

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

SPECIALISTIČNO DELO

ELEKTRONSKO BANČNIŠTVO V
SLOVENIJI

Ljubljana, september 2007

TANJA MAROLT

IZJAVA

Študentka Tanja Marolt izjavljam, da sem avtorica te specialistične naloge, ki sem jo napisala pod mentorstvom dr. Borke Jerman Blažič in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo specialistične naloge na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

KAZALO

1 UVOD	1
1.1 OPREDELITEV PROBLEMA, NAMEN IN CILJ DELA	2
1.2 METODE PREUČEVANJA IN ZASNOVE DELA	4
2 ELEKTRONSKO POSLOVANJE	4
2.1 OPREDELITEV ELEKTRONSKEGA POSLOVANJA	4
2.2 RAZVOJ ELEKTRONSKEGA POSLOVANJA	6
2.3 PREDNOSTI IN SLABOSTI ELEKTRONSKEGA POSLOVANJA	7
3 ELEKTRONSKO BANČNIŠTVO	8
3.1 POJEM ELEKTRONSKEGA BANČNIŠTVA	8
3.1.1 Razvoj elektronskega bančništva	10
3.1.2 Delovanje elektronskega bančništva	11
3.2 PREDNOSTI ZA BANKO IN KOMITENTA	13
3.3 SLABOSTI ZA BANKO IN KOMITENTA	14
4 VARNOST ELEKTRONSKEGA POSLOVANJA	15
4.1 OPREDELITEV VARNOSTNIH KOMPONENT	16
4.2 ELEKTRONSKI PODPIS	19
4.2.1 Digitalno potrdilo	21
4.2.2 Overitelj javnih ključev	24
4.2.3 Infrastruktura javnih ključev	25
4.3 PAMETNE KARTICE	26
4.4 GESLA IN DRUGA ZAŠČITA	28
5 PONUDBA BANK V SLOVENIJI	31
5.1 HALCOMOV PROGRAM	33
5.1.1 Nova Ljubljanska banka, d. d.	35
5.1.2 SKB banka, d. d.	37
5.1.3 Abanka Vipra, d. d.	38
5.2 BANKA KOPER, d. d.	38
5.3 NOVA KREDITNA BANKA MARIBOR, d. d.	42
5.4 VOLKSBANK – LJUDSKA BANKA, d. d.	44
6 SKLEP	50
7 LITERATURA IN VIRI	51

SEZNAM SLIK IN TABEL

Slika 1: Oblike elektronskega bančništva	9
Slika 2: Princip delovanja elektronskega bančništva – standardni način.....	11
Slika 3: Način delovanja sistemov elektronskega bančništva po internetu.....	12
Slika 4: Osnovni model zaščite lokalnega omrežja.....	18
Slika 5: Prikaz podpisovanja elektronskih dokumentov	19
Slika 6: Simetrično in asimetrično šifriranje.....	21
Slika 7: Pisno potrdilo o identičnosti digitalnega potrdila	23
Slika 8: Struktura EuroPKI	25
Slika 9: Kartica Banke Koper, d. d.....	26
Slika 10: Kartica ena za vse – Halcom, d. d.....	27
Slika 11: Kartica Volksbank – Ljudske banke, d. d.	27
Slika 12: Čitalniki pametnih kartic.....	28
Slika 13: Kartica NKBM, d. d.....	29
Slika 14: Kartica za uporabo SKB net-a (fizične osebe).....	30
Slika 15 : Primer biometrične zaščite s prepoznavanjem obraza	30
Slika 16: Enouporabniška različica programa Halcom	34
Slika 17: Pregled pooblastil pri Banki Koper, d. d.....	40
Slika 18: Pregled transakcijskega računa	40
Slika 19: Menjava valut.....	41
Slika 20: Kritje medvalutne menjave	42
Slika 21: Spletna banka NKBM – EUR različica (EPP7).....	43
Slika 22: Plačilni nalog NKBM	44
Slika 23: Spletna banka Volksbank online.....	45
Tabela 1: Prednosti e-poslovanja za podjetja, posameznika in družbo	7
Tabela 2: Tehnične in netehnične omejitve, ki jih prinaša e-poslovanje	8
Tabela 3: Pregled bank, ki omogočajo spletno bančništvo za pravne osebe.....	32
Tabela 4: Stroški, povezani z elektronsko banko	48
Tabela 5: Storitve elektronskega bančništva	49

1 UVOD

Elektronsko bančništvo za pravne osebe se je v Sloveniji od začetka reforme plačilnega prometa izjemno razmahnilo, tako da po deležu podjetij, ki z banko poslujejo elektronsko, Slovenija spada v sam svetovni vrh. V Sloveniji v povprečju dve tretjini vseh podjetij uporablja elektronsko banko in pri nekaterih bankah elektronske transakcije pokrivajo več kot 90 odstotkov vseh transakcij.

Glede na to, da je Slovenija po navadi zaostaja za Evropsko unijo, pa jo v plačilnem prometu močno prekašamo. V Sloveniji se plačila med komitenti posameznih bank poravnajo vsaj petkrat na dan, če gre za majhna plačila, in takoj, če gre za večja. V zahodni Evropi traja poravnava tri dni, v najbolj razvitih pa en dan.

V okviru oblikovanja enovitega evropskega plačilnega območja (SEPA) naj bi se poravnava opravila naslednji dan, kar je še vedno slabše, kar dosegamo v Sloveniji. Vzpostavil naj bi se Straight Through Processing, pri katerem se obdelava podatkov pri plačevanju računov opravi avtomatsko, kar v Sloveniji deluje že 15 let, v Evropi pa o tem šele razmišljajo.

Slovenija je ena redkih držav, v kateri lahko uporabnik z enim programom za elektronsko banko in z eno samo zaščitno kartico prihaja do transakcij pri različnih bankah.

Največ pomislekov imajo skeptiki seveda zaradi varnosti elektronskega poslovanja. Absolutne varnosti ni, ne v klasičnem ne v računalniškem svetu.

Vsak uporabnik bi moral poznati osnove računalniške varnosti, da lahko varno posluje pri delu s programi za elektronsko banko. Celovite varnosti ne more zagotoviti samo banka za varnost mora skrbeti tudi uporabnik; tako kot proizvajalec ne more zagotoviti varnosti pred krajo avtomobila, če ga sam lastnik ne zaklepa.

V specialistični nalogi sem skušala podati prednosti in slabosti posameznih bank, ki jih vsakodnevno uporabljam v svojem poslovnem svetu. Skupek vseh prednosti bi bila moja idealna elektronska banka, s katero bi bilo delo še večji užitek.

Glede na to, da je moje specialistično delo nastajalo ravno na prehodu v EUR različice elektronske banke, sem nekaj besed namenila tudi prehodu in ugotovitvam, ki sledijo po večmesečni uporabi.

Za tako temo specialistične naloge sem se odločila predvsem zato, ker je del mojega vsakdana in sem svoje ugotovitve želela napisati, morda nekoč pripeljejo do novih, še boljših elektronskih rešitev.

1.1 OPREDELITEV PROBLEMA, NAMEN IN CILJ DELA

Problematika in namen specialističnega dela

Elektronsko bančništvo je ena najpriročnejših in najcenejših načinov za posameznega uporabnika pri poravnavi dolgov in zmanjševanju zneska na svojem osebnem ali transakcijskem računu. Vsekakor je zelo mikavna možnost imeti informacijo 24 ur na dan o prilivu ali odlivu denarja/sredstev na računu uporabnika.

Elektronsko bančništvo omogoča, da se uporabnik udobno namesti v pisarniškem stolu ali doma in s klikom na miško narekuje programu, kako naj razporeja težko zaslužen denar. Elektronsko bančništvo je sestavni del sodobnega poslovanja z uporabo elektronskih medijev, ki jih poznamo kot elektronsko poslovanje.

Elektronsko poslovanje

Elektronsko poslovanje je področje, ki se uveljavlja tudi v Sloveniji. Nekaj let po uvedbi internetnih storitev so uporabniki predvsem samo preizkušali storitve interneta. Leta preizkušanja in prilagajanja so omogočila, da so uporabniki pridobili zaupanje v internet in se navadili uporabljati temeljne internetne storitve, kot je elektronska pošta in svetovni splet. Internet, tehnologija nove ekonomije, omogoča tudi hiter razvoj elektronskega poslovanja. Hitro uveljavljanje elektronskega poslovanja je hkrati tudi posledica neprestanega prilagajanja tržišču, kjer vlada močna konkurenca. Zato je učinkovito poslovanje ob uporabi elektronskih medijev bistvena sestavina konkurenčnega gospodarstva.

V pogledu definicij e-poslovanja obstaja širok spekter razlag. Sam pojem v angleščini (»electronic commerce«) se bolj kot v slovenščini navezuje na napačno razumevanje v smislu elektronskega trgovanja, kar oznaka e-poslovanje vsekakor presega in vključuje še vrsto drugih oblik uporabe informacijske in komunikacijske tehnologije v poslovnih odnosih. Sem sodijo trgovinske, proizvodne in storitvene organizacije kot tudi ponudniki informacij, potrošniki in državna uprava (Jerman Blažič, 2001, str. 13). Sestavni del elektronskega poslovanja je tudi elektronsko bančništvo.

Elektronsko bančništvo

E-bančništvo lahko opredelimo kot kakršenkoli način poslovanja stranke z banko, ki poteka neodvisno od poslovalnic bank in temelji na informacijski tehnologiji in elektronskih medijih. V širšo razlago vključujemo vse bančne storitve, ki se opravljajo po elektronski poti (Miš Svoljšak, 1997, str. 12):

- bančne avtomate,
- elektronsko bančništvo po internetu,
- telefonsko bančništvo,
- mobilno bančništvo in

- kartično poslovanje.

Iz tega je razvidno, da obstaja več vrst elektronskega bančništva, vsaka pa je namenjena določenemu segmentu bančnih komitentov. V elektronski banki lahko po internetu opravimo vrsto negotovinskih transakcij, kot so:

- prenosi med svojimi računi,
- plačila računov,
- pregledujemo stanje na svojih računih,
- izpisujemo prometne postavke za izbrano obdobje,
- pošiljamo sporočila banki in prejemamo bančna obvestila.

Bistveni element elektronskega bančništva je zagotovitev varnosti, ki je podobna varnosti v klasičnem bančnem poslovanju.

Varnost

Osrednja točka varovanja pri e-poslovanju so viri ¹, ki imajo za lastnika določeno vrednost in ki so izpostavljeni grožnjam. Organizacija, ki posluje elektronsko, ima za zagotavljanje varnosti na voljo naslednje varnostne storitve (Jerman Blažič, str. 101):

- overjanje, možnost preveriti identiteto subjekta;
- zaupnost, informacije ne smejo biti razkrite nepooblaščenim osebam;
- neokrnjenost, ohranjanje pristnosti podatkov;
- nadzor dostopa, preprečevanje nepooblaščne uporabe;
- preprečevanje zanikanja o sodelovanju v aktivnosti poslovanja ter
- razpoložljivost; storitve e-poslovanja so stalno na voljo.

Namen specialistične naloge je predstaviti prednosti in slabosti elektronskega bančništva. Z nalogo želim izluščiti prednosti, ki jih ima uporaba elektronskega bančništva za vsakega uporabnika. Predstavila bom tudi banke, ki v Sloveniji ponujajo e-bančništvo, in ocenila njihove storitve. Ta ocena lahko pomaga posamezniku oz. podjetju, da lažje izbere določeno banko v Sloveniji.

Cilji specialistične naloge so predvsem naslednji:

- predstaviti elektronsko poslovanje in elektronsko bančništvo,
- preučiti varnostno tehnologijo v elektronskem poslovanju,
- oceniti ponudbo elektronskega bančništva v slovenskih bankah,
- izpostaviti prednosti in pomanjkljivosti posameznih bančnih programov.

¹ Splošne kategorije virov so: podatki, informacije pri prenosu in hranjenju, strojna in programska oprema, uporabniki in odnosi med njimi ter dokumentacija o postopkih strojne in programske opreme v sistemu ali omrežju (Jerman Blažič, 2001, str. 100)

1.2 METODE PREUČEVANJA IN ZASNOVE DELA

V teoretičnem delu specialistične naloge so mi pomagali viri in obstoječa literatura (slovenske in tuje strokovne knjige, publikacije, internetno gradivo ter internet)

Praktični del specialistične naloge bo temeljil na izkušnjah, pridobljenih z delom na področju elektronskega bančništva.

V prvem delu sem v dveh poglavjih strnila teoretično osnovo. Prvo poglavje je namenjeno grobi predstavitvi elektronskega poslovanja, kjer sem podala tudi nekaj ključnih prednosti in slabosti za podjetja, posameznika in družbo. V drugem poglavju sem zajela bistvene lastnosti elektronskega bančništva, ki predstavlja jedro naloge, v okviru katerega sem podrobneje izpostavila le enega izmed možnih načinov storitev elektronskega bančništva, in sicer elektronsko plačevanje po internetu med bankami in podjetji.

Tretje teoretično poglavje, ki je po vsebini najobsežnejše, zajema varnostne mehanizme pri elektronskem poslovanju s poudarkom na elektronskem bančništvu. V nalogo sem zajela najpogostejše uporabljene tehnike varnostnih mehanizmov, ki se dopolnjujejo v kombinaciji z drugimi.

V zadnjem poglavju, v bolj praktičnem delu moje naloge, sem poskušala teoretične izsledke iz prvega dela združiti s predstavitvijo ponudb slovenskih bank ter se podrobneje osredotočiti na banke, s katerimi vsakodnevno poslujem. Želela sem predstaviti svoje stališče o uporabnosti in zasnovi posameznih elektronskih aplikacij.

2 ELEKTRONSKO POSLOVANJE

2.1 OPREDELITEV ELEKTRONSKEGA POSLOVANJA

Elektronsko poslovanje pomeni prehod iz klasičnega načina poslovanja, ki je potekal po telefonu in s pomočjo podatkov, informacij na papirju, v elektronsko obliko sporazumevanja in poslovanja. Pojem elektronsko poslovanje izhaja iz angleškega izraza »electronic commerce« in obsega celoto procesov, ki podpirajo trgovsko, poslovno dejavnost in lahko vključujejo potrošnike, proizvajalce, prodajalce, ponudnike storitev in posrednike (Pavliha, 2002, str. 24). Na intenzivnost uvajanja elektronskega poslovanja vplivajo: konkurenca, vrsta dejavnosti, stopnja razvitosti organizacije, stopnja razvitosti okolja, države potrošnikov ter znanje in osveščenost o elektronskem poslovanju (Pucihar, Gričar, 2002, str. 209). Med ključne tehnološke elemente elektronskega poslovanja štejemo: računalnik, programsko rešitev (aplikacija) in komunikacije. Dodati pa je treba še organizacijo poslovanja, saj šele skupaj z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema (Toplišek, 1998, str. 5).

Elektronsko poslovanje je več kot samo 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 trgovanje (trading),
- elektronsko bančništvo (banking, telebanking),
- elektronsko plačevanje (potrošniško: e-čeki, e-gotovina, e-kartice, bankomati),
- delo na daljavo (teleworking),
- elektronsko založništvo (e-publishing),
- elektronska ponudba (katalogi, videotekst),
- elektronsko zavarovalništvo,
- elektronsko borzno poslovanje,
- elektronska prodaja (potrošniška, retailing),
- notranje elektronsko poslovanje (npr. v organizaciji).

Pomembni elementi teh dejavnosti so naslednji (Jerman Blažič, 2001, str. 129):

- **način dela:** kjer se računalniško izmenjujejo podatki ob uporabi odprtih omrežij, kot npr: internet;
- **vsebina poslovanja:** prodaja blaga in storitev, plačevanje, prodaja informacij, bančne transakcije, izmenjava dokumentov in listin, storitve trženja in medosebnega komuniciranja, nakupovanje v spletnih trgovinah, opravljanje dela na daljavo, omogočanje pomoči na daljavo (npr. zdravniške), izvajanje pouka na daljavo, storitve državne uprave na daljavo in podobno;
- **udeleženci poslovanja:** med udeležence elektronskega poslovanja lahko štejemo posameznike (podjetnike, managerje, raziskovalce, občane, učitelje, študente, dijake, upravne delavce), podjetja, bolnišnice, muzeje, galerije, univerze, izobraževalne organizacije in državne organe. To je poslovanje znotraj posameznih skupin in poslovanje med skupinami. V zadnjem času prihaja v ospredje predvsem poslovanje med posamezniki ter med posamezniki in podjetji. Poslovanje med samimi podjetji 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, str. 144).

Bančništvo vsebuje nekatere specifične značilnosti, ki omogočajo, da ima ta dejavnost zelo dobre možnosti za uvedbo elektronskega poslovanja (Cetinski, 1999, str. 149):

- bančne storitve temeljijo v veliki meri na informacijah;
- večina občanov uporablja bančne storitve, tako da imajo večje slovenske banke, ki so sicer po mednarodnih merilih razmeroma majhne, tisoč in več strank;

- banke nudijo široko ponudbo storitev, od katerih so nekatere take, da jih mnoge stranke koristijo skoraj vsak dan ali pa tudi večkrat dnevno.

Glede na obsežnost pojma e-poslovanja lahko razlage e-poslovanja proučujemo iz različnih spektrov (Kalakota, 1997, str. 3):

1. **Komunikacijski pogled:** je prenos informacij, proizvodov in storitev po telefonu, računalniškem omrežju ali drugih komunikacijskih povezavah.
2. **Poslovno-procesni pogled:** v poslovni proces s pomočjo programskih aplikacij vnaša avtomatizacijo procesov in transakcij.
3. **Storitveni pogled:** omogoča večjo učinkovitost poslovanja z znižanjem stroškov, boljšo kakovostjo in s hitrejšo dobavo oz. izvedbo storitve.
4. **Povezovalni pogled:** deluje v omrežjih, ki so med seboj povezana in delujejo neposredno.

2.2 RAZVOJ ELEKTRONSKEGA POSLOVANJA

Začetki elektronskega poslovanja segajo v leto 1968, ko se je začel razvoj računalniških omrežij in interneta, združevanje informacijske in telekomunikacijske tehnologije ter z uvajanjem standardov za RIP². Računalniška tehnologija, ki je bila v začetku namenjena le računalniškim strokovnjakom in znanstvenikom, je z leti postala veliko bolj uporabna in prijazna tudi širšim uporabnikom.

V 70. letih se je s pojavom elektronskih finančnih prenosov med bankami po varnih zasebnih omrežjih spremenil način poslovanja na finančnem trgu. Veliko podatkov je iz papirne oblike prešlo na elektronsko obliko, ki so se znotraj podjetja prenašali z različnimi sistemi za prenos podatkov in po elektronski pošti. V poznih 70. in zgodnjih 80. letih se je e-poslovanje razširilo v okviru podjetij v obliki sistemov za prenos datotek, RIP in elektronske pošte. S tem so podjetja zmanjšala obseg papirnega dela in povečala se je avtomatizacija pisarniškega poslovanja. V poznih 80. in zgodnjih 90. letih so sistemi za izmenjavo sporočil postali integralni del računalniških sistemov in omrežij (Jerman Blažič, 2001, str. 13–14). Dotedanja praksa izmenjave podatkov je pokazala nekaj slabosti in usmerila nadaljnji razvoj (Škrlec, 2002, str. 18):

- natančno določena oblika podatkov in dokumentov, ki se izmenjujejo med različnimi aplikacijami na podlagi natančno določenih standardov.
- preslikava v zeleno obliko je bila draga in zapletena, težje dostopna in razumna za širši krog uporabnikov.

