UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jakob Jančič

Varnostni mehanizmi v elektronskem bančništvu in njihov pomen za uporabnika

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jakob Jančič

Mentor: izr. prof. dr. Jaroslav Berce

Varnostni mehanizmi v elektronskem bančništvu in njihov pomen za uporabnika

Diplomsko delo

Ljubljana, 2016

Varnostni mehanizmi v elektronskem bančništvu in njihov pomen za uporabnika

Elektronsko bančništvo postaja za vedno večje število ljudi glavni način poslovanja z banko. Uporabnikom omogoča hitro in preprosto uporabo bančnih storitev. Obstajajo pa tudi temne plati elektronskega bančništva. Uporabniki so tarča več vrst zlorab, zato smo opisali najpogostejše načine napadov na elektronske banke. Za varnost uporabnikov skrbi vrsta varnostnih mehanizmov, ki jih ponujajo banke v svojih elektronskih bankah. Varnostne mehanizme smo analizirali na treh segmentih: avtentikacija strežnika, identifikacija in avtentikacija uporabnika ter avtorizacija transakcije. Predstavili smo najpogostejše oblike varnostnih mehanizmov pri posameznih segmentih in izpostavili njihove dobre in slabe strani. Varnostni mehanizmi varujejo uporabnika pred zlorabami, a obenem vplivajo na zahtevnost uporabe elektronskih bank. Preverili smo tudi, kakšni so razlogi za uvedbo dodatnih varnostnih mehanizmov v slovenskih bankah. Ugotovili smo, da je med slovenskimi bankami v ospredju pravni vidik. Naredili smo tudi analizo uporabljenih varnostnih mehanizmov petih izbranih slovenskih bank ter primerjali pogled na varnost med Slovenijo in Združenimi državami Amerike. Ocenjena varnost izbranih slovenskih bank je višja kot varnost analiziranih bank v Združenih državah Amerike.

Ključne besede: elektronsko bančništvo, varnostni mehanizmi, zlorabe, uporabniška izkušnja.

Security mechanisms in electronic banking and their importance for the user

Electronic banking is becoming the main way of doing business with the bank for increasing numbers of people. It allows users to quickly and easily use the bank's services. There is also a dark side to electronic banking. Users are targets of many different types of frauds. We will describe the most common types of attacks on electronic banking. To make the use of electronic banking safer for the users, banks are implementing many different forms of security mechanisms. Security mechanisms were analysed in three segments: server authentication, user identification and authentication, and authorization of transactions. We describe the most commonly used forms of security mechanisms and highlight their strengths and weaknesses. Security mechanisms protect the user against fraud, but they also affect the ease of use of electronic banking. We also looked at the reasons for the introduction of additional security mechanisms in Slovenian banks. We found that among Slovenian banks the legal aspect is in the forefront. We made an analysis comparing the use of security mechanisms between five selected Slovenian banks. We also compared views on security between Slovenia and the United States. We found that the level of security in selected Slovenian banks is higher than that of the analysed banks in the United States.

Keywords: electronic banking, security mechanisms, frauds, usability.

KAZALO

KAZALO SLIK

KAZALO TABEL

KAZALO GRAFOV

1 Uvod

Uporaba interneta je postala pomemben del našega življenja. Na področju bančništva, je veliko ljudi opustilo klasično bančništvo in ga nadomestilo z elektronskim bančništvom (Prakash 2007, 1). Elektronsko bančništvo uporabnikom omogoča hiter in preprost dostop do informacij ter storitev (Koskosas 2011; Resnik v Berce 2014).

Sama uporaba zahteva od uporabnikov tudi nekaj znanja. Banke sicer oglašujejo, da lahko začnejo uporabniki elektronsko bančništvo uporabljati že v nekaj minutah, a če bi upoštevali vsa priporočila za varno uporabo bi večina uporabnikov za to potrebovala več ur ali dni, če so seveda dovolj tehnično usposobljeni, da to sploh naredijo (Mannan 2007, 11).

Nova Ljubljanska banka d.d. uporabniku med drugim priporoča:

- vestno posodabljanje protivirusnih programov,
- skrb za požarni zid,
- nameščanje vseh popravkov za operacijski sistem,
- uporabo najnovejše verzije brskalnika,
- reden obisk spletnih strani namenjenih varnostnim priporočilom. (Nova Ljubljanska banka d.d. 2016)

Rast uporabe elektronskega bančništva je pritegnila tudi zanimanje kriminalcev, ki poskušajo uporabnika izkoristiti (Mannan 2007, 1). Večina napadov na elektronske banke je usmerjena k uporabniku, ki predstavlja najšibkejši člen (Peotta in drugi 2011, 195). Čeprav banke pravijo, da je varnost skupna odgovornost, pa analize kažejo da je večina odgovornosti na plečih uporabnikov (Mannan 2007, 11). Večina uporabnikov nima želje, da bi se o varnosti podučila. Na varnostne mehanizme gledajo kot na oviro, ki jih pri uporabi elektronske banke upočasnjuje (Hertzum 2004; Singh 2006). Ker so varnostni mehanizmi nujni za zagotavljanje varnosti, se odpira vprašanje uporabniške izkušnje. Banke morajo najti ravnotežje med izboljšano varnostjo ter preprostostjo uporabe in koristnostjo za uporabnike (French 2012, 12). Hertzum (2004, 60) pravi, da je doseganje varnosti in preprostosti uporabe v elektronskem bančništvu težavno, ker ni samodejna, uporabniki pa se osredotočajo na svoj

glavni cilj, ki je uporaba storitve. Da bi dosegli dobro ravnovesje med varnostjo in uporabniško izkušnjo morajo banke zato uporabljati varnostne mehanizme, ki so čim bolj neodvisni od uporabnika (Peotta in drugi 2011, 195). Strah glede varnosti je tudi glavni razlog zaradi katerega mnogi uporabniki še ne uporabljajo elektronskega bančništva, čeprav so raziskave pokazale, da ta strah ni posledica slabih izkušenj (Meyer 2006, 3).

V prvem poglavju (Elektronsko bančništvo in uporabniška izkušnja) bomo pojasnili pojem elektronskega bančništva. Predstavili bomo podatke o razširjenosti uporabe elektronskega bančništva v Sloveniji, ki jih že od leta 2007 zbira Statistični urad Republike Slovenije. Opisali bomo razloge za povečanje uporabe ter izpostavili negativne strani uporabe elektronskega bančništva za uporabnike, in tiste, ki ga ne uporabljajo.

V drugem poglavju (Vrste zlorab uporabnika v elektronskem bančništvu) bomo opisali najpogostejše vrste zlorab, ki prežijo na uporabnika. Osredotočili se bomo samo na tiste vrste zlorab, ki se zgodijo v relaciji med uporabnikom in banko.

V tretjem poglavju (Varnostni mehanizmi v elektronskem bančništvu) bomo podrobno opisali varnostne mehanizme, ki so v uporabi v Sloveniji in po svetu. Pogledali bomo, kako uspešno varujejo pred posameznimi vrstami zlorab ter opisali njihovo uporabo s stališča uporabnika. Preverili bomo varnostne mehanizme, ki se uporabijo pri avtentikaciji strežnika, ki je prvi stik uporabnika z elektronsko banko. Nadalje bomo preverili varnostne mehanizme, ki se uporabljajo za identifikacijo in avtentikacijo uporabnika pri vstopu. Nazadnje bomo preverili še mehanizme, ki se uporabljajo za avtorizacijo transakcije.

V četrtem poglavju (Razlogi za uvedbo dodatnih varnostnih mehanizmov) bomo pogledali, kakšni so razlogi, zaradi katerih se banke odločajo za uvedbo dodatnih varnostnih mehanizmov. Preverili bomo, če se banke za dodatne varnostne mehanizme odločajo zaradi sprememb zakonodaje, stroškov, ki jih imajo zaradi zlorab ali pa želijo z izboljšanjem varnosti k uporabi elektronskih bank privabiti še tiste uporabnike, ki iz strahu pred zlorabami ali drugih razlogov elektronskega bančništva še ne uporabljajo.

V petem poglavju (Primerjava uporabe varnostnih mehanizmov v slovenskih bankah) bomo opisali uporabljene varnostne mehanizme v petih slovenskih bankah. Preverili bomo, kakšna je stopnja varnosti in izpostavili morebitne pomanjkljivosti za posamezno banko. Banke bomo

med seboj primerjali glede na uporabljene varnostne mehanizme. Poleg Banke Koper, ki velja za banko z dobro varnostjo (Zveza potrošnikov Slovenije, 2009), bomo v primerjavo vključili še štiri banke, pri razvoju katerih sem aktivno sodeloval v okviru sedanje zaposlitve.

V šestem poglavju (Razlike v uporabi varnostnih mehanizmov med Slovenijo in Združenimi državami Amerike) bomo naredili še analizo štirih največjih bank v Združenih državah Amerike in primerjali rešitve, ki jih uporabljajo, s slovenskimi bankami.

V zadnjem poglavju (Zaključek) bomo preverili podali čim realnejši odgovor na naša raziskovalna vprašanja in podali zaključek dela.

2 Metodološko-hipotetični okvir

V diplomskem delu želimo odgovoriti na nekaj vprašanj, povezanih z varnostnimi mehanizmi v elektronskem bančništvu. Bishop (2005, 3) varnostni mehanizem definira, kot metodo, orodje ali postopek za uveljavljanje varnostne politike. Varnostna politika je širši pojem, ki ga Bishop (2005, 3) opiše preprosto, kot izjavo o tem, kaj je dovoljeno in kaj ni. Prikazali bomo razloge za njihovo implementacijo in njihov pomen za uporabnika.

Pri preučevanju se bomo poslužili kvalitativnih metod. Analizirali bomo literaturo in sekundarne vire s področja elektronskega bančništva ter s tem povezanih področij. Pomagali si bomo tudi z izkušnjami, ki smo jih pridobili ob že skoraj dvajset let trajajoči karieri, na področju razvoja rešitev za elektronsko bančništvo.

Prva hipoteza, ki jo bomo preučevali, je, da **dodatni varnostni mehanizmi v elektronski banki vplivajo na uporabniško izkušnjo pri uporabi elektronskega bančništva**. Uporabniško izkušnjo definiramo, kot vse vidike interakcije končnega uporabnika s podjetjem, njegovimi storitvami in produkti (Norman in Nielsen 2016). Pogledati želimo, ali ima njihova vpeljava lahko določene negativne ali pa morebitne pozitivne vplive na uporabnost elektronske banke. Izhajamo iz domneve, da vsaka uvedba novega varnostnega mehanizma povečuje kompleksnost uporabe elektronske banke in posledično vpliva na uporabniško izkušnjo.

Druga hipoteza, ki jo bomo preučili, je, da so **razlogi za vpeljavo dodatnih varnostnih mehanizmov v elektronske banke v Sloveniji predvsem posledica zahtev zakonodajalcev**. Izpostavili bomo tri, po naši oceni glavne razloge, zaradi katerih se banke odločajo za uvedbo dodatnih varnostnih mehanizmov. So to zakonske zahteve, poskus zmanjšanja stroškov, ki jih ima banka z zlorabami ali želja, da bi uporabnike prepričali o varnosti uporabe elektronske banke? Naša domneva je, da se banke večinoma odzivajo le na zahteve zakonodajalca. Na podlagi analize sekundarnih virov bomo potrdili ali ovrgli domnevo, da so razlogi predvsem posledica zahtev zakonodajalcev.

Tretja hipoteza, ki jo bomo preučili, je, da **med Združenimi državami Amerike in Slovenijo obstajajo v pogledu na potrebo po dodatni varnosti razlike**. Ugotoviti želimo, ali je

predsodek razvijalcev slovenskih bančnih rešitev o nizki stopnji varnosti elektronskih bank v Združenih državah Amerike utemeljen. S pomočjo primerjalne metode, bomo vzporejali uporabo varnostnih mehanizmov petih slovenskih bank ter varnostne mehanizme bank v Združenih državah Amerike.

Po Raginovih (2007, 118) besedah raziskovalci, ki se ukvarjajo s primerjalnim raziskovanjem, preučujejo vzorce podobnosti in raznolikosti zmernega števila preučevanih primerov oziroma enot. Število primerov je omejeno, saj je za primerjalno raziskovanje pomembno, da podrobno poznamo vsak primer, ki je zajet v raziskavo.

Varnostne mehanizme, ki jih uporabljajo posamezne, v delu preučevane banke, bomo primerjali na osnovi analize podatkov, ki jih bomo pridobili na spletnih straneh izbranih bank in na podlagi mnenja drugih avtorjev.

Stopnjo varnosti posamezne banke bomo preučevali s primerjavo naslednjih segmentov varnosti: avtentikacija strežnika, identifikacija in avtentikacija uporabnika in avtorizacija transakcije.

Za oceno varnosti pri avtentikaciji strežnika, bomo uporabili spletno orodje SSL Server Test. Orodje na preprost način, z oceno od A do F, oceni varnost strežnika. Za izdelavo ocene, spletno orodje preveri, če je strežniški certifikat veljaven in izdan iz strani zaupanja vrednega overitelja. Spletno orodje tudi analizira nastavitve strežnika v treh kategorijah, in sicer: podprtih kriptografskih protokolih, izmenjavi ključev (ang. *Key exchange*) ter moči uporabljenih šifrirnih algoritmov (povzeto po Qualys SSL Labs 2015). Oceno varnosti pri identifikaciji in avtentikaciji uporabnika ter avtorizaciji transakcije, bomo naredili na podlagi izsledkov pridobljenih iz sekundarnih virov. Primerjavo bomo naredili tudi s pomočjo preglednice, kjer bomo pri uporabi varnostnih mehanizmov ugotavljali tudi obstoječe razlike med slovenskimi bankami.

3 Elektronsko bančništvo in uporabniška izkušnja

3.1 Definicija elektronskega bančništva

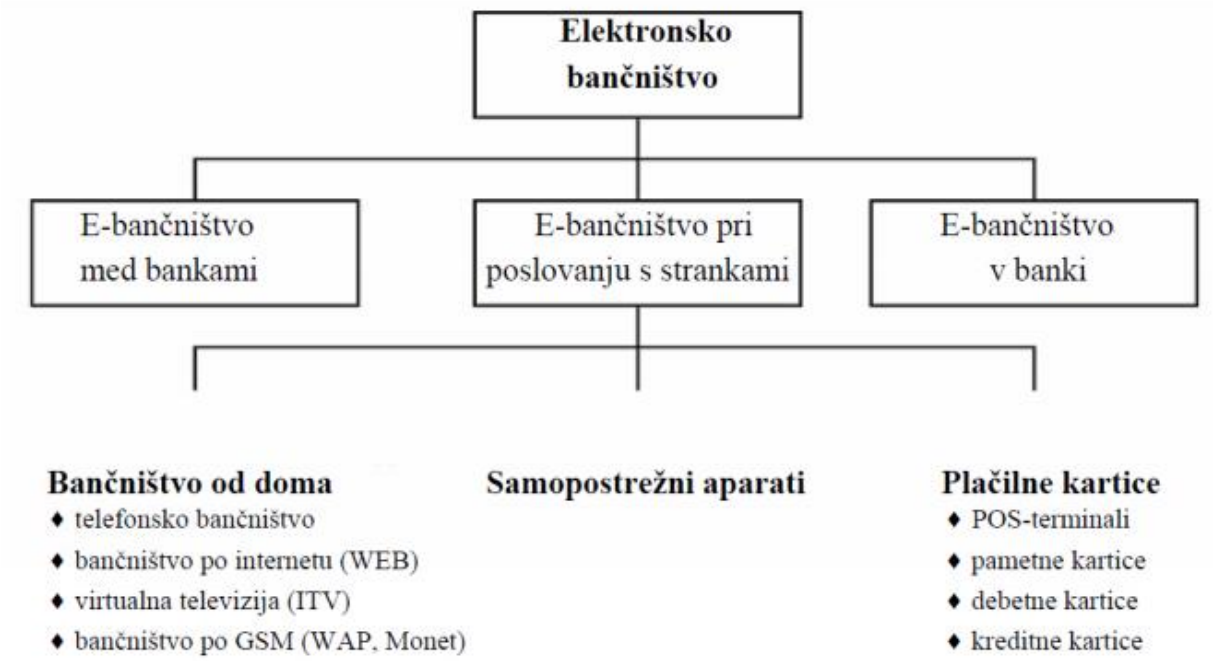
Elektronsko bančništvo je mogoče definirati široko, tako da vključimo v definicijo tudi bankomate, telefonsko bančništvu in druge oblike bančništva, kjer se posluje po elektronski poti ali pa bolj fokusirano, kjer pod tem imenom razumemo poslovanje bank s svojimi komitenti prek spleta. Lahko gre za poslovanje banke s podjetji ali pa poslovanje banke s fizičnimi osebami.

Elektronsko bančništvo (Insley in drugi v Berce 2014, 50) je krovni izraz za proces, s katerim lahko stranka opravlja bančne transakcije v elektronski obliki brez obiska institucije. Daniel (1999, 72) elektronsko bančništvo opiše kot posredovanje informacij ali storitev, ki jih banke nudijo svojim strankam prek računalnika. Keivani in drugi (2012, 62) podobno kot Insley pravijo, da je elektronsko bančništvo krovni izraz za postopek, s katerim lahko stranka opravlja bančne posle elektronsko brez obiska poslovalnice.

V domači literaturi Kadivec to opiše na preprost način: »S pojmom elektronska banka lahko opredelimo način opravljanja bančnih storitev, ki jih lahko kot bančni komitent opravite neposredno s svojega delovnega mesta ali od doma, brez neposredne pomoči bančnega uslužbenca, in to kadarkoli, 24 ur na dan, 365 dni v letu (Kadivec v Malenšek v Berce 2014, 50).«

Širšo definicijo nam ponuja Miš-Svoljšakova (v Berce 2014), ki elektronsko bančništvo deli na elektronsko bančništvo pri poslovanju s strankami, elektronsko bančništvo med bankami ter elektronsko bančništvo v banki. Tudi pri elektronskem bančništvu pri poslovanju s strankami lahko vidimo, da poleg bančništva od doma, kot del elektronskega bančništva omenja tudi samopostrežne aparate (bankomate) ter plačilne kartice. Zaradi obsežnosti področja, se bomo v diplomskem delu osredotočili samo na probleme povezane z bančništvom po internetu, natančneje elektronskim bančništvom za fizične osebe.

Slika 3.1: Storitve elektronskega bančništva



Vir: Miš-Svoljšak v Berce (2014).

3.2 Slabosti in koristi elektronskega bančništva za uporabnika

Uporaba elektronskega bančništva ima slabosti in koristi tako za banko, kot tudi za same uporabnike. (povzeto po Koskosas 2011, 54) Kot glavno prednost za uporabnika bi izpostavili prihranek časa, za banko pa nižje stroške poslovanja. Uporabnik ima možnost uporabe elektronske banke 24 ur na dan, kar mu omogoča vpogled v stanje na računu, plačevanje računov in opravljanje drugih bančnih storitev. Vse kar potrebuje je dostop do interneta in sredstvo za identifikacijo in avtentikacijo uporabnika.

Koskosas (2011, 55) kot glavne prednosti za uporabnika izpostavi udobnost uporabe, cenejšo uporabo, dodatne storitve, mobilnost, preprostost uporabe in prijaznost okolju. Podobno meni tudi Resnik, ki poleg prednosti za uporabnika opiše tudi prednosti elektronskega poslovanja za podjetja.

