

**UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE**

DOKTORSKA DISERTACIJA

***UTICAJ ELEKTRONSKOG BANKARSTVA NA
PONUDU FINANSIJSKIH SERVISA
U SRBIJI***

Mentor:

Prof. dr Budimir Stakić

Kandidat:

mr Tijana Radojević

Beograd, 2009.

S A D R Ţ A J

UVOD	5
------------	---

PRVI DEO

TEHNOLOGIJA ELEKTRONSKOG BANKARSTVA

1. KARAKTERISTIKE I RAZVOJ ELEKTRONSKOG BANKARSTVA	11
2. AUTOMATIZACIJA BANKARSKOG POSLOVANJA	16
3. NOVE TEHNOLOGIJE U BANKARSKOM POSLOVANJU	20
3.1. Elektronski novac	21
3.1.1. Osobine elektronskog novca	24
3.1.2. Osnovni protokol plaćanja	25
3.2. Elektronske platne kartice	26
3.2.1. Opšte karakteristike	26
3.2.2. Kartice sa magnetnom trakom	29
3.2.3. Smart kartice	30
3.2.4. EMV standardi	33
3.2.5. Funkcionalne aplikacije	34
3.3. Automatski samouslužni šalteri - ATM	36
3.3.1. ATM mreže	40
3.4. Maloprodajni terminali – EFT/POS terminali	41
3.5. Kućno bankarstvo (HB)	45
3.5.1. Telefonsko bankarstvo	46
3.5.2. On-line bankarstvo	47
3.5.3. Internet bankarstvo	48
3.5.3.1. Razvoj Internet bankarstva	49
3.5.3.2. Nivoi razvoja bankarskog prisustva na Internetu	51
3.5.3.3. Vrste usluga Internet banaka	51
3.5.3.4. Korišćenje elektronskih čekova u Internet bankarstvu	53
3.5.3.5. E-cash u Internet bankarstvu	54
3.5.3.6. Pametne kartice u Internet bankarstvu	55
3.5.3.7. Šifrovana kreditna kartica (World Wide Web Forma)	56
3.6. Mobilno bankarstvo	56
4. KONKURENCIJA TRADICIONALNIH I INTERNET BANAKA	59
5. PREKLAPANJE POSLOVA I POJAVA NOVIH INSTITUCIJA	62
6. PREDNOSTI INTERNET BANKARSTVA	63
6.1. Radno vreme Internet banaka	64
6.2. Prostorna neograničenost Internet bankarstva	64
6.3. Brzina obavljanja transakcija	64
6.4. Cena obavljanja bankarskih transakcija	65
7. NEDOSTACI INTERNET BANKARSTVA	65
7.1. Nepostojanje zakonske regulative	66
7.2. Odbojnost prema inovacijama kao prepreka u razvoju Internet bankarstva	67
8. MODELI ELEKTRONSKOG POSLOVANJA I ELEKTRONSKOG BANKARSTVA	67

DRUGI DEO

ELEKTRONSKI FINANSIJSKI SISTEMI

1. ELEKTRONSKI SISTEM ODNOSA SA KLIJENTIMA	73
2. ELEKTRONSKI NOVAC I MONETARNI SISTEM	75
2.1. Pojam	75
2.2. Struktura i funkcionisanje sistema elektronskog novca	76
2.3. Atributivne i funkcionalne karakteristike elektronskog novca	78
3. ELEKTRONSKE MREŽE I SISTEMI ELEKTRONSKOG PLAĆANJA	81
3.1. Generalne karakteristike	81
3.2. Definisanje procesa plaćanja	81
3.3. Međunarodna plaćanja	83
3.4. Plaćanja u zemlji – poslovi platnog prometa	84
3.5. Međubankarska plaćanja	84
3.6. Maloprodajna plaćanja	86

3.7. Internet plaćanja	86
3.7.1. Faze procesa plaćanja	87
3.7.2. Principi sistema plaćanja	88
3.7.3. Instrumenti Internet plaćanja	89
3.8. Korporativna elektronska plaćanja	94
3.8.1. Pojam i razvoj	94
3.8.2. Integracija komercijalnih i finansijskih informacija	95
3.8.3. Uvoćenje koncepta STP	97
3.8.4. Primena koncepta STP u praksi	99
3.8.5. STP u EMU	101
4. ELEKTRONSKO BERZANSKO TRGOVANJE	103
4.1. Pojam i karakteristike	103
4.2. Uloga Interneta	105
4.3. Sistemi za prenos podataka sa berze	107
4.4. Karakteristike novog poslovnog modela	109
4.5. Ekonomski aspekti	110

TREĆI DEO

UPRAVLJANJE RIZICIMA U ELEKTRONSKOM BANKARSTVU

1. VRSTE I KARAKTERISTIKE RIZIKA	113
1.1. Operativni rizik	115
1.2. Reputacioni rizik	116
1.3. Pravni rizik	118
1.4. Rizici internacionalnog poslovanja	119
1.5. Ostali rizici	119
2. UPRAVLJANJE RIZICIMA	122
2.1. Procena rizika	123
2.2. Upravljanje i kontrola rizika	124
2.3. Monitoring rizika	125
3. PRINCIPI UPRAVLJANJA RIZIKOM ZA ELEKTRONSKO BANKARSTVO – BAZELSKI KOMITET	127
3.1. Izazovi upravljanja rizikom	128
3.2. Principi upravljanja rizikom	129
3.2.1. Nadzor borda i menadžmenta	130
3.2.2. Kontrola sigurnost	134
3.2.3. Upravljanje pravnim i reputacionim rizikom	139

ČETVRTI DEO

PROBLEMI SIGURNOSTI I MERE ZAŠTITE

1. DIMENZIJE I FUNKCIJE SIGURNOSTI	145
2. TEHNOLOGIJA ZAŠTITE PODATAKA NA INTERNETU	148
2.1. Pojam zaštite podataka	148
2.2. Razumevanje sigurnosnih problema i dimenzija sajber – kriminala	149
2.3. Kako obezbediti dobar nivo sigurnosti u elektronskom poslovanju?	149
2.4. Osnovne sigurnosne pretnje u elektronskom poslovanju	150
2.5. Sistemi zaštite	151
2.5.1. Sistem zaštite na nivou telekomunikacione mreže	151
2.5.2. Sistem zaštite na aplikativnom nivou	152
2.5.3. Sistem zaštite na nivou poruka	152
3. KRIPTOGRAFIJA	153
3.1. Simetrična kriptografija	154
3.2. Asimetrična kriptografija – metod javnih ključeva	155
3.3. Asimetrična kriptografija upotrebom digitalnog potpisa i hash funkcije	156
3.4. Digitalne koverta	157
3.5. Digitalni sertifikat i infrastruktura javnih ključeva	158
3.5.1. Infrastruktura kriptografije sa javnim ključem	160
4. ZAŠTITA NA TEHNIČKOM NIVOU	161
4.1. Alati za zaštitu na nivou Internet komunikacionih kanala	162
4.2. Alati za zaštitu na nivou mreža, servera i klijenata	162
4.3. Protokoli	163

PETI DEO

PRAVNA REGULACIJA E-POSLOVANJA

1. PRAVNI OKVIR	166
1.1. Izgradnja pravne regulative u razvijenim zemljama	168
1.1.1. Važne politike, programi i specifične mere koji podržavaju izgradnju e-legislative u EU	171
1.2. Međunarodne organizacije i institucije i pravna regulativa u domenu elektronskog poslovanja	172
1.2.1. Komisija Ujedinjenih nacija za međunarodno trgovinsko pravo - UNCITRAL	172
1.2.2. Svetska organizacija za intelektualnu svojinu - WIPO	172
1.2.3. Svetska trgovinska organizacija - WTO	173
2. OBLASTI PRAVNOG REGULISANJA	177
2.1. Privatnost na mreži/Internetu	177
2.2. Zaštita intelektualne svojine na mreži: pravo kopiranja i patenti	178
2.3. Spam poruke	179
2.4. Online ugovori	180
2.5. Porezi na Internetu	180
3. PRAVNA REGULATIVA E-POSLOVANJA U SRBIJI	181
3.1. Zakon o elektronskom potpisu	182
3.1.1. Elektronski potpis i kvalifikovani elektronski potpis	183
3.1.2. Elektronski sertifikati i sertifikaciona tela	183
3.1.3. Prava, obaveze i odgovornosti korisnika i sertifikacionih tela	185

ŠESTI DEO

ELEKTRONSKO BANKARSTVO U SRBIJI

1. OPŠTE STANJE	188
2. MEĐUBANKARSKI PLATNI SISTEM U SRBIJI	191
3. KREDITNI BIRO	194
4. PLATNE KARTICE	196
5. TRGOVINA NA INTERNETU	199
6. STUDIJA SLUČAJA U JEDNOJ DOMAĆOJ BANCI	201
6.1. Primena elektronskog bankarstva u Komercijalnoj banci a.d. Beograd	201
6.1.1. E-bank za pravna lica	202
6.1.1.1. Osnovne funkcije Personal E-bank za pravna lica	204
6.1.2. E-bank za fizička lica	211
6.1.2.1. Osnovne funkcije Web E-bank servisa za fizička lica	213
6.1.3. Korišćenje SMS servisa	229
6.2. Pokazatelji ostvarenog prometa u E-banci Komercijalne banke a.d. Beograd	230
6.3. Unapređenje poslovanja E - bankarstva	234
ZAKLJUČNA RAZMATRANJA	236
LITERATURA	245

UVOD

Razvoj e-bankarstva vezan je za sve širu primenu računarske i telekomunikacione tehnologije u procesu obrade i prenosa podataka i informacija. Ove tehnologije dovode do krupnih promena u funkcionisanju banaka. Pokrenuti procesi dovode do uvođenja novih postupaka i tehnologija, koje sobom nose nove izazove i mogućnosti.

Tehničko - finansijske inovacije, sa svoje strane, vode intenziviranju konkurencije u svim segmentima. Dolazi, ne samo do reinjeringa poslovnih procesa u bankama, već i do reinjeringa u poslovnim procesima i odnosima između samih banaka, banaka i njihovih klijenata i između klijenata i trećih lica međusobno. Klasično bankarsko poslovanje i lični susret sa klijentima sve se više zamenjuju automatizovanom proizvodnjom i isporukom usluga. Troškovi velikih transakcija se smanjuju, a bankarske i finansijske usluge depersonalizuju.

Usled ubrzanog širenja elektronskih bankarskih sistema dolazi do velikih preokreta u suštini samog e-bankarstva, koje sve više postaje sinonim modernog bankarstva. Danas bankarsko poslovanje u potpunosti počiva na tehničko - tehnološkim resursima, a informaciono komunikacione tehnologije postaju vodič za strategiju i reinjering.

Trend modernog bankarstva je automatizacija svih funkcija (finansijskih operacija) primenom računarskih tehnologija. Primarni cilj uvođenja sistema elektronskih plaćanja je rešavanje problema sistema plaćanja zasnovanih na papiru, korišćenjem potencijalnih prednosti primene informacione tehnologije. Pojava elektronskog novca nametnula je potpuno novu filozofiju u bankarstvu koja se zasniva na elektronskoj razmeni podataka i sredstava (engl. *Electronic Funds Transfer*), koja je pojmovno određena kao elektronsko bankarstvo.

Glavni cilj e-bankarstva je da se bez obzira na geografsku udaljenost što brže i efikasnije povežu klijenti i tokovi informacija. Tajna uspešnog savremenog informacionog sistema je fleksibilna infrastruktura bazirana na personalnim računarima, modernim računskim mrežama i Internetu pre svega.

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja banaka tj. do uvođenja novih kanala distribucije bankarskih usluga, odnosno elektronskog bankarstva.

Primena elektronskog bankarstva na nacionalnom, regionalnom i na globalnom nivou, promoviše se u neophodan proces ekspanzije bankarskog sistema.

Predmet ovog rada je:

1. analiza osnovnih karakteristika elektronskog novca;
2. opis vrsta usluga u elektronskom bankarstvu;
3. opis sistema sigurnosti i zaštite poslovanja banaka na Internetu;
4. analiza tipova elektronskih sistema plaćanja, sa posebnim osvrtom na elektronsko bankarstvo u Srbiji;
5. prikaz novih finansijskih servisa u bankama u Srbiju koji su nastali pod uticajem elektronskog bankarstva.

Naučni cilj ovog istraživanja jeste naučni opis savremenih procesa u elektronskom bankarstvu Srbije, njegova komparacija sa tendencijama koje odlikuju najznačajnije bankarske sisteme u svetu danas; naučni opis promena u srpskom elektronskom bankarstvu na institucionalnom i funkcionalnom planu, iz ugla nove strukture banaka i novih proizvoda koje one nude.

Društveni cilj izrade ove doktorske disertacije je doprinos proučavanju i razumevanju savremenih tendencija u razvoju svetskog elektronskog bankarstva, kako bi se dalji razvoj elektronskog bankarstva u Srbiji odvijao u skladu sa sistemskim promenama na socijalnom, političkom i ekonomskom planu, a njegove korelacije sa integracionim procesima u svetu vodile dostizanju najvišeg kvaliteta bankarskih usluga u Srbiji.

Hipotetički okvir istraživanja sastoji se od sledećih pretpostavki:

Generalna hipoteza:

- U uslovima globalizacije poslovanja banaka, jake konkurentnosti i promenljivosti okruženja, elektronsko bankarstvo sve više dobija na važnosti.

Posebna hipoteza:

- Uvođenje informacionih tehnologija u bankarski sektor je neophodno, s obzirom na to da je u ovom sektoru konkurencija sve više izražena.
- Primena savremenih informacionih tehnologija u elektronskom bankarstvu utiče na brže i efikasnije povezivanje klijenata i tokova informacija.
- Uspešnost primene elektronskog bankarstva u direktnoj je korelaciji sa kvalitetom usluga elektronskog bankarstva (povećan broj transakcija, brža realizacija transakcija, kvalitetna podrška informacionih tehnologija, obučeno osoblje, kvalitetni bezbednosni sistem).

Pojedinačna hipoteza:

- Bankarsko tržište kao jak kontrolni mehanizam bankarskog upravljanja, intenzivno promoviše upotrebu elektronskog bankarstva radi ostvarenja boljih poslovnih i finansijskih performansi banaka.
- Transparentnost u radu banke i njena ukupna finansijska disciplina, pospešuju primenu elektronskog bankarstva.
- Od ekonomske snage banke direktno zavisi uvođenje novih tehnologija.

Metodološki pristup istraživanja koji će se primenjivati u izradi ove doktorske disertacije postavljen je veoma kompleksno i zahteva primenu:

- od analitičkih osnovnih metoda: metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- od sintetičkih osnovnih metoda: sintezu, konkretizaciju, generalizaciju i indukciju;
- od opštenaučnih metoda: hipotetičko - deduktivnu, analitičko - deduktivnu, komparativnu, statističku i metodu modelovanja.

Adekvatna primena ovog pristupa omogućiće da se steknu pouzdana saznanja o predmetu istraživanja, o činjenicama, pojavama, procesima i odnosima na kojima počiva i odvija se transformacija elektronskog bankarstva u Srbiji, ali i o pojmovima, stavovima, sudovima i zaključcima koji su relevantni za ispunjavanje svrhe ovog rada.

Primenom ovih metoda, kako pokazuju dosadašnji rezultati istraživanja moguće je validno ostvarenje naučnog i društvenog cilja istraživanja. Pristup istraživanju je integrativan, sintetički u tom smislu što se ni jednom metodološkom postupku ne daje isključiva prednost.

Analiza će biti ostvarena na dva nivoa:

- na nivou izvornih podataka, na osnovu izvornih dokumenata banaka i
- na nivou sekundarne analize rezultata ranijih istraživanja i adekvatne literature.

U radu će biti detaljno istraženo:

- da li su se (kad i kako) pojavili novi servisi,
- kako su stari unapređeni,
- da li su transakcije bezbednije,
- da li je povećan broj pronevera.

Na osnovu dobijenih rezultata istraživanja o prednostima elektronskog bankarstva, ova analiza će pokušati da utiče na modernizaciju bankarstva u Srbiji, koje je jedan od bitnih faktora za uspešan ekonomski razvoj zemlje u celini. Velike promene očekuju se u celoj nacionalnoj privredi (završetak procesa privatizacije društvenih preduzeća), a samim tim i u razvoju bankarstva, kao generatoru privrednog razvoja. U tom pogledu od ovog rada očekuje se određeni doprinos u intenziviranju napora da se bankarstvo u Srbiji po svojoj strukturi, organizaciji, funkcionisanju i tehničko-tehnološkoj opremljenosti približi modelima modernog svetskog e-bankarstva.

Očekuje se da sa stanovišta naučnog doprinosa ovaj rad izgradi celovit i konzistentan teorijski okvir za primenu elektronskog bankarstva u Srbiji. Ono što je posebno bitno, jeste da se kao rezultat ovog rada očekuju, pored naučno metodoloških doprinosa i veoma konkretne preporuke u modernizaciji i primeni informacionih tehnologija u srpskom bankarstvu.

Polazeći od postavljenih hipoteza i ciljeva istraživanja proistekla je i odgovarajuća struktura rada.

U prvom delu doktorske disertacije koja nosi naziv „Tehnologija elektronskog bankarstva“, biće obrađen razvoj elektronskog bankarstva, automatizacija bankarskog poslovanja, nove tehnologije u bankarskom poslovanju, kao i modeli elektronskog poslovanja i elektronskog bankarstva.

U drugom delu „Elektronski finansijski sistemi“, biće analizirani elektronski sistem odnosa sa klijentima, elektronski novac i monetarni sistem, elektronske mreže i sistemi elektronskog plaćanja, kao i elektronsko berzansko trgovanje.

Treći deo rada „Upravljanje rizicima u elektronskom bankarstvu“ pažnju posvećuje vrstama i karakteristikama rizika, upravljanju rizicima, kao i principima upravljanja rizikom u elektronskom bankarstvu.

U četvrtom delu „Problemi sigurnosti i mere zaštite“ analiziraće se tehnologija zaštite podataka na Internetu, funkcije sigurnosti, kriptografija, kao i alati za zaštitu na nivou Internet komunikacionih kanala.

U petom delu rada „Pravna regulacija e-poslovanja“ biće obrađen pravni okvir i pravna regulativa e-poslovanja u svetu i u Srbiji.

U šestom delu „Elektronsko bankarstvo u Srbiji“ biće analiziran razvoj e-bankarstva u Srbiji, sa posebnim osvrtom na elektronsko bankarstvo u Komercijalnoj banci a.d. Beograd.

Razvoj elektronskog bankarstva u Srbiji počinje sa reformama bankarskog sektora i prelaskom platnog prometa u bankarski sistem, u januaru 2003. godine. Do tog trenutka banke su jedini vid elektronskog poslovanja ostvarivale u domenu deviznog sektora tj. poslovnih odnosa sa inostranstvom i to putem SWIFT-a.¹

Prelaskom platnog prometa u poslovne banke, stvoreni su svi uslovi da domaće banke ponude nešto novo našem tržištu. To su bile bezgotovinske transakcije (virmanska plaćanja) putem Interneta. Krajem 2003. godine, pošto je uveden e-banking za pravna lica, banke u Srbiji su bile spremne i za e-banking za fizička lica.

Ovakav način poslovanja brzo su prihvatile gotovo sve banke, a neke postižu i da čak 50% ukupnog broja naloga dolazi u banku elektronskim putem.

Asortiman ponude e-bankarstva se drastično širi u kratkom vremenskom periodu. Preko kućnog računara, banke svojim klijentima omogućavaju: uvid u stanje računa, pregled prometa, pregled izvoda promena na računu, prijem i slanje ličnih poruka, plaćanje obaveza platnim nalogima sa tekućim datumima i datumima unapred.

Komercijalna Banka a.d. Beograd, sa izuzetno visokim rejtingom i imidžom u bankarskim krugovima, od samog početka je vrlo ozbiljno shvatila prednosti elektronskog poslovanja, i postala je predvodnik svim ostalim bankama u Srbiji.

Osluškujući permanentno potrebe klijenata kao i uvažavajući njihove želje, Banka je konstantno modifikovala i unapređivala svoja rešenja i postavljala uvek nove i više standarde u ovoj oblasti poslovanja. Komercijalna banka a.d. Beograd trenutno na tržištu ima najsavremenije elektronske servise iz oblasti korporativnog e-bankarstva i najobuhvatnije web rešenje namenjeno fizičkim licima koje predstavlja rezultat zajedničkog rada na razvoju između banke sa jedne i vendora - proizvođača softvera sa druge strane, što svakako predstavlja pozitivan primer kvalitetnog strateškog partnerstva.

U periodu od 2005-2008. godine, broj korisnika elektronskog bankarstva u Komercijalnoj banci a.d. Beograd iz godine u godinu se znatno povećavao.

Banka je na kraju 2005. godine imala 5.452 klijenta - pravna lica koji su koristili elektronsko bankarstvo, a u avgustu 2008. godine imala je 8.967 klijenata - pravnih lica, što predstavlja povećanje od 3.515 klijenata ili 64%. Povećanje u odnosu na 2007. godinu iznosi 10,58%.

Što se tiče fizičkih lica, Banka je na kraju 2005. godine imala 10.424 klijenata koji su koristili elektronsko bankarstvo, a 2008. godine imala je 23.682 klijenta, što čini povećanje od 13.258 klijenata, ili 127%. Povećanje u odnosu na 2007. godinu iznosi 11,86%.

¹ engl. *Society for Worldwide Interbank Financial Telecommunications* - Međunarodna finansijska mreža za transfer sredstava.

Kada se posmatra procentualno učešće elektronskih naloga u odnosu na ukupan broj naloga u platnom prometu Komercijalne banke a.d. Beograd, moć e se konstatovati da je prisutan stalni rast prometa preko e-banke. U januaru 2007. godine učešće je iznosilo 17,32%, da bi u junu 2008. godine iznosilo 24,76% u ukupnom platnom prometu Komercijalne banke a.d. Beograd.

Aplikativna rešenja vezana za elektronsko bankarstvo u Komercijalnoj banci a.d. Beograd, bilo pravnih ili fizičkih lica, odnose se isključivo na aktivnosti iz domena platnog prometa. Odnosno, klijentima se preko e-banke nudi mogućnost svih vrsta plaćanja u zemlji i inostranstvu za pravna lica i mogućnost izmirenja obaveza tj. plaćanja raznih računa za fizička lica u zemlji. Neminovnost daljeg razvoja elektronskog bankarstva, jeste dopuna osnovnog paketa usluga koji se trenutno nudi preko e-banke, pratećim servisima koji će imati za rezultat potpuno zatvaranje poslovnog procesa, odnosno mogućnost da se kompletan poslovni proces oko kredita obavi iz poslovne prostorije i od kuće bez odlaska u banku, kao i mogućnost zamene dokumentarne kontrole (trenutno obavezne u deviznom poslovanju) sa elektronskim dokumentima koji su digitalno potpisani, a samim tim i potpuno validni i identični papirnim.

Na kraju rada će se dati Zaključna razmatranja, kao i spisak korišćene literature i drugih izvora.

PRVI DEO

**TEHNOLOGIJA ELEKTRONSKOG
BANKARSTVA**

1. KARAKTERISTIKE I RAZVOJ ELEKTRONSKOG BANKARSTVA

Sve izraćenija deregulacija u bankarskom sektoru, kao i sve veći značaj informacionih i telekomunikacionih tehnologija, dovela je do uvoćenja novih kanala distribucije bankarskih usluga, odnosno elektronskog bankarstva i Internet bankarstva kao njegovog najizraćenijeg oblika.

Razvoj informacionih tehnologija je omogućio transformaciju klasičnog bankarstva, koje se ogleda u prenošenju informacija u realnom vremenu i obradi podataka. Informacione tehnologije omogućavaju smanjenje troškova obrade podataka i komunikacije, što utiče na smanjenje cene usluga krajnjim korisnicima.

Pored navedenog, informacione tehnologije omogućavaju nastanak virtuelnih banaka (koje nemaju fizičkih filijala i kod kojih su potrebe za brojem zaposlenih minimalne) i sve veće korišćenje elektronskog novca, što na kraju otvara mogućnost za stvaranje nebankarskih institucija, koje će isto nuditi bankarske usluge. Osnovni efekat razvoja informacione tehnologije jeste povećanje konkurencije na finansijskom tržištu, iz razloga što je olakšan pristup informacijama, koje nude davaoci korisnicima usluga.

Savremeno bankarstvo gotovo da nije moguće zamisliti bez masovne primene računara. Nikada u istoriji bankarskog poslovanja nisu učinjene tako velike i korenite promene kao za poslednjih tridesetak godina. Pojava plastičnog (kartice) i digitalnog novca učinili su preokret ka potpunoj dematerijalizaciji i virtuelizaciji novca. Internet, e-bankarstvo i mobilno bankarstvo su doveli do toga da je banka izašla iz svojih prostorija. Kroz istoriju, korisnik je uvek morao da dolazi u prostorije banke kako bi obavio posao. Danas se sve finansijske transakcije mogu obaviti od kuće, sa radnog mesta ili putem mobilnog telefona.²

Bankarsko poslovanje koje je vekovima funkcionisalo na tradicionalan način sa ustaljenom tehnologijom, odjednom se našlo u vrtlogu informacione tehnologije. Transformacije koje su u toku mogu se opisati na sledeći način:³

- „Brick and mortar“ institucija – Banka sa zgradom i personalnom uslugom;
- „Brick and click“ institucija – Banka sa fizičkom infrastrukturom i Internet bankarskim uslugama;
- „Virtual bank“ – Banka bez javne zgrade i postoji samo *on-line*;
- „Mobilno bankarstvo“ – poslovanje preko mobilnih uređaja uglavnom kao dodatak prethodnim varijantama bankarstva.

Elektronsko bankarstvo (engl. *e-banking*) je vid bankarskog poslovanja u kome se intenzivno koriste računске mreže, Web tehnologija, Internet i telekomunikacioni mediji. Njihova implementacija podrazumeva hardversko-softversku platformu, precizno definisane mrežne komponente, određenu organizacionu strukturu, standardizaciju i sl.

Elektronsko bankarstvo (e-bankarstvo) u užem smislu je još uvek u početnoj fazi razvoja. Ono podrazumeva tzv. virtuelne banke koje posluju isključivo preko Interneta i bez filijalske

² Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, Fakultet organizacionih nauka, Beograd, 2007. str.20

³ Isto, str.24

mreže. U širem smislu, ovim terminom se obuhvata i tzv. udaljeno bankarstvo (engl. *remote banking*) odnosno bankarsko poslovanje koje koristi informacionu tehnologiju i daljinske *online* komunikacione veze sa klijentima. Ovako šire shvaćeno, elektronsko bankarstvo se može posmatrati kao skup raznovrsnih načina izvođenja finansijskih transakcija upotrebom informacionih i telekomunikacionih tehnologija.⁴

Prvi sistem za koji bi se moglo reći da ima karakteristike primitivnog elektronskog transfera, sreće se još 1918. godine, je FED-ov sistem telegrafskih plaćanja. Kasnije, pedesetih godina *Bank of America* primenjuje ove elemente u obradi čekova, a sedamdesetih godina dolazi do naglog povećanja broja pristupnih kanala. Proces počinje najpre uvođenjem bankomata, zatim sredinom devedesetih uvođenjem telebankinga sa osvajanjem sve većeg broja domaćinstava. Internet tehnologije dovode do uvođenja prve generacije *online* bankarskih usluga. Prva Internet banka, SFNB (*Security First Network Bank*) počela je da funkcioniše 1995. godine u SAD.

Osnovne tendencije razvoja bankarskog sektora karakterisale su se naporima da se informaciona tehnologija upotrebi za snižavanje troškova bankarskog poslovanja i promene načina same bankarske usluge. Korišćenje informacione tehnologije kao sredstva za snižavanje troškova značilo je prvenstveno njenu upotrebu za eliminisanje troškova rada. Te promene su sobom donele i nove načine pružanja usluga, direktne isporuke putem novih kanala (telefon, Internet, digitalna televizija).

Sa uvođenjem svakog novog komunikacionog kanala rastao je i nivo očekivanja koji se odnosi na bankarske usluge. Dolazi do ponude pristupa statusnim informacijama svake pojedinačne transakcije i to u vreme kada su i na mestu gde su korisniku potrebni, a ograničenje na klasično radno vreme postaje neprihvatljivo. Danas se od banaka zahteva prilagođavanje potrebama svakog pojedinačnog klijenta - korisnika.

Najznačajnije promene koje su do sada ostvarene u domenu elektronskog bankarstva odnose se pretežno na domen rutinskih transakcija u bankama, i to pre svega u platnom prometu. Sistemi za elektronski prenos sredstava (engl. *Electronic Funds Transfer System - EFTS*) predstavljaju prve manifestacije uvođenja tehnoloških inovacija na bazi primene informacione i komunikacione tehnologije, tako da za ranu fazu e-bankarstvo praktično znači uvođenje informacione i komunikacione tehnologije u sistem plaćanja.

Kao osnovne komponente sistema za elektronski prenos sredstava pojavljuju se automatizovane klirinške kuće (engl. *Automated Clearing House - ACH*) i elementi tzv. daljinskog bankarstva. U ovu kategoriju distribucionih sistema spadaju: ATM sistemi (engl. *Automated teller machines - ATM*), kućno bankarstvo ili HB (engl. *Home Banking - HB*), POS sistemi (engl. *Point - of - sale*) ili EFTPOS (engl. *Electronic funds transfer at point of sale*). Njihov razvoj je tesno povezan sa pojavom i razvojem različitih varijanti plastičnih kartica i elektronskim novcem. U literaturi se ACH, ATM, i POS sistemi slikovito opisuju kao tri stuba EFTS tronošca pre pojave Interneta. Kasnije, sa pojavom Interneta ovi sistemi doživljavaju svoje dalje unapređenje i transformaciju pa postaju razne varijante Internet bankarstva.

U savremenim uslovima kontakti klijenata sa bankama mogu se uspostavljati na različite načine i pomoću različitih sredstava, odnosno kanala. Tradicionalne kanale za uspostavljanje

⁴ Vuksanović E.: „Elektronsko bankarstvo“, Fakultet za bankarstvo, osiguranje i finansije, Beograd, 2006. str.1

daljinskih komunikacionih kontakata sa klijentima čine zatvoreni informacioni sistemi, koji su vezani za jednu banku ili za grupu banaka. Često poseban posrednički provajder formira ove sisteme, a banke samo koriste određene servise za svoje klijente. U ovu grupu spadaju: višenamenski ATM sistemi, sistemi telefonskog bankarstva, *online* kućno bankarstvo, EFTPOS. U daljem razvoju *online* veze između klijenata i banaka dolazi do sve veće zastupljenosti Interneta kao najjeftinijeg i najperspektivnijeg komunikacionog kanala. Zbog toga banke usmeravaju svoje elektronske bankarske usluge ka Internetu, dok su ranije bile orijentisane na investiranje u sopstvenu tehnologiju.⁵

Kao rezultat najnovijeg trenda u razvoju bežičnih pristupa uslugama e-bankarstva pojavljuje se tzv. mobilno bankarstvo. U njemu danas daleko prednjače skandinavske zemlje, a u narednih nekoliko godina očekuje se da će njegova ekspanzija biti snažnija od ekspanzije Internet bankarstva. Mobilno bankarstvo omogućava izvršavanje transakcija putem prenosnih računara, digitalnih ličnih organizatora i mobilnih telefona.

Platni promet doživljava suštinsku promenu sa uvođenjem elektronskog prenosa novca (engl. *Electronic Funds Transfer - EFT*) koji rešava mnoge probleme prethodnih sistema plaćanja. Potreba za uvođenjem elektronskog prenosa sredstava u papirni platni promet javila se onda kada je obim platnog prometa narastao do te mere da je postalo nemoguće da se obavlja na postojeći način, zbog fizičkih ili finansijskih ograničenja. Dakle, osnovni problemi u funkcionisanju papirnih sistema plaćanja su:

1. nemogućnost praćenja porasta obima platnog prometa iznad određene granice;
2. troškovni pritisak usled porasta obima platnog prometa.

Tradicionalni sistemi su se zasnivali na čekovima i tiro platnom prometu. I jedan i drugi sistem plaćanja zahtevali su veliku količinu ljudskog rada, papira i dosta vremena za obavljanje plaćanja, što je doводilo do troškovnog pritiska na banke. Sve to je uticalo na potiskivanje papirnog načina plaćanja u korist elektronskog sistema plaćanja. Sedamdesetih godina prošlog veka dolazi do zamene papirnih sistema plaćanja elektronskim. EFT se uvodi, kako u međubankarske relacije, tako i u odnosima između banaka i njihovih klijenata.

Prve ideje za rešavanje problema porasta obima papirnih tokova platnog prometa kroz proces uvođenja informacionih tehnologija i eliminisanje papira, dala su dva američka profesora Jakobs Henri (*Jacobs Henry*) i Robert H. Gregori (*Robert H. Gregory*). Kada je u praksi počela primena informacionih tehnologija u sistemu plaćanja, menjale su se metode i tehnička rešenja, ali je suština koncepta ostala ista. Ona se sastoji u mogućnosti da se tehničko-tehnološke i ekonomske karakteristike informacione tehnologije iskoriste za:

1. eliminisanje papira iz sistema plaćanja;
2. povećanje brzine transakcionih i informacionih tokova;
3. snižavanje transakcionih troškova.

Pored platnog prometa, EFT je našao značajnu primenu i u drugim rutinskim operacijama koje banke vrše za svoje klijente, kao što su polaganje novca na transakcione i štedne račune, transfer novca sa jednog računa na drugi, upitima stanja na računima, transakcijama na deviznom i novčanom tržištu, kupovini i prodaji vrednosnih papira i itd.

⁵ Isto, str. 3

U praksi permanentno dolazi do širenja lepeze rutinskih bankarskih poslova koji se prevode na elektronsku osnovu. U tom kontekstu do sada posebno su došli do izražaja sledeći vidovi e-bankarskih poslova: pristup informacijama; pregled stanja računa i elektronsko plaćanje računa; pružanje korisnih informacija i novi kontakti; višesmerne komunikacije; usluge prenosa struktuiranih podataka; usluge prenosa nestruktuiranih podataka; sistemske usluge; transferi sredstava sa računa na račun; međubankarski transferi; menjački poslovi; elektronska procedura dodele kredita; otplata kredita i sl.⁶

Tri bitna faktora su uticala na razvoj elektronskog bankarstva:⁷

- a) visok nivo razvoja računarske tehnologije, pogodne za primenu u finansijskim institucijama, što je za direktnu posledicu imalo koncentraciju visoko stručnih i obrazovanih kadrova u bankarskim institucijama,
- b) složena finansijska struktura, koju karakteriše veliki broj finansijskih institucija,
- c) visok stepen deregulacije (kako na domicilnom tako i na svetskom) finansijskom tržištu, što ima za posledicu oštru konkurenciju između banaka.

Pod uticajem tehnološke revolucije dolazi do grubog razdvajanja elektronskog poslovanja banaka na:

1. elektronski vođene međubankarske poslove i
2. elektronski vođeno poslovanje sa klijentima.

Elektronsko poslovanje sa klijentima se dalje diferencira na dva segmenta:

1. e-bankarstvo na malo (engl. *retail banking*) i
2. korporativno e-bankarstvo (engl. *corporate banking*).

Era Interneta, koja nastupa sredinom devedesetih, omogućava bankama, ne samo da komuniciraju sa klijentima na potpuno nov način u oblasti prenosa informacija i obavljanja plaćanja, već i nov način obavljanja poslovanja. Za male banke je bitna mogućnost da se pomoću Interneta premoste tradicionalne troškovne barijere koje su imanentne uvođenju informacionih tehnologija.

Dok je za ranu fazu razvoja elektronskog bankarstva bila karakteristična upotreba informacione tehnologije za racionalizaciju pojedinih procesa (automatizacija kancelarijskog poslovanja i omogućavanje samousluživanja klijenata), u zreloj fazi sve značajnije postaju mogućnosti uvođenja različitih inovacija u oblast bankarskih proizvoda. Sa ovom promenom dolazi i do promena u samom poslovnom značaju informacione tehnologije.

Racionalizacijom poslovnih procesa omogućavano je reduciranje troškova obavljanja bankarskih poslova, a inovacijama u oblasti proizvoda omogućava se podizanje kvaliteta bankarskih usluga i po tom osnovu, uvođenje viših cena za ponuđene usluge. Zbog toga u mogućnostima racionalizovanja postojećih procesa i kreiranja novih bankarskih proizvoda treba videti samo podsticajna sredstva za brojne inovativne aktivnosti banaka u poslovanju sa stanovništvom i privredom.

⁶ Isto, str.4

⁷ Vunjak N., Kovačević Lj.: „Bankarstvo“ (Bankarski menadžment), Subotica, 2006., str. 263

U celini posmatrano, sve ove inovacije mogu se svrstati u četiri osnovne kategorije e-bankarstva:

1. elektronska plaćanja,
2. samousluživanje klijenata,
3. informacione usluge i
4. elektronsku kooperaciju.

Kako se njihove pojedinačne ili kombinovane primene zasnivaju na EFT, u međubankarskim relacijama i sa klijentima, porast kvantiteta i kvaliteta ponude e-bankarstva predstavlja direktan rezultat unapređenja funkcionisanja interorganizacionih informacionih sistema u ovoj oblasti.

Tradicionalni pristup upotrebi informacione tehnologije kao novom vidu racionalizacije u upotrebi bankarskih potencijala bio je usmeren na automatizaciju operativnih poslova. Danas, bankarsko poslovanje u potpunosti počiva na resursima informacionih i telekomunikacionih tehnologija. Znači, savremeno elektronsko bankarstvo nema ulogu dodatnih usluga koje bi nudile samo najmoćnije banke, već su elementi ove vrste zastupljeni u ponudi gotovo svih banaka. Zbog toga se ističe da je nepotrebno koristiti poseban termin elektronsko bankarstvo i da sam termin bankarstvo danas podrazumeva bankarsko poslovanje na bazi elektronske infrastrukture.

Osnovni pozitivni efekti primene elektronskih tehnologija u bankarstvu proizilaze iz potencijalne mogućnosti da se pomoću njih obezbedi ekonomičnije, efikasnije i sigurnije poslovanje u odnosu na tradicionalno, papirno poslovanje. Međutim, korišćenja troškovno efektivnih tehnologija, koje se inače mogu različito organizovati i kombinovati, nose sa sobom krupne zahteve i novine u mnogim domenima. Zbog toga se ono pojavljuje samo kao sredstvo koje otvara vrata ekonomičnom i efikasnom poslovanju, ali ne garantuje njegovo ostvarenje. Stepennostvarivanja ovih zahteva povezan je sa mogućnostima obezbeđenja potrebnog nivoa sigurnosti elektronskih poslovnih sistema, sa jedne strane i njihovog širenja u regionalnom i poslovnom smislu, sa druge strane. Kao fundamentalni faktori obezbeđenja ovih mogućnosti pojavljuju se standardi i reinženjering samog poslovanja (radnih procesa i organizacionih struktura), pri čemu između njih postoji visok stepen međuzavisnosti. Nameće se potreba paralelnog i sinhronizovanog unapređenja i informatičkih i poslovnih rešenja.

Tehničko - finansijske inovacije vode intenzivnoj globalnoj utakmici sa bankarskim okruženjem. Dolazi ne samo do reinženjeringa u bankama, već i do reinženjeringa u procesima između samih banaka, banaka i njihovih klijenata i između klijenata i trećih lica međusobno. Sa prelaskom na novu tehničko - tehnološku osnovu stvara se nova filozofija poslovanja koja sobom nosi prilagođavanje softverskih rešenja korisničkim potrebama, promenu strategije nastupa banaka, načina i metoda upravljanja rizicima itd.

Poslovna filozofija lokacijskog približavanja usluga korisnicima, nametnula je i ubrzani razvoj elektronskog bankarstva i njegovu standardizaciju. Banke su primorane da učestvuju u razvoju novog elektronskog bankarstva da ne bi izgubile svoju poziciju na tržištu. Tako danas u SAD oko 79% banaka nudi kućno elektronsko bankarstvo, dok se ostalim vidovima elektronskog bankarstva obavlja preko 50% ukupnih transakcija. U Japanu se skoro 90% transakcija obavlja preko sistema elektronskog bankarstva.

U većini evropskih zemalja, više od dve trećine negotovinskih transakcija obavlja se elektronskim putem, a od svih zemalja u svetu Finska i Švedska imaju najveći broj klijenata koji koriste bankarske usluge preko Interneta.

Zašto su Evropljani, a posebno Skandinavci, toliko ispred Amerikanaca kada je u pitanju elektronsko plaćanje?

Prvo, Evropljani su navikli da obavljaju plaćanja bez čekova i pre nego što su računari ugledali svetlost dana. Evropljani već dugo koriste tzv. žirnalna plaćanja, kod kojih banke i pošte transferišu sredstva u ime klijenta koji plaća račune. Drugo, Evropljani, a posebno Skandinavci, daleko više koriste mobilne telefone i Internet, nego Amerikanci. Finska je na prvom mestu u svetu po broju stanovnika koji koriste mobilni telefon, a zajedno sa Švedskom prednjači u broju stanovnika, korisnika Interneta. Skandinavci svoju high-tech kulturu objašnjavaju kao proizvod svojih dobrih sistema obrazovanja, te visokim stepenom obučenosti za rad na računaru, prisustvom kompanija vrhunske tehnologije, kao što je Finska „Nokija“ i Švedski „Ericsson“, kao i politikom vlade koja promovise korišćenje kućnih računara – u Švedskoj postoje poreske olakšice za kompanije koje svojim zaposlenima obezbede kućne računare. Finci i Šveđani su daleko najveći korisnici *on-line* bankarskih usluga u svetu.⁸

U domicilnim uslovima bankarskog poslovanja, razvoj elektronske banke počinje tek sa reformama bankarskog sektora i prelaskom platnog prometa u bankarski sistem. Do tog trenutka banke su jedini vid elektronskog poslovanja ostvarivale u domenu deviznog sektora tj. poslovnih odnosa sa inostranstvom i to putem SWIFT-a. Domaće banke u domenu elektronskog bankarstva, vide svoju šansu razvoja, te dolazi do ulaganja značajnog iznosa finansijskih sredstava i kupovine savremene informaciono - komunikacione tehnologije, koja omogućava početak poslovanja banaka u elektronskoj sferi. Danas se može konstatovati da većina banaka ima razvijen sistem elektronskog poslovanja koji podrazumeva saradnju banke i sa pravnim i sa fizičkim licima kao klijentima, ali i saradnju banaka sa nacionalnim regulatornim institucijama u Srbiji - NBS.

2. AUTOMATIZACIJA BANKARSKOG POSLOVANJA

Primarni cilj uvođenja sistema elektronskih plaćanja bio je rešavanje problema sistema plaćanja zasnovanih na papiru, korišćenjem potencijalnih prednosti primene informacione tehnologije.

Praksa je kasnije pokazala da ovi procesi znače mnogo više od zamene papirnih dokumenata i njihovog fizičkog prenosa elektronskim putem, odnosno da efikasno i ekonomično korišćenje ove tehnologije zahteva reinjening poslovnih procesa i mećuodnosaućesnika.

Uvoćenje savremenih informacionih tehnologija u bankarstvo je fenomen novijeg datuma, koji se odvija ubrzanim tempom poslednjih tridesetak godina. Bankarska industrija je u biti konzervativna i sklona tradicionalnim i proverenim metodama. Vremenom je, mećutim, broj transakcija u bankarstvu narastao do neslućenih razmera, tako da primena tradicionalnih metoda obrade transakcija više nije bila moguća. U Sjedinjenim Drćavama i Velikoj Britaniji ovaj problem je bio naroćito izraćen, a ogledao se u ogromnoj kolićini čekova i druge

⁸ Frederic S. Mishkin: „*Monetarna ekonomija, bankarstvo i finansijska trćiřta*“, prevod, Data status, Beograd, 2006., str.50

dokumentacije. Problem je pretio da ugrozi stabilnost čitavog finansijskog sistema. Zbog toga su sredinom šezdesetih godina XX veka, preduzete mere za automatizaciju transakcija, pogotovo onih koje se obavljaju često i u pravilnim vremenskim intervalima, a kao rezultat toga nastale su automatske klirinške banke i veliki nacionalni elektronski platni sistem poput Fedvajera (engl. *Fedwire*) i CHIPS-a (engl. *Clearing House Inter-Bank Payments System*). Ovi međubankarski obračuni i platni sistemi razvijeni su za velika plaćanja unutar nacionalnih granica, dok su se ostale transakcije izvan nacionalnih granica zasnivale na starijoj platnoj arhitekturi. Potreba automatizovanja transakcija izvan nacionalnih granica dovela je do stvaranja međunarodnog međubankarskog platnog sistema na veliko. Naime, početkom 1970-tih godina je osnovan SWIFT, a nešto kasnije IBOS (*International Banking - One Solution*) i FNA (*Financial Network Association*). Time je za izvesno vreme rešen problem automatizovanja transakcija u bankarstvu na veliko.⁹

Prema podacima UNCTAD-a (*United Nations Conference on Trade and Development*), troškovi papira i ostalih složenih formalnosti u vezi s tokovima trgovine izvan granica zemalja dostižu i do 10 procenata od konačne vrednosti proizvoda. Jedna tipična trgovinska transakcija može obuhvatiti nekoliko različitih strana i različitih dokumenata, a svi oni moraju da se provere, prenesu, ponovo unesu u različite informacione sisteme, obrade i uskladište. Prema procenama UNCTAD-a, nepotrebni transakcioni troškovi iznose preko 400 milijardi dolara godišnje, a oni se mogu smanjiti za 25 i više procenata putem skraćivanja procedura i razvoja trgovine „bez papira“. U centru ovakvih promena nalaziće se automatizacija obračuna plaćanja na malo.¹⁰

Automatizacija transakcija u bankarstvu na malo dugo je odlagana zbog toga što je vrednost prosečne transakcije relativno mala. Pre samo desetak godina, cene neophodne opreme i infrastrukture za formiranje platnih sistema na malo, bile su toliko visoke da bi troškovi za obradu jedne transakcije u novoformiranim sistemima bili veći od vrednosti same transakcije. Razvoj informacione i komunikacione tehnike i tehnologije, međutim, već danas omogućava automatizaciju transakcija u bankarstvu na malo uz prihvatljive troškove po jednoj transakciji. Za tehnologizaciju bankarstva na malo, dakle, od ključnog su značaja trendovi u informacionoj i komunikacionoj tehnologiji; upotreba javnih računarskih mreža (pre svega Interneta); kao i razvoj i primena metoda šifrovanja. Trendovi u informacionoj i komunikacionoj tehnologiji, kao što je smanjenje troškova računarske obrade podataka, razvoj digitalne bežične komunikacije, standardizacija i sl., utiču na smanjenje cena računarske i komunikacione opreme, čime se smanjuju troškovi po jednoj transakciji u bankarstvu na malo.

Nova revolucija u oblasti tehnoloških promena u bankarstvu na malo, međutim, bazirana je na ideji da se za automatizaciju transakcija u bankarstvu na malo ne formira nova infrastruktura, već da se iskoristi postojeća infrastruktura javnih računarskih mreža, pre svega Interneta. Internet spada u javne tj. otvorene mreže, kojima svako ima neograničeni pristup. Upotreba Interneta za automatizaciju transakcija plaćanja na malo, povoljna je zbog niskih troškova po jednoj transakciji. Veliki problem, međutim, predstavlja bezbednost transakcija koje se obavljaju preko Interneta. Zbog toga korišćenje kriptografije predstavlja veoma važnu sigurnosnu meru prilikom dizajniranja platnih sistema i protokola.

⁹ Hadžić M.: „Bankarstvo“, Univerzitet Singidunum, FFMO, Beograd, 2007., str. 51

¹⁰ http://home.bankerinter.net/pond/body_elektronsko_bankarstvo-razvo.html

Pojava elektronskog novca nametnula je potpuno novu filozofiju u bankarstvu koja se zasniva na elektronskoj razmeni podataka i sredstava (engl. *EFT- Electronic Funds Transfer*), koja je pojmovno određena kao elektronsko bankarstvo.¹¹

Elektronski transfer novca – EFT je postupak kojim se pomoću elektronskog prenosa poruke (putem elektronskog terminala, telefona, računara ili magnetne trake) prenosi novac između dva mesta, bez fizičkog prenosa gotovine.

Automatizacija transakcija u bankarstvu (na malo) dugo je odlagana usled:

1. Visokih cena neophodne opreme i infrastrukture;
2. Neusklađenih zakonskih propisa;
3. Neadekvatnog i neravnomernog razvoja tehnologije;
4. Visokih troškova marketinga.

Na afirmaciju elektronskog bankarstva od presudnog značaja su bili:

1. Trendovi u informacionoj i komunikacionoj tehnologiji;
2. Upotreba javnih računarskih mreža;
3. Razvoj i primena metoda kriptografije.

Banke implementiraju elektronsko poslovanje da bi podigle svoj ugled usled prihvatanja inovacija, ali isto tako kao i odgovor na uvođenje inovativnih usluga od strane konkurenata. Elektronsko bankarstvo omogućuje uštede u poslovanju i razvoj masovnih usluga prilagođenih specifičnim potrebama korisnika. Sa druge strane, omogućuje zadržavanje postojećih i pridobijanje novih klijenata banke.

Osnovni razlog za uvođenje računara u bankarske poslove je to što su banke centralizovane institucije i što im je veoma važno da u svakom trenutku mogu imati informaciju sa koliko novca raspolažu, koji deo novca je spreman za reinvestiranje i koji prilivi se očekuju. Širenje velikih bankarskih sistema na velike geografske udaljenosti nametnulo je potrebu da se izgrade informacioni sistemi i široko rasprostranjene računarske mreže.

Sa porastom potreba korisnika bankarskih usluga, raste i očekivani kvalitet usluge. Dobra strana automatizacije bankarskog poslovanja je što je omogućeno korišćenje usluga 24 časa neprekidno. Pored toga, postoji mogućnost da se proširi tržište, čak i izvan domicilne zemlje, s obzirom na to da više ne postoji potreba otvaranja kancelarija, odnosno organizacionih delova u svakom mestu. Takođe omogućava obavljanje većeg broja finansijskih transakcija, kao i sniženje, ne samo transakcionih troškova, nego i varijabilnih troškova, kojima je banka izložena (troškovi kancelarijskog materijala, habanja štampača i sl.) što u krajnjem ishodu ima za posledicu povećanje konkurentnosti na tržištu. Savremeni način poslovanja banaka omogućava klijentima da obave sve rutinske transakcije, kao što su transfer sredstava, upit u stanje računa, plaćanje računa i sl. na jednostavniji i brži način. Otvaranje računa se vrši *on-line* i na taj način se u potpunosti izbegava papirologija, a jednom unete informacije se ne moraju ponovo unositi za slične provere. Omogućeno je napraviti raspored budućih plaćanja koje će se obaviti automatski, kao i apliciranje za zajam ili platnu karticu. Ažuriranje informacija se sprovodi u realnom vremenu, a ono što je od velike važnosti za klijente banke je da su provizije niže nego pri obavljanju transakcija klasičnim putem.

¹¹ Stankić R.: „Elektronsko poslovanje“, Ekonomski fakultet, Beograd, 2007., str. 94

U domicilnim uslovima, uvođenje elektronskog poslovanja pruža mogućnost bankama za uspostavljanje leaderske pozicije. Trenutno, u Srbiji elektronsko bankarstvo koristi mali broj klijenata i za sada se ne može predvideti kojim će tempom ta primena rasti, što nameće potrebu ulaganja značajnih sredstava banke u razvoj i marketing. Nije zanemarljiv podatak da cena usluga elektronskog bankarstva iznosi samo oko 30% troškova tradicionalnih bankarskih usluga koje su prisutne u tradicionalnom poslovanju. Kao eksterni faktor uvođenja elektronskog bankarstva su svakako i sve izraženiji zahtevi klijenata za jeftinijim uslugama, jednostavnijim dolaskom do usluga i sve veće znanje klijenata o informacionoj tehnologiji i mogućnostima koje ona pruža u pojednostavljenju obavljanja redovnih aktivnosti i uštede vremena.

Potreba racionalizacije u tradicionalnom bankarskom poslovanju se odnosi na racionalizaciju broja zaposlenih, lokacija u filijalnoj mreži banke, troškova poslovanja i uštede po transakcijama. Za razliku od klasičnog bankarstva, u savremenom elektronskom bankarstvu se smanjuje potreba broja zaposlenih i menja se potrebna kadrovska struktura. Neophodno je ulaganje u visoko obrazovane kadrove, čije se znanje neće zasnivati samo na poznavanju klasičnog bankarskog poslovanja, već i savremenih trendova u informacionoj tehnologiji i telekomunikacijama. Smanjenje potrebe broja zaposlenih ima efekat i na broj potrebnih filijalskih mesta, odnosno lokacija šaltera i ekspozitura u okviru tradicionalnog bankarskog poslovanja. To direktno dovodi do smanjenja troškova iznajmljivanja objekata, troškova investicionog održavanja i režijskih troškova. U konačnom ishodu rezultat je smanjenje cene usluga klijentima banke, odnosno ušteda po transakcijama (smanjenje troškova transakcija u odnosu na klasične kanale distribucije). Naravno, niže cene elektronskih transakcija će se pretvoriti u uštedu jedino ako se veliki broj transakcija preseli iz klasičnih kanala u elektronske, odnosno *on-line* kanale.¹²

U poslednje vreme se javljaju korisnički zahtevi za boljom kontrolom i upravljanjem finansijama. Internet je omogućio masovni protok informacija i naterao banke da se više pozabave kvalitetom i dostupnošću informacija. Vrlo malo bankara će se usuditi da porekne uticaj Internet tehnologije na svoje poslovanje.

Trend modernog bankarstva je automatizacija svih funkcija (finansijskih operacija) primenom informacionih tehnologija. Tipični primeri automatizacije bankarskog poslovanja su uplate i isplate sa štednih uloga, upisivanje kamate, otplate kredita, konverzija valuta, transfer sredstava sa računa na račun, plaćanje kreditnom karticom, uvid u stanje računa, ili raznovrstan prikaz izvršenih transakcija za dati račun (prema hronologiji transakcija, tipu transakcije, odredišnom računu, svrsi uplate ili isplate itd.).

Uticaj informacione tehnologije na razvoj i poslovanje banaka je izuzetno veliki, dolazi do pomeranja granica „klasičnog“ bankarstva, poslovne banke sve su više okrenute elektronskom načinu poslovanja, s obzirom na to da im ovaj vid komunikacije sa klijentima omogućava značajniju racionalizaciju poslovanja, ali i brže i urednije servisiranje svih potreba klijenata.

Banke koje ne uspeju da održe korak sa razvojem informacione tehnologije, mogle bi da izgube deo svojih klijenata, smanje svoje poslovanje i ostanu bez većeg profita. Banke moraju ne samo da prate razvoj i ulažu u novu tehnologiju, već i da koordiniraju i kombinuju pružanje svojih usluga koristeći veći broj različitih kanala distribucije. Adekvatna primena savremene informacione tehnologije i informacionih sistema u bankarstvu, a naročito

¹² <http://www.eccf.su.ac.yu/obavestenja/inf-u-finansijama.htm>

korišćenje Interneta, obezbeđuje bankama konkurentnu tržišnu poziciju i dugoročnu poslovnu egzistenciju.

U domicilnim uslovima, odredbe centralne banke idu na ruku primeni informacionih tehnologija u bankarskom poslovanju, što se najbolje može pokazati na primeru prestanka upotrebe čeka kao sredstva „odloženog“ plaćanja i početka brze i masovne primene tzv. „plastičnog novca“, odnosno kreditnih kartica, kao supstituta ovog načina plaćanja u Srbiji. Danas u Srbiji, pored svih navedenih proizvoda koje poslovne banke imaju u paleti svoje ponude, prisutni su po prvi put i web krediti kod kojih „*retail*“ klijenti više nisu u obavezi da se pojave na šalterima poslovnih banaka, kako bi realizovali svoj kreditni zahtev.

Obavljanje kompletnog bankarskog poslovanja direktno iz kuće, bez fizičkog prisustva u banci, danas je uobičajena pojava u razvijenim zemljama sveta. Banke koriste različite načine da klijentima omoguće što efikasnije i bezbednije obavljanje bankarskih transakcija od kuće. Brojni su nazivi koje banke koriste za obavljanje ovih bankarskih aktivnosti. Najčešće korišćeni nazivi su: bankarstvo od kuće (engl. *Home Banking*), direktno bankarstvo (engl. *Direct Banking*), onlajn bankarstvo (engl. *On - line Banking*), Internet bankarstvo (engl. *Internet Banking*) i sajber bankarstvo (engl. *Cyber Banking*).

Uvođenje e-bankarstva donelo je revolucionarnu promenu u bankarskom poslovanju. Treba naglasiti da je to još uvek nova tehnologija i da se rezultati još uvek teško mogu sagledati. Posebno se to odnosi na nove tehnologije koje se ubrzano razvijaju, tako da će se rezultati videti tek za nekoliko godina. Može se reći da je dosadašnji razvoj tehnologije i spektar novih servisa doveo do:¹³

- Privlačenja novih korisnika,
- Povećanja broja transakcija,
- Smanjenja cena obavljanja transakcije,
- Povećanja zadovoljstva i lojalnosti korisnika,
- Povećanja profita koji se ostvaruje pružanjem novih servisa u odnosu na klasične bankarske poslove i usluge.

Banka ima zadatak da obuči ljude u IT i ostalim operacijama da bi bila sposobna da postigne 4A cilja (engl. *Any place, Any time, Any service, Any device*).

3. NOVE TEHNOLOGIJE U BANKARSKOM POSLOVANJU

U kontekstu tehnološke revolucije dolazi do stvaranja elektronskog bankarstva. Elektronsko bankarstvo podrazumeva obavljanje poslovnih procesa uz primenu savremenih informacionih tehnologija zasnovanih na Internetu i njegovim servisima. Ova vrsta tehnologije omogućava slanje velikog broja informacija, na velike daljine u kratkom vremenskom periodu. To omogućava bankama koje u svom poslovanju koriste savremenu informacionu tehnologiju zasnovanu na Internetu da ostvare značajne uštede u troškovima poslovanja, efikasnije obave svoje zadatke i budu konkurentnije na tržištu. Elektronsko bankarstvo predstavlja pokušaj spajanja više različitih tehnologija, od kojih se svaka razvijala u drugom smeru i na drugačiji način:

¹³ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.79

1. Elektronski novac;
2. Platne kartice;
3. Automatski samouslužni štalteri;
4. Maloprodajni terminali;
5. Kućno bankarstvo;
6. Mobilno bankarstvo.

3.1. Elektronski novac

Najveće tehnološko dostignuće u razvoju bankarstva je pojava elektronskog novca, a samim tim i elektronskog bankarstva. Tehnologija elektronskog plaćanja ne samo da je zamena za čekove, već je zamena i za gotovinu u formi elektronskog novca (e-novca), novca koji postoji samo u elektronskoj formi.

Novac je, u savremenoj interpretaciji, informacija o monetarnoj vrednosti koju je moguće transferisati kroz računarske mreže, to jest van uobičajenih kanala plaćanja koje tradicionalno podržavaju banke. Digitalni novac je kulminacija procesa dematerijalizacije novca i njegovo pretvaranje u informaciju koja jedino postoji *on-line*. Kroz njega se markira pravo nekog subjekta u odnosu na robu i usluge koje egzistiraju u jednom društvu. Umesto papirnog novca koristi se digitalna informacija koja je mnogo „inteligentnija“.

Sa pojavom Interneta i njegovom masovnom primenom u domenima plaćanja i bankarskih funkcija, elektronski novac je postao deo svakodnevnice i tek onda su se postavila pitanja koja su od životne važnosti, a vezana su za njega. Iako postoji više modela elektronskog novca koji teorijski zadovoljavaju ili su u praksi primenjivi, još uvek postoji čitav niz problema koje on mora da razreši da bi za korisnike bio prihvatljiviji i kako bi zamenio postojeći „klasični novac“.¹⁴

Osnovni preduslov da elektronski novac bude prihvatljiv za masovnu upotrebu je da postoji sigurnost i poverenje u njega. To znači da postoje efikasne metode za sprečavanje i otkrivanje falsifikovanja, dupliranja ili bilo kakve neadekvatne upotrebe. Već danas postoje razvijene metode koje se mogu smatrati dovoljno pouzdanim. Kriptografske metode zaštite (*SSL - Secure Socket Layer* i *SET - Secure Electronic Transaction*) kombinovane sa PIN (*Personal Identification Number*) brojevima i čip karticama pružaju visok stepen pouzdanosti. Trenutno su u razvoju novi sistemi za rad sa čip karticama tako da se može smatrati da će stepen sigurnosti biti ubuduće na zadovoljavajućem nivou.

Da bi zamenio „klasični novac“, elektronski novac mora biti univerzalno prihvatljiv, što znači da može da se daje iz „ruke u ruku“, ali i da funkcioniše u računarskim mrežama. Transakcije obavljene elektronskim novcem moraju biti jeftinije od klasičnih transakcija, izdavanje (emitovanje) novca, njegovo servisiranje i korišćenje moraju biti jeftinije od rada klasičnim novcem. Uopšteno govoreći, digitalni novac mora pružiti znatne prednosti kako bi od korisnika bio široko prihvaćen. Za sada digitalni novac samo u određenim segmentima uspešno zamenjuje klasičan novac, ali tamo gde je prihvaćen obezbeđuje veliku brzinu protoka novca. Prihvatljivost iz „ruke u ruku“ nije postignuta u zadovoljavajućem nivou.

Razlog za manju prihvatljivost elektronskog novca je u tome što u mnogim slučajevima, da bi se ponudio i prihvatio elektronski novac, mora da se izvrši provera stanja na računu ili

¹⁴ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.45

kreditna sposobnost onoga ko nudi elektronski novac. Kod klasičnog novca onaj ko nudi novac ne mora da dokazuje ništa i nikome, jer novac koji nudi je za sebe dokaz. Svako može da ponudi (klasičan novac), ili da ga prihvati bez ikakve provere (osim falsifikat), a transfer novca iz ruke u ruku je jednostavan. Ovo je nesumnjiva prednost klasičnog novca koja još dugo neće biti prevaziđena

Jedan od osnovnih problema koji se javlja kod elektronskog novca je što on ostavlja trag o tome gde je trošen i koliko. Svaka obavljena transakcija se registruje kao slog sa svim detaljnim podacima o njoj. Ovo praćenje je neophodno da bi se u slučaju spora mogla da rekonstruiše transakcija od početka do kraja. Ujedno ovo predstavlja mogućnost da neko sa lošim namerama iskoristi ove podatke. Praćenje klijenta gde je i šta trošio u različitim prilikama i uspostavljanje veza između transakcija predstavlja problem zaštite privatnosti.

Činjenica je da digitalni ili elektronski novac sve više dobija na značaju. Internet kao ogromni poslovni potencijal zahteva digitalni novac i uopšte nije sporno da će se njegova upotreba sve više širiti. Da bi zadovoljio korisnike mora da ispuni neke uslove. Mora biti lako prenosiv, da troškovi njegovog kreiranja i rukovanja budu mali ili bar manji od klasičnog novca, mora da omogućava promet bez posrednika, to jest da se sa njim mogu obavljati „off line“ transakcije. Posebno mora da obezbedi anonimnost učesnika u transakciji.¹⁵

Stvaranje elektronskog novca je sastavni deo šireg procesa finansijskih inovacija, s tim da se radi o specifičnim inovacijama koje se odnose na tehnologiju platnog prometa. Ove inovacije imaju potencijal da ugroze dominantnu ulogu gotovog novca u oblasti plaćanja na malo i da učine transakcije na malo mnogo lakšim i jeftinijim za potrošače i trgovce. Stoga i ne treba da čudi konstatacija da je elektronski novac najveće tehnološko dostignuće u razvoju bankarstva, koji zamenjuje gotovinu i čekove i omogućava kupovinu roba i usluga preko računara u okviru komercijalnih računskih mreža (npr. Interneta), ili poslovnih bankarskih mreža (npr. SWIFT-a).

Elektronski novac koji emituje neka banka predstavlja određenu sumu stvarnog (realnog) novca. Drugim rečima, razlika između softvera i novca nestaje. Realizacija elektronskog novca se zasniva na ideji da se novčanica umesto na papiru upakuje u niz cifara, digitalno potpiše i kao takva dalje koristi za plaćanja.¹⁶

Elektronski novac se definiše kao specifična „monetarna informacija“ koja se putem elektronskih impulsa u „realnom vremenu“ prenosi između transaktora koji obavljaju plaćanja.¹⁷

Ipak, ne postoji jedinstvena definicija elektronskog novca, jer ona zavisi od aspekta posmatranja, namere istraživača kao i od osobine koja se želi naglasiti.

Sistem elektronskog novca nastaje kada neka banka emituje elektronski novac u vidu brojeva koji nose određenu vrednost. Da bi se dobio ovakav elektronski novac mora postojati račun kod banke i osnovno pravilo je da kada se kupuje elektronski novac, pravi novac se povlači sa postojećeg računa. U protivnom bi se povećala novčana masa što bi dovelo do inflacije.

¹⁵ Isto, str.46

¹⁶ Isto, str.47

¹⁷ Stankić R.: „Elektronsko poslovanje“, cit. delo, str. 95

Elektronskim novcem se dalje može platiti trgovcu za proizvod ili usluge, a trgovac ga može deponovati u bilo kojoj banci ili ga može proslediti drugom trgovcu. Trgovac u svakom trenutku može proveriti ispravnost elektronskog novca kontaktirajući banku koja ga je emitovala.

Elektronski novac se može koristiti za *on-line* i *off-line* plaćanja. On-line plaćanje nije generalna karakteristika svih sistema, jer neki sistemi omogućavaju i off-line plaćanja. Ipak, većina sistema zahteva on-line autorizaciju.

Korisnici koji su zainteresovani za plaćanja elektronskim novcem u većini slučajeva moraju da instaliraju poseban softver na svom računaru koji im omogućava da komuniciraju sa bankom, kao i da podižu novac sa svog računa u banci, a zatim ga prebace u svoj „novčanik“ na računaru. Prilikom plaćanja, oni razmenjuju ovako podignuti novac sa trgovcem u zamenu za proizvode ili usluge koje žele da kupe. Banka koja prima depozite u elektronskom novcu, otkupljuje novac koji je trgovac dobio.¹⁸

Druga varijanta je da korisnici imaju „čip karticu“ i da pristupaju banci preko Interneta tako da se vrednost novca prebaci na karticu (kartica se napuni), a zatim se taj novac koristi za plaćanja.

Postoje dva osnovna oblika elektronskog novca:

1. Oblik zasnovan na karticama,
2. Mrežni elektronski novac.

Prvi oblici (*Mondex, Visa Cash i sl.*) su zasnovani na plastičnim karticama koje građani koriste za manja plaćanja. Takva plaćanja se mogu vršiti u prodavnicama koje imaju odgovarajuće terminale i vrše se na način što terminal automatski skida iznos sa kartice i taj iznos odobrava prodavnici. U većini prodavnica dovoljno je da provučete svoju karticu kroz čitač na kasi, pritisnete dugme i iznos koji ste potrošili na kupovinu biće oduzet s vašeg bankovnog računa. S obzirom na njihovu potencijalnu upotrebu i rast, proizvodi bazirani na karticama su dizajnirani tako da olakšaju plaćanja u svakodnevnim transakcijama na malo, pa će predstavljati supstitut bankomatima i gotovom novcu.

Mrežni elektronski novac (engl. *Network Money ili Cybercash*) je karakterističan po tome što se elektronske vrednosti elektronskog novca nalaze na hard diskovima personalnih računara. Transfer se vrši preko telekomunikacionih mreža, uglavnom preko Interneta. Plaćanja mrežnim elektronskim novcem se vrše između računa putem softvera koji poseduju razni korisnici ovog sistema plaćanja. Modeli bazirani na softveru koristili bi se za obavljanje plaćanja sa distance preko računskih mreža, tako da je verovatno da će oni zameniti kako gotovinu, tako i druge bezgotovinske instrumente plaćanja, kao što su čekovi.

Velika prednost elektronskog nad običnim novcem je u tome da je on informacija u računaru koja može da se programira. Ova razlika omogućava da elektronski novac postane pametni novac u obliku tzv. „pametnih kartica“. Dominantni oblik elektronskog novca je elektronski transfer sredstava na tački prodaje (engl. *Electronic funds transfer at point of sale - EFT/POS*) pomoću instaliranih terminala u trgovačkoj i uslužnoj mreži. Drugi oblik korišćenja elektronskog novca moguć je preko bankomata, koji omogućavaju podizanje gotovine,

¹⁸ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.49

polaganje depozita, prenos na druge račune i plaćanje sa različitih računa. Takođe sve je veće korišćenje personalnih računara u stanovima korisnika koji omogućavaju raspolaganje finansijskim sredstvima iz kuće, bez odlaska u banku.

Novim instrumentima omogućava se najpre udaljen ulaz na račune, njihovo korišćenje u svim varijantama i podizanje gotovine, da bi posle unapređenja samih instrumenata došlo do stvaranja potpuno novih instrumenata i aranžmana plaćanja, elektronskog novca koji se javlja u formi neke vrste elektronskog novčanika ili mrežnog elektronskog novca koji se distribuira preko zatvorene ili otvorene mreže.

Aranžmani za funkcionisanje prve kategorije elektronskog novca se pojavljuju u dve varijante: u prvoj, plaćanja predstavljaju praktično samo privremenu novčanu transakciju koja se finalno zatvara prenosom sredstava između transakcionih depozita kod bankarskih institucija, dok u drugoj, elektronski novac cirkuliše između korisnika na gotovo isti način kao i gotov novac, što znači da se plaćanje elektronskim novcem može smatrati finalnim već u ovom trenutku. Plaćanja mrežnim elektronskim novcem se vrši između računa putem softvera koji poseduju razni korisnici ovog sistema plaćanja.

Sam elektronski novac u formi „elektronskog novčanika“ bazira se na prethodno izvršenim uplatama monetarnih vrednosti koje su registrovane na mikročipovima elektronskih kartica, a mogu biti upotrebljene za plaćanje robe i usluga. Postojeći tipovi ovog novca još uvek nisu zakonska sredstva plaćanja u onom smislu u kome je to gotov novac, iza koga stoje centralna banka i država i koji primaju svi, već samo onaj krug učesnika koji je uključen u određeni aranžman plaćanja usled čega mogu nastati značajni pravni i monetarni problemi.

Treća forma elektronskog novca često se naziva i e-gotovina, a koristi se na Internetu radi kupovine dobara i usluga. Kupac dolazi do e-gotovine tako što otvara račun u banci koja je povezana sa Internetom, a potom se e-gotovina prebacuje na njegov račun. Kada počeli da kupi nešto pomoću e-gotovine, kupac posećuje prodavnicu na Internetu i za određeni artikal bira opciju „kupiti“, a e-gotovina se automatski doznaje s njegovog računa na račun prodavca. Prodavac potom može ta sredstva, koja su doznajena s bankovnog računa kupca na njegov račun, podići pre nego što kupcu isporuči robu.

3.1.1. Osobine elektronskog novca

Pošto novac u suštini predstavlja informaciju o nekoj vrednosti lako ga je pretvoriti u neki drugi oblik (elektronski) pogodan za prenos kroz računarsku mrežu. Rešenje je načeno tako što je novčanica postala „file“ datoteka koja je šifrovana, digitalno potpisana i dodati joj sertifikati. Drugim rečima, svi elementi iz realnog okruženja dobili su svoj pandan u elektronskoj formi. Datoteka je zamenila papir, ručni potpis je zamenjen digitalnim, a identifikacioni dokumenti (lična karta) su zamenjeni digitalnim sertifikatima. To je dovelo do sledećeg:¹⁹

- Razlika između softvera i novca nestaje i sve postaje informacija.
- Umesto da se novčanica smesti na papir ona se upakuje u niz cifara u digitalnom obliku i kriptografski zaštiti kako bi se sprečilo falsifikovanje.
- Ovakav novac je lako pokretan i prenosiv kroz mrežu.
- Posедуje visok nivo inteligencije.

¹⁹ Isto, str.49

- Elektronski novac ne poznaje granice.
- Može se programirati, pratiti i ograničavati, ovde nastaje problem (ko, kako i kada sme da izda ograničenja).
- Može se pratiti (veliki problem elektronskog novca je „problem privatnosti“).
- Ako se izgubi moć e da se zameni (kontrola duplikata).

3.1.2. Osnovni protokol plaćanja

U realnom okruženju korisnik odlazi u banku i sa svog računa podiže određenu sumu novca. Blagajnik ga identifikuje preko lične karte i bankarske kartice i isplaćuje mu traženi iznos novca. Korisnik tada odlazi u trgovinu i plaća tako dobijenim novcem. Trgovac je dužan da na kraju radnog dana preda pazar (novac) banci i tako je zatvoren krug u realnom okruženju. Ovakav protokol plaćanja je u potpunosti istovetan plaćanju digitalnim novcem. Protokol plaćanja digitalnim novcem ima tri faze:²⁰

- Povlačenje novca (engl. *withdrawal*) – podizanje novca iz banke, u kojem korisnik prenosi, u elektronskom obliku, deo novca sa svog računa u banci na karticu ili račun (novčanik).
- Plaćanje (engl. *payment*) – plaćanje, korisnik prenosi deo novca onom kome plaća.
- Depozit (engl. *deposit*) – deponovanje novca u banku, onaj ko je dobio novac deponuje taj novac na svoj račun u banci.

S obzirom na to da su modeli elektronskog novca još uvek relativna novost, postoji dosta različitih pristupa, kako tehničkih tako tehnoloških i organizacionih.

Modeli elektronskog novca se razlikuju po: tehnologiji, učesnicima, emitentima, trgovcima.

Postoje tri osnovne tehnologije upisa novčane vrednosti:

- Novac se nalazi na „Smart kartici“.
- Novac se nalazi u softverskom novčaniku na računaru.
- Treća varijanta je kombinacija prethodna dva sistema.