Kljub pomanjkljivosti, ki jih je dajal sistem, je bila dobra stran standardizacije in izgradnje komunikacijske infrastrukture v avtomatizaciji procesov, ki je skrajšala čas obdelave podatkov in zmanjšala stroške prenosa. To se je dogradilo v nadaljnjem razvoju, ki je bil hiter in učinkovit. Nove rešitve se dopolnjujejo s staro tehnologijo, kar podjetjem omogoča

² RIP oz. EDI – Electronic Data Interchange pomeni izmenjavo standardiziranih, kodiranih sporočil med dvema računalniškima aplikacijama (Toplišek, 1998, str. 13).

cenovno ugodno nadgradnjo sistema. 90. leta so z razvojem interneta ter s pojavom svetovnega spleta na internetu prinesla preobrat, ki je sprožil razvoj e-poslovanja na vse oblike uporabe, ki so poznane tudi danes in so se razširile med številne uporabnike. Njihovi temelji enostavne in preproste uporabe izhajajo iz ključnih predpostavk, ki gradijo internet. Te so:

- lokacijsko neodvisno in strankam dosegljivo omrežje kjerkoli in kadarkoli,
- povezava množice navzven odprtih manjših računalniških omrežij, ki nimajo skupnega lastnika ali osrednjega nadzornega organa,
- preprosta uporaba z vnaprej določenimi scenariji in
- strojna ter programska neodvisnost.

Komunikacija je izvedljiva po istih pravilih sporazumevanja, ki so poznana vsem uporabnikom. S tem je internet znižal stroške za učinkovito komuniciranje, odprl pot do novega načina poslovanja in novih trgov, povečal učinkovitost, skrajšal čas posameznih poslovnih postopkov, omogočil vpeljavo večpredstavnih storitev ter večjo prilagodljivost spremembam na trgu in zagotovil, da je ekonomija postala globalna, gospodarske organizacije pa globalno povezane.

2.3 PREDNOSTI IN SLABOSTI ELEKTRONSKEGA POSLOVANJA

Novosti, ki jih prinaša uporaba e-poslovanja, nekateri primerjajo s spremembami, ki jih je prinesla industrijska revolucija. Spremembe se kažejo v prednostih in slabostih uporabe e-poslovanja posameznika, družbe in podjetij (glej tabelo 1 in tabelo 2).

Tabela 1: Prednosti e-poslovanja za podjetja, posameznika in družbo

PREDNOSTI ZA PODJETJA	➤ razširitev trga, globalizacija ➤ zmanjšanje stroškov poslovanja, zalog
	➤ prilagoditev proizvodov željam kupca ➤ skrajševanje proizvodnega cikla
	➤ prenova poslovnih procesov, reinženiring ➤ zmanjšanje telekomunikacijskih stroškov
PREDNOSTI ZA STRANKO	➤ možna hitra primerjava cene in kakovosti ➤ hitra dobava digitalnih proizvodov
	➤ večja informiranost, konkurenca, večje ugodnosti ➤ izmenjava mnenj med kupci
PREDNOSTI ZA DRUŽBO	➤ možnost dela doma, manj potovanja, manjši promet in manjše onesnaževanje ➤ ugodnosti povečujejo življenjski standard
	➤ razvojne možnosti za tretji svet ➤ pospešuje dostavo javnih storitev

Vir: Turban, 2003, str. 16–20.

Tabela 2: Tehnične in netehnične omejitve, ki jih prinaša e-poslovanje

TEHNIČNE OMEJITVE	➤ pomanjkanje zanesljivosti, varnosti in tajnosti ➤ slab komunikacijski prenos
	➤ nekompatibilnost opreme in hitre programske spremembe ➤ hitre spremembe tehnologije ➤ dodatni stroški za tehnično podporo
NETEHNIČNE OMEJITVE	➤ stroški nabave računalniške opreme ➤ nezaupanje v varnost ➤ nezaupanje v obstoj podjetij ➤ različna zakonodaja in standardi

Vir: Turban, 2003, str. 20–21.

Zaradi številnih konkurenčnih prednosti, ki jih je moč dobiti z vstopom v e-poslovanje, se širi razkorak med uspešnimi in manj uspešnimi. Hitrost razvoja pogosto sili podjetja, da sprejmejo nekaj novega, kar še ni povsem uveljavljeno in preizkušeno. Podjetja se v konkurenčnem boju za višji tržni delež pogosto zatečejo k hitrim in neakovostnim rešitvam, ki pustijo slab in negativen rezultat. Neuspeli poskusi v e-poslovanju mečejo slabo luč na celotno področje, zato ljudje postanejo nezaupljivi.

Seveda si glede varnosti in zaščite ne moremo zatiskati oči, saj je skrb za varnost podatkov pred razkritjem in zlorabo upravičena. Že en vdor v sistem povzroči nezaupanje uporabnikov v digitalno obliko poslovanja in pusti za seboj veliko škodo. Zato se informatiki trudijo razvijati in graditi sisteme, ki bi zagotavljali želeno stopnjo varnosti in zadostno raven funkcionalnosti sistema. Računalniška varnost vključuje tako varnost fizičnega sistema, omrežnih in računalniških povezav kot tudi pravilno ravnanje uporabnikov. Dosežemo jo z učinkovitim procesom planiranja, uvajanja in preverjanja sistema varovanja pred vsiljivci. Za zagotovitev le-te so na voljo različne kombinacije programske in strojne opreme ter fizično varovanje. Oblika zaščite je odvisna od varnostne politike organizacije in odnosa, ki ga v organizaciji gojijo, do pomena varnosti in zaupnosti.

3 ELEKTRONSKO BANČNIŠTVO

3.1 POJEM ELEKTRONSKEGA BANČNIŠTVA

»S pojmom elektronska banka lahko opredelimo način opravljanja bančnih storitev, ki jih lahko kot bančni komitent opravite neposredno na svojem delovnem mestu ali od doma, brez neposredne pomoči bančnega uslužbenca, in to kadarkoli, 24 ur na dan, 365 dni v letu« (Kadivec, 2000, str. 3).

Bančništvo je za elektronsko poslovanje še posebej ugodna dejavnost. Elektronsko poslovanje učinkovito podpira hitro in kakovostno izvajanje bančnih storitev. Z njim je mogoče storitve poceniti, njihova uporaba ni več omejena zgolj na čas, ko so banke uradno odprte, in na lokacijo bančnih poslovalnic, predvsem pa tako bankam kot njihovim strankam omogoča

velike prihranke v času. Zato ne preseneča, da se elektronsko poslovanje prav v bančništvu uvaja in krepi hitreje kot v večini drugih dejavnosti. Elektronsko bančništvo je vsekakor bančna storitev prihodnosti. Prej ali slej se mu bodo morale prilagoditi vse banke, ki bodo želele ohraniti poslovno konkurenčnost. Podobno kot to velja za druge poslovne organizacije, lahko tudi elektronsko bančništvo na najvišjem nivoju razdelimo na tri temeljne segmente (Miš Svoltjšak, 1999, str. 4–5):

Slika 1: Oblike elektronskega bančništva



Bančništvo od doma

- ♦ telefonsko bančništvo
- ♦ bančništvo po internetu (WEB)
- ♦ virtualna televizija (ITV)
- ♦ bančništvo po GSM (WAP, Monet)

Samopostrežni aparati

Plačilne kartice

- ♦ POS-terminali
- ♦ pametne kartice
- ♦ debetne kartice
- ♦ kreditne kartice

Vir: Miš Svoltjšak, 1999, str. 4–5; Interna literatura podjetja Halcom, d. o. o. , 1999.

Glede na subjekte, ki nastopajo v elektronskem bančništvu, ločimo v grobem tri vrste poslovnih odnosov:

- med bankami (npr. SWIFT³),
- med banko in podjetjem (pravnimi osebami),
- med banko in posameznikom (fizičnimi osebami).

Elektronsko poslovanje med bankami je uveljavljeno že kar nekaj časa. Na mednarodni ravni se je izoblikovalo zaprto omrežje bančnih organizacij – SWIFT. Omogoča hitro in nemoteno opravljanje transakcij med bankami v različnih državah. Uporabniki pridejo v omrežje s pomočjo računalniško podprte opreme, ki si jo lahko izberejo sami, mora pa ustrezati standardom SWIFT-a.

Vedno več elektronskega načina poslovanja poteka tudi med banko in pravnimi osebami. Pri nas je uvedba elektronskega bančništva za podjetja tesno povezana z reformo plačilnega

³ S.W.I.F.T. – Society to Worldwide Interbank Financial Transakcion – omrežje bančnih organizacij

prometa oziroma prenosom tolarških računov podjetij z Agencije za plačilni promet (APP) na poslovne banke. APP je namreč imela uveljavljen sistem elektronskega poslovanja s podjetji, zato so nekatera podjetja kot pogoj za odprtje transakcijskega računa pri banki zahtevala elektronsko bančništvo.

Elektronsko bančništvo lahko obravnavamo s širšega in z ožjega vidika. **V širšem smislu** je **elektronsko bančništvo** 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 se nanaša le na storitve virtualnega bančništva oz. bančništva, ki ga uporabljamo po internetu oziroma s pomočjo spletnih strani. Elektronsko bančništvo lahko torej opredelimo kot kakršenkoli način poslovanja strank z banko, ki je neodvisna od poslovalnic in temelji na informacijski tehnologiji (Sjekloča, 1999, str. 31).

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

- neprekinjena dosegljivost 24 ur na dan, sedem dni v tednu,
- dosegljivost kjerkoli,
- varnost in
- popolna avtomatizacija.

3.1.1 Razvoj elektronskega bančništva

Banka mora pri razvoju elektronskega bančništva upoštevati predvsem želje oz. zahteve strank ter tehnološke možnosti. Pri razvoju moramo upoštevati predvsem naslednja dejstva (Bračun, 1997, str. 150):

- uporabniki želijo opravljati storitve kjerkoli, kadarkoli, na kakršenkoli način;
- vrsta tehnologije, ki jo imajo na razpolago uporabniki (strankam naj ne bi vsiljevali tehnologije, ampak naj bi upoštevali tisto, ki jo imajo doma oz. v podjetju);
- vrsta telekomunikacijske infrastrukture v Sloveniji;
- način povezave banke s strankami;
- dolgoročni in kratkoročni učinki elektronskega bančništva;
- uporabniki morajo imeti zaupanje v storitev;
- banka mora poskrbeti za najvišjo stopnjo varnosti;
- ciljna skupina uporabnikov.

Ljudje nimajo časa za obisk bančnega okenca in čakanje v dolgih vrstah, zato od bančnih storitev, ki jih banke ponujajo na ta način, pričakujejo visoko kakovost. Z banko bodo komitenti elektronsko poslovali le v primeru, če bo le-ta poskrbela za varno poslovanje. Banka mora poskrbeti za primerno programsko in strojno opremo, ki zaščiti komitente pred

nepooblaščenim dostopom do podatkov in izvajanjem kakršnihkoli transakcij (Vrešak, 1997, str. 61).

3.1.2 Delovanje elektronskega bančništva

Standardni način

Bančne storitve (plačilne kartice, bankomati) imajo vrsto pomanjkljivosti, saj niso na voljo ves čas in na vsakem mestu, zahtevajo operaterje, pri nekaterih je vprašljiva tudi njihova varnost.

Komitent opravi elektronsko bančno storitev, tako da se s posebnim vmesnikom priključi na komunikacijsko omrežje, po katerem tečejo informacije o željeni storitvi do banke, ki je na komunikacijsko omrežje priključena s svojim vmesnikom. Banka opravi storitev v svojem informacijskem sistemu in pošlje potrdilo o opravljeni storitvi komitentu (glej sliko 2).

Slika 2: Princip delovanja elektronskega bančništva – standardni način



Vir: Kovačič, 1997, str. 132.

Elektronsko bančništvo po internetu

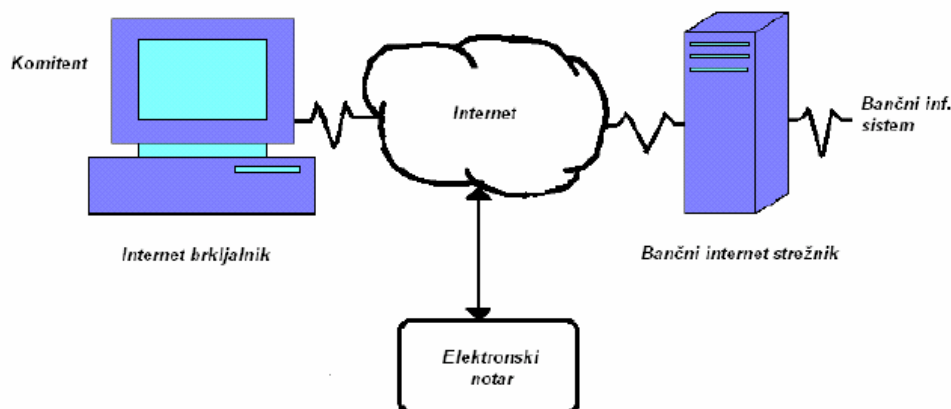
Ponujene storitve elektronskega bančništva delimo na **informacijske in transakcijske**. V okviru **informacijskih storitev** banka nudi informacije o stanjih in transakcijah na računih, o dogajanju na kapitalskih trgih itd.

Med **transakcijske storitve**, ki jih opravljamo s sistemi elektronskega bančništva, štejemo vse storitve, ki vključujejo plačilne instrumente.

Delovanje (glej sliko 3) elektronskega bančništva po internetu ima nekaj pomembnih prednosti (Kovačič, 1997, str. 132):

- temelji na javnem standardnem načinu prenosa po komunikacijskem omrežju, vmesniki so standardizirani;
- za uporabo komitenti potrebujejo le osebni računalnik z modemom, telefon in standardni vmesnik;
- vmesniki nekaterih najbolj uveljavljenih proizvajalcev so brezplačni;
- vmesniki podpirajo varen prenos podatkov po javnih telefonskih omrežjih;
- komitent in banka se lahko prepričata o medsebojni identiteti na standardiziran način.

Slika 3: Način delovanja sistemov elektronskega bančništva po internetu



Vir: Kovačič, 1997, str. 133.

Poglavitna področja bančne dejavnosti na internetu obsegajo internetno bančništvo (Internetbanking), domače bančništvo (PC banking) in informacije po internetu (webbased information delivery) ali internetno trženje.

Te dejavnosti so postale del bančnega poslovnega načrtovanja. Domači računalnik ali računalnik v podjetju postaja prava bančna podružnica, uporabnik bančne ponudbe pa neke vrste prostovoljni bančni uslužbenec. Iz tega lahko sklepamo o pozitivnih straneh elektronskega bančništva (Sjekloča, 1999, str. 31–33):

- zmanjšanje stroškov bančnega poslovanja;
- izginja potreba po klasičnem bančnem okencu, banke ne plačujejo stroškov komunikacije;
- stranki prihrani čas (krajše vrste v bankah);
- omogoča hitro in natančno informacijo o stanju računa ali bančnih storitvah;
- zanesljivost informacije (zaradi multimedijske komunikacije je ta zlahka preverljiva);
- kroženje denarja (pospešuje in omogoča bolj redno plačevanje obveznosti);
- spreminja profil bančnih uslužbencev (niso več administrativni delavci, ampak se posvečajo bolj dinamičnim poslom);
- odpira nove trge (domači računalnik je postal bančna podružnica, zato ni nujno, da je stranka v istem mestu kot banka. Tako izginjajo fizične meje trga).

Z reformo plačilnih sistemov so slovenske poslovne banke začele opravljati storitve plačilnega prometa tako za fizične kot za pravne osebe, s čimer so poleg novih poslovnih priložnosti naleteli tudi na organizacijske in tehnične probleme. Banke so se pri ponudbi svojih storitev namreč soočile z množico novih komitentov, katerim dotedanje tržne poti, po katerih so banke v začetkih devetdesetih let omogočale dostop do svojih storitev (bančno okence, bančni avtomat, telefaksno sporočanje in telefonski klicni center – teledom), zaradi obsežnosti njihovega poslovanja niso več zadoščale (Sistem elektronskega bančništva, 2004).

Že manjše podjetje namreč v povprečju opravi vsaj desetkrat več transakcij kot fizična oseba, vrednost teh transakcij je tudi stokrat višja, zato je zanj zelo pomemben sprotni vpogled v stanje in takojšnja možnost prenosa sredstev med svojimi računi na račune drugih oseb. Banka sredstva na računih komitentov obrestuje po minimalni obrestni meri, zato je na računih najbolje hraniti le toliko sredstev, kolikor jih podjetje potrebuje za zagotavljanje tekoče likvidnosti, vsa ostala sredstva pa takoj vloži v donosne transakcije.

3.2 PREDNOSTI ZA BANKO IN KOMITENTA

Tudi bančni trg se v skladu s trendi poslovanja bolj ali manj seli na internet, kar predstavlja za banke odlično priložnost za zniževanje različnih stroškov in hkrati za oblikovanje prijaznejših storitev po meri uporabnikov. Vendar tovrstni način poslovanja prinaša s seboj poleg različnih prednosti za ponudnike in komitente tudi različne slabosti.

Prednosti za komitente:

- prihranek časa,
- izognitev dolгим čakalnim vrstam pred bančnimi okenci,
- nizka cena storitev,
- večja preglednost in enostavnost uporabe ter možnost naročanja različnih storitev,
- večja svoboda uporabnika, ker ni časovnih omejitev,
- omogočena je večja stopnja zasebnosti,
- možnost dostopa do banke kjerkoli.

Med končnimi uporabniki je z uvedbo e-bančništva prisotna določena mera razočaranja, ker ni pričakovanega takojšnjega zmanjševanja stroškov in povečanja prihodkov. Vendar lahko koristi pričakujemo le na dolgi rok in so tako kot pri bankah kratkoročne koristi vidne v nemerljivih dejavnikih.

Banke vključujejo e-bančništvo kot del celovite strategije tržne poti. Najnaprednejše banke gledajo na e-bančništvo kot na osnovo za širšo strategijo e-poslovanja. Ne glede na strategijo mora banka imeti realna pričakovanja. Nikakor se račun ne izide, če pričakuje povrnitev stroškov investiranja v e-bančništvo čez noč. Koristi se ne pokažejo takoj, ampak jih lahko pričakuje v daljšem časovnem razmiku. Tako lahko koristi razvrščamo glede na čas. Kratkoročne koristi bančnega sektorja so: konkurenčna enakost, ohranjanje komitentov ter pridobivanje novih strank. Srednjeročne priložnosti so integracija tržnih poti, upravljanje informacij, celovit pogled na komitenta, migracija komitentov na ustrezne kanale ter tudi znižanje stroškov. Pozitivni rezultati investicije v e-bančništvo se pokažejo šele po 18. mesecih, tako glede zmanjševanja stroškov kot povečanja prihodka (Škedelj, 2002).

