UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

RAZVOJ BANČNIH STORITEV Z UPORABO TEHNOLOGIJ ELEKTRONSKEGA POSLOVANJA

Ljubljana, februar 2005 **DAVOR PAVLIĆ**

IZJAVA

Študent Davor Pavlić izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Borke Jerman Blažič in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 03. 02. 2005 Podpis: _____

KAZALO

1. UVOD

Korenine elektronskega poslovanja segajo v drugo polovico prejšnjega stoletja. S svojim revolucionarnim načinom je, v štirih desetletjih, zajelo praktično vsa področja našega življenja in dela. V devetdesetih letih prejšnjega stoletja je prišlo do razmaha elektronskega poslovanja na različnih področjih, med drugim je z velikimi koraki vstopilo tudi v sfero bančnega poslovanja. Dandanes si, kot bančni komitenti, ne znamo več predstavljati bančnega poslovanja brez, npr. bančnih avtomatov ali uporabe plačilnih kartic.

Toda s hitro razvijajočo se moderno tehnologijo elektronsko poslovanje dobiva nove razsežnosti in išče nove medije. Internet je postal najbolj razširjeno svetovno omrežje, ki je dostopno vsakomur preko računalnika in modema. Zaradi te prednosti se je elektronsko bančništvo preselilo tudi na internet. Poslovanje na internetu pa prinaša tudi tveganja, kajti nekdo lahko informacije in njihov pretok prestreže ter spremeni v svojo korist. Možnost zlorab je na internetu velika, zato je potrebno ustvarjati nove in posodobiti že obstoječe varnostne ventile in sita, ki lahko omogočajo varno poslovanje, kljub prežečim nevarnostim.

Pozitivni učinki elektronskega bančništva so številni. Bankam je uspelo zmanjšati stroške poslovanja in obenem pospešiti kroženje denarja, odpirajo se novi trgi ter omogoča bolj redno plačevanje obveznosti. Prav tako so zadovoljne stranke, ker jim poslovanje z banko vzame manj časa in jim postaja bolj udobno.

V svoji diplomski nalogi bom najprej predstavil, kaj sploh elektronsko poslovanje je in kako se je in se še vedno razvija. Ustavil se bom tudi pri spremembah, ki jih prinaša v primerjavi s tradicionalnim poslovanjem. V nalogi se bom predvsem osredotočil na elektronsko bančništvo in njegove segmente. Najprej bom predstavil delovanje, prednosti in slabosti ter razširjenost samopostrežnega bančništva ter nato hitro napredujočo novost, kot sta elektronski denar in elektronska denarnica. Predstavil bom telefonsko bančništvo s pomočjo avtomatskega odzivnika in z bančnim operaterjem. V nadaljevanju bom več prostora namenil internetnemu bančništvu, kjer bom razmišljal o nastanku, razvoju ter hitremu razmahu interneta. Primerjal bom uporabo interneta v Sloveniji in Evropi ter njegovo pogostnost uporabe. Razčlenil bom in vsebinsko opredelil temeljne funkcije internetnega bančništva ter nato predstavil tveganja pri tovrstnem poslovanju. Posebno pozornost bom namenil varnosti. Predstavil bom varnostne protokole, požarni zid, simetrično in asimetrično šifriranje, digitalni podpis in digitalni certifikat ter infrastrukturo javnih ključev. Zadnji del naloge bom namenil področju elektronskega bančništva, ki ima trenutno daleč največ možnosti potencialnega razvoja - mobilno bančništvo.

2. ELEKTRONSKO POSLOVANJE

2.1. Definicija elektronskega poslovanja

Elektronsko poslovanje je pojem, ki je razmeroma nov, zato obstaja zanj kar nekaj definicij. Najširše se elektronsko poslovanje lahko opredeli kot poslovanje, ki uporablja elektronske medije in za to potrebno tehnologijo, s pomočjo katere lahko uporabniki elektronsko poslujejo. Takšno poslovanje temelji na elektronskem procesiranju in prenosu podatkov med računalniki. Pomembna značilnost elektronskega poslovanja je, da med strankami ne pride do fizičnega stika, temveč se posluje s pomočjo elektronske tehnologije.

Sam pojem »elektronsko poslovanje« prihaja iz angleškega izraza »electronic commerce«, ki je nastal v trgovini in industriji. Na začetku se je nanašal na vsa gospodarska in poslovna področja. Obsega pa naslednje sestavine (Toplišek, 1998, str. 4):

- Način dela: elektronsko izmenjevanje podatkov (deloma tudi samodejne transakcije, informacijski tokovi…)
- Vsebine poslovanja so skoraj neomejene: blago, storitve, plačevanje, pred- in poprodajne aktivnosti, delovanje državnih organov in javnih služb…
- Glavne tri skupine udeležencev so: podjetja/podjetniki, državne/javne službe in posamezniki (potrošniki, uporabniki). Poslovanje poteka znotraj teh skupin in med njimi.

V javnosti se pojem elektronsko poslovanje vse preveč uporablja le za nakupovanje prek interneta, vendar pa ima precej širši pomen, saj vključuje tudi elektronsko bančništvo, plačilni promet na daljavo, elektronsko plačevanje, elektronsko borzništvo, storitve na zahtevo (ang. on-demand), elektronsko založništvo, elektronsko zavarovalništvo, komunikacijsko-informacijske storitve, delo na daljavo, distribucija v digitalni obliki…(Toplišek, 1998, str.17)

Med drugimi je tudi Evropska komisija poskušala opredeliti pojem »elektronsko poslovanje«. Zapisali so, da je elektronsko poslovanje: »katera koli oblika poslovne transakcije, v kateri stranke delujejo elektronsko, namesto da bi si pošiljale »telesna« sporočila (ang. physical exchanges) ali da bi bile v neposrednem stiku«. Hkrati pravijo, da je težko zajeti v definicijo dogajanje, ki je v tako kratkem času povzročilo toliko sprememb v načinu poslovanja (Toplišek, 1998, str. 4).

Dandanes je elektronsko poslovanje zajelo vse segmente modernega poslovanja in se širi z veliko hitrostjo. Elektronsko poslovanje tako poteka z državnimi ustanovami, med podjetji ali med podjetji in fizičnimi osebami. Za vse te subjekte pa sta ključnega pomena varnost poslovanja in zaupnost podatkov, o katerih bom spregovoril v tretjem poglavju.

2.2. Razvoj elektronskega poslovanja

Razvoj elektronskega poslovanja se je začel z razvojem računalniških omrežij in interneta, združevanjem informacijske in telekomunikacijske tehnologije ter standardom za računalniško izmenjavo podatkov, katerega začetki segajo v leto 1968. Računalniško izmenjevanje podatkov – RIP je tehnologija, ki omogoča organizaciji, da preko računalnika komunicira, to pomeni sprejema in pošilja poslovna sporočila računalnikom v drugi organizaciji, z uporabo vnaprej opredeljenih oblik sporočila. Na ta način prejemniku ni več potrebno ponovno vnašati podatkov v njegov informacijski sistem, ampak je sporočilo avtomatično sprejeto in prevedeno v obliko, ki je primerna za obdelavo v računalniškem sistemu prejemnika RIP sporočila.

Uvedba RIP-a je bila na začetku počasna zaradi visokih stroškov povezovanja preko omrežij z dodano vrednostjo. Ta tehnologija je bila v preteklosti vodilna oblika elektronskega poslovanja med organizacijami, vendar so manjše organizacije v pretežni meri izpadle iz tega načina povezovanja zaradi visokih stroškov. Takrat še ni bilo slutiti, kakšna bo hitrost in razvoj informacijske tehnologije in telekomunikacij, ki bo spremenila načina življenja in poslovanja. Zamenjava prenosnega medija RIP-a z omrežij z dodano vrednostjo v okolje interneta je bistveno znižala komunikacijske stroške. Hitra rast in sprejemljivost internetnih tehnologij pa je začela ustvarjati nove možnosti za elektronsko povezovanje, dostopnost do podatkov in organizacijsko povezljivost tako med organizacijami kot tudi znotraj organizacije.

Z razvojem RIP-a se je pojavila potreba po standardizaciji te tehnologije. Sredi sedemdesetih let so se po svetu na raznih poslovnih področjih začeli pojavljati standardi za RIP, ki so postopoma prerasli v nacionalne standarde. Kmalu pa je postalo jasno, da je treba mednarodne standarde harmonizirati in vzpostaviti mednarodni standard za RIP, ki bi zadostil vsem zahtevam sodobnega globalnega poslovanja. Evropska komisija za bančne standarde, ki je bila ustanovljena leta 1993, je kot standard za elektronsko poslovanje izbrala standard UN/EDIFACT[1] in izdala svoje strateško priporočilo v katerem je poudarila, da se uporaba tega standarda naglo širi v vsem bančnem okolju (Slana, Strojan, 1999, str. 25-31).

Računalniška tehnologija, ki je bila v začetku namenjena le računalniškim strokovnjakom in znanstvenikom, je z leti postala veliko bolj uporabna in prijazna. Sčasoma je postala nepogrešljiva tudi za laike (Jerman Blažič Borka, 2001, str. 13). V 90-ih letih prejšnjega stoletja je večina elektronskega poslovanja prešla na internet.

[1] UN/EDIFACT – mednarodni standard za el. poslovanje.

2.3. Spremembe, ki jih prinaša elektronsko poslovanje

Elektronsko poslovanje je prineslo veliko sprememb v življenje posameznikov in družbe. Najbolj vidne so sledeče (Jerman Blažič Borka, 2001, str.18):

- **Dematerializacija poslovanja; vztrajna rast storitev.** Med storitvami, ki se izvajajo brez papirja in drugih otipljivih elementov, so pisarniško poslovanje, elektronsko bančništvo – pojav elektronskega denarja, digitalizacija slik (slike, ki jih posnamemo z digitalnim fotoaparatom in jih hranimo v računalniku) tako za lastne potrebe kot za potrebe diagnosticiranja in arhiviranja v medicini ali za potrebe trga (prodaja tehničnih, umetniških slik prek interneta), optimizacija transporta, video na zahtevo, elektronsko zavarovalništvo, elektronsko svetovanje ipd.

- **Vztrajna rast mobilnosti ljudi, storitev in izdelkov.** Najsodobnejša tehnologija interneta omogoča brezvrvični dostop do storitev interneta, ki omogoča mobilnost uporabnika, delo na daljavo, nakupovanje na daljavo, ki je zlasti spremenilo obseg trgovin in njihove lokacije, storitve zasebne telefonske centrale na daljavo (sistem Centrex), videokonference, ki so na primer spremenile potovalne navade managerjev, sisteme za računalniško podprto delo, ki so spremenili delo na skupnih projektih, klicne centre ipd.
- **Spremenjen način dela.** Elektronska pošta in računalniško podprto sodelovanje postajata že vsakdanjost in nepogrešljiv komunikacijski pripomoček. Olajšan je prenos znanja, ki ni shranjeno samo v dokumentih, temveč tudi v procesih in postopkih. Več poslovnih procesov v podjetjih je podprtih s tehnologijami interneta, več dela je mogoče opraviti kjerkoli po svetu posamezno ali v skupini, katere člani skupaj delajo in ustvarjajo.

3. ELEKTRONSKO BANČNIŠTVO

Nekateri si razlagajo pojem elektronsko bančništvo kot bančništvo preko interneta. Toda, to je samo en segment elektronskega bančništva, ki zajema opravljanje vseh bančnih poslov na elektronski način, od samopostrežnega bančništva pa vse do mobilnega bančništva. Zato v elektronsko bančništvo uvrščamo:

3.1. SAMOPOSTREŽNO BANČNIŠTVO

Pri samopostrežnem bančništvu je značilno to, da lahko opravljamo želeno storitev brez bančnega operaterja, le s pomočjo elektronskega avtomata.

3.1.1. Bančni avtomati

Samopostrežne avtomate so razvili v poznih 60-ih letih. Pojavili so se kot odgovor na družbene in ekonomske potrebe. Takrat sta se vlada in sindikati v Veliki Britaniji odločili zapreti banke ob sobotah. Ker je bila sobota nakupovalni dan, je bilo potrebno kljub temu zagotoviti dostop do gotovine. Problem so rešili s postavitvijo samopostrežnih bančnih avtomatov, ki so izdajali gotovino (Svigals, 1996, str. 67-68).

Pri uvajanju samopostrežnih avtomatov ni šlo brez težav. Prve izkušnje pri avtomatih za javni prevoz in bančnih avtomatih so pripeljale do pomembnih ugotovitev (Svigals, 1996, str. 68):

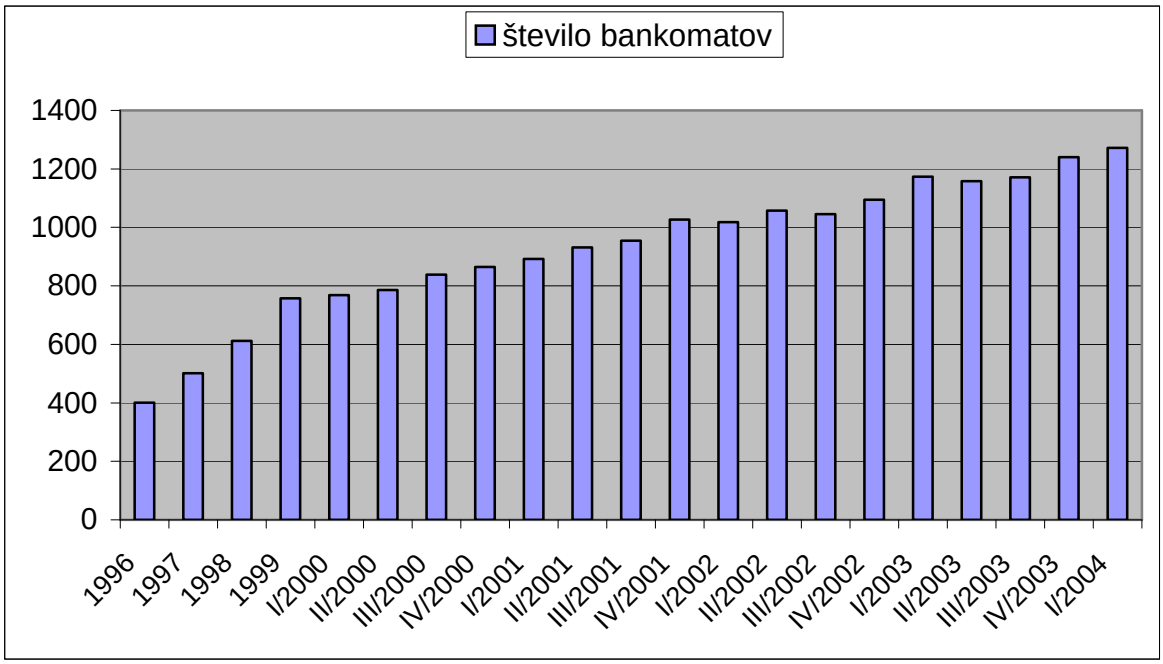
- Vsak samopostrežni avtomat mora biti oblikovan tako, da že po prvi demonstraciji uporabe aparata, lahko stranka samostojno in uspešno opravlja storitve na avtomatu.
- Navodila morajo biti natančna in jasna. Kot, na primer, pri zgodnjem uvajanju avtomatov za vozovnice, so bili avtomati na vhodu v železniško postajo, oblikovani tako, da so sprejemali kartice v vseh štirih možnih položajih. Menili so namreč, da bodo tako zasnovani avtomati omogočali hitrejši pretok potnikov in krajše vrste. Rezultat pa je bil, da so se uporabniki ustavljali in spraševali o pravilnem postopku, kar je povzročalo zastoje. Ugotovili so da uporabniki potrebujejo jasna navodila, razumljive znake in puščice za hitrejše opravljanje storitev.
- Terminologija mora biti splošno razumljiva brez računalniških izrazov. Izrazi, uporabljeni na prej omenjenih avtomatih, so bili računalniški in neprimerni za širšo množico uporabnikov. Zato so jih zamenjali z uporabnikom bolj prijaznimi in razumljivimi izrazi.

Pomembna prednost bankomatov je ta, da omogočajo bančnim komitentom opravljanje storitev 24 ur na dan. Bankomati so postavljeni na različnih lokacijah, ne samo ob bankah, temveč tudi pred trgovinami ali prodajnimi centri, železniškimi postajami, letališči itn. To je za stranke zelo priročno in udobno. Vse storitve lahko opravijo hitro in brezosebno, kar morajo storiti je le vstaviti kartico in vtipkati številko. Ponudba storitev na bankomatih se venomer veča, tako, da sedaj lahko na bančnem avtomatu plačujemo položnice, položimo denar ali napolnimo svoj račun na mobilnem telefonu. Sklepamo lahko, da bomo v bližnji prihodnosti lahko tudi opravljali druge storitve, npr. oddajali prošnje za posojila, naročali čeke in izdajali naloge za prenos sredstev na drug račun.

Na začetku je postavljanje bančnih aparatov potekalo počasi, toda povpraševanje je pospešilo postavljanje v devetdesetih letih prejšnjega stoletja.

Slika 1 kaže, kako je naraščalo število bančnih avtomatov v Sloveniji v obdobju od leta 1996 do prvega četrtletja leta 2004. Od leta 2000 naprej so podatki podani za vsako četrtletje.

Slika 1: Rast števila bankomatov v Sloveniji



Vir: Bilten Banke Slovenije, 2004.

3.1.2. Samopostrežni kioski

Samopostrežni kioski so avtomati, podobni bankomatom, le da ti omogočajo samo negotovinsko poslovanje. Stranke lahko na samopostrežnem kiosku dobijo različne informacije in opravljajo negotovinske storitve. Prednost takšnih kioskov je, da si stranke lahko informacije natisnejo. To pa za banko pomeni, da je večja verjetnost, da se bo komitent v banko vrnil po tehtnem premisleku doma, kot, če bi podatke le videl na zaslonu.

Druga funkcija samopostrežnih kioskov pa je konkretna storitev, za katero banka lahko zaračuna provizijo in pomeni na eni strani manjši strošek za opravljanje te storitve, po drugi strani pa je to prihodek iz poslovanja. Te storitve običajno obsegajo vloge za odprtje računa, prošnje za odobritev kredita (po neki raziskavi na Švedskem kar 90% komitentov za odobritev kredita raje uporablja »neosebni« kiosk kot »osebno« bančno okence), naročanje in tiskanje raznih dokumentov kot so čeki ali izpiski ter telefonsko, mobilno in internetno bančništvo, ki vključujejo plačevanje položnic in prenos sredstev med računi. Prav ti storitvi imata največji delež med bančnimi prihodki od provizij za opravljene storitve (Čanaki, 2001, str. 62).