Učesnici u sistemu plaćanja i organizacija poslovanja mogu biti različita, ali su učesnici sledeći:

- Emitenti elektronskog novca,
- Operateri, procesori,
- Korisnici,
- Trgovci,
- Kuće za kliring transakcija elektronskim novcem.

Najznačajniji su emitenti elektronskog novca. Mrežni operateri i dobavljači obezbeđuju tehničku podršku, dok su institucije za kliring obično banke ili specijalizovane institucije u vlasništvu banaka. Može biti jedan ili više emitenata u zavisnosti kako je sistem organizovan.

²⁰ Isto, str.50

Kada govorimo o karakteristikama modela elektronskog novca treba napomenuti i činioce koji utiču na širenje ovih sistema.

Emitenti, njihov rezon za formiranje sistema elektronskog novca zasniva se na profitu koji iz ovog posla treba da proizađe. Prihodi se ostvaruju po osnovu provizija za obavljene transakcije, zatim prihoda koji se ostvaruje na bazi povećanog broja dana odležavanja novca na računu emitenta i na kraju kao prihod od pojeftinjenja (smanjenja) troškova po transakciji. Trgovci moraju naći računicu i prihod od primanja elektronskog novca. Prvi osnovni uslov da trgovci prihvate ovakav vid plaćanja zavisi od provizije koju emitent uzima po transakciji. Drugi uslov za prihvatanje elektronskog novca su troškovi. Oni moraju biti manji od postojećeg realnog sistema i da ne zahtevaju značajnije dodatne investicije, dodatno angažovanje novčanih sredstava i kadrova. Trgovac svoj motiv za prihvatanje ovog sistema plaćanja mora da pronađe u povećanju prometa i povećanju obrta, a time i povećanju zarade. *On line* trgovci nemaju izbora između realnog i digitalnog novca i prinuđeni su da prihvate postojeće sisteme plaćanja. Pošto je izbor sistema plaćanja izuzetno veliki, njima ostaje da izaberu optimalna rešenja za plaćanja. Trgovci bi, s jedne strane, rado bili uključeni u sve sisteme plaćanja, jer time uvećavaju šanse da prodaju robu. S druge strane, sa povećanjem broja sistema plaćanja u koji su se uključili značajno komplikuju svoju administraciju i imaju dodatne troškove servisiranja većeg broja računa, tako da su prinuđeni da u svom domenu poslovanja optimiziraju svoje učešće u sistemima plaćanja. Ovo dalje uslovljava nestabilnost poslovanja operatera, jer ih trgovci lako menjaju eksperimentišući sa kojim će imati najveći promet.

Korisnici da bi prihvatili sistem elektronskog novca moraju imati značajan nivo ponuđenih usluga i koristi od njih. Osim toga, moraju imati poverenje i sigurnost kako bi ga nesmetano koristili. Korisnici, pre svega, moraju imati gde da plaćaju, što znači da sistemi elektronskog novca moraju ravnomerno da šire broj korisnika i mrežu trgovaca koji primaju taj novac.

3.2. Elektronske platne kartice

3.2.1. Opšte karakteristike

Razvoj e-bankarstva tesno je povezan sa razvojem platnih kartica kao sredstva koje omogućava aktiviranje terminala za masovno korišćenje bankarskih usluga na različitim punktovima. Sve platne kartice su istog oblika i veličine, a njihova celokupna fizička struktura je specificirana od strane Međunarodne organizacije za standardizaciju, ISO standardima 7810.

Istorijski razvoj platnih (kreditnih) kartica počinje u Sjedinjenim Američkim Državama tokom 1920-tih godina, kada su neke firme počele da izdaju platne kartice svojim potrošačima i koje su mogle da se koriste samo u prodajnim objektima kompanije koja ih je izdala. Prvu univerzalnu karticu koja je mogla da se koristi u raznovrsnim prodajnim, odnosno uslužnim objektima, izdaje 1950. godine Diner's Club. Ipak, prvi bankarski sistem od nacionalnog značaja bio je Bank Americard, koji je pokrenula Bank of America iz Kalifornije 1959. godine da bi isti bio licenciran u drugim državama 1966. godine. Ovaj bankarski sistem od 1976-77. godine nosi naziv VISA. Kreditne kartice su se u današnjem obliku pojavile u SAD-u krajem šezdesetih godina, da bi se tek kasnije proširile po svetu. Debitne kartice su novijeg datuma, a najbrže se razvijaju u Velikoj Britaniji.



Postoje raznovrsne definicije platnih kartica. Po jednoj, platne kartice su mali komadi plastike koji sadrže PIN za identifikaciju, što omogućava licu na koje kartica glasi da kupuje robu ili usluge na teret svog računa. Drugi, platnu karticu definišu kao specifičan instrument bezgotovinskog načina plaćanja emitovan od strane banke, trgovinske ili specijalizovane organizacije koja omogućava njenom vlasniku da jednostavnom prezentacijom kartice izmiri svoje obaveze plaćanja prema prodavcu robe ili vršiocu usluge.

Prednosti upotrebe platnih kartica su nesumnjive i to kako za klijente, tako i za banke. Klijentima banke se pruža komoditet u obavljanju poslova sa bankom kod podizanja gotovine na bankomatima, bez potrebe čekanja na šalterima i u bilo koje vreme nezavisno od radnog vremena banke. Prednosti upotrebe platnih kartica klijenti mogu osetiti i pri plaćanju određenih roba ili usluga. Korisnici platnih kartica nemaju potrebu da nose gotovinu sa sobom, s obzirom na to da su sve radnje obavezne da primaju platne kartice. To znači da korisnici platnih kartica mogu izvršiti plaćanje jednostavnim prezentovanjem iste. Sa druge strane, odobrena kreditna kartica omogućava korisnicima jednostavnu, pogotovo „impulsnu“ kupovinu proizvoda ili usluga. I na kraju, imaocima kartica pruža sigurnost u odnosu na gotov novac, jer u slučaju gubitka iste potrebno je samo pozvati autorizovani centar koji će blokirati mogućnost upotrebe iste.

Prednosti koje pružaju platne kartice su višestruke:

1. Oslobađaju rizika koji sa sobom proizvodi nošenje gotovine;
2. Vlasnik kartice znatno pojednostavljuje obavljanje platnih transakcija;
3. Smanjuje transakcione troškove;
4. Stvoren je jedinstven sistem plaćanja koji ne poznaje nacionalne i valutne granice;
5. Osiguran je od eventualnih zloupotreba, jer u slučaju nestanka obaveštava izdavaoca iste, koji nakon toga blokira dalju mogućnost njene upotrebe.

Prilikom korišćenja platne kartice, postoje određena pravila koja propisuje banka i koja korisnik treba da poštuje:

1. Platne kartice se mogu koristiti na mestima na kojima je istaknut znak kartičnog sistema, koju korisnik poseduje (npr. Visa ili Mastercard), pri čemu korisnik može da koristi karticu u okviru odobrenog mesečnog limita koji banka određuje.
2. Korisnik platne kartice ne sme da ostavlja karticu kao zalog ili sredstvo obezbeđenja.
3. Korisnik mora da ispoštuje zahtev za oduzimanje kartice ukoliko prodajno mesto ili banka to zatraže po nalogu Banke izdavaoca kartice.
4. Kartica čiji je rok važenosti istekao ne može biti korišćena.

Platne kartice se mogu koristiti za:²¹

1. Plaćanje roba i usluga – korisnik može da koristi karticu za bezgotovinska plaćanja robe i usluga u zemlji i inostranstvu, pri čemu potpisuje račun/slip na isti način kao što je potpisao karticu, ili koristi svoj PIN koji se tretira kao potpis.
2. Podizanje gotovine – korisnik može da podigne gotovinu na bankomatima i šalterima ovlašćenih banaka u zemlji ili inostranstvu. Korisnik se identifikuje unosom svog PIN-

²¹ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.200

a, pri čemu mora da vodi računa o njegovom ispravnom unosu, jer nakon trećeg neuspešnog unosa bankomat zadržava karticu. Obično se plaća provizija prilikom podizanja gotovine na bankomatima ili šalterima ovlašćenih banaka u zemlji i inostranstvu.

3. Plaćanje elektronskim putem – omogućava korisniku da obavlja plaćanje elektronskim putem (Internet, kataloga ili telefonska prodaja) i korisnik snosi rizik od zloupotrebe koji postoji pri prenošenju broja kartice i ličnih podataka kroz javnu mrežu.

U praksi, platne kartice predstavljaju kombinaciju instrumenata identifikacije i instrumenata platnog prometa. Njihova upotreba i doprinos razvoju elektronskog bankarstva zavise od tehničkih mogućnosti koje pojedine vrste pružaju. Međusobno mogu bitno da se razlikuju po stepenu bezbednosti, funkcionalnosti, redukciji papira i odnosu prema on-line infrastrukturi, sve u zavisnosti od funkcionalne aplikacije i tehnološke osnove na koju se ona implementira.

Elektronske platne kartice kao instrumente plaćanja možemo podeliti prema:²²

- a) tehnologiji koja je primenjena: kartice sa magnetnom trakom i inteligentne kartice (engl. *smart cards*) sa silicijumskim mikroprocesorskim čipom,
- b) prema vremenu plaćanja i anonimnosti transakcija: debitne kartice, kreditne kartice i kartice sa unapred uplaćenim iznosima novca,
- c) lokaciji primene: nacionalne (važe u zemlji gde su izdate) i internacionalne (važe ravnopravno, kako u zemlji tako i u inostranstvu),
- d) korisniku kartice: osnovnu, dodatnu, poslovnu i sl.

Platne kartice obezbeđuju identifikaciju izdavaoca i korisnika kartice na aparatima namenjenim finansijskim transakcijama i obezbeđuju input podataka potrebnih za takve transakcije. U tom kontekstu mogu da obavljaju više različitih funkcija među kojima su posebno značajne:²³

1. funkcija garantnog sredstva plaćanja (funkcija čekovnih i novčanih karti);
2. funkcija sredstva identifikacije i ulaska u sistem za podizanje gotovine na samouslužnim šalterima i bankomatima (*ATM* garantne karte);
3. teleplaćanja;
4. obavljanje kupovine na elektronskim terminalima u maloprodaji (*EFT/POS*);
5. preuzimanje funkcije elektronskog potpisa;
6. funkcija prenosa datoteke i sl.

U obavljanju pojedinih transakcija koristi se veći ili manji broj pomenutih funkcija, u zavisnosti od prirode transakcija i mogućnosti koje konkretna tehnologija kartice pruža. Sa aspekta tehničkih mogućnosti u tom smislu posebno je bitna razlika između standardne karte sa magnetnom trakom i karte sa čipom. Zbog ograničenosti obima memorije, kartica sa magnetnom trakom praktično može da obuhvati samo podatke potrebne za obezbeđivanje ulaza u sistem, dok izveštaje o transakcijama čuva memorija bankarskog računarskog sistema. Sa takvim karakteristikama može da bude sredstvo za obezbeđivanje ulaza u sistem. Kartica sa čipom, pored prethodnog može da vrši i naknadno memorisanje informacija i tako preuzima funkciju čuvanja elektronskog izveštaja koji obezbeđuje kontrolu transakcija na individualnom nivou.

²² <http://www.eccf.su.ac.yu/obavestenja/inf-u-finansijama.htm>

²³ Vuksanović E: „Elektronsko bankarstvo“, cit.delo, str. 45



U domicilnim uslovima poslovanja, kartice su po ukidanju čekova kao instrumenta kreditiranja (što nikada ček i nije pravno mogao da bude), dođivele pravi procvat u upotrebi. Danas, u našim poslovnim bankama mogu se dobiti sve vrste savremenih poslovnih kartica (od Dine, Vise, Mastercard-a do Diners-a) koje mogu biti elektronske (samo uz magnetnu traku), classic (embosirane), do najsavremenijih koje se baziraju na čip tehnologiji. Banke u svojim poslovnim budžetima ulažu značajna finansijska sredstva u razvoj kartičarstva s obzirom na višestruke (gore navedene) prednosti, ne samo za njihove korisnike nego i za banke.

Platne kartice sve više dobijaju na značaju kao metod obračuna za plaćanja na malo pri kupovini određenih proizvoda ili usluga. Najveće kompanije koje posluju sa kreditnim i debitnim karticama organizovale su zasebne elektronske klirinške i obračunske sisteme. MasterCard i VISA imaju svoje sopstvene mreže koje se koriste za verifikaciju transakcija širom sveta. Elektronski terminali na mestu prodaje, *EFT/POS* terminali, omogućavaju da se podaci sa kartice provere za manje od 15 sekundi u okviru mreže koja povezuje prodavce širom sveta sa centrom za obradu kreditnih ili debitnih kartica i emitentom kartica.

3.2.2. Kartice sa magnetnom trakom

Sa tehničkog aspekta to su standardne plastične kartice koje sadrže magnetnu traku na kojoj su upisani i na kojoj se čuvaju određeni podaci. Ova kartica je sačinjena od tri staze i nijedna od ovih staza nema kapacitet za čuvanje velike količine podataka. Prva staza koristi se za identifikaciju emitenta kartice (engl. *Bank Identification Number-BIN*) i pokazuje kojoj mreži pripada; druga za identifikaciju broja računa (engl. *Primary Account Number-PAN*); i treća za identifikaciju vlasnika računa (emgl. *Personal Identification Number-PIN*). PIN je vrsta šifre, odnosno numerička vrednost koja se u određenim sistemima koristi za pristup i autentifikaciju. PIN brojevi treba da budu poznati samo njegovom vlasniku i teški za pogađanje. Najčešće se koriste na bankomatima.²⁴

Pored toga, upisani podaci su podložni spoljnim uticajima, što znači da se mogu lako menjati, brisati ili oštetiti usled različitih razloga, slučajno ili namerno. Zbog nedovoljne sigurnosti upisivanje na njoj se gotovo ne vrši (mada postoji mogućnost), već se koristi isključivo kao memorijska kartica.

Sa takvim karakteristikama ona može biti osnova za obavljanje pre svega identifikacione funkcije za ulaz u određene sisteme (specijalne ATM kartice npr.) ili obavljanje funkcija novčanih i kreditnih kartica. Ova kartica ima relativno niske troškove upotrebe i kapacitet memorije koji dozvoljava da se pored podataka potrebnih za obavljanje transakcija, unose i podaci potrebni za obezbeđenje dodatne sigurnosti. Zbog toga se sa njihovom upotrebom kao novčanih i kreditnih kartica, došlo do eliminisanja specijalnih ATM kartica.

Usavršene kartice sa magnetnom trakom mogu se produktivnije koristiti, jer se na bazi porasta gustine samih magnetnih traka obezbeđuje povećanje kapaciteta njihovih memorija. Sa aspekta funkcionalnih mogućnosti same kartice ovakvo unapređenje je bitno, s obzirom na to

²⁴ Isto, str.46

da je kod standardne kartice prisutno ograničenje memorije. Međutim, njime se istovremeno i znatno povećavaju troškovi i same kartice i terminala koji su potrebni za njihovo korišćenje.

Kao mnogo racionalnije rešenje pojavljuje se memorijska kartica sa čipom. Njena prednost proizilazi iz jednostavne tehnologije što rezultira dalje niskom cenom. Međutim, i ova vrsta kartica se može relativno lako falsifikovati, bez obzira na to što se smešteni podaci štite sigurnosnom logikom. Memorijska kartica je specifična po tome što ne sadrži procesor, a ima ugrađen čip sa memorijom i neprogramibilnom logikom. Ona omogućava istovremeni pristup memoriji i podržava nekoliko neprogramibilnih naredbi. Tipičan predstavnik ove vrste je telefonska kartica koja postaje neupotrebljiva kada se potroši prethodno determinisan iznos.

Nedovoljan stepen sigurnosti, kapacitet memorije i prednost funkcionisanja sistema bez online veza, predstavljaju ključne razloge koji idu u prilog potiskivanju karte sa magnetnom trakom.

3.2.3. Smart kartice

Pojava smart kartica donosi sa sobom suštinske promene u funkcionisanju platnih kartica i proširenja njihovih aplikativnih mogućnosti. Samo na tehnološkoj osnovi pametne kartice, moguće je razvijati varijante tzv. kartičnog elektronskog novca. Takođe, multifunkcionalne aplikacije na jednoj kartici zahtevaju tehnološku osnovu pametne kartice.

U terminologiji se termin smart kartica izjednačava sa terminima platne kartice sa procesorom, inteligentne čip kartice, IC kartice (engl. *integrated circuit card*) i sl. Svi ovi izrazi se najčešće shvataju kao sinonimi, mada se može uočiti da ove terminološke razlike u izvesnoj meri odslikavaju tehnološke faze evolutivnog razvoja smart kartica. U ranim fazama pojavljuju se najpre memorijske kartice koje imaju čip koji pruža mogućnost upisa i čitanja podataka bez mogućnosti daljeg procesuiranja (engl. *simple memory card*). Nešto kasnije, tehnološki naprednija verzija dobija kontrolu procesa (engl. *hard logic card*), a potom se dodaje mikroprocesor. Kartice time dobijaju mogućnost autonomnog izvršavanja i memorisanja svih operacija, uključujući i šifrovanje odnosno dešifrovanje.

Znači, kartice sa mikročipom omogućuju korisnicima da potpuno odvojeno i bezbedno drže veći broj aplikacija na jednoj kartici. Mikroprocesor u kartici omogućuje automatsko izračunavanje novog stanja novca posle izvršene transakcije. Smart kartica ima oko 100 puta više memorijskog prostora i procesor pomoću koga su omogućena izračunavanja direktno na kartici. To znači da ceo proces (šifrovanje) počinje i završava se na samoj kartici i nikakvi podaci ne napuštaju karticu, što je čini bezbednijom.

Smart kartica je mikroračunar veličine standardne bankarske kartice koja u sebi sadrži:²⁵

1. jedno ili više integrisanih kola meću kojima se nalazi i mikroprocesor,
2. memoriju tipa *EPROM* ili *EEPROM* za smeštanje programa i podataka,
3. korisnički interfejs.

Smart kartica može da služi kao identifikaciona kartica za dokazivanje identiteta vlasnika. Takođe, smart kartica može da se koristi kao kreditna, odnosno debitna kartica koja

²⁵ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.109

omogućava izvršavanje off-line transakcija. Sve navedene funkcije zahtevaju da se poverljivi podaci smeste na karticu.

Danas se, zavisno od čipa razlikuju memorijske i mikroprocesorske kartice, dok se na bazi karakteristika prenosa podataka i mehanizama pristupa, razlikuju kontaktne, beskontaktne i kombinovane kartice.

Idejni tvorac smart kartice je Roland Moreno iz Francuske, a tehnološki ih je razvila firma *Bull Computers* u Francuskoj, 60-tih godina prošlog veka. Od tada veoma intenzivno raste interesovanje za njihovom upotrebom (posebno u Evropi). Smatra se da su one još u povoju, ali da već obećavaju veoma veliki uticaj na e-finansije (način poslovanja, procesuiranje, sigurnost). Sa njihovom primenom zloupotrebe platnih kartica u Francuskoj smanjene su sa 3-5% na 0,5%.

U suštini, smart kartica predstavlja mikro računar sa procesorom koji omogućava da se na njima vrši dodavanje, brisanje i manipulisanje informacijama. Funkcionalne mogućnosti ovih kartica uslovljene su vrstom memorije sa kojom čip može biti snabdeven. Ključne memorije su :²⁶

- 1) memorija na kojoj se nalazi operativni sistem (nepromenljiva, engl. *read-only memory - ROM*),
- 2) memorija koja se koristi za privremeno skladištenje prilikom rada procesora (promenljiva, engl. *random-access memory - RAM*),
- 3) memorija u kojoj su smešteni podaci od interesa kao što su broj računa, sertifikat, ključevi i sl. (engl. *electrically - erasable programmable read-only memory EEPROM*).

PROM (engl. *programmable read-only memory*) memorija omogućava menjanje postojećih memorisanih informacija sa ubacivanjem novih, tokom celokupnog veka trajanja kartice, pri čemu se sve informacije čuvaju i kada kartica nije u upotrebi. Ova memorija ima tri zone: tajnu, otvorenu i radnu. U prvoj zoni memorišu se informacije zaštite bez kojih mikroprocesor neće dozvoliti ulaz, u drugoj, informacije koje mogu biti čitane od strane terminala, a treća se koristi za vreme obavljanja transakcije.

Standardna ili kontaktna pametna kartica je istih dimenzija i debljine kao i konvencionalne plastične kartice, ali sadrži posebno ugrađenu memoriju i procesor, a za njeno korišćenje potrebno je uspostavljanje kontakta sa terminalom. Njene osnovne komponente su: čip, kontakt i plastično pakovanje. Konkretna tehnička rešenja odnosa procesora i memorije mogu biti dvojaka, sa dva ili jednim čipom. U prvom slučaju memorija i centralni procesor su na posebnim čipovima što znači da jedan čip sadrži isključivo memoriju, a drugi centralni procesor i radnu memoriju. U drugom slučaju i procesor i memorija nalaze se na istom čipu. Prvo tehničko rešenje je znatno jeftinije, ali sa manjim stepenom sigurnosti.

Kartice ove kategorije zahtevaju upotrebu terminala za svaku transakciju ili upit. Mikroprocesor kod njih može da bude korišćen za proveru identiteta korisnika bez potrebe da bude online povezan sa centralnim računom kao i za obavljanje svih procesa potrebnih za kompletiranje jedne transakcije (podatke o računu, kreditnoj liniji itd.). Ova vrsta kartica ne poseduje bilo kakve dodatne elemente kao što su tastatura, displej i sl., a poznata je i kao prva generacija čip kartica. Najrevolucionarniji koncept čip karte sa čipom, predstavljaju kartice koje su snabdevene sa displejom i tastaturom, a poznate pod nazivom super pametne kartice

²⁶ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.48

(engl. *Super Smart Card*). Ponekad se nazivaju i aktivnim ili samoautorizujućim pametnim karticama. Međutim, pojava novih bežičnih pristupa i protokola je relativizirala danas njihov značaj.

Za objašnjenje suštine funkcionisanja beskontaktna kartice značajno je imati u vidu da sistem smart kartice predstavlja praktično distributivni računarski sistem koji se sastoji od kartice, čitača kartice, operativnog sistema i komunikacionog interfejsa. Beskontaktna kartice u suštini sadrže antenu kojom se detektuju i prihvataju signali koji se emituju sa čitača, tako da prilikom upotrebe ne zahtevaju kontakt sa terminalom. Pored standardnih platnih kartica, beskontaktna tehnologije se danas pojavljuju i u formi prstena, nalepnica, stikera i sl.

U svetu su do polovine osamdesetih godina dominirale kartice sa magnetnom trakom, a potom dolazi do njihove, najpre postepene, a zatim sve intenzivnije zamene karticama sa čipom. U fazi prelaska sa jedne vrste na drugu korišćena je i hibridna tehnologija (kombinacija i magnetne trake i čipa). Ključni atributi koji karticama sa čipom daju prednost u odnosu na magnetne kartice su povećanje sigurnosti, ekonomičnosti i mogućnost multifunkcionalnosti.

Pojava pametnih kartica smatra se posebno značajnom za razvoj EFTPOS sistema. Po nekima, taj značaj je toliko izražen da se može reći da je bez upotrebe ovih kartica nemoguće širi razvoj EFTPOS sistema. To zbog toga što se čekanje na dobijanje autorizacije pojavljuje kao ograničavajući faktor svuda gde se radi o masovnim plaćanjima manjih iznosa. U uslovima takvih zahteva upotreba magnetne kartice prestaje da bude realno prihvatljiva jer usporava proces obavljanja kupoprodajne transakcije i zahteva online vezu koja nosi visoke troškove telekomunikacija.²⁷

Tabela 1: Razlike između magnetne i čip tehnologije u kartičarstvu

OSOBINE	MAGNETNE KARTICE	SMART KARTICE
količina podataka	mala	Veća do oko 100 puta
zaštita podataka od fizičkih oštećenja	mala	velika
zaštita od neovlašćenog pristupa	ne postoji	vrlo velika
cena kartice	\$ 0,05-0,5	\$ 2,5-15,0
cena terminala	\$ 100-800	\$ 100-800
broj kartica u upotrebi	preko 4 miliona	oko 100 miliona
broj terminala u upotrebi	preko 5 miliona	nekoliko puta manji od terminala za magnetne kartice
mogućnost korišćenja u elektronskim platnim sistemima	da, u sistemima kreditnih kartica	da, u sistemima kreditnih kartica i za čuvanje i prenos elektronske gotovine
mogućnost korišćenja iste kartice za više namena	ne	da

Smart kartice se sve više koriste za potrebe e-poslovanja, zbog toga su veoma moćno sredstvo za poboljšanje sigurnosti elektronskih transakcija. Najveća snaga *Smart Card* tehnologije je u raznovrsnosti mogućih primena. Na bazi nje moguće je razvijanje većeg broja različitih sigurnosnih aplikacija u oblasti zaštite pristupa računaru ili mreži, identifikacije, mobilne telefonije, elektronskog novca, digitalnog potpisa.

²⁷ Isto, str. 50

Samo na tehnološkoj osnovi pametne-smart kartice moguće je razvijati varijante tzv. kartičnog elektronskog novca. Aktivnosti smart kartica u svetu rastu po stopi od 30% godišnje.

Prednosti smart kartice su:²⁸

- Za svaki novi servis koji se stavi korisniku na raspolaganje kod smart kartice ne mora se dati nova lozinka, s obzirom na mogućnosti koje ona pruža.
- Sa smart karticom korisnik može da izvrši potvrdu ispravnosti poruke veoma lako. Ovo je zato što je kartica u direktnom kontaktu sa računarom. Korisnik generiše poruku na svom računaru. Dokument se zatim ubacuje u memoriju čipa gde se stvara zbirna vrednost (broj) kojom se nadalje proverava identitet pošiljaoca i verifikuje da tokom prenosa poruka nije pretrpela izmene. Pri prijemu koristi se isti ključ da se regeneriše zbirna vrednost (broj). Ako se primljeni i regenerisani broj poklope, poruka je validna.
- Digitalni potpis je sledeća prednost smart kartice. On funkcioniše na bazi privatnog i javnog ključa. Dokument prolazi kroz smart karticu koja ga potpisuje svojim privatnim ključem. Da dokaže da je dokument potpisao određeni korisnik, host-sistem dešifruje potpis koristeći njegov javni ključ. Ako rezultat odgovara sadržaju dokumenta potpis je validan. Ovako potpisana dokumenta mogu se slati preko Interneta uz pomoć standardnih alata za rad. Smatra se da je u ovom slučaju dokument potpuno zaštićen.
- Smart kartica može u sebi sadržati i digitalni sertifikat. Za digitalni sertifikat se može reći da je lična karta na Internetu. Sertifikat je string šifrovan sa privatnim ključem koji je u kartici. Ako host-sistem želi da proveri autentičnost korisnika na mreži, može zatražiti digitalni sertifikat koji je smešten na kartici. Kada je sertifikat poslat, host-sistem proverava sa trećom stranom korisnikov odgovarajući javni ključ koji koristi da dekodira sertifikat. Ukoliko je sve u redu korisnik dobija konekciju.

Pored dobrih osobina smart kartice imaju i određeni mana. Osnovna mana im je što su osetljive na mehanička oštećenja. Naime, čip je za plastiku zalepljen epoksi smolom koja vremenom i dugotrajnim mehaničkim naprezanjem (savijanjem) postaje krta i čip može da se pomeri. Neotporna je na vlagu i svako vlaženje kartice može da prouzrokuje njen otkaz. Sledeća mana ovih kartica je što su znatno skuplje od kartica sa magnetnim zapisom.

3.2.4. EMV standardi

Razvoj mikroprocesora pametnih kartica omogućava da se standardne platne funkcije kombinuju sa ostalim primenama u finansijama i informacionoj industriji (e-novčanik, mobilno bankarstvo) uz povećanje bezbednosti u e-trgovini. Da bi se omogućila multiaplikacijska kompatibilnost koju zahteva takav vid upotrebe bilo je potrebno donošenje posebnih standarda. Oni su doneti zajedničkom akcijom Europey, MasterCard i Visa sistema po kojima su i dobili naziv EMV standardi. Ovi sistemi su 1999. godine osnovali posebnu organizaciju za te namene, EMVco kojom danas upravlja skupština kartičarskih organizacija.

Najznačajnije prednosti koje pruža upotreba EMV standarda su:²⁹

²⁸ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.221

²⁹ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str. 51

1. povećanje stepena sigurnosti,
2. povećanje efikasnosti procesiranja i
3. omogućavanje interoperabilnosti različitih aplikacija.

Povećanje efikasnosti procesiranja transakcija zasniva se na omogućavanju dobijanja autorizacije u offline režimu, skraćivanjem vremena koje je potrebno za odvijanje transakcije. Interoperabilnost različitih platnih aplikacija EMV obezbeđuje time što rešava probleme procesiranja transakcija različitih platnih šema, uključujući i međudržavne transakcije i transakcije preko Interneta.

U uslovima e-trgovine nije dovoljno samo obezbeđenje potrebne zaštite poverljivosti podataka za vreme njihovog prenosa upotrebom asimetričnog sistema šifriranja, već je potrebno da se obezbedi utvrđivanje autentičnosti učesnika u transakciji. U odsustvu toga moguće su pojave različitih vidova zloupotreba kao što su falsifikovanje (engl. *counterfaiting*) i krađa zapisa (engl. *skimming*). Povećanje sigurnosti upotrebe pametnih kartica u ovom kontekstu EMV obezbeđuje korišćenjem SET protokola (engl. *Secure Electronic Transactions*). Težište ovog protokola je usmereno upravo na rešavanje problema koji proizilaze iz nemogućnosti međusobne identifikacije prodavca i kupca, obezbeđivanjem posebnih mera za identifikaciju.

Pored EMV standarda treba pomenuti još neke od značajnih standarda razvijenih za poslovanje sa platnim karticama. To su: ANSI X9 (za kriptografiju sa javnim ključevima), EN 726 (za telekomunikacione kartice sa čipom), EN 1546 (za elektronske novčanike), IEE P1362 (za javnu kriptografiju), ISO 7810 (za fizičke karakteristike identifikacionih kartica bez čipa), ISO 7811 (za postupke zapisa podataka na magnetne kartice), ISO 7816 (za položaj čipa i kontakata, opis protokola i komandi), ISO 9798 (za kriptografske postupke za autentifikaciju) itd.

3.2.5. Funkcionalne aplikacije

Sa aspekta razvoja savremenih sistema plaćanja, funkcionalne aplikacije na tehnologiji tradicionalnih plastičnih kartica nisu značajne, njihovo korišćenje bilo je ograničeno na lokalna tržišta, a uvođenje izvodljivo sa veoma skromnim iznosima. Mogućnosti funkcionisanja aplikacija na tehnološku osnovu kartice sa magnetnom trakom su znatno veće. One omogućavaju, pored identifikacione funkcije, obavljanje finansijskih funkcija novčanih kartica, kreditnih kartica, plaćanja na bazi prethodno izvršenih uplata i sl. Kapacitet memorije dozvoljava da se pored podataka potrebnih za obavljanje transakcija unose i podaci za obezbeđenje dodatne sigurnosti. Zbog toga, sa njihovom upotrebom kao novčanih i kreditnih kartica dolazi do eliminisanja specijalnih ATM karata i čekovnih garantnih karata.

Sa pojavom kartica sa čipom dolazi da suštinske promene u funkcionisanju platnih kartica i proširenja njihovih aplikativnih mogućnosti po tom osnovu. Ove mogućnosti javljaju se kao rezultat sledećih promena:

1. uvođenja autonomnosti obrade podataka na kartici u odnosu na sistem i
2. porasta kapaciteta memorije.

Smatra se da su kapacitet memorije, mogućnost funkcionisanja sistema bez online veza i veći stepen sigurnosti na bazi toga, razlozi koji idu u prilog potiskivanju kartica sa magnetnom trakom.

Kako korišćenjem platnih kartica dolazi do zamene tradicionalnih instrumenata, njihovo praktično korišćenje zasniva se na potrebama pojedinaca za transakcijskim medijima, a koje se mogu grupisati na:³⁰

1. korišćenje fiksnih nominalnih vrednosti (kovani novac, papirne novčanice, platni nalozi, poštanski nalozi, ĩetoni, karte sa memorisanom vrednošću);
2. korišćenje kredita (kreditne karte, otplata na rate, prodaja na kredit);
3. izbor načina skidanja sredstava sa depozitnog računa (novčane karte, čekovi, trajni nalozi).

Za sve tri pomenute aplikacije, mogu se ili koristiti posebne kartice za svaku pojedinačnu namenu ili jedinstvena multifunkcionalna kartica.

Sa ovakvim funkcionalnim karakteristikama, platne kartice postaju bitan elemenat infrastrukturne osnove koja omogućava funkcionisanje sistema plaćanja u elektronskoj trgovini. Mada se konkretne aplikacije plaćanja meĀusobno razlikuju po svojim tehniĀko-tehnološkim, funkcionalnim, ekonomskim i bezbedonosnim karakteristikama, gotovo da ni jedan platni sistem ne moĀe da funkcioniše bez upotrebe platnih kartica u nekoj od njihovih monetarnih ili nemonetarnih funkcija.

Na bazi ovih aplikacija mogu se realizovati tri osnovna koncepta e-plaćanja:

1. „prvo plati“,
2. „plati sada“ i
3. „plati kasnije“.

Prvi koncept se zasniva na karticama sa memorisanom monetarnom vrednošću, tzv. SVC (engl. *stored-value card*) ili *pre-paid* karticama kod kojih sredstva na samoj kartici mogu i da se povećavaju i da se smanjuju. Da bi se povećala sredstva na kartici vrši se njeno „punjenje“ monetarnom vrednošću, dok do smanjenja dolazi njenom upotrebom za plaćanje pri kupovini. Nazivaju se elektronskim novčanicima (engl. *electronic purse* ili *e-purse*). Javljaju se kao zatvoreni i otvoreni sistemi. U prvom slučaju memorisana monetarna vrednost moĀe se koristiti samo za kupovinu specifične robe ili usluge koju, po pravilu, nudi izdavalac kartice. U drugom slučaju, kartice sa memorisanom monetarnom vrednošću nude se od strane većeg broja izdavaca i prihvata ih veliki broj prodajnih mesta.

Koncept „plati sada“ zasniva se na upotrebi aplikacija debitnih (novčanih) kartica koje omogućavaju korisniku da povlači novčana sredstva sa svoga računa i/ili obavlja kupovinu direktnim zaduĀivanjem svog računa kod banke. Predstavlja Āisto tehniĀku inovaciju u plaćanjima stanovništva i zbog toga se ne oĀekuje da Āe bitno uticati na promenu prirode plaćanja u maloprodaji, ali se dalje unapreĀenje moĀe oĀekivati u domenu povećanja ekonomičnosti. Debitne ili novčane kartice omogućavaju prenos sredstava sa računa (Āekovnog ili štednog) korisnika kartice, na račun prodavca koji je uĀesnik u sistemu, pod uslovom da je korisnik odobrio prenos svojom personalnom identifikacijom, ali samo do iznosa pokrića na depozitnom računu korisnika kartice. Prilikom plaćanja robe ili usluga ovom vrstom kartice, autorizacioni centar odmah nakon transakcije, automatski zaduĀuje depozitni račun korisnika kartice. Bez obzira na to da li prodavac zahtev za prenos sredstava dostavlja odmah, ili posle odreĀenog vremenskog intervala, funkcionisanje sistema je veoma

³⁰ Isto, str. 53

slično funkcionisanju kliringa papirnih čekova. Zahtev za prenos sredstava ide preko banke do sistemskog operatera koji obezbeđuje zaduživanje računa kupca preko njegove banke (kupca) i istovremeno odobravanje sredstava na račun prodavca preko banke prodavca. I SVC i debitne kartice se u mnogim zemljama danas koriste kao siguran način za elektronska plaćanja.

Koncept „plati kasnije“ bazira se na upotrebi aplikacije kreditnih kartica koja korisniku omogućavaju korišćenje kreditne linije za obavljanje kupovine i/ili povlačenje gotovine do limita utvrđenog prethodnim aranžmanom. Prilikom plaćanja kreditnom karticom, korisnik aktivira kreditnu liniju i troši novac banke izdavaoca kartice. Važno je istaći da je račun korisnika, po kartici, odvojen od njegovog depozitnog (transakcionog računa). Odobreni kredit korisniku se obračunava u punom iznosu ili parcijalno, na kraju određenog vremenskog perioda. Drugim rečima, ona obezbeđuje odobravanje kredita korisniku karte koji je ugovorom obavezan da izvrši plaćanje kasnije, po obavljenoj kupovini roba ili usluga.

3.3. Automatski samouslužni šalteri - ATM

Razvijene informacione mreže su omogućile upotrebu informacionih tehnologija u šalterskom poslovanju putem bankomata, odnosno samouslužnih šaltera ATM i POS terminala, s ciljem povećanja kvaliteta usluga banaka i orijentacije prema klijentima. ATM su mašine koje su dislocirane i povezane u bankarsku mrežu i omogućuju da niz funkcija šalterskog radnika, obavi sam klijent, koristeći bankarsku platnu karticu kao sredstvo identifikacije.

Uvođenje bankomata je prvi korak ka elektronskom bankarstvu. Prvi bankomati (*Cash Dispensing Machine - CDs*), omogućavali su samo automatizaciju podizanja novca fiksiranog iznosa i u jednoj nominaciji. Kasnije dolazi do njihovog naglog razvoja u pravcu proširenja delokruga njihovog funkcionisanja, najpre u pravcu multipliciranja iznosa i nominacija novca koji se preko njih može automatizovano podizati, a zatim i dodavanjem sasvim novih vrsta usluga. Prvi bankomat pojavio se 1967. godine u filijali britanske „Barklays“ banke u formi bankomata koji je omogućavao samo isplatu gotovine. U to vreme bankari su očekivali da će njihovi klijenti koristiti ovaj bankarski uređaj samo onda kada su poslovnice koje pružaju kompletne usluge zatvorene.

Sa uvođenjem novih vrsta usluga stvaraju se kompletni samouslužni šalteri (engl. *Automated Teller Machines - ATM*) koji omogućavaju korišćenje kompletnih šalterskih usluga: deponovanje i podizanje novca, izdavanje čekovnih knjižica, naručivanje i primanje izveštaja, deponovanje i unovčavanje dokumenata plaćanja, transfer sredstava sa jednog računa na drugi, pa čak i korišćenje kredita određivanjem limita za prekoračenja. Pomoću CDs-a i ATM-ova klijenti mogu da obavljaju rutinske transakcije van prostorija i lokacija banke, na principu samousluživanja i nezavisno od radnog vremena banke. Sa ovakvim karakteristikama oni omogućavaju.³¹



- Prvo, apsolutno produžavanje vremena pružanja pomenutih usluga (jer ih klijenti mogu samostalno koristiti u svako doba) i
- Drugo, snižavanje troškova, eliminisanjem potrebe za otvaranjem klasičnih filijala i angažovanjem dodatnih šalterskih službenika.

³¹ Isto, str.110

Znači, uvođenjem bankomata, klijentu je omogućen pristup računu 24 časa, brza usluga, bez čekanja u redu ispred šaltera i sve šira lepeza usluga koja se nudi. Sa druge strane, uvođenje ATM za banke znači višestruko smanjenje troškova procesiranja transakcija, smanjenje redova i gužvi u bankama. Isto tako dovodi i do racionalizacije broja zaposlenih u poslovima sa stanovništvom i mogućnost ostvarivanja dodatnih prihoda od naknada za pružanje usluga korisnicima kartica drugih banaka.

Osnovni tehnički elementi bankomata su:³²

- 1) konzola za korisnika,
- 2) dispenser gotovine,
- 3) deo za prijem deponovanih sredstava,
- 4) centralni kontrolor,
- 5) mehanizam za štampanje i
- 6) softverska podrška.

Delom ovog sistema smatra se identifikaciona kartica korisnika, jer sistem bez nje ne može da funkcioniše. Kroz korisničku konzolu se uspostavlja veza sa korisnikom i daju uputstva kojima se on vodi kroz proces samousluživanja. Kada korisnik sistema ubaci svoju karticu koja sadrži PIN, sa nje se čitaju svi relevantni podaci. To su: broj računa, datum isticanja karte, dozvoljeni broj dnevnih korišćenja, ukupan broj dozvoljenih korišćenja za isplatu tokom životnog veka kartice, routing i transit number i druge informacije.

Tipičan ATM sadrži tri oblasti inputa (čitač kartice, numeričku tastaturu i funkcionalnu tastaturu) i tri oblasti outputa (displej za poruku, cash dispenser i štampač priznanice). Generalno, on se aktivira plastičnom karticom sa posebnim identifikacionim brojem (engl. *Personal Identification Number - PIN*) koji je ključ ulaska individualnog korisnika. Na funkcionalnoj tastaturi definišu se vrsta i broj usluga koje se žele u okviru raspoloživih mogućnosti transakcija. U tipičnim transakcijama ove vrste proces se obavlja u fazama (*step-by-step*):³³

1. Klijent ubacuje karticu – Ulaz klijenta u sistem obezbeđuje se ubacivanjem identifikacione kartice u odgovarajući čitač, prema predviđenom protokolu, u okviru limitiranog broja pokušaja (obično tri) i limitiranog vremenskog perioda. Ukoliko se tokom dešifrovanja podataka otkrije greška, kartica se ili vraća ili zadržava u aparatu (u zavisnosti od konkretnog rešenja).

2. Unošenje PIN-a – U tipičnim primerima biće potrebno da klijent unese svoj PIN u roku od 30 sekundi na numeričkoj tastaturi. Ukoliko je uneti broj netačan ili prekoračen vremenski limit, klijent će dobiti instrukciju za ponavljanje celog postupka i novih 90 sekundi na raspolaganju. U slučaju ponovnog neuspeha, postupak se može još jedan put ponoviti sa odobrenjem novih 90 sekundi. Za sve to vreme kartica je u aparatu i kontrolor vrši proveru da li ona pripada dotičnom sistemu ili ne.

Tek nakon pozitivnih rezultata identifikacije, postoji mogućnost ulaska klijenta u sistem i prijem daljih instrukcija koje se odnose na izbor tipa transakcije i željenog iznosa. Ta mogućnost će biti saopštena preko displeja sledećom instrukcijom: “Biraj vrstu transakcije“ i tada će otpočeti treća faza.

³² Isto, str.111

³³ Isto, str.112

3. Izbor transakcione opcije – Pritiskom na odgovarajuće funkcionalno dugme na tastaturi klijent vrši izbor. Ako npr. želi da deponuje sredstva na tekući račun pritisnuće funkcionalno dugme za deponovanje i dobiti dalje instrukcije.

4. Deponovanje na tekući račun – Unosi se iznos koji se deponuje, a u slučaju da se napravi neka greška moći će da se ispravi ponavljanjem postupka. Ako je sve u redu, klijent preko displeja dobija instrukciju za sledeći postupak, u zavisnosti od izabrane transakcione opcije. U konkretnom primeru sledeći postupak treba da bude ubacivanje koverte u depozitar i na displeju će biti data instrukcija za to.

5. Ubacivanje koverte u depozitor – Klijent ubacuje koverat kroz otvor koji se pojavljuje tek posle instrukcije za ubacivanje, a nakon provere, po obavljenoj transakciji, štampa se potvrda čiji jedan primerak dobija klijent.

U domicilnim uslovima, na bankomatima je moguće obaviti uglavnom dve operacije, a to su: upit stanja na tekućem računu građana i isplata gotovine.

Prikaz podizanja gotovine na ATM aparatu možemo dati na sledeći način (uprošćen prikaz):

1. korisnik aktivira ATM ubacivanjem platne kartice u aparat u deo predviđen za to,
2. ATM traži od korisnika da izabere jezik (uglavnom srpski ili engleski),
3. nakon izbora jezika, korisnik je obavezan da unese svoj PIN (*Personal Identification Number*) koji je vezan uz datu platnu karticu,
4. ATM proverava ispravnost PIN-a,
5. ukoliko je PIN prihvaćen, traži se od korisnika da odabere transakciju koju će izvršiti,
6. nakon opredeljivanja da želi da izvrši podizanje gotovine, prelazi u meni u kojem su mu naznačene koje vrste novčanica stoje na raspolaganju u ATM uređaju, kao i unapred definisane iznose koje može da podigne. Ukoliko želi da podigne neki drugi iznos, potrebno je da pokrene dodatnu opciju za to,
7. po unošenju željenog iznosa, ATM vraća korisniku platnu karticu,
8. ATM isplaćuje novac kroz deo predviđen za to,
9. ATM izbacuje listić potvrde na kojem je evidentiran datum transakcije i iznos sredstava koji je klijent podigao.

Sa aspekta akceptiranja ulaznih podataka, bankomati mogu funkcionisati na bazi off-line i on-line veza. U prvom slučaju sistem funkcioniše bez permanentne direktne veze sa računarom banke, pa zbog toga mora biti snabdeven posebnom memorijom sa crnim listama, sopstvenom logikom za čitanje ulaznih podataka i sredstvima za dnevnu kontrolu rada od strane bankarskog osoblja. Zbog nemogućnosti davanja trenutne autorizacije, klijentima se često preventivno ograničava unapred broj dozvoljenog podizanja gotovine u okviru određenog vremenskog perioda.

Samouslužni šalteri se ne koriste samo kao zamena za bankarske poslovnice na udaljenim lokacijama, već i u samim bankarskim poslovnicama u funkciji unapređenja poslovanja i pružavanja vremena pružanja bankarske usluge. Takve polu-automatizovane bankarske poslovnice najčešće su opremljene većim brojem samouslužnih uređaja za pojedinačne usluge ili kompletnim samouslužnim šalterima, pored klasičnih bankarskih šaltera. Poslovanje ovakve jedne poslovnice, podrazumeva kombinaciju mogućnosti korišćenja bankarskih usluga i na klasičnom šalteru banke i na samouslužnim šalterima, tokom radnog vremena. Nakon toga, sala sa klasičnim bankarskim šalterom se zatvara, a klijenti mogu da koriste i dalje

bankarske usluge na samouslužnim šalterima i specijalnim terminalima u delu koji ostaje otvoren za upotrebu i posle radnog vremena.

Produžavanje radnog vremena i snižavanje troškova predstavljaju i osnovu celokupne filozofije njihovog uvođenja. Prema jednom istraživanju od ukupnog broja korišćenja ATM, na vreme vikenda otpada 30%, van radnog vremena banke 40% i u toku radnog vremena 30%. Mogućnost snižavanja troškova direktno je uslovljeno realizacijom uslova za korišćenje ekonomije obima, s obzirom na to da u strukturi troškova, kapitalni troškovi učestvuju orijentaciono sa 42%, troškovi održavanja sa 37%, a troškovi podrške transakcija sa 20%. Zbog ovakve strukture troškova, u ranim fazama primene, oni često nisu imali uspeha, dok su posle izvesnog vremena doživljavali brzi razvoj.³⁴

U celini, ATM-ovi se visoko kotiraju kao sredstvo za povećanje efikasnosti zbog toga što zahtevaju znatno manje angažovanje ljudskih resursa. Prema istraživanju obezbeđuju obradu znatno većeg broja transakcija u odnosu na šaltersko bankarsko osoblje (šalterski službenici obrade prosečno mesečno 4300 transakcija, a bankomati obrade 6400 transakcija). Istovremeno, oni to mogu da učine po znatno nižoj ceni (cena transakcije po klijentu mesečno iznosi 3,75\$ kada se obavlja preko bankomata, dok u slučaju obrade šalterskih službenika iznosi 4,38\$).³⁵

Zbog ovakvih cenovnih relacija neke veće banke su eksperimentisale sa uvođenjem posebnih provizija, ukoliko bi se usluge koje mogu da se koriste preko bankomata, koristile uz angažovanje šalterskih službenika. Međutim, praksa je pokazala da povećano korišćenje ATM-ova ne mora da znači i profitabilnije obavljanje relevantnih operacija, zbog toga što klijenti pokazuju sklonost da ih koriste veoma često i za podizanje veoma sitnih iznosa, jednostavno zato što su raspoloživi za korišćenje 24 časa. Sa druge strane, za neke druge transakcije (npr. ulaganje sredstava, predaju platnih spiskova i sl.) pokazuju sklonost odlaženja na bankarske šaltire. Usled toga, banke dolaze u situaciju da i pored instaliranja znatnog broja bankomata, angažuju više šalterskih radnika.

Za klijente koji preferiraju personalnom odnosu sa šalterskim službenikom, što je posebno svojstveno starijoj populaciji, ATM nisu prihvatljivi.

Poseban ograničavajući faktor je nesigurnost sistema. U SAD-u je poznat slučaj dve banke koje su tokom 2001. i 2002. godine doživle takvu krađu gotovine da je jedna od njih bankrotirala. One su imale ugovor sa vlasnikom bankomata da upravlja celim lancem ovih uređaja i obezbeđuje transport gotovine blindiranim vozilom. Dogodilo se da sam vlasnik sklanja po deo gotovine za pokriće sopstvenih troškova, da u tome bude otkriven tek posle godinu dana, a banke pretrpe ogromne gubitke po tom osnovu.

Rapidno opadanje troškova elemenata računarskih sistema i usavršavanje inteligentnih terminala, deluju podsticajno na širenje sistema samouslužnih šaltera sa kompletnim asortimanom usluga. Istovremeno, potreba obezbeđenja posebnih prostorija za smeštaj opreme i mera bezbednosti za čuvanje gotovine u minijaturnim trezorima, deluju u pravcu porasta interesa za uvođenje različitih vrsta jednostavnih uređaja, od kojih bi svaki bio namenjen specifičnoj bankarskoj usluzi. Kao poseban faktor koji je delovao u tom pravcu, odnosi se na mogućnost da se mnoge usluge iz asortimana ATM, pruže preko znatno jeftinijih sistema kućnog bankarstva.

³⁴ Isto, str.114

³⁵ Isto, str.115

3.3.1. ATM mreže

U početku poslovanja putem ATM-a, posedovanje mreže bankomata bilo je pitanje prestiža među bankama, pa su se banke neprestano utrkivale u razgranavanju sopstvenih mreža bankomata. Kasnije su banke uvidele nesvrishodnost samostalnog razvoja bankomata, pa su otpočeli procesi njihove integracije, pri čemu se dve ili više banaka sporazumevaju o međusobnom korišćenju svojih mreža bankomata.

Mreže bankomata i samouslužnih terminala, u principu, mogu se koristiti kao samostalni ili kooperativni sistemi. U ranim fazama njihovog uvođenja jedna banka, po pravilu, vrši uvođenje ovih sistema samo za pružanje usluga sopstvenim klijentima.

Kasnije, sa porastom broja banaka koje uvode ove sisteme, pojavljuju se dve mogućnosti: prva, da paralelno funkcioniše više samostalnih sistema različitih banaka i druga, da banke vrše zajednička ulaganja i zajednički koriste istu tehničko-tehnološku infrastrukturu. Generalno, mogućnosti održavanja kompletne kontrole nad sistemom i uslugama, definisanim od strane institucije vlasnika predstavlja argument koji ide u prilog prvog rešenja, dok troškovi instaliranja i funkcionisanja ovih sistema (ekonomija obima) i potreba unapređenja usluga sistema (ekonomija diverzifikacije) deluju kao argument opredeljenja za drugo rešenje. Poseban faktor koji treba istaći u korist drugog rešenja je porast vrednosti ovakvih sistema za klijente sa porastom broja učesnika u sistemu, usled čega dolazi do ispoljavanja interesa korisnika za korišćenje jednobraznih mreža na što širim prostorima.

Stepen kooperacije može biti različit. Prvi vid kooperacije realizuje se kroz formu koalicije u kojoj se saradnja institucija članica ograničava na oblast operacionog korišćenja infrastrukture (korišćenje usluga sa karticama drugih institucija). Drugi vid je forma konzorcijuma koja podrazumeva zajedničko učešće i u operacionom korišćenju sistema i u razvoju. Konačno, postoji mogućnost da se ne formiraju sopstvene mreže već da se za ove namene koriste usluge specijalizovanih servis provajdera. Tu funkciju često obavljaju proizvođači opreme ili drugih elemenata koji predstavljaju finansijsku podršku sistema samouslužnih šaltera.

U zavisnosti od opredeljenja za samostalno ili zajedničko korišćenje sistema različito se organizuju i procesi davanja ovlašćenja, PIN-a i rukovanje crnom listom. U sopstvenim mrežama jednostavno svaka institucija obavlja posao za sebe. Ako se radi o zajedničkom korišćenju jedne mreže mora se jedinstveno rešavati rukovanje crnom listom, ovlašćenjima za korišćenje kartice, rukovanje ključem, a zahtevi za njih se razlikuju u zavisnosti od nivoa zajedničke mreže (nacionalni, međunarodni). Različiti nivoi se međusobno mogu i povezivati ali sistemska rešenja treba tako da budu postavljena da recimo nemogućnost korišćenja internacionalnog nivoa, ne znači i blokiranje korišćenja nacionalnog nivoa.³⁶

Zbog, neracionalnosti samostalnog razvoja, u novije vreme često veći broj institucija deli ATM da bi smanjili troškove. Formiraju se zajedničke mreže u koje se umrežavanju uređaji većeg broja institucija čije funkcionisanje podrazumeva postojanje zajedničkog *switching* centra. U ovako formiranim udruženim mrežama preciziraju se načini uzajamnog korišćenja ATM-ova drugih institucija. U ovakvim sistemima dolazi do diferenciranja usluga na usluge sopstvenim klijentima i klijentima drugih banaka.

³⁶ Isto, str.118

U ovakvim sistemima posebno pitanje je naplaćivanje provizije za korišćenje ATM aparata. Često se provizija ne naplaćuje klijentima banaka koji su članovi mreže dok se klijentima banaka koji nisu članovi mreže naplaćuje.

3.4. Maloprodajni terminali – EFT/POS terminali

EFTPOS ili POS sistem (engl. *Electronic Funds Transfer Systems-Point of Sale*) je sistem za elektronski transfer novca na mestu prodaje proizvoda ili usluga, a koji se ostvaruje povezivanjem maloprodajnog mesta sa mrežom i bazama podataka banaka. Ovaj sistem omogućava direktan prenos sredstava sa računa kupca na račun prodavca. EFTPOS terminali omogućavaju da se podaci sa kartice provere za manje od 15 sekundi u okviru mreže koja povezuje trgovce širom sveta sa centrom za obradu platnih kartica i emitentom kartica.

Maloprodajni terminali - POS sistemi, predstavljaju posebne punktove masovnog ulaska pojedinaca u elektronski sistem plaćanja i to direktno. Suština njihovog funkcionisanja sastoji se u mogućnosti aktiviranja terminala u maloprodaji određenom elektronskom karticom, koja služi kao sredstvo ulaza i identifikacije i kao sredstvo za obavljanje trenutnog prenosa sredstava sa računa kupca na račun prodavca. Korišćenje POS-a se aktivira provlačenjem platne kartice kroz terminal koji očitava magnetnu traku/čip platne kartice i unošenjem iznosa transakcije i to putem stalne telefonske linije ili ISDN³⁷ veze, pri čemu se na licu mesta, on-line, proverava stanje na račun korisnika. Na isti način se POS terminalu šalje povratna informacija na osnovu koje se štampa račun i to, po pravilu, u duplikatu, s tim što jedan primerak koji ostaje pružiocu usluge, odnosno prodavcu robe, kupac potpisuje.



Sam mehanizam funkcionisanja zasniva se na povezanosti terminala lociranih na određenim prodajnim ili uslužnim mestima sa računarskim centrima određenih finansijskih institucija.



Uvođenje ovih sistema počelo je sa eksperimentalnim programima u SAD-u, koji su se kasnije pretvarali u stalno funkcionalne sisteme. Osnovni problem koji se javljao u tim prvim periodima primene, manifestovao se u nesposobnosti banaka da ostvaruju profitabilnost na bazi ove vrste usluga. Razlog je bio u nedovoljnoj masovnosti korišćenja sistema, pošto su se tadašnji sistemi primenjivali u lokalnim relacijama i u relativno kratkom vremenskom periodu nije bilo mogućnosti za ostvarivanje prednosti ekonomije obima. U Evropi pionir je

bila Francuska, koja i kasnije dugo prednjači ispred ostalih zemalja po primeni ovih elektronskih sistema.

U ranoj fazi, u zavisnosti od broja finansijskih institucija koje su uključene u sistem diferencirana su tri modela:³⁸

³⁷ ISDN (Integrated Services Digital Network-digitalna mreža sa intergrisanim uslugama) predstavlja nadogradnju na postojeću javnu telefonsku mrežu. Posедуje dva izlaza, jedan se može koristiti za telefoniranje, dok se drugi, u isto vreme može koristiti za konekciju na Internet.

³⁸ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.119

- Prvi model je najprostiji i realno se mogao primenjivati samo u lokalnim relacijama, zato što podrazumeva uslove u kojima i kupac i prodavac imaju račune kod jedne iste banke.
- Drugi, tzv. prelazni model bio je nešto složeniji, u njega su uključivane dve ili više banaka koje izmeću sbe obavljaju operacije automatskog kliringa.
- Treći model je u suštini bio model mreže, funkcionisao je koristeći *switching* i *procesing* centre i bio je pogodan za primenu u nacionalnim i međunarodnim relacijama. Tokom kasnijeg razvoja, dominiraju sistemi koji pripadaju trećoj kategoriji, koji ne samo da su sve više prerastali u internacionalne sisteme, već je i izmeću vodećih svetskih sistema dolazilo do međusobnih kooperacija.

Konkretno funkcionalne aplikacije ovih sistema su se značajno menjale u skladu sa promenom ciljeva. U ranoj fazi, njihov osnovni i jedini cilj je bio povećanje efikasnosti i ekonomičnosti samog sistema plaćanja putem redukcije rada na obradi papirnih instrumenata, povećanja tačnosti, ubrzanja obrade i snižavanja troškova. Kasnije se pokazuje da ovi sistemi mogu znatno više, pa se njihova aktivnost proširuje na čitav spektar usluga trgovini kao što su npr. trenutna informacija o prodaji, davanje analize prodaje, kontrola zaliha, obavljanje knjigovodstvenih poslova, praćenje trgovinskih tokova i obavljanje transfera i sl.



Promociju ovih sistema vršile su finansijske institucije, a za njihovu širu primenu bilo je potrebno da postoji interes kupaca, trgovine i banaka. Trgovina je nalazila svoj interes u unapređenju usluga kupcima, smanjenju manuelne obrade papira, smanjenju rizika kod čekovnih plaćanja, ubrzanju obrta i modernizaciji svog imidža. Zainteresovanost kupaca mogla je da potiče od interesa za brže obavljanje transakcija, smanjenje brige i rizika upotrebe gotovog novca, eliminisanje pisanja čekova i eventualno ostvarivanje cenovnih beneficija.

Korišćenjem platne kartice (debitne ili kreditne) kupac uspostavlja online vezu sa računarnom banke i preko terminala daje elektronski nalog računarskom centru banke da transferiše novčana sredstva sa računa kupca na račun prodavca. Proces plaćanja platnom karticom na POS-u možemo prikazati na uprošćen način³⁹:

1. prodavac izračunava vrednost kupljenog proizvoda ili usluge i traži od kupca da plati,
2. kupac daje platnu karticu prodavcu,
3. prodavac provlači platnu karticu kroz POS terminal. Vrednost prodatog proizvoda ili usluge prodavac unosi ručno, ili preuzima iz registar kase,
4. prodavac prenosi podatke o platnoj kartici i vrednosti kupljene robe ili usluge svojoj poslovnoj banci, ili autorizacionom centru, sa zahtevom za autorizacijom. Ukoliko se zahtev prenosi poslovnoj banci trgovca, ona naknadno zahteva autorizaciju od banke emitenta kartice,
5. ukoliko vlasnik kartice ima dovoljno sredstava na svom računu ili mu je odobrena kreditna linija, banka emitent kartice ili autorizacioni centar autorizuju transakciju,
6. banka emitent kartice rezerviše sredstva na računu vlasnika kartice u iznosu vrednosti kupljenog proizvoda ili usluge. Račun korisnika kartice se još uvek ne zadužuje. Banka emitent kartice obaveštava poslovnu banku trgovca o prihvatanju (ili odbijanju) transakcije,

³⁹ http://www.-e-trgovina.co.yu/kartice/card_istorijat4.html

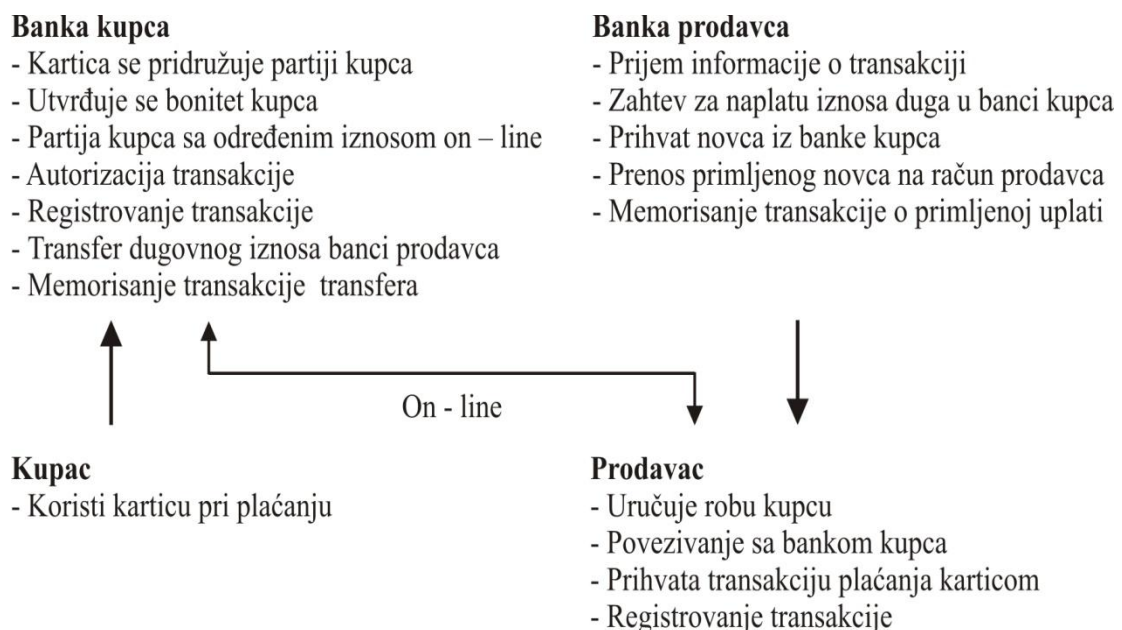
7. nakon određene transakcije, poslovna banka trgovca, ili autorizovani centar šalje šifru odobrenja (ili odbijanja) POS terminalu prodavca. Svaki POS terminal ima svoj jedinstveni identifikacioni broj, tako da je institucija koja vrši obradu transakcija u mogućnosti da prosledi podatke upravo tom terminalu,
8. prodavac štampa račun (slip) i zahteva od kupca da ga potpiše i na taj način obavezuje kupca da nadoknadi naznačeni iznos banci emitentu platne kartice,
9. na kraju radnog dana, prodavac upoređuje autorizacije koje su memorisane u POS terminalu sa potpisanim računima. Na osnovu tih podataka, banka koja je emitovala platnu karticu, odobrava poslovnoj banci prodavca iznos konkretnog računa. Prodavac je u obavezi da plati diskontnu proviziju od ukupnog iznosa prodaje (u procentu koji je dogovorio sa emitentom kartice).

Transakcija se odvija veoma brzo i jednostavno. Potrebno je da je POS terminal priključen na slobodnu telefonsku liniju. Slipom, koju je potpisao vlasnik kartice, se potvrđuje transakcija i istinitost iste. Jedan primerak slipa sa potpisom ostaje trgovcu, a drugi se uručuje kupcu, uz fiskalni račun.

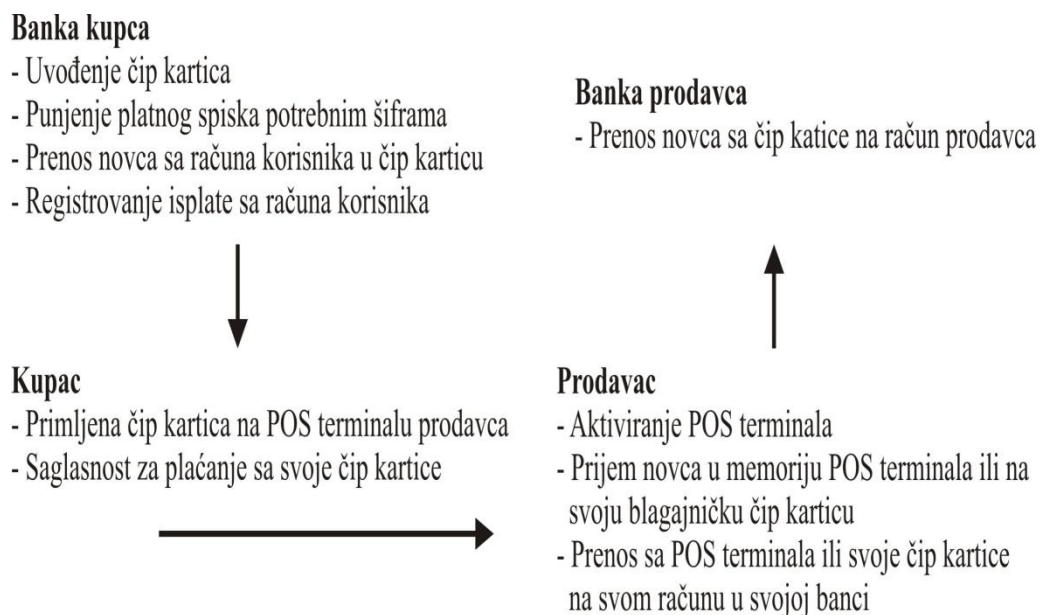
Za obavljanje ovih funkcija bile su neophodne sledeće tehničke komponente: maloprodajni terminali, koncentratori (kontrolori terminala), komunikaciona mreža, swiching centar, bankarski računarski centri i autorizacioni sistemi. Dugo vremena usko grlo ovih sistema bio je unos podataka koji je vršen preko maloprodajnih terminala. I maloprodajni terminali i mreža moraju biti polivalentni zbog toga što praktično ne postoji „tipična maloprodaja“, već svaka vrsta ima svoje specifične zahteve koji međusobno mogu biti manje ili više različiti.

Savremene mreže EFTPOS sistema sreću se skoro podjednako u *offline* i *online* varijantama. Kod offline varijante akumuliraju se sve transakcije klijenta koje su realizovane u toku dana i onda se sa računa klijenta skida ukupan iznos obavljenih transakcija. Za razliku od ove varijante, kod online sistema se vrši direktna trenutna autorizacija svake pojedinačne transakcije u trenutku njenog izvršavanja.

Slika 1: Dijagram toka plaćanja karticom sa magnetnom trakom



Slika 2: Dijagram toka plaćanja čip karticom



Poređenje cena ove dve varijante EFTPOS sistema pokazuje da su na kratak rok u prednosti sistemi tipa off-line, međutim, kako online sistemi bitno smanjuju mogućnost prekoračenja korisnika, smatra se da su oni ekonomičniji za banku na duži rok. U cilju sprečavanja nastajanja ne dozvoljenih prekoračenja kod off-line sistema banka mora prethodno da izvrši selekciju klijenata kojima će odobriti korišćenje određenih vrsta usluga i da to ugradi u program ukoliko se kao sredstvo ulaska u sistem koristi karta sa magnetnom trakom.

Pitanje koje se u ovom kontekstu postavlja je da li između EFTPOS sistema, ATM sistemima i sistema kućnog bankarstva - HB postoji odnos komplementarnosti ili supstitucije. Sa jedne strane, sličnost postoji u tome što se aktiviranjem terminala omogućava korišćenje sopstvenih finansijskih sredstava. Međutim, preko ATM šaltera obavljaju se samo rutinske šalterske operacije dok se kod EFTPOS vrši plaćanje u trenutku kupovine.

Ako klijent ima mogućnost izbora da, podigne novac sa ATM instaliranog u samoj trgovini (ili u njenoj blizini), ili da direktno upotrebi svoju novčanu karticu za plaćanje preko EFTPOS sistema, čime će njegov račun biti automatski zadužen, onda između ovih sistema postoje istovremeno i odnosi supstitucije i komplementarnosti. Zato je bilo logično očekivanje da dalji razvoj ovih sistema ide u pravcu objedinjavanja ovih funkcija.

Za maloprodajne terminale (sisteme elektronskih plaćanja u maloprodaji) se može reći da predstavljaju „najčistiji“ elektronski prenos sredstava.

Broj POS terminala se brzo povećava širom sveta. U SAD-u je broj POS terminala porastao sa 50.000 jedinica u vreme 1990-tih godina, na preko 100.000, početkom XXI veka. Danas većina prodajnih mesta prihvataju platne kartice kojima se mogu obaviti plaćanja⁴⁰. Plaćanje putem POS-a je korisna alternativa, kako za kupce, tako i za prodavce (naravno ne treba zaboraviti i korist za banke izdavaoce platnih kartica). Prodavci ne moraju da brinu da li

⁴⁰ U Srbiji je donet Zakon o fiskalnim kasama, po kome sve trgovine moraju instalirati POS terminal za prijem bar jedne platne kartice („Sl.glasnik RS“, br.135/04)

klijent ima sredstava na računu, s obzirom na to da je provera on-line, dok kupac ne mora da piše čekove i bezbednije je da ne nosi novac sa sobom.

3.5. Kućno bankarstvo (HB)

Homebanking se definiše kao sistem za direktno korišćenje bankarskih usluga od kuće, pošto omogućava neposredan transfer sredstava, informacija i naloga putem telefonske mreže, dakle bez pisanja pratećih dokumenata.⁴¹

Cilj ovih sistema je približiti uslugu klijentima i omogućiti im komunikaciju sa bankom od kuće, bez dodatnih napora u smislu odlaska na šalter banke ili posredne komunikacije.

Kućno bankarstvo (HB), predstavlja posebnu vrstu daljinskog bankarstva, koje klijentima banke pruža mogućnost uspostavljanja telekomunikacionog linka (putem telefona, televizora ili računara) sa računarskim centrom banke u cilju korišćenja određenih usluga. U početku, klijent je stupao u direktnu vezu sa službenikom banke i preko njega su se inicirale operacije bankarskom računaru. Danas, većina banaka u razvijenim zemljama raspolaže tzv. pozivnim centrima (engl. *call centers*), kao i sistemima za prepoznavanje glasa, sa kojima klijenti uspostavljaju direktnu vezu.⁴²

Sistemi kućnog bankarstva nastali su kao rezultat nastojanja da se mogućnosti elektronskog prenosa sredstava iskoriste za distribuiranje finansijskih usluga klijentima u njihovim stanovima. Prvi eksperimenti vršeni su u SAD-u polovinom osamdesetih godina, a kako su bili usmereni samo na korišćenje nove tehnike, pogodne za razvijanje sistema plaćanja sektora stanovništva, pojavljuju se pod terminom kućno bankarstvo (engl. *home banking*). Tada se mnogi od ovih sistema nisu pokazali kao profitabilni, pre svega zato što su primenjivani u lokalnim razmerama, sa nedovoljnim asortimanom usluga, tako da nisu mogle da dođu do izražaja ni informaciona ekonomija obima, ni informaciona ekonomija diverzifikacije.

Kako je tehnička osnova sistema kućnog bankarstva bila pogodna za obavljanje mnogobrojnih usluga privrednom sektoru, kućno bankarstvo je sve više dobijalo na značaju, upravo u ovoj oblasti, funkcionišući kao sistem kancelarijskog bankarstva (engl. *banking at business ili homeoffice banking*). Danas se sistem kućnog bankarstva posmatra kao element inicijalnog podsticaja za dalju ekspanziju ovog tipa usluga, koja je u velikoj meri omogućena usavršavanjem njene tehničko-tehnološke osnove i prelaskom sa telefona na videotekst, a kasnije na Intranet i Internet. Razvoj telekomunikacionog servisa u pravcu digitalizacije još više je otvorio vrata homebanking servisima u obliku digitalnih govornih tehnologija i sistema telefonskih govornih automata. S druge strane, globalizacija telekomunikacija preko postavljanja mreže svih mreža – Interneta, stvorila je preduslove za virtuelno bankarstvo od kuće.

U razvoju kućnog bankarstva, razlikujemo tri faze koje su se menjale u zavisnosti od oblika telekomunikacionih veza između banke i klijenta i to:

1. Telefonsko bankarstvo;
2. On-line bankarstvo (Kućno bankarstvo na bazi Intraneta);

⁴¹ Stankić R.: „Elektronsko poslovanje“, cit. delo, str.97

⁴² Vuksanović E.: „Elektronsko bankarstvo“, cit. delo, str.124

3. Internet bankarstvo (Internet Banking).

3.5.1. Telefonsko bankarstvo

Telefonsko bankarstvo u svetu se pojavilo 70-tih godina prošlog veka. Ono predstavlja direktno korišćenje bankarskih usluga od kuće putem telefonske mreže. Sistem plaćanja preko telefona u suštini je obavljanje platnoprmetne operacije na bazi oralne instrukcije korisnika, preko transakcionog telefona. Moguće su dve varijante za obavljanje pomenute operacije:

1. klijent stupa u direktnu vezu sa službenikom banke i preko njega se iniciraju operacije bankarskom računaru;
2. sam klijent uspostavlja direktnu vezu sa računarskim centrom banke.