Najpomembnejše prednosti za uporabnike:

- *različne možnosti dostopa do storitev in informacij,*
- *storitve so prilagojene v večji meri,*
- *uporabniki so vključeni v oblikovanje storitev in njihove izboljšave,*

- *uporabniki so vključeni v proces odločanja,*
- *stroški so nižji,*
- *prihrani se čas za opravljanje storitev in pridobivanje informacij,*
- *storitve so na voljo tudi izven delovnega časa.* (Resnik v Berce 2014, 45–46)

Najpomembnejše prednosti za podjetja:

- *kljub začetnim višjim investicijskim stroškom se dolgoročno posluje z nižjimi stroški,*
- *poslovanje je bolj pregledno,*
- *viri so bolje razporejeni,*
- *storitve za uporabnike so hitrejše,*
- *kakovost storitev je višja,*
- *manj je napak in podvajanja dela,*
- *elektronsko komuniciranje prinaša boljšo in modernejšo podobo podjetja pri poslovnih partnerjih in strankah,*
- *višja kvaliteta storitev oz. izdelka.* (Resnik v Berce 2014, 46)

V vsaki storitvi pa se seveda skrivajo tudi slabosti. Med temi bi izpostavili predvsem zapiranje poslovalnic, ki poslovanje z banko oteži tistim, ki elektronskega bančništva bodisi ne zmorejo bodisi ne znajo ali celo ne želijo uporabljati. Problem predstavlja tudi pomanjkljivo tehnično znanje povprečnega uporabnika, tako z vidika uporabe same elektronske banke, kot tudi varnosti uporabnikovega računalnika. Koskosas (2011, 56) slabosti elektronskega bančništva vidi pri osebnem stiku, težavah pri izvedbi transakcij, težavah pri dostopu do storitev ter varnosti. Podobno vidi slabosti elektronskega poslovanja tudi Resnik.

Omejitve predstavljajo različni dejavniki:

- *socialne potrebe (npr. osebni stik),*
- *kulturna vprašanja (npr. jezikovne ovire),*
- *ekonomski dejavniki (dostopnost informacijske tehnologije),*
- *dejavniki povezani z učenjem (npr. spoznavanje nove tehnologije, računalniška pismenost, spreminjanje navad ipd.),*
- *fizični dejavniki (npr. telesne nezmožnosti, slepota),*

- *razvitost omrežja za zagotavljanje storitev informacijske tehnologije.* (Resnik v Berce 2014, 46)

Ostale slabosti:

- *možnost zlorabe informacijske tehnologije,*
- *nezaupanje v novosti,*
- *neosebnost takšne oblike komuniciranja,*
- *napake in zamude, ki se pojavijo ob uvajanju novih tehnologij*. (Resnik v Berce 2014, 47)

3.3 Razmah elektronskega bančništva

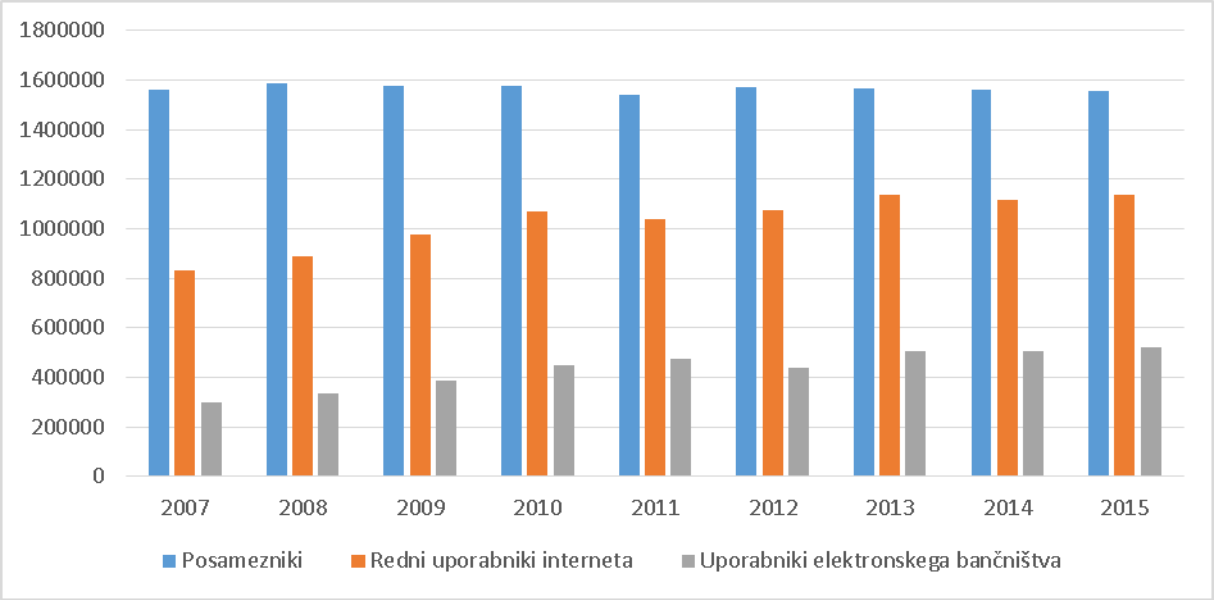
Po podatkih Statističnega urada Republike Slovenije se število rednih uporabnikov, ki so v zadnjih treh mesecih uporabljali internet, še vedno povečuje, čeprav se je tempo opazno upočasnil. Leta 2007 je internet redno uporabljalo nekaj več kot 53% prebivalcev starih od 16 do 74 let, v letu 2015 pa je teh uporabnikov že malce nad 73%. Enak trend je opazen tudi pri uporabi elektronskega bančništva, kjer vidimo, da storitve uporablja skoraj polovica uporabnikov interneta. Leta 2007 je bilo teh uporabnikov okrog 19%, število pa jedo leta 2015 postopoma naraslo na skoraj 34% prebivalcev.

Tabela 3.1: Odstotek rednih uporabnikov interneta in odstotek uporabnikov elektronskega bančništva, starih 16–74 let

	Redni uporabniki interneta	Uporabniki elektronskega bančništva
2007	53,30%	19,13%
2008	55,86%	20,98%
2009	61,97%	24,47%
2010	67,87%	28,53%
2011	67,34%	30,97%
2012	68,35%	28,08%
2013	72,68%	32,31%
2014	71,59%	32,28%
2015	73,10%	33,66%

Vir: Statistični urad Republike Slovenije (2016).

Graf 3.1: Uporaba elektronskega bančništva v slovenski populaciji od 16 do 74 let



Vir: Statistični urad Republike Slovenije (2016).

Slovenija je pri uporabi elektronskega bančništva še vedno pod evropskim povprečjem. Trend rasti uporabnikov interneta se je v zadnjih letih močno opočasnil, prav tako pa ni zaznati povečane uporabe elektronskega bančništva med trenutnimi uporabniki. Po rezultatih Eurostata je elektronsko bančništvo v državah Evropske unije v zadnjih treh mesecih leta 2012 v povprečju uporabljalo 38 % populacije stare od 16 do 74 let. Delež uporabnikov elektronskega bančništva v evropskih državah variira med 3 % in 86 % prebivalstva, kar pomeni, da Slovenija spada med manj razvite države na tem področju (povzeto po Eurostat v RIS 2013). Število uporabnikov elektronskega bančništva v Evropi, je po raziskavi Deutsche Bank nižje kot v Združenih državah Amerike. V Združenih državah Amerike, po njihovih ocenah uporablja elektronsko bančništvo 44% prebivalstva, medtem ko je evropsko povprečje 36% (Meyer 2006, 1).

4 Vrste zlorab uporabnika v elektronskem bančništvu

Vrst zlorab uporabnika v elektronskem bančništvu je več. Osredotočili se bomo na tiste vrste zlorab, ki se dogajajo na relaciji med uporabnikom in banko. Na tem mestu naj omenimo tudi interne zlorabe, ki predstavljajo veliko tveganje, vendar pri preprečevanju teh zlorab uporabnik storitev ni udeležen in zato v analizo niso vključene.

V Sloveniji je v primerjavi z večjimi državami trenutno malo zlorab elektronskega bančništva. Uradnih podatkov o tem ni, saj banke niso dolžne poročati o zlorabah (Vodopivec v Sušnik, 2010). V Novi Ljubljanski banki d.d., ki je največja slovenska banka pravijo, da je število zlorab glede na število uporabnikov in opravljenih transakcij zanemarljivo majhno (Ropret 2010). Nekaj zaslug gre pripisati dobri varnosti, predvsem pa majhnosti trga in nepoznavanju jezika, zaradi česar za mednarodne napadalce najverjetneje nismo najmikavnejša tarča. Po besedah Tadeja Vodopivca (v Sušnik 2010) gre pri trenutnih napadih na spletne banke večinoma za krajo gesel in certifikatov uporabnikov in posledično za krajo identitete ter denarja. Vodopivec dodaja, da so se dogajale kraje identitet (zasebnih ključev certifikatov), morda pa tudi preprostejše vrste MitB napadov.

4.1 Ribarjenje

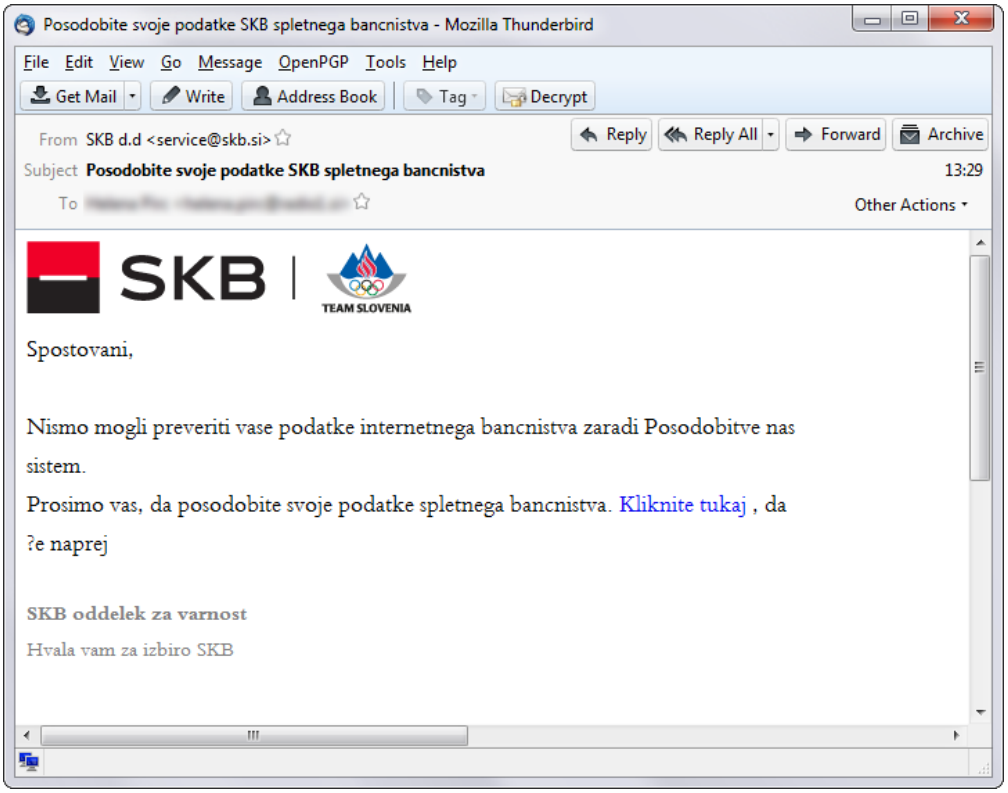
Ribarjenje ali lažno predstavljanje (ang. *Phishing*) je poskus zlorabe prek lažne elektronske pošte. Uporabnik prejme elektronsko pošto, ki na prvi pogled izgleda, kot da resnično prihaja iz banke. Napadalci praviloma uporabijo enake grafične elemente, kot jih uporablja banka. Uporabnika se poskuša pod različnimi pretvezami zvabiti na lažno spletno stran, ki od njega zahteva, da vnese svoje varnostne podatke ali izvozi digitalno potrdilo.

> *Sporočilo vsebuje informacije, ki so za žrtev pomembne (npr. nujna sprememba gesla na računu zaradi zagotavljanja varnosti, potrditev identitete v povezavi z bančnim računom, itd.), ter povezavo na lažno spletno stran. S klikom na omenjeno povezavo je potencialna žrtev preusmerjena na ponarejeno spletno stran za vnos zahtevanih podatkov, kot so npr. geslo, številka računa, kreditne kartice itd. (SI CERT, 2012). Običajno nujnost vnosa zahtevanih podatkov storilci utemeljujejo z zahtevo po »preverjanju« podatkov z namenom »zaščititi žrtev«.* (Dimc in Dobovšek 2012, 94–95)

Obisk same strani namenjene ribarjenju je šele prvi korak. Da pride do zlorabe mora uporabnik lažni strani tudi posredovati svoje podatke. Uporabnik, bi v tem prvem koraku še vedno lahko ugotovil, da je s spletno stranjo nekaj narobe, vendar mnogi uporabniki nimajo dovolj znanja, da bi prevaro prepoznali. V eni izmed študij je bilo ugotovljeno, da »23% uporabnikov legitimnost strani presoja po vsebini in ne preverjajo enolični krajevnik vira (ang. *Uniform Resource Locator*), mnogi tudi ne razumejo sestave domenskih imen (Dhamija v Mannan 2007, 3).« Druga študija na primer kaže, da je »samo 35% sodelujočih uporabnikov opazilo predpono https v enoličnem krajevniku vira. Nekateri med tistimi, ki so jo opazili, pa niso razumeli pomena te predpone v primerjavi s predpono http. Skoraj 45% sodelujočih pa sploh ni preverilo, kaj je bilo zapisano v enoličnem krajevniku vira (Downs v Mannan 2007, 3).« Pričakovanja bank, da bodo uporabniki znali sami preverjati legitimnost strani so se v realnosti izkazala za povsem nerealistična.

Ribarjenje je za povprečnega uporabnika zelo nevarno, medtem ko bi tehnično spretnejši uporabniki hitro ugotovili, da gre za poskus prevare. Pri elektronski pošti je zelo preprosto ponarediti naslov pošiljatelja, zato je najboljši način, na katerega se lahko uporabnik zavaruje, da v pristnost takšnih sporočil vsakokrat podvomi. Banka od uporabnika ne bo nikoli zahtevala, da ji posreduje gesla (Varni na Internetu 2013). V Sloveniji so takšni napadi pogosti. V letu 2014 so pri Si-CERT (Slovenian Computer Emergency Response Team) obravnavali 279 prijav, leta 2015 pa 83. (Si-CERT 2016b, 22) Besedila na srečo uporabnika praviloma vsebujejo zelo polomljeno slovenščino, zaradi česar uporabnik največkrat podvomi v avtentičnost prejetega sporočila. Zanimivo je, da banke informacijo o novem valu napadov pogosto dobijo od uporabnikov, ki jezno pokličejo zaradi napačne rabe slovenščine in ne od uporabnikov, ki bi to pravilno prepoznali kot napad.

Slika 4.1: Primer ribarjenja v polomljeni slovenščini



Vir: Si-CERT (2016c).

4.2 Zvabljanje

Zvabljanje (ang. *Pharming*) je podobno ribarjenju, vendar za razliko od tega ne zahteva sodelovanja uporabnika. Napadalci na različne načine preusmerijo povezavo na lažno stran. Čeprav uporabnik vnese pravi naslov elektronske banke, je kljub temu preusmerjen na lažno stran. Pod tem imenom se dejansko skriva več različnih vrst napadov. Lahko gre za spremembo *hosts* datoteke v računalnikih z operacijskim sistemom Windows, zlorabljen usmerjevalnik (ang. *Router*), lažno brezžično točko dostopa ali pa zlorabljen DNS servis.

4.3 Mož v sredini

Mož v sredini (ang. *Man-in-the-Middle*) je način napada, kjer se napadalec vrine v komunikacijo med uporabnikom in ciljnim strežnikom. V literaturi se namesto dolgega opisa uporablja kar okrajšava MitM. »Ta način napada je uspešen samo, če se lahko napadalec uspešno izdaja za legitimnega uporabnika, tako uporabniku kot ciljnemu strežniku. Uporaba SSL avtentikacije obojestransko zaupanega overitelja zagotavlja močno zaščito proti MitM

napadom (Gemalto 2016, 9).«

Čeprav po besedah podjetja Gemalto SSL avtentikacija zagotavlja močno zaščito, pa ne smemo pozabiti na vlogo uporabnika. Napad lahko namreč še vedno uspe, če uporabnik ignorira vsa varnostna obvestila brskalnika pri vzpostavitvi SSL seje.

4.4 Škodljiva programska oprema

Škodljiva programska oprema (ang. *Malware*) je termin za različne vrste škodljivih programov.

Najpogostejši tipi škodljive programske opreme so:

- Virusi, ki se samodejno širijo in okužijo računalnik,
- Trojanski konji, ki pod pretvezo koristne aplikacije škodujejo uporabniku,
- Črvi, ki se širijo prek omrežja,
- Vohunsko programje (ang. *Spyware*), ki omogoča krajo uporabnikovih podatkov in nadzor nad sistemom,
- Oglaševalsko programje (ang. *Adware*), ki uporabniku prikazuje nezaželene oglase,
- Izsiljevalsko programje (ang. *Ransomware*), ki zašifrira uporabnikove datoteke in zahteva plačilo za dešifriranje podatkov.

Škodljiva programska oprema je najnevarnejša grožnja, saj ima napadalec v tem primeru popolno kontrolo nad uporabnikovim računalnikom. Po ocenah APWG (Anti Phishing Work Group) je število okuženih računalnikov izjemno visoko. Na Kitajskem je okuženih 51% računalnikov, medtem ko se ta odstotek v evropskih državah giblje med 20% in 25% (povzeto po APWG 2016, 8).

Mož v brskalniku

»Mož v brskalniku (ang. *Man-in-the-Browser*) ali na kratko MitB je trojanski konj, ki okuži uporabnikov brskalnik in prestreza ter spreminja podatke poslane s strani uporabnika, še predno dosežejo varnostne mehanizme brskalnika. Pri MitB napadu gre za zmožnost spreminjanja spletne strani in vsebine transakcij na način, ki je za uporabnika in ciljno aplikacijo neopazen (Gemalto 2016, 8).« »V trenutku, ko je računalnik okužen s škodljivo

programsko opremo, lahko napadalec naredi vse, kar lahko dela tudi uporabnik, in to počne v njegovem imenu. Če se uporabnik prijavi v elektronsko banko, medtem ko je njegov računalnik okužen, lahko napadalec izvede katerokoli transakcijo, ki jo lahko izvede tudi uporabnik (Gemalto 2016, 9).«

Tak napad je zelo nevaren, od napadalca pa zahteva več tehničnega znanja. Večinoma so takšni napadi usmerjeni proti pravnim osebam, vseeno pa se dogajajo tudi napadi na fizične osebe. Zelo znani so primeri okužb s trojanskimi konji, kot so *Zeus, Silentbanker* ali *Spy Eye,* s katerimi so uspešno okužili na milijone računalnikov (povzeto po Entrust 2014, 5).

Seveda pa je za vsak napad vedno na voljo tudi obramba. »Proti napadom MItM in MItB se lahko zaščitimo z uvedbo mehanizma za preverjanje izvršene transakcije (plačila) na način, da je zagotovljeno načelo »sign what you see« (podpiši, kar vidiš op. a). Še posebej je to zagotovilo pomembno pri izvajanju novih transakcij (plačevanje na nov račun) (Moj mikro v Zupan in Bernik 2012, 6).« Tudi pri podjetju Entrust, kot učinkovito obrambo proti napadom MitB priporočajo uporabo ločenega kanala za preverjanje transakcije, kot je na primer mobilni telefon (povzeto po Entrust 2014, 17).