Prednosti za banke:

- zmanjšanje stroškov bančnega poslovanja: sem lahko uvrstimo predvsem nižje stroške bančnih transakcij, znižanje stroškov komunikacij, manjša poraba papirja... V primerjavi s klasičnim načinom poslovanja je strošek elektronske bančne transakcije do 15-krat manjši od cene klasične obdelave (Vozel, 1999, str. 47–75);

- boljši pregled nad poslovanjem in lažja obdelava podatkov;
- kakovostne storitve;
- zmanjšanje čakalnih vrst pred bančnimi okenci;
- pridobitev novih komitentov;
- ažurnost in informiranost o poslovanju komitentov;
- elektronsko zajemanje podatkov;
- natančno spremljanje dejanske uporabe;
- dolgoročno predstavlja takšen način poslovanja manj delovnih mest;
- manjše število potrebnih poslovalnic;
- pospešuje kroženje denarja in omogoča bolj redno plačevanje obveznosti (Sjekloča, 1999, str. 32);
- večja kakovost poslovanja, izhaja iz kakovostnejših podatkov, ki so v računalniški obliki in katerih obdelava ne dopušča napak, saj jih sistem obdela avtomatsko.

3.3 SLABOSTI ZA BANKO IN KOMITENTA

Slabosti za komitente:

- nezaupanje v tovrstni način poslovanja. To se kaže kot nezaupanje do elektronskih medijev, kar je značilno predvsem za starejše ljudi, hkrati pa komitente še dodatno skrbi varnost tovrstnega načina poslovanja z banko;
- pomanjkanje osebnega stika z banko.

Slabosti za banko:

- visoki stroški uvajanja tovrstnega načina poslovanja (vpeljava e-banke predstavlja zelo visoko finančno naložbo, vendar gre za dejansko dolgoročno zmanjšanje stroškov);
- pojavi se možnosti vdora v sistem in zlorabe podatkov;
- ustreznost kadra.

Banka mora zaposliti izobražen kader, ki je zanjo dražji, in to predstavlja dodatni strošek. Med vsemi stroški uvajanja elektronskega bančništva predstavlja največji strošek integracija v sistem, in sicer 50 odstotkov celotnih stroškov, sledi ji strošek strojne opreme s 30 odstotki in programska oprema z 20 odstotki.

Glede na prednosti in slabosti, ki sem jih predstavila v prejšnjih točkah lahko izluščimo, da so prednosti številčnejše, vprašljiva je edino varnost, ki je najpomembnejša, ko razmišljamo o lastnem denarju. Vendar varnost v današnjem času ni več vprašljiva, saj je ogromno varnostnih komponent, ki zaščitijo elektronske aplikacije vseh bank.

V nadaljevanju bom predstavila varnost e-bančništva, s katero želim posamezniku in podjetjem dokazati, da je e-bančništvo varno in nujno v današnjem poslovanju.

4 VARNOST ELEKTRONSKEGA POSLOVANJA

Z nastankom interneta se je razvil nov družbeni prostor, ki ga je nemogoče nadzorovati v celoti in ki omogoča tako stare kot tudi povsem nove oblike računalniške kriminalitete. Omrežje internet samo po sebi ne zagotavlja potrebnih pogojev za varno komunikacijo in e-poslovanje. Varnost računalniških sistemov in drugih pomembnih virov, ki jih obravnavamo v sklopu računalniškega omrežja, je treba zaščititi z izbiro ustreznih tehnologij, metod in rešitev, s kombinacijo ukrepov ter jih povezati v celoto tako, da bo varnost komunikacije po internetu največja.

Število možnih žrtev računalniške kriminalitete raste iz dneva v dan. Tako je že vsak uporabnik interneta postal potencialna možna žrtev (Power, 1998). Pri tem je opaziti, da naraščata tako obseg kot tudi raznovrstnost načinov in oblik izvajanja računalniškega kriminala. Zato nekatere, zlasti razvite države, ki so se že soočile z njimi, razmišljajo o zakonodajnih rešitvah, ki bi omogočile pregon tovrstnih kaznivih dejanj.

Zaščiteni oziroma zaupni podatki, ki so shranjeni na računalniških sistemih in potekajo po omrežjih, so za posameznike, podjetja in ostale ustanove kot npr. finančne organizacije, katerih dejavnost so denarni in kreditni posli, nevarnost razkritja podatkov, kar lahko pripelje do hudih posledic, kot je lahko finančni primanjkljaj. Zaupni podatki so lahko številke kreditnih kartic, poslovne skrivnosti, elektronske zdravstvene kartice, programske opreme sistemov, torej različne aplikacije, ki služijo za način izvedbe določene naloge. Napadi, pred katerimi se podjetja želijo zavarovati, ne prihajajo zgolj samo zunaj lokalnega omrežja podjetij, ampak tudi znotraj lokalnega omrežja, zato je treba sisteme zavarovati tako zunaj kot znotraj.

Internet je javno omrežje računalnikov, ki v veliki meri temelji na javnih telefonskih povezavah, katerim je relativno lahko prisluškovati. Podatke je zato treba narediti tajne in berljive le tistemu, ki so mu namenjeni. To dosežemo s šifriranjem (enkriptiranjem) podatkov na strani pošiljatelja in z dešifriranjem (dekriptiranjem) podatkov na strani naslovnika (Bedjanič, Lorenz, 1997, str. 58). Vsak komitent posebej in banka imata za šifriranje in dešifriranje podatkov dva ključa: javni in zasebni ključ. Zasebne ključe je treba varovati, javni pa morajo biti dostopni vsem. Javni ključ se uporablja za šifriranje podatkov, zasebni pa za dešifriranje podatkov.

Zagotovljena mora biti tudi možnost ugotavljanja verodostojnosti podatkov. To nam omogoča digitalni podpis, s katerim se zavarujemo pred spreminjanjem podatkov, ko ti potujejo po javnem omrežju. Vsakemu sporočilu dodamo še poseben izračunan povzetek, ki je šifriran s komitentovim zasebnim ključem, imenovanim digitalni podpis sporočila. Če se pri dešifriranju izračunani in sprejeti povzetek ne ujemata, lahko trdimo, da je prišlo do elektronskega vandalstva (Kovačič, 1997, str. 135).

Pred vsakršno uporabo javnega ključa je treba najprej preveriti njegovo avtentičnost oziroma ali ključ res pripada domnevnemu lastniku. To storimo s pomočjo certifikata, ki vsebuje javni ključ, tako da preverimo veljavnost digitalnega podpisa in ostalih podatkov v certifikatu. Identiteto podpisnika torej lahko popolnoma preverimo vsakič, ko preverjamo digitalni podpis. Pri lastnoročnih podpisih lahko avtentičnost podpisa potrdi le grafolog (Jerman Blažič, 2001). Preverjanje verodostojnosti zagotavljajo tako overovljeni certifikati bančnih komitentov kot tudi banke. Le-te pa shranjuje elektronski notar (certificate agency) – overitelj.

S protipožarno pregrado onemogočimo vdr v centralni bančni sistem. Kot zadnji element naj omenim kontrolo dostopa oz. avtorizacijo, ki določa, kaj stranka lahko počne in kaj ne. Poleg čim cenejših storitev, kar pomeni vse nižje obrestne mere in provizije, stranke želijo predvsem preprost dostop do svojega denarja ter hitro in natančno storitev. Banke, ki sledijo trgu, se morajo zavedati, da »stranka ni enaka stranki«. So stranke, ki so jim dovolj hitre elektronsko izvedene storitve, in so takšne, ki jim največ pomeni prijazna človeška beseda. Potrebno je spoznati svoje stranke. Hkrati pa ne smemo pozabiti, da elektronsko bančništvo pravzaprav ni bančna storitev v pravem pomenu besede, ampak je le distribucijski kanal. Zaradi tega naj navdušenje nad elektronskim bančništvom ne bi zameglilo pogleda bančnikom, tako da le-ti ne bi pozabili na osnovno nalogo bank (Miš-Svoljšak, 1998, str. 7).

4.1 OPREDELITEV VARNOSTNIH KOMPONENT

Za zagotovitev varnosti so na voljo različne kombinacije programske in strojne opreme ter fizičnega varovanja. Vodstvo je odgovorno za postavitve temeljne varnostne politike, kjer mora jasno definirati, kaj ščiti in zakaj, ter določiti, koliko sredstev je treba vložiti v varnostne ukrepe. Ukrepi morajo biti postavljeni široko, saj je težko vnaprej predvideti smer napada. Obseg varnostnih komponent je odvisen od stopnje zahtevane zaščite in oblike sistema.

Varnostna politika je kompromis med stroški in tveganji. Sistem je varen, ko imajo napadalci večje stroške od koristi vdora v sistem. V bančnih krogih je ta problematika še toliko bolj pomembna in občutljiva, saj operirajo s finančnimi podatki svojih komitentov. Stroški vdora v bančni sistem imajo lahko za posledice vidne (prenos denarja, koristoljubnost, izguba komitentov, izguba poslov, zloraba podatkov itd.) kot tudi nevidne (nezaupanje, zmanjšanje ugleda itd.) posledice, ki pogosto vplivajo posredno na vidne stroške (Kuščar, 2002, str. 8).

Osrednja točka varovanja pri e-poslovanju so viri, zoper katere preti nevarnost in imajo za lastnika določeno vrednost. Organizacija mora za zagotavljanje varnosti zadostiti naslednjim varnostnim storitvam (Jerman Blažič, 2001, str. 101):

- **overjanje**, možnost preveriti identiteto subjekta;
- **zaupnost**, informacije ne smejo biti razkrite nepooblaščenim osebam;
- **neokrnjenost**, ohranjanje pristnosti podatkov;
- **nadzor dostopa**, preprečevanje nepooblaščenih uporabe;
- **preprečevanje zanikanja o sodelovanju v aktivnostih e-poslovanja** ter

- **razpoložljivost**, storitve e-poslovanja so stalno na voljo.

Za zagotovitev omenjenih varnostnih storitev so na voljo različne metode. Njihova izbira je odvisna od zahtevanih varnostnih storitev, stopnje zaščite in oblike sistema. Vrste metod za zagotovitev varnosti v e-poslovanju so:

- kriptografija,
- požarni zid,
- elektronski podpis,
- gesla in drugo.

Splošne kategorije virov so: podatki, informacije pri prenosu in hranjenju, strojna in programska oprema, uporabniki in odnosi med njimi ter dokumentacija o postopkih strojne in programske opreme v sistemu ali omrežju (Jerman Blažič, 2001, str. 100).

Kriptografija

Že skozi zgodovino se je kriptografija ukvarjala s problemom, kako neko sporočilo prikriti ozkemu krogu ljudi. Kriptiranje oz. šifriranje je tako proces pretvarjanja berljivega teksta (čistopisa) v neberljivi tekst (tajnopis), ki ga je zelo težko ali celo nemogoče razbrati brez ustreznega ključa. Dekripcija pa je proces pretvarjanja šifriranega teksta v berljivo obliko.

V sodobnem elektronskem poslovanju se kriptografija uporablja tudi za ostale varnostne storitve (na primer za zagotavljanje, da vsebina originalnega dokumenta ni bila v času ali na poti spremenjena), ne le za zagotovitev tajnosti podatkov. Uporablja se tudi pri digitalnem podpisu ali časovnem žigu, pri plačevanju z digitalnim denarjem in na številnih drugih področjih interneta.

Simetrična kriptografija

Sprva se je uporabljala samo simetrična kriptografija, pri kateri uporabljamo isti ključ tako za šifriranje kot za dešifriranje. Pri tem nastane težava upravljanja s ključi: kako vsakemu uporabniku, ki bi želel naše sporočilo prebrati, ta ključ varno dostaviti. Zaradi tega se je uveljavila asimetrična kriptografija, ki rešuje ta problem.

Asimetrična kriptografija

Asimetrična kriptografija temelji na uporabi para ključev, javnega in zasebnega ključa. Če podatke šifriramo z enim ključem, jih lahko dešifriramo samo s pripadajočim komplementarnim ključem. Taka ključa imenujemo par asimetričnih ključev. Asimetrična kriptografija je mnogo počasnejša od simetrične, zato se v praksi uporablja hibridni pristop. Pri elektronski pošti je celotno sporočilo zašifrirano s pomočjo naključnega simetričnega ključa, nato pa je sam ključ zašifriran še z javnim ključem prejemnika.

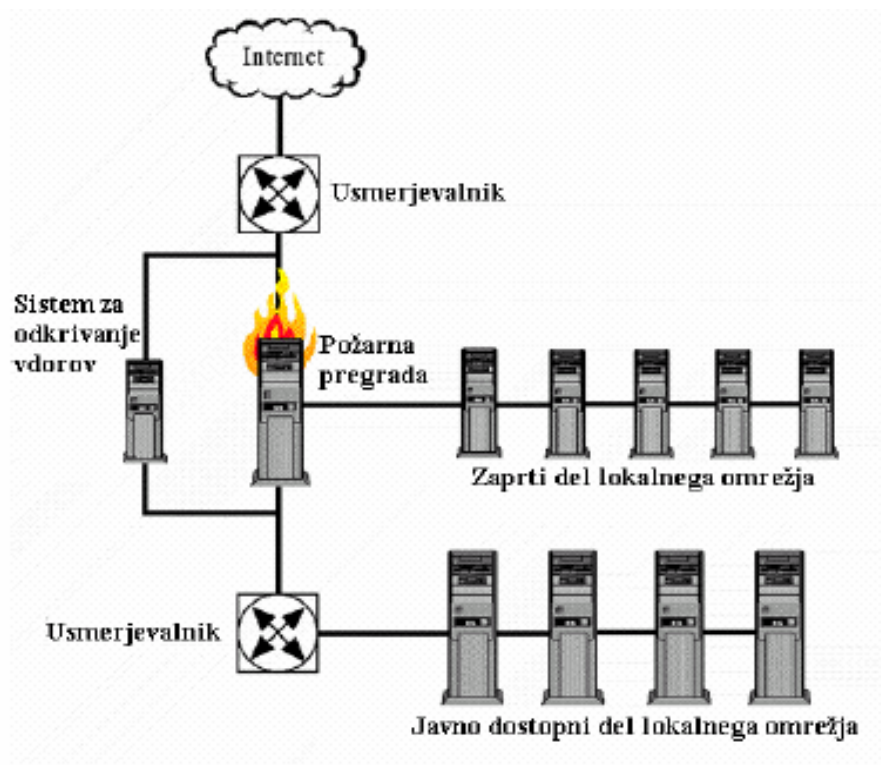
Sama uporaba asimetrične kriptografije v infrastrukturi javnih ključev nam zagotavlja celovitost, zaupnost, nezatajljivost sporočila in preverjanje identitete pošiljatelja. Če sporočilo

zašifriramo z javnim ključem prejemnika, ga lahko samo ta prejemnik dešifrira s svojim zasebnim ključem. Ravno obratno velja pri digitalnem podpisu, ko pošiljatelj podpiše sporočilo s svojim zasebnim ključem, prejemnik pa na podlagi njegovega javnega ključa preveri, ali je to sporočilo res podpisano s strani pošiljatelja in če med prenosom ni bilo spremenjeno.

Požarni zid

Požarni zid si lahko predstavljamo kot varnostna vrata ali vratarja, ki nepooblaščenim osebam ne dovoli vstopa v sistem, po drugi strani pa ne dopušča odnašanja podatkov iz sistema. Požarni zid z ustrezno strojno in programsko opremo implementira varnostno politiko v zvezi z uporabo virov in sistemov v internem lokalnem omrežju. Osnovna zahteva pri postavitvi požarne pregrade je, da imajo vsi uporabniki lokalnega omrežja čim manj oviran dostop do javnega omrežja, iz omrežja internet pa v lokalno omrežje prepuščamo le povezave do javnih strežnikov (glej sliko 4).

Slika 4: Osnovni model zaščite lokalnega omrežja



Vir: Young-Seock, 2000.

Požarna pregrada je tako namenjena preverjanju podatkov, ki se prenašajo med lokalnim omrežjem in internetom. Filter je tista komponenta požarnega zidu, ki nad vsakim paketom izvede množico pravil iz varnostne politike, določenih s strani administratorja. Pravila temeljijo na selektivni osnovi, ki filtrira vhodne dostope v svoje omrežje gleda na pravila, ki lahko temeljijo na uporabniških imenih, internetnih IP-naslovih pošiljatelja ali prejemnika, imenih domen, številkah komunikacijskih vrat itd. (Kalakota, 1997, str. 125). Požarni zid ne

more varovati virov podjetja pred napadi notranjih sodelavcev, saj je le vmesnik med internim omrežjem podjetja in internetom ali vmesnik med posameznimi oddelki podjetja, kot je to običajno v večjih podjetjih. V vsakem primeru lahko zaposleni v podjetju ukrade ključne informacije podjetja in poškoduje poslovne vire, ne da bi bilo to vidno na požarnem zidu. Tovrstne nevarnosti moramo rešiti z ustreznimi overitvenimi postopki (Collin, 1998).

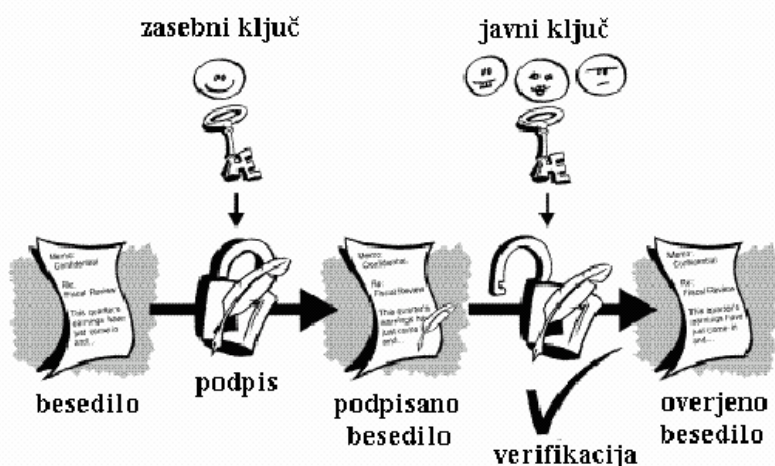
4.2 ELEKTRONSKI PODPIS

Poznamo več oblik elektronskega podpisovanja. Enostavne metode na podlagi simetričnih algoritmov ne zagotavljajo visoke stopnje varnosti kot to omogočajo metode na podlagi asimetričnih ključev. Elektronski podpis, ki je dobljen z elektronsko tehnologijo, za razliko od digitalnega podpisa, ki ga dobimo z asimetričnim šifrirnim postopkom, ne omogoča neokrnjenosti podpisanega dokumenta in identifikacije podpisnika (Toplišek, 1998, str. 30).

Elektronsko podpisovanje kot zaščita transakcij

Elektronski podpis je nadomestek lastnoročnega podpisa v elektronskem poslovanju. Razvitih je več metod elektronskega podpisovanja, med katere uvrščamo predvsem digitalni podpis, podpis z digitalnim peresom in biometrične metode. Podpis z digitalnim peresom je sistem, ki zajema sistem za zajemanje podpisa, sestavljen iz strojne in programske opreme, ter sistem za preverjanje podpisa. K biometričnim metodam spada kar nekaj metod, kot so npr. uporabnikovo glasovno sporočilo, test oči oz. dela očesa (šarenice), ki enolično določa vsakega človeka itd. Sistema sta zelo varna za identifikacijo uporabnika, vendar med uporabniki interneta zaradi prevelikih stroškov strojne opreme, potrebne za njegovo uporabo, ni doživel večjega uspeha. Danes se največ uporablja digitalni podpis, ki je zelo varen v elektronskem podpisovanju.