Pri nas je Nova Ljubljanska banka kot prva slovenska banka, naredila drugi korak v samopostrežno bančništvo. V prenovljeni poslovalnici na Trgu republike v Ljubljani je temu namenjen velik prostor ob vhodu v poslovalnico. Na enem mestu so štirje bankomati in kar osem samopostrežnih kioskov Wincor Nixdorf. Vsi kioski so opremljeni z velikim zaslonom LCD, občutljivim na dotik, stereo zvočniki, alfa-numerično tipkovnico iz nerjavečega jekla

ter čitalnikom magnetnih in čipnih kartic. Šest kioskov ima dodan A4 termični tiskalnik za tiskanje bančnih izpiskov in videokonferenčni paket s telefonsko slušalko in videokamero za povezavo s klicnim centrom. Trije kioski omogočajo uporabo sede, kar je prikladno tudi za invalide in udobno za tiste, ki se bodo za kioskom zadržali dlje časa (Čanaki, 2001, str. 63).

3.2. PLAČILNE KARTICE IN POS TERMINALI

Že dlje časa so plačilne kartice eden od najbolj priljubljenih načinov plačevanja med fizičnimi osebami in podjetji. Takšno plačevanje nam omogoča, da s seboj ne nosimo večje količine gotovine, kljub temu pa lahko plačamo in kupimo blago, ki si ga želimo. Večje plačilne kartice sprejemajo že skoraj povsod, tako, da lahko z njimi rezerviramo letalsko vozovnico, počitniški paket ali nakupujemo preko svetovnega spleta.

Prva plačilna kartica je bila izdana v ZDA že leta 1950. To bila kartica Diners Club. Namenjena je bila ožjemu krogu ljudi in sprejemali so jo le v nekaterih restavracijah. Konec petdesetih let se je pojavila kartica American Express, čez nekaj let pa še kartici Visa in Mastercard (Klapš, 1995, str. 22).

Te prve kartice niso še omogočale elektronskega poslovanja, saj je poslovanje s karticami potekalo ročno. Elektronski zapis podatkov na kartici je bil omogočen šele, ko so uvedli kartice z magnetnim trakom, ob koncu šestdesetih let prejšnjega stoletja.

3.2.1. Vrste kartic

Plačilne kartice lahko delimo po več kriterijih. Glede na način poravnave plačil ločimo debetne kartice, kreditne kartice in kartice s predplačilom. Glede izdajatelja pa jih delimo na bančne in podjetniške kartice. S tehnološkega stališča jih delimo na kartice z magnetnim trakom, kartice z mikročipom in laserske kartice.

3.2.1.1. Debetne, kreditne in kartice s predplačilom

Debetne kartice so kartice, ki so vezane na določen bančni račun. Poleg tega, da so identifikacijski dokument za plačilo s čekom in da z njimi lahko dvigamo gotovino, imajo še plačilno funkcijo z debetnim (takojšnjim) načinom poravnave obveznosti. Pri plačilu se prenos sredstev s strankinega računa izvrši v roku od nekaj minut do nekaj dni, odvisno od zmogljivosti tehnologije plačilnega sistema. Ta kartica ni izdana za zagotavljanje potrošniškega kredita, ampak za opravljanje enostavnega brezgotovinskega plačila. S to kartico se lahko plačuje le na prodajnih mestih opremljenih s Point of Sale[2] (POS) terminali.

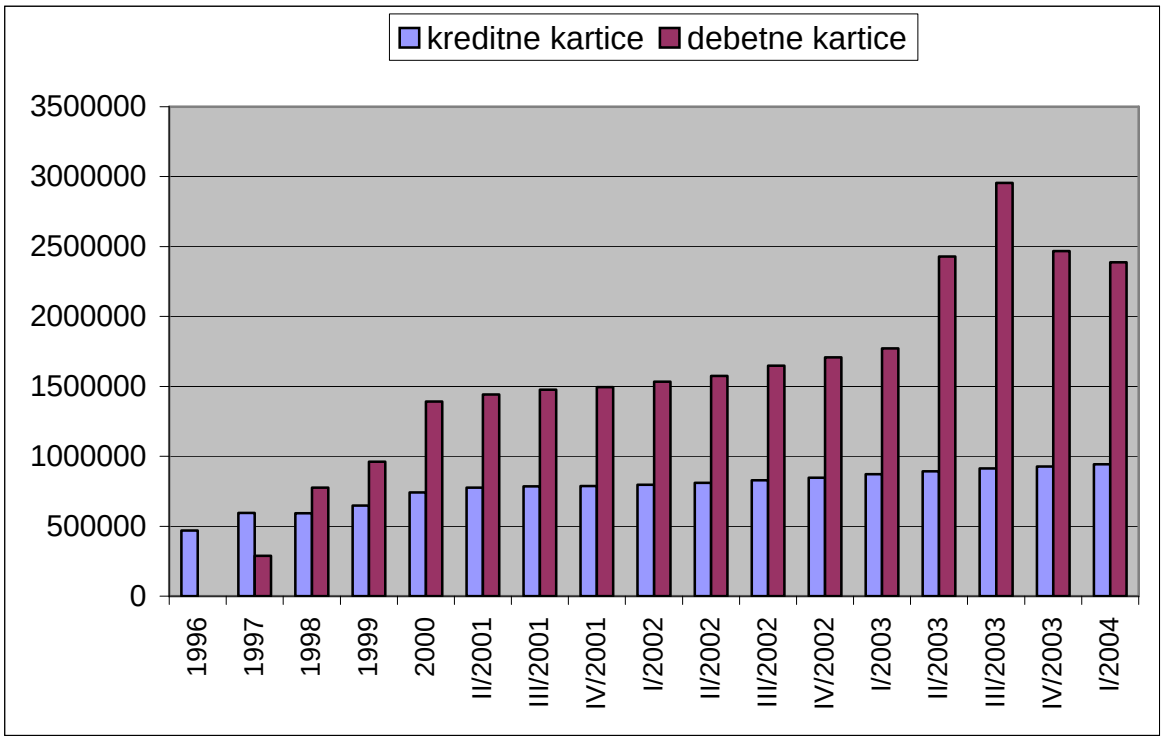
[2] Prodajno mesto.

Kreditne kartice omogočajo plačevanje raznovrstnih storitev in blaga pa tudi dvigovanje gotovine v bankah. V trenutku nakupa oziroma prevzema blaga do plačila dejansko še ne pride, kajti imetnik kreditne kartice s predložitvijo in s podpisom potrdi prevzem blaga, prodajalec pa mora račun izdati izdajatelju kreditne kartice. Ta plača račun prodajalcu in ga nato zaračuna imetniku kreditne kartice. Končno plača račun seveda imetnik kreditne kartice, to je kupec (Odar, 2000, str. 94).

Kreditne kartice delimo na kartice z odloženim plačilom in prave posojilne kartice. Pri prvih gre za zamik plačila, in sicer poravnava se opravi enkrat mesečno na določen dan. Pri pravih kreditnih karticah pa je imetniku za poravnavo odobreno posojilo. Vsak mesec plača le del obveznosti s pripadajočimi obrestmi.

Kartice s predplačilom so kartice, pri katerih je plačilo izvršeno še pred uporabo. Pri tej kartici ni potrebna identifikacija imetnika in ni nobenega tveganja glede plačila. Uporabljamo jih lahko dokler se vrednost na kartici ne porabi in jih nato zavržemo ali pa ponovno napolnimo. To je odvisno od tipa kartice. Uporablja se jih za plačevanje drobnih storitev na primer parkirnine, cestnine, avtobusnih vozovnic, najpogosteje pa za telefonske pogovore. Ena vrsta kartice s predplačilom je tudi tako imenovana elektronska denarnica, o kateri bom več napisal na koncu tega poglavja.

Slika 2: Rast števila kreditnih in debetnih kartic izdanih v Sloveniji



Vir: Bilten Banke Slovenije, 2004.

Slika 2 prikazuje rast števila kreditnih in debetnih kartic izdanih v Sloveniji od leta 1996 do 2004. Od leta 2001 naprej so podatki podani za vsako četrtletje posebej. Prve debetne kartice so bile izdane leta 1997 in so hitro presegle število kreditnih kartic.

3.2.1.2. Magnetne, pametne in laserske kartice

Magnetne kartice

Magnetna kartica je kartica, na kateri je postavljen magnetni trak in na katerega lahko shranimo nekaj številk in besed. Podatki shranjeni na kartici se ohranijo nekaj let. Tehnologija magnetnih kartic je res poceni, toda zaradi dejstva, da so podatki na njej slabo zaščiteni pred zlorabami, postaja počasi preteklost. Namreč, postalo je preveč enostavno prekopirati zapis z ene kartice na drugo.

To kartico so naredili že v poznih 60-ih letih, da bi zadovoljila več ciljev. Bančniki so iskali napravo, s katero bi omogočili strankam hitro in učinkovito opravljanje storitev na samopostrežnih bančnih avtomatih. Poleg tega naj bi s kartico lahko plačevali tudi preko POS terminalov (Svigals, 1996, str. 87).

Pametne kartice

Značilnost pametnih kartic je, da imajo vgrajen mikročip. O združitvi čipa z navadno plastično transakcijsko kartico so inovatorji sanjali že od prve pojave le-tega. Leta 1974 je Francoz Roland Moreno izumil pametno kartico in še istega leta tudi patentiral svoj izum. V svojem zgodnjem obdobju je bila uvedba pametnih kartic za banke še predraga. Šele v 90-ih letih je močno naraslo zanimanje za pametne kartice zaradi nižje cene kartic in naraščanja zlorab obstoječih kartic. V Franciji je Združenje francoskih bank zamenjalo magnetne s pametnimi karticami že leta 1993. Pri nas se banke šele sedaj odločajo za prehod na pametne kartice.

Že nekaj časa je s pomočjo mikroračunalniške tehnologije v integrirane sklope majhnih dimenzij mogoče shraniti veliko količino podatkov. Tehnologija pametnih kartic (ang. Smart Card) omogoča prenos in hranjenje informacij s pomočjo integriranega vezja, ki je vgrajen v kartico velikosti magnetne plačilne kartice. Na površini kartice se nahajajo kontakti, ki so namenjeni za pisanje oz. izmenjavo podatkov med kartico in čitalcem kartic. Pojem pametna kartica opisuje mikroračunalnik, ki je v ohišju kartice. Mikroračunalnik poskrbi, da se podatki z zunanjim svetom izmenjujejo na varen način. To pomeni, da so podatki zaščiteni pred nepooblaščenim dostopom (Mihelčič, 1999, str. 10).

Pametne kartice delimo na memorijske in procesorske kartice. Memorijske kartice vsebujejo samo čip s spominom. Uporabljajo pa se lahko kot nadomestilo za kovance za plačilo telefonskih pogovorov ter kot kartice s predplačilom za plačevanje cestnin, parkirnin in

podobnih storitev. Ker cena čipa ni posebej visoka, se kartica po izrabi mnogokrat odvrže. Procesorska kartica, pa vsebuje čip s spominom in mikroprocesor. Ta kartica ponuja tudi večjo količino pomnilnika za zelo veliko število pisanj, zaščiten prenos podatkov in dostop do pomnilnika, uporabnost za več aplikacij, itd. (Frelih, 2003).

Pametne kartice delimo tudi na kontaktne in brezkontaktne kartice. Zgoraj omenjene kartice so kontaktne kartice, katere imajo na površini kontakte za komunikacijo s čitalcem kartic. Brezkontaktne kartice imajo prav tako vgrajen čip, vendar razlika je v načinu prenosa podatkov s kartice na čitalec. Te kartice so sestavljene iz integriranega vezja in antene v obliki tuljave, oboje zalito v plastično ohišje. Za komunikacijo je dovolj, da kartico približamo čitalcu na določeno razdaljo (Frelih, 2003).

Pametne kartice imajo veliko prednosti pred magnetnimi karticami. Te prednosti so (Svigals, 1996, str.115-116):

- *Kapaciteta informacij*

Vsebina informacij je 20-200 krat večja kot pri obstoječi kartici z magnetnim trakom. To omogoča shranjevanje večje količine podatkov o stranki, seznam vseh transakcij, podatke o več relacijskih računih in informacije nadzora aplikacij.

- *Dinamična posodobitev aplikacij*

Posodobitev podatkov na kartici je možno doseči s ponovnim pisanjem na kartico pod varnostnim nadzorom. Elektronsko lahko posodobimo informacije o bančnem računu, spreminjamo imena in naslove, limit računa, poslovna pravila za vsako aplikacijo ali račun posebej ter lahko dodamo nov račun. Posledica te lastnosti je, da kartici podaljšamo življenjsko dobo, kar omogoča izdajateljem, dodajanje novih storitev na kartico, ne da bi izdali nove.

- *Varen nadzor aplikacij*

Dostop do podatkov na kartici je možen direktno ali pa s PIN[3] kodo, ki jo pozna le lastnik kartice in je običajno štirimestna številka. Informacije shranjene na kartici so razdeljene v tri področja. Prvo področje ima prost dostop do podatkov, ki so ekvivalentni podatkom z magnetne kartice. Drugo področje vsebuje zaupne informacije dostopne le z aplikacijsko logiko kot na primer odobritev zneska plačila s kartico. Posamezni oskrbovalec aplikacij ne more pogledati podatkov in poslovnih pravil drugega oskrbovalca. Tretje ali skrivno področje vsebuje informacije, ki niso dostopne od zunaj, kot recimo PIN koda kartice.

- *Rutinske odločitve na kartici*

Računalniško programiranje omogoča izdajatelju aplikacij, vnos niza poslovnih pravil in kontrolnih vrednosti v svojo aplikacijsko datoteko. Izdajatelj lahko določi pravilo poslovanja,

[3] Personal Identification Number.

kjer se kartica na podlagi le-teh odloči, ali bo transakcija potekala online ali offline. Tako lahko, na primer, omeji vse offline transakcije na maksimalno štiri transakcije v 30-ih dneh ali na skupno vrednost 300 dolarjev. Če je ena od teh omejitev presežena, kartica takoj zahteva on-line avtorizacijo. Omejitve se lahko nastavijo za vsakega imetnika kartice posebej. Ta metoda selektivne on-line kontrole zniža izgube izdajateljem v primerjavi s sistemom on-line avtorizacij kreditnih kartic z magnetnim trakom, ker lahko kartico zaradi slabega poslovanja zaklenemo.

- *Produktivnost komunikacij*

Veliko zmanjšanje števila transakcij, ki potrebujejo on-line avtorizacijo, omogoča obstoječemu omrežju vzpostaviti transakcijski sistem, ki ima večji obseg aktivnosti. Z obstoječim omrežjem lahko do deset krat povečamo obseg transakcij z uporabo pametnih kartic. Lokalne odločitve zmanjšajo nepotrebno uporabo telefonskih linij in s tem omejijo možnost vdora v on-line sistem.

- *Večja uporabnost*

Pametna kartica omogoča 16 različnih aplikacij, ki imajo lastna navodila in protokole za njihov nadzor. Vsaka aplikacija dovoljuje povezavo z oskrbovalcem določene aplikacije, ne da bi obremenjevala omrežja izdajatelja kartice. Za imetnika to pomeni bolj udoben način poslovanja, kajti ena pametna kartica lahko zamenja več različnih magnetnih kartic. Za oskrbovalce aplikacij pa najem prostora na pametni kartici pomeni nižje stroške, kot če bi sami morali izdajati kartice.

Med vsemi lastnostmi pametne kartice pa je najpomembnejša varnost. Pravilno načrtovane pametne kartice praktično ni moč ponarediti. Večji problem predstavlja vprašanje, kako zagotoviti, da kartico res uporablja njen zakoniti imetnik. Ta problem je pogost pri elektronskem poslovanju, kjer imajo stranke opravka s terminali brez operaterjev, ki bi lahko preverili stranko. Zaenkrat se večinoma uporablja metoda s PIN kodo, ki pa ni popolnoma zanesljiva, saj jo lahko ukradejo ali zlorabijo. Edina zares učinkovita metoda verificiranja imetnika kartice je merjenje fizioloških značilnosti, ki so edinstvene za vsakega posameznika in se jih ne da prekopirati ali zlorabiti. Takšne biometrije vključujejo sliko očesne mrežnice, geometrijo rok ali obraza, DNK, vendar najraje in najbolj sprejemljiva značilnost je prstni odtis. Prstni odtis zasede le nekaj sto zlogov prostora na kartici. Naprava za branje prstnih odtisov na terminalu preveri, ali se ujema s prstnim odtisom shranjenim na kartici in če se, omogoči uporabo kartice. Če se pa odtisa ne ujemata, kartica ne dovoli dostopa do ponudnika storitev.

Zaradi vseh naštetih lastnosti se pametna kartica vse bolj uveljavlja tako v poslovanju, kot vsakdanjem življenju. Razen tega, da lahko z njo plačujemo, lahko tudi nanjo shranimo podatke o zdravstvenem zavarovanju, lahko jo imamo za vstop v zavarovane dele svojega podjetja ipd. Omogoča nam, torej, opravljati najrazličnejše storitve na varen način.

Laserske kartice

Laserska ali optična kartica ima na svoji spodnji strani 35-milimetrski optični refleksijski trak, na katerega se s pomočjo laserja zapisuje in bere podatke. Prednosti te kartice so predvsem: velika kapaciteta shranjevanja podatkov, varnost in dolga življenjska doba. Na kartico lahko shranimo do 2000 strani besedila in nekaj slik, kar omogoča boljšo identifikacijo imetnika kartice. Ta kartica sodi med najvarnejše, saj je ni možno prekopirati ali spreminjati podatke, ker so šifrirani. Življenjska doba kartice je približno deset let, ob vsakdanji uporabi. Edina slabost pa je visoka cena tako kartic kot tudi bralno pisalnih naprav. Verjetno je tudi to razlog, da se jih v slovenskih bankah še ne uporablja (Rotovnik, 1999, str.18).

3.2.2. Prednosti kreditnih kartic

Uporaba kreditnih kartic se je v zadnjih letih zelo razširila, ker prinaša prednosti za izdajatelja, prodajalca in imetnika kartic. Najpomembnejše prednosti so (Odar, 2000, str. 96-97):

Prednosti za imetnike kreditnih kartic:

1. Za imetnika kreditne kartice je največja prednost, da mu omogoča kreditiranje. V trenutku nakupa je lahko brez likvidnih sredstev, kajti kupnino bo poravnal kasneje, ko ga bo v skladu s pogodbo k temu pozval izdajatelj kreditne kartice.
   Kredit, ki ga imetnik izkoristi, je lahko blagovni (nakup blaga) ali finančni (dvig gotovine z bančnega računa oziroma najpogosteje iz bančnega avtomata). S pogodbo med izdajateljem in imetnikom kreditne kartice so določeni pogoji za njeno uporabo, ti pa posredno opredeljujejo tudi kreditne pogoje.
2. Imetnik lahko kupuje blago oziroma poravnava svoje račune brezgotovinsko. Z uporabo kreditne kartice se izogne vsem tistim nevšečnostim, ki jih povzroča gotovinsko plačevanje, saj kartica omogoča nakup v vsakem trenutku, ne glede na to, ali ima pri sebi kaj denarja.
3. Z uporabo kreditne kartice denar, ki bi ga pri gotovinskem plačevanju morali dvigniti z računa pri banki, ni vezan. Dohodkovno je to velika prednost, saj se denar v banki obrestuje do trenutka dviga z računa.
4. Če je pravna oseba imetnica kreditne kartice, ji ni treba uporabljati naročilnic. Tako se izogne morebitnemu zavračanju naročilnic pri podjetjih, ki kupca oziroma njegove bonitete ne poznajo dovolj.
5. Pri podjetjih (tako pri kupcih kot tudi pri prodajalcih) se zmanjšajo evidence o dvigovanju in polaganju gotovine ter s tem povezani stroški, manjše pa je tudi tveganje, kakršno sicer spremlja gotovinsko poslovanje.