Za funkcionisanje druge varijante potrebna je snabdevenost transakcionih telefona posebnim čitačima koji čitaju podatke sa magnetne trake sredstva ulaza u sistem, ili tastaturom na kojoj klijent unosi sam podatke potrebne za ulaz u sistem. U oba slučaja, oni se proveravaju i na njih sistem odgovara zvučnim signalom. Ukoliko nema razloga za poništavanje ulaza i zahteva za dodatnim proverama, ulaz se odobrava i otvara mogućnost za prijem dodatnih informacija potrebnih za obavljanje željene operacije. Zasniva se na tzv. pozivnim centrima, odnosno na sistemima kojima se pristupa preko određenih šifri unetih preko tastature. Telefonsko bankarstvo može da se koristi za proveru stanja i transakcija na računima, otplate zajmova, plaćanja unutar banke, slanje stanja računa na korisnikov fax, naručivanje čekova, plaćanje računa u zemlji (telefonskih računa, računa za struju i sl.) i transfera novca. Za ovu vrstu usluga, radi identifikacije, pored šifre može da se koristi i token⁴³.

Za korišćenje ove usluge klijentu banke je potreban telefon kod kuće, na poslu ili putovanju i eventualno token (neke ga banke daju besplatno na korišćenje). Pomoću tokena ili unošenjem PIN-a (lično kreiranje lozinke) ostvaruje se pristup operateru telefonskog servisa. Preduslov za uključivanje u sistem je da korisnik ima otvoren tekući račun sa urednim poslovanjem. Pozivom na određeni telefonski broj, pristupa se servisu, koji je neprestano na raspolaganju. Nakon identifikacije putem tokena ili šifre, otvara se meni koji preko govornog automata vodi korisnika do željene usluge.

Telefonski servis omogućuje sigurno, brzo i jednostavno korišćenje sledećih usluga:

1. upit u stanje i promene na tekućem i deviznom računu,
2. sva plaćanja unutar banke putem naloga za prenos (prenos sa jednog tekućeg računa na drugi),
3. plaćanje rate kredita (koji su uzeti kod banke),
4. naručivanje čekovnih blanketa na željenu adresu,
5. pregled izvršenih naloga,
6. naručivanje platnih kartica,
7. prodaja i kupovina, kao i konverzija deviza,
8. naručivanje potvrde za pojedino izvršeno plaćanje putem faksa,
9. pregled kursnih lista i sl.

⁴³ Autentifikacioni tokeni su hardverska ili softverska sredstva koja služe za generisanje jednokratnih lozinki. Hardverski tokeni su lako prenosivi mali uređaji koji proučavaju lozinku. Korisnik pročita lozinku sa tokena i unosi ga prilikom prijavljivanja na sistem/aplikaciju. Njegova prednost je u tome što se ne povezuje na računar. Softverski tokeni se instaliraju na prenosive računare, jeftiniji su od hardverskih tokena, ali njihova bezbednost zavisi od bezbednosti računara na koji su instalirani.

Neke banke omogućuju plaćanje i drugih finansijskih obaveza (npr. računi komunalnih usluga, račune telekomunikacionog operatera, račune elektrodistribucije itd.). Sva plaćanja (prenosi) obavljani putem telefonskog servisa beleže se na izvodu⁴⁴ tekućeg računa, koji korisnik prima na način na koji je ugovorio sa Bankom (postoji mogućnost elektronskog primanja, kao i klasičnog podizanja izvoda na šalteru Banke ili dostave putem pošte).

Telefonsko bankarstvo pokazuje veliku ekspanziju u poslednje vreme, a najrazvijenije je u Francuskoj i Velikoj Britaniji, gde ga koristi oko 10% klijenata banke. U Francuskoj je došlo i veliki uspon pre nego u drugim zemljama zahvaljujući programu *Minitel France Telecom-a*, koji je uveden sredinom 80-tih. U cilju stimulisanja prihvatanja Mintel sistema *France Telecom* je davao besplatno kućne terminale korisnicima. Mintel je u samom startu predstavljao razvijenu verziju telefonskog bankarstva, jer je pružao kompletan videotext servis.

3.5.2. On-line bankarstvo

On-line bankarstvo predstavlja kombinaciju karakteristika programa za lične finansije i elektronskog plaćanja računa.

On-line bankarstvo se sprovodi putem Intraneta. Radi se o direktnoj komunikacionoj vezi između ličnog računara i računskog centra banke preko zatvorenog mrežnog komunikacionog sistema banke, Intraneta. On-line bankarstvo omogućava obavljanje bankarskih transakcija direktnom vezom klijenta i banke uz pomoć specijalizovanog softvera. Softver se instalira na klijentov računar, tako da omogućuje elektronsko povezivanje korisnika sa računarom banke. Svi podaci o izvršenim nalogima se nalaze na personalnom računaru na kome je instaliran softver. Za funkcionisanje on-line bankarstva koristi se direktna on-line komunikaciona veza između personalnog računara i računskog centra banke uz korišćenje modema i to preko Intraneta. On-line bankarstvo je veću primenu našlo kod pravnih lica, nego kod fizičkih lica.

Softver za on-line bankarstvo starije generacije, zahtevao je visok nivo poznavanja računara i iskustvo korisnika. Sadašnji programi koji se koriste za obavljanje on-line bankarskih transakcija postali su lakši za upotrebu, zbog toga što se implementiraju u standardni Windows grafički korisnički interfejs, koji pruža korisnicima dobro poznate komande i funkcije. Najveći napredak postignut je zahvaljujući firmi Microsoft, koja ima više iskustva od velikih banaka u pisanju softvera za klijente. Proizvođači softvera preuzeli su na sebe ulogu premošćavanja jaza između banaka i klijenata i omogućili su i manjim bankama da ponude proizvode on-line bankarstva putem softverskih rešenja (npr. Halcom-ovo rešenje za On-line bankarstvo za pravna lica). To je dovelo do izvesnog stepena uopštavanja on-line bankarstva, tako da ono više ne predstavlja proizvod kojim bi neka banka mogla da se diferencira od druge.

Pri obavljanju bankarskih transakcija u on-line bankarstvu:⁴⁵

1. potreban je specijalan softver koji se ugrađuje u računar klijenta;
2. klijent je ograničen na obavljanje transakcija sa sopstvenog računara;

⁴⁴ Izvod sadrži podatke o obavljenom plaćanju, kao i način obavljenog plaćanja i služi kao dokaz o plaćanju u slučaju prigovora od strane korisnika ove usluge Banke.

⁴⁵ Stankić R.: „Elektronsko poslovanje“, cit. delo, str.98

3. klijent posluje sa dve strane: sa bankom i softverskom kompanijom koja instalira i održava softver;
4. klijentovi podaci o bankarskim transakcijama ostaju na hard disku i nisu otporni na eventualne napade iz okruženja (mogućnost pljačke, ubacivanje računarskih virusa...);
5. potreban je novac za kupovinu softvera;
6. potrebno je vreme za instaliranje softvera, kao i vreme za ovladavanje programima.

Usluge, koje su 24 sata dostupne, su:

1. pristup stanju na tekućem računu i kreditnim karticama,
2. plaćanje računa,
3. planirano i zakazano plaćanje za određeni termin koje će se izvršiti automatski,
4. prenos novca sa računa na račun i
5. usluge vođenja finansija za šta je potreban dodatni softver.

Većina banaka u domicilnom okruženju koristi e-banking rešenja slovenačke softverske kuće Halcom. Jedna od prvih banaka iz domicilnog okruženja, koja je omogućila elektronsko bankarstvo jeste tadašnja Novosadska banka. Elektronsko bankarstvo, pod nazivom Novoklik, namenjeno je za pravna lica, klijente banke. Da bi klijent koristio Novoklik, potrebno je da instalira softver na svoj personalni računar. Pored toga potrebno je da korisnik poseduje čitač smart kartice i smart karticu (na kome se nalazi digitalni sertifikat). Čitač smart kartice priključen je na personalni računar. Za ulaz u program potrebno je staviti smart karticu u čitač i upisati lozinku. Aktiviranjem digitalnog sertifikata sa smart kartice ostvaruje se konekcija između korisnika i Banke. Ukoliko klijent izgubi karticu i ako je nalazač pokuša upotrebiti, kartica se sama uništi nakon tri pokušaja upisa pogrešne lozinke.⁴⁶

Nedostaci on-line bankarstva, poput ograničenja za obavljanje transakcija sa samo onog računara na kome je instaliran skupi softver, potrebno vreme za obuku za rad, kao i nezaštićenost podataka na hard disku korisnika na napade iz okruženja, okrenuli su veliki broj korisnika ka Internet bankarstvu.

3.5.3. Internet bankarstvo

Poslednju deceniju prošlog veka karakteriše ekspanzija Interneta u svim porama društva. Internet je, pojavom *e-commerce-a* i *e-banking-a*, milionima korisnika širom sveta promenio način kupovine robe i upravljanja njihovim finansijskim sredstvima. Internet sve značajnije utiče na način savremenog poslovanja i donosi nove izazove pred današnje banke. Postoji veliki broj zahteva koje treba ispuniti u cilju postizanja uspešnog poslovanja na Internetu, kao na primer, lakoća korišćenja aplikacija, sigurnost ličnih informacija, integracija sa postojećim sistemima, prihvatanje standarda otvorenih sistema itd.

Internet bankarstvo ili sajber bankarstvo (engl. *Cyber Banking*), predstavlja obavljanje bankarskog poslovanja direktno od kuće, posredstvom Interneta.

Pri obavljanju bankarskih transakcija u Internet bankarstvu:⁴⁷

1. nije potreban specijalni softver i ne postoje podaci uskladišteni na klijentovom hard disku, pa je veća sigurnost pri obavljanju transakcija,

⁴⁶ http://www.eccf.su.ac.yu/obavestenja/inf_u_finansijama.htm

⁴⁷ Stankić R.: „Elektronsko poslovanje“, cit. delo, str.99

2. pristup banci i računu je moguć sa bilo kog mesta na svetu, pod uslovom da na tom mestu postoji računar priključen na Internet,
3. banka brine o održavanju sopstvenog hardverskog i softverskog sistema zaštite,
4. moguće je i obavljanje on-line transakcija.

Internet nudi bankama veoma mnogo mogućnosti, mada se još uvek globalna mreža uglavnom koristi u promotivne svrhe.

Predviđanja su da će se ovaj vid bankarstva razvijati velikom brzinom. Internet bankarstvo je najjeftiniji oblik bankarskih usluga, dostupan 24 sata, praktično bez prostorne ograničenosti.

Internet bankarstvo predstavlja pribavljanje bankarskih informacija i realizaciju bankarskih transakcija preko Interneta. Internet bankarstvo je zasnovano na korišćenju *World Wide Web*⁴⁸, gde se korisniku omogućava direktan pristup putem web brauzera⁴⁹. 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.

3.5.3.1. Razvoj Internet bankarstva

Početak Internet bankarstva datira iz 1980. godine. Međutim, razvoj Internet bankarstva bio je spor sve do maja 1995. godine, kada banka *Wells Fargo* izrađuje prvi Web bankarski program za obavljanje poslovanja na Internetu. Iste godine osnovana je i prva specijalizovana Internet banka na svetu - *Security First Network Bank*, sa sedištem u Atlanti (SAD). Aprila 1996. godine registrovan je milioniti korisnik Internet bankarskih usluga u SAD. Krajem 1999. godine broj korisnika Internet bankarstva penje se na preko 10 miliona.⁵⁰

Razvoj Internet bankarstva i rast broja korisnika u tesnoj je vezi sa razvojem informacionih tehnologija.

Brže, sigurnije, lakše i jednostavnije poslovanje na Internetu, ciljevi su koje pred banke postavlja sve zahtevanije finansijsko tržište. Da bi se ovi ciljevi ispunili, u svetu se drastično povećava obim ulaganja u informacione tehnologije.

Razvoj Internet bankarstva tekao je u četiri faze:

1. Prva faza – sagledavanje prednosti, problema i nedostataka (na Internet su prvo izašle banke koje nemaju šta da izgube).
2. Druga faza – postavljanje informacija (oprezan pristup je i očekivan, jer poverenje sticano godinama ne sme se brzo prokockati nesmotrenim postupcima).

⁴⁸ World Wide Web (www/web) je globalna struktura za brz prenos informacija koja se sastoji iz sledećih elemenata: 1) Hypertext markup language (HTML)- formiranje web stanica i njihovo povezivanje, 2) Hypertext transfer protokol (HTTP)- protokol za komuniciranje između servera i čitača, 3) Common gateway interface (CGI)- za razmenu sa drugim serverima. Server predstavlja uređaj na koji su postavljene razne web stranice. Da bi korisnik upotrebio web, mora osim hardvera da poseduje Internet konekciju i web čitač.

⁴⁹ Web čitač-pretraživač (web browser) je softver za pretraživanje Interneta i čitanje strana na Internetu (npr. Netscape-Navigator, Mikrosft's Internet Explorer, Opera i dr.).

⁵⁰ http://www.eccf.su.ac.yu/obavestenja/inf_u_finansijama.htm

3. Treća faza – dvosmerna komunikacija (pritisak korisnika je bio ogroman, poseban pritisak su pravile virtuelne banke, tako da se moralo krenuti korak dalje).
4. Četvrta faza – omogućavanje transakcija (1995. godine prva virtuelna banka).

U samom početku pojavljivanja banaka na Internetu, banke su se predstavljale samo informativno. Takva jednosmerna komunikacija imala je uglavnom reklamni karakter. Kasnije, banke počinju sa dvosmernom komunikacijom sa klijentima i to putem e-mail-a, ili interaktivnim pristupom nekom servisu. Ovakav vid komunikacije, pored marketinškog aspekta omogućuje i raspolaganje dodatnim informacijama od strane klijenata. Nakon toga, banke su se opredelile za obavljanje bankarskih transakcija na Internetu i to predstavlja najviši nivo komunikacije banke sa svojim klijentima.

Platni sistemi i transakcioni mehanizmi danas naprosto ne mogu da zaobiđu Internet, koji se polako proširuje u sve ljudske aktivnosti. Većina banaka u SAD smatra Internet glavnim trendom, koji zahteva strateški odgovor. Procenjuje se da banke koje nude Internet bankarstvo već danas poseduju 40% depozitne baze u SAD.

Dva su osnovna razloga zbog kojih su banke zainteresovane za Internet bankarstvo:

1. Klijenti, koji će najverovatnije koristiti Internet bankarstvo, predstavljaju veoma zanimljiv segment tržišta, kako sa demografskog, tako i sa ekonomskog stanovišta, jer su korisnici Interneta uglavnom mlađi ljudi sa većim stepenom obrazovanja i većim prihodima od prosečnog klijenta;
2. Internet predstavlja vrlo efikasan i jeftin distribicioni kanal.

Širenjem primene Interneta i pojavom virtuelnih banaka, javio se pritisak na klasične banke da promene svoj pristup klijentima i poslovanje, jer su počele da gube klijente, poslove i profit, dok su sa druge strane virtuelne banke doživle uspeh. Opstanak klasičnih banaka je počeo da zavisi od njihove spremnosti da određeni deo poslovanja prenesu na Internet i pridruže se savremenom vidu poslovanja.

Platni sistemi i transakcioni mehanizmi danas naprosto ne mogu da zaobiđu Internet, koji polako proširuje sve ljudske aktivnosti. Internet je učinio da kućno bankarstvo bude jednostavnije za primenu i jeftinije, budući da su ulaganja u opremu minimalna ako je korisnik već priključen na Internet. To sve nagoveštava da će veću perspektivu imati kod domaćinstava. Sa druge strane, troškovi po transakciji su najniži ako banka kao kanal za pružanje usluga koristi Internet.

Sve forme virtuelnog bankarstva zavise od podrške call centra. Ova podrška je od izuzetne važnosti i kod Internet bankarstva. Pri korišćenju Internet bankarstva, klijenti imaju dosta pitanja, a posebno oko njima nepoznatih procedura. Banke koje pružaju usluge Internet bankarstva bi trebalo da omoguće da klijenti mogu da šalju e-mail poruke call centru, sa web sajta banke. Sledeći korak će verovatno biti uspostavljanje *chat room-a*, gde klijenti mogu obavljati konverzaciju sa bankarskim službenicima.

3.5.3.2. Nivoi razvoja bankarskog prisustva na Internetu

Postoje tri nivoa razvoja elektronskog bankarstva, odnosno Internet prisutnosti banke.⁵¹

1. Prvi nivo Internet prisutnosti je uspostavljanje sajta banaka sa ciljem informisanosti potencijalnih korisnika bankarskih usluga o pogodnostima i servisima koje banka pruža. Sajтови banaka, sa korisnim i rafiniranim sadržajima, motivišu Internet posetioce sajta da, po potrebi, odu do banke i obave željenu transakciju. Za dodatne informacije o uslugama koje banka pruža, i uslovima pod kojima radi, na raspolaganju je Internet servis e-mail (elektronska pošta). Na specifična pitanja interesanata – Internet posetilaca sajta banke - postoji mogućnost odgovora elektronskim pismom, ili ukazivanje na deo sajta gde se nalazi odgovor. Na ovom nivou, Internet posetilac može biti informisan o banci i poslovanju banke i postati klijent banke.
2. Drugi nivo Internet prisutnosti obuhvata sve elemente prvog nivoa i omogućava korisniku uvid u stanje njegovog računa, kao i praćenje promena na računu kroz raznovrsno uređene izveštaje o obavljenim transakcijama. Bankarski sajt na ovom nivou postaje ljubazni šalterski radnik, koji non-stop opslužuje klijentelu širom sveta.
3. Treći nivo Internet prisutnosti uključuje sve funkcije prethodna dva nivoa i dodaje ključne usluge – mogućnost izvršavanja transakcija interaktivno sa korisnicima i klijentima banke. Korisnik sada može preko Interneta izdati nalog za transfer novca sa svog računa na neki drugi račun i to preko Internet čitača kojim posmatra bankarski sajt. U daljem razvoju elektronskog bankarstva, banka komunicira sa drugim bankama preko Interneta i postaje deo globalnog bankarskog sistema. Odnosno, Internet pruža mundijalnost poslovanja: ceo svet može videti banku preko bančinog Web site-a i banka vidi ceo svet preko Internet servisa *www (Word Wide Web)*.

Prvi nivo ne iziskuje velike troškove uspostavljanja i eksploatacije. Drugi nivo zahteva više truda i stručnosti. Treći nivo Internet prisutnosti modernog elektronskog bankarstva je najosetljiviji i njegova implementacija zahteva krajnje ozbiljan i profesionalan pristup u implementaciji. Njemu se pristupa tek kada je obezbeđen dobro obučen tim radnika i sve pretpostavke Internet infrastrukture (dobri računari, kvalitetne telefonske linije ili kablovi kojima se vezuje na Internet itd).

3.5.3.3. Vrste usluga Internet banaka

Banke su shvatile da nije dovoljno da imaju samo Internet prezentacije koje dobro izgledaju. Danas se postavljaju dodatni zahtevi da prezentacije moraju da pruže i nešto više, da budu interaktivne, multimedijalne i da omogućavaju kompletno poslovanje direktno na Internetu. Zbog toga su banke u svoje Internet poslovanje uvele niz inovacija (virtuelne poslovnice, specijalne finansijsko - softverske programe koji brinu o budžetu klijenta, ulaganjima ...). Ipak, i pored pomenutih inovacija ponuda bankarskih proizvoda i usluga je gotovo uniformna. Na primer, banke sa područja SAD, posluju isključivo sa rezidentima SAD u američkim dolarima i ne obavljaju menjačke poslove, dok evropske banke imaju liberalnije uslove poslovanja i u svom Internet poslovanju one mogu obavljati i poslove menjačkog karaktera, kao i poslove sa rezidentima drugih država.

⁵¹ <http://www.psee.edu.cg.yu/Voluee/20x.pdf>

Tabela 2: Deset vodećih Internet banaka

RANG	BANKA
1.	Security First Network Bank
2.	Wells Fargo
3.	Net.B@nk
4.	First Internet Bank of Indiana
5.	WingspanBank.com
6.	CompuBank
7.	Bank One
8.	Citibank
9.	USAccess Bank
10.	Huntington

Bankarski poslovi i usluge koje nudi većina svetskih banaka u svom Internet poslovanju su:⁵²

1. Menjački poslovi,
2. Otvaranje i korišćenje zajmovnog računa (engl. *Loan account*),
3. Provera stanja na računima klijenta,
4. Otvaranje i korišćenje čekovnih računa,
5. Plaćanje računa elektronskim putem,
6. Korišćenje sistema kreditnih kartica (*Visa, Master Card...*),
7. Trgovina hartijama od vrednosti,
8. Obustave plaćanja (engl. *Stop Payment*),
9. Otvaranje i korišćenje tekućih računa,
10. Provera transakcija iz prethodnog perioda na svim računima klijenta,
11. Elektronski transferi između računa,
12. E-mail korespondencija (dostavljanje svih najvažnijih informacija za klijentovo poslovanje poput: informacije sa svetskih berzi, informacije o aktivnostima banke, informacije o stanju klijentovih ulaganja ...),
13. Otvaranje i korišćenje depozitnih računa,
14. Obavljanje brokerskih usluga za klijente banke,
15. Odobravanje hipotekarnih i ostalih kredita,
16. Savetodavna funkcija.

U pokušajima da se izvrši sistematizacija usluga Internet bankarstva, izdvajaju se tri osnovne vrste usluga:

- a. Konsolidovanje računa i obavljanje plaćanja,
- b. Obavljanje finansijskog transfera između različitih računa i
- c. Podnošenje aplikacija za kredite, osiguranja i slične usluge.

Prva vrsta usluga, koja je i najpopularnija, omogućava klijentima banke da izvrše konsolidaciju većeg broja računa koje plaćaju svakog meseca i da jedinstvenim nalogom izvrše skidanje sredstava sa svojih bankarskih računa. Druga vrsta usluga eliminiše potrebu za odlaskom u poslovnice ili ATM-ove za obavljanje prenosa sredstava. Slične efekte u smislu uštede vremena klijenata ima i treća vrsta usluga.

Bankarsko poslovanje na Internetu je brzo, efikasno i ekonomično. Otvaranje računa u Internet bankama je potpuno besplatno. Provizije za plaćanje računa elektronskim putem su

⁵² Stankić R.: „Elektronsko poslovanje“, cit. delo, str.102

minimalne ili u većini Internet banaka potpuno besplatne. Ostale provizije za Internet bankarske proizvode i usluge su identične ili manje od provizija u takozvanom tradicionalnom (filijalnom) bankarstvu.

Plaćanje računa preko Interneta elektronskim novcem ili pametnim karticama (engl. *Smart Cards*) je nova aktivnost koju Internet banke omogućavaju svojim klijentima.

Kao primer Internet bankarstva u domicilnim uslovima može poslužiti web banka Erste Bank a.d. Novi Sad pod nazivom NotoNet, koje u osnovi predstavlja Halcom-ovo rešenje. Ona pruža uslugu web, odnosno Internet bankarstva, koja je namenjena fizičkim licima klijentima Banke. Putem ovog savremenog vida poslovanja, Banka omogućava vlasnicima tekućih računa da svoje poslovanje sa Bankom obavljaju elektronskim putem. To znači da je klijentima omogućeno plaćanje računa, uvid u stanje na računu i poslovne promene na računu. Ovde se može izvršiti podela na plaćanje komunalnih računa (struja, voda, grejanje ...) koja je dostupna svima (bez posebnog zahteva korisnika) i plaćanje tzv. specijalnih računa na zahtev klijenta. U ovom slučaju klijentu se na lični zahtev u aplikaciji odobrava plaćanje određenih računa, na primer, usluga KDS-a, Mobtel-ovih računa ili uslugama određenim radnjama, udruženjima itd.⁵³

Klijentima Erste Bank a.d. Novi Sad je omogućen pristup NovoNet-u na dva načina: putem korisničkog imena i lozinke, odnosno smart kartice. Pristup korisničkim imenom i lozinkom omogućuje korisniku da vrši pregled stanja i prometa po računu već uvedenih primalaca (javna komunalna preduzeća), kao i registraciju i zatim i plaćanje primaoca za koje korisnici iskazu potrebu (koje registruju prema svojim ličnim potrebama, kao na primer, kablovski distributivni sistem). Navedeni način pristupa daje niži nivo zaštite u odnosu na pristup pomoću, na primer, smart kartice, ali sa druge strane ukoliko, eventualno, dođe do nedozvoljenog otkrivanja korisničkog imena i lozinke od strane neovlašćenog lica, prenos sredstava, odnosno plaćanja se mogu izvršiti samo na već unapred definisane račune, što smanjuje mogućnost zloupotrebe.

Glavna razlika u upotrebi korisničkog imena i lozinke u odnosu na upotrebu smart kartice, osim u nivou zaštite, jeste što se putem korisničkog imena i lozinke može pristupiti web banci sa bilo koje lokacije u svetu gde postoji računar sa pristupom na Internet. Sa druge strane, smart karticom se može pristupiti samo na mestima gde na računu postoji čitač kartice. Pored navedenog, upotrebom smart kartice se mogu obavljati plaćanja primaocima koje nije potrebno prethodno registrovati.

3.5.3.4. Korišćenje elektronskih čekova u Internet bankarstvu

Elektronski ček (engl. *e-check*) je trenutno u pilot fazi u SAD. Očekuje se da će u narednih nekoliko godina biti detaljno testiran i da će biti ponuđen širem tržištu.

Osnovne pogodnosti koje pruža ovaj elektronski način plaćanja su sledeće:⁵⁴

1. uravnotežuje platni sistem,
2. uklapa se u postojeću bankarsku praksu,

⁵³ Jedini problem za sve korisnike Web bankarstva može nastati što se ne može dobiti pečatom potvrđenu uplatnicu. Potvrdu o plaćanju korisnik može odštampati u vidu uplatnice, a ukoliko se od njega zatraži da priloži prvi primerak uplatnice, primalac može da informacije sa „uplatnice“ proveriti u svojoj banci.

⁵⁴ Stankić R.: „Elektronsko poslovanje“, cit. delo, str.107

3. funkcioniše na isti način kao i papirni ček, samo u elektronskoj formi i sa manje potrebnih koraka,
4. napravljen je da odgovori potrebama banaka i korisnika njihovih usluga, koristeći najnovije metode tehničkog obezbeđenja sigurnosti,
5. mogu da ga koriste svi koji imaju otvoren tekući račun.

Predviđa se da će e-check biti jedan od najznačajnijih instrumenata za prelazak sa tradicionalnog bankarskog poslovanja u svet elektronske razmene. On se definiše kao elektronska verzija, ili predstavnik papirnog čeka.

Elektronski i papirni ček sadrže iste informacije, bazirani su na identičnim pravnim osnovama i koriste se za iste namene, kao što se ček i do sada koristio.

Osobine elektronskog čeka su:⁵⁵

1. može da se momentalno razmeni između dviju strana,
2. povećava broj i kvalitet funkcija koje banka nudi korisnicima tekućih računa,
3. daje mogućnost da se upravlja bankarskim transakcijama, ali je ipak dovoljno siguran da može da se koristi preko Interneta,
4. pruža neograničenu mogućnost prenosa informacija, ali je ipak dovoljno kontrolisan,
5. značajno smanjuje mogućnost pronevera,
6. pruža mogućnost automatske verifikacije sadržaja i važenosti,
7. moguće je stornirati i stanje na računu vratiti u prethodno,
8. minimizira početne izdatke za banku, jer softver i hardver nisu preterano skupi,
9. odgovara svim postojećim industrijskim standardima.

Elektronski ček je baziran na:

1. posebnom finansijskom softveru – *the Financial Services Markup Language (FSML)*,
2. digitalnom potpisu koji koristi bilo koji do sada proizvedeni algoritam,
3. sigurnim zamenama novca, kao što su pametne kartice,
4. dosadašnjoj bankarskoj i poslovnoj praksi.

Kao što se iz svega navedenog može zaključiti, e-check je baziran na pozitivnim iskustvima papirnog čeka, s tim što maksimalno unapređuje brzinu, sigurnost i omogućava korišćenje savremene tehnologije.

3.5.3.5. E-cash u Internet bankarstvu

E-cash je novi koncept u sistemu on-line plaćanja, koji pokušava da zameni papirni novac. Gotovina još uvek predstavlja najviše korišćeni instrument plaćanja, iako je prošlo već 30 godina od početka razvoja elektronskog načina plaćanja.

Da bi zamenio gotovinu, elektronski novac mora da ima:

1. monetarnu vrednost,
2. mogućnost zamene sa drugim instrumentima plaćanja,
3. sigurnost izdavanja.

⁵⁵ Isto, str.108

Jedan od primera uređaja koji čuvaju e-cash je Mondex kartica. E-cash se zasniva na kriptografskom sistemu zvanom digitalni potpis. Lice koje želi e-cash može da ga kupi papirnim novcem, ili preko svog računa ako ima sredstva. Primer korišćenja e-cash za plaćanje u raznim valutama je Visa kartica, gde su Visa centri u raznim zemljama povezani on-line sa centralnim bankama u svim državama. Potrošač koristi e-cash softver da generiše slučajan broj koji predstavlja novac.

Banka koristi privatni ključ da prikaže za koji račun i koji iznos treba da izda banknote. U slučaju DigiCash-a, korisnici imaju račun u digitalnoj banci (First Virtual Bank) na Internetu. Korisnik zahteva određeni iznos koji predstavlja sumu novčanica određene nominacije. Zahtev za novac koji se traži šalje se u digitalnu banku. Banka dekodira šifru sa tajnim ključem i odobrava iznos⁵⁶.

3.5.3.6. Pametne kartice u Internet bankarstvu

Smart ili pametna kartica je mikroračunar veličine standardne bankarske kartice koja u sebi sadrži:

1. jedno ili više integrisanih kola, među kojima se nalazi i mikroprocesor,
2. memoriju tipa EPROM (*Erasable Programmable Read-Only Memory*) ili EEPROM (*Electrically Erasable Programmable Read-Only Memory*) za smeštanje programa i podataka,
3. korisnički interfejs.

„Pametna“ kartica (inteligentna zamena za novac) je plastificirana kartica koja ima ugrađen čip sa integrisanim kolom. Ona omogućava memorisanje podataka i određena izračunavanja.

Inteligentne (smart) kartice imaju veliki potencijal kao prenosni uređaj, kao nosioci tzv. „AA“ (*Anytime Anywhere*) elektronskog bankarstva (nova, šira koncepcija elektronskog bankarstva). Najveća prednost inteligentne kartice jeste njena multifunkcionalnost, a njena prava vrednost je u kombinaciji njenih funkcija. Inteligentna kartica omogućava potrošačima da potpuno odvojeno i bezbedno drže veći broj aplikacija na jednoj jedinoj kartici. Danas su na raspolaganju brojne aplikacije za inteligentne kartice, pa tako jedna jedina inteligentna kartica može da služiti kao identifikaciona kartica za dokazivanje identiteta njenog vlasnika. Takođe, smart kartica može da se koristi kao kreditna, odnosno debitna kartica, novčanik za uskladištenje elektronskog novca. Sve navedene funkcije zahtevaju da se poverljivi podaci smeste u karticu.

U bliskoj budućnosti se očekuje da će klasična magnetna kartica biti integrisana i zamenjena sa vešenamenskom smart karticom.

Fizička struktura smart kartice je specificirana od strane Međunarodne organizacije za standardizaciju (ISO).

⁵⁶ Isto, str.109

3.5.3.7. Šifrovana kreditna kartica (World Wide Web Forma)

Prve kompanije koje su prihvatile ovaj način plaćanja preko Interneta su *First Virtual* i *Open Market*.

Kupovina on-line preko Interneta odvija se u sledećim fazama:⁵⁷

1. Potrošač pristupa serveru OTPP (*on-line Third Party Processors*) popunjavanjem registracionog formulara (Informacije o potrošaču).
2. Kupac šalje preko Interneta svoj OTPP broj računa.
3. Prodavac kontaktira OTPP server preko broja računa kupca.
4. OTPP server verifikuje broj računa.
5. OTPP server šalje izveštaj kupcu (elektronska poruka – WWW forma, e-mail).
6. Prodavac odobrava kupovinu, ili odbija u zavisnosti od odgovora servera.
7. Kupac preko čitača kontaktira server prodavca preko URL-a (HTTP server).

U budućnosti ovaj način plaćanja će zauzimati značajno mesto u elektronskom sistemu plaćanja.

Konkurentska borba između konvencionalnih i elektronskih mehanizama plaćanja biće sve oštrija, ali je potpuno jasno da gotovinska plaćanja neće u potpunosti nestati iz upotrebe, zbog svoje jednostavnosti, fleksibilnosti i anonimnosti, mada će se značajan deo plaćanja koja prati obimna dokumentacija u bliskoj budućnosti obavljati isključivo elektronskim putem.

One banke koje ne uspeju da održe korak sa razvojem informacione tehnologije, mogle bi da izgube deo svojih klijenata, smanje svoje poslovanje i ostanu bez većeg profita.

Pojavom sve većeg broja novih kanala za obavljanje bankarskog poslovanja i približavanjem usluga korisnicima, broj obavljenih transakcija će rasti. Mogu ih inicirati različita lica sa najrazličitijih lokacija, korišćenjem brojnih medija, čiji izbor zavisi od prirode plaćanja i pogodnosti u datom momentu. Banke moraju ne samo da prate razvoj i ulažu u novu tehnologiju, već i da koordiniraju i kombinuju pružanje svojih usluga, koristeći veći broj različitih kanala distribucije.

Aдекватna primena savremene informacione tehnologije i informacionih sistema u bankarstvu, a naročito korišćenje Interneta kao globalne računarske mreže i mogućnosti za poslovanje na globalnom nivou, obezbeđuje bankama konkurentnu tržišnu poziciju i dugoročnu poslovnu egzistenciju.

3.6. Mobilno bankarstvo

Mobilno bankarstvo (engl. *Mobile Banking*) je najnoviji trend u razvoju elektronskog bankarstva. Prognozira se da će mobilno bankarstvo doživeti čak i snažniju ekspanziju od Internet bankarstva u narednih tri do pet godina.

Mobilno bankarstvo omogućava transakcije putem prenosnih računara (engl. *lap-top*), digitalnih ličnih organizacija (*PDA*) i mobilnih telefona, koji su opremljeni specijalnim softverom za mobilni pristup Internetu, što znači da korisnik može pristupiti svojoj

⁵⁷ Isto, str.110

finansijskoj instituciji pomoću mobilnog telefona i izvršiti željene transakcije. Mobilna plaćanja putem mobilnih telefona (engl. *Mobile payments/M-payments*) spadaju u grupu plaćanja na malo. Mobilni telefoni mogu biti uređaji kojima se obavlja plaćanje u sadejstvu sa drugim uređajima (npr., kao što je slučaj kod plaćanja mobilnim telefonom na POS terminalima⁵⁸) ili se plaćanje može obaviti samo upotrebom mobilnog telefona.

Učesnici u mobilnim plaćanjima su: korisnici, mobilni operateri, banke i trgovci. Sve transakcije se obavljaju na liniji korisnik-trgovac. Između njih dolazi do razmene novca i robe, ali su mrežni operater (prenosni kanal) i finansijska institucija (finansijski kanal) neophodni činioci poslovanja.

Korisnik je najznačajniji učesnik ovog poslovanja. Svi servisi su namenjeni njemu i on je taj koji plaćanjem svojih troškova izdržava mrežu. Korisnik, prvo, očekuje da mu sistem obezbedi neophodan minimum sigurnosti poslovanja i da ga zaštiti od krađe. Drugo, korisnik očekuje da njegova privatnost ne bude narušena i da niko nema mogućnosti da prati njegove transakcije. Treće, očekuje se od sistema da je lak za upotrebu. Ovaj zahtev je u suprotnosti sa prethodnim, jer što je sistem više zaštićen to je i njegovo korišćenje komplikovanije, posebno ako je za zaštitu potreban dodatni uređaj.

Da bi korisnik učestvovao u sistemu mobilnog poslovanja mora posedovati odgovarajući uređaj i mora imati konekciju ka mreži.

Mobilni operater je posrednik u poslovanju i ima zadatak da prihvati signal od korisnika i da ga prosledi dalje ka mreži. On mora da obezbedi mečupovezanost sa ostalim učesnicima u poslovanju, a to podrazumeva da u potpunosti mora da ispoštuje standarde poslovanja. Mora takođe da obezbedi prohodnost ka drugim mrežama.

Banka je posrednik u poslovanju i ima najteži zadatak. Pre svega mora da obezbedi autentifikaciju (prepoznavanje) korisnika. Potom, da obezbedi proveru stanja na računu korisnika, a zatim izda odobrenje za plaćanje ili odbijanje. Neophodno je da obezbedi da poruka tokom transporta ne bude presretnuta ili izmenjena, drugim rečima, mora da obezbedi potpun integritet finansijske transakcije. Autentifikacija i integritet treba da obezbede da korisnik ne može da odbije transakciju ukoliko je ona pravilno izvedena. Sve ovo ima za cilj da se mogućnost zloupotreba i krađesvede na minimalnu moguću meru.

Trgovac ili davalac usluga je drugi učesnik u poslovanju. Pre svega treba da obezbedi robu i usluge koje će naplaćivati preko mobilnih servisa. Za njega je sistem plaćanja od životnog interesa, jer na taj način realizuje svoj poslovni model. Mora da obezbedi sistem plaćanja, od njega se uglavnom naplaćuje provizija. Trgovac u okviru svog modela poslovanja, mora da obezbedi da korisnici lako i jednostavno pristupaju servisima koje on nudi, da reklamira servise i uopšte ponaša se poslovno u odnosu na svoje korisnike.

U našem okruženju, mogućnost obavljanja transakcija s mobilnog telefona je ponudila Privredna banka Zagreb a.d., koja je u partnerstvu s hrvatskim Telekomom predstavila mPay uslugu. Usluga mPay nudi mogućnost jednostavnog, bezgotovinskog plaćanja robe i usluga putem mobilnog telefona, na više od 2000 prodajnih mesta u Hrvatskoj koja su označena znakovima prihvatanja mPay usluge. Uskoro će se mPay koristiti i pri plaćanju komunalnih

⁵⁸ Potrošači mogu realizovati plaćanje ako imaju odgovarajući mobilni aparat, ako njihov operater mobilne telefonije omogućava primenu ovih dodatnih usluga, ako imaju račun u banci kojim je moguć bežični pristup, uz dopuštenje banke i ako trgovci imaju razvijen sistem kojim se primaju bežična plaćanja (u slučaju da se plaća za robu iz trgovine).

računa, kao i za kupovinu putem Interneta. U drugoj fazi, mPay usluga omogućiti će i korišćenje niza bankarskih usluga putem mobilnog telefona.

U početku su se mobilna plaćanja obavljala razmenjivanjem SMS poruka između klijenata i banke. Razvojem WAP standarda koji je omogućio pristup Internetu sa mobilnog telefona, bilo je moguće koristiti sve prednosti on-line bankarstva. To znači da je klijentima banke omogućeno da uz pomoć mobilnog telefona, a putem Interneta pristupe svom računu u banci. Konekcija sa bankom se ostvaruje putem mobilnog telefona koji u sebi ima ugrađen WAP uređaj. Da bi mogla da se koristi WAP usluga bilo koje banke, korisnik mora da ima WAP prilagođeni uređaj (mobilni telefon). Pri svemu tome korisnik jedino plaća utrošene impulse operatoru mobilne telefonije.

Faktori koji utiču na dinamičan razvoj mobilnog poslovanja su:⁵⁹

1. relativno mala ulaganja,
2. jednostavni uređaji i laki za upotrebu,
3. omogućavaju veći komfor u korišćenju.

Faktori koji utiču na usporavanje dinamičkog razvoja su:

1. nesigurnost potrošača da šalju podatke preko mobilne mreže,
2. nepostojanje jedinstvenih standarda u ovoj oblasti i sl.

Korišćenje mobilnog bankarstva putem mobilnog telefona je sasvim jednostavan proces. M-banking predstavlja uslugu Internet bankarstva na mobilnom telefonu. Nakon obavljene registracije, korisnik putem SMS-a dobija potvrdu registracije usluge, svoj PIN i uputstvo za korišćenje. Ovakav sistem mobilnog plaćanja izuzetno je jednostavan i siguran, budući da transakciju korisnik autorizuje svojim ličnim PIN-om. Korisnik se putem mobilnog telefona uključuje na Internet i ulazi u aplikaciju. U aplikaciji, korisniku je omogućeno da vrši odabir određene usluge banke (na primer, pregled stanja računa, vršenje plaćanja, pregled uplata i isplata po svim računima, oročavanje sredstava, poručivanje čekova, kursna lista, kalkulator valuta i sl.).

U Singapuru, korisnici mogu da proveravaju stanje na svom bankovnom računu, vrše transfer novca sa računa na račun i vrše plaćanja.

U SAD-u se nudi kompletna trgovina akcijama, počev od vrednosti akcija do ponude i verifikacije trgovine preko mobilnih uređaja.

U domicilnim uslovima, nekoliko banaka je najavilo uvođenje mobilnog bankarstva, a Halcom je još pre godinu dana prezentovao odgovarajuće rešenje.

Za korisnika prednost korišćenja mobilnih uređaja pri obavljanju bankarskih transakcija ogleda se u sledećem:⁶⁰

⁵⁹ Bjelić P.: „Mobilni telefon kao kanal elektronskog poslovanja“, Ekonomski anali br.151-2, oktobar 2001.-mart 2002., str.95

⁶⁰ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit. delo, str.338

Lična nezavisnost

- Kontrola od strane korisnika.
- Preko mobilnog telefona se dolazi do seta personalizovanih usluga korisniku.

Lako za korišćenje

- Spremno za upotrebu za nekoliko sekundi.
- Jednostavno korišćenje.
- Razumljiv korisnički interfejs.

Mobilnost

- Sposobnost komunikacije bilo gde i bilo kada.
- Korisnici mogu nositi mobilni uređaj svuda sa sobom.
- Platforma za lokalizovane usluge.

Sigurnost

- Čuvanje privatnosti.
- Mobilni uređaji podržavaju sigurne aplikacije.

Mobilno bankarstvo pruža mogućnost potpune fleksibilnosti, koristeći prednost socijalnog i tehnološkog razvoja.

Mobilno bankarstvo je novi kanal za usluge koje banke nude i platforma za nove buduće personalizovane usluge bazirane na informacijama u realnom vremenu koje stvaraju lojalnost i zadovoljstvo klijenta. Novi klijenti se mogu dobiti ukoliko se uvedu servisi i usluge, kao što su, na primer, pripaid kartice za mlađe ljude koji još uvek ne mogu da se kvalifikuju za kreditne kartice.

4. KONKURENCIJA TRADICIONALNIH I INTERNET BANAKA

Internet banke su lideri na elektronskom tržištu bankarskih usluga. Prema nekim predviđanjima, Internet banke će dobiti dominirajuću poziciju u bankarskom sistemu budućnosti.

Dosadašnja praksa je pokazala postojanje brojnih Internet banaka, ali je za sada njihova pozicija daleko od dominacije. One su najbrže napredovale osvajanjem posebnih „tržišnih niša“. Konkretni primeri pokazuju (slično stanju elektronske trgovine na drugim tržištima) istovremeno postizanje značajnih uspeha, na jednoj strani, kao i pojavu kriza i potpunih kolapsa, na drugoj strani. Zbog toga je pred bankarskim ekspertima još uvek otvoreno pitanje mogućnosti Internet banaka da nadjačaju i nadmaše tradicionalno bankarstvo, koje posluje u okvirima postojećih regulativa. U tom kontekstu se nameće i pitanje mogućnosti njihovog samostalnog nastupa, kao pravila ili izuzetka.

Za prenos tehnologija plaćanja na Internet, smatraju se ključnim dva međusobno povezana razloga:

- a. troškovna efikasnost i
- b. konkurentski pritisak.

Troškovna efikasnost se objašnjava eliminisanjem troškova otvaranja i održavanja sistema filijala, jer klijenti mogu usluge da dobiju direktnom interakcijom sa računarskim sistemima. Internet banke koje posluju isključivo preko Interneta, bez fizičkih filijala, u cilju ostvarivanja

konkurentne prednosti na tržištu, deo ušteda postignutih ovim putem prenose na klijente kroz snižavanje provizija i kamatnih stopa. Neke idu čak do izbora koji su nezamislivi u tradicionalnom bankarstvu i nude izuzetno nizak depozitni minimum, usluge bez, ili sa veoma niskim provizijama i sl.

Pored Internet banaka, kao značajni konkurenti tradicionalnim bankama pojavljuju se i Internet kreditni brokeri (*Quicken Loans, E-Loan, Lending Tree, Majkrosoftov HomeAdviser*) koji nude softvere za kreditne aranžmane. Korišćenjem ovih softvera, klijenti su u mogućnosti da vrše izbor između ponuđenih kreditnih proizvoda i kreditora sa kojima broker ima uspostavljen ugovorni odnos. Najznačajniji prodor Internet brokeri su ostvarili na tržištima kreditnih kartica i hipotekarnih kredita. Na tržištu kreditnih kartica bili su posebno uspešni u uslugama konsolidovanja računa, zaduživanjem po osnovu korišćenja ovih kartica. Na ovom tržištu konkurentna borba sa bankama je slabije izražena, zbog toga što sami trgovci deluju kao marketeri banaka koje tradicionalno izdaju kreditne kartice.⁶¹

Konkurencija je mnogo više izražena na hipotekarnom tržištu, na kome Internet brokeri često zauzimaju mesto službenika na kreditnim šalterima tradicionalnih finansijskih institucija koje odobravaju hipotekarne kredite. Kada su 90-ih godina u SAD-u kamatne stope na hipotekarne kredite znatnije opale i kod stanovništva porasla zainteresovanost za ulaganja u stambenu izgradnju i rekonstrukciju postojećih objekata, pojavljuju se zastoje i uska grla kod tradicionalnih tehnologija odobravanja hipotekarnih kredita. Takva situacija mnoge podstiče da alternativno rešenje potraže na Internetu (prema podacima jednog Internet brokera mesečni broj posetilaca na web-u se sa 35.000 popeo na 500.000). Kasnije je došlo do opadanja interesovanja, a prema predviđanjima nekih analitičara za 10 godina najmanje 10% hipotekarnih kredita biće inicirano preko Interneta.

Globalna karakteristika nastupa Internet bankarstva prethodnog perioda je upravo opadanje samostalnog nastupa Internet banaka. Primeri za to su *WingspanBank.com* i *BankOne* koje se navode kao pioniri u Internet bankarstvu. Prva se bori za profit Internet bankarstva, kao poslovnica tradicionalne institucije, a druga nudi odvojene, selektivne online bankarske usluge, kao dodatak tradicionalnim bankarskim uslugama koje se već nalaze u ponudi.

U principu, Internet banke u samom startu očekuju privlačenje velikog broja korisnika i ostvarenje visokih profita. Prema prognozama nekih optimista trebalo je u 90-im da se preko 50% korisnika prebaci na korišćenje bankarskih usluga putem Interneta. Međutim, mnogobrojni izazovi koji su uticali na znatno slabije prihvatanje ovog načina korišćenja bankarskih usluga, uticali su i na otežavanje samostalnog nastupa individualnih Internet banaka.

Prvo, ove banke u startu klijentima nude prednost u odnosu na tradicionalne, a to se posle često pokazuje kao teško održivo.

Drugo, kod jednog broja klijenata je veoma izražena potreba da prilikom korišćenja usluga, uspostavljaju kontakt sa službenikom banke licem u lice. Neke banke su u svom iskustvu imale primere da su klijenti imali potrebu da putuju kako bi videli fizičku poslovnicu banke preko koje će slati svoja sredstva.

⁶¹ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.186

Treće, ako Internet banke počinju kao potpuno nove, da bi bile uspešne u kratkom roku treba brzo da privuku klijente. Da bi to ostvarile, potrebne su im konkurentne prednosti u odnosu na već postojeće banke. Njih grade na bazi komparativnih troškovnih prednosti online usluga i ponudi viših kamatnih stopa na depozite (ponekad i do 20% iznad prosečnih kamatnih stopa tradicionalnih banaka).

Četvrto, Internet banke treba da ulože veliki napor da bi mogle da ponude pun obim bankarskih proizvoda koji tradicionalne banke u svojoj ponudi već imaju.⁶²

Konkurencija sa tradicionalnim bankama pokazala se znatno težom nego što je prvobitno bilo procenjeno. Kada je ranih 90-tih u *Wall Street Journal-u* objavljena serija rasprava o pitanjima budućnosti bankarstva, ocenjeno je da se tradicionalne banke nikada neće prilagoditi izazovima informacione tehnologije. Međutim, u praksi se kasnije dešavalo upravo suprotno i tradicionalne banke postaju oštri konkurenti na elektronskom tržištu. Gotovo svuda u svetu, ove banke dodaju online bankarske usluge svojim postojećim bankarskim proizvodima. Znači, online bankarske usluge počinju da prožimaju čitav bankarski sektor, da li kroz dalji razvoj tradicionalnih banaka ili uvođenjem novih Internet banaka. U takvim uslovima, Internet banke se u samom startu, susreću sa konkurencijom prethodno osnovanih tradicionalnih banaka. Istovremeno, to ih onemogućava da obezbeđuju sebi konkurentne prednosti po osnovu toga, što će se na finansijskom tržištu pojaviti kao institucije koje prednjače.

Suočene sa online konkurencijom tradicionalnih banaka, mnoge Internet banke se udružuju sa tradicionalnim bankama ili drugim institucijama i formiraju poslovne alijanse. Poznati primeri su poslovne alijanse *Netbank.com* sa *Fidelity Investments*, *Compubank.com* sa *General Electric* i *USABancshares.com* sa *Palm Pilot*. Ove banke nastavljaju samostalno da posluju sa svojim asortimanom usluga, a zahvaljujući partnerima omogućeno je da se izvrši proširenje ukupnog asortimana i time poveća konkurentnost u odnosu na tradicionalne banke.

Neke Internet banke nastoje da svoju konkurentsku poziciju obezbede prodorom na određene, specijalizovane tržišne segmente, odnosno formiranjem specijalizovanih „tržišna niša“. Tako npr. *Pointpathbank.com* je specijalizovana posebno za odobravanje hipotekarnih kredita za mlade braćne parove, *UmbrellaBank.com* za finansiranje renoviranja stambenog prostora stanovništva sa niskim nivoom zarada i sl.

Izgleda da nije moguće jasno uočiti pravac kretanja i sredstva koja tradicionalne i Internet banke koriste u svojoj konkurentskoj borbi, a još manje donositi definitivni sud u konačnoj pobedi jednih ili drugih („brick“ ili „click“). Neke Internet banke (*Everbank.com*, *Principal.com*) počinju da funkcionišu kao samostalni delovi ili filijale drugih finansijskih institucija, dok se druge približavaju tipu poslovanja tradicionalnih banaka. Tako ima i slučajeva da banke koje su poslovale isključivo preko Interneta, počinju da otvaraju svoje poslovnice (*VirtualBank.com*, *First-E.com*). Ovakva situacija daje osnova za procene koje ukazuju na mogućnost uspeha u oba domena, kako fizičkom, tako i virtuelnom (i „brick“ i „click“), pri čemu će on-line bankarstvo pratiti i dopunjavati usluge koje pružaju tradicionalne banke. U svakom slučaju, bankarske usluge su u procesu velikih promena, sve više usluga se nudi preko Interneta, pa će broj fizičkih filijala banaka verovatno opasti u budućnosti.

⁶² Isto, str.187

5. PREKLAPANJE POSLOVA I POJAVA NOVIH INSTITUCIJA

Kao članice monetarnog sistema, banke su uvek bile pod ozbiljnom monetarnom regulativom, a samo bavljenje bankarskim poslovima zahtevalo je dobijanje posebne dozvole. Danas banke nude sve veći broj online finansijskih usluga. One se često udružuju i sa nefinansijskim institucijama (*Microsoft, Intuit, General Electric*), a usluge koje ove institucije nude često su bliski supstituti bankarskih usluga.

Uticaj Interneta na promene u finansijskoj strukturi, manifestuje se prvenstveno kroz ubrzanje procesa koji su već otpočeli i u kojima su nebankarske finansijske institucije bile konkurenti bankama. Između različitih institucija došlo je do daljeg porasta delimičnog preklapanja aktivnosti, a različite finansijske institucije su sve više počele da liče jedna na drugu. *Merrill Lynch*, velika američka brokerska firma je i drugi po veličini investicioni fond, a sada postaje značajna i za poslove komercijalnog bankarstva, u svojoj ponudi ima račune sa mogućnošću korišćenja čekova, paket proizvoda koji omogućava klijentima da vrše online transfer između njihovih depozitnih računa, a od 1980. godine ulazi i u poslove kreditiranja SMEs. Danas *Merrill Lynch* ima reputaciju glavnog konkurenta na tržištu kreditiranja SMEs (tu oblast su svojevremeno neke veće banke ignorisale, a manje nisu mogle da je prihvate zbog nedostatka sredstava). Komercijalne banke takođe ulaze u zonu poslovanja koja je tradicionalno pripadala drugim finansijskim institucijama (npr. prodaja polisa osiguranja, udela u investicionim fondovima). Mnoge od njih omogućuju klijentima da vrše transfer sredstava između različitih računa putem Interneta.

Ovakve promene zahtevale su i odgovarajuće promene u zakonodavnoj regulativi, s obzirom na to da je tradicionalna zakonodavna regulativa koncipirana u skladu sa postojanjem suštinskih razlika između različitih institucija i oblasti njihovog poslovanja.

Postojeća konkurencija dobija dodatnu dimenziju u uslovima paralelne egzistencije tradicionalnog poslovanja banaka i poslovanja preko web-a, na Internetu (offline i online konkurencija). Kao posledica toga pojavljuje se u okviru istog zakona dozvola za osnivanje afilijacija između Internet banaka i nebankarskih finansijskih institucija kao što su brokerske firme, investicioni fondovi i osiguravajući zavodi. Ova dodatna legalizacija omogućava još intenzivniji razvoj opšte konkurencije, mada je pravo pitanje da li je i u kojoj meri ona samo iznućena mogućnostima koje su imanentne elektronskom poslovanju u ovoj oblasti.

Pojava online konkurencije, sa jedne strane, predstavlja pretnju za tradicionalno bankarstvo, a sa druge strane, izazov. Tako i u ovim relacijama počinje da dolazi do porasta delimičnog preklapanja u funkcijama i proizvodima, koji se prodaju kao vezani proizvodi istovremeno i putem tradicionalnih filijala i putem Interneta. Banke se preorjentišu na Internet prvenstveno zato što očekuju da će putem njega moći da ostvare dodatne izvore profita. U tom cilju, kao akt marketinga, uvode se i web bazirane „unakrsne prodaje“ odnosno, vrši se dodavanje novih finansijskih proizvoda postojećim klijentima. Angažujući se u unakrsnoj prodaji, banke „uvezuju“ finansijske proizvode u različite setove proizvoda koje prave za individualne korisnike, a klijenti dobijaju mogućnost da vrše izbor između različitih paketa. U okviru paketa često se vrši cenovna diskriminacija pojedinih usluga.

Kao konkurenti na elektronskom finansijskom tržištu pojavljuju se i nove nebankarske institucije koje postaju potencijalni provajderi nekih bankarskih usluga, tzv. agregatori

(Yahoo.com. AmericaOnline). Oni sa sobom donose nove Internet platforme koje pružaju prezentaciju ponuda finansijskih usluga i time direktno utiču na promenu postojećeg odnosa između banaka i njihovih klijenata. Neki online agregatori (Yodlee.com) sa korisnicima usluga ovog tržišta stupaju u posebne aranžmane prema kojima preuzimaju poslove prikupljanja svih online finansijskih podataka (npr. od njihovih brokera, osiguravajućih zavoda, penzionih fondova) i sve stavljaju na jedan sajt. Ovom uslugom korisnicima je omogućena dodatna ušteda vremena, jer se eliminiše potreba ulaska na različite sajtove u cilju samostalnog prikupljanja pomenutih podataka.

Obavljajući ove usluge, agregatori dobijaju pristup informacijama o finansijskim institucijama, vrsti usluga koje nude klijentima, kamatnim stopama koje plaćaju na depozite i naplaćuju na kredite, visini provizija i sl. Ovim oni ugrožavaju banke koje posluju preko web-a isto kao što to čine i web portali (Microsoft's MoneyCentral, Intuit's Quicken, Electric's GE financial Network) koji nude pojedincima upravljanje njihovim celokupnim finansijama na jednom web sajtu. Klijent dobija mogućnost da preko agregatora bira proizvode koje nude različite finansijske institucije, umesto da bira između različitih paketa koji se nalaze u ponudi njihove banke. Time se u velikoj meri relativiziraju naponi koje banke ulažu u formiranje web bazirane unakrsne prodaje.

Kao odgovor na ovako agresivan nastup agregatora, banke počinju agregatorima da uskraćuju pravo ulaska u određene sajtove klijenata ili postavljaju posebne sisteme zaštite. To sprovede ili putem uvođenja obaveza pristupanja posebnim ugovorima kojima se preciziraju posebni uslovi za identifikaciju, ili uvođenjem drugih zahteva za agregatore. Ovakvim ugovorima se, sa jedne strane, obezbeđuje dodatna zaštita informacija o klijentima, a sa druge strane, obezbeđuju uslovi bankama za sticanje preciznijeg uvida u oblasti interesovanja i aktivnosti agregatora. Naravno, ovi dodatni zahtevi donose sa sobom i dodatni porast troškova agregatora, koji se u krajnjem ishodu prevlađuju na korisnike preko cena.

U pogledu zakonodavnog tretmana poslovanja preko Interneta, SAD se zalaže za kompletnu kontrolu poslovanja, transakcija i podataka od strane državnih organa, a EU zauzima liberalniji stav koji teži istoj stavlja na zaštitu anonimnosti i privatnosti.

6. PREDNOSTI INTERNET BANKARSTVA

Bankarstvo se, kao poslovna oblast, veoma brzo globalizuje i u tom procesu se suočava sa snažnom konkurencijom na tržištima sveta, ne samo od drugih banaka, već i institucija koje posluju sa hartijama od vrednosti, osiguravajućih kompanija, kreditnih udruženja, finansijskih kompanija i hiljada drugih konkurenata na polju finansija. Sav ovaj finansijski potencijal nalazi se u procesu neprekidnog međusobnog približavanja, obavlja slične usluge i nudi ih klijentima. Banke i njihovi konkurenti prolaze i kroz proces tehnološke revolucije, pošto se upravljanje informacijama, proizvodnja i distribucija finansijskih usluga sve masovnije obavlja elektronskim putem. Elektronsko bankarstvo sve više uzima maha i sve više korisnika radije obavlja poslove sa bankom od kuće, ili sa posla nego u njenim ekspoziturama.

Pre pojave Interneta korisnik je morao da ode u banku da bi obavio posao. Sa Internetom, banka je došla kod korisnika u njegovu kuću, ili na radno mesto, to jest tamo gde se nalazi njegov računar.

Internet bankarstvo ima niz prednosti u odnosu na takozvano tradicionalno poslovanje banaka. Prednosti se uglavnom ogledaju u vremenskoj i prostornoj neograničenosti, brzini obavljanja transakcija, niskoj ceni i širokom asortimanu bankarskih proizvoda i usluga.

Prednosti poslovanja putem web banke su:⁶³

- a) mogućnost obavljanja poslova od kuće, ili sa bilo koje lokacije u zemlji ili svetu,
- b) ne postoji potreba odlaska na šalter banke,
- c) ušteda u vremenu i može u svoje slobodno vreme kreirati naloge,
- d) nije potreban specijalan softver i podaci nisu uskladišteni na klijentovom hard disku, što daje veću sigurnost pri obavljanju transakcija,
- e) prostorna neograničenost Internet bankarstva,
- f) jeftiniji način obavljanja poslovanja sa bankom – ušteda u novcu jer je usluga obavljena putem web banke jeftinija, nego usluga realizovana klasičnim metodama (na šalteru Banke). Provizije u Internet bankarstvu su, po pravilu, niže nego u klasičnom poslovanju (ili su potpuno besplatne),
- g) nema radnog vremena, odnosno mogućnost obavljanja poslova od strane klijenta sa bankom je 24 časa,
- h) brzina obavljanja transakcija, koja traje 1-3 minuta,
- i) ažurnost obaveštavanja o promenama na računu,
- j) jednostavnost priključivanja na web-banku,
- k) klijentu omogućuje tajnost podataka,
- l) lakoća upotrebe.

6.1. Radno vreme Internet banaka

Osnovna prednost Internet banaka je njihovo neograničeno radno vreme (24 sata, 7 dana u nedelji, 365 dana godišnje). U tradicionalnom bankarstvu za obavljanje bankarskih usluga non-stop bilo bi potrebno angažovati tri smene ljudi da svakodnevno radi 365 dana u godini i to u široko razgranatoj bankarskoj mreži. Potreban broj ljudi za obavljanje non-stop poslovanja bio bi veoma velik, kao i troškovi ovakvog načina poslovanja.

6.2. Prostorna neograničenost Internet bankarstva

Većina ljudi bira banku zbog blizine. Danas ljudi mogu imati banku unutar svog doma, bez obzira na to gde god da žive. Internet bankarsko poslovanje je moguće obavljati sa bilo kog mesta na svetu. Potrebno je da korisnik ima otvoren račun u nekoj banci koja pruža usluge Internet bankarstva, da na mestu iz kog obavlja poslovanje postoji računar sa pristupom Internetu i da korisnik zna sve šifre koje su mu potrebne za ulazak u Internet banku i njegov račun. U klasičnom bankarstvu korisnik je vezan za mesto i zemlju u kojoj postoje filijale banke u kojoj ima otvorene račune.

6.3. Brzina obavljanja transakcija

U klasičnom bankarstvu potrebno je utrošiti vreme za dolazak i odlazak u filijalu banke, zatim vreme za čekanje u filijalama, vreme za popunjavanje obrazaca, čekova i ostalih dokumenata, kao i vreme za obavljanje samih transakcija. Internet bankarstvo je daleko brži način za

⁶³ www.24x7.co.yu/default.aspx?cid=700&pid=banke-na-internetu

obavljanje bankarskog poslovanja. Za poslovanje u Internet banci potrebno je samo vreme za prijavljivanje u Internet banku i vreme za obavljanje bankarske transakcije.

6.4. Cena obavljanja bankarskih transakcija

Internet bankarstvo je najjeftiniji oblik obavljanja bankarskih transakcija. Provizije koje se plaćaju za obavljanje bankarskih usluga u Internet bankarstvu su, niže od onih u tradicionalnom bankarstvu. Preko elektronske banke, obrada platnih naloga je 10 do 15 puta niža od cene koja važi za konvencionalnu obradu. Naime, trošak za obradu elektronskih naloga ne uključuje zaposlene iza šaltera, troškove održavanja opreme, poštanske usluge, fiksne troškove i ostale troškove postupka. Pritisak na šaltere banke značajno opada uvođenjem kvalitetnog i rasprostranjenog elektronskog bankarstva.

Za obavljanje kvalitetnog bankarskog poslovanja u tradicionalnom bankarstvu je potrebno daleko više ljudi, poslovnog prostora i opreme, nego u Internet bankarstvu. Samim tim i troškovi obavljanja bankarskog poslovanja u tradicionalnom bankarstvu su daleko veći od onih u Internet bankarstvu.

Tabela 3: Troškovi bankarskog poslovanja

KANAL	TROŠKOVI PO TRANSAKCIJI
Filijala	1,070 \$
Telefon	0,540 \$
On-line bankarstvo	0,0150 \$
Internet bankarstvo	0,0100 \$

7. NEDOSTACI INTERNET BANKARSTVA

Nedostaci Internet bankarstva najviše su izraženi u odsustvu sigurnosti pri obavljanju poslovanja, nepostojanju zakonske regulative, nedostatku privatnosti, otuđenosti i odbojnosti prema inovacijama i opasnosti od zloupotrebe Internet bankarstva u kriminalne svrhe.

Sigurnost, odnosno nedostatak sigurnosti i sistemi zaštite na Internetu su ključni razlozi rasta i razvoja Interneta. Ti razlozi su veoma važni i za funkcionisanje i razvoj Internet bankarstva.

Sa rastućim publicitetom otvorenih mreža kao što je Internet i elektronskom razmenom informacija i novca između geografski udaljenih lokacija, obezbeđenje transakcija postaje od ključne važnosti. Banke koje koriste elektronsku razmenu podataka u zatvorenim mrežama (intranet) osiguravaju se utvrđivanjem identiteta i autorizacijom ljudi koji pristupaju mreži. U otvorenim mrežama, postojeći mehanizmi tehničke i pravne zaštite nisu dovoljni da spreče neautorizovan pristup i hakerske upade. Određenim kriptografskim tehnologijama koje uključuju digitalni potpis, definiše se nova infrastruktura čija je osnovna prednost viši nivo integriteta poruke i verifikacija pristupa.

Ovom tehnologijom šifriranje poruke obezbeđuje dve stvari za učesnike u razmeni:

1. da je njihova poruka osigurana i
2. da je druga strana autorizovana za pristup.

Šifrovanu poruku je teško falsifikovati, pa se očekuje da će tehnologija digitalnih potpisa biti primenjena i prilikom zaključivanja ugovora elektronskim putem.

7.1. Nepostojanje zakonske regulative

Globalni sistem komuniciranja, kakav je Internet, zahteva ađurne i adekvatne pravne okvire koji treba da definišu potrebe poslovnih subjekata i korisnika usluga. Zakonska regulativa u vezi Interneta i poslovanja na njemu, razlikuje se od zemlje do zemlje. Dva ekonomski najrazvijenija dela sveta SAD i Evropska unija imaju različite stavove po pitanju zakonske regulative na Internetu. Evropska unija ima daleko liberalnije stavove po pitanju privatnosti poslovanja od SAD. Usaglašavanje njihovih stavova o zakonskoj regulativi na Internetu, od velikog je značaja za kompletnu svetsku privredu.

Postoje dva moguća scenarija za rešenje zakonske regulative u poslovanju na Internetu.⁶⁴

Prvi scenario, za koji se zalađe Evropska unija, je liberalnog tipa i zasniva se na potpunoj anonimnosti i privatnosti poslovanja.

Drugi scenario, za koji se zalađe SAD, je zasnovan na kompletnoj kontroli poslovanja, transakcija i podataka od strane državni organa.

Potpuno anonimni sistem poslovanja na Internetu moguć je zahvaljujući sistemu šifrovanja podataka, uz pomoć koje je zagarantovana anonimnost u slanju svih poruka na Internetu. Na ovaj naćin, sistem štiti privatnost poslovanja pojedinca ili preduzeća, što je ujedno i osnovno pravilo bankarskog poslovanja i dobra strana ovog sistema. Sa druge strane, mane ovog sistema su što omogućavaju izbegavanje plaćanja poreza, carinskih obaveza, „pranje “ novca i prebacivanja kapitala u druge zemlje i to mimo znanja finansijskih, carinskih, poreskih i ostalih državni organa. Potpuno anonimni sistem Internet poslovanja, uz odsustvo zakonske regulative mogao bi uzdrmati ne samo državne organe, nego i ćitav bankarski sistem najrazvijenijih zemalja sveta. Bankarski sistemi SAD i Evropske unije bi bili ugrođeni zbog odliva velike kolićine kapitala u takozvane off-shore bankarske centre. To je doprinelo da Internet banke sa područja SAD mogu poslovati samo sa rezidentima SAD, unutar bankarskog sistema SAD i isključivo u amerićkim dolarima.

Drugi sistem rešenja zakonske regulative za poslovanje preko Interneta, zasniva se na kompletnoj kontroli i evidenciji transakcija i podataka na Internetu od strane državni organa. Ovaj sistem bi omogućavao državnim organima kompletan uvid u svaćiji bankovni raćun, u sve Internet transakcije i e-mail korespondenciju. Sloboda i privatnost pojedinaca kao i osnovna pravila poslovnog i bankarskog ponašanja ovim sistemom bi bila prekršena na najgori moguć naćin.

Pred vladama najrazvijenijih zemalja je zadatak da se slođe da li da redizajniraju monetarni i poreski sistem u skladu sa nastalim tehnološkim promenama, ili da naprave sistem u kome bi svako ulaganje, svaka kupovina, svaka transakcija svakog pojedinca i preduzeća bila praćena tokom ćitavog ćivota.

Oba prikazana sistema imaju dobre i loše strane. Kombinovanjem njihovih najboljih elemenata, dobilo bi se optimalno rešenje zakonske regulative za poslovanje na Internetu.

⁶⁴ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.105

Sigurno je da će još dosta vremena proteći dok se ne usaglase međunarodne zakonske regulative vezane za poslovanje pojedinaca i preduzeća na Internetu. Do tada, nedostatak međunarodne zakonske regulative onemogućavaće određene segmente poslovanja, dok će sa druge strane omogućavati primenu širokog spektra nezakonitih aktivnosti u poslovanju pojedinaca i preduzeća na Internetu.

7.2. Odbojnost prema inovacijama kao prepreka u razvoju Internet bankarstva

Inovacije i nove proizvode većina ljudi prihvata sa izvesnom dozom nepoverenja i nezainteresovanosti. Identična situacija je i sa Internetom i poslovanjem na njemu. Internet kao potpuno novi vid komuniciranja, u početku je prihvatio samo veoma uzak krug ljudi-inovatora i to prvenstveno naučnika, vojnih lica i univerzitetskih profesora. Vremenom je sve više ljudi koristilo Internet i pogodnosti koje on pruža. Biće potrebno još mnogo godina dok se Internet i poslovanje na njemu prihvati i implementira u svim delovima sveta.

8. MODELI ELEKTRONSKOG POSLOVANJA I ELEKTRONSKOG BANKARSTVA

Elektronsko poslovanje (engl. *electronic business*), predstavlja razmenu standardizovanih elektronskih poruka u obavljanju raznih poslova u kompanijama, bankama, upravi, aktivnostima građana i u svim drugim poslovnim transakcijama. Elektronsko poslovanje podrazumeva obavljanje poslovnih procesa uz primenu elektronske tehnologije. Ova vrsta tehnologije omogućava slanje velikog broja informacija, na velike daljine u kratkom vremenskom periodu. To omogućava kompanijama koje u svom poslovanju koriste elektronsku tehnologiju, da ostvare značajne uštede u troškovima poslovanja, efikasnije obave svoje zadatke i budu konkurentnije na tržištu. Pod uticajem primene elektronskog poslovanja reorganizuju se skoro sve delatnosti i tako danas imamo e-trgovinu, e-bankarstvo, e-upravu i sl.

Elektronsko poslovanje razvijalo se u dva pravca. Prvi je trebalo da omogući kompanijama da brže i lakše prenesu novac i informacije između sebe, odnosno bio je usmeren na saradnju dva pravna lica međusobno (kompanija, državne institucije), a drugi, noviji, predviđen za krajnje korisnike koji žele određeni proizvod ili uslugu.

Razvoj i primena elektronskog poslovanja moguća je jedino ukoliko su ispunjeni sledeći preduslovi⁶⁵:

1. razvijena primena Interneta,
2. usvojeni propisi o elektronskom poslovanju i elektronskom potpisu,
3. razvijena telekomunikaciona infrastruktura,
4. prihvatanje elektronskog poslovanja od strane rukovodstva,
5. finansijska ulaganja za uvođenje.

Elektronske transakcije se mogu obavljati između tri strane i to: vlada, kompanija i klijenata.

⁶⁵ <http://pravo.fon.bg.ac.yu/knjige> PDF/

Tabela 4: Elektronsko bankarstvo i trgovina i šira primena Interneta⁶⁶

	Vlada	Kompanija	Klijent
Vlada	G2G npr. koordinacija	G2B npr. informisanje	G2C npr. informisanje
Kompanija	B2G npr. komunikacija vlade sa poslovnim partnerima	B2B npr. elektronsko bankarstvo i trgovina	B2C npr. elektronsko bankarstvo i trgovina
Klijent	C2G npr. naplata poreza	C2B npr. upoređivanje cena	C2C npr. aukcijska tržišta

Najveći razvoj je iskazan u delu elektronskih transakcija koje se obavljaju između kompanija (B2B), i kompanija i klijenata (B2C), što znači da postoje dva osnovna modela elektronskog poslovanja:

- B2B - *Business to Business*
- B2C - *Business to Consumer*

Model elektronskog poslovanja B2B predstavlja poslovanje između kompanija tj. razmenu proizvoda, usluga ili informacija sa drugima kompanijama iz okruženja. Model B2B orijentisan je pre svega na efikasniju elektronsku podršku postojećih poslovnih aktivnosti, visok stepen operativnosti u razmeni informacija i proizvoda i usluga među kompanijama. Extranet je najčešće okruženje, odnosno osnova za implementaciju B2B elektronskog poslovanja.⁶⁷

U početku su kompanije koristile Internet samo za postavljanje web prezentacije, odnosno prezentacije kataloga svojih proizvoda i usluga sa navedenim kontakt informacijama. Pri takvom modelu rada, klijenti su mogli samo da se informišu o proizvodima i uslugama, a naručivanje se vršilo klasičnim putem. Razvojem sigurnosnih mehanizama omogućeno je i on-line naručivanje i plaćanje proizvoda i usluga.

Internet je značajno smanjio troškove komunikacije između kompanija i omogućio alternativu do tada korišćenoj skupoj mreži EDI (*Electronic Data Interchange*), koja je najčešće primenjivana u komunikaciji velike kompanije-kupca, sa većim brojem svojih dobavljača. Početak B2B poslovanja se vezuje za pojavu prvih EDI sistema. Velikim ulaganjima u informacionu tehnologiju, kompanije su postigle značajan stepen automatizacije internog poslovanja, ali se njihova komunikacija sa poslovnim okruženjem obavlja klasičnim putem. Znači, javila se potreba da se elektronskim putem omogući međusobna komunikacija informacionog sistema kompanije, sa informacionim sistemom njegovih poslovnih partnera. Rešenje je pronačeno u uvođenju EDI sistema koji predstavlja prvi vid B2B elektronskog poslovanja. EDI predstavlja elektronsku razmenu struktuiranih poslovnih podataka između računara posebnih kompanija. Razmena se vrši elektronskim putem, posredstvom standardizovanih poruka koje zamenjuju tradicionalne papirne dokumente. EDI nikada nije doživio masovnu upotrebu, pre svega zbog skupe, komplikovane i dugotrajne implementacije. Pored navedenog, zamera mu se i nedostatak fleksibilnosti u odnosu na brze promene u okruženju, kao i visoki troškovi održavanja koje su sebi mogle priuštiti samo velike kompanije. Nedostaci EDI mreže i pojava Interneta doveli su do primene Interneta u B2B.

