UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VARNOST ELEKTRONSKEGA BANČNIŠTVA: ANALIZA STANJA V SLOVENIJI

Ljubljana, september 2016 TANJA MAROLT

IZJAVA O AVTORSTVU

Podpisana Tanja Marolt, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom VARNOST ELEKTRONSKEGA BANČNIŠTVA: ANALIZA STANJA V SLOVENIJI, pripravljenega v sodelovanju s svetovalko prof. dr. Borko Džonovo Jerman Blažič.

IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 1.9.2016 Podpis študentke:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Zvečer, ko se vse umiri, se usedete v domači naslonjač in razporejate svoj težko prigarani denar, bodisi med vašimi računi bodisi med družinskimi člani. Pregledate lahko, koliko ste že zapravili in koliko imate še nerazporejenega denarja. Enostavno lahko pregledate vaše e-račune in jih z nekaj kliki tudi plačate, uredite dodaten limit na kartici ipd.

Elektronsko bančništvo je nepogrešljivo, tako za pravne kot fizične osebe. Lahko ga opredelimo kot poslovanje strank z banko, ki je neodvisno od lokacije in časa delovanja poslovalnice. Prav to je tudi razlog, da se fizične osebe vse pogosteje poslužujejo uporabe elektronskega bančništva, saj je dostopno 24 ur na dan.

Pred vzpostavitvijo enotnega plačilnega območja v evrih (Single Euro Payments Area v nadaljevanju SEPA) je Slovenija v večih pogledih zaostajala za Evropsko unijo, v plačilnem prometu pa jo je močno prekašala. Plačila med komitenti posameznih bank so se poravnavala vsaj petkrat na dan, v primeru majhnih plačil in takoj v primeru večjih. V zahodni Evropi je poravnava trajala tri dni, v najbolj razvitih pa en dan.

V okviru plačilnega območja SEPA, ki zajema 34 držav, so poravnave storile korak naprej. Pod določenimi pogoji se vršijo znotraj držav in med državami v območja SEPA, še isti delovni dan, glede na urnike posameznih bank. Zadovoljni so tako potrošniki kot podjetja, saj plačilo tako hitreje prispe na pravi račun.

Največ pomislekov je še vedno zaradi same varnosti elektronskega poslovanja. Zagotovljene totalne varnosti ni, ne v klasičnem ne v računalniškem svetu. Za čim večjo varnost pa lahko poskrbimo sami. Banke vse bolj stremijo k dodatnim elementom, ki bi uporabnikom elektronskega bančništva zagotovila čim večjo varnost. Med njimi je tudi varnostno SMS sporočilo, ki omogoča takojšnjo informacijo, kje je bilo plačilo z vašo kartico izvršeno in ali ste ga opravili vi ali nekdo, ki ni upravičen do vašega denarja. Informatiki v bankah vseskozi stremijo k temu, da so korak pred zlikovci, ki nikoli ne počivajo.

Vsa podjetja in posamezniki, ki ponujajo oblike e-poslovanja na svojih spletnih straneh, pozivajo k varni uporabi interneta. Uporabniki bi se morali seznaniti z osnovami računalniške varnosti, da bi bilo poslovanje pri elektronskem bančništvu varnejše. Ni samo banka tista, ki mora zagotoviti varnost, zato smo dolžni skrbeti tudi uporabniki, tako kot varnostne službe ne morejo preprečiti vloma v stanovanje, če ga lastnik ne zaklepa. Magistrsko delo se osredotoča na problematiko varnega poslovanja.

Problematika in namen magistrskega dela. Elektronsko bančništvo je zelo priročno in v primerjavi s klasičnim bančnim poslovanjem tudi cenovno ugodno za posameznega

uporabnika. Zelo mamljiva je misel na to, da lahko uporabnik v nekem trenutku kadarkoli v dnevu, tednu ali letu dobi informacijo o prilivih in odlivih na svoj transakcijski račun.

Elektronsko bančništvo omogoča uporabnikom razporejati prisluženi denar iz domačega naslonjača, za kar pa potrebujejo določeno računalniško opremo in stanje na transakcijskem računu. S klikom na miško ali sprehodom po ekranu lahko svoj denar brez večjega napora prenakažemo na transakcijski račun prejemnika. Postopek je lažji in krajši od klasičnega, pri tem pa se izognemo papirnemu poslovanju ter se vedemo okolju prijazno.

Namen magistrskega dela je pregled in povzetek spoznanj s področja elektronskega bančništva s poudarkom na varnosti poslovanja. Predstaviti želim, kako lahko uporabniki sami poskrbijo za varnost svojega računalnika in s tem tudi za varnost elektronske banke.

Cilji magistrskega dela so:

- predstaviti elektronsko poslovanje in elektronsko bančništvo,
- preučiti varnostno tehnologijo v elektronskem poslovanju,
- predstaviti primere zlorab v Sloveniji,
- analizirati varnost in uporabnost elektronskega bančništva v Sloveniji,
- predstaviti zadovoljstvo fizičnih oseb z izbrano banko in
- preveriti seznanjenost anketirancev z e-računom.

V magistrskem delu sem skušala podati oceno, ki sem jo pridobila s pomočjo anket, o tem, kako so uporabniki elektronske banke zadovoljni z njeno varnostjo in uporabnostjo.

Za temo sem se odločila predvsem zato, ker mi je elektronsko bančništvo blizu, saj se z njim srečujem tako na delovnem mestu kot v zasebnem življenju.

Elektronsko poslovanje. Prvi začetki internetnih storitev so bili osredotočeni zgolj na preizkušanje same storitve. Skozi preizkuse in prilagajanja si je internet pridobil zaupanje in tako so uporabniki začeli uporabljati tudi druge internetne storitve, ne le elektronske pošte in svetovnega spleta. Z uporabo interneta je bil omogočen tudi hiter razvoj elektronskega poslovanja, ki se neprestano prilagajanja tržišču, saj na njem vlada močna konkurenca.

Ob prebiranju literature lahko najdemo veliko razlag o e-poslovanju. Angleški pojem *electronic commerce* si v slovenščini razlagamo kot elektronsko trgovanje, kar oznaka e-poslovanje presega, saj pod njo lahko štejemo kot navaja Jerman Blažičeva (2001, str. 13) še vrsto drugih oblik uporabe informacijske in komunikacijske tehnologije v poslovnih odnosih. Sem sodijo trgovinske, proizvodne in storitvene organizacije kot tudi ponudniki informacij, potrošniki in državna uprava. Sestavni del elektronskega poslovanja je tudi elektronsko bančništvo.

Elektronsko bančništvo si lahko razlagamo kot poslovanje med komitentom in banko, ki ni odvisno ne od lokacije in ne od urnika obratovanja katerekoli od poslovalnic banke. Poslovanje med obema strankama v procesu, mora biti povezano z elektronskim medijem in zagotovljna mora biti določena tehnologija. Širši vidik e-bančništva vključuje vse bančne storitve, ki jih komitent lahko opravi po elektronski poti. To so (Miš Svoljšak, 1997, str. 12):

- spletna banka,
- bančni avtomati,
- kartično poslovanje,
- mobilna banka in
- telefonska banka.

Iz tega je razvidno, da v sklopu elektronskega bančništva lahko preko interneta opravimo več vrst storitev negotovinske transakcije:

- prenose med računi (znotraj ali izven svoje banke),
- plačila računov (tudi s pomočjo e-računa),
- pregled stanj na svojih računih (klasičnih in varčevalnih),
- izpis prilivov in odlivov za izbrano obdobje in
- pošiljanje ter prejemanje bančnih sporočil oz. obvestil.

Najpomembnejši element elektronskega bančništva je zagotavljanje varnosti. Banke in njihovi informatiki se trudijo ponuditi uporabnikom čim varnejšo rešitev, ki je podobna stopnji varnosti v klasičnem bančnem poslovanju.

Varnost. Kot navaja Jerman Blažičeva (2001, str. 101) so osrednja točka varovanja pri e-poslovanju viri, ki imajo za lastnika določeno vrednost in ki so izpostavljeni grožnjam. Splošne kategorije virov so podatki, informacije pri prenosu in hranjenju, strojna in programska oprema, uporabniki in odnosi med njimi, dokumentacija o postopkih strojne in programske opreme v sistemu ali omrežju ter denarna sredstva. Organizacija, ki posluje elektronsko, ima za zagotavljanje varnosti na voljo naslednje varnostne storitve:

- overjanje – identificiranje uporabnikov,
- zaupnost – dostop do podatkov imajo le pooblaščene osebe,
- neokrnjenost – ohranjanje pristnosti podatkov,
- nadzor dostopa – vstop dovoljen le registriranim uporabnikom,
- preprečevanje zanikanja o sodelovanju v aktivnosti poslovanja ter
- razpoložljivost.

Metode preučevanja in zasnove dela. V teoretičnem delu magistrskega dela sem uporabila vire in literaturo (slovenske in tuje strokovne knjige, publikacije, internetno gradivo ter splet). Praktični del magistrskega dela temelji na ugotovitvah, ki sem jih pridobila s pomočjo empirične raziskave.

V prvem delu sem povzela teorijo o elektronskem poslovanju in elektronskem bančništvu. V prvem poglavju je opisano elektronsko poslovanje, kjer predstavljam prednosti in slabosti za podjetja, posameznika in družbo**.** Drugo poglavje je posvečeno le eni veji elektronskega poslovanja, in sicer elektronskemu bančništvu, ki je tudi osrednji del magistrskega dela.

Tretje poglavje obsega predstavitev novejših pojmov in praks znotraj elektronskega bančništva, in sicer območja SEPA, UPN naloga ter e-računa.

V četrtem poglavju, ki je vsebinsko najobsežnejše, sem se lotila varnosti elektronskega poslovanja, predvsem pa varnosti elektronskega bančništva. Za zagotovitev varnosti so na voljo različne varnostne komponente. Predstavljam tudi nekaj zlorab v Sloveniji, ki so mi jih predstavili udeleženci ankete.

Za zadnje poglavje, ki obsega empirično raziskavo in je torej praktični del magistrskega dela, sem pripravila anketni vprašalnik, s katerim sem s preprostimi vprašanji skušala pridobiti čim več realnih odgovorov o tem, kako so uporabniki elektronskega bančništva zadovoljni z uporabnostjo in varnostjo svoje elektronske banke. Pripravila sem dve skoraj identični anketi, ki sta bili izvedeni v letih 2011 in 2016.

1 ELEKTRONSKO POSLOVANJE

1.1 Opredelitev elektronskega poslovanja

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

Elektronsko poslovanje je več kot samo navadno izmenjavanje računalniških podatkov in delovanje spletne trgovine. Vse, kar danes delamo v okviru poslovne dejavnosti s pomočjo raznih računalniških aplikacij in računalniških omrežij, imenujemo elektronsko poslovanje. To obsega (Bratina, 2005, str. 8):

- 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),
- elektronsko ponudbo (katalogi in videoteksti),
- elektronsko zavarovalništvo,
- elektronsko borzno poslovanje,
- elektronsko prodajo (potrošniško, retailing) in
- notranje elektronsko poslovanje (npr. v organizaciji).

Kot navaja Jerman Blažičeva (2001, str. 129) so pomembni elementi teh dejavnosti naslednji:

- **način dela**, kjer gre za računalniško izmenjavo podatkov ob uporabi odprtih omrežij, kot je npr. internet;
- **vsebina poslovanja**, kot so 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 itd. in
- **udeleženci poslovanja**, med katere lahko štejemo posameznike (podjetnike, managerje, raziskovalce, občane, učitelje, študente, dijake in upravne delavce), podjetja, bolnišnice, muzeje, galerije, univerze, izobraževalne organizacije in državne organe. Gre za poslovanje znotraj posameznih skupin in za poslovanje med skupinami. V zadnjem času prihaja v ospredje predvsem poslovanje med posamezniki ter med posamezniki in podjetji. Poslovanje med samimi podjetji je na trgu prisotno že dlje časa.

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

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

- bančne storitve temeljijo v veliki meri na informacijah;
- uporablja jih večina občanov, tako da imajo večje slovenske banke, ki so sicer po mednarodnih merilih razmeroma majhne, tisoč in več strank;
- banke nudijo široko ponudbo storitev, od katerih so nekatere take, da jih mnoge stranke koristijo skoraj vsak dan ali pa tudi večkrat dnevno.

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

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

1.2 Razvoj elektronskega poslovanja

Leto 1968 bi lahko označili za začetek elektronskega poslovanja, saj so v tistem času začeli razvijati internet ter računalniška omrežja. Prišlo je do združevanja telekomunikacijske in informacijske tehnologije ter uvajanje standardov za RIP (RIP oz. EDI (Electronic Data Interchange) pomeni izmenjavo standardiziranih, kodiranih sporočil med dvema računalniškima aplikacijama (Toplišek, 1998, str. 13)). Računalniško tehnologijo so v začetku uporabljali znanstveniki in računalniški strokovnjaki, kasneje je postala uporabnejša in dostopnejša za širše uporabnike.

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

- natančno določeno obliko podatkov in dokumentov, ki se izmenjujejo med različnimi aplikacijami na podlagi natančno določenih standardov, in

- preslikavo v želeno obliko, ki je bila draga in zapletena, težje dostopna in razumljiva za širši krog uporabnikov.

Kot navaja Škrlec (2002, str.18) je kljub pomanjkljivostim, ki jih je dajal sistem, je bila dobra stran standardizacije in izgradnje komunikacijske infrastrukture v avtomatizaciji procesov, ki je skrajšala čas obdelave podatkov in zmanjšala stroške prenosa. To se je dogradilo še v nadaljnjem razvoju, ki je bil hiter in učinkovit. Nove rešitve se dopolnjujejo s staro tehnologijo, kar podjetjem omogoča cenovno ugodno nadgradnjo sistema. 90. leta so z razvojem interneta ter s pojavom svetovnega spleta na internetu prinesla preobrat, ki je sprožil razvoj e-poslovanja na vse oblike uporabe, ki so poznane tudi danes in ki so se razširile med številne uporabnike. Njihovi temelji enostavne in preproste uporabe izhajajo iz ključnih predpostavk, ki gradijo internet. Te so:

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

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

1.3 Prednosti in slabosti elektronskega poslovanja

Uporaba e-poslovanja s seboj prinaša vrsto sprememb. Novosti so primerljive s tistimi, ki jih je prinesla industrijska revolucija.

Dobre poslovne ideje mnogokrat povlečejo podjetja v nepremišljene odločitve, zato pogosto tvegajo in se oprimejo nekakovostnih rešitev. Nekaterim kljub temu uspe, drugi imajo za posledice slabe finančne rezultate. Pogosto neuspeli poizkusi v ljudeh vzpodbudijo določen dvom in mečejo slabo luč na celotno e-poslovanje. Tistim, ki zares uspe pridobijo številne konkurenčne prednosti in na ta način prihaja do razkoraka med uspešnimi in manj uspešnimi (Pucihar, 1999, str. 7-13). V naših glavah je neprestano prisoten strah glede same varnosti in zaščite podatkov o naših stanjih na računu. Dodatno nezaupanje lahko povzroči že en sam vdor v bančni sistem, zato informatiki stremijo k stalnemu razvoju, ki bi zagotovil čim varnejši in funkcionalnejši sistem.

V e-poslovanju sodelujejo posamezniki, družba in podjetja, ki se srečujejo z določenimi prednostmi in slabostmi (Tabeli 1 in 2).

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

PREDNOSTI ZA PODJETJA	• širitev na nove trge, tudi globalne, • nižji stroški poslovanja in lastnih zalog, • prilagoditev proizvodov željam kupca, • skrajševanje proizvodnega cikla, • prenova poslovnih procesov, reinženiring, • nižji stroški telefonije,
PREDNOSTI ZA STRANKO	• primerjava cen za konkurenčne proizvode, • hiter dostop do akcijskih ponudb, • ocene in mnenja kupcev,
PREDNOSTI ZA DRUŽBO	• manjše onesnaženje okolja, zaradi spremembe delovnih navad, (delo od doma, manj prihodov na delovno mesto in manj potovanj), • možnosti razvoja za države tretjega sveta, pospeševanje dostave javnih storitev

Povzeto in prirejeno po E. Turban, M. H. Chung, J.Lee & D.King, Electronic Commerce, 2003, str. 16–20.

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

TEHNIČNE OMEJITVE	• pomanjkanje zanesljivosti, varnosti in tajnosti, • slab komunikacijski prenos, • nekompatibilnost opreme in hitre programske spremembe, • hitro spremenljiva tehnologija, • dodatni stroški za tehnično podporo, • dodatni stroški za nakup računalniške opreme,
NETEHNIČNE OMEJITVE	• dvom v varnost e-poslovanja, • nezaupanje v obstoj podjetij, • zakonodajne ovire, • različni standardi

Povzeto in prirejeno po E. Turban at al., Electronic Commerce, 2003, str. 20–21.

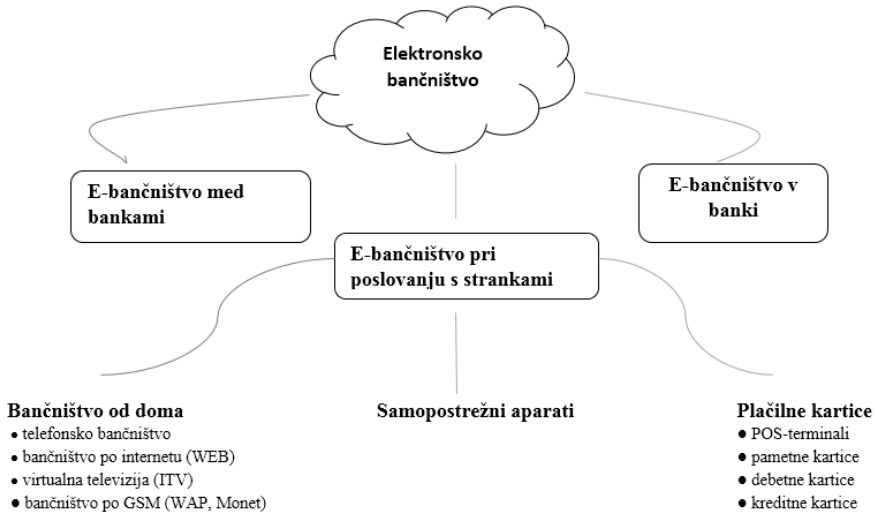
2 ELEKTRONSKO BANČNIŠTVO

2.1 Pojem elektronskega bančništva

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

Bančništvo je za elektronsko poslovanje še posebej ugodna dejavnost. Elektronsko poslovanje učinkovito podpira hitro in kakovostno izvajanje bančnih storitev. Z njim je mogoče storitve poceniti, njihova uporaba ni več omejena zgolj na čas, ko so banke uradno odprte, in na lokacijo bančnih poslovalnic, predvsem pa tako bankam kot njihovim strankam omogoča velike prihranke pri času. Zato ne preseneča, da se elektronsko poslovanje prav v bančništvu uvaja in krepi hitreje kot v večini drugih dejavnosti. Elektronsko bančništvo je vsekakor bančna storitev prihodnosti. Prej ali slej se mu bodo morale prilagoditi vse banke, ki bodo želele ohraniti poslovno konkurenčnost. Podobno kot to velja za druge poslovne organizacije, lahko tudi elektronsko bančništvo na najvišjem nivoju razdelimo na tri temeljne segmente (Slika 1).

Slika 1: Oblike elektronskega bančništva



Povzeto in prirejeno po I. Miš Svoljšak, V tujini se elektronsko bančništvo še povečuje, 1999, str. 4-5; Halcom, d.d., Interno gradivo, 1999.

V elektronskem bančništvu sodelujejo banke, podjetja in posamezniki, njihovi poslovni odnosi so sledeči:

- banka - banka (npr. medbančno komunikacijsko omrežje SWIFT – Society to Worldwide Interbank Financial Transakcion),
- banka - podjetje (pravne osebe) in
- banka - posameznik (fizične osebe).

Od začetkov elektronskega poslovanja med bankami je preteklo že kar nekaj časa. Za hitrejše in nemoteno izvajanje mednarodnih transakcij se je izoblikovalo medbančno komunikacijsko omrežje SWIFT. Gre za omrežje zaprtega tipa, preko katerega lahko banke v pravem formatu pošiljajo naloge za prenos finančnih transakcij. V Sloveniji se prelomno obdobje oz. porast števila uporabnikov elektronskega bančništva v podjetjih navezuje na obdobje prehoda z Agencije za plačilni promet (APP) na poslovne banke. Podjetja so takrat bankam postavila pogoj, da odprejo račun pri njih, v kolikor jim ponudi elektronsko bačništvo.

Elektronsko bančništvo lahko obravnavamo s širšega in z ožjega vidika. **V širšem smislu** je **elektronsko bančništvo** vse, kar je povezano z elektronskim poslovanjem. Sem uvrščamo bančne avtomate, telefonsko bančništvo, avtomatske odzivnike, poslovanje bančnih terminalov in mobilnih telefonov.

Ožja razlaga elektronskega bančništva se nanaša le na storitve virtualnega bančništva oz. bančništva, ki ga uporabljamo po internetu s pomočjo spletnih strani. Elektronsko bančništvo lahko torej opredelimo kot kakršenkoli način poslovanja strank z banko, ki je neodvisno od poslovalnic in temelji na informacijski tehnologiji (Sjekloča, 1999, str. 31).

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

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

2.1.1 Razvoj elektronskega bančništva

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

- uporabniki želijo opravljati storitve kjerkoli, kadarkoli in na kakršenkoli način;
- vrsto tehnologije, ki jo imajo na razpolago uporabniki (strankam naj ne bi vsiljevali tehnologije, ampak naj bi upoštevali tisto, ki jo imajo doma oz. v podjetju);

- vrsto telekomunikacijske infrastrukture v Sloveniji;
- način povezave banke s strankami;
- dolgoročne in kratkoročne učinke elektronskega bančništva;
- uporabniki morajo imeti zaupanje v storitev;
- banka mora poskrbeti za najvišjo stopnjo varnosti in
- ciljno skupino uporabnikov.

Stranke pričakujejo od banke kakovost na najvišjem nivoju. Če bo banka poskrbela za varno poslovanje, bo obdržala stalne stranke in pridobila tudi nove. Pred nepooblaščenimi vstopi v sistem se lahko brani z ustrezno programsko in strojno opremo (Vrešak, 1997, str. 61).

2.1.2 Delovanje elektronskega bančništva

Standardni način

O standardnem načinu lahko govorimo, kot o bančnih storitvah z določenimi omejitvami oz. pomanjkljivostmi. Uporaba bankomatov in plačilnih kartic je pogojena s časom in krajem ter občasno tudi z operaterji, med katerimi niso vsi vredni zaupanja.

Komitent opravi elektronsko bančno storitev tako, da se s posebnim vmesnikom priključi na komunikacijsko omrežje, po katerem 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 (Slika 2)(Kovačič, 1997, str. 132).

Slika 2: Princip delovanja elektronskega bančništva – standardni način

Vir: M. Kovačič, Storitve elektronskega bančništva, 1997, str. 133.

Elektronsko bančništvo po internetu

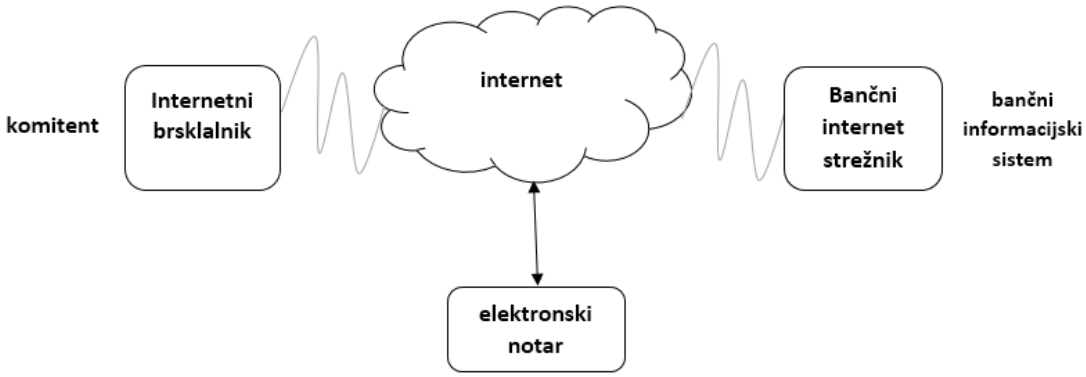
Ta tip bančništva je sodoben, ker odpravlja pomankljivosti standardnega načina. Storitve, ki jih ponuja elektronsko bančništvo delimo na **informacijske in transakcijske**. Vse informacije o spremembah na kapitalskih trgih, odlivih in prilivih na transakcijskem račun, lahko štejemo med informacijske storitve.

Med **transakcijske storitve**, ki jih opravljamo s sistemi elektronskega bančništva, štejemo vse storitve, ki vključujejo plačilne instrumente. Delovanje elektronskega bančništva po internetu (Slika 3) ima nekaj pomembnih prednosti (Kovačič, 1997, str. 132):

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

Domače bančništvo, internetno bančništvo ter internetno trženje so pomembnejše bančne dejavnosti, ki so postale del bančnega poslovnega načrtovanja.

Slika 3: Način delovanja sistemov elektronskega bančništva po internetu



Vir: M. Kovačič, Storitve elektronskega bančništva, 1997, str. 133.

Doma ali v službi si lahko ustvarimo virtualno poslovalnico, kjer se lahko uporabnik spletne aplikacije poistoveti z namišljenim bančnim uslužbencem. Poslovalnica ima neomejeno brezplačnega parkirnega prostora in je odprta 24 ur na dan. Sledi zadovoljstvo uporabnikov in ponudnikov elektronskega bančništva zaradi (Sjekloča, 1999, str. 31–33):

- znižanja bančnih stroškov;
- izginjanja potreb po klasičnih poslovalnicah;
- prihranka strankinega časa;
- omogočanja hitrih in natančnih informacij o bančnih storitvah in stanju na računu;
- zanesljivih informacij (enostavno za preverit, zaradi multimedijske komunikacije);
- kroženja denarja (zaradni rednih prilivov na račun, prihaja tudi do rednih odlivov in obratno);

- spreminjanje profila zaposlenih na banki (ne skrbijo zgolj za administracijo ampak so jim na voljo tudi bolj dinamična opravila) in
- odpiranje novih trgov (trg ni več omejen, fizične meje izginjajo, zato sta lahko banka in stranka v različnih krajih).

Z reformo plačilnih sistemov so slovenske poslovne banke začele opravljati storitve plačilnega prometa po internetu, tako za fizične kot za pravne osebe, s čimer so poleg novih poslovnih priložnosti naletele tudi na organizacijske in tehnične probleme. Banke so se pri ponudbi svojih storitev namreč soočile z množico novih komitentov, katerim dotedanje tržne poti, po katerih so banke v začetkih 90. let omogočale dostop do svojih storitev (bančno okence, bančni avtomat, telefaksno sporočanje in telefonski klicni center – teledom), zaradi obsežnosti njihovega poslovanja niso več zadoščale (Sistem elektronskega bančništva, 2004).

V povprečju fizične osebe opravijo vsaj desetkrat manj transakcij kot podjetja, vrednost le – teh je lahko tudi do stokrat nižja. Podjetja za transparentno poslovanje potrebujejo ažurno stanje na transakcijskem računu, da lahko v danem trenutku prenakažejo sredstva na transakcijski račun drugih pravnih ali fizičnih oseb, ali zgolj prenešajo sredstva med svojimi računi. Podjetja presežek sredstev na transakcijskih računih največrat prenesejo na varčevalne račune ali sklenejo z bankami pogodbe o vezavi depozita. V kolikor podjetje na določen dan potrebuje prosta denarna sredstva, na banko napiše e-mail ali odda sporočilo v elektronski banki, o višini črpanega zneska in številki transakcijsega računa, kamor naj se sredstva prenakažejo. Zaradi nizkega obrestovanja sredstev na transakcijskih računih, je nespametno hraniti na računu večje vsote denarja.

2.2 Prednosti za banko in komitenta

Vse se seli na internet, tako tudi bančno poslovanje ne zaostaja. Banke vidijo v tem nove priložnosti za preoblikovanje svojih storitev, ki bodo predvsem prijazne uporabnikom. Novosti imajo poleg prednosti, za udeležence, v poslovanju tudi različne slabosti. Le-te bodo predstavljene v naslednji točki.