Slika 5: Prikaz podpisovanja elektronskih dokumentov



Vir: NA, 1999, str. 19.

Uporabnik lahko uporablja isti par ključev za šifriranje in digitalno podpisovanje, vendar to ni priporočljivo, ker se varnostne zahteve v obeh primerih razlikujejo. Zasebni ključ, ki ga uporablja za podpisovanje, mora generirati in poznati le njegov lastnik, saj le tako lahko podpis dejansko določa podpisnika. Zasebni ključ, ki se uporablja za šifriranje, mora včasih poznati še kdo drug. Ta zasebni ključ ne identificira subjekta, ampak omogoča izdelavo šifriranih podatkov. Z digitalnim podpisom zagotovimo pristnost podatkov in s tem tudi identifikacijo osebe. Vendar se pri tem postavljajo vprašanja, ali smo prepričani, da ključ res pripada naslovniku šifriranega sporočila oz. domnevnemu podpisniku podpisanega sporočila.

Digitalni podpis

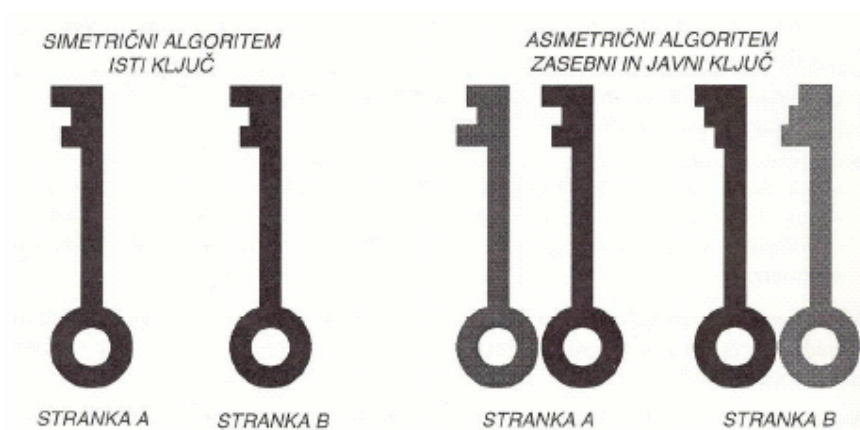
Digitalni podpis je kodiran oziroma šifriran prstni odtis ali zgoščena oblika elektronskega sporočila. Šifriranje spremeni podatke in informacije po nekem računskem postopku oz. algoritmu tako, da jih brez veljavnega kodnega ključa ne moremo dešifrirati oziroma povrniti v prvotno obliko. Pomen šifriranja je zagotavljanje zasebnosti sporočila, medtem ko digitalni podpis kot lastnoročni podpis v elektronski obliki omogoča večjo verodostojnost oziroma pristnost sporočila in nam razkrije identiteto osebe, ki se digitalno podpiše.

Da bi zagotovili identičnost lastnoročnega podpisa z digitalnim podpisom, mora podpis zadostiti naslednjim zahtevam:

- avtentičnost,
- podpisa se ne da ponarediti,
- podpisa se ne da kopirati,
- podpisanega dokumenta se ne da spremeniti in
- podpisa se ne da zanikati.

Podpisovanje dokumenta z uporabo metod asimetrične kriptografije poteka v dveh fazah. V prvi fazi podatke skrajšamo z eno izmed enosmernih zgoščevalnih funkcij, ki poljubno dolgo besedilo preslika v blok konstantne dolžine. Dobljeni blok, ki predstavlja »prstni odtis« besedila, šifriramo s svojim zasebnim ključem in tako dobimo digitalni podpis. Pri preverjanju podpisa naslovnik z javnim ključem pošiljatelja (podpisnika) dešifrira podpis in dobi povzetek. Ponovno izračuna povzetek pisma, ki je bilo poslano v nešifrirani obliki z isto zgoščevalno funkcijo kot pošiljatelj. Če se ujemata, pomeni, da je dobil tak dokument, kot ga je pošiljatelj podpisal. Če pa sta različna, je dokument podpisal nekdo drug ali je bila vsebina dokumenta spremenjena. Bistvo poteka digitalnega podpisovanja je, da podpisujemo s svojim zasebnim ključem, podpis pa preverimo z javnim ključem podpisnika.

Slika 6: Simetrično in asimetrično šifriranje



Vir: Pepelnjak, Bradeško, 1997, str. 164.

4.2.1 Digitalno potrdilo

Digitalno potrdilo je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo oziroma institucijo ali strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Je sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica) s specifičnim namenom, da zagotavlja varno in legitimno e-poslovanje. Potrdilo vsebuje javni ključ in informacijo o njegovem imetniku, ki jo podpiše oseba ali institucija, ki ji zaupamo. Potrdila so objavljena v splošno dostopnih imenikih ali na spletnih straneh.

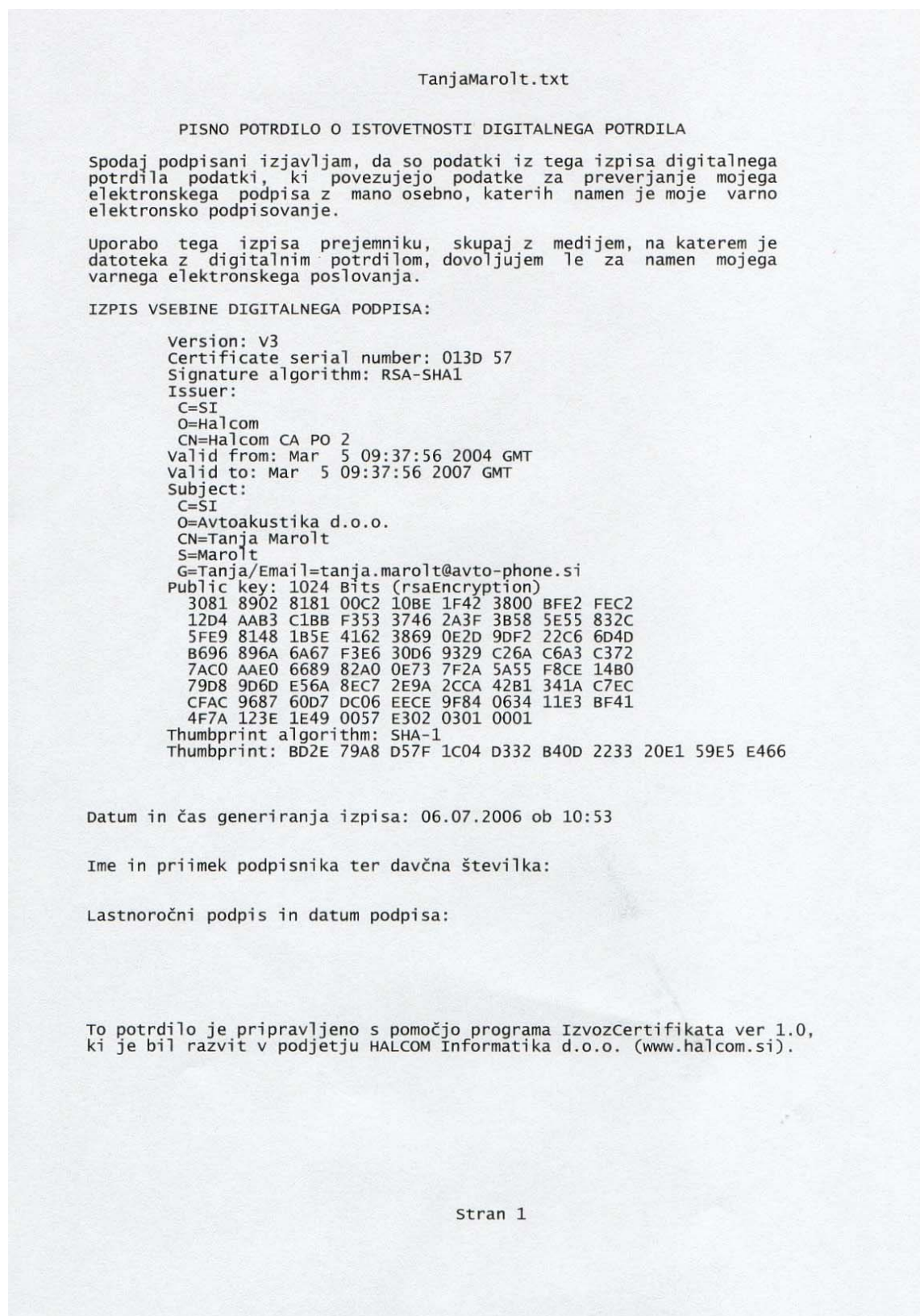
Digitalno potrdilo je digitalno podpisan računalniški zapis, ki vsebuje naslednje podatke:

- različico formata,
- serijsko številko potrdila,
- identifikator algoritmov,
- ime agencije, ki izdala potrdila,
- obdobje veljavnosti potrdila,
- ime lastnika javnega ključa,
- javni ključ in identifikator lastnika,
- enolično oznako uporabnika,
- razširitve in
- digitalni podpis teh podatkov, ki je narejen z zasebnim ključem.

Overjanje javnih ključev je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na simetrični kriptografiji oziroma digitalnem podpisu. Preverjanje povezave med identiteto uporabnika in njegovim ključem omogočajo v e-poslovanju posebne ustanove, imenovane overitelji javnih ključev.

Na naslednji sliki bo vidno moje staro digitalno potrdilo, ki ga izdajatelj digitalnega potrdila (v mojem primeru podjetje Halcom) pošlje ob prvem prevzemu oz. ob izdaji kartice. V prilogi dobite tudi zgoščenko, na kateri je nameščen program za kasnejši izpis digitalnega potrdila, če želite v svoj repertoar dodati še kakšno podjetje ali transakcijski račun že vključenega podjetja. Programček za izpis digitalnega potrdila se lahko dobi na internetni strani www.halcom.si, kjer izberete meni podpora ter program za izvoz digitalnih potrdil. V čitalniku mora biti nameščena kartica, s katere bi radi poslali potrdilo, saj program zahteva vnos zaščitne kode (PIN). Program shranite na računalnik in ga nato zaženete s shranjenega mesta. Ob zagonu se vam odpre spodnji dokument, v katerega je potrebno ročno dopisati še ime in priimek, davčno številko, lastnoročni podpis ter datum podpisa. Tako je dokument pripravljen za pošiljanje na banko.

Slika 7: Pismo potrdilo o identičnosti digitalnega potrdila



Vir: Lasten vir.

Preverjanje digitalnih potrdil

Kar nekaj podjetij in posameznikov že ima spletno digitalno potrdilo, ki je temeljni pogoj za uporabo nekaterih e-storitev, kot je elektronsko bančništvo. V Sloveniji sta za njihovo identifikacijo na voljo dve označbi: matična in davčna številka podjetja oziroma občana. Nekateri overitelji so se odločili, da davčno številko pravne ali fizične osebe vključijo v serijsko številko ali organizacijsko enoto razločevalnega imena v potrdilu, nekateri jo vključijo v posebno polje, nekateri pa je v potrdilo sploh ne zapišejo in vodijo lastno evidenco za identičnost potrdil z davčnimi številkami. Vprašanje pa je, kako preveriti potrdilo in pridobiti tudi podatke, ki so na njem zapisani. Lahko jih imenujemo spletni servisi posameznih podjetij.

Spletni servis za preverjanje davčnih številk preveri njihovo pravilnost. Pri nekaterih storitvah moramo vnesti tudi svojo davčno številko, ki jo servis na podlagi podatkov iz potrdila potrdi ali pa sporoči, da ni bila vnesena davčna številka. Servis deluje zgolj za potrdila, ki tako ali drugače vsebujejo zapis davčne številke. Tretji servis pa poskrbi za vračanje podatkov uporabniku storitev, a le tistih, ki so tako ali drugače že vsebovani v potrdilu in to ni v nasprotju z zakonom o varovanju osebnih podatkov.

Servis za preverjanje veljavnosti digitalnega potrdila preveri digitalni podpis, njegovo časovno veljavnost in preveri, ali je potrdilo morebiti preklicano. Bistvena pri tej zadevi je povezava z najnovejšim seznamom preklicanih potrdil. Z drugim imenom lahko temu rečemo tudi časovni žig.

4.2.2 Overitelj javnih ključev

Overitelj oz. agencija za certificiranje javnih ključev (CA) je ustanova, kateri zaupajo njeni komitenti – imetniki digitalnih potrdil. S tem jo tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Overitelj izdaja lastniku javnega ključa digitalno potrdilo, s katerim zagotavlja drugim uporabnikom avtentičnost ključa oziroma neločljivo veže uporabnika in njegov javni ključ. S pomočjo tega potrdila lahko lastnik dokaže lastništvo ključa in s tem tudi svojo identiteto.

Poleg agencij za overjanje javnih ključev imajo pomembno vlogo tudi uradi za registriranje (RA), ki sodelujejo pri izvajanju nalog CA. Razlika med agencijama (CA) in uradi (RA) je v tem, da agencija izda uporabniku digitalno potrdilo, s katerim jamči, da javni ključ res pripada lastniku potrdila, medtem ko so RA uradi, ki ne izdajajo potrdil, ampak preverjajo dokumente in registrirajo naročnika, ki zaprosi za potrdilo, preverijo njegovo identiteto in poznavanje javnemu ključu pripadajočega zasebnega ključa.

V svetu obstaja veliko različnih agencij za certificiranje javnih ključev. V Sloveniji imamo kar nekaj overiteljev javnih ključev, ki izdajajo potrdila za posamezna področja e-poslovanja. Za potrebe javne uprave in za uresničevanje projekta e-poslovanje javne uprave je bil

ustanovljen overitelj digitalnih potrdil na centru vlade Republike Slovenije za informiranje (CVI), ki izdaja dve različici digitalnih potrdil:

- SIGOV – CA (Slovenian GOVernmental Certification Authority), namenjena uporabi v javni upravi ter
- SIGEN – CA (Slovenian GENeral Certification Authority), namenjena pravnim in fizičnim osebam za izmenjavo podatkov z institucijami javne uprave in za dostop do podatkov, ki so v skrbništvu javne uprave.

4.2.3 Infrastruktura javnih ključev

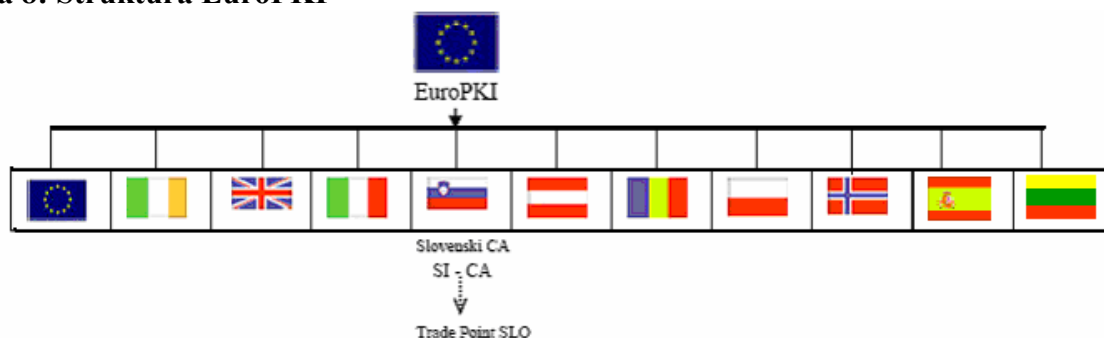
Infrastruktura javnih ključev (PKI – Public Key Infrastructure) je sistem za upravljanje s ključi in z digitalnimi potrdili, ki omogočajo vzpostavitev potrebnega zaupanja za e-poslovanje. Je kombinacija programske in strojne računalniške opreme ter politike in pravil certificiranja. Osnovna naloga PKI je omogočiti varno e-poslovanje uporabnikom, ki se ne poznajo in želijo varno komunicirati z uporabo asimetrične kriptografije. Podobno kot je nastajal sistem elektronskih naslovov in imen računalnikov, so začele nastajati posamezne infrastrukture javnih ključev, ki jih vpeljujejo vlade (Kanada, ZDA, Singapur, nekatere evropske države) ali posebne organizacije (Verisign, Thawte, EuroTrust). Te doslej še niso povezane med seboj, tako da lahko komunicirajo med seboj samo člani posamezne infrastrukture.

Pomembnejše storitve PKI so:

- generiranje, upravljanje, distribucija in hranjenje javnih ključev,
- overjanje ključev in izdajanje digitalnih potrdil javnih ključev,
- objavljanje digitalnih potrdil,
- preklicavanje digitalnih potrdil in
- časovna označitev postopkov.

Ključni se lahko uporabljajo za podpisovanje ali šifriranje v različnih okoljih (e-bančništvo, državna uprava, medorganizacijsko poslovanje, vojska itd.). Vsako okolje zahteva različno stopnjo varnosti in specifično strukturo PKI. Ena redkih PKI, katerih namen je združevanje CA iz različnih držav, je EuroPKI, ki je vrhovna agencija (glej sliko 8).

Slika 8: Struktura EuroPKI



Vir: Spletna stran Europki 2007.

Del te infrastrukture je tudi slovenska agencija za certificiranje SI-CA, ki podpisuje javne ključe drugih slovenskih overiteljev. PKI potrebujemo za vse storitve, katerih varnost se zagotavlja na podlagi asimetrične kriptografije, med njimi je tudi e-bančništvo. Na tem področju je ustanovljena vrhovna agencija – Identrus, ki so jo ustanovile največje svetovne finančne organizacije z namenom ponudbe globalnih storitev e-poslovanja med podjetji. Ključne lastnosti so globalni pristop, uporaba standardov odprtih sistemov, konsistentni poslovni proces in ocena tveganja pri e-poslovanju. Sistem je zasnovan na hierarhični infrastrukturi javnih ključev, ki povezuje sodelujoče banke s celega sveta (Jerman Blažič, 2001, str. 152).

Danes uporaba kriptografije za zagotavljanje varnosti ne zadostuje, zato si organizacije pomagajo še z dodatnimi mehanizmi, ki zaokrožajo neko varnostno celoto. To so: požarni zid, pametna kartica, uporaba gesel, varnostni protokoli itd.

4.3 PAMETNE KARTICE

Pametna kartica je plastična kartica z vgrajenim mikroposredstvom na čipu, ki se je v svetu prvič pojavila leta 1979.

Slika 9: Kartica Banke Koper, d. d.



Vir: Lasten vir.

Kartica je registrirana na ime podjetja in na osebno ime. Lahko se uporablja za bančne storitve za več podjetij, ki opravljajo plačilni promet oz. kakršnekoli druge storitve elektronskega bančništva.

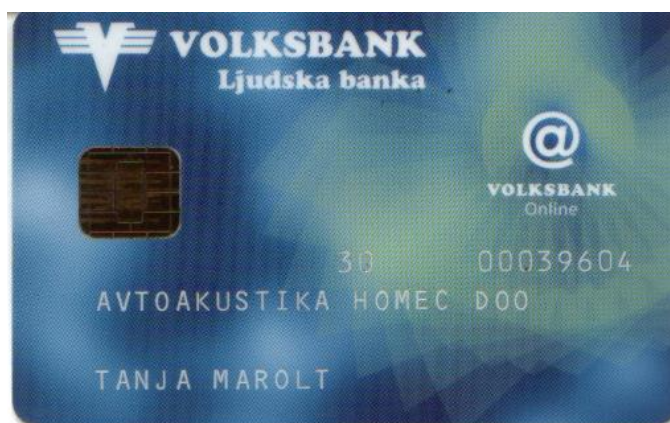
Slika 10: Kartica ena za vse – Halcom, d. d.