5 Varnostni mehanizmi v elektronskem bančništvu

Po besedah Zupanove in Bernika varnost elektronske banke na strani uporabnika zagotavljamo na treh segmentih:

- vzpostavitev varne povezave s pomočjo šifriranega kanala med e-banko in komitentom.
- dostop do e-banke in njenih storitev (identifikacija in avtentikacija)
- izvajanje plačnih transakcij v e-banki (avtorizacija)

(Zupan in Bernik 2012, 4)

Zupanova in Bernik izpostavljata uporabnika kot ključen člen varnosti. »Uporabnik mora poskrbeti za primerno zaščito informacijskih sredstev uporabljenih v procesu poslovanja z e-banko. Pri tem veljajo splošna navodila za boljše varovanje osebnih elektronskih identifikacijskih elementov ter računalniškega okolja: redno nameščanje varnostnih popravkov/ nadgradenj ter posodabljanje operacijskega sistema, brskalnika, antivirusne in ostale programske opreme idr. Primerna zaščita uporabnikov v 80% primerih zmanjša verjetnost zlorab (Zupan in Bernik 2012, 4).«

Tudi Peotta in drugi (2011, 194) so izpostavili uporabnika kot ključen člen. Uporabnik in njegova naprava za dostop do elektronske banke naj bi predstavljala najšibkejši člen v varnostni verigi. »V večini primerov varnost avtentikacijskega in avtorizacijskega procesa v elektronskem bančništvu temelji na skrivni informaciji, ki naj bi jo poznal samo uporabnik in ohranjal njeno tajnost. Zaradi teh težav morajo biti novi modeli avtentikacije in identifikacije čim bolj neodvisni od uporabnika ali varnosti naprave, ki jo uporablja, in naj se za potrebe avtentikacije in identifikacije zanašajo na več kot en vir (Peotta in drugi 2011, 194).«

Podobno pravi tudi Vodopivec. »Če bi uspeli zagotoviti varnost računalnika na strani uporabnika, smo že skoraj zmagali. Žal pa se je to v praksi izkazalo za nedosegljiv cilj. Sam uporabnik lahko tu veliko naredi, banka pa precej manj (Vodopivec v Sušnik 2010).« Vodopivec tudi pravi, da se mora fokus varovanja pri elektronskem bančništvu premakniti od identifikacije in avtentikacije uporabnika, kjer je varnost vsaj v Sloveniji že zadovoljiva, k avtorizaciji transakcije, kjer se odpira nova fronta v boju proti zlorabam. »Danes menim, da mora zaradi napadov na brskalnik, ko napadalci vskočijo v sejo šele tam, kjer je uporabnik že

prijavljen, biti ključna točka varovanja transakcija, predvsem rizična transakcija. Kaj je rizična transakcija, je ohlapen pojem. To je, recimo, nakazilo na račun, na katerega uporabnik še nikoli ni nakazoval, zelo visok znesek transakcije, Western Union Money Transfer in podobna nakazila (Vodopivec v Sušnik 2010).«

5.1 Avtentikacija strežnika

Avtentikacija strežnika je prvi obrambni zid, ko obiščemo spletno stran elektronske banke. Ob obisku varne spletne strani, se mora strežnik na katerega dostopamo najprej avtenticirati s strežniškim digitalnim potrdilom. Brskalnik na podlagi prejetega digitalnega potrdila prepozna ali je spletna stran vredna zaupanja in v primeru varnostnih tveganj opozori uporabnika ali vseeno želi obiskati spletno stran.

SSL / TLS

Transport Layer Security (TLS) in njegov predhodnik Secure Sockets Layer (SSL) sta kriptografska protokola, ki omogočata varno komunikacijo prek interneta. Čeprav se SSL v zadnjem času zaradi nižje varnosti ne uporablja več, se še vedno uporablja okrajšava SSL, čeprav je govora o novejšem TLS standardu. Vse elektronske banke in druge spletne strani, ki zagotavljajo varno komunikacijo, uporabljajo TLS standard. Nekatere sicer podpirajo še starejši SSL 3 standard, vendar je takšnih strani vedno manj.

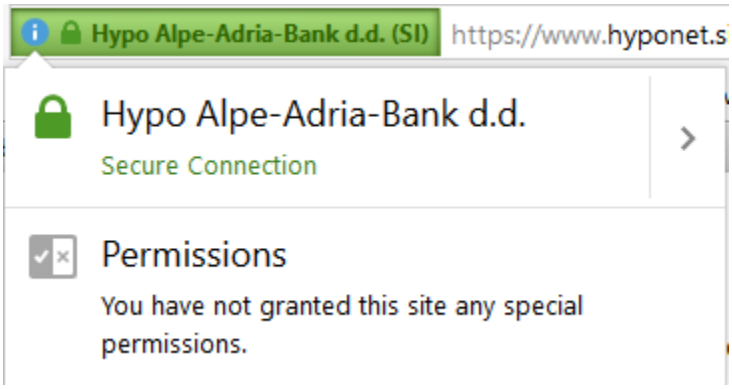
Protokol SSL je sestavljen iz dveh delov:

- *SSL Handshake Protocol - omogoča usklajevanje algoritmov, overjanje strežnika in odjemalca, prenos digitalnih potrdil in določitev skupnega ključa za simetrični kriptoalgoritem;*
- *SSL Record Protocol - definira osnovni format izmenjanih podatkov, zagotavlja neokrnjenost in šifriranje.*

Strežnik in odjemalec pri vzpostavitvi povezave najprej na podlagi prvega protokola preverita identiteto drug drugega, uskladita kriptografske algoritme ter si varno izmenjata ključe in ostale podatke, ki so potrebni za morebitno kasnejše šifriranje. Ko je postopek preverjanja, usklajevanja kriptografskih algoritmov, ki jih bosta uporabljala, ter izmenjave ključa za simetrično šifriranje končan, lahko s pomočjo drugega protokola začneta s pošiljanjem podatkov. (Jerman-Blažič in drugi 2001, 119–120)

SSL in TLS sta tako namenjena predvsem sami avtentikaciji strežnika in zagotavljanju varne povezave. Uporabnik lahko na ta način preveri, da je strežnik, na katerega se je povezal, avtentičen, prav tako pa je lahko prepričan, da nihče ne more prisluškovati komunikaciji med njim in strežnikom ter kakorkoli manipulirati podatke. Manaan opozarja da, »čeprav digitalno potrdilo avtenticira spletno stran, to seveda ne pomeni, da jo tudi zavaruje. Škodljiva programska oprema na računalniku lahko brez težav dostopa do vseh uporabnikovih podatkov, tudi če so zavarovani z SSL protokolom (Mannan 2007, 3).« Opozarja tudi na lažne spletne strani in pravi da, »mnoge spletne strani namenjene lažnemu predstavljanju prikazujejo zaklenjeno ključavnico v oknu brskalnika, da bi uporabnika prepričale, da je stran varna, kar pa ne pomeni, da stran resnično uporablja SSL. Povprečen uporabnik praviloma ne ve, da lahko katerakoli stran znotraj svoje vsebine prikaže kakršnokoli ikono ali tekst, ki si jo zaželi ustvarjalec strani (Mannan 2007, 3).«

Slika 5.1: Prikaz varne povezane na primeru brskalnika Firefox

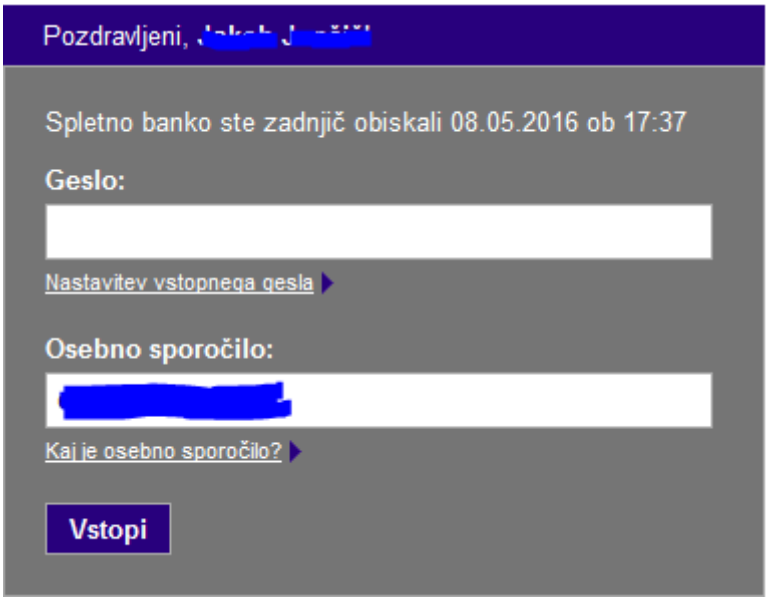


Osebno sporočilo

Osebno sporočilo je v Sloveniji pogosto uporabljena komplementarna metoda avtentikacije strežnika, zato jo bomo na kratko opisali. Uporablja se pri bankah, ki za identifikacijo in avtentikacijo uporabnika uporabljajo digitalna potrdila. V primeru uporabe digitalnega potrdila, banka že na vstopni strani, na podlagi podatkov zapisanih v digitalnem potrdilu, ve, kdo je uporabnik, ki želi vstopiti v elektronsko banko. Uporabniku se tako na vstopni strani prikaže osebno sporočilo, ki si ga je sam nastavil. Zlonamerna stran, ki bi se izdajala za elektronsko banko, nima informacije, kakšno je to osebno geslo. Ko uporabnik obišče takšno stran, lahko opazi, da osebnega gesla ni ali, da je napačno. Uporabnik, ki ima dovolj znanja o

varnosti, postopek vstopa zaustavi in se za pomoč obrne na bančno podporo.

Slika 5.2: Prikaz osebnega sporočila v NLB Klik



5.2 Identifikacija in avtentikacija uporabnika

»V uporabi so različne metode identifikacije (postopek prepoznavanja uporabnika pri dostopu v informacijski sistem) in avtentikacije (preverjanje istovetnosti identitete) uporabnika. npr. uporabniško ime je element identifikacije, geslo pa element avtentikacije. Povečevanje naporov v zaščito »vhodnih vrat« v e-banko učinkovito zmanjša možnost zlorab (Zupan in Bernik 2012, 4).«

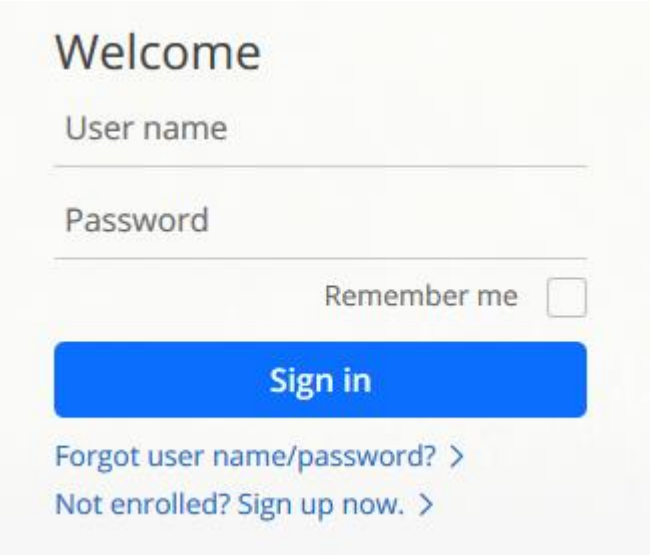
Uporabniško ime in geslo

Varnostni mehanizem, kjer se za identifikacijo in avtentikacijo uporabnika uporablja kombinacija uporabniškega imena in gesla je najpreprostejši način varnosti. Uporabniško ime je element identifikacije, geslo pa element avtentikacije (Zupan in Bernik 2012, 4). Implementacije se med seboj razlikujejo glede na predpisano dolžino uporabniškega imena in gesla, dovoljenimi znaki in ostalimi omejitvami. Čeprav ne gre za najbolj varen varnostni mehanizem, pa določene implementacije to varnost še dodatno znižajo z umetnimi omejitvami, kot so pretirano omejeno število znakov, zmanjšan nabor znakov, ki jih uporabnik lahko vpiše in odsotnostjo kontrole za preprečevanje vnosa najpogostejših gesel.

Ta varnostni mehanizem je zelo ranljiv v primeru ribarjenja, saj si je napadalec s tem praktično že zagotovil vse potrebne informacije, ki jih potrebuje za uspešen napad. Zupan in

Bernik (2012, 6) pravita, da v rešitvah, kjer je za avtentikacijo uporabljeno zgolj uporabniško ime in statično geslo obstaja nevarnost napadov z zvabljanjem in ribarjenjem ter nevarnost odtujitve gesel s pomočjo namenskih programov. Dodatno težavo predstavlja tendenca uporabnikov k uporabi enakih kombinacij uporabniškega imena in gesla na različnih spletnih straneh. Das in drugi (2014, 13) so ugotovili, da kar 43% uporabnikov uporablja enaka gesla, mnogi drugi pa gesla samo malenkostno spremenijo. Kraja gesel na kakšni nepomembni spletni strani tako pomeni grožnjo za vsakega uporabnika, ki preveč brezskrbno uporabi enako kombinacijo tudi za vstop v svojo elektronsko banko.

Slika 5.3: Primer vnosnega polja pri banki Chase



Vir: Chase (2016).

Kombinacija uporabniškega imena in gesla se pogosto uporablja v kombinaciji z dodatnimi varnostnimi vprašanji, kot je na primer dekliški priimek matere. Vnos teh vprašanj elektronska banka zahteva na primer takrat, ko se uporabnik prijavi iz neznanega računalnika. Vprašanja so kljub temu dovolj preprosta, da jih napadalec lahko pridobi iz drugih virov, saj mnogi uporabniki na straneh, kot je npr. Facebook idr., javno objavljajo informacije zasebne narave.

Nobena banka v Sloveniji ne uporablja opisanega načina identifikacije in avtentikacije uporabnika. Tudi prve slovenske elektronske banke so konec devetdesetih že od začetka uporabljale precej močnejši varnostni mehanizem v obliki digitalnih potrdil.

Digitalno potrdilo

Digitalno potrdilo ali digitalni certifikat je elektronska datoteka namenjena identifikaciji in je po Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ekvivalentna osebni izkaznici ali potnemu listu. Digitalno potrdilo je namenjeno identifikaciji uporabnika, medtem ko se za avtentikacijo praviloma uporablja geslo.

Digitalno potrdilo praviloma vsebuje sledeče podatke:

- Enolično oznako digitalnega potrdila,
- ime ali naziv lastnika javnega ključa,
- uporabnikov javni ključ,
- namen uporabe,
- čas veljavnosti digitalnega potrdila,
- ime algoritma, s katerim je podpisano digitalno potrdilo,
- naziv overitelja, ki je izdal digitalno potrdilo,
- podpis overitelja.

14. člen ZEPEP daje elektronskemu podpisu enak pomen kot lastnoročnemu, kar pomeni, da mora vse našteto veljati tudi za elektronski podpis. Označevati mora dokončnost, pristnost, istovetnost s podpisnikom, izvirnost dokumenta in podpisa. Vendar ni vsak elektronski podpis enakovreden lastnoročnemu: 15 člen ZEPEP namreč določa, da je le varen elektronski podpis, overjen s kvalificiranim potrdilom, enakovreden lastnoročnemu.

Varen elektronski podpis pa mora izpolnjevati naslednje zahteve:

- *povezan je izključno s podpisnikom,*
- *iz njega je mogoče zanesljivo ugotoviti podpisnika,*
- *ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom,*
- *povezan je s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave med njimi.* (Ciglarič 2007, 179)

Digitalni potrdilo imamo lahko shranjeno na računalniku, kjer za varnost skrbi operacijski sistem ali pa na pametni kartici. S stališča varnosti je namestitev na pametno kartico boljša izbira, vendar za uporabnika to pomeni dodaten strošek, ker mora kupiti strojno opremo ter

poskrbeti za namestitev programske opreme. Tudi prenos digitalnega potrdila z računalnika na pametni USB-ključek je lahko za povprečnega uporabnika kar trd oreh (Krisper 2013a). Zupan in Bernik o tem pravita: »Dostop do potrdila na trdem disku nadzira operacijski sistem, ki je ranljiv na vrsto napadov, zato je taka hramba zelo tvegana. Poleg tega se pri hrambi potrdila na disku generirani zasebni ključ začasno shrani v RAM, od koder ga je kasneje možno odtujiti. Tehnologija pametnih kartic in pametnih USB ključev ne dopušča izvoza zasebnega ključa, zato jo uvrščamo med bolj primerne metode (Zupan in Bernik 2012, 6).« Če ima napadalec dostop do računalnika, kjer je nameščeno digitalno potrdilo, lahko v imenu lastnika tudi vstopi v elektronsko banko in digitalno podpisuje dokumente.

Glede varnosti digitalnih potrdil Zupanova in Vodopivec navajata sledeče:

> *Uporaba digitalnega potrdila sicer omogoča obrambo pred ribarjenjem in napadi tipa MitM, ne omogoča pa zadostne obrambe pred MitB napadi. Elektronski podpisi transakcije z digitalnimi potrdili za napadalce predstavljajo oviro, vendar ne pomagajo pri kraji certifikata in zasebnega ključa. Pri napadu MitB mora napadalec ponarediti še prikaz podatkov ob podpisu, kar je manj verjetno a ni nemogoče*. (Zupan in Vodopivec v Zupan in Bernik 2012, 6)

Lahko torej rečemo, da je varnost digitalnih potrdil dobra, vendar je elektronska banka v primeru, da je to edini uporabljen varnostni mehanizem, ranljiva. Nameščena škodljiva programska oprema, ki napadalcu omogoča nadzor nad računalnikom ali pa uspešno izvedeno ribarjenje, pri katerem uporabnik napadalcu lastnoročno izvozi in pošlje digitalno potrdilo, napadalcu zagotovita vse potrebno za izvedbo zlorabe.

Uporaba digitalnega potrdila je za uporabnika preprosta, prevzem in namestitev pa sta za uporabnika že malce trši oreh. Napaka pri prevzemu pogosto pomeni, da je potrebno uporabniku izdati novo digitalno potrdilo. Digitalna potrdila so tudi časovno omejena, zato morajo uporabniki postopek na nekaj let obnavljati. Po navadi veljavnost digitalnega potrdila poteče v treh oziroma petih letih, za obnovo pa je treba plačati do 15 evrov (Krisper 2013a). Banke se trudijo postopek prevzema in namestitve čim bolje opisati, vendar je ta od primera do primera drugačen, glede na uporabljen operacijski sistem, verzijo operacijskega sistema ter glede na uporabljen brskalnik in verzijo brskalnika. Vemo, da nastane težava tudi v primeru menjave računalnika, ker zahteva postopek izvoza digitalnega potrdila na strani uporabnika

nekaj tehničnega znanja. Uporabniki si ob prevzemu praviloma ne naredijo varnostne kopije ali pa si svoj privatni ključ zaklenejo z dodatnim geslom, ki ga sčasoma pozabijo.

