UNIVERZA V MARIBORU
EKONOMSKO-POSLOVNA FAKULTETA, MARIBOR

DIPLOMSKO DELO

STORITVE E-BANČNIŠTVA V SLOVENIJI
E-BANKING SERVICES IN SLOVENIA

Kandidatka: TJAŠA DILICA
Študentka izrednega študija
Številka indeksa: 81541359
Program: visokošolsko strokovni '96
Študijska smer: finance in bančništvo
Mentor:dr. Bobek Samo

Hrvatini, oktober, 2009

PREDGOVOR

Banke so že od nekdaj nepogrešljiva inštitucija našega življenja. Z elektronskimi mediji, predvsem interneta, se je poslovanje z njimi močno spremenilo. Opravila, informacije in ponujene storitve so postale preproste in predvsem lažje dostopne vsem uporabnikom. Glavno spremembo je povzročil internet, ki je z svojo dostopnostjo in funkcionalnostjo omogočil popoln dostop do vseh želenih informacij. Namen diplomske naloge je pridobiti informacije o samem elektronskem bančništvu, o internetu, razvoju, varnosti ter predstaviti kakšne možnosti nam nudi elektronsko bančništvo v bodoče.

Za ta naslov sem odločila zato, ker imam računovodski servis in se vsak dan srečujem z elektronskim bančništvom različnih bank in ker menim, da postaja elektronsko bančništvo vedno bolj aktualno in verjamem, da je ta storitev olajšala poslovanje podjetnikom.

Poglaviten preboj in osnovno spremembo na področju e-bančništva pa je povzročil prav internetni razvoj, ki pa se nenehno dopolnjuje ter zavija v tehnološko napredni sistem za prav vsakega uporabnika med nami.

Novodobni in čedalje bolj zaposleni uporabniki e-bančništva so pozitivno zadovoljni s samo ponudbo elektronskega bančništva, ki jo trenutno ponujajo naše aktualne banke, le te pa se tudi same močno zavedajo, da se v sedanjem tržno naravnanem globalnem okolju nikakor nebi uspele preživeti brez progresivnega in stalnega razvoja na specifično naravnanem področju organizacijsko tehnološkega izpopolnjevanja.

Zahvaljujem se profesorju dr. Samu Bobku, za mentorstvo pri diplomskem delu ter svoji družini za podporo in pomoč pri zaključevanju študija

KAZALO VSEBINE

KAZALO TABEL

KAZALO SLIK

1 UVOD

1.1 Opredelitev področja in opis problema

V današnjem času se banke in druge finančne institucije soočajo z velikimi razvojnimi izzivi. Konkurenca na področju bančništva je iz dneva v dan močnejša in vse bolj razširjena in prav ta sili banke v iskanje novih rešitev in možnosti za pridobitev dodatnih konkurenčnih prednosti in s tem razširitev svojega obstoječega trga.

Uspešnost bank je v veliki meri odvisna od ustrezne informacijske tehnologije in njene učinkovitosti. Informacijska tehnologija ima v bančništvu veliko vlogo kot v drugih gospodarskih dejavnosti, zato ker je bančništvo storitvena dejavnost, ki temelji na natančnih, celovitih in predvsem ažurnih informacijah.

Prav zato se je bančništvo, kakor tudi veliko ostalih dejavnosti, preselilo v internetno poslovanje. Doba elektronskega poslovanja odpira nove načine in poti komuniciranja s strankami ter ponuja možnost uvajanja novih storitev.

Elektronsko bančništvo pa ni nastalo z razvojem interneta, saj smo že pred njim poslovali z bankomati, plačilnimi karticami in prek telefona. Internet nam je omogočil nadaljnjo širitev elektronskega bančništva.

Nov način poslovanja pomeni prihranek dragocenega časa, je enostavne uporabe in hkrati prinaša posodobitev bančnega poslovanja. Na ta način se z uvajanjem novih tehnologij odpirajo nove tržne poti, preko katerih se lahko stranka poveže z banko. V današnjem času banka brez ustrezne informacijske podpore elektronskega bančništva ne bi mogla več preživeti. V nekaj letih bi izgubila komitente, poleg tega pa ne bi zmogla minimizirati stroškov klasičnega načina poslovanja in zagotavljati konkurenčnosti.

Uspešno bodo poslovale in se obdržale oziroma povečale svoje tržne deleže le tiste banke, ki se bodo pripravljene hitro in neprestano prilagajati spremembam na trgu, izkoriščati nove priložnosti in slediti željam komitentov.

V prihodnje bo tradicionalističen način poslovanja preko bančnih okenc uporaben le v primeru, ko bo bančna storitev izrecno zahtevala človeško komunikacijo.

1.2 Namen, cilji in osnovne trditve

Namen v diplomski nalogi je poskusiti prikazati trenutno stanje na področju elektronskega bančništva, hkrati pa podati tudi sliko o tem, kaj elektronsko bančništvo sploh je, in katere so nove zmožnosti nove tehnologije. Posvetila sem se varnosti elektronskega bančništva, saj velja kot ključni dejavnik elektronskega poslovanja, na katerega so tako zagovorniki kot kritiki zelo pozorni.

Izognila sem se primerjave med posameznimi bankami ter opisovanju in naštevanju ponudbe, ker sem se želela omejiti na elektronsko bančništvo kot tako. Vendar pa to ne pomeni, da se nisem podrobno poglobil v možnosti, ki se ponujajo uporabniku, le da sem to naredila na nivoju vseh bank.

Med pisanjem pa sem poskušala vsebino prenesti na slovenski trg in ugotoviti, kako so slovenske banke pripravljene in kakšna je njihova izhodišče in ponudba. Na nekaterih mestih sem teoretično podkrepila s konkretnimi premeri in številkami.

1.3 Predpostavke in omejitve raziskave

V svojem diplomskem delu sem se osredotočila na rabo interneta kot tako, elektronskega bančništva kaj nam omogoča elektronsko bančništvo ter načini njegove uporabe v povezavi z njegovo varnostjo ter situacija v Sloveniji.

1.4 Predvidene metode raziskovanja

Predvidena metoda raziskovanja je dinamična, ker diplomska naloga preučuje nastajanje določenih sprememb kot posledico spremembe določene spremenljivke.

Pri pisanju sem uporabila vse razpoložljive vire, domačo in tujo literaturo in seveda internet.

2 INTERNET

2.1 SESTAVNI DELI IN DELOVANJE

Internet je danes postal povsem vsakdanjik, prenos podatkov in elektronsko poslovanje pa dostopna tako rekoč vsem. Vendar pa kljub temu le malokateri uporabnik ve, kako dejansko deluje internet in kakšne storitve vse omogoča. Poznavanje osnov tehnologije pa je vendarle nujno za razumevanje poslovanja preko interneta.

V današnjem času že skoraj ni dejavnosti, s katero bi se ukvarjal človek in je nebi našli na internetu. O tem pričajo tudi že številni reklamni izdelki, saj skorajda ni plakata oziroma televizijske reklame, ki v kakšnem vogalu nebi imela napisano »www«…, kar ne predstavlja nič drugega, kot »domač naslov« v svetu informacij, kjer hišne številke nadomeščajo internetni naslovi.

Internet je torej medij, ki omogoča, da posameznik svoj izdelek predstavi svoj izdelek širšemu okolju in s tem prispeva del podatkov v svetovno bazo. Možno je tudi sodelovanje s strokovnjaki na posameznih področij in vključevanje v razne projekte, kjer podatke združujemo, analiziramo, interpretiramo in primerjamo odkritja. S takšnimi projekti se zbirajo oziroma ustvarjajo resnične podatkovne baze.

Na internetu se vsak mesec objavi okoli 20 milijonov novih spletnih strani kar pomeni, da se vsako sekundo pojavi na internetu skoraj 10 novih naslovov. Seveda se ob tolikšnem številu naslovov upravičeno vprašamo: » Kako najti posamezen naslov oziroma podatke, ki jih iščemo? « Nemalokrat se namreč zgodi, da pri iskanju in zbiranju informacij zaidemo na kakšno stransko pot ali pa celo preusmerimo pozornost na kakšno drugo zanimivejšo stvar.

Seveda pa iskanje informacij preko interneta le ni tako težavno opravilo, saj danes že obstajajo številni iskalniki, ki nam preko ključnih besed omogočajo poiskati želeno informacijo.

Naštejmo nekaj iskalnikov:

- http://www.matkurja.com/
- http://www.google.com/
- http://www.yahoo.com/
- http://www.slowwenia.com/
- http://www.altavista.com/
- http://www.excite.com/

2.1.1 Strežnik in odjemalec

Strežnik (ang. Server) imenujemo program, ki omogoča opravljanje storitev (»streže«) drugim programom v istem ali drugih računalnikih. Na splošno pa se je isti naziv uveljavil tudi za računalnik, ki poganja ta program, čeprav lahko poganja več strežniških in odjemalskih programov hkrati.

Program ali računalnik, ki dostopa na strežnik in uporablja njegove usluge, se imenuje odjemalec (ang. Client). V primeru dostopa preko svetovnega spleta je odjemalec kar brskalnik kot npr Internet Explorer1 ali Netscape Navigator. Možno je tudi, da je isti računalnik hkrati strežnik in odjemalec.

V primeru elektronskega bančništva je strežnik bančni program, ki omogoča storitev, uporabnik pa nastopa kot odjemalec.

2.1.2 Protokol

Protokol je »jezik«, v katerem se računalniki pogovarjajo. Dejansko je protokol sestavljen iz množic procedur/postopkov, ki jih računalniški programi ustrezno interpretirajo. Na internetu daleč najbolj razširjena skladovnica protokolov je TCP/IP (Transport Control Protocol/ Internet Protocol), ki velja za standardno skladovnico protokolov. Ta status je dobila zaradi mednarodno priznane standardizacije in svoje odprtosti, danes pa jo najdemo vgrajeno v vsak operacijski sistem.

Naloga protokola je, da skrbi za pravilen prenos podatkov, zato TCP/IP prelomi niz podatkov na majhne dele (paketke), vsakega opremi s podatki o pošiljatelju in prejemniku in jih pošlje po omrežju. Tako lahko vsak paket potuje po omrežju neodvisno, skupaj pa se sestavijo pri prejemniku. Poleg TCP/IP obstaja še množica drugih, manj razširjenih komunikacijskih protokolov.

Naloga protokola IP je tudi sporočanje o delovanju samega protokola. Ta funkcija ni natančno določena in je po navadi omejena le na osnovna sporočanja, npr. o izmetu posameznega paketa IP v enem od usmerjevalnikov v omrežju.

Omrežni protokol IP ne vključuje mehanizmov za zanesljiv in kvaliteten prenos po omrežju. Deluje po načelu najboljše možne (best effort) dostave paketov IP. Zakasnitev pri potovanju paketov niso določene. V splošnem velja, da so pri manjših obremenitvah omrežja zakasnitve majhne (povezane predvsem s kapacitetami nosilnih storitev fizičnih omrežij), pri večjih pa postanejo nepredvidljive. Ker lahko paketi med končnima omrežnima povezavama potujejo po različnih poteh, ni zagotovljen niti vrstni red dostave paketov. Če se kateri od paketov okvari ali izgubi, omrežje IP samo nima mehanizmov za odpravo napake. Takšne mehanizme v internetnih sistemih zagotavljajo drugi protokoli.

Pri načinih uporabe (predvsem komunikacija med računalniškimi aplikacijami) za katero je bil protokol IP načrtovan, omenjene (slabe) lastnosti omrežij IP niso ključnega pomena. Izrazite pa postanejo takrat, ko želimo omrežja IP uporabljati za npr. prenos govora in

video signalov v realnem času. Vendar tudi tu sodobne ITKT (informacijske in telekomunikacijske tehnologije) iščejo in ponujajo ustrezne rešitve.

2.1.3 Naslov

Vsak računalnik ob priključitvi na internet dobi svoj naslov, ki je sestavljen iz 32-bitne IP številke. Tej številki rečemo internetni številčni naslov. Pišemo jo v desetiškem sistemu (4x8 bitov) kot npr. 117.28.36.2. Te številke označujejo tako računalnik kot omrežje, v katerem se nahaja. Vseh možnih naslovov je 4.294.967.296, kar bi sicer moralo zadostovati za trenutne potrebe, vendar jih zaradi načina dodeljevanja počasi zmanjkuje in bo potrebna razširitev številčnega naslova na 128- bitno osnovo (Jerman, Blažič 1999,41).

2.1.4 Dostopanje in povezljivost

V preteklosti je bil dostop do interneta nujen računalnik, ki ga še danes velika večina uporablja za dostopanje, vendar je tehnologija tako napredovala, da je danes moč priti na internet tudi s pomočjo GSM telefona, dlančnika in še nekaterih elektronskih naprav. Pričakuje se, da bo v prihodnosti večina stvari tako ali drugače povezana v omrežje, začenši z digitalno televizijo, avtomobili in nekaterimi hišnimi pripomočki.

Tabela 1: Načini dostopanja do interneta 1. četrtletja 2007 - 1. četrtletja 2009

	1. četrletje 2007 delež (%)	1. četrletje 2008 delež (%)	1. četrletje 2009 delež (%)
Ozkopasovna povezava	14	9	8
Širokopasovna povezava	44	50	56
Modem	9	5	4
ISDN	6	5	5
xDSL	29	30	31
Kabelski dostop	13	17	20
Druga širokopasovna povezava (npr. optično omrežje)	1	2	6
WAP, GPRS	24	27	21
UMTS	7	9	16

Vir: Muzlovič, Marko 2009. Uporaba interneta v gospodinjstvih in pri posameznikih.

