Elekronsko bankarstvo – Primena i Sigurnost

E-banking – Application and Security

Miloš N. Ilić, Fakultet tehničkih nauka Kosovska Mitrovica, Univerzitet u Prištini
Žaklina S. Spalević, Mladen Đ. Veinović, Univerzitet Singidunum

***Sažetak*—Ubrzani razvoj komunikacionih tehnologija, primena Interneta u svakodnevnom životu i radu pojedinaca, kao i sve veća pojava pametnih uređaja doveli su do približavanja elektronskih bankarskih usluga korisnicima. Bankarska industrija je domen poslovanja koji nudi svojim korisnicima veliki broj servisa korišćenjem novih komunikacionih medija. Ovakvi servisi trebaju da omoguće brzi udaljeni pristup, uštedu vremena korisnicima i najbitnije visok stepen sigurnosti. E-banking servisi nude korisnicima pristup njihovim nalozima, pregled većeg dela skorašnjih transakcija, prenošenje sredstva, plaćanje, pregled kamatnih stopa, ugovora i podnošenje različitih zahteva. Sigurnost ovakvih servisa regulisana je na nekoliko nivoa kako bi stepen pouzdanosti bio što veći. Zaštita korisnika je otežana zbog jaza koji je nastao između razvoja ovakvih servisa i zakonskih regulativa koje se primenjuju na same servise. Autori su u radu obradili primenu Internet bankarskih sistema kao jednog od oblika elektronskog bankarstva, funkcionisanje sigurnosnih mehanizama na većem broju nivoa kao i primenu zakonskih ragulativa. Sigurnost samog Internet bankarstva sagledana je iz ugla sigurnosti koja se nudi na nivou Internet protokola kao i u domenu kriptografskih algoritama kojima se šifriraju podaci koji je prenose u komunikaciji.**

***Ključne reči* – elektronsko bankarstvo; SSL protokol; RSA; zakonska regulativa**

***Abstract* – The rapid development of communications technologies and usage of the Internet in everyday life and work of individuals, as well as a growing popularity of smart devices has led to the convergence of online banking services to customers. The banking industry is the domain of business, which offers its customers a large number of services using new communication media. These services need to provide fast remote access, to save time of users and most importantly they must have high level of security. E-banking services offer customers access to their accounts for review of recent transactions and interest rates, for new transfers, payments, contracts and submittions. various claims. Safety of these services is regulated at several levels to the degree of reliability as high as possible. Protection of users is difficult due to the gap that has emerged between the development of these services and the legal regulations that apply to the services. In this paper, the authors provided an overview of banking system usage and safety mechanisms on several levels, as well as the application of legal ragulativa. Security of the electronic banking is viewed from the perspective of security offered by Internet protocols, as well as in the field of cryptographic algorithms used in process of data transmition.**

***Keywords* – E-banking; SSL protocol; RSA, law regulations**

I. UVOD

Tradicionalno banke nude veliki broj servisa svojim klijentima. Usluge ovakve prirode podrazumevaju transakcije klijenata, platni promet kao i davanje kredita pojedincima ili kompanijama. U poredjenju sa tradicionalnim načinima pružanja bankarskih usluga elektronsko bankarstvo koristi Internet kako bi dostavilo svoje usluge korisnicima. Pod uslugama u domenu elektronskog bankarstva spada otvaranje naloga, prebacivanje sredstava kao i elektronsko plaćanje računa [1]. Pojam elektronskog bankarstva predstavlja upotrebu novih tehnoloških rešenja, kako bi se omogućilo da korisnici sa bilo kog mesta i u bilo koje vreme obavljaju novčane transakcije korišćenjem računarskih mreža. Na ovakav način je značajno olakšan transfer novčanih sredstava. Elektronsko bankarstvo može se realizovati na dva osnovna načina. Prvi način jeste mogućnost da banka koja poseduje fizičke filijale i nudi tradicionalne bankarske usluge otvori web portal na kome će svojim korisnicima ponuditi i usluge elektronskog bankarstva. Na ovakav način korisnicima se nude dodatne povoljnosti bez bilo kakve naknade. Cilj ovakvog vida poslovanja jeste da se usluge banke približe korisnicima kao i da se korisnici i osoblje banke poštede velikih gužvi i čekanja na šalterima banaka.