Prednosti za prodajalce, ki sprejemajo kreditne kartice:

1. Prodajalci se odločajo prodajati na kreditne kartice, ker računajo, da se jim bo zaradi brezgotovinskega plačevanja in kreditiranja povečala prodaja. Ker kreditne kartice ne more pridobiti vsakdo, saj izdajatelj zanj pred izdajo preveri tudi boniteto, kupci s kreditnimi karticami pripadajo sloju ljudi, ki se praviloma odloča za nakup izdelkov višjega cenovnega razreda.
   Ker pa je kreditna kartica tudi kreditni inštrument, potrošniki pogosto kupujejo blago, ki jih običajno ne bi, ker pri sebi ne bi imeli dovolj gotovine ali čekov in ker se zavedajo, da bodo račun dejansko poravnali kasneje.
2. Izdajatelj plačilne kartice jamči za plačila; prodaja na kreditne kartice je tako zanesljivo plačana, to pa je danes zelo pomemben dejavnik, ki vpliva tudi na odločitve o načinu prodaje.

Prednosti za izdajatelje kreditnih kartic:

1. Izdajatelji kreditnih kartic so praviloma banke in druge specializirane finančne organizacije, ki kreditirajo potrošnike. Običajno gre za kratkoročno kreditiranje, ki ga kot enega izmed bančnih poslov opravljajo druge finančne organizacije.
2. Izdajatelji kreditnih kartic praktično živijo od članarine in/ali drugih zneskov, ki jih zaračunavajo imetnikom kreditnih kartic, pa tudi od provizije, ki jo zaračunavajo prodajalcem na kreditne kartice. Članarina se plačuje vnaprej, provizija pa sproti, tako da imajo izdajatelji zanesljive in stalne vire financiranja.
3. Z izdajanjem in uveljavljanjem kreditnih kartic izdajatelji uveljavljajo svoje ime oz. blagovno znamko, kar jim pomaga tudi pri drugih finančnih poslih, predvsem v povezavi z bankami ter pri dajanju in najemanju kreditov.

3.2.3. Slabosti kreditnih kartic

Toda kreditne kartice imajo tudi nekaj slabosti. Izstopajoče so naslednje (Odar, 2000, str. 97-98):

Slabosti za imetnike:

1. Ker je kreditna kartica namenjena kreditnemu in brezgotovinskemu nakupovanju, kar smo omenili kot veliko prednost, je to vsaj tako velika slabost predvsem za ljudi, ki so potrošniško usmerjeni in običajno ne vodijo evidence o potrošenih sredstvih oziroma ne razmišljajo o odhodkovni strani svojega proračuna. Ker je prodaja na kredit dokaj pogosto podprta z učinkovito reklamo in zato dokaj mamljiva, nekateri prekoračijo svoje finančne zmožnosti in kupujejo blago, ki si ga v resnici ne morejo privoščiti.
2. Članarina je lahko precejšen izdatek, ki dodatno bremeni imetnika kartice.

3. Izguba ali vsakršna drugačna, nezakonita odtujitev kartice lahko, kljub v sistem posameznega izdajatelja vgrajenim mehanizmom za preprečevanje zlorab, povzroči nezakonito in nepooblaščeno uporabo kartice z vsemi stroški v tej zvezi.

Slabosti za prodajalce, ki sprejemajo kreditne kartice:

1. Prodajalci morajo izdajatelju plačevati provizijo za prodajo na kreditne kartice. Provizija se določi s pogodbo in je običajno odvisna od prometa.
2. Če želi biti prodajalec konkurenčen, mora omogočati prodajo na različne kreditne kartice, kar pa je zanj dodatna obremenitev.

Slabosti za izdajatelje:

1. Izdajatelj mora od imetnika kreditne kartice čimprej izterjati plačilo in tako skrajšati čas plačila računa prodajalcu do prejetja plačila imetnika kartice. Ker je imetnikov veliko, mora izdajatelj računati tudi na njihovo nelikvidnost, bankrot ali druge težave, zaradi katerih plačila niso pravočasna. Tudi stroški tožb in izterjatve zapadlih plačil so lahko precejšnji, zato izdajatelji kartic pred izdajo temeljito preverjajo boniteto morebitnih imetnikov.

3.2.4. POS terminali

Včasih je plačevanje s plačilnimi karticami na prodajnih mestih potekalo s strojčkom za odtiskovanje s pomočjo katerih so se podatki s kartice ročno odtisnili na potrdilo ob nakupu. Pri vsakem nakupu je moral trgovec preveriti ali se kartica nahaja na seznamu preklicanih kartic, kar je bilo dokaj zamudno. Takšne aparate so zamenjale elektronske naprave, POS terminali, ki omogočajo elektronsko odčitavanje kartic in so povezani z bančnim računalniškim omrežjem preko telefonske linije.

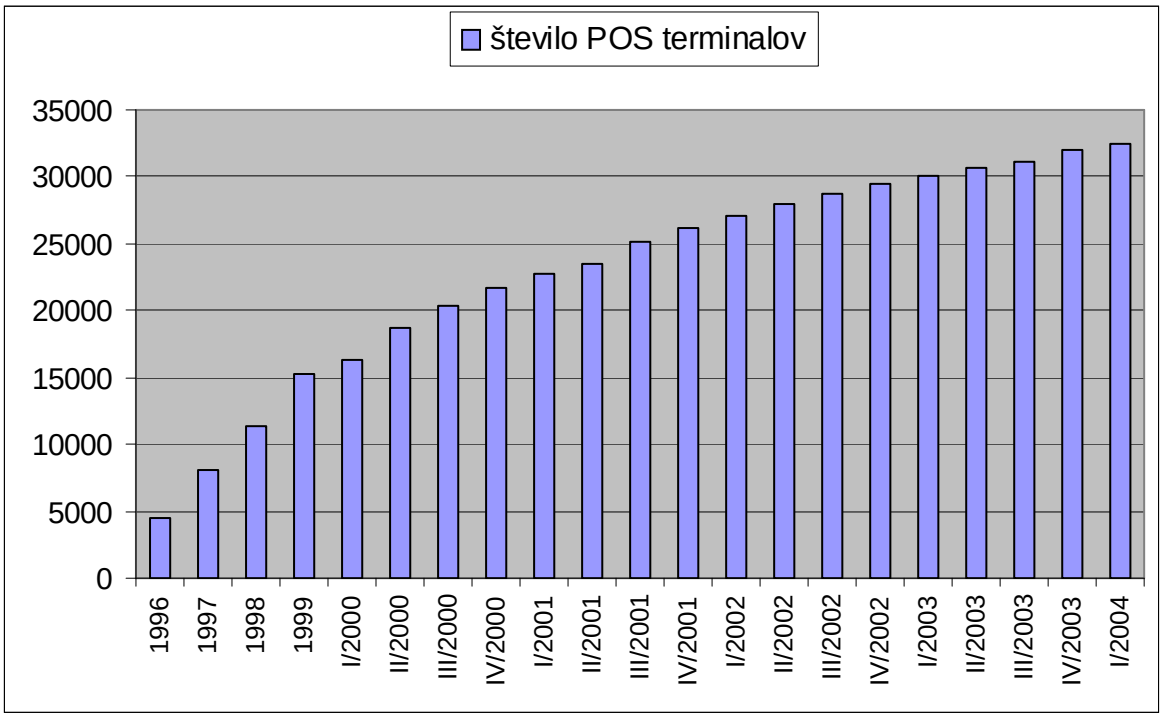
POS terminali imajo v primerjavi s poslovanjem s plačilnimi karticami naslednje prednosti (Novak, 1995, str. 46-47):

1. Terminal preveri, če se kartica nahaja na seznamu preklicanih kartic in seveda potem diskretno opozori prodajalca. Na ta način se prodajalec izogne vsakršnemu tveganju in posledicam škodne odgovornosti.
2. Terminal ugotovi veljavnost kartice in če je rok veljavnosti potekel, jo zavrne.
3. Prednost je avtomatska avtorizacija, kar pomeni, da v primeru plačevanja višjih zneskov odpade zamudno telefonsko preverjanje stanja na kupčevem računu, saj terminal potrdi avtorizacijo avtomatsko.
4. Terminal omogoča plačevanje storitev in blaga imetnikom različnih kartic.

5. POS terminal samodejno natisne potrdilo o nakupu z vsemi potrebnimi podatki o imetniku kartice in prodajnem mestu. Trgovcem ni več potrebno nabavljati, shranjevati ter pripravljati potrdil o nakupih, skratka manj papirnatega dela.
6. Delovanje POS terminala poteka v jedrnatem in jasnem slovenskem jeziku.
7. Plačila potekajo hitreje kot na ročni način.
8. Ni več potrebnih fizičnih poti v banko in pošiljanje dokumentov po pošti, saj se vse začne in zaključi preko komunikacije med terminalom in osrednjim računalnikom v banki. Obračun prometa med trgovcem, banko in imetnikom kartice poteka nevidno.
9. POS terminal omogoča enostaven zaključek poslovanja, saj ni več dolgotrajnega seštevanja potrdil o nakupu in pisanja specifikacij.

V Sloveniji narašča število elektronskih prodajnih mest. Nekatera prodajna mesta imajo celo dva POS terminala, kar pa ni najbolj smotrno, saj se nekateri stroški podvajajo. Slika 3 kaže rast števila POS terminalov v Sloveniji od leta 1996 naprej. Od leta 2000 so podatki prikazani za vsako četrtletje posebej.

Slika 3: Rast števila POS terminalov v Sloveniji



Vir: Bilten Banke Slovenije, 2004.

3.2.5. Elektronska denarnica in elektronski denar

Ob tradicionalnem načinu plačevanja z gotovino se vedno bolj uveljavlja tudi ti. elektronski denar (ang. digital cash). Teoretično bi si sicer lahko predstavljali družbo, kjer bi vsa plačila

potekala negotovinsko, v praksi pa bo zaradi svojih prednosti, kot so udobnost, hitrost, predvsem pa anonimnost poslovanja, gotovina še marsikje nenadomestljiva. (Zebec Koren, Cvjetović, 2001, str. 55). Menim, da bo v prihodnosti zelo narasel delež plačil opravljen negotovinsko, toda še dolgo se bodo ljudje oklepali gotovinskega poravnavanja računov, predvsem zaradi anonimnosti.

Prvi, ki mu je prišlo na misel ustvariti elektronski denar je bil David Chaum. Izvorna ideja so bili elektronski kovanci, ki bi omogočali anonimnost in varnost, tako kupcu, kot trgovcu. Elektronski kovanci predstavljajo denar, ki ga je bančni komitent dvignil s svojega računa in je bil pretvorjen v elektronske kovance shranjene v njegovi elektronski denarnici. Komitent lahko, kadarkoli želi, nakupuje oz. plačuje s takšnimi kovanci.

Uporaba pametnih kartic za hranjenje elektronskega denarja je praktična zato, ker jo kot plačilno kartico enostavno lahko nosimo s seboj in uporabljamo. Zagotavlja zaščito pred nepooblaščenim kopiranjem in razmnoževanjem. To pomeni, da je elektronska denarnica posebna izvedenka pametne kartice, ki ima vso potrebno programsko opremo za hranjenje in prenos denarja v elektronski obliki. Prenos denarja v elektronske denarnice izvajamo s pomočjo posebnih terminalov, bančnih terminalov - bankomatov, posebnih terminalov na javnih mestih in domačih terminalov.

Treba je poudariti, da se elektronsko denarnico predvidoma uporablja za hranjenje majhnih denarnih vrednosti. Zaščita pred nepooblaščeno uporabo je zagotovljena s pomočjo kode Personal Identification Number (PIN). Število napačnih vnosov je omejeno, tako da je zloraba praktično nemogoča. V vsakem primeru lahko najditelj denarja v gotovini svojo najdbo precej hitreje unovči, kot če najde elektronsko denarnico (Mihelčič, 1999, str. 10).

V devetdesetih letih prejšnjega stoletja se je po svetu pojavilo veliko število sistemov elektronskih denarnic. Med bolj znanimi so Mondex v Veliki Britaniji, Proton v Belgiji, Geldkarte v Nemčiji in VisaCash. V prvi polovici devetdesetih let so bila pričakovanja pri uvajanju prvih pilotskih projektov elektronskih denarnic visoka. Dokaj hitro so ugotovili, da so bila ta pričakovanja znatno precenjena. V drugi polovici devetdesetih let so opustili kar nekaj pilotskih projektov zaradi nezainteresiranosti javnosti. Ostali projekti pa so se nadaljevali, vendar z omejenim uspehom. Mondex je svoj prvi pilotski projekt začel leta 1995 v angleškem mestu Swindon, po treh letih pa je bil opuščen. Ob koncu je sodelovalo 14000 uporabnikov kartic, kar je precej manj, kot je bilo v načrtu, saj so že ob koncu leta 1995 načrtovali 25000 uporabnikov. Podobno usodo je doživel tudi projekt Mondex-a in VisaCash-a na Manhattan's Upper West Side-u. Opuščen je bil konec leta 1998, po petnajstih mesecih delovanja. S tehničnega stališča je bil test uspešen in je pokazal, da lahko dva sistema delujeta na isti opremi. Vendar ekonomsko je bil ta test polomija. Čeprav so trgovci prejeli brezplačne terminale, so enega za drugim ukinjali, tako da je blizu konca poskusa ostala v uporabi le četrtina od začetnih 675 terminalov. Odgovor potrošnikov je bil prav tako skromen, saj je bilo redno uporabljanih le 8 do 10 odstotkov izdanih elektronskih denarnic (Van Hove, 2000).

Začetno počasno prisvajanje elektronskih denarnic ima ekonomski smisel. Elektronske denarnice so predmet tako imenovane »mrežne stvarnosti«, kar pomeni, da uporaba elektronskih denarnic narašča skupaj z velikostjo lastne mreže, to je s številom prodajnih mest, kjer jo sprejemajo. Poleg tega pa naraščanje števila uporabnikov elektronskih denarnic spodbuja nove trgovce, da jih začnejo sprejemati. Spodbujajoče dejstvo je, da gre novejšim elektronskim denarnicam bolje, ker zgleda, da so premagali začetne težave, ki so pestile izdajatelje prvih elektronskih denarnic. Izkušnje so pokazale, da se je bolje izogniti prehitremu uvajanju sistema elektronske denarnice, ker premajhno pokritje lahko ogrozi pozitivni povratni učinek. V skrajnih primerih lahko povzroči celo negativen povratni učinek, ki ga lahko pospešijo uporabniki in mediji (Van Hove, 2000).

Bujna rast različnih programov digitalnih denarnic je bila posledica tega, da so bili sistemi med sabo nezdružljivi. Medsebojna združljivost (interoperabilnost) ima velik pomen pri podpori uporabe digitalnih denarnic. Želje po razširljivih in nadgradljivih sistemih, mednarodni uporabi, predvsem pa po cenovno dostopnih sistemih so še povečale potrebo in pomembnost specifikacije, ki bi bila globalna in medsebojno združljiva. Zato so Mastercard, Visa, Europay uvedle marca 1999 specifikacijo CEPS[4], ki določa zahteve za vse organizaciji potrebne komponente za uvedbo globalno delujočega programa digitalne denarnice, opisuje varnost sistema, potrjevanje in prenose. CEPS tlakuje pot za odprt, dejansko globalni standard digitalne denarnice (Zebec Koren, Cvjetović, 2001, str. 55).

CEPS zahteva združljivost s specifikacijo EMV (Europay Mastercard Visa) za pametne kartice in določa zahteve za medsebojno združljive kartične aplikacije, vmesnike kartica-terminal, terminalske aplikacije za prodajna mesta, podatkovne elemente in priporočeni format sporočil za transakcijsko procesiranje. CEPS zagotavlja funkcionalne zahteve za udeležence shem elektronskih denarnic in uporabo kriptografije javnih ključev za zagotovitev varnosti. CEPS je zgrajen na osnovi EMV, vendar z razširitvijo na globalno medsebojno združljivost shem digitalnih denarnic (Zebec Koren, Cvjetović, 2001, str. 55).

Prednosti za finančne ustanove sta, z uporabo specifikacije CEPS, vsaj dve. Zaradi razširjenosti in mednarodnega značaja so naložbe varnejše, ustanove pa lahko ponudijo izdelke in storitve z dodano vrednostjo. Lastniki digitalnih denarnic CEPS pridobijo možnost, da različne valute shranjujejo na eni sami kartici in da so njihove kartice sprejete tako doma kot na tujem, kjerkoli bo objavljen znak sprejemanja digitalnih denarnic CEPS. Prodajalci bodo omogočili nakupe tudi kupcem, ki že imajo, ali bodo šele imeli digitalne denarnice CEPS, po drugi strani pa si zagotovijo enostavno in varno plačevanje malih zneskov (Zebec Koren, Cvjetović, 2001, str. 55).

[4] Common Electronic Purse Specification.

3.3. TELEFONSKO BANČNIŠTVO

Telefonsko bančništvo je oblika elektronskega bančništva, ki omogoča strankam opravljati bančne posle po telefonu. Obstajata dve obliki telefonskega bančništva in sicer prva s pomočjo avtomatskega telefonskega odzivnika ter druga z bančnim operaterjem.

Pri avtomatskem odzivniku moramo slediti navodilom že vnaprej pripravljenih posnetkov, kateri nas vodijo pri opravljanju želenih storitev. Storitve izbiramo s pritiskom določenih tipk na telefonski tipkovnici. Pogoj za tovrstno opravljanje storitev je telefon s tonsko izbiro ali pa navaden telefon s piskačem. Storitve so na voljo 24 ur na dan, vse dni v tednu. Odzivnik daje neznanim uporabnikom splošne informacije o bančni ponudbi, novostih, menjalniških tečajih, obrestnih merah in podobno. Znanim uporabnikom, ki se ob prijavi morajo identificirati s pomočjo osebnega gesla, pa odzivnik omogoča opravljanje storitev osebne narave, in sicer vpogled v stanje na računih, plačilo položnic in računov, naročilo čekov, vezavo tolarskih in deviznih depozitov, prenos sredstev med računi, otvoritev, spremembo in ukinitev trajnih nalogov, sprejemanje prošenj za povišano prekoračitev stanja na tekočem računu, izdajo plačilnih kartic itd.

V drugem primeru gre za pogovor v živo z bančnim operaterjem, kateri v našem imenu opravi želene storitve preko računalnika. Lahko izbiramo med vsemi zgoraj naštetimi bančnimi storitvami. Zaradi varnosti je potrebna identifikacija uporabnika.

Izdelali pa so še telefon z LCD ekranom, s katerim komitent pokliče banko in vse, kar je potrebno za opravljanje storitev, se prikaže na ekranu. Želeno storitev izbere in opravi s pritiskom tipk na tipkovnici.

Prednosti telefonskega bančništva so v tem, da je enostavno, hitro, praktično in ne potrebujemo drage opreme, ampak samo telefonski aparat. Tako lahko opravimo večino bančnih poslov kar doma iz naslanjača.