2.1.5 Uporabniki

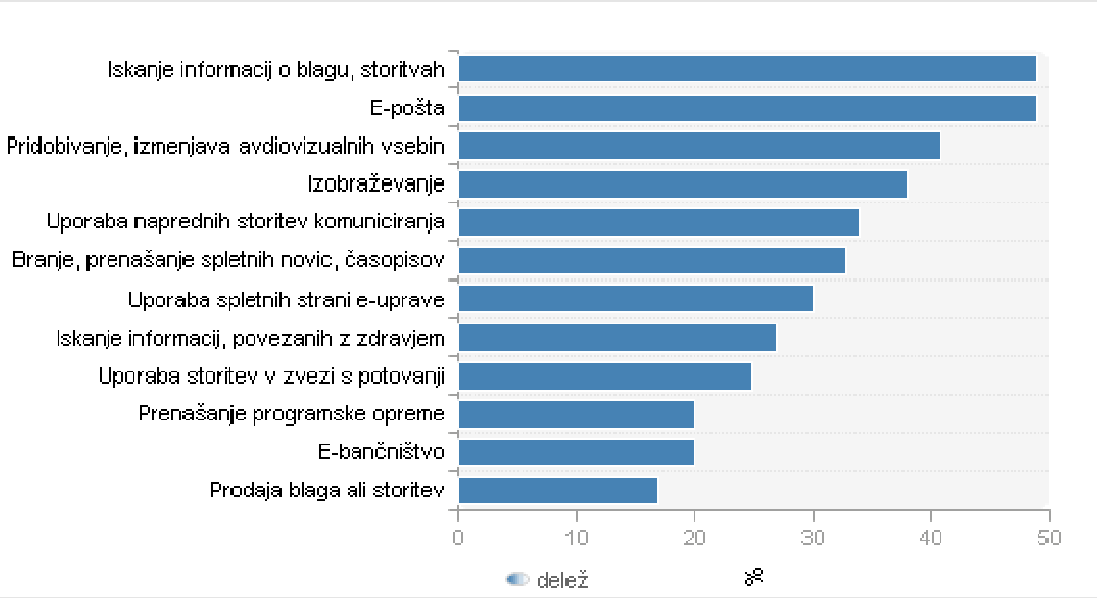
Mednarodno priznani inštitut za raziskavo trga GFK je objavil izsledke obsežne raziskave o uporabi svetovnega spleta v evropskem prostoru. V Evropi svetovni splet zdaleč največ uporabljajo Islandci in Skandinavci, saj na Islandiji internet redno uporablja kar 88 odstotkov prebivalcev, starejših od 14 let, na Finskem 81 odstotkov, na Norveškem in Danskem 76 odstotkov ter na Švedskem dobrih 73 odstotkov prebivalcev. Najnižja uporaba interneta v evropskem prostoru je v Albaniji, saj dostop do svetovnega spleta uporablja le odstotek prebivalstva. V Zahodni Evropi svetovni splet najmanj uporabljajo na Malti, kjer internet obiskuje komajda četrtina prebivalstva, sledijo ji Španci s 35 odstotki, Portugalci s 43, in Irci s 45 odstotki. V naši deželi je uporaba interneta dokaj visoka, saj ga uporablja 61 odstotkov prebivalcev, starejših od 14 let. V zlati sredini najdemo še Avstrijo s 67 odstotkov uporabe interneta, Veliko Britanijo s 63 odstotkov, Nemčijo z 61 odstotki, Francijo s 56 odstotki in v Italijo s 53 odstotki.

Tabela 2: Uporabniki interneta v letih 2004-2008

	1. četrtl. 05 delež (%)	1. četrtl. 06 delež (%)	1 četrtl. 07 delež (%)	1. četrtl. 08 delež (%)	1. četrtl. 09 delež (%)
10 – 74	50	54	56	58	64
16 – 74	47	51	53	56	62
10 – 15	83	92	90	95	98
16 – 34	77	81	84	88	91
35 – 54	45	50	53	56	66
55 - 74	(11)	14	14	17	22

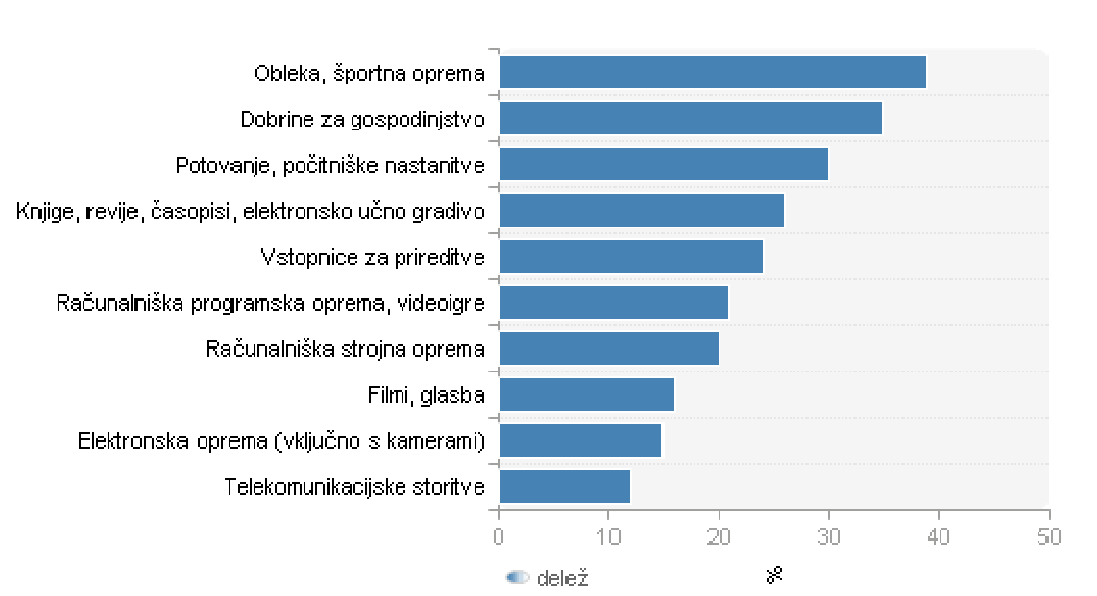
Vir: Muzlovič, Marko 2009. Uporaba interneta.

Slika 1: Namen uporabe interneta, Slovenija 1. četrtletje 2008



Vir: Zdrešar, Polona 2008. Uporaba interneta, 1. Četrtletje 2008.

Slika 2: Namen uporabe interneta, Slovenija 1. četrtletje 2009



Vir: Muzlovič, Marko 2009. Uporaba interneta.

2.2 Storitve

Internet ponuja vrsto storitev, ki pa so med uporabniki različno sprejete. Tako recimo v Sloveniji velika večina (90%) pozna in redno uporablja svetovni splet in elektronsko pošto. Ostale storitve so že bistveno manj poznane, saj je le četrtina uporabnikov dejansko kdaj prenašala datoteke, le 10% pa jih uporablja elektronske konference, poštne sezname in USENET konference. V nadaljevanju navajam osnovne internetne storitve.

2.2.1 Elektronska pošta

Elektronska pošta je najbolj enostaven način izmenjave sporočil med dvema ali več uporabniki, zato od nastanka računalniških omrežij nastopa kot najpogosteje uporabljano orodje dvosmerne komunikacije, pravi (Škerlep 1998, 28). Elektronska pošta je tudi najbolj uporabljano orodje, ki ga ponuja internet; uporablja ga štirikrat več oseb, kot je tistih z dostopom do interneta in 84 odstotkov vseh ljudi, ki imajo dostop do interneta, to počne z namenom komuniciranja prek elektronske pošte.

Elektronska pošta služi najrazličnejšim komunikacijskim namenom: uporabljamo jo lahko za povsem neformalno osebno komuniciranje, za neosebno formalno komunikacijo, ki je vezana na institucionalno komuniciranje in poklicno sodelovanje (npr. za komuniciranje med neko institucijo in njeno stranko). Zaradi svoje učinkovitosti in enostavne uporabe je e-pošta postalo priljubljeno orodje za večino praktikov odnosov z javnostmi, pri katerih je kot primarni medij komuniciranja nadomestila telefon.

2.2.2 Svetovni splet

Če za elektronsko pošto pravimo, da je najbolj uporabljeno orodje na internetu, lahko z gotovostjo trdimo, da je svetovni splet tisti dejavnik, ki je spodbudil rabo interneta tudi v širši javnosti. Svetovni splet danes predstavlja najbolj vplivno in uporabno orodje za podjetja, ki so vrsto let iskala možne načine za upravljanje odnosov s ciljnimi javnostmi. Svetovni splet podjetjem ne zagotavlja le dostopa do ciljnih javnosti, temveč jim omogoča, da na svojih spletnih straneh obiskovalcem ponudijo gradivo, ki ga bodo sami vzeli. Ljudje iščejo in sami »vlečejo« informacije z interneta (Holtz 2002, 52-53).

Raziskava Oddelka za trgovino v ZDA o rabi interneta pri Američanih je pokazala, da več kot 67 odstotkov vseh uporabnikov interneta uporablja internet za iskanje informacij. To pa poudarja potrebo podjetij po objavi informacij o njihovih produktih ali storitvah na svojih spletnih straneh.

Prednosti spleta, ki jih podjetje lahko izkoristi v komunikaciji s ciljnimi javnostmi (Holtz 2002, 54-55) so: hitrost- najnovejše informacije so lahko na spletni strani podjetja objavljene takoj; neomejenost prostora- v primerjavi s tiskanimi mediji, prostor, ki ga podjetja lahko uporabi na spletu, ni omejen; prilagajanje informacijsko-ekonomskih komunikacij prejemnikom- vstopna spletna stran podjetja je lahko oblikovana na način, da obiskovalcem omogoči, da hitro in enostavno poiščejo informacije, ki jih zanimajo. Stran

je lahko porazdeljena v različne sklope, po katerih lahko obiskovalec nadalje išče želene informacije (novica dneva, predstavitev podjetja, informacije za delničarje in vlagatelje, novinarsko središče, iskalnik, ipd.); priložnosti za komuniciranje in marketing s posamezniki (ena-na-ena) – marketing je antiteza množičnemu marketingu, kjer podjetje množico uporabnikov nagovarja z enakim sporočilom, pri tem pa se ne ozira na izkušnje posameznikov, njihove potrebe in želje.

2.2.3 Prenos datotek

FTP strežnike uporabljamo za prenos datotek med računalniki v internetu. Lahko so javni (možna anonimna prijava) ali zasebni (potrebujemo uporabniško ime in geslo). Navadno jih postavijo osebe ali organizacije, ki želijo posredovati datoteke širši javnosti. Prednost FTP-ja je hitrost, zanesljivost in možnost izmenjave datotek med več uporabniki. Storitev je navadno že vgrajena v odjemalce in strežnike svetovnega spleta.

Besedila, tabele, grafikone, podatkovne baze, video in zvočne zapise, animacije, ilustracije, fotografije in druge računalniške datoteke je mogoče enostavno prenesti iz enega računalnika na drugega ali pa jih shraniti na strežniku in omogočiti dostop do vsem, ki jih potrebujejo (Holtz 2002, 58).

2.2.4 Omrežne novice in klepetalnica

Pri omrežnih novicah gre za konferenčni sistem, kjer lahko uporabniki razpravljajo, si izmenjujejo mnenja, podatke, ali berejo prispevke drugih. Zaradi obsežnosti in lažjega pregleda so konference razdeljene hierarhično po tematiki. Sistem ni interaktiven, za uporabo pa navadno zadostuje isti program kot za elektronsko pošto.

Klepetalnica omogoča več uporabnikom hkratni klepet prek interneta s pomočjo tipkovnice (tekstovni način) in je trenutno priljubljena predvsem pri mladini. V prihodnosti se pričakuje preklop iz tekstovnega načina na način, ki bo podpiral tudi zvok in sliko (princip video konference), vendar je za to potrebna velika prepustnost omrežja.

Dostop do določenih ciljnih javnosti podjetja je na spletu nekoliko lažji, saj se običajno povezujejo t.i. virtualne skupnosti-spletna stičišča ljudi s skupnimi interesi. Skupnosti, ki se oblikujejo na spletu bi lahko poimenovali tudi diskusijske skupine, saj uporabniki skozi različna spletna orodja (klepetalnice, forume, bloge idr.) razpravljajo o različnih temah, izmenjujejo najnovejše informacije, svoja mnenja in izkušnje o določenih izdelkih, storitvah,… ter na podlagi pridobljenih informacij tudi oblikujejo svoje mnenje in stališče do določenih tem.

2.2.5 Elektronsko poslovanje

Elektronsko poslovanje pomeni prehod iz klasičnega načina poslovanja, ki je potekal preko telefona in podatkov, informacij na papirju v elektronsko obliko sporazumevanja in poslovanja.

Pojem elektronsko poslovanje izhaja iz angleškega izraza »elektronic commerce« in obsega celoto procesov, ki podpira trgovsko, poslovno dejavnost in lahko vključujejo potrošnike, proizvajalce, prodajalce, ponudnike storitev in posrednike (Pavliha 2002, 24).

Na intenzivnost uvajanja elektronskega poslovanja pa vplivajo konkurence, vrsta dejavnost, stopnja razvitosti organizacije, stopnja razvitosti okolja, države, potrošnikov ter znanje in osveščenost o elektronskem poslovanju (Pucihar, Gričar 2002, 209).

Med ključne tehnološke elemente elektronskega poslovanja štejemo: računalnik, programsko rešitev (aplikacija) in komunikacije. Dodati pa je še potrebno organizacijo poslovanja, saj šele skupaj z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema.

Pri elektronskem poslovanju gre za več kot navadno izmenjavanje računalniških podatkov in delovanje spletne trgovine. Vse, kar danes delamo v okviru poslovne dejavnosti s pomočjo raznih računalniških aplikacij in računalniških omrežij, imenujemo elektronsko poslovanje. To obsega: elektronsko bančništvo, elektronsko trženje, elektronsko trgovanje, spletno trgovino, elektronsko zavarovalništvo, delo na daljavo, računalniško podprte skupine.

Pomembni elementi teh dejavnosti so naslednji (Jerman, Blažič 2001, 1289):

- Način dela: kjer gre za računalniško izmenjavo podatkov, ob uporabi odprtih omrežjih, kot npr: internet,

- Vsebina poslovanja: gre za prodajo blaga in storitev, plačevanje, prodajo informacij, izmenjavo dokumentov in listin, bančne transakcije, storitve trženja in medsebojnega komuniciranja, podpora porazdeljenemu poslovnemu informacijskemu sistemu, nakupovanje v spletnih trgovinah, opravljanja delo na daljavo, izvajanje pouka na daljavo in podobno,

- Udeleženci poslovanja: med udeležence elektronskega poslovanja lahko štejemo posameznike (podjetnike, menedžerje, raziskovalce, občane, učitelje, študente, dijake, upravne delavce), podjetja, bolnišnice, muzeje, galerije, univerze, izobraževalne organizacije in državne organe. Pri tem gre za poslovanje znotraj posameznih skupin in za poslovanje med skupinami. V zadnjem času prihaja v ospredje predvsem poslovanje med posamezniki ter med posamezniki in podjetji. Poslovanje med samimi podjetji pa je na trgu prisotno že dlje časa.