⁶⁶ Jonathan Coppel: „E-commerce: Impacts and Policy Challenges“, OECD, 2000., www.oecd.org/eco/eco

⁶⁷ http://www.eccf.su.ac.yu/obavestenja/inf_u_finansijama.htm

Glavni razlozi primene Interneta u B2B su:⁶⁸

- globalna dostupnost Interneta,
- lako povezivanje,
- niska cena usluga.

B2B baziran na Internetu pruža brojne prednosti: uspostavlja se efikasnija komunikacija svih učesnika u procesu, postiže se veća produktivnost zaposlenih u procesu nabavke i efikasnije upravljanje zalihama, brže prilagođavanje potrebama klijenata i sl. Nesumnjivo, B2B postaje jeftin i efikasan marketinški i prodajni kanal.

B2B uključuje sledeće aktivnosti:⁶⁹

- internu elektronsku poštu i obaveštavanje;
- on-line publikovanje dokumenata kompanija;
- on-line pretraživanje dokumenata, projekata;
- distribucija bitnih i pravovremenih informacija zaposlenima;
- upravljanje korporativnim finansijama i personalnim sistemima;
- slanje informacija/izveštaja klijentima i dobavljačima;
- upravljanje logistikom i proizvodnjom;
- upravljanje kanalima nabavke;
- praćenje narudžbina i isporuka.

Model elektronskog poslovanja B2C je okrenut krajnjem korisniku – klijentu. Zadatak B2C je širenje tržišta, kao i zadovoljavanje potreba postojećih klijenata kako u domenu prodaje roba ili usluga, tako i u domenu pružanja informacija, servisa i podataka u korišćenju. Medijum B2C je primarno Internet. B2C uglavnom uključuje aktivnosti kao što su traženje informacija o proizvodima i uslugama, naručivanje proizvoda i usluga, plaćanje za proizvode i usluge, kao i obezbeđivanje on-line usluga klijentima.⁷⁰

Osnovna razlika između B2B i B2C elektronskog poslovanja je u tome ko je kupac, kompanija ili fizičko lice. Poređenje obeležja modela elektronskog poslovanja B2B i B2C baziranih na Internetu dati su u tabeli.

Tabela 5: Poređenje B2B i B2C⁷¹

Tržišna obeležja	B2B	B2C
Vrednost transakcija	Velika vrednost	Relativno mala, uključujući mini narudžbine
Odnos kupac/prodavač	Najčešće dugoročan, bazira se na ugovoru; Faktori koji nisu vezani za cenu su bitni za kupce; I kupac i prodavač definišu uslove	Uglavnom kratkoročan, prodaja je na licu mesta; Transakcije vrše strane koje se ne poznaju – cena je najbitnija stavka za kupca; Tržište uglavnom uslovljavaju kupci
Učesnici	Više učesnika u transakcijama – mreže dobavljača; Partneri i kupci	Mnoštvo kupaca koji posluju sa jednim prodavcem (jedan dobavljač, mnoštvo kupaca)
Funkcionalni zahtevi	Zahteva se visok stepen funkcionalnosti; Vagani su, pored cene i ostali faktori	Osin cene, praktično se ne zahtevaju dodatne informacije

⁶⁸ www.e-trgovina.co.yu/b2b/b2b_uvod2.html

⁶⁹ www.austin.tex.ac

⁷⁰ http://www.eccf.su.ac.yu/obavestenja/inf_u_finansijama.htm

⁷¹ Ebit, specijalan dodatak uz magazin Ekonomist: Elektronsko tržište, april 2002., str 35

Tržišna obeležja	B2B	B2C
Cene	Cene se formiraju ili dogovorno, dugoročnim ugovorima, aukcijama ili su kataloške	Fiksne cene, uglavnom kataloške
Način plaćanja	Kreditne kartice, bankarski krediti, elektronsko plaćanje (transfer sa računa na račun)	Kreditne kartice, elektronsko plaćanje (transfer sa računa na račun)
Izvršavanje narudžbi (dostava)	Strogi zahtevi vezani za dostupnost proizvoda i precizan način izvršavanja; Univerzalna ekspresna dostava	Zahtevi su manje strogi; Univerzalna ekspresna dostava
Infrastrukturni zahtevi	Sloteniji, prilagođeni	Minimalni zahtevi-web browser i pristup Internetu
Uslovi ulaska na tržište	Cene tehnologije i razvoja mogu izazvati prepreke za ulazak na tržište, posebno za prodavce	Ne postoje veće prepreke za ulazak na tržište
Efekti „umrežavanja“	Koristi se za kupce i prodavce	Koristi prodavcima, u većoj i kupcima u manjoj meri
Posrednici	Posrednici se izbegavaju, ali se koriste u pojedinim slučajevima	Posrednici se izbegavaju
Opis proizvoda	Posebno napravljen na osnovu specifikacije	Standardizovan
Prodajne procedure	On-line katalozi, tenderi	On-line katalozi
Sigurnosne mere	Sigurnost mreže i kompanijska privatnost	Zaštita informacija o korisnicima i njihovim zahtevima

Možemo zaključiti da je u modelu B2C uključeno mnoštvo kupaca koji kupuju proizvode relativno male vrednosti i kojima je cena, praktično, najbitnija. Cene su fiksne, a plaćanje se vrši pomoću platnih kartica, ili putem elektronskog plaćanja. Za razliku od modela B2B, kod B2C modela ne postoje znatnije prepreke za ulazak kupaca na tržište, jer se zahteva samo web pretraživač i pristup na Internet. Kod oba modela se izbegavaju posrednici i koriste se on-line katalozi, a u modelu B2B i tenderi. B2B model predstavlja trgovinu kao što i samo ime kaže između poslovnih strana, samim tim ova trgovina je daleko veće vrednosti od B2C, takođe ove mreže su više zatvorenog nego otvorenog tipa i zahteva se ispunjavanje određenih faktora kako bi se moglo nastupiti u B2B transakcijama. Takođe, bitno je napomenuti da se za pristupanje B2B transakcijama zahteva značajnija infrastrukturna platforma. Ukratko, B2C predstavlja razgranatu maloprodajnu mrežu u trgovine putem Interneta, za koju nisu potrebna ulaganja (izuzev običnog računara) i koji omogućava kupovinu širom sveta artikala relativno male vrednosti, ali kataloški standardizovane. Nasuprot B2C, B2B podrazumeva velike transakcije među poslovnim učesnicima, koji radi sopstvene sigurnosti, zaštite podataka i drugih faktora insistiraju na određenim hardversko-softverskim platformama.

Što se tiče učesnika u elektronskom poslovanju, kod modela B2B učestvuje više učesnika u transakcijama, odnosno, dobavljača, partnera i kupaca, za razliku od B2C modela gde jedan prodavac posluje sa velikim brojem kupaca. U oba slučaja se izbegavaju posrednici, s tim da se mogu javiti u poslovnom odnosu između kompanija. Pozitivne efekte „umrežavanja“ možemo naći kod oba modela, s tim da je kod modela B2C izražena korist za prodavce, u odnosu na kupce. Formiranje cena se obavlja različito u zavisnosti od modela poslovanja. Kod poslovanja između kompanija, cene se mogu formirati na više načina i to dogovorno, dugoročnim ugovorima, aukcijski ili kataloški. Nasuprot tome, cene kod modela B2C su fiksne, uglavnom kataloške. Za izvršavanje plaćanja se koriste kreditne kartice i elektronsko plaćanje, stima da kod modela B2B, u slučaju da kompanija ne poseduje dovoljno sredstava plaćanje može obaviti i putem bankarskog kredita. Postoji i određena razlika u zahtevima sigurnosnih mera. Kod modela B2B težište se stavlja na sigurnost mreže i kompanijsku privatnost, dok se u modelu koji je okrenut ka krajnjem korisniku-fizičkom licu, težište stavlja na zaštitu informacija o korisnicima, kao i njihovim zahtevima.

Elektronsko poslovanje (B2B i B2C) može biti sprovedeno preko otvorenih mreža⁷² ili zatvorenih mreža⁷³.

Oblici komuniciranja između kompanija B2B, uglavnom se svode na mreže zatvorenog tipa – što je naravno i slučaj u domicilnoj bankarskoj praksi (gde je komunikacija banaka sa NBS bazirana na mreži zatvorenog tipa). Reče su primene otvorenih mreža u komunikaciji između dve poslovne strane i one se svode uglavnom na komunikaciju putem elektronske pošte i na ovaj način određene vidove razmene informacija. Sa druge strane, komunikacija B2C je u mnogome prisutnija na otvorenim mrežama, iz razloga njihove masovnosti i pogodnosti-udobnosti za primenu od strane krajnjih potrošača. Tipičan primer ovog vida komunikacije u domicilnim uslovima odnosi se na Internet kupovinu preko web sajtova (u počecima u našoj zemlji), ali i on-line bankarstvo koje je uvedeno i razvijeno u svim poslovnim bankama. B2C putem zatvorenih mreža u domaćim uslovima je nerazvijen i možemo konstatovati da je ovo segment koji tek treba da doživi veći stepen primene, a sve iz razloga relativne nesigurnosti primene Interneta i javnih sajtova i servisa kao sredstava komunikacije i razmene poverljivih podataka između kompanija i klijenata kao krajnjih korisnika.⁷⁴

Pored osnovnih modela elektronskog poslovanja, postoje i sledeći oblici poslovanja:

- C2C – *Consumer to Consumer*

Potrošači direktno trguju sa drugim potrošačima. Kompanija koja podržava ove transakcije mora naći neki netradicionalan način za naplatu usluge. Naplata usluge je obično mali procenat transakcije, članarina za uslugu ili neki vid kombinacije ovih načina.

- B2C2B – *Business to Consumer to Business*

Predstavlja noviji model elektronskog poslovanja. B2C2B je definisan kao korišćenje modela B2B kao podrške poslovanju kompanija po modelu B2C. B2B pruža mogućnost B2C kompanijama da smanje troškove i poboljšaju B2C usluge. Aplikacija koja povezuje jedan online katalog sa drugim može se smatrati B2C2B aplikacijom jer doprinosi uspehu oba oblika poslovanja.

- C2B2C – *Consumer to Business to Consumer*

C2B2C model povezuje potrošače koristeći online preduzeće kao posrednika. Primer ovog tipa aplikacije je www.autotrader.com. Ovaj sajt omogućava transakcije polovnih automobila između korisnika, ali takođe sadrži i katalog novih automobila.

⁷² Otvorena mreža predstavlja mrežu koja nema određenog menadžera ili kontrolora (na primer, World Wide Web-WWW). Svako može da se poveže na mrežu, ako poseduje potrebnu tehničku opremu.

⁷³ Zatvorene mreže mogu biti u okviru velikih kompanija (intraneti) i mreža koje povezuju više poslovnih partnera (ekstraneti) koje nisu vezane za Internet. Korisnik mreže se može postati samo uz odobrenje administratora mreže, odnosno dozvole drugih partnera, prihvatanjem određenih uslova i pravila za upotrebu mreže. To omogućava da trgovanje bude sigurnije jer su svi potencijalni klijenti poznati, a broj potencijalnih klijenata limitiran.

⁷⁴ http://www.eccf.su.ac.yu/obavestenja/inf_u_finansijama.htm

DRUGI DEO

ELEKTRONSKI FINANSIJSKI SISTEMI

1. ELEKTRONSKI SISTEM ODNOSA SA KLIJENTIMA

Na globalnom modernom tržištu finansijskih usluga dolazi do izuzetno izraženog porasta konkurentskog pritiska. Da bi se izborile sa novim tržišnim zahtevima koje sa sobom nosi jačanje konkurencije, banke su primorane da razvijaju nove elemente borbe za očuvanje lojalnosti svojih klijenata. Tržišna dinamika razvoja novih elemenata uslovljena je pojavom nove tehnologije, porastom očekivanja samih klijenata, globalizacijom poslovanja, konvergencijom tradicionalnih tržišta i pojavom novih kanala za kontakte sa klijentima.⁷⁵

Savremeni klijenti su, po pravilu, bolje informisani, otvoreniji prema tehnološkim inovacijama, fleksibilniji u odnosima sa svojim finansijskim institucijama, imaju znatno veće mogućnosti izbora alternativnih kanala i proizvoda. Pod dejstvom ovih elemenata dolazi do porasta tražnje za naprednijim bankarskim proizvodima, kao sa posebno izraženim individualizovanim potrebama sa pogodnošću korišćenja.

Kao odgovor na ovakve promene, banke se fokusiraju na potrebe pojedinačnih klijenata. U skladu sa tim, usvajaju strategiju baziranu na klijentu (engl. *Customer - centric strategy*) kao sredstvu za unapređenje svojih konkurentskih prednosti. U tom smislu formiraju tzv. "one-to-one" bankarsku marketing strategiju, a CRM (*Customer Relationship Management*) se pojavljuje kao najnapredniji način za realizaciju ove vrste marketing strategije. Njen cilj je privlačenje, zadržavanje i proširenje profitabilnih odnosa sa klijentima.

CRM je koncept koji zahteva novi poslovni model baziran na klijentu, fokusiran na glatku integraciju svakog posla koji tangira klijenta. Pomoću njega banke obezbeđuju personalizovanje i relevantne komunikacije kroz elektronske i tradicionalne kanale, a na principima interaktivnog kontakta sa klijentima.

Osnovni ciljevi integrisanog CRM-a su:⁷⁶

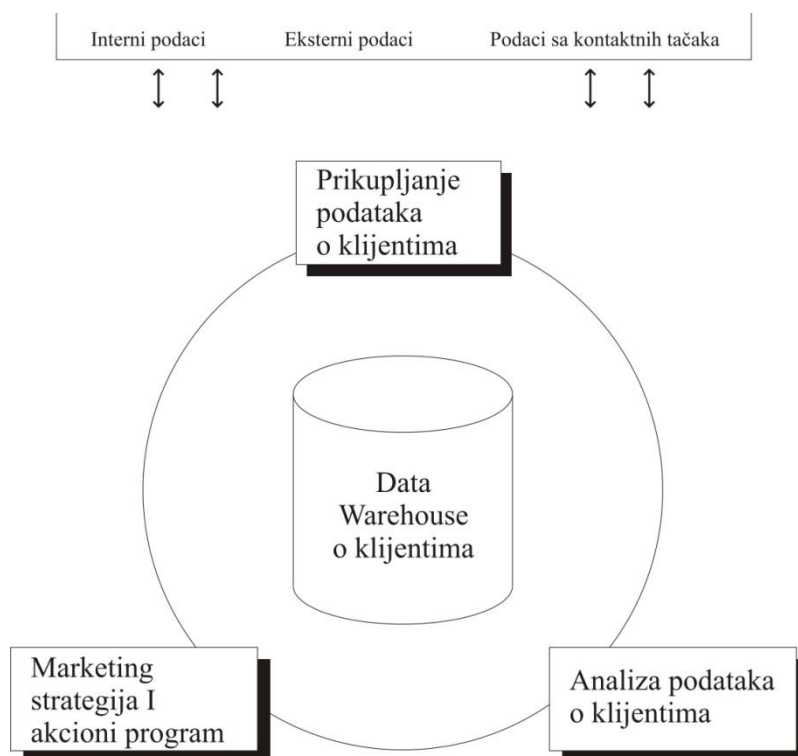
1. proširenje odnosa sa klijentima (kroz prihvatanje novih klijenata, proširenje na nova tržišta i identifikovanje i targetiranje novih segmenata);
2. produbljivanje postojećih odnosa na duži rok (povećavajući perceptivnu vrednost proizvoda i uvođenjem novih proizvoda) i
3. produbljivanjem odnosa sa klijentima (iniciranjem unakrsne prodaje, razumevanjem sklonosti različitih segmenata klijenata za kupovinu i povećanje prodaje).

Implementacija sistema CRM pomaže da se stekne kompletna slika o postojećim klijentima, koncipiraju finansijski proizvodi i usluge prema klijentu (engl. *Customer - oriented*) i tržištu (engl. *Market - driven*), kao i ekstenzivnih istraživanja finansijskog tržišta. Sve ovo sprovodi se u cilju povećanja lojalnosti klijenata i profita kroz integraciju solucija informacione tehnologije i poslovnih operacija u svakom procesu bankarskog poslovanja koji je relevantan za klijenta.

⁷⁵ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.192

⁷⁶ Isto, str.193

Slika 3: Ciklus CRM u bankama



Da bi se realizovala puna vrednost CRM-a, banka mora da uvede i unapredi proces za svakog klijenta koji će obuhvatiti obezbeđenje informacija, analizu i formiranje marketing strategije i akcionog programa. Integrisane CRM solucije omogućavaju banci da postavi zatvoren CRM ciklus koji je sastavljen od niza interaktivnih procesa. On upravlja ukupnim *end-to-end* procesom (prikupljanjem podataka, analizom profila klijenata, donošenjem marketing odluka i optimiziranjem marketing kampanje, strategije prodaje kroz multikanale banke).

Zatvoren ciklus CRM se sastoji iz sledećih faza, a to su:⁷⁷

1. prikupljanje podataka o klijentima,
2. analiza podataka o klijentima i
3. marketing strategija i akcioni program (planiranje, izvršavanje i efikasna evaluacija).

Kako su podaci koji se prikupljaju veoma heterogeni (usled velike geografske disperzije, multikanalnog funkcionisanja itd.) potrebno je da se formira multikanalni interfejs sa klijentima. Da bi se to postiglo, moraju da se formiraju centralizovane integrisane baze podataka na jednom mestu za potrebe analize stručnjaka i marketing menadžera (*Data Warehouse*). Ovakva baza podataka mora da bude ažurirana u realnom vremenu, da obuhvata i eksterne podatke i podatke iz firme, kao i relevantne istorijske podatke.

Podaci u bankarskom transakcionom sistemu su često organizovani oko koncepta kao što su „računi“, „proizvodi“, „kanali“ i sl. tako da se limitira mogućnost identifikacije pojedinačnog klijenta i njegovog potpunog meĎuodnosa sa bankom. Zbog toga je jedan od glavnih ciljeva sistema CRM konsolidacija ovih „informativnih ostrva“ i separativnih solucija, da bi se

⁷⁷ Isto, str.194

formirao unakrsni bankarski sistem od koga svi izvršioci, zaposleni u filijalama i poslovnicama, mogu da koriste informacije. Baza integrisanog CRM-a treba da se sastoji od:⁷⁸

1. operacionih izvora (odnosno iz podataka koji se dobijaju iz kontaktnih tačaka klijenata sa bankom – lični kontakti, kol centri, ATM, mobilno bankarstvo, Internet bankarstvo itd.);
2. internih izvora, odnosno raspoloživih „informativnih ostrva“, drugih bankarskih proizvodno orijentisanih sistema i baza podataka (depoziti, kartice, investicije itd.), analize meta podataka, rezultata data mining i marketing kompanija;
3. eksternih izvora, kao što su marketing istraživanja, informativnih posrednika, psihografski podaci i podaci o životnom stilu koji mogu da pomognu u sticanju potpunije slike o klijentu.

Korišćenjem jednostavnijih ili složenijih tehnika analize (*Data mining, OLAP, itd.*) obezbeđuje se pružanje korisnog uvida iz prikupljenih podataka u *Data Warehouse*. (Koriste se diferenciranja/segmentacije, distribucije i koncentracije, analize širih/dužih/dubljih odnosa sa klijentima). Analiza omogućava identifikaciju profila klijenta, njihovih preferencija za specifične proizvode i usluge, kao i ukazivanje na najprihvatljivije kanale distribucije.

Na bazi prikupljenih podataka i rezultata analize omogućava se poboljšanje marketing procesa, poruka i strategija. Glavni cilj u okviru CRM-a je planiranje, izvršavanje i monitoring strategije i akcionog programa, koji personalizuju i optimiziraju kontakt sa svakim klijentom. Za banke nije bitno samo pronalaženje podataka i otkrivanje uzoraka već takođe potreba i operacionalizacija kroz bankarske aktivnosti, kao odgovor na uvid u informacije o klijentima. Finalni deo ciklusa CRM je evaluacija rezultata. To je ujedno i kritično za merenje performansi i povratne sprege rezultata.

2. ELEKTRONSKI NOVAC I MONETARNI SISTEM

2.1. Pojam

Termin elektronski novac se često u slobodnijem korišćenju odnosi na različite instrumente i mehanizme maloprodajnih plaćanja. Preciznu definiciju elektronskog novca u ovom trenutku je teško dati, jednim delom zato što se promene u ovoj oblasti velikom brzinom dešavaju, a drugim delom zato što tehničke inovacije zanemaruju razlike između oblika novca i mehanizama plaćanja. Zbog toga je značajno, u meri u kojoj je to moguće, utvrđivanje pojamovne distinkcije između „proizvoda elektronskog novca“ i „proizvoda ulaza“ u konvencionalne platno prometne usluge, sa jedne strane i „proizvoda elektronskog novca“ i tradicionalnih oblika novca, sa druge strane.

Elektronski novac se danas nalazi u eksperimentalnoj fazi razvoja, bez značajnije praktične primene. Ocene o naglom razvoju bezgotovinskog društva, koje su prezentirane šezdesetih godina, pokazale su se kao nerealne. Međutim, očekuje se da će u budućnosti doći do naglog porasta njegove upotrebe, sa porastom stepena sigurnosti, ekonomičnosti i spremnosti njegovog prihvatanja.

Pitanje utvrđivanja njegovih monetarnih i ekonomskih karakteristika i perspektiva postalo je bitno zbog toga što dijalektika razvoja novca predstavlja sintetički izraz evolutivnih promena

⁷⁸ Isto, str.195

oblika novca, pojmovnog određivanja novca i organizacije monetarnih sistema. Promena forme novca otvara pitanja definisanja, merenja i kontrole novca. Za odgovor na ta bitna pitanja ključno je adekvatno proceniti šta nova forma novca znači u pravnom, ekonomskom i funkcionalnom smislu, jer će od toga zavisiti i pravac promena u bankarskom i monetarnom sistemu.

2.2. Struktura i funkcionisanje sistema elektronskog novca

Projekti o funkcionisanju elektronskog novca su još uvek u fazi testiranja ili ograničene praktične upotrebe. U njima se koriste različita tehnička rešenja, a iskustva pokazuju da su potrebna mnoga poboljšanja pre njihove šire implementacije. U tim nastojanjima se definišu sami zahtevi koje elektronski novac treba da ispunjava, da bi bio ekonomski i društveno prihvatljiv, a zatim se formiraju određeni protokoli i procedure pomoću kojih treba da se obezbede uslovi za ispunjavanje ovako postavljenih zahteva. Valorizacija konkretnih rešenja je u direktnoj zavisnosti od stepena ispunjavanja zahteva koji se smatraju manje ili više bitnim za obavljanje funkcije novca.⁷⁹

Sami zahtevi se još uvek nalaze u fazi utvrđivanja, mada se u osnovi svode na nastojanja da se obezbedi što veća sličnost sa karakteristikama gotovog novca. U nekim analizama vrši se klasifikacija svih zahteva za jedinstvenu valutu, koja bi se koristila za transakcije preko Interneta u tri grupe. Prvu grupu bi sačinjavali obavezni zahtevi, odnosno zahtevi bez čijeg ispunjavanja sistem ne bi mogao da funkcioniše (obezbećenje sigurnosti npr.). Drugu grupu bi sačinjavali bitni zahtevi, odnosno zahtevi koji sistem čine korisnim i predstavljaju preduslove za njegovo šire prihvatanje (troškovi, pogodnost upotrebe, nosivost itd.). Međutim, u slučajevima kada prouzrokuju neprihvatanje sistema, oni takođe mogu dobiti značaj obaveznih zahteva. Treću grupu bi sačinjavali opcioni zahtevi, odnosno zahtevi koji bi odgovarali posebnim željama (npr. trajnost, deljivost, nezavisnost itd.).⁸⁰

Generalno posmatrano, pri konstrukciji operativnih šema funkcionisanja elektronskog novca polazi se od neophodnosti obezbećenja tri grupe zahteva:⁸¹

1. sigurnost,
2. pogodnost upotrebe i
3. posedovanje osobina gotovog novca.

Kako je preduslov šire upotrebe elektronskog novca, poverenje društva u njega, potrebno je onemogućavanje njegove nepravilne upotrebe (promenom, falsifikovanjem ili dupliranjem). Da bi se to obezbedilo, potrebno je da se sigurnosne mere multiplicitiraju na različitim tačkama, tako da u slučaju kompromitovanja jednih mera sigurnosti, mogu da deluju druge. Kao konkretni nivoi obezbećenja sigurnosti pojavljuju se:

1. prevencija nepravilne upotrebe i
2. identifikacija zlonamernih korisnika.

Da bi elektronski novac bio šire prihvaćen, potrebno je da ima viši stepen pogodnosti upotrebe od tradicionalnog gotovog novca (da može da se koristi kao gotov novac u

⁷⁹ Isto, str.197

⁸⁰ Isto, str. 197

⁸¹ Isto, str.199

prodavnicima, kao novi medijum plaćanja, za plaćanja preko Interneta i da bude deljiv). Smatra se da konkretna rešenja treba da obezbede njegovu deljivost, jednostavnost obavljanja plaćanja i efikasno upravljanje emisijom i funkcionisanjem.

Elektronski novac bi morao da poseduje osobine gotovog novca da bi mogao da obavlja funkciju njegovog supstituta. Ovi zahtevi se manifestuju u dve dimenzije:⁸²

Prvo, treba da bude obezbećena mogućnost njegovog opšteg korišćenja bez obzira na kredibilnost platioca, jer novac sam po sebi sadrži vrednost. U tom smislu se ističe potreba omogućavanja njegovog korišćenja bez posrednika, mogućnost prenošenja drugim pojedincima i obezbećivanje identičnog tretmana, bez obzira na banku od koje je povučen.

Drugo, obezbećuje zaštitu privatnosti korisnika koja podrazumeva da:

1. privatnost korisnika, ne može da bude narušena čak i kada su prodavac i banka u tajnom sporazumu i
2. ne postoji mogućnost uspostavljanja veze između informacija o upotrebi elektronskog novca iste osobe na različitim lokacijama.

U cilju obezbećivanja ovih zahteva traži se offline operabilnost, direktna transferibilnost između individua, nosivost i operabilnost većeg broja banaka.

U samoj strukturi sistema, pored banaka kod kojih se nalaze individualni računi klijenata, sa kojih klijenti mogu da povlače sredstva da bi na bazi njih dobili elektronski novac, pojavljuju se nove institucije koje se specijalizuju za emisiju elektronskog novca, a u nekim rešenjima i posebne registracione institucije za registraciju korisnika elektronskog novca i njihovog snabdevanja javnim ključevima.

Okamoto i Ohta su 1993. godine pokazali da elektronski novac može biti konstruisan korišćenjem modela emitovanja novčanica (engl. *note-based model*). Ovaj model kasnije 1996. godine unapređuju Fujisaki i Okamoto tako što omogućavaju da se šema implementira na tehnološku osnovu smart kartice (engl. *smart card basis*). U njoj se garantuje privatnost korisnika uvođenjem trećeg učesnika u transakcioni proces, usvaja standardni digitalni potpis koji novac čini prenosivim, a obim obrade i telekomunikacioni prenos redukuju. Ipak ona ostavlja nerešena sledeća pitanja:

1. zaštite (glavni element zaštite je post detekcija upotrebe);
2. posedovanja osobina gotovog novca (pojavljuje se problem operabilnosti većeg broja banaka, jer ako pojedinac ima novac kod različitih banaka, a svaka banka ima svoju šemu biće otežano korišćenje) i
3. efikasnosti upravljanja emisijom i funkcionisanjem (kako podaci o svim trošenjima elektronskog novca moraju da se čuvaju u datoteci banke u cilju otkrivanja previsokih trošenja, pojavljuje se problem zbog preobimne banke podataka).⁸³

Ove probleme nastoje da reše *Nakayama, Moribatake, Masayuki, Fujisaki*. Prema njihovim tehničkim rešenjima u sistem su uključene banke, registracione institucije i institucije koje emituju elektronski novac. Zadatak registracione institucije je da obezbedi registraciju korisnika elektronskog novca i snabde ga javnim ključem, emisione institucije da emituje

⁸² Isto, str.199

⁸³ Isto, str.200

elektronski novac, upravlja njegovim korišćenjem i detektuje zloupotrebe u tim procesima, a banke da upravlja računima klijenata i izdaje potvrde potrebne za povlačenje elektronskog novca. Korisnici elektronskog novca mogu njime da vrše plaćanja, da ga podižu sa računa i da ga deponuju na račun.

Sama procedura dobijanja elektronskog novca sastoji se iz dve faze:

Prvo, faze u kojoj registrovani klijenti (kod registracione institucije) dobijaju priznanice od banke na bazi kojih može da se izvrši podizanje elektronskog novca i

Drugo, faze dobijanja elektronskog novca od emisione institucije na bazi podnete priznanice dobijene od banke.

Unapređenje se ostvaruje po osnovu smanjenja troškova i porasta stepena zaštite. Snižavanje troškova se obezbeđuje drastičnim smanjenjem veličine banke podataka u instituciji koja emituje elektronski novac. To se postiže time što se u banci podataka emisione institucije, briše deo elektronskog novca koji je upotrebljen i kao takav vraćen, tako da ostaje evidentiran samo nepotrošeni deo. Emisiona institucija jedina ima podatke o nepotrošenom elektronskom novcu. Ukoliko deo emitovanog elektronskog novca nije vraćen posle upotrebe, znači da je došlo do neke nepravilnosti, ili zloupotrebe.

Emisiona institucija ima samo javni ključ, a samo banka koristi tehnologiju „slepog“ potpisa (engl. „*blind*“ *signature*), tako da banka ne može na bazi certifikata sa javnim ključem izdatog od registracione institucije da uspostavi vezu sa informacijama o korisniku, a emisiona institucija ne može da poveže informacije o emitovanom novcu sa informacijama o korisniku. Ukoliko se identifikuje nevraćanje elektronskog novca, emisiona institucija šalje javni ključ registracionoj instituciji, koja na bazi njega može da identifikuje zlonamernog korisnika iz baze podataka.

Kao posebna prednost ovakvog dizajna ističe se mogućnost korišćenja jedne zajedničke šeme za veći broj banaka (naravno uz uvođenje posebne institucije za međubankarski obračun), čime se povećava opšta efikasnost funkcionisanja sistema.

2.3. Atributivne i funkcionalne karakteristike elektronskog novca

Testiranje i valorizacija različitih šema funkcionisanja elektronskog novca, pokazuju da elektronski novac kao novi javni oblik novca postaje više od nove tehnike i ideje o njoj primeni, jer istovremeno izražava i stav društva prema mogućnostima njihove upotrebe i spremnosti da se sa prihvatanjem novog monetarnog oblika novca, prihvati potrebna reorganizacija novčanog sistema i eventualno redefinicija samog pojma novca. Zbog toga postaje potrebno utvrđivanje razlike između ovog oblika novca i tradicionalnih oblika novca.

Kada su prvi oblici elektronskog novca i plaćanja počeli da se razvijaju (1993.), pojavila se definicija prema kojoj se elektronski novac shvata kao skladište monetarnih vrednosti na tehničkom uređaju, koji se može široko koristiti za obavljanje plaćanja bez neophodnog uključivanja bankarskih računa u transakciju. Sa aspekta sadašnjih posmatranja, može se zaključiti da se ona odnosi samo na jedan oblik elektronskog novca, kartični elektronski novac (engl. *Card - based products*). Ključni elementi u ovoj definiciji elektronskog novca odnose se na:

1. višenamenski karakter upotrebe (elektronski novčanik) i
2. unapred izvršenu uplatu određene kupovne snage (prepaid card).⁸⁴

Prvi elemenat se javlja kao rezultat potrebe da se napravi razlika između jednonamenskih i višenamenskih kartica sa memorisanom vrednošću. Prema njoj, pojam elektronski novac odnosio bi se samo na višenamenske kartice sa memorisanom vrednošću koje se koriste za kupovine različitih vrsta robe od većeg broja prodavaca, a ne i na jednonamenske kartice koje se koriste za kupovinu jedne vrste robe, ili usluga, ili proizvoda od jednog prodavca. Njihov tretman bio bi identičan tretmanu bonova i četona koji služe za kupovinu samo određene vrste robe u papirnim sistemima plaćanja. U skladu sa tim, telefonske kartice sa memorijskom vrednošću smatraju se samo elektronskom varijantom četona.

Drugim elementom se pravi razlika između „kartica sa upisanom vrednošću“ (engl. *multi-purpose prepaid cards*) koje predstavljaju elektronski novac i klasičnih oblika debitnih i kreditnih kartica koje ne spadaju u elektronski novac, jer nisu zasnovane na plaćanju unapred. Inače, ovaj problem je dodatno složen zbog činjenice da kartice mogu da funkcionišu kao jednofunkcionalne (kao jedna vrsta instrumenta plaćanja) ili višefunkcionalne (kao više vrsta instrumenata plaćanja - npr. istovremeno kao kreditna, debitna i kartica memorisane vrednosti). Pored njihove osnovne svrhe, one se koriste i za neke druge nemonetarne ciljeve (kao garantno sredstvo plaćanja, sredstvo za identifikaciju, autorizaciju pristupa, prenosnik podataka ili sredstvo za elektronsko potpisivanje).

Sa pojavom proizvoda koji koriste specijalne softvere (engl. *Software - based products*) na personalnim računarima, a koji omogućavaju transfer monetarnih vrednosti putem telekomunikacionih mreža kao što je Internet, dolazi do proširenja definicije elektronskog novca. Zajedničke karakteristike oba oblika svode se na obavezu da monetarna vrednost koja se memoriše u elektronskoj formi, na mikročipu ili hardveru, mora da bude prethodno uplaćena. U oba slučaja novac je predstavljen šifrovanim nizom bitova, a razlike se svode samo na aspekte karakteristika medijuma čuvanja i tehničke sigurnosti.

Za utvrđivanje karakteristika elektronskog novca značajne su i konkretne karakteristike tehnologija njegovog korišćenja. Ključno pitanje u ovom kontekstu je, da li se plaćanje finalizuje u trenutku plaćanja elektronskim novcem, ili tek odgovarajućim promenama na depozitnim računima i sa tog aspekta može se napraviti razlika između dve varijante: gotovinske i depozitne.

Gotovinski tip (engl. *cash type system*) omogućava da elektronski novac cirkuliše među korisnicima na isti način kao i gotov novac, direktnim prenosom između učesnika u platnom prometu (engl. *face-to-face*). Tehničku osnovu ove varijante predstavljaju proizvodi kod kojih je izvršena prethodna uplata na elektronskom uređaju koji je u posedu klijenta, a sam mehanizam korišćenja iznosa memorisane vrednosti zasniva se na njenom smanjenju pri korišćenju za plaćanja. Kod ovakvih rešenja plaćanja između transaktora bi se mogla smatrati finalnim u trenutku njihovog izvršenja, a primljena monetarna vrednost se ne vraća na bankovni račun, što znači da može da se koristi za dalja plaćanja.⁸⁵

Prema varijanti depozitnog tipa (engl. *deposit type system*) elektronski novac se posle svake transakcije vraća emitentu, tako da plaćanje elektronskim novcem predstavlja samo

⁸⁴ Isto, str.202

⁸⁵ Isto, str.203

privremenu novčanu transakciju koja se finalno zatvara tek prenosom sredstava između transakcionih depozita kod banaka. Smatra se da se svi oblici novca koji se na ovaj način koriste za plaćanje, mogu podvesti pod kategoriju mrežnog novca, bez obzira na vrstu proizvoda na kojoj se baziraju (kartica ili računar). U tehničkom smislu, ova varijanta se bazira na proizvodima ulaza (engl. „*access“ products*) i softverima kojima je klijentima omogućeno da vrše ulaz u svoje depozitne račune preko određenih mreža.

U nastojanjima da se definišu novi oblici elektronskog novca, prisutni su naponi za utvrđivanjem razlika između njih i klasičnih oblika gotovog i depozitnog novca. Kao najbitnije razlike između elektronskog i gotovog novca koji danas cirkuliše u platnom prometu navode se sledeći elementi:⁸⁶

1. kod elektronskog novca koristi se kriptografija za obezbeđenje autentifikacije transakcije, zaštite poverljivosti i integriteta podataka, dok se kod gotovog novca postavlja samo problem fizičke sigurnosti samog novca;
2. elektronski novac, ne samo da može, već se najčešće i koristi za udaljena plaćanja (bez potrebe fizičke razmene), dok kod gotovog novca to nije slučaj;
3. u većem broju šema koje su danas raspoložive za korišćenje, elektronski novac koji je jednom primljen od korisnika nije moguće ponovo koristiti, dok primljeni gotov novac poverilac može da koristi za plaćanja.

Manje su jasne razlike i sličnosti elektronskog novca u odnosu na depozitni novac jer, dok su neki oblici elektronskog novca slični depozitnom novcu po tome što oba oblika zahtevaju pripadnost određenoj finansijskoj instituciji, drugi oblici elektronskog novca se pojavljuju kao konkurent depozitnom novcu. Kod varijanti elektronskog novca koji zahteva pripadnost određenoj finansijskoj instituciji razlike se svode na vrstu instrumenata kojom se obezbeđuje korišćenje novca: kod depozitnog novca u tu svrhu se koriste čekovi, virtumanski nalozi i dr., a kod elektronskog novca, specifični instrumenti koji su reprezent medijuma čuvanja kupovne snage.

Inače, posmatrano u elektronskom smislu, uvek kada je emitent elektronskog novca kreditna institucija, on može biti samo podskup bankarskog novca, a razlike koje se evidentiraju imaju samo jasan tehnički i operacioni karakter. Kao potvrda ovog stava navode se razlike u praktičnoj upotrebi depozitnog i elektronskog novca za plaćanja veoma malih i velikih vrednosti. Dok tradicionalni depozitni novac najčešće nije u praksi korišćen za plaćanja veoma malih vrednosti, zbog toga što ga karakter i visina troškova procesiranja baš u ovakvim slučajevima čine ekonomski neisplativim, elektronski novac neće biti korišćen za transakcije veoma velikih vrednosti zbog toga što ga za takve namene čine nepogodnim rizici koji su generalno imanentni elektronskom novcu.⁸⁷

Ipak, sve prethodno pomenute razlike i sličnosti postojećih oblika elektronskog novca u odnosu na tradicionalne oblike novca nisu ni približno bitne, kao što je položaj u odnosu na državni tretman i pravnu regulativu. Ni jedan od postojećih oblika elektronskog novca nema status zakonskog sredstva plaćanja kao što to ima papirni novac iza koga stoji država. Zbog toga, državni novac primaju svi, elektronski novac primaju samo oni koji su uključeni u određene konkretne sisteme plaćanja, a u literaturi se posebno potenciraju problemi koji mogu nastati zbog toga.

⁸⁶ Isto, str.204

⁸⁷ Isto, str.205

Ovakvo stanje se može posmatrati samo kao nastavak prakse koja je bila prisutna u celokupnoj istoriji razvoja novčanih sistema. Sam novac je nastao pre države i njene regulative, svi savremeni novčani sistemi (gotov novac i depozitni novac) razvili su se prvo mimo države i dugo se tako upotrebljavali u platnom prometu, da bi ih tek nakon toga, sa dostizanjem usavršene forme, država priznala kao novac. Država postaje bitna onda kada određuje zakonsko sredstvo plaćanja na bazi državne prinude, tako što svojom regulativom uređuje pravila i obezbeđuje poštovanje tih pravila.

Praksa pokazuje takođe da i u uslovima kada se novac zasniva na državnoj prinudi, ona može samo do određene mere uticati na primanje novca u prometu, a iznad toga deluje spremnost ljudi da prihvate ili ne prihvate novac koji se bazira na državnoj prinudi. To se manifestuje u uslovima krupnijih inflatornih poremećaja kada u sukobu između stvarne i propisane vrednosti, pre ili kasnije, pobeđuje stvarna (npr. u periodima visoke inflacije).

Da bi država mogla svojom podrškom da kompenzira eliminisanje elemenata materijalne sadržine novca, bilo je potrebno da izvrši odgovarajuće promene u oblasti organizacije funkcionisanja monetarnih sistema. U uslovima prelaska sa robnog novca na papirni novac, problem je rešen uvođenjem nove institucije, centralne banke i tek sa njom postalo je moguće da se novom monetarnom obliku novca obezbedi opšta prihvatljivost. Evidentno je da će organizaciona struktura elektronskog monetarnog sistema ići u pravcu stvaranja mrežnih grupacija i jačanja integracije sistema razmene na jednom višem nivou.

3. ELEKTRONSKE MREŽE I SISTEMI ELEKTRONSKOG PLAĆANJA

3.1. Generalne karakteristike

Obavljanje elektronskog plaćanja na siguran način predstavlja srž realizacije kupoprodajnih transakcija elektronske trgovine. U tom cilju uvode se posebni protokoli, koji u manjoj ili većoj meri obezbeđuju sigurnost, efikasnost i ekonomičnost različitih tehnologija plaćanja u elektronskoj trgovini.

Infrastrukturnu osnovu koja omogućava funkcionisanje elektronskih sistema plaćanja, čine različite institucije, tehničko - tehnološka sredstva i procedure. Mada su mnogi projekti još u fazi testiranja, na bazi funkcionisanja postojećih sistema, mogu se kao ključne izdvojiti sledeće komponente: elektronski novčanik, softverski registar trgovca, servis za plaćanja na Internetu, finansijske institucije i sistemi za verifikaciju.

Na bazi ovih komponenti razvijaju se različite aplikacije plaćanja, koje se međusobno razlikuju po svojim tehničko - tehnološkim, funkcionalnim, ekonomskim i bezbedonosnim karakteristikama. Obezbeđenje sigurnosti postaje dominantan preduslov koji zahteva da konkretna rešenja pruže mogućnosti za: identifikaciju učesnika, adekvatnu autorizaciju transakcije, obezbeđenje integriteta, neopozivosti i privatnost.⁸⁸

3.2. Definisanje procesa plaćanja

Platni promet predstavlja sva plaćanja koja se vrše između pravnih i fizičkih lica. Plaćanje je proces prenosa novca iz vlasništva jednog subjekta u vlasništvo drugog subjekta, posredstvom finansijskih institucija (banke). Plaćanja su inicirana nekim dužničko - poverilačkim

⁸⁸ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.156

(obligacionim) odnosom između dva subjekta. Obično nastaju povodom razmene neke ekonomske vrednosti – najčešće robe, tako da je tok plaćanja, suprotan toku robe.⁸⁹

Osnovna funkcija banaka jeste posredovanje u plaćanjima (poslovi platnog prometa), mada mogu imati i ulogu aktivnih subjekata – inicijatora plaćanja u vezi sa sopstvenim poslovima (na primer, kupovina hartija od vrednosti).

Plaćanja mogu da se podele na osnovu različitih kriterijuma, kao što su:⁹⁰

- a) kriterijum upotrebe gotovine, prema kojem se plaćanja dele na gotovinska i bezgotovinska;
- b) zavisno od mesta plaćanja, razlikuje se plaćanje u zemlji i plaćanje u inostranstvu i
- c) zavisno od tehnologije koja se koristi za plaćanje, postoje tradicionalna plaćanja, pomoću tradicionalnih platnih instrumenata i elektronska plaćanja, koja se obavljaju upotrebom elektronske tehnologije.

Prema subjektima između kojih se obavlja plaćanje, razlikuju se:⁹¹

- Međubankarska plaćanja, koja se obavljaju između banaka. Ako su banke inicijatori plaćanja, onda su to tzv. sopstvena plaćanja. Kada banka plaća realizaciju za račun klijenta, takvi tokovi se nazivaju platni promet. Međubankarska plaćanja se nazivaju plaćanja velikih vrednosti.
- Privredna plaćanja su plaćanja između preduzeća, kao i maloprodajna plaćanja (plaćanja između građana i preduzeća) i čine plaćanja male vrednosti. Prema broju operacija, to su najznačajnija plaćanja u unutrašnjem platnom prometu. Plaćanja koja se između privrednih subjekata obavljaju na Internetu nazivaju se Internet plaćanjima.

Prema funkcionalnim karakteristikama, sistemi elektronskog plaćanja mogu se podeliti u dve kategorije:

- prvo, na plaćanja zasnovana na sredstvima sa računa i
- drugo, na plaćanja koja se baziraju na kreditu.

Elektronska plaćanja podrazumevaju transfer novca i izvršenje plaćanja primenom elektronske tehnologije.

Elektronska plaćanja velikih vrednosti se obavljaju upotrebom privatnih informacionih mreža. Korisnici ovih mreža su banke i druge finansijske institucije. Ovakve mreže se koriste i za obavljanje međunarodnih plaćanja (kao što je mreža *S.W.I.F.T.* organizacije) i za unutrašnji platni promet (primer američke mreže *FEDWIRE*).

Plaćanja malih vrednosti se elektronski obavljaju uglavnom primenom platnih kartica. Najsavremeniji vid platnih kartica su platne kartice sa elektronskim očitavanjem informacija i one omogućavaju elektronska plaćanja, uglavnom primenom elektronskog prenosa sredstava sa mesta prodaje (engl. *electronic funds transfer at point-of-sale - EFTPOS*). Korišćenje Interneta kao komunikacionog kanala i u oblasti plaćanja, je uslovalo pojavu Internet plaćanja

⁸⁹ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, Beogradska poslovna škola, Beograd, 2005. str.261

⁹⁰ Isto, str. 263

⁹¹ Isto, str. 263

i odgovarajućih instrumenata kojima se ova plaćanja obavljaju i to: elektronske gotovine, elektronskih čekova i Internet platnih kartica.⁹²

Elektronska trgovina postavlja stroge zahteve u odnosu na sistem plaćanja. Elektronski sistemi plaćanja moraju biti pogodni za kupovinu na Web-u, prenosivi kroz mrežu, dovoljno jaki da spreče elektronske smetnje i troškovno isplativi za jako male vrednosti transakcija.

3.3. Međunarodna plaćanja

Da bi bankarske transakcije bile dovoljno brze i pouzdane i da bi zadovoljile potrebe sve obimnijeg međunarodnog poslovanja, banke od sedamdesetih godina XX veka koriste savremenu informacionu tehnologiju za elektronski transfer sredstava (engl. *electronic fund transfer*). Tako su nastala elektronska plaćanja, prva oblast elektronskog poslovanja. Elektronski sistemi su prvo korišćeni za bankarske transakcije u zemlji, a zatim su počeli da se koriste i u međunarodnim bankarskim plaćanjima.

Najznačajniji sistem za međunarodna bankarska plaćanja je međunarodna bankarska mreža SWIFT (*Society for Worldwide Interbank Financial Telecommunications*), osnovana 1973. godine. Osnivači su bile 239 banaka iz 15 zemalja, a mreža je postala operativna 9. maja 1977. godine⁹³. U mrežu su uključene banke iz Evrope, Amerike, Azije i Afrike. To je mreža zatvorenog karaktera, tako da pristup imaju samo članice. Svaka banka članica ima svoju SWIFT adresu. Mreža je sastavljena od niza manjih (regionalnih) centara tzv. *SWIFT Access Point*. Poruke u SWIFT-u su standardizovane i klasifikovane po nameni, u sledećih deset kategorija:⁹⁴

1. transferi za klijente,
2. bankarski transferi,
3. devizni i kreditno-depozitni odnosi,
4. naplate,
5. hartije od vrednosti,
6. plemeniti metali,
7. dokumentarni akreditiv,
8. specijalni platni mehanizam,
9. specijalne poruke,
10. opšte poruke.

Prednosti transfera sredstava putem SWIFT-a jesu:⁹⁵

- vremenski rok uručenja poruke je pet minuta za hitne poruke, odnosno 100 minuta maksimalno, za normalne poruke;
- efikasna kontrola prilikom emitovanja i uručenja poruka;
- bezbednost pri prenosu poruka, jer neovlašćeni korisnici ne mogu da budu na mreži;
- informacije o promenama i stanja međusobnih računa su ažurne, što omogućava bolje iskorišćenje sredstava;
- automatizacija obrade naloga jer su poruke standardizovane;

⁹² Bjelić P.: „Elektronsko trgovanje“, Institut za međunarodnu politiku i privredu, Beograd, 2000. str. 8

⁹³ URL: www.Swift.com

⁹⁴ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str. 264

⁹⁵ Materijal Udruženja banaka YU za seminar o SWIFT-u, str 7 i SWIFT Bulletin.

- smanjeni troškovi prenosa (uštede se kreću od 8,5 do 14 dolara po poruci).

Bankarska mreža SWIFT ima višestruku namenu, na primer: za direktna plaćanja u realnom vremenu uz više dodatnih usluga, za klirinška plaćanja velikih vrednosti i za razmenu hartija od vrednosti. Nebankarske finansijske institucije su dobile pristup SWIFT-u 1987. godine, tako da je sada moguć i kontakt sa brokerima i razmena hartija od vrednosti. Jedna od značajnih namena mreže vezana je i za Evropski sistem plaćanja u evrima TARGET, koji povezuje centralne banke EU i koji se obavlja preko SWIFT-a.

Procedura plaćanja je sledeća: banka putem SWIFT-a izdaje nalog drugoj banci, sa kojom ima kontokorentne odnose, da zaduži njen račun, a odobri račun korisnika plaćanja za navedeni iznos u SWIFT poruci. Ako je poruka napisana prema SWIFT standardima, obrada se u banci koja prima poruku može obaviti automatski.⁹⁶

3.4. Plaćanja u zemlji – poslovi platnog prometa

Elektronsku tehnologiju banke koriste i kada komuniciraju sa svojim klijentima u zemlji. Tada obično koriste FEDI (*Financial Electronic Data Interchange*), da bi mogle da razmenjuju ne samo dokumenta već i platne naloge. Klijenti elektronski upućuju naloge banci, koja ih zatim elektronski ispunjava. Na taj način se ubrzava platni promet. Prednost FEDI-ja je i u tome što je operativan 24 sata. Zloupotreba se sprečava korišćenjem različitih sigurnosnih sistema. Osim plaćanja, FEDI služi i za razmenu: informacija o obavljenom plaćanju, o stanju na računu klijenta, o budućim poslovima i slično. Da bi komunicirale sa svojim klijentima, banke imaju ugrađen FEDI server, koji prima i odašilje ne samo finansijske već i klasične EDI poruke. FEDI serveri mogu da primaju i SWIFT poruke, tako da se FEDI može koristiti i za komunikaciju sa ostalim bankama i finansijskim institucijama.⁹⁷

3.5. Međubankarska plaćanja

To su plaćanja između banaka, do kojih dolazi kada banka obavlja svoju posredničku ulogu u platnom prometu za račun svog klijenta. Kada je reč o međunarodnim međubankarskim plaćanjima, ona se uglavnom obavljaju po bruto ili direktnom sistemu plaćanja. Za međubankarska plaćanja u zemlji koriste se neto ili klirinški sistem plaćanja. Ukoliko je reč o plaćanjima koja banke obavljaju između sebe (i centralne banke), ona se nazivaju plaćanja velikih vrednosti. S druge strane, plaćanja koja banke obavljaju za preduzeća i građane nazivaju se plaćanjima malih vrednosti.

Pod bruto (direktnim) sistemom plaćanja podrazumeva se transfer celokupnog iznosa plaćanja i on je tehnički ispravniji jer se svako plaćanje odmah realizuje. Prepreka za razvoj tog sistema u mnogim zemljama jeste nedovoljna likvidnost banaka. Najsavremeniji sistem bruto plaćanja jeste sistem bruto poravnanja u realnom vremenu (engl. *Real Time Gross Settlement - RTGS*), u kojem se svi nalozi realizuju u toku istog dana, pa se stiče utisak da su plaćanja trenutna (u realnom vremenu). U tom sistemu, koji je tehnološki usavršen, sva plaćanja su elektronska. Većina zemalja ima te sisteme, mada su više u upotrebi sistemi neto poravnanja.⁹⁸

⁹⁶ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str. 265

⁹⁷ Isto, str. 265

⁹⁸ Isto, str. 266

Tabela 6: RTGS sistemi prema zemljama

Zemlja	RTGS sistem
SAD	FEDWIRE
Švajcarska	SIC (Swiss Interbank Clearing System)
Švedska	RIX
Irska	IRIS (Irish real-time Interbank Settlement System)
EU	TARGET

Izvor: Bjelić, 2000, str.119

FEDWIRE prvi je bruto sistem plaćanja, a razvijen je u SAD još kao telegrafski sistem, te odatle i naziv (*wire-tica*). Koristi se za plaćanja između komercijalnih banaka, jer one imaju otvorene račune kod neke od banaka iz sistema federalnih rezervi (engl. *FED*). Plaćanja su sada elektronska. U sistemu se nalazi oko 7.000 komercijalnih banaka, a dnevna vrednost obavljenih plaćanja iznosi više od 1.000 milijardi dolara.

TARGET je platni sistem Evropske monetarne unije. Uveden je radi sprovođenja jedinstvene monetarne politike i obezbeđenja efikasnog mehanizma za obavljanje međunarodnih plaćanja. Operativan od januara 1999. godine, sa početkom druge faze monetarne unije. Sistem se odnosi isključivo na evro transakcije, a zasnovan je na platnim sistemima RTGS zemalja članica EU i platnom sistemu Evropske centralne banke. Ti platni sistemi se objedinjuju preko jedinstvene računске i informatičke infrastrukture uz standardne procedure. SWIFT mreža, kao provajder za TARGET, nametnula se kao racionalno postojeće rešenje.⁹⁹

Sistemi za neto plaćanja (engl. *netting system*) podrazumevaju samo transfer salda svih plaćanja. Odnosno, transfer novca se obavlja u iznosu nekompenzovanih plaćanja – tzv. poravnanje (operacija poznata pod nazivom kretanje salda). Za takav sistem plaćanja, potrebno je manje angažovanje sredstava i zbog toga se mnogo koristi u unutrašnjim platnim prometima zemalja. Većina sistema za neto plaćanje prelazi na Swift kao kanal komunikacije. U budućnosti zemlje moraju da teže većoj likvidnosti i primeni RTGS sistema plaćanja.

Tabela 7: Netting sistemi prema zemljama

Zemlja	Netting sistem
Francuska	SNP – System net Protege
Španija	LCN – Local Currency netting System
Velika Britanija	CGO (the UK's gilts settlement system)

Izvor: Bjelić, 2000, str 120

Klirinška kuća (engl. *clearing house*) nastala je s mogućnošću da se obavi kliring ne samo između dve banke, već i između više banaka (multilateralna kompenzacija). Cilj tog sistema jeste prebijanje većih suma novca, odnosno, svođenje kretanja novca između banaka na najmanju moguću meru. Da bi se taj poduhvat efikasno obavio komercijalne banke se udružuju i osnivaju specijalne finansijske institucije – klirinške kuće, čija je funkcija organizacija kliringa između banaka članica (kasnije su i centralne banke u pojedinim zemljama osnovale klirinške kuće). Novina je kliring na području više zemalja, radi međunarodne trgovine, kao što radi CHIPS (*Clearing House Inter-Bank Payments System*), američka klirinška kuća, koju su 1970. godine osnovale komercijalne banke, da bi obavljala

⁹⁹ Isto, str. 267

elektronski kliring meću bankama članicama. Kliring je organizovala i na području evra Evropska organizacija klirinških kuća (engl. *European Clearing House - ECHO*).¹⁰⁰

Tabela 8: Klirinške kuće prema zemljama

Zemlja	Klirinška kuća
SAD	CHIPS , AGH (Automated Clearing House)
Velika Britanija	CHAPS Clearing House Automated Payment System B.A.C.S. Ltd. Bankers Automated Clearing Services
Nemačka	EAF
Irska	The Dublin Bankars Clearing
Španija	SNCE
Belgija	CEC
Poljska	KIR – Krajowa Izba Rozliczenioma

Izvor: Bjelić, 2000, str. 121

3.6. Maloprodajna plaćanja

Maloprodajna plaćanja obuhvataju finansijske transakcije u kojima krajnji potrošači plaćaju svoju robu u maloprodaji i to su uglavnom plaćanja male vrednosti. Odnos između maloprodaje i banaka uslovljen je funkcionisanjem platnog prometa zemlje. U maloprodajnim plaćanjima banke su posrednici i to:¹⁰¹

1. između maloprodaje i njenih dobavljača – maloprodaja plaća preuzetu robu ispostavljanjem naloga za prenos sredstava sa svog računa, na račun dobavljača, primenom finansijskog EDI-ja (*FEDI*);
2. između maloprodaje i krajnjeg potrošača – naplata proizvoda koje maloprodaja prodaje potrošaču primenom EFT sistema (engl. *electronic fund transfer*) sa mesta prodaje (engl. *point of sale*) – EFTPOS/EPOS. Na taj način se sredstva sa računa potrošača, prenose na račun maloprodavca, kod njegove poslovne banke. Pod elektronskim prodajnim mestom podrazumeva se primena računara na mestu naplate u maloprodaji, a sistem radi na principu prepoznavanja EAN brojeva za numeraciju artikala.

U maloprodajnim plaćanjima potrošač može da koristi različite instrumente plaćanja, kao što su: gotovina, čekovi ili platne kartice.

Platna kartica je nastala evolucijom čekovne kartice. One se najviše koriste u SAD, gde 75% stanovništva ima bar jednu karticu. Ta revolucija plastičnog novca, kako nazivaju platne kartice ima dinamičan rast. Postoji više vrsta platnih kartica, a dele se prema različitim kriterijumima: području primene, sistemu plaćanja, tehnici koja se koristi u naplati, nameni kartica.¹⁰²

3.7. Internet plaćanja

Internet trgovina je uslovila razvoj plaćanja preko Interneta, kako bi se što potpunije iskoristile prednosti ove globalne mreže. Pojava Interneta otvorila je novu eru o novcu i sistemima plaćanja. To su uglavnom, maloprodajna plaćanja, koja se obavljaju na Internetu.

¹⁰⁰ Isto, str. 268

¹⁰¹ Isto, str.268

¹⁰² Bjelić P.: „Elektronska trgovina“, cit.delo, str.147

Razvoj Interneta i sistema plaćanja preko njega otvorilo je velike mogućnosti za globalno poslovanje. Razvoj savremenih finansijskih instrumenata je omogućio da i međunarodna plaćanja postanu efikasna, pa je Internet tržište zaista globalno. Svi tradicionalni instrumenti su digitalizovani i imaju svoju Internet verziju.

Učesnici u procesu elektronskog plaćanja su:¹⁰³

- 1) Korisnik kartice – sklapa ugovor sa bankom i od nje dobija karticu. Obavezan je da ima kod banke tekući račun dinarski i devizni (ovaj drugi samo ako kartica može da se koristi i u inostranstvu).
- 2) Trgovac – sklapa ugovor sa bankom principalom o prijemu njenih kartica. Može imati veći broj ugovora sa različitim principalima, što znači da može primati više različitih kartica. Sklapa ugovor sa provajderom preko koga je povezan na Internet. Može se desiti da su provajder i trgovac ista firma. Takođe sklapa ugovor sa obračivačem (procesorom).
- 3) Provajder – sklapa ugovore sa obračivačem (procesorom) i sa trgovcem ili trgovcima, ukoliko je veći broj trgovaca kod jednog provajdera.
- 4) Obračivač (procesor) – sklapa ugovore sa bankama, provajderima i trgovcima.
- 5) Banka – sklapa ugovore sa: obračivačem (procesorom), trgovcima i korisnicima kartica.

3.7.1. Faze procesa plaćanja

Proces plaćanja roba i usluga preko Interneta može se podeliti u nekoliko faza.¹⁰⁴

- 1) Faza informisanja:
 - Pregled elektronskog kataloga ponuđenih proizvoda.
- 2) Faza dogovora i ugovaranja:
 - Registracija na strani trgovca;
 - Provera i potvrda autentifikacije;
 - Izbor servisa i slanje porudžbine;
 - Provera stanja na računu i kreditne sposobnosti;
 - Potvrda porudžbine.
- 3) Faza plaćanja:
 - Slanje kriptovanih podataka;
 - Provera i potvrda šifrovanih podataka;
 - Slanje ključa za dešifrovanje debitnog računa,
 - Dešifrovanje i potvrda servisa;
 - Slanje potvrde.
- 4) Faza bankarskog postprocesiranja:
 - Prijem podataka o izvršenim transakcijama;
 - Zaduživanje računa korisnika;
 - Formiranje zbirnih naloga po trgovcima;
 - Izvršenje plaćanja trgovcima.

¹⁰³ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.116

¹⁰⁴ Isto, str.117

Ovaj način plaćanja zahteva značajno povećanje broja učesnika u procesu plaćanja. Procedura rada je sledeća: Korisnik preko Interneta pronalazi trgovca i na njegovom sajtu bira robu. Sa svoje strane trgovac omogućava korisniku da on pretražuje njegov sajt, čeka robu i formira „potrošačku korpu“. Kada je korisnik završio sa punjenjem korpe, dakle, napravio je total za plaćanje, prelazi u sledeću fazu a to je plaćanje. Korisniku se na sajtu nudi izbor kojom će karticom obaviti plaćanje.

Korisnik bira karticu tako što klikne na nju. U tom trenutku korisnik napušta sajt trgovca i prelazi na sajt „procesora plaćanja“ i aktivira SSL. Procedura se dalje nastavlja tako što se korisniku otvara stranica za prijavu na sistem za plaćanje. Od korisnika se traži da popuni sledeće podatke: Ime i prezime, broj kartice, datum važenosti i PIN broj (engl. *Personal identification number*). Kada je sve ispunjeno dalju proceduru preuzima procesor plaćanja. Prvi nivo je provera podataka koji su uneti. Ako su svi podaci ispravni proverava se PIN kod, a ako je i to ispravno procedura se nastavlja tako što se proverava stanje na računu u banci kroz posebnu zaštićenu mrežu. Ukoliko stanje na računu pokazuje da ima novca, transakcija se odobrava, šalje se poruka procesoru plaćanja i on dalje obaveštava strane učesnice u transakciji da je sve izvršeno regularno. Procesor generiše broj pod kojim se vodi transakcija i dostavlja ga korisniku i trgovcu. Ovaj broj je značajan zato što ako nešto kasnije nije u redu, po njemu se obavljaju reklamacije. Ovim je sama transakcija plaćanja završena, ali je ostala faza bankarskog postprocesiranja. Pošto je banka skinula sredstva sa računa korisnika, potrebno je da taj novac doznači na račun trgovca. Ovo se dalje radi standardnim postupcima mećubankarskih plaćanja.

3.7.2. Principi sistema plaćanja

Bez obzira na tip sistema plaćanja, svaki sistem plaćanja počiva na sledećim osnovnim principima:¹⁰⁵

a) Poverenje

U osnovi, kupac bi trebalo da veruje da će mu prodavac zaista isporučiti robu. Zatim prodavac bi trebalo da veruje da će obećanje dato po pitanju plaćanja biti ispunjeno. Kada se kao sredstvo plaćanja koristilo zlato ili srebro, proveravao se njegov kvalitet na različite načine. Kada je u pitanju papirni novac, kao dokaz originalnosti služe vodeni žigovi i štampa na specijalnom papiru. Za kreditne kartice originalni mehanizam za uspostavljanje poverenja je upoređivanje potpisa kupca sa potpisom na polećini kartice. Mećutim, sa povećanjem broja prevara sa kreditnim karticama, postalo je veoma uobićajeno da se vrši on-line autorizacija, čak i za plaćanja male sume novca. Elektronsko plaćanje pomoću kreditnih kartica, koristi obe tehnike i digitalni potpis i on-line autorizaciju.

b) Bezbednost

Transakcija mora da se obavlja na siguran način. Za plaćanja u gotovom novcu, to je samo pitanje fizićke bezbednosti. Kod plaćanja kreditnom karticom, stvar je sloćenija. Kupac želi da detalji o njegovoj kreditnoj kartici ne budu otkriveni. Prodavac želi da bude siguran da će plaćanje biti izvršeno bez smetnje.

¹⁰⁵ Isto, str.118

Kriptografske tehnike se koriste za zaštitu od ovih rizika. U idealnom svetu, svi kupci i prodavci bi trebalo da budu potpuno poverljivi i sve transakcije bi bile potpuno bezbedne. U realnosti, svaka transakcija nosi određeni rizik i sistem plaćanja pokušava da minimizira taj rizik na način koji je adekvatan vrednosti plaćanja i opasnostima u okruženju u kome se odvija.

3.7.3. Instrumenti Internet plaćanja

Instrumenti Internet plaćanja su:

1. elektronska (digitalna) gotovina,
2. elektronski ček i
3. platne kartice za plaćanja na Internetu.

Elektronska (digitalna) gotovina (engl. *Electronic or digital cash*) predstavlja elektronske impulse koji se kao sredstvo plaćanja razmenjuju između učesnika elektronskih sistema plaćanja. Digitalna gotovina je digitalna forma čuvanja i razmene vrednosti koja ima ograničenu konvertibilnost u druge forme (roba, usluge), pa je potreban posrednik koji vrši proces konvertovanja vrednosti.¹⁰⁶

E-Cash je anonimni digitalni novac čija se ispravnost proverava on-line, od strane odgovarajuće finansijske institucije.

Iako već duže vreme postoje elektronski sistemi plaćanja, gotovina predstavlja i dalje značajan instrument plaćanja. Razlozi ovakvog stanja su nepoverenje u banke, ali i specifične karakteristike gotovine kao zakonskog sredstva plaćanja, što omogućava da se ona može razmenjivati bez posredovanja finansijskih institucija i svi subjekti je moraju primati.

Zato je 1994. godine holandska firma DigiCash konstruisala softver kojim se mogu obavljati plaćanja putem Interneta. U početku jedino je Mark Tven Banka prihvatila ovaj program, ali su ga kasnije prihvatili *Deutsche Bank AG*, *Swiss NetPay AG* i *Eunet*, a danas postoji više preduzeća koja pružaju takve usluge.

Potrošači povlače digitalni novac sa svog E-Cash računa upotrebom tzv. „slepe metode“ i skladište ga na fiksnom disku svog računara. „Slepa metoda“ funkcioniše na sledeći način:¹⁰⁷

Klijent šalje digitalnu novčanicu, sa šifrovanim serijskim brojem, finansijskoj instituciji. Finansijska institucija „overava“ novčanicu i šalje je nazad klijentu. Klijent zatim dešifruje serijski broj. Prema tome, serijski broj nije poznat finansijskoj instituciji, što garantuje anonimnost. Da bi se sprečila dvostruka potrošnja, finansijska institucija mora da evidentira serijske brojeve svih prispelih digitalnih novčanica. Pri svakoj kupovini preko Interneta, potrošač daje digitalne novčanice trgovcu. Trgovac odmah upućuje ove novčanice u svoju banku, kako bi proverio da li su ispravne. Trgovčeva banka registruje brojeve emitovanih digitalnih novčanica, bez mogućnosti identifikacije potrošača koji ih je utrošio. Konačno, ako je sve u redu, saldo na računu trgovca povećava se za dati iznos, a trgovac isporučuje proizvode ili usluge.

¹⁰⁶ Vidas-Bubanja M.: „E - poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str. 277

¹⁰⁷ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.119

Digitalne novčanice mogu se koristiti samo jednom. E-Cash se može smatrati valutom za sebe. Finansijske institucije moraće da koriste specijalne račune. One će, takođe, garantovati konverziju u realni novac. Zbog toga će centralne banke imati poteškoće pri kontrolisanju novčane mase, jer finansijske institucije mogu kreirati dodatni novac i time povećati novčanu masu.

Bezbednost E-Cash-a postiže se upotrebom asimetričnog kriptografskog algoritma.

Pristup računaru može dodatno biti zaštićen upotrebom ličnih lozinki. Registrovanjem serijskih brojeva digitalnih novčanica sprečava se dvostruko trošenje. Troškovi provere autentičnosti digitalnih novčanica su relativno veliki, jer provera treba da se obavi on-line. To znači da je pogodnost ovog sistema za mikro-plaćanja (plaćanja u veoma malim iznosima) pod znakom pitanja. Svako lice koja ima E-Cash račun može da prima E-Cash novčanice. Danas se E-Cash-om obavlja većina digitalnih transakcija na Internetu, ali je njegova budućnost neizvesna zbog odlučnog instiranja na potpunoj anonimnosti, čime je ukinuta bilo kakva mogućnost praćenja transakcija.

Elektronski čekovi (engl. *Electronic cheques*) su elektronski platni instrumenti koji se putem specijalnih softvera ispisuju na računaru i preko raznih komunikacionih sredstava upućuju korisniku plaćanja. Konceptijski se zasnivaju na klasičnim papirnim čekovima, ali imaju elektronski oblik i potpisuju se i indosiraju¹⁰⁸ primenom digitalnih potpisa. Pošto su papirni čekovi i dalje najvažniji instrument bezgotovinskog plaćanja, smatra se da će i njihov elektronski oblik biti popularniji od elektronske gotovine. Prednosti koje pružaju elektronski čekovi su:¹⁰⁹ popunjavaju se na sličan način kao i klasični čekovi, mogu se koristiti i za plaćanja malih vrednosti, jer sistem njihove kriptografske zaštite ih čini pogodnim za kliring. Proces plaćanja čekom sastoji se od nekoliko faza:¹¹⁰

1. Platilac najpre dobija od emitenta, kod koga ima otvoren račun, softver i ovlašćenje za izdavanje čekova,
2. Na osnovu softvera platilac piše ček za kupljenu robu i usluge i šalje ga korisniku plaćanja,
3. Korisnik šalje ček emitentu na autentifikaciju i naplatu,
4. Po izvršenoj autentifikaciji, emitent obaveštava korisnika o ispravnosti i
5. Vršiti plaćanje preko banke korisnika za račun korisnika,
6. Banka korisnika obaveštava svog klijenta da mu je račun odobren.

Trenutno postoji nekoliko firmi koje organizuju plaćanja elektronskim putem čekovima i to:

Tabela 9: Firme koje organizuju plaćanja elektronskim putem

Firma	Instrument	Plaćanja
Univerzitet Južne Kalifornije	NetChegue	Plaćanja bez ograničenja iznosa
BankNet	e-cheque	Plaćanja za robu i usluge

NetCheque je najpopularniji sistem elektronskih čekova. Razvio ga je Univerzitet Južne Kalifornije, ista ustanova koja je razvila NetCash. Plaćanje se odvija preko NetCheque

¹⁰⁸ Indosament je tehnika prenošenja čekova u vlasništvo drugog lica i sastoji se od naredbe sa potpisom starog vlasnika.

¹⁰⁹ Bjelić P. : „Elektronsko trgovanje“, cit.delo, str.156

¹¹⁰ Isto, str.156

računovodstvenog servera i korisnici ovog servera mogu jedni drugima da plaćaju za robu i usluge koristeći e-mail, ili neku drugu mrežu.

Konzorcijum za tehnologiju finansijskih usluga (FSTC) je angažovan na izgradnji unifikovanog čekovnog sistema na Internetu.

Platne kartice za plaćanja na Internetu (engl. *ON-line payments credit cards*) su najčešće primenjivani platni instrumenti na Internetu. Plaćanje se obavlja tako što se po kupovini trgovcu šalju podaci sa platnih kartica kako bi on od banke emitenta naplatio iznos računa. Strane koje učestvuju u toj transakciji su: kupac, prodavac, klirinška kuća, banka prodavca i banka koja je izdala kupčevu kreditnu karticu. Da bi moglo da se realizuje online plaćanje, prodavac mora da ima otvoren račun kod banke, preko koga se mogu procesuirati plaćanja ove vrste i primati sredstva po osnovu računa na osnovu kojih su izdate kreditne kartice.

Koraci u upotrebi kreditnih kartica u online transakciji¹¹¹

- 1.korak Kupac je izabrao proizvode i stavio u svoja kolica na Web-u
- 2.korak Kada kupac želi da plati za kupljeni proizvod, kreira se sigurni tunel kroz Internet upotrebom SSL standarda. Koristeći šifrovanje, SSL osigurava prolazak informacija o kreditnoj kartici do trgovca.
- 3.korak Kada je dobio informacije o podacima sa kreditne kartice kupca, trgovčev softver kontaktira klirinšku kuću – posrednika.
- 4.korak Klirinška kuća verifikuje račun i utvrđuje stanje na računu sa bankom kupca koja je izdala karticu.
- 5.korak Banka kupca upućuje potreban iznos na račun trgovca.
- 6.korak Kupac mesečno dobija izveštaj o iznosima koje je utrošio sa svog računa (kartice).

Dobra strana ovog načina plaćanja je što korisnik u trenutku kada pronađe ono što je tražio može odmah da plati, a da za kratko vreme na naznačenu adresu dobije poručenu i plaćenu robu. Sa stanovišta trgovca, ovo je dobar metod jer istog trenutka kada je roba poručena, dobijen je i novac za nju. Kupcu je ovo najkonforniji način plaćanja.

Najveći problem sa upotrebom ovih kreditnih kartica jeste sigurnost. Mnoge kompanije rade na izradi sigurnosnih protokola za plaćanje preko Interneta (*SSL, SET*), ili procedura za dobijanje autorizacije treće strane (npr. *Virst Virtual*).

Protokol SSL (*Secure Socket Layer*), koji je danas široko prihvaćen, obezbeđuje potrebnu zaštitu poverljivosti podataka za vreme njihovog prenosa, upotrebom asimetričnog sistema šifriranja. Međutim, pomoću njega ne može da se obezbedi utvrđivanje autentičnosti učesnika u transakciji (kupca i prodavca), što znači da ne može da se obezbedi zaštita u pogledu sprečavanja odustajanja ili opoziva plaćanja isporučene robe i obrnuto.