3.4. INTERNETNO BANČNIŠTVO

3.4.1. Internet

Internet, oziroma medmrežje, je največje računalniško omrežje na svetu, ki povezuje računalniške sisteme. Uporabnikom omogoča komunikacijo in dostop do podatkov. Je popolnoma decentralizirano in dostopno vsakomur. Zaradi hitre širitve in prednosti, ki jih ponuja, si dandanes težko predstavljamo poslovanje brez interneta.

3.4.1.1. Razvoj interneta

Prvo elektronsko omrežje namenjeno komunikaciji, je bilo postavljeno leta 1969, ko so štiri univerze v Združenih državah Amerike skupaj z ameriškim obrambnim ministrstvom razvile omrežje računalnikov, poznano pod imenom ARPANET. Cilj omrežja je bil omogočiti akademikom dostop do oddaljenih računalnikov. ARPANET je omogočal znanstvenikom opravljanje interaktivnih razprav, dostop do oddaljenih podatkovnih baz, izmenjavo datotek in pošiljanje elektronske pošte.

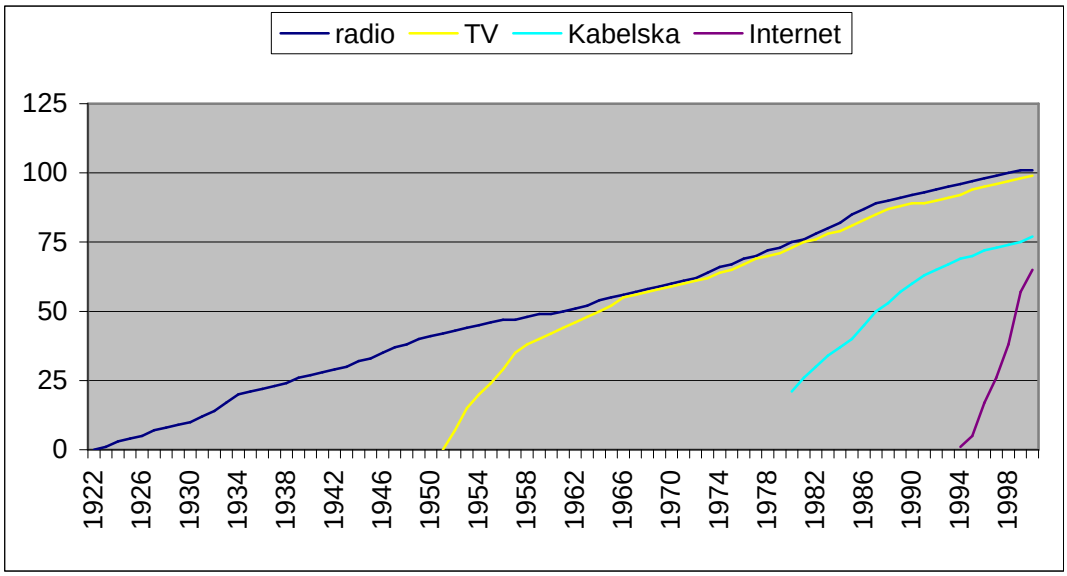
ARPANETOV protokol za nadzor omrežja, ki je bdel nad tem, kako so bile informacije poslane v njegovo lastno omrežje, so v zgodnjih osemdesetih zamenjali s protokolom TCP/IP. TCP/IP je standardiziral pretok informacij po omrežju. Protokol uporabnike omrežja razpoznava na osnovi njihovega internetnega naslova oz. domene. Njegova glavna prednost je bil izjemno robusten način prenašanja sporočil, saj uporablja individualno naslovljene pakete informacij. Načrtovan je bil za nezanesljivo omrežje, kar pomeni, da so načrtovalci predvidevali razne možnosti okvar, od prekinitve telefonske linije pa do atomskega napada.

Leta 1990 je Tim Berners-Lee s tem, ko je postavil prvo spletno stran v laboratoriju za fiziko delcev pri Evropskem centru za jedrske raziskave na francosko-švicarski meji, ustvaril splet. Berners-Leejev izum je obsegal tudi protokol za povezavo računalnikov, jezik HTML in sistem naslavljanja, kar je omogočilo nastanek neskončno bogatega omrežja dokumentov, povezanih v omrežju TCP/IP (Osojnik, 2002, str. 3).

Internet pa ni le sredstvo za komuniciranje, temveč tudi multimedijski prenosnik, na katerega se počasi, vendar vztrajno selijo tradicionalni mediji (TV postaje, časopisi, revije…). Seveda je širitev interneta bistveno hitrejša, kot je bilo to v primeru klasičnih medijev. Tako je npr. v ZDA radio potreboval 38 let, da je dosegel 50 milijonov uporabnikov, televizija 13 let, kabelska TV 10 let, Internet pa le 5 let.

V prvih letih se je internet najhitreje širil v ZDA: v letih 1995-1998 je odstotek uporabnikov med prebivalstvom starim od 15 do 65 let, naraščal po vzorcu, ki so mu kasneje sledile tudi druge države (1995 – 6% uporabnikov v populaciji 15-65 let, 1996 – 13%, 1997 – 27%, 1998 – 40%). V nekaterih skandinavskih državah je bila rast celo hitrejša in odstotek uporabnikov presega odstotek v ZDA. Širitev je v začetku eksponencialna, nato pa se nekoliko upočasni. Ob tem se seveda postavlja vprašanje, kje so meje širitve interneta. Ena od možnih omejitev je lahko delež prebivalstva, ki uporablja osebni računalnik. Seveda je taka omejitev vezana na trenutni tehnološki okvir interneta in se lahko s spremembo tehnologije – npr. zlitje računalnika s televizijo – hitro spremeni in drastično poveča (Vehovar, 1998, str. 153).

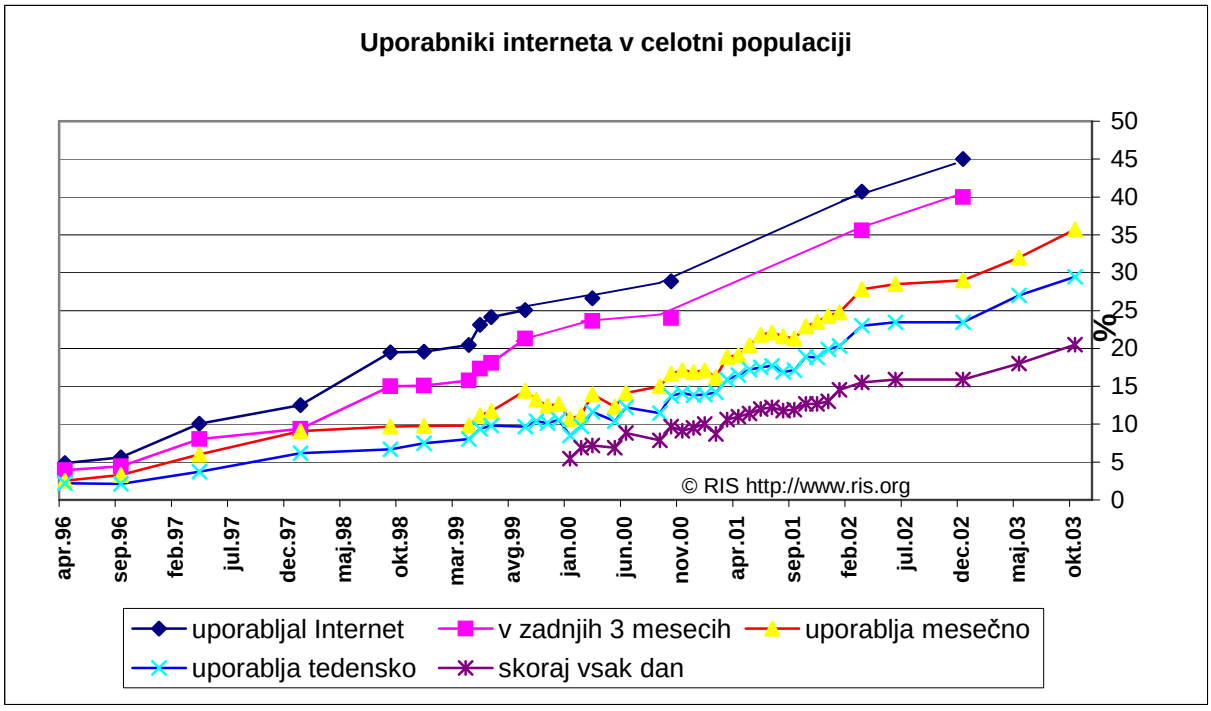
Slika 4: Difuzija medijev ZDA: radio, TV, kabelska TV in Internet (po Morgan Stanley)



Vir: Vehovar,1998, str. 153.

Širitev interneta v Sloveniji lahko vidimo na spodnjem grafu, kjer je prikazan rast deleža uporabnikov interneta v celotni populaciji (cca. 2,000,000 oseb) glede na pogostost uporabe interneta, za obdobje od aprila 1996 do maja 2003. V vsakem primeru pa se pri širjenju interneta očitno nahajamo v fazi povsem upočasnjene letne rasti, ki znaša zgolj 10-15% letno.

Slika 5: Uporabniki interneta v celotni populaciji* RIS, 1996 – 2003 (oktober).



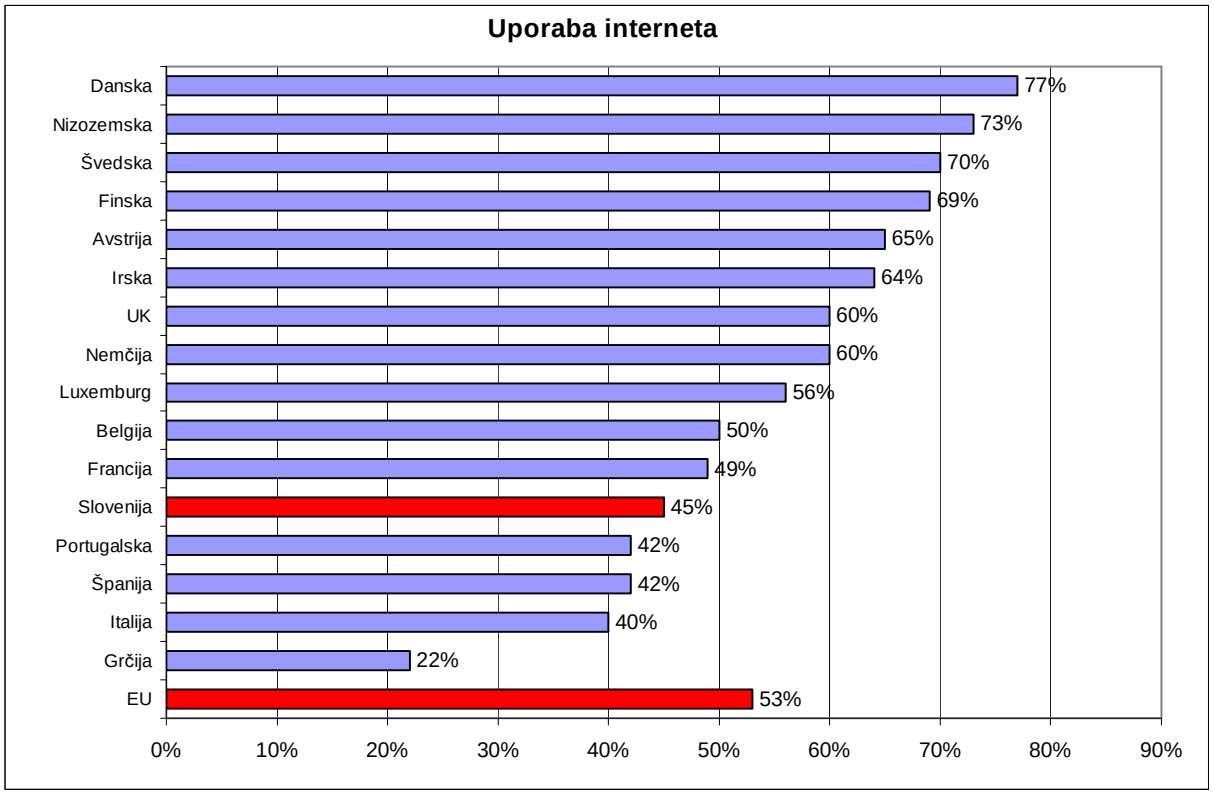
* Celotna populacija pomeni 1,985,557 oseb, kar so zaokrožili na 2,000,000 oseb.

Vir: RIS, Gospodinjstva: Uporaba Interneta, 2004, str. 26.

Zanimiva pa je primerjava razširjenosti interneta v Sloveniji in drugih Evropskih državah. Konec leta 2002 je 45% Slovencev starih 15 let in več, izjavilo, da uporabljajo internet vsaj na eni od lokacij. To je 8% manj kot v EU, kjer delež uporabnikov interneta po enakih meritvah znaša 53%.

Med vsemi državami EU je delež uporabnikov interneta najmanjši v Grčiji (22%) in največji na Danskem (77%). Slovenija je po deležu uporabnikov pred državami iz juga EU (Grčija, Italija, Španija in Portugalska) in zaostaja za vsemi državami severno od sebe. Razlike v deležu uporabnikov interneta so spodaj prikazane še grafično.

Slika 6: Uporaba interneta: primerjava Slovenija – EU, december 2002



Vir: Primerjava Slovenija – EU, 2003, str.10.

3.4.1.2. Storitve interneta

Internet ponuja uporabnikom več storitev. To so predvsem orodja, ki omogočajo medsebojno komunikacijo in dostop do podatkov vseh vrst po vsem omrežju internet. Medsebojno komunikacijo omogočajo elektronska pošta (ang. e-mail), protokol za prenos datotek (ang. File Transfer Protokol-FTP), klepet (ang. Chat), novice (ang. USENET), medtem ko dostop do podatkov pa svetovni splet (ang. World Wide Web- WWW) in hrček (ang. Gopher).

Najpogosteje uporabljani storitvi pa sta elektronska pošta in svetovni splet, ki ju bom na kratko opisal.

Elektronska pošta omogoča pošiljanje in sprejemanje elektronskih sporočil med uporabniki interneta. Sistem je zelo podoben sistemu klasične pošte, vendar je precej hitrejši. Sporočila iz Slovenije potujejo v ZDA le nekaj minut. Poleg samega teksta lahko pošiljamo tudi razne dokumente, slike, animacije in druge podatke. Programi, ki služijo kot odjemalci elektronske pošte, so praviloma že vgrajeni v operacijske sisteme in vsebujejo visoke varnostne standarde (Jerman Blažič, 1996, str. 23).

Svetovni splet ali WWW (World Wide Web) je praktično neomejen vir informacij, ki iz dneva v dan raste. Ta storitev je dosegla izjemen uspeh, ker je prijazna do vseh uporabnikov, tudi tistih z malo računalniškega znanja. Glavna značilnost je ta, da so v njej dokumenti predstavljeni v obliki hiperteksta, besedila obogatenega z večpredstavnimi elementi, kot so slike, zvok in video. Nekateri deli besedila so lahko vez (ang. link) do drugih sorodnih dokumentov, kar omogoča lažje in bolj pregledno iskanje in pregledovanje dokumentov. Prednost svetovnega spleta je tudi njegova interaktivnost, saj omogoča uporabniku, ne le sprejemanje informacij, temveč tudi pošiljanje povratnih informacij. Za iskanje po spletu so nam na voljo računalniški programi, ki nam omogočajo iskanje po posameznih področjih ali po ključnih besedah, kar nam bistveno olajša iskanje v tem morju informacij.

3.4.2. Temeljne funkcije internetnega bančništva

Bančništvo preko interneta ne zajema le izvajanje nekaterih bančnih transakcij, ampak se prek njega lahko izvajajo štiri temeljne funkcije (Bec, 2000, str. 53-54):

1. **Predstavitev informacij:** Gre za enosmerno komunikacijo, kjer poteka predstavitev informacij o bančnih storitvah in je najpreprostejša oblika uporabe interneta v bančništvu. Banka obvešča svoje komitente o svojih storitvah preko vnaprej izdelane multimedijske predstavitve na svetovnem informacijskem spletu.

2. **Predstavitev informacij z dvosmerno komunikacijo** predstavlja nadgradnjo predstavitve informacij, kjer banka s komitentom vzpostavi dvosmerno komunikacijo, velikokrat kar z uporabo elektronske pošte. Pri predstavitvi informacij z eno ali dvosmerno komunikacijo internet služi le kot cenen medij, ki nadomešča tradicionalne načine tržne komunikacije, npr. časopis, radio, TV, pošto itd.

3. Pri **interakciji z uporabniki** banka preko interneta ponudi uporabniku dostop do njegovih podatkov, npr. vpogled v stanje na vseh računih, vpogled v promet na tekočem računu, vpogled v stanje portfelja vrednostnih papirjev itd. Omenjeni podatki so zaupne narave, zato je potrebna ustrezna identifikacija in avtorizacija uporabnikov.

4. **Izvajanje transakcij** je najzahtevnejša oblika bančništva preko interneta, kjer se opravljajo razna plačila (npr. plačevanje položnic, plačevanje s plačilnim nalogom), prenos sredstev in še druge storitve. V okviru transakcij preko interneta so banke in njeni komitenti izpostavljeni velikemu tveganju v smislu morebitnih zlorab, zato morajo banke zagotoviti učinkovite varovalne mehanizme in temu posvetiti zelo veliko pozornosti, da se bo še bolj povečalo zaupanje v izvajanje transakcij preko interneta.

3.4.3. Tveganja pri internetnem bančništvu

Internetno bančništvo prinaša tudi tveganja, katerih se banke zavedajo in zato uporabljajo kombinacije sodobnih tehnologij za zaščito poslovanja. Nekatera od tveganj za banke so (Bilten Banke Slovenije, 2003):

- tveganja varnosti in nedotakljivosti zaupnih podatkov;
- tveganja zagotavljanja ustreznega nivoja razpoložljivosti (24/7, odzivni čas);
- tveganja prenov informacijskih sistemov;
- tveganja informacijske strukture (pomanjkljivost novih znanj);
- tveganja oddaje del (uporaba zunanjih izvajalcev – razvoj programske opreme, ponudniki interneta, celotno izvajanje posameznih podpor);
- tveganja neizvajanja revizije in kontrole za nova področja;
- tveganja neustreznega upravljanja s kakovostjo (pomanjkljiva testiranja);
- tveganja zaradi neustreznega obvladovanja sprememb (planiranje, spremljanje, ukrepanje)

Za uporabnika internetnega bančništva pa so bolj izpostavljena tveganja sledeča:

- nepooblaščen vpogled sredstev na računu
- nepooblaščen prenos sredstev z računa
- prestrezanje gesla
- razkritje zasebnega ključa
- nepooblaščena uporaba zasebnega ključa

3.4.4. Varnost

Zaradi naštetih tveganj je varnost poslovanja na internetu ključni segment tovrstnega poslovanja. Kajti internet je omrežje, ki se neprestano spreminja. Z vsako novo storitvijo ali dodatkom k obstoječi storitvi se lahko pokaže ranljivo mesto in s tem morebitni viri težav. Kljub napredku na področju varnostnih sistemov vdiralcem pogosto uspe, preko interneta vdreti na spletne strani ali v informacijski sistem. Zato je potrebno informacije na spletnih straneh in poslane podatke zaščititi z varnostnim sistemom, ki je dovolj prožen, da se lahko

prilagaja novim potrebam. Vdiralce je potrebno odvrniti, tako da se jim ne bo zdelo vredno porabiti časa in sredstev, da bi nas ogoljufali (Osojnik, 2002, str. 122).