Prednosti za komitente:

- dostop 24 ur na dan (brez čakanja na bančnih okencih),
- dostop od kjerkoli (pogoj je internetni dostop),
- nižje cene storitev,
- višja stopnja zasebnosti,
- enostavna uporaba in boljša preglednost ter
- naročanje bančnih storitev.

Končni uporabnik od sodobnih bančnih storitev pričakujejo, da se bodo stroški njihovega poslovanja hitro znižali. Žal temu ni tako saj bodo koristi, vidne šele čez čas in jih bo moč čutiti v nemerljivih dejavnikih, kot je npr. zadovoljstvo uporabnikov.

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

Prednosti za banke:

- nižji stroški bančnih transakcij; manjša poraba pisarniškega materiala;
- V primerjavi s klasičnim načinom poslovanja je strošek elektronske bančne transakcije do petnajstkrat manjši od cene klasične obdelave (Vozel, 1999, str. 47–75);
- avtomatizirano zajemanje podatkov, ki omogoča enostavnejšo in kakovostnejšo obdelavo podatkov;
- nižji stroški dela (zmanjšanje delovnih mest);
- zmanjšanje števila poslovalnic;
- ažurnost;
- pospešuje kroženje denarja in omogoča bolj redno plačevanje obveznosti (Sjekloča, 1999, str. 32)
- novi komitenti in
- krajše vrste pred bančnimi okenci.

2.3 Slabosti za banko in komitenta

Kot je bilo že v prejšnjem poglavju omenjeno, novosti s seboj prinašajo tako prednosti kot slabosti.

Slabosti za komitente:

- nezaupanje v nove bančne storitve, predvsem pri starejši generaciji, ki ni vajena elekronskih medijev;
- dvom o varnosti e-bančništva in
- manj osebnega stika z bančnimi referenti.

Slabosti za banko:

- visoki stroški, ki so povezani z lansiranjem novega načina poslovanja;
- visoka začetna naložba ter
- dodatni stroški za izobraževanje kadra.

Za vpeljavo e-bančništva je potrebno zaposliti ali najeti strokovni kader, ki tudi izobražuje notranje zaposlene. Za izpeljavo tega projekta je potreben časa in predvsem denar. Stroške lansiranja e-bančništva bi lahko delili na 3 dele. 50 % stroškov predstavlja integracija e-bančništva, 30 % strojna oprema in 20 % strošek programske opreme.

Na podlagi predstavljenih prednosti in slabosti lahko povzamem, da so slabosti v manjšini. Dvom v varnost je tista največja slabost, ki jo najdemo tako na strani banke kot na strani komitentov. Nove in nove varnostne komponente so tiste, ki skrbijo za najboljšo možno varnost elektronskih aplikacij.

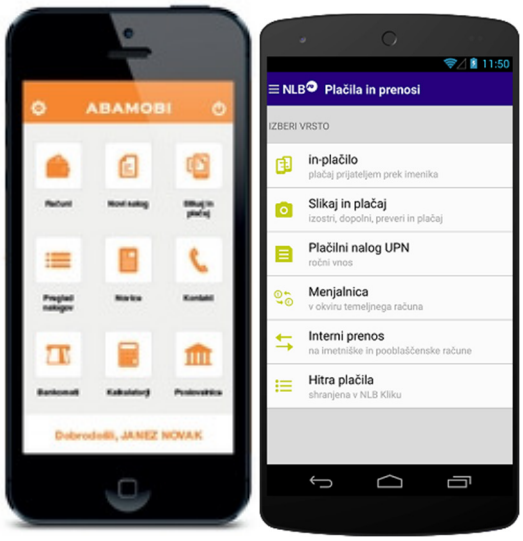
2.4 Mobilno bančništvo

Elektronsko bančništvo se seli tudi na mobilne telefone. Pred časom so se kupovali vse manjši mobilni aparati, danes pa gre vse skupaj ravno v nasprotno smer. Večji je ekran boljša je preglednost pri brskanje po spletu in branju različnih prilog. Z uporaba mobilnih telefonov so prekoračene še prostorske meje, saj mobilni aparat praktično nosimo s seboj na vsakem koraku. Za uporabo mobilne aplikacije je potreben dostop do wi-fi omrežja ali vključenost prenosa podatkov preko mobilnega operaterja. Cene prenosa podatkov so se danes že močno znižale, v velikih primerih mobilni operaterji že ponujajo cenovno ugodne pakete, z že zakupljeno količino prenosa podatkov.

O samem mobilnem bančništvu lahko govorimo takrat, ko za izvedbo transakcij ali drugih bančnih storitev uporabljamo mobilne telefone. V Sloveniji se uporaba mobilnega bančništva razlikuje (Slika 4) od banke do banke, ki ponujajo različne storitve. Te pa so:

- pregled stanja na računu (osebnem in varčevalnem),
- plačevanje računov (Klasičen vnos podatkov v obrazec za plačevanja ali prepoznava določenih podatke z računa s pomočjo skenerja. Le-ti se prenesjo v telefon, aplikacija zahteva od uporabnika le še dodatno potrditev za končno izvedbo plačila.),
- informacije o poslovalnicah in bankomatih (tudi navigacija, ki vas pripelje do izbrane poslovalnice ali bankomata),
- informacije o tečajnih listah,
- menjalnice,
- itd.

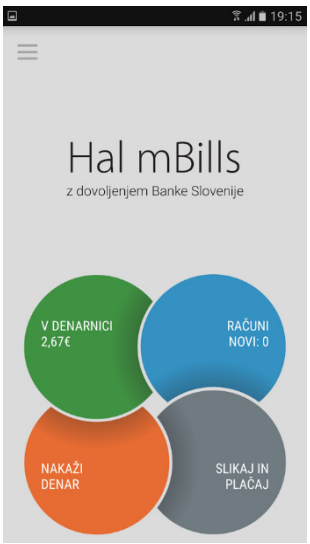
Slika 4: Primera mobilne banke



Vir: Abanka d.d., Mobilna banka Abamobi, 2016; NLB d.d., Mobilna banka Klikin, 2016.

Na tržišču se je pojavila tudi storitev Hal mBills, ki jo trži novoustanovljeno podjetje Halcom Plačila d.o.o. Za novo aplikacijo so s strani Banke Slovenije v letu 2015 prejeli licenco. Slednja nadzira Halcomov transakcijski račun, kjer se zbirajo zneski v mobilno denarnico.

Slika 5: Aplikacija Hal mBills



Vir: Halcom plačila d.o.o., Aplikacija Hal mBills, 2016.

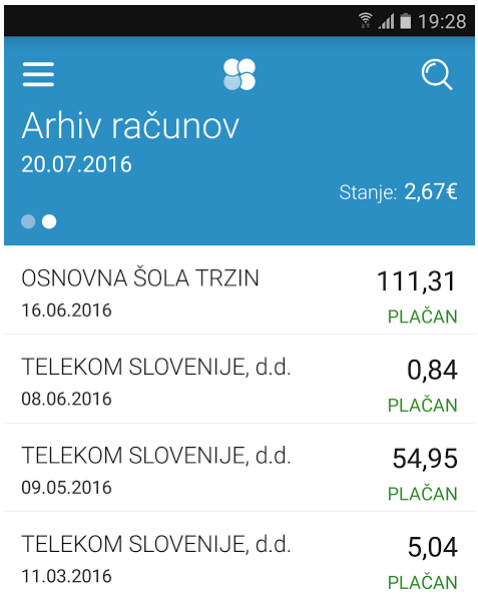
Za uporabo aplikacije je potrebno oddati nekaj osebnih podatkov, med njimi tudi transakcijski račun in davčno številko, ter podpisati pogodbo, ki jo dostavijo kamorkoli v Slovenijo. Ob podpisu pogodbe je potrebno podpisati tudi pooblastilo SEPA, ki dovoljuje prenos denarja s transakcijskega računa v uporabnikovo mobilno denarnico. Namestitev

aplikacije je brezplačna od junija 2016, plačevati pa je potrebno nadomestilo za uporabo storitve Hal mBills v višini 0,25 EUR mesečno, vendar samo v primeru, da je uporabnik opravil vsaj eno plačilo. Z vpisom osebnega gesla v samo alikacijo, se pojavi vstopno okno, (Slika 5) kjer lahko izberete eno izmed storitev.

Rešitev je zasnovana po zadnjih varnostnih standardih, kot je uporaba mobilnih generatorjev enkratnih potrditvenih kod in digitalnih potrdil za preverjanje identitete uporabnika (Monitorpro, 2016). Za vstop v aplikacijo je potrebno vnesti kodo PIN, ki je sestavljena iz šestih znakov. Storitev omogoča prejem računa direktno v mobilno aplikacijo, v kateri lahko z nekaj dotiki zaslona račun tudi plačate. V kolikor računa ne plačate takoj, vas aplikacija opozori, da se bliža valuta plačila. Račun lahko s pomočjo kamere brez nepotrebnega pretipkavanja številk tudi skenirate in ga nato plačate. V sodelovanju z Upravo Republike Slovenije za javna plačila so Hall mBills vključili v vrtce in šole. Tudi večja slovenska podjetja že sodelujejo pri lansiranju aplikacije na slovenski trg.

Aplikacija je zasnovana po načelu, da nadomesti gotovino, saj v Halcom Plačila menijo, da gotovino lahko pozabimo doma, telefona pa zagotovo ne. Aplikacja je namenjena tudi prenakazilom med sodelavci, ki hodijo skupaj na malico, s seboj pa vsi ne nosijo gotovine. Na Sliki 6 je v levem kotu vidno stanje denarja v mobilni denarnici in stanje računov z različnimi statusi.

Slika 6: Arhiv računov Hal mBills



Vir: Halcom plačila d.o.o., Aplikacija Hal mBills, 2016.

3 SEPA, UPN IN E-RAČUNI

3.1 Poslovanje v evropskem prostoru – SEPA

SEPA (kratica za Single Euro Payments Area) je okolje, ki je prijazno potrošnikom in poslovnim subjektom. Omogoča, da se plačila pri ponudnikih plačilnih storitev v evrih vršijo pod enakimi pogoji, ne glede nato ali se nahajate znotraj ali izven države v območju SEPA. Območje se razprostira preko 34 držav. Obsega države evro območja, v nekaterih evro še ni nacionalno plačilno sredstvo, države evropskega gospodarskega prostora in druga ozemlja zunanjih območij in kolonij.

Slika 7: Območje SEPA

Vir: European Peyment council, SEPA Scheme Countries and Territories, 2016.

Na zemljevidu (Slika 7) je označeno območje SEPA, ki zajema 34 držav:

- 28 držav Evropske unije,
- Islandijo,
- Lihtenštajn,
- Monako,
- Norveško,
- San Marino in
- Švico.

V SEPA območju je tudi 9 držav, kjer evro še ni nacionalno plačilno sredstvo, in sicer:

- Bolgarija,
- Češka,
- Danska,
- Hrvaška,
- Madžarska,
- Poljska,
- Romunija,
- Švedska in
- Združeno kraljestvo.

Pri projektu SEPA sodeluje več kot 4000 bank, ki prihajajo iz različnih nacionalnih okolij, z različno stopnjo razvitosti, različnimi tveganji in nenazadnje tudi z različno poslovno prakso. Nove plačilne sheme so rezultati pogajanj in kompromisov.

Projekt SEPA je projekt z močno politično podporo Evropske komisije in Evropske centralne banke. Njegov cilj je uskladiti domača in čezmejna plačila na takšen način, da, ne glede na to preko katerega plačilnega kanala se bodo vršila, bodo osnove in standardi za vsa plačila enaki. Ne bo več pomembno, kje ima uporabnik odprt račun, kam v območje SEPA plačuje in katera je njegova banka.

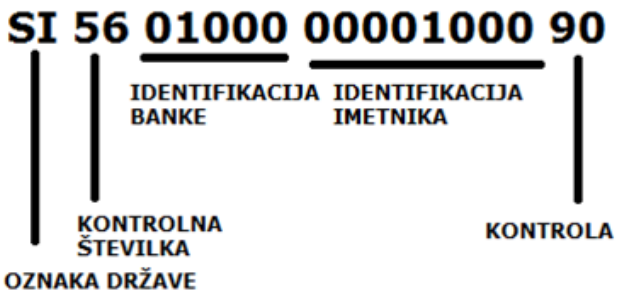
Znotraj območja SEPA so bile postavljene tudi nove sheme plačilnih storitev, in sicer:

- **kreditna plačila**, ki zajemajo nakazila in prilive, in pri katerih gre za prenos sredstev z eno samo transakcijo na račun zunaj ali znotraj države v enem dnevu, in
- **direktna obremenitev SEPA**, ki omogoča podjetju ali posamezniku, ki se nahaja znotraj ene države, da lahko neposredno obremeni račun v drugi državi.

Za izvajanje plačil med državami je bil v Evropi sprejet mednarodni standard za identifikacijo plačilnih računov, ki se imenuje IBAN (International Bank Account Number). IBAN je mednarodna številka bančnega računa, ki je v Sloveniji sestavljena iz 19 znakov

(Slika 8). Prvi štirje znaki izhajajo iz standardov ISO, in sicer oznaka SI in število 56, nadaljnjih 15 znakov pa predstavlja osnovno številko bančnega računa oz. BBAN. Za plačilo v območje SEPA je poleg IBAN potrebna še bančna identifikacijska koda BIC (Bank Identifier Code) SWIFT, ki jo imajo vse banke, vključene v medbančno komunikacijsko omrežje. Za države, kjer evro še ni nacionalno valuta, se predvideva uvedba kreditnih plačil in direktnih obremenitev do konca oktobra 2016.

Slika 8: Sestava IBAN številke



Povzeto in prirejeno po Banki Slovenije, Enotna struktura transakcijskega računa, 2016.

Poleg že omenjenih dveh storitev, kreditnih plačil in direktnih obremenitev, imajo SEPA plačilne kartice visoko stopnjo zaščite in raven varnosti. Trgovci lahko brez tveganja sprejemajo kartice, ki so bile izdane kjerkoli v Evropi.

Končni cilj SEPA je zagotoviti, da bodo lahko potrošniki, podjetja in javni sektor uporabljali plačilne storitve, ki bodo zadovoljevale njihove potrebe, in jih bo mogoče znotraj Evropske skupnosti uporabljati na enoten način, s čimer znotraj geografskega območja SEPA ne bo več razlikovanja med plačili v evrih znotraj posamezne države ali čez njene meje. Imetniki plačilnih računov bodo lahko izvajali negotovinska plačila, znotraj evroobmočja z enega samega plačilnega računa, in z uporabo enega niza plačilnih instrumentov tako enostavno, učinkovito in varno kot znotraj državnih meja. Uporabniki plačilnih storitev bodo imeli možnost izbire ponudnika plačilnih storitev z najprivlačnejšo ponudbo ne glede na državo ponudnika. Na podlagi Uredba (ES) št. 1781/2006 Evropskega parlamenta in Sveta z dne 15. 11. 2006, so vsi ponudniki plačilnih storitev dolžni spremljati podatke o plačnikih za vse pologe in dvige denarnih sredstev nad 1.000 EUR. Podatke o plačnikih tako lahko uporabijo in povežejo s financiranjem terorizma in pranjem denarja.

3.2 Univerzalni plačilni nalog – UPN

Ime UPN so sprejeli v Združenju bank Slovenije, obrazec je v uporabi v Sloveniji od 1. 11. 2010. Gre za obrazec, ki je bil pripravljen s strani slovenskih bank pripravile v želji po poenotenju plačevanja, ki je posledica vzpostavitve enotnega območja plačil v evrih – SEPA. S 1. 1 .2012 je v celoti zamenjal naslednje obrazce:

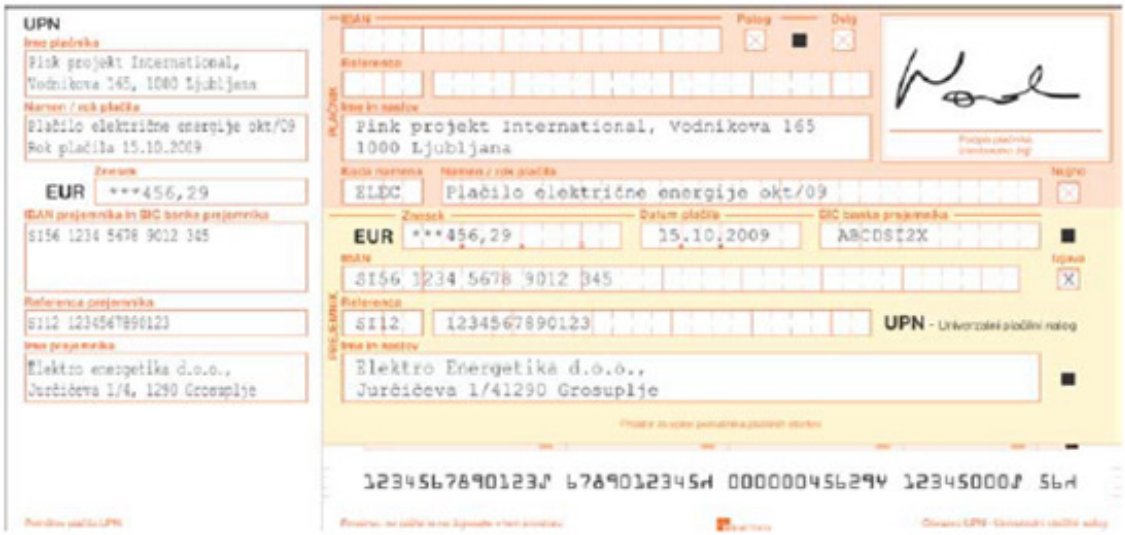
- posebno položnico PP02,
- bančni nalog BN02 in
- regulirano plačilo RP01.

UPN obrazec se uporablja za dvige in pologe gotovine ter gotovinska in negotovinska plačila. Na internetni strani SEPA so predstavljene prednosti uporabe UPN za izdajatelje:

- poenoten obrazec namesto prejšnjih obrazcev (BN02 in PP02),
- en standard za izdajo UPN ,
- enotno procesiranje plačilnih transakcij (prej ločeno za BN02 in PP02),
- vplačana in izvršena plačila so še isti dan odobrena na računu prejemnika (prej so bila vplačila s PP02 na računu odobrena naslednji delovni dan),
- opustitev vzdrževanja dveh ali več zalednih sistemov pri izdajateljih in
- za izdajatelje UPN z OCR vrstico ni več vključevanja v Zbirni center pri Bankart d.o.o.

Na Sliki 9 je primer izpolnjenega UPN obrazca. V obrazcu je vidno, da dve polji (plačnikov IBAN in sklic) nista izpolnjeni, saj nista obvezni za izvedbo samega plačila.

Slika 9: Izgled izpolnjenega papirnega obrazca UPN



VIR: Uprava Republike Slovenije za javna plačila, Univerzalni plačilni nalog, 2016.

Glede na prejšnje obrazce je v UPN nekaj sprememb pri samem izpolnjevanju. Na starih obrazcih se je zapisoval transakcijski račun, na obrazcu UPN pa je potreben vnos mednarodne številke IBAN. Potrebna je tudi koda namena, ki je povzročala nemalo težav pri uslužbencih na banki saj gre za kratice angleških izrazov (Tabela 3).

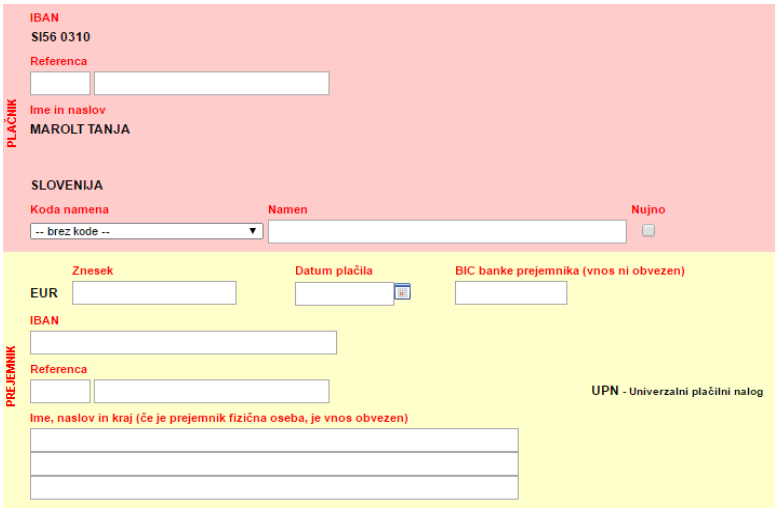
Tabela 3:Primeri kod namena pri nalogu UPN

KODA	POMEN	PREVOD
ADVA	Advance Payment	Plačilo avansa oz. predplačilo
COST	Costs	Plačilo stroškov
ELEC	Electricity Bill	Račun za elektriko
INTE	Payment of Interest	Plačilo obresti
LOAR	Repayment of Loan	Odplačilo kredita
OTHR	Other Payment Purpose	Drugi nameni plačila
OTLC	Other Telecom Related Bill	Drugi računi – telekomunikacije
TAXS	Payment of Taxes	Plačilo davka

Vir: NLB d.d, Kode namena plačila, 2016.

Banke so v programih elektronskega bančništva pripravile obrazec UPN, ki v sistemu SKB NET izgleda takole (Slika 10):

Slika 10: UPN nalog v SKB NET



Vir: SKB d.d., UPN nalog, 2016.

3.3 E-računi

V letu 2007 se je v sodelovanju med nekaterimi bankami in Združenjem bank Slovenije (ZBS) utrnila ideja o vzpostaviti sistema za elektronsko izmenjavo računov. Na ta način so lahko preko že preverjenih virov uporabniki elektronske banke izmenjavali račune v elektronski obliki. Prve izmenjave računov v elektronski obliki so se izvedle v letu 2008, ko sta bili v projekt vključeni samo dve banki, kasneje se je krog razširil na sedem bank. 1. 6. 2011 se je preko Bankarta vzpostavil sistem za izmenjavo računov v elektronski obliki.

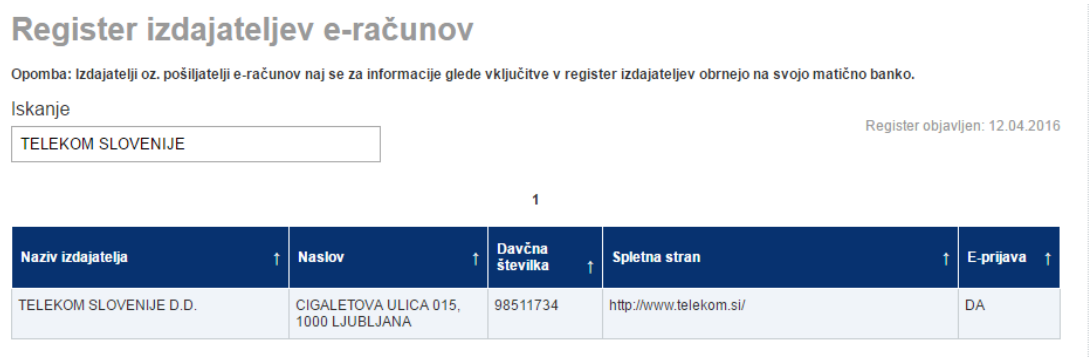
(Bankart, 2016).

E-račun je enakovreden papirnemu računu, s to razliko da mora izpolnjevati določene tehnične pogoje in se nahaja v predpisani elektronski obliki. Izdajatelj je dolžan tudi e-račun dostaviti prejemniku, le da je ta pot dostave enostavnejša in predvsem hitrejša. (Uprava Republike Slovenije za javna plačila (UJP), 2011).

Pravilnik o standardih in pogojih izmenjave elektronskih računov pravi, da mora **e-račun** po obliki in vsebin ustrezati vsem zahtevam in pogojem določenim v zakonu in podzakonskem predpisu, ki ureja sistem plačevanja davka na dodano vrednost ter zahtevam posebnih predpisov in standardov, ki urejajo računovodsko poslovanje, elektronsko poslovanje in elektronski podpis, varstvo dokumentarnega in arhivskega gradiva, varstvo podatkov in poslovna razmerja med dolžnikom/plačnikom ter upnikom in ponudnikom plačilnih storitev (Pravilnik o spremembah in dopolnitvah, Uradni list RS, 75/2015).

Družba Bankart d.o.o. je v Sloveniji posrednik med izdajatelji in prejemniki e-računov. Na njihovi spletni strani najdete register izdajateljev e-računov. Na ta način lahko preverite ali je podjetje, ki za vas opravlja določene storitve, že na seznamu izdajateljev. Na Sliki 11 je izpis iz registra izdajateljev, ki poda informacijo o statusu, ki ga ima družba Telekom Slovenije. Status DA pomeni, da se lahko preko svoje elektronske banke naročite na prejemanje njihovih e-računov.

Slika 11: Register izdajateljev e-računov



Register izdajateljev e-računov

Opomba: Izdajatelji oz. pošiljatelji e-računov naj se za informacije glede vključitve v register izdajateljev obrnejo na svojo matično banko.

Iskanje

TELEKOM SLOVENIJE

Register objavljen: 12.04.2016

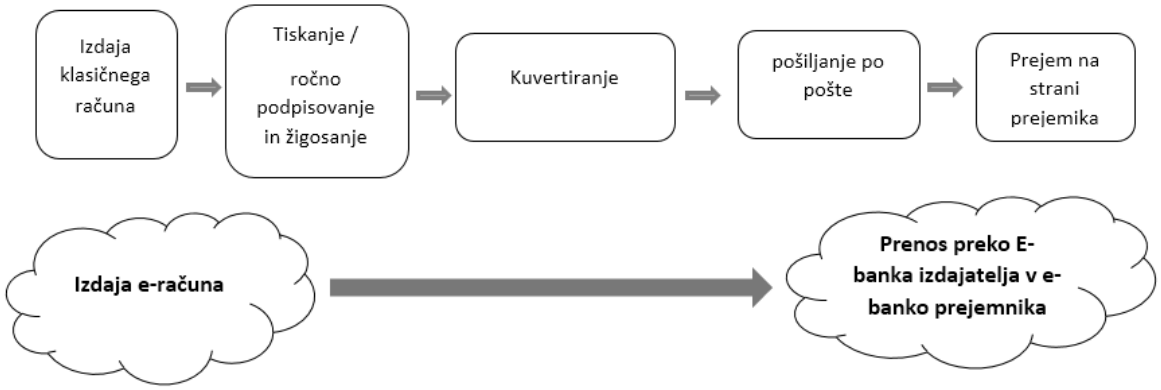
1

Naziv izdajatelja	Naslov	Davčna številka	Spletna stran	E-prijava
TELEKOM SLOVENIJE D.D.	CIGALETOVA ULICA 015, 1000 LJUBLJANA	98511734	http://www.telekom.si/	DA

Vir: Bankart d.o.o., Register izdajateljev računov, 2016.

1. 1. 2015 je Vlada Republike Slovenije uveljavila obvezno prejemanje in izdajanje e-računov za proračunske uporabnike. Zato je potrebno tudi, da vsa podjetja, ki poslujejo s proračunskimi uporabniki, ured ijo kanale, po katerih bodo računi bodisi prihajali bodisi odhajali do njih. Na Sliki 12 sta prikazani poti od izdaje do prejema klasičnega računa in e-računa.

Slika 12: Pot klasičnega in e-računa



Povzeto in prirejeno po DataStudio d.o.o., Pot klasičnega in e-računa, 2016.

Uporaba e-računov vam prihrani čas, saj poenostavi plačevanje računov in zniža stroške. Hkrati je tak način poslovanja naravi prijazen, saj z e-računi zmanjšamo porabo papirja in uporabo tiskalnikov. Izdaja e-računa je enaka pri klasičnem računu in pri e-računu, vsi nadaljnji postopki do prejema pa so pri klasičnem računu časovno veliko bolj zamudni. Če upoštevamo, da je potrebno pošiljko še dostaviti na pošto in njen prenos po Sloveniji, je e-račun res učinkovitejša storitev. V Tabeli 4 podajam primerjavo klasičnega pošiljanja računov in uporabe e-računa.