U transakciji sa SSL zaštitom, prodavac prima informacije sa kreditne kartice kupca, a zatim ih preko svog softvera dostavlja klirinškoj kući na potvrđivanje autentičnosti kreditne kartice i verifikaciju raspoloživosti potrebnih sredstava (engl. *account balance*), što klirinška kuća obavlja dobijanjem informacija putem svog kontakta sa bankom koja je izdala karticu. Nakon

¹¹¹ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str. 273

ove verifikacije, banka izdavalac kartice odobrava sredstva prodavcu (preko njegove banke) i zadužuje račun kupca za iznos svih kupovina u određenim intervalima.¹¹²

U cilju prevazilaženja problema koji su ostali nerešeni primenom SSL standarda, koncipiran je SET protokol (*Secure Electronic Transaction*). Ponučen je kao otvoreni standard za e-trgovinu od strane MasterCard i Visa institucija u cilju podizanja stepena sigurnosti plaćanja kreditnim karticama. Težiste ovog protokola je usmereno upravo na rešavanje problema koji proizilaze iz nemogućnosti međusobne identifikacije prodavca i kupca, što se obezbeđuje posebnim dodatkom za identifikaciju (utvrđivanje identiteta) pošiljaoca, u poruci koja se šalje. Institucije koje izdaju kreditne kartice, svoje članove snabdevaju digitalnim certifikatima u određenim digitalnim torbicama (engl. *digital wallet*) za upotrebu u online transakcijama. Prodavca koji se uključuje u online transakciju, sličnim certifikatom snabdeva njegova banka. Sam proces plaćanja je sličan standardnoj online transakciji plaćanja kreditnom karticom, izuzev što uključuje identifikaciju kupca i prodavca. U tipičnoj transakciji kupac bira plaćanje sa SET opcijom („*Payment with SET*“) na sajtu i karticu koju želi da koristi. Server prodavca može da vrši identifikaciju kupca, kao što kupac može da identifikuje prodavca.¹¹³

U sistemu obezbeđenja plaćanja dobijanjem autorizacije treće strane, posebna institucija funkcioniše kao posrednik između e-kupca i e-prodavca, koji su kod nje registrovani i imaju otvorene račune, preko kojih se obavlja plaćanje. Celokupna komunikacija se obavlja elektronskom poštom. Tehnički, ovaj offline model ne koristi Internet uopšte za obavljanje finansijskih transakcija, već samo za slanje i potvrđivanje naloga, dok najosetljivije delove finansijskih transakcija obavlja preko privatnih mreža (preko *ACH* i *First USA Merchant Services*).

Primer ovog načina obezbeđenja sreće se kod *First Virtual*, a sama transakcija bi se obavljala po sledećoj proceduri:¹¹⁴

Kupac se registruje kod *First Virtual* banke i kod nje se evidentira broj kreditne kartice, primajući istovremeno svoj identifikacioni broj. Prilikom kupovine, on bi trgovcu elektronskom poštom slao poruku u kojoj bi navodio broj svog računa. Prodavac dobijeni broj kupca, šalje takođe elektronskom poštom *First Virtual* banci radi identifikacije i verifikacije kupca, pri čemu prodavac ni u jednom trenutku ne zna lični identitet kupca. Kada *First Virtual* banka izvrši identifikaciju kupca, elektronskom poštom mu šalje upit za dobijanje potvrde o obavljanju kupovine i odobrenja za izvršavanje plaćanja, na šta kupac odgovara na isti način.

Za plaćanja preko Interneta najviše se koriste elektronske kartice sa čipom i njih izdaju sledeće firme:

Tabela 10: Elektronske kartice sa čipom

Firma	Filijala	Vrsta instrumenta	primer
MasterCard	MasterBanking	Platne kartice sa čipom	
Visa int.	Visa Interactive	Platne kartice sa čipom	Next card
Mondex	Mondex.com	Memorisanje 5 valuta na kartici	

¹¹² Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.158

¹¹³ Isto, str.158

¹¹⁴ Isto, str.159

Ograničenja online sistema plaćanja pomoću kreditnih kartica su sledeća:¹¹⁵

- sigurnost, jer postojeći sistemi nude nizak nivo sigurnosti;
- trgovački rizik, budući da postoji veliki rizik za trgovca da kupac odbije da plati troškove, iako je roba isporučena, ili je digitalni sadržaj preuzet;
- troškovi, koji su za trgovca, takođe značajni – oko 3,5% od vrednosti kupovine plus dodatni izdaci za transakcionu maržu od 20 do 30 centi po transakciji, plus ostali troškovi vezani za pribavljanje potrebnih alata za takav način poslovanja (hardver + softver). Otuda se trgovcu ne isplati online prodaja robe čija je cena niža od 10 dolara po jedinici;
- socijalna jednakost, jer svi potencijalni kupci nemaju pristup kreditnim karticama.

Dok su maloprodajna plaćanja osvojila Internet, međubankarska plaćanja još nisu počela da se obavljaju preko ove mreže, zbog još uvek prisutne nesigurnosti, kada se radi o velikim iznosima transfera. Ipak Internet je budućnost međubankarskih transfera, o čemu govori i odluka SWIFT-a o postepenom prelasku na Internet komunikaciju uz primenu sigurnosnih internet protokola (SIP) i EDIFACT standarda.¹¹⁶

Nastanak novih zaštitnih sistema će pomoći da se razvije kompletno bankarsko-finansijsko poslovanje na Internetu, jer se kao motiv pojavljuju znatno niži troškovi poslovanja. Sistem zaštite ne sme suviše povećavati troškove poslovanja, kako ne bi postalo neracionalno da se posluje na Internetu, ali u isto vreme troškovi sigurnosnog sistema su mali kada se ima u vidu potencijalna šteta nastala neovlašćenim upadom u sistem banke.

Za većinu novih sistema digitalnog plaćanja neophodna je neka forma digitalnog-elektronskog novčanika (engl. *electronic wallet*, *e- wallets*). Reč je o softverima koje koriste potrošači za plaćanja preko Interneta. Oni na svojim programima kreiraju elektronske impulse koji predstavljaju novac. Softverom se ti impulsi šalju i u njemu se i čuvaju – na osnovu toga su dobili naziv.

Digitalni novčanik obavlja sledeće značajne funkcije:¹¹⁷

- 1) autentifikacije kupca pomoću digitalnog sertifikata, ili drugih kriptografskih tehnika,
- 2) čuva i transferiše vrednost i
- 3) osigurava proces plaćanja između kupca i trgovca.

Tim svojim funkcijama, digitalni novčanik obezbeđuje kupcu značajne prednosti. Naime, kupac sada može da ide na bilo koju Web stranu i da pomoću svog digitalnog novčanika obavlja svoju autentifikaciju i plaća sve što želi da kupi, pomoću bilo kog sistema plaćanja – digitalnih kreditnih kartica, digitalnih čekova itd. Za kupca digitalni novčanik značajno snižava transakcione troškove, jer više nije potrebno da ispunjava formulare sa različitim podacima pri svakoj online kupovini. Pritiskom na digitalni novčanik, softver novčanika daje sve informacije o kupovini i isporuci robe.

Određene prednosti od upotrebe digitalnog novčanika imaju i trgovac i finansijski posrednik. Trgovac takođe snižava transakcione troškove, povećava svoje mogućnosti za marketing i

¹¹⁵ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.274

¹¹⁶ Bjelić P.: „Elektronsko trgovanje“, cit.delo, str.158

¹¹⁷ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.275

lakše dolazi do posetioca svojih Web strana koji će brzo odlučiti da postanu i kupci. Prednosti finansijskog posrednika vezane su za maržu koju naplaćuje prilikom ostvarivanja tih transakcija.

Postoje dve kategorije digitalnih novčanika:¹¹⁸

- *Client based* digitalni novčanici su softverske aplikacije koje kupci moraju da instaliraju na svoje računare i koje im omogućavaju automatsko popunjavanje upitnika i formulara pri online kupovinama. Isti softver moraju da instaliraju i trgovci da bi mogli da primaju informacije iz client based digitalnih novčanika. *Gator.com* i *Mastercard Wallet* primer su za tu kategoriju novčanika.
- *Server based* digitalni novčanici su softversko rešenje za usluge autentifikacije i plaćanja koje se prodaje finansijskim institucijama, a one prodaju ta rešenja trgovcima direktno, ili kao deo svoje finansijske usluge. Inicijalni provajderi softvera obezbeđuju infrastrukturu koja je neophodna za funkcionisanje celog koncepta tako da za te novčanike, kupci ne moraju da instaliraju posebne softvere na svojim računarima i softveri se mogu lako dinamički obnavljati. Taj koncept novčanika je više prihvaćen, a jedan od najpopularnijih je server based digitalni novčanik *Microsofts Passport*. Trenutno je besplatno dostupan trgovcima i kupcima.

Očigledno je da će tehnika digitalnih novčanika pružati korisnicima sve prednosti, tek kada bude široko prihvaćena i među trgovcima i među kupcima, što će marginalne prednosti učiniti značajnim za svakog pojedinačnog učesnika u transakciji.

Internet plaćanja će se u budućnosti razvijati u pravcu olakšane primene instrumenata plaćanja, jedinstvenih standarda i bolje zaštite.

3.8. Korporativna elektronska plaćanja

3.8.1. Pojam i razvoj

Korporativno e-bankarstvo se odnosi na usluge koje banke pružaju velikim, poslovnim i korporativnim klijentima. Specifičnost ovog segmenta usluga je u tome što su one izrazito personalizovane i kao takve posebno naručivane. Ova specifičnost se može videti na nekim od ponuda usluga iz ovog domena od strane individualnih banaka. Npr. *Citibank* nudi naplatu računa, upravljanje novčanim tokovima, čuvanje, rukovanje i trgovinu sa hartijama od vrednosti; *Deutsche Banke* nudi upravljanje novčanim tokovima i kompletnim portfoliom, *Bank of America* obavljanje poslova na tržištu kapitala; *Royal Bank* poslove sa akreditivima i uopšte poslove vezane za izvoz i uviz itd. Da bi banke odgovorile na tražnju svojih najkrupnijih klijenata za ovakvom vrstom usluga, često se udružuju sa tehnološkim provajderima. Tako su npr. *Citibank* i *Bott mline technology* kreirali sistem online naplate računa; *Bank One* i *EDS* solucije za integrisanje fakturisanja plaćanja i sl.

Istorijski posmatrano, prvi oblici ovih usluga razvijani su na istim tehničko - tehnološkim osnovama kao i sistem kućnog bankarstva za stanovništvo.

Sistem upravljanja novčanim tokovima (engl. *Cash Management*) je jedan od prvih i esencijalnih proizvoda elektronskog, samouslughnog bankarstva u preduzeću. Pojavio se u

¹¹⁸ Isto, str.275

SAD-u kao bankarski proizvod namenjen multinacionalnim kompanijama, a njegov primarni cilj bio je usmeren na kontrolu tokova sredstava u različitim valutama, u jednoj ili većem broju banaka. Realizacija ovakvog zahteva podrazumevala je pružanje obimnih informacionih usluga klijentima, usled čega se upravljanje novcem transformiše u upravljanje celokupnim portfoliom i pružanje online platno prometnih usluga.¹¹⁹

Dalji razvoj korporativnog e-bankarstva je pod uticajem kombinacije rasta upotrebe Interneta i Web tehnologija, sa trendovima ekonomske globalizacije i koncentracije finansijskih usluga. Kao komunikaciona platforma za poslovanje koja nudi univerzalnu povezanost, Internet nudi i dodatne beneficije i potencijale za redukciju troškova. Prednosti se odnose prvenstveno na proširivanje ovih mogućnosti na sva preduzeća, bez obzira na njihovu veličinu.

U cilju prevazilaženja problema koji su proizilazili iz odvojenosti trgovinskih tokova i tokova plaćanja, uvodi se koncept direktnog procesinga ili STP (engl. *Straight-through-Processing*). On se bazira na ideji da se podaci samo jednom unose u određenu bazu i da se iz nje koriste prenosom za potrebe procesinga svih faza u proceduri elektronske trgovine. Cilj je da se na bazi smanjivanja broja unosa podataka i automatizacije omogućiti dodatno povećanje efikasnosti, smanjivanje grešaka i rizika. Na bazi ovog pristupa, najpre se teži ostvarenju beneficija u relacijama banka-banka, ili banka-klijent, a kasnije beneficije po tom osnovu postaju nedovoljne. U cilju podizanja stepena ostvarivanja dodatnih koristi prelazi se na tzv. „end-to-end“ integraciju u povezivanju preduzeća (B2B) preko banaka. Sa takvim konceptom javlja se i potreba za jedinstvenom dostupnošću bankarskih mreža privrednim društvima širom sveta, kako bi ona mogla lako da vrše plaćanja na globalnom nivou, preko jedne platforme, koja bi bila povezana sa internim računovodstvenim i drugim sistemima.¹²⁰

Posebne aktivnosti sprovode se u oblasti prekogranične trgovine, koja je tradicionalno bila skupa i obimna, karakterisala se logističkom i vremenskom neefikasnošću, kao i visokim troškovima. Zahtevala je veći broj finansijskih i robnih dokumenata (akreditiv, menicu, ...). Banke uočavaju da elektronskim distribuiranjem tih dokumenata (sa digitalnim potpisom) različitim tržišnim učesnicima, mogu da obezbede skraćivanje vremena i snižavanje troškova. Zbog toga velike multinacionalne banke počinju da razvijaju nove finansijske solucije da bi pomogle korporacijama da ubrzaju automatizaciju tokova plaćanja i procese finansiranja trgovine. Jedan od najznačajnijih projekata u toj oblasti je BOLERO (*Bills of Lading Electronic Registry Organization*).

3.8.2. Integracija komercijalnih i finansijskih informacija

Evolutivni razvoj elektronske trgovine pokazuje visok stepen zavisnosti od opšteg tehnološkog razvoja i mogućnosti integracije različitih elemenata, koji se u početku razvijaju izolovano u heterogenim poljima, a kako dolazi do njihove progresije počinju da se integrišu po više osnova i širom sveta. Kao ključni elementi elektronske trgovine, EDI i EFT su implementirani u različitim formama i različitim poslovnim funkcijama, pri čemu je EFT sve više potiskivao elemente papirnih sistema plaćanja u finansijskom sektoru, a EDI elemente papirnih sistema u trgovini.

EDI (Elektronska razmena podataka) je jedna od prvih tehnologija koja je obezbeđivala tačnost i pravovremenost informacionog (dokumentacionog) toka, koji prati fizički tok robe i

¹¹⁹ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.164

¹²⁰ Isto, str.165

predstavlja sastavni deo same transakcije. U funkciji rešavanja informacionih potreba poslovnih transakcija, EDI je u principu mogao da zameni bilo koji papirni dokumenat čija se razmena vrši između kupca i prodavca. EDI se koristio za razmenu dokumenata kao što su narudžbenice, fakture, priznanice, špediterski prateći dokumenti. Svi ovi dokumenti su bili u elektronskoj formi, lako su se primali, slali i brzo su stizali na svoje odredište. Na ovaj način su eliminisana kašnjenja koja su posledica slanja papirne dokumentacije, prepisivanja i umnožavanja. Pošto je proces automatizovan to je i cena formiranja i slanja dokumentacije znatno niža.

EDI se može definisati kao: „razmena strukturiranih poslovnih podataka između računara zasebnih firmi, izvršena bez manuelne intervencije, elektronskim putem, posredstvom standardizovanih poruka koje zamenjuju tradicionalne papirne dokumente“.¹²¹

U ranim fazama je bilo praktično moguće i prihvatljivo direktno komuniciranje između trgovinskih partnera. Ovaj način je od partnera zahtevao slične komunikacione protokole, iste brzine prenosa, istovremenu raspoloživost linija i kompatibilnost računarskih sistema. Kako su ovi uslovi bili sve teže ostvarivi sa multipliciranjem broja partnera, rešenje je načeno u uvođenju posebnih informacionih mreža (VAN-ova), koje su obično pružale i dodatne usluge. Sami podaci su se u ranim fazama prezentirali u privatnim formama, zasnovanim na dogovoru manjeg broja partnera, da bi kasnije, sa multipliciranjem broja učesnika sposobnih za elektronsko poslovanje, bili zamenjeni nacionalnim i internacionalnim standardizovanim formatima.¹²²

Kao mehanizam koji se koristi za slanje „digitalnog novca“ kroz mrežu, sa jednog računa na drugi, EFT predstavlja srž elektronskog plaćanja između privrednog društva, države i drugih institucija, samim tim i elektronske trgovine uopšte. Njegova funkcija u elektronskoj trgovini je da obezbeđuje razmenu informacija potrebnih za prenos monetarne vrednosti elektronskim putem sa jednog računa na drugi, bilo direktnom međubankarskom komunikacijom, ili preko posrednika. Specifična karakteristika ovog mehanizma sastoji se u tome što zahteva izuzetno visok nivo tačnosti i sigurnosti u procesima provere autentičnosti i davanja autorizacije. Međutim, primenom ovih mehanizama obezbeđuje se samo autorizacija za prenos sredstava sa računa kupca na račun prodavca, odnosno samo međusobni obračun između kupca i prodavca. Kako se plaćanja vrše kao kompenzacije, ili naknade za prijem robe ili usluga, a na bazi informacija iz odgovarajućih dokumentacija, u praksi se problem odvojenosti ovih oblasti dugo pojavljuje kao „mrtav čvor“ u daljem unapređivanju trgovinskih procesa.

U takvim uslovima bilo je moguće vršenje plaćanja elektronskim putem, a da se istovremeno poslovna komunikacija partnera obavlja na klasičan način i obrnuto. Kako je parcijalna primena značila odvojenost tokova prenosa komercijalnih od finansijskih informacija potrebnih za prenos sredstava sa računa kupca na račun prodavca, poslovni proces je i dalje zahtevao naknadno sravnjivanje informacija koje su u jednom segmentu dobijane elektronskim putem, sa informacijama koje su u drugom segmentu dobijane na papiru. Zbog toga su mnoge potencijalne beneficije izostajale, a u mnogim slučajevima se zaključivalo da ne dolazi do bitnijeg smanjenja troškova papira i rada.

Kako parcijalna primena EDI tehnologije često nije dovođila do dovoljnog unapređenja u pogledu ekonomičnosti i efikasnosti poslovanja, sa povećanjem dometa njene primene sve se više uočava potreba za elektronskim povezivanjem trgovinskih i finansijskih tokova, a ovo

¹²¹ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit.delo, str. 182

¹²² Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.166

povezivanje dobija i svoj poseban terminološki izraz-finansijski EDI (FEDI). Nastaje prirodno kao rezultat porasta broja funkcionalnih oblasti i odnosa, koji se pokrivaju interorganizacionim informacionim sistemima i činjenice da potencijalne mogućnosti njegove primene prevazilaze zamenu papirnih dokumenata elektronskim ekvivalentima.¹²³

Za razliku od EDI-ja koji je korišćen za međusobnu komunikaciju partnera direktno ili preko VAN-ova, FEDI često uključuje mnogo kompleksnije operacije i zahteva znatno širu infrastrukturu mrežu. Po pravilu, tu se uključuje najmanje 4-5 učesnika, trgovinskih partnera i banaka. U suštini, uspostavlja se veza segmenata koji su funkcionalno povezani, mada ne i identični. Zbog toga što uključuje i bankarski sistem on je najkomplikovaniji, ali zato i najviše doprinosi redukciji papira i rada. Sa ubrzanim razvojem elektronskog trgovanja postaje sve značajniji. Međutim, da bi FEDI bio stvarno koristan i dužniku i poveriocu, odnosno kupcu i prodavcu, potrebno je da svako od njih, kao i njihove banke da budu u potpunosti osposobljene za ovu funkciju.

3.8.3. Uvođenje koncepta STP

Koncept direktnog procesinga ili STP (engl. *Straight-Through-Processing*) uveden je na inicijativu Asocijacije za globalni STP (engl. *Global Straight Through Processing Association - GSTPA*), grupe koja deluje na globalnom nivou i koja je otvorena za sve investicione menadžere, brokere i dilere uključene u proces međunarodne trgovine. Sama inicijativa pojavila se kao rezultat nastojanja da se reše problemi koji dolaze do izražaja u uslovima nepotpune integrisanosti u poslovnim tokovima i procesima međunarodnog trgovanja. Operacionalizacija STP kasnije sobom donosi radikalne promene u mnogim segmentima obavljanja bankarskih delatnosti.

Inicijalna primena koncepta STP vrši se upravo u međunarodnoj trgovini zbog toga što su svi nedostaci nedovoljne integrisanosti upravo kod nje posebno dolazili do izražaja. Upravo ona se u tradicionalnim uslovima karakteriše obimnim manuelnim aktivnostima, velikim brojem provajdera, nedostatkom standardizacije, relativno visokim stopama grešaka, visokim gubicima i sl. Najnoviji ekonomski, demografski i finansijski trendovi (porast međunarodnog investiranja) potenciraju dodatno uticaj svake od prethodno pomenutih karakteristika.

Automatsko procesiranje posla može da reši samo deo problema. Tipično finansiranje trgovine akreditivom koje zahteva 15 dana za obradu i obuhvata 12 dokumenata, može biti smanjeno na par dana uz izrazito smanjenje direktnih i indirektnih troškova. Međutim, ukoliko postoji nekonzistentnost između podataka u preduzeću i eksterno, kod trgovinskih partnera ili korisnika, neće biti realizovane beneficije procesa automatizacije u potpunosti. To znači da će preduzeću biti potrebno više vremena i napora da bi se izvršila usklađivanja koja zahteva kompletiranje transakcije, kao i da greške u trgovini ne mogu biti identifikovane i automatski ispravljene. Zbog toga se jednostavno povezivanje smatra nedovoljnim, a postizanje mnogo višeg stepena integracije kroz STP postavlja kao imperativ.¹²⁴

Primarni zadatak koncepta STP odnosio se na ubrzanje informacionih trgovinskih tokova, stvaranje uslova za smanjivanje broja nerealizovanih međunarodnih transakcija i drugih rizika, kao i troškova trgovinskog saldiranja. Za ostvarivanje ovih zahteva bilo je potrebno obezbeđivanje visokog stepena međupovezanosti između svih učesnika uključenih u različite

¹²³ Isto, str.167

¹²⁴ Isto, str.169

faze trgovinskog procesa u širem smislu (uključujući i pre-trgovinske i post-trgovinske procese).

Polazna ideja za dizajniranje koncepta STP je minimiziranje ljudske intervencije u obavljanju kompletnih poslova trgovanja i saldiranja pomoću „glatkih“ *front-to-back* integracija (engl. *seamless integration*). Prema ovom konceptu, podaci se samo jednom unose u određenu bazu, a iz nje se direktnim prenosom koriste za potrebe procesinga svih narednih faza i od strane različitih učesnika u procesu obavljanja elektronske trgovine. Suština je u mogućnosti da se na bazi smanjivanja broja unosa podataka i automatizacije omogući dodatno povećanje ekonomičnosti, efikasnosti, smanjivanje grešaka i rizika.

Pored ubrzanja tokova prenosa komercijalnih i finansijskih informacija potrebnih za kompletiranje procesa plaćanja, koncept STP pruža mogućnosti za tzv. *end-to-end procesing* i povezivanje sa mnogim pratećim administrativnim aktivnostima (upravljanje novčanim tokovima, kreditiranje i sl.). Tu se ne radi samo o uštedi troškova i podizanju operacione efikasnosti u kompaniji, već o fundamentalno novom načinu obavljanja poslova. Zbog toga se očekuje da će ova oblast biti jedan od najznačajnijih investicionih prioriteta za finansijske institucije u narednih nekoliko godina.¹²⁵

Na bazi ovog pristupa, se najpre teži ostvarenju beneficija u relacijama banka-banka, ili banka-klijent, a kasnije se postignuta unapređenja po tom osnovu pokazuju nedovoljnim. U cilju podizanja stepena ostvarivanja dodatnih koristi prelazi se na tzv. „end-to-end“ integraciju u povezivanju privrednih društava (B2B) preko banaka. Sa ovakvim konceptom javlja se i potreba za jedinstvenom dostupnošću bankarskih mreža privrednim društvima širom sveta, kako bi ona mogla lako da vrše plaćanja na globalnom nivou, preko jedne platforme, koja bi bila povezana sa internim računovodstvenim i drugim sistemima.

Kompanije danas zahtevaju mnogo sofisticiranije finansijske analize i dodatne usluge koje se šire van prostog prijema uplata i vršenja isplata na celokupno finansijsko upravljanje. One zahtevaju razumevanje poslovanja blagajne, upravljanje likvidnošću i novčanim tokovima koji su u vezi sa kliringom i saldiranjem, elektronskim bankarstvom, netting-om i poolingom, kao i problemima valutnog i kamatnog rizika. Mnoge multinacionalne korporacije sve više traže načine, da automatizuju izmirenje računa kroz sisteme kliringa i saldiranja i preko Interneta. One, takođe, već duže osećaju potrebu za unapređenjem standarda u ovoj oblasti.

Da bi se obezbedilo dobro i integrisano koordiniranje svih funkcija i procesa između različitih zainteresovanih poslovnih entiteta, kupaca, prodavaca i njihovih banaka, potrebno je precizno utvrđivanje uloge i odgovornosti svakog pojedinačnog učesnika (kupca, prodavca, banke, regulatorne institucije i provajdera servisa i logistike). U tom cilju Aberden grupa (*Aberdeen Group*) je postavila okvir upravljanja finansijskim lancem vrednosti (engl. *Financial Value Chain Management - FVCM*), koji pruža sistemski pristup ulozi i odgovornosti svih pojedinačnih učesnika u finansijskom lancu vrednosti. Koncept koji je postavljen 2001. godine, finansijski lanac vrednosti (engl. *Financial Value Chain-FVC*) definiše se kao skup međusobno povezanih funkcija i procesa na kojima se zasnivaju B2B intra i inter kompanijske transakcije, što znači da obuhvata i informacije koje se odnose na kretanje dobara i usluga.¹²⁶

Prema ovom konceptu, FVC se sastoji od podprocesa koji povezuju različite komponente i funkcije sa njihovim izvršiocima. Dva glavna segmenta su: segment kreiranja transakcije i

¹²⁵ Isto, str.170

¹²⁶ Isto, str. 171

segment saldiranja. Za prvi segment relevantne su četiri komponente (kvalifikacija, finansiranje, cena, obezbećenje), a za drugi segment pet komponenti (fakture, pregledi, reklamacije, plaćanja i analize). Kako se ova analiza bavi problemima plaćanja, ključni značaj imaju sledeće dve komponente: „finansiranje“ i „plaćanje“. Prva komponenta odnosi se na pitanja bankarskog finansiranja kupca za izvršenje plaćanja i u velikoj meri je vezana za problem kreditnog rizika. Tipični instrumenti za realizaciju ove funkcije su: trgovinski kredit, komercijalne kreditne linije, faktoring, akreditiv i lizing. Druga komponenta, koja pokriva operacije plaćanja, obuhvata funkcije deponovanja sredstava na račun banke i upotrebu različitih metoda za izvršavanje plaćanja na bazi tih sredstava (novčane/kreditne kartice, GIRO, elektronski prenos).

3.8.4. Primena koncepta STP u praksi

Operacionalizacija koncepta STP vrši se prvenstveno u domenu međunarodnih plaćanja iz dva razloga. Prvo, sa porastom prihvatanja e-trgovine, globalna e-plaćanja sve više postaju realnost, a same granice između domaćih i međunarodnih plaćanja se relativiziraju. Drugo, karakteristike međunarodnih plaćanja su takve da pružaju znatno veće mogućnosti da se primenom „glatkih integracija“ postignu relativno značajnija unapređenja. Ove transakcije, ne samo da zahtevaju obimniju dokumentaciju i više vremena, već podrazumevaju funkcionisanje sistema u uslovima primene različitih valuta i regulatornih rešenja. Zbog toga, skraćivanje vremena, ubrzanje prenosa novca i informacija i njihova integrisanost, postaju značajniji kako zbog snižavanja troškova, tako i zbog eliminisanja različitih rizika.¹²⁷

U sam proces se pored banaka koje posluju na globalnom nivou, uključuju i druge različite institucije, samostalno ili kroz konzorcijume sa bankama. Najpoznatiji primeri novih finansijskih solucija, koje razvijaju velike multinacionalne banke su: *ABN AMRO sa servisom AllTrade*, *Citibank sa Electronic Documents*, *JP Morgan sa Trade Doc* i *Standard Chartered sa B2BeX*. Tradicionalni finansijski učesnici kao što su *ACH*, *SWIFT* i asocijacije platnih kartica bili su usmereni pre svega na jedan segment trgovinskog ciklusa, plaćanje. Zbog toga, sagledavajući pogodnosti integracije celokupnog ciklusa trgovinske transakcije, uključujući i plaćanja, novi nebankarski učesnici počinju da se pojavljuju sa posebnim solucijama, među kojima se po svom značaju posebno ističu već prisutni *Bolero.Net*, *Rosseta Net* i *Trade Card* i noviji, *Identurs-Eleanor* i *TWIST*.¹²⁸

Različite bankarske institucije razvijaju različite sopstvene solucije za dematerijalizaciju komercijalnih i finansijskih dokumenata, njihovo integrisano obuhvatanje, procesing i elektronsko distribuiranje relevantnim učesnicima. *ABN AMRO's* nudi posebne modele ovih usluga za male, srednje i velike banke na bazi tehnologije blueprint-a. Servis *AllTrade* omogućava kupcima, prodavcima i njihovim provajderima usluga, da online koordiniraju sve aspekte transakcije, olakšavajući time inkorporiranje dodatnih činjenica i vrednosti kao što su: obračun troškova morskog prevoza, identifikaciju dozvole uvoza i izvoza. Solucija za integrisano upravljanje izvozom (*Electronic Documents*), koju je kreirala *Citibank*, korisnicima omogućava da dobiju uvid u širok spektar podataka koji se odnose na njihove trgovinske transakcije, što može biti značajno za sagledavanje potencijalnih oblasti rizika, posebno kod dokumentarnog akreditiva. Dok se dokumenta pripremaju za slanje, učesnici su upoznati sa statusom pripremnog procesa, a kada se kompletiraju obezbeđen je uvid u njih preko portala.

¹²⁷ Isto, str. 173

¹²⁸ Isto, str.173

Mećusolucijama koje razvijaju nebankarske institucije u okviru konzorcijuma poseban značaj se daje sistemima *Bolero.Net* i *Eleanor*. *Bolero.Net* je finansijski servis sa posebnom logistikom i infrastrukturom, koji je osnovan 1998. godine na inicijativu *SWIFT-a*. *Eleanor* je koncipiran na inicijativu *Identrus-a*, vodećeg mećunarodnog bankarskog konzorcijuma, sa ciljem da se, koncipiranjem specifikacija koje su potrebne za obezbećivanje zakonski sprovodive globalne interoperabilnosti, premosti gep koji postoji i na globalnom nivou u ovoj oblasti.

Ključne karakteristike *Bolero.Net-a* su: otvorena platforma, globalni domet, obezbećanje izvesnosti, sigurnosti i informacione razmene. Radi se o otvorenom, neutralnom sistemu koji se ne razvija po internim pravilima i procedurama kao što je slučaj sa privatnim, zatvorenim sistemima. Činjenica da su najveće svetske banke i trgovačke kuće priključene ovom sistemu, upućuje na njegov globalni domet, dok obezbećivanje globalne zakonodavne infrastrukture pruža izvesnost u poslovanju pojedinačnim članovima. Sa sistemom poruka kojima operiše *SWIFT*, rigoroznim procedurama registracije i upotrebom najnovijih tehnologija šifriranja, smatra se da sistem daje mnogo više u domenu sigurnosti u odnosu na tradicionalne trgovinske transakcije koje se zasnivaju na papiru. Legalizovani xml standardi (*boleroxml*) omogućavaju svim učesnicima u procesu trgovanja „gladak mećusobni razgovor“.¹²⁹

Ključne komponente sistema su: tehničke, aplikacione, zakonodavne, standardi i protokoli. Tehničke komponente pokrivaju probleme procesa prenosa poruka i njihove sigurnosti, a koncipirane su tako da obezbećuju sprećavanje mogućnosti naknadnog poricanja. Aplikacione komponente obezbećuju sistem registracije koji je potreban za adekvatan prenos konosmana. On omogućava da konosman može da se kreira, prenosi i dopunjava, ali tako da samo ovlašćena institucija može registru da naloži i kompletiranje transakcije. Protokoli specificiraju proces saldiranja upotrebom *XML* standarda, koje banke inaće koriste sa klijentima koji još uvek koriste tradicionalne tokove. Zakonodavna pravila prihvaćena od odgovarajućih zakonodavnih vlasti treba da obezbede zakonsku sigurnost sistema. Problem se u praksi javlja zbog toga što mnoge zemlje imaju sopstvenu regulativu i pokazuju otpor prema primeni ove globalne regulative.

Eleanor-Identurs se formira kao zatvoreno ugovorno društvo koje, u odsustvu jedinstvene zakonodavne regulative za e-poslovanje usvojene na globalnom nivou, definiše tehničke standarde (*Identurs*) i operativna pravila za iniciranje plaćanja za participirajuće banke i njihove klijente (*Eleanor*). Sistem je prilagoćen različitim okrućenjima uključujući e-nabavku, trgovačke web servere i e-tržišta. U tom cilju kreira se interoperabilna mreža banaka i njihovih klijenata, tako da plaćanja koja iniciraju privredna društva-kupci u korist prodavaca mogu da se realizuju bez obzira na lokaciju partnera i njihovih banaka.

Za razliku od sistema mećubankarskog kliringa i saldiranja, *Eleanor* je usmeren primarno na rešavanje segmenta iniciranja plaćanja, a dalji kliring i saldiranje iniciranih transakcija vrše se preko postojećih mećubankarskih mreža i njihovih platformi (*ACH*, *RTGS*, *SWIFT*). Da bi se obezbedila podrška za efikasno i ekonomično izvršavanje trgovinskih transakcija, obezbećuju se tehnička i poslovna interoperabilnost svih učesnika. U tom cilju izvršene su funkcionalne, tehničke i operacione specifikacije. Funkcionalne specifikacije pružaju opis pojedinačnih vrsta plaćanja i njihovih atributa; tehničke specifikacije obezbećuju standarde i protokole za prenos elektronskih poruka, a operacione specifikacije razraćuju pitanja prava i obaveza po pojedinim nivoima i učesnicima.

¹²⁹ Isto, str.174

Eleanor B2B za elektronsku trgovinu, bazira se na troslojnom modelu kod koga su prva dva nivoa formirana na odnosima meĎusobne kooperacije izmeĎu uĉesnika, a treći nivo na principima konkurencije. Ovakav pristup omogućava preko prvog nivoa uspostavljanje neophodne tehniĉke kooperativnosti (globalni interoperabilni sistem na bazi PKI i standarda), a preko drugog nivoa uspostavljanje funkcionalne kooperativnosti (preko zajedniĉkih standarda i pravila funkcionisanja). Na ovakvim zajedniĉkim osnovama svaka banka-ĉlanica sistema moĝe (u okviru trećeg nivoa) da razvija asortiman sopstvenih proizvoda i usluga, sa kojima (na bazi zajedniĉke tehniĉke i funkcionalne osnove) moĝe da konkuriše drugim uĉesnicima.¹³⁰

3.8.5. STP u EMU

U aktivnostima koje se u EU sprovode u cilju formiranja Jedinstvenog evropskog elektronskog trĝišta (engl. *The Single European Electronic Market - SEEM*), poslovni integracioni procesi tretiraju se kao kritiĉni elemenat. U skladu sa tim, predlaĝe se ubrzanje razvoja ovog segmenta u svim zemljama, postojećim i potencijalnim ĉlanicama. U tom kontekstu, e-lanac vrednosti se posmatra kao kljuĉ za produktivnije poslovanje, u nacionalnim i evropskim relacijama, potencira se potreba brzog progressa u ovoj oblasti, a u bankama vide uĉesnici od velikog znaĉaja.¹³¹

U prevazilaĝenju problema postojećih fragmentacija i stvaranja uslova za „glatko“ integrisanje plaćanja u poslovne procese vidi se osnova za razvoj SEPA (engl. *Single European Payment Area*) ka *end-to-end STP*. U tom cilju je ECBS (engl. *European Committee for Banking Standards*) inicirao preduzimanje aktivnosti obezbeĉivanja uslova za korišćenje istih elemenata u domaćim i meĎunarodnim standardima (*XML-koverat* za prenos fakture i ubacivanje u *SWIFT C2BXML*). Ovim putem se vrši eliminisanje znaĉajnih troškova i omogućava eventualna reupotreba sigurne mreĝe globalnih plaćanja za fakture koje startuju iz Evrope.

Smatra se da je brz i ekonomičan prelaz na integrisane poslovne procese u lancima vrednosti nemoguć bez centralnog uĉešća banaka, zbog toga što su one te koje već imaju uspostavljene odnose sa klijentima, znaĉajnu prodajnu snagu, već izgraĉeno poverenje, sredstva i visok stepen spremnosti za prilagoĉavanje već uspostavljenim navikama i obiĉajima svojih klijenata. Bankarske usluge su potrebne kao deo u integracionim finansijskim lancima vrednosti da bi se obezbedili:

1. sigurnost (kroz identifikaciju i eliminaciju trgovinskog rizika),
2. niĝi troškovi (upotrebom sredstava kojima već raspoloĝu i mogu da obezbede dodatno delovanje ekonomije opsega) i
3. maksimalna brzina implementacija (reupotrebom postojećih komponenti).

U ovom trenutku EU zaostaje za integracionim aktivnostima u odnosu na SAD i neke azijske zemlje. MeĎutim, iskustva u sprovoĉenju konkretnih aktivnosti pokazuju da traĝnja za korišćenjem pristupa *FVCM* veoma brzo raste u *B2B*, zbog obimnih ušteda i podizanja kvaliteta usluga. Takoĉe, ocenjuje se da nedostatak pan-evropske implementacije ne smanjuje progres sam po sebi, ali bi zajedniĉki pristup evropska preduzeća generalno uĉinio mnogo

¹³⁰ Isto, str.176

¹³¹ Isto, str.177

konkurentnijim, pri čemu mala preduzeća dobijaju dodatnu šansu u odnosu na velika i to bez značajnijih, dodatnih ulaganja.¹³²

Procene izvršene na primeru Nordijskih zemalja pokazuju (prema R. Naatsaari) da je implementacija e-fakturisanja upotrebom ePI (engl. *Electronic Payment Initiator*) veoma jednostavna za uključivanje u postojeći sistem, a tržišni odgovor na postojeću ponudu ohrabrujući. U praksi, Finske („*Nordea*“) banke su prve startovale sa dogovornim standardom za e-fakture upotrebom ePI, a istim putem idu i Švedske i Norveške banke. Praksa je pokazala da je za preduzeća bitno da prelaz na novi sistem ne zahteva dodatne investicije, jer se fakture šalju u banku kao fajlovi. Konkretno rešenje, bazira se na upotrebi XML formata (za sopstvene klijente, druge banke, operatere), ili štampanje za primaoca koji nisu elektronski osposobljeni.

U cilju ubrzanja razvoja i podsticanja prihvatanja ovog sistema, u Finskoj je u proces promocije bila aktivno uključena i država. Ministarstvo finansija je podržalo usvajanje e-fakturisanja i *Finvoice standard* sa ciljem da se postigne 50% povećanje korišćenja sistema do 2005.godine. Ponuđači softvera i operatori sa fakturisanjem su već u visokom stepenu prilagodili proizvode, politike i procedure za podršku migraciji na novi sistem. Bilo je ocenjeno da samo banke sa njihovim prodajnim snagama, sigurnom mrežom i pripremljenim solucijama mogu da budu nosioci ovih usluga. Na ponude banaka, veliki primaoci faktura javljali su se dobrovoljno i istovremeno upućivali pozive svojim poslovnim partnerima da se uključe u novi sistem (nedeljno je pristupalo u proseku 70-80 učesnika).

Pokazalo se da primenjen model može lako da se integriše u proces plaćanja u sistemima koje koriste preduzeća i banke, poseduje adekvatnu ambalažu za uključivanje svih relevantnih informacija (reference prodavca, kupca, kompletne računovodstvene informacije, a kada je potrebno i mogućnost realizacije mehanizama direktnim zaduživanjem). Elektronsko iniciranje plaćanja (ePI) i e-faktura zajedno omogućavaju visok nivo automatizacije u logistici i obračivanju naloga, u knjigovodstvu i pratećim poslovima.

Procenjuje se, da je u cilju ubrzanja procesa operacionalizacije celokupnog sistema potrebna primena zajedničkih standarda i postojanje slobodne konkurencije. Početni rezultati koje pokazuje praksa zemalja uključenih u prezentirani projekat (u nacionalnim i međunarodnim relacijama) pokazuju nekoliko značajnih činjenica¹³³:

1. integrisani sistemi se mogu formirati preuzimanjem i prilagođavanjem već postojećih elemenata iz asortimana usluga plaćanja;
2. moguće je ostvarivanje veoma velikih ušteda u troškovima (posebno kroz e-fakturisanje);
3. rešavanje sigurnosnih potreba, transakcija će doprineti sprečavanju zloupotrebe fakturisanja i unaprećivanju mehanizama odbrane od pranja novca i
4. otvara se prostor za dalje unaprećenje usluga individualnih banaka (prema R. Naatsaari).

Posle dvogodišnjih primena, u okviru finsko-slovenačke kooperacije otvorena je oktobra 2004. godine „*eInvoicing LivingLab*“ u okviru koje će se sprovoditi multidisciplinarno istraživanje i testiranje platforme sa pozicija potreba korisnika. Ova istraživanja treba da daju odgovor na dva suštinska pitanja: kakve su potrebe korisnika bankarskih usluga u B2B i kako

¹³² Isto, str.178

¹³³ Isto, str.179

bankarstvo moće odgovoriti na ove potrebe? Inicijativa je otvorena za organizacije iz zemalja ovog regiona, posebno kroz univerzitetsku mrežu, „eBusiness ALADIN“.

4. ELEKTRONSKO BERZANSKO TRGOVANJE

4.1. Pojam i karakteristike

Aktuelna kretanja na finansijskim tržištima ukazuju na to da je danas teško naći tržište, koje nije u fazi zamene klasičnog trgovanja, elektronskim trgovanjem, ili koje ne planira ovakav poduhvat. Globalizacija berzanskog poslovanja, podrazumeva automatizaciju postojećih sistema i povezivanje sa berzama. Na ovakav način omogućava se realizacija ponude usluga svim potencijalnim korisnicima, ma gde se nalazili. Značaj ovakvog uticaja povećan je nastankom Evropske monetarne unije (EMU), u kojoj je uvođenje nove valute evro ubrzalo promene u pravcu napuštanja klasičnih načina trgovanja akcijama. Elektronski način trgovanja jeftiniji je i fleksibilniji od dosadašnjeg načina trgovanja akcijama i idealna je solucija za rastuće potrebe korisnika za trgovanjem bez vremenskog ograničenja.¹³⁴

Elektronske berze, kao tehnološki napredniji modalitet organizacije ovog poslovanja, baziraju se na primeni informacionih tehnologija, a posebno mrežne ekonomije. U tom kontekstu posebnu ulogu ima Internet kao multimedijaska svetska mreža, zbog toga što omogućava transformaciju samog berzanskog poslovanja, primenu njegovog modela, oblikovanje drugačijih odnosa između učesnika i doprinosi promenama u strukturi. Berze su sve manje fizičke institucije, a sve više virtuelne institucije koje omogućavaju pojednostavljen i uprošćen pristup informacijama, kao i funkcionisanje po principu rada na daljinu.¹³⁵

Mada se tradicionalni poslovi sa hartijama od vrednosti po svom karakteru baziraju na personalnim kontaktima i pregovorima, danas se sve veći broj segmenata ovih poslova prevodi na elektronsku formu. Prodiranje informacione tehnologije u berze i njihovo poslovanje predstavlja jedan od najznačajnijih fenomena u ovoj oblasti. Suština primene informacione tehnologije u obavljanju berzanskog trgovanja odnosi se na obezbeđenje nove logističke ponude, koja omogućava direktno povezivanje izdavaoca i primaoca naloga, kao i finansijskih tržišta različitih zemalja. Pre pojave Interneta mnogi berzanski posrednici su već prešli na automatsko obavljanje procesa trgovanja, a sa pojavom Interneta dobijaju mogućnost prelaska na čisto elektronsko trgovanje.

Tradicionalne berzanske prostorije i sistemi trgovanja bazirani na oštroj fizičkoj komunikaciji postaju prošlost. Od 1995. do 1999. godine vrednost sedišta, koje je omogućavalo pojedincima trgovinu na Njujorškoj berzi, opada 30-40%. Razlog ove promene leži u pojavi *on-line* supstituta za tradicionalni način finansijskog trgovanja. Kada je u Francuskoj MATIF (*Marche a Terme International de France*) uveo sistem elektronskog trgovanja, paralelno sa postojećim sistemom tradicionalnog trgovanja, uz ostavljanje slobode izbora načina trgovanja, praksa pokazuje da tržište preferira novi način. U periodu od dve nedelje, dominantan deo se opredeljuje za sistem elektronskog trgovanja, a posle šest nedelja dolazi do potpune eliminacije tradicionalnog načina trgovanja.¹³⁶

¹³⁴ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.111

¹³⁵ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.206

¹³⁶ Isto, str.207

Ovaj masovni entuzijazam nije tako iznenađujući ako se ima u vidu da pruža mogućnosti individualnim investitorima da samostalno upravljaju svojim investicijama i drugim aktivima proaktivno u znatno većoj meri. Mnogi investitori u upravljanju sopstvenim finansijama prihvataju pristup „uradi sam“, redukujući oslanjanje na finansijske planere, savetodavce i brokere i direktno povezujući svoje trgovinske aktivnosti sa servis provajderima kao što su *Schwab* i *E-Trade*.

Online trgovina vrednosnim papirima je revolucionarni i popularni koncept koji razvija fleksibilne i bezbedne mehanizme trgovanja. Rast njegove primene posebno dolazi do izražaja u razvijenim tržištima kao što su Švedska, Nemačka, Francuska i sl. U mnogim slučajevima online trgovanje je ograničeno na tržište SAD-a. Za realizaciju internacionalnog trgovanja formiraju se posebni aranžmani i odvojene oblasti na lokalnim tržištima.

U praksi, mnogi koriste usluge tradicionalnih brokera i iniciranje trgovanja na tradicionalan način, ali preko elektronske platforme. Poznata automatizovana tržišta su *CORES* (automatizovano tržište za trgovinu državnim obveznicama u Tokiju) i *CATS* u Torontu. Internet povezuje individualne investitore direktno sa brokerima i transformiše funkcionisanje tržišta akcija. Ovaj razvoj počinje sa osnivanjem jedne od najznačajnijih kompanija u ovoj oblasti *E-Trade.com*, zatim *Ameritrade.com* i *Schwab.com*. Ove kompanije nude kupovinu akcija online.¹³⁷

U SAD-u se decentralizovano (*OTC*) trguje akcijama preko NASDAQ-a (engl. *National Association of Securities Dealers Automated Quotation*) od februara 1971. godine. NASDAQ startuje kao slaba mreža u koju je uključeno stotinjak firmi koje trguju sa akcijama. U to vreme informacioni sistem se bazira na telefonskim pozivima. Sistem je pokazivao kvote akcija i telefonske brojeve brokera za poziv. Danas NASDAQ povezuje oko 500 dilera preko računarskih sistema, u trgovinu je uključeno preko 500 akcija, tako da od 1998. godine NASDAQ postaje najveća berza u SAD-u.¹³⁸

Berzanske kuće najčešće ne razvijaju sopstvene informacione sisteme, već koriste usluge računarsko-informativnih kuća za generisanje svih potrebnih informacija i izveštaja i obavljanje kupoprodajnih transakcija. U Kanadi i SAD-u postoji više takvih posrednika, a najpoznatiji je „*Financial system*“ koji ima regionalne centre u Torontu, Njujorku i Londonu. On omogućava čak i rad korisnika od kuće. U Evropi je poznat sistem *Tradepoint* (TFN), a u SAD-u *NASDAQ*.

U domenu elektronske revolucije u obavljanju poslova hartijama od vrednosti postoje dva tehnološka standarda: otvoreni i zatvoreni. Zatvoreni sistem vezan za informacione tehnologije pokazao je svoje prednosti na početku tranzicije na elektronsko tržište sa centralnom berzom, koja u svom sastavu ima i klirinšku kuću. Prelaskom na informacioni sistem otvorenog tipa berze evoluiraju u pravcu povezivanja širokog spektra učesnika na tržištu, koji su istovremeno članovi većeg broja berzi, nezavisnih klirinških organizacija, međuposrednika i različitih sistema plaćanja. Suština primene informacionih tehnologija u obavljanju poslova na finansijskom tržištu odnosi se na obezbeđenje nove logističke ponude koja omogućava direktno povezivanje izdavaoca i primaoca naloga, kao i finansijskih tržišta više zemalja.¹³⁹

¹³⁷ Isto, str.208

¹³⁸ Isto, str.208

¹³⁹ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.111

4.2. Uloga Interneta

Ni u jednoj privrednoj grani Internet nije učinio tako duboke promene kao što je to učinio u svetu finansija. Iako su računari veoma rano postali standardni deo komunikacije finansijske industrije, tek je sa pojavom Interneta običan korisnik stekao mogućnost da lagodno pristupi nekim finansijskim operacijama.

Aktivno trgovanje obveznicama preko Interneta u SAD-u počelo je 1998. godine. Za kupovinu, bilo je potrebno otvaranje posebnog računa („*Treasury Direct*“) da bi se pomoću njega pristupilo Internet servisu „*Buy Direct*“. Koristeći broj „*Treasury Direct*“ računa i poreskog i identifikacionog broja vršilo se logovanje na sistem „*virtual lobby*“ preko koga se vrši unos naloga. Pojedinačno online trgovanje bilo je omogućeno samo za naloge koji se ne odnose na trgovinu po konkurentnim cenama (cene kojima se podstiče prodaja na nedeljnim i mesečnim aukcijama). Trgovina obveznicama preduzeća je prilično nerazvijena iz više razloga.

Trgovanje akcijama preko Interneta u SAD-u je danas vrlo popularno, mada su brokerske kuće imale problema u nekim slučajevima. To je dovelo do reakcije posebne komisije koja nadgleda izdavanje i trgovanje akcijama u ovoj zemlji (*Securities and Exchange Commission*). Kako akcijama putem Interneta praktično može trgovati svako ko ima računar i pristup Internetu, otvoren je novi prostor za internacionalni transfer kapitala. Mnoge zemlje pokušavaju ovu mogućnost da ograniče posebnim zakonima kojima zabranjuju iznošenje kapitala iz zemlje, čime direktno ograničavaju i mogućnost kupovine hartija od vrednosti u inostranstvu.

U samom procesu trgovine sa hartijama od vrednosti Internet je značajan po više osnova:¹⁴⁰

1. predstavlja najnoviji i potencijalno najbolji kanal za plasiranje informacija,
2. najprikladnije je sredstvo za pružanje pomoći kod donošenja odluka i
3. obezbeđuje virtuelni prostor za sam proces trgovanja sa hartijama od vrednosti.

1. Internet je uneo veliki napredak u izmeni poslovnog modela trgovanja akcijama posebno u pristupu informacijama o akcijama, što je izuzetno važno. U uslovima tradicionalne trgovine, informacije o stanju cena i prinosa vrednosnih papira bile su dostupne širokoj publici samo putem javnih medija (novine, telefoni brokerske kuće i sl.), u formi dnevnih izveštaja na kraju berzanskog radnog dana. Praćenje promena cena i prinosa vrednosnih papira u realnom vremenu i uvid u analize podataka o preduzećima čijim se akcijama trguje, bile su relevantne za korišćenje od strane stručnjaka, a ne širokog kruga malih investitora. Sada su one, zahvaljujući Internetu, dostupne svima i to besplatno, ili po veoma niskim, gotovo simboličnim cenama. Na primer, danas za on-line praćenje cena akcija na Londonskoj berzi putem Web-a košta mesečno 5 funti za 15 minuta kašnjenja i 20 funti za praćenje u realnom vremenu. Naravno tu su i servisne informacije o kompaniji kao npr. o kupovini akcija od strane svojih menadžera, detaljni poslovni rezultati, praćenje cene u nekoliko prethodnih godina, preporuke brokera i sl. Znatno su smanjene i brokerske provizije u trgovanju akcijama. Dakle, korisnici sada raspolazu sa mnogo više informacija o akcijama, uz mnogo jeftiniju mogućnost kupovine akcija i on-line praćenje svojih portfelja i informacija o kompanijama čije deonice poseduju.¹⁴¹

¹⁴⁰ Vuksanović E.: „Elektronsko bankarstvo“, cit.delu, str.209

¹⁴¹ Stankić R.: „Elektronsko poslovanje“, cit.delu, str.112

Finansijski web sajtovi, koji se smatraju jednim od najozbiljnijih poslova na Internetu, danas nude informacije o stanju i prometu vrednosnih papira u celom svetu. Oni mogu biti manje ili više sofisticirani. Neki od njih ograničavaju se na najnovije podatke o ceni i količini prometa vrednosnih papira, dok drugi nude znatno širi asortiman informacija (istorijske podatke, kumulativni broj transakcija, kumulativni ostvareni promet u određenoj valuti, najviša, najniža i poslednja postignuta cena na određeni dan, prosečna cena, procenat promene u odnosu na prethodni dan). Takođe, postoje posebni programi koji obezbeđuju verodostojne i brze informacije o trenutnom stanju i cenama na nekoj berzi, namenjeni investitorima, menadžerima i akcionarima. Neki Web sajtovi pružaju krajnje specificirane informacije o određenom portfelju vrednosnih papira i vrše njihovo ažuriranje (pored klasičnih finansijskih izveštaja o kompaniji, daju detaljne prikaze ostvarenih rezultata i preporuke brokera npr.).

Investicioni fondovi takođe formiraju sopstvene informativne Web sajtove, preko kojih pružaju informacije o vlastitim raspoloživim portfeljima vrednosnih papira, a veoma retko pružaju mogućnost za online trgovinu.

JP Morgan Chase je otvorila Web platformu za klijente svog investicionog bankarstva pod nazivom *ChaseSpace*. Na ovoj platformi distribuirane su informacije po osnovu istraživanja, tekućih audio/video izveštaja, tržišnih komentara, cena hartija od vrednosti i ostale informacije koje se odnose na trgovinu hartijama od vrednosti. Druge velike banke su, takođe, uvele slične sajtove.¹⁴²

Najpoznatije mesto na Internetu za informisanje o emisijama akcija putem Interneta je *The Direct Stock Market Inc.* Investitori mogu da dobiju tekuće informacije o javnoj ponudi malih preduzeća. Kompanijama koje izdaju akcije poklanja se puna pažnja. Omogućena je i ponuda i tražnja za akcijama. Jedna od najpropulzivnijih kompanija je E-Trade. Većina takvih sajtova omogućava on-line praćenje cena akcija na berzama, praćenje i proveru cene akcija u poslednjih pet godina, vesti o kompaniji i sl. Osim toga, korisnici imaju svoje portfelje na Web stranicama brokerske kuće putem koje kupuju akcije. Sve to zajedno je izuzetno zahtevno za održavanje i upravljanje. Takvi sajtovi su vrlo zahtevni, a promet na njima dostigao je i više od 180.000 transakcija na dan. Vrlo je veliki pritisak i na pouzdanost tih sajtova, jer svaki zastoj u radu, korisnike može stajati mnogo novca, dok traje zastoj, cena akcija se menja, pa korisnici mogu izgubiti novac, ako ne uspeju da obave kupovinu ili prodaju akcija. Brokerske kuće koje nude on-line trgovanje akcijama imale su teškoća, što je dovelo i do reakcije američke *Securities and Exchange Commissions*, koja nadgleda izdavanje i trgovanje akcijama u Americi, te do nekih tužbi protiv brokerskih kuća kod kojih se zastoj dogodio. U Americi je trgovanje akcijama na Internetu vrlo popularno, kao što su popularne i akcije Internet kompanija, kojima cena nakon izlaska na berzu uglavnom raste i to ponekad i višestruko.¹⁴³

Pored svih pomenutih prednosti, treba imati u vidu prisustvo određenih rizika koji mogu nastati usled povredivosti informacija na mreži. Mogućnosti zloupotreba i distribuiranja pogrešnih informacija značajno utiču na stepen poverenja investitora.

2. Internet se koristi kao sredstvo za pružanje pomoći kod donošenja investicionih odluka preko Web sajtova za istraživanje investicionih mogućnosti. Smisao ovih sajtova je da putem prezentiranja finansijskih izveštaja, vesti, saveta, poruka, preporuka, upozorenja i sl. pomognu investitorima u donošenju odluka. U tom kontekstu treba pomenuti posebne

¹⁴² Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.210

¹⁴³ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.113

finansijske centre usmerene na pružanje pomoći pojedincima u upravljanju ličnim finansiranjima.¹⁴⁴

3. Najviši nivo uticaja Interneta na trgovinu vrednosnim papirima, manifestuje se kroz obezbeđenje virtuelnog prostora za sprovođenje samog procesa trgovanja sa vrednosnim papirima. U odnosu na sajtove informativnog karaktera, sajtovi koji obezbeđuju virtuelni prostor za trgovanje su malobrojni, najčešće su organizovani od strane američkih kompanija i primenjivani na nivou svetskog online tržišta. Poznati su kao finansijski portali.

Svaki sistem ima jedinstvene karakteristike. Međutim, generalno govoreći trgovci su povezani putem računarskih konekcija i koriste specijalne softverske programe za pristup informacijama finansijskih tržišta određenih hartija od vrednosti. Na ekranu računara trgovca, softver pokazuje cene i iznose ponuda, prethodne cene, obime trgovanja, iznose ponuda i sl. Trgovci koriste tastaturu za uspostavljanje interakcija sa sistemom i realizovanje trgovinske transakcije. Ulazak u elektronski svet trgovine kapitalom omogućava pojedinačnim korisnicima direktno trgovanje, bez usluga fizičkih brokerskih kuća.¹⁴⁵

Sam proces trgovanja podrazumeva da učesnik u trgovanju mora da ima obezbeđen priključak na Internet. Pre otpočinjanja samog procesa trgovanja potrebno je da se na Internetu izabere odgovarajuća elektronska investiciona ili brokerska firma preko koje će se obavljati trgovina. Poznate svetske firme ove vrste su *E-Trade Charles Sharles*; *Pwys Financial Network* i dr. Kada se izvrši izbor konkretne Internet berze, šalje joj se zahtev za registraciju (obično elektronskom poštom). Uz odgovor se dobija, i konkretna aplikacija koju treba popuniti radi upisa. Da bi trgovina mogla da se realizuje, učesnik mora da ima otvoren račun u banci, sa deponovanim sredstvima koja će biti upotrebljena za realizaciju kupovine. Ta sredstva se prosleđuju elektronskoj berzi za plaćanje kupljenih vrednosnih papira.

Znači, u procesu trgovanja bi se najpre davao nalog za prodaju/kupovinu, a sistem bi automatski lansirao verifikacionu proceduru u kojoj se:

1. potvrđuje da nisu bile primljene ranije ponude za prodaju,
2. proverava da li je ova cena jednaka, ili manja od glavnog istaknutog naloga kupovine i
3. vrši prenos informacija o obavljenoj transakciji klirinškoj kući.

Online trgovinska platforma omogućava investitorima izbor vrste željenog naloga (tržišni, prodajni, kupovni, stop nalog, alternativni nalog, nalog „sve ili ništa“, nalog „izvrši ili otkazi“ itd). Pored kotiranja u realnom vremenu, izvršavanja transakcija, pruža mogućnost istraživanja, izbora, alociranja pozicija, dobijanja informacija o istoriji trgovanja, obračuna dobitka i gubitka, ulaza u multiračun i glavne vesti.¹⁴⁶

4.3. Sistemi za prenos podataka sa berze

Početkom osamdesetih godina XX veka počinje intenzivniji razvoj i rast finansijskih tržišta u svetu. Od uglavnom bankarske i dilersko-brokerske interesne sfere, finansijska tržišta postaju interesantna i za „običan svet“. Fokus pojedinaca se prebacuje sa klasičnog bankarsko-kamatnog aspekta na aspekt učesnika na finansijskom tržištu.

¹⁴⁴ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.210

¹⁴⁵ Isto, str.211

¹⁴⁶ Isto, str.211

Razvojem finansijskih tržišta, razvila se i tehnologija koja ih prati. Sa vrlo malog broja učesnika na tržištu, ograničenog samo na one direktno prisutne, broj se povećao na milione povezane najnovijom tehnologijom sa svetskim berzama. Dnevno se na Njujorškoj berzi razmeni 527 miliona akcija (rekord je 1 milijarda akcija u jednom danu) vrednosti od oko 23 milijarde dolara. U tim transakcijama učestvuju trgovci iz svih delova sveta. Putem sistema za prenos podataka i programa za njihovu analizu, trgovci širom sveta imaju pristup bazama podataka, analizama, istraživanjima i svim drugim informacijama vezanim za određeno tržište. Ta povezanost omogućuje trgovcima da budu aktivni na više tržišta širom sveta. Kapital se seli sa jednog na drugo tržište u zavisnosti od trenutne situacije.¹⁴⁷

Uzevši u obzir broj učesnika na tržištu, kao i njihovu geografsku lociranost, sistemi za prenos podataka sa berze omogućavaju ovim učesnicima da njihovo okruženje ima bar približno iste karakteristike kao i okruženje onih učesnika koji su direktno locirani u samoj zgradi berze. Osnovni preduslov za to je pravovremeni prenos podataka o ceni, obimu i tržišnom materijalu kojim trguju i dr. Ta vrsta prenosa podataka se naziva *Real Time Data Feed*.

U svetu su se razvila tri načina za prenos podataka ove vrste:¹⁴⁸

1. putem telefonskih linija;
2. putem satelita i
3. putem Interneta.

Pružanjem ovih vrsta usluga se bave, uglavnom američke kompanije sa par evropskih izuzetaka. Te kompanije obezbeđuju softver kao i hardver za te usluge. Korisnik sam bira koje će berze da prati kao i ostale informacije koje želi da dobije. Korisnicima su takođe dostupne i vesti vezane za politiku, meteorologiju, statistiku itd. Takođe, moguće je dobijati razne analize od strane konsultantskih kompanija. Preko tih kompanija se mogu nabaviti i programi za tehničku analizu podataka (*Telerate, Trade Station, Super Charts, Option Station i dr.*). Ove programe softverski podržavaju uglavnom svi provajderi. Postoji oko 250 različitih programa za analizu. Neke od poznatijih kompanija koje pružaju te usluge su: *S&P Comstock, DBC Signal, Bloomberg, Future Source, Dow Jones Telerate, Knight Ridder i dr.*¹⁴⁹

Prvi navedeni način prenosa podataka je telefonskim putem. On je trenutno i najzastupljeniji u zemljama Zapadne Evrope, SAD i Kanade. Uglavnom su to zemlje sa velikim brojem korisnika. Svaki korisnik je povezan iznajmljenom linijom sa provajderom. Računar korisnika dobija podatke koje zatim pomoću posebnog programa prezentira korisniku. Korišćenje podataka u odnosu na stvarno stanje zavisi od kvaliteta veze i uglavnom je zanemarljivo malo, maksimalno 3 sekunde.

Drugi način prenosa podataka je putem satelita i najčešće se primenjuje u zemljama sa malim brojem korisnika, tj. tamo gde provajder nije našao interes za otvaranje sopstvene filijale. Maksimalno kašnjenje koje je moguće je od 5-10 sekundi u odnosu na promene na samoj berzi. Provajderi za ovaj način prenosa su isti kao i za prenos putem telefonskih linija.

Treći vid prenosa podataka se pojavio poslednji na svetskom tržištu i razvijao se uporedo sa razvojem Interneta. U svetu je doživio veliku ekspanziju u poslednjih godinu dana. Odlikuje

¹⁴⁷ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.114

¹⁴⁸ Isto, str.114

¹⁴⁹ Isto, str.114

ga niska cena koštanja kao i to da je uglavnom povezan sa brokerskim kućama koje omogućavaju davanje naloga putem Interneta uz nisku proviziju. To uveliko snižava troškove telefoniranja ukoliko je korisnik van zemlje u kojoj se nalazi berza ili broker. Korisnik je povezan sa lokalnim Internet centrom putem koga se spaja sa provajderom i bazom podataka na Internetu. Da li će korisnik imati zakupljenu vezu sa centrom ili će se povezivati po potrebi, zavisi od obima njegovih poslova. Ovaj vid prenosa podataka je najzastupljeniji meću privatnim investitorima, koji posao obavljaju od kuće i za svoj lični račun. Kašnjenje podataka zavisi od kvaliteta telefonske veze i broja konekcija na Internetu i ne bi trebalo da predstavlja problem za rad na ovakvom sistemu.

Za koji vid prenosa podataka tj. kog provajdera će se opredeliti korisnik pre svega zavisi od njegovih potreba, obima trgovine kao i veličine kompanije kojoj je sistem potreban.

Reuters je sistem koji je najviše zastupljen u trgovini valutama i prenosu vesti i kao takav najviše je zastupljen kod centralnih i velikih banaka učesnika na tržištu. Brokerske kuće, investicioni fondovi, zajednički fondovi i ostale kompanije koje se bave trgovinom i posredovanjem su više okrenute ka provajderima kao što su *S&P Comstock* i *Bloomberg* i to pre svega kao korisnici nekog od programa za analizu. Ovi provajderi su zastupljeni i meću individualnim investitorima mada se oni sve više okreću ka provajderima putem Interneta.¹⁵⁰

4.4. Karakteristike novog poslovnog modela

Stvaranje novog virtuelnog prostora dovodi do promene odnosa učesnika u ovim transakcijama po dva osnova:

Prvo, sam karakter elektronske trgovine, odnosno elektronskih aukcija menja odnos brokera prema berzi.

Drugo, promena načina komuniciranja dovodi do promene odnosa između brokera i klijenta.

U celini, može se reći da ulazak u elektronski svet trgovine kapitalom omogućava pojedinačnim korisnicima eliminisanje „fizičkih“ brokerskih kuća, uz manji utrošak vremena i novca.¹⁵¹

Praktična mogućnost realizovanja ove eliminacije zavisi od konkretne zakonodavne regulative ove oblasti, a realizuje se po principima „zatvorenog kruga“, odnosno mećusobnoj kupovini i prodaji vrednosnih papira direktnih učesnika, bez posrednika. Ovakve ponude daju posebne kompanije (npr. *Spring Street Brewing*) preko svojih web strana, ali se one još uvek ne pojavljuju u velikom broju.

Ovaj način trgovanja doveo je do stvaranja posebnog zanimanja („*day trades*“) i posebnih firmi koje pojedincima pružaju ovu vrstu usluga. „*Day trader*“ je osoba koja svakodnevno upravlja mnogim transakcijama sa hartijama od vrednosti sa ciljem da od te aktivnosti obezbedi sebi profit i izvor sredstava za život. U nekim slučajevima pojedinci to čine samostalno, dok u drugim angažuju posebne „*day traders*“ firme koje pružaju usluge, kao što

¹⁵⁰ Isto, str.115

¹⁵¹ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.212

su trenutni uvid u podatke i novosti i sl. U SAD-u provizija za ove vrste usluga kreće se od 50-600\$ mesečno.¹⁵²

Sam sistem „*day trades*“ postoji od 1980-tih. Investitori koji ga koriste izvršavaju desetine, ili stotine transakcija u kojima se nadaju ostvarivanju zarade na bazi „hvatanja“ malih raspona u promenama cena. Mnogi profesionalci u ovoj oblasti koji trguju sa blokovima od 500-1000 akcija su se istorijski oslanjali na EDAT platformu (engl. *electronic direct access trading*) koja uključuje iznajmljene komunikacione linije, garantovani pristup na tržište i bogatu RT kotaciju. Izvesne usluge u trgovanju obveznicama su se takođe pojavile kao što su npr. *Bonds online*, *Bondtracc*, *BondExchange* i *BondExpress*.

Automatizacija globalnog finansijskog tržišta omogućava kontinuitet trgovanja, bez obzira na razlike u vremenskim zonama različitih berzi. Trgovac u Tokiju može da vidi cenu hartija od vrednosti u Njujorku i da inicira transakciju u vreme kada je otvorena berza u Tokiju i da se njeno saldiranje vrši sledećeg poslovnog dana u Njujorku, ako se radi o državnim hartijama od vrednosti (npr. transakcija koja je aranžirana u sredu u Tokiju, mogla bi da bude saldirana u četvrtak uveče u Njujorku).¹⁵³

Oko jedna trećina celokupnog obima dnevnih transakcija je procesirana preko elektronske mreže (engl. *electronic communication networks - ECN*). Ove aukcije putem Interneta povezuju kupce i prodavce širom sveta. Prelaz na trgovinu preko Interneta nudi nekoliko prednosti investitorima. Time se omogućava realizacija ponude usluga svim potencijalnim korisnicima, bez obzira na to gde se oni nalaze. Ovaj način trgovanja je jeftiniji (ECN zaračunava znatno nižu proviziju) i fleksibilniji od tradicionalnog i idealna je solucija za trgovanje sa produženim radnim vremenom, a u nekim slučajevima i bez vremenskog ograničenja. Dve najveće ECN Istinet i Island funkcionišu 24 časa. Takođe nudi se i posebna pogodnost koja se odnosi na pružanje mogućnosti simultanog uvida u cene akcija sa drugih berzi (npr. Istinet nudi pregled sa 16 drugih berzi).

Kao posebna prednost ističe se i anonimnost u trgovanju putem ECN, jer ovi izveštaji daju samo informacije o cenama i obimu trgovanja, a ne i identitet trgovca. Ovo se smatra značajnim kao zaštita institucionalnih investitora od prakse zvane „*front running*“, u kojoj učesnici u trgovini na neki način idu ispred da bi ostvarili zaradu od male promene u ceni, koja kasnije može da proizađe iz transakcije institucionalnih investitora.

4.5. Ekonomski aspekti

Najznačajniji podsticajni elemenat za pojedince je svakako snižavanje cena koje se kreću u rasponu od 50-90% cena tradicionalne trgovine. Poređenje u SAD-u pokazuje, da se visina bankarske provizije sa 100 \$ u tradicionalnoj trgovini, snižava na 15 \$ u online trgovini.

Proširenje ulaza i snižavanje troškova vode podizanju efikasnosti tržišta. Međutim, društvene koristi mogu da neće u ovoj meri snižavanja troškova biti izražene. Kao faktor koji deluje u tom smislu, navodi se potreba da pojedinac troši znatan iznos svog sopstvenog vremena i računarske resurse za realizaciju ove trgovine. Npr. ako za 2000 akcija provizija iznosi 500\$ u tradicionalnoj trgovini, a 100 u online, trebalo bi da ušteda bude 400\$. Međutim, ako se u

¹⁵² Isto, str.212

¹⁵³ Isto, str.213

obzir uzmu oportunitetni troškovi za utrošeno vreme i korišćenje računara (npr. 50\$) onda će iznositi 350\$. Razlike nisu male ako se to primeni na celokupan broj izvršenih transakcija.¹⁵⁴

Da bi se konektovali za online trgovinu Internet, trgovci ubacuju svoju identifikaciju i lozinku za račun. U jednoj tipičnoj transakciji, on dobija ulaz u paket usluga koje bi bile skuplje kada bi se odvojeno koristile, a ne u paketu. Posle povezivanja na Internet, on može da skenira portfolio, traži ključne informacije o privrednom društvu čije akcije ima u vlasništvu i šalje nalog za prodaju ili kupovinu još akcija. Sve to može da uradi za nekoliko minuta.

Najveći broj online brokera sada nudi prodavcu informacije o akcijama i njihovu evaluaciju, a neki nude ove usluge u obliku online trgovinskog paketa. To omogućava skraćivanje vremena potrebnog za ispitivanje akcija u poređenju sa prethodnom situacijom. Rezultat je snižavanje oportunitetnih troškova kada se trguje online, a to dalje vodi potencijalnim društvenim uštedama.

Ovakva trgovina nesumnjivo ima pozitivne efekte na brokersko-dilerske firme, zbog toga što im omogućava da sa manje osoblja i filijala obezbede svojim klijentima dodatne web usluge. Međutim, prilagođavanje nije uvek lako. Tako, navodi se da je u SAD-u 16. jula 1996. godine, za samo dva meseca trgovanja došlo do iznenadnog pada cena akcija, a hiljade ljudi je ove događaje pratilo online. Za mnoge brokere je to bio test kapaciteta njihovih sistema i neki od njih su na njemu pali.

Pojedinci su tada reagovali pravljjenjem novih preraspodela na svom portfoliu, ali neki od njih nisu bili u mogućnosti da se loguju i provere tržišne indekse, ili stanje na svojim računima, dok su drugi otkrili da su im računi zamrznuti. Desilo se da su u jednom slučaju, čak i posle uspešne konekcije posle dužeg vremena, prezentirane pogrešne informacije. Broker je pokušavao da mu nadoknadi štetu koja je proizašla iz nemogućnosti obrade neočekivano velikog obima prometa toga dana.¹⁵⁵

Danas je situacija drugačija i mnogo bolja opremljenost eliminiše ovakve probleme. Međutim, ovo iskustvo je pokazalo da ne postoji apsolutna otpornost na neke nove vrste lomova na tržištima akcija. Trenutno uključivanje veoma velikog broja učesnika može da dovede do preopterećenosti sistema i blokiranja određenih segmenata ovih usluga. U nekim situacijama učesnici koji žele da iz minuta u minut kontrolišu stanje na tržištu, mogu biti usled blokade eliminisani sa tržišta.