Pri elektronskem bančništvu je varnost eden od ključnih dejavnikov zaradi katerih se komitenti odločajo oz. ne odločajo za uporabo internetnega bančništva. Zanimivi so rezultati raziskave RIS (Raba Interneta v Sloveniji), kjer so uporabnike interneta spraševali, zakaj ne uporabljajo elektronskega bančnega poslovanja. Kar 13 odstotkov anketirancev je odgovorilo, da tovrstnemu bančništvu ne zaupa. To je še dodaten razlog za banke, da vlagajo čimveč sredstev za večjo varnost internetnega poslovanja.

3.4.4.1. Varnostne storitve

Med najpomembnejše varnostne storitve, ki nam omogočajo nadzor varnosti, uvrščamo pristnost, avtorizacijo, zaupnost, celovitost, nezavrnitev in nadzor pretoka (Šinigoj, Turk, 1999, str. 459):

Pristnost (ang. authentication)

Pristnost oz. avtentikacija sporočila zagotavlja prejemniku, da je sporočilo res poslal navedeni pošiljatelj in je pristno oz. ni ponarejeno.

Pri uporabnikih interneta največkrat srečamo dve vrsti dokazovanja pristnosti:
- dokazana pristnost za delo v nekem sistemu
- storitev mora zagotavljati, da povezava ni prestrežena ali motena (ang. interfered) na tak način, da bi se neka tretja oseba prikopala do neavtoriziranega oddajanja ali sprejemanja podatkov. Iz tega tudi sledi, da veliko sporočil, transakcij in elektronske pošte prek interneta zahteva dokazovanje pristnosti vira. To lahko storimo z uporabo digitalnega podpisovanja.

Avtorizacija - pooblastilo (ang. autorisation)

Pri avtorizaciji gre za nadzor dostopa do določenih informacij. Uporabnik, ki želi informacije dostopa, se mora identificirati in hkrati dokazati svojo pristnost, da je res objekt, ki ima pravico do teh podatkov. Največkrat gre za uporabo gesla in uporabniškega imena. Pojma avtorizacija in pristnost se v praksi večkrat mešata.

Zaupnost (ang. confidentiality)

Vsaka zaupna informacija, ki se prenaša po internetu, bi morala biti šifrirana. Šifriranje zaščiti občutljive informacije, vsebovane v elektronski pošti, FTP-ju in elektronskem trgovanju prek interneta. Skoraj vse rešitve pri zaupnosti podatkov uporabljajo različne metode šifriranja, ki postaja ena najpomembnejših tehnoloških rešitev v elektronskem poslovanju.

Celovitost (ang. integrity)

Za določen tip podatkov bodo uporabniki interneta potrebovali zagotovilo, da se podatki niso spremenili med prenosom preko interneta. Celovitost podatkov je lahko, npr. potrebna pri prenosu FTP-ja ali datotek elektronske pošte po internetu. Pri tem je potrebno ovreči dvom, da je bilo sporočilo med prenosom oz. shranjevanjem spremenjeno, skrajšano ali mu je bilo kaj dodano.

Nezavrnitev (ang. nonrepudiation)

Nezavrnitev pomeni ustvarjanje dokaza o izvoru podatkov, o opravljeni transakciji oz. o posredovanju podatkov. Pomeni zaščito pred tem, da bi pošiljatelj lažno zanikal, da je podatke poslal ali da bi prejemnik lažno zanikal, da jih je prejel. Prejemnik sporočila lahko dokaže, da je bilo sporočilo res poslano od omenjenega pošiljatelja in pošiljatelj lahko dokaže, da je prejemnik sporočilo res prejel. Najpogosteje gre v tem primeru za najrazličnejše pravne spore med dvema poslovnima strankama.

Nadzor pretoka (ang. transfer control)

Privatne mreže posameznih bank ali ustanov imajo vozlišča, ki prestrezajo in analizirajo sporočila, ki prihajajo iz ali pa so namenjena v internet. To vozlišče prestreza vsa sporočila, ki prihajajo iz interneta in preveri pristnost vsakega izmed njih. Poleg tega ta vozlišča filtrirajo pakete, ki temeljijo na naslovih IP[5] storitev interneta.

3.4.4.2. Varnost svetovnega spleta – varnostni protokoli[6]

Veliko časa je veljalo, da sta bili glavni pomanjkljivosti interneta uporabnost in varnost. Od začetka prejšnjega desetletja, ko je bil v švicarskem centru razvit HyperText Transfer Protocol (HTTP protokol) in zaradi uporabniku prijaznih vmesnikov in drugih orodij, je postal svetovni splet najprijaznejša in najbolj uporabljena storitev interneta. Še vedno pa ostaja problem varnosti.

Varnostne zahteve svetovnega spleta vključujejo zagotavljanje varne avtentikacijske poti, preverjanje pristnosti, zagotavljanje šifriranja in celovitosti podatkov med odjemalcem in strežnikom. Med številnimi varnostnimi protokoli na internetu so za varnost prenosa spletnih strani najpomembnejši: Secure Internet Protocol (IPsec) na omrežnem nivoju, Secure Sockets Layer (SSL) na transportnem nivoju in Secure HyperText Transfer Protocol (S-HTTP) na nivoju aplikacije.

[5] Internet Protocol.

[6] Celotno poglavje povzeto po Šinigoj, Turk, 1999, str. 463-464.

VAREN INTERNETNI PROTOKOL (IPsec)

Eden poglavitnih razlogov, zakaj prihaja do varnostnih problemov na internetu, je osnovna arhitektura in ranljivost protokola TCP/IP, saj ni bil originalno razvit zaradi tega, da bi omogočal resnično varne komunikacijske poti. Naslovi IP identificirajo vsakega gostitelja na internetu in mu dostavijo ustrezne podatke. Izboljšana varnost prometa IP je bila potrebna iz dveh ključnih razlogov:

- Internet, intraneti in ekstraneti podjetij temeljijo na protokolih IP. Ves promet mora potovati skozi nivo IP in ves promet potuje v obliki paketov IP.

- Z zaščito nivoja IP zaščitimo in izoliramo tudi višje nivojske aplikacije pred napadi oz. dopolnimo obstoječe varnostne mehanizme na višjih nivojih.

Varen internetni protokol (v nadaljevanju IPsec) je dodatek k že obstoječemu IP-u, da bi preprečil spreminjanje, branje IP paketov ter razkritje naslovnika. IPsec je nastal kot del nove različice IP: Internet protokol naslednje generacije (ang. Internet Protocol next generation – Ipng), hkrati pa je bil prirejen, da deluje tudi na sedanji verziji IP (Ipv4). Varnost protokolov IPsec je zagotovljena prek dveh protokolov: IP AH (IP Authentication Header[7]) in IP ESP (IP Encapsulating Security Payload[8]).

PROTOKOL SECURE SOCKETS LAYER (SSL)

Secure Sockets Layer (v nadaljevanju SSL) protokol je varnostni protokol na transportnem nivoju, ki ga je razvilo podjetje Netscape, da bi zagotovil varno povezavo med odjemalcem in strežnikom, ki komunicirata prek javnega kanala in je najpogosteje uporabljen varnostni protokol pri komuniciranju med strežnikom in odjemalcem. SSL omogoča avtentikacijo, enkripcijo in celovitost sporočila. Ko dva računalnika začneta komunicirati s pomočjo SSL-ja, najprej določita šifrirne algoritme in ključe, ki se bodo pri komunikaciji uporabljali. SSL je sestavljen iz treh protokolov: Record Protokol, Handshake Protokol in Alert Protokol.

PROTOKOL SECURE HYPERTEXT TRANSFER (S-HTTP)

Protokol Secure HyperText Transfer (v nadaljevanju S-HTTP) je razvilo podjetje Enterprise Integration Technologies, da bi zagotavljal varnostne storitve za transakcije HTTP. Varnostne storitve pri S-HTTP so zaupnost, avtentičnost, celovitost in nezavrnitev izvora transakcije in delujejo na nivoju aplikacije. Protokol poudarja čim večjo fleksibilnost pri izbiri mehanizmov za upravljanje s ključi, varnostne politike in šifrirnih algoritmov s podpiranjem možnosti za pogajanje med odjemalcem in strežnikom pri vsaki transakciji.

[7] IP AH preverja, če so podatki celoviti.

[8] IP ESP podatke šifrira.

Če odjemalec, ki podpira S-HTTP, vzpostavi povezavo s strežnikom, ki je ne podpira, ali pa obratno, potem tovrstna povezava ne uporablja varnostnih storitev S-HTTP. S-HTTP tudi ne zahteva certificiranega javnega ključa s strani odjemalca za šifriranje komunikacije, kar je pomembno, saj posameznim uporabnikom ni potrebno imeti javni ključ pred vzpostavitvijo povezave.

3.4.4.3. Preventivni načini in metode za zmanjšanje varnostnih tveganj

Požarni zid

Vsaka stalno aktivna internetna povezava poteka preko usmerjevalnika (ang. router) in obvezno preko neke oblike požarnega zidu (ang. firewall). Usmerjevalnik je naprava, ki upravlja pretok paketov med različnimi deli omrežja. Paketi so delčki informacij, ki potujejo po omrežju. Z uporabo filtrov, ki jih nastavimo v konfiguraciji samega usmerjevalnika, lahko nadziramo pretok paketov. Določenim vrstam paketov dovolimo ali onemogočimo dostop do določenih računalnikov. Opisano funkcionalnost vsebuje tudi požarni zid. Požarni zid je računalnik z ustrezno programsko opremo, ki omogoča zaščito notranjega omrežja pred vdori iz omrežja – interneta. Požarni zid razmeji in logično loči internet in notranje omrežje kakšne organizacije ter prepušča samo dovoljeni omrežni promet. V primerjavi s filtri na usmerjevalnikih, sistem požarnega zidu omogoča tudi višjo raven funkcionalnosti kot je, npr. protivirusna zaščita, njegova postavitev pa je enostavnejša (Osojnik, 2002, str. 122).

Banke uporabljajo požarni zid za zaščito svoje računalniške mreže pred vdori iz interneta in s tem, zaščito uporabnikovih zaupnih podatkov, ki so shranjeni v bančnem računalniku.

Toda požarni zid ne zagotavlja popolne varnosti omrežja pred vrstami paketov, ki so navidez varni. Primer takšne vrste paketov informacij je nov virus, ki ga požarni zid ne prepozna kot nevarnega. Zaradi tega mora banka nenehno nadgrajevati programsko opremo požarnega zidu.

Šifriranje

Ko se podatki prenašajo po različnih prenosnih poteh, so zelo ranljivi. V bančništvu gre za prenos podatkov med komitentom in banko pri internetnem bančništvu, telefonskem bančništvu in mobilnem bančništvu, pri samopostrežnem bančništvu pa gre za prenos podatkov med bančnim avtomatom in banko. Med prenosom jih lahko nepooblaščena oseba prestreže, zbriše ali spremeni. Za zmanjšanje teh tveganj je priporočljiva uporaba šifriranja podatkov med prenosom. Če želimo zagotoviti zasebnost nekega dokumenta, ga moramo šifrirati tako, da ga zna dešifrirati tisti, ki mu je dokument namenjen, vsem ostalim pa je vsebina dokumenta nedostopna. S šifriranjem sporočilo oz. čistopis pretvorimo v obliko, ki onemogoča njegovo razumevanje, v tajnopis. V taki obliki potuje sporočilo prek interneta do

njegovega končnega prejemnika, ki to sporočilo dešifrira in ga pretvori v njegovo prvotno obliko, v čistopis. Stopnja zasebnosti, ki jo dosežemo s šifriranjem je odvisna predvsem od učinkovitosti šifrirnega postopka in tajnosti dešifrirnega postopka. Za šifriranje so pomembni tako postopek zakrivanja in razkrivanja podatkov, imenovan tudi kriptografski algoritem kot šifrirni ključi, ki določajo delovanje algoritma. Današnji algoritmi so večinoma znani do podrobnosti, skriti morajo ostati le šifrirni ključi. V uporabi sta dve obliki šifriranja, simetrično in asimetrično šifriranje.

Simetrično šifriranje

Značilnost simetričnih šifrirnih algoritmov je uporaba istega ključa, tako za šifriranje kot tudi za dešifriranje sporočila. Problem uporabe simetrične kriptografije v javnih omrežjih je, kako skupni šifrirni ključ varno razdeliti pooblaščenim subjektom. Vsak naslovnik šifriranega sporočila mora namreč imeti pri sebi ključ, s katerim je bilo sporočilo zaščiteno, da bi lahko sporočilo dešifriral in razbral vsebino. Subjekti si morajo ključ izmenjati osebno, če želijo ohraniti skrivnost zase. Dandanes pa je to nesprejemljivo, saj komunicirajo z ljudmi po vsem svetu (Jerman Blažič, 2001, str. 103). Uporabnost simetričnega šifriranja je omejena, saj s takim šifriranjem lahko dosežemo le zaupnost sporočila, ne moremo pa z uporabo teh tehnologij dokazati tudi izvora šifriranega sporočila, saj morata isti ključ za šifriranje poznati tako pošiljatelj kot naslovnik.

Poznamo več simetričnih algoritmov, za katere je značilno, da nimajo varnostnih lukenj, kar pomeni, da jih napadalec lahko dešifrira le s poskušanjem vseh možnih ključev. Najbolj znan je algoritem DES, ki ga pa ni več priporočljivo uporabljati, saj ima ključe dolge le 56 bitov. Z zmogljivim računalnikom lahko preizkusimo vse možnosti dešifriranja v enem dnevu. Na primer algoritem IDEA uporablja 128 bitov dolge ključe, kateri nam danes zagotavljajo varnost. Z razvojem vse zmogljivejših in hitrejših računalnikov se morajo večati tudi ključi za zagotavljanje primerne varnosti (Jerman-Blažič, 2001, str. 105).

Asimetrično šifriranje

Značilnost asimetričnih kriptosistemov oziroma kriptosistemov javnih ključev je, da ključa za šifriranje in dešifriranje nista enaka. Ključi nastopajo v parih, najpomembnejša lastnost takih kriptosistemov pa je, da iz enega ključa, brez poznavanja dodatnih informacij, ni mogoče določiti preostalega. En ključ, imenovani javni ključ, lahko zato javno objavimo. Drugi ključ iz para, ki ga mora lastnik varno shraniti, pa je zasebni ključ. Kdorkoli nam želi poslati zaupno sporočilo, ga šifrira z našim javnim ključem. Samo mi, ki edini poznamo ustrezni zasebni ključ, pa lahko šifrirano sporočilo dešifriramo (Jerman-Blažič, 2001, str. 103).

Danes se najbolj uporablja algoritem RSA, ki ima ime po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adeleman). Metoda je bila v ZDA patentirana, patent pa je potekel septembra 2000. Do tega časa je bilo treba za uporabo v ZDA plačevati licenčnino, zato

algoritem ni bil vključen v nekatere produkte (Algoritmi z javnim ključem, 2003). RSA postopek šifriranja je priznan kot izjemno varen postopek in zadovoljuje tudi najstrožje vojaške zahteve. Temelji na matematičnem problemu – faktoriranju velikih števil. Za razbitje teh algoritmov obstajajo poleg poizkušanja vseh možnih ključev tudi druge metode, vendar je še vedno najpomembnejša dolžina ključev. Zaradi tega enako dolgi ključi pri simetričnih in asimetričnih algoritmih ne ponujajo enake varnosti. 1028 bitov dolgi ključ pri RSA algoritmu zagotavlja podobno stopnjo varnosti kot 72 bitov dolgi ključ pri simetričnih algoritmih. Zaenkrat je smiselno uporabljati 1024 bitov dolg ključ, za pomembne operacije pa 2048 bitov.

Slabost asimetričnih kriptosistemov v primerjavi s simetričnimi je predvsem hitrost šifriranja in dešifriranja. Asimetrični kriptoalgoritmi so veliko počasnejši od simetričnih, zato jih le redko uporabljamo za šifriranje daljših sporočil. Običajno šifriramo podatke s simetričnimi kriptoalgoritmi, ključe za te algoritme pa z asimetričnimi. Kriptosisteme javnih ključev torej uporabljamo pri šifriranju večinoma le za razdeljevanje ključev (Jerman Blažič, 2001, str. 104).

Znani so tudi asimetrični algoritmi, ki temeljijo na eliptičnih krivuljah (ECC - Eliptic Curve Cryptosystems). Ideja je znana že od leta 1985. V primerjavi z RSA zadoščajo krajši ključi, zato kaže, da bodo v bodočnosti ti algoritmi prevladali vsaj pri uporabi v manj zmogljivih napravah. Tabela 1 prikazje primerjavo dolžin ključev ECC in RSA pri enaki stopnji varnosti (Algoritmi z javnim ključem, 2003).

Tabela 1: Primerjava dolžine ključev ECC in RSA

Dolžina ključa ECC	Dolžina ključa RSA
106 bitov	512 bitov
132 bitov	768 bitov
160 bitov	1024 bitov
191 bitov	1536 bitov
211 bitov	2048 bitov

Vir: Algoritmi z javnim ključem, 2003.

Digitalni podpis

Digitalni podpis je v sodobnem elektronskem poslovanju, ko prihaja do izmenjav najrazličnejših dokumentov, zamenjal lastnoročni podpis. Proces digitalnega podpisovanja se prične z izdelavo digitalnega odtisa (ang. Hash Code) prvotnega sporočila. Postopek izdelave odtisa zagotavlja, da ob spremembi besedila ta odtis ni več enak in da iz odtisov ne moremo ustvariti besedila. Odtis ima vedno fiksno dolžino in je odvisen od algoritma, ki ga uporabljamo. Odtis se kasneje šifrira z zasebnim ključem podpisnika, kar zagotavlja, da je podpis res njegov in pripne k podpisanemu sporočilu. Prejemnik sporočila lahko z javnim ključem podpisnika dešifrira odtis in s tem preveri pristnost podpisnika. Nato z istim

algoritmom napravi novi seštevek sporočila. V primeru, da se seštevka ujemata, mu to zagotavlja neokrnjenost sporočila (Osojnik, 2002, str. 125).

S podpisom dokumenta smo torej zagotovili, da vsebina sporočila ne bo spremenjena ter smo prejemniku dokumenta zagotovili, da smo ga poslali prav mi. Pomembno pa je, da naš podpis ne bo možno prenesti na neki drugi dokument.

Za še večjo varnost pa je priporočljivo, da zasebni ključ hranimo na pametni kartici. Pomembna lastnost pametnih kartic je v tem, da zasebni ključ ne zapusti pametne kartice, zato tudi ni nevarnosti, da bi bil razkrit. Šifriranje in digitalno podpisovanje tako namreč potekata na sami kartici. Dostop do kartice je zaščiten z geslom, sodobnejše kartice pa imajo vgrajene tudi čitalnike prstnih odtisov, s čimer kartico res lahko uporablja samo njen pravi lastnik (Jerman-Blažič, 2001, str. 109).