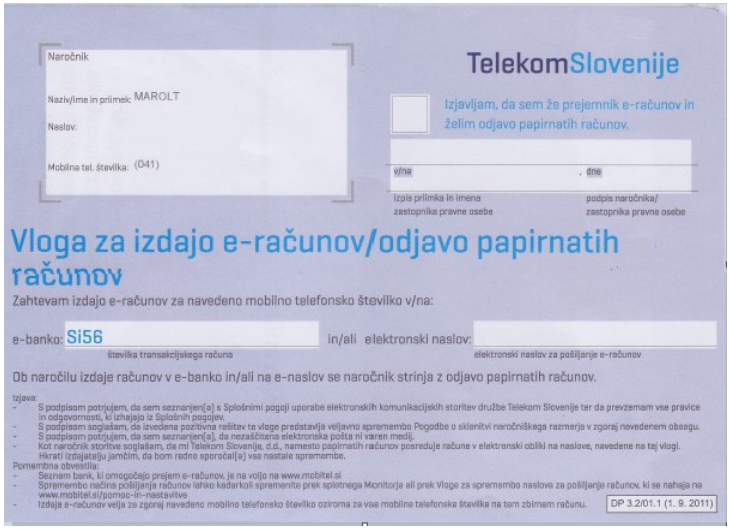
Tabela 4: Primerjava klasičnega in e-računa

klasična pošta	→	elektronska izmenjava
papirni račun	→	elektronski račun (standard)
klasična ovojnica	→	elektronska ovojnica
lastnoročni podpis	→	elektronski podpis (digitalno potrdilo)
naslov prejemnika	→	elektronska ovojnica
zaupnost pošiljke	→	šifriranje sporočila
arhivska omara	→	dolgoročna elektronska hramba
poštni nabiralnik	→	elektronski nabiralnik
poštar	→	ponudnik e–izmenjav oz. elektronskih poti

Vir: Datalab, d.d, Primerjava klasičnega in e-računa, 2016.

Večja slovenska podjetja so že v letu 2011 spodbujala podjetja in posameznike k prijavi na e-račune. Ob sami prijavi na e-račun se lastnik strinja tudi z odjavo papirnih računov. Na Sliki 16 je prikazan papirni obrazec družbe Telekom Slovenije iz leta 2011.

Slika 13: Vloga za izdajo e- računov iz leta 2011



Vir: Telekom Slovenije d.d., Vloga za izdajo e-računov, 2011.

Na spletni strani Telekoma Slovenije d.d se tudi v letu 2016 nahaja povabilo k uporabi e-računov, bodisi vam e-račun pošljejo v spletno banko ali v elektronski predal (e-naslov). Na e-račune se naročite v vaši spletni banki na zavihku e-prijave/e-odjave, kjer vpišete davčno številko podjetja, katerega e-račune želite prejemati. V kolikor se podjetje še ni odločilo za izdajanje e-računov ga na seznamu izdajateljev ni mogoče najti. V nasprotnem primeru se vam odpre seznam izdajateljev in vsi računi, s katerimi podjetje operira (Slika 14). V kolikor se prijavite na prejemanje e-računov bodo v prihodnjem mesecu ukinjeni papirni računi in v vašem zavihku v elektronski banki boste našli e-račun.

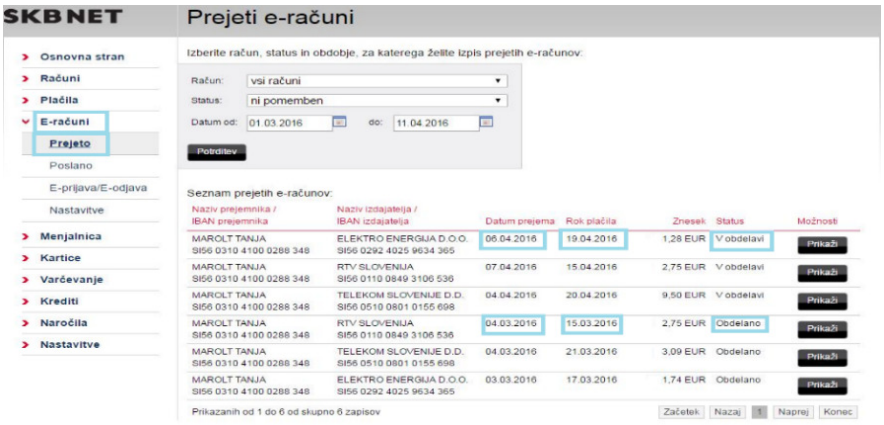
Slika 14: Prijava/odjava na e-račun

Vir: SKB d.d., SKB NET, 2016.

Storitev vam omogoča enostaven pregled vseh prejetih e-računov. Na Sliki 15 so računi za dvomesečno obdobje. Za mesec marec je status obdelan, kar pomeni, da so nalogi že bremenili vaš račun, aprilski računi pa imajo status v obdelavi, kar pomeni, da so nalogi v

čakalni vrsti. Na seznamu prejetih računov so podani tudi datumi prejemov, ki kažejo, kdaj je e-račun prispel v vaš nabiralnik in roki plačil, ki kažejo, kdaj je bil oz. bo nalog izvršen.

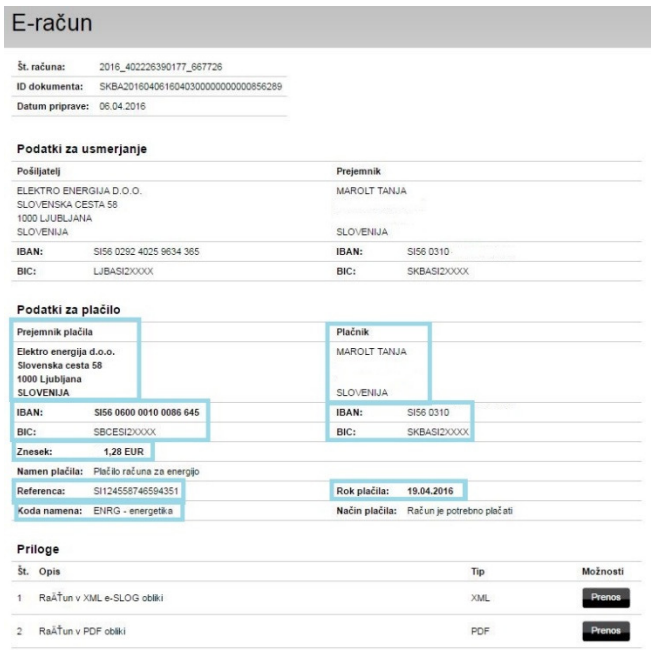
Slika 15: Prejeti e-računi



Vir: SKB d.d., SKB NET, 2016.

V programu SKB NET se ob izbiri možnosti e-račun odpre oblika e-računa prikazanega na Sliki 16. Zapisani podatki za usmerjanje, so podatki o pošiljatelju in prejemniku e-računa ter podatki za plačilo, ki vključujejo podatke o plačniku in o prejemniku. Gre za naziv fizične ali pravne osebe, naslov, IBAN in BIC kodo. Pomembna podatka za izvedbo plačila sta tudi koda namena in sklic. Na Sliki 16 so označeni glavni elementi, ki so nujni za plačilo preko UPN naloga.

Slika 16: Izgled e-računa



Vir: SKB d.d., SKB NET, 2016.

Ovojnica s seboj nosi dve datoteki. Prva je v formatu XML, ki omogoča nadaljnjo obdelavo – plačilo računov brez dodatnega pretipkavanja in/ali uvoz računov v programe za knjiženje. Druga datoteka je v formatu PDF, ki ga poznamo kot kopijo originalnega računa. E-račune je možno posredovati tudi preko e-pošte. Te različice se bodo po vsej verjetnosti posluževala predvsem podjetja, ki so med seboj povezana preko lastnika oz. poslovanja z istim računovodskim servisom. Prejemnik lahko e-račun poleg preko e-banke in e-pošte prejme tudi v lastno aplikacijo ali ERP. 1. 6. 2011 je bilo v sistem e-račun vključenih 16 slovenskih bank, kjer je vzpostavljena medbančna izmenjava preko Bankarta.

4 VARNOST ELEKTRONSKEGA POSLOVANJA

Z razvojem interneta se je ustvaril nov družbeni prostor, ki daje navdih kriminalcem, saj ga je nemogoče nadzorovati. Internetno omrežje samo ne omogoča varne komunikacije med uporabniki, zato je potrebno združiti ustrezno tehnologijo in preverjeno znanje, da bi lahko zagotovili varnost računalniških sistemov in drugih virov.

Potencialne žrtve računalniške kriminalitete smo vsi, ki dnevno uporabljamo stroritve interneta (Power, 1998). Vsakodnevno se povečuje verjetnost, da boste prav vi naslednja žrtev kriminalcev, saj kroži po medmrežju ogromno število virusov, ki jih lahko prejmete tudi z interno pošto. V razvitih državah ramišljajo, kako zakonsko zmanjšati tako obsežne in raznolike napade računalniškega kriminala.

4.1 Opredelitev varnostnih komponent

Da bi zagotovili čim večji nivo varnosti je potrebno združiti različne kombinacije programske in strojne opreme ter fizičnega varovanja. Za močne varnostne ukrepe je potrebno investirati ogromno denarja in vodstvo je tisto, ki je odgovorno za postavitev temeljne varnostne politike. Določiti je potrebno, kaj ščititi in zakaj. Cilji zaščite morajo biti določeni v več smeri, saj je vnaprej težko predvideti usmerjenost napada.

Kot navajata Belič & Lesjak (2006, str. 128) je varnostna politika organizacije skupek pravil in postopkov, ki opredeljujejo, kako v organizaciji upravljati, ščititi in ravnati z določenimi viri z namenom doseganja konktetno zastavljenih varnostnih cijev. Dobra varnostna politika je prilagodljiva in uporabna v praksi.

Varnostna politika je kompromis med stroški in tveganji. Varen sistem je tisti, kjer imajo napadalci pri samem vdoru manjše koristi od stroškov. Podatki o finančnih transakcijah posameznikov in podjetij so vsekakor med občutljivejšimi, zato je pomen varnosti še toliko pomembnejši. Vdor v bančni sistem lahko utrpi tako vidne (prenakazilo denarja, zloraba podatkov, koristoljubje, izguba poslov, izguba komitentov, itd.) kot nevidne posledice

(nezaupanje v banko, izguba ugleda itd.), ki pogosto vplivajo posredno na vidne stroške (Kuščar, 2002, str. 8).

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

- **overjanju** (identificiranje uporabnikov),
- **zaupnosti** (dostop do podatkov imajo le pooblaščene osebe),
- **neokrnjenosti** (ohranjanje pristnosti podatkov),
- **nadzoru dostopa** (vstop dovoljen le registriranim uporabnikom),
- **preprečevanju zanikanja o sodelovanju v aktivnostih e-poslovanja** ter
- **razpoložljivosti**.

Da bi zagotovili zgoraj naštete varnostne storitve, se uporabljajo naslednje metode:

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

Njihova izbira je odvisna od zahtevanih varnostnih storitev, stopnje zaščite in oblike sistema. Splošne kategorije virov so podatki, informacije pri prenosu in hranjenju, strojna in programska oprema, uporabniki in odnosi med njimi ter dokumentacija o postopkih strojne in programske opreme v sistemu ali omrežju (Jerman Blažič, 2001, str. 100).

Kriptografija

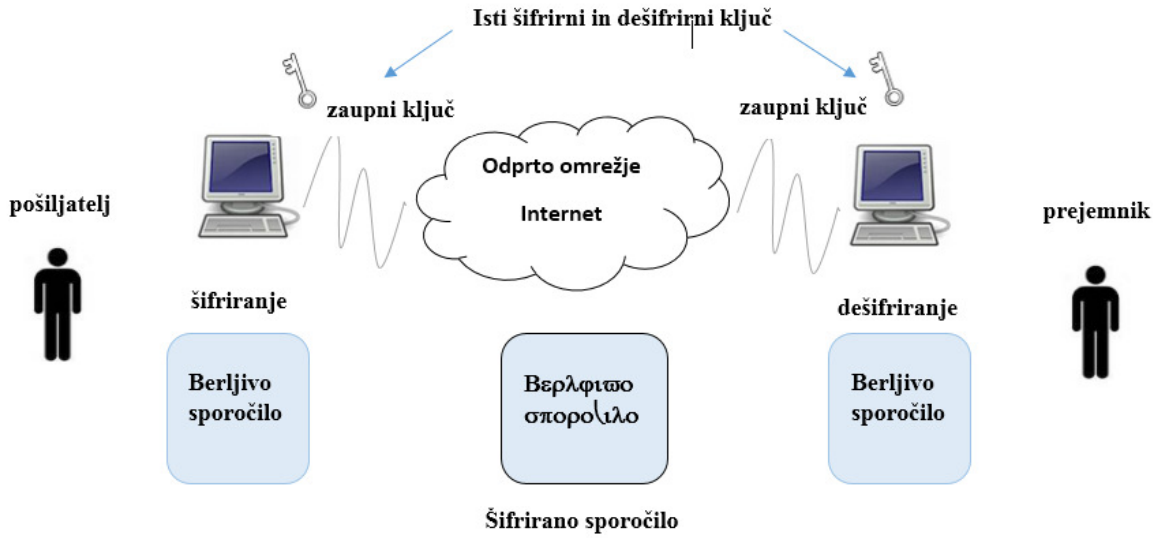
Kriptografija je veda, ki se ukvarja s šifriranjem. Besedilo bi lahko razbrali le tisti, ki bi poznali ustrezen ključ. Nasprotni proces kriptografije je dekripcija, ki razkriva šifrirano besedilo v berljivo obliko. Prvotno besedilo lahko imenujemo berljiv tekst oz. čistopis, ki ga s pomočjo kriptografije pretvorimo v neberljivi tekst oz. tajnopis.

V sodobnem poslovanju se v sklopu elektronskega poslovanja kriptografija ukvarja predvsem z odkrivanjem in preučevanjem računalniških algoritmov in protokolov, ki bi čim bolj učinkovito zaščitili pomembne informacije. Kriptografija poleg zaščite informacij skrbi tudi za to, da se ohranja avtentičnost dokumenta, torej ohranja izvirnost dokumenta na poti od pošiljatelja do prejemnika. Uporablja se na številnih področjih interneta – pri digitalnem podpisovanju, pri časovnem žigosanju in v sklopu plačevanja z digitalnim denarjem ter pri izmenjavi podatkov, ki jih želimo zaščititi.

Simetrična kriptografija

Simetrična kriptografija je bila do leta 1976 edina poznana metoda šifriranja podatkov. Njena naloga je bila šifriranje in dešifriranje informacij z enim samim ključem (Slika 17). Težava, ki se je pojavila pri simetrični kriptografiji, je bila, kako edinstveni ključ varno dostaviti do končnega prejemnika informacije, ali osebno ali s pomočjo zaupanja vrednega vira.

Slika 17: Simetrična kriptografija



Povzeto in prirejeno po Narandža – Štanta, Primerjalna analiza spletnega bančništva za fizične osebe, 2006.

Da bi se lahko izognili težavam, ki jih srečujemo pri simetrični kriptografiji, se je razvila asimetrična kriptografija.

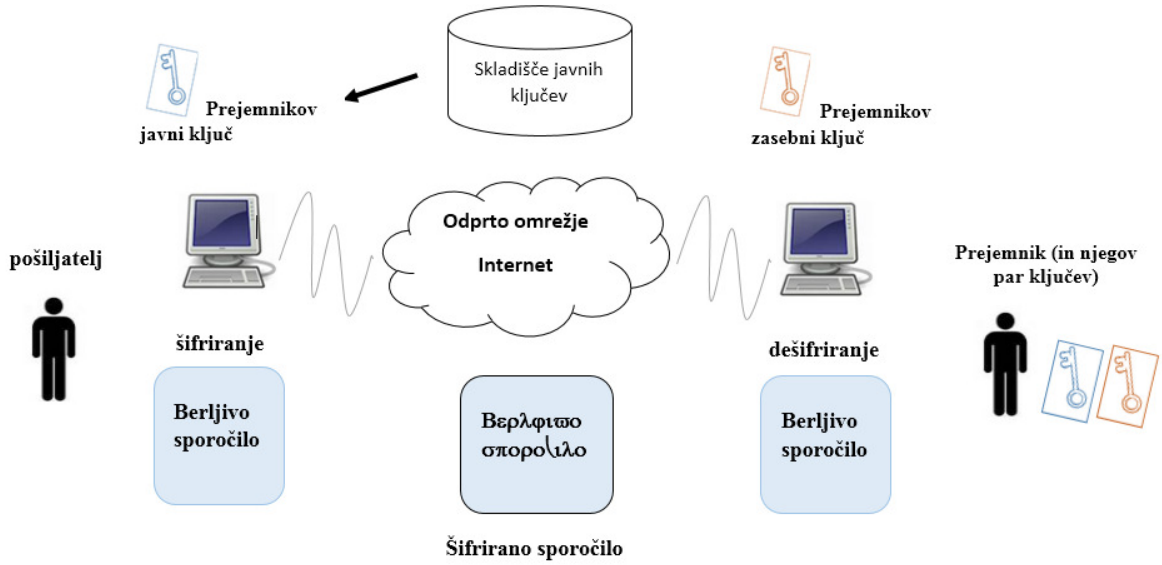
Asimetrična kriptografija ali kriptografija javnih ključev

Asimetrična kriptografija v nasprotju s simetrično kriptografijo uporablja dva ključa – javnega in zasebnega. Uporabnik s pomočjo računalnika ustvari dva ključa, zasebnega obdrži zase, javnega pa posreduje določenemu krogu preko e-pošte ali pa ga objavi na spletni strani. Sporočilo je moč dišifrirati le s pripadajočim komplementarnim ključem. Ustvarjanje parov ključev je enostaven in kratkotrajen postopek, a to ne pomeni, da je kratkotrajen oz. lahek postopek preko enega ključa najti drugega. Sama uporaba asimetrične kriptografije v infrastrukturi javnih ključev nam zagotavlja celovitost, zaupnost, nezatajljivost sporočila in preverjanje identitete pošiljatelja (Halcom d.d, 2016).

Asimetrična kriptografija (Slika 18) omogoča generiranje digitalnega podpisa, kjer pošiljatelj s svojim zasebnim ključem podpiše pripravljeno sporočilo. Prejemnik na drugi

strani z javnim ključem preveri, ali je bilo sporočilo res podpisano s strani pošiljatelja in če se vsebina med samim prenosom ni spremenila.

Slika 18: Asimetrična kriptografija



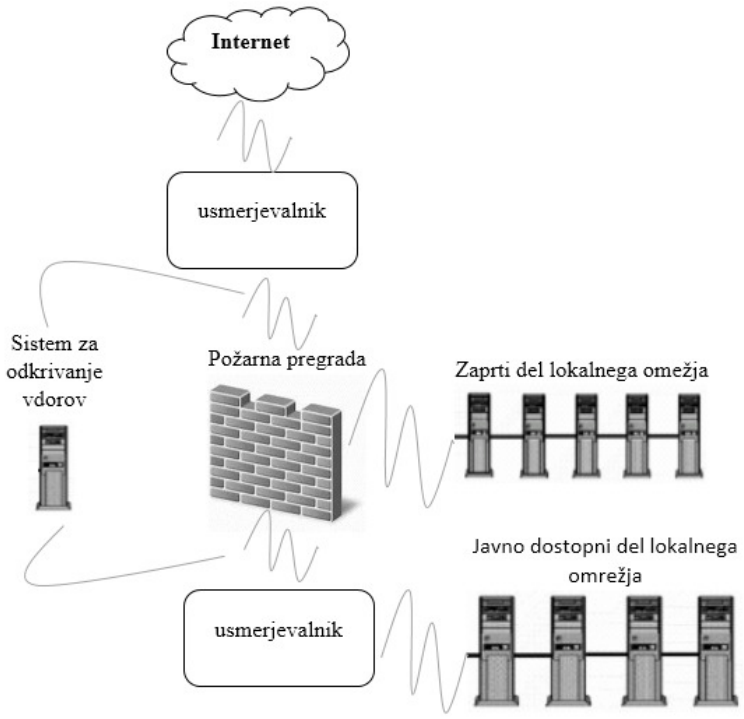
Povzeto in prirejeno po D. Narandža – Štanta, Primerjalna analiza spletnega bančništva za fizične osebe, 2006.

Požarni zid

Požarni zid je namenjen zaščiti podatkov pred nepooblaščenimi osebami, ki bi v sistem prinašale ali odnašale določene informacije. Zagotavlja varnost med dvema omrežjema in je nepogrešljiv za vsako napravo, ki vzpostavlja povezavo z internetom. V klasičnem poslovanju bi lahko požarni zid primerjali z vratarjem, ki pri vstopu v stavbo selekcionira ljudi in tako določa, kdo bo sprejet in kdo zavrnjen. Požarni zid z ustrezno strojno in programsko opremo implementira varnostno politiko v zvezi z uporabo virov in sistemov v internem lokalnem omrežju. Pri sami postavitvi požarne pregrade je vsem uporabnikom lokalnega omrežja omogočen čim boljši dostop do javnega omrežja, iz omrežja internet pa nazaj v lokalno omrežje sprejmejo le povezave do javnih strežnikov.

Nemen požarne pregrade je preveriti podatke, ki pritekajo z interneta v lokalno omrežje. Administrator določi selektivna pravila, ki dovoljujejo vstop določenim podatkom v lokalno omrežje (Slika 19). Filter za vstop v sistem je lahko ime domene, IP naslov prejemnika ali pošiljatelja, uporabniško ime ipd. (Kalakota & Whinston, 1997, str. 125). Nevarnosti lahko prežijo tudi od znotraj, vendar v tem primeru požarni zid ni rešitev, saj vmesnik deluje le za kontrolo zunanjih virov. Na požarnem zidu ni moč videti, če je prišlo do zlorabe informacij s strani zaposlenih v podjetju. Nastalo situacijo je potrebno reševati z določenim overitvenimi postopki.

Slika 19: Osnovni model zaščite lokalnega omrežja



Povzeto in prirejeno po Young-Seock, Osnovni model zaščite lokalnega omrežja, 2006.

4.2 Elektronski podpis

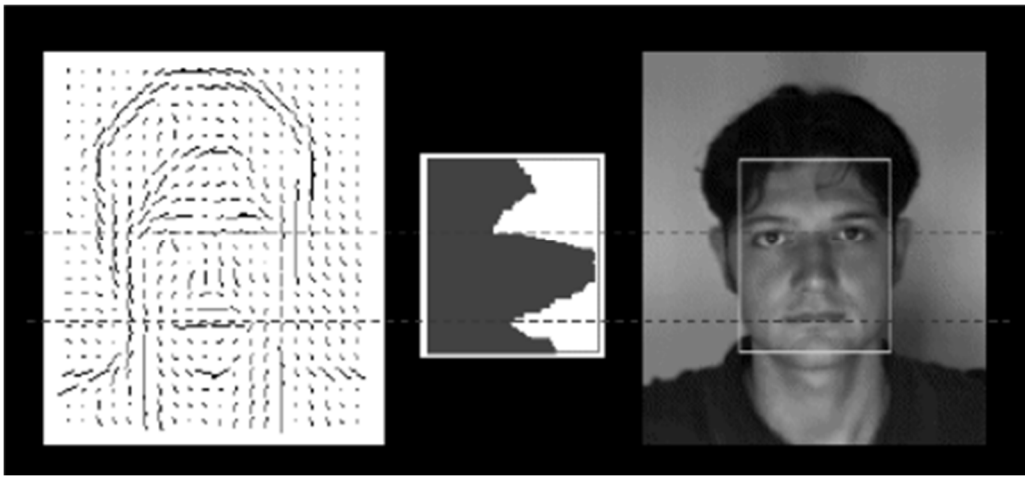
V sklopu elektronskega podpisovanja poznamo več oblik Od enostavnejših, ki temeljijo na simetričnih algoritmov in predstavljajo šibkejšo obliko varnosti, do tistih, ki temeljijo na asimeričnih algoritmih in predstavljajo visoko stopnjo varnosti. Elektronski podpis je skeniran lastnoročni podpis v elektronski obliki, ki ga pridobimo z elektronsko tehnologijo. Za razliko od digitalnega podpisa, ki ga dobimo z asimetričnim šifrirnim postopkom, ne omogoča neokrnjenosti podpisanega dokumenta in identifikacije podpisnika (Toplišek, 1998, str. 30).

Elektronsko podpisovanje kot zaščita transakcij

Elektronski podpis je varnostni element, ki nadomešča lastnoročni podpis v elektronskem poslovanju. Pri njem uporabljamo digitalni podpis, biometrične metode in elektronski podpis z digitalnim peresom. Z biometričnimi metodami lahko identificiramo posameznika glede na njegove edinstvene lastnosti – prstni odtis, glas, del očesa, DNK ipd. Biometrične metode so glede varnosti med najzanesljivejši metodami. S pomočjo infrardeče kamere, ki skenira naš obraz (Slika 20), pridobimo zapis žilnega sistema obraza, kar postane naše unikatno geslo. Postavlja se vprašanje, kaj vse lahko zmoti infrardečo kamero pri sami identifikaciji osebe. So to brada, izraz na obrazu ali drugačna frizura? Strokovnjaki zatrjujejo, da je najbolj

zanesljiv del na našem obrazu trikotnik med očmi in nosom, saj se ne spreminja veliko, prav tako so edinstvena tudi znamenja in pege.

Slika 20: Primer biometrične zaščite s prepoznavanjem obraza



Vir: D.Ošlak, Varnost elektronskega poslovanja v slovenskem bančništvu, 2005.

Z uporabo biometričnih naprav so povezani visoki stroški, zato v sklopu elektronskega poslovanja zaenkrat še ni prišlo do uporabe v večjih razsežnosti, zato se največ uporablja digitalni podpis.

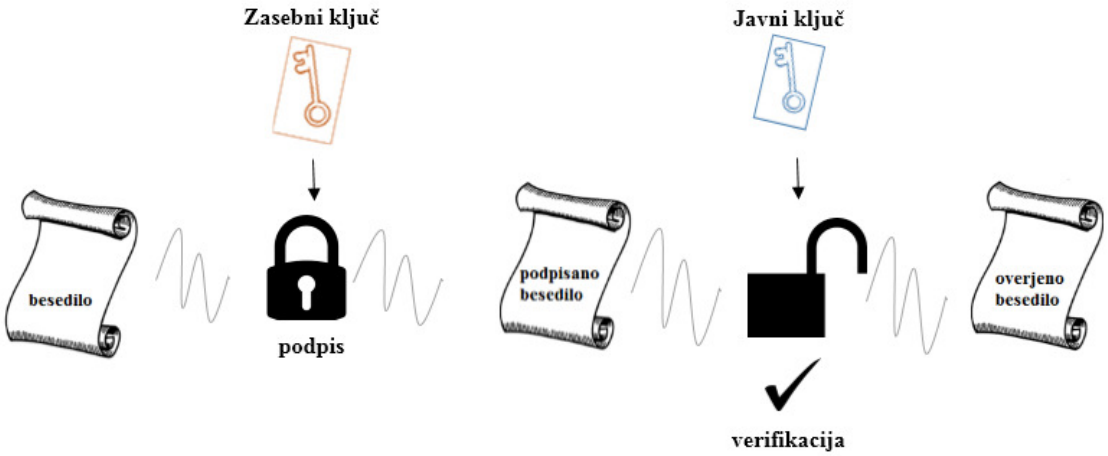
Digitalni podpis

Digitalni podpis je šifriran prstni odtis ali zgoščena oblika elektronskega sporočila. Šifrirani mehanizem pretvori podatke po računskem postopku oz. algoritmu tako, da jih brez veljavnega kodnega ključa ne moremo dešifrirati oz. povrniti v prvotno obliko (Slika 21). Glavna naloga šifriranja je zagotavljanje zasebnosti sporočila, medtem ko digitalni podpis omogoča večjo verodostojnost avtorja sporočil in razkrije identiteto osebe, ki se digitalno podpiše.