Nasuprot ovakvoj organizaciji banaka koje nude kako tradicionalne usluge svojim klijentim tako i usluge elektronskog bankarstva, postoji i drugi način organizacije. Drugi način podrazumeva pružanje bankarskih usluga samo putem elektronskih uređaja i računarskih mreža [2]. Ovo znači da banke nemaju fizičke filijale, već se sve usluge pružaju virtualno. Ovakav vid poslovanja nudi korisnicima znatno jeftinije usluge, uz naplatu manjih provizija za obavljene usluge. Problem koji se ovde može javiti jeste kako obezbediti kvalitetnu uslugu klijentima bez fizičkog prisustva. Probleme ovakvog tipa virtualne banke reševaju tako što stupaju u saradnju sa bankama koje zaista fizički postoje. Na ovaj način svojim korisnicima nude mogućnost da u filijalama i na bankomatima banaka saradnica fizički preuzmu svoj novac. Glavni preduslov primene elektronskog bankarstva jeste računarski sistem. Ovo pre svega uključuje pristup Internetu, web servere, menadžment upravljanja bazama podataka, kao i web aplikacije koje generišu dinamičke HTML web strane. Svaki od delova koji čine jedan ovakav sistem mora ispuniti određene kriterijume kako u pogledu performansi, tako i u pogledu zadovoljena sigurnosnih standarda. Sigurnost podataka i privatnost korisnika sistema mora biti na prvom mestu. Na sigurnosnim mehanizmima radi se svakoga dana i posvećuje mu se sve veća pažnja.

DOI: 10.7251/ZRSNG1501113I

II. PRIMENE ELEKTRONSKOG BANKARSTVA

U uslovima vrlo jake konkurencije gde postepeno nestaju razlike između banaka, investicionih banaka, brokerskih firmi i osiguravajućih kompanija, finansijske organizacije su pod stalnim pritiskom da zadrže korisnike svojih usluga, smanje troškove, upravljaju ruzikom i koriste tehnologiju kao izvor konkurentske prednosti. u culju sagledavanja primene elektronskog bankarstva, potrebno je naglasiti da elektronsko bankarstvo ne mora uvek jednobrazno da znači Internet bankarstvo. Primene elektronskog bankarstva mogu se videti od upotrebe bankomata, kućnog bankarstva, web tv bankarstva, mobilnog bankarstva, SMS bankarstva, pa sve do Internet bankarstva. Osnovna razlika među navedenim primerima jeste u načinu realizacije usluga, broju učesnika u komunikaciji, kao i u tome da li banka direktno komunicira sa klijentom ili ne. Primera radi kućno bankarstvo predstavlja komunikaciju poslovne banke i klijenta koji se fizički nalazi u kući. Komunikacija se obavlja putem telekomunikacionih servisa. Kako bi se primenila govorna tehnologija potrebno je da se telefonski aparat preko telefonske mreže poveže sa hardverskim dodatkom koji numeričke podatke iz datoteke pretvara u govorni signal.

Kod Web Tv bankarstva vrši se povezivanje televizije i interneta u jednu celinu. Ovakav vid bankarstva namenjen je ljudima koji nemaju pristup računaru, a u isto vreme imaju potrebu da koriste internet servise. U ovom slučaju vrši se povezivanje tv uređaja sa telefonskom infrastrukturom [3]. Na taj način se tv prijemnik pomoću daljinskog koristi za pokretanje i upravljanje internet servisima. Na tv prijemnik mogu se povezati kao dodatni uređaji tastatura i štampač. Ovakav oblik elektronskog bankarstva omogućava obavljanje kupovine od kuće, plaćanje računa, kao i vršenje bankarskih transakcija. Kako bi se obezbedila sigurnost ovakvog vida elektronskog bankarstva pored tv prijemnika još jedan od osnovnih uređaja jeste i čitač smart katrica.