Vir: Lasten vir.

Kartica je registrirana na ime podjetja, čeprav to ni razvidno s same kartice. V sklopu Halcomovih rešitev se lahko uporablja za več transakcijskih računov, odprtih pri različnih bankah in za več podjetij hkrati.

Slika 11: Kartica Volksbank – Ljudske banke, d. d.



Vir: Lasten vir.

Kartica je registrirana na ime podjetja in na osebno ime. Lahko se uporablja za bančne storitve za več podjetij, ki opravljajo plačilni promet, oz. kakršnekoli druge storitve elektronskega bančništva.

Pojem pametna kartica opisuje mikroračunalnik, ki je v ohišju kartice. Tehnologija pametnih kartic nam omogoča prenos in hranjenje informacij s pomočjo integriranega vezja, ki je vgrajeno v kartico in na katerem lahko hranimo šifrirni ključ oz. digitalno potrdilo. Kartica poskrbi, da se podatki z zunanjim svetom izmenjujejo na varen in zanesljiv način. Na površini kartice so priključki, ki so namenjeni izmenjavi podatkov med čitalnikom in kartico. Tako je s pomočjo čitalnika s temi karticami mogoče poslovati kjer koli, vendar je treba čitalnik predhodno namestiti na računalnik.

Slika 12: Čitalniki pametnih kartic



Vir: Internetna stran Halcom, d. d.

Danes so pametne kartice nadomestile uporabo kartic z magnetnim zapisom, ki se na trgu pojavljajo že dlje časa in so cenejše ter slabše zaščitene pred zlorabami. S pomočjo posebnih naprav se lahko zapis z magnetne kartice prekopira na drugo. Magnetno kartico se lahko uporablja brez poznavanja gesla (PIN), saj za uporabo zadošča že podpis, ki ga lahko oseba brez težav ponaredi. V primerjavi z magnetno kartico pametna kartica dovoli e-podpisovanje le z vnosom osebnega gesla, ki ga pozna samo imetnik kartice. Poleg tega tehnologija pametne kartice preveri, ali je terminal, po katerem poteka plačilo originalen ter preveri pravilnost kartice in identifikacijo imetnika kartice z uporabo PIN-kode. Takšen postopek je varnejši, saj je pametna kartica brez ustreznega PIN-a praktično neuporabna in se ob treh napačnih poskusih gesla zablokira. To je tudi glavni razlog, zakaj je uporaba pametne kartice varnejša od uporabe magnetne kartice.

4.4 GESLA IN DRUGA ZAŠČITA

Najstarejši in najenostavnejši način preverjanja identitete je identifikacija s pomočjo gesla oz. določene informacije, ki določa neko osebo ali subjekt. V e-poslovanju kot tudi v e-bančništvu se z gesli ali identifikacijskimi številkami srečujemo praktično na vsakem koraku. Predstavljajo najenostavnejši način identifikacijske uporabnosti in so ključ dostopa do varovanih podatkov.

Gesla uvrščamo med šibkejšo zaščito varovanja zaradi naslednjih razlogov:

- uporabniki si večinoma sami izbirajo gesla, ki si jih je lažje zapomniti in katera se da tudi lažje razkriti. Ugotavljanje tujih gesel poteka s pomočjo elektronskih slovarjev, s poznavanjem uporabnikovih podatkov in s preizkušanjem že uporabljenih gesel. Daljša izbrana gesla si uporabniki pogosto zaradi možnosti izgube nekje zapišejo, kar je lahko lahek plen za nepridiprave;
- pri identifikaciji razkrijemo svoje geslo in tako omogočimo naslovniku, da se izdaja pod našim imenom;
- gesla se po navadi prenašajo v nešifrirani obliki in so tako lahko tarča napadalcev. Čeprav so gesla predhodno šifrirana, jih napadalec lahko prestreže in uporablja v takšni obliki za kasnejše predstavljanje.

Zaradi navedenih razlogov šibko overjanje s pomočjo gesel ni primerno za preverjanje identitete v e-poslovanju, razen za dostop do lokalnega sistema ali, aktiviranje določenih naprav (pametne kartice, internetni brskalnik itd.). Pogosto gesla zamenjujejo PIN-kode, ki se uporabljajo za avtorizacijo pri bankomatih, POS-terminalih ter v kombinaciji z magnetnimi in s pametnimi karticami.

Varnost gesel v javnih omrežjih lahko izboljšamo z varnostjo z enkratnimi gesli. Posamezno geslo se uporabi le enkrat, zato prestrezanje gesel nima pravega pomena. Pri tem načinu je zelo pomembno, da se iz preteklih gesel ne da izračunati prihodnjega gesla. Najenostavnejši način brez uporabe kriptografskih algoritmov je uporaba enkratnih gesel z vnaprej generiranih določenih naključnih gesel. Slabost takšnega sistema je, da gesla shranimo v računalnik in jih za overjanje uporabljamo po seznamu.

Najbolj znan način za identifikacijo s pomočjo enkratnih gesel je uporaba kartice, ki vsebuje mikroprocesor in ekran ter je sinhroniziran z uro na strežniku. Kartica Secur ID (glej sliko 13) spreminja svoje geslo vsakih 60 sekund, kar je razvidno s črtic v levem robu zaslona. Za aktiviranje te kartice ne potrebujete nobenega dodatnega gesla, saj vam kartico pošljejo posebej programirano za vaše uporabniško ime in geslo. Drugačen je postopek pri zasnovi kartice SKB banke, d. d., izdelane za elektronsko bančništvo za fizične osebe (glej sliko 14). Uporabnik, ki želi dokazati svojo identiteto, vtipka na kartici geslo za njeno uporabo, algoritem pa nato na podlagi trenutnega časa generira geslo, katero uporabnik pošlje na strežnik.

Slika 13: Kartica NKBM, d. d.



Vir: Internetna stran NKBM, d. d.

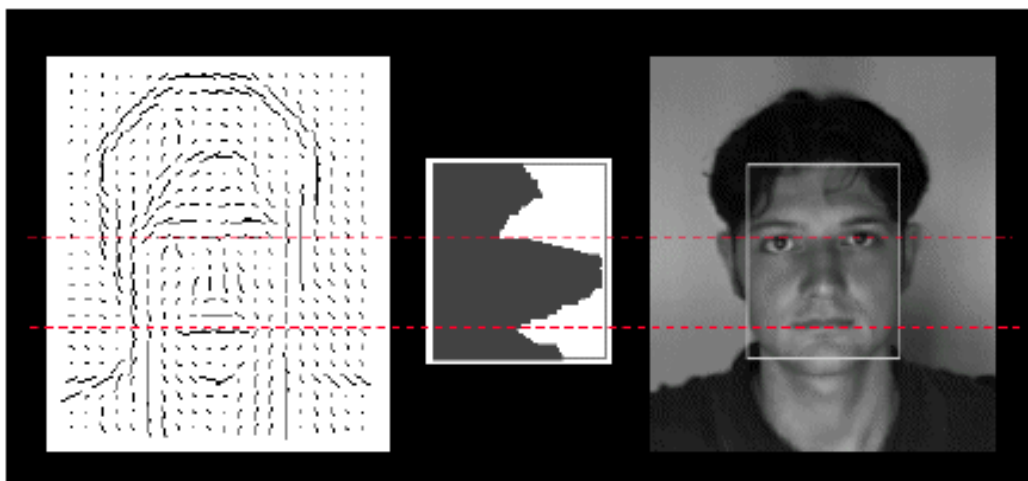
Slika 14: Kartica za uporabo SKB net-a (fizične osebe)



Vir: Internetna stran Actividentety Corporation.

Poleg enkratnih gesel poznamo še druge načine dokazovanja identitete uporabnika. Boljši načini dokazovanja identitete so na podlagi biometričnih lastnosti. Preverjanje uporabnika bo nekoč temeljilo na biometriki, ki se nanaša na poznavanje in razlikovanje fizičnih karakteristik posameznika. Uporabljala se bo lahko tehnologija prepoznavanja obraza (glej sliko 15), prstnih odtisov, prepoznavanje glasu ali celo zenice. Pri tehniki prepoznavanja obraza infra rdeča kamera skenira obraz in s tem dobi zapis žilnega sistema našega obraza, ki ga nato shrani kot obrazni termogram. Vsakič, ko bomo hoteli poslovati s svojo banko, nam bo ta naprava skenirala in hkrati preverila, ali ustrežamo vzorcu, zapisanem v bazi dostopa.

Slika 15 : Primer biometrične zaščite s prepoznavanjem obraza



Vir: Ošlak, 2005.

5 PONUDBA BANK V SLOVENIJI

V Sloveniji je elektronsko bančništvo zelo razvito, saj ga ponujajo praktično vse banke, ki se dobro zavedajo pomembnosti elektronskega poslovanja in predvsem elektronskega poslovanja po internetu, saj ima danes že skoraj vsaka banka razvito spletno bančništvo tako za pravne kot tudi za fizične osebe.

Z začetkom internetnega bančništva je povezano poslovanje SKB banke v letu 1997. Začetni problem SKB je bila organiziranost, klasične enote in elektronsko bančništvo sta bila dva samostojna dobičkonosna centra. Pri tem je nastal problem, saj klasične enote niso želele reklamirati oziroma promovirati internetnega bančništva, saj so s tem izgubljale svoje stranke. Zakaj? S tem, ko so uporabniki svoje storitve opravili po internetu, je provizijo zaračunal drug dobičkonosni center, kot bi ga v primeru klasičnega poslovanja preko okenca. Problem so hitro rešili in internetno bančništvo je postalo podkanal klasičnih enot, se pravi le drugačna, cenejša tržna pot do uporabnika, kar so logično posnemale tudi ostale banke (Bračun, 2004).

Danes se e-bančne poslovalnice med seboj zelo razlikujejo. Predvsem je opazna razlika med večjimi in bolj znanimi slovenskimi bankami ter tistimi manjšimi, saj prve vlagajo znatno več sredstev v razvoj in popularizacijo njihovih e-bančnih storitev, zato so tudi bolj dopolnjene, organizirane, atraktivne in predstavljene.

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 drag. Vedeti pa moramo, da se po velikosti tudi naše največje banke ne morejo primerjati z večjimi evropskimi ali s svetovnimi bankami.

Največjo prednost ima Nova Ljubljanska banka, katere e-bančna storitev, Klik in Proklik, je najbolj razširjena med vsemi, saj jo uporablja tudi nekaj drugih bank (kar bo vidno tudi iz spodnje razpredelnice - glej tabelo 3).

Tabela 3: Pregled bank, ki omogočajo spletno bančništvo za pravne osebe

ZAP. ŠT.	IME BANKE	URL	E-BANČNIŠTVO ZA PRAVNE OSEBE
1	ABANKA VIPA, d. d.	http://www.abanka.si/	Abanet
2	BANK AUSTRIA CREDITANSTALT, d. d., LJUBLJANA	http://www.ba-ca.si/	Online b@nka
3	BANKA CELJE, d. d.	http://www.banka-celje.si/	eBankir
4	BANKA KOPER, d. d.	http://www.banka-koper.si/	i-Net Banka
5	BANKA SPARKASSE, d. d.	http://www.sparkasse.si/	Net.Stik
6	DEŽELNA BANKA SLOVENIJE, d. d.	http://www.dbs.si/	DBS PRONET
7	FACTOR BANKA, d. d.	http://www.factorb.si/	Elektronsko bančništvo
8	GORENJSKA BANKA, d. d., KRANJ	http://www.gbkr.si/	LINK+, LINK C
9	HYPO ALPE-ADRIA-BANK, d. d.	http://www.hypo-alpe-adria.si/	HYPOnet
10	NLB BANKA DOMŽALE, d. d.	http://www.banka-domzale.si/	Proklik NLB
11	NLB BANKA ZASAVJE, d. d.	http://www.banka-zasavje.si/	Proklik NLB
12	NLB KOROŠKA BANKA, d. d.	http://www.koroska-banka.si/	Proklik NLB
13	NOVA KREDITNA BANKA MARIBOR, d. d.	http://www.nkbm.si	Poslovni Bank@Net
14	NOVA LJUBLJANSKA BANKA, d. d., LJUBLJANA	http://www.nlb.si/	Proklik NLB
15	POŠTNA BANKA SLOVENIJE, d. d.	http://www.pbs.si/	Poslovni PBS.net
16	PROBANKA, d. d.	http://www.probanka.si/	Poslovni Prosplet
17	RAIFFEISEN KREKOVA BANKA, d. d.	http://www.r-kb.si/	Eureka, RB-online
18	SKB BANKA, d. d., LJUBLJANA	http://www.skb.si/	PRO SKB NET, MULTI SKBNET, B2B SKB NET, SOGECASH
19	VOLKSBANK - LJUDSKA BANKA, d. d.	http://www.volksbank.si/	Volksbank online

Vir: Spletni podatki bank v Sloveniji

Sistem elektronskega bančništva so banke zasnovale in razvile na podlagi lastnega kadra oz. so programske rešitve kupile od specializiranih ponudnikov:

1. Halcom, d. d. (NLB, d. d., Abanka Vipra, d. d., SKB banka, d. d. ...)
2. Zrcalo, d. o. o. (NKBM, d. d. ...)
3. Adacta, d. o. o. (Banka Koper, d. d., Volksbank – Ljudska banka, d. d.)
4. ...

Ponudniki so prisiljeni izdelati čim kvalitetnejšo rešitev, ki naj bi bila zasnova za čim večjo varnost in bi zagotavljala enostavno funkcionalnost in preglednost. Slabost se kaže v nepovezanem razvoju. Proizvajalci ponujajo programske aplikacije, ki podpirajo različne programske vmesnike in uporabnikom, ki poslujejo z več bankami hkrati, otežuje delo, ker so prisiljeni nameščati in vzdrževati več sistemov. Posledica tega je precej različna in bolj ali manj nezdružljiva programska oprema e-bančništva.

5.1 HALCOMOV PROGRAM

E-banka je sistem za e-bančništvo, zasnovan pri podjetju Halcom, d. d. V Sloveniji ga uporablja več kot 40.000 podjetij pod različnimi imeni (Proklik NLB, Abacom, E-bank). Že na samem začetku, ki sega v leto 1996, so poudarjali pomen varnosti. V svoje izdelke so vgrajevati vse tri komponente varnosti, ki jih predvideva PKI-sistem zaščite. Te so:

- zagotavljanje zasebnosti na osnovi šifriranja,
- preverjanje istovetnosti uporabnika in javnega ključa na osnovi digitalnega potrdila,
- preverjanje verodostojnosti podatkov na osnovi digitalnega podpisa.

Uporaba vseh treh varnostnih komponent skupaj omogoča, da je varnost nadzorovana in neodvisna od varnosti trenutnih različnih brskalnikov ali drugih elementov operacijskega sistema oziroma spletne aplikacije.

Pri E-bank gre za princip varovanja samega plačilnega naloga z digitalnim podpisom. Uporabnik vsak nalog digitalno podpiše s svojim zasebnim ključem, ki ga ima shranjenega na pametni kartici in ne na računalniku, kar omogoča banki nedvoumno ugotavljanje pristnosti podatkov. Banka za vsak plačilni nalog preveri istovetnost uporabnika. Princip pošiljanja podatkov in digitalno podpisovanje sta zasnovana na kombiniranem šifrirnem načinu podobno SSL-u⁴. Na začetku izmenjave podatkov bančni strežnik in uporabnikov programski paket tvorita simetrični ključ, ki si ga izmenjata z uporabo svojih javnih ključev z algoritmom RSA (1024-bitni ključ na strani podjetja in 2048-bitni ključ v banki). S simetričnim ključem se podatki s pomočjo algoritma 3DES zašifrirajo in na strani banke dešifrirajo z istim ključem. Identifikacija uporabnika in elektronsko podpisovanje potekata z zaščitno kartico, ki hrani digitalno potrdilo in zasebni ključ. Digitalna potrdila izdaja podjetje Halcom, saj ima lastno agencijo za certificiranje.

Podjetje Halcom svojim strankam ponuja dve uporabniški različici, ki se razlikujeta glede na število računalnikov, povezanih v sistem elektronskega bančništva v podjetju.

Večuporabniška različica

Večuporabniška različica je namenjena tistim podjetjem, ki želijo izvajati domači plačilni promet in plačilni promet s tujino na različnih računalnikih, povezanih v lokalno mrežo. Ta različica deluje na principu odjemalec - strežnik zato potrebuje za nemoteno poslovanje

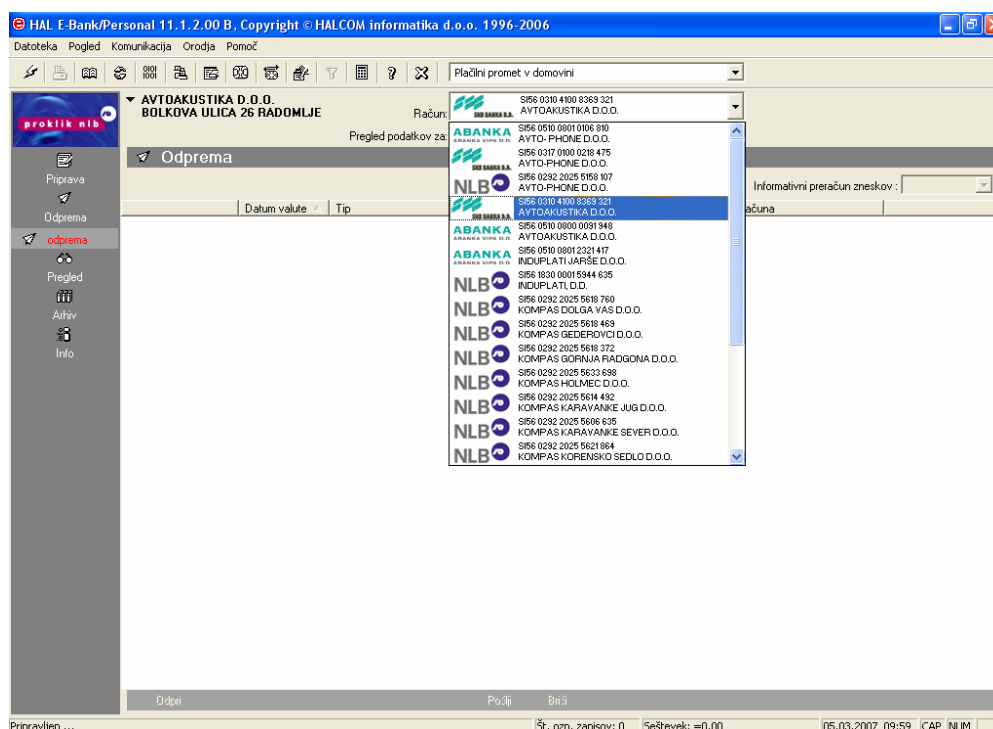
⁴ SSL (Secure Sockets Layer) je splošno sprejet varnostni protokol za varen prenos občutljivih podatkov po internetu. Podatki so na poti med odjemalcem (brskalnik) in internetnim strežnikom zakodirani.

skupno zbirko podatkov, ki so nameščeni na »centralnem« računalniku v podjetju. Zato potrebujemo tudi neki centralni strežnik, ki je praviloma zmogljivejši od drugih in ima vlogo baznega strežnika. Centralni računalnik mora imeti nameščeno programsko opremo strežnika podatkov, kot je na primer zbirka IBM DB2 UDB Workgroup Edition 6.1, za odjemalske delovne postaje (torej vse druge uporabljene računalnike) pa ustrezen uporabniški vmesnik, kot je: IBM Client Application Enabler ter programsko opremo ustrezno konfigurirati.