Kao posebna prednost ovog načina trgovanja, ističe se njegova spontanost i mogućnost značajnog povećanja broja dnevnih transakcija. Prema navodima koje daje *VanHoose David*, prosečan klijent tradicionalnog brokera obavi nešto preko četiri transakcije u godini (0,01 dnevno), dok kod Internet brokera prosečni klijent obavi preko 15 transakcija godišnje, a u nekim slučajevima i do 25.¹⁵⁶

¹⁵⁴ Isto, str.214

¹⁵⁵ Isto, str.214

¹⁵⁶ Isto, str.215

TREĆI DEO

UPRAVLJANJE RIZICIMA U ELEKTRONSKOM BANKARSTVU

1.VRSTE I KARAKTERISTIKE RIZIKA

Razvoj usluga elektronskog bankarstva i elektronske trgovine (uključujući i elektronski novac) mogu da pruže značajne mogućnosti za banke. Primera radi, to su širenje tržišta za depozitne i kreditne poslove, mogućnost ponude novih proizvoda i usluga, poboljšanje konkurentne pozicije, smanjenje troškova banke, i sl. Međutim, primena informacione tehnologije u bankarstvu donosi, sa jedne strane, snažan porast organizacionih i ekonomskih potencijala, a sa druge strane, otvara prostor za pojavu novih oblika rizika. Znači, brzi razvoj potencijala e-bankinga nosi i rizike i koristi. Zbog toga se adekvatno obezbeđenje sigurnosti, pojavljuje kao poseban kritičan faktor u funkcionisanju elektronskog bankarstva. Suština problema bezbednosti savremenih sistema elektronskog bankarstva svodi se na rizike narušavanja bezbednosti podataka i identiteta subjekata, pri čemu se relativni odnos značaja pomenutih elemenata menja sa tehnološkim razvojem.

Problemi koji su relevantni za ovu grupu kritičnih faktora zahtevaju:¹⁵⁷

1. utvrđivanje obima i prirode novih rizika,
2. mogućnost i cenu zaštite i
3. određivanje ključa podele dodatnih troškova koje ona sobom nosi.

Ostvarivanje potrebnog nivoa bezbednosti zahteva multidisciplinarni pristup, odnosno pružanje podrške sistemima zaštite od rizika, kako tehničko-tehnološkim sredstvima, tako i odgovarajućim organizacionim merama, kao i adekvatnom zakonodavnom regulativom. U skladu sa ovakvom potrebom došlo je do formiranja posebne Grupe za elektronsko bankarstvo pri Bazelskom komitetu koji se bavi globalnim nadzorom nad bankama. Banke se tokom pružanja usluga elektronskog bankarstva i upotrebe elektronskog novca suočavaju sa određenim setom specifičnih rizika,¹⁵⁸ koji su razmatrani u dokumentima Bazelskog komiteta za bankarsku superviziju, a to su:¹⁵⁹

- operativni rizik,
- reputacioni rizik,
- pravni rizik,
- rizik internacionalnog poslovanja,
- ostali rizici.

Sa razvojem tehnologije informacionih sistema, dolazi do bitnih promena u suštinskim karakteristikama samih rizika, sa jedne strane, i razvoju mehanizama i sistema zaštite od gubitaka koje oni proizvode, sa druge strane. Postoje različite klasifikacije rizika koji su imanentni e-bankarstvu, a brzina promena u tehničko-tehnološkoj osnovi otvara prostor za nove sistematizacije i proširenja. Jedna od korisnih klasifikacija može biti podela (prema uzrocima nastanka) na objektivne i subjektivne rizike. Objektivni rizici bi bili oni koji nastaju kao posledica prirode i karakteristika samih informacionih sistema, a subjektivni rizici bi bili oni koji nastaju namernim ponašanjem pojedinaca ili grupe.¹⁶⁰

¹⁵⁷ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.55

¹⁵⁸ Rizika usmerenih na retail banking.

¹⁵⁹ Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, mart 1998., www.bis.org/publ/bcbs35.pdf

¹⁶⁰ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.56

Objektivni rizici obuhvataju:

1. rizik infrastrukture (nedovoljna zaštita, ranjivost hardvera na fizička oštećenja, loši planovi za slučaj opasnosti, nedostatak mrežnih barijera-*firewall*, nedostaci primene kriptografije);
2. aplikacioni rizik (greške u aplikacijama, nekoordiniranje programske izmene, nedostatak kontrole na ulazu i obradi, nedostatak obezbeđenja softvera);
3. rizik poslovnih obrada (nekompletan prenos podataka, neujednačeno funkcionisanje sistema zaštite u svim delovima, nekorektni mehanizmi kontrole, nepotpuna kontrola pristupa).

Subjektivni rizici predstavljaju pretnju integritetu i poverljivosti podataka. Povreda integriteta može da nastane usled manipulacije podacima (od strane lica koje je ili zaposleno u banci, ili je van banke), sabotage, prevare, hakerisanja ili ubacivanja virusa, a kao posledice ovih povreda mogu nastati gubici podataka, prekid rada sistema (koji sobom nosi troškove ponovnog uspostavljanja), gubitak poverenja i klijenata, sudske troškove i kazne. Povreda poverljivosti može nastati usred otkrivanja podataka, špijuniranja pri neovlašćenom pristupu, osluškivanju komunikacija, hakerisanju i dejstvu virusa. Usled ovih povreda može doći do povrede privatnosti, prevara ili pokušaja iznućivanja, prekida rada sistema, gubitka poverenja i klijenata, narušavanja ugleda i pada prometa i sudskih troškova i kazni.

Sa uvođenjem i razvojem računarskih sistema pojavljuju se i nove vrste grešaka, pri čemu dolazi i do njihovog permanentnog evoluiranja u zavisnosti od karakteristika odgovarajućih računarskih sistema. Za rani period bile su karakteristične greške koje su nastajale usled grešaka u programiranju, a u kasnijoj fazi ta vrsta grešaka biva gotovo potpuno eliminisana. Međutim, istovremeno je došlo do pojave novih grešaka koje su inicirane ulazom informacija u računarski sistem.

Sam razvoj pojedinih elemenata računarskih sistema deluje kao jedno od osnovnih oružja obezbeđenja, zbog toga što zahteva sve viši tehnički nivo pomoćnih sredstava za izvršavanje kriminala (tipičan primer je nemogućnost falsifikovanja kartice sa čipom u odnosu na mogućnost koja postoji kod standardne kartice sa magnetnom trakom). Međutim, ovaj element se u velikoj meri neutrališe usavršavanjem sredstava kojima može da se realizuje zloupotreba i širenjem upotrebe novih sistema.

Filozofija otvorenih mreža otvorila je put brojnim novim zloupotrebama, kao što su računarske krađe, upadi u mrežu, informacioni atak, softversko piraterstvo, tehnološka špijunaža, pranje novca što je dovelo u pitanje kompetentnost aktuelnih mera bezbednosti za informacione i komunikacione sisteme i podatke koji su smešteni u tim sistemima.

Zahtevi sigurnosti u bežičnom okruženju svode se na iste elemente kao i u tradicionalnom, ali je u ovom okruženju znatno teže implementirati odgovarajuću zaštitu zbog sledećih razloga:¹⁶¹

1. ograničena snaga obrade podataka u uslovima bežične infrastrukture dovodi do teškoće u funkcionisanju sigurnosnih algoritama,
2. bežična infrastruktura odlikuje se visokim stepenom latentnosti i nestabilnosti,
3. ne postoji tzv. end-to-end zaštita i

¹⁶¹ Isto, str.58

4. trenutno još uvek nije dovoljno razvijena mreža sertifikata za mobilne medijume.

Međutim, upravo su u toku projekti koji rade na rešavanju ovih problema i uklanjanju pomenutih ograničenja. U tom smislu posebna očekivanja su prisutna u odnosu na podršku plaćanja na Internetu (engl. *Internet Payment Provider - IPP*).

1.1. Operativni rizik

Operativni rizik nastaje iz potencijalnog gubitka usled nedostataka u sistemu pouzdanosti i integriteta. Razmatranje sigurnosti je od najveće važnosti, usled mogućnosti internih i eksternih napada na banku, odnosno njenih sistema i proizvoda. Operativni rizik može nastati i usled zloupotrebe od strane klijenata ili neadekvatnog dizajniranog ili implementiranog elektronskog bankarstva ili sistema elektronskog novca. Shodno iznetom, mogući su sledeći oblici operativnog rizika, i to:¹⁶²

- rizici sigurnosti (pouzdanosti i integriteta sistema),
- rizici dizajniranja, implementacije i održavanja sistema,
- rizici zloupotrebe proizvoda ili usluga od strane klijenata.

Rizici sigurnosti se pojavljuju u vezi sa kontrolom informacija pomoću kojih banka komunicira sa okruženjem, transfera elektronskog novca, kao i sprečavanja pronevere, odnosno falsifikata. Kontrola pristupa sistemu banke postaje sve kompleksnija s obzirom na proširenje računarskih sistema, geografske disperziranosti pristupnih tačaka sistemu i upotrebe različitih komunikacionih puteva, uključujući i javnu mrežu kao što je Internet. Neautorizovani pristup sistemu banke od strane hakera može prouzrokovati zloupotrebu poverljivih informacija o klijentima, kao i direktne troškove banke. Takođe u odsustvu adekvatne kontrole, neovlašćeno lice može pristupiti sistemu i ubaciti virus u njega. Nije zanemarljiva i moguća zloupotreba od strane zaposlenih, čija preventiva iziskuje uspostavljanje sistema adekvatne kontrole. Postoji i rizik falsifikovanja elektronskog novca, čija preventiva zahteva određene vidove tehničke zaštite.

Primer mogućeg rizika sigurnosti jeste neautorizovani pristup sistemu. To znači da poverljive informacije mogu biti presretane od strane neautorizovanih lica, na primer, od strane hakera koji ulaze u interne sisteme. Moguće je ubacivanje virusa u bankarski sistem, što dovodi do oštećenja ili uništenja bankarskog sistema ili podataka. Potencijalni efekat na banku je gubitak i krađa podataka. Pored toga, onemogućava se funkcionisanje bankarskog informacionog sistema ili bar jednog dela. Javljaju se i troškovi za otklanjanje problema. Pored toga, može se stvoriti potencijalna nesigurnost u bankarski sistem i negativna reklama. Banke mogu da primene određene mere za upravljanje rizikom. Moguće je primeniti sigurnosne komunikativne mere, kao što su „*fire wall*“, lozinke, tehnologiju šifrovanja i autorizaciju korisnika. Potrebno je vršiti testiranje na „ranjivost“ sistema, kao i stalno proveravanje sistema na viruse.

Treba pomenuti i mogući rizik po sistem koji se sprovodi od strane zaposlenih, odnosno prevare zaposlenih. Moguća je zloupotreba podataka kako bi iskoristili sredstva sa računa banke ili prikupili određene informacije iz sistema. Pored toga, moguća je i krađa smart

¹⁶² Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, mart 1998., www.bis.org/publ/bcbs35.pdf

kartica. Banka bi imala određene troškove za vraćanje sredstava klijentu i obavezu da rekonstruiše tačne podatke. Klijent može da posmatra banku kao nepouzdanu, a banka se može suočiti i sa pravnim sankcijama, kao i sa negativnim publicitetom. Mere koje banka može uvesti su uvođenje interne kontrole, uvođenje eksterne revizije rada zaposlenih, adekvatna kontrola skladišta podataka, pristupa smart karticama, i sl.

Rizici dizajniranja, implementacije i održavanja sistema imaju bitan uticaj na razvoj sistema elektronskog bankarstva i elektronskog novca. Rizici koji se mogu manifestovati iz ovog delu su prekid ili usporavanje sistema, što može imati negativne konsekvence na klijente banke. Nije redak slučaj da se banke opredeljuju za spoljne provajdere i eksperte za implementaciju, funkcionisanje i podršku koja obezbeđuje nesmetano odvijanje elektronskog bankarstva i poslove sa elektronskim novcem. Ovakav vid *outsourcinga* ima svoj rizik kada provajderi nisu dovoljno stručni ili nisu u mogućnosti da modernizuju svoju tehnologiju u skladu sa zahtevima koji se pred njih postavljaju. Usled intenzivnog razvoja informacione tehnologije javlja se rizik narušavanja operativne aturnosti sistema, zbog zamene zastarele tehnologije. Rizik u poslovanju se može javiti i zbog nedovoljne pripremljenosti zaposlenih u bankama za promene u tehnologiji i načina rada, što može rezultirati slabljenjem funkcionisanja sistema.

Jedan od mogućih rizika dizajniranja, implementacije i održavanja sistema, predstavljaju zaposleni i menadžment koji teže prihvataju inovacije. Izuzetno brze izmene tehnologije mogu da dovedu do toga da menadžment i zaposleni u banci nisu u potpunosti u mogućnosti da shvate prirodu nove tehnologije koja se primenjuje u bankama. Rezultat toga je slaba implementacija novih tehnologija i nemogućnost da se obezbedi kontinuirana podrška razvoju. Neophodno je sprovoditi obuku, kao permanentni proces, i za menadžment i za zaposlene.¹⁶³

Zloupotreba proizvoda i usluga od strane klijenata, bilo namerna ili nenamerna, je još jedan izvor operativnog rizika. Rizik se povećava usled neadekvatne edukovanosti klijenata, od strane banke, o merama sigurnosti prilikom verifikacije transfera elektronskog novca. Personalne informacije klijenata banke koji učestvuju u elektronskom bankarstvu (broj kreditne kartice, broj računa u banci, i sl.) moraju biti posebno zaštićene prilikom transakcija elektronskog novca.

Primer rizika zloupotrebe proizvoda i usluga od strane klijenata jeste i poricanje izvršenja transakcije. Klijent može da poriče da je obavio transakciju i da zahteva povraćaj sredstava. Javljaju se troškovi banke vezani sa dokazivanjem da je klijent autorizovao transakciju. Moguć je nastanak gubitka za banku ukoliko se ne može dokazati da je transakcija i stvarno obavljena. Potrebno je da banka implementira sigurnosne mere koje će obezbediti identifikaciju klijenta, kao što su personalni identifikacioni brojevi.

1.2. Reputacioni rizik

Reputacioni rizik je rizik negativnog javnog mnjenja, koji rezultira značajnom gubitku sredstava ili odlivu klijenata iz banke. Njegov negativan efekat na imidž banke, može da bude trajan. Može nastati i kao posledica preduzimanja akcija koje imaju za posledicu gubitak javnog poverenja u sposobnost banke da obavlja svoje poslovanje. Značajno narušavanje

¹⁶³ www.eccf.su.ac.yu/obaveštenja/inf_u_finansijama.htm

imidža banke može nastati i usled loših komunikacionih mreža, pri čemu klijenti nisu u stanju da saznaju informacije o stanju na svojim računima, i sl.

Reputacioni rizik može nastati ako proizvodi ili usluge koje banka pruža ne zadovoljavaju očekivanja svojih klijenata, što dovodi do negativne javne reakcije, ili ako je banka izložena malverzaciji i obmani od eksterne strane, koja će se odraziti kroz nesigurnost klijenata ka bankarskom sektoru. Održavanje reputacionog rizika je bitno ne samo zbog održavanja dobrog imidža pojedine banke već i celokupnog bankarskog sektora, jer ako bi bila naneta šteta odrećnoj banci u delu elektronskog poslovanja, time bi bila poljuljana sigurnost i u druge banke, odnosno u celokupan sistem.¹⁶⁴

Primer reputacionog rizika je narušavanje bezbednosti sistema. Ulazak hakera u interni sistem, ili ubacivanje virusa u bankarski sistem može izazvati značajne probleme u funkcionisanju sistema ili u očuvanju integriteta podataka. To može dovesti do toga da klijenti prestanu da koriste usluge banke, odnosno utiče na odliv klijenata iz banke. Moguća mera je testiranje sistema i primena sigurnosnih mera, kao i proveravanje sistema na viruse.

Primer reputacionog rizika za banke svakako bi mogao biti i sprečavanje nastanka odrećnog događaja. Ako se banka može pohvaliti da u prethodnom vremenskom periodu od nekoliko godina nije imala neovlašćenih ulazaka u operativni - elektronski sistem banke, da garantuje tajnost podataka koje elektronski obrađuje, svakako za ovu banku možemo reći da je minimizirala reputacioni rizik. Nasuprot tome, ako je banka poznata po „čestim“ neautorizovanim ulascima u operativni sistem i ako se na ovaj način može desiti da dođe do zloupotrebe dobijenih informacija svakako da ova banka može u budućnosti očekivati probleme sa klijentima upravo usled nastanka reputacionog rizika.

Da bi banka mogla da se zaštiti od reputacionog rizika, potrebno je da pruža usluge elektronskog bankarstva dosledno i konstantno, a sve u skladu sa visokim očekivanjima klijenata. Banka mora da ima mogućnost da pruža usluge elektronskog bankarstva svim korisnicima, tako da je potrebno da održava dostupnost sistema u svim okolnostima. Bitno je da se uspostave mehanizmi za vanredne situacije da bi se minimizirao reputacioni rizik koji može proizići iz neočekivanih događaja, uključujući interne i eksterne prodore u sistem koji mogu uticati na pružanje usluga elektronskog bankarstva.

Banke bi, u cilju ispunjenja očekivanja klijenata, trebale da efikasno planiraju kapacitete, poslovni kontinuitet i postupanje u slučaju nepredviđenih okolnosti. To znači da bi trebale da izrade odgovarajuće planove za vanredne situacije, uključujući komunikacijsku strategiju, koja bi obezbedila kontinuitet poslovanja, kao i kontrolu reputacionog rizika. Planovi za vanredne situacije bi omogućili oporavak sistema i usluga elektronskog bankarstva pri različitim scenarijima. Analiza scenarija bi trebala da obuhvati razmatranje verovatnoće nastanka rizika i njegovog uticaja na banku. Pored toga, banke bi trebale da utvrde mehanizme za utvrđivanje nastale vanredne situacije čim se ona pojavi, uz jasno definisanje protivmere koja treba da budu sprovedena da bi se minimizirao efekat nastalog događaja. Takođe je neophodno da službe za podršku klijentima redovno prate i preispituju pritužbe klijenata, jer se na ovaj način mogu dobiti značajne informacije o nefunkcionalnosti sistema i budućim poljima koje je potrebno uspešnije servisirati, kako bi operativnost i efikasnost sistema bila na višem nivou.

¹⁶⁴ www.eccf.su.ac.yu/obaveštenja/inf_u_finansijama.htm

1.3. Pravni rizik

Pravni rizik nastaje usled narušavanja ili neusaglašenosti sa zakonima, pravilima, regulativama ili propisane prakse ili u slučaju kada zakonska prava i obaveze učesnika u transakcijama nisu pravno regulisana. Posebno mora biti regulisano sprečavanje pranja novca, jer savremena mogućnost poslovanja u velikoj meri može biti veoma atraktivna za takav vid zloupotrebe. To dovodi do zaključka da banke koje primenjuju elektronsko bankarstvo i poslovanje sa elektronskim novcem, moraju posebnu pažnju posvetiti identifikaciji, odnosno autentifikaciji klijenta, kao i zaštiti privatnosti (kao metod autentifikacije banke mogu da koriste digitalne sertifikate).

Jedan od pravnih rizika je i pranje novca. Elektronska banka može biti zloupotrebljena od strane klijenata i za kriminalne radnje, odnosno pranja novca. Moguće su pravne sankcije za banke, odnosno kazne za neprimetno kršenje zakona. Neophodno je da banka razvije mehanizme za identifikaciju klijenata, kao i procedure koje će omogućiti da se uoči i izvesti o sumnjivim transakcijama. Pored toga, potrebno je razviti planove za slučaj da se dogode nepredviđene situacije i da se vrši konstantna obuka zaposlenih.

Jedan od rizika je i zaštita privatnosti klijenata. Ukoliko bi banka objavila informacije o finansijskim transakcijama klijenta bez njegove prethodne saglasnosti, mogla bi biti tužena za narušavanje privatnosti, kao i da snosi troškove tužbe. U tom slučaju, banka može da se suoči sa pravnim sankcijama. Potrebno je da banka preispita procedure zaštite privatnosti i da vrši periodično preispitivanje istih, kao i da obučava zaposlene za primenu usvojenih procedura.

Zaštita klijenata, kao i propisi i zakoni koji se odnose na privatnost klijenata se razlikuje od zemlje do zemlje. Ipak, banke imaju odgovornost da osiguraju svojim klijentima određen nivo sigurnosti, što se tiče objavljivanja informacija, zaštite podataka o njima, kao kada bi klijenti obavljali poslove preko tradicionalnih bankarskih kanala distribucije proizvoda i usluga.

Za banke je ključna odgovornost očuvanje poverljivosti informacija o klijentima. Zloupotreba ili neautorizovano objavljivanje poverljivih podataka o klijentima može da izloži banku pravnom i reputacionom riziku. Da bi banke obezbedile poverljivost informacija o klijentima, potrebno je da ustanove politike i standarde koje se odnose na privatnost klijenata, a koje bi trebale da budu usklađene sa svim propisima i zakonima o privatnosti koji se primenjuju u zemljama u kojima banka pruža proizvode i usluge elektronskog bankarstva. Pored toga, podaci o klijentima se ne bi smeli koristiti, osim u posebno dopuštene svrhe i ako su klijenti autorizovali njihovo korišćenje. U nekim zemljama, zakoni i propisi ne obavezuju banke da traže od klijenata dopuštenje za korišćenje podataka o njima u interne svrhe. Međutim, oni mogu obavezivati banke da klijentima pruže mogućnost odbijanja davanja dopuštenja banci da deli takve informacije s trećom stranom ili s povezanim društvom. U drugim zemljama, klijenti mogu imati pravo da spreče banke da se koriste njihovim podacima bilo u interne bilo u eksterne svrhe.

Da bi banke minimizirale pravni rizik, povezanim sa poslovima elektronskog bankarstva koji se obavljaju u zemlji i inostranstvu, potrebno je da osiguraju pružanje adekvatnih informacija na svojim web stranicama. Na taj način bi se klijentima omogućilo da provere identitet i regulatorni status banke pre nego što se upuste u transakcije elektronskog bankarstva. Primera radi, informacije koje se mogu staviti na web sajt mogu biti ime banke i lokacija sedišta, kao i lokalne filijale, način na koji klijent može kontaktirati sa bankom po pitanju reklamacija,

sumnje na zloupotrebu računa i sl., način na koji se klijenti mogu žaliti organu koje se bavi zaštitom potrošača, i dr.

U domicilnim uslovima, značajnom smanjenju pravnog rizika doprinela je i Narodna banka Srbije nizom mera i odluka kojim su uredile poslovanje banaka u ovoj sferi. Brojni su primeri zaštite potrošača putem obelodanjivanja osnovnih informacija o banci (na primer, na svim dopisima tj. memorandumima poslovnih banaka obavezno je da se navedu podaci koji se odnose na naziv banke, matični broj, sedište, broj računa, ali i podaci koji se odnose na poslednji poznat iznos tj. visinu kapitala banke). Zatim, NBS insistira i na uvođenju novog odeljenja¹⁶⁵ u poslovanje banaka - odeljenja *Compliance*.

1.4. Rizici internacionalnog poslovanja

Elektronsko bankarstvo i aktivnosti elektronskog novca su bazirani na tehnologiji koja ne poznaje geografske barijere. Takva tržišna ekspanzija može da se širi preko nacionalnih granica, ali se sa tim povećava i rizik poslovanja. Rizici, karakteristični za domicilno bankarstvo su takođe relevantni i za internacionalno bankarstvo, s tim što ovi rizici mogu biti još naglašeniji. Primera radi, u poslovanju putem Internet bankarstva mogući su karakteristični pravni zahtevi (zaštita potrošača, zakonski propis o sprečavanju pranja novca, i sl.), čije neprimenjivanje može da izloži banku pravnim rizicima. U internacionalnom poslovanju povećan je i kreditni rizik usled otežane ocene kreditne sposobnosti tražioca kredita.

Banke koje se odluču da pružaju usluge klijentima na raznim nacionalnim tržištima trebalo bi da upoznaju razne nacionalne pravne zahteve, kao i da razumeju nacionalne razlike u očekivanju i poznavanju proizvoda i usluga od strane klijenata. Sa druge strane, neophodno je da banka proceni rizik zemlje i razvije planove nepredviđenih obaveza koji će predvideti aktivnosti u slučaju ekonomskih ili političkih problema na nacionalnom tržištu. Pod ekonomskim problemima se podrazumevaju promene privrednih kretanja, privrednog razvoja, uslova poslovanja u određenoj zemlji i njena spoljna likvidnost, dok se pod političkim problemima podrazumeva promena u sastavu vlade ili vladine politike, politički nemiri ili ratovi. Naravno da se navedene ekonomske i političke promene smatraju problemima ukoliko idu na štetu poslovanju banke.

Rizik transfera raste sa prihvatanjem inostranih procesora i drugih inostranih učesnika u elektronskom poslovanju. Strani procesori ili drugi učesnici u elektronskom poslovanju sa bankom mogu biti u nemogućnosti da ispune svoje obaveze zbog socijalnih, ekonomskih ili političkih razloga. Postoje i potencijalni troškovi rešavanja problema kupaca. Pored toga, banka može da se suoči sa tužbom korisnika usluga. Mere koje banka može primeniti u upravljanju rizikom jeste da izvrši procenu rizika zemlje.

1.5. Ostali rizici

Ostale bankarske rizike uključuje i kreditni rizik, rizik likvidnosti, kamatni rizik i tržišni rizik, koji mogu nastati iz elektronskog bankarstva i poslovanja sa elektronskim novcem.

¹⁶⁵ Zakonom o bankama koji je stupio na snagu oktobra 2006. godine, banke su u obavezi da osnuju posebno odeljenje – compliance – koje je direktno vezano u organizacionoj šemi banke sa predsednikom izvršnog odbora, a osnovni i jedini zadatak ovog odeljenja jeste praćenje usklađenosti poslovanja banaka sa zakonskim i drugim propisima i međunarodnim standardima.

Kreditni rizik je rizik koji se odnosi na korisnika kredita da neće ispuniti svoju obavezu u punoj vrednosti ili u predviđeno vreme. Banke imaju mogućnost da elektronskim putem prime zahteve za kredit i da ga odobre, što zahteva adekvatne procedure za utvrđivanje kreditne sposobnosti klijenata, jer se u protivnom povećava rizik za banku.

Kao što je navedeno, primer kreditnog rizika je i nesposobnost plaćanja obaveza dužnika koji je kredit dobio putem Interneta. Banka može odobriti kredit klijentima van svog tržišta, pri čemu se može desiti da joj podaci nisu poznati ili su skupi da bi ih prikupila. Potencijalni efekat za banku je da mora da izvrši rezervisanja za loše plasmane. Banka može da sprovede određene mere za upravljanje rizikom. Primera radi, da obezbedi da je procena kreditne sposobnosti klijenata koji su na ovaj način zatražili kredit, ista kao i kod „tradicionalnih” tražilaca kredita i da izvrši reviziju procedura odobravanja kredita.

Mogući rizik za banku je i nesposobnost plaćanja obaveza izdavaoca elektronskog novca. Izdavalac elektronskog novca može postati nesolventan i nelikvidan, dok banka „drži” elektronski novac u svom posedu. Efekat toga je da će banka možda morati da koristi sopstvena sredstva kako bi oslobodila elektronski novac koji se nalazi kod njenih klijenata. Moguće mere za upravljanje rizikom jeste revizija svih izdavatalaca elektronskog novca i monitoring, odnosno nadgledanje finansijske snage izdavatalaca elektronskog novca.

Kreditni rizik predstavlja osnovni rizik u poslovanju banke sa klijentima, koji nastaje kada dužnici banke nisu u mogućnosti da servisiraju svoje obaveze prema banci, odnosno da vrate kredit (ili druge vidove plasmana) sa pripadajućom kamatom (i/ili naknadom) o roku njihovog dospeća. Kao rezultat toga javlja se gubitak u bilansu uspeha banke. Banka može da upravlja sa kreditnim rizikom na sledeće načine:¹⁶⁶

- a) primenom limita (odnos rizične i ukupne aktive, odnos gotovine i kratkoročnih hartija od vrednosti prema ukupnoj aktivni, odnos kapitala i rezervi banke),
- b) rigoroznom selekcijom kreditnih zahteva,
- c) diverzifikacijom plasmana kreditne aktive (na veći broj korisnika kredita sa manjim obimom odobrenih kreditnih iznosa),
- d) instrumentima obezbeđenja (cedirano potraživanje, lombardna zaloga, hipotekarna zaloga, položen depozit za izmirenje glavnice kredita i kamata, položen budući devizni priliv i sl.).

Jedan od najpoznatijih metoda merenja rizika jeste *CreditMetrics* model, razvijen 1997. godine od strane *J. P. Morgan Bank*.¹⁶⁷ Suština navednog modela jeste kvantitativni okvir za sagledavanje kreditnih rejtinga. Za razliku od drugih poznatih modela (*Z-score* - koji daje samo verovatnoću izvršavanja i neizvršavanja kreditnih obaveza dužnika), *CreditMetrics* daje permanentnu rekalkulaciju kvaliteta bankarskih zajmova i tržišne vrednosti portfolia banaka. Primer delovanja metode bazira se na sledećoj konstataciji. Ako se kreditni rejting određene kompanije koja je dobila kredit, snizi u toku otplate kredita, ova kompanija bi trebala da počne da plaća višu kamatnu stopu, kako bi se kompenzovao novonastali povećani rizik. Međutim, ako je kompanija dobila kredit po fiksnoj stopi, banke nemaju mogućnosti promene iste, pa samim tim vrednost ovog kredita na sekundarnom tržištu bi opala, odnosno dobila bi se smanjena tržišna vrednost zajma u sadašnjem momentu i naravno obrnuto, u slučaju rasta rejtinga kompanije koja je dobila bankarski kredit, banka bi na sekundarnom tržištu bila u

¹⁶⁶ Vunjak N.: „Finansijski menadžment“, Proleter – Bečej, Subotica, 2005., str. 342

¹⁶⁷ Čirović M.: „Bankarstvo“, Beograd, 2001., str. 335

mogućnosti da isti proda po višoj stopi, tj. tržišna vrednost zajma bi porasla. Nedostatak ovog modela u domicilnim uslovima jeste što se on može primenjivati samo u razvijenim tržišnim ekonomijama koje imaju agencije koje se bave publikovanjem kreditnih rejtinga (na primer, *Standard & Poor's*, *Moody's*, *Fitch*). Nažalost, kod nas još ni jedna kompanija nema međunarodni rejting, a iz neposrednog okruženja jedino su kompanije „Pliva“ i Zagrebačka banka a.d. dobile rejtinge od strane ovih međunarodnih rejting agencija.

Rizik likvidnosti je rizik koji nastaje u slučaju da banka nije u mogućnosti da izvršava dospele obaveze koje nastaju tokom elektronskog bankarstva. Rizik likvidnosti je rizik mogućnosti nastanka negativnih efekata na finansijski rezultat i kapital banke usled nesposobnosti banke da ispunjava svoje dospele obaveze. Banka svojom imovinom i obavezama upravlja na način koji joj omogućava da u svakom trenutku ispunji svoje dospele obaveze (likvidnost) i da trajno ispunjava sve svoje obaveze (solventnost). U cilju efikasnog upravljanja rizikom likvidnosti, banka usvaja i sprovodi politiku upravljanja likvidnošću, koja obuhvata planiranje priliva i odliva novčanih sredstava, praćenje likvidnosti i donošenje odgovarajućih mera za sprečavanje ili otklanjanje uzroka nelikvidnosti.

Nelikvidnost izdavaoca elektronskog novca može da iznenadno poveća tražnju za povlačenjem elektronskog novca iz opticaja. Banka može pretrpeti gubitke tražeći alternativne izvore finansiranja. Ukoliko se u javnosti nasluti problem likvidnosti, biće još više prisutnije povlačenje depozita iz banke ili povlačenje elektronskog novca. Neispunjavanje ovih obaveza (u smislu povrata depozita) može dovesti i do ozbiljnih reputacionih problema. Mere koje banka može sprovoditi su da investira sredstva u likvidnu aktivu i da razvije monitoring korišćenja sredstava. Primer rizika likvidnosti u elektronskom bankarstvu je primer rizika sekundarnog značaja, naime rizik likvidnosti je više klasičan bankarski rizik i nastaje u trenucima kada banka nije u mogućnosti da ispunjava svoje dnevne obaveze usled povećanog povlačenja depozita njenih klijenata ili usled velikog odliva sredstava. Isto ovakvo dejstvo rizik likvidnosti može da proizvede i kod poslovnih banaka koje su se orijentisale na elektronsko poslovanje (u domicilnim uslovima još uvek nemamo ovakvu instituciju i moramo napomenuti da su sve banke, banke klasičnog – univerzalnog tipa koje su više ili manje razvile elektronske kanale komunikacije sa klijentima). Naime, usled određene informacije koje se mogu pojaviti na tržištu (pogotovo u razvijenim zemljama gde je pristup informacijama lakši i brži), usled loših poslovnih poteza uprave banke ili lošeg, odnosno pogrešnog investiranja finansijskih sredstava, u javnosti može da se stvori utisak da banka ne posluje adekvatno, da će u budućnosti pretrpeti gubitke i dr. Sve ovo može da dovede, ukoliko uprava i menadžment banke ne odgovori adekvatno, do odliva depozita i fizičkih i pravnih lica i narušavanja likvidnosti banke. U ovakvim situacijama banka mora da ima plan odnosno odgovor kako bi se sa jedne strane smanjile i minimizirale posledice nastanka štetnog događaja, a sa druge strane banka mora da zaduživanjem na finansijskom tržištu prebrodi problem likvidnosti koji je nastao kao posledica povlačenja sredstava klijenata.

Kamatni rizik se odnosi na smanjenje kamatnih stopa do stepena kada negativna kretanja kamatnih stopa smanjuje vrednost imovine u zavisnosti od neispunjenih obaveza.

Neočekivane i nepoželjne izmene u kamatnim stopama mogu umanjiti vrednost aktive izdavaoca elektronskog novca u odnosu na stanje izdatog elektronskog novca. Neočekivano opadanje vrednosti aktive može dovesti do situacije da banka ne ispunjava zakonske zahteve. Može nastati i problem likvidnosti. Kamatni rizik se sastoji od rizika promene kamatnih stopa na plasmane i obaveze banke, naravno ukoliko su ove promene nepovoljne za banku. Na primer, klijenti uvek imaju zahteve prema poslovnim bankama da se plasman sredstava banke

vrši uz što niže kamatne stope, s obzirom na tržišnu utakmicu između poslovnih banaka. Rizik kamatne stope može da nastane u slučajevima kada banke odobre određene plasmane po fiksnim kamatnim stopama na duže vremenske periode, koji nisu praćeni adekvatnom strukturom izvora sredstava banke. Ovo znači da je banka plasirala sredstva po određenoj kamatnoj stopi na duže rokove nego što ima obezbeđene depozite. U slučaju određenih poremećaja na tržištu, izvori sredstava mogu da poskupe, što bi dovelo do situacije da banke imaju određene gubitke na plasmanima - kreditima koji su odobravani na duže rokove i pod uslovima koji su trenutno neodrživi na tržištu. Ovde se uvek postavlja pitanje koji je način odbrane banaka od pojave kamatnog rizika. Prvi slučaj bi bio da banke imaju ročnu usklađenost bilansa, zatim da banke imaju valutnu usklađenost bilansa. Ukoliko pak ovo nije slučaj, postoje alternativni ali manje popularni načini odbrane od kamatnog rizika. Jedan od njih svakako jeste revizija kamatnih stopa u unapred utvrđenim vremenskim intervalima, kako na plasmane banke, tako i na depozite banaka (ugovaranje promenljive, a ne fiksne kamatne stope). Drugi model, koji je sve prisutniji i na domaćem tržištu kod banaka koje su privatizovane od strane poslovnih banaka iz inostranstva, jeste da se odobravanje kredita vrši uz promenljivu kamatnu stopu (EURIBOR) i fiksnu marginu. Na ovaj način, povlačenjem sredstava iz inostranstva (najčešće od banke – *head office*) uz iste uslove EURIBOR i margina banke smanjuju mogućnost nastanka kamatnog rizika. U domicilnim uslovima, jedini rizik koji se u ovim slučajevima može pojaviti jeste rizik države - odnosno promene obavezne rezerve na zaduživanja u inostranstvu, čime se i cena koštanja povučenih sredstava značajno menja.

Tržišni rizik koji može nastati usled promene u cenama na tržištu, uključivši i promene deviznog kursa, kojeg svakako karakterišu oscilacije, tako da su banke koje obavljaju plaćanja u formi elektronskog novca u stranoj valuti izložene riziku.

Može se javiti uvećanje rizika deviznog kursa nastalog zbog prihvatanja stranih valuta kao načina plaćanja. Izmene u deviznom kursu mogu da dovedu do gubitaka u poslovanju banke, i konačno do smanjenja prihoda. Primer za ovaj slučaj rizika odnosi se na prihvatanje određenih rizika u poslovanju sa nestabilnim valutama. Slučaj koji možemo navesti iz domaće poslovne prakse odnosio bi se na investiranje banke u npr. državne zapise koji imaju određenu fiksnu stopu prinosa izraženu u dinarima. S obzirom na nestabilnost domaće valute (i trenutni nizak kurs evra), postavlja se pitanje, šta ukoliko banke investiraju određenu količinu sredstava u dinarske zapise države i posle određenog vremenskog perioda (6 meseci do godinu dana) dočedo poremećaja na tržištu deviza i pomeranja kursa evra. Ovo može dovesti do toga da poslovna banka ne zaradi ništa na ovakvom vidu poslovanja, bez obzira na relativno visoku nominalnu kamatnu stopu, već čak i da pretrpi određene gubitke usled oscilacija kursa dinara. Takođe, možemo da navedemo i „drugu stranu medalje“ koja se odnosi na činjenicu da je u toku 2006. godine, kurs evra značajnije, čak za 10% opao. To je dovelo do činjenice da su banke kao i druga pravna i fizička lica koja su uložila svoju aktivu u dinarske plasmane (obveznice, štednju...), ostvarile ne samo adekvatnu zaradu po pitanju kamata na prinose, već su i iznosi koji su vraćeni po isteku perioda na ime glavnice vredeli u evrima više nego što je to bilo na dan ulaganja.

2. UPRAVLJANJE RIZICIMA

Elektronsko bankarstvo i poslovanje sa elektronskim novcem je postalo široko primenjivano od strane banaka, kao i od strane korisnika bankarskih usluga i trgovaca. To je doprinelo da ovaj savremeni vid poslovanja prate brojni rizici. Cilj banaka je da ostvare kontrolu i upravljanje rizikom. Proces upravljanja rizikom uključuje sledeće faze: procenu rizika,

upravljanje i kontrolu rizika i monitoring rizika. Ovi procesi moraju biti pod nadzorom top menadžmenta banke.¹⁶⁸

2.1. Procena rizika

Procenu rizika potrebno je organizovati kao permanentan proces, koji se odvija u tri faze. U prvoj fazi potrebno je da banka identifikuje, a po mogućnosti i kvantifikuje rizike. Identifikacija rizika je ključna polazna pretpostavka u procenama rizika, s obzirom na to da su najopasniji rizici oni kojih banke nisu svesne, jer mogu da dovedu do velikih i neplaniranih troškova. Identifikacija rizika moguća je na nekoliko načina, a najčešći metodi odnose se na empirijska iskustva dosadašnjeg poslovanja banaka, kao i na razmenu iskustava između samih poslovnih banaka. Ukoliko nije moguće kvantifikovati rizik, potrebno je utvrditi kako potencijalni rizik nastaje i kakve su mogućnosti da se ovi rizici ograniče. Pored toga, bitno je i to da se utvrdi učestalost, odnosno frekvencija pojave rizika. U drugoj fazi određuje se mogućnost banke u pogledu nivoa tolerancije rizika, baziranoj na oceni gubitka koji će banka moći da podnese. Ključno za sve banke jeste da, kada postanu svesne rizika s kojim posluju, načina njegovog ispoljavanja i frekventnosti pojave, utvrde procenu ispoljavanja određenog rizika. Ova procena je izuzetno bitna s obzirom na to da na osnovu procenjene vrednosti - odnosno gubitka usled ispoljavanja određenog rizika, banka treba da definiše preventivne i korektivne mere. Prioritet svakako treba da bude definisanje preventivnih mera i eliminisanje svih preliminarnih faktora koji mogu da dovedu do nastajanja određenog rizika.

S tim u vezi banke bi trebalo da za svaki od utvrđenih rizika definišu koji su to indikatori, odnosno pokazatelji čije bi pojavljivanje moglo da ukaže na nastanak određene negativne pojave, tj. rizika i da na osnovu tih indikatora definišu listu akcija za otklanjanje istih. Korektivni faktori imaju samo dejstvo na ublažavanje posledica nastalih dejstvom određenog rizika odnosno negativnog slučaja u poslovanju banke. U trećoj fazi ocenjuje se da li se izloženost riziku kreće u okviru podnošljivih limita. Treća faza je faza u kojoj bi trebalo da se definiše nadgledanje rizika ukoliko se on i desi. Ovo se posebno odnosi na primenu korektivnih mera kojima bi rizik, odnosno njegov uticaj treba da se minimizira.

Upravljanje bankarskim rizicima može biti kvalitativno i kvantitativno. Kvalitativno upravljanje rizicima se uglavnom koristi za rizike koji se ne mogu kvantifikovati. Ova metoda upravljanja rizikom se zasniva na iskustvenim ocenama bankarskih eksperata. U savremenom bankarstvu tendencija je da se, kada je god to moguće, koriste kvantitativne metode upravljanja rizicima. Kod kvantitativnog sagledavanja bankarskih rizika, osnovni pristup se sastoji u sagledavanju prosečnog iznosa gubitaka, kao i stope disperzije gubitaka. Proračunavanje rizika se može vršiti po tipovima aktive, linijama bankarskih proizvoda i nivoa individualnih klijenata. Postoje i mišljenja da je najefektivniji pristup u upravljanju rizicima onaj koji uključuje mešavinu kvantitativnog i kvalitativnog pristupa, odnosno koji bi uskladio matematičko modeliranje sa tržišnim iskustvom.

Ukoliko banka ne bi dobro upravljala rizicima, postoji opasnost od nesolventnosti. Iz tog razloga je težište upravljanja rizicima preneto na povezivanje visine rizika sa adekvatnim nivoom kapitala, uključujući i rezerve, kao izvora za njihovo pokrivanje. Očekivani gubici se

¹⁶⁸ www.eccf.su.ac.yu/obaveštenja/inf_u_finansijama.htm

pokrivaju iz operativnih rezervi za pokriće gubitaka, dok kapital banke služi kao izvor za pokriće samo neočekivanih gubitaka.

2.2. Upravljanje i kontrola rizika

Nakon što se procene rizici i odrede nivoi njihove tolerancije, na menadžmentu banke je da počne sa upravljanjem rizicima i njihovoj kontroli. Upravljanje rizikom uključuje aktivnosti: implementaciju sigurnosnih mehanizama i mera, koordinaciju interne komunikacije, vrednovanje i poboljšanje proizvoda i usluga, implementaciju mera za kontrolu rizika koji se odnose na spoljne davaoce usluga (engl. *outsourcing*) i planiranje nepredvidivih okolnosti.¹⁶⁹

Sigurnosni mehanizmi i mere koje se primenjuju pri upravljanju i kontroli rizika, podrazumevaju kombinaciju sistema zaštitnih mera, aplikacija i interne kontrole, koji se koristi da se osigura integritet, autentičnost i pouzdanost podataka, operativnih procesa (obrada) i izveštaja. Zaštita je bazirana na razvoju i implementaciji adekvatnih sigurnosnih mehanizama i mera za interne procese. Pored toga, razvijaju se i implementiraju mehanizmi i mere za komunikaciju između banke i eksternih sistema, sve u cilju smanjenja rizika od eksternih i internih napada na sistem elektronskog bankarstva i elektronskog novca. Sigurnosne mere su kombinacija hardverskih i softverskih alata. Kao sigurnosne mere koristi se: šifrovanje podataka, digitalni sertifikat, instalacija zaštitnih zidova, antivirusna kontrola, korišćenje PIN-a, i sl.

Šifrovanjem podataka se rešava problem tajnosti prenosa podataka putem računarskih komunikacionih mreža. Šifrovanje je proces transformacije informacija u šifrovane sadržaje koje razume primalac informacija. Proces šifriranja uključuje šifrovanje podataka, gde pošiljalac poruke vrši šifriranje sa ključevima za šifrovanje i dešifrovanje podataka, gde primalac poruke vrši dešifrovanje sa ključevima za dešifrovanje.

Digitalni sertifikat (DC) predstavlja elektronsku potvrdu kojom se potvrđuje veza između podataka za verifikaciju elektronskog potpisa i identiteta korisnika. Digitalni sertifikat izdaju sertifikaciona tela (CA).

Zaštitni zidovi (engl. *firewall*) predstavljaju kombinaciju hardvera i softvera i ograničavaju eksterni pristup internom sistemu priključenom na otvorenu mrežu, kao što je Internet. Poruke koje dolaze iz eksternog okruženja preko zaštitnog zida nisu apsolutno zaštićene od virusno zaraženih programa koji dospevaju preko Interneta. U tu svrhu se koriste antivirusni programi.

Antivirusna kontrola se koristi sa ciljem da se predupredi upad i nanošenje štete od strane računarskih virusa, koji predstavljaju napisane programe koji uzrokuju štetno dejstvo kod korisnika računara, kao što je prisustvo raznim porukama, a zatim i brisanje datoteka i diskova. Računarski virusi se obično prenose Internet porukama, putem disketa i CD-a. Poznati antivirus programi koji se koriste kao zaštita su: *IBM Anti Virus*, *Kaspersky*, *Norton*, i sl.

PIN se koristi u cilju prevencije od neautorizovanog pristupa podacima banke.

¹⁶⁹ www.eccf.su.ac.yu/obaveštenja/inf_u_finansijama.htm

Sigurnosne mere koje se primenjuju predstavljaju kombinaciju hardverskih i softverskih alata, koje služe za smanjivanje rizika od internih i eksternih napada na sistem elektronskog bankarstva. Putem njih se osigurava integritet, autentičnost i pouzdanost podataka, operativnih procesa i izveštaja. Upotrebom navedenih sigurnosnih mera se vrši dodeljivanje i kontrola autorizacije korisnika sistema i aplikacija elektronskog bankarstva. Oni obezbeđuju čuvanje podataka iz sistema, odnosno obezbeđuju zaštitu i kontrolu pristupa. Na taj način se sprečava neautorizovani pristup ključnim sistemima elektronskog bankarstva, bazama podataka i aplikacijama. Navedene mere služe i za minimiziranje eksternih pretnji za sisteme elektronskog bankarstva. Navedene sigurnosne mere štite od neautoriziranog pristupa eksternih strana kao što su posetioци (na primer na web-u), spoljni saradnici ili tehnička lica. To znači da je potrebno primenjivati postupke preispitivanja sigurnosti za zaposlene, korisnike usluga, kao i pružaoce eksternih usluga.

Za menadžment je od osnovnog značaja da uspostavi komunikaciju sa zaposlenima u banci koji su zaduženi za funkcionisanje elektronskog bankarstva (koordinaciju interne komunikacije). Takođe, neophodna je komunikacija menadžmenta sa IT sektorom u pogled funkcionisanja dizajniranog sistema i informisanja o eventualnim slabostima, sa predlogom mera za njihovo otklanjanje. Za implementaciju i funkcionisanje elektronskog bankarstva potreban je visok nivo edukacije zaposlenih i korisnika usluga banke, što za rezultat ima direktno smanjenje operativnog i reputacionog rizika.

Operativni i reputacioni rizik se može smanjiti i vrednovanjem proizvoda i usluga banke pre nego što se ponude na tržištu. Ovo uključuje: testiranje validnosti opreme u skladu sa željenim rezultatima, izrada pilot programa i prototip projekata novih aplikacija i njihovo testiranje, kao i testiranje dizajniranog sistema elektronskog bankarstva. Nakon izvršenog testiranja i analize rezultata, vrše se eventualne korekcije dizajniranog sistema u cilju poboljšanja.

Da bi osigurale nesmetano funkcionisanje elektronskog bankarstva, banke angažuju spoljne davaoce (informacionih) usluga (engl. *outsourcing*). To u uslovima elektronskog bankarstva označava angažovanje spoljnih isporučioца sigurnosnih paketa, odnosno, provajdera.

Tehnologija elektronskog bankarstva zahteva planiranje nepredvidivih okolosti koje mogu dovesti do rizika u funkcionisanju, bilo da su nastali u internim procesima ili eksternim (od strane davaoca usluga). Ovo planiranje treba da obuhvati: mogućnost obnove podataka, organizovanje *back-up* sistema (rezervni sistem), podršku servisima prema korisnicima usluga. Tehnologija elektronskog bankarstva oslanja se na eksterne entitete, kao što su: isporučioци harvera, softvera, telekomunikacione kompanije i Internet provajdere. Neophodno je da i oni imaju organizovane *back-up-ove* sistema.

2.3. Monitoring rizika

Monitoring rizika je važan aspekt bilo kog procesa upravljanja rizikom. Banka može na nekoliko načina upravljati rizikom, a jedan od osnovnih „alata“ jeste ALM (engl. *Asset and Liability Management*) koncept ili upravljanje aktivom i pasivom poslovne banke. Proces ALM-a podrazumeva da se u okviru banke identifikuju i analiziraju svi rizici, definišu odgovarajući limiti rizika (koji su u saglasnosti sa strategijom alokacije kapitala), kao i da se kontrolisano prate limiti rizika preko savremenih informacionih sistema.¹⁷⁰ Primena ALM

¹⁷⁰ Vunjak N.: „Finansijski menadžment“, cit.delo, str. 340

koncepta zahteva od „top“ menadžmenta da stalno modifikuje i popravlja sisteme upravljanja rizikom.

Pored ALM koncepta postoje i brojni „interni“ modeli kontrole i monitoringa poslovnih rizika. Jedan od najpoznatijih jeste metod *Chase Manhattan Bank*, gde ova banka koristi četiri metode monitoringa kreditnim rizikom:¹⁷¹

- a) banka sprovodi monitoring svake kreditne transakcije iz više uglova (strukture zajma, standardizovanosti zajma i dr.), te na osnovu ovoga banka može da donese odluku da li određeni zajam želi da zadrži u svom portfelju ili će ga prodati na sekundarnom tržištu,
- b) kreditni rizik kontroliše se i preko kreditne koncentracije. Ovde možemo meriti koncentraciju u velikim kreditima, na primer, prvih deset velikih kompanija korisnika kredita ne sme da učestvuje više od 15% u ukupnim kreditima poslovne banke ili koncentraciju rizika u određenoj grani, na primer, 25% je dozvoljena maksimalna koncentracija rizika u trgovini ili teškoj metalurgiji. Na ove načine banke se mogu efikasno zaštititi od mnogih kriza koje mogu pogoditi različita tržišta, a diversifikacijom svojih plasmana rizik nastanka negativnog slučaja se minimizira,
- c) kreditni rizik kontroliše se i putem stres testova,
- d) banka vrši monitoring svih korisnika kredita u određenom vremenskom periodu (u proseku jednom godišnje ili jednom polugodišnje). Na ovaj način banka može na vreme da primeti određene pozitivne ili negativne trendove u kretanju kompanije i da se putem sekundarnog tržišta „oslobodi“ neželjenog dela ili celog kreditnog aranžmana. U banci postoji nezavisna grupa koja upravlja rizicima. Ova grupa testira modele i upravljačke informacione sisteme, proučava teorije na kojima se baziraju modeli i daje nezavistan pogled na poslovne aktivnosti banke.

Za poslove elektronskog bankarstva i elektronskog novca posebno je istaknuta važnost aktivnosti monitoringa, s obzirom na to da se pod uticajem raznih inovacija poslovi brzo menjaju i što se određeni proizvodi pružaju putem korišćenja otvorene mreže. Upravljanje rizikom zahteva permanentan monitoring, koji se ostvaruje putem: testiranja sistema i revizije.

Testiranje sistema (testiranje operacija sistema) se vrši u cilju otkrivanja mogućih grešaka prilikom projektovanja i implementacije projekta elektronskog bankarstva, kako bi se izvršile korekcije pre puštanja sistema u rad. Posebna pažnja se posvećuje sistemima zaštite sistema. Testiranje operacija sistema može da pruži pomoć u otkrivanju oblika neuobičajenih aktivnosti i da se na osnovu toga spreče veći problemi, kao na primer, napadi na sistem. Provera prodora se izvršava sa ciljem identifikacije, izdvajanja i potvrde grešaka u projektovanju i sprovođenju mehanizama sigurnosti kontrolisanim pokušajima da se prodre u sistem izvan normalnih postupaka. Sa druge strane, nasuprot proveri prodora, nadzor se vrši sa ciljem praćenja rutinskih operacija, ispitivanja anomalija i provere efikasnosti sigurnosti sistema.

Revizija, koja može biti interna i eksterna, obezbeđuje mehanizam kontrole radi otkrivanja nedostataka i sprovođenja rizika na najmanju meru kod obezbeđivanja usluga elektronskog bankarstva i elektronskog novca. Revizija se organizuje u cilju otkrivanja propusta i minimiziranja rizika prilikom obezbeđivanja usluga elektronskog bankarstva. Revizor osigurava da se razvijaju odgovarajući standardi, politika i postupci i da ih se zaposleni u

¹⁷¹ Ćirović M.: „Bankarstvo“, cit.delo, str. 359

banci dosledno pridržavaju. U cilju objektivnog sagladavanja postojeće situacije, potrebno je da interni revizor bude nezavisan od zaposlenih u banci koji donose odluke o upravljanju rizikom. To znači da je neophodno da organizacijski budu odvojene organizacione jedinice u banci koje donose odluke o upravljanju rizikom i one koje vrše kontrolu preuzetih rizika. I pored postojanja interne revizije, rukovodstvo banke može i mora da traži pomoć kvalifikovanih eksternih revizora pri monitoringu rizika, uz obavezu da svi finansijski izveštaji, budu eksterno potvrđeni od strane ovlašćenih revizorskih kuća najmanje jednom godišnje (zahtev Narodne banke Srbije).

Primer monitoringa rizika u poslovanju banaka, s fokusom na elektronske kanale distribucije proizvoda, bila bi reakcija banke u slučaju „pada“ servera koji omogućuje nesmetanu realizaciju elektronskih naloga. Šta se dešava u ovom slučaju i na koji način banke reaguju, tema je koja treba da okupira ne samo internu reviziju nego i druge delove poslovne banke. Potrebno je da banka ima utvrđene mere koje je potrebno sprovesti u slučaju na primer „pada“ sistema. U tom slučaju, kada je izgrađen sistem preventivnih mera, dolazi do bržeg otklanjanja uzroka koji su doveli do grešaka. Ipak, ukoliko se ona desi, nastupa delovanje korektivnih faktora, na primer, postoji mogućnost uključivanja rezervnog servera što omogućuje nastavak nesmetane komunikacije sa klijentima.

3. PRINCIPI UPRAVLJANJA RIZIKOM ZA ELEKTRONSKO BANKARSTVO – BAZELSKI KOMITET

Bankarske institucije već godinama pružaju elektronske usluge na daljinu klijentima i privredi. Elektronski transfer sredstava, uključujući mala plaćanja i sisteme upravljanja novcem za privredu, kao i javno pristupačne automatske mašine za podizanje gotovine i upravljanje računima građana, predstavljaju globalni pribor. Međutim, povećano prihvatanje Interneta u svetu, kao kanala isporuke za bankarske proizvode i usluge, pruža nove poslovne mogućnosti za banke kao i usluđne pogodnosti za njihove klijente.

Stalne tehnološke inovacije i konkurencija između postojećih bankarskih organizacija i novih učesnika na tržištu omogućile su mnogo širi spektar elektronskih bankarskih proizvoda i usluga za građane i privredu kao klijente banaka. Ove usluge obuhvataju tradicionalne aktivnosti kao što su pristup finansijskim informacijama, dobijanje kredita i otvaranje depozitnih računa, kao i relativno nove proizvode i usluge, kao što su usluge elektronskog plaćanja računa, personalizovani finansijski „portali“, agregiranje računa¹⁷² i *bussiness-to-business* tržišta i berze.

Nezavisno od značajnih koristi tehnoloških inovacija, brzi razvitak e-bankinga nosi rizike kao i koristi i važno je da bankarske organizacije identifikuju i upravljaju ovim rizicima na prudenčijalan način. Ovaj razlog naveo je Bazelski komitet za bankarsku kontrolu da 1998. godine¹⁷³ sprovede preliminarno istaživanje implikacija upravljanja rizikom na e-banking i e-novac. Ova rana studija pokazala je jasno potrebu za još mnogo rada u oblasti upravljanja

¹⁷² Usluge agregiranja računa omogućavaju klijentima da dobiju konsolidovanu informaciju o njihovim finansijskim i nefinansijskim računima na jednom mestu. Agregator u suštini nastupa kao agent za klijenta da bi pružio objedinjenu informaciju o računima klijenta kod nekoliko finansijskih institucija. Klijenti daju agregatoru potrebnu sigurnosnu šifru ili lični identifikacioni broj da bi pristupio i konsolidovao informacije o računima prvenstveno preko ekrana, procesa koji obuhvata prikupljanje podataka sa veb-sajtova drugih institucija, često bez njihovog znanja, ili kroz ugovorom aranžiran direktan tok podataka između finansijskih institucija.

¹⁷³ „Risk Management for Eletronic Banking and Eletronic Money Activities“, mart 1998. godine, dostupno na Bank for Intrenational Settlements, <http://www.bis.org>

rizikom e-bankinga i ta misija je poverena radnoj grupi sastavljenoj od kontrolora banaka i centralnih banaka, *Electronic Banking Group* (EBG), koja je formirana u novembru 1999. godine.

Bazelski komitet je objavio EBG Izveštaj o upravljanju rizikom i pitanjima kontrole koja nastaju iz razvoja e-bankinga u oktobru 2000. godine.¹⁷⁴ Ovaj Izveštaj opisuje i bavi se glavnim rizicima koji su povezani sa e-bankingom: strateški, reputacioni, operativni (uključujući rizik sigurnosti i pravni rizik)¹⁷⁵, kreditni, tržišni i likvidnosni rizik. EBG je zaključila da aktivnosti e-bankinga ne stvaraju rizike koji nisu već bili identifikovani u prethodnom radu Bazelskog komiteta. Međutim, zapazila je da e-banking povećava i modifikuje neke od ovih tradicionalnih rizika, čime utiče na ukupan profil rizika bankarstva. Naročito je izvesno da su strateški, operativni i reputacioni rizici povećani brzim uvođenjem i osnovnom tehnološkom složenosti aktivnosti e-bankinga.

3.1. Izazovi upravljanja rizikom

EBG je zabeležila da osnovne karakteristike e-bankinga (kao i e-trgovine uopšteno) nose jedan broj izazova za upravljanje rizikom:

- Brzina promena u vezi sa tehnološkim inovacijama u uslugama klijentima u e-bankingu je bez presedana. Istorijski, nove bankarske aplikacije bile su primenjivane u relativno dugim periodima i samo posle temeljnih provera. Danas, međutim, banke trpe konkurentske pritiske da spremne nove poslovne aplikacije u vrlo kratkim vremenskim okvirima - često samo nekoliko meseci od koncepta do produkcije. Ova konkurencija intenzivira izazove za menadžment da obezbedi da se adekvatne strateške procene, analize rizika i istraživanja sigurnosti sprovedu pre primena novih aplikacija e-bankinga.
- Transnacionalni e-banking veb-sajtovi i povezane aplikacije u poslovima sa građanima i sa privredom obično su integrisani što je moguće više u postojeće računarske sisteme da bi se postiglo neposredno procesuiranje elektronskih transakcija. Takvi neposredni automatizovani procesi smanjuju prostor za ljudske greške i prevare koje se javljaju kod manuelnih procesa, ali takođe povećavaju zavisnost od zdravog projektovanja i arhitekture sistema.
- E-banking povećava zavisnost banaka od informatičke tehnologije, povećavajući tehničku složenost mnogih operativnih i sigurnosnih pitanja i nastavljajući trend prema većem broju aranzmana partnerstva, alijansi i outsorcinga sa trećim stranama, od koje mnoge nisu podvrgnute regulativi. Ovaj razvoj vodi stvaranju novih poslovnih modela koji uključuje banke i nebankarske subjekte, kao što su provajderi Internet usluga, telekomunikacione kompanije i druge tehnološke firme.
- Internet je svuda prisutan i globalan po prirodi. To je otvorena mreža kojoj mogu svuda u svetu pristupiti od nepoznate strane, rutiranjem poruka kroz nepoznate lokacije i putem bežičnih uređaja koji se brzo razvijaju. Otuda, Internet u velikoj meri povećava značaj kontrole sigurnosti, tehnika autentifikovanja klijenata, zaštite podataka, procedura vođenja dnevnika i standarda privatnosti klijenata.

¹⁷⁴ „Electronic Banking Group Initiatives and White Papers“, oktobar 2000. godine, <http://www.bis.org>

¹⁷⁵ Ovaj Izveštaj koristi definiciju Bazelskog Komiteta za operativni rizik – „rizik od gubitka koji nastaje od neadekvatnih ili neuspešnih internih procesa, ljudi i sistema ili od eksternih događaja“

3.2. Principi upravljanja rizikom

Bazelski komitet za bankarsku kontrolu naložio je *Electronic Banking Group* (EBG), da identifikuje ključne principe upravljanja rizicima koji bi pomogli bankarskim institucijama da prošire svoju postojeću politiku nadzora rizika i procese, tako da pokriju aktivnosti e-bankinga i takođe, da unapređuju sigurnu i zdravu elektronsku isporuku bankarskih proizvoda i usluga.

Identifikovano je četrnaest principa upravljanja rizikom za elektronsko bankarstvo, koji se dele u tri široke i često preklapajuće kategorije pitanja, koje su radi jasnoće grupisane na sledeći način:

1. Nadzor borda i menadžmenta;
2. Kontrola sigurnosti i
3. Upravljanje pravnim i reputacionim rizicima.¹⁷⁶

Principi upravljanja rizikom za elektronsko bankarstvo koji su identifikovani, nisu dati kao apsolutni zahtevi niti čak kao „najbolja praksa“, već kao smernice za unapređenje sigurnih i zdravih aktivnosti e-bankinga. Klijent veruje da postavljenje detaljnih zahteva za upravljanjem rizicima u oblasti e-bankinga može da bude kontraproduktivno, makar i zbog toga što bi oni verovarno ubrzano postali zastareli zbog brzine promena u tehnološkim inovacijama i inovacijama proizvoda. Otuda ovi principi izražavaju očekivanja kontrolora u vezi sa opštim ciljem bankarske kontrole, da obezbedi sigurnost i zdravlje finansijskog sistema, a ne stroj i regulativu.

Klijent smatra da ta očekivanja kontrolora treba da budu krojena i adaptirana prema distribucionim kanalima e-bankinga, ali tako da ne budu suštinski različita od očekivanja prema bankarskim aktivnostima koja idu drugim distribucionim kanalima. Otuda, principi koji se dalje izlažu uglavnom su izvedeni i adaptirani iz principa kontrole koje su već ranije izrazili klijent ili nacionalni kontrolori tokom proteklih godina. U nekim oblastima, kao što su upravljanje odnosima autorsinga, kontrola sigurnosti i upravljanje pravnim i reputacionim rizicima, karakteristike i implikacije distribucionih kanala Interneta stvaraju potrebe za detaljnim principima od onih koji su do sada postojali.

Klijent uvažava činjenicu da će banke morati da razvijaju procese upravljanja rizicima koji odgovaraju njihovom pojedinačnom profilu rizika, operativnoj strukturi i kulturi korporacionog upravljanja i koji su u skladu sa specifičnim zahtevima upravljanja rizicima i politici koju su postavili bankarski kontrolori u svojoj konkretnoj jurisdikciji.

Klijent ne pokušava da diktira konkretna tehnološka rešenja za tretman određenih rizika ili da postavlja tehničke standarde u vezi sa e-bankingom. Tehničkim pitanjima moraće neprestano da se bave bankarske institucije i različita tela za standarde onako kako se tehnologija razvija. Ova rešenja će se verovatno odnositi i na pitanja u vezi sa činjenicom da se banke razlikuju po veličini, složenosti i kulturi upravljanja rizicima i da se jurisdikcije razlikuju po svojim zakonskim i regulatornim okvirima.

¹⁷⁶ Vuković D.: „*Principi upravljanja rizikom za elektronsko bankarstvo*“, prevod, Jugoslovenski pregled, Beograd, 2007., str.101

Iz ovih razloga, klijent ne veruje da pristup „jedna veličina pristaje svima“ odgovara upravljanju rizicima u e-bankingu i zato podržava razmenu dobre prakse i standarda radi bavljenja dodatnim dimenzijama rizika koje donose kanali isporuke e-bankinga. Očekuje se da principe upravljanja rizicima nacionalni kontrolori koriste kao alate i da ih primenjuju uz adaptacije koje će da odraze specifične nacionalne zahteve gde je to potrebno, da bi pomogli unapređenje sigurne i bezbedne aktivnosti i operacije e-bankinga.¹⁷⁷

Klijent uvažava da je profil rizika svake banke različit i da zahteva pristup ublažavanju rizika koji odgovara veličini operacija e-bankinga, stvarnim rizicima koji su prisutni i spremnosti i sposobnosti institucije da upravlja tim rizicima. Ove razlike impliciraju da principi upravljanja rizicima, imaju za cilj da budu dovoljno fleksibilni da bi bili primenjeni kod svih relevantnih institucija u raznim jurisdikcijama. Nacionalni kontrolori će proceniti realnost rizika koji se odnose na aktivnosti e-bankinga prisutnih u datoj banci i da li u kom stepenu su principi upravljanja rizikom za e-banking adekvatno ispunjeni kroz bančin okvir za upravljanje rizicima.

3.2.1. Nadzor borda i menadžmenta

Nadzor borda i menadžmenta obuhvata principe (1 do 3):

1. Efektivni nadzor menadžmenta nad aktivnostima e-bankinga.
2. Postojanje obuhvatnog procesa kontrole sigurnosti.
3. Obuhvatan „due diligence“ i proces upravljanja menadžmenta odnosima outsorsinga i drugih zavisnosti od trećih strana.

Bord direktora i viši menadžment odgovorni su za razvoj poslovne strategije bankarske institucije. Eksplicitna strateška odluka u pogledu toga da li bord želi da banka pruža transakcionalne usluge e-bankinga treba da se donese pre početka ponude takvih usluga. Konkretno, bord treba da obezbedi da planovi e-bankinga budu jasno integrisani u korporacione strateške ciljeve, da je sprovedena analiza rizika predloženih aktivnosti e-bankinga, da su postavljeni odgovarajući ublaživači rizika i procesi monitoringa za ublažavanje rizika, kao i da se stalno sprovode pregledi za procenjivanje rezultata aktivnosti e-bankinga u odnosu na biznis planove i ciljeve institucije.

Pored toga, bord i viši menadžment bi trebalo da obezbede da se dimenzije operativnog i bezbednosnog rizika poslovnih strategija institucije u e-bankingu razmatraju i tretiraju na odgovarajući način. Obezbeđenje finansijskih usluga preko Interneta može znatno da modifikuje ili čak poveća tradicionalne bankarske rizike (npr. strateški, reputacioni, operativni, kreditni i likvidnosni rizik). Zato treba preduzeti korake da se obezbedi da bančini postojeći procesi upravljanja rizikom, kontrole sigurnosti, „due diligence“ i procesi nadzora odnosa outsorsinga budu procenjeni i modifikovani na odgovarajući način da bi obuhvatili i usluge e-bankinga.

Princip 1 : Bord direktora i viši menadžment treba da postave efektivni upravljački nadzor nad rizicima povezanim sa aktivnostima e-bankinga uključujući postavljanje konkretne odgovornosti, politike i kontrole upravljanja ovima rizicima.

¹⁷⁷ Isto, str.113

Budni upravljački nadzor od bitnog je značaja za obezbeđenje efektivne interne kontrole nad aktivnostima e-bankinga. Pored specifičnih karakteristika kanala distribucije Interneta, sledeći aspekti e-bankinga mogu da predstavljaju znatne izazove za tradicionalne procese upravljanja rizicima:

- Glavni elementi kanala isporuke (Internet i povezane tehnologije) izvan su neposredne bankarske kontrole.
- Internet olakšava isporuke usluga kroz višestruke nacionalne jurisdikcije, uključujući one usluge koje sada institucija ne pruža kroz fizičke lokacije.
- Složenost pitanja koja su povezana sa e-bankingom, a koja uključuju visoko tehnički jezik i koncepte u mnogim slučajevima su izvan tradicionalnog iskustva borda i višeg menadžmenta.

U svetlu jedinstvenih karakteristika e-bankinga, nove projekte e-bankinga koji mogu da imaju značajni uticaj na profil rizika banke i na strategiju treba da reviduju bord direktora i viši menadžment i treba da prođu odgovarajuće strateške i troškovno/prihodne analize. Bez adekvatne inicijalne strateške revizije i stalnog ocenjivanja preformansi prema planu, banke su izložene riziku da potcenjuju troškove, ili precenjuju isplativost svojih inicijativa u pogledu e-bankinga.

Pored toga, bord i viši menadžment treba da obezbede da banka ne ulazi u nove poslove e-bankinga ili usvajanje novih tehnologija ukoliko nema potrebnu ekspertizu da obezbedi stručni upravljački nadzor. Ekspertiza menadžmenta i zaposlenih treba da bude u skladu sa tehničkom prirodom i složenošću bančinih aplikacija za e-banking i osnovne tehnologije. Adekvatna ekspertiza je bitna, nezavisno od toga da li se bančnim sistemima e-bankinga i uslugama upravlja u kući ili se one daju u outsorsing trećim stranama. Procesi nadzora višeg menadžmenta treba da funkcionišu dinamično da bi efektivno intervenisali i ispravljali bilo koje materijalne probleme sistema e-bankinga ili kršenja sigurnosti koja mogu da se pojave. Povećani reputacioni rizik povezan sa e-bankingom zahteva budno praćenje operativnosti sistema i zadovoljstvo klijenta kao i odgovarajuće izveštavanje o incidentima bordu i višem menadžmentu.

Najzad, bord i viši menadžment treba da obezbede da procesi upravljanja rizicima u aktivnostima e-bankinga budu integrisani u bančin ukupan pristup upravljanju rizicima. Bančina postojeća politika upravljanja rizicima i procesi treba da budu procenjeni da bi se obezbedilo da budu dovoljno robustni da pokriju nove rizike koje donose tekuće ili planirane aktivnosti e-bankinga. Dodatni koraci nadzora upravljanja rizicima koje treba da razmotre bord i viši menadžment obuhvataju:¹⁷⁸

- Jasno ustanovljenje apetita za rizikom bankarske organizacije u vezi sa e-bankingom.
- Ustanovljenje ključnih delegacija i mehanizama izveštavanja, uključujući potrebnu proceduru eskalacije za incidente koje utiču na bančinu sigurnost, zdravlje ili reputaciju (npr. prodor u mrežu, kršenje sigurnosti od strane zaposlenih i bilo koja ozbiljna zloupotreba računara).¹⁷⁹

¹⁷⁸ Isto, str. 121

¹⁷⁹ Pored zahteva za internim izveštavanjem, procedure eskalacije izveštaja o incidentima treba takođe da postave potrebno izveštavanje odgovarajućim kontrolnim vlastima.

- Tretman bilo kojih jedinstvenih faktora rizika povezanih sa obezbećenjem sigurnosti, integriteta i raspoloživosti proizvoda i usluga e-bankinga i zahtev da treće strane, kojima su banke dale u autsorsing ključne sisteme ili aplikacije, preduzimaju slične mere.
- Obezbećenje da se odgovarajuća „*due diligence*“ i analiza rizika sprovede pre nego što banka preduzme prekogranične aktivnosti e-bankinga.

Internet uveliko unapređuje bančinu sposobnost da distribuira proizvode i usluge širom virtuelno neograničenog geografskog područja, uključujući prelazak nacionalnih granica. Takva prekogranična aktivnost e-bankinga, naročito ako se sprovodi bez bilo kakvog postojećeg licenciranog fizičkog pristupa u „zemlji domaćinu“, potencijalno izlaže banke povećanom pravnom i regulatornom riziku, kao i riziku zemlje, zbog značajnih razlika koje mogu da postoje između jurisdikcija u pogledu davanja ovlašćenja bankama, kontrole i zahteva za zaštitom klijenata. Zbog potrebe da se izbegne nenamerno nepridržavanje zakona ili propisa strane zemlje, kao i da se upravlja relevantnim faktorima rizika zemlje, banke koje razmatraju da otpočnu prekogranične aktivnosti e-bankinga moraju da u potpunosti istraže ove rizike pre nego što preduzmu takve operacije i efikasno upravljenju njima.¹⁸⁰

Sadržaj i složenost programa za upravljanje rizikom razlikovaće se među bankarskim organizacijama zavisno od sadržaja i složenosti aktivnosti e-bankinga. Resursi koji su potrebni za kontrolu usluga e-bankinga treba da budu primereni transakcionoj funkcionalnosti i kritičnosti sistema, ranjivosti mreža i osetljivosti informacija koje se transmituju.

Princip 2: Bord direktora i viši menadžment moraju da reviduju i odobravaju ključne aspekte bančinog procesa kontrole sigurnosti.

Bord direktora i viši menadžment moraju da kontrolišu razvoj i kontinuirano održavanje infrastrukture kontrole sigurnosti koja na odgovarajući način štiti sisteme e-bankinga i podatke od internih i eksternih pretnji. Ovo treba da obuhvati uspostavljanje odgovarajućih privilegovanih ovlašćenja, logičke kontrole i kontrole fizičkog pristupa, kao i adekvatne infrastrukture sigurnosti za održavanje odgovarajućih ograničenja i restrikcija aktivnosti internih i eksternih korisnika.

Očuvanje bančine aktive je jedna od poverenih dužnosti borda i jedna od osnovnih odgovornosti višeg menadžmenta. Međutim, to je težak zadatak u ubrzano promenljivoj okruženju e-bankinga zbog složenih bezbednosnih rizika povezanih sa poslovanjem preko javne Internet mreže korišćenjem inovativne tehnologije.

