DIPLOMSKO DELO

ELEKTRONSKO BANČNIŠTVO PRAVNIH OSEB NOVE LJUBLJANSKE BANKE D.D.

Ljubljana, maj 2003

JASMINA JOKIĆ
IZJAVA

Študentka Jasmina Jokić izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom prof.dr. Andreja Kovačiča in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 5.5.2003

Podpis:
Kazalo

1. UVOD .............................................................................................................................................. 1
2. ELEKTRONSKO POSLOVANJE ......................................................................................................... 2
   2.1. MEDSEBOJNO DELOVANJE UDELEŽENCEV ELEKTRONSKEGA POSLOVANJA ..................... 3
   2.2. VARNO IN UČINKOVITO ELEKTRONSKO POSLOVANJE ...................................................... 3
       2.2.1. Varovani viri in vrste napadov ......................................................................................... 4
       2.2.2. Ukrepni varovanja sistemov in drugih virov ..................................................................... 5
   2.3. ELEKTRONSKO PODPISOVANJE KOT ZAŠČITA TRANSAKCIJ ............................................... 5
   2.4. PRAVNA UREDITEV ELEKTRONSKEGA POSLOVANJA ....................................................... 6
3. ELEKTRONSKO BANČNIŠTVO ........................................................................................................ 7
   3.1. RAZVOJ ELEKTRONSKEGA BANČNIŠTVA ............................................................................... 7
   3.2. DELOVANJE ELEKTRONSKEGA BANČNIŠTVA .................................................................... 8
       3.2.1. Standardni način ..................................................................................................................... 8
       3.2.2. Elektronsko bančništvo preko interneta .......................................................................... 8
   3.3. KATEGORIJE BANČNIH KOMITENTOV ................................................................................. 9
   3.4. POZITIVNI UČINKI ELEKTRONSKEGA BANČNIŠTVA ....................................................... 10
   3.5. VARNOST IN ZAŠČITA ............................................................................................................ 10
4. INTERNET ......................................................................................................................................... 11
   4.1. RAZVOJ INTERNETETA ............................................................................................................ 12
   4.2. UPORABA INTERNETETA ........................................................................................................ 13
       4.2.1. Ponudniki priklopa na internet ............................................................................................ 13
   4.3. NAJPOMEMBNEJŠE STORITVE INTERNETETA .................................................................. 14
   4.4. STANDARDI, PROTOKOLI IN JEZIKI, KI OMOGOČAJU KOMUNIKIRANJE PO OMREŽJIH .. 15
5. ELEKTRONSKO BANČNIŠTVO PRAVNIH OSEB NOVE LJUBLJANSKE BANKE .............. 16
   5.1. ELEKTRONSKO BANČNIŠTVO NOVE LJUBLJANSKE BANKE ................................................. 16
   5.2. UVAJANJE E-BANKE ZA SAMOSTOJNE PODJETNIKE IN PRAVNE OSEBE ....................... 17
       5.2.1. Reforma plačilnega prometa ............................................................................................... 19
   5.3. SISTEM ELEKTRONSKEGA BANČNIŠTVA .......................................................................... 20
   5.4. E-BANČNIŠTVO OMOGOČAJU AVTOMATIZACIJO POSTOPKOV .................................... 21
   5.5. POSTOPKI VKLJUČITVE UPORABNIKA V E-BANKO ........................................................ 22
       5.5.1. Kdo so uporabniki elektronske banke? ........................................................................... 22
       5.5.2. Kaj sistema omogočata? .................................................................................................... 23
       5.5.3. Potrebna računalniška in komunikacijska oprema ............................................................ 23
           5.5.3.1. ZA PROKLIK NLB ......................................................................................................... 23
           5.5.3.2. ZA PROKLIK PLUS NLB .............................................................................................. 24
       5.5.4. Pogoji za odobritev uporabe Proklika NLB ali Proklika plus NLB ................................. 25
       5.5.5. Postopek za priključitev uporabnika .................................................................................. 25
       5.5.6. Kaj prejme uporabnik, po odobritvi zahtevka, za nemoteno poslovanje? ..................... 26
       5.5.7. Obveznosti pri poslovanju s Proklik NLB in Proklik Plus NLB .................................... 27
           5.5.7.1. OBVEZNOSTI UPORABNIKA OZ. POOBLAŠČENCA ......................................................... 27
           5.5.7.2. OBVEZNOSTI BANKE .................................................................................................. 28
           5.5.7.3. OBVEZNOSTI KOMERCIJALISTA ............................................................................... 28
       5.5.8. Pooblaščila za uporabo ........................................................................................................ 28
       5.5.9. Možni postopki po vključitvi uporabnika .......................................................................... 29
       5.5.10. Ukinitev uporabe programa ............................................................................................. 30
       5.5.11. Cena uporabe Proklika NLB in Proklika plus NLB ......................................................... 30
   5.6. ZANIMANJE ZA SODOBNE TRŽNE POTI NARAŠČA ............................................................. 31
   5.7. POSLOVNI VIDIK ELEKTRONSKEGA BANČNIŠTVA ........................................................ 33
       5.7.1. Stroški elektronskega bančništva ....................................................................................... 33
           5.7.1.1. STROŠKI BANKE ........................................................................................................... 33
           5.7.1.2. STROŠKI UPORABNIKOV ............................................................................................ 34
           5.7.2. Prednosti elektronskega bančništva ................................................................................. 34
           5.7.2.1. PREDNOSTI ZA BANKO .................................................................................................. 34
5.7.2.2. PREDNOSTI ZA UPORABNIKE ................................................................. 35
5.7.3. Slabosti elektronskega bančništva ....................................................................................... 36
  5.7.3.1. SLABOSTI ZA BANKO ......................................................................................... 36
  5.7.3.2. SLABOSTI ZA UPORABNIKE ............................................................................. 37
5.8. KAKO VARNO JE OPRAVLJANJE STORITEV PREKO E-BANKE? ......................................... 37
  5.8.1. Overitelji .............................................................................................................. 38
  5.8.2. Digitalno potrdilo ..................................................................................................... 39
  5.8.3. Digitalni podpis ........................................................................................................ 39
  5.8.4. SSL (Secure Sockets Layer) ..................................................................................... 40
  5.8.5. Povzetek .................................................................................................................. 40

6. SKLEP .......................................................................................................................... 41

LITERATURA ..................................................................................................................... 43

VIRI ........................................................................................................................................ 44

PRILOGE

Priloga 1: Seznam uporabljenih kratic
Priloga 2: Zakonska opredelitev temeljnih pojmov elektronskega poslovanja
Priloga 3: Opredelitve izrazov, ki jih banka uporablja pri elektronskem bančništvu
Priloga 4: Blagovni znamki elektronske banke za pravne osebe in zasebnike v NLB
1. UVOD


Elektronsko poslovanje, ki temelji na združevanju informacijske in telekomunikacijske tehnologije je nam dobro poznane vrste poslovanja (zavarovalništvo, bančništvo) popeljalo na višji nivo. Razvoj interneta in njegova eksplozivna rast popularnosti sta omogočila nov način opravljanja storitev. Velika trgovska podjetja so začela ponujati svoje izdelke preko svetovnega spleta (e-nakupovanje - internet trgovina). Banke, katerih bančna okončna so bila vedno prepolna komitentov, so z razvojem elektronskega bančništva uvedle nove tržne kanale, s katerimi so želele znižati stroške poslovanja in masovne posle prenesti iz poslovalnic ter ugoditi strankam.

Namen mojega diplomskega dela je v grobem predstaviti elektronsko bančništvo in natančneje opredeliti elektronsko banco na področju pravnih oseb in zasebnikov ter izpostaviti prednosti in slabosti, ki izhajajo iz tega načina poslovanja. Pri tem sem se osredotočila na elektronski banki Nove Ljubljanske banke (Proklik NLB) in Proklik plus NLB.

V drugem poglavju sem opredelila elektronsko poslovanje, saj je temelj elektronskega bančništva, o katerem govori moje diplomsko delo. Navedla sem njegove značilnosti in udeležence. Ker elektronsko poslovanje poteka preko omrežij in sistemov, ki so vse bolj in bolj odprti, sem kar nekaj pozornosti posvetila tudi na zaščito, ki je nujna za obstoj le-tega.

V tretjem poglavju v tem nameni sem vodila glavne smernice, ki so omogočile razvoj elektronskega bančništva v Sloveniji ter kategorizirala uporabnike. Izpostavila sem tudi pozitivne učinke elektronskega bančništva ter Stanford Le-tera.

V nadaljevanju sem opredelila omrežje internet, njegov razvoj, kakšne storitve lahko opravljamo in nekaj protokolov oz. standardov, ki nam služijo v ta namen.

Dejstvo, da je varnost pri elektronskem bančništvu največji problem oz. tema pomislekov predvsem s strani komitentov, me je vodilo k podrobnjejši obravnavi varnostnih elementov čisto na koncu diplomske naloge. Razlaga temelji na zahtevah, ki jih morajo izpolnjevati tako banka kot komitenti.

2. ELEKTRONSKO POSLOVANJE

 Razvoj elektronskega poslovanja označujemo z razvojem računalniških omrežij in interneta, z združevanjem informacijske in telekomunikacijske tehnologije ter standardom za računalniško izmenjavo podatkov, katerega začetek segajo v leto 1968. Takrat ni nihče slušil, s kakšno hitrostjo in kako intenzivno bo razvoj informacijske tehnologije in telekomunikacij vplival na spremembo načina življenja in poslovanja (Jerman-Blažič, 2001, str. 13).

Ključnega pomena za elektronsko poslovanje so tehnološke sestavine (računalnik, programska rešitev (aplikacija) in komunikacije) katerim je potrebno dodati še organizacijo poslovanja, saj šele skupaj z njo osnovne tehnološke sestavine podpirajo cilje poslovnega sistema.

Pojem elektronsko poslovanje izhaja iz angleškega izraza »electronic commerce (EC)«. Nastal je v trgovini, industriji in se nanaša na vsa gospodarska (poslovna) področja. Danes se za elektronsko poslovanje vse pogosteje uporablja naziv e-business, ki ne obsega samo navadno izmenjavo podatkov (RIP - ang. EDI) in delovanje spletnih trgovin, ampak vse kar danes delamo v sklopu svoje poslovne dejavnosti s pomočjo računalniških aplikacij in omrežij.

Tako lahko elektronsko poslovanje, ko imamo v mislih vrste poslovanja, opredelimo tudi kot: 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) ter notranje elektronsko poslovanje (npr. v organizaciji) (Toplišek, 1998, str. 5).

Pomembni elementi teh dejavnosti so:

• **način dela:** gre za računalniško izmenjavo podatkov ob uporabi odprih omrežij kot je 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;
• **udelježenci poslovanja:** posamezniki (podjetniki, raziskovalci, managerji, občani, kulturni delavci, študenti, učitelji, dijaki, upravni delavci), podjetja, bolnišnice, muzeji, galerije, univerze, izobraževalne ustanove in državne ustanove. Gre za poslovanje znotraj posameznih skupin in za poslovanje med skupinami. V zadnjem času je vse več predvsem poslovanje med posamezniki ter med posamezniki in podjetji (Jerman-Blažič, 2001, str. 11-12).
Značilnosti poslovanja, kateremu smo priča zadnjih deset let in to predvsem zaradi uporabe interneta, so:

- globalizacija (briše geografske meje),
- hitrost (hitrost poslovanja je nekajkrat večja od klasičnega načina poslovanja) in
- prilagodljivost (predvsem spremembam na trgu).

S širitvijo elektronskega poslovanja (v nadaljevanju EP) so se pojavile različne interpretacije in če jih povzamemo, lahko rečemo, da je EP katerakoli oblika poslovanja, v kateri stranke delujejo elektronsko, si izmenjujejo informacije z uporabo kakršnekoli informacijsko-komunikacijske tehnologije - ICT in je alternativa papirnim metodam komunikacije in hranjenja informacij.

### 2.1. MEDSEBOJNO DELOVANJE UDELEŽENCEV ELEKTRONSKEGA POSLOVANJA

Tovrstno poslovanje je pomembno predvsem na štirih področjih, kjer so se oblikovale tri glavne vrste poslovanja (glej tabelo 1).

Tabela 1: Področja in vrste poslovanja

<table>
<thead>
<tr>
<th>PODROČJA POSLOVANJA</th>
<th>VRSTE POSLOVANJA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Povezovanje med organizacijami in potrošniki</td>
<td>Podjetje-potrošnik (B2C)</td>
</tr>
<tr>
<td>Žnotranje poslovanje organizacij</td>
<td></td>
</tr>
<tr>
<td>Poslovanje med organizacijami</td>
<td>Podjetje-podjetje (B2B)</td>
</tr>
<tr>
<td>Poslovanje državne administracije med seboj in z občani</td>
<td>Javna in državna uprava-javnost in občani (tako podjetja (G2B) kot posamezniki (G2C))</td>
</tr>
</tbody>
</table>


Elektronsko poslovanje med podjetji in potrošniki (B2C) zajema področja, ki večinoma temeljijo na poslovanju z uporabo internetnih spletnih strani. Na ta način lahko potrošnik opravlja raznovrstna opravila (izobraževanje, nakupi, plačevanje položnic) preko domačega računalnika.