Enouporabniška različica

Enouporabniška različica je namenjena predvsem tistim podjetjem in samostojnim podjetnikom, ki želijo imeti program nameščen le na enem računalniku. V tem primeru je baza podatkov nameščena na istem računalniku kot program. Na tem računalniku lahko opravlja elektronski plačilni promet eden ali več uporabnikov, vendar se mora vsak identificirati s svojo pametno kartico, poleg tega mora imeti pooblastilo vodstvo podjetja.

Slika 16: Enouporabniška različica programa Halcom



Vir: Lasten vir.

S slike 16 je lepo razvidno, da se program lahko uporablja za poslovanje večjega števila podjetij in bank. Pri programu je možnost, da sami izberemo, katero podjetje želimo, da se nam prikaže ob prvi prijavi. V nadaljevanju, ko želimo pregledovati podatke za drugo podjetje, kliknemo na puščico in izberemo, za katero podjetje želimo pregledati stanje, plačati obveznosti ...

Pri sami prijavi stanje sredstev na računu ni osveženo, zato moramo pri prvem vstopu v program, za osvežitev podatkov klikniti na ikono za osvežitev programa in ponovno vpisati osebno geslo. To je treba ponoviti za vsako banko posebej.

Če je treba osveževati vsako banko posebej, da dobimo osvežena stanja, je pri imeniku prejemnikov le-ta skupni, za celoten program.

Če našemu trenutnemu seznamu podjetij dodamo novo podjetje, ki posluje pri isti banki kot že prijavljena podjetja, se bo le-to prikazalo na seznamu ob prvi osvežitvi stanja izbrane banke podjetja.

Če že obstoječe podjetje odpre račun pri banki, ki še ni na našem seznamu, moramo v zavihku komunikacija izbrati opcijo moja prva povezava na banko, izbrati to novo banko ter potrditi izbor. Nekatere banke nas pokličejo in obvestijo, naj sprožimo aktivnost moja prva povezava.

S pomočjo programa Halcom je možno poslovanje z več računi na različnih bankah v Sloveniji:

1. Nova Ljubljanska banka, d. d.
2. NLB Banka Domžale, d. d.
3. Banka Zasavje, d. d.
4. Koroška banka, d. d.
5. Abanka Vipava, d. d.
6. Bank Austria Creditanstalt, d. d.
7. SKB banka, d. d.
8. Factor banka, d. d.
9. Kärntner Sparkasse, d. d.
10. Raiffeisen Krekova banka, d. d.
11. Hypo Alpe-Adria-bank, d. d.
12. Probanka, d. d.

5.1.1 Nova Ljubljanska banka, d. d.

Nova Ljubljanska banka (v nadaljevanju NLB) je največja banka in hkrati matična banka v skupini NLB, kjer je vključenih več kot 50.000 podjetij in 900.000 individualnih strank. NLB lahko s svojimi absolutnimi primerjalnimi prednostmi v slovenskem prostoru – z velikostjo, močjo in mednarodnimi referencami – učinkovito poslovno podpira tudi največja in najbolj dinamična podjetja pri njihovem poslovanju doma in na mednarodnih trgih.

Glavna konkurenčna prednost pred drugimi je v hitrosti in stroških prometa. V tem kontekstu je za gospodarske subjekte izjemno pomembno, da lahko opravijo čim več prometa znotraj enega bančnega sistema, saj ima interni promet številne prednosti pred eksternim. Je objektivno najcenejši, najhitrejši (izvaja se v realnem času), njegov umik pa je do 2 uri daljši od umika za eksterna medbančna plačila prek sistemov žiro kliringa in BPRČ. Vendar pa velikost banke pogosto požene v precejšno togost in okretnost, saj zaradi preobremenjenosti pogosto prihaja do prekinitev povezav in do počasnejšega delovanja sistema.

V Novi Ljubljanski banki so razvili že celo paleto poti poslovanja z banko oz. kot jih v NLB-ju imenujejo »bližnjic do banke«. Komitente so razporedili v dve skupini, na fizične (občane, študente) in na pravne osebe. V slednjo poleg podjetij uvrščajo tudi samostojne podjetnike, ki imajo pri poslovanju določene lastnosti pravnih oseb. V nadaljevanju bom predstavila elektronski banki **Proklik NLB** in **Proklik plus NLB**, ki ju je banka razvila za pravne osebe in zasebnike, da bi kar najlažje opravljali plačilni promet doma in s tujino.

Razlog, da so razvili dve rešitvi, je v prilagajanju potrebam strank banke, ki zaradi različnih informacijskih sistemov v podjetju potrebujejo različne načine povezave z bančnim strežnikom. Potrebo po tem je pokazala raziskava, ki so jo opravili med srednjimi in velikimi podjetji – komitenti NLB.

Pot za opravljanje transakcij preko bank bančne skupine Nove Ljubljanske banke, ki je bila sprva na voljo samo samostojnim podjetnikom, so poimenovali Proklik NLB (v nadaljevanju Proklik). Uporabljati so jo začeli v začetku maja leta 1999. Po manj kot dveh mesecih delovanja so sredi junija zabeležili več kot 500 uporabnikov, ki so s pomočjo Proklika posredovali več kot 5000 nalogov. Istočasno so Proklik testno ponudili tudi pravnim osebam. V začetku leta 2000 pa je bil na voljo vsem podjetjem.

Banka je na ta način uporabniku zagotovila povezavo do strežnika elektronskega bančništva preko lastne vstopne točke, torej klicni dostop. Povezava poteka podobno kot po internetu, razlika je v tem, da se podatki ne prenašajo po nenadzorovanih delih omrežja. Vendar pa se je pri nekaterih komitentih pojavila potreba, da bi za izvajanje plačilnega prometa po elektronski poti uporabljali program, ki bi omogočal dostop do bančnega strežnika po internetu. Velika tržna zahteva po tej možnosti je NLB usmerila v razvoj nove rešitve, ki bi to omogočala. Razvili so Proklik plus NLB. Strankam je bil na voljo v začetku meseca aprila 2001. Do konca leta je število podjetij, ki so uporabljala to sodobno pot naraslo na 800. Ta vrsta povezave je zanimiva pravzaprav za vsakega uporabnika, saj je danes le malo podjetij, ki nimajo priključka na internet. Povezovanje z bančnim strežnikom na ta način je še posebej zanimivo za podjetja, ki imajo račun pri različnih bankah, za podjetja, ki imajo široko razporedeno svojo lastno mrežo računalnikov in so geografsko razpršena.

Program Proklik plus NLB je bil dne 16. 1. 2006 dokončno ukinjen. Na NLB, d. d. kot vzrok ukinitve navajajo, kratko in jedrnato, da gre za poslovno odločitev banke.

Vrste uporabnikov

Vsi tipi uporabnikov se enakovredno vključujejo in uporabljajo isti uporabniški program, čeprav ima vsak tip uporabnika določene posebnosti. Nekatere so določene z vnosom tipa uporabnika v sistem, druge pa z omejitvami, ki jih postavlja zakonodaja ali bančna pravila. Uporabniki so:

- samostojni podjetniki,
- neporavnalne banke (hranilno-kreditne službe in hranilnice),

- pravne osebe z odprtim transakcijskim računom v eni izmed bank, naštetih v prejšnji točki.

5.1.2 SKB banka, d. d.

Leta 1995 je SKB banka prvič predstavila e-bančništvo (5 let po prvi spletni banki v svetu). Nekaj mesecev kasneje so začeli uporabljati storitve e-bančništva že prvi uporabniki. Že od samega začetka je na protokolu SSL poskrbljeno za varnost pri prenosu z 128-bitnim šifriranjem. Sčasoma so dograjevali varnostne komponente, saj je bila zahtevana visoka varnostna politika. Svojo programsko rešitev so zaščitili s sistemom PKI v sodelovanju z družbo ActivCard – tehnologijo pametnih kartic. V letu 2000 se je ponudba razširila na mobilno bančništvo z WAP⁵ protokolom. Danes SKB banka v povezavi s SEB sistemom ponuja integriran sistem bančništva v sistem podjetja (Bračun, 2003).

Banka se poskuša prilagoditi vsem oblikam podjetij in jim ponuja programske različice:

1. **SKB NET** za samostojne podjetnike in manjša podjetja, ki opravijo do 100 nalogov na mesec. Dostopen je s kateregakoli računalnika z dostopom do interneta. Za njegovo uporabo ne potrebujemo posebnih programov, dovolj je sodoben brskalnik s 128-bitnim varnostnim ključem.
2. **Poslovni SKB NET** za srednja in velika podjetja, ki poslujejo tudi s tujino in opravijo do 1000 nalogov na mesec. Za razliko od SKB NET-a omogoča delo brez stalne povezave z banko.
3. **Multi SKB NET** za velika in zelo velika podjetja z več kot 1000 transakcijami na mesec. Omogoča dostop do večih bank z eno samo pametno kartico in zagotavlja prilagoditev e-bančništva obstoječemu računovodskemu sistemu v podjetju. Multi SKB NET je primeren za podjetja, ki poslujejo s tujimi poslovnimi partnerji, saj je Multi SKB NET vključen v MultiCash sistem, ki povezuje poslovalnice po vsem svetu.

Elektronsko bančništvo SKB banke je sodoben in varčen način poslovanja, ki omogoča varen dostop do banke, poslovnih partnerjev in do sveta nasploh. Da lahko uporabljamo elektronsko bančništvo, potrebujemo samo transakcijski račun in seveda računalnik, da omogoča delo z internetom. SKB banka nudi kar nekaj elektronskih produktov, in sicer: SKB net, poslovni SKB net, multi SKB net, Sogecash in multi SKB net B2B. Poleg teh produktov je še na voljo zbirni center SKB net in telefonsko bančništvo, kot je zeleni telefon, bankotel, avtomatski odzivnik za devizne tečaje in mobilno bančništvo – Wap SKB net. Te sodobne bančne poti lahko uporabljajo pravne osebe, samostojni podjetniki, obrtniki in drugi. SKB Banka, d. d. spada med tri največje banke v Sloveniji, v določenih segmentih poslovanja (elektronsko bančništvo) pa so že leta med vodilnimi. SKB banka, d. d., je začela poslovati kot samostojna banka, delniška družba po odcepitvi od Ljubljanske banke v januarju 1990, čeprav je poslovala že pred tem, in sicer kot specializirana stanovanjsko-komunalna banka. Danes ima SKB banka, d. d., vse značilnosti splošne komercialne banke, s sposobnim vodstvom, dobro razvitim mednarodnim poslovanjem in ponudbo, ki jo dopolnjujejo podjetja bančne skupine.

⁵ WAP ali Wireless Application Protocol je sprejet industrijski standard, ki omogoča brezžičnim napravam dostop do interneta.

5.1.3 Abanka Vipa, d. d.

Abanka je kot podružnica Jugoslovanske banke za zunanjo trgovino začela delovati že v letu 1955. Po več kot dvajsetih letih poslovanja, 1977, se je podružnica preimenovala v Jugobanko – Temeljno banko Ljubljana. Po obsegu poslovanja s tujino so takrat v sistemu Jugobanke zavzemali že tretje mesto. Kot Abanka, d. d., Ljubljana so začeli samostojno poslovati januarja 1990, 15. 12. 2000 je Abanka z Banko Vipa podpisala Pismo o nameri kapitalskega in poslovnega povezovanja, ki predvideva postopno združitev obeh bank. Do združitve je prišlo 31. 12. 2002, ko so se uspešno združili z Banko Vipo, d. d.

Njihova dolgoročna strategija razvoja je povezovanje s slovenskimi bančnimi in finančnimi institucijami ter Zavarovalnico Triglav, ki dolgoročno postaja večinski lastnik banke. Skupaj naj bi oblikovali močno slovensko banko, ki bi zasedla 2. ali 3. mesto v slovenskem bančnem prostoru, in sledili razvoju zavarovalniškega in bančnega trga v Evropi in svetu.

Začetki spletnega bančništva v Abanki, d. d., segajo v april leta 2000, ko se je začelo uporabljati njihov program Abanet. Spletno bančništvo v Abanki za osebno bančništvo se imenuje Abacom.

Abacom je samostojen program za osebne računalnike (deluje v okoljih Windows). Dostop do strežnika Abanke omogoča s pomočjo klicne linije (z modemom) ali po internetni povezavi. Stranka s strežniki v Abanki ne potrebuje stalne zveze, podatki pa se shranjujejo na osebni računalniku. Varnost zagotavlja pametna kartica, na kateri sta shranjena digitalni certifikat in ključ (vsak uporabnik ima svojo kartico, možna so različna pooblastila).

5.2 BANKA KOPER, d. d.

Istrska komunalna banka je bila ustanovljena leta 1955, ima podružnico v Piranu in ekspoziuro v Izoli. V naslednjih letih je ustanovila še podružnice v Ilirski Bistrici, Postojni in Sežani. Nova bančna zakonodaja v letu 1961 pomeni razširitev obsega poslovanja, saj banka prevzame tudi tiste kreditne posle, ki so bili do tedaj v domeni Narodne banke. Preimenuje se v Komunalno banko Koper in začenja krepiti lastni kreditni potencial tudi s sredstvi prebivalstva.

Leta 1965 se banka reorganizira in še enkrat dobi novo ime: Kreditna banka Koper. Po novem je to komercialno-investicijska banka, ki hitro postaja prava poslovna banka. Mrežo svojih enot razširi še na območje Ljubljane, Nove Gorice in Reke.

Z ustanovitvijo deviznega oddelka leta 1967 se začenja intenzivnejše poslovanje s tujino. Nove razmere spodbujajo nove oblike poslovnega sodelovanja z drugimi bankami, tudi z Ljubljansko banko, s katero financira pomembne investicijske projekte.

Sprememba zakonodaje leta 1978 narekuje združevanje bank in pripelje k vključitvi vseh slovenskih bank v sistem Ljubljanske banke. Tako nastane LB – Splošna banka Koper. V drugi polovici osemdesetih prevzame aktivno vlogo pri razreševanju slabšanja položaja podjetij v regiji. V ta namen leta 1989 banka ustanovi podjetje Finor, v istem letu pa se tudi preoblikuje v delniško družbo.

Z osamosvojitvijo Slovenije leta 1991 in novo finančno zakonodajo se začne slovenski bančni sistem približevati razvitim evropskim sistemom. Ko se Ljubljanska banka leta 1994 umakne kot lastnik, preide banka v lastništvo najpomembnejših gospodarskih družb v regiji, s čimer se še pospeši poslovanje z gospodarstvom in s posamezniki.

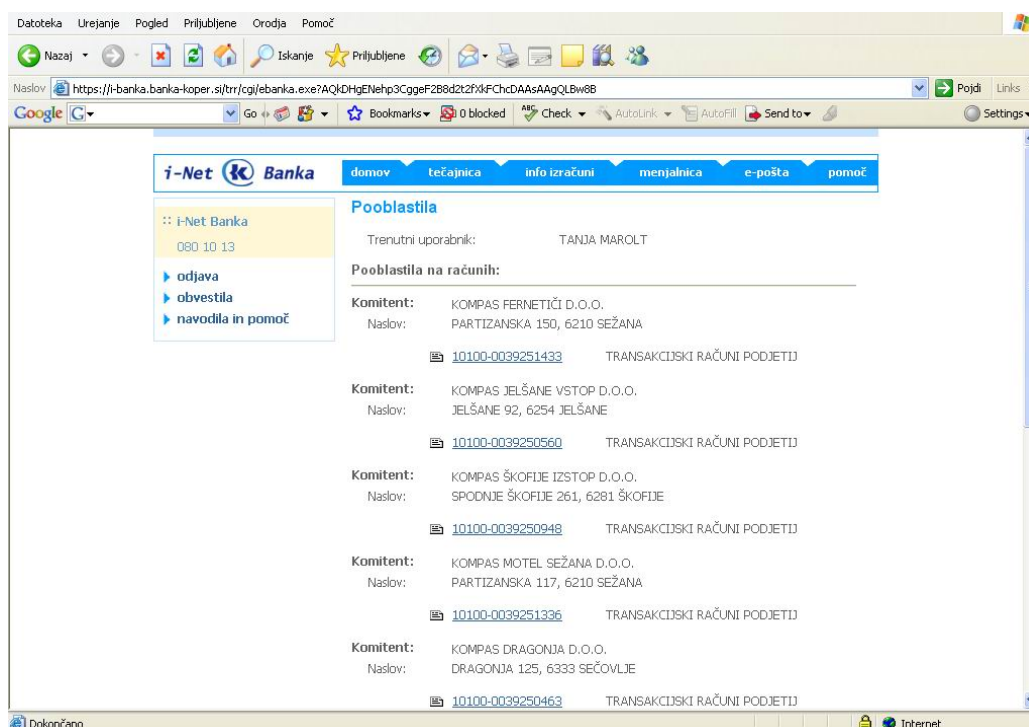
Banka začne ponovno širiti poslovno mrežo po vsej Sloveniji. Prenovi svojo notranjo organiziranost, se leta 1997 preimenuje v Banko Koper in dobi sedanjo grafično podobo. Skupaj z M-banko ustanovi bančno skupino, čez dve leti ji sledi pripojitve te banke. Hkrati okrepi poslovno mrežo, kjer opravlja vse več bančnih poslov in se s tem še bolj približa komitentom.

Razvija nove bančne storitve, še posebej na področju elektronskega bančništva, kjer z lastnim razvojem uresniči nekatere pionirske projekte v Sloveniji in celo v mednarodnem merilu.

Elektronska internet banka, poimenovana i-Net, ki jo komitenti uporabljajo od aprila 1999, omogoča optimalno upravljanje s transakcijskim računom, saj vključuje opravljanje plačilnega prometa preko transakcijskega računa, devizni plačilni promet kot tudi druge bančne storitve in produkte.

Program je zasnovan s strani podjetja Adacta, d. o. o. in nadgrajen oz. dopolnjen s strani Banke Koper, d. d. Program se lepo uporablja. V primerjavi s Halcomovim programom pa je njegova slabost ta, da se program izključi takoj, ko odstanimo pametno kartico iz čitalnika. Če en uporabnik posluje z dvema pametnima karticama in želi osvežiti stanje na računih, ki se nahajajo pri drugi banki, vam bo program Halcom dovoljeval vnos nalogov, pregled prometa ter izpis podatkov, ne da bi imeli vstavljen pametno kartico, medtem ko pri Banki Koper, d. d. ne morete storiti ničesar. Program Volksbank, d. d. deluje po enakem sistemu kot Banka Koper (Adacta, d. o. o.).