V primeru poslovanja med stranko oz. posameznikom in podjetjem oz. poslovnim sistemom omogoča elektronsko poslovanje strankam večji vpliv pri oblikovanju produktov in na to, kako so produkti narejeni ter način dostopa do storitev. V tem primeru govorimo o poslovanju med stranko in poslovnim sistemom. V primeru bank imenujemo tovrsten način elektronskega poslovanja elektronsko bančništvo (Bračun, Cetinski 1998,144).

3 ELEKTRONSKO BANČNIŠTVO

3.1 Opredelitev elektronskega bančništva

Elektronsko bančništvo lahko opredelimo kot način poslovanja strank z banko, ki je neodvisen od poslovalnic banke in temelji na informacijski tehnologiji ter elektronskih medijih. Med elektronske medije, ki podpirajo elektronsko bančništvo, uvrščamo: osebni računalnik, telefon (v živo in avtomatski odzivnik), internet, bankomati, televizija, in druge informativne informacijske naprave, kot so informacijski terminali, pametne kartice, elektronska denarnica, elektronska pošta itd. (Bračun 1997, 149).

Elektronsko bančništvo vedno bolj nadomešča tradicionalen način poslovanja z banko in s tem gotovinsko poslovanje iz dneva v dan zgublja na pomenu.

Poslovanje je vedno bolj usmerjeno na uporabo elektronski terminalov, bankomatov, interneta,… .

Elektronsko bančništvo lahko obravnavamo s širšega in ožjega vidika. V širši razlagi elektronsko bančništvo obsega vse, kar je povezano z elektronskim poslovanjem. Sem uvrščamo bančne avtomate, telefonsko bančništvo, avtomatske odzivnike, poslovanje bančnih terminalov in mobilnih telefonov. Ožja razlaga elektronskega bančništva pa se nanaša le na storitve virtualnega bančništva oz. bančništva, ki ga uporabljamo prek interneta oziroma s pomočjo spletnih strani. Elektronsko bančništvo torej lahko opredelimo kot kakršenkoli način poslovanja strank z banko, ki je neodvisna od poslovalnic in temelji na informacijski tehnologiji.

Banka mora pri razvoju elektronskega bančništva upoštevati predvsem želje in zahteve strank ter tehnološke zmožnosti. Pri razvoju je potrebno upoštevati in predvidevati predvsem naslednja dejstva (Bračun 1997, 150):

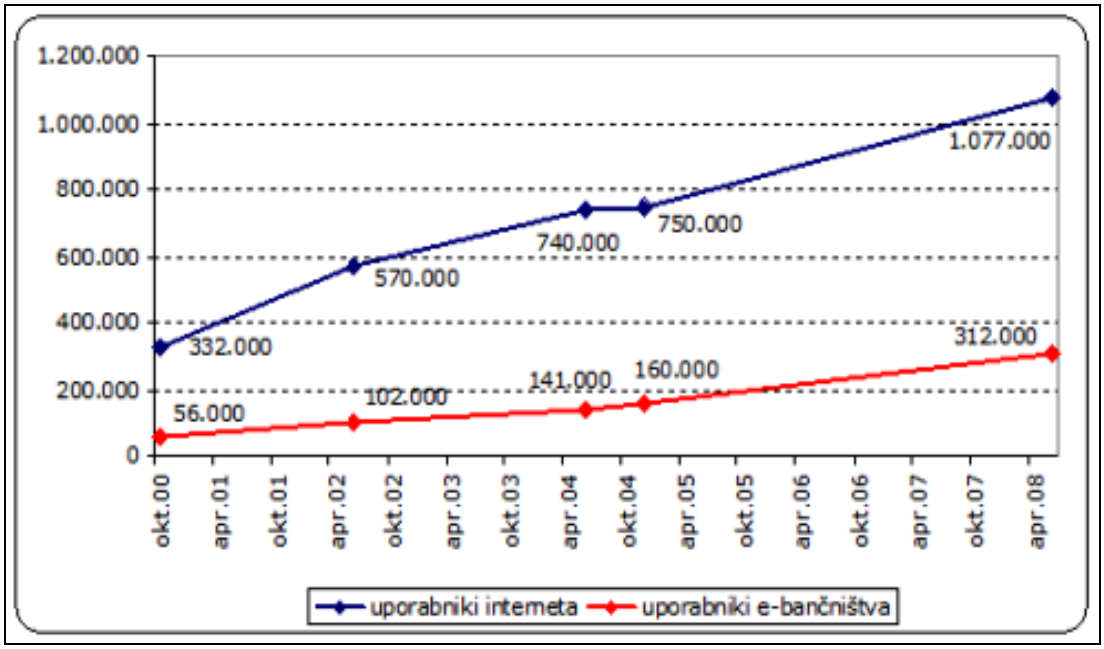
- Uporabniki želijo opravljati storitve kjerkoli, kadarkoli in na kakršen koli način,
- Kakšno tehnologijo imajo na razpolago uporabniki (stranki naj ne bi vsiljevali določeno tehnologijo, ampak bi upoštevali tisto kar že imajo doma ali v podjetju),
- Kakšna je komunikacijska infrastruktura v Sloveniji,
- Kakšno povezavo želi banka vzpostaviti s strankami,
- Kakšni so dolgoročni in kakšni so kratkoročni učinki elektronskega bančništva,
- Uporabniki morajo imeti zaupanje v storitve,
- Banka pa mora poskrbeti za najvišjo stopnjo možne varnosti,
- Kakšna je ciljna skupina uporabnikov.

Da bi ločili storitve elektronskega bančništva od zastarelih nestandardnih sistemov, morajo le-te storitve ustrezati naslednjim kriterijem (Kovačič 1997, 133):

- Neprekinjena dosegljivost 24 ur na dan, sedem dni v tednu,
- Dosegljivost kjerkoli,
- Morajo biti varne in
- Popolnoma avtomatizirane.

E-bančništvo se je v zadnjem desetletju izkazalo za eno najbolj dobičkonosnih spletnih storitev. Glede na vedno večjo ponudbo storitev preko spleta, je za ponudnike ključnega pomena pridobitev kakovostne splošne slike o panogi. Glavni dejavniki, ki vplivajo na uporabo (in raven uporabe) e-bančništva po podatkih RIS so predvsem skrb za varnost oz. zasebnost, finančna tveganja, način dojemanja prednosti, uporabnosti storitve ter odnos do spletnih storitev nasploh. Ponudba e-bančništva bo v prihodnje eden izmed ključnih momentov pri odločanju za izbiro banke,spletne storitve bodo postale ključni faktor pri ohranjanju oz. pridobivanju ali izgubi tržnega deleža med komitenti.

Slika 3: Primerjava uporabnikov interneta in e-bančništva



Vir: Kozic, Tina, Katja Prevodnik, Vehovar Vasja in Kogovšek Luka 2009. E-bančništvo 2009.

Leta 2004 je RIS napovedal letno rast uporabnikov e-bančništva za 15%, kar v absolutnem pomeni letno rast v povprečju za 20.000 uporabnikov. Napovedi so se v celoti uresničile,

vendar pa se za prihodnja leta kaže počasnejši trend rasti. Ob sedanjem trendu rasti za EU15 oz. EU27 lahko v EU do leta 2020 v povprečju pričakujemo današnjo raven skandinavskih držav (okoli 60 ali 70% uporabnikov e-bančništva v populaciji 16-75 let). Ob sedanjem trendu rasti v Sloveniji, pa lahko takšno raven v Sloveniji pričakujemo šele do leta 2035. Slovenija s trenutnimi trendi ne zmanjšuje razkoraka za razvitejšimi evropskimi državami. Banke bodo morale v prihodnjih letih oblikovati ponudbo, ki bo zadržala obstoječe uporabnike ter privabila nove. Kakšna so gibanja na strani ponudbe (tržni deleži, število in razporeditev ponudnikov) in povpraševanja – npr. kdo so (ne)uporabniki, zadovoljstvo in lojalnost komitentov – bodo za obstoječe in nove ponudnike ključna vprašanja v naslednjih nekaj letih intenzivne ekspanzije.

3.2 Zakonodaja pri elektronskem bančništvu

Zakonodajo na področju varnosti elektronskega bančništva ureja Zakon o elektronskem poslovanju in elektronskem podpisu (v nadaljevanju ZEPEP). Ta zajema poslovanje v elektronski obliki z uporabo informacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu. (ZEPEP, 2000).

Pomen nekaterih izrazov iz ZEPEP, ki so uporabljeni tudi v moji diplomski nalogi:

1. Podatki v elektronski obliki so podatki, ki so oblikovani ali shranjeni na elektronski način.

2. Elektronsko sporočilo je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.

3. Elektronski podpis je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.

4. Varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve:
   - Da je povezan izključno s podpisnikom,
   - Da je iz njega mogoče zanesljivo ugotoviti podpisnika,
   - Da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom,
   - Da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njim.

5. Časovni žig je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času.

6. Pošiljatelj elektronskega sporočila je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.

7. Naslovnik elektronskega sporočila je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo.
8. Prejemnik elektronskega sporočila je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.

9. Posrednik elektronskega sporočila je oseba, ki za drugo osebo pošlje, prejme, shrani elektronsko sporočilo ali nudi druge storitve v zvezi z elektronski sporočilom.

10. Podpisnik je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.

11. Informacijski sistem je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.

12. Podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.

13. Sredstvo za elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.

14. Sredstvo za varno podpisovanje je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena tega zakona.

15. Podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.

16. Sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.

17. Oprema za elektronsko podpisovanje je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.

18. Potrdilo je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje identiteto.

19. Kvalificirano potrdilo je potrdilo, ki izpolnjuje zahteve iz 28. člena tega zakona in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona.

20. Overitelj je fizična oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Po kazenskih določbah ZEPEP ob ugotovitvi prekrška se posameznika kaznuje z denarno kaznijo, ki pa so različne, in sicer po 47. členu ZEPEP.

V primeru, če je overitelj pravna oseba, se z denarno kaznijo od 208,64 € do 417,29 € kaznuje za prekršek tudi odgovorna oseba pravne osebe, ki je storila prekršek.

Elektronska izmenjava podatkov po Združenju bank Slovenije:

- Banka lahko za uporabo elektronskih komunikacijskih poti predpiše svoje splošne poslovne pogoje,

- Za varno elektronsko izmenjavo podatkov s stranko banka uporablja take zaščitne mehanizme, da lahko zanesljivo preveri identiteto nalogodajalca bodisi z uporabo enolične identifikacijske kode, ki jo dodeli imetniku transakcijskega računa, bodisi z uporabo podobnega načina preverjanja identitete. Banka in stranka se zavezujeta k doslednemu spoštovanju varnostnih ukrepov, ki jih zagotavlja čim manjše tveganje ne avtoriziranega pristopa k podatkov, za spreminjanje podatkov in izgubo teh,

- Banka mora seznaniti stranko z načini uporabe posamezne komunikacijske poti ter s priporočljivimi varnostnimi ukrepi z navodili za uporabo oziroma prek drugih medijev (npr. spletnih strani),

- Vsa elektronska sporočila med banko in stranko, posredovana po dogovoru in varno, veljajo za verodostojna in nepreklicna,

- Banka ne prevzema odgovornosti in škode zaradi morebitne izgube ali uničenja katerih podatkov in opreme uporabnika zaradi namestitve in uporabe elektronske komunikacijske poti,

- Banka krije morebitno škodo, ki bi jo stranki povzročile tretje osebe z vdorom v bančni informacijski sistem.

3.3 Storitve elektronskega bančništva

Zgodovinsko gledano smo do sedaj imeli tri poglavitne korake samopostrežnega bančništva. Prvi se je pojavil v sedemdesetih s bančnimi avtomati, nato je v osemdesetih sledilo telefonsko bančništvo, v devetdesetih pa poslovanje prek interneta.

3.3.1 Bankomati

Bančni avtomati so samopostrežni terminali, ki so povezani z nekim glavnim ali matičnim računalnikom. Z njihovo pomočjo lahko komitenti opravijo hitro in enostavno različna bančna opravila brez prisotnosti bančnega delavca. Prvotno so bili bankomati namenjeni le izdaji gotovine, sčasoma pa so prerasli v avtomate za poslovanje s plačilno-kreditnimi karticami, plačevanje računov in polaganje gotovine na račun, kar jih označuje za transakcijske avtomate oz. za samopostrežne kioske. Plačilo posebnih položnic, kot samostojna storitev na bankomatu, komitentom omogoča plačilo položnic s takojšnjim prejemom potrdila o izvedenem plačilu, je cenejša in uporabnikom na voljo 24 ur na dan

vse dni v letu! Za banke implementacija storitve pomeni racionalizacijo pri poslovanju, višjo stroškovno učinkovitost in dodatno ponudbo komitentom.

V prihodnosti bi bankomati lahko predstavljali informacijsko okno, kjer bi bil komitent povezan s spletnimi stranmi, preko info-terminalov pa bi potekale predstavitve in oglaševanje. Predstavljal bi prodajno okno, kjer bi bil komitent povezan s podjetji. Le-to bil bilo mesto za prodajo znamk, kinematografskih, letalskih ali železniških kart in avtobusnih vozovnic, mesto za plačilo dohodnine, plačilo raznih obveznosti na račune posameznih podjetij itd.

Bančni avtomati avtomatizirajo in s tem nadomeščajo delo blagajnika. Dela, ki jih je prej opravljal človek, ne opravljajo enako ampak boljše. Delujejo 24 ur na dan. Pri svojem delu so hitri, natančni, se ne zmotijo in ne utrudijo (Gradišar, Resinovič 1996, 365).

Uporaba bankomata je razmeroma zelo preprosta, slediti je potrebno le navodilom, ki nas vodijo skozi postopek posamezne storitve in pravilno vnesti številko PIN (Personal Identification Number). Medtem ko se slovenske banke še vedno trudijo prepričati stranke, naj uporabljajo bančne avtomate in s tem skrajšajo vrste pred okenci, v tujini vse več bank uporabo bančnih avtomatov tudi zaračuna. Za zaračunavanje se pogosteje odločajo manjše banke. Vzrok je seveda v stroških, ki jih imajo banke z bančnimi avtomati (Miš 1999, 37).