Enkratno geslo (OTP)

Enkratno geslo (ang. *One-time password*) ali na kratko OTP je za razliko od običajnega gesla veljavno samo enkrat. Ko je geslo uporabljeno, istega gesla ni možno več ponovno uporabiti. Enkratna gesla tako niso ranljiva na ponovitvene napade (ang. *Replay attack*). Tudi v primeru da nam napadalec geslo prestreže, ga ne more ponovno uporabiti, saj je bilo že porabljeno. Obstaja več različnih implementacij enkratnih gesel. Najpreprostejša oblika je spisek veljavnih gesel. Ko uporabnik vsa gesla porabi, mora od banke prejeti nov spisek. Ko govorimo o enkratnih geslih, praviloma mislimo na strojne naprave v obliki ključkov ali v novejšem času tudi namensko programsko opremo na mobilnem telefonu. Naprednejše verzije teh naprav omogočajo tudi dvostopenjsko overjanje (ang. *Two-factor authentication*). Za uporabo se zahteva nekaj kar uporabnik ima (OTP generator, mobilni telefon..) in nekaj kar uporabnik ve (PIN). Enkratna gesla so namenjena avtentikaciji uporabnika, medtem ko je za identifikacijo praviloma potrebno vpisati uporabniško ime.

Enkratna gesla so, kakor digitalna potrdila, prav tako ranljiva na večino običajnih napadov, zato je priporočljivo, da banka zahteva dvostopenjsko dodatno avtorizacijo transakcije. »Podatki o zlorabah v tujini kažejo, da gesla za enkratno uporabo, ki jih lahko uporabljamo za vstop v storitev in za potrditev posameznega plačila, ne zagotavljajo zadostne stopnje varnosti. Če je geslo neodvisno od vsebine transakcije, namreč delujejo tudi napadi tipa MitB, kjer napadalec nadzira uporabnikov brskalnik in zamenja le ciljni račun in znesek transakcije (RIS v Zupan in Bernik 2012, 6).«

Slika 5.4: RSA SecurID generator enkratnih gesel

Vir: RSA (2016).

Za razliko od digitalnih potrdil enkratna gesla ne zahtevajo namestitve dodatne programske opreme. Uporabnik lahko do svoje elektronske banke dostopa iz katerekoli naprave, če seveda ima pri sebi generator enkratnih gesel. Nekatere vrste enkratnih gesel, kot na primer RSA SecurID, ne zahtevajo niti vnosa dodatne PIN številke, tako da si mora uporabnik zapomniti samo svoje uporabniško ime. S stališča uporabniške izkušnje je to preprostejše, vendar vnos dodatne PIN številke predstavlja dodatno stopnjo varnosti. Takšni generatorji prav tako ne omogočajo dvostopenjskega overjanja. Opažamo, da se vedno pogosteje uporabljajo tudi programski generatorji enkratnih gesel, ki si jih uporabnik namesti na svoj mobilni telefon.

5.3 Avtorizacija transakcije

Avtorizaciji transakcije je v zadnjem času namenjeno veliko pozornosti. Avtorizacija transakcije predstavlja za napadalca zadnjo oviro, ki je v primeru dobre implementacije praktično nepremostljiva. Opisali bomo nekaj najpogostejših varovalnih mehanizmov za avtorizacijo transakcij, ki so v uporabi v Sloveniji in po svetu.

Zupanova in Bernik (2012, 4) varnostne mehanizme, ki se uporabljajo za avtorizacijo transakcij, delita na dve vrsti, glede na število uporabljenih avtorizacijskih faktorjev:

- enostopenjski avtorizacijski faktor (uveljavitev statičnega ali dinamičnega gesla za izvedbo avtorizacije transakcije)
- dvostopenjski avtorizacijski faktor (avtorizacijski podatki za izvedbo avtorizacije transakcije so sestavljeni iz dela transakcijskih podatkov in dela avtorizacijskih podatkov).

Razlog za to delitev je v stopnji varnosti, ki jo zagotavljata ta dva pristopa. Enostopenjski avtorizacijski faktor je ranljiv za naprednejše napade tipa MitB, kjer napadalec spremeni ciljni račun in znesek. Dvostopenjski avtorizacijski faktorji močno zmanjšajo verjetnost zlorabe. Lahko bi celo rekli, da jo povsem preprečijo, vendar lahko vztrajnost napadalcev v kombinaciji z naivnostjo uporabnikov, našo trditev hitro ovrže. Po besedah avstrijske nacionalne banke je bistvena lastnost dvostopenjskih avtorizacijskih faktorjev ta, da je »vsaka posamezna transakcija predhodno overjena in avtorizirana (npr. z vnosom sestavljenega PIN-a ali digitalnega podpisa transakcije). Druga pomembna lastnost dvostopenjske avtorizacije je, da napadalec zgolj s krajo avtentikacijskih podatkov ne more izvajati plačil, saj je geslo časovno omejeno in poleg tega za izvedbo napada potrebuje še aktivno sejo in elemente

avtorizacije (pri dvojni avtorizaciji gre običajno tudi za več uporabljenih mehanizmov, nekaj, kar uporabnik ve in nekaj, kar uporabnik ima) (Oesterreichische nationalbank v Zupan in Bernik 2012, 5).«

Digitalni podpis

Digitalni podpis je varnostni mehanizem, ki se v Sloveniji uporablja pred izvedbo transakcije. Ni sicer nujen pogoj, a uporablja se pri bankah, ki za vstop uporabljajo digitalna potrdila, saj je za sam digitalni podpis potrebno imeti digitalno potrdilo. Jerman Blažič digitalni podpis opiše kot postopek, »ki temelji na kombinaciji asimetričnih algoritmov in funkcije zgoščevanja. Ker pri podpisovanju ne gre primarno za zaščito vsebine pred vpogledom, temveč predvsem za povezavo podpisnika z vsebino in zaščito vsebine pred spreminjanjem, sam proces temelji na izdelavi prstnega odtisa podatkov (Jerman Blažič 2004).« Prstni odtis dobimo tako, da na podatkih, ki jih podpisujemo, uporabimo zgoščevalno funkcijo (ang. *Hash*) in jih potem šifriramo s svojim tajnim ključem. Prejemniki tega dokumenta lahko preverijo identiteto podpisnika in celovitost dokumenta. »Prejemnik digitalni podpis preveri tako, da najprej izračuna izvleček sporočila. Nato s pomočjo pošiljateljevega javnega ključa odklene prejeto originalno zgoščeno vrednost in obe primerja. Če se ujemata, je sporočilo verodostojno in identiteta pošiljatelja je potrjena, V tem primeru pošiljatelj ne more zanikati, da je res on poslal sporočilo (Ciglarič 2007, 78).« Če se podpis ne ujema, sklepamo, da je bil dokument po podpisu spremenjen in podpis ni veljaven. Kaj je to zgoščevanje, nam dobro opiše Ciglarič.

> *Zgoščevanje je preslikava, ki za poljubne vhodne podatke (na primer dokument poljubne dolžine) poišče izhodno vrednost fiksne dolžine, ki ji rečemo digitalni izvleček (digest), prstni odtis (fingerprint) ali zgoščena vrednost (hash) dokumenta. Ker je izhodna vrednost - izvleček - fiksne dolžine, vhodnih vrednosti pa je možnih neskončno mnogo, je načeloma možno, da imata dva različna dokumenta isto vrednost izvlečka, vendar pa je zelo malo verjetno, da bomo našli tak primer. Zgoščevanje je enosmerna preslikava. Iz izvlečka je nemogoče ugotoviti vsebino originalnega dokumenta. Že ob majhni spremembi dokumenta se izvleček močno spremeni in zelo težko, če ne celo praktično nemogoče, je za dani dokument poiskati še enega, ki ima enak izvleček.* (Ciglarič 2007, 178)

Digitalni podpis je tehnično sicer dobra rešitev, vendar se v svetu nikoli ni uveljavil kot pogosto uporabljen varnostni mehanizem. Čeprav se je poskušalo postopek standardizirati, je

trenutno stanje še vedno enako kot pred 20 leti. Za podpisovanje se uporabljajo namensko razvite komponente, ki od uporabnika za pravilno delovanje in namestitev pogosto zahtevajo veliko tehničnega znanja. Nadgradnje operacijskih sistemov, brskalnikov, Java platforme in drugih programskih delov računalnika po naših izkušnjah pogosto povzročijo nedelovanje in posledično slabo voljo uporabnikov.

CAPTCHA

CAPTCHA (ang. *Completely automated public turing test to tell computers and humans apart*) sicer ni varnostni mehanizem, ki bi se ga uporabljalo za avtorizacijo transakcij. Omenjamo ga predvsem kot spremljevalni varnostni mehanizem, ki ga mnoge slovenske banke uporabljajo kot del digitalnega podpisa. Predstavlja dodaten varovalni mehanizem v primeru avtomatiziranih vdorov, saj mora napadalec v tem primeru s pomočjo OCR algoritmov prebrati vsebino slike. Peotta in drugi (2011, 189) pravijo, da je to metoda uporabljena v določenih bančnih sistemih, katere namen je napraviti avtomatizirane napade na avtenticirane seje neučinkovite. Ta metoda od legitimnega uporabnika zahteva, da vnese informacijo, prikazano na zamaskirani sliki, ki jo avtomatizirani roboti težko obdelajo in prepoznajo.

Slika 5.5 Primer vnosa CAPTCHA kode pri digitalnem podpisu

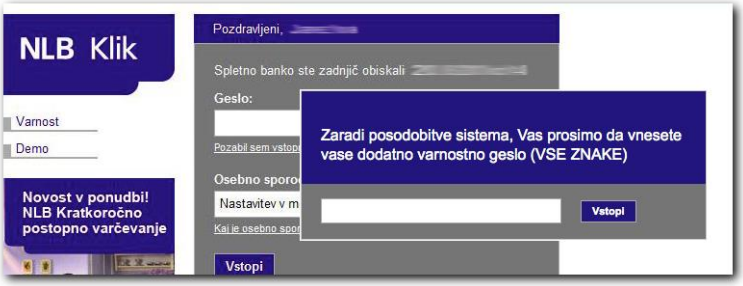
Vir: Poštna banka Slovenije d.d. (2016).

Virtualna tipkovnica

Namen virtualne tipkovnice je, da oteži krajo gesel. Ideja je preprosta, saj mora uporabnik namesto po pravi fizični tipkovnici z miško klikati po tipkovnici prikazani v brskalniku. Na ta način kraja gesla prek beležnika tipkanja (keylogger) ni mogoča. V Sloveniji takšen koncept varnostnega mehanizma pod imenom »dodatno varnostno geslo« uporablja Nova Ljubljanska banka d.d. za namene potrjevanja transakcij, ki niso izvedene po funkcionalni hitrih plačilih, ter pri plačilih v tujino in nakazilih denarja skozi Western Union sistem. Uporabnik dobi pri

tem načinu varovanja dodatno varnostno geslo v obliki dokumenta, s pomočjo katerega na virtualni tipkovnici z miško vnese dva naključno izbrana znaka, ki ju zahteva sistem, vsakokrat v drugi kombinaciji (povzeto po Nova Ljubljanska banka d.d. 2016).

Slika 5.6: Primer ribarjenja, ki zahteva vnos gesla za virtualno tipkovnico v NLB Klik



Vir: Si-CERT (2016a).

Slabost tega varnostnega mehanizma s stališča uporabnosti je, da lahko uporabnik zelo hitro založi dokument, na katerem je geslo zapisano. V tem primeru mora uporabnik od banke zahtevati nov dokument in posledično nekaj dni ne more izvrševati transakcij, ki zahtevajo vnos dodatnega varnostnega gesla. Kot lahko vidimo na zgornji sliki, je ta varnostni mehanizem ranljiv v primeru ribarjenja.

Dodatni vnos enkratnega gesla

Banke, ki za vstop uporabljajo enkratno geslo, pogosto uporabljajo isti mehanizem tudi za avtorizacijo transakcije. Čeprav bi morda napadalec ukradel enkratno geslo za vstop, bi ob poskusu nakazila moral ponovno vpisati geslo, ki ga nima. V primeru preprostejše metode generiranja enkratnega gesla, uporabnik izvede enak postopek kot v primeru vstopa v elektronsko banko. Boljše rešitve za generiranje enkratnega gesla uporabijo tudi podatek o znesku in računu prejemnika, s čimer lahko preprečijo napade tipa MitB. »Podatki o zlorabah v tujini kažejo, da so rešitve z gesli za enkratno uporabo, ki jih lahko uporabljamo za vstop v storitev in potrditev posameznega plačila, ranljive na napad MItB. Geslo, ki je neodvisno od vsebine transakcije, napadalec lahko pridobi s tem, da nadzira uporabnikov brskalnik in zamenja le ciljni račun ter znesek transakcije (RIS v Zupan in Bernik 2012, 6).«

Slika 5.7: Primer dodatnega vnosa enkratnega gesla

Vir: Addiko Bank d.d. (2016).

SMS potrjevanje

V zadnjem času je z razmahom mobilne telefonije zelo aktualen mehanizem za avtorizacijo transakcij postalo SMS potrjevanje. V sporočilu lahko banka poleg kode pošlje tudi osnovne informacije o plačilu, ki ga bo uporabnik potrdil. To preprečuje napade tipa MitB, kjer napadalec spremeni podatke o prejemniku, saj uporabnik v samem sporočilu vidi, če so bili podatki spremenjeni. Seveda mora biti uporabnik pozoren na vsebino sporočila. Dodatna prednost je v tem, da je mehanizem za avtorizacijo v tem primeru ločen od mehanizma za identifikacijo in avtentikacijo. Verjetnost, da bi imel napadalec poleg sredstva za avtentikacijo nadzor še nad uporabnikovim mobilnim telefonom je izredno majhna.

Slika 5.8: Primer prejete varnostne kode prek SMS

Vir: Addiko Bank d.d. (2016).

6 Razlogi za uvedbo dodatnih varnostnih mehanizmov

6.1 Pravni vidik

V Sloveniji je leta 2000 začel veljati Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). V njem je zakonsko urejeno vprašanje uporabe digitalnih podpisov, ki ga še danes mnoge slovenske banke uporabljajo za avtorizacijo transakcij. Zakon ne predpisuje varnostnih mehanizmov, vendar je zakonska ureditev digitalnih podpisov bankam omogočila, da so nekatere storitve, ki so prej zahtevale obisk poslovalnice, uporabnikom ponudile tudi prek spleta. Razlog se skriva v izenačitvi digitalnega podpisa z lastnoročnim. V 15.členu ZEPEP je zapisano: »Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.”

Zakon v 37. in 38. členu predpisuje tudi tehnične zahteve za varno elektronsko podpisovanje.

37. člen

(1) Sredstva za varno elektronsko podpisovanje morajo z uporabo ustreznih postopkov in infrastrukture zagotavljati naslednje:

1. *podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena;*
2. *podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa, elektronski podpis pa je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije;*
3. *podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom.*

(2) Sredstvo za varno elektronsko podpisovanje ne sme spremeniti podatkov, ki se podpisujejo ali preprečiti prikaza podatkov podpisniku pred podpisom.

38. člen

(1) Med postopkom preverjanja varnega elektronskega podpisa mora biti z uporabo ustreznih postopkov in infrastrukture zagotovljeno naslednje:

1. *podatki, ki se uporabljajo za preverjanje elektronskega podpisa, morajo biti enaki podatkom, ki so prikazani uporabniku;*
2. *podpis mora biti zanesljivo preverjen in rezultati preverjanja ter identiteta podpisnika pravilno prikazani uporabniku;*
3. *uporabnik lahko zanesljivo ugotovi vsebino podpisanih podatkov;*
4. *pristnost in veljavnost potrdila morata biti preverjeni v času preverjanja podpisa;*
5. *raba psevdonima mora biti jasno označena;*
6. *vse spremembe, ki kakorkoli vplivajo na varnost elektronskega podpisa, morajo biti ugotovljene.*

(Ur. l. RS 98/2004)

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje v tretjem podčlenu 26 člena, predpisuje da:

Sredstvo za preverjanje varnega elektronskega podpisa mora uporabniku omogočati, da jasno ugotovi, kateri podatki in v kakšnem obsegu so bili podpisani. Če so podpisani podatki povezani z drugimi podatki ali se na druge podatke sklicujejo ter je uporabniku omogočen samodejen preskok na te podatke, mora sredstvo jasno opozoriti uporabnika, če ti podatki niso zajeti s preverjenim elektronskim podpisom.
(Ur. l. RS 77/2000)

Čeprav je slovenski zakonodajalec predpisal samo, kako naj elektronski podpis deluje, ne pa tudi obvezne uporabe, so ga mnoge banke kljub temu vpeljale v svoje rešitve. Z vstopom Slovenije v Evropsko unijo si z ostalimi državami delimo tudi vso zakonodajo.

Leta 2013 je Evropska centralna banka sprejela Priporočila za varnost spletnih plačil. Oblikoval jih je Evropski forum za varnost plačil malih vrednosti, SecuRe Pay (v nadaljevanju forum). Osnovni namen foruma je zagotoviti splošno poznavanje in razumevanje zadev povezanih z varnostjo elektronskih plačilnih storitev malih vrednosti. Cilj foruma je, da

se vzpostavi usklajena minimalna stopnja varnosti na območju Evropske unije in evropskega gospodarskega prostora. (povzeto po Evropska centralna banka 2013, 1)

Priporočila temeljijo na štirih vodilnih načelih in sicer:

- *Banke morajo izvajati ocene tveganj, povezanih z zagotavljanjem spletnih plačilnih storitev. Ocene je potrebno redno posodabljati v skladu z razvojem groženj varnosti na spletu in mehanizmov goljufij.*
- *Spletna plačila in dostop do občutljivih podatkov morajo biti zaščiteni z močno avtentikacijo strank. Občutljivi podatki so opredeljeni kot podatki, ki se lahko zlorabijo za goljufijo. Močna avtentikacija stranke je postopek, ki temelji na uporabi vsaj dveh elementov izmed poznavanja, lastništva in neločljive povezave. Lastništvo je nekaj kar ve samo uporabnik na primer geslo, koda ali osebna identifikacijska številka. Lastništvo je nekaj kar ima uporabnik. To je lahko žeton, pametna kartica ali pa na primer mobilni telefon. Neločljiva povezava pa je nekaj kar uporabnik je na primer prstni odtis.*
- *Banke morajo izvajati učinkovite postopke za odobritev transakcij ter prav tako za spremljanje transakcij in sistemov, da bi lahko prepoznali neobičajne vzorce plačevanja pri strankah in preprečili goljufije.*
- *Banke morajo sodelovati v programih za ozaveščanje in izobraževanje strank o varnostnih vprašanjih v zvezi z uporabo spletnih plačilnih storitev.*

(povzeto po Evropska centralna banka 2013, 2–3)

»Uporaba smernic je v Sloveniji postala obvezna avgusta 2015. Banka Slovenije, kot pristojen organ za nadzor nad bankami, je v Uradnem listu RS št. 47/2015 in št. 55/2015 objavila obvezno uporabo Smernic o varnosti spletnih plačil (Združenje bank Slovenije 2015).« Nekatere banke že sedaj ponujajo rešitve, ki ustrezajo novim smernicam, medtem ko bodo morale mnoge svoje rešitve še nadgraditi.

6.2 Stroškovni vidik

Poleg zakonskih zahtev je eden od glavnih razlogov za uvedbo dodatnih varnostnih mehanizmov tudi vedno večja škoda. Leto 2009 je bilo prelomno leto v porastu *on-line* kriminalnih dejanj. Škoda realiziranih *on-line* napadov je prvič v zgodovini presegla škodo v realnem svetu (povzeto po Ždrnja v Zupan in Bernik 2012, 3).