Digitalni certifikat

Bistvena težava, ki se pri asimetričnem šifriranju pojavi, je overjanje javnih ključev, zaradi česar se uporabljajo certifikati. Certifikat je elektronsko zapisano potrdilo, ki enoznačno veže uporabnika na njegov javni ključ, ki ga lahko izda agencija za izdajanje certifikatov oz. elektronski notar (ang. Certifiying Authority). Certifikat omogoča preverjanje ali določen javni ključ res pripada določenemu posamezniku ali organizaciji. Največkrat certifikat vsebuje javni ključ in ime uporabnika, rok veljavnosti ključa in ime agencije za izdajanje certifikatov. Digitalni podpis lahko potemtakem smatramo za zanesljiv, če je bil izdan digitalni certifikat, ki dokazuje pristnost pošiljatelja, jamči za celovitost sporočila in njegovo nezavrnitev (Šinigoj, Turk, 1999, str. 462).

Infrastruktura javnih ključev - PKI[9]

Izraz infrastruktura javnih ključev zajema celoten sistem za uporabo asimetrične kriptografije v elektronskem poslovanju. Ker izmenjava ključev pri velikem številu uporabnikov oz. lastnikov digitalnih potrdil ni enostavna ali celo možna (kjer ni možno, da si vsi uporabniki osebno izmenjajo javne ključe), je potrebna neka javno dostopna baza podatkov oz. imenik, ki hrani potrdila z javnimi ključi. Organizacija, ki omogoča dostop in skrbi za imenik z digitalnimi potrdili je že zgoraj omenjena agencija za izdajanje certifikatov. Le-ta praviloma tudi upravlja s ključi, torej skrbi za izdajanje, preklic, podaljševanje itd. Overitelj tako predstavlja ustanovo, ki ji njegovi komitenti (lastniki digitalnih potrdil) zaupajo. S tem ga tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Podobno je overitelj ustanova, ki ji lahko zaupajo tudi ostali overitelji ali posamezniki in posredno s tem zaupajo tudi lastnikom vseh digitalnih potrdil, ki jih je overitelj izdal in potrdil. Tako se lahko različni overitelji povezujejo na različne načine, bodisi horizontalno, kjer se medsebojno overijo in s tem

[9] Public Keys Infrastructure.

omogočijo varno in zanesljivo komunikacijo med lastniki digitalnih potrdil obeh ustanov, ali vertikalno, ko nek overitelj pooblasti neko drugo ali druge ustanove za izdajanje digitalnih potrdil v svojem imenu, kar je seveda nujno potrebno pri upravljanju z velikim številom digitalnih potrdil (Osojnik, 2002, str. 127). Poleg agencij za overjanje javnih ključev, lastnikov certifikatov in uporabnikov certifikatov imajo pomembno vlogo agencije oziroma uradi za registracijo. Ti uradi ne izdajajo certifikatov, lahko pa registrirajo naročnika, ki zaprosi za certifikat, preverijo njegovo identiteto in poznavanje javnemu ključu pripadajočega zasebnega ključa (Jerman-Blažič, 2001, str. 111).

Pomembnejše storitve infrastrukture so dodeljevanje imen posameznikom in institucijam, registracija in identifikacija naročnikov certifikatov, podpisovanje javnih ključev, podaljševanje veljavnosti javnega ključa, zamenjava para ključev, objava certifikatov, preklic certifikata oziroma javnega ključa in objava seznama preklicanih certifikatov (Jerman-Blažič, 2001, str. 112).

3.4.5. Načini uvajanja internetnega bančništva

V Evropi je večina internetnih bank podružnica klasične banke. V zadnjem času se pogosto pojavlja vprašanje, ali je bolj smiselno ustanoviti popolnoma ločeno internetno banko s svojim imenom, ki nima nikakršne povezave z imenom banke matere, ali pa je e-banka le razširitev storitev banke. Na eni strani gre za tveganje, ki mu je banka izpostavljena v primeru, da njena internetna podružnica propade, na drugi strani pa se banke ubadajo z vprašanjem zaupanja strank e-banki, ki je »še« povsem neznana. Pri finančnih storitvah je namreč zaupanje pomemben dejavnik odločanja (Voljč, Šega, 2001, str. 114).

Banke uvajajo internetno bančništvo na naslednje načine (Oman, 2002, str. 19):

- Čisto internetno bančništvo: banka mati je popolnoma ločena od svoje internetne banke (nekoč Wingspan v ZDA, v Veliki Britaniji Egg, Marbles, Cahoot, Smile, v Franciji e-cortal).
- Hibridi na spletu: banke pogosteje razširijo svojo blagovno znamko na mrežo (bankamerica.com, wellsfargo.com). Ime internetne banke je tako prepoznavno in povezano z imenom off-line banke. Prednost je v tem, da se lojalnost off-line banke prenaša na internetno banko, poleg tega pa je lažje najti bankino spletno stran.
- Spletne povezave: banka lahko poveča bazo svojih strank tudi s povezavo s telekom podjetjem ali ponudnikom internetnih storitev. V letu 2000 je bilo napovedanih kar nekaj takih povezav (SanPaolo IMI in Tiscali – ponudnika internetnih storitev v Italiji, BBVA in Telefonica v Španiji).
- Tiha partnerstva (white labelling, private labelling): banke postajajo tihi partnerji. Lahko, na primer, zagotovijo storitve procesiranja transakcij (back office) drugi ustanovi in ji tako omogočijo, da odpre banko (Bank of Scotland opravlja te transakcije za Sainsbury's Bank in za banko supermarketa Tesco's).

3.4.6. Vpliv informacijske tehnologije in interneta na bančništvo

Bistvo interneta je, da je globalen. Za banke to v prvi vrsti pomeni vstop na tuje trge, ne da bi bilo treba razmišljati o širitvi mreže. Po drugi strani internet prvič v celotni zgodovini bančništva bankam pomeni resno grožnjo za izgubo posla. Banke so namreč finančni posredniki, ki povezujejo varčevalce s porabniki (posojilojemalce). Internet pa omogoča odpravo posredništva, saj strankam zagotavlja zadostne informacije po zelo nizkih stroških, tako da se varčevalci in porabniki lahko sami povežejo, brez posredovanja banke. Največja zavora pri množični uporabi interneta pri finančnih poslih, namreč varnost transakcij, postopno izginja s hitrim razvojem tehnologije. Finančne institucije, ki so bile v preteklosti najbolj tradicionalne ustanove, tako postajajo pomembni pospeševalci razvoja (Voljč, Šega, 2001, str. 114).

Vpliv informacijske tehnologije na bančništvo je tako velik predvsem zato, ker je to informacijsko zelo intenzivna panoga. Banke se že leta ukvarjajo z denarjem, ki je bil za večino strank že doslej navidezen. Imetniki bančnih računov so vajeni mesečnih izpiskov, na katerih je njihov denar predstavljen s serijo številk ali pa s svetlečimi zelenimi številkami na bančnih avtomatih. Denar je torej blago, ki ga lahko brez najmanjše težave porabimo, prenesemo in dostavimo elektronsko (Oman, 2002, str. 17).

Razvoj informacijske tehnologije vpliva na banko in njeno poslovanje. Najprej zmanjšuje stroške zbiranja, shranjevanja, obdelave in prenosa informacij. Nato pa spreminja poti, po katerih so strankam dostopne bančne storitve. Vse večje banke ponujajo elektronsko bančništvo svojim strankam.

Spreminja se tudi okolje v katerem banke delujejo, s tem pa način konkuriranja med njimi, in sicer na dva načina. Prvič, na povpraševalni strani – stranke imajo možnost enostavnejšega pridobivanja informacij o storitvah različnih bank in s tem možnost primerjave le teh. In drugič, na ponudbeni strani, kjer so ovire za vstop na trg na drobno nižje, saj za doseganje kritične mase strank ne potrebujejo več velike poslovne mreže. Zaradi nižjih ovir za vstop na bančni trg se ne povečuje le konkurenca med bankami, temveč je omogočen vstop tudi nebančnim finančnim posrednikom in konkurentom, za katere banke v preteklosti sploh niso vedele, da obstajajo. To so lahko trgovska podjetja, letalske družbe, proizvajalci avtomobilov in telekomi. Med tradicionalnimi bankami je to sprožilo preplah. Ne le, da lahko nove banke v celoti izkoristijo novo tehnologijo, saj začenjajo povsem od začetka, medtem ko stare banke nosijo s seboj breme preteklosti, temveč prinašajo v bančni svet tudi nove ideje o proizvodih, storitvah, trženju in cenovni politiki. Pogosto ponujajo ugodnejše obrestne mere kot tradicionalne banke. Banke so šele z njihovo navzočnostjo doumele, da njihove stranke prav hitro lahko postanejo stranke koga drugega, sploh nekoga, s katerim so že navezale odnos zaupanja, ki lahko celo dosega višjo raven kot tisti z banko. Uveljavljena podjetja, ki niso finančne institucije, imajo lahko prednost pred bankami, saj že imajo široko bazo strank, ki jim lahko lažje in ceneje ponudijo tudi svoje finančne storitve. Gre predvsem za stranke, ki

uporabljajo podjetniške kartice, s katerimi si podjetja zagotavljajo njihovo zvestobo, zaupanje in posledično izboljšajo svoj poslovni rezultat. Potencialni konkurenti so lahko tudi podjetja, kot npr. Yahoo! ali AOL, ki imajo na svojih straneh milijone obiskovalcev in slovijo kot zanesljiva. Za posameznika bi bilo vsekakor idealno, da bi lahko vse svoje finančne posle opravil na enem mestu oz. na eni strani, kjer bi imel na voljo vse od bančnih računov, zavarovalnih polic do delnic. Uporabnik bi imel tako eno samo geslo, s katerim bi lahko imel dostop do vseh online finančnih poslov (Voljč, Šega, 2001, str. 114-115).

Oviro postavlja regulativa, saj ta v številnih državah EU preprečuje lastništvo industrijskih podjetij v bankah. Banka mora biti vsaj delni lastnik internetne banke, ki jo je ustanovilo podjetje, če ta želi pridobiti licenco za opravljanje bančnih poslov. Gledano s tega stališča je morda vprašljiv ves preplah glede izgube posla, saj si banke le pridobivajo nove trge in nove kupce ob pomoči novih partnerjev in novih poti.

Nova ekonomija zato zahteva od bank korenito spremembo kulture – zasuk od birokratskih metod do usmerjenosti k stranki. Številni novi konkurenti (e-banke, trgovska podjetja, telekomi), ki opravljajo finančne posle, so prisilili banke, da so svoje storitve prilagodile stranki. Vedno bolj se uveljavlja misel, da bodo preživeli le tisti finančni posredniki, ki bodo postavili stranko na prvo mesto, kar pomeni, da bodo morale banke korenito spremeniti filozofijo, strategijo in taktike. Stranki bodo morale zagotoviti dostop do najboljših storitev in proizvodov. Časi, ko je bila stranka doživljenjsko zvesta eni banki, so s hitrim tehnološkim razvojem minili (Voljč Šega, 2001, str. 111).

3.4.7. Ali predstavljajo virtualne banke grožnjo tradicionalnim bankam?

Prva banka, ki je 18. oktobra 1995, začela poslovati prek interneta in je bila obenem »virtualna« banka, je Security First Network Bank (SFNB) Iz Atlante, ZDA. Cilj bank začetnic je bil znižanje stroškov, torej transakcijskih stroškov – stroškov zbiranja, shranjevanja, obdelave in prenosa informacij. Prvi izračuni so namreč kazali, da stane bančna transakcija prek interneta banko le en cent, kar je desetina stroškov bančne transakcije prek bančnega okenca (Oman, 2002, str. 17-18). V ceno namreč ni treba upoštevati stroškov uslužbenca za bančnim okencem, stroškov prostora in opreme, poštne storitve, papirja in podobnega. Bančni uslužbenci so razbremenjeni, zato lahko več časa namenijo strankam in jim pobližje predstavljajo in prodajajo nove bančne storitve

Po ocenah Lehman Brothers pa prihranki banke niso tako veliki, saj so stroški servisiranja on-line računa le za 14 % nižji od servisiranja off-line računa, zlasti ker večina bank sočasno z uvedbo on-line bančništva ne zmanjšuje števila zaposlenih in ne ukinja klicnih centrov ter poslovalnic, kar preprosto pomeni, da internet povečuje celotne stroške banke. Še bolj kot doslej morajo banke vlagati v razvoj novih tehnologij, tako da se večina prihrankov pri delovnih močeh, ki nastajajo pri krčenju bančnih podružnic, hitro izniči z zaposlovanjem novih, pogosto še bolj izobraženih in dražjih kadrov (Oman, 2002, str. 18).

Banke so sprva začele uvajati on-line bančništvo zato, da bi zmanjšale stroške poslovanja in povečale neobrestne prihodke. Obrestni prihodki se namreč, zaradi konkurence nenehno zmanjšujejo. Sedaj pa se banke odločajo za vzpostavitev internetnega bančništva zaradi konkurenčnosti in večanja navezanosti njihovih strank ter zato, da bi si lažje pridobili nove. Dejstvo je, da banke, ki ne omogočajo poslovanja tudi preko interneta, tvegajo odhod strank h drugim bankam, ki takšno poslovanje omogočajo.

Virtualne banke, ki so se leta 1995 pojavile na bančnem trgu, so začele poslovati izključno prek interneta in niso imele nikakršnega zaledja v podjetjih, bile pa so pogosto banke hčere manjših tradicionalnih bank ali pa popolne internetne začetnice, nastale ob pomoči tveganega kapitala. V ZDA je bilo v letu 2000 mogoče našteti vsaj 50 takšnih bank. Prva naj bi bila že omenjena Security First Network Bank, ki zdaj ne posluje več, vse pa so nastale na podlagi ocene stroškov, ki so za »virtualno« banko zelo nizki. Še v začetku leta 2000 so jim napovedovali velik vzpon; bile so največja grožnja tradicionalnim bankam, nekateri so napovedovali celo propad le-teh. Njihova strategija je bila ob nizkih transakcijskih in zanemarljivih operativnih stroških prenašati prihranke na komitente in ponuditi višje obrestne mere na bančnem trgu ter tako uspeti. Vendar že konec leta 2000 se je izkazalo, da veliki stroški s pridobivanjem komitentov, uveljavljanjem blagovne znamke in plačevanjem visokih provizij za uporabo bančnih avtomatov drugih finančnih posrednikov spodjedajo njihovo strategijo, ki je temeljila prav na nizkih stroških (Oman, 2002, str. 19).

Virtualne banke niso več grožnja tradicionalnim bankam, ki imajo trenutno kvečjemu koristi od te konkurence, saj razočarane stranke pri njih odpirajo on-line račune. Izkazalo se je, da so bile tradicionalne banke v veliki prednosti že od samega začetka, predvsem zaradi znanja in izkušenj pri upravljanju tveganj in široke informacijske baze strank. Pa tudi, v tradicionalnih bankah so bili stroški uvajanja novih tehnoloških rešitev previsoki. Nekatere so morda investirale preveč in prehitro. Zdaj se ubadajo s problemom hitro rastoče ponudbe storitev internetnega bančništva, za katero zelo zaostaja povpraševanje po teh storitvah, kar pa tradicionalnim bankam prinaša le nizko realizacijo.

Virtualne banke pa so imele v primerjavi s tradicionalnimi bankami še eno oviro, t.i. psihološko zavoro potencialnih komitentov. Izkazalo se je, da so ljudje težko zaupali denar nekomu, ki se ga pravzaprav ne vidi ali nekomu, ki danes je, jutri pa ga morda ne bo. Dvajsetnadstropna zgradba banke je veliko bolj prepričljiva kot elektronski naslov. Zato je v obdobju elektronizacije storitev blagovna znamka še pomembnejša (Sjekloča, 1999, str. 33).

3.4.8. Pozitivni učinki internetnega bančništva

Banke se odločajo za uvajanje elektronskega bančništva zaradi večjega števila različnih pozitivnih učinkov. Nekateri med njimi so (Sjekloča, 1999, str. 32-33):

- Zmanjšanje stroškov bančnega poslovanja: manj papirja, izginja potreba po klasičnem bančnem okencu, banke ne plačujejo stroškov komunikacije.
- Stranki prihrani čas: krajša vrste v bankah in omogoča hitro in natančno informacijo o stanju računa ali bančnih storitvah. Pred bančnim okencem stojimo večino časa zato, da bi dvignili izvode, gotovino, plačali račune, preverili prispele čeke, kar bančništvo na internetu kaj hitro rešuje. Banke, s ponudbo storitev prek interneta, posredno vplivajo na odločitve strank, da se priključijo na internet.
- Ker je komunikacija multimedijska, je zanesljivost informacije zlahka preverljiva.
- Pospešuje kroženje denarja in omogoča bolj redno plačevanje obveznosti.
- Vpliva na spremembo poslovanja banke, profil bančnih uslužbencev, ki niso več administrativni delavci, da bi vpisovali v knjige ali šteli denar, ampak se posvečajo bolj dinamičnim poslom.
- Odpira nove trge. Ker je domači računalnik postal bančna podružnica, ni nujno, da je stranka v istem mestu kot banka. Tako izginjajo fizične meje trga.
- Vnaša nove elemente v makroekonomsko politiko. Uveljavljanje elektronskega denarja bo zahtevalo drugačno monetarno politiko, spremembe v statistiki in večjo disciplino bank.