Da bi se obezbedila odgovarajuća kontrola aktivnosti e-bankinga, bord i viši menadžment moraju da potvrde da li banka ima obuhvatni proces sigurnosti, uključujući politiku i procedure, koje su usmerene na potencijalne interne i eksterne sigurnosne pretnje u pogledu prevencije incidenata i reagovanja. Ključni elementi efikasnog procesa sigurnosti e-bankinga obuhvataju:¹⁸¹

¹⁸⁰ Za dalji razvoj, videti Basel Committee on Banking Supervision, Management and Supervision of Cross-border Electronic Banking Activities, jul 2003

¹⁸¹ Vuković D.: „Principi upravljanja rizikom za elektronsko bankarstvo“, cit.delo, str.125

- Raspodelu eksplicitne odgovornosti menadžmenta/zaposlenih za kontrolu uspostavljanja i održavanja korporacijske politike obezbeđenja.¹⁸²
- Dovoljne fizičke kontrole da se predupredi neovlašćeni fizički pristup računarskom okruženju.
- Dovoljne logičke kontrole i procese monitoringa¹⁸³ da se predupredi neovlašćeni interni¹⁸⁴ i eksterni pristup aplikacijama i bazama podataka e-bankinga.
- Redovnu reviziju i testiranje mere sigurnosti i kontrole, uključujući stalno praćenje razvoja savremenih kretanja i sigurnosti bankarske industrije i instaliranje odgovarajućih poboljšanja softvera, paketa usluga i druge potrebne mere.¹⁸⁵

Princip 3: Bord direktora i viši menadžment moraju da ustanove obuhvatni i neprestani „due diligence“ i proces kontrole za upravljanje bančnim odnosima po osnovu outsorsinga i drugih zavisnosti od treće strane koja podržava e-banking.

Povećano oslanjanje na partnere i provajdere usluga za obavljanje kritičnih funkcija e-bankinga smanjuje neposrednu kontrolu bančinog menadžmenta. Zato je neophodan obuhvatan proces za upravljanje rizicima povezanim sa outsorsingom i drugim zavisnostima od treće strane. Ovaj proces treba da obuhvati aktivnosti trećih strana partnera i provajdera usluga, uključujući podugovaranje aktivnosti datih u outsorsing koje mogu da imaju materijalne posledice po banku.

Istorijski, outsorsing je često bio limitiran na jednog provajdera usluga za datu funkciju. Međutim, u poslednje vreme odnosi banka po osnovu outsorsinga povećali su obim i složenost kao direktnu posledicu napretka u informatičkoj tehnologiji i pojave e-bankinga. Složenost dalje pojačava činjenica da usluge e-bankinga date u outsorsing mogu podugovorom da se prenesu drugim provajderima usluga, ili da se izvode u stranoj zemlji. Dalje, pošto su aplikacije i usluge e-bankinga postale tehnološki naprednije i dobile u strateškom značaju, izvesne funkcionalne oblasti e-bankinga zavise od malog broja specijalizovanih vendora i provajdera usluga. Ovaj razvoj može da vodi do povećane koncentracije rizika koja zasluži pažnju pojedinih banaka kao i sistemski stav bankarske industrije.

Uzeti zajedno, ovi faktori podcrtavaju potrebu za obuhvatnim i neprestanim procenjivanjem odnosa u outsorsingu i drugim eksternim zavisnostima, uključujući povezane implikacije za bančin profil rizika i sposobnosti kontrole u okviru upravljanja rizikom.¹⁸⁶ Kontrolu borda i višeg menadžmenta nad odnosom outsorsinga i zavisnostima od treće strane treba naročito usmeriti na to da obezbedi da:¹⁸⁷

¹⁸² Ova odgovornost normalno ne treba da bude deo funkcije revizije, koja ima odgovornost za to da se kontrola bezbednosti efikasno sprovodi.

¹⁸³ Uključujući kontrolisana prava pristupa i privilegija kao i stalni monitoring pokušaja upada u mrežu.

¹⁸⁴ Uključujući zaposlene, ugovarače i one koji imaju pravo pristupa na osnovu odnosa outsorsinga.

¹⁸⁵ Uključujući mere za monitoring funkcionisanja mreže, pokušaja neovlašćenog ulaganja i izveštavanje o kršenju bezbednosti.

¹⁸⁶ Takvo procenjivanje treba da uzme u obzir stepen kontrole koja se sprovodi nad trećom stranom. Veliki akcionar u zajedničkom ulaganju može, u mnogim slučajevima, da sprovodi više kontrole nego u slučaju ugovornog odnosa sa provajderom usluga. Međutim, ne treba kod takvog razlikovanja izvesti zaključak da će akcionarska kontrola kod zajedničkog ulaganja ili partnerstva biti nužno i dovoljna, naročito ako tehnologiju i usluge potrebne za zajedničko poslovanje pruža manjinski akcionar. Takve razlike se uglavnom koriste da se potvrdi da procenjivanje treba raditi od slučaja do slučaja.

¹⁸⁷ Vuković D.: „Principi upravljanja rizikom za elektronsko bankarstvo“, cit.delo, str.127

- banka u potpunosti razume rizike povezane sa ulaskom u outsorsing ili partnerski aranžman za svoje sisteme e-bankinga ili aplikacije.
- pre ulaska u svaki ugovor za usluge e-bankinga bude sprovedena odgovarajuća „due diligence“ revizija kompetentnosti i finansijskog boniteta treće strane provajdera usluga ili partnera.
- ugovorna odgovornost svih strana u outsorsingu¹⁸⁸ ili partnerskom odnosu bude jasno definisana. Na primer, mora da bude jasno definisana odgovornost za pružanje informacija provajderu i primanje informacija od provajdera.
- svi sistemi e-bankinga i operacija dati u outsorsing budu podvrgnuti upravljanju rizikom, politici bezbednosti i privatnosti koja ispunjava bančine sopstvene standarde.
- periodične nezavisne interne, ili eksterne revizije operacija datih u outsorsingu imaju najmanje isti obim koji bi se zahtevao da se te operacije sprovedu unutar kuće.
- moraju da postoje odgovarajući rezervni planovi za autorisane aktivnosti e-bankinga.

Zbog toga što su bord direktora i viši menadžment odgovorni za razvoj poslovne strategije institucije i ostvarivanje efikasnog upravljačkog nadzora nad rizicima, od njih se očekuje da donesu eksplicitnu, informisanu i dokumentovanu stratešku odluku u pogledu toga kako će banka da pruža usluge e-bankinga. Inicijalna odluka treba da obuhvati specifičnu odgovornost, politiku i kontrolu za bavljenje rizicima, uključujući rizike koji nastaju u prekograničnom kontekstu. Efektivan upravljački nadzor treba da obuhvati revidovanje i odobrenje ključnih aspekata bančinog procesa kontrole sigurnosti, kao što su razvoj i održavanje infrastrukture kontrole sigurnosti koja valjano štiti sisteme e-bankinga i podatke za upravljanje rizicima povezanim sa povećanom složenošću i povećanim oslanjanjem na odnose outsorsinga i zavisnošću od treće strane u obavljanju kritičnih funkcija e-bankinga.

3.2.2. Kontrola sigurnosti

Kontrola sigurnosti obuhvata principe (4 do 10):

4. Autentifikacija klijenata e-bankinga.
5. Neporicanje i odgovornost za transakcije e-bankinga.
6. Odgovarajuće mere da se obezbedi razdvajanje dužnosti.
7. Valjanje kontrole autorizacije u sistemima e-bankinga, bazama podataka i aplikacijama.
8. Integritet podataka iz transakcija e-bankinga, arhiva i informacija.
9. Ustanovljenje jasnih dnevnika za transakcije e-bankinga.
10. Poverljivost ključnih bankarskih informacija.

Princip 4: Banke treba da preduzimaju odgovarajuće mere da bi autentifikovale¹⁸⁹ identitet i ovlašćenje klijenata sa kojima se vodi poslovanje preko Interneta.

¹⁸⁸ Ovo takođe uključuje podugovarače.

¹⁸⁹ Autentifikacija u ovom Izveštaju odnosi se na tehnike, procedure i procese koji se koriste za verifikovanje identiteta i autorizacije potencijalnih i postojećih klijenata. Identifikacija se odnosi na procedure, tehnike i procese koji se koriste da se ustanovi identitet klijenta kada otvara račun. Autorizacija se odnosi na procedure, tehnike i procese koji se koriste za utvrđivanje da klijent ili zaposleni imaju legitiman pristup računu u banci ili ovlašćenje da sprovedu povezanu transakciju na tom računu.

Od suštinskog je značaja u bankarstvu da se potvrdi legitimnost određene komunikacije, transakcije ili zahteva za pristupom. Zato, banke treba da koriste pouzdane metode za proveru identiteta i ovlašćenja novih klijenata kao i autentifikovanje identiteta i ovlašćenja postojećih klijenata koji traže da otpočnu sa elektronskim transakcijama.

Verifikacija klijenata tokom otvaranja računa značajna je za umanje rizika krađe identiteta, prevarnih zahteva za otvaranje računa i pranja novca. Bančin propust da na adekvatan način autentifikuje klijente može da dovede do toga da neovlašćeni pojedinci ostvare pristup računima u e-bankingu i da na kraju ostane finansijski gubitak i reputaciona šteta za banku kroz prevaru, odavanje poverljivih informacija ili nenamerno uključenje u kriminalnu aktivnost.

Uslovljavanje i autentifikovanje identiteta pojedinaca i autorizacija da pristupi bankarskim sistemima u isključivo elektronskom okruženju otvorene mreže može da bude težak zadatak. Autorizacija legitimnog korisnika može da bude zloupotrebljena kroz tehnike koje se generalno znaju pod nazivom „spoofing“.¹⁹⁰ Onlajn hakeri mogu takođe da preuzmu komunikaciju legitimnog ovlašćenog pojedinca korišćenjem „sniffer“-a¹⁹¹ i da izvodi aktivnosti nestašne ili kriminalne prirode. Procesi kontrole autentifikacije mogu da se dalje zaobiđu putem zamene baza podataka za autentifikaciju.

Zato je od ključnog značaja da banke imaju formalnu politiku i procedure kojima identifikuju odgovarajuće metodologije da se na valjan način autentifikuje identitet i ovlašćenje određenog pojedinca, agenta ili sistema¹⁹² sredstvima koja su jedinstvena i u meri u kojoj je to praktično, isključuje neovlašćene pojedince ili sisteme.¹⁹³ Banke mogu da koriste razne metode za ustanovljenje autentifikacije, uključujući PIN, password, smart kartice, biomertiju i digitalne certifikate.¹⁹⁴ Ovi metodi mogu da budu sa jednim faktorom ili su višefaktorski. Multifaktorna autentifikacija generalno daje jaču sigurnost.

Banka mora da utvrdi koje će metode autentifikacije koristiti na osnovu toga kako menadžment procenjuje rizike koje donosi sistem e-bankinga kao celina ili njegove razne komponente. Ova analiza rizika treba da proceni transakcione sposobnosti¹⁹⁵ sistema e-bankinga (npr. transfer sredstava, plaćanje računa, otvaranje računa, spajanje računa itd.), osetljivost i vrednost pohranjenih podataka e-bankinga i lakoću korišćenja metoda autentifikovanja za klijenta.

Robusni procesi identifikacije i autentifikacije klijenata naročito su od značaja u kontekstu prekograničnog e-bankinga pri datim dodatnim poteškoćama koje mogu da nastanu iz poslovanja elektronskim putem preko nacionalnih granica, uključujući veći rizik od imitiranja identiteta i veće poteškoće u sprovođenju efikasnih provera potencijalnih klijenata.

¹⁹⁰ Spoofing je oponašanje legitimnog klijenta korišćenjem njegovog/njenog broja računa, passworda, ličnog identifikacionog broja (PIN) i/ili email adrese.

¹⁹¹ Sniffer je metod koji omogućava prisluškivanje telekomunikacionog saobraćaja, hvatanje passworda i podataka u tranzitu.

¹⁹² Sistemi uključuju sopstvene web sajtove institucije.

¹⁹³ Sistemi moraju da osiguraju da rade sa autentifikovanim pojedincem, agentom ili sistemom i sa važećom bazom podataka za autentifikaciju.

¹⁹⁴ Banka može da izda klijentu certifikate koristeći infrastrukturu javnih ključeva (public key infrastructure-PKI) da bi se obezbedilo komuniciranje sa bankom.

¹⁹⁵ Efikasne mere autentifikacije mogu takođe da umanje rizik odbijanja, u kome ovlašćeni korisnik kasnije poriče da je ovlastio jednu određenu transakciju.

Kako se metodi autentifikacije i dalje razvijaju, banke su podstaknute da prate i usvajaju zdravu praksu bankarske industrije u ovoj oblasti koja obezbeđuje da

- Baze podataka za autentifikaciju koje daju pristup računima klijenata e-bankinga ili osetljivi sistemi budu zaštićene od upada i kvara. Svaki pokušaj upada treba da bude utvrdiv i treba da postoje dnevnici da bi se dokumentovali ti pokušaji.
- Bilo koji dodatak, brisanje ili promena kod pojedinca, agenta ili sistema u bazi podataka za identifikaciju budu valjano autorizovani od strane izvora autentifikacije.¹⁹⁶
- Postoje odgovarajuće mere za kontrolu sistema e-bankinga tako da nepoznate treće strane ne mogu da zamene poznate klijente.
- Autentifikovane sesije e-bankinga ostaju sigurne tokom celokupnog trajanja sesije ili u slučaju greške u sigurnost treba da zahtevaju ponovno autentifikovanje.

Princip 5: Banke treba da koriste metode autentifikacije transakcija koje unapređuju neporicanje i ustanovljavaju odovornost za transakcije e-bankinga.

Neporicanje obuhvata stvaranje dokaza o nastajanju ili isporuci elektronske informacije da bi se zaštitio pošiljalac od lažnog poricanja primaoca da je podatak primljen ili da bi se zaštitio primalac od lažnog poricanja pošiljaoca da je podatak bio poslat. Rizik da transakcija bude poricana već je pitanje otvoreno kod konvencionalnih transakcija kao što su kreditne kartice ili transakcije sa hartijama od vrednosti. Međutim, e-banking povećava ovaj rizik zbog poteškoća kod pozitivne autentifikacije identiteta i ovlašćenja strana koje iniciraju transakcije, potencijalne mogućnosti da se promene ili preotmu elektronske transakcije i potencijala da korisnici e-bankinga tvrde da su transakcije bile prevarno promenjene.

Da bi rešavale ove povećane probleme banke moraju da ulože razumne napore, saglasne sadržini i vrsti transakcije e-bankinga, kako bi se obezbedilo da:¹⁹⁷

- Sistemi e-bankinga budu projektovani tako da umanje verovatnoću da ovlašćeni korisnici iniciraju nenameravane transakcije i da klijenti u potpunosti razumeju rizike povezane sa transakcijama koje iniciraju.
- Sve strane u transakciji budu pozitivno autentifikovane i da se održava kontrola nad autentifikovanim kanalom.
- Podaci o finansijskim transakcijama budu zaštićeni od izmena ili da svaka izmena bude utvrdiva.

Bankarke organizacije su počele da primenjuju različite tehnike koje omogućavaju da se ostvari neporicanje i obezbedi poverljivost i integritet transakcija e-bankinga, kao što su sertifikati koje koriste infrastrukturu javnih ključeva (PKI). Banka može da izda digitalni sertifikat klijentu ili partneru da bi omogućila njihovu jedinstvenu identifikaciju/autentifikaciju i umanjila rizik poricanja transakcije. Mada je u nekim zemljama pravo klijenta da negira transakcije predviđeno u posebnim zakonskim odredbama, u nekim nacionalnim jurisdikcijama je propisano da su digitalni potpisi po zakonu obavezujući. Sa daljim razvojem tehnologije verovatno će doći do šireg globalnog zakonskog prihvatanja ovih tehnika.

¹⁹⁶ U nekim slučajevima, izvor autentifikacije može da bude elektronski izvor.

¹⁹⁷ Vuković D.: „*Principi upravljanja rizikom za elektronsko bankarstvo*“, cit.delo, str.133

Princip 6: Banke treba da obezbede primenu odgovarajućih mera za unapređenje adekvatnog podvajanja dužnosti unutar sistema e-bankinga, baza podataka i aplikacija.

Podvajanje dužnosti je osnovna mera interne kontrole koja ima za cilj da umani rizik od prevara u operativnim procesima i sistemima i da obezbedi da transakcije i aktiva kompanije budu valjano autorizovane, zabeležene i čuvane. Podvajanje dužnosti je od ključnog značaja da se obezbede tačnost i integritet podataka i služi kao preventiva od preventivnih radnji pojedinca. Ako su dužnosti pravilno podvojene, prevara može biti izvršena samo kroz dosluh.

Usluge e-bankinga mogu zahtevati modifikovanje načina na koji se podvajanje dužnosti ustanovljava i održava zbog toga što se transakcije događaju preko elektronskih sistema na kojima se identitet može zgodnije maskirati ili lažirati. Pored toga, operativne funkcije i funkcije zasnovane na transakcijama u mnogim slučajevima su postale saštete i integrisane u aplikacije e-bankinga. Zato, kontrola koja se tradicionalno zahteva za održavanje podvojenosti dužnosti mora da se revidira i adaptira da bi obezbedila održavanje odgovarajućih nivoa kontrole. Zbog toga što pristup slabo obezbeđenim bazama podataka može lakše da se ostvari kroz internu ili eksternu mrežu, treba naglasiti striktnu proceduru autorizacije i identifikacije, sigurnu i zdravu arhitekturu *straight – through* procesa i vođenje adekvatnih dnevnika.

Uobičajena praksa koja se koristi za ustanovljenje i održavanje podele dužnosti unutar okruženja e-bankinga obuhvata sledeće:¹⁹⁸

- Transakcioni procesi i sistemi treba da budu tako projektovani da obezbede da ni jedan zaposleni/provajder usluge date u outsorsingu ne može da učestvuje i završi transakciju.
- Podvojenost treba da se održava između onih koji iniciraju statističke podatke (uključujući sadržaj veb sajta) i onih koji su odgovorni za proveru njenog integriteta.
- Sistemi e-bankinga treba da se testiraju da bi se obezbedilo da se ne zaobilazi podvojenost dužnosti.
- Treba da se održava podvojenost između onih koji razvijaju i onih koji administriraju sisteme e-bankinga.

Princip 7: Banke treba da obezbede valjanju kontrolu autorizacije i privilegija za pristup sistema e-bankinga, bazama podataka i aplikacijama.

Da bi se održala podvojenost dužnosti, banke moraju da striktno kontrolišu autorizaciju i privilegije pristupa. Propust da se obezbedi adekvatna kontrola autorizacije može da dopusti pojedincima da izmene svoje ovlašćenje, zaobiđu podvojenost i ostvare pristup sistemima e-bankinga, bazama podataka ili aplikacijama za koje nemaju tu privilegiju.

U sistemima e-bankinga, autorizacija i prava na pristup mogu da se ustanove na centralizovani ili decentralizovani način unutar banke i obično se čuvaju u bazama podataka. Zaštita tih baza podataka od upada ili kvara je zato od suštinskog značaja za efikasnu kontrolu autorizacije.

¹⁹⁸ Isto, str.137

Princip 8: Banke treba da obezbede primenu odgovarajućih mera zaštite integriteta podataka transakcija e-bankinga, arhive i informacija.

Integritet podataka se odnosi na obezbeđenje sa informacija koja je u tranzitu ili u bazi ne bude izmenjena bez autorizacije. Neuspeh održavanja integriteta podataka o transakcijama, arhive i informacijama može da izloži banku finansijskim gubicima kao i znatnom zakonskom i reputacionom riziku.

Priroda *straight-through* procesa za e-banking može da učini da greške u programiranju ili prevarne radnje budu teže uočljive u ranoj fazi. Zato je važno da banke primene *straight-through procesing* na način koji obezbeđuje sigurnost i integritet podataka.

Pošto se e-banking transaktuje preko javnih mreža, transakcije su izložene dodatnoj pretnji oštećenja, prevare i krađe podataka. Zato, banke treba da obezbede odgovarajuće mere koje osiguravaju tačnost, potpunost i pouzdanost transakcija e-bankinga, arhive i informacija koje se prenose preko Interneta, čuvaju u internim bančnim bazama podataka ili prenose/čuvaju kod provajdera usluga za račun banke.¹⁹⁹ Uobičajena praksa koja se primenjuje za održavanje integriteta podataka u e-banking okruženju obuhvata sledeće:²⁰⁰

- Transakcije e-bankinga treba da se sprovode na način koji ih čini visoko otpornim na upade tokom celokupnog procesa.
- Arhiva e-bankinga treba da se čuva, da bude dostupna i da se menja na način koji je čini visoko otpornim na upade.
- Transakcije e-bankinga i procesi arhiviranja treba da su projektovani na takav način da bude praktično nemoguće da se zaobiđe detektovanje neautorizovanih izmena.
- Adekvatna politika kontrole promena, uključujući procedure monitoringa i testiranja, potrebne su za zaštitu od promena u sistemu e-bankinga koje mogu greškom ili nenamerno da nanosi štetu kontroli ili pouzdanosti podataka.
- Svako upadanje u e-banking transakcije ili arhivu treba da se detektuje u funkcijama procesovanja transakcija, monitoringa i arhiviranja.

Princip 9: Banke treba da obezbede postojanje jasnih dnevnika za sve transakcije e-bankinga.

Pružanje finansijskih usluga preko Interneta može da otežava bankama primenu i sprovođenje interne kontrole i održavanja jasnih dnevnika ako ove mere nisu prilagođene okruženju e-bankinga. Banke ne samo da moraju da obezbede postojanje efikasne kontrole u visoko automatizovanom okruženju, već takođe da kontrola bude podvrgnuta nezavisnoj reviziji, naročito kada se radi o svim kritičnim događajima i aplikacijama u e-bankingu.

Bančino okruženje za internu kontrolu može da bude oslabljeno ako nije u mogućnosti da održava jasne dnevnike za svoje aktivnosti e-bankinga. Ovo zbog toga što je veliki broj, ako nisu i svi, zapisi i evidencije koje podržavaju transakcije e-bankinga u elektronskoj formi. Kod određivanja gde treba održavati jasne dnevnike, treba uzeti u obzir sledeće transakcije e-bankinga:

¹⁹⁹ Banke treba da obezbede da sistemi arhiviranja budu projektovani i postavljeni na način koji dozvoljava povraćaj podataka koji su bili napadnuti ili degradirani.

²⁰⁰ Vuković D.: „Principi upravljanja rizikom za elektronsko bankarstvo“, cit.delo, str.139.

- Otvaranje, vođenje ili zatvaranje računa klijenta.
- Bilo koja transakcija sa finansijskim posledicama.
- Bilo koja autorizacija data klijentu da prekorači limit.
- Bilo koje odobrenje, izmena ili opoziv prava pristupa sistemima ili privilegija.

Princip 10: Banke treba da preduzmu odgovarajuće mere da se očuva poverljivost ključnih informacija u e-bankingu. Mere preduzete za očuvanje poverljivosti treba da su u skladu sa osetljivošću informacija koje se prenose i/ili čuvaju u bazama podataka.

Poverljivost je sigurnost da ključne informacije ostaju privatne za banku i ne mogu da ih vide ili koriste lica koja nemaju ovlašćenje za to. Zloupotreba ili neovlašćeno otkrivanje podataka izlaže banku reputacionom i pravnom riziku. Dolazak e-bankinga predstavlja dodatne izazove za obezbeđenje u bankama jer povećava izloženost riziku da informacije koje se transmituju putem javne mreže ili se čuvaju u bazama podataka budu dostupne neovlašćenim ili neodgovarajućim licima ili da se koriste protivno namerama klijenta koji daje informacije. Pored toga, povećano angažovanje provajdera usluga može da izloži bančine ključne podatke drugim stranama.

Da bi se odgovorilo ovim izazovima koji se tiču očuvanja poverljivosti ključnih informacija iz e-bankinga, banke moraju da obezbede da su:²⁰¹

- Sve poverljive baze podataka i arhive dostupne samo valjano autorizovanim i autentifikovanim licima, agentima ili sistemima.
- Svi poverljivi podaci održavani na siguran način i zaštićeni od neovlašćenog uvida ili izmena tokom transmisije preko javne, privatne ili interne mreže.
- Ispunjeni svi bančini standardi i kontrole za korišćenje podataka i njihovu zaštitu kada treće strane imaju pristup podacima u odnosima autorsinga.
- Svi pristupi zaštićenim podacima logovani i da se čine odgovarajući napor da se obezbedi da pristupni logovi budu otporni na upad.

Mada je bord direktora odgovoran da obezbedi odgovarajuće procese kontrole sigurnosti za e-banking, suština ovih procesa zahteva specijalnu pažnju menadžmenta zbog pojačanih pretnji sigurnosti koje donosi e-banking. Ovo treba da uključi postavljanje odgovarajućih mera poverljive autorizacije i autentifikacije, logičke kontrole i kontrole fizičkog pristupa, adekvatnu infrastrukturu sigurnosti za održavanje odgovarajućih ograničenja i restrikcija za aktivnosti internih i eksternih korisnika i integritet podataka o transakcijama, arhive i informacija. Pored toga, treba obezbediti postojanje jasnih dnevnika, jer sve transakcije e-bankinga treba da su obezbeđene i mere za obezbeđenje poverljivosti ključnih informacija e-bankinga treba da odgovaraju osetljivosti tih informacija.

3.2.3. Upravljanje pravnim i reputacionim rizikom

Upravljanje pravnim i reputacionim rizikom obuhvata principe (11 do 14):

11. Odgovarajuće obelodanjivanje za usluge e-bankinga,
12. Privatnost informacija o klijentima,
13. Kapacitet, poslovni kontinuitet i planovi za svaku eventualnost da bi se osiguralo funkcionisanje sistema i usluga e-bankinga.

²⁰¹ Isto, str.141

14. Planiranje reagovanja na incidente.

Specijalni propisi i zakoni za zaštitu potrošača i privatnosti razlikuju se od jurisdikcije do jurisdikcije. MeCutin, banke generalno imaju jasnu odgovornost da pruže svojim klijentima nivo sigurnosti u pogledu objavljivanja podataka, zaštite podataka o potrošačima i poslovne dostupnosti koja se približava nivou koji bi oni uživali da obavljaju poslovanje kroz tradicionalne bankarske kanale distribucije.

Princip 11: Banke treba da obezbede da na svojim veb-sajtovima pružaju adekvatne informacije koje omogućavaju potencijalnim klijentima da donose informisane zaključke o bančinom identitetu i pravnom statusu banke pre nego što uđu u transakcije e-bankinga.

Da se minimiziraju pravni i reputacioni rizici povezani sa domaćim i prekograničnim aktivnostima e-bankinga, banke treba da obezbede da se na njihovim veb-sajtovima pružaju adekvatne informacije koje će omogućiti njihovim klijentima donošenje informisanih zaključaka o identitetu i pravnom statusu banke pre nego što uđu u e-transakciju.

Primeri takvih informacija koje banka pruža na svom web-sajtu obuhvataju.²⁰²

- Naziv banke i lokaciju centrale (kao i lokalnih jedinica ako je potrebno).
- Identitet kontrolora banke nadležnog za kontrolu bančine centrale.
- Kako klijenti mogu da stupe u kontakt sa bančnim centrom za pružanje usluga klijentima u vezi sa problemima, reklamacijama, sumnjama u vezi sa zloupotrebom računa, itd.
- Kako klijenti mogu da ostvare pristup i kontakt sa ombudsmanom ili šemama za pritužbe potrošača.
- Kako potrošači mogu da ostvare pristup informacijama o nacionalnoj šemi za kompenzacije ili osiguravajuće pokriće depozita kao i o nivou zaštite koje one pružaju (ili linkovane na veb-sajtove koji pružaju takve informacije).
- Druge odgovarajuće informacije, kao i one koje se zahtevaju u odnosnim jurisdikcijama.²⁰³

Princip 12: Banke treba da preduzimaju odgovarajuće mere koje obezbeđuju pridruživanje zahteva za privatnost potrošača koji važe u jurisdikciji na kojoj banka pruža usluge i proizvode e-bankinga.

Očuvanje privatnosti informacija o potrošačima predstavlja ključnu odgovornost banke. Zloupotreba ili neovlašćeno otkrivanje poverljivih podataka o potrošačima izlaže banku i pravnom i reputacionom riziku. Da bi se odgovorilo izazovima koji se tiču očuvanja privatnosti informacija o potrošačima, banke treba da čine razumne napore da:

- Bančina politika i standardi o privatnosti potrošača uzmu u obzir i pridržavaju se propisa i zakona o privatnosti koji važe u jurisdikciji na kojoj banka pruža usluge i proizvode e-bankinga.
- Potrošači budu obavešteni o bančinoj politici privatnosti i o odgovarajućim pitanjima privatnosti vezanim za korišćenje proizvoda i usluga e-bankinga.

²⁰² Isto, str.143

²⁰³ Na primer, banka može da navede zemlje u kojima namerava da pruža usluge e-bankinga ili, obrnuto, one zemlje, u kojima ne namerava da pruža takve usluge.

- Potrošači mogu da odbiju („opt out“) da dozvole banci da deli sa trećom stranom u cilju marketinga bilo koju informaciju o njihovim ličnim potrebama, interesovanju, finansijskoj poziciji ili bankarskoj aktivnosti.
- Podatke o potrošačima ne koristi za potrebe izvan onih potreba koje su izričito dozvoljene ili za potrebe izvan onih za koje je potrošač dao saglasnost.²⁰⁴
- Bančini standardi za korišćenje podataka o potrošaču moraju da se poštuju kada treće strane imaju pristup podacima o potrošačima kroz odnose outsorringa.

Princip 13: Banke treba da imaju efektivni kapacitet, poslovni kontinuitet i procese planiranja da bi se obezbedilo funkcionisanje sistema i usluga e-bankinga.

Da bi se banke zaštitile od poslovnog, pravnog i reputacionog rizika, usluge e-bankinga moraju da se pružaju na trajnoj osnovi i blagovremeno u skladu sa očekivanjima klijenata. Da bi se ovo ostvarilo, banka mora da ima sposobnost da pruža usluge e-bankinga krajnjim korisnicima bilo putem primarnih (npr. internim bančnim sistemima) ili sekundarnih izvora (npr. sistemi aplikacije provajdera usluga).

Održavanje adekvatne raspoloživosti takođe zavisi od sposobnosti *back-up* sistema da ublaže posledice prekida pružanja usluga ili drugih događaja koji mogu potencijalno da izazovu prekid poslovanja.

Izazovi da se održi i kontinuirano funkcionisanje sistema e-bankinga i aplikacija mogu da budu znatni pri datim visokim zahtevima za transakcijama, naročito tokom špičeva. Pored toga, visoka očekivanja klijenata vezana za kratak ciklus procesiranja transakcije i stalne raspoloživosti (24 x 7) takođe su povećala značaj zdravog kapaciteta, poslovnog kontinuiteta i planiranja za slučaj nezgoda. Da bi se klijentima pružile usluge e-bankinga koje oni očekuju, banke moraju da obezbede da su:

- Postojeći kapacitet sistema e-bankinga i njegova buduća skalabilnost predmet analize u svetlu ukupne tržišne dinamike za e-komerc i projektovane stope prihvatanja proizvoda i usluga i usluga e-bankinga kod klijenata.²⁰⁵
- Procene kapaciteta za procesiranje transakcija e-bankinga uvedene, podvrgavane stresnim testovima i periodično revidovane.
- Doneti i redovno testirani planovi za odgovarajući poslovni kontinuitet i za slučaj prekida ključnih sistema za procesing i davanje usluga e-bankinga.

Princip 14: Banke treba da razvijaju odgovarajuće planove za odgovor na incidente da bi savladale, obuzdale i minimizirale probleme koji nastaju iz neočekivanih događaja, uključujući interne i eksterne napade, koji mogu da spreče pružanje usluga sistema e-bankinga.

Mehanizmi za pružanje efikasnih odgovora od ključnog su značaja za minimalizaciju operativnog, pravnog i reputacionog rizika koji nastaju kao posledica neočekivanih događaja kao što su interni ili eksterni napadi koji mogu da pogode funkcionisanje sistema i usluga e-bankinga. Banke treba da razvijaju odgovarajuće planove za reagovanje na incidente,

²⁰⁴ U nekim jurisdikcijama zakoni i propisi ne obavezuju banke da traže saglasnost od potrošača da koriste podatke o njima za interne potrebe. Međutim, oni mogu da obavezuju banke da daju potrošačima pravo na opciju da ne dozvole banci da deli takve informacije sa trećom stranom ili afilijacijom. U drugim jurisdikcijama, potrošači imaju pravo da spreče banku da koristi podatke o njima za interne i eksterne potrebe.

²⁰⁵ Sadašnji i budući kapital ključnih sistema za pružanje usluga e-bankinga potrebno je stalno preispitivati.

uključujući strategije komunikacija, koje obezbeđuju poslovni kontinuitet, kontrolu reputacionog rizika i limitiranje obaveza u vezi sa prekidom pružanja usluga e-bankinga, uključujući one koje nastaju iz sistema i operacija datih u outsorsing.

Da bi se obezbedio efektivan odgovor na nepredviđene incidente, banke treba da razviju:²⁰⁶

- Planove za reagovanje na incident da bi se rešilo ponovno osposobljavanje sistema i pružanja usluga e-bankinga po raznim scenarijima, poslovima i geografskim lokacijama. Analiza scenarija treba da obuhvati razmatranje verovatnoće nastajanja rizika i njegovog uticaja na banku. Sistemi e-bankinga koji su dati u outsorsing provajderima usluga treba da budu integralni deo ovih planova.
- Mehanizme za identifikovanje incidenta ili kriza čim se budu javile, procenu njihovog materijalnog efekta i kontrolu reputacionog rizika povezanog sa bilo kojim prekidom usluge.²⁰⁷
- Strategiju komunikacije za adekvatno bavljenje eksternim tržištem i medijskim problemima koji mogu da nastanu u slučaju povrede sigurnosti, onlajn napada i/ili grešaka sistema e-bankinga.
- Jasan proces za alarmiranje odgovarajućih regulatornih vlasti u slučaju nužde i koji su dovoljno obučeni da analiziraju sisteme za detekciju incidenta/reagovanje i tumačenje značaja odgovarajućih autputa.
- Jasan lanac komandovanja, koji obuhvata interne aktivnosti i aktivnosti date u outsorsing, da bi se obezbedila promptna akcija koja odgovara značaju incidenta. Pored toga, treba da se razviju procedure eskalacija i interne komunikacije koje će obuhvatiti i prema potrebi i obaveštavanje borda.
- Proces koji obezbeđuje da sve relevantne spoljne strane, uključujući i klijente banke, partnere i medije, budu obaveštene blagovremeno i na odgovarajući način o prekidima e-bankinga koji imaju materijalne posledice, kao i o nastavku poslovanja.
- Proces za prikupljanje sudskih dokaza da bi se olakšala odgovarajuća kasnija analiza incidenta u e-bankingu kao i da se pomaže u sudskom gonjenju počinilaca napada.

Rizici u bankarskom poslovanju su sastavni deo posla. Novi komunikacioni kanal koji opštim imenom možemo nazvati elektronsko bankarstvo, donelo je značajne prednosti kako banci tako i njenim klijentima. Činjenica je da je elektronsko bankarstvo učinilo da banke, prvi put u svojoj istoriji, načine iskorak iz svog poslovnog prostora i dopuste da korisnici samostalno obavljaju svoje poslove vezane za banku. Ovaj iskorak doneo je, s jedne strane bankama značajne uštede i proširenje korisničke baze ali je, s druge strane, naterao banke da deo svojih poslova dislociraju (outsorsuju) u druge specijalizovane firme. Ovo je novost za banke. Njihovi klijenti i njihovi računi se sada nalaze kod nekog drugog i nisu pod apsolutnom kontrolom bankara. Poseban problem je što outsorsing nije samo odnos sa jednim ASP partnerom, već se poslovi dalje šire na druge firme i poslovne partnere. Sve ovo zahteva razvijanje posebnih metoda kontrole i nadzora, a to je funkcija koju banke moraju da razvijaju do maksimuma kako bi zadržale visok nivo poverenja i sigurnosti svojih korisnika.²⁰⁸

²⁰⁶ Vuković D.: „Principi upravljanja rizikom za elektronsko bankarstvo“, cit.delo, str.149

²⁰⁷ Monitoring iz deska za pomoć i aktivnosti podrške klijenata i redovni pregled žalbi klijenata mogu da pomognu da se identifikuju prekidi u uočavanju informacija i izveštavanju kroz ustanovljene kontrole bezbednosti nasuprot stvarnih upada.

²⁰⁸ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit.delo, str.392

Da bi se banke zaštitile od poslovnog, pravnog i reputacionog rizika, usluge e-bankinga moraju da se pružaju konzistentno i blagovremeno, u skladu sa visokim očekivanjima klijenata u pogledu stalne i brze raspoloživosti, ali i u skladu sa potencijalno visokom tražnjom za transakcijama. Banke moraju da budu sposobne da pružaju usluge e-bankinga svim krajnjim korisnicima i da budu u stanju da održe takvu raspoloživost u svim okolnostima. Efektivni mehanizmi za reagovanje na incidente su takođe od ključnog značaja za umanjenje operativnog, pravnog i reputacionog rizika koji nastaju kao posledica neočekivanih događaja, uključujući interne i eksterne napade, koji mogu da ugroze pružanje e-banking sistema i usluga. Da bi se odgovorilo očekivanjima klijenata, banke moraju da imaju efektivan kapacitet, poslovni kontinuitet i planove za svaku eventualnost. Banke treba da razviju odgovarajuće planove za reagovanje na incidente, uključujući komunikacione strategije, koje obezbeđuju kontinuitet poslovanja, kontrolu reputacionog rizika i limitiranje obaveza po osnovu poremećaja u njihovim uslugama e-bankinga.

ČETVRTI DEO

PROBLEMI SIGURNOSTI I MERE ZAŠTITE

1. DIMENZIJE I FUNKCIJE SIGURNOSTI

U konkretnim projektima obezbeđenja adekvatnog nivoa sigurnosti bitna su dva momenta:

1. procena konkretnog rizika i
2. pronalaženje konkretne troškovno-efikasne solucije.

Priroda poruke koja se prenosi treba da opravda troškove koji će biti načinjeni za njeno obezbeđenje. U uslovima elektronskog prenosa, sigurnost sistema odnosi se na sigurnost prenosa i sigurnost prijema, analogno sigurnosti elektronske razmene podataka uopšte. Osnovni zahtev prenosa u ovom kontekstu je obezbeđenje raspoloživosti i pouzdanosti mreže. Emitent inicijator mora biti ovlašćen i ne bi trebalo da bude u mogućnosti da demantuje (porekne) slanje poruke, poruka mora stići na pravu adresu bez modifikacije, a primalac poruka ne bi imao pravo i mogućnost da demantuje izvršen prijem.

Konkretni rizici ove vrste koji mogu nastati su:²⁰⁹

1. gubitak usluge korišćenja mreže;
2. modifikacija sadržaja, porekla i destinacije poruke (usled greške, prevare i sl.);
3. gubitak poruke, odricanje (demantovanje) poruke od inicijatora ili primaoca;
4. nedozvoljeno obelodanjivanje njenog sadržaja,
5. ilegalne upotrebe računarskih sistema ili mreže za prenos.

U cilju eliminisanja ovih rizika razvijaju se posebne funkcije sigurnosti.²¹⁰

1. raspoloživost mreže – podrazumeva obezbeđenje dostupnosti mreže za korišćenje određenom entitetu,
2. integritet poruke – podrazumeva sprečavanje menjanja ili uništenja poruke nedozvoljenim rukovanjem,
3. neporecivost – mera dizajniranja zaštite od naknadnog demantovanja od strane entiteta koji su uključeni u komunikaciju učesćem u delimičnoj ili celokupnoj komunikaciji,
4. poverljivost podataka – sprečavanje mogućnosti da podaci budu dostupni i na raspolaganju neovlašćenim pojedincima, entitetima ili procesima,
5. potvrda – mera obezbeđenja od naknadne zloupotrebe prenete poruke kroz potvrđivanje validnosti prenosa, stacioniranja i porekla,
6. kontrola pristupa – ograničavanje prava ili mogućnosti subjekta da nedozvoljeno komunicira sa drugim subjektima, ili upotrebljavaju funkcije i usluge u sistemu ili mreži.

Mogućnost zaštite od različitih vrsta rizika odgovarajućim funkcijama sigurnosti i njima pripadajući mehanizmi dati su u tabelarnim pregledima.

²⁰⁹ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.58

²¹⁰ Isto, str.59

Tabela 11: Funkcije zaštita od rizika

Funkcije	Rizici						
	Gubitak mreže	Modifikacija	Gubitak poruke	Odgovor	Odricanje poruke	Obelodanjanje	Ilegalna upotreba
Poverljivost pod.		+				+	
Potvrda		+		+			+
Integritet		+	+				
Neodricanje					+		
Kontrola							+
Raspoloživost	+						

Tabela 12: Mehanizmi obezbeđenja pojedinačnih funkcija zaštite

Funkcije						
Mehanizmi	Poverljivost	Potvrda	Integritet	Neodricanje	Kontrola pristupa	Raspoloživost
Knjiženje	X	X	X			
Zaštita od grešaka u pripremi podataka			X			
Zaštita od grešaka u prenosu podataka			X			
MAS (kod potvrđivanja poruka)		X	X			
Funkcija pretraživanja		X				
Sekvenčialni broj, slučajni broj, dat. i vr. potvrde		X				
Digitalni znak		X	X	X		
Lozinka					X	
Elektronski znak					X	
Biometrija					X	
Procedura udruživanja						X

(prema Hodoklin A., 1993.)

Program sigurnosti može biti postavljen na različitim tehničkim rešenjima, mora da bude sproveden na svim podnivoima koji predstavljaju oblast povredivosti.²¹¹

1. nivo terminala,
2. nivo računara i komunikacionih veza i
3. nivo obezbeđenja funkcionalnosti celokupnog sistema.

Problem obezbeđenja sigurnosti terminala i identifikacije klijenta svodi se na uklanjanje dve vrste rizika:

1. rizika od zloupotrebe trećih lica i
2. rizika zloupotrebe od samog klijenata/korisnika usluge.

U prvom slučaju radi se o problemu sprečavanja nedozvoljenog ulaska trećih lica u sistem, a u drugom o sprečavanju zloupotrebe samih sredstava ulaza klijenata. Problemi identifikacije

²¹¹ Isto, str.60

klijenata koji imaju dozvoljen pristup i njegovo korišćenje za određene, dozvoljene namene povećava se sa porastom broja i vrste terminala, a konkretna rešenja dosta zavise od prirode veza sa računarskim centrom.

Identifikacija pojedinačnih učesnika, korisnika određenih sistema je posebno značajna zbog toga što su pojedinci kao individualni korisnici elektronskih sistema plaćanja veoma brojni, mada su iznosi njihovih plaćanja relativno mali. U skladu sa tim, sredstvo ulaza koje oni koriste treba da bude, pogodno za nošenje i upotrebu, da poseduje visok stepen zaštite od zloupotrebe i relativno jeftino. Praksa je pokazala da će takvu funkciju moći da obavljaju već pomenute transakcijske finansijske kartice. U ovom domenu problemi nastaju zbog mogućnosti korišćenja tuđih izgubljenih, ili ukradenih kartica. Složenost sprečavanja zloupotreba ove vrste pokazuje iskustvo SAD koje spadaju u najveće korisnike elektronskih kartica u svetu.

Kontrola pristupa na terminalima obezbeđuje se uvođenjem lozinke, elektronskih signala (simbola) i biometrijskim sredstvima. Ključno sredstvo koje je korišćeno za zaštitu u ovom domenu je uvođenje tzv. PIN-a (engl. *Personal Identification Number*) koji se ugrađuje na magnetnu traku ili čip, a sastoji se od nekoliko digitalnih znakova ili algoritama. Problemi su se u praksi javljali u slučajevima kada su treća lica otkrivanjem PIN-a tuđih ukradenih ili izgubljenih kartica uspevala da uđu u sistem. Sama mogućnost ovakve zloupotrebe u velikoj meri je zavisila od samog tehničkog rešenja pisanja i korišćenja PIN-a.²¹²

Za posebno osetljive transakcije ili za velike novčane transfere primenjuje se dodatni sistem zaštite – TAN (engl. *transaction access number*). TAN predstavlja niz slučajnih brojeva koje generiše banka i daje ih korisniku kartice. Korisnik kada želi da obavi transfer novca ili plaćanje popunjava broj kartice, zatim unosi PIN i na kraju unosi TAN. TAN je broj za jednokratnu upotrebu, za samo jednu transakciju i ne može se više koristiti.²¹³

Alternative za PIN poznate su kao biometrijske metode, zbog toga što se zasnivaju na merenju i verifikovanju jedinstvenih fizičkih karakteristika pojedinaca. Do sada je poznato pet metoda biometrijske identifikacije: verifikacija potpisa, geometrija šake, poređenje otisaka prsta i dlana, merenje otisaka sluha i snimanje očne zenice, a pojavljuje se i ideja o šestom - uzorak krvi. Identifikacija lica koje koristi karticu vrši se veoma jednostavno. Prilikom izdavanja kartice, potrebne biometrijske informacije se memorišu u sistem i sa njima se vrši poređenje određenih biometrijskih karakteristika lica koje koristi karticu. Praktični problemi za njihovu primenu nastaju zbog toga, što je za identifikaciju korisnika potreban veliki obim podataka, tako da njihova upotreba pretpostavlja korišćenje kartice sa čipom i kompleksnost uređaja za čitanje. Pored toga, iz raznih razloga (npr. bolesti) kod biometrijskih karakteristika može doći do promena. Po svojoj prirodi, a u zavisnosti od biometrijske metode, brojni neuspeli pokušaji identifikacija mogu dovesti do nezadovoljstva korisnika. Najveći problem je što su biometrijski podaci neizostavno javni i što mogu biti upotrebljeni iako stvarni vlasnik nije fizički prisutan. Jednom kada je biometrijski zapis napravljen u digitalnom obliku može biti kopiran i korišćen vrlo lako za obmanu. Jednom kompromitovana biometrija ne može se izmeniti. Ovo je manji problem kod zatvorenih mreža ili pojedinačnih sistema, ali za udaljenu identifikaciju preko Interneta postaje ozbiljan problem. Industrija koja se bavi biometrijskim metodama preporučuje standardan set principa za očuvanje privatnosti. To je redovno šifrovanje biometrijskih podataka pre bilo kakvog slanja i stroga kontrola distribucije podataka.

²¹² Isto, str.61

²¹³ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit.delo, str.296

Kada se radi o problemu eliminisanja rizika od neadekvatnog korišćenja finansijskih transakcijskih kartica od strane samog vlasnika, onda se postavlja pitanje uklapanja njihovih tehničkih karakteristika sa bankarskim principima poslovanja. Kako one u osnovi predstavljaju samo tehniku, njihova implementacija može da se usklađuje sa različitim konkretnim finansijskim aranžmanima koje banka izgrađuje sa svojim klijentima (korišćenje sredstava sa određenih računa, kreditne linije do određenog iznosa i sl.). Konkretnu soluciju, banka bi trebalo da bira u skladu sa procenom boniteta svakog pojedinačnog klijenta i odmeravanja vlastite politike sigurnosti.

Slabijim klijentima moglo bi se vršiti maksimiranje iznosa po pojedinačnoj upotrebi preko mehanizma dozvoljenog opterećenja finansijske transakcione karte. Klijentima prosečnog boniteta mogao bi se odrediti maksimalni broj korišćenja (ili iznosa) preko kojih klijent više ne bi mogao da koristi karticu, dok bi klijentima izuzetnog boniteta mogao biti dozvoljen automatizam u korišćenju bez ikakvih posebnih ograničenja.

Problem funkcionisanja računarskog sistema kao celine odnosi se na neophodnost, da sistem kao celina permanentno i ispravno funkcioniše u tehničkom smislu. Ovaj problem dobija posebno na značaju, zbog toga što se teškoće u radu jednog centra prenose na rad ostalih delova sistema i mogu izazvati blokadu celokupnog sistema. U praksi su poznati problemi izazvani ovim razlozima. Elektronski bankarski sistem u SAD-u je 2003. godine pretrpeo veliki udarac ove vrste, u trajanju od nekoliko časova, kada se pojavio virus koji se širio velikom brzinom sa računara na računar, usled čega je došlo do prekida u nekoliko globalnih informacionih mreža. Hiljade mejlova je satima kasnilo, a usluge na mrežama ATM-ova nekoliko vodećih banaka SAD-a i Kanade bile su ugrožene. U konkretnom slučaju, sistem je vraćen u on-line funkcionisanje u toku istog dana, ozbiljnim naporima banaka.²¹⁴

2. TEHNOLOGIJA ZAŠTITE PODATAKA NA INTERNETU

2.1. Pojam zaštite podataka

Nivo zaštite podataka kod razmene elektronskih poruka izuzetno je značajan element na osnovu kojeg se korisnici opredeljuju za ili protiv primene e-transakcija. To je posebno karakteristično u slučajevima kada gubitak, izmena, neovlašćeni uvid ili neke druge pretnje elektronskim dokumentima mogu da izazovu značajne pravne i finansijske posledice po učesniku u online transakciji. Naime, u e-poslovanju i razmeni elektronskih dokumenata učestvuju brojni partneri i svi moraju da imaju odgovarajući nivo zaštite.

Pod zaštitom podataka podrazumeva se namera da podaci ostanu poznati samo pošiljaocu i primaocu, i tako da jedino oni mogu da ih koriste. Mogućnost uvida trećih lica može da dovede do zloupotrebe određenih podataka, a to može da izazove negativne posledice po učesnike u razmeni. Podaci mogu da se podele na sledeće četiri grupe:

- javni podaci – podaci u koje svi mogu da imaju uvid;
- autorizovani podaci – podaci u koje svi imaju uvid, ali su od neautorizovanog korišćenja zaštićeni autorskim pravom;
- poverljivi podaci – podaci koji su tajni (čiji sadržaj ne sme da bude čitljiv neovlašćenim licima).

²¹⁴ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo , str.62

Za zaštitu poverljivih i tajnih podataka koriste se mnoge metode i tehnike. Ako se podaci šalju nekim sredstvom komunikacije, primenjuju se tehnike koje su razvijene u kriptologiji. Kada se podaci čuvaju ili primaju na određenom mestu, obezbeđuju se primenom tehnika personalne identifikacije. Za zaštitu informacionih sistema od negativnih uticaja sa Interneta obično se koristi granični server (engl. *firewall*), antivirusni softveri i sl.²¹⁵

2.2. Razumevanje sigurnosnih problema i dimenzija sajber – kriminala

Postoji mnogo razloga zbog kojih se teško mogu proceniti stvarne dimenzije sajber – kriminala, a brojne slučajeve kompanije i ne prijavljuju zato što strahuju od gubitka poverenja potencijalnih korisnika i potrošača. Ali, i u slučajevima kada je kriminalna radnja prijavljena vlastima, često se teško može proceniti nivo gubitka.

Motivi svih sajber – kriminalnih radnji nisu vezani za novac – neki napadi su sračunati samo na to da unište ili onespobu Web stranu. Gubici u takvim slučajevima ne čine samo sredstva koja su potrebna za obnavljanje svoje Web strane već i gubitak reputacije i imidža sajta, kao i prihoda koji bi se ostvario u periodu dok sajt nije radio.

Može se zaključiti da je sajber – kriminal usmeren na e-trgovinske sajtove u porastu, da je reč o šteti koja se teško može tačno proceniti i da se očekuje njen dalji rast. S obzirom na nivo gubitka kompanija nastalih zbog sajber – kriminalnih radnji, razvoj i primena dobro osmišljene politike zaštite postaje prioritetan zadatak i potreba.

2.3. Kako obezbediti dobar nivo sigurnosti u elektronskom poslovanju?

Smanjivanje rizika u elektronskom poslovanju kompleksan je postupak, koji obuhvata nove tehnologije, organizacione politike i procedure, nove zakone i industrijske standarde na osnovu kojih će se dati ovlašćenja nadležnim organima da gone i kažnjavaju počinioce sajber – kriminalnih radnji. Međutim, potpuna sigurnost ne postoji. Svaki sigurnosni sistem može da bude „provaljen“, ukoliko se u ostvarenje takve namere ulože dovoljna sredstva. Ali, trajna sigurnost u informatičkoj eri nije ni potrebna. Podaci obično imaju vrednost u određenom vremenskom periodu, tako da se prema potrebi zaštite jedan dan, ili mesec, ili godinu.

Nivo sigurnosti povezan je sa sagledavanjem dva odnosa:²¹⁶

1. Odnos nivoa sigurnosti i lakoće upotrebe sajta je divergentan. Brojne mere sigurnosti koje se dodaju e-trgovinskom sajtu čine da sajt postaje sporiji i teži za korišćenje. Tako prevelika sigurnost može da naškodi profitabilnosti, dok nedovoljan nivo sigurnosti, s druge strane, može vlasnika da izbac iz posla;
2. Takođe postoji divergentan odnos između nastojanja pojedinaca da obezbede svoju sigurnost i sakriju svoj identitet i potrebe da se obezbedi odgovarajući nivo javne sigurnosti, koju mogu da ugroze kriminalci i teroristi.

²¹⁵ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.235

²¹⁶ Isto, str.237

2.4. Osnovne sigurnosne pretnje u elektronskom poslovanju

Da bi se razumeli različiti sistemi zaštite na pojedinim nivoima zaštite, neophodno je da se znaju najčešći oblici pretnji i narušavanja sigurnosti u elektronskom poslovanju. To su.²¹⁷

1. Zlonamerni kod (engl. *Malicious code*). Ovu grupu štetnih uticaja čine virusi, crvi, „trojanski konji“ i „*bad applets*“ koji su pretnja integritetu sistema i njegovoj kontinuiranoj operativnosti. Njihovo delovanje, donekle različito, uglavnom se ispoljava u promeni načina rada sistema, ili promeni dokumenata kreiranih u okviru sistema.

Virusi su računarski programi koji imaju sposobnost da se umnožavaju, da prave sopstvenu kopiju i da se šire na druge fajlove. Osim toga donose i tzv. „*payload*“, koji može da bude manje opasan, u slučajevima da pokazuje nepotrebne poruke i slike, ili veoma destruktivan – kada uništava fajlove, reformatizuje računarski drajv, ili izaziva pogrešan rad programa. Najveću kategoriju (75-80%) čine makrovirusi, koji napadaju samo aplikacije za koje su kreirani na primer, Exel, Word, Power Point, zatim virusi koji najčešće napadaju izvršne fajlove kao što su *.exe, *.drv. i *.dll. fajlovi i script virusi, napisani u script programskim jezicima, kao što su *Visual Basic Script* i *JavaScript* (*I love you virus*).

Osim što se šire iz fajla u fajl, crvi su dizajnirani tako da se šire sa računara na računar.

„Trojanski konj“, nije virus, jer se ne umnožava, ali je put kojim virusi, ili slični štetni uticaji, ulaze u računar, po čemu je i dobio ime.

Java applets i *ActiveX* kontrole su programi koji deluju u okviru brauzera. Oni dodaju funkcionalnost Web strani i čine je interaktivnom, ali su i visok sigurnosni rizik, jer se mogu aktivirati jednostavnim surfovanjem po Internetu i preuzimanjem appleta na klasični računar.

2. Hakeri i sajbervandalizam. Haker se definiše kao pojedinac koji želi da ostvari neovlašćeni pristup računarskom sistemu. Nekada se zadovoljavaju time što prodru u fajlove e-trgovinskog sajta, ali ima slučajeva kada im je namera vezana za tzv. sajbervandalizam, što podrazumeva prekidanje, promenu ili uništavanje sajta. U okviru hakerske zajednice, krekerima se nazivaju hakeri koji preduzimaju kriminalne aktivnosti. Tokom vremena, aktivnosti hakera se menjaju i šire, pa se, osim na upad u sistem, orijentišu i na krađu informacija i robe, kao i na uništavanje sistema.
3. Zloupotreba kreditnih kartica/krača. To je najčešća pojava i jedan od glavnih razloga zbog kojeg više potrošača ne učestvuje u elektronskoj trgovini. Najčešći slučaj je izgubljena ili ukradena kartica koju koristi neko drugi, kao i krađa brojeva kreditnih kartica radi dalje zloupotrebe i lažnog predstavljanja identiteta vlasnika kartice.

U elektronskoj trgovini najveća pretnja kupcima je da će prodavčev server izgubiti podatke o kreditnim karticama koji su na njemu deponovani, ili će dozvoliti da se

²¹⁷ Isto, str.237

koriste u kriminalne svrhe. Osim toga, e-trgovinski sajtovi su odličan izvor personalnih podataka kupaca (ime, adresa, broj telefona), koji mogu da se zloupotrebe.

4. Lažno predstavljanje (engl. *Spoofing*). Hakeri nekad pokušavaju da prikriju svoj pravi identitet, ili se lažno predstavljaju na osnovu lažne (tuđe) e-mail adrese. *Spoofing* može da znači i preusmeravanje Web linka na adresu drugačiju od nameravane, pri čemu se lažna adresa prikazuje kao da je prava (lažni sajt je identičan pravom). Na taj način hakeri mogu da preuzimaju porudžbine i krađu posao pravom sajtu. Ukoliko im je namera da nanese štetu, mogu da izmene originalnu porudžbinu i zatim da je pošalju na prvi sajt, a rezultat je nezadovoljan kupac, koji dobija ono što nije poručio, tako da se obično ne vraća navedenom sajtu. Na taj način, osim integriteta, *spoofing* narušava i princip autentičnosti, jer otežava utvrđivanje identiteta prave ličnosti koja šalje poruku.
5. Napadi usmereni na odbijanje usluge sajta (engl. *Denial of service attacks*). Hakeri nekad optereće Web sajt nekorisnim porukama (saobraćajem) da bi opteretili mrežu, što često izaziva zatvaranje mreže i nanosi štetu reputaciji sajta i odnosima sa potrošačima. Za sajtove kao što su *eBay* i *Buy.com* takvi napadi su skupi, jer dok je sajt zatvoren kupci ne mogu da poručuju robu.
6. „Njuškanje“, uhoćenje (engl. *Sniffing*). Tip programa za prisluškivanje koji prate informacije koje se kreću po mreži i omogućavaju hakerima da ukradu poverljive informacije sa bilo koje lokacije na mreži, uključujući e-mail poruke, fajlove kompanije i poverljive izveštaje. „Njuškanje“ je u stvari, pretnja da će poverljive informacije biti javno prezentovane.
7. Napadi iznutra. Iako je najveća pretnja od spoljnih napada, postoji i značajna opasnost da zaposleni, iznutra, neovlašćeno koriste podatke i informacije koje su im dostupne.

2.5. Sistemi zaštite

Najosetljivije tačke na kojima treba postaviti zaštitne mehanizme, sa tehnološkog gledišta, jesu sledeći nivoi zaštite:²¹⁸

1. zaštita na nivou telekomunikacione mreže,
2. zaštita na aplikativnom nivou i
3. zaštita na nivou poruke.

2.5.1. Sistem zaštite na nivou telekomunikacione mreže

Na ovom nivou, definišu se zaštitni mehanizmi pristupa određenoj prenosnoj mreži. Naime, na mrežu se uključuju samo autorizovani korisnici i to na osnovu korisničkih identifikacionih kodova i lozinki. Na taj način, neregistrovani i neautorizovani korisnici ne mogu da dobiju pristup i pravo korišćenja prenosne mreže.

²¹⁸ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.240

Tabela 13: Alati koji su raspoloživi za postizanje sigurnosti sajta

Šifrovanje	Zaštitna barijera	Sigurnosni alati
Mrežni bezbedonosni protokoli	Upravljanje bezbednošću	Kontrole pristupa
Virtualna privatna mreža		Autentifikacija
Tuneling	Prox/agent sistem	Detekcija uljeza

Postoji čitav niz alata namenjenih očuvanju bezbednosti sajta

Izvor: Laudon, Traver, 2002, str.246.

Osnovna zaštita na mrežnom nivou je pouzdana i nedvosmislena identifikacija strana uključenih u proces razmene pošiljaoca i primaoca poruke. Identifikacija se obavlja pomoću sertifikata koji dostavlja sertifikaciono telo – treća strana u razmeni, u koju strane u razmeni imaju poverenje i koja vodi registar svih partnera u razmeni. Treća strana garantuje identitet partnera dostavom sertifikata sa svojim digitalnim potpisom.

2.5.2. Sistem zaštite na aplikativnom nivou

Pod zaštitom na aplikativnom nivou podrazumevaju se dodatne restrikcije ili dozvole, vezane za korišćenje raspoloživih podataka, koje se uvode za korisnike, koji su zadovoljili uslove bezbednosnog sistema na mrežnom nivou. Prava se određuju na osnovu lozinki. Naime, određene aplikacije ili podaci, mogu da budu dostupni ili zabranjeni za korišćenje, određenim korisnicima. Nivo mogućih intervencija na podacima može da bude različito definisan za različite korisnike (pravo samo na unošenje podataka, pravo samo na čitanje, pravo na čitanje i izmenu podataka, pravo na slanje podataka drugim stranama u razmeni i slično).

2.5.3. Sistem zaštite na nivou poruka

Pošto se e-trgovina obavlja preko javne Internet mreže, poruka prolazi hiljade rutera i servera, pa stručnjaci za sigurnost stoga veruju da se najveće pretnje sigurnosti nalaze upravo na nivou komunikacija na Internetu. To je sasvim drugačija situacija, od one kada poruka (kao u sistemu EDI-ja) ide preko privatne mreže, uspostavljene između dva partnera koja veruju jedan drugom.

Visok nivo zaštite na nivou poruka izuzetno je značajan u elektronskoj razmeni poslovnih dokumenata. Pretnje mogu da budu izazvane namerno, kao posledica neovlašćene manipulacije sadržajem poruka, ili nenamerno, kao rezultat grešaka u komunikacionom prenosu kojima se menja sadržaj poruka. Za zaštitu su razvijeni brojni bezbednosni mehanizmi za koje se koriste jedna ili više metodologija zaštite.

Tabela 14: Dimenzije e-trgovinske sigurnosti prema shvatanju kupca i prodavca

Sigurnosne dimenzije	Iz perspektive kupca	Iz perspektive prodavca
Integritet	Da li je informacija koju sam poslao ili primio promenjena?	Da li su podaci na sajtu promenjeni neautorizovani? Da li su validni podaci koje sam primio od kupca?
Neporecivost	Da li partner u akciji može posle poreći svoju radnju?	Da li kupac može poreći svoju porudžbinu?
Autentičnost	Sa kim poslujem? Kako mogu biti siguran da je preduzeće/osoba ona za koju se predstavlja?	Koji je pravi identitet kupca?

<i>Sigurnosne dimenzije</i>	<i>Iz perspektive kupca</i>	<i>Iz perspektive prodavca</i>
Poverljivost	Može li neko drugi, osim očekivanog primaoca, pročitati moju poruku?	Da li su poruke ili poverljivi podaci dostupni svima, ili samo ovlašćenim osobama?
Privatnost	Mogu li kontrolisati informacije o sebi koje sam poslao e-prodavcu?	Da li se lične informacije o kupcima mogu zloupotrebiti?
Raspoloživost	Mogu li dobiti pristup sajtu?	Da li je sajt operativan?

Izvor: Laudon, Traver, 2001, str.235.

Opšte pretnje u pogledu bezbednosti poruka mogu najbolje da se sagledaju analizom postojećih šest dimenzija e-trgovinske sigurnosti:²¹⁹

1. integritet je sposobnost da se obezbedi da informaciju koja je postavljena na sajt, ili je poslata/primljena preko Interneta, neovlašćena osoba ne izmeni ni na koji način. Mehanizam za zaštitu integriteta štiti poruke koje se prenose od dupliranja, dodavanja, brisanja, gubitka, ili ponavljanja nekog njihovog dela, ili celine;
2. neporecivost (priznavanje) je sposobnost da se obezbedi da učesnici u e-trgovini ne poriču/priznaju svoje online akcije. Naime, treba zaštititi primaoca od eventualnog pokušaja pošiljaoca poruke da porekne njeno slanje, ili njen sadržaj i treba zaštititi pošiljaoca, od mogućnosti da primalac porekne da je tu poruku primio;
3. autentičnost je sposobnost utvrđivanja individualnog ili poslovnog identiteta učesnika u transakciji. Primalac poruke se štiti od mogućeg lažnog predstavljanja, odnosno, od slanja poruke pošiljaoca koji se predstavlja kao neko drugi;
4. poverljivost znači da su informacije i podaci poslani online, dostupni samo primaocu, tj. licu koje je ovlašćeno da ih vidi, odnosno da su razmenjivani podaci zaštićeni od neovlašćenog uvida, kopiranja, ili otkrivanja sadržaja poruke;
5. privatnost je sposobnost kontrole upotrebe informacija koje dostavljaju kupci o sebi i
6. raspoloživost znači dostupnost i operativnost Web sajta u svakom trenutku.

Pitanje zaštite na nivou poruka u e-trgovini upravo se odnose na sprečavanje narušavanja bilo kojeg od navedenih nivoa sigurnosti.

3. KRIPTOGRAFIJA

Kriptografija se bavi čuvanjem tajnosti informacija, što ima poseban značaj kada se poverljivi podaci prenose, odnosno smeštaju u bilo kakav elektronski sistem. Da bi se obezbedila sigurnost poruka koje se šalju preko Interneta, koriste se različite tehnologije kriptografije. Ova tehnologija bazira se na dva podprocesa: nakon generisanja poruke ona se na predaji šifrjuje, a na prijemu se vrši njeno dešifrovanje. Kriptografija (engl. *Cryptography*) je nauka koja u postupku šifrovanja transformiše podatak iz izvornog/otvorenog oblika u šifrovani kriptografski oblik (engl. *encryption*), pomoću odgovarajućih algoritama, korišćenjem kriptografskih ključeva. Dešifrovanje primljene poruke je proces inverzan šifrovanju, odnosno pretvaranje šifrovanih podataka - kriptografskog oblika u otvorenu/izvornu poruku (engl. *decryption*) i vrši se takođe pomoću algoritama, upotrebom odgovarajućeg ključa. Kriptoanaliza je tehnika napada na kriptografske sisteme, koja i bez poznavanja kriptoloških

²¹⁹ Isto, str.242

ključeva, a korišćenjem odgovarajućih slabosti u postupku šifrovanja pokušava da otkrije izvorene (otvorene) poruke. U prevodu kriptografija znači pisanje tajni.²²⁰

Slika 4: Kriptografski proces



Komunikacioni kanal

Šifrovanjem, poruka treba da se zaštiti tako da je ne može pročitati niko osim njenog pošiljaoca i primaoca. Sigurnost prenosa šifrovane poruke zavisi od tajnosti ključa, a u zavisnosti od odnosa između ključeva koji se koriste za šifrovanje i dešifrovanje pravi se razlika između dve osnovne vrste kriptografskih sistema: simetričnih i asimetričnih.

Kombinovanjem i nadgradnjom ove dve osnovne tehnike, danas je razvijeno više različitih formi kriptografskih tehnologija kojima se obezbeđuje značajno podizanje stepena bezbednosti u prenosu podataka. Njome se obezbeđuje četiri od šest dimenzija e-sigurnosti:

1. integritet poruke (obezbeđuje sigurnost da je poruka verodostojna, odnosno da nije bila promenjena),
2. neporecivost poruke (obezbeđuje nemogućnost odricanja učesnika da su poruku poslali/primili),
3. autentičnost (obezbeđuje da se verifikuje osoba/mašina sa koje je poruka poslata) i
4. poverljivost (osigurava da poruku ne pročita neko ko za to nije ovlašćen).

Na današnjem nivou razvoja primenjuju se dve osnovne kriptografske tehnologije:²²¹

1. simetrična kriptografija, ili metod simetričnog tajnog ključa,
2. asimetrična kriptografija, ili metod javnih ključeva.

Primenom kriptografskih metoda mogu se primeniti i sledeće tehnike: kriptografija pomoću javnih ključeva, digitalnog potpisa i hash funkcije, digitalna koverta i digitalni sertifikat i infrastruktura javnih ključeva.

3.1. Simetrična kriptografija

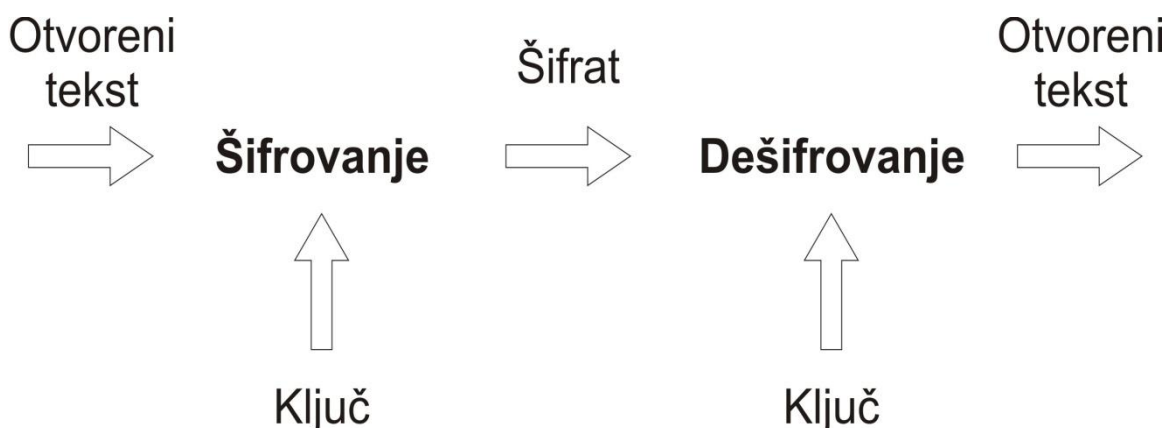
Simetrična kriptografija (simetrični kriptosistemi), ili metod jedinstvenog simetričnog tajnog ključa, podrazumeva korišćenje identičnog ključa i za šifrovanje i za dešifrovanje šifrovane poruke. Pošiljalac i primalac koriste isti, tajni ključ, koji poseduju samo oni. Ovaj sistem funkcioniše brzo i jednostavno, ali su u njegovoj operativnoj primeni prisutna dva problema. Prvi problem odnosi se na samu sigurnost ključa, odnosno sigurnost kanala kroz koje se vrši distribucija ključeva. Ključ se nikada ne može distribuirati istim komunikacionim kanalom

²²⁰ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.63

²²¹ Isto, str.64

kojim se prenosi šifrat, tj. ključevi se distribuiraju tajnim kanalom. Drugi problem odnosi se na broj ključeva, jer u ovakvom sistemu za svakog klijenta, ili partnera treba obezbediti poseban ključ. Znači, problem je broj ključeva i kako ih razmeniti. Najpoznatiji standardi ovog sistema su DES (*Data Encryption Standard*), koji su razvili NSA i IBM pedesetih godina, a zatim 3DES, AES (*Advanced Encryption Standard*), IDEA (*Internacional Data Encryption*) i RC2 (šifrovanje Ronovim kodom).²²²

Slika 5: Simetrična kriptografija



U opštoj oceni sistema simetrične kriptografije, može se konstatovati da ona obezbeđuje šifrovanje – zaštitu tajnosti podataka. Autentifikacija i neporicanje se lakše realizuju sa asimetričnim sistemima.

Simetrična kriptografija se koristi za zaštitu tajnosti podataka (*AES DES*, *3DES* itd), dok se za druge funkcije primenjuju asimetrični sistemi. Zbog toga je za potrebe elektronske trgovine i poslovanja preko Interneta razvijen novi metod šifrovanja – asimetrično šifrovanje.

3.2. Asimetrična kriptografija – metod javnih ključeva

Otkriće tehnike asimetrične kriptografije predstavljalo je pravu revoluciju u kriptografiji. Otkrili su je 1976. godine *W. Diffie i Martin Hellman*, a kasnije razvio *R. Merkle*. Suština asimetrične kriptografije je da ključevi ne moraju da budu simetrični i tajni. Ova tehnika podrazumeva korišćenje dva matematički povezana digitalna ključa: javnog i privatnog. U kriptografskom procesu jedan ključ služi za šifrovanje (zaključavanje) poruke, a drugi za dešifrovanje (otključavanje) poruke. Usled korišćenja dva ključa, taj metod se naziva asimetrična kriptografija (engl. *asymmetric cryptography*). Šifrovanje podataka u javnoj kriptografiji vrši se javnim ključem primaoca poruke. Dešifrovanje poruke nije moguće izvršiti istim javnim ključem. Dešifrovanje se vrši komplementarnim privatnim ključem primaoca.

Svi kriptosistemi ove vrste baziraju se na istoj ideji sigurnosti: nemogućnosti određivanja privatnog ključa za poznati javni ključ, bez obzira na tehničke resurse, vreme i metode koje se koriste. U ovom sistemu svaki učesnik ima svoj par privatnih i javnih ključeva.

²²² Isto, str.64

Tabela 15: Koraci u primeni metoda asimetričnih ključeva²²³

1. korak - pošiljalac formira digitalnu poruku	Poruka može da bude dokument, tabela ili digitalni objekat
2. korak - pošiljalac koristi primaočev javni ključ iz javnog direktorijuma i primenjuje ga na poruku	Javni ključ je dostupan u okviru sertifikata
3. korak - primena primaočevog javnog ključa omogućava šifrovanje poruke	Poruka koja je jednom šifrovana pomoću javnog ključa ne može da se dešifruje primenom istog ključa. Proces je nepovratan.
4. korak - šifrovana poruka se šalje preko Interneta	Šifrovana poruka se prenos sistemom paketske komutacije preko Interneta
5. korak - primalac koristi svoj privatni ključ za dešifrovanje poruke.	Dešifrovanje može obaviti samo onaj ko poseduje taj privatni ključ – pravi primalac poruke.

Asimetrični ključevi obezbeđuju jednostavniju realizaciju funkcija privatnosti, autentifikacije i neporicanja. U poređenju sa simetričnim sistemima oni rade sporije. Tajnost asimetričnih sistema se ne može matematički dokazati kao kod simetričnih sistema.

3.3. Asimetrična kriptografija upotrebom digitalnog potpisa i hash funkcije

Upotreba računara i telekomunikacija dovele su do potrebe uvođenja digitalnog potpisa kao zamene za funkciju svojeručnog potpisa (engl. *written signature*) u uslovima tradicionalnog bankarskog poslovanja.