Čeprav Slovenija ni najmikavnejši cilj za napadalce se tudi pri nas dogajajo zlorabe. »V letu 2011 so odmevali predvsem phishing napadi. V letu 2010 beležimo še en odmeven dogodek in sicer s trojanskim botnetom Mariposa (poimenovan po španski kriminalni organizaciji), so preko 13.000 uporabnikom odtujili uporabniška imena, gesla in druge podatke za izvedbo napada (Slovenska policija v Zupan in Bernik 2012, 3).« »V letu 2012 je bil medijsko izpostavljen predvsem primer kraje denarnih sredstev podjetju iz okolice Kranja, in sicer so napadalci s kombinacijo socialnega inženiringa in namestitvijo trojanskega konja podjetju odtujili 105.000 EUR (Slovenska policija v Zupan in Bernik 2012, 3).«

V Sloveniji to področje ureja ZPlaSS (Zakon o plačilnih storitvah in sistemih, 2009, 2011), ki v 120. členu predpisuje odgovornost uporabnika do največ 150 EUR. Zneske nad tem krije banka, razen v primeru hude malomarnosti uporabnika. »Meja med hudo malomarnostjo uporabnika in nivojem povprečnega obvladovanja informacijske tehnologije s strani uporabnika je v praksi zabrisana, presoja o tem je na strani sodišča. Banke so postavljene pred nov izziv: rešitve e-bančništva urediti na način, da te ne bodo zahtevale naprednih znanj s področja informacijske tehnologije, bodo varne in hkrati čim bolj enostavne za uporabo in vzdrževanje (Zupan in Bernik 2012, 3).«

Zmanjšanje stroškov zaradi zlorab je banki v interesu, ker po slovenski zakonodaji večino stroškov prevzame banka, razen v primeru hude malomarnosti uporabnika. Znan je primer iz leta 2009, ko je bilo uporabniku odtujeno 5.000 EUR. Banka se je sklicevala na hudo malomarnost, saj uporabnik ni prepoznal lažne spletne strani. Sodišče ni pritrdilo stališču banke in je presodilo, da je banka uporabniku dolžna povrniti vso škodo (povzeto po Krisper 2013b).

6.3 Uporabniški vidik

Uporabnost je po standardu ISO 9241–11 (1998) opredeljena kot obseg, v katerem se lahko produkt s strani uporabnikov uspešno, učinkovito in zadovoljivo uporablja za dosego natančno določenih ciljev (povzeto po Hertzum 2004 , 53).

Uvedba dodatnih varnostnih mehanizmov je za uporabnika dvorezen meč. Večja kot je varnost, slabša je uporabniška izkušnja. Banka mora tehtati na eni strani morebitne stroške zlorabe in na drugi strani stroške uvedbe dodatnih varnostnih mehanizmov in slabše

uporabniške izkušnje (povzeto po Gemalto 2016, 4).
Po eni strani uporabnik želi varnost, po drugi strani pa čim preprostejšo uporabniško izkušnjo. Singh (2006, 73) pravi, da banke želijo, da bi potrošniki elektronsko bančništvo videli kot varno, z namenom povečanja uporabe elektronskega bančništva v primerjavi s tržnimi potmi, kot so poslovalnice, telefonsko bančništvo ali bankomati. Bankam je torej v interesu, da bi čim več ljudi uporabljalo elektronsko bančništvo in eden od načinov za realizacijo tega cilja je, če uporabnikom zagotavljajo opravljanje bančnih storitev na varen način. Karat (v Singh 2006, 74) meni, da uporaba varnostnih mehanizmov ni primarni cilj uporabnika. Dodaja, da si uporabniki varnosti želijo, a je sekundarnega pomena, ko izpolnjujejo svoje osnovne cilje. Hertzum (2004, 53) opozarja, da je več študij pokazalo, da lahko varnostni mehanizmi, ki so neprijazni uporabniku tudi zmanjšajo varnost, saj se uporabniki aktivno upirajo uporabi.

Pri uporabniškem vidiku varnostnih mehanizmov, je potrebno upoštevati tudi človeško komponento. Domnevamo, da večina ljudi ne zna oceniti učinkovitosti uporabljenih varnostnih mehanizmov, vseeno pa imajo neko percepcijo varnosti pri uporabi elektronskega bančništva. »Raziskave kažejo, da je občutek varnosti pri uporabniku odvisen predvsem od uporabnikovega občutka, da ima nadzor v svojih rokah. Percepcija varnosti pri elektronskem poslovanju je odvisna predvsem od preprostosti uporabe in dostopnosti podpore uporabnikom. Čeprav se razprave o varnosti ukvarjajo predvsem s tehničnimi vprašanji o šifriranju, varnih sejah, avtentikaciji, digitalnih potrdilih itd, pa se ljudje počutijo varne ker »je preprosto za uporabo« (D'Hertefelt v Singh 2006, 74)«

Singh nadalje ponudi tri načine, kako lahko ponudniki spletnih storitev izboljšajo uporabnikovo percepcijo varnosti. Prvi je, da povečamo udobje in uporabnost spletnih transakcij. Drugi način je, da bo v primeru zlorab poskrbljeno za uporabnikove interese in da ne bo utrpel finančne škode. Tretji način je, da ima uporabnik večji nadzor nad transakcijami. (povzeto po Singh 2006, 77)

Da ima varnost velik vpliv na uporabo elektronskega bančništva so pokazale tudi raziskave. Mannan (2007, 2) navaja raziskavo triindvajset tisoč evropskih uporabnikov interneta, ki je pokazala, da nezaupanje v varnost 40% vprašanih odvrača od uporabe elektronskega bančništva. Varnost pa skrbi tudi že obstoječe uporabnike elektronskega bančništva. Mannan (2007, 2) dodaja, da so internetne zlorabe vplivale na skoraj 30% uporabnikov elektronskega bančništva. Več kot 75% teh vprašanih je zato redkeje uporabljalo elektronsko bančništvo,

medtem ko jih je 14% povsem prenehalo s spletnim plačevanjem računov.

Banke so pri uvedbi dodatnih varnostnih mehanizmov ujete v iskanje ravnovesja. Po eni strani uporabniki hočejo večjo varnost, saj je strah pred zlorabami pri mnogih uporabnikih še vedno velik. Po drugi strani pa je elektronsko bančništvo že sedaj precej zapleteno opravilo za mnoge uporabnike, tudi brez postopkov, ki so posledica vpeljave dodatnih varnostnih mehanizmov. Po raziskavah sodeč je za zadovoljstvo uporabnikov dovolj, da banka poskrbi samo za percepcijo varnosti (povzeto po D'Hertefelt v Singh 2006, 74), vendar mora banka, če resnično želi obvarovati uporabnika pred zlorabami, vpeljati tudi prave varnostne mehanizme, ki bodo uporabniško izkušnjo verjetno poslabšali. Čeprav bo torej varnost višja, obstaja možnost, da se bo percepcija varnosti zaradi slabše uporabniške izkušnje pri uporabnikih celo znižala.

7 Primerjava uporabe varnostnih mehanizmov v slovenskih bankah

Primerjali bomo uporabo varnostnih mehanizmov pri rešitvah, ki so namenjene fizičnim osebam. Pri elektronskem bančništvu za pravne osebe in mobilnem bančništvu se uporabljajo podobne rešitve, vendar se jim ne bomo podrobneje posvetili. Pri primerjavi varnostnih mehanizmov slovenskih bank bomo preverili stanje na treh segmentih.

Prvi segment je varnost pri avtentikaciji strežnika, za katero skrbi banka sama. Banke uporabljajo pri avtentikaciji strežnika vse enake rešitve, razlike se pojavijo le v ažurnosti spremljanja najnovejših varnostnih tveganj. Pogosto ugotovimo, da varnostni mehanizmi, ki so še nedolgo nazaj veljali za varne, ne ponujajo več zadostne stopnje varnosti, zaradi česar jih umikamo iz uporabe. Za analizo bomo uporabili spletno orodje SSL Server Test, ki na preprost način prikaže ocenjeno varnost strežnika.

Drugi segment je varnost pri identifikaciji in avtentikaciji. Preverili bomo, kakšne varnostne mehanizme uporabljajo posamezne banke in njihovo stopnjo varnosti glede na tehnično znanje uporabnika. Slovenske banke uporabljajo predvsem digitalna potrdila in različne implementacije enkratnih gesel. Nekatere ponujajo tudi oba načina identifikacije in avtentikacije. V zadnjem času je veliko pozornosti namenjene enkratnim geslom, ker so z vidika uporabnika, predvsem v primeru uporabe na tabličnih računalnikih in mobilnih telefonih, lažja za uporabo.

Tretji segment predstavlja varnost pri avtorizaciji transakcije, ki ji je v zadnjem času posvečeno največ pozornosti. To je segment, ki zagotavlja dodatno varnost tudi v primeru, da ima dostop do računalnika legitimnega uporabnika nepooblaščen uporabnik, za potrditev transakcije se namreč uporablja kanal, do katerega ima dostop samo uporabnik.

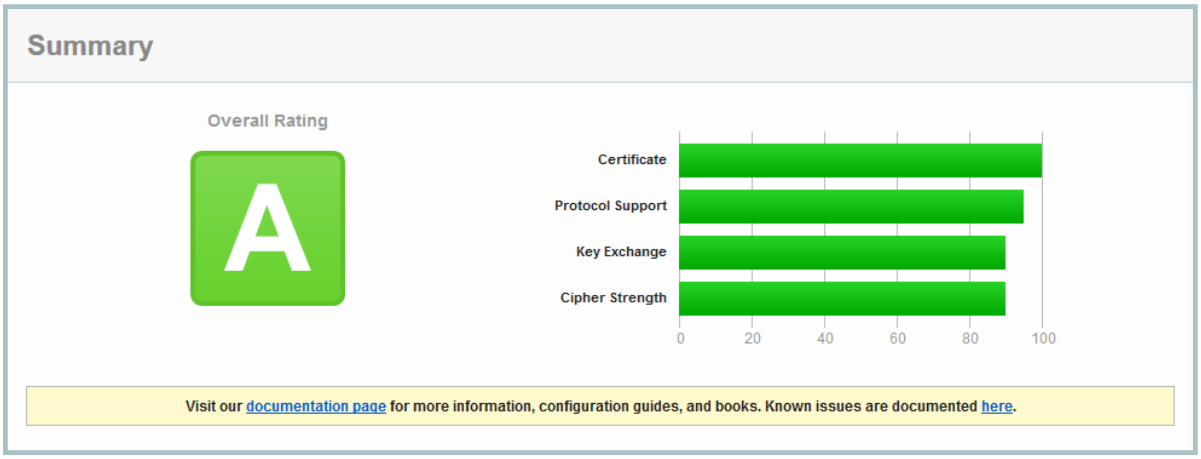
Podatke o uporabljenih varnostnih mehanizmih, bomo pridobili iz javno objavljenih informacij na spletnih straneh bank ter znanja, ki smo ga pridobili s sodelovanjem pri razvoju štirih analiziranih elektronskih bank. V primeru, da kakšen podatek, ki ga poznamo, ni javen, ga bomo zaradi varovanja tajnosti podatkov izpustili iz primerjave.

7.1 Nova Ljubljanska banka d.d.

Nova ljubljanska banka d.d. (v nadaljevanju Nova Ljubljanska banka oziroma banka) je v Sloveniji med prvimi uvedla elektronsko bančništvo pod blagovno znamko NLB KLIK. Prvotno je bila zaščitena s kombinacijo varne povezave in digitalnih potrdil v povezavi z geslom.

Da bi ocenili varnost avtentikacije strežnika smo uporabili spletno orodje *SSL Server Test*. Banka uporablja 2048 bitni ključ. Podprti protokoli so TLS 1.0, TLS 1.1 in TLS 1.2. Starejših protokolov, ki niso več varni, kot je na primer SSL 3, ne dovoljujejo. Spodnja slika prikazuje, da je ocenjena stopnja varnosti visoka.

Slika 7.1: Ocena stopnje varnosti strežnika Nove Ljubljanske banke



Vir: Qualys SSL Labs (2016).

Strežnik je bil prvotno tudi zaščiten s korenskim potrdilom overitelja AC NLB, pred časom pa so ga zamenjali s korenskim potrdilom overitelja Entrust, Inc. Čeprav je AC NLB v Sloveniji priznan overitelj, njegovo korensko potrdilo ni bilo v naboru vnaprej nameščenih potrdil v brskalnikih, kar je povzročilo, da so uporabniki dobili varnostno opozorilo ob obisku elektronske banke. Za odpravo te težave je bil potreben uvoz korenskega potrdila, ki je za uporabnike po našem mnenju zahteven postopek. Sprememba overitelja je za uporabnika dobrodošla, zaradi manjšega števila klicev tehnične podpore pa je najverjetneje prihranila tudi banka. Kasneje je bilo na vstopno stran dodano še osebno sporočilo, ki si ga v elektronski banki nastavi uporabnik sam. Ker je prikaz osebnega sporočila odvisen od identifikacijskih podatkov digitalnega potrdila, s katerim smo se povezali na elektronsko banko, je ta dodaten

mehanizem pristnosti strežnika na voljo samo uporabnikom, ki v elektronsko banko vstopajo z digitalnim potrdilom.

Za identifikacijo in avtentikacijo uporabnika ponuja banka poleg digitalnega potrdila v zadnjem času tudi enkratna gesla. Za izdajo digitalnih potrdil uporablja lastnega overitelja (AC NLB), ki izdaja kvalificirana digitalna potrdila. Enkratna gesla so uporabnikom na voljo v obliki samostojnega generatorja OTP ali v obliki aplikacije Klikin z generatorjem OTP za mobilne naprave, IOS in Android. Uporabniki, ki v elektronsko banko vstopijo z enkratnim geslom, ne morejo uporabljati storitev, ki zahtevajo digitalni podpis, ker zakonsko gledano enkratno geslo ni enakovredno lastnoročnemu podpisu.

Za dodatno varnost pri avtorizaciji transakcije, so na Novi Ljubljanski banki že zelo zgodaj vpeljali dodatno varnostno geslo v obliki virtualne tipkovnice. Sprva je bila uporaba dodatnega varnostnega gesla le dodatna možnost, kasneje pa je postala njegova uporaba obvezna za vsa nakazila med računi, ki niso shranjeni med hitrimi plačili.

> *Virtualna tipkovnica (Dodatno varnostno geslo) je sestavljena iz 8 številčnih in črkovnih znakov. Ob vsakem plačilu ali prenosu sredstev med računi, ki jih komitent nima shranjenih med Hitrimi plačili, bo NLB Klik ali mKlik zahteval vnos dveh naključno določenih znakov. Zahtevana znaka je potrebno vnesti z navidezno tipkovnico, ki se prikaže na dnu zaslona. Prav tako NLB Klik zahteva vnos dveh znakov gesla ob vsakem naročilu za nakazilo sredstev v tujino, pri naročilu nakazila denarja po sistemu Western Union, pri spremembah nastavitev višine limita dnevne in mesečne porabe ter spremembi elektronskega naslova za obveščanje v poglavju Nastavitve.* (Nova Ljubljanska Banka d.d. 2016)

NLB Klik uporablja tudi digitalni podpis, vendar ne kot varnostni mehanizem za podpis transakcij. Uporablja ga predvsem kot nadomestek lastnoročnega podpisa pri storitvah, kot so sklenitev varčevanja, naročilo e-računov, odprtje varčevalnega računa ter plačevanje v spletnih trgovinah.

Nova ljubljanska banka ponuja tudi dodatne varnostne mehanizme, ki so izbirni in uporabniku omogočajo spremljanje dogajanja v elektronski banki. Banka ponuja uporabniku sledeče načine spremljanja dogodkov:

- SMS sporočilo ob vstopu v NLB Klik,
- SMS sporočilo o izvedeni finančni transakciji v NLB Kliku,
- Dnevni in mesečni limit porabe v NLB Kliku.

NLB Klik uporabniku ponuja visoko stopnjo varnosti. Potencialno grožnjo varnosti predstavlja morda le avtorizacija transakcije, kjer varnostna tipkovnica v primeru napada MitB ne zagotavlja zadostne zaščite.

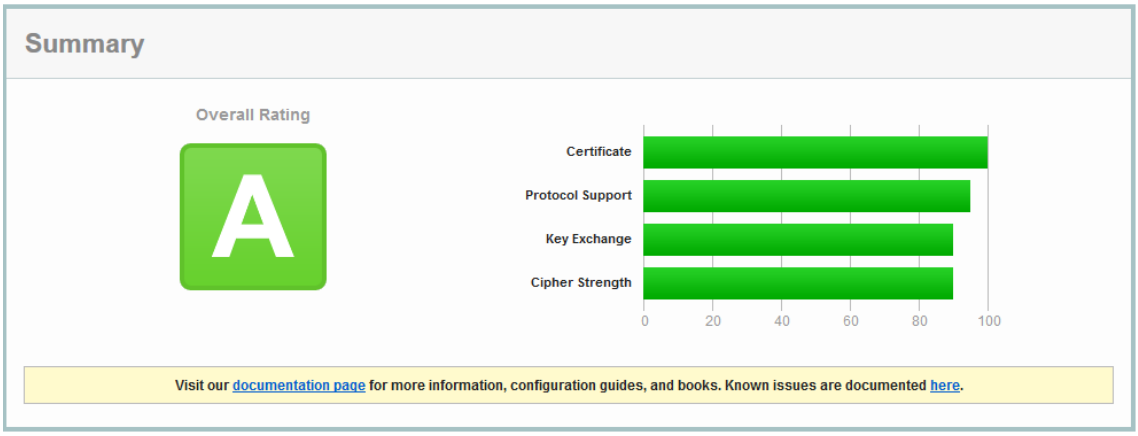
7.2 Gorenjska banka d.d.

Gorenjska banka (v nadaljevanju Gorenjska banka oziroma banka) ponuja fizičnim osebam spletno storitev imenovano Link. Poleg osebnega bančništva ponuja še rešitev za poslovno bančništvo Link c ter mobilno bančništvo Link m. Opisali bomo samo varnostne mehanizme, ki se uporabljajo v spletni banki Link.

Za vstop v elektronsko banko uporablja Gorenjska banka poleg varne povezave digitalno potrdilo v kombinaciji z osebnih geslom. Digitalna potrdila za uporabnike izdaja banka sama in v ta namen ne uporablja zunanjih overiteljev.

Da bi ocenili varnost avtentikacije strežnika smo uporabili spletno orodje SSL Server Test. Banka uporablja 2048 bitni ključ. Podprti protokoli so TLS 1.0, TLS 1.1 in TLS 1.2. Starejših protokolov, ki niso več varni, kot je na primer SSL 3, ne dovoljujejo. Ocenjena stopnja varnosti je visoka.

Slika 7.2: Ocena stopnje varnosti strežnika Gorenjske banke



Vir: Qualys SSL Labs (2016).

Na vstopni strani se uporabnikom digitalnega potrdila prikaže tudi osebno sporočilo, ki še dodatno potrjuje pristnost strežnika, uporabnik si ga nastavi sam v elektronski banki.

Za identifikacijo in avtentikacijo uporabnika banka trenutno ponuja samo digitalna potrdila. Pričakovati je, da bodo v prihodnosti ponudili tudi vstop z enkratnimi gesli, saj je uporaba digitalnih potrdil na mobilnih napravah uporabnikom še manj prijazna, kot njihova uporaba na računalnikih.

Za potrebe avtorizacije transakcije se uporablja digitalni podpis v kombinaciji s CAPTCHA.

Banka kot dodatni varnostni mehanizem izbirno omogoča SMS obveščanje, vendar ne omogoča pa obveščanja o vstopih v elektronsko banko ali o v elektronski banki izvedenih transakcijah.