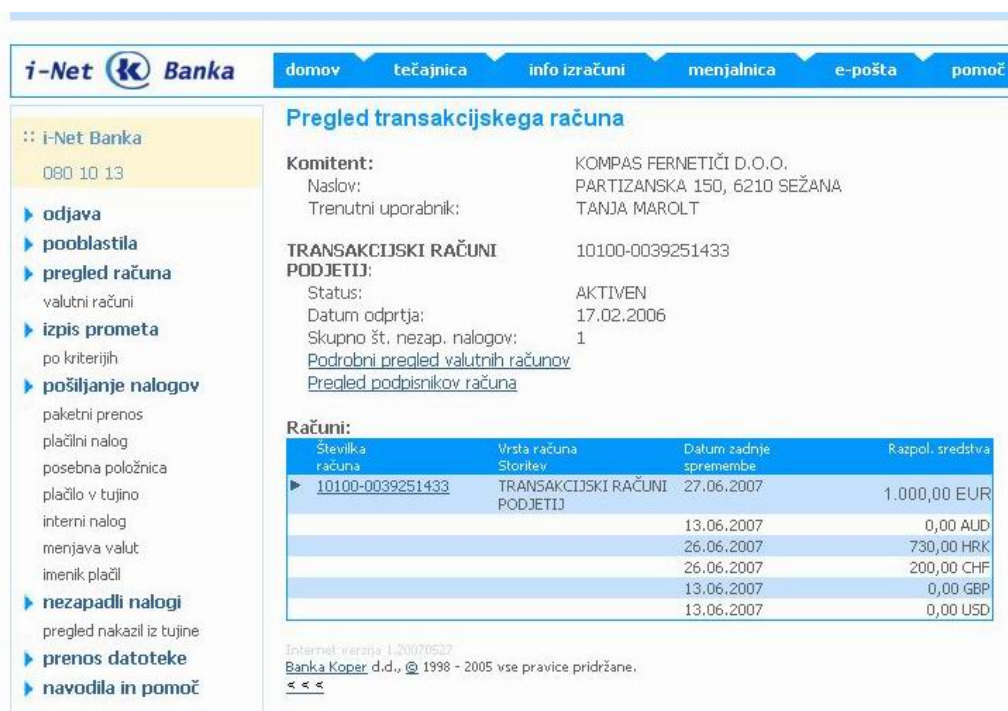
Slika 17: Pregled pooblastil pri Banki Koper, d. d.



Vir: Lasten vir.

Slika 17 prikazuje seznam podjetij, za katere je pooblaščen trenutni uporabnik. S klikom na transakcijski račun izberete podjetje, s katerim želite poslovati. Nato se vam odpre stran pregled transakcijskega računa, kjer se vam pokaže stanje na računu za vse valute. Na levi strani so vidne funkcije, ki jih lahko uporabljate pri poslovanju za izbran račun (glej sliko 18).

Slika 18: Pregled transakcijskega računa



Vir: Lasten vir.

Glede na to, da mi je pri Banki Koper najbolj med vsemi funkcijami všeč menjava valut sem se odločila, da vam to predstavim na naslednjih dveh slikah. Na prvi sliki (glej sliko 19) je obrazec za menjavo valut, ki ga uporabljamo za menjavo tuje valute za domačo ali pa menjavo tuje valute za tujo valuto.

Slika 19: Menjava valut

Banka Koper: i-Net Banka - Microsoft Internet Explorer

Datoteka Urejanje Pogled Priključene Orodja Pomoč

Naslov <https://i-banka.banka-koper.si/Trr/cg/ebanka.exe?AQKdHhMMAG93CgseAvRpfm19b313fhN8cndicGR4F2p6agwKCR4GBw6cBwMKBAoHFxd+cGoMBQ8WAQCNBw8YbXRqbVF>

Google

Go Bookmarks 0 blocked Check AutoLink AutoFill Send to Settings

i-Net Banka domov tečajnica info izračuni menjalnica e-pošta pomoč

Menjava valut

Datum izvišitve: 26.06.2007

REFERENČNA ŠTEVILKA: RAČUN: 10100-0039250948

NAMEN: Menjava valut NAZIV, NASLOV: KOMPAS ŠKOFJE IZSTOP D.O.O.

ZNESEK, KI GA ŽELITE PREJETI: SPODNJE ŠKOFJE 261

6281 ŠKOFJE

Kritje Pošlji

(Nakazilo v tujino | Pregled nakazil iz tujine | Interni nalog | Menjava valut)

Internet verzija 1.20070527
Banka Koper d.d., © 1998 - 2005 vse pravice pridržane.

Vir: Lasten vir.

Obrazec lahko uporabljamo na dva načina. Glede na to, kakšno količino zneska (določene valute) želimo prejeti oz. kakšno količino določene valute želimo zamenjati. S klikom na puščico se nam pojavijo vse razpoložljive valute. Gumbek kritje nam ponudi pod obrazec (slika 20), kjer si izberemo valuto, ki jo želimo zamenjati. S slike je lepo razvidno, kakšno je razpoložljivo stanje valute, ki jo želimo zamenjati. Prednost tega programa (obrazca) je v tem, da nas opozori, da prekoračitev stanja ni mogoča. V drugih bankah lahko obrazec izpolnimo in pošljemo v obdelavo kljub prekoračitvi stanja. Nalog bo postavljen v čakalno vrsto in bo v takem stanju do konca delovnega dneva, razen če ne dobimo na naš račun ustrezni znesek menjalne valute.

Slika 20: Kritje medvalutne menjave

Kritje - medvalutna menjava

Datum izvršitve: 28.06.2007

VALUTA	STANJE	ZNESEK, KI GA ŽELIM ZAMENJATI	PROTIVREDNOST V VALUTI, KI JO ŽELIM PREJETI
USD	0,00	0,00	

Dodaj

Vsota protivrednosti: EUR Potrdi

Banka si pridržuje pravico pri izvršitvi te transakcije, ki vsebuje menjavo valut, določiti drugačen tečaj od tistega, ki je objavljen v tečajni listi Banke Koper d.d. v trenutku prejema tega naloga. O drugačnem tečaju menjave banka obvesti komitenta med postopkom izvršitve naloga. V kolikor se komitent ne strinja z drugim tečajem, se nalog šteje za preklicanega in se ne izvrši.

Dokončano Internet

Vir: Lasten vir.

5.3 NOVA KREDITNA BANKA MARIBOR, d. d.

Za sam začetek Nova kreditna banka Maribor, d. d. (v nadaljevanju NKBM), bi lahko označili leto 1862, ko je začela poslovati Mestna hranilnica Maribor, ki je kasneje postala del NKBM. 100 let kasneje se Mestna hranilnica pripoji h Komunalni banki Maribor in 3 leta kasneje začne poslovati kot Kreditna banka Maribor.

V tem dolgem razdobju se je banki pripojilo še kar nekaj bank, združila pa se je tudi z dvaindvajsetimi temeljnimi bankami v Ljubljansko banko – združeno banko. Leta 1990 postane delniška družba, nato pa leta 1993 izstopi iz Ljubljanske banke – združene banke. Leta 1994 je bila z novim ustavnim zakonom ustanovljena Nova kreditna banka, d. d.

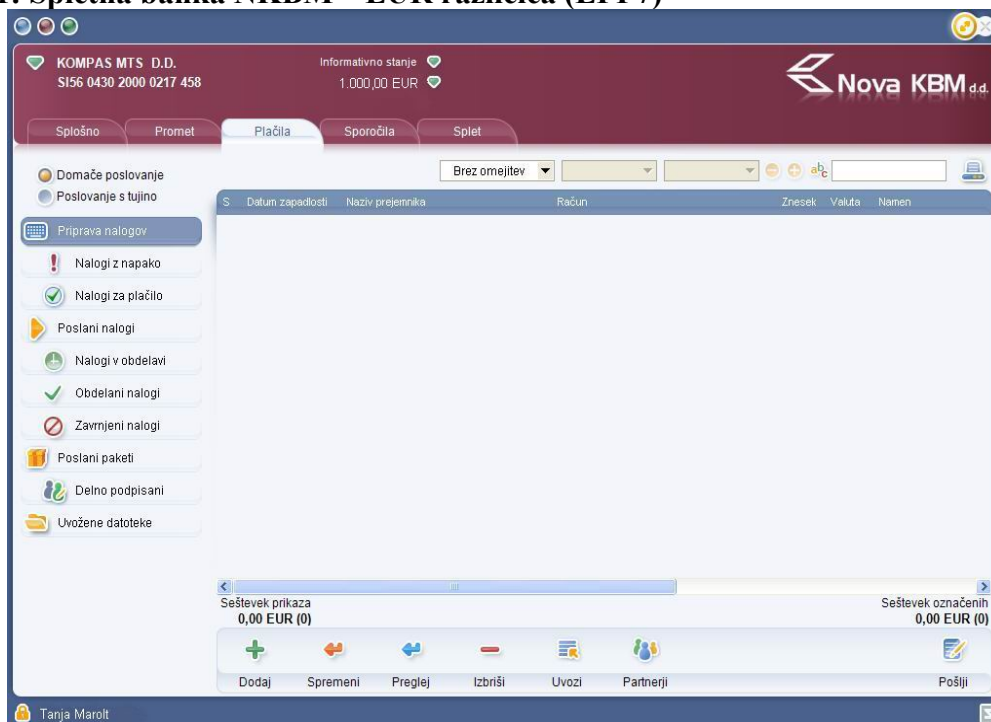
Nova Kreditna banka Maribor, d. d. je ena vodilnih slovenskih finančnih institucij in je s skoraj 300.000 komitenti druga največja banka v državi. Povezani s Pošno banko Slovenije nudijo komitentom celovit in široko dostopen bančno-finančni servis v 614 poslovalnicah po vsej Sloveniji. Klasične bančne storitve dopolnjujemo s ponudbo družb finančne skupine NKBM, ki vključuje zavarovalništvo, vzajemne sklade in storitve borznega posredništva. Njihove storitve odlikujejo učinkovitost, varnost, zanesljivost in osebni pristop pri reševanju finančnih izzivov posameznika.

Nova kreditna banka Maribor ima svojo spletno poslovalnico poimenovano Bank@Net. Storitve je na voljo že od 26. oktobra 1998. V okviru ponudbe elektronskega bančništva lahko podjetja izbirajo med več različicami uporabniških aplikacij:

Internetna različica z uporabo enkratnih gesel omogoča mobilnost uporabnika, saj se lahko z bančnim strežnikom poveže kjerkoli in povsod tam, kjer ima na osebнем računalniku omogočen dostop do interneta ter nameščen ustrezen spletni brskalnik, pri sebi pa ima elemente identifikacije (PIN, kartico za določanje enkratnih gesel). Baza podatkov se oblikuje na bančnem strežniku in zanjo skrbi banka. Ta različica je posebej primerna za podjetja, ki imajo v svojem informacijskem sistemu možnost medsebojnega paketnega posredovanja podatkov (npr. seznama plačilnih nalogov v elektronski obliki, izpiski prometa) in ki sistem uporabljajo predvsem za hiter pregled ali paketno posredovanje podatkov ali pa poslujejo z manjšim številom ročno vnešenih plačilnih nalogov (to pomeni, da izvršijo dnevno le nekaj plačil).

Namestitvena različica omogoča opravljanje številnih funkcij brez stalne internetne povezave, saj ima uporabnik aplikacijo nameščeno na osebнем računalniku. Uporabnik lahko pripravi in pregleda plačilne naloge, pregleda bazo starih izpiskov, pripravi statistike brez uporabe interneta, z bančnim strežnikom pa se poveže le pri pošiljanju in sprejemanju podatkov s protokolom za prenos datotek. Baza podatkov se oblikuje pri uporabniku, ki zanjo tudi skrbi. Lokalna različica je primerna predvsem za srednje velika in velika podjetja. Odvisno od narave dela v podjetju je možno uporabljati tudi kombinacijo obeh različic. Namestitvena različica Poslovnega Bank@Neta omogoča opravljanje domačega in tujega plačilnega prometa, uporabniki internetne različice pa lahko zaenkrat elektronsko opravljajo le domači plačilni promet. Omogočeno je tudi kolektivno podpisovanje. Na sliki 21 je prikazana namestitvena različica bank@Net-a.

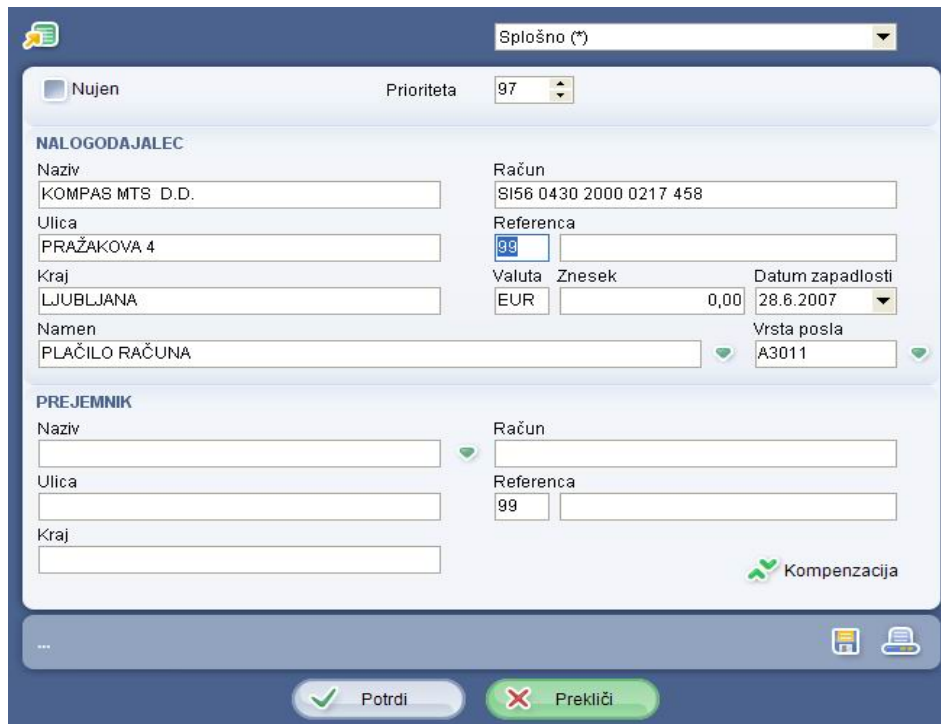
Slika 21: Spletna banka NKBM – EUR različica (EPP7)



Vir: Lasten vir.

Tolarska različica se mi je zdela funkcionalno bolje dopolnjena in je bila tudi po odzivih v medijih med ljudmi bolj priljubljena. Snovalci programa v NKBM se očitno zavedajo, da so pri »prenovi«, zakrivila napake, ki jih skušajo popraviti s pogostimi nadgradnjami.

Slika 22: Plačilni nalog NKBM



Splošno (*)

☐ Nujen Prioriteta: 97

NALOGODAJALEC

Naziv: KOMPAS MTS D.D. Račun: SI56 0430 2000 0217 458

Ulica: PRAŽAKOVA 4 Referenca: 99

Kraj: LJUBLJANA Valuta: EUR Znesek: 0,00 Datum zapadlosti: 28.6.2007

Namen: PLAČILO RAČUNA Vrsta posla: A3011

PREJEMNIK

Naziv: Račun: Kompenzacija

Ulica: Referenca: 99

Kraj: Potrdi Prekliči

Vir: Lasten vir.

Plačilni nalog NKBM je sestavljen iz enakih komponent kot ostali nalogi, le da je pomikanje po samih postavkah (valuta, znesek itd.) v drugačnem zaporedju.

5.4 VOLKSBANK – LJUDSKA BANKA, d. d.

Volksbank – Ljudska banka na slovenskem trgu uspešno deluje že od leta 1993, ko je Österreichische Volksbanken-AG (ÖVAG) prevzela Štajersko banko obrti in podjetništva (ustanovljena leta 1991). Večinski delničar Volksbank - Ljudske banke, d. d. je Volksbank International AG s sedežem na Dunaju.

Skupino Österreichische Volksbanken-AG (ÖVAG) so leta 1922 ustanovile komercialne posojilne zadruge in je danes v večinski lasti avstrijskih Volksbank (zadružnih bank). Banka je osrednja institucija ene najpomembnejših bančnih skupin v Avstriji, deluje pa tudi kot mednarodna poslovna banka. Že leta 1991 je bila ÖVAG ena od prvih bank, ki je sprejela izziv širjenja na trge Srednje in Vzhodne Evrope.

Volksbank International AG (VBI) danes upravlja uspešno in rastočo bančno mrežo v Srednji in Vzhodni Evropi, ki jo sestavlja 149 poslovalnic v osmih državah Srednje in Vzhodne Evrope. Podružnice ima v Slovaški republiki, Češki republiki, na Madžarskem, na Hrvaški, v

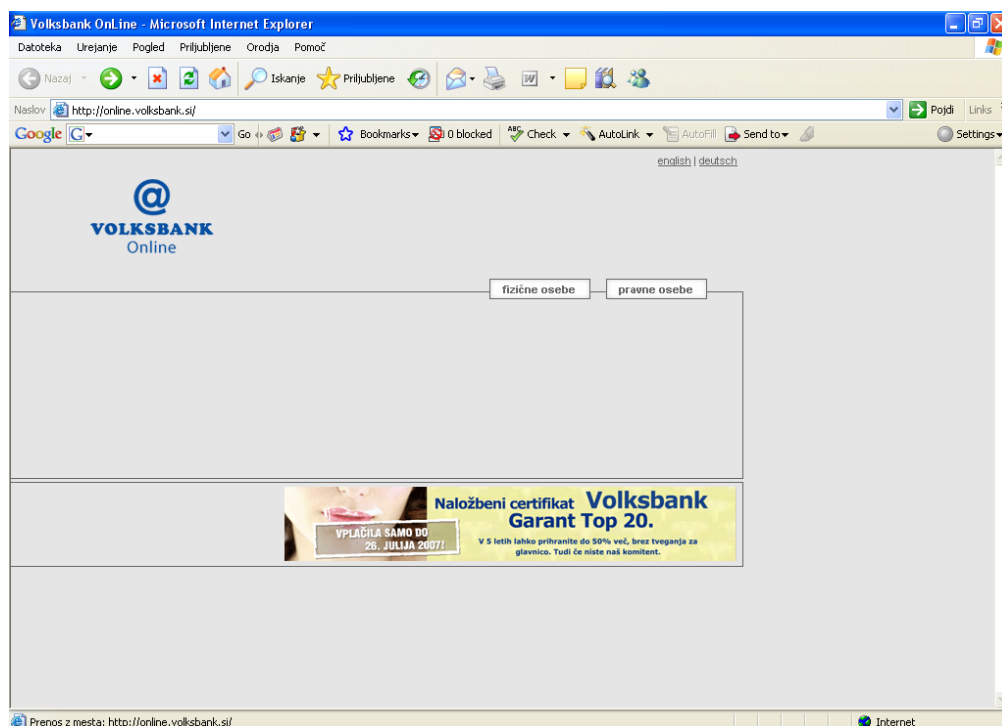
Sloveniji, Bosni in Hercegovini ter Srbiji in Romuniji. Mednarodno mrežo koncerna ÖVAG dopolnjujeta podružnica na Malti in predstavništvo v Vicenzi, Italija.

V letu 2004 je Volksbank International AG okrepila sodelovanje z nemško in s francosko partnersko banko, DZ BANK / WGZ-Bank in Banque Fédérale des Banques Populaires, ki imata v njej manjšinski delež, in sicer vsaka 24,5 odstotka. V skladu z vodilom VBI, da **"širi meje"**, bo ta strateška povezanost omogočila razširitev mreže in izboljšanje nabora storitev, ki jih ponujajo svojim strankam.