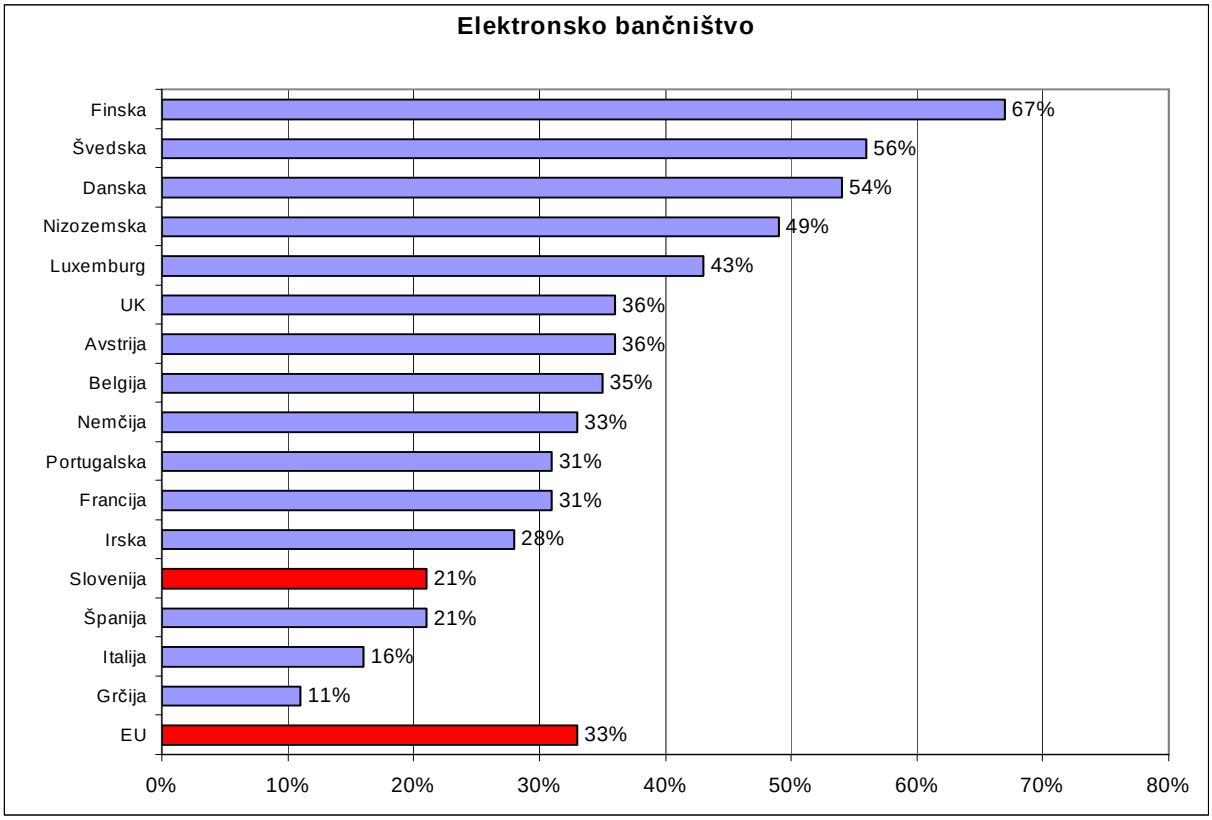
3.4.9. Internetno bančništvo v Evropi in v Sloveniji

Pravi uspeh je online bančništvo doživelo v skandinavskih državah. Finska, Švedska, Norveška pa tudi Danska imajo največje število uporabnikov interneta in mobilnih telefonov na svetu, poleg tega pa so ti tudi najbolj aktivni uporabniki obeh. Na Švedskem storitve on-line bančništva uporablja menda kar 31 odstotkov prebivalcev. Po številu uporabnikov storitev on-line bančništva vodi Nordea, največja regionalna banka v Evropi. Gre za eno redkih uspešnih čezmejnih konsolidacij na evropski celini, ki je nastala z združitvijo finske banke Merita, švedske Nordbanken, danske Unidanmark in norveške banke Christiania. Sama trdi, da ima 2,2 milijona uporabnikov on-line bančništva. Nordea ima svoje korenine na Finskem, v telefonski banki, ki je začela ponujati svoje storitve že v letu 1982, v letu 1994 je uvedla PC-bančništvo, internetno bančništvo v letu 1996 in bila v oktobru 1999 prva na svetu pri uvedbi Wireless Application Protokol - WAP bančništva (Oman, 2002, str. 20).

V nadaljevanju je prikazana primerjava med Slovenijo in EU pri uporabi interneta za elektronsko bančništvo, vendar vedno za osebne potrebe. Vprašanje v obeh raziskavah, ki služita za primerjavo med Slovenijo in EU se je glasilo enako*: Ali za vaše osebne potrebe uporabljate internet tudi za elektronsko bančništvo?*

Slika 7 prikazuje relativne deleže uporabnikov interneta za elektronsko bančništvo in ne deleže uporabnikov v celotni populaciji. V Sloveniji tako internet uporablja za elektronsko bančništvo 21%, v EU pa 33% vseh uporabnikov interneta v starostni skupini 15 let in več.

Slika 7: Uporaba interneta za elektronsko bančništvo, primerjava Slovenija – EU, december 2002



Vir: Primerjava Slovenija – EU, 2003, str. 28.

Po raziskavi Forrester Research iz leta 2003 naj bi bilo v Evropi 60 milijonov uporabnikov internetnega bančništva, kar pomeni, da že vsak peti Evropejec uporablja storitve internetnega bančništva. Za leto 2007 pa napovedujejo porast števila uporabnikov na 130 milijonov (Forrester research, 2003).

V Sloveniji so, v drugi polovici devetdesetih let prejšnjega stoletja, banke začele ponujati svoje storitve tudi preko interneta. Na začetku so se komitenti bolj previdno odločali za uporabo tega medija, največkrat zaradi nezaupanja v varnost tovrstnih novih storitev. S časoma so se navadili na elektronsko poslovanje in je število uporabnikov internetnega bančništva naraslo. Sedaj banke v Sloveniji intenzivno spodbujajo svoje komitente k uporabi internetnega bančništva s tem, da povečujejo razliko v stroških med internetnim in klasičnim načinom poslovanja. V primerjavi z drugimi evropskimi državami glede uporabe interneta za bančno poslovanje pa smo še vedno pri repu lestvice.

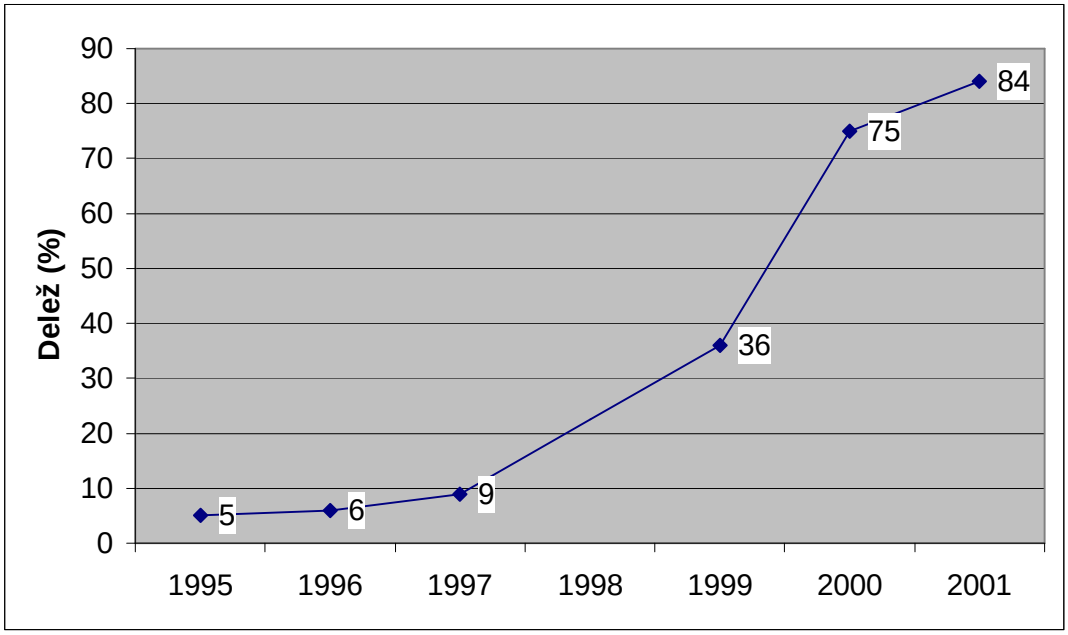
3.5. MOBILNO BANČNIŠTVO

Banke ne bi smele le opazovati hitrega razvoja mobilne tehnologije, ker ni nobena skrivnost, da bodo v naslednjem petletnem obdobju operaterji mobilne telefonije na področju plačilnega prometa in potrošniških posojil majhnih vrednosti postali njihov zelo resen konkurent. Projekt

mobilna banka je danes na mizah večine direktorjev mobilnih operaterjev, pogoji zanjo pa postajajo iz dneva v dan bolj realni. Čeprav se banke v Sloveniji po nekaterih informacijah zanašajo na regulativo, ki opravljanje posojilno-denarnih transakcij omejuje zgolj na bančno sfero, pa trdnih elementov za obrambo svojih stališč nimajo. Na drugi strani pa ni nerealno pričakovati, da bodo imeli mobilni operaterji kmalu v svojih rokah tehnološke in kadrovske elemente, ki bodo povsem upravičevali projekt mobilne banke. Če si pogledamo samo nekatere, vidimo, da ima, na primer, največji slovenski mobilni operater danes večjo bazo individualnih strank kot katerakoli slovenska banka, da ima ob tem na voljo tehnologijo, ki mu bo omogočala spremljati večino elementov na dejavnost vezanega kreditnega tveganja, da si lahko v določenem obdobju med uporabniki še poveča že zdaj visoko stopnjo kredibilnosti in zaupanja in da razpolaga s potencialno kapitalsko ustreznostjo, ki projektu mobilna banka povsem zadostuje. Če tem elementom dodamo še tehnološko izpopolnjen sistem zaračunavanja, v prihodnosti nedvomno zelo izpopolnjene varnostne elemente prenosa podatkov prek mobilnih omrežij in že danes dostopne mehanizme procesiranja plačilnih instrumentov, potem je jasno, da banke razvoja tovrstne tehnologije ne bi smele gledati z »očmi daljne prihodnosti« (Karpe, 2001, str. 43-44).

Mobilno bančništvo omogoča svojim uporabnikom, da se kadarkoli in od koderkoli, kjer sega GSM[10] signal mobilne telefonije, povežejo z banko preko svojih mobilnih telefonov. Tako lahko opravljajo vrsto storitev, kot so pregledovanje stanja in prometa na bančnih računih, plačevanje računov, prikaz tečajnih list, informativnih izračunov.

Slika 8: Naraščanje deleža gospodinjstev z mobilnim telefonom v Sloveniji



Vir: Mobilna telefonija, 2001, str. 6.

[10] Global System for Mobile Communications.

Za uvajanje mobilnega bančništva je pomembna čim večja razširjenost uporabe mobilnih telefonov med prebivalstvom, saj le tako imajo zagotovljeno dovolj veliko število potencialnih uporabnikov mobilnega bančništva. Slika 8 nam kaže, kako je naraščalo število gospodinjstev z mobilnim telefonom, od leta 1995 do leta 2001.

Mobilna telefonija tako spreminja bančno poslovanje, da bodo mogoče zapletene bančne strani odveč in bo zadostovalo enostavno in učinkovito mobilno bančništvo. Ameriška Bank of Montreal je pred letom uvedla mobilno bančništvo, ki je postalo dobesedno uspešnica. 41% njihovih strank je to storitev uporabljalo iz avtomobila, 21% z delovnega mesta, 18% v času prevoza, 10% od doma in prav toliko iz restavracij in gledališča (Bartolini, 2000, str. 69).

Banke ponujajo dva načina mobilnega bančništva in sicer SMS bančništvo in WAP bančništvo.

3.5.1. SMS bančništvo

SMS[11] je storitev, ki uporabnikom mobilnih telefonov omogoča pošiljanje in sprejemanje kratkih alfanumeričnih sporočil. V omrežjih GSM navadno znaša 160 znakov. Storitev deluje na principu shrani in posreduj (ang. Store and Forward) in spominja na elektronsko pošto. Sporočilo se od izvora do ponora prenese preko omrežja s pomočjo SMSC[12] strežnika, ki poskrbi za shranjevanje in posredovanje sporočila, tudi v primeru, ko je prejemnik trenutno nedosegljiv (Rupnik, 2000, str. 242).

Banke uporabljajo SMS predvsem za bolj preproste informativne bančne storitve, kot so vpogled v stanje in zadnje spremembe na računu. Uporabnik lahko naroči pri banki prejemanje periodičnih obvestil o stanju na računu in podobnih storitev. Ima pa možnost tudi kadarkoli naročiti želeno obvestilo, tako da pošlje SMS z dogovorjeno ključno besedo.

3.5.2. WAP bančništvo

Prenašanje podatkov prek omrežja GSM je še vedno zelo počasno in pogosto neuporabno za resno delo in potrebe po brezžični povezavi v splet iz dneva v dan naraščajo. Tega se zavedajo tudi vodilni razvijalci mobilne opreme. Tako je večina omrežij GSM oplemenitenih s protokolom brezžičnih aplikacij (Wireless Application Protocol, WAP). Mobilna telefonija tretje generacije - UMTS[13] omogoča veliko hitrejši in bolj kakovosten prenos podatkov, s tem pa razvoj in uporabo že znanih in novih storitev. S tem sistemom lahko sedaj hkrati prenašamo besedilo, slike in zvok, lahko videotelefoniramo, v prihodnosti pa bo zagotovo možno opravljati še vrsto novih storitev. Žal, WAP pa ne odpira vrata v splet na široko,

[11] Short Message Service.

[12] Short Message Service Center.

[13] Universal Mobile Telecommunications System.

temveč nam omogoča le pogled skozi ključavnico. Strani, prilagojene za prikazovanje na mobilnih telefonih, so namreč precej okleščene, kar je pričakovano, saj že sami aparati ne premorejo primerno velikega zaslona.

Leta 1997 je Omnitel, ameriški operater mobilne telefonije, objavil razpis, ki je bil povod za nastanek WAP foruma. Izkaže se, da je bil to povod za nastanek WAP-a. Še istega leta so Motorola, Nokia, Ericsson in ameriško softversko podjetje Unwired planet (danes Phone.com) postavili temelje protokola WAP. Šlo je za definicijo standarda, ki bi omogočal uporabnikom mobilnih terminalov dostop do vsebine na internetu, saj le ta predstavlja, tako rekoč že pripravljen, globalni vir informacij (Rupnik, 2000, str. 242).

Zamisel WAP-a je temeljila na veliki razširljivosti, saj predvideva (Rupnik, 2000, str. 242):

- Možnost uporabe od enostavnih terminalov z enovrstičnim zaslonom do pametnih telefonov (SmartPhone).
- Za nosilca katerokoli storitev: od SMS, Prenosa podatkov, USSD[14] do GPRS[15].
- Podpira katerikoli omrežni standard, kot npr. CDMA[16], GSM ali UMTS.

Poslovne možnosti, ki jih je omogočil internet, so neizmerne. WAP, kot poseben primer uporabe interneta oz. širitve interneta, je nova arena možnosti, je novo tržišče z novimi pravili. Mobilni telefoni in ostale mobilne naprave so postali medij, katerega si zaradi njegove množičnosti in razširjenosti nihče ne bo mogel privoščiti, da bi jih ignoriral.

Pri elektronskem bančništvu WAP pomeni, da banke svojim komitentom lahko ponudijo poleg osnovnih storitev mobilnega bančništva, ki so informacijskega značaja, tudi vse ostale storitve, ki jih ponuja internetno bančništvo. Nekatere od teh so plačilo položnic, prenos sredstev med računi, varčevanje, naročanje čekov in plačilnih kartic.

Pomen WAP-a je ravno v mediju, na katerem deluje. Mobilni telefoni in ostale mobilne naprave imajo namreč dolgoročno gledano širši krog uporabnikov, kot je uporabnikov interneta. Ker je WAP poseben primer širitve interneta, bo WAP po drugi strani približal internet še dodatnim uporabnikom, ki sicer samega interneta mogoče ne bi uporabljali.

3.5.3. Varnost mobilnega bančništva

Za uporabnike in ponudnike mobilnega poslovanja sta bistvena identifikacija uporabnika in varen prenos podatkov. Uporabniki se namreč raje izogibajo poslovanju, če to ne zagotavlja primerne stopnje varnosti. Štirje elementi elektronskega poslovanja so:

[14] Unstructured Supplementary Services Data.

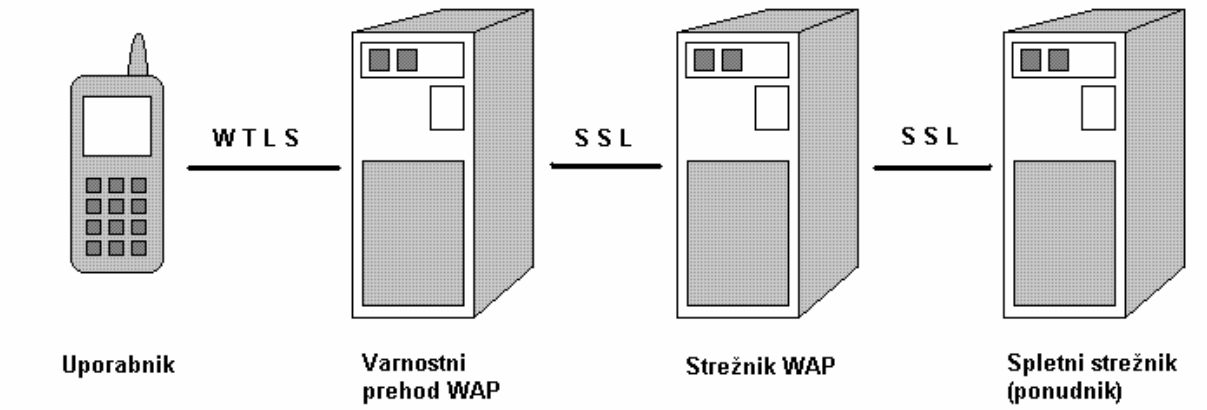
[15] General Packet Radio Service.

[16] Code Division Multiple Access.

- identifikacija in overovitev uporabnika,
- zaupnost izmenjanih podatkov,
- integriteta informacije in
- pravnomočnost opravljenih storitev.

Pri razvoju WAP-a so vrinili med sloje brezžičnega protokola tudi ustrezen varnostni mehanizem. Sloj WTLS[17] je nekakšna okleščena različica pravega transportnega varnostnega sloja (ang. Transport Layer Security-TLS). Ta je med transportnim slojem in aplikacijo, njegova skrb pa je varno prenašanje podatkov. Zasnovan je predvsem za uporabo v omrežjih z majhnimi prenosnimi zmogljivostmi in netekočim pretokom podatkov. Podobno kot TLS podpira identifikacijo in overovljanje uporabnika ter vzpostavljanje varnega prenosnega kanala (Jerman Blažič, 2000, str. 70).

Slika 9: WTLS – brezžični transportni varnostni sloj



Vir: Jerman Blažič, 2000, str. 70.

Vendar za varno mobilno bančništvo sam WTLS ne zagotavlja dovolj varnosti. Zato je WAP Forum v različici WAP 1.2 izboljšal varnostne mehanizme. Najpomembnejša posodobitev je WAP Identity Modul (WIM), ki ima dve pomembni vlogi, izvršitev avtentikacije WAP stranke in vodenje postopka na strankini strani v WTLS sloju ter izvajanje digitalnega podpisa za WAP stranko v aplikacijskem varnostnem sloju (WML Script Cripto Library). V obeh primerih WIM hrani kriptografske zasebne ključe, izvrši povezane algoritme javnih ključev (RSA, EC-DA ali EC-DSA) in varuje uporabo teh algoritmov z lokalnim PIN-om. Edinstvena

[17] Wireless Transport Layer Security.

stopnja varnosti je odvisna od dveh pomembnih dejavnikov: kriptografski zasebni ključi ne smejo nikoli zapustiti WIM-a in ne smejo biti dosegljivi zunanjim napravam. Tu igra ključno vlogo pametna kartica, kajti njena tehnologija je odporna na zunanje vdore in samo ona lahko zagotavlja to stopnjo varnosti (Imbert, 2001).