Elektronsko poslovanje med podjetji (B2B) zajema povezavo med prodajalci na drobno in dobavitelji, elektronsko bančništvo, sodelovanje na skupnih projektih itd.. Po ocenah raziskav le-to predstavlja največji del elektronskega poslovanja.

Pri poslovanju z državno upravo ločimo njeno poslovanje s podjetji (G2B) in poslovanje s prebivalci (G2C). Zadnje je eno najzahtevnejših področij, ker zahteva lokalni dostop do teh storitev vseh državljanih in članov skupnosti.

### 2.2. VARNO IN UČINKOVITO ELEKTRONSKO POSLOVANJE

Elektronsko poslovanje se iz doslej večinoma zaprtih sistemov širi na globalno raven. Prav vse večja odporno in medsebojna povezanost računalniških omrežij, preko katerih poslovanje poteka, odpira vrsto varnostnih vprašanj in zahtevata celovito obravnavo in trdne rešitve.
Nevarnost razkritja zaupnih podatkov, ki so shranjeni na računalniških sistemih oz. se pretakajo preko omrežij, postavlja pred vpletena podjetja, ustanove in organizacije, ki se s tem področjem namensko ukvarjajo, nove naloge (Pepelnjak, Bradeško, 1997, str. 155).

Osebna točka varovanja pri elektronskem poslovanju je preprečevanje nepooblaščenega zmanjševanja vrednosti virov. Viri so lahko zaupni podatki kot so: poslovne skrivnosti, elektronski dokumenti o zdravstvenem stanju pacienta, številke kreditnih kartic, strojna in programska oprema sistemov. Iz tega razloga je način varovanja odvisen od vrednosti virov, potencialnih groženj in učinkov teh groženj.

Napadi, pred katerimi se podjetja želijo zavarovati, ne prihajajo zgolj samo zunaj lokalnega omrežja podjetij. Nepooblaščena uporaba virov oz. razkritje zaupnih informacij sta tudi posledici nedovoljene dejavnosti subjektov znotraj lokalnega omrežja, zato je potrebno sisteme zavarovati tako zunaj kot znotraj.

2.2.1. Varovani viri in vrste napadov

V računalniškem sistemu varujemo shranjene podatke, ki so ponavadi končni cilj potencialnega napadalca. Za zavarovane vire moramo zaradi tega zagotoviti (Pepelnjak, Bradeško, 1997, str. 157):

• **varnost dostopa**, kjer so predmet zaščite viri in storitve v sistemu,
• **varnost uporabe**, kjer je potrebno zagotoviti, da za dostop pooblaščeni uporabniki v sistemu počno le tisto, kar jim glede na njihov položaj pripada; zaščito potrebujejo tudi uporabniki sami – ne moremo dopustiti, da bi uporabnik storitve (npr. vpogled v bankov račun) pri tem doživel zlorabo s strani tretje osebe,
• **varnost transakcij** izvedenih preko teh virov – vsi pomembni podatki, ki se izmenjujejo preko komunikacijskih poti, morajo preko le-neh potovati varno, brez možnosti, da bi jih kdo prestregel ali celo poneveril.

Iz zgoraj navedenih postavk lahko tudi opredelimo vrste napadov na varovane vire (glej sliko 1) (Pepelnjak, Bradeško, 1997, str. 157-158):

• **vderi v sistem** - ti imajo lahko za posledico le nepooblaščen dostop do podatkov in njihovo krajo, lahko pa tudi spremembo ali še huje, uničenje podatkov (med te napade lahko uvrstito večino današnjih računalniških virusov, ki se prikrajejo do sistema in povzročijo določeno škodo),
• **prestrezanje sporočil** - tu napadalec ne vdre v sam sistem, pač pa za dostop do podatkov (in tudi morebitno spremembo le-teh) uporabi prenosne poti, kjer z ustreznim strojno in programsko opremo premoži prilisškuje ali spreminja podatke, ki potujejo po napadeni poti,
• **onemogočanje storitev** (denial-of-service) - kjer napadalec poskuša poslabšati kakovost storitve ali jo povsem onemogočiti (npr. z izjemno pomnočenim številom zahtev po določeni storitvi v sistemu, ki pod tako obremenitvijo ne deluje več optimalno, ali pa z umetnim ustvarjanjem nepotrebnega omrežnega prometa, ki zasiči prenosne poti),
• **povzročanje stroškov** - tu napadalec izkoristi določene varnostne pomanjkljivosti in uporabi storitev, do katere sicer ni upravičen – to napadenemu povzroča nepotrebne stroške, druge škode ponavadi nima; ti napadi so danes zelo popularni, saj napadalec pride do informacijskih virov zastoj ali mnogo ceneje kot sicer.
Omenjene napade srečujemo tudi v kombinirani obliki. Z nedolžnim prisluškovanjem se napadalec lahko prikoplje do podatkov (npr. gesel), s katerimi lahko povzroči veliko škode.

Slika 1: Vrste napadov v omrežjih

Vir: Pepelnjak, Bradeško, 1997, str. 159.

2.2.2. Ukrepi varovanja sistemov in drugih virov

Varnost računalniških sistemov in drugih informacijskih virov, ki jih obravnavamo v sklopu računalniškega omrežja zagotovimo s kombinacijo naslednjih ukrepov (Pepelnjak, Bradeško, 1997, str. 159):

- strogo ločiti zasebni del omrežja (produkcijsko omrežje) od javnega dela omrežja, le-tega pa nadzorovano povezati z javnim omrežjem (s požarno pregrado - firewall),
- zagotoviti overjanje (avtentikacija - authentication) uporabnikov,
- določiti in nadzorovati uporabo pravic (avtorizacija - authorisation), ki jih imajo pooblaščeni uporabniki pri uporabi sistema,
- zaščititi vse transakcije, v katerih se izmenjujejo podatki, katerih razkritje ali nepooblaščena sprememba bi lahko privedla do škode (s šifriranjem in digitalnimi podpisi),
- zagotoviti beleženje (logging) vseh varnostnih dogodkov (dostopov do sistema, prenosov podatkov ipd.),
- vgraditi varnost v zavest uporabnikov, saj še tako dobra varnost nima učinka, če je nihče ne uresničuje.

2.3. ELEKTRONSKO PODPISOVANJE KOT ZAŠČITA TRANSAKCIJ

Elektronski podpis je nadomestek lastnoročnega podpisa v elektronskem poslovanju. Razvitih je več metod elektronskega podpisovanja. Načini podpisovanja se v praksi uporabljajo
zaporedoma ali prepleteno. Nekateri od teh so navedba imena kot podpis, skupina znakov (gre za niz (računalniških) znakov, ki zamenjajo podpisnikovo ime), digitalizirani lastnoročni podpis, ki ga lahko izvedemo na tri načine: s pomočjo računalniške slike, digitalnega posnetka in z digitalnim peresom. Najpomembnejši od vseh pa je digitalni podpis, ker zagotavlja največjo varnost. Največjo možno varnost podatkov pa si zagotovimo, če uporabimo kartico, na kateri imamo shranjen zasebni ključ v sistemu podpisovanja s ključi.

Digitalni podpis

Primer enojnega ključa je geslo pri shranjevanju besedila na računalniku ali pa osebno geslo (številka) pri bančni kartici. Pošiljatelj in prejemnik uporabita isti ključ (simetrični ključ). Pošiljatelj uporabi dogovorjeni ključ, vsebino sporočila in algoritem, ki vsebino premeša v nesmiselno množico znakov. Prejemnik podpis preveri z istim ključem.

Pri sistemu dvojnih ključev ima vsak pošiljatelj svoj zasebni ključ (tajni, privatni), ki je znan le njemu in ga lahko še dodatno zavaruje z geslom. Da bi prejemnik lahko sporočilo dešifriral, mu mora biti znan drugi pošiljateljev ključ, ki se imenuje javni ključ; tega lahko pozna kdorkoli. Zasebni in javni ključ sta v zahtevnem medsebojnem matematičnem razmerju, vendar je iz javnega ključa dejansko nemogoče izpeljati zasebnega.

Podpis s kartico
Elektronska kartica (chipcard, smart card) je naprava, ki je podobna kreditni kartici. Na njej imamo običajno shranjen zapis o istovetnosti pooblaščenega imetnika (certifikat), lahko pa vsebuje tudi množico drugih podatkov. Kot preprosto pomnilniško sredstvo se kartica uporablja tudi za elektronsko podpisovanje. Imetnik ima tako na elektronski kartici shranjen svoj zasebni ključ, ki ga naprava pri podpisovanju dokumentov avtomatično prebere s kartice.

2.4. PRAVNA UREDITEV ELEKTRONSKEGA POSLOVANJA

Uporaba informacijske tehnologije in z njo povezano elektronsko izmenjevanje sporočil ter hranjenje pomembnih dokumentov v digitalni obliki v vsakodnevni gospodarski in upravnem poslovanju je vse večja in z uveljavitvijo interneta dobiva še močnejši zagon. Pomanjkanje ustrezne zakonske ureditve lahko znatno ovira sporočanje pravno pomembnih in zavezujočih informacij v elektronski obliki in povzroči splošno pravno negotovost. Zato je potrebno zagotoviti pravno varnost najširše uporabe elektronskega poslovanja v domačem in mednarodnem gospodarstvu.

Za vzpostavitev urejenega elektronskega poslovanja je pomemben, da udeleženi subjekti zaupajo ureditvi elektronskega poslovanja in se nanjo zanesajo. Vzpostavljanje zaupanja je dolgotrajen proces, ki je z stališča potrošnika povezan s kakovostjo, s stališča ponudnika pa z varstvom lastnine. Zagotavljanje varnosti je prvi korak pri vzpostavitvi zaupanja kot nepogrešljivega elementa elektronskega poslovanja.
Zakonsko je potrebno urediti zelo široko področje, ki obsega prenos podatkov, izmenjavo elektronskih sporočil z uporabo javnih ali zaščitenih standardov preko javnih ali zasebnih omrežij ali pa najbolj splošno prenašanje golega besedila v elektronski obliki. Zaradi širine področja bo ureditev vplivala na izvajanje velikega števila zakonov in drugih predpisov ter je zato potrebno sprejeti enega ali več zakonov. Področje, ki ga je potrebno urediti, je tako široko tudi zaradi tega, ker zakonodajno urejanje elektronskega poslovanja posega tudi v zelo obširen spekter obstoječo zakonodajo, saj spreminja temeljne pravne pojme kot so izvirnik oz. original, pisna oblika, lastnoročni podpis pogodbenih strank in podobne pojme, ki jih zasledimo v večini slovenskih zakonov.


3. ELEKTRONSKO BANČNIŠTVO

Konkurenca na trgu bančnih storitev in razvoj informacijsko-računalniške ter komunikacijske tehnologije, sta banke vzpodbijala k iskanju novih distribucijskih kanalov, ki bi te storitve pripeljali k strankam. Če povzamemo, lahko ugotovimo, da banke danes ponujajo prav iste storitve le na nekoliko strankam prijaznejši in prikladnejši način kot so jih včeraj.

Z izrazom elektronsko bančništvo (v nadaljevanju EB) opisujemo vse storitve, ki na kakršenkoli način potekajo preko elektronskih medijev. Tako so se standardnemu načinu stika s komitenti preko bančnega okenca pridružili še bankomati, plačilne kartice, telebanking, POS terminali itd., ki strankam omogočajo neodvisno poslovanje od poslovalnic banke.

Razvoj globalnega računalniškega omrežja internet nakazuje prelomnico v razvoju komunikacij. Njegova univerzalnost, velika razširjenost ter dostopnost so povzročili, da iz tržišča izpoldriva vse ostale načine elektronske komunikacije, tako da se bo v prihodnje glavnina storitev elektronskega bančništva opravljala preko interneta.

3.1. RAZVOJ ELEKTRONSKEGA BANČNIŠTVA

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

⇒ uporabniki želijo opravljati storitve od kjerkoli, kadarkoli, na kakršenkoli način,
⇒ kakšno tehnologijo imajo na razpolago uporabniki (strankam naj ne bi vsiljevali tehnologije, ampak naj bi upoštevali tisto, ki jo imajo doma oz. v podjetju),
⇒ kakšna je telemunikacijska infrastruktura v Sloveniji,
⇒ kakšno povezavo želi banka vzpostaviti s strankami,
⇒ kakšni so dolgoročni in kakšni so kratkoročni učinki elektronskega bančništva,
⇒ uporabniki morajo imeti zaupanje v storitev,
⇒ banka mora poskrbeti za najvišjo stopnjo varnosti,
⇒ kakšna je ciljna skupina uporabnikov.

3.2. DELOVANJE ELEKTRONSKEGA BANČNIŠTVA

3.2.1. Standardni način

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

Komitent opravi elektronsko bančno storitev, tako da se s posebnim vmesnikom priključi na komunikacijsko omrežje, preko katerega tečejo informacije o želeni 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

![Slika 2: Princip delovanja elektronskega bančništva](Vir: Kovačič, 1997, str. 132)

3.2.2. Elektronsko bančništvo preko interneta

Ponujene storitve preko EB 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 preko interneta 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 standarden vmesnik,
- vmesniki nekaterih najbolj uveljavljenih proizvajalcev so brezplačni,
- vmesniki podpirajo varen prenos podatkov preko javnih telefonskih omrežij,
- komitent in banka se lahko prepričata o medsebojni identiteti na standardiziran način.
Vir: Kovačič, 1997, str. 133.