V Sloveniji smo prvi bankomat dobili leta 1990 in danes se je do njihovo število po podatkih Banke Slovenije povzpelo nad 1.000 kar je razvidno tudi iz spodnje tabele. V samem začetku poslovanja z bankomati se je njihovo poslovanje povečalo po 20 odstotkov letno, v zadnjih letih pa je to nekaj manj kot 20 odstotkov letno. V Sloveniji imamo trenutno 600 bankomatov na milijon prebivalcev, povprečje EU pa znaša 650 bankomatov na milijon prebivalcev. Naj omenim, da je v svetovnem merilu število bankomatov dosti višje in sicer znaša 1.300 bankomatov na milijon prebivalcev v ZDA, 1.000 na milijon prebivalcev na Japonskem in tudi v Španiji.

Tabela 3: Rast števila bankomatov v Sloveniji po obdobjih

Leto	Število bankomatov
2000	865
2001	1.027
2002	1.095
2003	1.240
2004	1.389
2005	1.456
2006	1.522
2007	1.643
2008	1.727

Vir: Bankart 2009. Upravljanje mreže bančnih avtomatov.

Naraščanje števila bankomatov pa je posledica številnih prednosti, ki so jih deležni njihovi uporabniki, med katere štejemo: 24-urno dostopnost do bankomatov, izognitev dolgim čakalnim vrstam pred bančnimi okenci ter zelo hitra in enostavna uporaba. Kot edino slabo lastnost bankomatov lahko omenim neoseben odnos do komitenta, kar povzroča, da zlasti starejši ljudje zelo malo uporabljajo bankomate.

3.3.2 Kartice

Plačilne kartice ali plastični denar so se, glede na vse novosti, ki jih doživljamo v zadnjih dveh dekadah, še posebej intenzivno pa zadnja leta, v svetu pojavile že zelo zgodaj, »davnega« leta 1950. Zaradi njihovih očitnih prednosti, število izdanih kartic v svetu nenehno narašča in je danes že preseglo 1,672 mrd (Vir: VISA). V Sloveniji smo jih začeli uporabljati že v 60. letih, resničen razmah pa so doživele v zadnjem desetletju, ko so na trgu začeli delovati tudi domači izdajatelji in ponudniki kartic. Tako je danes v Sloveniji v uporabi že preko 2,5 mio kartic (po podatkih Banke Slovenije jih je bilo do 31.3.2000 že 1.917.160).

Vsekakor v tem, da nam omogoča poravnavanje obveznosti brez gotovine ali zamudnega pisanja čekov, da nam v denarnici ni potrebno prenašati bolj ali manj zajetnih šopov bankovcev, odpadejo tudi problemi z drobižem, da bi poravnali znesek, ki se ne konča z okroglo številko in tudi problemi, kako priti do denarja, ko so bančne ustanove zaprte. Nekatere plačilne kartice nam omogočajo nakupe ali dvige gotovine tudi, ko na svojem računu začasno nimamo dovolj denarja, z nekaterimi pa lahko na preprost način najamemo kredit.

Plačilnih kartic je več vrst, ločiti pa se jih da po različnih kriterijih. Glede na to, da pri razvrstitvi in predstavitvah posameznih plačilnih kartic uporabljamo različne termine, jih na tem mestu na kratko pojasnjujemo.

Glede na izdajatelje se da plačilne kartice ločiti na:

- bančne kartice (izdajajo jih banke - v Sloveniji: večina bank),

- podjetniške kartice (izdajajo jih podjetja - v Sloveniji: večja trgovska podjetja),

- partnerske kartice (izdajajo jih podjetja v sodelovanju z bankami – v Sloveniji: MERKUR, ADRIA AIRWAYS, DELO, NAMA in druge),

- licenčne kartice (izdajajo jih banke ali podjetja v sodelovanju s podjetji v tujini, ki so nosilci kartic – v Sloveniji: kartice Eurocard/Mastercard, Visa, Diners, American Express).

Glede na funkcijo, ki jo plačilne kartice opravljajo ločimo na:

- predplačne kartice (lahko jih v naprej kupimo in po izrabi zavržemo - telefonske kartice ali pa jih v naprej napolnimo in jih nato uporabimo za plačevanje različnih storitev - telefon, parkirnina, cestnina, avtobusni prevoz),

- debetne kartice (kartice, vezane na tekoči račun, kjer nas izdajatelj kartice za nakup blaga oz. storitve oz. za dvig gotovine obremeni takoj – npr. BA in MAESTRO),

- kreditne kartice oz. kartice z odloženim plačilom (izdajatelj kartice nas obremeni s stroški nakupov oz. dvigi gotovine samo enkrat v mesecu, do plačila pa nas izdajatelj kreditira – primeri kartic: ACTIVA, VISA, EC/MC, DINERS CLUB),

- posojilne kartice (izdajatelji - banke oz. podjetja - nam z njimi omogočajo nakupe ali porabo gotovine na obročno odplačevanje – npr. posojilna KARANTA, posojilna VISA).

Danes je vse več kartic kombiniranih, saj združujejo več kot le eno funkcijo.

Plačilne kartice v najširšem pomenu nudijo dve temeljni storitvi:

- dvig gotovine in

- nakup blaga in storitev.

Dvig gotovine je v Sloveniji mogoče opraviti na bankah, izdajateljicah kartic, na poštah in prodajnih mestih z oznako «gotovina« ter na bankomatih z oznakami kartic, ki jih uporabljamo. V Sloveniji je največ avtomatov mreže BA in sicer že več kot 838.

Tabela 4: Storitvene možnosti poslovanja z kartico doma in po svetu

Doma:	V tujini:
dvig gotovine z BA dvig gotovine z Eurocard in VISA karticami vpogled v stanje na TR vstavitev ovojnice (v kateri je lahko gotovina, položnica, ali oboje skupaj) predplačilo storitev v mobilnih omrežjih Debitel, Mobitel in SiMobil	dvig gotovine dvig gotovine z Eurocard, Visa, American Express, Diners, JCB in še drugimi karticami vpogled v stanja na računih depozit zahtevek za zvišanje limita prenos sredstev med računi plačilo 'položnic' izdajo osebnih čekov internet storitve nakup vstopnic nakup poštnih znamk - HIT leta 1998 v ZDA nekatere druge storitve

Vir: MojDenar 2009.

Plačilne kartice v današnji družbi so postale skoraj nepogrešljiv sopotnik vsakega posameznika. Sodijo med elektronske plačilne inštrumente, kjer je mogoče plačilo opraviti le s pomočjo elektronskih terminalov, preko katerih se nalog za plačilo v elektronskem omrežju posreduje do banke, pri kateri ima imetnik plačilne kartice deponirana denarna sredstva. Tako banka na podlagi prejetega naloga izvede plačilo na ciljni račun (Trstenjak, 2003, 24).

3.3.3 Mobilno bančništvo

Mobilno bančništvo je precej sveža oblika elektronskega distribucijskega kanala bank, ki predstavlja preprost, učinkovit in od lokacije neodvisen način komuniciranja komitentov s banko. Z novimi tehnologijami se tako banke iz poslovalnic selijo tudi na mobilne terminale. S sodobno mobilno telefonijo imamo možnost dostopa do interneta in tudi do banke kar preko mobilnega telefona. Sem pa ne moremo vključevati le mobilne telefonske aparate, temveč tudi vse druge majhne prenosne naprave, kot so denimo prenosni in žepni računalnik ter izjemno majhni pametni telefoni, ki združujejo žepni računalnik, dlančnik in mobilni telefon (Vagaja 2000, 10).

Uporabniki lahko uporabljajo bančne storitve ne glede na kraj in čas, v katerem se nahajajo z uporabo mobilnega terminala. Sistem mobilnega bančništva lahko omogoča opravljanje skoraj vseh bančnih storitev, od ponujenih bančnih informacij, tečajnih list, informativnih izračunov, pregledovanju stanja in prometa na računu itd.

Vendar se storitve mobilnega bančništva ni vpeljala preveč dobro, ker uporabniki bančnih storitev imajo rajši drugačne, preprostejše načine dostopa do banke. To je razvidno tudi iz opravljenih raziskavah RIS-a, kjer so ugotovili, da je med domačimi gospodinjstvi 19-

odstotkov takih, ki dostopajo do interneta preko mobilnega telefona. Delež uporabe mobilnih telefonov v Sloveniji za dostop do interneta je srednje visok, kljub temu je še vedno nad povprečjem EU, kjer znaša le 6-odstotno. Wap bančništvo se nahaja v zgodnji fazi razvoja. V bodoče bo lahko z nadaljnjim tehnološkim razvojem in dodatno izboljšavo pridobilo na pomenu in postalo pomemben del elektronskega bančništva.

Wap je skupek protokolov, ki omogočajo celovit proces brezžične komunikacije za dostavo, pregled in uporabo spletnih strani na mobilni telefonih. Wap v večini mobilnih omrežij in je skladen z vsakim operacijskim sistemom (Ručigaj 2000, 10).

Vendar imamo danes že v uporabi mobilne terminale z GPRS storitvami (General Packet Radio Service), ki temelji na paketnem dostopu in hkratnem prenosu podatkov po več kanalih radijskega vmesnika. V tem primeru gre za hitrejši prenos podatkov in skrajšan odzivni čas, ki omogoča pravo mobilno poslovanje in s tem tudi mobilno bančništvo (Grobelšek 2001, 8).

3.4 Napake pri uvajanju elektronskega bančništva

Pri vsesplošnem navdušenju za elektronsko bančništvo pa se je tudi pokazalo, da niso vse banke ubrale prave razvojne smeri oziroma so napravile nekaj napak (Vozelj 1999, 74-75).

Zanašanje na počasnemu razvoju interneta temelji na ideji, da je internet le alternativa klasičnim načinom poslovanja, pri čemer imajo pogosto v mislih bančne avtomate, pri katerih je zelo dolgo trajalo, da so se prijeli, in tako zaključijo, da bo enako z internetom. Tak razvoj bi jim dal dovolj časa za prilagajanje. Take banke gledajo na to, da so uporabniki elektronskega bančništva predvsem mlajši bolj izobraženi uporabniki, ki si lahko privoščijo nakup opreme. Ti sicer res predstavljajo le manjši segment populacije, toda kmalu za tem so jim sledili tudi ostali uporabniki, pri čemer se bo izkazalo, da je čakanje slaba taktika, saj smetano poberejo tisti, ki so prvi.

Pri čakanju na rešitev sistemskih problemov pa banke čakajo, da drugi poiščejo rešitev za vse tehnične probleme, povezane z novo tehnologijo, t.i. pomisleke v zvezi z varnostjo, varovanjem osebnih podatkov, zasebnostjo, vprašanje pranja denarja, nudenje pomoč uporabnikom v težavah ipd. Pri tem menijo, da bodo lahko v določenem trenutku hitro prišli na trg s tem, da bodo tehnološke rešitve, ki so se pokazale kot dobre, enostavno kupili. Tudi ta strategija se ni izkazala za uspešno, saj so navadno banke zamudile prvi vlak elektronskega bančništva.

Nekatere banke pa so se odločile za tradicionalni marketinški pristop in sicer so se banke zanašale predvsem na svojo že uveljavljeno blagovno znamko, ki je v preteklosti še posebej v bančnem sektorju zagotavljala lojalnost strank. Vendar pa se je pokazalo, da je samo blagovna znamka v svetu interneta premalo, saj so internetni uporabniki na splošno precej nelojalni in so pripravljeni hitro pristopiti h konkurenci. Prav tako se ni dobro zanašati, da jih bo uporabnik sam opazil na internetu preko reklam in iskalnikov. Banka ne

sme komitentu prepustiti iskanja svoje ponudbe, ampak ga mora voditi. Razviti mora posebna marketinška orodja, prek katerih bo na internetu postala opazna in prepoznavna, sicer se lahko zgodi, da je stranke preprosto ne opazijo.

4 VARNOST ELEKTRONSKEGA BANČNIŠTVA

Spletno komuniciranje nam pri vsakdanji rabi ponuja številne prednosti in priložnosti, hkrati pa nas postavlja pred nova vprašanja glede varnosti. Banke, ki že dalj časa ponujajo uporabo storitev prek tega sodobnega medija, se dobro zavedajo informacijskih tveganj in zato z najsodobnejšimi tehnologijami zagotavljajo visoko stopnjo varnosti pri elektronskih komunikacijah s komitenti.

Banke uporabnikom svetujejo upoštevanje minimalnih standardov varnost spletnega načina poslovanja. Čeprav se uporabniki držijo teh standardov, pa lahko zaradi uporabe osebnega računalnika za druge namene v delovnem ali domačem okolju pride do zlorabe zaupnih podatkov, npr. gesla, PIN-a (osebna identifikacijska številka), digitalnega potrdila, številka kreditne kartice ipd. Banke spremljajo delovanje svojih sistemov in redno uvajajo ustrezne varnostne ukrepe, žal pa so ti učinkoviti samo, če tudi komitent pri uporabi svojega osebnega računalnika upoštevajo priporočila bank za zagotavljanje varnosti elektronskega poslovanja prek javnega omrežja. (Barle, Žibrat 2007, 3).

4.1 Varnosti standardi

Ko govorimo o elektronskem bančništvu, je nemogoče, da se ne bi podrobneje ustavili pri varnosti elektronskih sistemov. Zaradi povezanosti sistemov lahko en sam vdor v bančni sistem pusti katastrofalne ali celo nepopravljive posledice, proti katerim bi navaden bančni rop izgledal kot nedolžna praska. Zato se temu vprašanju upravičeno posveča velika pozornost, hkrati pa se morebitni varnostni spodrsljaj navadno zamolčijo v želji, da se ohrani zaupanje strank.

Pomembno je, da je zagotovljena varnost dostopa in uporabe kot varnost elektronskih transakcij, pri čemer je dobro, če lahko uporabniki sami vidijo, da je sistem varen in da se da to tudi dokazati.

Ker se transakcije v elektronski bazi izvajajo prek javnih komunikacijskih medijev je zaščita transakcij bistvenega pomena. Celovitost zaščite v elektronski banki se dosega tako, da se upošteva vse varnostne principe:

- pristnost- zagotavlja prejemniku, da je sporočilo res poslal pošiljatelj in da ni ponarejeno; uporaba digitalnih podpisov, certifikatov in gesel,

- avtorizacija- do podatkov lahko pride le tisti, ki je pooblaščen; uporaba imena in gesla, biometrična identifikacija,

- zaupnost- preprečuje nepooblaščeno razkritje podatkov; uporaba šifriranja, kriptografije, zaupanja vredne tretje strani,

- celovitost – podatki se pred prenosom ne spreminjajo; uporaba šifriranja in digitalnih podpisov,

- nezavrnitev – zaščita pred tem, da bi pošiljatelj lažno zanikal, da je podatke poslal, ali prejemnik lažno zanikal, da jih je prejel,

- nadzor pretoka – obrambni zid,

- tajnost – podatki so namenjeni le naslovniku in nikomur drugemu ni treba vedeti za prenos.