Da bi zagotovili identičnost lastnoročnega podpisa z digitalnim podpisom, mora podpis zadostiti naslednjim zahtevam (Ministrstvo za javno upravo, 2006):

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

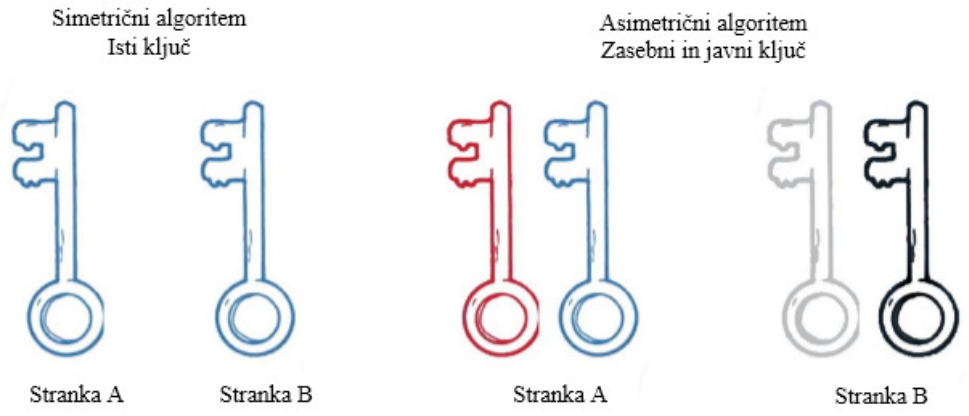
Slika 21: Prikaz podpisovanja elektronskih dokumentov



Vir: NA – Network Associattes, An Introduction to Cryptography, 1999.

Podpisovanje dokumenta (Slika 21) z uporabo metod asimetrične kriptografije poteka v dveh fazah. V prvi fazi podatke skrčimo z eno izmed enosmernih zgoščevalnih funkcij, ki poljubno dolgo besedilo preslika v blok konstantne dolžine. Dobljeni blok, ki predstavlja prstni odtis besedila, šifriramo s svojim zasebnim ključem in tako dobimo digitalni podpis. Pri preverjanju podpisa naslovnik z javnim ključem pošiljatelja (podpisnika) dešifrira podpis in dobi povzetek. Ponovno izračuna povzetek pisma, ki je bilo poslano v nešifrirani obliki, z isto zgoščevalno funkcijo kot pošiljatelj. Če se ujemata, pomeni, da je dobil tak dokument, kot ga je pošiljatelj podpisal. Če pa sta različna, je dokument podpisal nekdo drug ali pa je bila vsebina dokumenta spremenjena. Bistvo poteka digitalnega podpisovanja je, da podpisujemo s svojim zasebnim ključem, podpis pa preverimo z javnim ključem podpisnika (Pepelnjak & Bradeško, 1997, str. 164).

Slika 22: Simetrično in asimetrično šifriranje



Vir: Pepelnjak & Bradeško, Varnost računalniških sistemov elektronskih transakcij, 1997.

Pri simetrični kriptografiji tako pošiljatelj kot prejemnik uporabljata isti ključ (Slika 22) , ki ga morata skrbno varovati. V naprej se dogovorita, kateri in kako dolg ključ bo dostopen obema in kako bosta med seboj prenesla tajno informacijo. Takšna oblika prenosa podatkov je lahko tarča za nepridiprave, ki želijo prestreči podatke. Z uporabo asimetrične kriptografije se rešuje osnovna pomankljivost simetrične kriptografije.

Pri asimetrini kriptografiji pošiljatelj naredi par ključev, kjer zasebni ključ varno shrani – najvarneje je na pametno kartici, ki je zaščitena z geslom. Prejemnika obvesti, kje lahko dobi javni kluč, ki ga lahko popolnoma nezavarovanega pošlje v kakšen javni imenik. Prejemnik nato šifrira pošiljateljev čistopis z javnim ključem in ga pošlje nazaj v obliki tajnopisa, ki ga lahko dešifrira le pošiljatelj.

4.2.1 Digitalno potrdilo

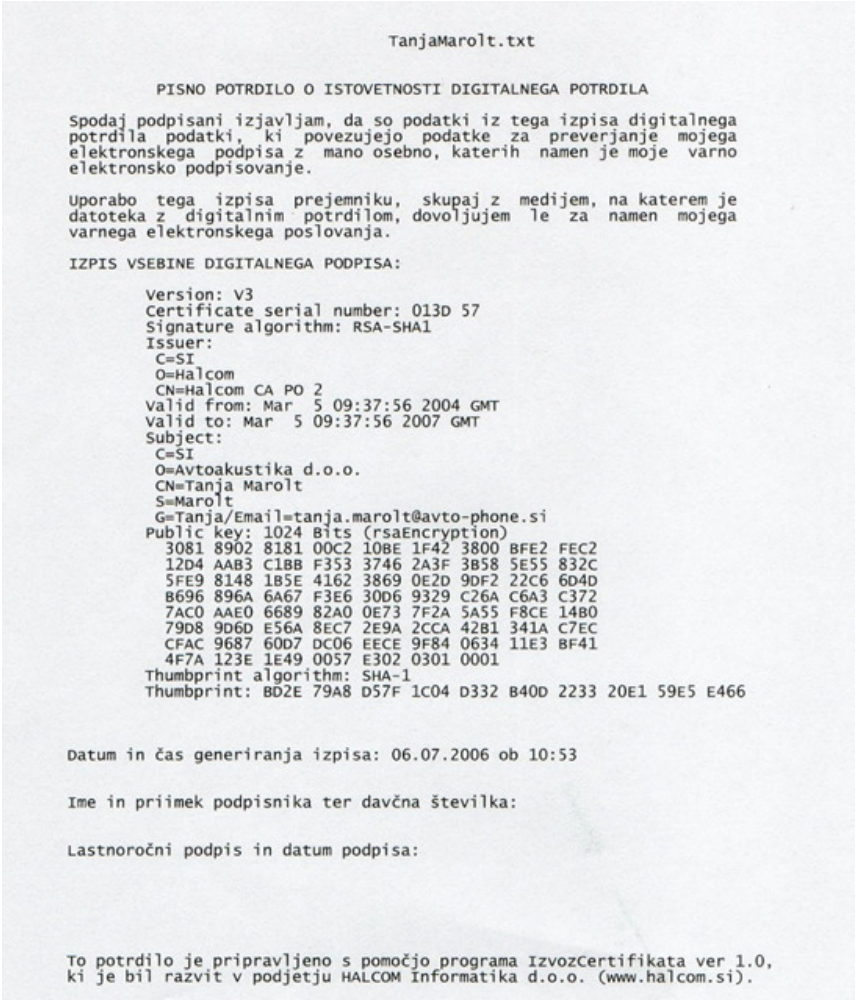
Digitalno potrdilo je digitalni dokument, ki dokazuje povezavo med javnim ključem in osebo oz. institucijo ali strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Je sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica ipd.) s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

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

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

Na Sliki 23 je staro digitalno potrdilo, ki ga izdajatelj digitalnega potrdila (podjetje Halcom d.d.) pošlje ob prvem prevzemu oz. ob izdaji kartice.

Slika 23:Pisno potrdilo o istovetnosti digitalnega potrdila



TanjaMarolt.txt

PISNO POTRDILO O ISTOVETNOSTI DIGITALNEGA POTRDILA

Spodaj podpisani izjavljam, da so podatki iz tega izpisa digitalnega potrdila podatki, ki povezujejo podatke za preverjanje mojega elektronskega podpisa z mano osebno, katerih namen je moje varno elektronsko podpisovanje.

Uporabo tega izpisa prejemniku, skupaj z medijem, na katerem je datoteka z digitalnim potrdilom, dovoljujem le za namen mojega varnega elektronskega poslovanja.

IZPIS VSEBINE DIGITALNEGA PODPISA:

Version: V3
Certificate serial number: 013D 57
Signature algorithm: RSA-SHA1
Issuer:
C=SI
O=Halcom
CN=Halcom CA PO 2
Valid from: Mar 5 09:37:56 2004 GMT
Valid to: Mar 5 09:37:56 2007 GMT
Subject:
C=SI
O=Avtoakustika d.o.o.
CN=Tanja Marolt
S=Marolt
G=Tanja/Email=tanja.marolt@avto-phone.si
Public key: 1024 Bits (rsaEncryption)
3081 8902 8181 00C2 10BE 1F42 3800 BFE2 FEC2
12D4 AAB3 C1BB F353 3746 2A3F 3B58 5E55 832C
5FE9 8148 1B5E 4162 3869 0E2D 9DF2 22C6 6D4D
B696 896A 6A67 F3E6 30D6 9329 C26A C6A3 C372
7AC0 AAE0 6689 82A0 0E73 7F2A 5A55 F8CE 14B0
79D8 9D6D E56A 8EC7 2E9A 2CCA 42B1 341A C7EC
CFAC 9687 60D7 DC06 EECE 9F84 0634 11E3 BF41
4F7A 123E 1E49 0057 E302 0301 0001
Thumbprint algorithm: SHA-1
Thumbprint: BD2E 79A8 D57F 1C04 D332 B40D 2233 20E1 59E5 E466

Datum in čas generiranja izpisa: 06.07.2006 ob 10:53

Ime in priimek podpisnika ter davčna številka:

Lastnoročni podpis in datum podpisa:

To potrdilo je pripravljeno s pomočjo programa IzvozCertifikata ver 1.0, ki je bil razvit v podjetju HALCOM Informatika d.o.o. (www.halcom.si).

Vir: Halcom d.d., Pisno potrdilo o istovetnosti digitalnega potrdila, 2006.

V prilogi dobite tudi zgoščenko, na kateri je nameščen program za kasnejši izpis digitalnega potrdila, če bi želeli v svoj repertoar dodati še kakšno podjetje ali transakcijski račun že vključenega podjetja. Program za izpis digitalnega potrdila je dostopen na internetni strani podjetja Halcom d.d., kjer izberete meni podpora ter program za izvoz digitalnih potrdil. V čitalniku mora biti nameščena kartica, s katere bi radi poslali potrdilo, saj program zahteva vnos kode PIN. Program shranite na računalnik in ga nato zaženete s shranjenega mesta. Ob zagonu se vam odpre dokument, v katerega je potrebno ročno dopisati še ime in priimek, davčno številko, lastnoročni podpis ter datum podpisa. Po vpisu podatkov je dokument pripravljen za pošiljanje na banko.

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

Preverjanje digitalnih potrdil

V Sloveniji sta za identifikacijo digitalnega potrdila na voljo matična in davčna številka podjetja oz. občana. Nekateri overitelji so se odločili, da davčno številko pravne ali fizične osebe vključijo v serijsko številko ali organizacijsko enoto razločevalnega imena v potrdilu, drugi jo vključijo v posebno polje, tretji pa je v potrdilo sploh ne zapišejo in vodijo lastno evidenco za identičnost potrdil z davčnimi številkami. Vprašanje pa je, kako preveriti potrdilo in pridobiti tudi podatke, ki so na njem zapisani. To nalogo opravljajo spletni servisi posameznih podjetij.

Spletni servis za preverjanje davčnih številk preveri njihovo verodostojnost. Pri nekaterih storitvah jo moramo vnesti, servis pa jo na podlagi podatkov iz potrdila potrdi ali pa sporoči, da ni bila vnešena. Servis deluje zgolj za potrdila, ki vsebujejo zapis davčne številke. Tretji postopek servisa poskrbi za vračanje podatkov uporabniku storitev, a le tistih, ki so že vsebovani v potrdilu in ki niso v nasprotju z Zakonom o varstvu osebnih podatkov. Servis za preverjanje veljavnosti digitalnega potrdila preverja časovno veljavnost potrdila. Bistvena je povezava z najnovejšim seznamom preklicanih potrdil (Halcom d.d., 2016).

4.2.2 Overitelj javnih ključev

Overitelj oz. agencija za certificiranje javnih ključev (CA) je ustanova, ki ji zaupajo njeni komitenti – imetniki digitalnih potrdil. S tem jo tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Overitelj izda lastniku javnega ključa digitalno potrdilo, s katerim zagotavlja drugim uporabnikom avtentičnost ključa in neločljivo veže uporabnika in njegov javni ključ. S pomočjo tega potrdila lahko lastnik dokaže lastništvo ključa in s tem tudi svojo identiteto.
Poleg agencij za overjanje javnih ključev imajo pomembno vlogo tudi uradi za registriranje (RA), ki sodelujejo pri izvajanju nalog CA. Razlika med agencijami in uradi je v tem, da agencija izda uporabniku digitalno potrdilo, s katerim jamči, da javni ključ res pripada samo njemu, medtem ko uradi preverjajo dokumente in registrirajo naročnika, ki zaprosi za potrdilo, preverijo njegovo identiteto in ujemanje javnega in zasebnega ključa.

V svetu obstaja veliko različnih agencij za overjanje javnih ključev. V Sloveniji imamo kar nekaj overiteljev javnih ključev, ki izdajajo potrdila za posamezna področja e-poslovanja. Za potrebe javne uprave in za uresničevanje projekta e-poslovanje znotraj te je bil ustanovljen overitelj digitalnih potrdil na Centru Vlade Republike Slovenije za informatiko (CVI), ki deluje v sklopu Ministrstva za javno upravo, ki izdaja dve različici digitalnih potrdil:

- SIGOV – CA (Slovenian GOVernmental Certification Authority), ki je namenjeno uporabi v javni upravi ter

- SIGEN – CA (Slovenian GENeral Certification Authority), ki je namenjeno pravnim in fizičnim osebam za izmenjavo podatkov z institucijami javne uprave in za dostop do podatkov, ki so v skrbništvu javne uprave.

4.2.3 Infrastruktura javnih ključev

Infrastruktura javnih ključev (PKI – Public Kay Infrastructure) je sistem za upravljanje s ključi in z digitalnimi potrdili, ki omogočajo vzpostavitev potrebnega zaupanja za e-poslovanje. Je kombinacija programske in strojne računalniške opreme ter politike in pravil certificiranja. Osnovna naloga PKI je zgraditev infrastrukture overiteljev digitalnih potrdil. Podobno kot je nastajal sistem elektronskih naslovov in imen računalnikov, nastajajo tudi posamezne infrastrukture certifikatskih agencij – overiteljev digitalnih potrdil, ki jih vpeljujejo vlade (Kanada, ZDA, Singapur, nekatere evropske države) ali posebne organizacije (Verisign, Thawte, EuroTrust). Te doslej še niso povezane med seboj, tako da lahko komunicirajo med seboj samo člani posamezne infrastrukture.

Pomembnejše storitve PKI so:

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

Ključi se lahko uporabljajo za podpisovanje ali šifriranje v različnih okoljih (e-bančništvo, državna uprava, medorganizacijsko poslovanje, vojska itd.). Različna okolja zahtevajo različno stopnjo varnosti. Naloge PKI so združevanje overiteljev s podobno varnostno politiko izdaje potrdil in graditev sistema zaupanja. Šifrirani sistemi so danes postali sestavni del varnostnih mehanizmov, kot so požarni zid, pametna kartica, uporaba gesel, varnostni protokoli itd. PKI zgradijo overitelji, ki si zaupajo, kar pomeni, da imajo enako politiko certificiranja in izdajo potrdil z enako varnostno politiko. Člani PKI izdana potrdila overiteljev iz seznama PKI sprejemajo kot vredna zaupanja.

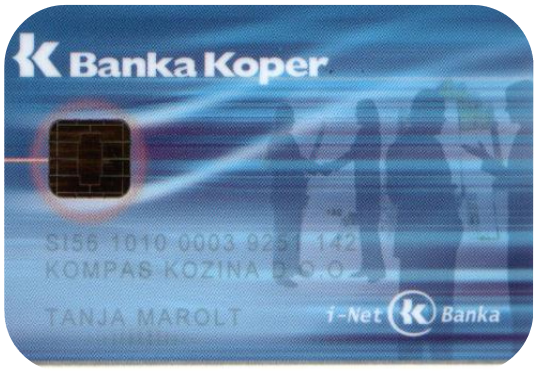
4.3 Pametne kartice

Pojav pametne kartice sega pred leto 1980. Danes obstaja več vrst pametnih kartic od tistih, ki odpirajo hotelska vrata do tistih, ki se jih uporablja pri elektronskem bančništvu. Kartice, ki jih uporabljamo za sodobne bančne poti imajo na sprednji strani kartice čip, ki ima vgrajenim mikroprocesor Samo podpisovanje dokumentov (bodisi računov, naročil ipd.) poteka v tem mikroprocesorju. Za uporabo kartice je potrebna koda PIN, ki omogoča dostop do digitalnega podpisovanja, ne pa tudi do zasebnega ključa, ki je varno shranjen na njej. Za

varno hrambo kvalificiranih potrdil je zatorej najvarnejše uporabljati pametno kartico. Tehnologija, ki podpira hrambo na pametnih karticah je zasnovana na kriptografskih vezjih. (Halcom d.d., 2016).

Na Sliki 24 je prikazana kartica Banke Koper, ki je registrirana na ime podjetja in osebno ime. Lahko se uporablja za bančne storitve pri več podjetij, ki opravljajo plačilni promet oz. kakršnekoli druge storitve elektronskega bančništva.

Slika 24: Kartica Banke Koper d.d



Vir: Banka Koper d.d., Primer pametne kartice, 2006.

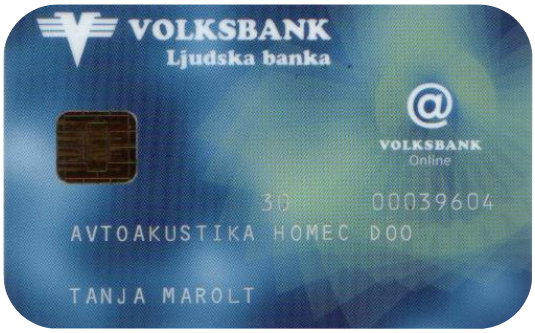
Kartica Ena za vse (Slika 25) je registrirana na ime podjetja, čeprav s kartice to ni razvidno, je pa vidno na izpisu digitalnega potrdila. V sklopu Halcomovih rešitev se lahko uporablja za več transakcijskih računov, ki so odprti pri različnih bankah, in za več podjetij hkrati. Hal E-Bank uporablja že več kot 60 bank v Albaniji, Nemčiji, Bosni in Hercegovini, Iranu, Kosovu, Katarju, Srbiji, Črni gori in Sloveniji.

Slika 25: Kartica ena za vse – Halcom, d.d

Vir: Halcom d.d., Kartica ena za vse, 2006.

Na Sliki 26 je kartica Volksbank Ljudske banke d.d, ki je od 15. 2. 2012 v 100% lasti ruske Sberbanke. V letu 2013 se tudi dokončno preimenuje.

Slika 26: Kartica Volksbank – Ljudske banke, d.d



Vir: Volksbank d.d., Primer pametne kartice, 2006.

S pomočjo pametne kartice poteka izmenjava podatkov z zunanjim svetom na varen in zanesljiv način. Čip na sprednji strani kartice omogoča izmenjavo podatkov, med čitalnikom pametnih kartic in samo pametno kartico. Po namestitvi čitalnika na računalnik je možno s karticami poslovati kjerkoli. Pametne kartice je potrebno po zaključku dela odstraniti iz čitalnika, saj na ta način poskrbimo za dodatno zaščito pred vdori v elektronsko banko. Na Sliki 27 sta prikazana 2 različna čitalnika pametnih kartic.

Pametna kartica nudi boljšo zaščito pred zlorabo kot njena predhodnica, kartica z magnetnim zapisom. Uporaba magnetne kartice namreč ni pogojena s PIN kodo, saj zadošča že lastnoročni podpis, ki pa ga je mogoče ponarediti brez večjih težav, prav tako pa je mogoče s pomočjo posebnih napravprekopirati zapis z ene magnetne kartice na drugo.

Slika 27: Čitalniki pametnih kartic

Vir: Halcom d.d, Tip čitalnika pametnih kartic, 2016.

Pri uporabi pametne kartice pa je, v nasprotju z magnetno kartico, možen e-podpis le z vnosom osebnega gesla, ki naj bi ga poznal le imetnik kartice. Terminal omogoča tri poskuse

vnosa gesla, če je tudi tretji neuspešen, se kartica zablokira. Poleg pametnih kartic se vse več uporabljajo tudi pametni USB ključi, na katerih je prav tako shranjen zasebni ključ.

4.4 Gesla in druga zaščita

Najpreprostejša in hkrati najstarejša oblika s katerimi preverjamo identitete posamezne osebe je prepoznava s pomočjo gesel. Uporabo gesel srečujemo na vsakem koraku, kot prvo se identificiramo z geslom že pri samem vstopu v računalnik. Preko dneva gesla uporabljamo za vstop do raznih spletnih aplikacij in tudi za vstop do e-banke. .

Zaradi naslednjih 3 razlogov štejemo gesla za šibkejšo obliko zaščite (Jerman Blažič, 2001, str. 116):

- Uporabniki si gesla oblikujejo sami na podlagi podatkov, ki si jih je lažje zapomniti, po drugi strani pa jih je zato tudi lažje razkrinkati. S pomočjo znanih podatkov uporabnikov je velikokrat lahko priti do samih gesel. V kolikor programi zahtevajo kompleksnejša gesla, si jih uporabniki zabeležijo in na ta način ponudijo priložnost nepridipravom.
- Pri identifikaciji uporabniki razkrijejo svoje geslo in tako omogočijo naslovniku, da se izdaja pod njihovim imenom.
- Gesla so izpostavljena socialnemu inženiringu.

Zaradi navedenih razlogov štejemo gesla za šibko overjanje, zatorej gesla niso primerna za preverjanje identitete v e-poslovanju. Njihiva uporaba je primerna za dostop do lokalnega sistema ali internetnih brskalnikov. Za preverjanje identitete v e-poslovanju se pogosteje uporabljajo PIN kode, ki jih uporabljamo za storitve na bankomatu, pri plačilu z bančno kartico ali elektronskem bančništvu.

Vse več bank v Sloveniji stremi k dodatnim varnostnim ukrepom, ki bi uporabnikom kljub dodatnim kontrolam omogočile čim varnejše poslovanje. Te so:

- **dnevni limit porabe, ki ga je možno preseči z dodatnimi varnostnimi kontrolami;**
- **novi transakcijski računi,** na katere želimo v elektronski banki nakazati denar in še niso shranjeni med našimi hitrimi plačili, zahtevajo dodatne varnostne kontrole;
- **sporočilo ob vstopu v program,** ki ga lahko prejmete kot SMS ali e-pošto, in
- **osebno sporočilo**, ki ga ne vidite, če gre za lažno povezavo z vašo banko.

Dodatno varnost v elektronskem bančništvu omogočajo tudi enkratna gesla. Uporabiti ga je mogoče zgolj enkrat, pri čemer je najpomembnejše, da naslednjega gesla ni moč napovedati oz. izračunati. Kot navaja Jerman Blažičeva (2001, str. 116) je najbolj znan način za identifikacijo s pomočjo enkratnih gesel uporaba kartice, ki vsebuje mikroprocesor in ekran, ki je sinhroniziran z uro na strežniku.

Kartica SecurID (Slika 28) je programirana za določenega uporabnika, zatorej ni potrebno vnašati uporabniškega imena in gesla. Numerično geslo na zaslonu se zamenja vsako minuto. Levo na zaslonu je 6 črtic, ki ponazarjajo teh 60 sekund.

Slika 28: Kartica NKBM, d.d

Vir: NKBM d.d, Kartica Secur ID, 2011.

Drugačen je postopek pri kartici banke SKB, ki je namenjena elektronskemu bančništvu za fizične osebe (Slika 29). S pomočjo tipkovnice je potrebno na kartici vnesti kodo PIN, ki nato generira numerično geslo za vstop v elektronsko banko. Dodatna zaščita, ki jo je banka uvedla že pred časom je dodatna aktivacijska koda, ki jo je po vstopu potrebno vtipkati v kartico in dodatno vpisati v elektronsko banko. Šele ko opravite te formalnosti, lahko začnete uporabljati storitve elektronskega bančništva.

Slika 29: Kartica za uporabo SKB NET za fizične osebe

Vir: SKB d.d., Identifikacijska kartica, 2011.

5 OBDELAVA PRIMEROV – ŽRTVE ZLORABE PRI UPORABI ELEKTRONSKEGA BANČNIŠTVA

Opisala bom štiri primere zlorab. Prvi dve sta se zgodili v letu 2011 na bančnih avtomatih in sta primera skimminga, ki je vse prepogosto na seznamu zlorab. V javnih objavah s strani banke NLB je pojasnjeno, kaj je skimming. Nepridipravi s posebno napravo, ki je nameščena na bankomat, s kartic prekopirajo magnetni zapis in nato ponaredijo kartice. Za izvedbo transakcij potrebujejo še številko PIN, ki jo dobijo tako, da na bankomat namestijo kamero. Zadnja dva primera pa naj bi nakazovala na zlorabo s t.i. ribarjenjem (ang. Phishing). Gre za zavajanje uporabnikov s pomočjo lažnih spletnih strani, ki so zelo podobne pravi strani banke. Z vnosom podatkov na lažno spletno stran pride do izdaje podatkov o uporabniškem imenu in geslu, ki zadostujejo za zlorabo bančnega računa.

Da bi se v čim večji meri izognili zlorabam, je v letu 2012 Združenje bank Slovenije podalo osnovna pravila varne rabe elektronskega bančništva, ki so objavljena na spletni strani Združenja bank Slovenije in na drugih spletnih naslovih bank in hranilnic. V osnovnih pravilih opozarjajo uporabnike naj:

- po zaključku dela ugasnejo računalnik,
- odstranijo ključke ali kartice iz računalnika ali čitalca in jih shranijo na varno mesto,
- redno spremljajo prilive in odlive na transakcijskem računu,
- ne pošiljajo gesel ali digitalnih potrdil po elektronski pošti,
- kodo PIN večkrat zamenjajo in je ne hranijo skupaj s kartico ali ključkom,
- ne odpirajo sumljivih elektronskih sporočil in ne nameščajo programov iz nepreverjenih virov in
- nikoli ne dostopajo do povezav banke preko e-mail sporočil.

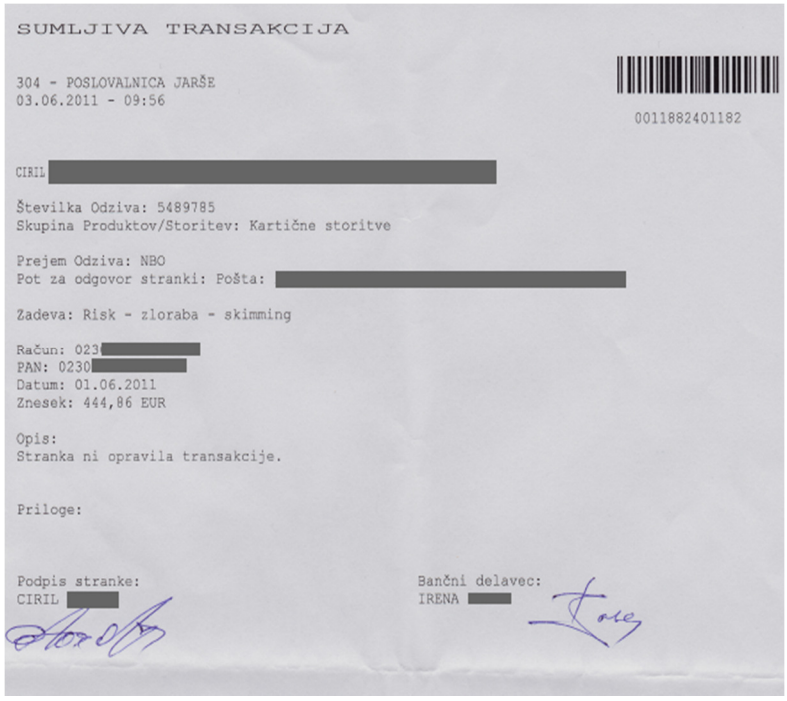
Za varnost računalnika je potrebno skrbeti s požarnimi pregradami in osveženimi protivirusnimi programi. Do zlorab prihaja tudi tako, da se neznanci predstavijo kot osebe podporne službe in zahtevajo občutljive podatke ali celo dostop do našega računalnika.

Primer 1: gospod Ciril

Gospod Ciril je v mesecu maju 2011 dvignil denar na bančnem avtomatu pri poslovalnici NLB v Zgornjih Jaršah. 2. 6. 2011 je prejel klic s strani uslužbenke NLB iz Ljubljane, da so mu preklicali bančno kartico in da naj se zglasi v svoji matični banki.