Varnost banke je dobra, vendar bi lahko stanje izboljšali. Ponarejanje digitalnega podpisa sicer ni lahko, vendar je izvedljivo v primeru napada MitB. Pav tako je banka ranljiva v primeru kraje digitalnega potrdila, saj ima v tem primeru nepooblaščena oseba vse potrebno za izvedbo transakcije. Rešitev bi bila dodatno potrjevanje transakcij z SMS sporočili, prav tako pa bi bilo dobro razširiti nabor storitev SMS obveščanja.

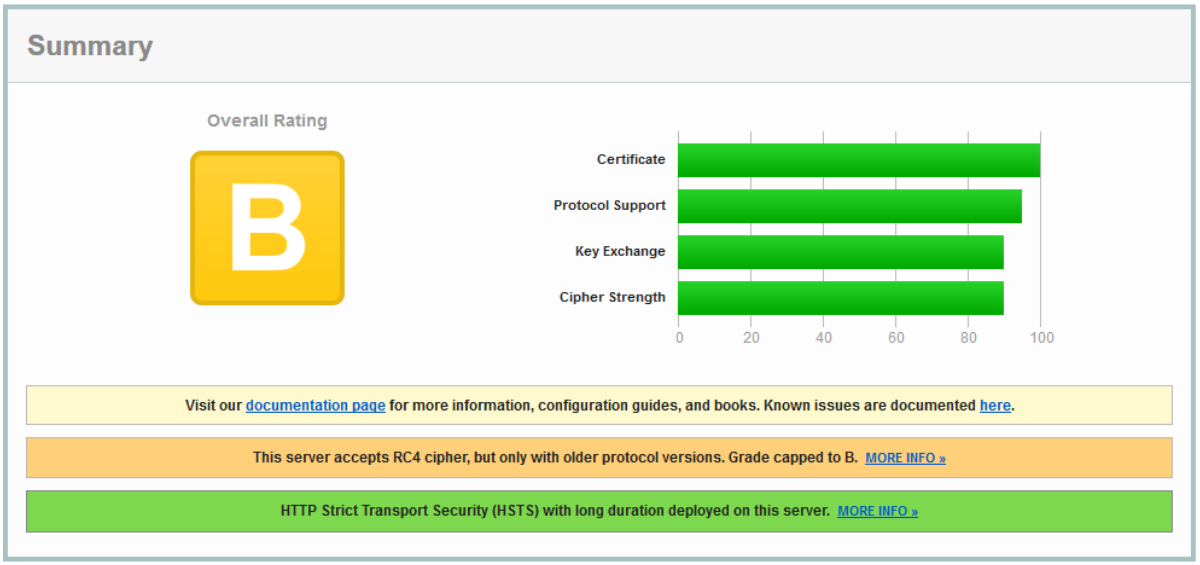
7.3 Addiko Bank d.d.

Addiko Bank d.d. (v nadaljevanju Addiko Bank oziroma banka) poleg varne povezave za

vstop uporablja še enkratna gesla. Ker enkratna gesla ne omogočajo identifikacije uporabnika pred prijavo v elektronsko banko, vstopna stran ne ponuja možnosti prikaza osebnega gesla.

Da bi ocenili varnost avtentikacije strežnika smo uporabili spletno orodje SSL Server Test. Banka uporablja 2048 bitni ključ. Podprti protokoli so TLS 1.0, TLS 1.1 in TLS 1.2. Starejših protokolov, ki niso več varni, kot je na primer SSL 3, ne dovoljujejo. Ocena varnosti je bila znižana na B, ker strežnik dovoljuje šifrirni algoritem RC4. Trenutno to sicer ne predstavlja realne grožnje uporabnikom, vendar se priporoča, da se ta šifrirni algoritem umakne iz uporabe.

Slika 7.3: Ocena stopnje varnosti strežnika Addiko Bank



Vir: Qualys SSL Labs (2016).

Banka uporabniku za potrebe identifikacije in avtentikacije omogoča uporabo strojnega generatorja enkratnih gesel proizvajalca ActivIdentity, po nedavni prenovi elektronske banke pa tudi programski generator enkratnih gesel, ki je del mobilne aplikacije za IOS in Android. Vstop v elektronsko banko je možen s kombinacijo uporabniškega imena ter generiranega enkratnega gesla.

Za avtorizacijo transakcije uporabnik lahko uporabi SMS potrditev ali enkratno geslo. Uporabnik si lahko sam nastavi, katero metodo za avtorizacijo bo uporabljal. Prednost SMS potrditve je v tem, da je v samem sporočilu razviden tudi znesek in račun prejemnika in je zato v primerjavi z OTP potrditvijo varna pri napadu tipa MitB. SMS potrditev je na voljo

samo v primeru avtorizirane telefonske številke, kar lahko komitent uredi samo v primeru obiska poslovalnice. Možna je tudi sprememba avtorizirane telefonske številke, ampak le , če ima uporabnik dostop do prejšnje številke. To napadalcu onemogoča, da bi spremenil ciljno telefonsko številko brez vednosti uporabnika. Slabost pri uporabi SMS avtorizacije je odvisnost od delovanja storitve SMS pri ponudniku mobilne telefonije. Uporabnik potrditveno kodo potrebuje takoj, vendar se pogosto zgodi, da mu je zaradi zamude pri prejemu SMS sporočila plačilo onemogočeno.

Poleg tega omogoča banka uporabniku še širok izbor izbirnih obvestil o dogodkih prek SMS ali elektronske pošte, med drugim o vstopu v elektronsko banko in o izvedbi transakcije.

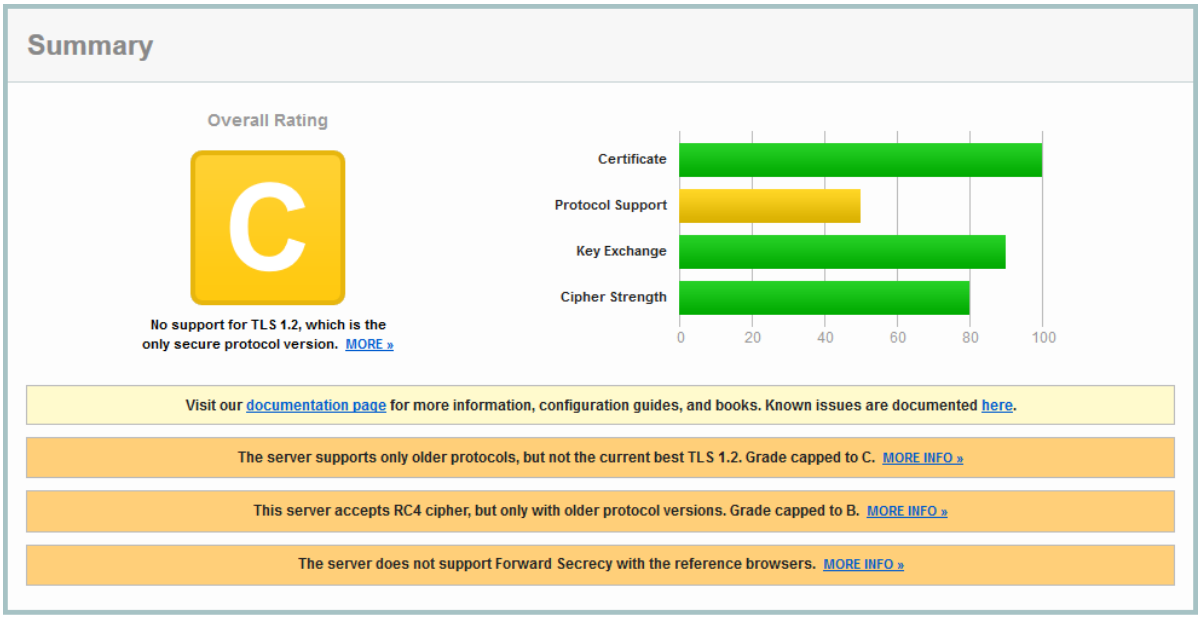
Zagotovljena varnost je zelo dobra, na to pa je vplivala tudi prenova elektronske banke. Prejšnja različica ni vsebovala dodatne varnostne potrditve pri izvedbi transakcije in je bila zato ranljiva v primeru kraje avtentikacijskih podatkov.

7.4 Poštna banka Slovenije d.d.

Poštna banka Slovenije d.d. (v nadaljevanju Poštna banka Slovenije oziroma banka) fizičnim osebam ponuja storitev z imenom PBS.net in je ena redkih slovenskih bank, ki še niso doživele večje prenove. Kljub temu ponuja varno povezavo in možnost vstopa tako z digitalnim potrdilom kot tudi z enkratnim geslom. Za razliko od drugih predstavljenih bank omogoča vstop tudi z digitalnim potrdilom drugih overiteljev in ne samo lastnega POŠTA®CA.

Da bi ocenili varnost avtentikacije strežnika smo uporabili spletno orodje SSL Server Test. Banka uporablja 2048 bitni ključ. Podpirajo samo protokol TLS 1.0. Starejših protokolov, ki niso več varni, kot je na primer SSL 3, ne dovoljujejo, a obenem ne podpirajo novejših, varnejših, kot so TLS 1.1 in TLS 1.2. Podpirajo tudi šifrirni algoritem RC4, za katerega se podpora odsvetuje. Ocenjena varnost je sicer sprejemljiva, vendar bi morala banka uvesti uporabo TLS 1.2 protokola ter umakniti možnost uporabe RC4 algoritma.

Slika 7.4: Ocena stopnje varnosti strežnika Poštne banke Slovenije



Vir: Qualys SSL Labs (2016).

Čeprav na Poštni banki Slovenije trenutno ne ponujajo pričakovane ravni varnosti, kaže, da se potrebnih sprememb zavedajo. Spremembe pri varnostnih mehanizmih so že napovedali in uporabnikom posredovali obvestilo.

> *»Trenutno banka razen digitalnega podpisa ne podpira dodatnih mehanizmov za avtorizacijo transakcije je pa trenutno v fazi razvoja nadgradnja elektronske banke, ki bo omogočila dodatno potrjevanje plačil.*
>
> *V Poštni banki Slovenije smo v skladu z zahtevami o dodatni varnosti, ki jih je oblikoval evropski forum za varnost plačil malih vrednosti, SecuRe Pay, nadgradili elektronsko banko. Pri tem sta nas vodila dva osnovna namena: zagotoviti skladnost z evropskimi smernicami glede varnosti spletnih plačil ter strankam zagotoviti še varnejšo elektronsko banko.*
>
> *Nadgradnja vpliva samo na uporabnike, ki v elektronsko banko vstopajo s kombinacijo uporabniškega imena in enkratnega gesla (pridobljenega s pomočjo ACO žetona ali OTP čitalca). Zaradi nadgradnje je potrebno dodatno potrditi:*
>
> - *vsak vnos novega oz. spremembo obstoječega računa prejemnika v vzorcih*

plačil,

- *vsako plačilo v višini 30 EUR ali več, če račun prejemnika ni shranjen med vzorci plačil.*

Za uporabnike, ki v elektronsko banko vstopajo s kvalificiranimi digitalnimi potrdili, ni sprememb.« (Poštna banka Slovenije d.d. 2016)

Banka uporabnikom ne omogoča storitve SMS obveščanja za transakcije izvedene v elektronski banki.

Čeprav je usoda banke zaradi napovedane združitve z Novo kreditno banko Maribor negotova, moramo odločitev za izboljšanje varnosti pozdraviti.

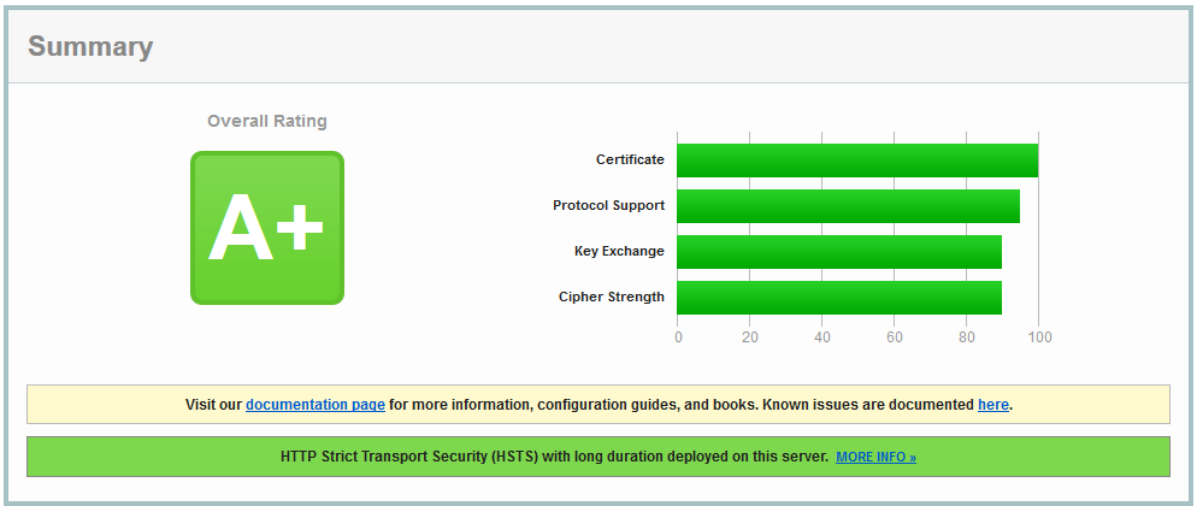
7.5 Banka Koper d.d.

Banka Koper d.d. (v nadaljevanju Banka Koper oziroma banka) ponuja uporabnikom uporabo spletne banke z imenom Banka IN. Strežnik, kot je to ustaljena praksa, omogoča varno povezavo. Za vstop v elektronsko banko imajo uporabniki na voljo tri načine prijave:

- prijavo s prenosnim čitalnikom in kartico,
- prijavo z mobilno napravo in
- prijavo z digitalnim potrdilom na kartici.

Da bi ocenili varnost avtentikacije strežnika smo uporabili spletno orodje SSL Server Test. Banka edina izmed analiziranih Izmed bank, ki ji analiziramo v tem delu, je Banka koper edina, ki uporablja 4096 bitni ključ. Podprti protokoli so TLS 1.0, TLS 1.1 in TLS 1.2. Starejših protokolov, ki niso več varni, kot je na primer SSL 3, ne dovoljujejo. Ker strežnik podpira *HTTP Strict Transport Security*, je med analiziranimi bankami dobil najvišjo oceno.

Slika 7.5: Ocena stopnje varnosti strežnika Banke Koper



Vir: Qualys SSL Labs (2016).

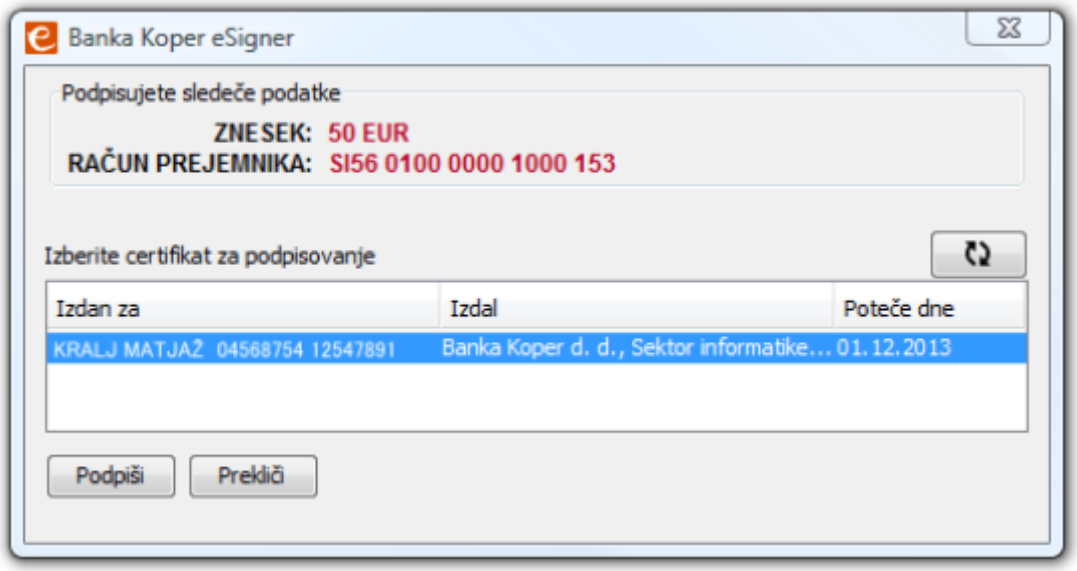
V primerjavi z drugimi, v tem delu analiziranimi bankami Banka Koper ne omogoča uporabe digitalnega potrdila zapisanega na disk, ampak samo varnejši način, kjer je digitalno potrdilo shranjeno na kartici. Uporabnik mora pred uporabo namestiti še programsko opremo Crypto Module, ki omogoča uporabo čitalnikov pametnih kartic. Postopek je za uporabnika precej zapleten, zato je verjetno pametneje, da se odloči za uporabo prenosnega čitalnika.

V primeru vstopa s prenosnim čitalnikom ali z mobilno napravo je zahtevani postopek sledeč:

- vstavite pametno plačilno kartico v prenosni čitalnik ali zaženite mobilno aplikacijo,
- v prenosni čitalnik ali aplikacijo vnesite pozivno številko, ki jo dobite prikazano na spletni strani,
- vnesite vašo osebno številko (PIN),
- z zaslona prenosnega čitalnika ali mobilne aplikacije prepišite enkratno geslo v spletno stran.

Za potrebe avtorizacije transakcije v primeru uporabe digitalnega potrdila uporabljajo digitalni podpis. Za podpisovanje uporabljajo komponento *eSigner*, ki so jo razvili sami. Za delovanje komponenta potrebuje namestitev Java platforme. Rešitev pa podpira samo računalnike z nameščenim operacijskim sistemom Windows. Rešitev je zanimiva, saj v sami komponenti za podpisovanje vidimo znesek in račun prejemnika, medtem ko pri ostalih bankah vidimo te podatke prikazane v brskalniku, kjer so ranljivejši za manipulacijo v primeru napada MitB.

Slika 7.6: Primer digitalnega podpisa



Vir: Banka Koper (2016).

V primeru potrjevanja plačil s prenosnim čitalnikom ali z mobilno napravo je postopek podoben vstopu v elektronsko banko. Poleg osebne številke (PIN) je potrebno vnesti tudi znesek plačila in zadnje štiri številke računa, na katerega nakazujemo denar. To onemogoča, da bi v primeru napada MitB podpisali nakazilo na drug račun.

Čeprav ima Banka Koper že sedaj zavidljivo stopnjo varnosti, so se v luči sprejetja Smernic o varnosti spletnih plačil odločili, da postopek avtorizacije še dodatno zaostrijo.

Banka Koper (2016) svojim uporabnikom v obvestilu za javnost sporoča:

> *»V Banki Koper smo vedno pripisovali velik pomen varnemu poslovanju naših komitentov, ter temu cilju vseskozi zvesto sledili. Tako smo v skladu s postavljenimi višjimi varnostnimi standardi našo spletno banko »Banko IN« prilagodili na način, da bodo od 17.8.2015 dalje njeni uporabniki vsak plačilni nalog, ne glede na znesek, elektronsko podpisovali (podpis +). Izvzeta bodo le plačila, ki se izvedejo med računi istega komitenta znotraj banke. Uporabnik Banke IN tako pri nastavitvi podpisovanja nalogov ne bo imel več možnosti nastavitve najnižjega zneska podpisa nalogov.«*

7.6 Primerjava med bankami

Pri varnosti avtentikacijskega strežnika med bankami ni večjih razlik. Razen Poštne banke Slovenije, ki je bila ocenjena z oceno C, imajo ostale banke strežnike dobro konfigurirane. Banke, ki uporabljajo digitalna potrdila, praviloma za dodatno varnost na vstopni strani prikazujejo tudi osebno sporočilo.