Poleg tega pa morajo bančne storitve zadoščati naslednjim zahtevam: dosegljive morajo biti od kjerkoli 24 ur na dan in 7 dni v tednu, biti morajo popolnoma avtomatizirane, njihovo opravljanje pa mora biti varno.

3.3. KATEGORIJE BANČNIH KOMITENTOV


• fizične osebe; mladina, študentje, gospodinjstva,
• samostojni podjetniki, pravne osebe – podjetja.

Mladina in študentje uporabljajo elektronsko banko večinoma za vpogled v stanje in promet tekočega (transakcijskega) računa. Nevarnost poslovanja s to kategorijo je zelo nizka za obe strani, zato so ustrezne zaščite lahko razmeroma enostavne in poceni. Za preverjanje komitentove identitete zadoščajo že navadna gesla.

Gospodinjstva želijo poleg vpogleda v stanje svojih računov in prometa na njih tudi možnost plačevanja svojih rednih obveznosti, prenos sredstev iz enega računa na drugega, vezavo denarja, zato mora biti stopnja zaščite varnega delovanja zelo visoka, sredstva za

Slika 3: Princip delovanja sistemov elektronskega bančništva preko interneta
zagotavljanje tega pa ustrezno zahtevnejša in tudi dražja. Vrhunsko stopnjo varnosti zagotavlja pametna kartica (smart card).

Ti komitenti niso odvisni od delovanja interneta, hkrati jim mora biti omogočeno direktno priključevanje na bančni strežnik brez uporabe le-tega. Za te komitente je značilna lastna ali poverjena knjigovodska ali računovodska dejavnost. Od elektronske banke se zato za podjetnike in podjetja zahteva, da jo je mogoče povezati z njihovim knjigovodskim oz. računovodskim informacijskim sistemom. Sistem elektronske banke za samostojne podjetnike in podjetja mora biti sposoben prevzemati podatke iz drugih poslovnih aplikacij in na drugi strani vanje prenašati lastne podatke, kar pomeni, da gre za avtonomen informacijski sistem, sposoben lokalne priprave in obdelave podatkov, ki se z bančnim strežnikom povezuje le v času prenosa podatkov.

3.4. POZITIVNI UČINKI ELEKTRONSKEGA BANČNIŠTVA

Informatizacija bančnega poslovanja sega še v čas pred internetom, vendar imamo zdaj v mislih večinoma bančne storitve, ki se opravljajo preko interneta. Poglavitna področja bančne dejavnosti na internetu obsegajo internetno bančništvo (Internet banking), domače bančništvo (PC banking) in informacije preko interneta (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 potegnemo pozitivne strani elektronskega bančništva (Sjekloča, 1999, str. 31-33):

→ Zmanjšanje stroškov bančnega poslovanja
→ Manj papirja, izginja potreba po klasičnem bančnem okencu, banke ne plačujejo stroškov komunikacije.

→ Stranki prihrani čas
→ Krajša vrste v bankah in omogoča hitro in natančno informacijo o stanju računa ali bančnih storitvah.

→ Zanesljivost informacije
→ Zaradi multimedijske komunikacije je ta zlahka preverljiva.

→ Kroženje denarja
→ Ga 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.

3.5. VARNOST IN ZAŠČITA

Osrednji problem elektronskega bančništva je gotovo zagotavljanje zaščite vsem stranem, ki so vpletene v opravljanje bančnih transakcij preko javnih komunikacijskih medijev. Banke komitentom ponujajo specializirani programski paket, s katerim je mogoče priključiti računalnik neposredno na bančni sistem, toda večina se odloča za posredni način preko interneta in komercialnega programskega paketa. Prvi sistem je sicer varnejši, kajti internet je oprotn sistem z mnogimi varnostnimi luknjami.
Pri opravljanju oz. izvajanju finančnih transakcij preko interneta je potrebno upoštevati predvsem naslednje elemente, ki zagotavljajo varnost pri opravljanju finančnih transakcij (Bračun, 1997, str. 153):

- kriptografska orodja in protokoli,
- identifikacija,
- protipožarna pregrada (firewall),
- kontrola dostopa oz. avtorizacija.


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

Identifikacija oz. avtentičnost izvora podatkov je postopek, ki omogoča enolično identifikacijo stranke. Z njo ugotavljamo ali je pošiljatelj res ta, ki se izdaja zanj. Z zagotavljanjem avtentičnosti je pošiljateljem hkrati odvzeta možnost, da bi se poslanim podatkom odrekli ali jih zatajili. Identitetu zagotavljajo tako overovljeni certifikati bančnih komitentov, ki so shranjeni v elektronskih notarnjih (certificate agency) - overitelj.

S protipožarno pregrado onemogočimo vdor v centralni bančni sistem. Kot zadnji element naj omenim kontrolo dostopa oz. avtorizacijo, ki določa, kaj stranka lahko počne in kaj ne.


4. INTERNET

Internet je postal nekaj modnega in nujnega, nekaj, brez česar se skorajda ne da več poslovati, če že ne živeti. Je neurejeno in ogromno računalniško omrežje brez pravega središča, ki z nekaj sivimi lisami pokriva ves planet.
To je pravzaprav le skupno ime za množico med seboj povezanih manjših omrežij, medtem ko internet kot podjetje ali ustanova sploh ne obstaja (Logar, 1996, str. 50).


4.1. RAZVOJ INTERNETA

Internet dandanes po svetu uporabljajo tisti ljudje, ki so že spoznali in tudi že uporabljajo prednosti elektronskega oz. računalniškega povezovanja, ko govorimo o računalniških mrežah in omrežjih. V začetnem obdobju računalništva so imeli dostop do računalniških obdelavah vedno večje. Z razvojem računalnikov so se rojale nove ideje, kako bi njegovo uporabo še razširili.

Konec šestdesetih let so ameriški znanstveniki začeli raziskovati, kako bi po različnih komunikacijskih poteh, katerih osnovna je seveda telefonska, pokrivali čim širše območje oz. velike razdalje za pošiljanje podatkov. V posredno pomoč so jim bile razmere hladne vojne. Ameriško obrambno ministrstvo je takrat potrebovalo računalniški komunikacijski sistem, ki bi deloval tudi po morebitnem jedrskem napadu. Namesto enega računalniškega središča, ki bi bil enostavna tača, so si zamislili poljubno število centrov, med seboj povezanih na najrazličnejše načine (od telefonskih do satelitskih) (Logar, 1996, str. 51). Tako je nastalo poskusno omrežje ARPAnet (Advanced Research Projects AGENCY ali Agencija za napredne raziskovalne projekte), s katerim so rešili obe osrednji težavi: prenos podatkov in iskanje najboljše poti do ciljnega računalnika.


Računalniška tehnologija, ki je bila v začetku namenjena le računalniškim strokovnjakom in znanstvenikom, je z leti postala veliko bolj uporabna in prijazna.
4.2. UPORABA INTERNETA

Internet, kot svetovno omrežje računalnikov in računalniških omrežij, povezuje na tisoče manjših regionalnih omrežij iz celega sveta. Je globalno omrežje, ki združuje veliko računalnikov po celem svetu. Nanj se lahko priključimo preko klicne telefonske linije, najete telefonske linije, javnega omrežja za prenos podatkov ter ISDN linije za digitalni prenos podatkov. Internet tako podpira dokumente, ki vsebujejo besedilo, slike, zvok in film.

Povod za nastanek interneta je bilo medsebojno povezovanje računalnikov, tako se lahko skoraj vsakdo v razvitem svetu vključi v internet. Da bi se lahko po omrežju sprehajali, pa potrebovamo za to potrebno računalniško opremo, ki jo delimo na strojno (hardware) in programsko (software).


4.2.1. Ponudniki priklopa na internet

Do devetdesetih let so bile omrežne storitve kar dobro razširjene med podjetji a premalo med navadnimi uporabniki. S pojavom svetovnega spleta na internetu je prišlo do preobrata. Nove tehnologije in aplikacije so zagotovile prijaznost do uporabnika in enostavnejšo uporabo, poslovanje se je pocenilo, hkrati pa splet omogoča raznovrstne poslovne aktivnosti. Dostopen je tako organizacijam kot fizičnim osebam.


Množica in raznolikost podatkov sta tolikšni in tako zelo vabljivi, da so se naposled pojavili tudi komercialni ponudniki storitev internet. Internet je znižal stroške komuniciranja, odprl pot do novega načina poslovanja in novih trgov, povečal učinkovitost in zagotovil, da je ekonomija postalna globalna, gospodarske organizacije pa globalno povezane. Podjetja so hitro ugotovila, da lahko s ponudbo na spletu pridobijo nove kupce, tako da danes v njem
prevladujejo podjetniki z vsega sveta, ki prodajajo najrazličnejše dobrine (od delnic in nepremičnin do plošč in arhivskih vin). Ta podjetja in gospodinjstva dostopijo do interneta preko komercialnih ponudnikov. Pri nas imamo že kar nekaj podjetij, ki se ukvarjajo s tovrstno dejavnostjo. Nekatera od njih so: AMIS.NET, AGENDA, K2.NET, MOJ NET, BOTER, SIOL in VOLJATEL. To so ponudniki modemskega pristopa preko najetih vodov ali klicnega dostopa.

4.3. NAJPOMEMBNJEŠE STORITVE INTERNETA

Storitve, ki jih omrežje internet ponuja, so najpomembnejše za uporabnika, kajti omogočajo medsebojno komunikacijo in dostop do podatkov vseh vrst po vsem omrežju. Storitve so zasnovane na načelu odjemalec/strežnik. Komunikacija med odjemalcem in strežnikom se odvija s pomočjo protokolov in je za uporabnika nevidna. Programa tipa odjemalec/strežnik sta različna. Računalniki v omrežju internet, ki posredujejo podatke, poganjajo strežni program, medtem ko uporabnik interneta poganja odjemalne programe. Storitve so:


**TELNET** – storitev, ki omogoča dostop do oddaljenih računalnikov (ki so v nekem trenutku priključeni in vklopljeni v internet) in s tem do njihovih storitev (z dovoljenjem za uporabo – geslo). Podoben je običajnim terminalskim programom, ki jih osebni računalnik uporablja za povezovanje z oddaljenim računalnikom. Danes ga uporablja bolj malo ljudi, ker ne omogoča veliko povezav, dve od teh sta katalogi knjižnic in elektronske oglasne deske.


**CHAT in Internet Relay Chat (IRC)** (internetni klepet v realnem času) – Chat je star sistem, katerega je že v celoti skoraja nadomestil IRC. Je sistem, ki omogoča več ljudem, da se sočasno pogovarjajo oz. omogoča zbiranje uporabnikov na strežniku IRC in klepet med njimi.

**E-MAIL** (elektronska pošta) – je ena od najstarejših in najbolj razširjenih storitev interneta. Je prenos elektronskih pisem med lastniki elektronskih naslovov. Sporočila se preko interneta prenašajo s protokolom preprostega prenašanja sporočil SMPT (Simple Mail Transport Protocol). Uporabnik s prijavo vstopi v računalniški sistem, napiše sporočilo in ga naslovi na...
uporabnika drugega sistema. Sporočilo nato potuje po omrežju med seboj povezanih računalniških sistemov, dokler ne doseže naslovnika.


4.4. STANDARDI, PROTOKOLI IN JEZIKI, KI OMOGOČAJO KOMUNICIRANJE PO OMREŽJIH


Na začetku razvoja so bile računalniške naprave zaradi svoje visoke cene dosegljivele izredno ozkemu krogu ljudi, lkrati pa naprave različnih proizvajalcev niso omogočale komuniciranja med seboj. Takšni sistemi sta bili zelo togi. Uporabniki pa so želeli komunikacijski sistem, ki bi bil neodvisen od proizvajalcev. Zaradi tega se je na področju računalniških sistemov in komunikacijske opreme pojavila potreba po standardih (standard - pomeni enega ali več formalno sprejetih dogovorov, ki ga razumejo vsi uporabniki).

Razvoj standardov je tako potekal v dveh smereh: standardi proizvajalcev (ki se zaradi praktične in široke uporabe hitro uveljavljajo) in standardi s pripadajočimi protokoli, katere pripravijo in priporočijo posebne organizacije za standardizacijo. Najbolj znani standardi proizvajalcev so:

- SNA (System Network Architecture) - IBM,
- XNS (Xerox Network System) - Xerox,
- DSN (Distributed System Network) - Hewllett-Packard.

Najbolj znane mednarodne organizacije pa so:

- ISO (International Standard Organization),
- IEEE (Institut of Electrical and Electronic Engineers),
Ko govorimo o računalniških komunikacijah oz. o komunikacijskih protokolih, imamo v mislih predvsem računalniško komunikacijo, kar pomeni komunikacijo med računalniki. Za to lustrijevamo besede in slovnična pravila, računalniki pri svojem povezovanju uporabljajo računalniški jezik. Ta je strukturiran v obliki dogovorjenih pravil in postopkov, ki jim pravimo protokoli (protokol je računalniški jezik, strukturiran v obliki različnih pravil, dogovorov in postopkov, ki vodijo in opravljajo prenos informacij).