Dobra zaščita je v elektronski banki ključnega pomena, saj ji moramo zaupati tako komitenti (uporabniki) kot banke. V sodobnih bankah se zato navadno uporablja tehnologija pametne kartice kot podlaga za identifikacijo uporabnikov in digitalno podpisovanje transakcij na podlagi podpisanih zasebnih in javnih ključev.

Na splošno za varnostno opremo in varnostne mehanizme velja, da morajo ustrezati naslednjim zahtevam:

- celovitost in strukturiranost,

- vladni predpisi,

- standard.

Kljub vsem varnostnim ukrepom se število poskusov vdorov, goljufij in zlorab močno povečuje, strežniki večjih bank pa so skorajda dnevno priča napadom hekerjev. Še prav posebej so sistemi elektronskega bančništva primerni za pranje denarja in goljufije, saj je v večini primerov denar ali nesledljiv, izredno hiter ter zagotavlja kršilcu zakona anonimnosti.

Od tod danes izhaja dilema, ali ne bi bilo morda bolje zagotoviti sledljivost za vsaka uporabljen e-dolar, kar bi izničilo eno izmed prednosti e-bančništva – anonimnost.

To se prav gotovo sprašujejo preiskovalci na WTC in Pentagon 11. Septembra v ZDA, saj so napadalci redno uporabljali elektronsko bančništvo in z njegovo pomočjo z veliko hitrostjo preusmerjali denar čez več različnih kanalov, dokler ni prišel v roke teroristom. Ocenjujejo, da naj bi teroristi razpolagali s približno 600.000 USD, vendar so do sedaj našli in se prebili po transakcijski poti nazaj do vira le za okoli 325.000 USD (Risen 2002, 3).

Občasno so na omrežju in v računalniških revijah pojavljajo govorice, da naj bi hekerji katero izmed bank oropali za večje vsote denarja, vendar se praviloma izkaže, da je nemogoče preveriti tovrstne informacije, saj tako napadalci kot napadeni vztrajno molčijo. Po podatkih National Fraud Centra se le vsak stoti oškodovanec dejansko odloči obvestiti javnost o svoji izgubi. V luči tega podatka dobijo navidezno nizke številke.

4.2 Nevarnosti elektronskega bančništva

Nevarnosti, da stvari ne bodo potekale tako, kot bi morale, je več. Nekatere so rezultat namenskega delovanja, kot so recimo napadi hekerjev, druge pa so predvsem posledica nezanesljive opreme, ki odpove takrat ko ne bi smela.

Razlika je tudi v namenu in načinu delovanja kršilcev zakonov, saj v večini primerov poskušajo ogoljufati naivne ljudi, saj je to precej preprosteje, kot pa poskušati vdreti v elektronsko banko, ki je zaščitena z vsemi varnostnimi mehanizmi.

Medtem ko nedelujoča oprema navadno povzroča le stroške, se hekerji spravijo nad bančne sisteme z drugačnimi nameni. Po stereotipu gre za izobražene blede mladiče, ki cele dneve gledajo v računalniški ekran in obvladajo skrivnosti programskih jezikov do najmanjših podrobnosti. Proti njim so tudi naperjeni varnostni mehanizmi, saj predstavljajo največjo nevarnost.

Virusi pa lahko povzročijo v sistemih bank in podjetij ogromno škodo, saj se bliskovito širijo in imajo pogosto uničujoče posledice. Obstaja ogromno različnih virusov. Nekateri vam bodo ukradli številko kreditne kartice, če jo imate spravljeno v datoteki, drugi bodo prisluškovali početju na računalniku, čakajoč na uporabniška imena in gesla, spet tretji se bodo lotili formatiranja trdega diska ali pa celo uničevanja strojne opreme. Vsem pa je skupno to, da se bodo poskusili razširiti na vse dosegljive računalnike in da so navadno izdelovalci zaščite vedno korak za avtorji.

Občasno se zgodi, da kakšen del strojne opreme odpove in ogrozi delovanje celega sistema. Najpomembnejši del strojne opreme so bančni strežniki in njihovi trdi diski, saj morajo delovati neprekinjeno brezhibno. Za vsak slučaj se vedno dela varnostne kopije podatkov, da se v primeru izgube lahko vzpostavi prvotno stanje.

Nevarnost lahko preži tudi v primeru ko imamo nezanesljivo programsko opremo. Nekateri uporabniki imajo računalnike starejše izdelave in pogosto uporabljajo tudi starejšo programsko opremo, ki ne podpira vseh modernih varnostnih standardov. Posebej je to očitno pri internetnih brkljalnikih, kjer starejši programi ne podpirajo dovolj visoke stopnje kriptografije za zaščito pred današnjimi močnimi računalniki.

Pred večjim razmahom dostopa prek najetih linij je večina komitentov dostopala do svojih bank prek modema in klicnih linij, ki pa so razmeroma nezanesljive, saj se je pogosto dogajalo, da so uporabniki padali z linij. Vzrok so slabe linije in zastarele centrale. V zadnjem času se povečuje število uporabnikov, posebej podjetij, ki imajo najete linije, ki so precej bolj zanesljive.

V zadnjih letih pa so se tudi pojavili primeri, ko so se banke pojavljale z zvenečimi imeni, ki so bila nadvse podobna imenom uveljavljenih in znanih mednarodnih bank. Te banke so pogosto obstajale samo na internetu na domenah majhnih otočkov v samostojnih državicah s povsem svojo zakonodajo in z očitnim namenom, da se izognejo pretirano radovednim državnim organom. Neprevidni poslovneži so na primer nasedli European Union Bank iz

Antigue ali Rotschild International Ltd. Iz Kamajskih otokov, ki so potem, ko so jih ogoljufale za velike vsote denarja, na hitro poniknile in pustile kliente na cedilu.

4.3 Varnosti ukrepi

Zelo pomembno je, da se zavedamo, da so zlorabe možne, da poznamo nevarnosti, ki prežijo na nas pri e-poslovanju, predvsem pa , da se znamo pred njim zaščititi in upoštevati pravil varovanja.

Poznamo pa dvanajst zlatih pravil za varno elektronsko poslovanje:

1. Varujte podatke, ko jih pošiljate po odprtih komunikacijskih poteh; splošno pravilo je, da se po odprtih komunikacijskih poteh občutljivi in zaupni podatki (geslo, PIN, digitalno potrdilo, številka kreditne kartice ipd.), če niso zaščiteni, ne pošiljajo (podatki so zaščiteni takrat, ko se v oknu brskalnika pojavi ikona zaklenjene ključavnice). Ne pozabite: ko ste na spletu, lahko spreten zasledovalec vašega dela pridno spremlja vse vaše aktivnost. Prav tako lahko razbere, v katerem območju IP naslov je vaš računalnik. Vaš osebni računalnik ima svojo edinstveno številko (IP številko), ki vas, ko ste priključeni v spletu, enoznačno označuje in je vedno dostopna vsakemu spletnemu uporabniku.

2. Prepričajte se s kom elektronsko komunicirate; pozorno preglejte spletno stran, ali je res taka, kot ste je vajeni (naslov se začne z nizom https://..., v oknu brskalnika je ikona zaklenjene ključavnice ipd.). Zlikovci namreč lahko ponaredijo spletno stran in prek nje zahtevajo vnos naših zaupnih podatkov (npr. Digitalno potrdilo, ...), po katerih vas vaša banka sicer nikoli ne povpraša. Če torej na spletni strani nekdo od vas zahteva katerega od zaupnih osebnih podatkov, potem je to že znamenje, da je stran lažna, zato jo takoj zapustite.

   Prek take lažne strani bo »ponudnik bančne storitve« brez težav dobil naše zaupne podatke, saj smo jim ponudili sami. Velika verjetnost je, da bo tako pridobljene podatke nato zlorabil.

   Zato je pomembno, da zanesljivo preverite, ali je spletna stran prava. Vedno se moramo prepričati, ali smo resnično povezani po zaščiteni komunikaciji-SSL. Identiteto bančnega strežnika pa preverimo z dvoklikom na zaklenjeno ključavnico v spodnjem delu brskalnika. Tako si lahko ogledamo podrobnosti o varni povezavi z našo banko, še preden bomo vnesli podatke, ki so sicer nujni za spletno poslovanje z banko (npr. geslo).

3. Skrbno ravnajte z občutljivimi podatki in pozornost na medije za pristop;

   Skrbno ravnanje z občutljivimi podatki, ki so shranjeni na prenosnem mediju. Hramba občutljivih podatkov na teh medijih ni varna, če npr. puščamo disketo v disketni enoti, pametno kartico v čitalniku, generator gesel ali druge medije v dosegu nepooblaščenih oseb. Zato nikoli ne posredujte ali prepustite svojih zaupnih podatkov za pristop do

bančnih spletnih strani tretjim osebam. Za družinske člane in pooblaščence obstajajo sistemi ločeni in sledljivi pooblastil tudi za uporabo v elektronskih bankah. Še več. Sami moramo skrbeti, da nepooblaščena oseba nima dostopa do našega digitalnega potrdila in zasebnega ključa ali gesel.

Digitalno potrdilo in zasebni ključ lahko hranite na disku, pametni kartici ali na spominskem ključu USB. Če je le mogoče, ne shranjujte podatkov (gesel, PIN, digitalno potrdilo, ...) na trdi disk. Temu se še posebno izogibamo, če za elektronsko poslovanje uporabljamo službeni računalnik, ki ga delimo s sodelavci.

Če posumimo, da je bilo naše digitalno potrdilo zlorabljeno, oz. če ste ga izgubili, o tem moramo nemudoma obvestiti overitelja, ki je digitalno potrdilo izdal in svojo banko, ki bo potrdilo takoj blokirala. Če že imamo digitalno potrdilo shranjeno na disku računalnika, ga zavarujemo z geslom. Digitalnega potrdila na nikakršno zahtevo ne izvažamo in nikomur ne posredujemo gesla, s katerim je digitalno potrdilo zavarovano.

Če za hranjenje digitalnega potrdila uporabljamo pametno kartico ali spominski ključ USB, ju ne vstavljamo v čitalnik/računalnik pred začetkom dela s spletno banko. Tako bomo preprečili vzpostavitev neželene komunikacije. Hrambi kartice, generatorja gesel ali spominskega ključa USB namenimo posebno pozornost, da ne bi prišlo do odtujitve.

4. Izberimo varno geslo; Za vstop v spletno banko se morate najprej prijaviti v splet. Ob prijavi se identificiramo z digitalnim potrdilom, geslom ali kombinacijo obeh. Pri prvi prijavi v spletno banko si bomo morali določiti svoje osebno geslo oz. uporabniško ime za vstop v spletno banko. Nadvse pomembno je, da gesla in uporabniški imeni nikamor ne zapišemo, temveč si jih poskušamo zapomniti.

   Geslo in uporabniško ime naj bosta sestavljeni tako, da ju bo težko uganiti in bosta edinstveni. Dovolj zanesljivo geslo je navadno dolgo šest do devet znakov in je kombinacija velikih in malih črk ter številk in posebnih znakov. Pri izbiri gesla se izogibajte priljubljenim in pogosto uporabljenim pojmom zlasti v delovnem okolju, lastnega imena in kombinacij z rojstnimi datumi, ponavljanju enega znaka ali uporabi znakov v zaporedju na tipkovnici. Geslo spremenimo na določeno časovno obdobje. Če sumimo, da geslo kdo poskuša odkriti, ga takoj moramo spremeniti.

5. Uporabljamo programsko opremo, ki ima uradno licenco; Ne prenašajte programske opreme s spletnega naslova, če ni popolnega zagotovila, da ste prenos in njeno delovanje varna ter verodostojnost pošiljatelja neoporečna. Pri postopkih prenašanja s spleta je mogoče, da boste hkrati s programsko opremo prenesli tudi virus, trojanskega konja ali celo skriti spletni naslov.

6. Uporabljamo najnovejše različice programske opreme; Uporabljamo samo najnovejše različice operacijskega sistema in druge programske opreme. Samo najnovejše različice programske opreme lahko zagotavljajo visoke varnostne standarde.

Izdelovalci programskih rešitev nenehno izboljšujejo svoje izdelke. Pomembno je, da poskrbimo, da so novosti, zlasti nove različice protivirusnih programov, sproti nameščene na računalnik, s čimer zmanjšate verjetnost morebitnih zlorab.

7. Ne zanemarjamo varnostnega preverjanja; Pri uporabi elektronske pošte ne odpiramo pripetih datotek, če nam pošiljatelj elektronskega sporočila ni znan. Če pa vseeno nameravamo pregledati prejeto pošto, je najbolje, da jo shranite in vsebino pred aktiviranjem preverimo z varnostnim programom. To še posebej velja za zvočne zapise in slike. V obeh tipih datotek so lahko skrite prevare. Skrivanje sporočil in programja v avdio in video zapise je poseben izziv za računalniške zlikovce. Kopiranje programske opreme (datoteke s končnico .exe) kot tudi prenašanje neplačljivih programov s spleta se šteje za veliko varnostno tveganje.

   Preden se povežemo s spletno banko, pozorno izvedemo varnostne postopke in aktiviranje antivirusnih programov.

   Če storitve spletnega bančništva uporabljamo v domačem ali službenem računalniku, ki ga delimo z drugimi osebami, poskrbimo za to, da se mora vsak uporabnik prijaviti s svojim uporabniškim imenom in geslom. Najvarneje, je da pred uporabo spletne banke opravimo postopek za začetek delovanja in po končani uporabi postopek za zaključek delovanja (prijava v računalnik/odjava z računalnika). S tem boste zanesljivo počistili za sabo vse začasne datoteke. Najmanj kar lahko naredimo za varnost, je da po končani uporabi spletne strani sami zapremo svoj brskalnik. S tem bomo tistemu, ki bo uporabljal za nami, onemogočil, da bi uporabljali naše spletne naslove ali celo prepoznal uporabljena gesla.