Pri identifikaciji in avtentikaciji vidimo, da slovenske banke uporabljajo širok nabor varnostnih mehanizmov. Mnoge od njih podpirajo več kot en način identifikacije in avtentikacije. Opazen je trend prehoda k enkratnim geslom, ki je za uporabnike enostavnejši. Z razmahom mobilne tehnologije se popularnost enkratnih gesel, ki jih generiramo na mobilnih telefonih povečuje, saj je to cenovno ugodno tako za banko kot uporabnika. Stopnja varnosti pri vseh analiziranih bankah je dobra, saj nobena ne uporablja najpreprostejše kombinacije uporabniškega imena in gesla.

Glavne razlike med bankami se kažejo pri avtorizaciji transakcije. V preteklosti večina bank ni zahtevala dodatne avtorizacije transakcije. Banke, ki uporabljajo digitalna potrdila, večinoma zahtevajo digitalno podpisovanje plačil, ki pa je kljub temu ranljivo za napade MitB. Nova Ljubljanska banka je že zelo zgodaj vpeljala vnos dodatnega gesla prek virtualne tipkovnice, ki močno poveča varnost v primeru kraje identifikacijskih podatkov, vendar so se, kot smo lahko videli, že pojavili napadi, ki od uporabnika zahtevajo, da izda celotno geslo. Mnoge banke so se že odzvale na nove smernice pri varnosti spletnih plačil in od uporabnika zahtevajo dodatno potrditev prek ponovnega vnosa enkratnega gesla ali vnosa gesla, ki ga prejmejo v SMS sporočilu. Banke, ki dodatnega potrjevanja transakcije še nimajo, so večinoma že napovedale spremembe svojih elektronskih bank.

Tabela 7.1: Primerjava med slovenskimi bankami

	NLB	GBKR	AB	PBS	BK
Avtentikacija strežnika					
SSL/TLS	X	X	X	X	X
Osebno sporočilo	X	X		X	
Identifikacija in avtentikacija uporabnika					
Digitalno potrdilo	X	X		X	X
Enkratno geslo	X		X	X	X
Avtorizacija transakcij					
Digitalni podpis		X		X	X
Virtualna tipkovnica	X				
Dodatni vnos enkratnega gesla			X		X
SMS potrjevanje			X		

Legenda:

NLB - Nova Ljubljanska banka

GBKR - Gorenjska banka

AB - Addiko Bank

PBS - Poštna banka Slovenije

BK - Banka Koper

8 Razlike v uporabi varnostnih mehanizmov med Slovenijo in ZDA

Da bi dobili realnejšo sliko o varnosti elektronskega bančništva pri slovenskih bankah, je po našem mnenju dobro pogledati tudi v druge države. Zaradi skupnega gospodarskega prostora in sorodnosti kulture bi primerjava z drugimi evropskimi bankami najverjetneje pokazala podobne rešitve. Razlike so v pogostosti uporabe, kjer v uporabi elektronskega bančništva prvo mesto zasedajo zahodne države, predvsem Skandinavija, srednjo raven dosegajo južne dežele in tudi Slovenija, medtem ko je raven uporabe elektronskega poslovanja v vzhodnih državah precej nizka (povzeto po Eurostat v RIS 2013). Združene države Amerike imajo močan bančni sektor, visoko življenjsko raven in predvsem drugačno regulativo kot v Evropi, zato predstavljajo dober cilj za primerjavo. Percepcija v Sloveniji je, da so ZDA tehnološko naprednejše in bi pričakovali, da bo tako tudi v primeru elektronskega bančništva.

Aaron M. French v članku »A case study on E-Banking Security - When security becomes too sophisticated for the user to access their information« opiše tipičen primer vstopa v elektronsko banko in pravi:

> *Veliko bank v Združenih državah je v prizadevanju, da bi se zaščitile pred eksternimi grožnjami, implementiralo petstopenjski pristop do elektronske banke.*
>
> *V prvem koraku mora uporabnik vnesti kodo za dostop do svojega računa, ki mu jo dodeli banka. Problem povezan s to kodo je dolžina in pomanjkanje pomena te številke za uporabnika. Če si uporabnik kode za dostop ne more zlahka zapomniti, obstaja velika verjetnost, da si podatke za prijavo napiše na kos papirja.*
>
> *V drugem koraku se od uporabnika zahteva, da vnese geslo za dostop do svojega računa.*
>
> *Tretji in četrti korak od uporabnika zahtevata, da odgovori na varnostna vprašanja, na katera je uporabnik že odgovoril. Seznam pogostih varnostnih vprašanj vključuje:*
>
> - *Kakšen je dekliški priimek vaše matere?*

- *Kako se imenuje vaša najljubša restavracija?*
- *Kdo je vaš najljubši igralec?*
- *Katera je vaša najljubša barva?*
- *Kakšno je bilo ime vašega prvega hišnega ljubljenčka?*

Medtem ko ta vprašanja predstavljajo dodatno varnost, so kljub temu ranljiva, še posebej s strani ljudi, ki uporabnika poznajo ali pa s strani tistih, ki bi uporabili socialni inženiring. Uporaba pretežkih vprašanj bi povzročila, da se jih uporabnik ne bi spomnil, kar bi mu onemogočilo dostop do elektronske banke. V tem primeru bi se uporabnik zatekel k pisanju odgovorov na kos papirja, na katerem ima zapisane že ostale podatke za dostop.

V zadnjem, petem, koraku uporabnik identificira sliko, ki jo je že predhodno označil. (French 2012, 10–11)

Ko pogledamo ta, po avtorjevem mnenju tipičen primer varnosti, bi pomislili, da gre za varnostno politiko kakšnega nepomembnega spletnega foruma, kamor sicer ne bi želeli, da nam vdrejo, vendar ob tem ne bi utrpeli večje škode. Pričakovali bi, da bo eden od korakov uporaba digitalnega potrdila ali enkratnega gesla, po avtorjevem mnenju pa to pri vstopu v elektronsko banko v Združenih državah Amerike, kot vidimo, ni običajen del varnosti. Da bi preverili, če to drži, smo analizirali elektronske banke štirih največjih bank v Združenih državah Amerike. Za analizo varnosti strežnika bomo uporabili že pri slovenskih bankah uporabljeno spletno orodje SSL Server Test, medtem ko bomo podatke o uporabljenih varnostnih mehanizmih za identifikacijo in avtentikacijo uporabnikov ter morebitno avtorizacijo transakcije pridobili iz spletnih strani posameznih bank.

8.1 Chase

Chase banka je podružnica v svetu bolj znanega podjetja JP Morgan Chase & Co. Trenutno je to največja banka v Združenih državah Amerike, tesno pa ji sledijo preostale tri analizirane banke. Ostale so opazno manjše, vendar je v primerjavi z njimi tudi Nova ljubljanska banka, ki je največja slovenska banka, pravi pritlikavec. (povzeto po US Bank Locations 2016)

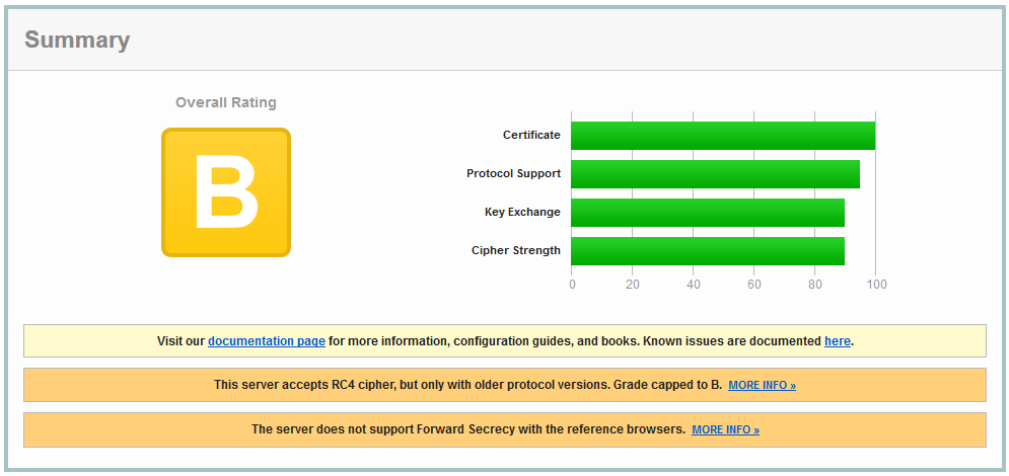
Čeprav bi od tako velike banke pričakovali, da bo v implementacijo varnostnih mehanizmov

vložila veliko denarja, je popis varnostnih mehanizmov na njeni spletni strani precej suhoparen.

> *Uporabljamo varno tehnologijo za šifriranje vaših osebnih podatkov na internetu, kot so na primer vaše uporabniško ime, geslo in podatki o računu. Da so podatki šifrirani vidite, ko se spletni naslov začne s predpono »https://« in je v brskalniku prikazan simbol zaklenjene ključavnice.* (Chase 2016)

Za začetek smo preverili varnost strežnika, ki je sprejemljiva, vendar bi od tako velike organizacije pričakovali boljši rezultat.

Slika 8.1: Ocena stopnje varnosti strežnika Chase banke



Vir: Qualys SSL Labs (2016).

Za identifikacijo in avtentikacijo uporabnika se uporablja preprosta kombinacija uporabniškega imena in gesla. Obe vrednosti si nastavi uporabnik sam, kar že tako nizko raven varnosti še dodatno zmanjša, saj uporabniki pogosto uporabijo isto kombinacijo kot na drugih spletnih straneh. V primeru, da banka zazna, da se je uporabnik v elektronsko banko prijavil iz neznane naprave, pošljejo še dodatno varnostno kodo prek SMS sporočila ali elektronske pošte.

Banka ne uporablja dodatnih varnostnih mehanizmov pri avtorizaciji transakcije.

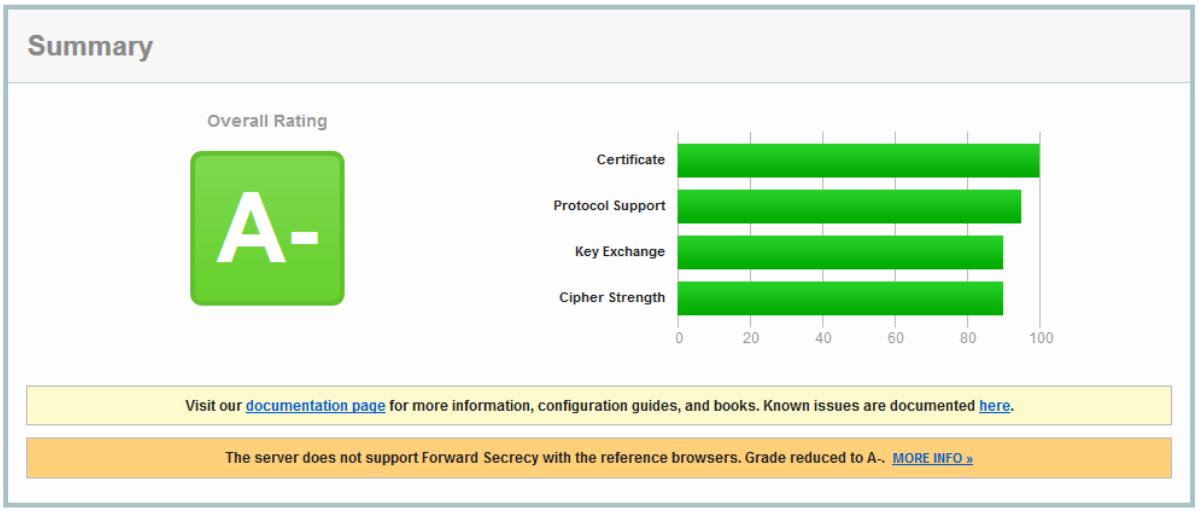
8.2 Bank of America

Bank of America je po višini depozitov druga največja banka v Združenih državah Amerike .

(povzeto po US Bank Locations 2016)

Preizkus varnosti strežnika je pokazal, da je za avtentikacijo strežnika dobro poskrbljeno.

Slika 8.2: Ocena stopnje varnosti strežnika banke Bank of America



Vir: Qualys SSL Labs (2016).

Za identifikacijo in avtentikacijo uporabnika uporabljajo kombinacijo uporabniškega imena in gesla. Funkcionalnost je podobna kot pri Chase banki, vendar uporabljajo tudi dodatne varnostne mehanizme v obliki varnostnih vprašanj. Uporabnik mora odgovoriti na varnostno vprašanje v primeru, da strežnik ne prepozna računalnika, s katerega uporabnik dostopa. To izboljša varnost v primeru kraje uporabniškega imena in gesla, vendar ne varuje v primeru, da ima napadalec dostop do žrtvinega računalnika.

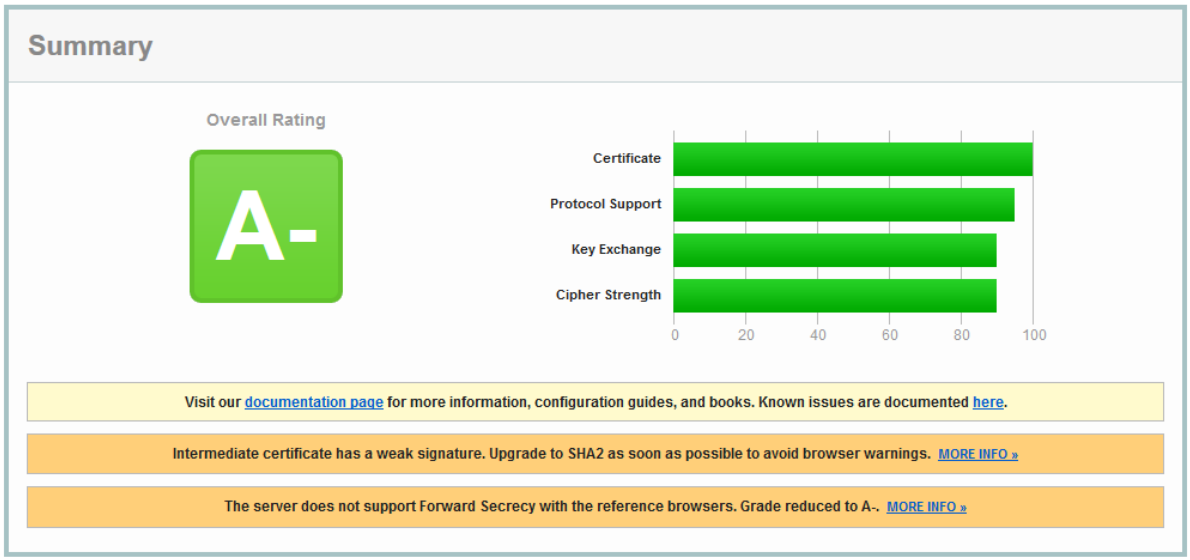
Banka ponuja še izbirne varnostne mehanizme. Na voljo so obvestila za menjavo gesla vsakih 90 dni ter obvestila o vstopih iz naprav, ki jih strežnik ne prepozna. Avtomatično pošljejo še elektronsko pošto v primeru sumljivih dogodkov pri plačilih ali v primeru spremembe kontaktnih podatkov. Uporabnik si lahko nastavi tudi pošiljanje kode za avtorizacijo transakcije prek SMS sporočila ali pa naroči strojno kartico za generiranje enkratnih gesel, ki je plačljiva.

8.3 Wells Fargo

Tudi Wells Fargo banka, ki je tretja največja banka Združenih držav Amerike, se je na testu varnosti avtentikacije dobro odrezala. Rezultat je za odtenek boljši kot pri Bank of America in

podoben Chase banki.

Slika 8.3: Ocena stopnje varnosti strežnika Wells Fargo banke



Vir: Qualys SSL Labs (2016).

Za potrebe identifikacije in avtentikacije uporabnika uporabljajo že poznano kombinacijo uporabniškega imena in gesla. Banka uporabnikom ponuja tudi varnejši način avtentikacije z uporabo RSA SecurID generatorjem enkratnih gesel, ki je plačljiv.

Uporabnik ima možnost uporabljati dodatno zaščito za avtorizacijo transakcije. V primeru, da uporabnik nakazuje na nov račun, dobi prek SMS sporočila potrditveno kodo.

8.4 CitiBank

CitiBank je bila edina ameriška banka, pri kateri varnosti strežnika nismo mogli preveriti, ker tega ne dovoljujejo. Ali je vzrok za to dodatna varnost ali poskušajo zakriti slabšo varnost, ostaja odprto vprašanje.

Po ustaljeni praksi tudi CitiBank omogoča vstop le z uporabniškim imenom in geslom. Varnejših mehanizmov vstopa ne ponujajo in so posledično ranljivi v primeru kraje uporabnikovih podatkov.

Banka pri določenih transakcijah zahteva vnos odgovora na varnostno vprašanje. Varnostno vprašanje se pojavi samo pri tistih transakcijah, za katere bančni sistem meni, da so lahko sumljive.

8.5 Primerjava s slovenskimi bankami

Kot smo lahko videli, so si analizirane ameriške banke med seboj precej podobne. Za varnost strežnika je pri vseh dobro preskrbljeno, zaplete pa se pri varnosti identifikacije in avtentikacije uporabnika. Vse analizirane banke uporabljajo najpreprostejši način uporabniškega imena in gesla. Praviloma ob obisku spletne strani iz neznanega računalnika zahtevajo še odgovor na varnostna vprašanja, vendar to raven varnosti ne izboljša veliko. Nekatere banke ponujajo tudi vstop s pomočjo enkratnih gesel, vendar je že iz spletnih strani razvidno, da gre samo za dodatno storitev, ki je precej skrita, najverjetneje, ker zahteva od uporabnika dodatne stroške.

Banke praviloma ne zahtevajo dodatne avtorizacije transakcij, če avtorizacija transakcije obstaja, pa gre za preprosto varnostno vprašanje.

Če primerjamo ameriške banke s slovenskimi, vidimo, da so primerljive le na nivoju varnosti strežnika. Čeprav nekatere izmed njih ponujajo varnejši način vstopa z enkratnimi gesli, je velika večina uporabnikov varovana samo s preprostimi gesli. Nič drugače ni pri avtorizaciji transakcije, kjer ne ponujajo praktično nobene zaščite. Lahko rečemo, da je V Sloveniji večina bank varna pred večino napadov in so ranljive le za najkompleksnejše napade tipa MitB, pri čemer v primerjavi z drugimi evropskimi in svetovnimi bankami majhne banke praviloma niso tarča tovrstnih napadov. Po analizi Kaspersky Laba (2014, 10) je bilo kar 59,5% vseh napadov usmerjenih na 25 največjih bank na svetu. Stanje v Združenih državah Amerike napram Sloveniji je povsem nasprotno, saj že sama kraja identifikacijskih podatkov omogoča napadalcem praktično neomejen dostop do bančnega računa.