5. ELEKTRONSKO BANČNIŠTVO PRAVNIH OSEB NOVE LJUBLJANSKE BANKE

5.1. ELEKTRONSKO BANČNIŠTVO NOVE LJUBLJANSKE BANKE

Elektronsko bančništvo opredeljujemo kot način poslovanja strank z banko, ki je neodvisen od poslovnic banke, vendar pa tisti, ki uporabljajo to besedno zvezo, razumejo pod tem pojmom različne stvari: od raznovrstnega komuniciranja bančnih komitetov z banko, do...
pravih finančnih in denarnih transakcij. Vse to pa seveda temelji na informacijski tehnologiji in poteka s pomočjo elektronskih medijev.

Mediji, ki podpirajo elektronsko bančništvo vključujejo:

- telefon (v živo in avtomatski odzivnik),
- osebni računalnik,
- bančne avtomate,
- on-line storitve in internet,
- informacijske terminale,
- televizijo,
- mobilne telefone-GSM,
- pametne kartice,
- elektronske denarnice,
- elektronsko pošto itd.

Vse več bančnih komitentov tako opravlja enostavne transakcije (dvig gotovine, poizvedbe) izven poslovalnic in se selijo na druge medije, ki nudijo večje udobje in razpoložljivost. Ta način poslovanja je koristen tako za komitente kot za banko. Strankam poleg udobja nudi velik prihranek časa, banke pa na ta način razbremenijo delavce na bančnih okencih, ki se lahko bolj posvetijo posameznim strankam (Bračun, 1997, str. 149).

V Novi Ljubljanski banki (v nadaljevanju NLB) so razvili že celo paleto poti poslovanja z banko oz. kot jih v NLB-ju imenujejo »bližnje do banke«. Komitente so razporedili v dve skupini, na fizične (občane, študente) in na pravne osebe. V slednjo poleg podjetij štejejo 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.

Rešitvi sta si funkcionalno podobni, vendar se bistveno razlikujeta v tehnološki podpori. Razvili so ju v sodelovanju z zunanjimi izvajalci, Proklik NLB s podjetjem Halcom Informatika, Proklik plus NLB pa s podjetjem Hermes Softlab (Zaslon) (NLB, 2002a).

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. Podjetje se lahko glede na lastni informacijski sistem in specifične potrebe odloča med obema rešitvama. Podjetja in samostojni podjetniki lahko tako urejajo in izvajajo vse storitve preko osebnega računalnika od doma ali iz delovnega mesta.

5.2. UVAJANJE E-BANKE ZA SAMOSTOJNE PODJETNIKE IN PRAVNE OSEBE

Elektronska banka naj bi omogočala uporabo vseh bančnih negotovinskih storitev. Banka od komitentova prejema zahtevke, on pa od nje najrazličnejše vrste podatkov: od poročil o finančnih transakcijah na njegovem računu do odgovorov na zahtevke, sporočil in obvestil, ki so namenjena njemu osebno ali pa so globalnega pomena za vse komitente.

Ciljna skupina uporabnikov e-banke v NLB so bili najprej samostojni podjetniki, ker je za njihovo uspešno poslovanje zelo pomembna finančna ažurnost ter imajo podobne potrebe kot pravne osebe.

→ Ažuren pregled nad stanjem računa  
→ Priprava podatkov naj poteka lokalno  
→ Možna izbira datuma valutacije  
→ Obrazci naj bodo vizualne kopije sedanjih  
→ Obstajati mora nadzor nad stanjem predanih zahtevkov  
→ Omogočati mora povezavo z drugimi aplikacijami  
→ Zagotavljati mora najvišjo stopnjo varnosti poslovanja

→ Uporabnik mora imeti sliko o trenutnem stanju na računu in spisek vseh transakcij, ne glede na to kje in kako so bile sprožene.  
→ Povezava se vzpostavi občasno, ko je potrebno osvežiti podatke bodisi na strani komitenta bodisi na strani bančnega strežnika.  
→ Izvajanje nakazil z računa mora dopuščati izbiro datuma za vnaprej.  
→ Izpolnjevanje le-nehora biti kontrolirano pravopisno in pomensko, sistem mora dopuščati vključitev imenika pravnih oseb ter lastnega imenika poslovnih partnerjev.  
→ Uporabnik ima pregled nad izvajanjem vsakega izdanega zahtevka. Stanje zahtevka mu pove ali ga je poslal v banko ali ga je ta sprejela in potrdila in ali ga je že obdelala.

→ V smislu tajnopisa, avtentičnosti podatkov in bančnih udeležencev do zaščite bančnega strežnika pred vdorom.

Pri načrtovanju in izvedbi je bilo ključnega pomena sodelovanje strokovnjakov Nove Ljubljanske banke in Halcoma. Da so povezali že obstoječe bančne aplikacije in strežnik elektronske banke ter obvladovali postavljene omejitve, je bilo potrebno doseči obojestransko razumevanje obeh segmentov.

Ob zagonu e-banke so uvedli stalen nadzor nad delovanjem sistema, hkrati pa so z zapisovanjem opažanj in odstopanj zgodaj odkrivali težave in jih pravčasno odstranili, še predno bi te začele ogrožati delovanje sistema.


Banka je na ta način uporabniku zagotovila povezavo do strežnika elektronskega bančništva preko lastne vstopne točke, torej klicni dostop. Uporabljali so to pot do konca leta, ko je bil na voljo v celoti bančni skupini NLB (v nadaljevanju Proklik +). 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 razpredano svojo lastno mrežo računalnikov in so geografsko razpršena.

5.2.1. Reforma plačilnega prometa

Elektronsko bančništvo je že pred nekaj leti začela uvajati Agencija RS za plačilni promet (APP) vendar pa so bili pogoji zanj takrat precej bolj neprimerni. Ni bilo primernih tehnologij za zaščito podatkov in ni obstajalo močno javno omrežje, v katero bi bil lahko vsakupnik računa vključen. Agencija je takrat za pošiljanje plačilnih nalogov uporabljala elektronsko pošto, ki pa danes ni več primerna, ker ne zagotavlja nadzora nad časom dobave sporočila. Poleg tega pa je banka stroški plačilnega prometa potekala po elektronski banki Proklik, ki je strankam omogočala premoženje dogajanja na njihovem računu (Potočnik, 1999, str. 2).

Prav zaradi te reforme sedaj ves plačilni promet potekal preko bank. Uvedba EB v času prenosa računov pravnih oseb je bankom omogočila, da so lahko prevzeli delo Agencije RS za plačilni promet brez odpiranja novih dragih bančnih okenc in brez zaposlovanja velikega števila novih delavcev.
Elektronsko bančništvo pa ne prinaša prednosti le bankam, temveč tudi uporabnikom. V reformiranem plačilnem prometu se plačila med komitenti z računi pri isti banki izvajajo v realnem času. To pomeni, da se znotraj banke plačilo opravi po prevzemu in se takoj pokaže na računu prejemnika, ne glede na to kaj sta plačnik in prejemnik: pravna ali fizična oseba oz. samostojni podjetnik. Prejemnik lahko takoj razpolaga s svežimi prilivi in hitreje obrača svoj denar.

Plačila komitentov, ki imajo račune pri različnih bankah, se prav tako poravnajo v krašnjem času. Plačila, katerih vrednost presega dva milijona tolarjev, se poravnajo preko sistema BPRČ, manjša plačila pa preko sistema ŽK. Ta plačila se ravno tako knjižijo na račune komitentov, takoj ko banke prejmejo obvestilo.

V okviru reforme sta se združila domači plačilni promet in plačilni promet s tujino, saj ima komitent le en transakcijski račun pri banki tako za domači kot tudi za plačilni promet s tujino. Tolar je le ena od valut istega transakcijskega računa. Poslovanje s tujino je tako bolj hitro in enostavno. Banki ni potrebno čakati na potrditev tolarske plačila pri APP. Podjetja in zasebniki z eno potezo nakazujejo sredstva s svojega računa, konverzija iz tolarjev v devize je opravljena v banki, celotno stanje na računu pa je pregledno v realnem času.

5.3. SISTEM ELEKTRONSKEGA BANČNIŠTVA

Raziskave o tem, katero od sodobnih poti elektronskega poslovanja bančni komitenti postavljajo na prvo mesto kažejo, da je v ospredju uporaba internetne tehnologije, kar je tudi ena od karakteristik globalizacije. Vendar pa je internetno bančništvo le ena od sodobnih tržnih poti. Prav zaradi heterogenosti v bančnih informacijskih sistemih je bilo potrebno zgraditi sistem, ki temelji na načelih integralnosti in varnosti ter bo v podporo vsem distribucijskim kanalom in različnim finančnim produktom ob upoštevanju centralnega nadzora in upravljanja (Trampuž, Cajhen, 1999, str. 158).

Sistem, ki omogoča hiter, poceni in učinkovit razvoj storitev, zasnovanih na sodobnih distribucijskih kanalih, se imenuje Sistem Elektronskega Bančništva (SEB). Z integralno rešitvijo, kot je SEB, se banka prilagodi poslovnim potrebam in zahtevam komitentov. Celotna ponudba bančništva na daljavo Nove Ljubljanske banke tako temelji na modularnem sistemu elektronskega bančništva, ki ga je razvilo podjetje Zaslon.

Zaradi uporabe enotnega skrbniškega sistema vseh distribucijskih kanalov, ki so vezani na SEB, je poenostavljeno vzdrževanje in razvoj sistema. Sistem temelji na industrijskih standardih in odprtosti sistemov, ki omogočajo nadgradnjo in hitro prilagajanje novim tehnologijam, kar pomeni, da je treba sistem neprestano izboljševati z dodajanjem novih vrednosti k procesom elektronskega bančništva.

5.4. E-BANČNIŠTVO OMOGOČA AVTOMATIZACIJO POSTOPKOV


Informacijski sistem podjetja ima nenehno svežo informacijo o spremembi stanja na računu, saj je vsaka sprememba na bančnem računu nemudoma vidna v informacijskem sistemu podjetja, ne da bi bil potreben dodaten ročni poseg ali celo prepisovanje podatkov. Rešitve imajo vgrajen mehanizem, ki omogoča popolnoma avtomatizirano zapiranje plačilnih nalogov na osnovi pripadajočih prometnih postavk. Omogočajo kombinacijo ročnega in avtomatičnega pristopa. Imajo največjo fleksibilnost formatov (poleg APP in B2B), podpirajo tudi računovodske pakete, format XML ali druge posebne formate. Zaradi posebnega vmesnika pa hkrati omogočajo enoten način za poslovanje z različnimi bankami.
Prednosti uporabe B2B E-Bank in avtomatizacije postopkov so (Halcom I., 2002c):

- vpeljava najsodobnejšega, varnega in zanesljivega načina elektronskega poslovanja z bankami,
- izboljšanje nadzora nad likvidnostjo podjetja,
- možnost hitrejšega obračanja sredstev podjetja v povezavi s svežimi informacijami in postopki v zaledni obdelavi,
- elektronsko plačevanje v domovini in v tujino,
- neposredna povezava z več bankami, kjer so odprti računi podjetja,
- zmanjšanje možnosti napak pri plačilih.

Te rešitve Halcoma se v Novi Ljubljanski banki skrivajo pod imeni, s katerimi trži EB za pravne osebe in zasebnike.

5.5. POSTOPKI VKLJUČITVE UPORABNIKA V E-BANKO

5.5.1. Kdo so uporabniki elektronske banke?

Uporabniki Proklika in Proklika plus najprej razdelimo glede na banko, v kateri imajo odprt poslovni račun, nato še na tip uporabnika.

BANKE UPORABNICE

Nova Ljubljanska banka je oktobra leta 2001 zaključila proces združevanja z naslednjimi bankami:

- Dolenjska banka, d.d.
- Banka Velenje, d.d.
- Pomurska banka, d.d.

Vse tri so prenehale obstajati kot samostojne pravne osebe in so pod okriljem Nove Ljubljanske banke pošlale regionalne divizije poslovne mreže. Poleg tega pa je NLB povezana še s tremi bankami, ki so tako imenovane banke bančne skupine NLB:

- Banka Domžale, d.d
- Banka Zasavje, d.d.
- Koroška banka, d.d.

Vsi komitenti, ki imajo račun odprt v naštetih bankah, lahko uporabljajo bančni rešitvi.

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.
5.5.2. Kaj sistema omogočata?