Internet bankarstvo predstavlja pribavljanje bankarskih informacija i realizaciju bankarskih transakcija preko Interneta. Internet bankarstvo je zasnovano na korišćenju World Wide Web-a, gde se korisniku omogućuje direktan pristup putem web pretraživača. Napredak u proizvodima on-line bankarstva, promene u konkurentskoj strukturi i rastuća popularnost Interneta su stvorili okruženje u kome Internet bankarstvo postaje proizvod za masovnu potrošnju. Klijentima banke ovakvim vidom poslovanja pruža se mogućnost da korišćenjem bilo kog personalnog računara bez odlaska u banku obavljaju većinu poslova putem svog web naloga. Kod Internet bankarstva pristup računu omogućen je putem pretraživača, što eliminiše potrebu za specijalnim softverom. Internet bankarstvo omogućuje pristup elektronskoj banci sa bilo kog računara u svetu, koji je na neki način priključen na Internet. Podaci o obavljenim transakcijama se ne skladište lokalno, tako da korisnik ne mora da brine o tome sa čijeg računara pristupa. Ovim je obezbeđeno da je i sigurnost veća, a banka održava zaštitu sistema.

Sve transakcije se obavljaju on-line, što dovodi do toga da je potrebna sigurna Internet konekcija. Klijentima je omogućen pristup na više načina: putem korisničkog imena i lozinke, broja računa i ličnog identifikacionog broja, odnosno smart kartice. Pristup putem smart kartice pruža viši nivo zaštite u odnosu na druga dva načina pristupa, ali je manje univerzalan: putem korisničkog imena i lozinke može se pristupiti web banci sa bilo koje lokacije u svetu gde postoji računar sa pristupom na Internet, dok se smart karticom može pristupiti samo na mestima gde na računaru postoji čitač kartice.

Kao i u tradicionalnom načinu pružanja bankarskih usluga i kod Internet bankarstva moraju da postoje sredstva kojima će se vršiti plaćanje. Jedan od vidova ovakvog načina plaćanja jeste elektronski novac. Elektronski novac se može definisati kao informacija o monetarnoj vrednosti koju je između ostalog, moguće prenositi kroz računarske mreže, odnosno van uobičajenih kanala plaćanja koje tradicionalno podržavaju banke. Elektronski čekovi su drugi način plaćanja u elektronskom i Internet bankarstvu. Kod ovog načina plaćanja korisnik putem računara formira ček koji će kasnije koristiti u plaćanjima. Kako bi se osigurao ovakav ček korisnik ga mora digitalno potpisati, dodati digitalni sertifikat banke i spakovati u digitalnu kovertu. Digitalni potpis se kreira uz pomoć privatnog ključa, a služi kao dokaz autentičnosti različitih e-transakcija. Digitalni potpis osigurava ispunjenje osnovnog uslova svake finansijske transakcije – neporecivost. Digitalni sertifikat je elektronski dokument kojim korisnik dokazuje svoj identitet prilikom obavljanja transakcije na Internetu. Izdaje ga ovlašćena nacionalna organizacija, tj. telo koje ima međunarodno pravno definisan naziv “certification authority” (CA).

Digitalni sertifikat sadrži korisnikovo ime, serijski broj, datum isteka, kopiju sertifikata vlasnika javnog ključa (koji se koristi za kriptovanje i dekriptovanje poruka i digitalnih potpisa) i digitalni potpis CA, kuće koji potvrdjuje da je sertifikat valjan. Treći način plaćanja koji se javlja u Internet bankarstvu jesu kreditne kartice. Kod kreditnih kartica podaci sa kartica se razmenjuju putem Interneta. Ovi podaci se razmenjuju bez šifriranja što uzrokuje da tajnost podataka i identitet pravog vlasnika u nekom trenutku mogu biti ugroženi. Upravo iz ovih razloga drugi vid plaćanja pomoću kartica jesu šifrirane kartice. Kod ovog načina plaćanja poruka u kojoj se šalju podaci o kreditnoj kartici se pre slanja enkriptuje. Druga strana prlikom primanja enkriptovane poruke proverava identitet vlasnika kreditne kartice. Provera ispravnosti podataka o kartici i digitalnom potpisu vrši banka koja ispravnost podataka potvrđuje potvrdom ispravnosti koju šalje. Sigurnosni mehanizni i način kreiranja digitalnog potpisa opisani su sledećem odeljku.