Jon Oberheide, CTO podjetja Duo Security o razlogih, zakaj banke ne izboljšajo varnosti, pravi sledeče:

> *Zaradi ohlapnih smernic ponujajo banke minimalne varnostne mehanizme v obliki varnostnih vprašanj in odgovorov ter varnostnih slik. Uporabniki jih lahko vidijo, ko*

> *se prijavijo v svoj račun. Varnostna slika in varnostno vprašanje, ki ga je uporabnik predhodno odgovoril, naj bi uporabnika prepričala, da je njegova prijava varna. V resnici nudijo ti mehanizmi le malo zaščite pred ribarjenjem in drugimi vrstami zlorab identifikacijskih podatkov uporabnika. Z drugimi besedami, banke ne naredijo več za varnost zato, ker jim ni treba. Dokler bodo ponujale garancije pred izgubami zaradi zlorab in bo znesek goljufij v primerjavi z njihovimi globokimi žepi ostal relativno majhen, banke za varnost uporabnikov ne bodo naredile nič dodatnega.* (Aguilar 2015)

Electronic Fund Transfer Act, ki je bil sprejet že leta 1978, regulira pravice in obveznosti potrošnikov pri elektronskem prenosu sredstev. V primeru elektronskega bančništva ima uporabnik 60 dni od dneva prejema izpiska čas, da prijavi neavtorizirane transakcije svoji banki. Če uporabnik ta rok zamudi, škode ne dobi povrnjene, vendar je rok vseeno tako dolg, da so uporabniki v primeru zlorabe dobro zavarovani (povzeto po Federal Reserve 2008). Slovenska zakonodaja je strožja in v primeru hude malomarnosti uporabnika banka povzročene škode ne krije. Se pa glede na izkušnje bank v sodnih postopkih sodišča raje postavijo na stran potrošnika. Dokazovanje hude malomarnosti se je namreč izkazalo za težje izvedljivo. Kot vidimo, ameriškim bankam zakonodajalec uvedbe dodatnih varnostnih mehanizmov ne nalaga. Izkazalo se je tudi, da je stroškovni vidik zlorab za njih obvladljiv. Pokazalo se je, da je z uporabniškega vidika preprostost uporabe najpomembnejša in pogosto tudi enačena z varnostjo.

9 Zaključek

V diplomskem delu smo si pobliže ogledali varnostne mehanizme v elektronskem bančništvu. Na kratko smo opisali področje elektronskega bančništva in njegov pomen v trenutni družbi. Prikazali smo najpogostejše grožnje, ki ogrožajo uporabnike pri uporabi elektronskega bančništva. Podrobno smo opisali varnostne mehanizme, ki se najpogosteje uporabljajo za varovanje uporabnika. Izpostavili smo njihove prednosti in slabosti za varnost in za uporabniško izkušnjo. Preverili smo tudi, kakšni so morebitni vzroki za uvedbo dodatnih varnostnih mehanizmov na strani bank. Na koncu smo naredili primerjavo varnostnih mehanizmov izbranih slovenskih bank. Da bi dobili širši pogled na problematiko smo preverili tudi kakšno je stanje v Združenih državah Amerike v primerjavi s Slovenijo.

Cilj naloge je bil, da odgovorimo na nekaj vprašanj povezanih z varnostjo elektronskega bančništva.

Prva hipoteza, ki smo jo postavili je, da **dodatni varnostni mehanizmi vplivajo na uporabniško izkušnjo**. Uporabniki, si želijo elektronsko banko uporabljati na čim preprostejši način, večina varnostnih mehanizmov pa od uporabnika zahteva določen napor. Pri tem gre lahko za uporabo ločenih naprav v obliki generatorjev enkratnih gesel, namestitve potrebne programske opreme za digitalno podpisovanje, uporabo mobilnega telefona za potrjevanje plačil ali pa preprost list papirja z natisnjenimi gesli za virtualno tipkovnico. Kot smo prikazali v nalogi, mnogi avtorji izpostavljajo, da si uporabniki želijo čim preprostejše uporabe. Videli smo tudi, da čeprav je velik del bremena zagotavljanja varnosti na plečih uporabnika, uporabniki praviloma nimajo dovolj znanja, da bi za varnost samostojno skrbeli. Tako citirani avtorji kot lastne izkušnje pri razvoju elektronskih bank kažejo, da vsak dodaten varnostni mehanizem povečuje kompleksnost uporabe. Lahko trdimo da dodatni varnostni mehanizmi negativno vplivajo na uporabniško izkušnjo. Po drugi strani pa je treba priznati, da bi bila v primeru odsotnosti teh mehanizmov, uporabniška izkušnja v primeru zlorabe precej slabša. Trenutno stanje ni zadovoljivo in banke bi morale vložiti več truda v izboljšanje trenutnih varnostnih mehanizmov. Ne toliko s stališča same varnosti le-teh, ampak predvsem s stališča preprostosti uporabe. Na koncu lahko našo hipotezo potrdimo s trditvijo, da dodatni varnostni mehanizmi vplivajo na uporabniško izkušnjo, tako v pozitivni, kot tudi v negativni smeri.

Druga hipoteza, ki smo jo postavili, je bila, da so **razlogi za vpeljavo dodatnih varnostnih mehanizmov v Sloveniji predvsem posledica zahtev zakonodajalcev**. Izpostavili smo tri glavne vidike za uvedbo, in sicer pravni, stroškovni ter uporabniški. Čeprav stroškovni in uporabniški vidik nista nepomembna in bi verjetno prevladala nad pravnim, pa se je pokazalo, da zakonodajalec bankam ne daje veliko manevrskega prostora. Vse banke so v svoje obstoječe elektronske banke obvezane vpeljati dodatne varnostne mehanizme. Mnoge izmed njih, kot razlog za nadgradnjo eksplicitno navajajo nove smernice za varnost spletnih plačil. Hipotezo lahko zato potrdimo. Potrebno je izpostaviti, da veljavnost te hipoteze velja samo za Slovenijo. Po odločitvi Banke Slovenije, je uporaba teh smernic v Sloveniji obvezna. V preostalih državah Evropske unije so, razen v primeru drugačne odločitve njihovih centralnih bank, smernice samo priporočilo. Kot smo lahko videli, pri pregledu bank v Združenih državah Amerike, pri njih ni zakonskih zahtev, glede uporabe dodatnih varnostnih mehanizmov.

Tretja hipoteza, ki smo jo postavili, je da **med Združenimi državami Amerike in Slovenijo obstajajo razlike v pogledu na potrebo po dodatni varnosti**. Ko je pri našem delu govora o varnosti, se pogosto omenjajo razlike v stopnji varnosti med Slovenijo in Združenimi državami Amerike. Ker nismo ne uporabniki njihovih bank in tudi poslovno ne sodelujemo z njimi, nas je zanimalo ali je v tej trditvi tudi kaj resnice. Analiza varnostnih mehanizmov njihovih štirih največjih bank je pokazala, da obstajajo glede na slovenske banke precejšnje razlike. Gledano s strani razvijalca v Sloveniji, so njihove rešitve popolnoma nezadostne, saj uporabljajo le najpreprostejše varnostne mehanizme za identifikacijo in avtentikacijo uporabnika. Največja razlika se pokaže pri avtorizaciji transakcije, kjer varnostnih mehanizmov ni, ali pa so precej preprosti in posledično nudijo slabšo varnost. Hipotezo lahko potrdimo. Kljub temu, se je po našem mnenju potrebno vprašati ali je njihov pristop res napačen. Če pogledamo stopnjo uporabe elektronskega bančništva, je ta precej višja kot v Sloveniji in tudi višja kot je povprečje v Evropi. Tudi ogroženost uporabnikov je zaradi velikosti trga precej večja, kot pri kakšni manjši slovenski banki, vendar kljub temu ne vidijo zadostnih razlogov za vpeljavo dodatnih varnostnih mehanizmov. Čeprav se, po besedah Aguilarja (2015), razlog skriva v nizkih stroških zlorab v primerjavi z dobički, ter v garanciji uporabnikom o povračilu denarja, pa bi bilo zanimivo pogledati tudi manjše banke v Združenih državah Amerike.

10 Literatura

1. Aguilar, Mario. 2015. *Here's Why Your Bank Account Is Less Secure Than Your Gmail*. Gizmodo. Dostopno prek: http://gizmodo.com/heres-why-your-bank-account-is-less-secure-than-your-gm-1683777281 (17. junij 2016).
2. APWG. 2016. *Phishing Activity Trends Report 1st Quarter 2016*. Dostopno prek: http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf (12. julij 2016).
3. Banka Koper d.d.. 2016. *Spletna banka Banka IN*. Dostopno prek: http://www.banka-koper.si/Fizicne_osebe/Poti_do_banke/Banka_IN (6. junij 2016).
4. Bank of America. 2016. *Online Banking Security from Bank of America*. Dostopno prek: https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/online-banking-security.go (7. junij 2016).
5. Bishop, Matt. 2005. *An Overview of Computer Security*. Dostopno prek: http://www.informit.com/articles/article.aspx?p=363728 (16. julij 2016).
6. Berce, Mojca. 2014. *Varnostni vidiki e-bančništva v Sloveniji*. Magistrsko delo. Dostopno prek: https://repozitorij.uni-lj.si/Dokument.php?id=30427 (20. junij 2016).
7. Chase. 2016. *Chase Security Center*. Dostopno prek: https://www.chase.com/digital/resources/privacy-security (7. junij 2016).
8. Ciglarič, Mojca. 2007. Elektronsko upravljanje in poslovanje v službi uporabnika. V *Varno obnašanje uporabnikov v omrežnem okolju,* ur. Uroš Pinterič in Uroš Svete, 176–191. Fakulteta za družbene vede.
9. Citi. 2016. *Online Security*. Dostopno prek: https://online.citi.com/US/JRS/pands/detail.do?ID=OnlineSecurity&JFP_TOKEN=YA9P5GIP (7. junij 2016).
10. Daniel, Elizabeth. 1999. Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing* 17/2. Dostopno prek: http://ce.sharif.ir/courses/86-87/1/ce428/resources/root/ebanking%20service%20quality/2.pdf (11. julij 2016).
11. Das , Anupam, Joseph Bonneau, Matthew Caesar, Nikita Borisov in XiaoFeng Wang. 2014. *The Tangled Web of Password Reuse*. Dostopno prek: http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf (12. julij 2016).
12. Dimc, Maja in Bojan Dobovšek. 2012. *Kriminaliteta v informacijski družbi*. Ljubljana :

Fakulteta za varnostne vede.

13. Entrust. 2014. *Defeating Man-in-the-Browser Malware.* Dostopno prek: https://www.entrust.com/wp-content/uploads/2014/03/WP_Entrust-MITB_March2014.pdf (10. julij 2016).
14. European Banking Authority. 2014. *Končne smernice o varnost spletnih plačil*. Dostopno prek: https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_SL+Guidelines+on+Internet+Payments.pdf/986085dd-b2fa-494c-89f3-350693c3df27 (5. junij 2016).
15. Evropska centralna banka. 2013. *Priporočila za varnost spretnih plačil*. Dostopno prek: https://www.bsi.si/library/includes/datoteka.asp?DatotekaId=5194 (5. junij 2016).
16. Federal Reserve. 2008. *Electronic Fund Transfer Act*. Dostopno prek: https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf (11. julij 2016).
17. French, Aaron M. 2012. *A case study on E-Banking Security - When security becomes too sophisticated for the user to access their information*. Journal of internet banking and commerce. August 2012, vol.17 No.2.
18. Gemalto. 2016. *Top Online Banking Threats to Financial Service Providers in 2010*. Dostopno prek: http://www2.gemalto.com/email/2010/MITB-2010/WhitePaper_Top-Threat-to-Financial-Service-Providers-in-2010_FINAL.pdf (13. junij 2016).
19. Gorenjska banka d.d.. 2016. *Varnost, digitalna potrdila, pametne kartice*. Dostopno prek: https://www.gbkr.si/osebne-finance/spletno-bancnistvo-29/spletna-banka-link/varnost-digitalna-potrdila-pametne-kartice/ (4. junij 2016).
20. Hertzum, Morten, Niels Jørgensen in Mie Nørgaard. 2004. *Usable Security and E-Banking: Ease of Use vis-a-vis Security*. Australasian Journal of Information Systems, vol 11, special issue 2004: 52–65.
21. Hypo Alpe-Adria-Bank d.d.. 2016. *Priporočila za varno internetno poslovanje*. Dostopno prek: http://www.hypo-alpe-adria.si/sl/content/priporocila-za-varno-internetno-poslovanje (5. junij 2016).
22. Jerman Blažič, Aljoša. 2004. *Informacijska varnost*. Dostopno prek: http://www.monitor.si/clanek/informacijska-varnost/122021/?xURL=301 (17. junij 2016).
23. Jerman-Blažič, Borka, Tomaž Klobučar, Zoran Perše in Dragan Nedeljković. 2001. *Elektronsko poslovanje na internetu*. 1. natis. Ljubljana : GV založba.
24. Kaspersky Lab. 2014. *Financial cyber threats in 2013*. Dostopno prek: http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-

2013-eng-final.pdf (12. julij 2016).

25. Keivani , F.Sameni, M.Jouzbarkand, M.Khodadadi in Z.Khalili Sourkouhi. *A General View on the E-banking.* 2012. International Proceedings of Economics Development & Research, 43: 62–65. Dostopno prek: http://ipedr.com/vol43/013-ICFME2012-M00033.pdf (11. julij 2016).
26. Koskosas, Ioannis. 2011. T*he pros and cons of internet banking: a short review*. Business Excellence and Management Volume 1 Issue 1 / December 2011: 49–58. Dostopno prek: https://www.researchgate.net/profile/Ioannis_Koskosas/publication/227489888_THE_PROS_AND_CONS_OF_INTERNET_BANKING_A_SHORT_REVIEW/links/02e7e5296f3ff45437000000.pdf?origin=publication_detail (11. julij 2016).
27. Krisper, Boštjan. 2013a. *Za varnejšo uporabo spletne banke*. Zveza potrošnikov Slovenije. Dostopno prek: https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/6296-za-varnejo-uporabo-spletne-banke-62013 (10. julij 2016).
28. --- 2013b. *ZPS dosegla pomembno zmago za uporabnike spletne banke*. Zveza potrošnikov Slovenije. Dostopno prek: https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/6620-zps-dosegla-pomembno-zmago-za-uporabnike-spletne-banke (10. julij 2016).
29. --- 2015. *Nova pravila za varnost pri spletnih plačilih*. Zveza potrošnikov Slovenije. Dostopno prek: https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/7661-nova-pravila-za-varnost-pri-spletnih-placilih-11-12-2015 (8. junij 2016).
30. Mannan, Mohammad. 2007. *Security and usability: The Gap in Real- World Online Banking*. Dostopno prek: https://www.ccsl.carleton.ca/paper-archive/mannan-nspw07.pdf (14. maj 2016).
31. Meyer, Thomas. 2006. *Online banking - What we learn from the differences in Europe*. Deutsche Bank Research. Dostopno prek: https://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000196129.PDF (13. julij 2016).
32. Norman, Don in Jakob Nielsen. 2016. *The Definition of User Experience.* Nielsen Norman Group. Dostopno prek: https://www.nngroup.com/articles/definition-user-experience/ (16. julij 2016).
33. Nova Ljubljanska banka d.d.. *Klik*. Dostopno prek: https://www.nlb.si/klik (4. junij 2016).
34. Peotta, Laerte, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus in Rafael Timóteo de Sousa Jr.. 2011. A formal classification of intenet banking attacks and vulnerabilities.

International Journal of Computer Science & Information Technology, 3(1): 168–197.

35. Poštna banka Slovenije d.d.. 2016. *PBS.net - elektronska banka*. Dostopno prek: http://www.pbs.si/si/PBSnet.wlgt (5. junij 2016).
36. Prakash, Atul. 2007. *Security in practice - Security-usability chasm*. Dostopno prek: http://web.eecs.umich.edu/~aprakash/papers/iciss-prakash.pdf (13. julij 2016).
37. Ragin, Charles C. 2007. *Družboslovno raziskovanje - enotnost in raznolikost metode*. Ljubljana: Fakulteta za družbene vede.
38. RIS. 2016a. *E-bančništvo.* Dostopno prek: http://www.ris.org/index.php?fl=2&lact=1&bid=9400 (13. junij 2016).
39. --- 2016b. *Varnost slovenskega e-bančništva je 'solidna'?*. *Dostopno prek:* http://www.ris.org/db/26/11518/Novice/Varnost_slovenskega_e-ban%C4%8Dni%C5%A1tva_je_'solidna (13. junij 2016).
40. Ropret, Matjaž. 2010. *Napadi na komunikacijo med banko in uporabnikom vse pogostejši.* Dostopno prek: http://www.delo.si/druzba/infoteh/napadi-na-komunikacijo-med-banko-in-uporabnikom-vse-pogostejsi.html (10. julij 2016).
41. RSA. 2016. *RSA SecurID Hardware Tokens*. Dostopno prek: https://www.rsa.com/en-us/products-services/identity-access-management/securid/hardware-tokens (10. julij 2016).
42. Qualys SSL Labs. 2015. *SSL Server Rating Guide*. Dostopno prek: https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf (1. avgust 2016).
43. --- 2016. *SSL Server Test*. Dostopno prek: https://www.ssllabs.com/ssltest/index.html (4. junij 2016).
44. Si-CERT. 2016a. *SI-CERT 2012-16 / Bančni trojanec, ki krade avtentikacijske podatke za Klik NLB*. Dostopno prek: https://www.cert.si/si-cert-2012-16-bancni-trojanec-ki-krade-avtentikacijske-podatke-za-klik-nlb/ (19. junij 2016).
45. --- 2016b. *Poročilo o omrežni varnosti za leto 2015.* Dostopno prek: https://cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf (11. julij 2016).
46. --- 2016c. *SI-CERT 2012-09 / Phishing napad na komitente SKB banke*. Dostopno prek: https://www.cert.si/si-cert-2012-09-phishing-napad-na-komitente-skb-banke/ (19. junij 2016).
47. Singh, Supriya. 2006. The Social Dimensions of the Security of Internet banking. *Journal of theoretical and Applied Electronic Commerce Research*, 1(2): 72–78.
48. Statistični urad Republike Slovenije. 2016. *StatWeb*. Dostopno prek: http://www.stat.si/StatWeb/ (27. junij 2016).

49. Sušnik, Matjaž. 2010. *Kako varno do e-banke?*. Dostopno prek: http://www.monitorpro.si/41188/praksa/kako-varno-do-e-banke/ (13. junij 2016).
50. *Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.* Ur. l. RS 77/2000 (14. junij 2016).
51. US Bank Locations. 2016. *Banks Ranked by Total Deposits*. Dostopno prek: http://www.usbanklocations.com/bank-rank/total-deposits.html (7. junij 2016).
52. Varni na Internetu. 2013. *Vdori v sisteme e-bančništva slovenskih podjetij*. Dostopno prek: https://www.varninainternetu.si/2013/vdori-v-sisteme-e-bancnistva-slovenskih-podjetij/ (12. julij 2016).
53. Wells Fargo. 2016. *How We Protect You*. Dostopno prek: https://www.wellsfargo.com/privacy-security/fraud/protect-yourself (7. junij 2016).
54. *Zakon o elektronskem poslovanju in elektronskem podpisu (uradno prečiščeno besedilo)* (ZEPEP-UPB1). Ur. l. RS 98/2004 (14. junij 2016).
55. Združenje bank Slovenije. 2016. *Uporaba Smernic o varnosti spletnih plačil*. Dostopno prek: http://www.zbs-giz.si/news.asp?StructureId=1216&ContentId=8037 (6. junij 2016).
56. Zupan, Lucija in Igor Bernik. 2012. *Zahteve za varovanje e-bančnih storitev - izzivi varovanja*. Dostopno prek: http://www.fvv.um.si/KonferencaIV/zbornik/Zupan_Bernik.pdf (14. maj 2016).
57. Zveza potrošnikov Slovenije. 2009. *Varnost spletnih bank*. Dostopno prek: https://web.archive.org/web/20111102173822/http://www.zps.si/osebne-finance/varnost-placil/varnost-spletnih-bank.html?Itemid=666 (11. julij 2016).