Naslednji dan so ga na matični banki izprašali, če je 1. 6. 2011 opravljal kakšne transakcije v tujino. Ker je bil odgovor negativen, so mu povedali, da je prišlo do zlorabe. Neznanci so mu odtujili dobrih 3.000 EUR skupaj s stroški dviga gotovine.

Slika 30: Sumljiva transakcija



SUMLJIVA TRANSAKCIJA

304 - POSLOVALNICA JARŠE
03.06.2011 - 09:56

0011882401182

CIRIL [redacted]

Številka Odziva: 5489785
Skupina Produktov/Storitev: Kartične storitve

Prejem Odziva: NBO
Pot za odgovor stranki: Pošta: [redacted]

Zadeva: Risk - zloraba - skimming

Račun: 023[redacted]
PAN: 0230[redacted]
Datum: 01.06.2011
Znesek: 444,86 EUR

Opis:
Stranka ni opravila transakcije.

Priloge:

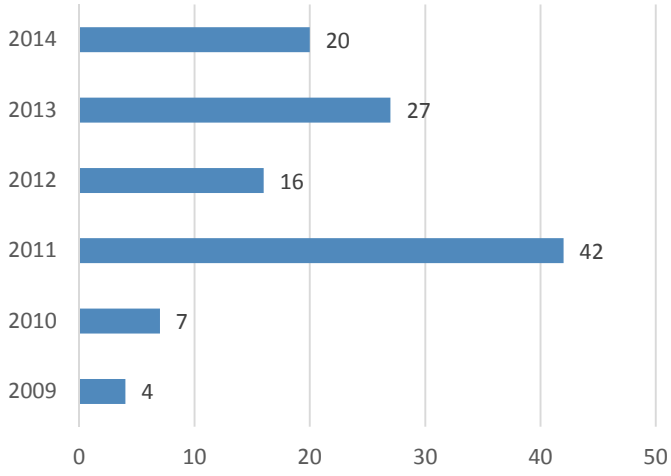
Podpis stranke:
CIRIL [redacted]

Bančni delavec:
IRENA [redacted]

Vir: NLB d.d., Sumljiva transakcija, 2011.

Gospod Ciril je s strani banke dobil v podpis dokument sumljiva transakcija (Slika 30), ki potrjuje, da je šlo za zlorabo, natačneje skimming, pod opis pa je zapisano, da stranka ni opravila transakcije.

Slika 31: Nameščene skimming naprave 2009–2014

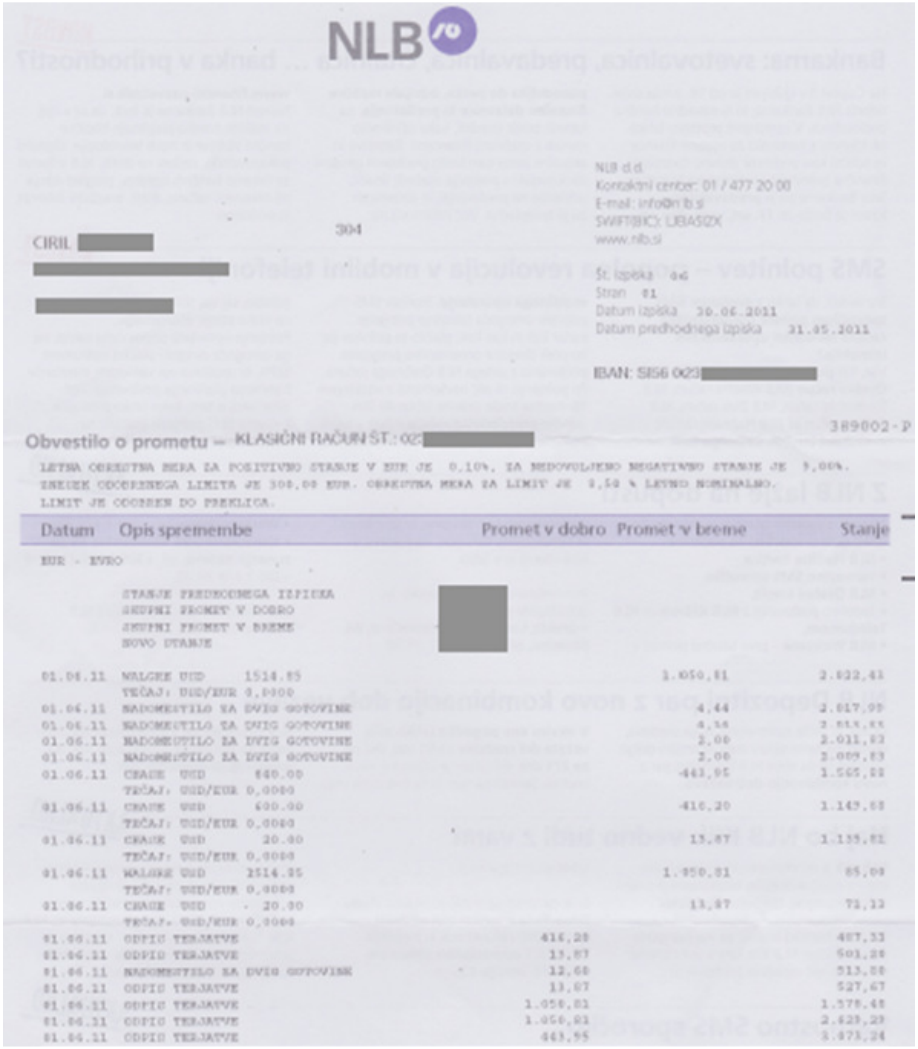


Vir: Voh Boštic, Kiberkriminal v Sloveniji (2): zakaj je boljša varnost vzrok za več zlorab bančnih kartic, 2015.

Po podatkih policije je bil največji napad na slovenske bankomate v letu 2011, ko je bilo v Sloveniji zaznati 42 nameščenih skimming naprav (Slika 31). V primerjavi z letom 2010, gra kar za 6-kratno povečanje nameščenih skiming naprav, ko je bilo zaznanih le 7 nameščenih skiming naprav. Po letu 2011 se je število napadov znatno zmanjšalo. Po podatkih policije je Slovencem v letu 2011 z računov izginilo okrog 300.000 EUR.

Na bančnem izpisku (Slika 32) je vidno, da je šlo za dobrih 4.300 dolarjev. Denar je bil prenakazan v Ameriko.

Slika 32: Bančni izpisek gospoda Cirila


NLB

NLB d.d.
Kontaktni center: 01 / 477 20 00
E-mail: info@nlb.si
SWIFT/BIC: LJBASI2X
www.nlb.si

304

CIRIL [redacted]

[redacted]

[redacted]

Št. izpiska 046
Stran 01
Datum izpiska 30.06.2011
Datum predhodnega izpiska 31.05.2011

IBAN: SI56 023[redacted]

389002-P

Obvestilo o prometu – KLASIČNI RAČUN ŠT.: 02[redacted]

LETNA OBRESTNA MERA ZA POZITIVNO STANJE V EUR JE 0,10%, ZA NEDOVOLJENO NEGATIVNO STANJE JE 9,00%.
ZNESEK ODOBRENEGA LIMITA JE 300,00 EUR. OBRESTNA MERA ZA LIMIT JE 2,50 % LETNO NOMINALNO.
LIMIT JE ODOBREN DO PREKLICA.

Datum	Opis spremembe	Promet v dobro	Promet v breme	Stanje
EUR - EVRO				
	STANJE PREDHODNEGA IZPISKA	[redacted]		
	SKUPNI PROMET V DOBRO			
	SKUPNI PROMET V BREME			
	NOVO STANJE			
01.06.11	VALGRE USD 1514.85		1.050,81	2.822,41
	TEČAJ: USD/EUR 0,9000			
01.06.11	NADOMESTILO ZA DVIG GOTOVINE		4,44	2.617,99
01.06.11	NADOMESTILO ZA DVIG GOTOVINE		4,56	2.613,43
01.06.11	NADOMESTILO ZA DVIG GOTOVINE		2,00	2.011,43
01.06.11	NADOMESTILO ZA DVIG GOTOVINE		2,00	2.009,43
01.06.11	CRADE USD 480.00		441,95	1.565,51
	TEČAJ: USD/EUR 0,9080			
01.06.11	CRADE USD 600.00		416,20	1.149,68
	TEČAJ: USD/EUR 0,9080			
01.06.11	CRADE USD 20.00		13,87	1.135,81
	TEČAJ: USD/EUR 0,9080			
01.06.11	VALGRE USD 2514.35		1.950,81	85,00
	TEČAJ: USD/EUR 0,9080			
01.06.11	CRADE USD 20.00		13,87	71,13
	TEČAJ: USD/EUR 0,9080			
01.06.11	ODPIS TERJATVE	416,20		487,33
01.06.11	ODPIS TERJATVE	13,87		501,20
01.06.11	NADOMESTILO ZA DVIG GOTOVINE	12,00		513,00
01.06.11	ODPIS TERJATVE	13,87		527,67
01.06.11	ODPIS TERJATVE	1.050,81		1.578,48
01.06.11	ODPIS TERJATVE	1.050,81		2.629,29
01.06.11	ODPIS TERJATVE	441,95		3.071,24

Vir: NLB d.d., Bančni izpisek, 2011.

Skimming naprave preberejo magnetni zapis s kartice in s pomočjo kamere posnamejo PIN kodo. V tujini se nato izdelajo ponarejene bančne kartice, ki jih kriminalci uporabijo na bankomatih in POS terminalih. Največ škode utrpijo banke, ki morajo svojim klientom povrniti škodo. Naprave so nameščene na bankomatih, kjer je dnevno opravljenih veliko

dvigov, saj je na ta način v kratkem času možno priti do velikih količin podatkov. Po podatkih policije je bilo v obdobju petih let v Ljubljeni nameščenih 84 naprav, sledi pa ji Maribor z 76. Na Sliki 33 je primerjava dveh bankomatov enega s skimming napravo in drugega brez skimming naprave.

Slika 33: Primerjava bankomata s skimming napravo in brez

Vir: RTV Slovenija, Tatovi bančnih PIN-številk spet na delu, 2011.

Pred letom 2011 je bil možen dvig na bankomatu s ponarejeno kartico, danes pa to ni več mogoče, saj je prišlo do nadgradnje kartic z magnetnim zapisom z vgraditvijo čipa (EMR standard). V Sloveniji se podatki berejo s čipa, magnetni zapis pa je uporaben le še za dvige v tujini. V tujini bi zaradi velikega števila bankomatov zamenjava predstavljala visok strošek, zato nekatere države še nimajo vpeljanega EMR standarda. Če pride do kraje identitete na bankomatu tujih bank, so dolžne kriti škodo slovenskim komitentom.

Za večjo varnost lahko poskrbimo sami s prekrivanjem tipkovnice, saj je prekopiran zapis s kartice neuporaben brez številke PIN, izjeme so le brezstične kartice. Slovenske banke na bankomate nameščajo naprave, ki motijo prepisovanje magnetnih zapisov in ukrepajo takoj, ko zasledijo pogostejše dvige na bankomatih v tujini.

V juniju 2011 je tudi sodelavec gospoda Cirila prejel klic s strani banke zaradi preklica bančne kartice. Obvestili naj bi več oseb, ki so tisti dan dvigali denar na bančnem avtomatu v Jaršah pri Domžalah. Gospodu Ciril je banka zagotovila, da bo odtujeni denar dobil povrnjen v celoti najkasneje v roku enega meseca. Denar je bil vrnjen v celoti vključno z nadomestili za dvig gotovine. Na izpisku je vračilo denarja prikazano kot odpis terjatev, ki so se zgodile isti dan kot sama bremenitev (zloraba) na računu.

Kot trdijo pri NLB, goljufi v primeru skimminga naenkrat ne morejo dvigniti več denarja, kot je uporabnikov dnevni limit za dvig gotovine na bankomatih. Gospod Ciril je zatrdil, da njegov dnevni limit ni bil nikoli dodatno zvišan, kar pomeni, da je trditev banke vprašaljiva.

Na Sliki 34 so prikazane podrobnosti skimming naprave, ki so zelo dobro prikrite.

Slika 34: Podrobnosti skimming naprave

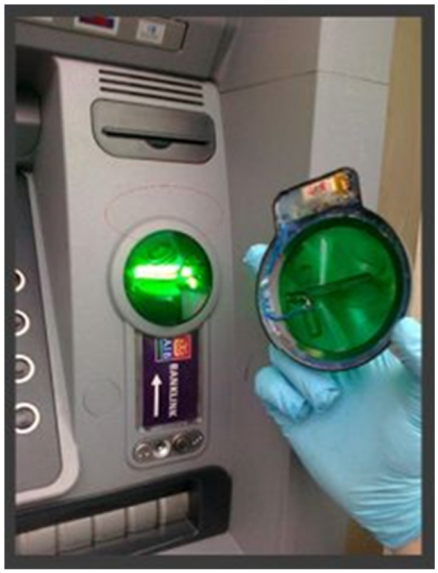
Vir: RTV Slovenija, Tatovi bančnih PIN-številk spet na delu, 2011.

S strani bank in v javnih objavah je bilo pogosto zaslediti opozorila, da je potrebno biti pozoren pri dvigih na avtomatu. Reža za kartico in odprtina, ki poda denar, sta bolj poudarjeni oz. izbočeni kot običajno. Opaziti jih je težko, saj je nastavek s kamero debelejši maksimalno za tri milimetre.

V začetku juniju 2011 so v Domžalah odkrili še eno skimming napravo, pri kateri pa zaradi hitrega ukrepanja niso zabeležili nobene škode. O odkritju skimming naprave je vedno obveščena policija, druge banke in same stranke, ki jim zamenjajo PIN kode ali blokirajo kartico.

Tudi na Irskem so v začetku junija 2011 odkrili napravo (Slika 35), kjer je nazorno viden lažni čitalec za branje magnetnega zapisa.

Slika 35: Primer skimming naprave odkrite na Irskem



Vir: RTV Slovenija, Tatovi bančnih PIN-številk spet na delu, 2011.

Primer 2: gospa Martina

V petek, 25. 11. 2011, je gospa Martina želela dvigniti denar na bankomatu na Gorenjskem. Bančni avtomat ji denarja ni izplačal, ampak ji je odvzel bančno kartico. Ker je bil bankomat pri banki, je šla vprašat, za kaj gre. Uslužbenka je pred njo prestrigla bančno kartico in ji zatrdila, da je bila ena izmed tistih, ki so jim preventivno blokirali kartico zaradi skimming naprav v Ljubljani. Gospa Martina je pred tem res dvigala denar na bankomatu v Ljubljani in je zato bila vključena na seznam oseb s povečanim tveganjem odtujitve denarja.

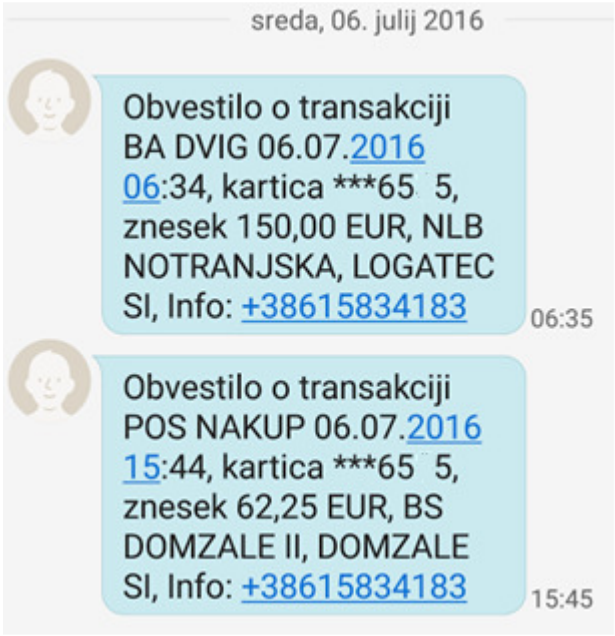
Za večjo varnost pri kartičnem poslovanju lahko uporabljate storitve varnostnega SMS sporočila, ki ga imetnik kartice lahko prejme po vsaki uspešno opravljeni avtorizaciji. Imetnik lahko izbira, za katere transakcije želi prejemati obvestila. Kriteriji so znesek transakcije in plačilo ali dvig s kartico, ki je lahko omejeno na plačevanje doma ali v tujini. Storitev varnostnega SMS sporočila je zasnoval Bankart v sodelovanju z bankami in mobilnimi operaterji. Na storitev SMS se lahko komitenti na matičnih bankah naročijo ob izpolnitvi obrazca. Storitev zagotavlja dodatno varnost uporabnikom plačilnih kartic in preprečuje zlorabe, saj prejem sporočila omogoča nadzor nad njihovo uporabo. SMS sporočilo nam torej služi kot varovalo oz. potrdilo, da smo kartico bremenili sami in ne nekdo drug.

Podatki, ki jih vsebuje varnostni SMS (Slika 36) so:

- opis transakcije,
- datum in ura transakcije,

- zadnje štiri številke imetnikove kartice,
- znesek,
- kraj in država transakcije in
- telefonska številka, na katero lahko pokličete v primeru zlorabe.

Slika 36: Primer SMS sporočila na mobilnem telefonu



Vir: SKB banka d,d,, Primer SMS sporočila, 2016.

V kolikor pride do zlorabe, mora imetnik kartice nemudoma javiti zlorabo v banko ali klicni center Bankart, kjer kartico takoj blokirajo. Na seznamu bank, ki omogočajo storitev varnostnih SMS sporočil svojim komitentom je trenutno 9 bank (Bankart, 2016):

- NLB,
- Abanka Vipa,
- Delavska hranilnica,
- Unicredit Banka Slovenije,
- Gorenjska banka,
- NKBM,
- Hypo Alpe Adria Banka,
- Banka Sparkasse in
- Banka Celje.

Bankart je storitev varnostnih SMS sporočil že prenesel na banke v JV Evropi, za katere izvaja kartično poslovanje. Na seznamu Bankarta ni SKB banke, ki pa tudi že ponuja varnostno SMS sporočilo.

Banke v sklopu dodatnih varnostnih nastavitev ponujajo izbiro dnevnega limita za dvig na bankomatu in višino odobrenega negativnega stanja, izberete pa lahko tudi višino maksimalnega zneska za plačilo na POS terminalu. Banke omogočajo prost izbor uporabe kartice na bankomatih ali POS terminalih. Kartico lahko zaščitite tudi na ta način, da dovolite le njeno uporabo na POS terminalih na čip ali blokirate uporabo na omenjenih terminalih in bankomatih v tujini.

Slika 37: Rokovanje z brezstično kartico

Vir: M. Bizovičar, Brezstična kartica bo vsaj enako varna, kot je čipna, 2016.

Na eni strani imamo dodatne varnostne ukrepe s SMS sporočili, na drugi pa nove oblike plačilnih brezstičnih kartic, ki prinašajo plačevanje računov nižjih zneskov brez vnosa številke PIN. Tehnologija brezstičnega prenosa podatkov iz kartice ali NFC (near field communication) je visokofrekvenčna komunikacijska tehnologija, ki omogoča izmenjavo podatkov do 10 cm razdalje od čitalca. Pri plačevanju manjših zneskov ne potrebujete kode PIN, omogoča pa tudi, da čitalec kartico prebere z razdalje nekaj centimetrov. Pri plačevanju zneskov višje vrednosti je še vedno potreben vnos številke PIN.

Na Sliki 37 sta prikazana brezstična kartica in POS terminal, ki prebere podatke s kartice. Na brezstični kartici je poseben znak, ki ponazarja radijsko frekvenco in označuje možnost brezstičnega plačevanje. Na POS terminalu je prikazana kartica, kamor plačnik približa kartico.

Banke zagotavljajo, da je poslovanje z brezstičnimi karticami enako varno kot poslovanje s klasičnimi čipiranimi karticami. Preko POS terminala se prenesejo samo podatki o številki kartice in datumu veljavnosti kartice, le v redkih primerih pa tudi ime in priimek imetnika

kartice. Gre za podatke, ki so vidni tudi na sprednji strani plačilne kartice. Za samo zlorabo so potrebne še dodatne informacije, ki pa jih ni moč prebrati.

V primeru, da ste lastnik več brezstičnih kartic, je eno izmed njih potrebno iz denarnice le vzeti in jo približati terminalu. Banke vidijo prednost tudi v tem, da je ni potrebno več izpustiti iz rok. V zadnjem času je tudi pri poslovanju s klasičnimi karticami vse več trgovcev, ki vas prosijo, da sami vstavite kartico v režo in tudi iz nje. V Sloveniji strokovnjaki zatrjujejo, da je večja verjetnost, da pride do fizične kraje kartice kot pa do prenosa podatkov. Opozarjajo pa, da lahko kombinacija mobilnega telefona in kartice prenese podatke v napačne roke. Do tega lahko pride, v kolikor na mobilni telefon nameščate nepooblaščeno programsko opremo (24 ur, 2016).

Slika 38: Uporaba brezstične kartice

Vir: Visa Europe, Pogosta vprašanja, 2016.

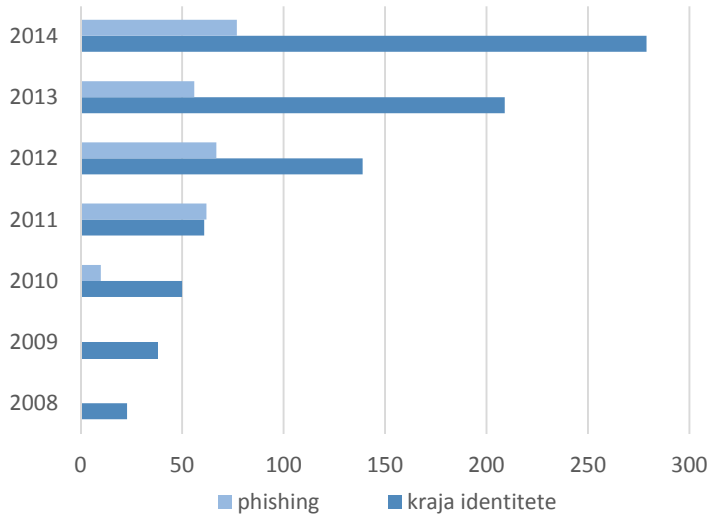
Na bankah podajajo različne informacije glede zneskov in števila zaporednih plačil v primeru brezstičnega plačevanja. NLB ponuja 5 zaporednih vnosov pod 15 EUR v enem dnevu, ob naslednjem nakupu pa POS terminal zahteva vnos kode PIN. Na SKB niso omejeni na dnevni limit, ampak na višino zneska do 50 EUR, ki ga lahko dosežete v daljšem časovnem obdobju.

Primer 3: gospod Marko

V letu 2008 je gospod Marko v svoji elektronski banki ugotovil, da je bilo z njegovega osebnega računa izvršeno plačilo, ki ga sam ni opravil. Plačilo v znesku 600 EUR je bilo nakazano na račun nekega moškega iz Maribora. Poklical je na banko, da bi preveril, kako je do takšne transakcije prišlo. Uslužbenka ga je vprašala, če do svoje spletne banke dostopa preko zaznamkov na svojem internetnem brskalniku. Odgovor je bil pritrdilen.

Gospod Marko se je še istega dne zglasil v svoji matični banki, kjer mu je uslužbenka zatrdila, da ga bodo kontaktirali pravniki. Naslednji dne so ga obiskali policisti in mu zasegli službeni računalnik, istega dne pa je tudi brez dodatnih pojasnil na svoj bančni račun dobil vrnjen denar. Še vedno ne ve zagotovo, ali je v njegovem primeru šlo za ribarjenje ali zgolj za napako enega izmed uslužbencev. Policija mu je v roku enega meseca vrnila računalnik, vendar o njegovem primeru ni podala dodatnih ugotovitev.

Slika 39: Goljufije in prevare



Vir: SI-CERT, Goljufije in prevare, 2016.

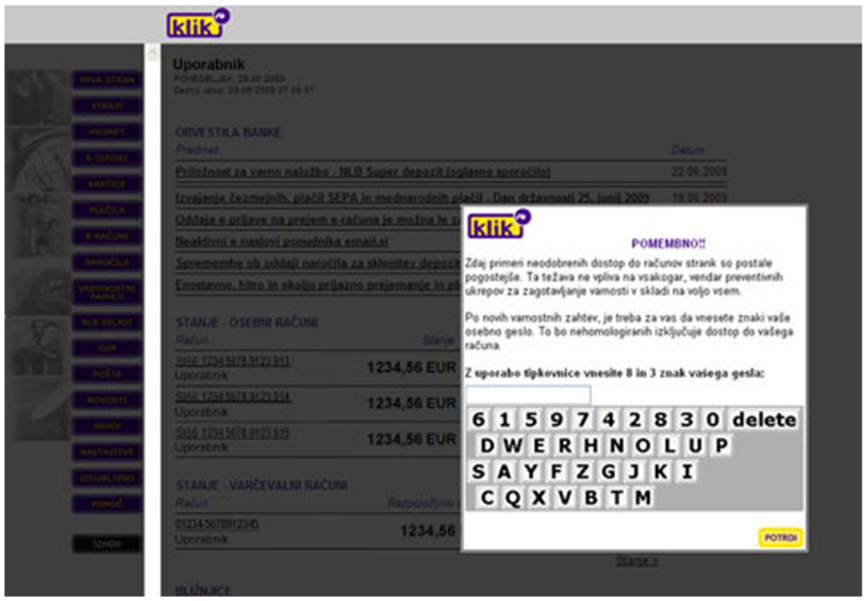
Ribarjenje je pridobitev oz. kraja podatkov, s katerimi zlikovci pridobijo dostop do gesel in uporabniških imen in s katerimi lahko dostopajo do spletnih strani oz. elektronske banke pod našim imenom. Prvi korak pri phishing prevari je zavajajoče elektronsko sporočilom, ki nas v imenu banke nagovarja, naj se s pomočjo spodnje povezave prijavimo in vpišemo svoje podatke. Na ta način komitenti z identifikacijo na lažni spletni strani razkrijejo potrebne informacije.

Po podatkih, ki jih je v poročilu objavil nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT (Slovenian Computer Emergency Response Team), se število incidentov iz leta v leto povečuje. Na grafu sta ponazorjeni dve obliki goljufij, in sicer kraja identitete in phishing. Iz Slike 39 je razvidno, da število obeh kriminalnih dejanj v obdobj-u šestih let močno raste. Kraja identitete se je sicer v letu 2013 glede na leto 2012 znižala, vendar je bilo v leto 2014 spet zaznati večji porast. Phishing napadi so prvi večji porast dosegli leta 2012, ko se je število napadov iz 61 (l. 2011) povzpelo na 139.

Kot je razvidno iz statistike, je vse bolj potrebna pozornost na sumljiva elektronska sporočila in spletne strani. Ponudniki spletnih storitev od strank nikoli ne zahtevajo vnosa določenih

podatkov. Mediji in banke na svojih spletnih straneh redno obveščajo uporabnike, če so bili odkriti novi napadi in to tudi dodatno podprejo s slikovnim materialom. S strani policije in ostalih pristojnih organov so vseskozi posredovana obvestila o ustrezni zaščiti za računalnike v zasebni in poslovni lasti.

Slika 40: Lažna prva stran



Vir: NLB d.d, Lažna prva stran, 2011.

Slika 41: Prava vstopna stran NLB Klik

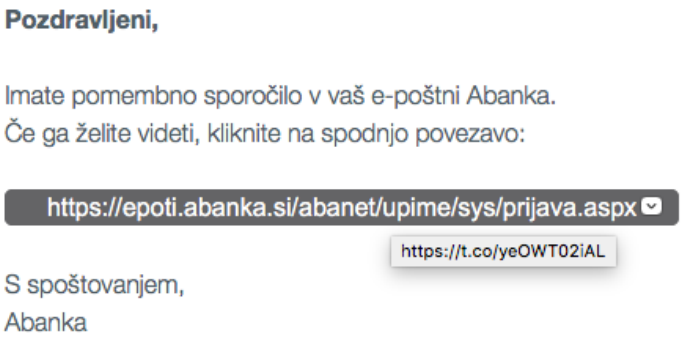
Vir: NLB d.d, Prava vstopna stran NLB Klik, 2011.