III. SIGURNOSNI MEHANIZMI INTERNET BANKARSTVA

Kako internet bankarstvo nudi mogućnost da korisnik pristupa svom nalogu i vrši transakcije sa bilo kog mesta potrebno je obezbediti visok nivo sigurnosti. Sigurnost ovakvih sistema trebalo bi da se zasniva na pravilno kreiranoj autentifikaciji korisnika na samom početku korišćenja sistema. U ovakvim slučajevima preporuka autora jeste da se koriste autentifikacioni tokeni. Autentifikacioni tokeni su mali prenosivi uređaji koji se koriste za potvrdjivanje identiteta korisnika kada pristupaju uslugama na Internetu. Njihova glavna karakteristika je da ne zahtevaju instalaciju nikakvog hardvera i softvera, što ih čini mobilnima i upotrebljivima kod

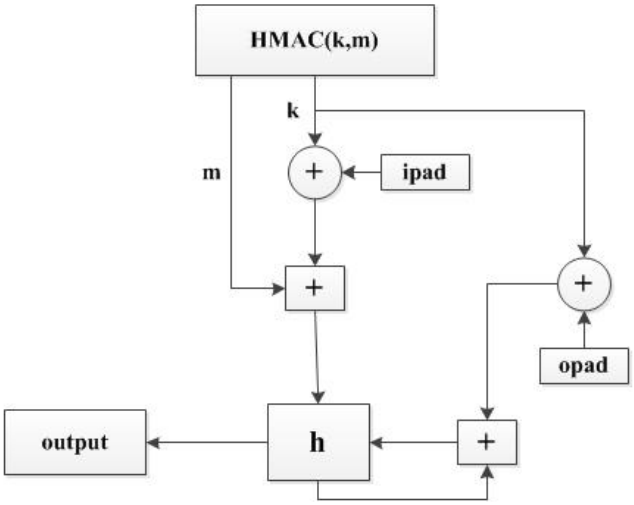
DOI: 10.7251/ZRSNG1501113I

različitih kanala komunikacije. Sigurnost elektronskih bankarskih sistema trebala bi da bude obezbeđena na više nivoa.

Kao jedan od nivoa autori su u nastavku prikazali sigurnosne mehanizme na nivou TCP/IP protokol steka, tačnije Secure Sockets Layer (SSL) protokol. Generalno ovaj protokol je dizajniran za potrebe industrije i ima unapred zadatu namenu [4]. Ovaj protokol je dizajniran tako da zapravo predstavlja dva nivoa protokola. Osnovna uloga SSL protokola je da obezbedi sigurnosne servise protokolima višeg nivoa koji se nalaze iznad njega. U TCP/IP strukturi protokol steka SSL protokol se nalazi između protokola višeg nivo i TCP protokola [8]. Handshake je protokol koji se nalazi u sklopu SSL protokola i može se slobodno reći da je ovo najkompleksnji deo SSL protokola. Handshake je našao primenu u domenu računarske komunikacije koji je uvek najranjiviji, a to je komunikacija izmedju servera i klijenta. Ovaj deo SSL protokola obezbeđuje svu potrebnu enkripciju kao putem MAC algoritama. Pored toga obezbeđuje kriptografske ključeve koji su porebni kako bi se zaštitili podaci koji se šalju putem SSL zapisa. Upravo u ovom delu je potrebno obratiti veliku pažnju i odabrati što bolji kriptografski algoritam u sklopu MAC algoritma.

Poređenja radi u nastavku je data komparacija nekih od algoritama koji se mogu koristiti za ovu namenu. Zapravo kriptografski algoritmi se koriste u domenu funkcije za ekripciju u okviru MAC algoritma koji se primenjuje nad kompresovanim podacima. Heš ključ kod za autentifikaciju poruke ili takozvani HMAC predstavlja jedan od načina kodovanja koji se mogu koristiti za proces u kome se ustanovljava da li je dobijena poruka autentična. On se dobija korišćenjem kriptogrfskih heš funkcija u kombinaciji sa tajnim ključem. Ovime se može istovremeno potvrditi integritet podataka i autentičnost poruke. U tu svrhu može se koristiti bilo koja kriptografska heš funkcija kao što je na primer Tirger Hash, MD5 ili SHA-1. Ove haš funkcije se koriste u proračunu HMAC-a. Kriptografska snaga HMAC-a zavisi od kriptografske snage heš funkcije koje čine njegovu osnovu, od veličine ključa kao i od dužine heš izlaza u bitovima. Na Sl. 1, dat je šematski prikaz HMAC-a. Simbolom *h* na slici označena je korišćena kriptografska funkcija. Simbol *k* je tajni ključ dopunjen nulama do veličine bloka heš funkcije. Simbolom *m* označena je poruka koja se autentifikuje, + označava konkatenaciju, dok $\oplus$ označava XOR operaciju. *Opad* i *ipad* predstavljaju spoljašnje i unutrašnje dopunjavanje, tačnije predstavljaju dve heksadecimalne konstante dužine jednog bloka.