»Poslovanje ni le hitrejše, preglednejše, stalno dostopno in bolj diskretno, temveč tudi cenejše!« je povedal vodja priprav na elektronsko banko Vilijem Krpič (Petek, 1999, str. 3).

a) Proklik NLB in Proklik plus NLB banki omogočata:
- vpogled v podatke o uporabniku,
- vpogled v stanje, promet, izpise, prilive, plačilne naloge v domovini in s tujino uporabnika po računih, vključenih v sistem,
- pošiljanje sporočil posameznim uporabnikom, različnim skupinam uporabnikov ali vsem uporabnikom,
- razvrščanje nalogov uporabnika glede na njihovo prioriteto (obveznosti do države),
- avtomatizirano pripravo podatkov za poročanje o bruto plačah uporabnikov,
- avtomatsko blokacijo računa, če ni sredstev za plačilo prioritetnih nalogov,
- avtomatizacijo postopka poročanja in predaje v izterjavo prioritetnih nalogov.

b) Proklik NLB in Proklik plus NLB uporabnikom omogočata:
- pregledovanje stanja računov,
- pregledovanje in tiskanje prometa, izpiskov in obvestil o prilivih,
- posredovanje plačilnih nalogov za:
  - tolerska nakazila (s tekočim datumom ali datumom valute vnaprej);
  - devizna nakazila (s tekočim datumom),
- pregledovanje prometa na računih po različnih časovnih obdobjih,
- izpis podatkov iz vpisanih plačil, prometnih postavk, izpiskov in podobno,
- izmenjava nalogov in prometnih postavk z računovodskimi programi uporabnika,
- vpogled v prejeta plačila iz tujine,
- tisk nalogov/paketov za domači plačilni promet in promet s tujino,
- uvoz/izvoz podatkov v/iz datoteke v formatu za domači plačilni promet,
- uvoz podatkov v formatu za plačilni promet s tujino,
- izmenjava sporočil med uporabnikom in banko (pritožba na bančno poslovanje, zahtevek za izdajo potrdila o plačilu, pošiljanje poročila o bruto plačah banki),
- pošiljanje podatkov za statistiko za Banko Slovenije,
- konverzije med različnimi valutami na deviznem računu, nakup deviz, prodajo deviz banki, vezavo tuje valute, prenos deviznih sredstev na račun pri drugi banki, nakup vrednostnih papirjev v tujini.

5.5.3. Potrebna računalniška in komunikacijska oprema

5.5.3.1. ZA PROKLICK NLB

Program je naložen lokalno pri uporabniku kot odjemalski program. Glede na namestitev baze podatkov in dostopa do njih lahko izbiramo med dvema različicama programa Proklik; enouporabniško in večuporabniško. Za elektronsko poslovanje pa potrebujemo:

- ustrezen računalnik, na katerem se izvaja Windows 95/98/ME ali Windows NT ali Windows 2000,
- modem za klicni dostop (analogni ali ISDN vmesnik),
• zaščitno kartico s čitalnikom zaščitne kartice in program Proklik NLB, ki jih dobimo v banki.

ENOUPORABNIŠKA (NEMREŽNA) RAZLIČICA


VEČUPORABNIŠKA (MREŽNA) RAZLIČICA


5.5.3.2. ZA PROKLIK PLUS NLB

Program, ki ga komitenti dobijo s strani Nove Ljubljanske banke, da bi elektronsko poslovali na daljavo in se skriva pod blagovno znamko Proklik +, se imenuje Bančni asistent. Podjetje ZASLON je razvilo programsko opremo (Bančni asistent) za podporo bančnemu poslovanju preko interneta. Podjetje se lahko na podlagi svojih potreb odloči za dva načina elektronskega poslovanja z banko; Bančni asistent 2000 in Bančni asistent 2000+.

BANČNI ASISTENT 2000

Bančni asistent 2000 je spletni uporabniški vmesnik, ki komitentom omogoča - podjetja z uporabo brskalnika (npr. MS Internet Explorer) - izvedbo negotovinskih bančnih opravil. Ciljna skupina so predvsem mala in srednje velika podjetja, za izvajanje posameznih opravil pa tudi velika podjetja.

Glavni značilnosti:
• možnost izvedbe posameznih opravil je mogoča tudi v okolju, kjer uporabnik ne želi ali ne more namestiti Bančnega asistenta 2000+ (npr. v času potovanja lahko na tujem računalniku pooblaščena oseba podpiše plačilni nalog, ki ga predhodno vnese operativno osebje v podjetju),
• možnost izvedbe opravil izven pogostega delovnega okolja (npr. na potovanju z javno dostopnim računalnikom).
BANČNI ASISTENT 2000+

Bančni asistent 2000+ je modularni sistem, ki je nameščen na strani podjetja in je namenjen izvajanju negotovinskih bančnih opravil. Ciljna skupina so predvsem velika in srednje velika podjetja.

Glavne značilnosti:
- delo v času (npr. vnosi plačil, pregledi) ko program ni povezan z bančnim strežnikom,
- večbančno poslovanje: istočasen pregled nad računi iz različnih bank,
- upravljanje s pravicami uporabnikov v okviru omejitev, ki jih opredeli banka.


Delo v času:
- ON LINE – povezava je vzpostavljena in podatki se med programom in bančnim strežnikom sproti obnavljajo,
- OFF LINE – lahko opravljamo nekatere dejavnosti, ki neposredne povezave ne zahtevajo (priprava plačilnega naloga). S pritiskom na gumb Pošlji/Prejmi sprožimo povezavo v internet in plačilni nalog pošljemo banki v obdelavo.

Večbančno poslovanje pomeni, da lahko uporabniki uporabljajo en program in en zaščitni sistem za povezavo z več bankami hkrati. Tako lahko uporabljajo le eno orodje za najrazličnejše finančne transakcije in za hkraten pregled trenutnega stanja na različnih bankah. Program sam skrbi, da se podatki obnavljajo in so v skladu z dejanskim stanjem v banki. Podjetje ima tako z enim klikom na zaslonu pregled stanja na transakcijskih računih različnih bank.


Za vsako od programskih rešitev v banki prav tako priporočijo ustrezno konfiguracijo računalnika.

5.5.4. Pogoji za odobritev uporabe Proklika NLB ali Proklika plus NLB

Uporabniku je odobrena uporaba če:
- banki predloži pravilno izpolnjen in podpisan zahtevek za odobritev uporabe Proklika ali Proklik plus,
- zakoniti zastopnik uporabnika pooblasti eno ali več oseb za uporabo Proklika ali Proklik plus, ali na zahtevku določi, da bo Proklik ali Proklik plus uporabljal tudi sam,
- ima v banki odprt temeljni račun,
- korektne posluje s transakcijskim računom,
- za opravljanje plačilnega prometa s tujino z banko sklene dogovor o načinu izvrševanja nakazil v tujino.
5.5.5. Postopek za priključitev uporabnika

Sprejem in odobravanje zahtevkov poteka v poslovalnici. Ko Sektor za sodobne tržne poti (SSTP) prejme odobrene zahtevke, izvede ali naroči vse potrebne aktivnosti za otvoritev novega uporabnika (glej sliko 5).

Pri otvoritvi novega uporabnika SSTP koordinira postopke, pri katerih sodelujejo tudi druge institucije oz. organizacijski deli banke. Ti postopki so povezani z doseganjem zahtevane ravni varnosti.

Predviden najdaljši čas od oddaje zahtevka do začetka rednega poslovanja je 11 delovnih dni. Ta časovni okvir velja za primere, ko bo uporabnik dobil vse potrebno opremo po pošti, namestitev pa bo opravil sam. V posebnih primerih na pobudo poslovalnice namestitev pri uporabniku izvede banka vendar to lahko pomeni nekaj dni časovnega zamika.

Če uporabnik želi izvedeti, v kateri fazi je postopek za otvoritev njegove uporabe oz. okviren čas, v katerem bo začel uporabljati Proklik ali Proklik +, se o tem lahko pozana v SSTP ali v poslovalnici, ki informacijo pridobi od SSTP.

Slika 5: Osnovni procesi

Vir: Interno gradivo NLB.

5.5.6. Kaj prejme uporabnik, po odobritvi zahtevka, za nemoteno poslovanje?

a) Za uporabo sistema Proklik NLB prejme:
   - priročnik za uporabo programa Proklik NLB,
   - parametre klicnega dostopa,
   - čitalnik zaščitne kartice,
   - programski paket za uporabo Proklika NLB,
   - navodila za izpolnjevanje toalarskih in deviznih plačilnih nalogov.
Vsak pooblaščenec na naslov pravne osebe oz. samostojnega podjetnika prejme:
- začetno kartico in
- osebno številko (PIN).

Uporabnik oz. njegov pooblaščenec lahko sam izvede namestitev programa v skladu s prejetimi navodili, opredeljenimi v priročniku za uporabo programa Proklik NLB, ali pa mu pri tem pomaga uradni pooblaščenec banke.

b) Za uporabo sistema Proklik plus NLB prejme:
- priročnik za uporabo Proklika plus NLB,
- urnik za sprejem in obdelavo plačilnih nalogov,
- čitalnik začetne kartice,
- začetno kartico,
- programski paket za uporabo Proklika plus NLB in
- navodila za izpolnjevanje nalogov za plačilni promet v domovini in s tujino.

Vsak pooblaščenec na naslov družbe oz. samostojnega podjetnika prejme:
- referenčno številko po elektronski pošti,
- geslo za prevzem certifikata s poštno pošiljko s povratnico in
- certifikat.

Uporabnik oz. njegov pooblaščenec izvede prevzem certifikata sam v skladu s prejetimi navodili, opredeljenimi v priročniku za uporabo Proklika plus NLB, pri namestitvi programa pa mu lahko pomaga tudi uradni pooblaščenec banke.

5.5.7. Obveznosti pri poslovanju s Proklik NLB in Proklik Plus NLB

5.5.7.1. OBVEZNOSTI UPORABNIKA OZ. POOBLAŠČENCA

Zakoniti zastopnik uporabnika in/ali njegovi pooblaščenci se zavezujejo, da bo/do:
- varovali parametre klicnega dostopa, programsko opremo Proklik NLB s pripadajočimi podatki in začetni komplet in jih ne bodo dajali tretjim osebam v uporabo ali na vpogled, pri čemer nosijo/je popolno odgovornost za škodo, ki je bodisi posredno ali neposredno povzročena, zato ker so tretje nepooblaščene osebe uporabile uporabnikov klicni dostop ter osebno številko in/ali začetno kartico,
- takoj obvestili banko o vseh nepravilnostih,
- ob prvi uporabi Proklika NLB in kasneje najmanj enkrat na mesec menjavali svojo osebno številko (PIN) in geslo za klicni dostop, pri čemer osebna številka ali geslo ne sme biti krajše od šest alfa-numeričnih znakov,
- ali
- varovali osebno geslo ter zasebni ključ in jih ne bo/do dajal(i) tretjim osebam v uporabo ali na vpogled, pri čemer nosijo polno odgovornost za vsako škodo, ki je bodisi posredno ali neposredno povzročena, zato ker so tretje nepooblaščene osebe uporabile uporabnikov dostop do Proklika plus NLB,
- takoj obvestili banko o vseh nepravilnostih,
- najmanj enkrat mesečno menjavali svoje osebno geslo, pri čemer osebno geslo ne sme biti krajše od šest alfa-numeričnih znakov,

hkrati pa tudi
- redno spremljali poslovanje na temeljnem in sekundarnih računih,
pri svojem poslovanju poleg splošnih pogojev upoštevali tudi priručnik za uporabo programov ter druga navodila, ki jih uporabniku posreduje banka in veljavno zakonodajo,

**zahtevali ustavitev uporabe programov, če se ne bodo strinjaši z novimi oz. s spremenjenimi splošnimi pogoji in to v 15 dneh od datuma obvestila o spremembi.**

### 5.5.7.2. **OBVEZNOSTI BANKE**

- **Banka** zagotavlja uporabniku izvedbo vseh pravilno izpolnjenih in pravočasno oddanih plačilnih nalogov po veljavnem urniku predaje in obdelave nalogov pod pogojem, da je na temeljnem in/ali sekundarnem računu kritje in račun ni blokiran. **V primeru, da na računu ne bo kritja v višini, ki je potrebna za izvršitev plačilnega naloga,** bo banka plačilne naloge poskušala obdelati do ure, navedene na urniku. Po tem času bo naloge brez ustreznega kritja na računu uporabnika dokončno zavrnila, o čemer bo banka uporabnika ob prvi naslednji povezavi z banko obvestila preko programa. Banka ob tem upošteva tudi vse zakonske in podzakonske predpise s področja opravljanja storitev plačilnega prometa,

- programa omogočata uporabniku sprotni vpogled v promet in stanje na temeljnem in/ali sekundarnem računu ter status plačilnih nalogov,
- banka pošlje urnik uporabniku ob pošiljanju zaščitnega kompleta,
- banka si pridržuje pravico, da spremeni oz. dopolni urnik in se zavezuje, da bo uporabnika oz. njegove pooblaščence obvestila o spremembi urnika v roku osmih dni pred uvedbo nameravane spremembe urnika z obvestilom, ki ga prejmejo v elektronski obliki preko programsko vgrajene opcije v obeh sistemih,
- banka se zavezuje, da bo ob vsaki spremembi oz. dopolnitvi splošnih pogojev obvestila uporabnika,
- spremembe splošnih pogojev v času uporabe Proklika dobi uporabnik v elektronski obliki v sistemu sporočila Proklika ali po pošti v pisni obliki,
- spremembe splošnih pogojev v času uporabe Proklika + bodo objavljene na spletnih straneh Proklika +, uporabnikom bodo poslana tudi s priporočeno pošto s povratnico v pisni obliki.

### 5.5.7.3. **OBVEZNOSTI KOMERCIALISTA**

Komercialist (poslovni skrbnik) mora ob sprejemu celotne dokumentacije preveriti identiteto zakonitega zastopnika in pooblaščencev, preveriti njihove podpise in podatke, vpisane v različne zahtevke. Komercialist odgovarja za pravilnost podatkov in podpisov na zahtevkih.