Na spletni strani NLB je slikovna ponazoritev, razlik med pravo in lažno spletno stranjo. Lažna prva stran je sivo obarvana. V belem, manjšem oknu je t.i. pomembno obvestilo, v katerem zlikovci v slabi slovenščini, naprošajo komitenta za vnos dodatnega varnostnega gesla, s čimer naj bi prišli do dodatnih zasebnih informacij (Slika 40). Tipkovnico na ekranu, uporabniki elektronske banke uporabljajo le pri izvrševanju plačil in naročil. Na Sliki 41 je prikazan izgled prave vstopne strani za uporabnike spletne banke Klik.

Virtualno tipkovnico se v programu Klik uporablja pri izvrševanju plačil na račun prejemnika, ki v preteklosti še ni bil dodan na t.i. hitri seznam plačil. Program zahteva vnos naključnih dveh znakov uporabnikovega gesla.

Med zadnji primeri phishinga, ki se je zgodil v aprilu 2016, so nepridipravi želeli pretentati uporabnike Abanke z lažno povezavo do spletne aplikacije. Banke pozivajo, da uporabnikom nikoli ne pošiljajo e-pošte z vsebino, kjer bi od njih zahtevali, naj sledijo določeni povezavi. Na Sliki 42 je lažno sporočilo, na katerem je naslov, kamor naj bi se uporabniki prijavili, pravilen, dejanska povezava pa je drug naslov, ki je skrit v ozadju.

Slika 42:Lažno sporočilo v imenu Abanke



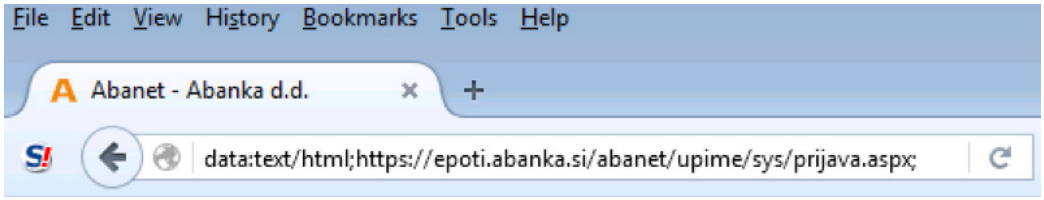
Vir: SI-CERT, Phishing z "inline" spletno stranjo, 2016.

S premikom puščice v desni spodnji kot povezave je vidno, da je dejanska povezava drugačna od tiste, ki je navedena z odebeljenimi črkami. Da je situacija še bolj otežena, lažna povezava naredi še dodatno preusmeritev, in sicer na zavajajočo stran, ki je vidna na Sliki 43. Z malo nepazljivosti lahko hitro spregledate začetni tekst, kar izpostavlja pomembnost pazljivosti pri uporabi elektronskega bančništva.

V maju 2016 je bilo v Sloveniji mogoče zaslediti več lažnih klicev, pri katerih se je klicatelj predstavil kot podporna služba družbe Microsoft. V slabi angleščini je žrtve nagovarjal, naj mu zaradi okužbe omogočijo oddaljen dostop do njihovega računalnika. Metodi s prigovarjanjem ter vzbujanjem zaupanja pravimo socialni inženiring. Vsak takšen napad je

potrebno nemudoma prijaviti, da bi ga lahko v čim večji meri zatrli in preprečili nadaljne napade.

Slika 43: Naslov, ki ne vodi na zaščiteno spletno stran Abanke



Vir: SI-CERT, Phishing z "inline" spletno stranjo, 2016.

Primer 4: Gospod Beno

Gospod Beno je med pripravami na potovanje v tujino oktobra 2015 preko spletne agencije Ticketmaster kupil vstopnice za športne prireditve v ZDA. To se je zgodilo na četrtek, v ponedeljek pa ga je na mobilno številko klicala neznana številka, kjer se je klicateljica predstavila kot predstavnica centra Efunds, ki za SKB opravlja avtorizacije. Ker temu ni verjel, je na internetu preveril telefonsko številko, za katero se je dejansko izkazalo, da pripada omenjeni ustanovi. Klicateljica mu je naštela sumljive transakcije in na elektronski naslov poslala reklamacijski zapisnik.

Ko je v elektronsko banko SKB NET prejel izpisek, je izpolnil reklamacijski zapisnik, kamor je vpisal vse transakcije, ter ga poslal na poštni naslov za prijavo zlorab. Trajne naloge za bremenitev računa iz kartice MasterCard ima gospod Beno 18. v mesecu in vsi zneski so bili dejansko trgani z računa v istem dnevu. Zneski so bili povrnjeni v celoti še istega dne.

Na Sliki 44 je podpisana izjava gospoda Bena, ki jo je podpisal banki, s katero zagotavlja, da transakcij ni opravil, niti ni dovoli, da bi kdo na mesto njega uporabljal njegovo bančno kartico.

SKB v oktobru 2015 še ni imela možnosti pošiljanja SMS sporočil za vsako transakcijo. V tem primeru bi gospod Beno za zlorabi izvedel prej, tako pa so ga z zamikom opozorili s strani procesnega centra. V obdobju naslednjega pol leta je banka SKB poskrbela tudi za svoje uporabnike in storitev omogočila za vsako transakcijo. Gospod Beno si je storitev SMS vključil za obe svoji kartici (Visa in MasterCard).

Slika 44: Podpisana izjava gospoda Bena

Datum: Ljubljana , 6.11.2015

Št. kartice: Mastercard 5406****

Ime in priimek : Ben

Datum	Prodajno mesto	Znesek
30.10.2015	STAPLES 00116798, 2497 SW 27TH AV	1.524,26 USD
30.10.2015	STAPLES 00102350, 1901 E SILVERSP	644,45 USD
30.10.2015	STAPLES 00102350, 1901 E SILVERSP	592,54 USD
31.10.2015	STAPLES 00117788, 18591 S DIXIE H	285,56 USD

Izjavljam, da nisem opravil(a) zgoraj navedenih transakcij, niti nisem dovolil(a) komurkoli drugemu, da jih opravi v mojem imenu. V času transakcij je bila kartica pri meni.

Podpis:

TRANSLATION OF CARDHOLDER´S LETTER

Neither me or anyone authorized by me engaged in listed transaction(s). The card was in my possession on the transaction(s) date(s).

The Cardholder

Vir: SKB banka d.d., Izjava, 2015.

6 PONUDBA BANK V SLOVENIJI IN REZULTATI EMPIRIČNE RAZISKAVE

V današnjem času je v Sloveniji elektronsko bančništvo nepogrešljivo, česar se zavedajo tudi naše banke. Z lastnimi ali zunanjimi strokovnjaki skoraj vse slovenske banke ponujajo razvito spletno bančništvo – za pravne kot tudi za fizične osebe.

Začetki elektronskega bančništva v Sloveniji segajo v leto 1997. Banka SKB, je bila tista, ki ga je strankam poleg klasičnih poslovalnic ponudila prva. Težava se je pojavila predvsem pri promoviranju storitve, saj so se klasične poslovalnice počutile ogrožene zaradi možnosti

izgube strank, zato elektronskega bančništva niso želele oglaševati. Do tedaj sta bila to dva ločena dobičkonosna centra, ki so jih kasneje preoblikovali (Bračun, 1997, str. 149–154).

Elektronsko bančništvo se med bankami razlikuje, predvsem večje slovenske banke so ga bolj izpopolnile in so zato zanimivejše za stranke. Njihov vložek namenjen za razvoj in varnost bančnih storitev je večji od manjših bank, lažje pa poskrbijo tudi za večjo prepoznavnost in atraktivnost njihove ponudbe. Banke so aplikacije za spletno banko pripravile s pomočjo lastnega kadra oz. so kupile že razvite programe od specializiranih ponudnikov.

V Tabeli 5 je pregled slovenskih bank, ki omogočajo e-bančništvo za fizične osebe. Navedeno je na kateri spletni strani lahko najdete vse podatke o posamezni e-banki in kako se imenuje spletna rešitev posamezne banke.

Tabela 5: Pregled bank, ki omogočajo spletno bančništvo za fizične osebe

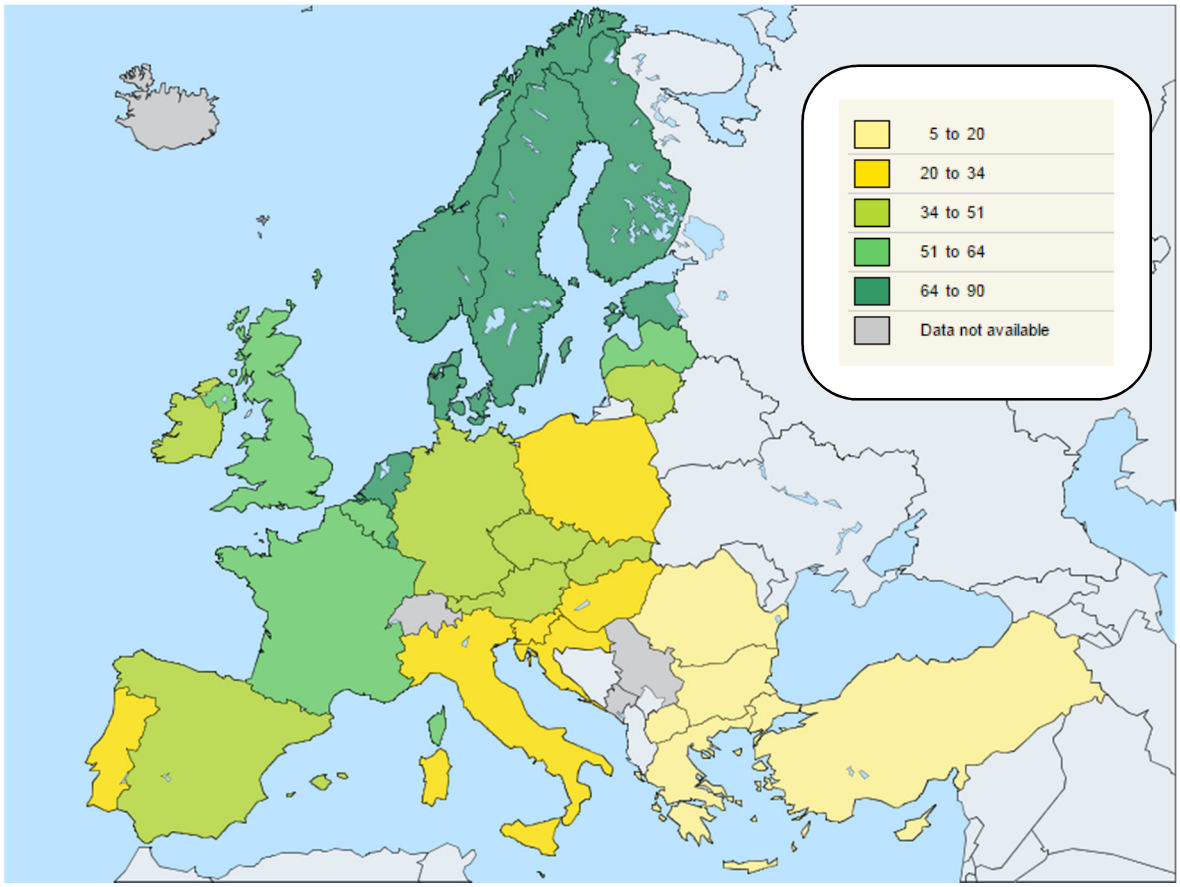
ZAP. ŠT.	IME BANKE	URL	E-BANČNIŠTVO ZA FIZIČNE OSEBE	VIR
1	ABANKA VIPA, d. d.	http://www.abanka.si/	Abanet	Banka Vipa, d. d., Spletna banka Abanet, 2016.
2	BANKA KOPER, d. d.	http://www.banka-koper.si/	Banka IN	Banka Koper, d. d., Spletna banka Banka@Net, 2016.
3	BANKA SPARKASSE, d. d.	http://www.sparkasse.si/	Net.Stik	Banka Sparkasse, d. d., Spletna bankaNet.stik, 2016.
5	DEŽELNA BANKA SLOVENIJE, d. d.	http://www.dbs.si/	DBS NET	Deželna banka Slovenije, d. d., Spletna banka DBS NET, 2016.
6	GORENJSKA BANKA, d. d.	http://www.gbkr.si/	E-banka link	Gorenjska banka, d. d., Spletna banka E-banka link, 2016.
7	HYPO ALPE-ADRIA-BANK, d. d.	http://www.hypo-alpe-adria.si/	HYPOnet	Hypo Alpe-Adria-Bank, d. d., Sapletna banka Hyponet, 2016.
8	NOVA KREDITNA BANKA MARIBOR, d. d.	http://www.nkbm.si	Bank@Net	Nova kreditna banka Maribor, d. d., Spletna banka Bank@Net, 2016.
9	NOVA LJUBLJANSKA BANKA,	http://www.nlb.si/	NLB klik	Nova Ljubljanska banka, d.d., Spletna Banka NLB klik, 2016.
10	POŠTNA BANKA SLOVENIJE, d. d.	http://www.pbs.si/	PBS.net	Poštna banka Slovenije, d. d., Spletna banka PBS.net, 2016.
11	RAIFFEISEN BANKA, d. d.	http://www.r-kb.si/	ReiffeisenNET	Raiffeisen Banka, d. d.; Spletna banka Reiffeisen Net, 2016.
13	SBERBANK D.D.	https://www.sberbank.si/	Sberbank spletna banka	Sberbank, d.d., Spletna banka Sberbanka spletna banka, 2016.
14	SKB BANKA, d. d.,	http://www.skb.si/	SKB NET	SKB banka, d. d., Spletna banka SKB NET, 2016.
15	UNICREDIT BANKA SLOVENIJE D.D.	http://www.unicreditbank.si/	Online b@nka	Unicredit banka Slovenije d.d., Spletna banka Online b@nka, 2016.

Ponudniki so prisiljeni izdelati čim kvalitetnejšo rešitev, ki naj bi bila varna, obenem pa naj bi zagotavljala enostavno funkcionalnost in preglednost. Slabost se kaže v nepovezanem razvoju – proizvajalci namreč ponujajo programske aplikacije, ki podpirajo različne programske vmesnike, kar uporabnikom, ki poslujejo z več bankami hkrati, otežuje delo, saj

so prisiljeni nameščati in vzdrževati več sistemov. Posledica je precej različna in bolj ali manj nezdružljiva programska oprema.

Na Sliki 45 so z barvno lestvico označeni odstotki internetnih uporabnikov, ki uporabljajo internetno bančništvo. Podatki so objavljeni na spletni strani Eurostata, ki združuje podatke, na podlagi pridobljenih podatkov s strani nacionalnih statističnih uradov. Slovenija se nahaja v rumenem območju, ki predstavlja 20–34%. V tem območju so nahajajo tudi nekaj sosednjih držav in sicer Hrvaška, Italija in Madžarska. Med najbolj aktivne uporabnike internetnega bančništva sodijo Skandinavske države. Ankete so bile izvedene v letu 2015 med posamezniki starimi od 16 do 74 let.

Slika 45:Odstotek internetnih uporabnikov, ki uporabljajo elektronsko bančništvo za leto 2015



Vir: European Commission, Uporaba interneta za namene internetnega bančništva, 2016.

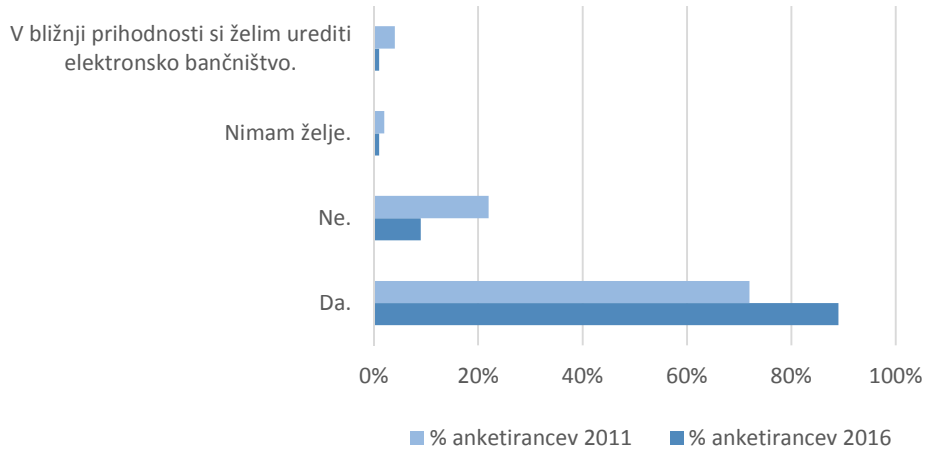
V nadaljevanju želim predstaviti pogled fizičnih oseb na varnost in uporabnost elektronskega bančništva. Anketo sem skušala pripraviti čim bolj preprosto, saj se mi zdi, da kratke in jasne ankete privedejo do dobrih rezultatov.

V okviru petih let sta bili izpeljani dve anketi – prva konec leta 2011 pred uvedbo UPN naloga in v času zametkov e-računa, druga pa je bila izvedena spomladi 2016, ko je UPN nalog že postal ustaljena praksa in so e-računi že prestali prve preizkuse. Anketi sem oblikovala s pomočjo spletnega programa za raziskave. Povezavo do ankete sem objavila na družabnem omrežju Facebook, posredovani pa sta bili tudi sodelavcem in znancem po e-pošti.

V letu 2011 je bilo v celoti izpolnjenih 220 anket, v letu 2016 pa 140. V prvi raziskavi je sodelovalo 61% žensk in 39% moških. Najštevilčnejša populacija, ki je sodelovala pri anketi, je 30–40 let in to kar z 54%. V drugi raziskavi je sodelovalo 70% žensk in 30% moških, najštevilčnejša populacija pa je prav tako 30–40 let s še več – 57%.

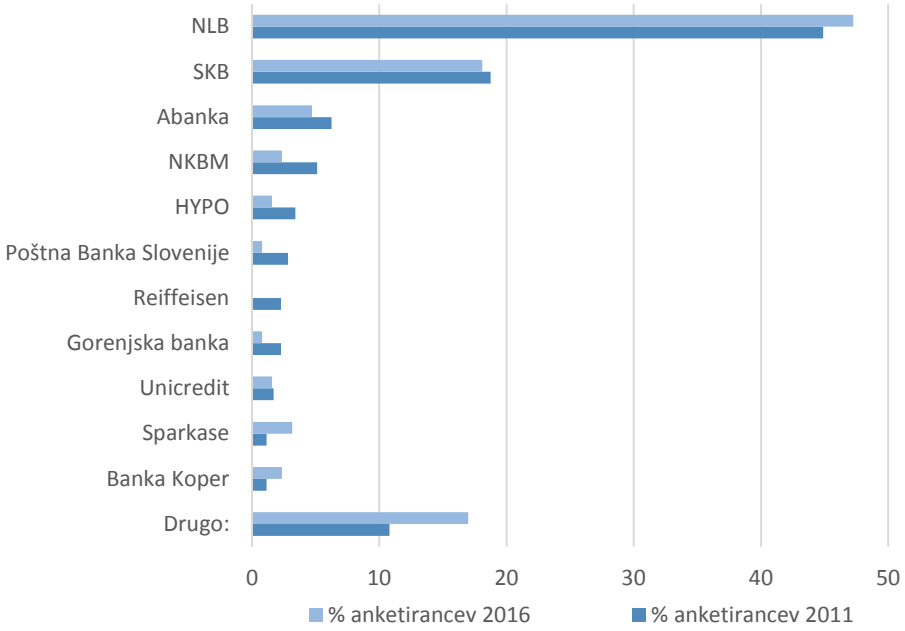
V prvi anketi (Slika 46) je 72% vprašanih že uporabljalo elektronsko banko, 4% anketirancev pa so si v bližnji prihodnosti želeli urediti elektronsko bančništvo. Zgolj 2%, kar pomeni 5 posameznikov, ni imelo želje po elektronskem bančništvu. V letu 2016 se je delež uporabnikov elektronskega bančništva zvišal na 89%. Ostaja 10% takšnih, ki elektronske banke nimajo in le 1% teh, ki nimajo želje po njegovi ureditvi.

Slika 46: Ali uporabljate elektronsko banko?



Pri izbiri ponudnika elektronskega bančništva se izbira Slovencev na prvih treh mestih ne spreminja. Še vedno stremijo k uporabi elektronskega bančništva naše največje banke NLB. Več kot za polovico zaostaja banka SKB. Abanka ter NKBM sta bili pri anketi v letu 2011 odstotkovno blizu, v letu 2016 pa je NKBM izgubila svoje privržence (Slika 47).

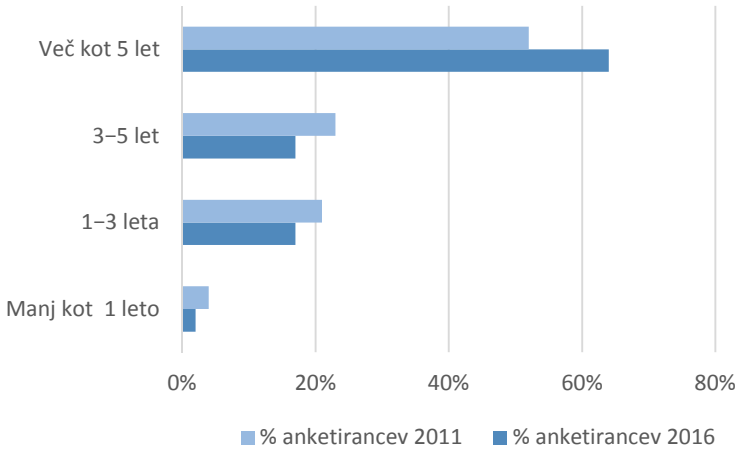
Slika 47: Katero spletno banko uporabljate?



V anketi iz leta 2011 je pod odgovorom ostalo 9% bank, ki niso posamezno opredeljene. Med izbor ostalo si je Unicredit banka prislužila 2 odgovora, vse ostale banke po enega. V letu 2016 se je 24% vprašanih opredelilo za ostale banke, ki niso bile naštete med podanimi odgovor. Pod dodatni opis izbire banke, so štirje anketiranci navedli Sparkasse, trije Delavsko hranilnico, dva banko BKS in ostale po enkrat. Anketiranci iz leta 2011 so uporabljali elektronsko bančništvo večih ponudnikov, saj so to zapisali pod drugo.

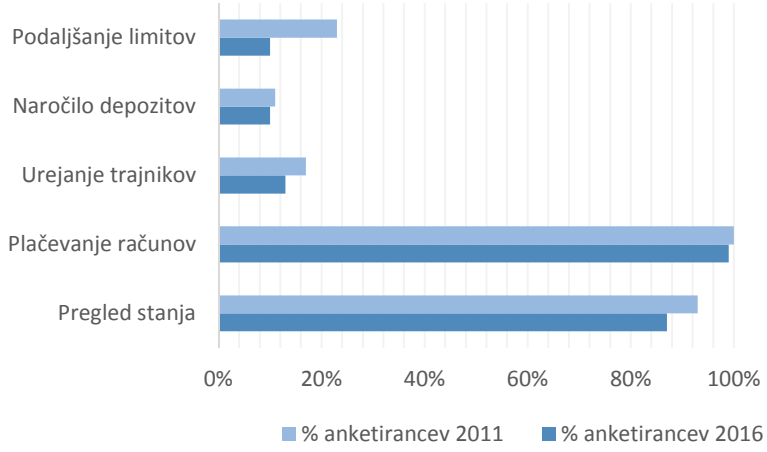
Velika večina anketirancev elektronsko banko uporablja že več kot 5 let (Slika 48), iz česar sledi, da bodo odgovori bolj podkrepljeni z navedbami o njihovi ustreznosti. Glede na to, da gre za isti nabor anketirancev je na spodnjem grafu prikazan porast tistih, ki banko uporabljajo več kot 5 let, saj je v času med anketama preteklo nekaj manj kot 5 let.

Slika 48: Koliko časa že uporabljate elektronsko banko?



Anketiranci so se odločili za elektronsko banko iz več razlogov, ki sem jih tudi ponudila med možnimi odgovori (Slika 49).

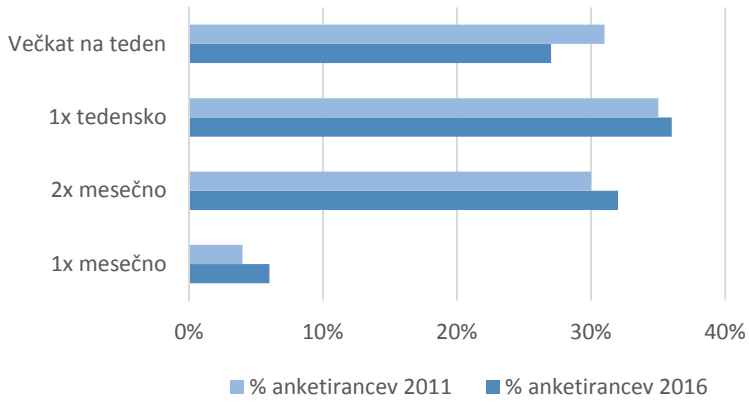
Slika 49: Za kakšne namene uporabljate elektronsko banko?



V anketi iz leta 2011 so se prav vsi uporabniki elektronske banke posluževali storitve plačevanja računov, od tega jih je 92% tudi redno pregledovalo stanje na osebnem računu. Podaljševanje limitov je na tretjem mestu z 23%. V anketi iz leta 2016 99% uporabnikov elektronsko bančništvo uporablja za plačevanje računov, medtem ko jih nekaj manj v primerjavi s preteklo anketo preverja stanje na računu. Kar za 13% se je v skoraj petih letih znižala storitev podaljševanja limita.

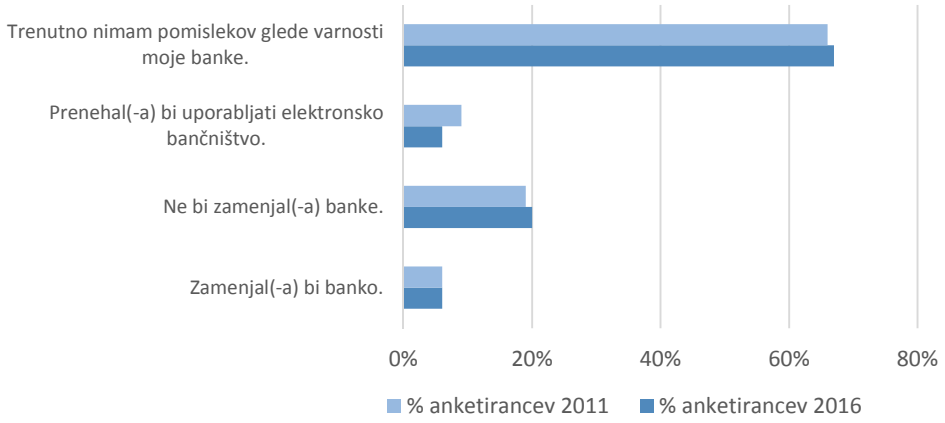
Najpogostejši odgovor je bil, da imajo banko na dosegu roke 24 ur na dan. Med večkrat izbranimi odgovori je tudi cenejša provizija. Tudi odgovor, ki izpostavlja čakanje na bančnem okencu ni zanemarljiv, saj se je 36% vprašanih v anketi iz leta 2016 odločilo zanj. V primerjavi z letom 2011 se je delež znižal za 13%.

Slika 50: Kako pogosto uporabljate elektronsko banko?



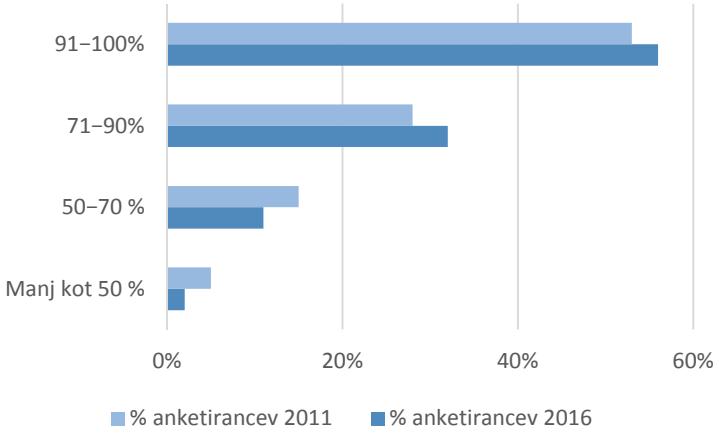
V letih 2011 in 2016 36% anketirancev elektronsko banko uporablja enkrat tedensko, sledijo pa jim uporabniki, ki banko uporabljajo dvakrat mesečno z 31% leta 2011 in 32% leta 2016. Znižanje je zaznati pri tistih z obiski elektronskega bančništva večkrat tedensko, in sicer iz 29% na 27%.