Dve kriptografske heš funkcije koje se mogu primeniti u bloku koji je označen sa *h* jesu MD5 i SHA1. MD5 obrađuje poruke koje imaju promenljivu dužinu i kreira izlaz fiksne dužine od 128 bitova. Ovaj algoritam radi sa 128-bitnim vektorom stanja, podeljenim na četiri 32-bitne reči. Ove reči su inicijalizovane sa određenim fiksnim konstantama. Glavni algoritam radi pojedinačno sa svakom 512-bitnom blok porukom. U algoritmu svaki blok menja stanje. Obrada bloka poruke sastoji se od četiri slične runde. Svaka runda se sastoji od šestaest međusobno sličnih operacija zasnovanih na nelinearnoj funkciji, modularnom sabiranju i levoj rotaciji. Postoje četiri moguće nelinearne funkcije i u svakom krugu se koristi različita funkcija. SHA-1 algoritam u odnosu na MD5 kreira izlaz iz poruke koji je veličine 160 bitova, sa maksimalnom dužinom poruke od 2^{64}-1 bitova. Izlaz se bazira na principima koji se primenjuju i u projektovanju kod MD5. Ipak, iako na izgled nema velikih razlika između ova dva algoritma one ipak postoje. Pored veličine izlaza broj rundi u SHA-1 je veći nego kod MD5 i iznosi 80, nasuprot broju rundi kod MD5 koji iznosi 64. Svaka od rundi ima jedan bit rotacije više, što dovodi do toga da se mešanje kao operacija razlikuje [5].



Sl. 1. Blok šema HMAC algoritma

Izračunavanje bita rotacije je kod SHA-1 isto u svim rundama, dok se kod MD5 razlikuje od runde do runde i za svaku rundu se iznova računa. Ovaj dodatni bit čini da SHA-1 bude znatno otporniji na kolizione napade. Kolizija se u ovom algoritmu pojavljuje samo teoretski, nikada praktično nije dostignuta, što je njegova velika prednost. Funkcije kombinovanja bitova i zaokruživanja kod ova dva algoritma se takođe razlikuju. Ako se pogleda broj elementarnih operacija za svaki ulazni bajt (što se manje ili više slika na veličinu koda ili brzinu, posebno na GPU), može se primetiti da je SHA-1 oko 30% zahtevniji algoritam od MD5, dok je novija verzija ovog algoritma pod nazivom SHA-356 približno duplo zahtevniji od SHA-1.

RSA algoritam obezbeđuje enkripciju javnim ključem kako bi se osigurala poverljivost poruka. Tačnije, ovaj sistem koristi jedinstveni par javnog i privatnog ključa kako bi kreirao digitalni potpis. Glavni problemi u domenu transakcije poruka uključuju ne samo privatnost podataka koji se prenose, već i autentičnost i pošaljioca i primaoca.

Digitalni potpis se koristi za autentifikaciju. Digitalni potpis se kreira na sledeći način: najpre se izračunava sažetak poruke, a zatim se enkriptuje sažetak poruke uz pomoć privatnog ključa pošiljaoca. Prilikom prijema poruke, primalac dekriptuje enkriptovanu poruku pomoću javnog ključa pošiljaoca, čime se potvrđuje njegov indetitet. Pored identifikacije, digitalni potpis potvrđuje da prilikom transporta nije došlo do koruptiranja sadržaja poruke.

Primalac može iskoristiti originalni hash algoritam za kreiranje i upoređivanje novog sažetka poruke koji se dobija dekripcijom dobivene poruke sa originalnim sažetkom poruke.

DOI: 10.7251/ZRSNG1501113I

Ako su jednaki, poruka sigurno nije izmenjena prilikom transporta. Iako enkripcija javnim ključem i digitalni potpis osiguravaju poverljivost i autentičnost poruke, postoji potencijalna opasnost da informacije koje pošaljiaoc daje nisu tačne.