Za opravljanje plačilnega prometa s tujino mora, po navodilih Banke Slovenije, uporabnik skleniti dogovor o načinu izvrševanja nakazil v tujino, brez predložitve dokumenta, iz katerega bi bila razvidna osnova plačila. Komercialist s podpisom na zahtevku potrdi, da je uporabnik sklenil ta dogovor z banko.

### 5.5.8. **Pooblastila za uporabo**

Pri Prokliku imamo devet nivojev pooblastil (NLB, 2002b):

1. pooblastilo za administriranje je namenjeno administrativnim posegom v Prokliku NLB, kot so brisanje lokalne baze podatkov, osveževanje programa iz bančnega strežnika, spreminjanje gesla vstopne točke itd.,
2. pooblastilo za vnašanje podatkov je namenjeno pripravi plačilnih postavk, izpiskov, stanj, obvestil,
3. pooblastilo za pregledovanje je namenjeno pregledu prometnih postavk, izpiskov, stanj, obvestil,
4. pooblastilo za vsebinsko podpisovanje (verificiranje) je namenjeno le pregledovanju in potrjevanju plačilnih nalogov, hkrati pa tudi spreminjanju in dopolnjevanju imenika (če nalog ni podpisan, ga ni možno poslati),
5. pooblastilo za pošiljanje podatkov je namenjeno komunikaciji z bančnim strežnikom in elektronsko podpiše poslane podatke.

Zadnje štiri vrste pooblastil pa se pri Prokliku podvojijo, ker imajo funkcije ločene glede na vrsto plačilnega prometa (domovina, tujina). Pri tem pa ima lahko pooblastilo za pošiljanje podatkov le oseba, ki jo zakoniti zastopnik uporabnika pooblasti za razpolaganje s sredstvi na uporabnikovem temeljnem in/ali sekundarnem računu.

Proklik plus ima šest nivojev pooblastil (NLB, 2002c):

1. pooblastilo za vnašanje podatkov omogoča uporabnikov vnos in uvoz plačilnih nalogov, ne pa tudi podpisovanje in pošiljanje le-teh. Prav tako mu ni omogočen pregled finančnih podatkov,
2. pooblastilo za pregledovanje je namenjeno pregledu finančnih podatkov,
3. pooblastilo za individualno podpisovanje je namenjeno individualnemu podpisovanju in pošiljanju plačilnih nalogov,
4. pooblastilo za desno podpisovanje omogoča desno podpisovanje plačilnih nalogov,
5. pooblastilo za levo podpisovanje omogoča levo podpisovanje plačilnih nalogov,
6. pooblastilo za urejanje čakalne vrste omogoča urejanje čakalnih vrst nalogov.

Pooblastilo za individualno podpisovanje se izključuje s pooblastili za desno in levo podpisovanje. Ostala pooblastila se med seboj ne izključujejo, kar pomeni, da lahko uporabnik pooblaščencu dodeli več pooblastil hkrati. V primeru, da ima pooblaščene pravico levega in desnega podpisnika se lahko podpiše samo na eno pozicijo hkrati.

5.5.9. Možni postopki po vključitvi uporabnika

Uporabniki lahko tudi potem, ko že uporabljajo program, spreminjajo določene predpostavke. Med drugim lahko zastopnik uporabnika med rednim poslovanjem pooblaščence dodaja, ukinja, jim spreminja pooblastila; spreminja račune (dodaja, ukinja); naroča dodatne čitalce; če pride do spremembe matičnih podatkov uporabnika, se le-ta javi v SSTP, ti pa v roku treh dni vnesejo nove podatke.

5.5.10. Ukinitev uporabe programa

Banka lahko ustavi uporabo programa na pobudo uporabnika ali poslovalnice ter zaradi spremembe statusa temeljnega računa. V vseh primerih mora uporabnik vrniti čitalce kartic in kartico oz. kartice. Bančni delavec kartico oz. kartice uniči pred uporabnikom, obrazec za ukinitev in čitalce pa pošlje v SSTP. Plačilni nalogi, ki jih je uporabnik preko programa oddal pred ukinitvijo, bodo obdelani tudi, če so valutirani s kasnejšim datumom.

Banka lahko izvede ukinitev na predlog poslovalnice ali SSTP zaradi nekorektnega poslovanja, suma poskusa zlorabe, malomarnega ravnanja z varnostnimi elementi ipd..

V primeru, da je ukinjen temeljni račun ali je imetnik računa umrl (oz. je pravna oseba prenehala obstajati), poslovalnica izpolni in v SSTP pošlje obrazec ukinitev poslovanja, na podlagi kateregak bo SSTP ukinil uporabo programa vsem pooblaščencem uporabnika.

5.5.11. Cena uporabe Proklika NLB in Proklika plus NLB

Poslovanje preko elektronskega bančništva je cenejše od poslovanja v enotah banke. Cene obdelave nalogov so zaradi avtomatične obdelave nižje od stroškov, ki bi jih imeli, če bi plačilne naloge nosili v banko (glej tabelo 2).

Pristopnina za uporabo Proklika ali Proklika + znaša 7.000 tolarjev. Cena pametne kartice znaša 15.000 tolarjev in čitalnik 8.000 tolarjev.

Tabela 2: Tarifa za plačilni promet v domovini

<table>
<thead>
<tr>
<th></th>
<th>Uporabniki poslovnega računa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interno nakazilo</td>
<td>30,00 sit</td>
</tr>
<tr>
<td>Eksterno nakazilo – poravnava v sistemu ŽK</td>
<td>50,00 sit</td>
</tr>
<tr>
<td>Eksterno nakazilo – poravnava v sistemu BPRČ</td>
<td>490,00 sit</td>
</tr>
</tbody>
</table>

Vir: Interno gradivo NLB.

Tarifa za plačilni promet s tujino
- nakazilo v tujino - 0,15% od vrednosti naloga, najmanj 1.500,00 sit in dejanski stroški 1.000,00 sit,
- nakazilo iz tujine - 0,15% od vrednosti naloga, najmanj 1.500,00 sit in dejanski stroški 1.000,00 sit.
5.6. ZANIMANJE ZA SODOBNE TRŽNE POTI NARAŠČA


Slika 6: Število transakcij po sodobnih tržnih poteh v milijonih


Skupina NLB je v letu 2001 z elektronskim bančništvom pri segmentu prebivalstva dosegla 52-odstotni tržni delež, pri segmentu podjetij in zasebnikov pa 47-odstotni delež z več kot 16.500 odprtimi poslovnimi računi. Tržni delež telefonskega bančništva dosega 77 odstotkov, pri poslovanju z bančnimi avtomati skupine NLB pa 54-odstotni delež. V prihodnosti pričakujejo nadaljnjo rast tržnega deleža pri poslovanju z elektronskim bančništvom.


Uporaba oz. naraščanje števila uporabnikov Proklika + se ne da primerjati z naraščanjem števila uporabnikov Proklika, pa vendarle je tudi ta pot dosegla svoje uspehe. Konec leta 2001 ga je uspešno uporabljal kar 800 podjetij. Preko te tržne poti so posredovali nekaj več kot 100.000 nalogov, ki predstavljajo plačilni promet v domovini. Konec leta 2002 pa se je število uporabnikov približalo 4.000 ter uspešno obdelalo nekaj več kot 2 milijona nalogov, ki predstavljajo plačilni promet v domovini (glej sliko 8).

Slika 8: Število uporabnikov Proklika plus NLB po četrtertijih

Vir: Interno gradivo NLB.
Kot sem že omenila, se imetniki poslovnega računa (POR), ki je en od pogojev uporabe e-banke za pravne osebe in zasebnike, odločajo za uporabo ene ali druge tržne poti za opravljanje plačilnega prometa doma in v tujini na podlagi lastne informacijske strukture. Pri tem pa je, sodeč po podatkih do konca marca 2002 opaziti, da je način opravljanja plačilnega prometa preko elektronske banke Proklik +, bolj priljubljen med gospodarskimi družbami kot med zasebniki (glej sliko 9). Eden izmed glavnih razlogov za to je verjetno ta, da ima večina srednje velikih in velikih podjetij stalen dostop do interneta, saj brez tega podjetje težko ostaja konkurenčno na trgu.

Slika 9: Uporabniki e-banke – imetniki poslovnega računa v NLB


5.7. POSLOVNI VIDIK ELEKTRONSKEGA BANČNIŠTVA

Elektronsko bančništvo (kot sodoben način opravljanja storitev) je predvsem poenostavilo poslovanje. Z uvedbo so imeli tako banke kot komitenti določene stroške, hkrati pa je prinesla kar nekaj prednosti. Ne moremo pa trditi, da elektronsko bančništvo nima slabih strani. V nadaljevanju bom opredelila elektronsko bančništvo tudi s teh vidikov.

5.7.1. Stroški elektronskega bančništva

5.7.1.1. STROŠKI BANKE

Ob uvedbi kakšne novosti je cenovna plat prvi vidik, s katerim se sooči vsako podjetje kot tudi banka. Razvoj in uvedba elektronskega bančništva sta predstavljala največji strošek pri banki. Končnega zneska ne poznam, ker je to podatek, ki ga banka ne želi izdati v javnost.


Delovanje sistema je odvisno tudi od kvalitete opreme - strežnikov, ki ustrezajo zahtevam EB, najema oz. nakupa telefonskih linij. Nemoteno delovanje sistema pa je v največji meri odvisno od ponudnika internetnih storitev, s katerim NLB sodeluje in to je podjetje Siol.
Poleg tehničnih zahtev je banka morala usposobiti ustrezni kader, saj je bančno osebje moralo imeti tudi ustrezno računalniško znanje. Tehnologi so usposobljeni za pomoč uporabnikom. Za opravljanje dela jim je banka zagotovila ustrezne prostore in računalnike s programsko opremo.


5.7.1.2. STROŠKI UPORABNIKOV

Pravne osebe in zasebniki morajo imeti primerno opremljen in zmogljiv računalnik. Ta je v večini primerov osnovni pogoj za opravljanje dejavnosti, zato se njihovi stroški pri uporabi Proklika in Proklika + nanašajo predvsem na:
- pristopnino za uporabo v znesku 7.000 tolarjev,
- nakup pametne kartice v znesku 15.000 tolarjev,
- nakup dodatne pametne kartice v znesku 16.500 tolarjev,
- izdajo nove kartice zaradi izgube ali poškodbe v znesku 18.000 tolarjev,
- nakup čitalnika pametne kartice v znesku 8.000 tolarjev.

V primeru, da želi podjetje tudi namestitev s strani banke, ga to stane 8.000 SIT/uro.

Tisti uporabniki, ki se odločijo za Proklik +, morajo imeti tudi dostop do interneta. Večina ga ima že zaradi rednega poslovanja. Trendi kažejo, da brez dostopa do interneta podjetja težko ostajajo konkurenčna.

Raziskava, ki je bila narejena že leta 1999, o rabi interneta je pokazala, da ima dostop do interneta že 99 % velikih podjetij, srednje velikih podjetij z dostopom je 97 % in v več kot 80 % imajo urejen dostop do interneta tudi mala podjetja (vprašanje je bilo postavljeno podjetjem z računalniško opremo) (RIS 1999, 2003a). V začetku leta 2001 so imela dostop do interneta že praktično vsa velika podjetja in velika večina malih podjetij.


5.7.2. Prednosti elektronskega bančništva

5.7.2.1. PREDNOSTI ZA BANKO

Prednosti, ki jih elektronsko bančništvo prinaša bankam je kar nekaj.

opravimo v poslovalnici, 0,6 dolarja, če jo opravimo preko telefona, in le 0,02 dolarja, če jo opravimo preko spleta (Kapital, 2002b).

→ **Razbremenitev bančnih uslužbencev** - z uvedbo EB se je v banki močno zmanjšal pritisk na bančna okenca. Bančni uslužbenci za okenci se lahko bolj posvetijo strankam. To pa posledično pripelje do boljšega razumevanja ter uresničevanja finančno bančnih potreb strank.

→ **Kakovostno trženje drugih bančnih storitev** - banka lahko preko EB bolj učinkovito trži svoje storitve, kar ne velja samo za obstoječe storitve, temveč tudi za vse nove, ki jih banka sedaj enostavneje vključuje v svoje poslovanje. Uporabniki se na novo ponudbo banke lahko odzovejo takoj.

→ **Pridobitev novih komitentov** - zaradi internetnega načina poslovanja lahko banka pridobi nove komitente tudi na lokacijah, kjer nima poslovalnic.

→ **Znižanje stroškov obveščanja o stanju na računu** - banke svoje komitente obveščajo o stanju na računu in drugih novostih preko elektronske pošte oz. komitent ima zaradi elektronskega poslovanja z banko že avtomatičen vpogled v stanje. Obveščanje po običajni postavi preko pošte ni več potrebno.

→ **Večja kontrola poslovanja** - zaradi elektronskega poslovanja so podatki organizirani v pregledni obliki in je kontrola nad njimi lažja.