Zaradi sodelovanja s Confédération Internationale des Banques Populaires, ki se ponaša z mrežo 30 tisoč bančnih poslovalnic v Evropi, Severni Afriki, Argentini, Kanadi in Japonski, lahko Volksbank – Ljudska banka, svojim strankam zagotovi prisotnost v vseh pomembnejših finančnih središčih sveta.

Volksbank - Ljudska banka, d. d., nam ponuja svoje storitve po internetu pod spletno banko z imenom Volksbank online. Zasnovana je s strani podjetja Adacta in dodelana znotraj podjetja Volksbank.

Slika 23: Spletna banka Volksbank online



Vir: Lasten vir.

Ob vnosu naloga ali paketnem prevzemu Volksbank Online preveri pravilnost podatkov v vseh poljih. Pri nalogih z neustreznimi podatki dobi nalog oznako naloga z napako, ki ga mora stranka ustrezno popraviti. Uporabnik ima na voljo tudi šifrant računov, ki je vezan na centralni register transakcijskih računov Banke Slovenije, v katerem se nahajajo vsi transakcijski računi podjetij, društev in bank, ki imajo aktivne račune. Ta šifrant se dnevno

osvežuje. Na voljo je tudi šifrant statističnih šifer, kjer uporabnik lahko poišče zeleno statistično šifro plačila.

Ta šifrant računov je eden velikih plusov pri programu Volksbank online, saj na ta način težje pride do reklamacij.

Kot zahtevni in mobilni uporabniki potrebujemo zaradi uporabe večih bank in podjetij kartico ENA ZA VSE. Stroški, ki nastanejo z izdelavo te kartice, so 85,13 €. Kartica je veljavna 3 leta, kar je razvidno tudi s same kartice. Mesec pred iztekom digitalnega potrdila začne program uporabnika obveščati o poteku certifikata. Samo podjetje Halcom je v začetku leta 2007 začelo izvajati obveščanje po elektronski pošti z navodili o prevzemu obnovljenega certifikata. Če želite prevzeti obnovljeni certifikat, pošljete naročilo, plačate predračun in čakate, da vam podjetje Halcom, po prejemu plačila posreduje nadaljnja navodila. Ponovno dobite nov e-mail, ki omogoča povezavo na njihovo internetno stran, na kateri lahko nadaljujete s prevzemom obnovljenega digitalnega potrdila. Cena te storitve je 49,20 €.

V naslednji tabeli sem razporedila stroške na dva kriterija, in sicer glede na banko in vrsto storitve, ki nam jo posamezna banka nudi.

Naj omenim, da ne glede na to, ali poslujete z eno ali več bankami potrebujete le en čitalnik, saj so vse kartice zasnovane po enakem standardu.

Zakaj pri NKBM ne potrebujemo čitalnika? Ker uporabljamo kartico, ki nima vgrajenega čipa kot ostale kartice, ampak deluje po sistemu, povezanem z uro.

Stroški se mi zdijo kar približno enaki pri vseh bankah z malenkost nižjimi stroški se lahko pohvali Volksbank – Ljudska banka, d. d. V tabelo stroškov sem dodala tudi rubriko prilivni nalogi, ki se že počasi pojavlja v našem elektronskem bančništvu, ni pa še prisotno v vseh bankah.

V nadaljevanju se bom osredotočila predvsem na funkcionalnost mojih izbranih bank. Za storitve, ki jih ponujajo posamezne banke, sem pripravila tabelo (glej tabelo 5), v kateri so razvidne storitve, ki jih ponujajo posamezne banke.

Osebnost mi je po izgledu najbolj všeč stara različica programa (EPP 5) NKBM. Program ima zelo lepo razporejene ikone, ki jih želiš uporabiti. Desno zgoraj je nameščena urica, poleg katere klikneš na znak NKBM in program ti osveži stanje trenutnega podjetja. Nova (EUR) verzija v začetku leta 2007 tega ni omogočala, sedaj ko pa je po kritikah v dnevniku najbrž ugotovila, da je bil prejšnji program boljši, so to stvar le spremenili. Večjo pozornost so z novo različico namenili varnosti, saj je bilo po novem potrebno namesto dveh vnesti kar pet gesel. V službi za podporo uporabnikov naj bi menda deževalo pritožb, kar je pripomoglo k pripravi prenovljenih različic.

Vsak program ima dobre in slabe elemente. Ker smo vsi ljudje in smo vsi zmotljivi, prihaja od časa do časa tudi do pomot pri plačilih v elektronskem bančništvu. V tem primeru je zelo dobrodošla funkcija preklic že podpisanih nalogov. To funkcijo pogrešam pri programu EPP7 (tudi pri stari različici EPP5 ni bila možna). Pri drugih bankah enostavno klikneš na zeleni nalog, izbereš funkcijo preklic naloga in nato s ponovnim vnosom PIN kode prekličeš funkcijo poslanega naloga v banko. Pri NKBM pa je postopek dolgotrajnejši, lahko pošlješ sporočilo na banko in napišeš vse podatke za preklic naloga (prejemnika, znesek, valuto) oz. pokličeš svojega skrbnika in ga prosiš za preklic naloga.

Kaj ima zopet NKBM, kar druge banke nimajo? To je podvajanje nalogov v pripravi. Ta funkcija je zelo uporabna, če imamo za plačilo več računov istega podjetja. Postaviš se na pripravljen nalog, pritisneš desni klik na miški in izbereš opcijo podvoji. Program te obvesti, da se v mapi priprava nalogov nahaja nov nalog. Program te postavi na podvojeni nalog, ki ga lahko popravljamo po želji.

Te opcije ne podpira ne Halcomov program ne program podjetja Adacta. V okviru podjetja Halcom nam NLB, d. d., ponuja opcijo priprava predloge za tiste naloge, ki jih pogosto potrebujemo pri svojem delu. V sklopu Banke Koper in Volksbank lahko posamezne naloge shranimo v imenik. Slabost tega našega osebnega imenika je ta, da ko želimo nalog priklicati v uporabo, se na nalogu ne izpišejo podatki prejšnjih nalogov (o namenu plačila, zneska plačila ...), ampak ponudijo le podatek o prejemniku plačila.

Vse banke nam nudijo pregled stanja na računu, pregled prometa, plačevanje obveznosti na zelo podoben način.

Tabela 4: Stroški, povezani z elektronsko banko

	NLB	ABANKA	SKB	BANKA KOPER	NKBM	VOLKSBANK
Vodenje računa	10,85 EUR	8,35 EUR	8,76 EUR	8,39 EUR	8,35 EUR	6,00 EUR
Pristopnina – začetni paket	29,21EUR	25,04 EUR	20,86 EUR	0 EUR	20,86 EUR	45,00 EUR
Kartica s čipom oz. Secur Id (NKBM)	68,85EUR	75,60 EUR	41,73 EUR	10,43 EUR*	62,59 EUR	20,00 EUR
Čitalec - USB	♦	35,47 EUR	20,86 EUR	0 EUR	ne potrebuješ	25,00 EUR
Mesečni stroški	0 EUR	8,35 EUR	6,26 EUR	5,01 EUR**	4,17 EUR	0 EUR
Nalog - domača banki	0,33 EUR	0,35 EUR	0,31 EUR	0,33 EUR	0,31 EUR	0 EUR
Nalog – tuja banka	0,75 EUR	0,77 EUR	0,69 EUR	0,71 EUR	0,73 EUR	0,50 EUR
Nujni nalog	5,42 EUR	5,00 EUR	6,26 EUR	5,42 EUR	4,60 EUR	2,50 EUR
Prilivni nalog	0 EUR	0,10 EUR	0 EUR	0 EUR	0,10 EUR	0 EUR

Vir: Spletne strani slovenskih bank, 2007.

♦ Oblikovan imajo seznam trgovcev, ki prodajajo čitalnike pametnih kartic, tako da so cene različne.

* Prva kartica je brezplačna.

** Nadomestilo se ne zaračuna v prvem mesecu uporabe Poslovne i-Net Banke.

Tabela 5: Storitve elektronskega bančništva

	NLB	ABANKA	SKB	BANKA KOPER	NKBM	VOLKSBANK
Pregled stanja	√	√	√	√	√	√
Pregled prometa	√	√	√	√	√	√
Plačevanje obveznosti	√	√	√	√	√	√
Prenos sredstev med računi	√	√	√	√	√	√
Preklic podpisanih nalogov	√	√	√	√		√
Plačevanje v tujino	√	√	√	√	√	√
Nakup in prodaja tuje valute	√	√	√	√	√	√
Pregled, tiskanje izpiskov	√	√	√	√	√	√
Podvajanje nalogov v pripravi					√	
Podvajanje nalogov v arhivu	√	√	√			
Imenik plačil				√		√
Kreiranje in urejanje predlog	√					
Paketno podpisovanje	√	√			√	
Uvoz in izvoz podatkov	√	√	√	√	√	√

Vir: Spletne strani slovenskih bank, 2007.

Iz tabele je tudi razvidno, da vse banke nudijo tiskanje izpiskov. Banka Koper ponuja uporabnikom brezplačno možnost pošiljanja izpiskov po elektronski pošti še isti dan okoli devetnajste ure. Tudi uporabniki Abanke Vipe, d. d., se lahko pohvalijo z zelo hitro dostopnimi izpiski, in sicer okoli osemnajste ure. NKBM je imela z EUR različico kar nekaj težav, saj izpiski občasno niso bili pripravljeni za pregled tudi do 11. ure naslednjega dne. V EUR različici so pripravili tudi prenovljene izpiske, vendar so to kasneje dopolnili s tisto staro v PDF-formatu.

6 SKLEP

Elektronsko bančništvo je v današnjem svetu za slehernega podjetnika že skoraj nepogrešljivo. Morda le še za tiste majhne, ki sploh ne vedo, da obstaja, ali pa niso imeli priložnosti, da bi se поблиže srečali z njim.

Čas, ki ga porabimo na bančnem okencu in na poti do banke ter parkirnine in provizija, ki je vsaj še enkrat višja od tiste elektronske provizije ... Se nam splača? Ne časovno in ne finančno. Vložimo raje ta denar v elektronsko bančništvo, zagotovimo si pregled našega stanja na računu vsako minuto. Čas pa raje namenimo iskanju nove stranke ali izboljšanju drugih pomanjkljivosti, ki nas zavirajo pri uspehu. Omogočite svojim zaposlenim, da vstopijo v sedanost in začnejo spoznavati prihodnost.

Dvom o varnosti je vsekakor manjši kot v preteklosti, je pa dejansko še prisoten. Absolutne varnosti torej ni. Zloraba, tako fizična kot elektronska, nam sledi na vsakem koraku. Strokovnjaki, ki kljubujejo varnosti v elektronski banki so vseskozi na preži in skušajo biti vedno korak pred zmikavti, ki ogrožajo naš denar.

V Sloveniji je elektronsko bančništvo zelo razvito, saj ga ponujajo praktično vse banke, ki se dobro zavedajo pomembnosti elektronskega poslovanja in predvsem elektronskega poslovanja po internetu, saj ima danes že skoraj vsaka banka razvito spletno bančništvo tako za pravne kot tudi za fizične osebe.

Ponudniki so prisiljeni izdelati čim kvalitetnejšo rešitev, ki naj bi bila zasnova na čim večjo varnost in bi zagotavljala enostavno funkcionalnost in preglednost. Slabost se kaže v nepovezanem razvoju. Proizvajalci ponujajo programske aplikacije, ki podpirajo različne programske vmesnike in uporabnikom, ki poslujejo z več bankami hkrati, otežuje delo, ker so prisiljeni nameščati in vzdrževati več sistemov. Posledica tega je precej različna in bolj ali manj nezdružljiva programska oprema e-bančništva.

Vsekakor moramo pohvaliti Slovenski bančni sistem, saj smo kljub majhnosti lahko vzgled celotni Evropi. Prekašamo jih tako v domačem kot tujem plačilnem prometu in smo praktično ena redkih držav, v kateri lahko uporabnik z enim programom za elektronsko banko in z eno samo zaščitno kartico prihaja do transakcij pri različnih bankah.

7 LITERATURA IN VIRI

LITERATURA

1. Bedjančič Borut, Lorenz Katarina: Elektronsko bančništvo. Bančni Vestnik, Ljubljana 1997, 12, str. 57–59.
2. Bračun Franc: Praktične izkušnje pri uvajanju e-bančništva. Banke in tveganje, zveza ekonomistov Slovenije. Ljubljana, 1997, str. 149–154.
3. Bračun Franc, Cetinski Andrej: Elektronsko poslovanje v SKB banki, d. d. Organizacija, Kranj, 1998, 3, str. 144.
4. Cetinski Andrej: Elektronsko poslovanje v bančništvu. Organizacija, Kranj 32 (1999), 3, str. 149–152.
5. Jerman Blažič Borka: Elektronsko poslovanje na internetu. Ljubljana: Gospodarski Vestnik, 2001, str. 206.
6. Kalakota Ravi, Whinston Andrew: Electronic Commerce. A Manager's guide. B.k.: Addison – Wesley Longman, 1997. XVI, str. 431.
7. Kovačič Matevž: Storitve elektronskega bančništva. Banke in tveganje. Zbornik III. Strokovnega posvetovanja o bančništvu. Portorož. Zveza ekonomistov Slovenije 1997, str. 155–165.
8. Kuščar Samo: O varnosti in odgovornosti. Monitor, Ljubljana, Infomedij, št. 11, nov. 2002, str. 8.
9. Ošlak Darinka: Varnost elektronskega poslovanja v slovenskem bančništvu. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 2005, str. 83.
10. Miš Svoljšak Irena: Osnove trženja finančnih storitev. Maribor: Združenje bank Slovenije, 1997, str. 23.
11. Miš Svoljšak Irena: Do denarja - kjerkoli, kadarkoli. PC Kapital (prologa k reviji Kapital), Maribor, 1998, str. 7–8.
12. Na – Network Associates. An Introduction to Cryptography. Santa Clara: Network Associates Inc. 1999.
13. Pavliha Marko: Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. Ljubljana: GV Založba, 2002, str. 222.
14. Pepelnjak Ivan, Bradeško Marjan: Varnost računalniških sistemov in elektronskih transakcij. Zbornik, Banke in tveganje. Portorož. Zveza ekonomistov Slovenije, 1997, str. 155–165.
15. Pinterič Mojca: Pametne kartice izpodrivajo gotovino. Ljubljana, Gospodarski vestnik 1995, str. 5–29.
16. Power Richard: How NOT to build a firewall. Computer Security Institute, 1998. [URL: <http://www.spirit.com/CSI/Papers/hownot.htm>], 5. 10. 2006.
17. Pucihar Andrej, Jože Gričar: Izraba informacijske tehnologije za elektronsko poslovanje. Organizacija, Kranj, 2000, 3, str. 207–212.
18. Robinson Peter: Understanding Digital Certificates and Secure Sockets Layer (SSL). Entrust, Inc., 2001 [URL: <http://entrust.com/resourcenter/whitepapers.htm>], 1. 5. 2006.

19. Schneier Bruce, *Secrets & Lies. Digital Security in a network World*. NY: Wiley Computer Published, 2000, str. 412.
20. Sejkloča Marko: *Elektronsko bančništvo*. Bančni vestnik, Ljubljana, 1999,1/2, str. 31–32.
19. Škrlec Ivan: *E-poslovanje in uporaba formata XML*. Finance, Ljubljana, 2002, 6. maj, str. 18.
20. Toplišek Janez: *Elektronsko poslovanje*. Ljubljana: Založba Atlantis, 1998, str. 336.
21. Turban Efraim, et al.: *Electronic Commerce. A Managerial Perspective*. New York: Prentice Hall, 2003, str. 512.
22. Vrešak Sabina: *Internet in elektronsko bančništvo*. Ljubljana: Bančni vestnik, 1997, 12, str. 60–63.
23. Zupančič Dušan, et al.: *Aplikacija za varno elektronsko podpisovanje in preverjanje podpisa*. Ljubljana. Junij 2004, str. 28.
24. Zupančič Dušan, et al.: *Pravna vprašanja elektronskega podpisa, elektronskega poslovanja in elektronskih arhivov*. Ljubljana, april 2004, str. 39.
25. Young-Seock, Cha: *E-Commerce Security Technologies*. Network Security Library, 2000. [URL: <http://secinf.net/info/fw/ecom/>], 10. 10. 2006.

VIRI

1. Abanka Vipava, d. d. [URL:<http://www.abanka.si/>]
2. Actividentety Corporate [URL:<http://www.actividentity.com/>]
3. Adacta Ljubljana, d. o. o. [URL:
<http://www.adacta.si/index.asp?content=Resitve&submenu=InetBank&lang=SI>]
4. Bank Austria kreditanstalt, d. d., Ljubljana [URL: <http://www.ba-ca.si/>]
5. Banka Celje, d. d. [URL: <http://www.banka-celje.si/>]
6. Banka Koper, d. d. [URL:<http://www.banka-koper.si/index.php>]
7. Banka Slovenije: Seznam poslovnih bank [URL:<http://www.bsi.si/>]
8. Banka Sparkasse, d. d. [URL: <http://www.sparkasse.si/>]
9. Cente vlade RS za informatiko [<http://www.sigov.si/tečaj/html/html.html>]
10. Deželna banka Slovenije, d. d. [URL: <http://www.dbs.si/>]
11. EUROPKI [URL: <http://www.europki.org/>]
12. Factor banka, d. d. [URL: <http://www.factorb.si/>]
13. Finance on-net [URL: <http://www.finance-on.net/?MOD=show&id=170234>]
14. Gorenjska banka, d. d., Kranj [URL: <http://www.gbkr.si/>]
15. GfK Gral-Iteo tržne raziskave, d. o. o. [URL: <http://www.gfk.si/>]
16. Halcom, d. d. [URL: <http://www.halcom.si/>]
17. Hermes softlab [URL: <http://www.hermes-softlab.com/SLO/default.asp>]
18. Hypo Alpe-Adria-Bank, d. d. [URL: <http://www.hypo-alpe-adria.si/>]
19. Interna gradiva posameznih Slovenskih bank
20. NLB Banka Domžale, d. d. [URL: <http://www.banka-domzale.si/>]

21. NLB Banka Zasavje, d. d. [URL: <http://www.banka-zasavje.si/>]
22. Nova Kreditna banka Maribor, d. d. [URL:<http://www.nkbm.si/>]
23. Nova Ljubljanska banka, d. d., Ljubljana [URL: <http://www.nlb.si/>]
24. Poštna banka Slovenije, d. d. [URL: <http://www.pbs.si/>]
25. Probanka, d. d. [URL: <http://www.probanka.si/>]
26. RIS: E-bančništvo 2006
[URL: <http://www.ris.org/index.php?fl=0&p1=276&p2=285&p3=&id=507>]
27. Raiffeisen Krekova banka, d. d. [URL :<http://www.r-kb.si/>]
28. Skb banka, d. d. [URL:<http://www.skb.si/>]
29. Volksbank – Ljudska banka, d. d. [URL <http://www.volksbank.si/>]
30. Zrcalo, d. o. o. [URL: <http://www.zrcalo.si/ng2005/index.php>]