Slika 51: Ste razmišljali, da bi zaradi varnosti/nevarnosti zamenjali banko ali prenehali uporabljati elektronsko bančništvo?



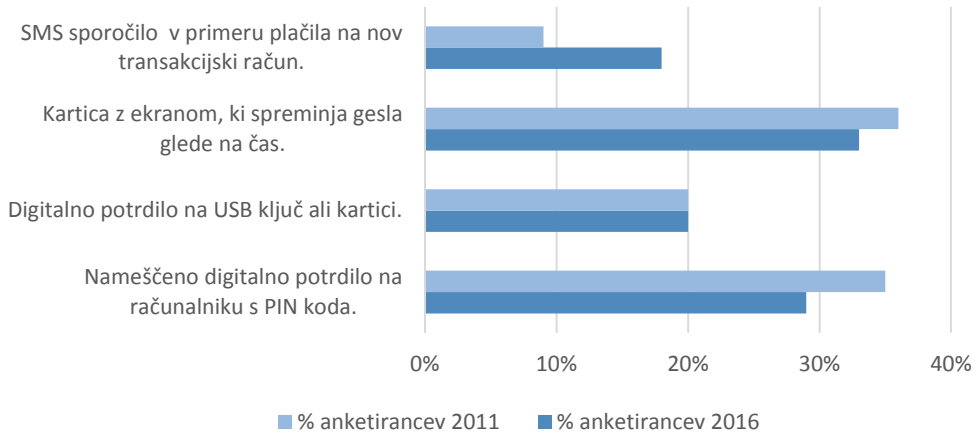
Več kot polovica vprašanih iz obeh let meni, da je njihova banka varna (90–100%) – leta 2011 53% in leta 2016 56%. Prav tako se je iz 28% na 32% povzpel delež tistih, ki menijo, da je njihova banka varna v 71–90%. Le 2% v letu 2016 meni, da je njihova banka varna v manj kot 50%. Leta 2011 je bilo takega mnenja 5% anketirancev.

Slika 52: Kako varna se vam zdi vaša elektronska banka?



V obeh anketah nekaj več kot 65% anketirancev, ki nimajo pomislekov glede prenehanja uporabe elektronskega bančništva. Približno 20% je takšnih, ki banke ne bi zamenjali, med 12 in 15% pa se giblje številka pri tistih, ki s svojo banko niso zadovoljni – prenehali bi uporabljati elektronsko bančništvo ali pa bi zamenjali banko.

Slika 53: Katero sredstvo se vam zdi najvarnejše?



Na podlagi rezultatov zadnjih dveh postavk je moč sklepati, da so uporabniki elektronskega bančništva vse bolj zadovoljni z varnostjo svoje banke in da nimajo pomislekov glede aplikacij, ki jih uporabljajo. Na Sliki 51 grafični prikaz o varnosti elektronske bake.

Uporabniki elektronske banke tako v letu 2011 kot v letu 2016 najbolj zaupajo karticam, ki generirajo enkratna gesla glede na čas. Podvojil se je delež tistih, ki v primeru plačila na nov transakcijski račun zaupajo prejetemu SMS sporočilu.

Dejstvo je, da se zlorabe v elektronskem bančništvu dogajajo, vendar 10% anketirancev za njih še ni slišalo. V obeh letih pri tej postavki ni bistvenih razlik. Na srečo je bil le 1% vprašanih vpleten v zlorabo, 4% anketirancev pa ima znance, ki so bili njene žrtve.

Med storitvami elektronskega bančništva je tudi e-račun, za katerega je 79% anketirancev iz leta 2016 že slišalo, 12% pravi, da redno mesečno prejemajo več e-računov, 6% pa se je na to storitev tudi naročilo. Leta 2011 je bil e-račun novost, vendar so bili anketiranci z njim enako seznanjeni. Vedeli so, da storitev e-račun obstaja, delež uporabnikov pa je enak kot pri rezultatih iz leta 2016.

Glede na to da me zanima uporabnost elektronske banke, bi bilo potrebno predstaviti tudi nekaj glavnih stroškov, ki nastanejo z njeno uporabo, in razlike v njihovi višini glede na plačilo pri bančnih okencih ali preko spletne banke.

Vse banke na območju Republike Slovenije so dolžne poročati Banki Slovenije o nadomestilih, ki jih zaračunavajo svojim komitentom in nekomitentom. Na spletni strani Banke Slovenije so nadomestila tudi javno objavljena.

Povzetek stroškov bom predstavila v več razpredelnicah. V prvi razpredelnici so prestavljeni stroški odprtja transakcijskega računa in pristop k elektronski banki ter redni mesečni stroški obeh storitev. Poleg sem dodala tudi storitev dviga gotovine na bankomatu, ki ga opravljamo večkrat mesečno. Vrednost (0) v tabeli pomeni, da banka ne zaračunava nadomestila za določeno storitev. Vrednost (-) pomeni, da banka posamezne storitve nima v ponudbi.

Tabela 6:Redni mesečni stroški v EUR

BANKA	OSNOVNI TRANSAKCIJSKI RAČUN		ELEKTRONSKA BANKA		BANKOMATI	
	ODPRTJE	VODENJE (MESEČNO)	OSNOVNA REŠITEV – PRISTOP	(OSNOVNA REŠITEV) – UPORABA (MESEČNO)	LASTNI	DRUGA BANKA - V DRŽAVI IN ČEZMEJNO V EUR
ABANKA VIPA d. d.	0,00	2,15	5,00	0,61	0,00	0,50
BANKA CELJE d. d.	0,00	2,15	27,50	0,61	0,00	0,50
BANKA KOPER d. d.	0,00	2,20	-	1,07	0,00	0,54
BANKA SPARKASSE d. d.	0,00	2,14	28,00	0,00	0,00	0,00
BKS BANK AG	0,00	1,70	16,00	0,00	0,00	0,00
DELAVSKA HRANILNICA d. d.	0,00	1,25	0,00	0,42	0,00	0,00
DEŽELNA BANKA SLOVENIJE d. d.	0,00	2,05	19,00	0,60	0,00	0,45
GORENJSKA BANKA d. d.	0,00	2,12	24,00	0,92	0,00	0,49; (samo na nekaterih bankomatih v neposredni bližini bankomatov Gorenjske banke)
HRANILNICA IN POSOJILNICA VIPAVA d. d.	0,00	1,56	0,00	0,00	-	0,00
HRANILNICA LON d. d.	0,00	2,05	10,90	0,49	0,00	0,30
HYPO ALPE-ADRIA-BANK d. d.	0,00	2,15	27,50	0,56	0,00	0,52
NLB d. d.	0,00	2,30	27,28	0,75	0,00	0,53
NOVA KBM d. d.	0,00	2,10	0,00	0,50	0,00	0,48
POŠTNA BANKA SLOVENIJE d. d.	0,00	2,10	26,00	0,58	0,00 (velja tudi za bankomate v lasti NKBM)	0,48
RAIFFEISEN BANKA d. d.	0,00	od 2,99 EUR do14,90 EUR (odvisno od paketa)	20,86	1,25	0,00	0,00
SBERBANK BANKA d. d.	0,00	2,79	22,50	0,00	0,00	0,47 (od 4. dviga dalje) - veljavnost od 1.2.2016
SKB BANKA d. d.	0,00	2,20	25,00	0,70	0,00	0,52
UNICREDIT BANKA SLOVENIJA d. d.	0,00	1,75	0,00	0,65	0,00	0,55

Vir: Banka Slovenije, Pregled nadomestil za opravljanje plačilnih storitev za imetnike transakcijskih računov – potrošnike (rezidente), 2016.

Odprtje računa vse banke opravijo brezplačno, se pa razlikuje mesečno nadomestilo za vodenje računa. Najnižji mesečni strošek za vodenje računa ima Delavska Hranilnica, najvišje pa Sberbank. Za uporabo elektronskega bančništva je na začetku potrebno plačati pristopnino, ki je pri nekaterih bankah brezplačna, in sicer pri Unicredit banki, Novi KBM

in Delavski hranilnici. Najvišjo pristopnino morajo plačati uporabniki banke Sparkasse, in sicer 28 EUR, so pa zaradi tega upravičeni plačevanja mesečnih stroškov uporabe osnovnega elektronskega paketa. V Sloveniji je veriga bankomatov zelo močna, se pa vseeno zgodi, da bankomata naše matične banke ni blizu, zato sem v tabelo dodala tudi stroške, ki jih plačamo, če dvigujemo na bankomatih drugih bank. Najdražje nadomestilo (0,55 EUR) zaračuna Unicredit banka Slovenija, nekatere banke pa to storitev še vedno ponujajo brezplačno.

Leta 2009 so v Banki Slovenije začeli s pripravo analize za nadomestila bančnih storitev in izračunom stroškov košaric plačilnih storitev. Tudi po preteku šestih let še vedno uporabljajo enako metodologijo, kar omogoča primerjavo med posameznimi leti. V analizo so skupno vključe 3 hranilnice in 18 bank. Tudi pri Zvezi potrošnikov Slovenije (ZPS) letno opravljajo izračun košarice plačilnih storitev, ki pa se razlikuje od prvega. Košarica Banke Slovenije je izračunana na podlagi plačil fizičnih oseb, pri ZPS pa ga pripravijo v sodelovanju z nekaterimi bančnimi strokovnjaki. Primerjave so narejene za tradicionalne kupce in kupce, ki uporabljajo e-bančništvo.

Tabela 7: Ponudba plačilnih storitev po košaricah v letu 2015

FO								
Ponudnik plačilnih storitev	**Košarica BS**				**Košarica ZPS**			
	Tradicionalni komitent	**Indeks**	**e-komitent**	**Indeks**	**Tradicionalni komitent**	**Indeks**	**e-komitent**	**Indeks**
Abanka d.d.	101,25	108,61	49,8	110,41	183,24	110,47	77,4	115,71
Banka Celje d.d.	101,25	108,61	49,8	110,41	183,24	110,47	77,4	115,71
Banka Koper d.d.	110,69	118,74	52,24	115,82	201,36	121,4	81,12	121,27
Banka Sparkasse d.d.	94,77	101,66	42,27	93,71	165,6	99,84	57,6	86,11
BKS Bank AG	86,13	92,39	36,43	80,77	152,64	92,02	50,4	75,35
Delavska hranilnica d.d.	27,94	29,97	24,44	54,18	39,96	24,09	32,76	48,98
Deželna banka Slovenije d.d.	62,25	66,78	41,25	91,45	98,28	59,25	55,08	82,34
Gorenjska banka d.d.	106,28	114,01	48,88	108,37	193,32	116,55	75,24	112,48
Hranilnica LON d.d.	65,96	70,76	43,91	97,35	110,52	66,63	65,16	97,41
Hranilnica in posojilnica Vipava d.d.*	46,72	50,12	29,22	64,78	76,32	46,01	40,32	60,28
Hypo Alpe-Adria-Bank d.d.	112,75	120,95	50,1	111,07	210,96	127,18	82,08	122,71
Nova KBM d.d.	111,23	119,32	49,28	109,26	213,6	128,77	86,16	128,81
Nova Ljubljanska banka d.d.	106,89	114,66	50,89	112,82	197,88	119,3	82,68	123,6
Poštna banka Slovenije d.d.	71,83	77,05	48,38	107,26	123,6	74,52	75,36	112,66
Probanka d.d.	109,41	117,37	42,91	95,13	196,68	118,57	59,88	89,52
Raiffeisen Banka d.d.	96,33	103,34	50,13	111,14	156,12	94,12	61,08	91,31
SKB banka d.d.	110,44	118,47	51,64	114,49	204,24	123,13	83,28	124,5
UniCredit Banka Slovenija d.d.	102,5	109,95	43	95,33	181,8	109,6	59,4	88,8
Sberbank banka d.d.	146,58	157,24	52,43	116,24	262,2	158,07	68,52	102,44
POVPREČJE	**93,22**	**100**	**45,11**	**100**	**165,87**	**100**	**66,89**	**100**

Vir: Banka Slovenije, Analiza nadomesti bank in hranilnic za plačilne storitve in izračun stroškov košaric plačilnih storitev – 2015, 2016

Zadnja analiza je bila objavljena v marcu 2016 za leto 2015. Izkazalo se je, da je najugodnejša Delavska hranilnica in da ni večjih razlik med tradicionalnim in e-komitentom. Po metodologiji Banke Slovenije je najdražja banka Sberbank, in sicer v primerjavi tradicionalnim komitentom Delavske hranilnice za občutnih 119 EUR. Razlika med e-komitentoma obeh bank je slabih 28 eur. Velika razlika je že znotraj same banke Sberbank, saj e-komitent v primerjavi s tradicionalnim komitentom privarčuje skoraj 95 EUR. Podrobnejše rezultati po posameznih bankah so prikazani v Tabeli 7 (Banka Slovenije, 2016).

Na podlagi izbranih košaric me je zanimalo, kakšne so cene za posamezne storitve pri posameznih bankah. V Tabeli 8 so prikazani stroški za interna plačilo, torej plačila, ki se vršijo med komitenti posamezne banke, v Tabeli 9 pa eksterna plačila, ki se vršijo med komitenti različnih bank. Pri Novi KBM in Sberbank so bili stroški za eksterna plačilo občutno višji kot pri ostalih bankah, zato sem jih dodatno preverila in dobila točne zneske.
Ker v magistrskem delu primerjam klasični način poslovanja s sodobnimi bančnimi potmi, sem izpostavila tudi primerjavo cen na bančnem okencu in elektronske banke. Potrebno je opredeliti še kratici iz tabele, in sicer f. o., ki se uporablja za fizične osebe in p. o, ki se uporablja za pravne osebe.

Banke svoja plačila delijo na velika in mala. Meja med njimi je 50.000,00 EUR. Če komitenti nakazujejo velika plačila, so nadomestila načeloma višja, le pri nekaterih bankah ostajajo nespremenjena. NLB ima najvišje cene pri velikih internih plačilih, tako na okencu kot pri poslovanju preko elektronske banke. Nadomestilo za plačilo na bančnem okencu v primeru plačevanja na račun pravne osebe znaša 7,44 EUR, preko elektronske banke pa 5,31 EUR. Prav tako je med dražjimi tudi Hypo Alpe Adria, pri kateri so stroški plačil na okencu 7,15 EUR oz. 4,95 EUR preko elektronske banke. Razlika v stroških znaša dobra 2 evra.

Fizične osebe redno uporabljamo mala plačila. V sklopu iste banke na bančnem okencu plačamo približno 0,6 EUR pri Delavski hranilnici in posojilnici Vipava in 2,18 EUR na Hypo Alpe Adria, medtem ko nadomestilo za plačilo internega naloga pri elektronski banki v večini primerov ni višje od 0,4 EUR, če denar nakazujemo na transakcijski račun podjetja.

Nalogi, ki jih plačujemo prejemnikom pri drugi banki so dražji kot interni, in sicer se cene za malo plačilo na bančnem okenc gibljejo med 1,59 EUR pri Reiffeisen banki do 6 EUR pri Hranilnici in posojilnici Vipava. Nadomestila za mala nakazila preko elektronske banke se gibljejo od 0,2 do 0,42 EUR. Najugodnejša so pri Delavski hranilnici, najdražja pa pri banki SKB.

V Tabeli 8 so označena, nežno modra okenca, za najugodnejšo storitev v sklopu internih in ekternih plačil, temnejša modra pa označuje najvišjo ceno, ki jo plačate za izvedbo določene storitve na izbrani banki.

Tabela 8: Interna plačila v EUR

BANKA	KREDITNA PLAČILA V DRŽAVI – OKENCE				PLAČILA ELEKTRONSKA BANKA			TRAJNI NALOGI		DIREKTNE BREMENITVE	
	INTERNO – VELIKO	INTERNO – MALO	NUJNI NALOG – INTERNO	UPN Z OCR IN IZJAVO – INTERNO	INTERNO – VELIKO	INTERNO – MALO	NUJNI NALOG – INTERNO	INTERNO	OBVESTILO O NEIZVRŠITVI PLAČILA	INTERNO	OBVESTILO O NEIZVRŠITVI PLAČILA
ABANKA VIPA d. d.	na TRR f.o. 0,00, na TRR p.o. 1,85	na TRR f.o. 0,00, na TRR p.o. 1,85	6,50	1,20	na TRR FO 0,00, na TRR PO 0,38	na TRR FO 0,00, na TRR PO 0,38	-	0,00	2,00	0,26	2,00
BANKA CELJE d. d.	1,85	1,85	7,00	1,85	0,38	0,38	0,38	0,00	2,00	0,26	2,00
BANKA KOPER d. d.	na TRR f.o. 0,35, na TRR p.o. 1,65	na TRR f.o. 0,35, na TRR p.o. 1,65	na TRR f.o. 0,35, na TRR p.o. 1,65	na TRR f.o. 0,35, na TRR p.o. 1,65	na TRR FO 0,35, na TRR PO 0,38	na TRR FO 0,35, na TRR PO 0,38	0,40	0,00	2,05	0,33	2,05
BANKA SPARKASSE d. d.	1,20	1,20	1,20	1,20	0,00	0,00	0,00	0,00	1,69	0,00	1,69
BKS BANK AG	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	2,00	0,00	2,00
DELAVSKA HRANILNICA d. d.	0,00	0,00	0,00	0,00	0,00	0,00	-	0,00	1,00	0,12	1,00
DEŽELNA BANKA SLOVENIJE d.d.	na TRR f.o. 0,00, na TRR p.o. 0,50	na TRR f.o. 0,00, na TRR p.o. 0,50	-	na TRR f.o. 0,00, na TRR p.o. 0,50	0,00	0,00	0,00	0,00	1,00	0,00	1,00
GORENJSKA BANKA d. d.	6,5 na TRR p.o.; 0 na OSR	1,99 na TRR p.o.; 0 na OSR	-	1,99 na TRR p.o.; 0 na OSR	na OSR 0; na TRR pr.os. 0,35	na OSR 0; na TRR pr.os. 0,35	-	0,00	2,15	0,00	2,15
HRANILNICA IN POSOJILNICA VIPAVA d.d.	0,60	0,60	0,60	0,60	0,00	0,00	0,00	0,00	0,00	0,00	0,00
HRANILNICA LON d. d.	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,65	0,00	1,65
HYPO ALPE-ADRIA-BANK d. d.	na trr f.o.0,00-na trr p.o.7,15	na trr f.o. 0,0 na trr p.o.2,18	-	trr f.o.0,00 trr p.o.2,18	trr f.o.0,00- trr p.o.4,95	na trr f.o.o. 0,00- na trr p.o.0,39	-	0,00	1,35	0,23	1,35
NLB d. d.	na TRR f.o. 0,00, na TRR p.o. 7,44	na TRR f.o. 0,00, na TRR p.o. 2,00	na TRR f.o. 0,00, na TRR p.o. 7,44	2,00	na TRR f.o 0,00, na TRR p.o. 5,31	na TRR f.o. 0,00, na TRR p.o. 0,38	na TRR f.o. 0,00, na TRR p.o. 5,31	0,00	2,42	0,24	2,42
NOVA KBM d. d.	na TRR f.o. 0,00, na TRR p.o. 1,90	na TRR f.o. 0,00, na TRR p.o. 1,90	na TRR f.o. 0,00, na TRR p.o. 1,90	na TRR f.o. 0,00, na TRR p.o. 1,90	0,35	0,35	0,35	f.o. 0,00; p.o. 0,81	-	0,23	2,14
POŠTNA BANKA SLOVENIJE d. d.	5,36	do vrednosti 98,00 EUR 1,05; nad 98,00 EUR do 501,00 EUR 1,07 % od vrednosti transakcij; nad 501,00 EUR 5,36	-	1,05	na TRR f. o. 0,00; na TRR p. o. 0,35	na TRR f. o. 0,00; na TRR p. o. 0,35	na TRR f. o. 0,00; na TRR p. o. 0,35	0,00	2,14	0,23	2,14
RAIFFEISEN BANKA d. d.	3,99	1,29	1,29	1,29	0,00	0,00	-	0,00	1,10	0,00	1,10
SBERBANK BANKA d. d.	1,10	1,10	0,00	1,10	0,00	0,00	0,00	0,23	0,99	0,23	0,99
SKB BANKA d. d.	2,10	2,03	7,00	2,03	0,00 - osebni račun; 0,40 - poslovni račun	0,00 - osebni račun; 0,40 - poslovni račun	3,50	0,00	4,50	0,00	4,50
UNICREDIT BANKA SLOVENIJA d. d.	2,10	2,10	12,00	2,10	0,40	0,40	6,60	0,40	4,50	0,40	4,50

Vir: Banka Slovenije, Pregled nadomestil za opravljanje plačilnih storitev za imetnike transakcijskih računov – potrošnike (rezidente), 2016.

Tabela 9: Eksterna plačila v EUR

BANKA	KREDITNA PLAČILA V DRŽAVI -OKENCE				PLAČILA ELEKTRONSKA BANKA			TRAJNI NALOGI		DIREKTNE BREMENITVE	
	EKSTERNO – VELIKO	EKSTERNO – MALO	NUJNI NALOG – EKSTERNO	UPN ZOCR IN IZJAVO – EKSTERNO	EKSTERNO – VELIKO	EKSTERNO – MALO	NUJNI NALOG – EKSTERNO	EKSTERNI TRAJNI NALOGI	OBVESTILO O NEIZVRŠITVI PLAČILA	EKSTERNO	OBVESTILO O NEIZVRŠITVI PLAČILA
ABANKA VIPA d. d.	7,00	1,85	7,00	1,20	4,00	0,38	4,00	0,26	2,00	0,26	2,00
BANKA CELJE d. d.	7,00	1,85	7,00	1,85	5,85	0,38	5,85	0,26	2,00	0,26	2,00
BANKA KOPER d. d.	7,00	2,10	7,00	do 50.000 EUR 2,10, sicer 7,00	5,50	0,40	5,50	0,33	2,05	0,33	2,05
BANKA SPARKASSE d. d.	5,10	1,85	5,10	1,85	3,10	0,35	3,10	0,35	1,69	0,21	1,69
BKS BANK AG	4,80	1,75	6,60	1,60	2,60	0,33	3,20	0,30	2,00	0,22	2,00
DELAVSKA HRANILNICA d. d.	3,40	do 460,00 EUR 0,30 EUR, sicer 0,16% (max. 2,00)	do 2250 EUR 3,40, sicer 0,16%	do 460,00 EUR 0,30%, sicer 0,16% (max. 2,00)	2,00	0,20	2,00	0,00	1,00	0,12	1,00
DEŽELNA BANKA SLOVENIJE d. d.	7,50	plačila do 200,00 EUR 1,20; plačila od 200,01 do 500,00 EUR 1,60; plačila nad 500,00 EUR 5,00	7,50	plačila do 200,00 EUR 1,20 ; plačila od 200,01 do 500,00 EUR 1,60 ; plačila nad 500,00 EUR 5,00	2,50	0,35	2,50	0,22 (ročni 0,95)	1,00	0,22 (ročni 0,95)	1,00
GORENJSKA BANKA d. d.	6,50	1,99	-	1,99	0,35	0,35	-	0,29	2,15	0,29	2,15
HRANILNICA IN POSOJILNICA VIPAVA d. d.	6,00	do vrednosti 1000,00EUR 0,80, sicer 0,16% (max.6,00)	6,00	do 1000,00EUR 0,80, sicer 0,16% (max 6,00)	0,30	0,30	2,25	0,00	0,00	0,00	0,00
HRANILNICA LON d. d.	6,45	do 500,00 EUR: od 0,31 EUR do 0,96 EUR, sicer 3,13 EUR	do 87,78 EUR 4,15 sicer 6,45	0,85	0,33	0,33	2,30	0,28	1,65	0,22	1,65
HYPO ALPE-ADRIA-BANK d. d.	7,15	2,18	7,15	2,18	4,95	0,39	4,95	0,56	1,35	0,23	1,35
NLB d. d.	7,44	2,00	na TRR f.o. 0,00, na TRR p.o. 7,44	2,00	5,31	0,38	na TRR f.o. 0,00, na TRR p.o. 5,31	0,56	2,42	0,24	2,42
NOVA KBM d. d.	6,75	2,15	9,50	2,15	5,00	0,38	7,50	1,13	-	0,23	2,14
POŠTNA BANKA SLOVENIJE d. d.	5,36	do vrednosti 98,00 EUR 1,05; nad 98,00 EUR do 501,00 EUR 1,07 % od vrednosti transakcij; nad 501,00 EUR 5,36	-	1,05	5,00	0,38	5,00	0,23 (ročni 1% od zneska (min 1,00; max 4,00))	2,14	SEPA izvršitev 0,23	2,14
RAIFFEISEN BANKA d. d.	4,25	1,59	4,25	1,59	3,11	0,27	-	0,24	1,10	0,24	1,10
SBERBANK BANKA d. d.	10,50	do vrednosti 1000,00EUR 2,6; do 50.000 7,7 eur	dodatno 2,00 (samo v državi)	do vrednosti 1000,00EUR 2,6; do 50.000 7,7 eur	2,50	0,41	dodatno 2,00 (samo v državi)	0,23	0,99	0,23	0,99
SKB BANKA d. d.	7,00	2,10	7,00	2,10	3,50	0,42	3,50	0,48	4,50	0,26	4,50
UNICREDIT BANKA SLOVENIJA d. d.	2,10	2,10	12,00 (samo v državi)	2,10	0,40	0,40	6,60 (samo v državi)	0,40	4,50	0,40	4,50

Vir: Banka Slovenije, Pregled nadomestil za opravljanje plačilnih storitev za imetnike transakcijskih računov – potrošnike (rezidente), 2016.

SKLEP

Elektronsko bančništvo je v današnjem svetu nepogrešljivo, in morda je nepotrebno le še za nekaj posameznikov, ki niso seznanjeni s storitvami, ki jih elektronsko bančništvo omogoča. V današnjem času nam je odveč, če je potrebno iskati parkirni prostor ter čakati v vrsti pred bančnim okencem. Pri tem je potrebno tudi preračunati stroške parkirnine in provizije na banki, ki je občutno višja od tiste v spletni banki – se nam vse to res splača? Odgovor je verjetno, da ne časovno in tudi ne finančno. Bolje bi bilo, da ta denar vložimo v elektronsko bančništvo in si s tem kadarkoli zagotovimo pregled stanja na našem računu.

V primerjavi s preteklostjo, se je zaupanje v varnost elektronskega bančništva povečalo, kar pa ne pomeni da dvom ni več prisoten. Zloraba se nam lahko zgodi kadarkoli, bodisi elektronska, bodisi fizična. Strokovnjaki, ki so specializirani za varnost elektronske banke, skušajo biti korak pred zlikavci in jim preprečiti dostop do našega denarja.

Cilj magistrskega dela je bil preučiti varnostno tehnologijo v elektronskem poslovanju. Ugotovljeno je bilo, da je sistem varen, ko so koristi vdora v sistem nižje kot sami stroški. Med šibkejšo zaščito varovanja sodijo gesla, saj so slabo izbrana zaradi lažje zapomnitve, kar seveda pomeni, da jih je tudi lažje razkrinkati. Najzanesljivejša metoda za identifikaijo posameznika so biometrične metode, pri katerih se uporablja identifikacija s pomočjo prstnega odtisa, glasu, dela očesa ipd. Žal so z njihovo uporabo povezani visoki stroški. V elektronskem poslovanju se največ uporablja digitalni podpis.

Nevarnosti uporabnikom prežijo povsod, bodisi za domačim računalnikom bodisi pri uporabi bančnih avtomatov, zato sem predstavila skimming in phishing. Uporabniki se morajo zavedati, da za svoj denar v veliki meri lahko poskrbijo sami. Pri dvigu denarja na bankomatu je potrebno prekriti številčnico z roko, da v primeru skimming naprav ni dopuščena možnost kraje številke PIN. Potrebno je biti tudi pozoren na vse nenavadne spremembe spletne strani naše banke, saj gre lahko za lažno spletno stran. Vsakršna spletna zahteva ponudnika bančnih storitev o našem razkritju osebnih podatkov je sporna. Phishing napadi so prvi večji porast dosegli leta 2012, ko se je število napadov iz 61 povzpelo na 139. V naslednjih letih se je število prevar samo še povečevalo.