→ **Večja kakovost poslovanja** - Pomembna pridobitev je tudi kakovost zajetih podatkov, saj elektronska obdelava praktično ne dopušča napak. S tem je kakovost podatkov večja, kajti že same aplikacije imajo vgrajene mehanizme, ki skrbijo, da ne prihaja do napak. Če pa pride do nepravilnosti, je vzrok zanjo relativno lahko najti.

→ **Elektronsko zajemanje in obdelava podatkov** - uporabniki sami vnesejo potrebne podatke, potem pa sistem avtomatsko obdela te podatke. Banki ni treba dodatno vnašati podatke, ker se ti takoj prenesejo in so elektronsko obdelani.

→ **Večja ažurnost in informiranost o poslovanju komitentov** - ker so vsi načini poslovanja povezani preko enega sistema ima banka oz. bančni uslužbenec vpogled v trenutno stanje svojih komitentov, tako lažje in hitreje odgovarja na njihove želje in jim hkrati svetuje.

5.7.2.2. PREDNOSTI ZA UPORABNIKE

Elektronsko bančništvo ima kar nekaj prednosti tudi za uporabnike, kajti le obojestranske koristi zagotavljajo uspešen razvoj te vrste poslovanja.

→ **Enostavnost opravljanja transakcij** - tisti, ki v podjetju upravlja s sredstvi, lahko s svojega računalnika opravlja transakcije preko banke.

→ **Nič več čakanja v vrsti** - velika večina sovražnih čakanj v dolgih vrstah pred bančnim okencem, spletne poslovanje jih razbremeni teh težav.

→ **Prihranek časa** - v poslovnem svetu je čas denar, le-tega pa stranke ne želijo porabiti za opravila, ki jih lahko izvedejo preko računalnika.

→ **Možnost opravljanja storitev 24 ur na dan** - saj se vse spremembe zaradi izvedene transakcije takoj zabeležijo v zbirko podatkov, tako da lahko uporabnik spletne banke takoj vidi spremembe na svojem računu.

→ **Možnost hitrih reakcij** - EB je lahko v veliko pomoč v situacijah, ko je treba hitro ukrepati (opraviti določeno plačilo).

→ **Nižji stroški** - cenejše in hitrejše transakcije. Podjetja, ki dnevno izvajajo veliko število nakazil, bodo gotovo upravičila osnovno investicijo v spletno poslovanje s svojimi
bankami že s prihranki pri provizijah. Podjetja, ki imajo kupce in dobavitelje po celi Sloveniji in poslujejo z NLB, bodo lahko hitreje in ceneje opravila transakcije znotraj banke kot pa v medbančnem okolju.

→ **Nižja cena bančnih storitev** - v primerjavi z zneskom, ki ga komitent plača pri klasičnem načinu poslovanju na bančnem okencu, je transakcija preko elektronske banke dosti cenejša, saj znaša samo 30 tolarjev, če gre za poravnavo znotraj banke (glej tabelo 3).

Tabela 3: Cena poslovanja preko različnih tržnih poti v NLB

<table>
<thead>
<tr>
<th>Negotovinsko poslovanje</th>
<th>Preko elektronske banke</th>
<th>Na magnetnem mediju</th>
<th>V dnevno-nočnem trezor</th>
<th>V papirni obliki na bančno okence</th>
<th>Preko Teledoma (samo zasebniki)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oddano</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vを受け方</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOLARSKO poslovanje</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plačilo stranki pri NLB</td>
<td>30</td>
<td>65</td>
<td>130</td>
<td>160</td>
<td>155</td>
</tr>
<tr>
<td>Plačilo stranki v ŽK</td>
<td>50</td>
<td>80</td>
<td>160</td>
<td>170</td>
<td>165</td>
</tr>
<tr>
<td>Plačilo stranki v drugi banki - BPRČ</td>
<td>490</td>
<td>510</td>
<td>590</td>
<td>600</td>
<td>590</td>
</tr>
</tbody>
</table>

→ **Večja preglednost nad računi** - EB omogoča stalen vpogled v stanje računov, ni več potrebno čakati na obvestilo, ki prihaja po pošti.

→ **Povečana storilnost zaposlenih** - s hitrim in učinkovitim izvajanjem nakazil, to pa je hkrati za podjetje glavna dodana vrednost spletnega bančništva (Kapital, 2002a).

→ **Informacije so stalno dostopne** - z internetnim trženjem oz. objavo na domači spletni strani, banka konstantno obvešča svoje komitente o novostih.

5.7.3. Slabosti elektronskega bančništva

5.7.3.1. **SLABOSTI ZA BANKO**

Pri vsaki novosti se poudarjajo predvsem njene pozitivne lastnosti in koristi, vendar pa ima vsaka taka noviteta tudi svoje slabe strani.

→ **Visoki začetni stroški** - zaradi heterogenosti v bančnem informacijskem sistemu je bilo potrebno v banki zgraditi sistem elektronskega bančništva, ki je podpora vsem tržnim kanalom in različnim finančnim produktom. Velik del stroškov pa pripada še trženju, torej reklami, saj je bilo potrebno novo distribucijsko pot predstaviti uporabnikom.

→ **Zaposlitvi ustrezni kader** - zaradi določenih strokovnih znanj, ki jih zahteva elektronsko bančništvo, mora banka zaposlitvi nov kader – bolj izobražen in dražji.

→ **Nezaupanje novi tehnologiji** - kljub temu, da nas računalnik spremlja že na vsakem koraku, nekateri ne zaupajo takemu načinu poslovanja – skeptični so predvsem zaradi varnosti podatkov. Iz navedenega pa izhaja naslednje dejstvo.

→ **Uporaba klasičnega načina poslovanja** - ljudje raje uporabljajo že utečeni način poslovanja, kateremu zaupajo, s tem povzročajo še vedno visoke stroške na bančnih okencih in zmanjšujejo potencialno učinkovitost EB.
5.7.3.2. SLABOSTI ZA UPORABNIKE

Zaradi slabosti EB se nekateri uporabniki ne odločajo za ta način poslovanja.

→ **Varnost finančnih podatkov** - podatki potujejo po omrežjih in sistemih, za katere nam nihče ne more zagotoviti popolne varnosti. Res je, da obstajajo mehanizmi in protokoli varovanja, vendar imajo tudi ti luknje, katere so tarča napadov.

→ **Zasebnost podatkov** - vprašljiva je nedotaknjjenost podatkov na poti v bančni sistem, ter ravanjanje bančnih uslužbencev v skladu z varovanjem podatkov.

→ **Osebni kontakt** - kot sem že omenila, se ljudje razlikujemo. Tako je nekaterim zelo pomemben osebni kontakt z bančnimi uslužbenci. Poslovni odnos želijo graditi na medsebojnem sodelovanju in zaupanju.

→ **Pisno potrdilo** - klasičen način poslovanja nas je naučil, da za vsako transakcijo prejmemo potrdilo kot dokazno listino. Pri EB stranimo nimajo nobenega potrdila v rokah o izvedeni transakciji. V primeru, da ga potrebujejo, ga lahko preko aplikacije ali po telefonu naročijo in prejmejo po pošti.

→ **Poznavanje delovanja EB** - uporabniki ne vedo kako dejansko deluje elektronsko bančništvo. Prav zaradi nerazumevanja postopkov ne zaupajo in posledično tudi ne uporabljajo teh storitev.

5.8. KAKO VARNO JE OPRAVLJANJE STORITEV PREKO E-BANKE?

Razvoj računalništva in elektronskih komunikacijskih tehnologij, njihova razširjenost in množičnost uporabe, odpirajo nove možnosti v medsebojnem komuniciranju. Hkrati pa je zaradi različnih možnosti, velike razširjenosti in dostopnosti javnega omrežja pogosto čutiti nezaupanje v take dejavnosti, predvsem z vidika osnovnih zahtev varnosti, zaupnosti in prepoznavnosti (avtentičnosti) elektronskih podatkov ter preverjanja identitete posameznikov, s katerimi komuniciramo.

Pri uvajanju varnostnih rešitev je potrebno upoštevati, da le-te ne otežijo uporabo storitev in da imajo naslednje lastnosti: omogočajo razširitev, so cenovno optimalne, so primerne za različne tipe storitev, omogočajo nadaljnje širitve storitev in medsebojno povezovanje ter so čimbolj transparentne za končnega uporabnika (Trampuž, Cajhen, 1999, str. 160).


- zagotavljanje zasebnosti na osnovi šifriranja (kriptiranja),
- preverjanje istovetnosti uporabnika na osnovi digitalnega potrdila (avtentičnost),
- preverjanje verodostojnosti podatkov na osnovi digitalnega podpisa.
Slika 10: Varnostne rešitve


Za varen prenos podatkov so v NLB prav tako poskrbeli s šifriranjem in elektronskim podpisovanjem sporočil. Pri tem uporabljajo asimetrično metodo imenovano algoritem RSA, ki zagotavlja 2048 bitov dolg ključ na strani strežnika in 1024 bitov dolg ključ na strani odjemalca (namenjena avtentičnosti in izmenjavi ključev) ter metodologijo šifriranja. Za Proklik NLB kriptografijo – 3DES, medtem ko za Proklik plus NLB metodo RC4 (128-bitni).


Slika 11: Pari ključev

Vir: www.gov.si/cvi/

5.8.1. Overitelji

Preverjanje povezave med uporabnikom in njegovim javnim ključem omogočajo v elektronskem poslovanju posebne ustanove, agencije za overjanje javnih ključev »Certification Authority« ali skrajšano CA. CA izvajajo storitve v zvezi z upravljanjem javnih ključev in v okviru teh storitev izdajo lastniku javnega ključa digitalno podpisano potrdilo ali digitalni certifikat, s katerim le-ta lahko vedno zagotavlja drugim uporabnikom avtentičnost uporabljjenega ključa. S tem potrdilom lahko lastnik certifikata dokaže lastništvo ključa in svojo identiteto v elektronskem okolju.

Overitelj tako predstavlja ustanovo, kateri zaupajo njeni komitenti - imetniki digitalnih potrdil ter ostali overitelji. S tem overitelja tudi pooblaščajo, da upravlja z njihovimi digitalnimi
potrdili. Vsak overitelj objavi svoj javni ključ in dokument (Certification Policy), ki opisuje postopek, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ. Overitelji morajo poskrbeti za varnost svojega zasebnega ključa, saj bi bila sicer potrdila, ki jih izdajajo, brez pomena, še več, lahko bi prišlo do poneverb, ki bi jih prepozno opazili. Hraniti ga morajo na dobro zaščitenem računalniku.

V primeru, da pozabimo geslo za uporabo svojega zasebnega ključa ali pa se je pokvarila naprava, kjer smo ključ hranili, je treba tvoriti nov par ključev in dobiti novo digitalno potrdilo, staro pa preklicati.

Nastajajo tudi overitelji, ki se omejijo na neko določeno področje. Tako so vodilne svetovne banke (okrog 33 bank) ustanovile podjetje Identrus, ki na osnovi sprejetih pravnih podlag bankam in drugim finančnim ustanovam omogoča izdajanje certifikatov. Deluje predvsem kot vrhovna agencija, ki verja javne ključe večjim finančnim ustanovam, te pa naprej podjetjem ali končnim uporabnikom.

V javni register overiteljev Republike Slovenije sta trenutno vpisani dve agenciji, ena deluje s strani Centra vlade za informatiko, druga pa je Halcomova certifikatna agencija – Halcom-CA. Nova Ljubljanska banka ima svojo službo za izdajanje digitalnih certifikatov, s tem da lahko lastniki certifikatov, le-te uporabljajo samo za dostop do bančnih aplikacij ustrezne banke.

5.8.2. Digitalno potrdilo

Digitalno potrdilo je potrdilo, ki je sodobna alternativa klasičnim osebnim identifikatorjem kot so osebna ali zdravstvena izkaznica, potni list, bančna kartica in podobno. Predstavljen je kot računalniški zapis, ki vsebuje najmanj osnovne osebne podatke o imetniku (lastniku), njegov elektronski naslov, njegov javni ključ in podatke o izdajatelju digitalnega potrdila ter obdobje veljavnosti zapisa. Ta zapis je računalniško narejen, tako da je digitalno podpisan z zasebnim ključem izdajatelja. Računalniško okolje omogoča izdajanje digitalnih potrdil fizičnim, pravnim osebam in tudi računalnikom, računalniškim rešitvam ali računalniškim zbirkam podatkov.

Namen potrdil je zagotavljanje varnega in legitimnega e-poslovanja, hkrati pa so sestavni del tehnioloških rešitev, ki nudijo (Terčelj, 2000, str. 4): ➢ zaupnost – le pošiljatelj in od njega izbrani prejemniki lahko dešifrirajo in berejo prejeto,
 ➢ avtentičnost pošiljatelja in nezmožnost zanikanja lastništva posredovane informacije – oboje je zagotovljeno z digitalnim podpisom pošiljatelja,
 ➢ celovitost sporočila – najmanjši del sporočila ni bil spremenjen ali drugače popravljen brez vednosti pošiljatelja.

Nova Ljubljanska banka uporablja verjena digitalna potrdila pri obeh tržnih poteh. Izdana so posameznim pooblaščencem. Ker v banki vedo komu so digitalno potrdilo izdali, lahko na podlagi digitalnega podpisa ugotovijo identiteto pošiljatelja (Smrekar, 2003, str. 5).