Na primer, pošaljioc može da enkriptuje broj bankovne kartice koji pripada nekom drugom, koristeći svoj privatni ključ. Da bi se osigurala validna autentifikacija, postoji potreba za procesom sertifikacije. Treća strana, kojoj veruju i pošiljaoc i primalac izdaje par ključeva korisnicima koji obezbede dovoljno podataka za utvrđivanje identiteta. Jedna pretpostavka se bazira na poverenju primaoca da ključevi CA, koji se koriste u procesu sertifikacije, nisu kompromitovani. Pod pretpostavkom da SET utiče na stepen korišćenja RSA enkripcije za kućno bankarstvo i online servise za plaćanje, postavlja se pitanje da li SET treba da bude usvojen i za sve bankarske transakcije koje se ne vezuju za kreditne kartice. SET može da omogući plaćanja bez kartica, jer nije specifičan za transakcije sa njima, već podržava generičke transakcije, autentifikaciju, sertifikacihju, enkripciju i slično.

Opisani metodi obezbeđenja sigurnosti u elektronskom bankarstvu su najviše instance koje danas imamo. Primena različitih enkripcionih sistema, različitih načina sigurne komunikacije i utvrđivanja identiteta sigurno će se razlikovati kod davaoca usluga i klijenata. Svi sigurnosti mehanizmi i mehanizmi enkripcije podataka se moraju idalje razvijati i usavršavati.

IV. PRAVNI OKVIRI ELEKTRONSKOG BANKARSTVA

Sistemi elektronske trgovine, elektronskog poslovanja, elektronskog bankarstva pa samim tim i Internet bankarstva moraju biti regulisani zakonskim odredbama kako bi izvršavali svoje delantnosti. U zavisnosti od regiona do regiona elektronsko bankarstvo je u većoj ili manjoj meri pokriveno odgovarajućim zakonskim regulativama. Ono što je na samom početku ovog dela rada potrebno naglasiti jeste da ovakav vid obavljanja elektonskih bankarskih usluga nije najbolje osiguran odgovarajućim zakonskim regulativama. U zavisnosti od toga da li se radi o poslovnim ili privatnim korisnicima, odnosu banke prema klijentima ili odnosu klijenta prema banci, zakonske regulative se razlikuju od zemlje do zemlje. Takođe, organizacija obavljanja medjunarodnog elektronskog bankarstva može biti veoma usporena pravnim barijerama.

Zakonom o elektronskoj trgovini uređuju se uslovi i način pružanja usluga informacionog društva, obaveze informacionog korisnika usluga, komercijalna poruka, pravila u vezi sa zaključenjem ugovora u elektronskom obliku odgovornost pružaoca usluga informacionog društva, nadzor i prekršaji [6]. Ovako definisan zakon se ne premenjuje na zaštitu podataka, oporezivanje, zastupanje stranaka i zaštitu njihovih interesa pred sudovima kao ni na igre na sreću sa novčanim ulozima. Kada se kao pretpostavka punovažnosti i nastanka ugovora zahteva potpis lica, smatra se da taj uslov zadovoljava elektronska poruka potpisana kvalifikovanim elektronskim potpisom, u skladu sa zakonom kojim se uređuje elektronski potpis. Republika Srbija je donošenjem Zakona o elektronskom potpisu, započela proces stvaranja pravnog okvira, neophodnog za uspešno uspostavljanje, funkcionisanje i razvoj informacionog društva. Punom implementacijom tog zakona stvaraju se uslovi za primenu elektronskog potpisa i razmena elektronskih dokumenata uz poverenje najšire javnosti u delovanje i upotrebu elektronskog potpisa, čime se stvara prostor za intenzivnije delovanje sistema elektronske trgovine, koja sve više postaje imperativ konkurentnosti na svetskom tržištu.