8. Vklopimo varnostne nastavitve spletnega brskalnika; Naš brskalnik je mogoče z ustreznimi nastavitvami varnostno izboljšati. Za res varno delo s spletno banko je najbolje izklopiti samodejno aktiviranje ActiveX kontrole. Prav tako je priporočljivo izključiti samodejno shranjevanje nastavitve spletnega brskalnika. Ta funkcija shranjuje nastavitve in zato tudi imena in gesla, ki smo jo pred tem uporabljali. Te funkcije lahko uporabimo le pri zaupanju vrednih spletnih staneh, kot je stran naše banke.

   Pri delu s spletom se srečamo tudi s tako imenovanimi piškoti. V piškotke spletni brskalnik pri brskanju po spletu zapisuje sporočila, tako da z njihovo pomočjo računalnik hitreje najde že obiskano spletno stran. To beleženje ima tudi svojo slabo stran. Podatki v piškotih, poslani na strežnik, se lahko zlorabijo za nepredvidene namene, zato jih je po končanem delu pametno zbrisati.

9. Namestimo na računalnik lovce virusov in dodatno zaščito programske opreme; Operacijski sistem ne zagotavlja vseh varnostnih postopkov, zato je treba namestiti dodatno zaščitno programsko opremo. Eden od pomembnih dodatnih stražarjev, ki nikakor ne bi smela manjkati na našem računalniku je redno posodobljeno orodje za odkrivanje virusov-protivirusni program.

Brez aktivne varnostne zaščite lahko neznani zasledovalec vašega dela neopazno namesti program za samodejno vohljanje in sporočanje. Lahko ga namesti celo na spletno stran, ki jo pogosto uporabljamo in zato ne opazimo drobnih sprememb na njej. Tako neopazno posname številko bančnega računa, številko bančne kartice ali geslo in jih odpošlje na samo njemu znan elektronski naslov.

V kakovostno varnostno programsko opremo sodi tudi požarni zid. Ta ves čas nadzira vse vhodne in izhodne informacije na našem računalniku ter dovoli samo znane in avtorizirane povezave.

10. Redno arhiviranje pomembne podatke; Sprotno in dosledno arhiviranje za vas pomembnih podatkov je eno od zlatih pravil varnega dela z računalnikom. Izguba podatkov, ki jih včasih celo ni mogoče več preklicati, je lahko zelo boleča izkušnja. Za shranjevanje podatkov si izbirate izmenljivi disk, spominski ključ USB ali zgoščenko.

    Ni tako zelo pomembno, za kateri medij se odločite, pomembneje je, da podatke shranjujete redno, da preverimo, kar smo shranili, in da na koncu arhivskih medij shranimo na varno mesto, ki ni dostopno nepooblaščenim osebam. Shranjevanje podatkov je še posebno pomembno, ko prepustite računalniku serviserju.

11. Za varnost poskrbite tudi pri vzdrževanju računalniške opreme; Ob okvarah računalniške opreme se za pomoč obrnite na preverjanje in usposobljene servisne službe.

    Če na našem računalniku hranite zaupne osebne podatke, s katerimi se lahko prijavite na spletne bančne storitve, jih pred predajo računalniške opreme servisni službi ali podjetju začasno shranimo na prenosni medij in jih na našem računalniku izbrišemo.

    Po odpravi okvare in prevzemu računalniške opreme lahko zaupne osebne podatke ponovno namestimo na naš računalnik.

12. Redno preverjanje stanje na našem bančnem računu; Sprotno in dosledno preverjanje stanje in transakcije na našem bančnem računu, s čimer lahko pripomoremo k hitremu odkrivanju morebitnih neskladij.

    Velika ponudba povezav v svetovni splet in njihova enostavna uporaba sta omogočili široko dostopnost informacij in najrazličnejše nove storitve, tudi spletno bančništvo. Poslovanje prek spleta je vse bolj priljubljeno zaradi svojega 24-urnega delovanja oz. priročnost in enostavnost uporabe. Vendar pa so z njim povezane tudi nekatere nevarnosti. Zato je nujno, da se kot uporabnik e-storitev zavedete pomena nenehne skrbi za varnost poslovanja. Z upoštevanjem zlatih pravil varovanja in samozaščite bomo bistveno manj izpostavljeni možnim zlorabam.

4.4 Poglavitni varnostni mehanizmi

Med temeljne rešitve za varno elektronsko poslovanje uvrščamo: požarno pregrado, overjanje, varnostno kartico, digitalni podpis in šifriranje.

Požarna pregrada ali firewall

Pri požarnem zidu gre za celovit sklop opreme, ki tvorijo komunikacijske naprave in računalnik. Bistvo požarnega zidu je v tem, da prepreči dostop nepooblaščenim osebam ali osebam iz privatnega omrežja. Vsa sporočila, ki pridejo iz privatnega omrežja, gredo skozi inštaliran požarni zid, ki ta sporočila pregleda in jih v primeru neizpolnjevanja varnostnih pogojev izloči. Obrambni zid lahko nadzira dostop do določenega omrežja na dva načina:

- Dopusten način (Permissive access), ki dovoljuje vse, razen tveganega prometa,

- Restriktiven dostop (Restrictive access), ki pa ne dovoljuje ničesar, razen strogo dovoljenega prometa.

Požarne zidove lahko uvrščamo med najbolj razširjene varnostne mehanizme, saj jih zasledimo skoraj pri vseh slovenskih bankah.

Overjanje

Pri dostopu na varovani sistem mora uporabnik ustrezno overiti, kar pomeni, da mora dokazati svojo verodostojnost. Gre za postopek, kjer skušamo ugotoviti, kdo dostopa do določenega omrežnega vira. Najbolj pogosta načina identifikacije uporabnikov sta identifikacija z uporabniškim imenom in geslom. Tovrstni sistem overjanja pa zasledimo skoraj pri vseh slovenskih bankah zaradi njegove praktičnosti, enostavnosti in preglednosti nad trenutnimi uporabniki posameznega sistema.

Varnostna kartica

Za ugotavljanje istovetnosti uporabnikov so potrebna gesla, kakor sem že omenila pri overjanju. Gesla pa ljudje zelo pogosto pozabljamo ali pa nam grozi možnost zlorabe gesla s strani druge osebe. Zato imamo danes rešitev na obe zgoraj omenjeni težavi izdelane posebne kartice, ki vsako minuto tvorijo novo geslo in so sinhronizirane z računalnikom, ki to geslo preverja. Vpis tega gesla omogoči nemoten dostop do strežnika banke (Bradeško 1998,76). Ta sistem velja za enega najboljših, hkrati pa tudi najbolj praktičnih načinov overjanja. Zato je uporaba varnostih kartic zelo razširjena tudi med slovenskimi bankami in sicer lahko njihovo uporabo zasledimo pri naslednjih bankam: Novi Kreditni banki Maribor, PBS, Gorenjski banki, Banki Koper, Probanka in Novi ljubljanski banki.

Digitalni podpis

Digitalni podpis nam zagotavlja pristnost sporočil. Preprečuje spreminjanje in zlorabljanje sporočil, tako da zagotavlja, da podatek med banko in njenim komitentom ostane

nespremenjen. Digitalni podpis predstavlja elektronsko različico lastnoročnega podpisa, s katerim komitent zagotavlja:

- avtentičnost dokumenta,
- avtentičnost podpisa,
- Istovetnost imetnika digitalnega podpisa,
- Neizpodbitno lastništvo poslanih podatkov,
- Celovitost sporočila.

Digitalno potrdilo vsebuje zasebni in javni ključ za podpisovanje. Zasebni ključ je znan le lastniku potrdila. Zato ker uporabnik podatke podpiše z zasebnim ključem, mora zelo dobro poskrbeti za varnost svojega zasebnega ključa, ki ga uporablja za preverjanje digitalnega podpisa.

Kiptografija ali šifriranje

Kiptografija je veda o šifriranju oz. zakrivanju sporočil. Šifriranje omogoča zakrivanje sporočila, tako da jih morebiti prisluškovalec ne more razbrati. S tem postopkom pretvorimo sporočilo v obliko, ki je nemogoča za razumevanje, tajnopis. V tajni obliki potuje sporočilo od pošiljatelja pa vse do prejemnika sporočila. Prejemnik pa to sporočilo dešifrira in ga pretvori v njegovo prvotno obliko. Pri šifriranju podatkov in sporočil se uporablja ključ. Ta predstavlja določene vrednosti algoritma, ki spremeni sporočilo v kodirano sporočilo. Kriptografija je eden izmed najbolj razširjenih varnostnih mehanizmov med slovenskimi bankami poleg že omenjenih požarnih zidov. Ločimo dve temeljni vrsti šifriranja sporočil:

- Simetrično šifriranje; uporabljamo za šifriranje in dešifriranje isti ključ. Sporočilo, ki je šifrirano z enim simetričnim ključem, je lahko dešifrirano le z enakim simetričnim ključem. Tako šifriranje sporočil pa je varno, dokler ključ ne odkrije neka druga oseba in v tem primeru lahko nastopi zloraba podatkov. Problem pri tovrstnem šifriranju podatkov je v veliki verjetnosti zlorabe omenjenega mehanizma. Zato se večinoma uporablja za šifriranje podatkov asimetrično šifriranje.

- Asimetrično šifriranje; Pri asimetričnem šifriranju podatkov gre za uporabo sistema dvojnih ključev. Pri tem sistemu ključ za šifriranje sporočila in ključ za dešifriranje sporočila nista enaka. Ključi nastopajo v parih in najpomembnejša lastnost tovrstnih ključev je v tem, da iz enega ključa, brez poznavanja dodatnih informacij, ni mogoče določiti drugega. Zato lahko v tem primeru en ključ javno objavimo. Objavljeni ključ imenujemo javni, ostali ključ pa zasebni (Jerman, Blažič 2001, 103). Omenjeni način šifriranja podatkov zasledimo pri Gorenjski banki, Raiffeisen Krekovi banki, SKB, PBS in v Unicredit bank.

Banke imajo na razpolago različne varnostne mehanizme za zagotavljanje varnega in nemotenega poslovanja preko njihovih sistemov. V večini primerov lahko zasledimo, da slovenske banke ne uporabljajo le enega varnostnega mehanizma, temveč poskušajo izkoristiti sinergijo različnih mehanizmov in tako zagotoviti višjo stopnjo varnosti pri ponujenih storitvah. Torej varnostni mehanizmi se ne izključujejo med seboj, temveč se odlično dopolnjujejo.

4.5 Tveganje v bankah

Pri storitvah elektronskega bančništva se banke soočajo z različnimi vrstami tveganja. Zato je temeljnega pomena poslovanja banke, da imajo izdelane natančne rešitve za varno elektronsko poslovanje. Banke se uspešno nadzorujejo različne vrste tveganj ob uporabi zgoraj naštetih varnostnih mehanizmov.

Vrste tveganj, s katerimi se srečujejo banke, in izdelane rešitve: Pri tveganju vdora v sistem banka uporablja požarni zid, ki sproti registrira število pristopov in število (neregistriranih) poskusov udora. Ta podatek nam omogoča oceniti tudi minimalno verjetnost za vdor skozi požarni zid, vendar ta ne more zaustaviti poskusa vdora, če ga predhodno ne registrira, in s tem se dejanska verjetnost vdorov avtomatično poveča. Za preverjanje stopnje tveganja se predvidijo aktivnosti za verifikacijo dejanske zaščite, in hkrati tudi učinkovitost preprečevanja dostopa do posameznih PC-jev.

Tveganje zaradi ne odzivanja na želje komitentov po informacijah ali osebnih stikih: v tem primeru banka izdela sistem skrbništva in nadzora nad skrbništvom. Tako omogoča komitentom dostop do informacij in želenih osebnih stikov. Statistika odprtih napak da oceno za tovrstno tveganje.

Tveganja zaradi namerno ali nenamerno nepravilno usmerjenih transakcij elektronskega bančništva: Pri tovrstnem tveganju banka verificira transakcije, sproščanje transakcij na ravni celotne banke. Vendar je potrebno predhodno opraviti ponovno avtomatsko kontrolo na pozitivno stanje na računu in avtomatsko kontrolo pravilnosti sklica. V primeru odkritja neavtorizirane inicirane transakcije, (ki je lahko v breme ali dobro) storjene mimo uporabniške zaščite, je še vedno na razpolago neko minimalno časovno obdobje, v katerem lahko komitent odkrije in takoj zahteva od banke blokado vseh transakcij. Omenjeno tveganje odkriva statistika tovrstnih problemov.

Tveganja pri uporabi storitev elektronskega bančništva preko interneta: v tem primeru ima banka na voljo dva različna pristopa za preprečitev ali zmanjšanje tovrstnega tveganja. Lahko uporablja kontrolo poslovanja svojih komitentov na transakcijskih računih, druga alternativa pa je v oblikovanju posebnih rezervacij glede na višino odobrenih limitov na transakcijskih računih.

Banka Slovenije priporoča vsem bankam, ki se ukvarjajo z elektronskim poslovanjem, naj skrbno izdelajo varnostno politiko, metodologijo možnih tveganj, privzeto servisno tehnično kulturo ter naj upoštevajo vse standarde, sprejeta merila kakovosti računalniških rešitev, varnostnih sistemov in priporočil za varnost ter kakovost na področju elektronskega poslovanja.

5 ELEKTRONSKO BANČNIŠTVO V SLOVENIJI

5.1 Razvoj E-bančništva v Sloveniji

Elektronsko bančništvo z velikimi koraki prihaja tudi v Slovenijo in danes si je skorajda nemogoče zamisliti moderno banko, ki ne bi ponujala svojih storitev tudi prek interneta. Če je še leta 1998 le tretjina anketirancev vedela, da je mogoče oditi na banko tudi prek domačega zaslona, se jih danes zanima za tovrstno storitev že 75% (RIS 2002).

Temu trendu so sledile tudi slovenske banke, ki so v minulih letih bistveno izboljšale svojo ponudbo in za nekajkrat povečale število uporabnikov e-bančništva. Večina se jih je tega lotila z lastnimi močmi in pomočjo slovenskih zunanjih sodelavcev in pri tem naletela na nemalo težav. Mnoge bi se dalo rešiti, če bi bilo med bankami več sodelovanja, posebej pri določanju standardov.