Predstavljene so bile štiri zlorabe, ki so se razrešile, saj so bili vse sporne transakcije po določenem obdobju povrnjene na račune komitentov. Vsekakor pa je neugodno, če v nekem trenutku ostaneš brez denarja na računu, odvzamejo ti bančno kartico ali odpeljejo računalnik. Vsi štirje sogovorniki so po neljubih dogodkih dodatno pozorni na vse nenavadne spremembe, ki bi jih lahko stale lastnine.

V sklopu anket sem prišla do spoznanj, da se povečuje število uporabnikov najmlajše in najstarejše generacije. Mladi odrastejo s sodobno tehniko, generacija nad 50 let pa želi iti v

korak s časom. Število uporabnikov elektronskega bančništva se je v petih letih povečalo, ostaja le še peščica, ki vztraja pri klasičnem bančnem poslovanju in si ne želi pristopiti k novi obliki. Uporabniki elektronske banke zaupajo svoji banki bolj kot v preteklosti. Prav gotovo so k temu pripomogli dodatni varnostni elementi, ki jih ponujajo banke. Eden izmed njih je tudi varnostno SMS sporočilo, ki ga uporabnik prejme za vsa plačila ali dvige na bankomatu in tako lahko v trenutku izve, če je slučajno prišlo do zlorabe na bančnem računu. Tudi sama sem se, v obdobju pisanja, naročila na to storitev. Shranjena sporočila lahko služijo tudi kot hiter pregled odlivov z bančnega računa.

Vse več bank v Sloveniji stremi k dodatnim varnostnim ukrepom, ki bi uporabnikom omogočili čim varnejše poslovanje, kot so dnevni limit porabe, dodatna kontrola ob plačilu na nov transakcijski račun, SMS sporočilo ob vstopu v elektronsko banko in osebno sporočilo, ki ga vidite samo, če vstopate na pravo povezavo.

Uvedba e-računa je velika prednost za podjetja, ki izdajajo račune, saj se izognejo tiskanju, kuvertiranju in pošiljanju po klasični pošti. Prejemnik, podjetje ali fizična oseba, dobi e-račun na elektronski naslov ali v elektronsko banko, kjer nalog lahko brez dodatnih vnosov plača.

K izboljšanju plačilnega sistema v Evropi je pripomoglo okolje SEPA, ki uporabnikom plačilnih storitev omogoča enake pogoje znotraj države ali med državami svojega območja. Kreditna plačila omogočajo prenos sredstev z eno samo transakcijo na račun v enem samem dnevu zunaj ali znotraj države. Direktna obremenitev SEPA omogoča podjetju ali posamezniku v eni držav, neposredno obremenitev računa v drugi državi. Evropskim trgovcem SEPA plačilne kartice omogočajo veliko stopnjo varnosti za vse kartice izdane kjerkoli v Evropi.

Na področju plačevanja s plastičnimi karticami se porajajo nova vprašanja in dvomi. Pojavile so se brezstične kartice, ki omogočajo plačevanje brez vnosa številke PIN in dotika POS terminala. Strokovnjaki ne dvomijo in pojasnjujejo, da je z njimi varnost na najvišjem nivoju. Ob samem plačilu se s kartice preberejo le določeni podatki, ki pa goljufom ne zadostujejo, da bi izvedli zlorabo. V primeru kraje kartice lahko pride le do manjše zlorabe, saj ob dosegu skupnega limita POS terminal zahteva vnos PIN številke.

Tudi mobilno bančništvo in aplikacija Hall mBills so med storitvami prihodnosti, saj vsi stremimo (stremijo) k dostopnosti na vsakem koraku bodisi za službene bodisi za osebne namene. Če že ne sami, od nas to zahtevajo nadrejeni, ki želijo sodoben način poslovanja. Mobilne telefone (t.i. pametne telefone) nosimo povsod, za uporabo sodobnih elektronskih poti pa smo kljub temu odvisni od internetne povezave ali prenosa podatkov.

Če vse funkcionira, se lahko poslužujemo enostavnega plačevanje računov, s samim skeniranjem. Skener prepozna podatkov na računu in nam tako prihrani nevšečnosti pri prepisovanju podatkov in tudi manjšo verjetnost napak.

Elektronsko bančništvo napreduje – povečuje nivoje varnosti in skrbi, da uporabnikom omogoča enostavnejša in hitrejša plačila v domačem in tujem bančnem prostoru.

LITERATURA IN VIRI

1. A.Č. (2011, 25. november). *Tatovi bančnih PIN-številk spet na delu*. Najdeno 5. marca 2016 na spletnem naslovu http://www.rtvslo.si/slovenija/tatovi-bancnih-pin-stevilk-spet-na-delu/271429
2. Abanka vipa d.d. (2016). *Spletna banka Abanet*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.abanka.si/e-poti/spletna-banka-abanet
3. Banka Celje d.d. (2016). *Elektronsko bančništvo*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.banka-celje.si/osebne-finance/trzne-poti/elektronsko-bancnistvo
4. Banka Koper d.d. (2006). *Primer pametne kartice* (interno gradivo). Koper: Banka Koper d.d.
5. Banka Koper d.d. (2016). *Spletna banka Banka IN*. Najdeno 29. januarja 2016 na spletnem naslovu
6. Banka Slovenija d.d. (2016). *Banke v Sloveniji.* Najdeno 28. januarja 2016 na spletnem naslovu http://www.bsi.si/nadzor-bank.asp?MapaId=521
7. Banka Slovenije (2016). *Pregled nadomestil za opravljanje plačilnih storitev*. Najdeno 5. marca 2016 na spletnem naslovu http://www.bsi.si/orodja/tarife-ps.asp?MapaId=1439#tabela
8. Banka Slovenije d.d. (2016). *Enotna struktura transakcijskega računa*. Najdeno 28. april 2016 na spletnem naslovu https://www.bsi.si/placilni-sistemi.asp?MapaId=1452
9. Banka Sparkasse d.d. (2016). *Net.Stik.* Najdeno 29. januarja 2016 na spletnem naslovu http://www.sparkasse.si/netstik
10. Bankart d.d. (2016). *SEPA, E-račun.* Najdeno 5. marca 2016 na spletnem naslovu http://www.bankart.si/si/ponudba/simp/
11. Bankart d.o.o. (2011). *Bankart v sodelovanju z bankami vzpostavil enotni sistem za izmenjavo računov v elektronski obliki.* Najdeno 15. marca 2016 na spletnem naslovu http://www.bankart.si/si/novice/2011/bankart-v-sodelovanju-z-bankami-vzpostavil-enotni-sistem-za-izmenjavo-racunov-v-elektronski-obliki/
12. Bankart d.o.o. (2016). *Varnostno SMS sporočilo*. Najdeno 28. januarja 2016 na spletnem naslovu http://www.bankart.si/si/ponudba/upravljanje-mreze-bancnih-avtomatov/varnostno-sms-sporocilo/
13. Bankart d.o.o. (2016). *Register izdajateljev računov*. Najdeno 18. maja 2016 na spletnem naslovu http://www.bankart.si/si/ponudba/simp/register-e-racunov/
14. Belič, I., & Lesjak, B. (2006). Varovanje informacijskih sistemov pred kriminalnimi napadi. *Zbornik Kriminalni napadi na premoženje gospodarskih subjektov*. Maribor: Fakulteta za policijsko – varnostne vede
15. Bizovičar, M. (2014, 27. oktober). Brezstična kartica bo vsaj enako varna, kot je čipna. *Delo.* Najdeno 5. marca 2016 na spletnem naslovu http://www.delo.si/gospodarstvo/brezsticna-kartica-bo-vsaj-enako-varna-kot-je-cipna.html

16. Bračun, F. (1997*).* Praktične izkušnje pri uvajanju e-bančništva. *Zbornik Banke in tveganje* (str. 149–154). Portorož: Zveza ekonomistov Slovenije.
17. Bračun, F., & Cetinski A. (1998). *Elektronsko poslovanje v SKB banki, d.d* Organizacija, 31(3), 144.
18. Bratina, M. (2005*). Uporaba tehnologije elektronskega poslovanja z vidika bančnih storitev* (diplomsko delo). Maribor: Ekonomsko – poslovna fakulteta
19. Cetinski, A. (1999). *Elektronsko poslovanje v bančništvu*. Organizacija, 32 (3), 149–152.
20. Datalab d.d. (b.l). *Primerjava klasičnega in e-računa.* Najdeno 15. marca 2016 na spletnem naslovu ftp://ftp.datalab.si/Marketing/Brosure/Brosura_eRacun_Nov_2014_B_pop_WEB_2.pdf
21. Datastudio d.o.o. (2016). *Pot klasičnega in e-računa*. Najdeno 15. marca 2016 na spletnem naslovu http://www.datastudio.si/e-racuni/
22. European Commission (2016). Uporaba interneta za namene internetnega bančništva. Najdeno 30. junija 2016 na spletnem naslovu http://ec.europa.eu/eurostat/tgm/mapToolClosed.do?tab=map&init=1&plugin=0&language=en&pcode=tin00099&toolbox=types
23. European Peyment council (2016). *SEPA Scheme Countries and Territories.* Najdeno 5. marca 2016 na spletnem naslovu http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/map-of-sepa-scheme-countries-and-territories/epc064-16-map-of-sepa-countries-and-territories/
24. Gorenjska banka d.d. (2016). *Spletno bančništvo*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.gbkr.si/osebne-finance/spletno-bancnistvo-29/
25. Halcom d.d. (1999). *Interno gradivo podjetja Halcom d.d*. Ljubljana: Halcom d.d.
26. Halcom d.d. (2006). *Kartica ena za vse* (interno gradivo). Ljubljana: Halcom d.d.
27. Halcom d.d. (2016) *Pametna kartica.* Najdeno 30. januarja 2016 na spletnem naslovu http://www.halcom-ca.si/?section=18
28. Halcom d.d. (2016). *Spletni servis ena za vse.* Najdeno 5. marca 2016 na spletnem naslovu http://www.halcom.si/si/produkti/spletni-servis-2/spletni-servis/
29. Halcom d.d. (2016). *Spletni servis ena za vse.* Najdeno 5. marca 2016 na spletnem naslovu http://www.halcom.si/si/produkti/spletni-servis-2/spletni-servis/
30. Halcom d.d. (2016). *Tip čitalnika pametnih kartic*. Najdeno 29. januarja 2016 na spletnem naslovu Najdeno 29. januarja 2016 na spletnem naslovu http://www.halcom.si/si/produkti/digitalno-potrdilo/citalniki/naroci-citalnik-pametnih-kartic/
31. Halcom d.d.(2016) *Pisno potrdilo o istovetnosti digitalnega potrdila* (interno gradivo). Ljubljana: Halcom d.d.
32. Halcom plačila d.o.o. (2016). Aplikacija Hal mBills. Najdeno 20. junija 2016 na spletnem naslovu Najdeno 20. julij 2016 na spletnem naslovu

https://play.google.com/store/apps/details?id=com.halcom.epay.ebill.mobile.pilot.prod&hl=en
33. Halcom plačila d.o.o.(2016). *Pogosta vprašanja*. Najdeno 31. maja 2016 na spletnem naslovu http://www.mbills.si/pogosta-vprasanja/?action=GoToCategory&data=85%2Fall%2Fposition%2F0%2F10
34. Hermes Softlab d.o.o. (2004*). Sistem elektronskega bančništva*. Najdeno 15. oktobra 2004 na spletnem naslovu http://www.hermes-softlab.com/SLO/industries/ebanking/ebanking.html http://www.banka-koper.si/Fizicne_osebe/Poti_do_banke/Banka_IN
35. Hypo Alpe Adria d.d. (2016). *E-bančništvo*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.hypo-alpe-adria.si/sl/content/e-bancnistvo-0
36. Jerman Blažič, B. (2001). *Elektronsko poslovanje na internetu*. Ljubljana: Gospodarski Vestnik
37. Kadivec, J. (2000). *Elektronska banka – priročnik za uporabo sistema PPD E – bank*. Ljubljana: NLB d.d
38. Kalakota, R., & Whinston, B. A. (1997). *Electronic Commerce*. A Manager s guide. B.k.: Addison – Wesley Longman
39. Kovačič, M. (1997). Storitve elektronskega bančništva. *Banke in tveganje*. *Zbornik III. Strokovnega posvetovanja o bančništvu* (str. 130–165) Portorož. Zveza ekonomistov Slovenije
40. Kuščar, S. (2002, 11. november). O varnosti in odgovornosti. *Monitor*, str. 8.
41. Ministrstvo za javno upravo (2016) *Digitalni podpis.* Najdeno 5. marca 2016 na spletnem naslovu *http://www.si-ca.si/kripto/kr-podp.htm*
42. Miš Svoljšak, I. (1997). Osnove trženja finančnih storitev. *Združenje bank Slovenije*, 23.
43. Miš Svoljšak, I. (1999). V tujini se elektronsko bančništvo še povečuje. *Kapital*, 9.
44. Monitor Pro (2015). *Halcom Plačila predstavil Hal mBills*. Najdeno 6. junija 2016 na spletnem naslovu http://www.monitorpro.si/170767/novice/halcom-placila-predstavil-hal-mbills
45. Na – Network Associates. *An Introduction to Cryptography*. Santa Clara: Network Associates Inc. 1999.
46. Narandža – Štanta D. (2006). *Primerjalna analiza spletnega bančništva za fizične osebe* (diplomsko delo). Kranj: Fakulteta za organizacijske vede
47. NKBM d.d. (2011). *Kartica Secur ID.* Najdeno 28. novembra 2011 na spletnem naslovu https://www.nkbm.si/bankanet
48. NLB d.d. (2011). *Bančni izpisek* (interno gradivo). Ljubljana: NLB d.d.
49. NLB d.d. (2011). *Sumljiva transakcija* (interno gradivo). Ljubljana: NLB d.d.
50. Nlb d.d. (2016). *Kode namena plačila.* Najdeno 29. januarja 2016 na spletnem naslovu http://www.nlb.si/sepa-koda-namena
51. Nlb d.d. (2016). *NLB Klik*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.nlb.si/klik

52. NLB d.d.(2016). *NLB Klik*. Najdeno 29. januarja 2016 na spletnem naslovu http://www.nlb.si/klik
53. Ošlak, D. (2005). *Varnost elektronskega poslovanja v slovenskem bančništvu* (magistrsko delo). Ljubljana: Ekonomska fakulteta
54. Pavliha, M. (2002). *Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem*. Ljubljana: GV Založba
55. Poštna banka Slovenije d.d. (2016). *PBS.net - elektronska banka*. Najdeno 30. januarja 2016 na spletnem naslovu http://www.pbs.si/si/PBSnet.wlgt
56. Pepelnjak, I. & Bradeško M. (1997). Varnost računalniških sistemov in elektronskih transakcij. *Zbornik Banke in tveganja*. Portorož: Zveza ekonomistov Slovenije, 164.
57. Power, R. (1998). *How NOT to build a firewall*. Computer Security Institute. Najdeno 5.oktobra 2006 na spletnem naslovu http://www.spirit.com/CSI/Papers/hownot.htm
58. Pravilnik o spremembah in dopolnitvah Pravilnika o standardih in pogojih izmenjave elektronskih računov prek enotne vstopne in izstopne točke pri Upravi Republike Slovenije za javna plačila (2015). *Uradni list RS*, št. 75/2015).
59. Pucihar, A. (1999) *Priložnosti in težave elektronskega poslovanja med organizacijami v Sloveniji*. Uporabna informatika, 7 (4), 7–13.
60. Pucihar, A., & Gričar, J. (2000). *Izraba informacijske tehnologije za elektronsko poslovanje*. Organizacija (3), 207–212.
61. Raiffeisen banka d.d. (2016). *Elektronsko bančništvo*. Najdeno 30. januarja 2016 na spletnem naslovu http://www.raiffeisen.si/osebno_bancnistvo/poti_do_banke/elektronsko_bancnistvo_raiffeisennet/
62. SI-CERT (2006). *Goljufije in prevare.* Najdeno 5. marca 2016 na spletnem naslovu https://www.cert.si/wp-content/uploads/2015/05/Porocilo-o-omrezni-varnosti_2014.pdf
63. Sjekloča, M. (1999). Elektronsko bančništvo. *Bančni vestnik 48* (1-2), 31–32.
64. SKB banka d.d. (2011). *Identifikacijska kartica.* Najdeno 28. novembra 2011 na spletnem naslovu https://www.SKB.si/www-SKB-net/sl/identifikacijska-kartica
65. SKB d.d. (2016). *E-bančništvo.* Najdeno 30. januarja 2016 na spletnem naslovu http://www.skb.si/osebne-finance/sodobne-bancne-poti/skb-net-spletno-bancnistvo
66. SKB d.d. (2016). *Spletno bančnišrvo SKB Net*. Najdeno 24.maja 2016 na spletnem naslovu http://www.skb.si/osebne-finance/sodobne-bancne-poti/skb-net-spletno-bancnistvo
67. SKB d.d. (2016). *UPN nalog.* Najdeno 28. maja 2016 na spletnem naslovu https://www.SKB.si/www-SKB-net/sl/identifikacijska-kartica
68. SKB d.d.(2016). *Primer SMS sporočila.* Ljubljana: SKB d.d.
69. Spletna banka BANK@NET. Najdeno 29. januarja 2016 na spletnem naslovu http://www.nkbm.si/bankanet
spletnem naslovu http://www.sepa.si/slo/potrjenidokumenti/nacionalni%20program%20sepa%20v%20sloveniji_febr2010.pdf

70. Škedelj, F. (2002). *Informacijska podpora prenovi plačilnega prometa*. Najdeno 5. oktobra 2006 na spletnem naslovu www.zaslon.si/informacijska-podpora-prenovi-placilnega-prometa/
71. Škrlec, I. (2002, 6.maj). E-poslovanje in uporaba formata XML. *Finance*, str. 18.
72. Telekom Slovenije d.d (2011). *Interno gradivo podjetja Telekom Slovenije d.d.* Ljubljana: *Telekom Slovenije d.d.*
73. Telekom Slovenije d.d., (2016). *Vloga za izdajo e-računov*. *Ljubljana:* Telekom Slovenije d.d.
74. Toplišek, J. (1998). *Elektronsko poslovanje*. Ljubljana: Založba Atlantis
75. Turban, E., Chung, M. H., Lee, J.,& King, D. (2003). *Electronic Commerce*. A Managerial Perspective. New York: Prentice Hall
76. Unicredit banka Slovenije d.d. (2016). *E-bančništvo Banka na daljavo*. Najdeno 10. junija 2016 na spletnem naslovu http://www.unicreditbank.si/sl/Prebivalstvo/Elektronsko_bancnistvo
77. Uprava Republike Slovenije za javna plačila *(2016). Univerzalni plačilni nalog.* Najdeno 5. marca 2016 na spletnem naslovu https://www.ujp.gov.si/docDir/SEPA/Tehnicni_standard_UPN.pdf
78. Visa Europe (2016)., *Pogosta vprašanja*. Najdeno 15. maja 2016 na spletnem naslovu https://www.visaeurope.si/produkti/visa-contactless/pogosta-vprasanja
79. Voh Boštic, A. (2015, 11. januar). *Kiberkriminal v Sloveniji (2): zakaj je boljša varnost vzrok za več zlorab bančnih kartic*. Najdeno 15. marca 2016 na spletnem naslovu https://podcrto.si/kiberkriminal-v-sloveniji-2-zakaj-je-boljsa-varnost-vzrok-za-vec-zlorab-bancnih-kartic-2/
80. Vozel, A. (1999): Napake v internetni strategiji bank. *Gospodarski vestnik,* 47*, 57–59*
81. Vrešak, S. (1997). Internet in elektronsko bančništvo. *Bančni vestnik, 46*(12), 60–63.
82. Young-Seock (2006). *Osnovni model zaščite lokalnega omrežja*. Najdeno 10. Oktobra 2006 na spletnem naslovu http://secinf.net/info/fw/ecom
83. ZBS Združenje bank Slovenije (2010). *Nacionalni program SEPA v Sloveniji*. Najdeno 20. oktobra 2015 na spletnem naslovu http://www.sepa.si/slo/potrjenidokumenti/nacionalni%20program%20sepa%20v%20sloveniji_febr2010.pdf
84. ZBS Združenje bank Slovenije (2010). *Zapisnik*. Najdeno 20. oktobra 2015 na
85. ZBS Združenje bank Slovenije (2010).*Univerzalni plačilni nalog*. Najdeno 20. oktobra 2015 na spletnem naslovu http://www.upn.si/uploads/public/tehnicni_standard_UPN.pdf

PRILOGE

KAZALO PRILOG

PRILOGA 1: Vprašalnik iz leta 2011

Pozdravljeni

Sem Tanja Marolt, študentka Ekonomske fakultete v Ljubljani. Za zaključno nalogo sem si izbrala temo Varnost elektronskega bančništva: analiza stanja v Sloveniji.

Pripravila sem vam anketni vprašalnik, ki je namenjen fizičnim osebam. Na vprašalnik, prosim, odgovarjate korektno, saj je anketa anonimna.

Pridobljeni podatki bodo služili za sumarno obdelavo in posamično ne bodo objavljeni. Hvala za sodelovanje in lep pozdrav,

Tanja Marolt

1. Spol
   a) moški
   b) ženski

2. Starost
   a) 20–30
   b) 30–40
   c) 40–50
   d) 50 in več

3. Izobrazba
   a) osnovnošolska izobrazba
   b) srednješolska izobrazba
   c) višja strokovna izobrazba
   d) visoka ali univerzitetna izobrazba
   e) specializacija ali magisterij
   f) doktorat

4. Ali uporabljate elektronsko banko?
   a) da.
   b) ne.
   c) nimam želje.
   d) v bližnji prihodnosti si želim urediti elektronsko bančništvo.

5. Katero spletno banko uporabljate?
   a) NLB Klik

b) SKB NET
c) Abanet
d) Bank@Net
e) i-Net
f) HYPOnet
g) Drugo:

6. Koliko časa že uporabljate elektronsko bančništvo?
   a) manj kot 1 leto
   b) 1–3 leta
   c) 3–5 let
   d) več kot 5 let

7. Kakšen je razlog, da ste se odločili za elektronsko banko?
   a) Zaradi vrst na bančnih okencih.
   b) Zaradi dostopnosti 24 ur na dan na različnih lokacijah.
   c) Zaradi preglednosti poslovanja.
   d) Zaradi cenejše provizije.
   e) Drugo: _____.

8. Kako pogosto upobljate elektronsko banko?
   a) 1x mesečno
   b) 2x mesečno
   c) 1x tedensko
   d) večkat na teden

9. Za kakšne namene uporabljate elektronsko banko? Možnih je več odgovorov.
   a) pregled stanja
   b) plačevanje računov
   c) urejanje trajnikov
   d) naročilo depozitov
   e) podaljšanje limitov
   f) nakup oz. prodaja tuje valute

10. Ali pri plačevanju že uporabljate UPN nalog?
    a) Da.
    b) Ne.
    c) plačeval/a sem že z njim, vendar še uporabljam BN-02 nalog (stari način).
    d) Nisem še slišal/a za UPN.

11. Ali ste že slišali za e-račune?

a) da
b) ne
c) Sem se že naročil/a na to storitev.

12. Kako varna se vam zdi vaša elektronska banka?
    a) 100%
    b) 75%
    c) 50%
    d) manj kot 50%

13. Katero sredstvo se vam zdi najbolj varno?
    a) Nameščen certifikat na računalniku – pin koda.
    b) Certifikat na USB ključu ali kartici.
    c) Kartica z ekranom, ki spreminja gesla glede na čas.
    d) SMS sporočilo v primeru plačila na nov transakcijski račun.

14. Ste že slišali za zlorabe v elektronskem bančništvu?
    a) Da.
    b) Ne.
    c) Mojim znancem se je pripetila zloraba.
    d) Meni se je pripetila zloraba.

15. Ali se vam zdi, da je pametno določiti mesečni limit na računu, da ne prihaja do večjih zlorab?
    a) da
    b) ne

16. Ste razmišljali, da bi zaradi varnosti/nevarnosti zamenjali banko ali prenehali uporabljati elektronsko bančništvo?
    a) Zamenjal/a bi banko.
    b) Ne bi zamenjal/a banke.
    c) Prenehal/a bi uporabljati elektronsko bančništvo.
    d) Trenutno nimam pomislekov glede varnosti moje banke.

PRILOGA 2: Vprašalnik iz leta 2016

Pozdravljeni!

Pripravljam magistrsko delo na temo **" Varnost elektronskega bančništva: analiza stanja v Sloveniji ",** zato bi vas prosila za pomoč pri raziskavi.

Anketni vprašalnik je namenjen **fizičnim osebam**. Na vprašanja, prosim, odgovarjate korektno, saj je anketa anonimna.

Pridobljeni podatki bodo služili za sumarno obdelavo in posamično ne bodo objavljeni.

Povezava do ankete:

https://www.1ka.si/a/88717

Hvala za sodelovanje in lep pozdrav,
Tanja Marolt

1. Spol
   a) moški
   b) ženski

2. Starost
   a) 20–30
   b) 30–40
   c) 40 –50
   d) 50 in več

3. Izobrazba
   a) osnovnošolska izobrazba
   b) srednješolska izobrazba
   c) višja strokovna izobrazba
   d) visoka ali univerzitetna izobrazba
   e) specializacija ali magisterij
   f) doktorat

4. Ali uporabljate elektronsko banko?
   a) Da.
   b) Ne.

c) Nimam želje.
d) V bližnji prihodnosti si želim urediti elektronsko bančništvo.

5. Katero spletno banko uporabljate?
   a) NLB Klik
   b) SKB net
   c) Abanet
   d) Bank@Net
   e) Banka IN
   f) HYPOnet
   g) Drugo:

6. Koliko časa že uporabljate elektronsko bančništvo?
   a) manj kot 1 leto
   b) 1–3 leta
   c) 3–5 let
   d) več kot 5 let

7. Kakšen je razlog, da ste se odločili za elektronsko banko?
   a) Zaradi dolgih vrst na bančnih okencih.
   b) Zaradi dostopnosti 24 ur na dan na različnih lokacijah.
   c) Zaradi preglednosti poslovanja.
   d) Zaradi cenejše provizije.
   e) Drugo: _____.

8. Kako pogosto uporabljate elektronsko banko?
   a) 1x mesečno
   b) 2x mesečno
   c) 1x tedensko
   d) Večkrat na teden.

9. Za kakšne namene uporabljate elektronsko banko? Možnih je več odgovorov.
   a) pegled stanja
   b) plačevanje računov
   c) urejanje trajnikov
   d) naročilo depozitov
   e) podaljšanje limitov

10. Ali ste že slišali za e-račune?
    a) Da.
    b) Ne.

c) Sem se že naročil(-a) na to storitev.
d) Mesečno prejemam več e-računov.

11. Kako varna se vam zdi vaša elektronska banka?
    e) manj kot 50%
    f) 50–70%
    g) 71–90%
    h) 91–100 %

12. Katero sredstvo se vam zdi najbolj varno?
    a) Nameščen certifikat na računalniku – pin koda.
    b) Certifikat na USB ključu ali kartici.
    c) Kartica z ekranom, ki spreminja gesla glede na čas.
    d) SMS sporočilo v primeru plačila na nov transakcijski račun.

13. Ste že slišali za zlorabe v elektronskem bančništvu?
    a) Da.
    b) Ne.
    c) Mojim znancem se je pripetila zloraba.
    d) Meni se je pripetila zloraba.

14. Ali se vam zdi, da je pametno določiti mesečni limit na računu, da ne prihaja do večjih zlorab?
    c) da
    d) ne

15. Ste razmišljali, da bi zaradi varnosti/nevarnosti zamenjali banko ali prenehali uporabljati elektronsko bančništvo?
    e) Zamenjal(-a) bi banko.
    f) Ne bi zamenjal(-a) banke.
    g) Prenehal/a bi uporabljati elektronsko bančništvo.
    h) Trenutno nimam pomislekov glede varnosti moje banke.