Prilikom pružanja usluga informacionog društva, pružalac usluga nije dužan da pregleda podatke koje je skladištio, preneo ili učinio dostupnim, odnosno da ispituje okolnosti koje bi upućivale na nedopušteno delovanje korisnika usluga. Pružalac usluga mora da obavesti nadležni državni organ ako osnovano sumnja da korišćenjem njegove usluge korisnik usluga preduzima nedopuštene aktivnosti, ili je korisnik njegove usluge pružio nedopušteni podatak [1]. Nadzor nad primenom ovog zakona vrši ministarstvo nadležno za poslove trgovine i usluga, odnosno ministarstvo nadležno za poslove telekomunikacija i informacionog društva. Inspekcijski nadzor nad primenom ovog zakona ministarstvo nadležno za poslove trgovine i usluga vrši preko tržišnih inspektora, a ministarstvo nadležno za poslove telekomunikacija i informacionog društva preko inspektora za poštanske usluge i inspektora za telekomunikacije i informatiku. Radi vršenja nadzora, pružaoci usluga dužni su da ovlašćenim licima organa inspekcije omoguće pristup računarskoj opremi i uređajima, kao i da bez odlaganja pokažu ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora.

Prema zakonu o platnim uslugama, elektronski novac označava elektronski (uključujući magnetno) pohranjenu novčanu vrednost koja čini novčano potraživanje prema izdavaocu tog novca, a izdata je nakon prijema novčanih sredstava radi izvršavanja platnih transakcija i prihvata je fizičko i/ili pravno lice koje nije izdavalac tog novca. Imalac elektronskog novca označava fizičko ili pravno lice kome se izdaje ili je izdat elektronski novac, odnosno fizičko ili pravno lice koje se obratilo izdavaocu elektronskog novca radi izdavanja tog novca, kao i svako drugo fizičko ili pravno lice koje ima novčano potraživanje[2]. U skladu sa stavom 1 člana 111 Zakona o platnim uslugama elektronski novac može prihvatiti svako fizičko ili pravno lice koje sa izdavaocem elektronskog novca odnosno pružaocem platnih usluga zaključi ugovor o prihvatanju tog novca. Prema istom članu izdavaoc elektronskog novca može prihvatiti elektronski novac koji je izdao a može prihvatiti i elektronski novac koji je izdao drugi izdavalac tog novca.

Tajnost i zaštita elektronskog novca propisana je članom 74 i 75 Zakona o platnim ulugama. Pomenutim članom 74. definisana je tajnost podataka o platnim uslugama. Ovim članom jasno su definisane odredbe po kojima obaveznik čuvanja poslovne tajne može trećim licima dostaviti podatke koji se smatraju poslovnom tajnom. Prema ovom članu poslovnom tajnom smatraju se podaci do kojih je u toku poslovanja došao pružalac platnih usluga, a odnose se na

[1] Zakon o elektronskoj trgovini, *Službeni glasnik RS*, br. 41/2009 i 95/2013, datum pristupa: 1.10.2015; Dostupan na: http://www.paragraf.rs/propisi/zakon_o_elektronskoj_trgovini.html

[2] Zakon o platnim uslugama, *Službeni glasnik RS*, br. 139/2014, datum pristupa: 1.10.2015; Dostupan na: http://www.nbs.rs/export/sites/default/internet/latinica/20/zakoni/pp_platnim_uslugama_novo.pdf

DOI: 10.7251/ZRSNG1501113I

korisnika platnih usluga, uključujući i podatke o njegovoj ličnosti, kao i podaci o platnoj transakciji i stanju i promenama na platnom računu korisnika platnih usluga. Obaveza čuvanja poslovne tajne iz stava 1. ovog člana za obveznike čuvanja te tajne ne prestaje ni posle prestanka statusa na osnovu kog su ostvarili pristup podacima koji su predmet tajne.

Prema članu 75. ovog zakona pružaoci platnih usluga, učesnici u platnom sistemu i agent za poravnanje dužni su da pri prikupljanju i obradi podataka o ličnosti iz člana 74. stav 1. ovog zakona postupaju u skladu s propisima kojima se uređuje zaštita podataka o ličnosti. Pružaoci platnih usluga i učesnici u platnom sistemu mogu prikupljati i obrađivati podatke iz stava 1. ovog člana radi sprečavanja, ispitivanja ili otkrivanja prevarnih radnji ili zloupotreba u vezi s platnim uslugama.