Na začetku je ponudba obsegala le informativne izračune kreditov in nekatere osnovne informacije, vendar so se kmalu po vzoru modernih bank pojavile tudi storitve z neposrednimi, interaktivnim dostopom bančnega računa, tako da danes lahko rečemo, da danes s tega vidika slovenske banke povsem konkurenčne marsikateri večji uglednejši banki.

5.2 Ponudba slovenskih bank

Slovenske banke ponujajo številne transakcije in informacijske storitve. Med slednje štejemo informacije o stanjih, dogajanjih na kapitalskih trgih, obrestnih merah, pogojev za pridobitev posojil in potrebni dokumentaciji za pridobitev posojila. Tako danes ponujajo slovenske banke fizičnim osebam različne storitve (Interno gradivo Banka Koper 2008, A-banka 2008):

- Vpogled stanja na računu,
- Možnost izpisa izpiskov po datumu,
- Plačilo obveznosti prek posebne položnice ali splošne položnice BN-02,
- Prenos sredstev med računi znotraj banke in na druge banke,
- Naročilo in blokada čekov,
- Zahtevek za izdajo limita na računu in plačilni kartici,
- Napoved dvigov večjih zneskov gotovine,
- Zahtevek za nakazilo in prevzem gotovine prek sistema Western Union,

- Vezavo depozitov in prekinitev podaljšanja vezave depozitov,
- Sklenitev, polog in napoved dviga z varčevalnega računa z odpovednim rokom,
- Naročilo obrazcev za različno vrsto posojil,
- Prijava izgube vseh vrst kartic,
- Izmenjava sporočil z banko,
- Priprava podatkov za nakazila z valutacijo vnaprej,
- Priprava osebnega imenika prejemnikov in plačnikov,
- Odpiranje in ukinitev trajnih pooblastil,
- Aktualni borzni komentar,
- Vpogled v portfelj vrednostnih papirjev.

Pravne osebe imajo preko sistemov elektronskega bančništva v Sloveniji poleg smiselno izbranih zgornjih storitev možnost opravljati še naslednje storitve (NLB 2008, Interno gradivo, Abanka 2008, Interno gradivo):

- Posredovanje plačilnih nalogov s tekočim datumom ali datumom valute vnaprej,
- Posredovanje plačilnih nalogov za devizna nakazila,
- Pregledovanje tekočega stanja, tekočega prometa, izpiskov in obvestil o prilivih iz tujine,
- Uvoz/izvoz podatkov v/iz datotek v formatih za domači oziroma devizni plačilni promet,
- Pregled tečajnih list,
- Avtomatizirano izmenjavo podatkov med računovodskim programom podjetja in banko 8AIP),
- Pripravo podatkov za statistiko BS,
- Pregled obvestil o zavrnjenih nalogih,
- Vpogled v status obdelave plačilnega naloga.

Banke pravijo, da komitenti spletne banke največkrat uporabljajo za plačevanje različnih položnic, spremljanje stanja in prometa na tekočem računu. Čedalje bolj pa se uveljavlja tudi sklepanje pogodb za različne bančne storitve, kot so recimo vezava denarja, izdajanje naročil za odobritev izrednim limitov, kupovanje v spletnih trgovinah.

Banke iz leta v leto opažajo povečano zanimanje za spletno bančništvo in rast števila novih uporabnikov. Po podatkih ki so nam jih posredovali, je delež uporabnikov spletnega bančništva od 12 do 30 odstotkov tistih, ki imajo odprte tekoče račune, v Unicredit v Volksbank pa navajajo, da jih 40 odstotkov. Po podatkih, ki nam jih je uspelo pridobiti, ima največ uporabnikov, okoli 180 tisoč, NLB oziroma njihov NLB KLIK. Banke pa opažajo še eno zanimivost in sicer, da se za uporabo spletne banke odloča čedalje več upokojencev oziroma starejših ljudi.

Tudi uradni podatki Banke Sloveniji kažejo na povečanje število uporabnikov spletnih bank. Konec leta 2007 jih je dobrih 400 tisoč, lani aprila pa že 463 tisoč. Toda po drugi strani anketni podatki projekta Raziskave interneta Slovenije (RIS) že deset let kažejo precej manjše število aktivnih uporabnikov, v letu 2008 kar za četrtino manj, kot kažejo uradni podatki Banke Slovenije.

Podatki RIS se povsem ujemajo s podatki Evrostata, po katerih Slovenija po uporabi spletnega bančništva izrazito zaostaja za povprečjem EU- 27, skoraj za 50 odstotkov. V Sloveniji je namreč v populaciji od 16-74 let le dobrih 20 odstotkov uporabnikov spletnega bančništva, v EU-27 pa v povprečju že približno 30 odstotkov, opozarja Vasja Vehovar , vodja projekta RIS na fakulteti za družbene vede v Ljubljani, in dodaja, da trend zadnjih let tudi nakazuje, da se razlika oziroma zaostajanje Slovenije celo povečuje.

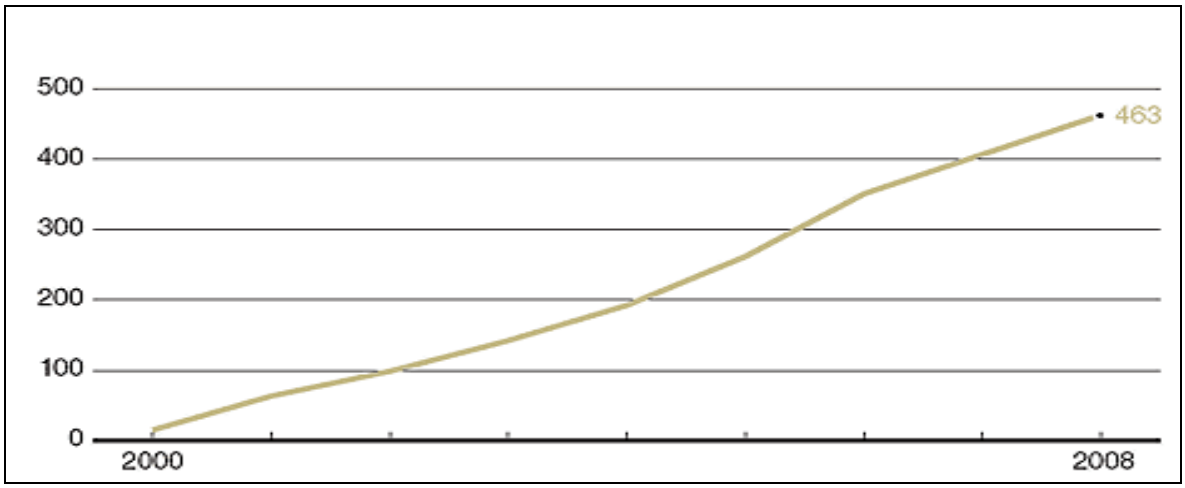
V najnovejši raziskovani RIS e-Bančništvo 2009 so analizirali razloge za tak zaostanek. Gre za dejavnike, ki so vezani na položaj in širši kontekst storitev informacijske družbe v Sloveniji ter ovir za njihovo uporabo. Storitve so v Sloveniji med uporabniki sicer dobro sprejete in tudi zadovoljstvo s storitvami spletnega bančništva je izjemno veliko. Težave so okolje in vstopne ovire za neuporabnike, pravi Vehovar. (Mojeuro 2009)

Tabela 5: Število uporabnikov spletne banke v Sloveniji

ŠTEVILO UPURABNIKOV SPLETNE BANKE	
Banka Koper (i-net)	33.000
Gorenjska banka (Link)	9.000
Hyp Alpe-Adria Bank (HYPOnet)	12.000
NLB (NLB Klik)	180.000
PBS (PBS.net)	5.100
SKB (SKB Net)	63.000

Vir: Moj evro 2009.

Slika 4: Število uporabnikov spletnega bančništva v Sloveniji (v tisočih)



Vir: Moj evro 2009.

5.3 Problemi, ki so se pojavili pri uvajanju elektronskega bančništva

Problemi, ki so se pojavili pri razvoju so precej predvidljivi, kar pa ne pomeni, da so bili lahko rešljivi. Izkazalo se je, da je eden največjih problemov dobiti ustrezen kvaliteten kader, ki bo sposoben voditi razvoj tako pomembnega in velikega projekta. Pri tem so bila potrebna predvsem računalniška znanja, obogatena s poznavanjem delovanja bančnega trga in bančnih storitev. Banke so si pri tem pomagale predvsem z zunanjimi sodelavci, vendar je treba imeti ustrezne ljudi tudi znotraj banke. Še danes lahko človek z ustreznim računalniškim znanjem hitro dobi službo v večini slovenskih bank.

Večina slovenskih bank je imela sredi 90-ih let zastarelo, nezanesljivo in neustrezno opremo, ki je včasih povzročala probleme tudi pri klasičnem poslovanju. Predvsem so manjkali zmogljivejši strežniki in pa zanesljiva programska oprema, kar pa ni bila vedno krivda bank. Danes so sektorji elektronskega bančništva v vseh bankah med najbolje opremljenimi, saj je to edini način, da nudijo kvalitetne storitve.

Za elektronsko bančništvo je potrebna povezava med banko in uporabniki, ki je v večini primerov potekala preko prastarih telefonskih kablov, za katere ni nihče mislil, da jih bodo uporabljali za prenos podatkov na ta način. Prav tako so za telefonijo in za medmrežne storitve veljale sorazmerno visoke cene.

Z izjemo največjih treh, štirih bank so vse ostale izrazito majhne in običajno zgolj lokalno usmerjene. To pogosto pomeni relativno malo denarja za razvoj in tudi preveč omejeno število strank, ki bi storitve uporabljale. Za take banke je razvoj elektronskega bančništva izredno draga zadeva.

Razvoj sistemov je bil povsem nepovezan in prepuščen posamezni banki, rezultat te politike pa je kar osem tehnično različnih in bolj ali manj nezdružljivih storitev

elektronskega bančništva. Glavni krivec je centralna banka, ki je namero predpisati enotno obliko poslovanja že pred časom opustila, na njenih straneh pa najdemo le priporočila. Pobudo je nato prevzela delovna skupina v okviru združenja bank Slovenije in se lotila vzpostavitve enotnega elektronskega standarda za izmenjavo podatkov za domači in mednarodni plačilni promet, vendar napreduje zelo počasi, saj se pri tem srečuje z različnimi interesi bank oziroma dobavitelji opreme. Mnenje več slovenskih bančnikov je, da je implementacija standarda časovno zelo nedefinirana. Še bolj heterogeni so na drugi strani računovodsko-informacijski sistemi, ki jih uporabljajo slovenska podjetja, saj je v Sloveniji v uporabi več kot 100 različnih RIS. Vzpostavitev neposredno vez med uporabniki in bankami, kot vidimo, za podjetje ni enostavna a vendar se stvari izboljšujejo in napredujejo naprej.

5.4 Načrti za prihodnost

Načrti slovenskih bank na splošno sledijo trendom v svetovnem bančništvu. Gre predvsem za povezavo med različnimi finančnimi storitvami, ki naj bi jih bilo moč dobiti na enem mestu.

Na splošno bi lahko opredelili, da se banke pojavljajo trije izzivi (NLB 2008, interno gradivo):

- Tehnološki- Novi sistemi morajo biti kompatibilni z že obstoječim, obstaja problem velikega števila konkurenčnih bančnih sistemov in pomanjkanje skupnih standardov za področje varnosti in prenosa podatkov,

- Marketinški- Pojavljajo se nove tržne poti in veča se potreba po razlikovanju od drugih bank,

- Strateške-nove storitve bodo zahtevale, da banke tekmujejo tudi proti nebančnim konkurentom, kar zahteva dobro premišljen dolgoročni strateški načrt. Na srečo bank imajo prednost pred ostalimi z obstoječo bančno mrežo, dostopom do strank in veliko bazo podatkov.

Prihodnost s plačilni inštrument SEPA

SEPA je kartica za Single Euro Payments Area, ki predstavlja enotno območje plačil v evrih. Vključuje 16 držav evroobmočja, 11 preostalih držav EU, kjer evro ni nacionalno plačilno sredstvo, Islandijo, Norveško, Liechtenstein, Švico in devet območij, ki so pod upravo držav EU.

Na tem območju bodo potrošniki, gospodarske družbe in drugi uporabniki plačilnih storitev v bankah lahko plačevali in sprejemali plačila v evrih pod enakimi osnovnimi pogoji, z enakimi pravicami in obveznostmi tako znotraj posamezne države EU kot med državami EU.
Stranke bodo imele možnost izbrati najboljšega ponudnika plačilnih storitev, ne glede na državo izvora. To bo omogočilo učinkovito konkurenco ponudnikov plačilnih storitev

znotraj trga EU in bo najprej zahtevalo odpravo pravnih, poslovnih in tehničnih ovir, ki danes ločujejo nacionalne trge.

Prednosti Sepa so v tem, da posamezniki in podjetja bodo lahko znotraj evro območja izvajali negotovinska plačila z enega bančnega računa kjer koli v evro območju in iz enega niza plačilnih instrumentov tako enostavno, učinkovito in varno, kot lahko plačujete danes znotraj državnih meja.

Sepa bo prinesla večjo konkurenco, ker bo evro območje postalo povezan trg, na katerem lahko ponudniki povsod nudijo svoje storitve. Zaradi večje izbire med ponudniki storitev bodo imele stranke na voljo več konkurenčnih rešitev za plačila, ki bodo še bolj prilagojene potrebam potrošnikov.

Kaj bo SEPA prinesla potrošnikom:

- Potrošniki bodo potrebovali samo en sam bančni račun. S tega računa boste lahko opravljali evrska kreditna plačila in direktne obremenitve kjer koli v evro območju prav tako enostavno, kot jih zdaj opravljamo v Sloveniji. Pod takimi pogoji bomo lahko plačevali počitnice v tujini, najemnina za stanovanja za otroke, ki študirajo v tujini ali druge storitve, ki jih zagotavljajo evropske gospodarske družbe (mobilni operaterji, zavarovalnice, javne gospodarske službe itd.). Vsi, ki živijo , delajo ali študirajo v drugi državi, ne boste potrebovali dveh ali več bančnih računov, ampak bo zadostoval le eden,

- Uporaba plačilnih kartic bo učinkovitejša, saj boste lahko uporabljali isto kartico za plačevanje v državah območja SEPA. S tem se bo zmanjšala potreba, da bi s seboj nosili gotovino,

- Dolgoročni cilj je, da se plačilni instrumenti SEPA uporabljajo samo v elektronski obliki. Plačila bo mogoče enostavno uporabiti skupaj s storitvami, namenjenih poenostavitvi postopka plačila pred poravnavo plačila in po njej, tako za stranke kot za podjetja. To vključuje elektronsko izdajanje računov, izvedbo mobilnega ali internetnega plačevanja. E-letalske vozovnice ali obvestila o kreditnem plačilu. S tem boste za plačevanje porabili manj časa.