3.5.3.1. Mobilni certifikati

Problem varne brezžične komunikacije se skriva v šifrirnih algoritmih in formatu certifikatov, s katerimi se mobilni telefoni ne morejo spoprijeti. Nekateri proizvajalci ponujajo svoje rešitve, prilagojene omenjenim pomanjkljivostim. Podjetje Certicom je razvilo tehnologijo eliptične krivuljne kriptografije (Eliptic Curve Criptography, ECC), namenjene žepnim računalnikom in mobilnim telefonom. Tehnologija ECC sloni na manj zahtevnih in hitrejših, a še vedno zanesljivih algoritmih. Potrebam v mobilnem omrežju so zaenkrat namenjene preprostejše izpeljanke certifikatov, t.i. certifikati WTLS, na katerih se nahajajo ime uporabnika, serijska številka certifikata, čas veljavnosti, uporabnikov javni ključ in še nekaj drugih atributov. Ti certifikati so pravzaprav popolnoma enaki prvi različici certifikatov X.509, definiranih leta 1988. Kasnejšim različicam so bila dodana še nekatera polja, med njimi tudi kazalec seznam neveljavnih certifikatov (ang. Revocation List-RL). Ta atribut je izjemno pomemben, saj govori o veljavnosti certifikata (Jerman Blažič, 2000, str. 70).

Ker je certifikat zelo obsežen in zahteva več procesorske moči za obdelavo, kot pa jo mobilni telefon sploh zmore, so certifikati shranjeni le v telefonih. Certifikat se ob identifikaciji uporabnika in vzpostavljanju varnega kanala prenese v strežnik, ki ga lahko preveri in obdela brez težav. Strežnik tako obsežnega certifikata ne more poslati nazaj, saj bi ga telefon le s težavo sprejel. Zato naj bi strežniki uporabljali preprostejše certifikate. Takšni certifikati ne ustrezajo varnostnim merilom, in zato naj bi bila njihova življenjska doba omejena le na nekaj dni. Ob vsakem ponovnem vzpostavljanju povezave mora zato agencija za izdajanje certifikatov mobilnim uporabnikom (Wireless Certification Authority- WCA) izdati nov certifikat (Jerman Blažič, 2000, str. 70).

Preprostejša rešitev je, če uporabnik certifikata sploh ne hrani, temveč posreduje strežniku le naslov URL, kjer se nahaja certifikat. Na tem naslovu pa je že mogoče shraniti tudi najnovejšo različico certifikata x.509v3. Uporabnikov certifikat je možno shraniti v telefon ali kar na kartico SIM. Slednja rešitev bi lahko povzročala preglavice, saj je potrebno zamenjati že obstoječo kartico z novo, ki ima prostor tudi za certifikat. V tretji različici protokola WAP (1.2) je shranjevanju certifikatov in preverjanju identitete uporabnika že namenjen dodatni identifikacijski modul WIM (Jerman Blažič, 2000, str. 70).

3.5.3.2. Identifikacija in varna povezava

Identifikacija uporabnika in vzpostavljanje varne povezave poteka v več korakih. Ko se uporabnik poveže s strežnikom (WAP Security Gateway), mu ta kot odgovor pošlje svoj

certifikat z javnim ključem. Da bi se uporabnik prepričal o veljavnosti certifikata in s tem tudi javnega ključa, kontaktira strežnik s seznamom preklicanih certifikatov. Ko se uporabnik prepriča o verodostojnosti strežnika, temu pošlje simetrični ključ, potreben za vzpostavitev varne povezave. Ta ključ je razmeroma kratek in zašifriran s strežnikovim javnim ključem, tako da ne more prispeti v napačne roke ter podpisan z uporabnikovim javnim ključem (podpis rabi identifikaciji uporabnika). Zašifrirani ključ strežnik dešifrira s svojim zasebnim ključem, preveri uporabnikov podpis in uporabi simetrični ključ za vzpostavitev varnega kanala. Simetrični ključi so unikatni, kar pomeni, da so generirani za vsako povezavo posebej (Jerman Blažič, 2000, str. 72).

3.5.4. Mobilno bančništvo v Sloveniji

V Sloveniji se je razvoj mobilne telefonije začel leta 1991 s postavitvijo omrežja NMT (Nordic Mobile Telephony). Ta sistem je bil prva generacija mobilne telefonije, ki je še temeljil na analogni tehnologiji. Druga generacija mobilne telefonije se je pojavila leta 1996 z digitalnim omrežjem GSM. Sistem UMTS pa se je pri nas pojavil leta 2003, tako kot drugod po Evropi.

Opravljanje bančnih storitev preko mobilnega telefona ponuja v Sloveniji že nekaj bank. Naša največja banka NLB ponuja mobilno bančništvo preko sistema Moba. Leta 2002 je v sodelovanju z družbo Mobitel uvedla mobilno banko Moba NLB. Tako je omogočila svojim komitentom dostop do bančnih storitev preko mobilnega telefona. Že po dveh mesecih je Mobo uporabilo že več kot 2400 ljudi, s čimer so presegli začetna pričakovanja (Mobitelova Moba nad pričakovanji, 2004).

Komitenti lahko na ta način opravljajo naslednje storitve:

- vpogled v stanje osebnega računa ali računa, na katerem je oseba pooblaščena,
- vpogled v promet na računu (zadnje štiri transakcije),
- vpogled v promet na računu, izveden prek mobilnega telefona (zadnje štiri transakcije),
- plačilo obveznosti prek posebne položnice, plačilnega naloga,
- prenos sredstev med računi znotraj bančne skupine NLB,
- nastavitev alarmov o prekoračitvi osebnega limita,
- naročilo povišanja limita na računu,
- vezavo sredstev,
- prijavo novega delovnega računa oziroma odjavo delovnega računa, spremembo nastavitev (spremembo bančnega PIN-a ali spremembo naziva računa).

V prihodnosti lahko pričakujemo tudi nove storitve, kot so trgovanje z vrednostnimi papirji in plačevanje nakupov v spletnih trgovinah.

Za plačevanje z mobilnim telefonom pa je družba Mobitel uvedla sistem Moneta. Ta sistem zagotavlja enostavno uporabo in hitro izvedbo nakupa vsem Mobitelovim naročnikom GSM, kmalu pa načrtujejo razširiti ponudbo še na predplačniške Mobi uporabnike. Uporabniku zagotavlja enostaven potek plačila blaga ali storitev z mobilnim telefonom, ki v tem primeru deluje kot kreditna kartica. Znesek kupljenega blaga poravnamo naenkrat, vendar zakasnjeno skupaj z mesečnim računom telefonskih pogovorov. Takšen sistem predstavlja konkurenco bančnim plačilnim karticam. Še več, omogoča elektronsko plačevanje tudi segmentu potrošnikov, ki ne izpolnjujejo zahteve za pridobitev kreditne kartice. Sistem eMoneta omogoča plačevanje blaga in storitev preko interneta, sistem aMoneta na avtomatih in najnovejši sistem posMoneta preko POS terminalov. Število ponudnikov blaga in storitev, ki sprejemajo sistem Moneta, je iz dneva v dan vse večje.

4. SKLEP

Razvoj tehnologije je povzročil veliko sprememb v bančništvu in poslovanju nasploh. Elektronsko bančništvo je postalo, v kratkem času, vsakdanji pojav ter nujen del bančne ponudbe, če banka želi še ostati konkurenčna in obdržati svoje komitente. Le-ti so se namreč navadili, da imajo dostop do svojega denarja in opravljanja bančnih storitev 24 ur na dan, 365 dni na leto. Z uveljavljanjem elektronskih medijev v bančništvu, pa sta postala varnost in zaupnost podatkov ključen segment modernega bančnega poslovanja. Banke morajo in bodo morale tudi v bodoče, nenehno vlagati v vzpostavitev in nadgradnjo svojih varnostnih sistemov, ki so zelo ranljiv del elektronskega poslovanja.

S pojavom elektronskega denarja in elektronskih denarnic se vedno bolj uveljavlja digitalna gotovina. Zaradi trenda konstantnega upadanja uporabe tradicionalne gotovine si lahko že predstavljamo, v bodočnosti, praktično popoln prehod na digitalno gotovino. Toda do takrat, bo poslovanje potekalo z digitalno in tradicionalno gotovino istočasno.

Internet postaja vodilni komunikacijski sistem. Banke so sprejele nov način poslovanja in s tem zmanjšale operativne stroške ter postale bolj konkurenčne. Ravno tako so se v deležu, ki se venomer povečuje, tudi njihovi komitenti, privadili bolj udobnega opravljanja bančnih storitev preko interneta. V času, ko življenje teče izredno hitro in ko je dobrodošla vsaka sprememba, ki nam prihrani čas, je za marsikoga bolj priročno in praktično opraviti bančne posle kar od doma, iz službe ali medtem ko je na poti. Slovenija še vedno zaostaja za razvitejšimi evropskimi državami po uporabi interneta in po poslovanju preko tega medija. Toda razkorak ni več tako velik, kot je bil le nekaj let nazaj. Sedaj se je trend naraščanja uporabe upočasnil, toda delež oseb in podjetij, ki uporabljajo oz. poslujejo na internetu se nenehno veča. V naslednjih desetih letih lahko predvidimo, da se bo izenačil z državami zahodne Evrope.

Zaradi izjemne razširjenosti uporabe mobilnega telefona, ima mobilno bančništvo ogromno število potencialnih strank. Banke so že začele izkoriščati tudi ta medij in nuditi tudi storitve preko SMS in WAP bančništva. V Sloveniji se trenutno malo ljudi odloča za takšno poslovanje z banko. Razlog je najbrž ta, da je komitentom poslovanje z banko preko interneta, za sedaj, bolj praktično ob uporabi računalnika kot mobilnega telefona. Toda to področje se bo v bližnji prihodnosti v svetu in v Sloveniji, izjemno hitro razvijalo in širilo, saj smo sedaj šele na začetku odkrivanja, kaj vse nam mobilni aparat/telefon omogoča.

LITERATURA

1. Bartolini Brane: Samo še skozi virtualno okence. Moj mikro, Ljubljana, 2000, 7/8, str. 68-69.
2. Bec Suzana: Elektronsko bančništvo. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2000. 127 str.
3. Čanaki Peter: Samopostrežno bančništvo. Moj mikro, Ljubljana, 2001, 6, str. 62-63.
4. Imbert Patrick: Securing the wireless Internet. [URL: http://www.gemplus/wireless], maj 2001.
5. Jerman Blažič Aleksej: Banka v žepu. Moj mikro, Ljubljana, 2000, 7/8, str. 70-72.
6. Jerman Blažič Borka: Internet. Ljubljana : Novi Forum, 1996. 87 str.
7. Jerman Blažič Borka et al.: Elektronsko poslovanje na Internetu. Ljubljana : GV založba, 2001. 206 str.
8. King Ben: ATMs cuntinue to improve. Banking Technology Solutions. London : Cornhill publications limited, 1998, str. 76-78.
9. Klapš Srečko: Ponudba plačilno kreditnih in bonitetnih kartic v Sloveniji. Kapital, Maribor, 5(1995), 98, str. 22-29.
10. Karpe Primož: Bančništvo in »Nova tehnologija«. Bančni vestnik, Ljubljana, 50(2001), 12, str. 41-44.
11. Logar Miha: Troboj plastičnih kartic. Bančni vestnik, Ljubljana, 45(1996), 1/2, str. 37.
12. Mesec Dejan: Moneta – Mobilni telefon kot plačilno sredstvo. Mobinet, Grosuplje, 2004, 4, str. 39.
13. Mihelčič Martin: Pametne kartice preplavile svet. Bančnik, Ljubljana, 1999, 4, str. 10.
14. Miš-Svoljšak Irena: V tujini se elektronsko bančništvo še povečuje. Kapital, Maribor, 9(1999), 207, str. 30.
15. Novak Irena: Terminal namesto blagajne. Podjetnik, Ljubljana, 11(1995), 4, str. 46-47.
16. Odar Marjan: Kreditne (zaupanjske) kartice. IKS, Ljubljana, 27(2000), 9, str. 93-107.
17. Oman Saša: On-line bančništvo v svetu in Sloveniji. Bančni vestnik, Ljubljana, 51(2002), 6, str. 17-21.
18. Osojnik Mojca et al.: Skrivnosti elektronskega poslovanja: Priročnik za mala in srednje velika podjetja. Ljubljana : Založba GZS, 2002. 288 str.
19. Rotovnik Tomaž: Izziv v svetu kartičnega poslovanja. Bančnik, Ljubljana,1999, 9, str. 18-19.
20. Rupnik Rok et al.: Je vstop digitalne mobilne telefonije v svet poslovne informatike avantura ali (r)evolucija?. Zbornik posvetovanja Dnevi slovenske informatike 2000. Ljubljana : Slovensko društvo informatika, 2000, str. 240-248.
21. Savodnik Tomaž: Rast ovira nepoznavanja. Moj mikro, Ljubljana, 2000, 1, str. 16.
22. Sjekloča Marko: Elektronsko bančništvo. Bančni vestnik, Ljubljana, 48(1999), 1/2, str. 31-33.
23. Slana Lidija, Strojan Janez: Elektronsko poslovanje – uvajanje mednarodnega standarda UN/EDIFACT v poslovno in bančno okolje. Uporabna informatika, Kranj, 7(1999), 4, str. 25-31.

24. Svigals Jerome: Bank Branching 2010. Dublin : Lafferty Pub., 1996. 219 str.
25. Šinigoj Aleksander, Turk Tomaž: Sodobno elektronsko poslovanje – varnostni vidiki. Dnevi slovenske informatike Portorož 1999. Zbornik posvetovanja. Ljubljana : Slovensko društvo informatika, 1999. str. 457-466.
26. Toplišek Janez: Elektronsko poslovanje. Ljubljana : Atlantis, 1998. 336 str.
27. Van Hove Leo: Electronic Purses: (Which) Way To Go?. First Monday. [URL: http://www.firstmonday.dk/issues/issue5_7/hove/], 2000.
28. Vehovar Vasja et al.: Internet v Sloveniji, projekt RIS 96-98. Izola : DESK 1998, 315 str.
29. Voljč Marko, Šega Polona: Prihodnji razvoj slovenskih bank. Bančni vestnik, Ljubljana, 50(2001), 5, str. 111-117.
30. Zebec Koren Marko, Cvjetovič Srdjan: Razširjeno e-bančništvo?. Moj mikro, Ljubljana, 2001, 6, str. 55.

VIRI

1. Algoritmi z javnim ključem (asimetrični algoritmi). [URL: http://www.gov.si/tečaj/kripto/kr-asim.htm], 12.12.2003.
2. Bilten Banke Slovenije. Ljubljana : Banka Slovenije, 13(2004), 6, 133 str.
3. Bilten Banke Slovenije. Ljubljana : Banka Slovenije, 12(2003), 4, 111 str.
4. Forrester research. [URL: http://www.forrester.com/ER/Press/Release/0,1769,788,00.htm], 03.04.2003.
5. Frelih Tomaž: Tehnologije identifikacijskih kartic. [URL: http://www.avtomatika.com/automation/Vsebine/A16/4way/CARDTECH3-automatika-part2.htm], 26.11.2003.
6. Mobitelova Moba nad pričakovanji. [URL: http://www.mobitrg.com/novice/izpis_cela.php?id_novice=120], 02.08.2004.
7. Primerjava Slovenija – EU. RIS, Gospodinjstva. [URL:http://www.sisplet.org/ris/uploads/publikacije/2003/36%20Gospodinjstva%20slo_eu.pdf], junij 2003.
8. Uporaba Interneta. RIS, Gospodinjstva. [URL:http://www.ris.org/uploadi/editor/ris2003_3_koncna_4_2_2004_javno.rar], februar 2004.
9. Mobilna telefonija. RIS. [URL:http://www.sisplet.org/ris/uploads/publikacije/2003/8%20Mobilna%20telfonija.pdf], junij 2001.
10. Tveganja pri elektronskem bančništvu. Kapital, Maribor, 9(1999), 207, str. 29.

SLOVARČEK IZRAZOV

- authentication	- pristnost; varnostna storitev pri internetnem poslovanju, ki prejemniku zagotavlja, da je sporočilo res poslal navedeni pošiljatelj
- autorisation	- avtorizacija; varnostna storitev pri internetnem poslovanju, ki omogoča nadzor dostopa do določenih informacij
- back office	- pisarna v ozadju; izraz se v diplomski nalogi pojavi za podjetje, ki enemu drugemu podjetju zagotavlja storitve procesiranja transakcij
- Certifiying Authority	- elektronski notar; agencija za izdajanje certifikatov na internetu
- chat	- klepet; storitev na internetu, kjer lahko komuniciramo oz. ″klepetamo″ z drugimi, tako, da si pošiljamo elektronska sporočila
- confidentiality	- zaupnost; varnostna storitev pri internetnem poslovanju, kjer se zaradi zaupnosti podatkov, le-ti šifrirajo pri prenosu
- Digital Cash	- digitalna gotovina
- electronic commerce	- elektronsko poslovanje; poslovanje, ki uporablja elektronske medije za izmenjevanje podatkov med računalniki
- e-mail	- elektronska pošta; storitev na internetu, ki omogoča pošiljanje in sprejemanje elektronskih sporočil
- firewall	- požarni zid; računalnik z ustrezno programsko opremo, ki omogoča zaščito notranjega omrežja pred vdori iz interneta
- Gopher	- hrček; storitev na internetu, ki omogoča raziskovanje in iskanje po internetu
- Hash Code	- koda, ki izdela digitalni odtis sporočila za digitalen podpis
- integrity	- celovitost; varnostna storitev na internetu, ki zagotavlja prejemniku, da se podatki niso spremenili med prenosom
- learning curve of one	- enojna krivulja učenja; krivulja učenja, ki omogoča uporabo naučenega po eni sami demonstraciji
- link	- vez; storitev na spletnih straneh, ki omogoča hitro povezavo z drugo spletno stranjo podobne vsebine
- nonrepudation	- nezavrnitev; varnostna storitev na internetu, ki zagotavlja pošiljatelju, da je prejemnik sporočilo res prejel ter prejemniku, da je pošiljatelj res sporočilo poslal
- offline	- brez povezave; stanje, ko računalnik ni povezan z nobenim drugim računalnikom preko modema
- on-demand	- na zahtevo
- online	- povezan z; stanje, ko sta vsaj dva računalnika povezana preko modema
- physical exchanges	- telesna sporočila; sporočila, ki jih oddajamo in sprejemamo, ko smo v fizični bližini z drugimi
- Point of sale (POS)	- elektronsko prodajno mesto
- router	- usmerjevalnik; naprava, ki upravlja pretok paketov informacij med različnimi deli omrežja

- Smart Card	- pametna kartica; kartica z vgrajenim mikročipom, ki omogoča prenos in hranjenje informacij
- store and forward	- shrani in posreduj
- transfer control	- nadzor pretoka; varnostna storitev pri internetnem poslovanju, kjer vozlišča, t.i. obrambni zidovi, privatnih mrežnih hiš preverijo vsako sporočilo, ki prihaja iz ali pa je namenjeno v internet
- USENET	- konferenčni sistem na internetu, namenjen pogovoru o različnih temah med veliko sodelujočimi
- white labelling	- tiha partnerstva; banke postanejo tihi partner banki, ki ponuja internetno bančništvo