Veoma često korisnici elektronskog bankarstva i elektrosnke trgovine nisu dovoljno upućeni o svojim pravima i obavezama prema davaocu usluga. S jedne strane to je greška samih korisnika jer ne posvete dovoljno pažnje ugovoru koji potpisuju kao i obaveštenjima koja dobijaju prilikom prvog pokretanja neke elektronske usluge. Federalna komisija za trgovinu u SAD-u objavila je pravni bilten koji definiše i jasno stavlja do znanja korisnicima koja su njihova prava kada koriste elektronske metode plaćanja. U ovom biltenu elektronskog bankarstva korisnici mogu da dobiju informacije o tipovima ličnih informacija koje banka može da objavi. Takođe, isti dobijaju upustva na koji način da postupe kada dođe do greške u obeloganjivanju informacija, kao i tome koje su prave institucije kojima se treba obratiti u slučaju ovakvih propusta [7].

Prema važećim zakonima u SAD-u korisnik od strane banke i finansiskih institucija mora dobiti informacije o pravima i obavezama, obavezama koje korisnik ima kada koristi elektronske bankarske servise, periodične izveštaje i listing plaćanja. Ako se uporede informacije koje su dostupne korisnicima u SAD-u i korisnicima elektronskog bankarsva u Republici Srbiji dolazi se do zaključka da nema velikih razlika. Razlike se mogu javiiti u domenu institucija zaduženih za realizovanje nastalih problema i propusta.

V. ZAKLJUČAK

Elektronsko bankarstvo kao i svi vidovi elektronskog poslovanja pružaju velike prednosti svojim korisnicima. Korisnici ovakvih sistema bilo da su poslovni ljudi, kompanije ili fizička lica naglašavaju da im ovakav vid poslovanja u mnogome štedi vreme i ubrzava poslovanje.

Kako bi krajnji korisnici bili što sigurniji potrebno je stalno raditi na usavršavanju sigurnosti u komunikacionim sistemima, kao i na enkripcionim algoritmima kojima bi se kriptovali lični podaci korisnika.

O nedostacima u ovakvim sistemima koliko se god oni činili sigurnima svakoga dana nam svedoče slučajevi pronevera i zloupotreba servisa za elektronsko poslovanje. Na povećanju sigurnosti ne mogu raditi samo davaoci, već i krajnji korisnici moraju dati svoj doprinos.

Njihov doprinos se mora ogledati u delu pravilnog čuvanja ličnih podataka, pristupnih šifara i autentifikacionih tokena. Davalac usluga ne može zaštititi podatke bilo kog korisnika, ukoliko je pristup nalogu urađen pravilno i ukoliko je zlonamerni korisnik prošao sve mehanizme autentifikacije.

Takođe, potrebno je i na nacionalnom i nameđunarodnom nivou raditi na izgradnji što jasnijih i preciznijih zakonskih okvira koji bi dali pravnu osnovu za zaštitu ovakvih servisa. Ovi okviri bi se ogledali kako u delu brzog procesuiranja i otrkivanja počinioca, tako i domenu adekvatnog kažnjavanja onih osoba koje načine prestup.

LITERATURA

[1] K. Furst, W. Lang and D. Nolle, “Special Studies on Technology and Banking”, Office of the Comptroller of the Currency Quarterly Journal vol. 19, no. 2, 2000, pp. 29–48.

[2] J. Wenninger, “ The Emerging Role of Banks in E-Commerce”, Federal Reserve Bank of New York Current Issues in Economics and Finance, vol. 6, no. 3, 2000, 1–6.

[3] O. Šušak, “Elektronsko bankarstvo i elektronski novac”, Univerzitet Singidunum, Beograd, 2010, pp. 31-100.

[4] McNub, C., Network Security Assessement, O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2nd edition, 2007, pp. 102-196.

[5] V. Vučković, P. Rajković, “Zaštita informacija”, Elektronski fakultet Niš, 2010.

[6] Zakon o elektronskoj trgovini, *Službeni glasnik RS*, br. 41/2009 i 95/2013, datum pristupa: 1.10.2015; Dostupan na: http://www.paragraf.rs/propisi/ zakon_o_elektronskoj_trgovini.html.

[7] Zakon o platnim uslugama, *Službeni glasnik RS*, br. 139/2014, datum pristupa: 1.10.2015; Dostupan na: http://www.nbs.rs/export/sites/default/internet/latinica/20/zakoni/pp_platnim_uslugama_novo.pdf

[8] M. Veinović, A. Jevremović, “Računarske mreže”, Fakultet za informatiku i računarsvo, Univerzitet Singidunum, Beograd, 2011.

DOI: 10.7251/ZRSNG1501113I