Kaj bo SEPA prinesla gospodarskim subjektom:

- Gospodarske družbe bodo lahko svoje finančne transakcije v evrih opravile centralno z enega bančnega računa in z uporabo plačilnih instrumentov SEPA. Obdelava plačil bo poenostavljena, ker se bo za prelive in odlive uporabljala enaka struktura podatkov. Gospodarske družbe, ki posluje na celotnem evroobmočju, bo z združitvijo upravljanja plačil in likvidnosti na enem mestu prihranile ne le denar, ampak tudi čas,

- Storitve, kot je npr., elektronsko izdajanje računov, bodo gospodarskim družbam omogočile nadaljno optimizacijo obdelave plačil. Danes so te storitve pogosto na voljo samo na nacionalni ravni, ker je zaradi različnih oblik plačil čezmejna uporaba

zahtevna in nepredvidljiva. Zaradi standardiziranih plačilnih instrumentov SEPA bo to oviro lažje premagati.

E-bančništvo pot do E-računov:

- Ena od zadnjih načrtov prihodnosti je uporaba SEPA plačil in izmenjave e-računov, ki na eni strani pri podjetjih ustvarijo pomembne prihranke, na drugi strani pa ne zahtevajo velikih investicij,

  SEPA plačila in e-računi na prvi pogled nimajo veliko skupnega. Vendar je ravno projekt SEPA tisti, ki je v Evropski uniji spodbudil bančni sektor, da je pričel razmišljati o uporabi kanalov plačilnega prometa za izmenjavo e-računov. V prihodnosti lahko pričakujemo, da bo izmenjava e-računov s pomočjo bančnih mrež možna v celotni EU,

- A trenutno banke in njihove stranke bolj zanima, kaj je že možno in kakšne spremembe še lahko pričakujemo v bližnji prihodnosti. Predstavniki slovenskih bank so se na konferenci osredotočili predvsem na to, kaj pomeni SEPA za banke in komitente že danes in kakšen je načrt zamenjave obstoječih plačilnih inštrumentov s SEPA inštrumenti. Uvedba v praksi bo sicer postopna, a SEPA DD bo tako za slovenske banke kot tudi za pravne osebe prinesla veliko sprememb v poslovanju. Vodja projekta SEPA v NLB je zato predstavila te spremembe in njihov vpliv na poslovanje v bankah in pri pravnih osebah, zlasti v infrastrukturnih podjetjih, ki so največji izdajatelji računov. Na okrogli mizi, ki je sledila, pa so razpravljali o SEPI v praksi in o tem, kaj še čaka podjetja na tem področju v prihodnosti. Pravne osebe nastopajo tako v vlogi izdajatelja kot tudi v vlogi prejemnika računov, v obeh primerih pa obstajajo zanje velike koristi, če lahko račune prejemajo in pošiljajo v elektronski obliki. A e-računi lahko podjetju prinesejo uspeh in racionalizacijo poslovanja le, če med izdajatelji in prejemniki e-računov obstaja zanesljiva in enotna komunikacijska infrastruktura. In ta obstaja. V drugem delu konference je g. Ivan Janc, vodja projekta e-računi v Abanki Vipa v živo predstavil izmenjavo e-računov tako na strani izdajatelja kot tudi prejemnika. G. Tomaž Kraškovic, direktor sektorja financ v Telekomu Slovenija, je pojasnil, kako pristopiti k uvedbi e-računov v velikih poslovnih sistemih. Telekom Slovenije je eden prvih izdajateljev e-računov in bo s 1. junijem 2010 prejemal le še e-račune. (Halcom 2009).

6 SKLEP

Ko bomo čez leta gledali nazaj bomo brez dvoma dejali, da je bil eden najpomembnejših dosežkov 90-ih let vsesplošen razvoj interneta. Elektronsko pošta je poenostavila komunikacijo v poslovnem in v našem vsakdanjem življenju. Vsak, ki lahko objavi poslovno stran na internetu ima možnost pridobitve novih potencialnih strank.

Prihodnost je v rokah elektronskih medijev in od skromnih začetkov do zmanjšanja dvomov o elektronski prihodnosti je prišlo v izredno kratkem času, vendar še vedno obstaja veliko priložnosti, poti, idej, ki nakazujejo, da smo pravzaprav šele na začetku digitalne dobe.

Tehnologija ima moč, da lahko spremeni naše življenje. Že v zgodovini se je pokazalo kako lahko vpliva na naše življenje. Ob izumu žarnice do prve brezžične komunikacijske naprave (radio).

Pojma elektronsko bančništvo in internet sta postala nerazdružljiva. Kmalu bo prišel čas, ko bo internet postal povsem nepogrešljiv in si finančnih in poslovnih aktivnosti sploh ne bomo znali predstavljati brez njega.

Določena podjetja v slovenskem prostoru so že začela uveljavljati elektronske račune, sicer je še v fazi uvajanja in te zasledimo predvsem za pravne osebe.

7 POVZETEK / ABSTRACT

V diplomski nalogi sem predstavila internet kot osnovni pogoj za nastanek elektronskega bančništva njegovo varnost ter kako se je elektronsko bančništvo razvilo v Sloveniji in kakšni so načrti za razvijanje elektronskega bančništva v bodoče. Elektronsko bančništvo je namreč prijazen način bančnega poslovanja prek interneta. Z uporabo osebnega računalnika hitro in enostavno lahko dostopamo do različnih storitev, ki nam jih nudi banka in lahko pridobivamo različne informacije na tem področju.

Diplomsko delo je razdeljeno na tri tematska sklopa. Za takšen način opredelitve sem se odločila zato, da bralcu prikažem najprej internet nato splošno elektronskem bančništvo, šele na to pa prikaz nadaljnega razvoja na področju elektronskega bančništva.

Prvi del je namenjen razlagi pojma internet. V tem poglavju je opisano kako internet deluje, opisani so njegovi sestavni deli za delovanje ter storitve, ki nam internet nudi.

Drugi del je namenjen elektronskemu bančništvu in varnosti elektronskega bančništva. Opredeljeno je kaj elektronsko bančništvo predstavlja, njegova zakonska podlaga ter storitve, ki jih nam nudi. Pri varnosti elektronskega bančništva pa so opredeljeni njegove nevarnosti ter varnostne mehanizme, ki jih lahko uporabimo.

Tretji je del pa je namenjen izključno elektronskemu bančništvu v Sloveniji, ponudba slovenskih bank ter načrti za nadaljnji razvoj elektronskega bančništva.

Elektronsko bančništvo je za banke izrednega pomena. Seveda pa se banke zavedajo, da je njegov cilj je zadovoljen odjemalec, z njim pa mora posledično temu krepiti predvsem dobre odnose ter v nadaljevanju omogočati nadaljno širitev in obseg in imeti tendenco na kakovost poslovanja.

Ključne besede: internet, elektronsko bančništvo, varnost elektronskega bančništva, banka, elektronski podpis, elektronsko poslovanje, varnostni ukrepi

In my diploma paper, the Internet is presented as the underlying infrastructure for electronic banking (e-banking), the appertaining security thereof, the course of development of e-banking in Slovenia and the outlook for development of e-banking in the future. E-banking is a very user-friendly mode of using Internet-based banking. A personal computer enables us a quick and easy access to a variety of banking services offered by our bank and to the information available on this area.

The diploma paper is divided into three thematic segments. I decided for such a structure to demonstrate the use of the Internet and e-banking in general, and after that to present further development in the sphere of e-banking to the reader.

The first part is intended to explain the term ‘Internet’, namely how the Internet functions, what components are necessary for the functioning and provision of Internet-based services.

The second part is dedicated to e-banking and the security thereof. The definition of e-banking and the legal groundwork are given with an outline of services provided in the scope of e-banking. In the part covering the security in e-banking are indicated the risks to which e-banking is exposed, and the security mechanisms available to us for protection.

Part Three deals with e-banking in Slovenia, the range of services offered by the Slovenian banks, and the perspectives for the future development of e-banking.

Electronic banking is of vital importance for banks. Accordingly, they are aware of the customer's role for their target market: a satisfied customer is in the first place, which should be later on upgraded by strengthening their good relations with the customers and enabling further expansion and volume, bearing in mind the quality of service.

Key words: Internet, E-banking, security in e-banking, bank, electronic signature, e-commerce, safety measures/ precautions

8 VIRI IN LITERATURA

Bankart. 2009. Upravljanje mreže bančnih avtomatov. [online]. Dostopno na: http://www.bankart.si/si/ponudba/upravljanje_mreze_bankomatov/ [10. 05. 2009]

Barle, Tadej in Aleksandra Žibrat. 2007. Priporočila za varno uporabo storitev spletne banke. Združenje bank Slovenije - GIZ.

Bezgovšek, David. 2008. Skandinavija vodilna v uporabi interneta. Računalniške novice 9, 10-11.

Bračun, Franc. 1997. Praktične izkušnje pri uvajanju elektronskega bančništva. Zveza ekonomistov Slovenije, 149-154.

Bračun, Franc in Andrej Cetinski. 1998. Elektronsko poslovanje v SKB d.d.. Organizacija 3, 144.

Bradeško, Marjan. 1998. Varnost računalniških omrežij in storitev. Podjetnik 2, 74-77

Gradišar, Miro in Gortan Resinovič. 1996. Informatika v poslovnem okolju. Ljubljana: Ekonomska fakulteta.

Grobelšek, Matic. 2001. Mobilne telekomunikacije. Gospodarski vestnik 16, 8.

Grošelj, Bojan in Saša Prešeren. 2000. Informatika za podjetnike. Kranj: Visoka šola za podjetništvo.

Holtz, Shel. 2002. Public Relations on the Net. New York: Amacom

Interna gradiva A-banke d.d.. 2008.

Interna gradiva Banke Koper d.d.. 2008.

Internetno gradivo Halcom d.d.. 2009

Interna gradiva Nove Ljubljanske banke d.d.. 2008.

Interna gradiva Nove Ljubljanske banke d.d.. 2009.

Javornik, Boža. 2000. Revizija v razmerah elektronskega poslovanja. Ljubljana: Zveza ekonomistov Slovenije in Zveza računovodij, finančnikov in revizorjev Slovenije.

Jerman-Blažič, Borka. 1997. Internet. Maribor: Forum Media.

Jerman-Blažič, Borka. 1999. Izbrana poglavja računalniških komunikacij in elektronsko poslovanje. Ljubljana. GV Založba.

Jerman-Blažič, Borka. 2001. Elektronsko poslovanje na internetu. Ljubljana: GV Založba.

Jurišič, Aleksandra in Jernej Tonejc. 2001. Pametne kartice in varnost. Monitor 6, 66-75.

Kovačič, Matevž. 1997. Storitve elektronskega bančništva. Banke in tveganja. Zveza ekonomistov Slovenije, 133-138.

Kozic, Tina, Katja Prevodnik, Vehovar Vasja in Kogovšek Luka. 2009. E-bančništvo 2009. [online]. Dostopno na:
http://www.ris.org/2008/10/RIS_porocila/Ebancnistvo_2009/? [10. 05. 2009].

Miš, Irena. 1999. Za vogalom stoji. Kapital 3, 36-37.

MojDenar. 2009. Bančništvo - Plačilne kartice. [online]. Dostopno na: http://www.mojdenar.com/BANKE/plac_kart_splosno.asp [10. 10. 2009]

Moj evro. 2009. Kam v spletno banko. [online]. Dostopno na: http://www.mojevro.si/244781 [04. 04. 2009]

Muzlovič, Marko. 2009. Uporaba interneta v gospodinjstvih in pri posameznikih, Slovenija, 2009. [online]. Dostopno na:
http://www.stat.si/novica_prikazi.aspx?id=2670 [05. 10. 2009].

Pavliha, Marko. 2002. Zakon o elektronskem poslovanju in elektronskem podpisu. Ljubljana: GV Založba.

Pucihar, Andreja in Jože Gričar. 2000. Izraba informacijske tehnologije za elektronsko poslovanje. Organizacija 3, 207-212.

Pustišek, Matevž in Marko Popič. 2001. Osnove internetnih sistemov. [online]. Dostopno na:
http://it.fe.uni-lj.si/gradiva/viri/razno/elektotehniškenovice_osnove_ip_sistemov_v1.14.pdf [10. 05. 2009].

RIS. 2002. E- bančništvo. [online]. Dostopno na: http://www.ris.org//uploadi/editor/1237817193E-bancnistvo.pdf [10. 05. 2009]

Risen, James. 2002. Sept. 11 Hijackers said to fake date on bank accounts. [online]. Dostopno na: http://www.nytimes.com/2002/07/10/us/sept.11-hijackers-said-to-fake-data-on-bank-accounts.html?scp=5&sq=risen+james&st=nyt [10. 05. 2009]

Ručigoj, Simon. 2000. GSM + internet + WAP. Telemonitor 4/5, 10-13.

Savodnik, Tomaž. 1999. Bančništvo od doma. Moj mikro 7/8, 24-27.

Sejklača, Marko. 1999. Elektronsko bančništvo. Bančni vestnik 1/2, 31-32.

Škerlep, Andrej. 1998. Model računalniško posredovane komunikacije. Ljubljana: Fakulteta za družbene vede.

Trstenjak, Mojca. 2003. Zloraba plačilne kartice. Kapital 305, 24-25.

Uradni list RS. 2000. Zakon o elektronske poslovanju in elektronskem 57/2000.

Vagaja, Aleksandra. 2000. Z Wap-om do komitenta. Finance 46, 10-12.

Voljč, Marko. 2001. Prihodnji razvoj slovenskih bank. Bančni vestnik 5, 111-117.

Vozelj, Aleksander. 1999. Napake v internetni strategiji bank. Gospodarski vestnik 47, 74-76.

Zdrešar, Polona. 2008. Uporaba interneta v gospodinjstvih, Slovenija, 1. četrtletje 2008. [online]. Dostopno na: http://www.stat.si/novica_prikazi.aspx?id=1907 [01. 10. 2008]