupca;
2. poslovanje sa nepoznatim klijentima, bez straha od prevare;
3. čvrste garancije kupcu u pogledu kvaliteta ponuđene robe i njene isporuke;
4. da pogoduje bržem obavljanju finansijskih transakcija i protoka novca;
5. da minimizira rizike od nepotrebnih troškova i problema, naročito vezanih za sigurnost podataka i transakcija i
6. da pravovremeno izvještava o isporukama robe, obavlja potvrdu izvršenih aktivnosti, te fakturisanje i plaćanje u najkraćem roku.[4]

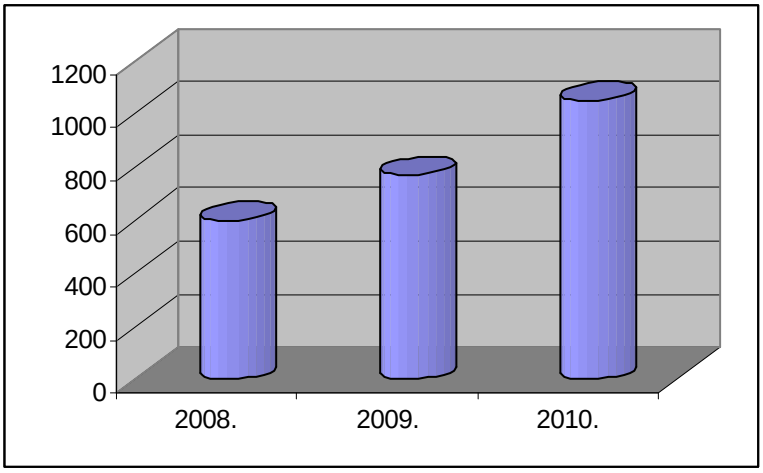
---

[2] *Wolfgang, R., Wolfgang, E., "Smart card handbook", Third Edition, Whiley, 2004., str. 18.*

[3] *http://www.*readwriteweb*.com*

[4] *Marić, A., V., Elektronsko poslovanje, Ekonomski fakultet, Banja Luka, 2008, str. 148.*

Slika 3: Prihodi (u milionima dolara) po osnovu pametnih kartica u Hong Kongu



Izvor: http://www.readwriteweb.com

BEZBJEDNOST PAMETNIH KARTICA

Naglo širenje Interneta i njegovo sve veće korišćenje u poslovne svrhe nametnuli su potrebu za promjenama u funkcionisanju svjetske mreže. Sve veći broj povjerljivih podataka koji se prenose mrežom, kao i porast trgovine preko Interneta, stavili su u prvi plan problem sigurnosti komunikacije. Naročito je aktuelan problem sigurnosti u komunikaciji *web* servera i klijenta.

Standardni protokoli za komunikaciju među računarima ne nude rješenje za ove probleme ni *TCP/IP* ni protokoli višeg nivoa *http, smtp, pop3, imap*, i sl. Zato je razvijeno više protokola koji obezbjeđuju pouzdanu komunikaciju na Internetu. Neki od njih su na aplikativnom nivou poput *Secure HTTP-a (HTTPS*-a), ili *Secure Socket Layer (SSL*) protokol koji je *de facto* standard za sigurnu komunikaciju na Internetu, radi na transportnom sloju neposredno iznad *TCP*. To znači da ga mogu koristiti svi protokoli aplikativnog nivoa koji za transport imaju *TCP*, a to su na primjer *http, smtp, pop3, imap*.

Problem tajnosti u računarskim komunikacijama rješava se kriptovanjem podataka na izvoru i dekriptovanjem na odredištu. Savremene metode kriptovanja zasnivaju se na javno dostupnim algoritmima, a tajnost podataka garantovana je tajnošću ključa. Za kriptovanje se mogu koristiti različiti algoritmi koji se dijele na dvije velike grupe: algoritme sa simetričnim ključem i algoritme sa javnim ključem (odnosno asimetričnim ključevima, od kojih je jedan javni, a drugi tajni).

Secure Socket Layer (SSL) protokol 2.0 i 3.0. kao i na njemu zasnovan *TLS (Transport Layer Security)* koristi prednosti i simetričnog i asimetričnog šifrovanja. Najvažnije mjesto svake strukture sa javnim ključem je lokacija na kojoj se čuvaju privatni ključevi. Bezbjednost čitavog sistema ugrožena je činjenicom da su najosjetljiviji podaci sačuvani na hard diskovima radnih stanica i servera gdje su izloženi mogućim zloupotrebama. Druga velika slabost je što proces kriptovanja i dekriptovanja obavlja operativni sistem ili aplikativni softver koji je podložan i neotporan na snažnije napade.

Rješenje ovih ključnih problema pronađeno je u upotrebi specijalizovanih hardverskih komponenti koje na sebi imaju dovoljno memorije za čuvanje svih kriptografski bitnih informacija i dovoljno procesorske snage da obavljaju osnovne kriptografske operacije nezavisno od operativnog sistema i aplikacija. Takvo rješenje je *Smart* kartica.

ZAKLJUČAK

Očekuje se brz razvoj upotrebe pametnih kartica. Da bi se to dogodilo, mora se riješiti problem identifikacije, naći način kako digitalno sačuvati vrijednost i pri tom obezbijediti anonimnost korisnika. Danas, to može obezbijediti računar sa kriptosistemima sa javnim ključevima i pametnim karticama. Zbog potreba

memorisanja brojnih šifri, ključeva za prepoznavanje, ključeva za sprečavanje tajnosti, upravo pametne kartice čuvaju ih na jednom mjestu i paze da nikada ne napuste zaštićeno mjesto, a istovremeno, spriječeno je korišćenje falsifikata.

Za kriptosistem sa javnim ključevima preporučene su dužine ključeva do 2000 bita. Dodavanje komponenti utiče na poskupljenje kartice, a istovremeno se može smanjiti njihova pouzdanost, a time i sigurnost. Ipak se kod nedostatka memorije i procesorske moći može pomoći ovim tehnologijama, koje omogućavaju kraće ključeve i brže računanje i pri tom čuvaju jednak stepen sigurnosti.

LITERATURA:

1. Grimaud, G., Standaert, FX., "*Smart Card Research and Advanced Applications*", 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008, Springer science+business media, 2008.
2. Keith, E., M., *Smart Cards, Tokens, Security and Applications* (Hardcover), Springer science+business media, 2008.
3. Marić, A. V., *Elektronsko poslovanje*, Ekonomski fakultet, Banja Luka, 2008.
4. Stankić, R., Krsmanović, B., *Elektronsko poslovanje*, Fakultet spoljne trgovine, Bijeljina, 2007.
5. Wolfgang, R., Wolfgang, E., *Smart card handbook*, Third Edition, Whiley, 2004.

WEB Izvori:

http://www.smartcardbasics.com
http://www.smartcardstrends.com
http://www.readwriteweb.com
http://www.smartcardalliance.org
http://www.icongrouponline.com