5.8.3. Digitalni podpis

Pod pojmom digitalni podpis najpogosteje razumemo povzetek dokumenta z zgostitvenim algoritmom (hash), šifriran z avtorjevim zasebnim ključem po asimetričnem algoritmu.
Najpomembnejša prednost digitalnega podpisa je, da zagotavlja neokrnjenost podpisanega dokumenta, saj je njegova lastnost ta, da najmanjša sprememba dokumenta podpis razveljavi, saj je ta odvisen od vsebine sporocila. Preverjanje digitalnega podpisa je učinkovito, saj je hitro, avtomatizirano in računalniško nezmotljivo.

V NLB bodo varnost podatkov v prihodnosti izboljšali tudi s širitvijo nabora pooblastil. Podatki bodo tedaj potrebovali več podpisov različnih pooblaščencev za pošiljanje v banko (zaenkrat je dovolj samo en podpis). Podjetje bo na računu določilo število potrebnih levih in desnih podpisov, posameznemu pooblaščencu pa vrsto podpisa (levi, desni, levi ali desni in individualni podpis).

Da digitalnemu podpisu verjamemo, mora postopek podpisovanja zagotoviti (CVI, 2003a):
- avtentičnost (verjamamo, da je podpisnik res tisti, za kogar se izdaja),
- da se podpisa ne da ponaredivi,
- da se podpisa ne da kopirati,
- da se podpisanega dokumenta ne da spremeniti in
- da se podpisa ne da zanikati (podpisnik ne more reči, da ni on podpisal dokumenta).

Lastnik digitalnega podpisa se lahko nevarnosti kopiranja oz. večkratne uporabe podpisa s strani prejemnika izogne, tako da vsako sporočilo opremi s podpisom, ki vsebuje tudi čas nastanka (timestamp) – natančen datum in omejitev veljavnosti sporocila.

Da bi se izognili varnostnim luknjam v postopku digitalnega podpisovanja, je potrebno predvsem zaščititi dostop do zasebnega ključa. Odločitev, hraniti zasebni ključ na disku računalniškega sistema, je predvsem odvisna od tega, komu še dovolimo uporabljati ta računalnik. Lastnik si bo večjo varnost zagotovil le, če bo zasebni ključ shranil na pametno kartico, do katere je dostop dodatno zaščiten z geslom (PIN koda), v sodobnejši izvedbi kartic celo s čitalnikom prstnega odtisa.

5.8.4. SSL (Secure Sockets Layer)

Pri navajanju varnostnih mehanizmov pa ne smejo pozabiti, da mora biti tudi pot, po kateri se informacije prenašajo, dobro zavarovana. Vsa komunikacija med uporabnikovim spletnim odjemalcem in bančnim strežnikom poteka preko protokola SSL (Secure Sockets Layer), ki predstavlja obliko varnosti, kakršno uporabljajo največje mreže po svetu, in deluje na vseh spletnih straneh, ki zahtevajo zaščito podatkov (CVI, 2003b). SSL je splošno sprejet varnostni protokol za varen prenos občutljivih podatkov preko interneta.

5.8.5. Povzetek

Vsak operacijski sistem je ranljiv pred samodejno namestitvijo tako imenovanih špijonskih programov, ki se v računalnik prikračujejo preko e-pošte, spletnih strani, CD-jev, nato pa v ozadju sistema neopazno tehčejo in prisluškujejo delovanju sistema. Prav tako kot moramo v vsakdanjem življenju poskrbeti za varnost (npr. vgrajujemo alarmne naprave), se je potrebno v »virtualnem« računalniškem svetu zavarovati pred napadi in vdori.

Banke imajo svoje sisteme zavarovane z najboljšimi možnimi metodami na trgu. Ti varnostni ukrepi zagotavljajo, da lahko s sredstvi na računu upravlja samo pooblaščenec s svojo pametno kartico in certifikatom, da podatke, ki so bili pri uporabniku digitalno podpisani, na
poti v bančni strežnik ne more nihče spremeniti. Žal pa banka ne more ugotavljati in skrbeti, kako je za varnost poskrbljeno na uporabnikovi strani.

Absolutne varnosti ni ne v realnem ne v računalniškem svetu. Zato ni dovolj, da za varnost skrbi le banka, velika mera odgovornosti, je potrebna tudi in predvsem na strani uporabnika. Bančni sektor je na področju informacijske varnosti pred drugimi panogami, saj so podatki v bazah dragoceni (denar). V te sisteme je zato težje vdirati. Lažja tarča so uporabniki, kateri bi morali upoštevati vse načine, s katerimi preprečimo, da se špijonski program ne prikraje v sistem. Priporočila za delo z računalnikom, na katerem teče elektronska banka (Strojan, 2002, str. 4):

- preprečevanje dostopa nepooblaščenim osebam do pametne kartice in računalnika,
- namestitev podatkovne zbirke na strežnik, ki je fizično in drugače varovan,
- namestitev in stalno osveževanje proti virusnih programov z novimi različicami,
- prepoved brskanja po internetu in sprejemanja elektronske pošte zaradi možnosti neopaznega nameščanja špijonskih programov,
- skrbno in nadzirano prenašanje novih datotek na računalnik,
- pregledovanje izvršenih plačilnih nalogov, ki jih pošilja banka.

6. SKLEP

Elektronsko bančništvo je tako v svetu, kakor tudi pri nas ena novejših storitev, ki jih ponujajo banke. Ravno konkurenca na trgu bančnih storitev je banke vzpodbudila k iskanju novih kanalov za opravljanje storitev. V prihodnje se bo glavnina storitev elektronskega bančništva opravljala preko interneta, saj se vse več podjetij povezuje v to omrežje. Internet je pripomogel k temu, da so bile premagane geografske in časovne omejitve poslovanja in bankam omogočil, da s svojo ponudbo vstopijo na svetovno bančno tržišče ter pridobijo nove stranke.


V prihodnje bodo banke okrog elektronskega bančništva intenzivno razvijale dodatne storitve v smislu celovitega bančnega poslovanja. Znotraj bank trenutno prevladuje usmeritev v posodabljanje informacijske tehnologije, to pa posledično vodi v prenovo oz. racionalizacijo procesov. Internet kot javna povezovalna infrastruktura bo zadovoljil večino komunikacijskih potreb med banko in komitentom. Poleg klasičnih prednosti o učinkovitejšem in cenejšem poslovanju, tako za stranke kot za banko, ima elektronsko bančništvo še dodatne prednosti. Banke so s svojimi strankami vzpostavile varno komunikacijsko infrastrukturo, ki jo lahko stranke same kot tudi banke pričnejo uporabljati tudi za druge namene povezane z elektronskim poslovanjem in elektronskim podpisom. V prihodnosti bodo elektronske pogodbe elektronsko podpisane izpodrinite papirnate, kar velja tudi za vse druge oblike dokumentov. Na ta način bodo banke lahko ponudile cel niz novih storitev kot so: pogodbe o vezavah sredstev za dolgo dobo, zahtevek za odobritev kredita, najava dvigovanja ekov, gotovine, pogodbe o depozitih itd. Elektronsko podpisane dokumente pa si bodo podjetja lahko izmenjavala med seboj z ali brez posredovanja bank.

Silen razmah telekomunikacijske in informacijske tehnologije nas spreminja v pripadnike informacijske družbe, v kateri postaja elektronski način poslovanja eden od temeljnih pogojev za uspešnost. Elektronsko bančništvo je gotovo ena od najbolj uporabljenih aplikacij, saj ga skoraj že vsako podjetje uporablja pri poslovanju. In kot sem že omenila bo ostalo osrednja in najbolj hitro se razvijajoča aplikacija v sodobnih bankah.
LITERATURA


VIRI

15. NLB: Izvleček iz tarife in sklepa o obrestnih merah Nove Ljubljanske banke d.d.  
16. NLB: Pogoji za uporabo elektronske banke Proklik NLB.  
17. NLB: Pogoji za uporabo elektronske banke Proklik plus NLB.  
[URL: http://www.zaslon.si], 15.11.2002.
PRILOGA 1: Seznam uporabljenih kratic

<table>
<thead>
<tr>
<th>Kratica</th>
<th>Namaščanje</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer</td>
</tr>
<tr>
<td>BPRČ</td>
<td>Bruto poravnava v realnem času</td>
</tr>
<tr>
<td>CVI</td>
<td>Center vlade za informatiko</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>G2B</td>
<td>Government to Business</td>
</tr>
<tr>
<td>G2C</td>
<td>Government to Consumer</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System of Mobile Communications</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>MS</td>
<td>Microsoft</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>RIP</td>
<td>Računalniška izmenjava podatkov</td>
</tr>
<tr>
<td>RIS</td>
<td>Raba interneta v Sloveniji</td>
</tr>
<tr>
<td>RSA</td>
<td>Algoritem poimenovan po avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman)</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>ŽK</td>
<td>Žiro kliring</td>
</tr>
</tbody>
</table>
PRILOGA 2: Zakonska opredelitev temeljnih pojmov elektronskega poslovanja

1. **elektronski podatki** so podatki, ki so oblikovani ali shranjeni na elektronski način;
2. **elektronsko sporočilo** je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto;
3. **elektronski podpis** je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;
4. **varen elektronski podpis** je elektronski podpis, ki izpolnjuje naslednje zahteve: da je povezan izključno s podpisnikom, da je iz njega mogoče zanesljivo ugotoviti podpisnika, da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom, da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi;
5. **časovni žig** je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času;
6. **pošiljatelj elektronskega sporočila** je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila;
7. **naslovnik elektronskega sporočila** je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo;
8. **prejemnik elektronskega sporočila** je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila;
9. **posrednik elektronskega sporočila** je oseba, ki za drugo osebo pošlje, prejme, shrani elektronsko sporočilo ali nudi druge storitve v zvezi z elektronskim sporočilom;
10. **podpisnik** je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis;
11. **informacijski sistem** je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki;
12. **podatki za elektronsko podpisovanje** so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
13. **sredstvo za elektronsko podpisovanje** je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;
14. **sredstvo za varno elektronsko podpisovanje** je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena tega zakona;
15. **podatki za preverjanje elektronskega podpisa** so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;
16. **sredstvo za preverjanje elektronskega podpisa** je nastavljena programska ali strojna oprema, ki se uporabljajo za preverjanje elektronskega podpisa;
17. **oprema za elektronsko podpisovanje** je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov;
18. **potrdilo** je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto;
19. **kvalificirano potrdilo** je potrdilo, ki izpolnjuje zahteve iz 28. člena tega zakona in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona;
20. **overitelj** je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpismi.
PRILOGA 3: Opredelitev izrazov, ki jih banka uporablja pri elektronskem bančništvu

- **uporabnik** je pravna oseba ali samostojni podjetnik, ki je komitent banke, in ki mu banka omogoči poslovanje preko e-banke;
- **zakoniti zastopnik uporabnika** je fizična oseba, ki v skladu z Zakonom o gospodarskih družbah zastopa pravno osebo ali samostojnega podjetnika in je kot taka navedena v listini o vpisu v sodni register;
- **pooblaščenec za uporabo** e-banke (v nadaljevanju pooblaščenec) je fizična oseba, ki je poslovno in opravilno sposobna in jo zakoniti zastopnik uporabnika pooblasti za uporabo programa e-banke;
- **temeljni račun** je transakcijski račun uporabnika. V primeru opravljanja plačilnega prometa s tujino, je temeljni račun transakcijski račun;
- **sekundarni račun** je tekoči ali transakcijski račun uporabnika, odprt pri katerikoli banki, ki je vključena v e-banko in svojim komitentom omogoča uporabo e-banke;
- **zaščitna kartica** je varnostni instrument, ki služi za identifikacijo, preverjanje identitete, elektronsko podpisovanje in šifriranje;
- **čitalce zaščitne kartice** služi čitanju zaščitne kartice;
- **osebna številka (PIN)** je zaporedje znakov, ki skupaj z zaščitno kartico omogoča uporabo Proklika NLB;
- **osebno geslo** za uporabo zaščitne kartice Proklika plus NLB;
- **certifikat** je elektronska identifikacija uporabnika pri komuniciranju preko Proklika plus NLB;
- **referenčna številka** je številka, ki se sistemsko določi ob izdaji certifikata in se uporablja za prevzem certifikata;
- **varnostni ključ** je po naključju izbrano zaporedje znakov, ki omogoča varno poslovanje pri uporabi Proklika plus NLB;
- **klicni dostop** je dostop, pri katerem je treba z modemom poklicati telefonsko številko, na kateri uporabnika sprejme računalnik, ki ga vključi v določeno omrežje;
- **parametri klicnega dostopa** (uporabniško ime, geslo za klicni dostop, IP številka) so podatki, ki jih uporabnik potrebuje za vzpostavitev povezave z banko;
- **zaščitni komplet** za uporabo e-banke vsebuje: zaščitno kartico, osebno številko, čitalce pametnih kartic, IP številko, uporabniško ime in geslo za nastavitev klicnega dostopa;
- **SSTP** – Sektor za sodobne tržne poti Nove Ljubljanske banke d.d.
PRILOGA 4: Blagovni znamki elektronske banke za pravne osebe in zasebnike v NLB