U realnom svetu se kao potvrda validnosti dokumenata uobičajeno koristi svojeručni potpis. U „digitalnom svetu“ i on-lajn komunikacijama njemu odgovara digitalni potpis, koji je u stanju da garantuje proveru integriteta dokumenta i njegovog porekla (autora), kao i njegovu neporecivost. Digitalni potpis je način da se sa velikim poverenjem i sigurnošću omogući da primljena poruka zaista potiče od onoga ko se prikazuje kao njen pošiljalac. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca) i da obezbedi garantovanje identiteta pošiljaoca poruke. Ovakav potpis se može u pravnim postupcima i radnjama smatrati digitalnim ekvivalentom svojeručnog potpisa na papirnom dokumentu. Ova izvanredna karakteristika čini digitalni potpis upotrebljivim u mnogim aplikacijama za e-Banking, e-Business, e-Commerce, e-Government itd. Mada treba da obezbedi elemente zaštite analogno svojeručnom potpisu, digitalni potpis nije elektronski zapis običnog potpisa. Smatra se čak da potenciranje potrebe pravljenja analogije između pravnih propisa koji regulišu funkcionisanje digitalnog i svojeručnog potpisa, deluje kao kočnica razvoja elektronskog bankarstva, jer između njih postoje bitne razlike.

Digitalni potpis je kriptografska tehnika kojom se elektronski dokument prvo hashuje (izračunava se sažeti dodatak poruke), a zatim se dobijeni hash šifruje privatnim ključem pošiljaoca.

²²³ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.246

Samo pravi pošiljalac može da upotrebi svoj privatni ključ i potpiše poruku, a samo pravi primalac može svojim privatnim ključem da dešifruje šifrovanu poruku.

Pošto digitalni potpis kombinuje dve tehnike (privatni ključ i hash funkciju), on se koristi za:

1. proveru integriteta poruke,
2. proveru autentičnosti porekla i
3. obezbeđenje neporicanja poruke.

Digitalni potpis se smatra najvišim stepenom zaštite.

Tabela 16: Koraci u primeni metoda digitalnog potpisa i hash funkcije²²⁴

1. korak-pošiljalac formira originalnu poruku.	Poruka može da bude bilo koji digitalni fajl
2. korak-pošiljalac primenjuje hash funkciju i dobija 128-bitni hash rezultat.	Hash funkcija sažima poruku
3. korak-pošiljalac šifruje dobijeni hash RSA algoritmom (asimetrični) svojim privatnim ključem za digitalno potpisivanje	Digitalno potpisani hash može da se proveriti samo primenom javnog ključa pošiljaoca
4. korak-pošiljalac šifruje poruku i digitalni potpis (najčešće simetričnim)	Primalac dobija zaštićeni fajl koji može da dešifruje
5. korak-rezultat tog duplog šifrovanja se šalje preko Interneta. Primalac koristi odgovarajući ključ za dešifrovanje dobijenog	Poruka proputuje Internet kao serija nezavisnih paketa.
6. korak-primalac koristi pošiljaočev javni ključ da bi autentifikovao poruku – proverio digitalni potpis	Poruku je mogao da pošalje samo imalac digitalnog potpisa – pravi pošiljalac.

Takva primena asimetrične kriptografije uz hash funkciju i digitalni potpis mnogo je realnija, jer obezbeđuje poverljivost poruke i autentičnost pošiljaoca. Naime, samo pravi pošiljalac može da upotrebi svoj privatni ključ i potpiše poruku – samo pravi primalac svojim privatnim ključem može da dešifruje kriptovanu poruku.

Ova tehnologija je posebno važna za zaštitu podataka na Internetu. Od razrešenja ovih problema (zaštite podataka) će zavisiti razvoj poslovanja na Internetu.

3.4. Digitalne koverta

To je tehnika simetrične kriptografije koja se koristi za šifrovanje i dešifrovanje, najčešće velikih dokumenata. Kod ovog sistema asimetrična kriptografija (metod javnih ključeva) koristi se za šifrovanje i slanje simetričnog tajnog ključa. Cilj ovakve kombinacije je korišćenje prednosti i simetrične i asimetrične kriptografije, odnosno i brzina simetrične i fleksibilnost asimetrične kriptografije. Pošiljalac šifruje dokument pomoću simetričnog

²²⁴ Isto, str.247

ključa koji će primalac koristiti za dešifrovanje dokumenta. Simetrični tajni ključ se generiše na predajnoj strani i šifrjuje se upotrebom javnog ključa primaoca i time dobija digitalna koverta („ključ u ključu“). Kada primalac preko Web-a primi digitalnu kovertu, najpre koristi svoj privatni ključ da bi dešifrovao simetrični ključ, a zatim simetrični ključ da bi dešifrovao tekst dokumenta. Ušteda u vremenu se bazira na činjenici da su i šifrovanje i dešifrovanje brže kada se koristi simetrični ključ. Slabost ove tehnike je u tome što se simetrični ključ prenosi komunikacionom kanalom.²²⁵

3.5. Digitalni sertifikat i infrastruktura javnih ključeva

Digitalni sertifikati i infrastruktura kojom se podržavaju javni ključevi, pokušaj su da se reši problem digitalnog identiteta. Suština ovog rešenja bazira se na javnim ključevima i procedurama digitalnog potpisivanja koji su opšte prihvaćeni. Ključni elementi ove infrastrukture su: sertifikaciona tela, registraciona tela i digitalni sertifikat.²²⁶

Sertifikaciona tela su institucije od poverenja (engl. *Certification Authority*) tzv. ovlašćena treća strana. U SAD privatna korporacija *VeriSign* i vladina agencija *US Postal Services*, deluju kao takva tela.

Registraciono telo je institucija čiji je zadatak da prihvata zahteve korisnika za izdavanje sertifikata, vrši proveru identiteta korisnika i prosleđuje zahtev sertifikacionom telu u određenom formatu. Ona uspostavlja vezu između korisnika i sertifikacionog tela. Kvalitet načina provere identiteta podnosioca zahteva, određuje nivo poverenja koji se ugrađuje u sertifikacioni zahtev.

Digitalni sertifikat je digitalni dokument koji izdaje ovlašćeno sertifikaciono telo i koji sadrži ime subjekta, ili privrednog društva, javni ključ subjekta, serijski broj digitalnog sertifikata, datum izdavanja i rok važenosti sertifikata kao i ostale informacije potrebne za identifikaciju. Svi navedeni podaci su digitalno potpisani od strane sertifikacionog tela i sastavni su deo sertifikata.

Procedura izdavanja sertifikata počinje sa upućivanjem zahteva korisnika, sertifikacionom telu za izdavanje sertifikata. Tom prilikom on pravi kombinaciju privatnog i javnog ključa. Sertifikaciono telo sačinjava sertifikat koji sadrži korisnikov javni ključ i ostale potrebne informacije, šalje poruku (slično hash funkciji) i potpisuje je svojim privatnim ključem. Tako se dobija potpisani sertifikat koji predstavlja jedinstveni šifrovani dokument.²²⁷

U svetu može da postoji samo jedan isti potpisani sertifikat.

Razvijene zemlje se bave pitanjima zakonodavnog regulisanja kriptografskih tehnika i primene digitalnog potpisa. Na primer, još 1997. godine EU je najavila svoju politiku primene kriptografske tehnike i digitalnog potpisa. Takođe, članice Unije do jula 2001. godine trebalo je da donesu sopstvene propise o elektronskom potpisu. U SAD usvojena je Preporuka o digitalnim potpisima. Politikom primene digitalnog potpisa i kriptografskih tehnika bave se i međunarodna tela i organizacije. OECD je 1997. godine usvojila preporuke za politiku o

²²⁵ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.67

²²⁶ Isto, str.68

²²⁷ Isto, str.69

kriptografiji, a OUN i Međunarodna trgovinska komora iz Pariza, preporučuju svim zemljama da se pri izradi svojih propisa iz oblasti elektronskog poslovanja i elektronskog potpisa rukovode njihovim predlozima.²²⁸

Na nacionalnom nivou, zemlje nastoje da donesu sopstvene zakone o digitalnom potpisu. U Srbiji je krajem 2004. godine donet Zakon o elektronskom potpisu,²²⁹ a 2009. godine Zakon o elektronskom dokumentu.²³⁰

U Zakonu se na sledeći način definišu neki osnovni pojmovi i određuje njihov sadržaj i upotreba:

- Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
- Kvalifikovan elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih poruka ili dokumenata i nemogućnost naknadnog poricanja odgovornosti za njihov sadržaj. To je skup numeričkih podataka kojima se na kriptografski pouzdan način utvrđuje veza između sadržaja elektronskog dokumenta i identiteta njegovog potpisnika. On ima isto pravno dejstvo i dokaznu snagu u odnosu na podatke u elektronskom obliku, kao i svojeručni potpis i pečat u odnosu na podatke u papirnom obliku. Za realizaciju takvog pravnog dejstva on mora da ispunji sledeće uslove: da je isključivo povezan sa korisnikom, da nedvosmisleno identifikuje korisnika, da nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod njegovim nadzorom, da je direktno povezan sa podacima na koje se odnosi, da je formiran sredstvima za formiranje kvalifikovanog elektronskog potpisa i da se proverava na osnovu kvalifikovanog elektronskog sertifikata korisnika.
- Elektronski sertifikat je elektronski dokumenat kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;
- Kvalifikovani elektronski sertifikat je elektronsko uverenje kojim se jednoznačno utvrđuje identitet ovlašćenog učesnika elektronskog poslovanja. Izdaje ih ovlašćeno sertifikaciono telo. To može da bude svako pravno lice koje ispunjava uslove koji su predviđeni tim zakonom. Vlada određuje nadležni organ za akreditaciju i praćenje rada sertifikacionih tela koji vodi i registar akreditovanih sertifikacionih tela za elektronsko poslovanje i kontroliše njihov rad. Vlada određuje i naknadu za akreditaciju sertifikacionih tela. Kvalifikovani elektronski sertifikat sadrži podatke predviđene zakonom i to: jednoznačni identifikator vlasnika sertifikata, naziv sertifikacionog tela koje je izdalo sertifikat, datum izdavanja i rok važenosti sertifikata, serijski broj sertifikata, javni ključ vlasnika, kvalifikovani elektronski potpis sertifikacionog tela-izdavaoca sertifikata. Oni mogu da se izdaju na različitim elektronskim medijima: smart-karticama, disketama itd., mada savremeni sistemi javnih ključeva u svetu najviše koriste smart kartice kao medijume za izdavanje elektronskih sertifikata. Posedovanje ovog sertifikata je neophodno za formiranje kvalifikovanog elektronskog potpisa. Kvalifikovani elektronski sertifikati inostranih sertifikacionih tela ravnopravni su sa domaćim, ukoliko je inostrano sertifikaciono telo registrovano od strane nadležnog organa.
- Čuvanje izdatih sertifikata je takođe definisano. Vlasnik kvalifikovanog elektronskog sertifikata (*KES*) mora da čuva podatke i sredstva za elektronsko poslovanje i

²²⁸ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.251

²²⁹ „Sl.glasnik RS“, br. 135/04

²³⁰ „Sl.glasnik RS“, br. 51/09

verifikaciju kvalifikovanih elektronskih potpisa, da ih koristi prema zakonu i da spreči neovlašćeni pristup tim podacima i sredstvima. Sertifikaciono telo mora da čuva kompletnu dokumentaciju o izdatim i opozvanim sertifikatima – radi dokaznog materijala i verifikacije u sudskim, upravnim i drugim postupcima – najmanje pet godina od njihovog izdavanja. Prema tome, za obavljanje elektronskog poslovanja učesnici moraju da poseduju kvalifikovane elektronske sertifikate i računarsku opremu (hardver i softver):

- a) za kreiranje i čuvanje elektronskih dokumenata, za slanje i prijem elektronskih poruka (personalni računar i odgovarajući sistemski i komunikacioni softver) i
- b) za generisanje i verifikaciju elektronskih potpisa (hardver i softver za generisanje i verifikaciju elektronskog potpisa).

Zakon o elektronskom potpisu definiše i proceduru za osnivanje sertifikacijske ustanove u Srbiji (Institut za standardizaciju Srbije), kao i zadatke sertifikatora, kao što su:²³¹

1. Izdavanje sertifikata
 - kreiranje javnog i tajnog ključa,
 - primanje zahteva za izdavanje sertifikata,
 - utvrđivanje identiteta tražioca,
 - izdavanje sertifikata,
 - upis u bazu podataka sertifikata.
2. Opoziv sertifikata
 - suspenzija ako tajni ključ bude poznat svima,
 - ukidanje,
 - upis u bazu podataka suspendovanih ili ukinutih.

3.5.1. Infrastruktura kriptografije sa javnim ključem

Osim sintagme „digitalni sertifikat“, neophodno je da se razjasni sintagma „infrastruktura kriptografije sa javnim ključem“ jer je relativno nova i različito se tumači u novijoj literaturi. Infrastruktura javnih ključeva (engl. *Public Key Infrastructure - PKI*) je skup postupaka, dokumenata, resursa i aplikacija koje formiraju specifičan okvir za uspostavljanje digitalnog identiteta osobe, kao i za njegovo administriranje, upravljanje i nadzor tokom životnog ciklusa. PKI omogućava učesnicima, koji se uobičajeno i ne moraju unapred poznavati, da međusobno uspostave sa poverenjem međusobnu elektronsku komunikaciju, zasnovanu na međusobnoj autentifikaciji, verifikaciji digitalnog potpisa i poverljivosti. Ponekad se sistem javnih ključeva opisuje kao jednostavna hijerarhija poverenja zasnovana na kriptografiji sa javnim ključem, a ponekad kao kriptografski sistem sa mogućnošću digitalnog potpisivanja krajnjih korisnika. U stvari, pod PKI podrazumevaju se servisi i protokoli za upravljanje ključevima, a sastoji se od komponenata koje ne koriste uvek kriptografske operacije pomoću ključeva. Osnovne komponente PKI sistema su sledeće:

- sertifikaciono telo ili autoritet od poverenja (engl. *Certification Authority*);
- registraciono telo (engl. *registration Authority*).

Servisi koji se često mogu naći u PKI sistemu su:²³²

²³¹ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit.delo, str.311

- registracija ključa (izdavanje novog sertifikata za javni ključ);
- povlačenje sertifikata (poništanje prethodno izdatog sertifikata);
- izbor ključa (generisanje javnog ključa korisnika);
- procena poverenja (određivanje validnosti sertifikata i skupa autorizovanih operacija);
- rekonstrukcija ključa (ponovno izračunavanje para ključeva).

Funkcionisanje PKI sistema zasniva se na osnovnom dokumentu sistema (engl. *Certificate Practice Statements - CPS*). To je dokument koji sadrži i detaljan opis svih procedura značajnih za funkcionisanje PKI sistema, kao i bezbednosnu politiku koja se primenjuje. Tipično, tim dokumentom se propisuje rad sertifikacionog tela,²³³ način rada sa digitalnim sertifikatima (način izdavanja i povlačenja, izrada lista povučenih sertifikata) i način rada sa kriptografskim ključevima (generisanje, čuvanje i izdavanje korisnicima).

Sistem PKI obezbeđuje pouzdano okruženje za realizaciju četiri osnovne funkcije zaštite komercijalnih i poslovnih transakcija: autentičnost strana u komunikaciji, integritet poruka, nemogućnost naknadnog poricanja transakcija i zaštitu tajnosti podataka. Prve tri funkcije se ostvaruju na osnovu tehnologije digitalnog potpisa, primenom asimetričnih šifarskih sistema, dok se funkcija zaštite tajnosti najčešće realizuje primenom simetričnih šifarskih sistema.²³⁴

Primeri zaštićenih PKI aplikacija su: zaštićene Web transakcije, zaštićeni e-mail servis, zaštićen FTP servis, bezbedno upravljanje dokumentacijom, bezbedna funkcija kontrole pristupa i bezbedni sistem elektronske trgovine i plaćanja.

Sistem PKI s digitalnim sertifikatima mnogo je skuplji za implementaciju od tradicionalnih metoda autentifikacije, kao što su lozinke i PIN-ovi, ali njegova cena drastično pada uporedo sa sazrevanjem tehnologije.

4. ZAŠTITA NA TEHNIČKOM NIVOU

Osnovni problem sigurnosti na Internetu je što je on projektovan da bude koristan, a ne da bude siguran. S obzirom na to da je razvijen u akademskom okruženju da bi se istraživačima omogućila razmena informacija nije mnogo vođeno računa o sigurnosti. Tek razvojem poslovanja na Internetu nametnut je problem sigurnosti, a uvođenje na scenu različitih tipova korisnika problem sigurnosti je postao dominantan.

Najčešći oblici napada na računarske mreže Internet/Intranet tipa su:²³⁵

- Prisluškivanje - neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama.
- Lažno predstavljanje - neautorizovani pristup podacima ili kreiranje neautorizovanih podataka.
- Napad tipa ukidanja servisa (engl. *denial-of-service*) - onemogućavanje funkcionisanja mrežnih servisa i resursa.

²³² Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.252

²³³ Institut za standardizaciju Srbije – www.jus.org.yu

²³⁴ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.253

²³⁵ Vasković V.: „Sistemi plaćanja u elektronskom poslovanju“, cit.delo, str.312

- Ponavljanje poslatih poruka - neovlašćena kontrola komunikacije subjekata i ponavljanje, izmena ili sprečavanje prenosa podataka.
- Pogađanje lozinke - neovlašćeni pristup podacima uz pomoć otkrivene lozinke.
- Kriptoanaliza - otkrivanje tajnih ključeva - otkrivanje podataka u otvorenom obliku na bazi šifrata i otkrivenog tajnog ključa.
- Napadi tipa „Trojanski konj“ - distribucija zlonamernih programa na radne stanice.
- Virus - uništenje podataka.

Da bi se obezbedio potreban nivo zaštite celokupnog E-commerce poslovanja potrebno je da celokupan sistem, od korisnika do trgovaca i banke, bude zaštićen i obezbeđen od napada. Zaštita jednog dela poslovanja i neobebeđenost ostalih delova, dovodi do kompromitovanja čitavog posla.

4.1. Alati za zaštitu na nivou Internet komunikacionih kanala

Postoji više alata koji se koriste za obezbeđenje komunikacionih kanala na Internetu. To su:²³⁶

1. zaštitni omotač jezgra (engl. *Secure Socket Layer - SSL*), kao najčešća forma obezbeđivanja Internet servisa. Taj protokol obezbeđuje šifrovanje podataka, autentifikaciju servera, autentifikaciju klijenta i integritet poruke za TCP/IP konekcije;
2. S-HTTP (engl. *Secure Hypertext Transfer Protocol*), koji obezbeđuje samo Web protokole i ne može da se koristi za obezbeđenje poruka koje nisu HTTP;
3. virtuelne privatne mreže (engl. *Virtual Private Network - VPN*), koje omogućavaju udaljenim korisnicima siguran pristup unutrašnjoj mreži preko Interneta pomoću *Point-to-Point Tunneling Protokola* (PPTP), mehanizma za kodiranje koji omogućava da jedna lokalna mreža uspostavi vezu sa drugom uz korišćenje Interneta kao medijuma (kanala).

4.2. Alati za zaštitu na nivou mreža, servera i klijenata

Pošto su obezbeđeni komunikacioni kanali, treba obezbediti alate kojima će se zaštititi mreže, serveri i klijenti. Ti alati uključuju:²³⁷

1. Zaštitni uređaj (engl. *firewalls*) u vidu softverske aplikacije, koje deluju kao filteri između privatne mreže kompanije i Interneta, sprečavajući da udaljena neovlašćena klijentova mašina napadne internu mrežu kompanije. *Firewalls* prate i vrednuju sve ulazne i izlazne poruke. Svaku poruku obrađuje *firewalls* softver, koji utvrđuje da li zadovoljava ustanovljena načela sigurnosti. Ako zadovoljava, može da dođe u dalju distribuciju po internoj mreži, a ako ne, blokira se.
Postoje dva osnovna metoda koja *firewalls* koriste da bi procenili saobraćaj na mreži: paketski filteri (engl. *packet filters*) i aplikacioni prolazi (engl. *gateways*). Paketski filteri istražuju pakete podataka, da bi odredili da li su usmereni na zabranjeni port, ili da li potiču sa zabranjene IP adrese. To znači da filter proverava izvor i destinaciju informacije, njen port i paketski tip, da bi procenio može li sa se emituje. Aplikacioni prolazi (engl. *gateways*) su tip *firewalls-a*, koji filtriraju komunikacije na osnovu tražene aplikacije, a ne prema izvoru ili destinaciji poruke.

²³⁶ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.254

²³⁷ Isto, str.255

2. proxy – softverske servere, koji prvenstveno deluju tako da spoljašnjim Internet servisima ograniče mogućnost pristupa unutrašnjim klijentima i često se definišu kao prolazi (engl. *gateway*);
3. kontrola operativnih sistema (engl. *Operating System Controls*), što znači ugradnju korisničkog imena (engl. *username*) i lozinke (engl. *password*), koji garantuju određeni nivo autentifikacije. Neki operativni sistemi imaju funkciju kontrole pristupa (engl. *Access Control Function*), odnosno kontrolišu korisnički pristup na različitim područjima mreže.
4. anti virus softver, tj. jeftin i lak način da se identifikuju i spreče najčešći tipovi virusa koji ulaze u računar, kao i da se unište oni, koji su već na hard disku računara.

4.3. Protokoli

Protokol označava skup pravila koja definišu kako dva programa mogu da uspostave komunikaciju, da se ta komunikacija održi određeno (potrebno) vreme i da se po potrebi prekine. Svaki protokol radi transparentno sa ostalim protokolima u sistemu. Svi protokoli mogu se grupisati u tri kategorije: protokole za transport, za mrežu i za aplikaciju. Najniži nivo su fizički protokoli koji uključuju aktuelna sredstva za prenos podataka, dok su na najvišem nivou aplikacioni protokoli čije funkcionisanje zavisi delimično i od korisnika. U svojoj celini, oni čine protocol stok. U daljem tekstu dat je pregled najznačajnijih protokola.²³⁸

- FTP (engl. *File Transfer Protokol*) je protokol za prenos datoteka sa jednog umreženog računara na drugi, korišćenjem TCP/IP protokola. Nastao je pre Web-a i veoma je dobro sredstvo za preuzimanje (engl. *download*) datoteka sa internetovih FTP mesta (engl. *FTP Site*).
- TCP/IP (engl. *Transmission Control Protocol/Internet protocol*) je protokol za kontrolu prenosa i usmeravanje i isporuku poruka. Koriste ga gotovo sve računarske mreže koje su na Internetu kao i lokalne mreže za prenos podataka između računara i servera. Zbog velike ekspanzije postaje sve problematičniji i trenutno je u fazi izrade njegova verzija.
- S-HTTP (engl. *Hyper Text Transfer Protokol*) obezbeđuje samo Web protokole i ne može se koristiti za obezbeđenje poruka koje nisu HTTP (protokol za razmenu hipertekstualnih fajlova, odnosno za prenos Web stranica od servera do klijenta).
- Protokol SSL (engl. *Secure Socket Layer - SSL*) u prevodu znači zaštitni omotač jezgra. Danas je široko prihvaćen. Zasniva se na upotrebi asimetričnog sistema šifriranja (parova privatnih i javnih ključeva). Obezbeđuje potrebnu zaštitu poverljivosti podataka za vreme njihovog prenosa nezavisno od aplikativne funkcije. Relativno je jednostavniji. Međutim, pomoću njega se ne obezbeđuje autentifikacija učesnika u transakciji.
- SET protokol (engl. *Secure Electronic Transaction*) je koncipiran u cilju prevazilaženja problema koji mogu proizaći iz upotrebe SSL protokola. Nastao je kao rezultat zajedničke saradnje Visa i Master Card-a. Bazira se na upotrebi sistema kriptografije sa digitalnim potpisom javnim ključem i autentifikaciji, korišćenjem digitalnih sertifikata svih učesnika. U sebi sadrži podprotokole za: (1) autorizaciju plaćanja i integritet podataka, (2) proveru sertifikata i (3) naručivanje robe i usluga. Pruža veće mogućnosti zaštite, ali zahteva i dodatne elemente u infrastrukturi. Prema

²³⁸ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.71

prvobitnoj verziji, protokol obezbeđuje poverljivost, integritet, autentifikaciju računa korisnika karte, autentifikaciju prodavaca i interoperabilnost sistema. Teorijski je gotovo perfektan, ali veoma kompleksan. Znatno viši stepen privatnosti postiže se procedurom dvostrukog potpisa (engl. *dual signature*), gde informacije sa kreditne karte kupca ostaju nepoznate prodavcu, a informacije o naručivanju nepoznate banci.

- SMTP (engl. *Standard Mail Transfer Protocol*) - standardni protokol za prenos pošte putem Intraneta i Interneta.

Elektronsko poslovanje nesporno je donelo mnoge „blagodeti“, ali i brojne opasnosti. Što je njegov rast i zastupljenost veća, to su i posledice zloupotrebe teže. U zemljama u kojima se ovaj oblik poslovanja nalazi u stalnoj ekspanziji, preduzimaju se mnogobrojne aktivnosti u zaštiti, ali i hvatanju i kažnjavanju onih kojima zloupotrebe postaju „zanimanje“.

PETI DEO

PRAVNA REGULACIJA E-POSLOVANJA

1. PRAVNI OKVIR

Rast koji je u nekoliko poslednjih godina doživelo elektronsko poslovanje u odnosu na klasične tipove poslovanja, prouzrokovao je promene pravila poslovanja i njegove regulacije.

Kako elektronsko poslovanje omogućava izvršavanje klasičnih poslovnih zloupotreba kao što su prevare, finansijske malverzacije, ili izbegavanje plaćanja poreza na nov način, potrebno ga je posebno regulisati, jer se pravila i kontrolni mehanizmi klasičnog poslovanja ne mogu primeniti. Međutim, to nije tako jednostavno, prvenstveno zato što je ovo nova oblast poslovanja koja je u stalnim i brzim promenama. Pored toga, tehnologija koja se primenjuje nije ograničena samo na jedan region, ili zemlju. To opet, sa svoje strane dovodi do problema na koji postojeći pravni sistemi ne daju zadovoljavajuće odgovore, pošto je njihovo važenje ograničeno teritorijom države u kojoj se primenjuje. Izlaz je pokušao da se nađe u međunarodnim organizacijama i telima kao što su Ujedinjene nacije, Svetska trgovinska organizacija, ili u okviru regionalnih ekonomskih integracija, kao što je Evropska unija. Sporost u dogovaranju koja je posledica usaglašavanja stavova između zainteresovanih država, prouzrokuje relativnu neefikasnost ovih tela. Pored toga, njihove odluke su obavezne samo za one države koje su se izjasnile da ih prihvataju. Međutim, potrebe za smanjenjem troškova poslovanja i želja za povećanjem tržišta koja je sublimirana u elektronskom poslovanju, dovela je do toga da mnoge razvijene zemlje ubrzano pristupaju njegovom regulisanju.

Ulogu međunarodnih organizacija vezanu za elektronsko poslovanje, može da, najbolje ilustruje OECD koji je 1996. godine doneo izveštaj pod nazivom „Globalna informaciona infrastruktura – globalno informaciono društvo“ prvenstveno namenjen vladama članicama, ali zahvaljujući uticaju koji ima. U Izveštaju se ističe globalni karakter elektronskog poslovanja i sugeriše vladama, uvažavajući sve političke i pravne razlike između država, da podrže digitalno poslovanje, stvarajući uslove uz što manje povećanje regulacije. Kako nacionalna zakonodavstva nisu i neće biti direktno primenjiva u svim oblastima *cyberspace* poslovanja, potrebno je regulaciji ovog područja pristupiti putem samoregulacije. Naročitu pažnju treba obratiti sigurnosti i autentičnosti elektronskih dokumenata koja se razmenjuju između subjekata iz različitih država, kako bi ona bila pravno valjana. OECD predlaže da se što pre dođe do zajedničkih stavova vezanih za legalnost elektronskih dokumenata putem elektronskog potpisa.²³⁹

Postavlja se pitanje, čije pravne norme će se koristiti u slučaju spora u prekograničnom prometu robe i usluga putem mreže? Nalaženjem rešenja za ovaj problem, sigurno će pozitivno uticati na uspeh elektronskog poslovanja. Jedno od rešenja bi moglo biti da je za pravne posledice proizašle iz ugovora koji se odnose na elektronsko poslovanje, nadležan pravni sistem sa teritorije gde se nalazi prodavac. Problem se uslođnjava kada se posao vodi u nekoliko zemalja. Takođe se postavlja pitanje, da li je sedište prodavca u elektronskom poslovanju tamo gde je lociran server sa koga on nudi svoju robu i usluge ili negde drugde. U globalnom elektronskom poslovanju uobičajeno je da organizacija u nekoj zemlji ima server i ništa više, to je naročito izraženo kod „virtualnih organizacija“ koje sigurno ne potpadaju ni pod jedan geografski ograničen pravni sistem.

²³⁹ Drakulić M.: „Pravna regulacija e-poslovanja“, www.e-trgovina.co.yu/pravo/regulacija1.html

Regulisanje pravnih aspekata elektronskog poslovanja je veoma značajno, jer ovaj vid poslovanja direktno dovodi u pitanje funkcionisanje tradicionalnih pravnih rešima koji su zasnovani na pravilima pismene evidencije, postojanju originalnih potpisanih dokumenata i sličnim faktorima koji nemaju svoje ekvivalente u domenu elektronskog poslovanja.

Za domen je bitna i činjenica da elektronske tehnologije čini teritorijalne granice nerelevantnim, što takođe potkopava temelje tradicionalne pravne regulative, zasnovane na teritorijalnom principu. U sajber-prostoru postaje teško utvrditi da li se transakcija stvarno odigrala i u čijoj je pravnoj nadležnosti. Ovo je posebno problem u *business to consumer* elektronskim transakcijama, jer u *business to business* transakcijama nadležno je zakonodavstvo koje se primenjuje na zaključeni poslovni ugovor. Prema zakonskom predlogu EU (novembar 1998.), kompanije koje nude *online* usluge biće regulisane po zakonodavstvu zemlje u kojoj su osnovane (*country of origine*), a ne, na primer, po zakonodavstvu zemlje u kojoj je lociran host ili računar, ili prema zakonu zemlje u kojoj se usluga prima. Osim pravne jurisdikcije, na listi zakonskih dilema su i sledeća pitanja:

- privatnost informacija,
- utvrđivanje identiteta,
- sigurnost transakcije,
- sertifikacija i slično.

Izgradnju pravne regulative za elektronsko poslovanje možemo posmatrati na nacionalnom, regionalnom i međunarodnom nivou.

Što se nacionalnog nivoa tiče, može se reći da potpuno adekvatna zakonska regulativa za elektronsko poslovanje praktično još uvek ne postoji ni u većini razvijenih zemalja najvećih korisnika elektronskih tehnologija, a da se zemlje u razvoju i zemlje u tranziciji još uvek nalaze na samom početku izgradnje legislative u ovom domenu. Kao polazište za izgradnju nacionalne ET regulative može da posluži Model zakon za ET koji je 1996. godine razvila Komisija UN za međunarodno trgovinsko pravo (*UNCITRAL*). Model pruža set međunarodno prihvatljivih pravila za nacionalne vlade u domenu elektronske trgovine. Za mikronivo-privredna društva, Model daje instrukcije za izradu ugovora o ET sa drugim partnerima.²⁴⁰

Na nacionalnom nivou u pogledu načina na koji bi se pravno uredili odnosi koji nastaju kada se poslovna transakcija zaključuje korišćenjem računara, postoje razne mogućnosti kao što su:

- dopuna relevantnih zakona odredbama koje bi ukazale na pravnu valjanost dokumenata koji je dostavljen elektronski,
- doneti jedinstven zakon (po Model zakonu) koji bi regulisao osnovna pitanja vezana za elektronski model zaključivanja posla u međunarodnom i unutrašnjem prometu,
- kombinacija oba načina u meri u kojoj je to potrebno.

U okviru pravnog regulisanja na međunarodnom nivou, najznačajnije je doći do prihvatljivih pravila za legalnu valjanost elektronskog izvora i autentifikaciju elektronske procedure, kao i o drugim značajnim pitanjima na kojima rade međunarodne institucije kao što su *UN/ECE*, *FAN*, *UNCITRAL*, *WTO*, *ISO* i dr.²⁴¹

²⁴⁰ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.354

²⁴¹ Isto, str.354

1.1. Izgradnja pravne regulative u razvijenim zemljama

Razvijene zemlje, kao najveći korisnici elektronskog poslovanja, sigurno su i najaktivnije u svim oblastima razvoja i podrške uvođenju elektronskih transakcija, pa i u izgradnji pravnog okvira.

SAD su još 1977. godine donele Okvir za globalnu ET kao strategiju američke administracije po pitanjima podrške i daljeg razvoja elektronske trgovine. Stav administracije je još tada bio da Internet kao medijum mora delovati bez nepotrebne regulative, u kome konkurencija i izbor potrošača oblikuju tržište.

U tom smislu, definisani su principi delovanja i to:²⁴²

- privatni sektor ima odlučujuću ulogu u razvoju Interneta,
- potrebno je izbegavati uvođenje restrikcija,
- uloga države jeste da osigura konkurenciju, zaštiti intelektualnu svojinu i privatnost, spreči prevare, omogući transparentnost, olakša rešenje sporova u online transakcijama,
- neophodno je revidirati zakone i regulativu koja odgovara novoj elektronskoj eri,
- elektronska trgovina mora biti regulisana na globalnoj osnovi nezavisno od lokalne jurisdikcije.

Sprovođenje navedenih principa nije nimalo lako i ono zahteva delovanje u više različitih oblastima:

- carine i porezi – formiranje globalne slobodne zone trgovanja (*global - free zone*);
- elektronski sistem plaćanja – rešavanje problema tehnikom slučaj po slučaj;
- razviti uniformni zakon za ET – primeniti načelo autonomije volje;
- zaštita intelektualne svojine – uz primenu dozvola (*copyright*), patenata i tržišnih tajni, što mora sprečiti pirateriju i prevaru;
- privatnost;
- sigurnost;
- razvoj telekomunikacione infrastrukture;
- uklanjanje nekarinskih barijera;
- razvoj tehničkih standarda.

U Evropi, svest o značaju informacionog društva i potrebi izgradnje jedne koherentne politike u tom domenu inicirana je 1993. godine izlaskom tzv. Belog papira Evropske Komisije „Rast, konkurentnost i zaposlenost“. On je ukazao na značaj informacionog društva za dalji ekonomski rast Evropske unije, nivo njene konkurentnosti, potrebu kreiranja novih radnih mesta i uopšte unapređenja kvaliteta života i nivoa životnog standarda njenih stanovnika. Kao reakcija na Beli papir, Grupa za informaciono društvo (engl. *High level group on information society*) sačinila je izveštaj pod nazivom „Evropa i globalno informaciono društvo“. Izveštaj daje uputstva i preporuke kako da Evropska Unija sačini povoljan regulatorni, tehnološki i socijalni okvir za razvoj informacionog društva. Ovo je bila osnova koja je omogućila da se juna 1994. godine usvoji prvi akcioni plan EU za razvoj informacionog društva pod nazivom „Evropski put u informaciono društvo“.

²⁴² Isto, str.355

Glavni ciljevi ovog akcionog plana bili su sledeći:²⁴³

- ubrzati punu liberalizaciju telekomunikacionih usluga i infrastrukture, koja je i ostvarena 1998. godine;
- ojačati i preusmeriti ICT istraživačke programe;
- uključiti novu dimenziju informacionog društva u sve relevantne komunitarne politike.

Revidirana verzija ovog Akcionog plana usvojena je 1996. godine.

Takođe, Evropa je da bi podržala rast ET u svom regionu i da bi definisala buduće aktivnosti Evropske Komisije u ovom domenu, usvojila je 1997. godine Evropsku inicijativu u elektronskoj trgovini. Inicijativa definiše i četiri principa delovanja u domenu adaptacije evropskog regulatornog okvira za realizaciju elektronskih transakcija.

To su sledeći principi:

- izbegavati nepotrebnu i suvišnu regulativu,
- svaka regulativa mora bazirati na četiri slobode jedinstvenog tržišta,
- regulativa mora uvažiti poslovne realnosti,
- regulativa mora zadovoljiti opšte interese.

Uprkos uspehu u prvoj fazi, Evropi je postalo jasno da su novi podsticaji razvoju savremenih ICT tehnologija neophodni, kao i nova vizija u tom domenu. Globalno informaciono društvo je u svetu postajalo realnost, u koju se Evropa trebala uklopiti na što bolji način uz maksimalnu koordinaciju politika u svojim zemljama članicama. Realizaciji ovog cilja trebalo je da doprinese inicijativa usvojena decembra 1999. godine, pod nazivom eEurope – Informaciono društvo za sve (engl. *An Information Society for All*).

Inicijativa eEurope je lansirana 8. decembra 1999. godine, a ciljevi su bili definisani na sledeći način:²⁴⁴

- podići nivo primene digitalne tehnologije širom Evrope,
- obezbediti da svi Evropljani imaju potrebna znanja za upotrebu ove tehnologije,
- u programu ekonomske i socijalne obnove Evrope, aktivnostima vezanim za eEvropu dati centralno mesto.

Usvajanjem ove Inicijative, evropski lideri su potvrdili svoje opredeljenje da Evropu transformišu u dinamično i konkurentno tržište. Značajan podsticaj u tom pravcu se očekuje od tržišta i privatnog sektora, međutim, nadležnosti države ostaju nezamenljive u kreiranju jasnog regulatornog okvira za novu ekonomiju, u domenu obrazovanja stanovništva i u samom procesu uvođenja novih tehnika rada i poslovanja. Veliki značaj ima rukovodstvo, posebno top menadžment koji će Evropu povesti u pravcu e-ekonomije.

Inicijativa eEurope podržana je i od strane Evropskog Saveta koji je u Lisabonu 2000. godine, postavio strateški cilj prema kome bi Evropa trebalo da „do 2010. postane u svetu najkonkurentnija i najdinamičnija ekonomija koja se zasniva na znanju, sa usavršenim modelom zapošljavanja i povećanom socijalnom kohezijom“. Da bi Savet realizovao ovaj cilj

²⁴³ Isto, str.355

²⁴⁴ Isto, str.356

Lisabonske strategije, Evropska komisija dobija zadatak da sačini eEurope akcioni plan, koji je usvojen juna 2000. godine na Evropskom Savetu u Feiri. Plan eEurope 2002 je definisao sve ciljeve koje EU treba da realizuje do 2002. godine i koji su grupisani oko tri glavna cilja.²⁴⁵

1. Jeftiniji, brži i sigurniji Internet:

- jeftiniji i brži pristup Internetu;
- brži Internet za istraživače i studente;
- sigurne mreže i kartice;

2. Investiranje u ljude i njihova znanja i sposobnosti:

- uvesti evropsku omladinu u digitalnu eru;
- upoznati način rada u ekonomiji zasnovanoj na znanju,
- obezbediti učešće svih u e-ekonomiji;

3. Stimulisati upotrebu Interneta:

- ubrzati primenu e-trgovine;
- obezbediti funkcionisanje e-vlade (vlade online): elektronski pristup javnim uslugama;
- obezbediti online rad u zdravstvu;
- definisati evropski digitalni sadržaj za globalne mreže;
- uvesti inteligentni transportni sistem.

Evropski savet je zatražio od Komisije da rezultate ostvarene Akcionim planom eEurope 2002., dalje unapredi i da definiše nova područja delovanja u akcionom planu eEurope 2005. Novi akcioni plan je Komisija usvojila 28. maja 2002. godine, a predstavljen je na zasjedanju Evropskog saveta u Sevilji juna 2002. godine.

Plan eEurope 2005. obuhvata dve grupe aktivnosti koje podstiču jedna drugu. Aktivnosti na strani tražnje imaju za cilj da stimulišu razvoj novih usluga, aplikacija i sadržaja u domenu e-vlade, e-medicine, e-učenja i e-poslovanja. Korišćenje novih servisa i aplikacija zahteva odgovarajuću infrastrukturu. Zato druga grupa aktivnosti na strani ponude ide u pravcu razvoja širokopojasne (engl. *broadband*) infrastrukture i bavi se rešavanjem pitanja sigurnosti te infrastrukture.

Jedan od glavnih ciljeva svih akcija EU u domenu razvoja informacionog društva jeste, osigurati da se prednosti informacionog društva konzistentno i ravnopravno šire u celoj EU. Da bi se to postiglo bilo je neophodno razviti jasan legalni okvir koji bi definisao razvoj i upotrebu novih tehnologija i aplikacija. Ovaj legalni okvir promoviše raspoloživost i pristupačnost Internetu, elektronsku trgovinu i predstavlja zajedničke tehničke standarde u mobilnoj telefoniji (kao što su *GSMN* i *UMTS*), digitalnoj televiziji (kao što je *DVD*) i radiju. Okvir uključuje i odredbe koje se tiču mernih indikatora (engl. *benchmarking*) za informaciono društvo da bi se osiguralo konzistentno finansiranje primene novih alata, razvoj regulative i tehnologije u svim zemljama članicama Unije.

²⁴⁵ Isto, str.356

Regulativa u oblasti telekomunikacija predstavlja ključni deo regulatornog okvira informacionog društva. Telekomunikaciona politika EU je od početka bila orijentisana ka kompletiranju jedinstvenog unutrašnjeg tržišta i ka liberalizaciji infrastrukture i procesa pružanja usluga. Počev od 1. januara 1998. godine puna liberalizacija evropskog telekomunikacionog tržišta je postala realnost. Novi regulatorni paket u oblasti telekomunikacija, Komisija je usvojila 2000. godine da bi dalje podržala konkurenciju u ovom domenu, posebno u lokalnim komunikacijama, a u cilju ostvarenja prednosti za privredu i korisnike. Prema Komisiji, prelazak na novi regulatorni okvir će podržati kontinuirani rast sektora elektronskih komunikacija i posebno širokopojasnih veza, kao glavnog faktora koji može doprineti ostvarenju ciljeva Lisabonske deklaracije EU.

Razvoj elektronske trgovine u EU zavisi od kreiranja takvog legalnog okvira koji će obezbediti značajne pravne garancije za komercijalne transakcije koje se realizuju elektronski i koji će omogućiti slobodno kretanje elektronskih usluga. Pristup EU u ovom domenu balansira između potrebe regulisanja e-trgovine i opasnosti preterane regulacije koja može ugroziti dalji razvoj ovog novog sektora. Više od 15 direktiva, predloga i preporuka pokušavaju da regulišu e-trgovinu kao što su: Direktiva o e-potpisu, Direktiva o prodaji na daljinu, Direktiva o zaštiti podataka, Direktiva o e-trgovini, Direktiva o autorskom pravu i dr.²⁴⁶

Kao glavni izazovi na globalnom nivou za Evropu su: porezi i carine, zaštita podataka, sigurnost i autentičnost, pouzdanost, zaštita prava intelektualne svojine, ilegalni škodljivi sadržaji.

1.1.1. Važne politike, programi i specifične mere koji podržavaju izgradnju e-legislative u EU

Politike i mere koje podržavaju izgradnju e-legislative u EU su:²⁴⁷

- politika sigurnosti i privatnosti koja ima za cilj da kreira povoljna legalna i tehnička rešenja za autentifikaciju, integritet, poverljivost, zaštitu ličnih podataka, sigurnost mreža i dr;
- kreiranje unutrašnjeg tržišta EU za e-trgovinu, koje treba da obezbedi slobodno pružanje elektronskih usluga širom EU;
- pružanje kompanijama i potrošačima legalnih garancija koje su neophodne da bi se oni uključili u e-trgovinu;
- program e-sadržaj (engl. *e-Content*) koji podržava razvoj evropskih jezičkih i kulturnih multimedijalnih sadržaja za Internet;
- akcioni plan e-učenje (engl. *e-Learning*) koji koordinira aktivnosti u uniji koje su vezane za obrazovanje u digitalnoj eri.

²⁴⁶ Isto, str.358

²⁴⁷ www.europe.eu.int/information society

1.2. Međunarodne organizacije i institucije i pravna regulativa u domenu elektronskog poslovanja

Internet i e-poslovanje su globalni po prirodi, što znači da bi minimum zajedničkih pravila trebalo da bude doneto na međunarodnom nivou. Otuda su mnoge međunarodne organizacije uključene u rad na ovim pitanjima kao što su:²⁴⁸

- Međunarodna telekomunikaciona unija (engl. *International Telecommunication Union - ITU*),
- Svetska trgovinska organizacija (engl. *World Trade Organisation - WTO*),
- Međunarodna organizacija za intelektualnu svojinu (engl. *World Intellectual Property Organisation - WIPO*),
- Organizacija za ekonomsku saradnju i razvoj (engl. *Organisation for Economic Cooperation and Development - OECD*) i dr.

Od međunarodnih organizacija koje su aktivne u radu na razvoju pravne regulative u domenu elektronskog poslovanja, analiziraćemo samo neke:

- Komisiju Ujedinjenih nacija za međunarodno trgovinsko pravo (engl. *United Nations Commission on International Trade Law - UNCITRAL*),
- Međunarodnu organizaciju za intelektualnu svojinu – *WIPO* i posebno
- Svetsku trgovinsku organizaciju - *WTO*.

1.2.1. Komisija Ujedinjenih nacija za međunarodno trgovinsko pravo - UNCITRAL

Komisija UN za međunarodno trgovinsko pravo, *UNCITRAL*, donela je 1996. godine Model zakona za elektronsku trgovinu. Pri tome, Komisija se opredelila za formu model zakona, a ne recimo konvencije, jer se preko model zakona (naročito za oblasti koje nisu regulisane) podstiče najefikasnije unifikacija najpre domaćih, a zatim i međunarodnih propisa koji se odnose na određenu oblast. Model sporazum se po pravnom principu autonomije volje, može zaključiti između strana koje to žele za konkretan pravni posao. Takođe, Model sporazum služi i za regulisanje odnosa poslovanja u nekoj konkretnoj grani, a celishodno je rešenje za kompleksno regulisanje svih oblasti koje zahtevaju kontinuirano praćenje i doradu.

1.2.2. Svetska organizacija za intelektualnu svojinu - WIPO

Intelektualna svojina je proizvod intelekta koji je vlasništvo nekog pojedinca ili organizacije i koji, prema tome, može da odabere da ga slobodno koristi, ili da ga ustupi drugom licu, s tim da kontroliše njegovu dalju upotrebu (knjige, filmovi, softver, lekovi, i sve što je nastalo zahvaljujući napretku nauke i tehnologije). Sistem pravne zaštite intelektualne svojine treba da obezbedi korist i njegovom tvorcu i društvu kao celini u smislu održavanja lojalne konkurencije, podrške proizvodnji najnovijih proizvoda i usluga, unapređenja tehnološkog i kulturnog razvoja, rasta ukupnog fonda svetskog znanja.²⁴⁹

²⁴⁸ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.359

²⁴⁹ Isto, str.360

Prava intelektualne svojine ustupaju se u skladu sa nacionalnim zakonima i meĎunarodnim konvencijama. Svetska organizacija za intelektualnu svojinu i Svetska trgovinska organizacija zaduĝene su za primenu mnogobrojnih meĎunarodnih konvencija i ugovora kao ŝto su:

- Pariska konvencija o zaštiti industrijske svojine, prva konvencija iz ove oblasti, koja datira joŝ iz 1883. godine,
- Bernska konvencija koja se bavi zaštitom knjiĝevnih i umetniĝkih dela,
- Rimska konvencija posvećena zaštiti izvoĎaĝa, proizvoĎaĝa fonograma i radio-TV organizacija.

TakoĎe, Svetska organizacija za intelektualnu svojinu je 1996. godine donela dva ugovora koji stimuliŝu i olakŝavaju elektronsku trgovinu i preuzimanje razliĝitih sadrĝaja sa mreĝe i to *WIPO Ugovor o autorskom pravu* (engl. *Copyright Treaty*) i *WIPO Ugovor o izvoĎanjima i fonogramima* (engl. *Performances and Phonograms Treaty*). Ovi ugovori idu dalje od Bernske Konvencije i ukljuĝuju odredbe o pravu komuniciranja, zloupotrebi u domenu tehnoloŝkih mera i integriteta informacije.

Dodatni podsticaj zaštiti intelektualne svojine i definisanju njene vaĝnosti dao je Sporazum u vezi sa merama zaštite prava intelektualne svojine sa efektom na trgovinu (engl. *Trade Related Intellectual Property Agreement - TRIPS*), usvojen od strane ĉlanica Svetske trgovinske organizacije, nakon Urugvajске runde multilateralnih pregovora (1986-1994), koji je stupio na snagu 1. januara 1995. godine. Ovaj sporazum obuhvata sve oblasti intelektualne svojine i predstavlja prvi meĎunarodni Ugovor o intelektualnoj svojini koji zahteva usvajanje i primenu specifiĝnih mera primene i procedure reŝavanja sporova.

1.2.3. Svetska trgovinska organizacija - WTO

Prema analizi struĝnjaka WTO, elektronska trgovina ima i kvantitativan i kvalitativan uticaj na meĎunarodni sistem trgovanja koji je u njihovoj nadleĝnosti i postaje nezaobilazna tema razgovora na novoj rundi multilateralnih trgovinskih pregovora, od interesa za sve zemlje ĉlanice WTO, bez obzira na nivo njihove razvijenosti i trenutnu ukljuĝenost i prisustvo na elektronskom trĝiŝtu.²⁵⁰

Inaĝe, pitanja vezana za tretman elektronske trgovine inicirana su na drugoj WTO Ministarskoj konferenciji, odrĝanoj u Ţenevi 1998. godine. Imajuĝi u vidu svu sloĝenost i kompleksnost liste pitanja u okviru WTO, posebno je interesantan i nov segment koji tretira problematiku vezanu za ukljuĝenje elektronske trgovine u sistem meĎunarodnog multilateralnog trgovanja. Radi se o setu pitanja koja su od posebnog znaĝaja prvenstveno za razvijene zemlje, gde je taj vid trgovanja najviŝe i razvijen i koje nastoje da meĎunarodnim regulisanjem ovog domena obezbede svoje interese i perspektivne profile u ovoj oblasti. S druge strane, su zemlje u razvoju koje i ako joŝ udaljene od problema elektronskog poslovanja ne smeju dozvoliti da se fundamentalna pitanja u ovom domenu reŝe bez uvaĝavanja i njihovih potreba i interesa. Ove zemlje su svesne da neukljuĝivanje u savremene elektronske moguĝnosti poslovanja vodi u marginalizaciju i na periferiju ekonomskog napretka, tako da je njihovo aktivno prisustvo u reŝavanju svih pitanja vezanih za ET od samog poĉetka neophodno i korisno.

²⁵⁰ WTO ima 153 zemlje ĉlanice i 30 zemalja posmatraĝa (gde spada i Srbija)

Eksplozivni rast Interneta, dao je veći značaj elektronskom poslovanju, nego što se to uopšte moglo naslutiti u toku Urugvajске runde pregovora, tako da je tema multilateralnog regulisanja elektronskog poslovanja tek kasnije mogla biti definisana i uključena u sistem WTO, sa perspektivom da postane jedna od značajnih tema nove runde multilateralnih trgovinskih pregovora. To se obrazlaže činjenicom što je kvalitativan uticaj ET daleko veći i dublji, jer elektronska trgovina utiče na trgovinske politike i trgovinsku konkurentnost svih zemalja, tako da ova tema za WTO postaje izuzetno važna iz sledećih razloga.²⁵¹

- *Trgovinske politike.* Moraju biti redizajnirane saglasno novim potrebama elektronskog komuniciranja, gde dostupnost informacionim mrežama postaje nezaobilazan element nacionalnih politika. Paralelno sa trgovinskom, neophodne promene je potrebno realizovati i u investicionoj, fiskalnoj i monetarnoj politici zemlje koja uvažava nove relacije elektronskog tržišta i sve njegove implikacije. Socijalna dimenzija ET takođe mora biti zastupljena i prisutna, naročito u domenima vezanim za trening i obuku potrebnih profila kadrova.
- *Uloge vlada i kompanija.* S obzirom na to da se prva iskustva i znanja o elektronskom poslovanju nalaze u sektoru kompanija koje ga primenjuju, vlade koje ozbiljno pristupaju dizajniranju ekonomskog ambijenta svoje nacionalne ekonomije novim uslovima informatičke ere ovo moraju imati u vidu. Znanja i iskustva korporativnog sektora moraju biti udružena sa znanjima vladinih eksperata u jednoj novoj vrsti partnerstva usmerenog na pripremu nacionalne ekonomije za poslovanje u novom digitalnom veku.
- *Odnos između elektronske i klasične (fizičke) trgovine.* I pored bitnih razlika, obuhvat elektronske trgovine je tako širok da se ne sme i ne može isključiti ni kada je u pitanju problematika vezana za pitanja tipična za klasičnu trgovinu kao što su carine, osiguranje, bankarstvo, transport. U svim ovim domenima adekvatna rešenja se moraju naći i za transakcije obavljene elektronski.

Pitanja vezana za ET prvi put su na određeni način ušla u WTO na prvoj WTO Ministarskoj konferenciji u Singapuru 1996. godine, koja je usvojila Ministarsku deklaraciju o trgovini proizvodima informacione tehnologije (engl. *Information Technology Agreement - ITA*). Ovim sporazumom se iz trgovine postepeno uklanjaju carine na proizvode koji su vezani za informacione i telekomunikacione tehnologije, gde su uključeni i mnogi infrastrukturni proizvodi važni za realizaciju elektronske trgovine. Prema usvojenoj deklaraciji WTO će težiti: „maksimalnoj slobodi svetske trgovine proizvodima informacione tehnologije“.²⁵²

Na Drugoj WTO Ministarskoj konferenciji održanoj u Ženevi 20. maja 1998. godine, usvojena je Deklaracija o globalnoj elektronskoj trgovini. Deklaracija predviđa da do daljnjeg elektronske transakcije ostanu oslobođene carina. Deklaracija je usvojena na predlog i inicijativu SAD, koje su naglasile da se predlog ne odnosi na poresku politiku i na robu poručenu putem Interneta, ali isporučenu putem normalnih komercijalnih kanala. Usvajanjem ove Deklaracije prema stavu SAD „WTO zauzima vodeće mesto u rešavanju pitanja globalne elektronske trgovine i time otvorenih izazova novog veka.“²⁵³

Slično SAD i EU zastupa mišljenje da WTO svakako mora imati jednu od ključnih uloga kada je u pitanju postavljanje međunarodnih okvira za elektronsku trgovinu. Evropska unija, međutim, ukazuje na širinu pitanja koja su vezana za ET, a u nadležnosti su WTO, kao na

²⁵¹ Isto, str.361

²⁵² UNCTAD, 1999.

²⁵³ Fokus, februar, 1998.

primer: prava intelektualne svojine, javne nabavke, finansijske usluge, telekomunikacije i proizvodi informacione tehnologije.

Zemlje u razvoju su podržale Deklaraciju, ali su izdvojile kao važne i sledeće aspekte:²⁵⁴

- radi se o kompleksnoj problematici sa potencijalnim koristima za zemlje u razvoju;
- postoji potreba za tehničkom saradnjom i pomoći koja bi zemljama u razvoju olakšala uključanje u ET;
- jasna je neophodnost izučavanja uticaja i posledica ET na zemlje u razvoju i njihov razvoj.

Na Drugoj Ministarskoj konferenciji postavljen je i zahtev Generalnom Savetu WTO „da utvrdi radni program koji će ispitati sve aspekte i uticaje globalne ET na tokove međunarodne trgovine“.²⁵⁵ Radni program je utvrđen i pod nadzorom je Generalnog Saveta WTO, a u rad na tom programu su uključena sledeća WTO tela:

- Savet za trgovinu uslugama,
- Savet za trgovinu robom,
- Savet za TRIPs i
- Komitet za trgovinu i razvoj.

Svako od nadležnih WTO tela je dobilo zadatak da u okviru svog domena ispita implikacije elektronske trgovine.

U organizaciji UNCTAD-a i WTO septembra 1998. godine, održan je ekspertski sastanak na temu „Priprema za buduće multilateralne trgovinske pregovore: Pitanja i istraživanja koja su neophodna iz razvojnih perspektiva“. U vezi ET na ovom sastanku postavljene su sledeće dileme:²⁵⁶

- Kako se ET može uklopiti u postojeći sistem WTO;
- Pravni aspekti i aspekti intelektualne svojine vezani za ET;
- Implikacije ET na razvoj.

Imajući u vidu da su to pitanja koja predstavljaju bazu za uvođenje cele ET problematike u WTO i u buduće multilateralne trgovinske pregovore, svako od njih će biti ukratko razmotreno.

Osnovno pitanje koje se nameće na početku svake priče o uključanju ET u WTO jeste, da li ovu problematiku izučavati kao posebno izdvojenu celinu, ili pojedine aspekte ET razmatrati u okviru onih WTO sporazuma koji su za njih nadležni. Iz sadašnjih perspektiva, druga alternativa izgleda kao daleko prihvatljivija i realnija varijanta. Inače, pitanja ET se određenim delom nalaze u sledećim WTO sporazumima: *GATS*, *GATT 94*, *TRIPS*.

GATS (Opšti sporazum o trgovini uslugama) – pokriva sledeće elektronske transakcije: Internet usluge i proizvode koji se mogu isporučiti u digitalnoj formi kao što su finansijske usluge, telekomunikacione, računске usluge, usluge zabave, poštanske i kurirske usluge, usluge vezane za avio-saobraćaj (rezervacija karata) i sl.

²⁵⁴ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.362

²⁵⁵ UNCTAD, 1999, str.100

²⁵⁶ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.363

Članovi GATS-a relevantni za ET su:²⁵⁷

- obuhvat (uključujući modalitete isporuke), član I;
- MFN²⁵⁸, član II;
- transparentnost, član III;
- rastuće učešće zemalja u razvoju, član IV;
- domaća regulativa, standardi i priznavanja, članovi VI i VII;
- zaštita privatnosti i praksa zloupotreba, član XIV;
- pristup tržištu elektronske ponude i usluga, član XVI;
- nacionalni tretman, član XVII;
- trgovina telekomunikacionim uslugama i principi konkurentnosti;
- carine i
- pitanja klasifikacije prema GATS klasifikaciji.

Infrastrukturni razvoj je jedan od preduslova za mogućnost širenja ET i uključenje što većeg broja zemalja u ovaj vid poslovanja. Ovaj razvoj infrastrukture pored WTO Ugovora o liberalizaciji bazičnih telekomunikacija (1997) i Ugovora WTO o postepenom eliminisanju carina u trgovini IT proizvodima (ITA, decembar 1996), podržava i telekomunikacioni aneks GATS-a.

GATT 94 – Proizvodi koji su kupljeni i plaćeni preko Interneta, ali se fizički isporučuju klasičnim kanalima podvode se pod postojeću WTO regulativu za trgovinu robom. U nadležnosti WTO Komisije za promet robom su pitanja vezana za:²⁵⁹

- pristup tržištu robe vezane za ET;
- pitanje carina, fiskalnih opterećenja, licencnih procedura i posebno primena člana VII GATT 94;
- standardi;
- pravilo o poreklu (engl. *rules of origine*) i
- klasifikaciona pitanja.

TRIPS – WTO Sporazum o merama zaštite prava intelektualne svojine sa efektom na trgovinu, sadrži tradicionalne principe međunarodnog zakona o pravu kopiranja (engl. *copyright*), zasnovanog na Bernskoj Konferenciji. Na taj način ovaj sporazum pokriva pitanja zaštite prava kopiranja i trgovinskih marki i u elektronskim transakcijama, ali ne specificira kako u ovom domenu suzbiti neovlašćeno „skidanje“ (engl. *downloading*) i distribuciju sadržaja.

TRIPS ugovor je značajan za ostvarenje elektronskih transakcija u domenima zaštite i ostvarivanja prava na kopiranje (engl. *copyright*), zaštite i ostvarivanja prava trgovinskih znakova, prava novih tehnologija i pristupa tim tehnologijama.²⁶⁰

U okviru Ministarske deklaracije koja je usvojena na četvrtoj WTO Ministarskoj konferenciji održanoj u Dohi 2001. godine, analiziran je dosadašnji rad nadležnih WTO saveta i klijenata u okviru Radnog programa za elektronsku trgovinu, a Generalni Savet WTO je podržao dalji

²⁵⁷ UNCTAD, 1999, str.104-105

²⁵⁸ MFN-Most Favoured Nation – princip najpovoljnije nacije

²⁵⁹ UNCTAD, 1999, str.106

²⁶⁰ Isto, str.106

rad na ovom programu. Kao razlog za ovakav stav navedena je činjenica da elektronska trgovina kreira nove izazove i mogućnosti za trgovinu članica WTO na svim nivoima razvoja i konstatovano je da WTO prepoznaje važnost kreiranja i održavanja okruženja koje će pogodovati implementaciji i razvoju elektronske trgovine u pojedinim zemljama članicama. Takođe, podržan je moratorijum na uvođenje carinskih obaveza u elektronskim transakcijama. Isti stav po navedenim pitanjima (nastavak radnog programa i moratorijum carinskih obaveza) zadržan je i na petoj Ministarskoj WTO konferenciji održanoj u Kankunu 2003. godine.

2 . OBLASTI PRAVNOG REGULISANJA

U cilju sagledavanja pravnih rešenja prisutnih u pojedinim oblastima od značaja za obavljanje online transakcija, analiziraćemo samo neke značajnije kao što su: pravo na privatnost, zaštita intelektualne svojine, porezi u online transakcijama.

2.1. Privatnost na mreži/Internetu

Internet kao globalna, otvorena mreža deluje kao samoregulišući medijum, što mu omogućava razvoj i delovanje bez ograničenja od strane zakonske regulative. Takvi uslovi, međutim, kreiraju mogućnost narušavanja nekih prava i normi koje tradicionalni zakoni nameću kao obaveznim. Jedno od takvih je i pravo pojedinca na privatnost i ograničenu mogućnost upotrebe njegovih ličnih podataka. U SAD, na primer, pravo na privatnost nije eksplicitno garantovano Ustavom, ali je implicitno obezbeđeno kroz prvi, četvrti, deveti i četrnaesti Amandman.

Mnoge Internet kompanije prikupljaju lične informacije o korisniku za vreme njegove posete određenom sajtu. Zagovornici zaštite privatnosti smatraju da i ovaj čin predstavlja narušavanje prava privatnosti, dok online marketing i reklamne kompanije tvrde da se ne radi o zloupotrebi privatnih podataka, već samo o nameri da kroz blisku upoznavanje šta kupac voli ili ne voli, postaje moguće zadovoljiti njegove potrebe na adekvatniji način.

Analiza američke Savezne komisije za trgovinu (engl. *Federal Trade Commission-FTC*) pokazala je da 97% od proučavanih Web sajtova, prikupljaju lične podatke korisnika. Od toga, 62% sajtova obaveštava kupca o korišćenju takvih podataka, dok 52% sajtova koristi posredničke mehanizme praćenja podataka o kupcima. Upravo zbog toga osnovana je i Komisija sa zadatkom da prati pitanja iz domena online privatnosti. Zakon koji najdirektnije reguliše upravljanje i korišćenje informacija o kupcima u SAD je Zakon o modernizaciji finansijskih usluga iz 1999. godine. Prema njemu, kompanije moraju obezbediti kupcima opciju da li žele da svoje lične podatke i preferencije podele sa trećom stranom, ili ne. Inicijativa koja okuplja Web reklamne kompanije u SAD (engl. *Network Advertising Initiative-NAI*) nastoji da razvije protokole koji će se poštovati pri korišćenju privatnih podataka – zabrana korišćenja privatnih podataka iz medicinskih ili finansijskih izvora, ali sloboda u korišćenju kombinacije ličnih podataka koje dajete pri online kupovinama i podataka o preferencijama i poseti pojedinih sajtova.²⁶¹

Studije i ankete pokazuju da za kupce najveći problem predstavlja sigurnost na mreži i da je njihovo oklevanje da kreditnom karticom plate svoju online transakciju vezano za dilemu da li će njihovi privatni podaci biti negde sačuvani i posle zloupotrebljeni.

²⁶¹ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.365

Dimenzije privatnosti nalazimo i u odnosu zaposleni-poslodavac. Naime, mnogi poslodavci preko računara prate rad i eventualne zloupotrebe svojih radnika. Postoje posebni softveri, laki za upotrebu, kao što je *keystroke softer*, koji omogućava poslodavcu da prati produktivnost i eventualnu zloupotrebu opreme od strane zaposlenih (da li je, na primer, slao sa posla privatne e-mailove i slično).

Da bi ste se zaštitili kao korisnik i onemogućili da bez vaše saglasnosti koriste podatke o vama možete upotrebiti poseban softver koji vam omogućava tzv. falsifikovani identitet – pseudonim. Na primer, *PrivacyX.com*, besplatan Internet servis, omogućava korisnicima da neidentifikovani surfuju Internetom.

Kompanija koja poseduje Web sajt može zaštititi sopstvenu reputaciju i primenom adekvatne politike privatnosti koja će garantovati da koristite informacije o svojim posetiocima sa posebnom pažnjom i poštujući postojeće zakone. Dakle, omogućite da posetioci vašeg sajta u svakom trenutku budu svesni da li koristite i na koji način podatke o njima i da su sa takvim činom saglasni. Postoji više servisa na Internetu koji kompanijama omogućavaju takvu politiku privatnosti: *PrivacyBot.com*, *BetterWeb* programi, *TRUSTe.com* i slično.

Takođe, treba pomenuti uspeh *Privacy Seal* programa. To su neprofitne, globalne i nezavisne inicijative, koje su lansirane da bi obezbedile mehanizam kojim Web sajtovi mogu da smanje brigu potrošača kada je privatnost u pitanju. Suština je u tome da se vizuelni simbol – *Privacy Seal* nalazi na svakom sajtu koji zadovoljava zahteve programa vezane za privatnost, odnosno vezane za sakupljanje podataka i njihovu distribuciju. Web sajtovi koji nose *Privacy Seal* su prošli evaluaciju i zadovoljavaju zahteve ovih programa u oblasti privatnosti.²⁶²

Posebno važno pitanje u ovoj oblasti postaje zaštita privatnosti dece. Deca postaju sve značajniji segment korisnika Interneta i dolaze u poziciju da u toku svog krstarenja naiđu na neadekvatne i škodljive sadržaje. U SAD, na primer *Communication Decency Act* iz 1996. godine i *Child Online Protection Act* iz 1998. godine imaju za cilj da zabrane pornografiju na Internetu, prvenstveno u interesu dece. Zabranu Web sajtovima da prikupljaju privatne podatke dece ispod 13 godina bez odobrenja roditelja, uvodi *Children's Online Privacy Protection Act* iz 2000. godine. Tinejdžeri predstavljaju grupu čiji se privatni podaci najčešće koriste od strane sajtova, jer su oni ciljna grupa za promotivne i reklamne kompanije određenih kategorija proizvoda i usluga atraktivnih u njihovom uzrastu. Softverske kompanije nude na tržištu softvere za blokiranje i filtriranje sadržaja sa Interneta koji mogu biti dostupni deci i omladini.

U Evropskoj uniji ključna direktiva koja reguliše pitanje privatnosti je Direktiva o zaštiti privatnih podataka. Prema ovoj Direktivi, svaka organizacija koja poseduje podatke o vama, mora da vam, na vaš zahtev, te podatke da na uvid. Prema ovoj direktivi pojedinci u Evropi imaju znatno više kontrole nad svojim ličnim podacima od onih u SAD. Ove razlike imaju korena u kulturnim razlikama između Evrope i SAD, a primenom „*Safe Harbor*“ principa posledice ovih različitih stavova ne otežavaju međusobnu e-trgovinu.

2.2. Zaštita intelektualne svojine na mreži: pravo kopiranja i patentni

Velike mogućnosti koje Internet otvara za preuzimanje, kopiranje i deljenje fajlova koji su identični originalu, ozbiljno pokreće pitanje zaštite prava intelektualne svojine u ovom domenu, posebno kada su u pitanju dela kao što je muzika, softver i slično. U SAD, *Digital*

²⁶² Isto, str.366

Millennium Copyright Act (DMCA) iz 1998. godine daje pravo kreatorima da zaštite svoje delo, ali i pravo profesorima i ponuđačima sadržaja da pristupe tim delima. Kupovinom licence dobijate pravo da nudite takve sadržaje. Zapravo, *DMC* zakon štiti fer upotrebu materijala koji je pod zaštitom. Pri tome, fer upotreba se definiše kao pravo upotrebe tih materijala u obrazovne, istraživačke svrhe, u cilju kritike i slično. Uvode se četiri kriterijuma za procenu da li se radi o fer upotrebi sadržaja pod zaštitom i to:²⁶³

1. svrha za koju se materijal koristi,
2. priroda materijala koji se koristi,
3. obim materijala koji je reprodukovani
4. efekat koji je ostvaren tom reprodukcijom.

Patent garantuje kreatoru otkrića isključivo pravo na njegovu upotrebu i pravo nadoknade za upotrebu patentom zaštićenih sadržaja. Postoje podeljena mišljenja o adekvatnoj dužini patentne zaštite. Jedna grupa zastupa mišljenje da je 20-godišnje trajanje patenta, predugo i destimulativno za dalji razvoj i unapređenje softvera.

Registrowanje domena koji je sličan imenu određenog trgovinskog znaka, takođe može da stvori konfuziju i dovede do zloupotrebe. Trgovinski znaci koji pripadaju osobi ili kompaniji koja ne poseduje i domen sa sličnim nazivom su zaštićeni. Vlasnici takvih domena ne podleću kazni ukoliko su registrovani pre prve upotrebe registrovanog trgovinskog znaka.

Stav EU je, da pored uvažavanja mnogih međunarodnih konvencija iz oblasti zaštite intelektualne svojine, potrebno je obezbediti i viši nivo zaštite donošenjem brojnih direktiva i uredbi u ovoj oblasti. Neke od njih su:

- Direktiva o pravnoj zaštiti dizajna iz 1998. godine;
- Direktiva o harmonizaciji zakona zemalja članica u pogledu žigova iz 1998. godine;
- Direktiva o pravnoj zaštiti računskih programa iz 1991. godine;
- Direktiva o autorskim i srodnim pravima u informacionom društvu i druge.

2.3. Spam poruke

E-mail je popularan vid elektronske komunikacije koji je u značajnoj upotrebi kako u poslovnom, tako i u privatnom sektoru. Prema procenama AOL-a (engl. *America On Line*), skoro trećina e-mail poruka koje putuju mrežom spada u grupu tzv. *unsolicited* komercijalnih poruka, poznatijih kao spam poruke. Za ove nepoželjne poruke, deo troškova direktno snose oni koji ih primaju plaćanjem nadoknada Internet servis provajderima. Zakonska regulativa koja se kreira u ovom domenu zalaže se za stav da priroda e-mail poruke mora biti jasno naznačena. Na primer, reklame moraju biti jasno označene kao takve.

Postoje načini da sebe ili kompaniju zaštitite od neželjenih e-mail poruka. Web sajtovi kao što je na primer *unitedmessaging.com* nude uslugu koja omogućava pretplatnicima da se zaštite od neželjenih poruka.

²⁶³ Deitel et al., 2001, str.319

2.4. Online ugovori

Američki zakon poznatiji kao *E-sing bill* iz 2000. godine promovise e-trgovinske transakcije tako što čini legitimnim online ugovore. Prema ovom zakonu, digitalni ugovor ima isti nivo validnosti kao i papirni ugovor. Zakon omogućava stranama koje sarađuju da kreiraju sopstveni ugovor. Ova zakonska odredba treba da smanji vreme i troškove koji su povezani za rešavanje ugovornih odnosa papirnim putem.²⁶⁴

U mnogim slučajevima Web sajt će od svojih korisnika tražiti da se prvo saglase sa određenim uslovima vezanim za uslugu koju koriste, ili proizvod koji poručuju. Ovi uslovi se obično pojavljuju na monitoru i izborom opcije DA, korisnik prihvata definisane uslove, što mu omogućava da nastavi sa korišćenjem servisa Web strane. Ovi tipovi ugovora se smatraju validnim kod američkih sudova.

2.5. Porezi na Internetu

Oprezivanje na Internetu je vrlo složena i kontradiktorna tema, koja već nekoliko godina na Zapadu izaziva brojne polemike, lobiranja i donošenje novih zakona. Dok se jedni zalažu za ukidanje poreza na Internetu, drugi smatraju da je neophodno plaćati poreze i u online transakcijama. Ključni je problem da li će lokacija kupca, vendedora, IS provajdera, ili servera biti ona prema kojoj će se definisati plaćanje poreskih opterećenja.

Oponenti poreza na Internetu smatraju da bi njihovo plaćanje ugrozilo rast Interneta. Prema njima, postoji 7.500 različitih poreskih metoda. Da bi se zadovoljili poreski zahtevi svih učesnika u online transakcijama trebalo bi primeniti sve te metode.

Američka komisija za poreze na Internetu prihvatila je preporuke vezane za produženje moratorijuma na poreze na Internetu i u međunarodnim e-trgovinskim transakcijama kao i eliminaciju poreza na digitalne sadržaje.²⁶⁵

Problem poreza na Internetu je međunarodnog karaktera. Evropska unija usvojila je još tokom 2003. godine Zakon o primeni poreza na dodatnu vrednost na sve elektronske sadržaje koji se distribuiraju putem Interneta, a slični zakoni su doneti i u petnaestak saveznih država u SAD.

U EU, na primer, uveden je porez na dodatnu vrednost koji moraju da plaćaju sve evropske kompanije. Ukoliko ne-evropska kompanija online isporučuje proizvod kupcu u Evropi, PDV se ne plaća i tako proizvod postaje jeftiniji. Selektivna primena ovih zakona u različitim državama može da izazove brojne probleme na tržištu, pokrene migracije kompanija i proizvede nelojalnu konkurenciju.

Međutim, sigurno je da će aktuelna ekonomska kriza uticati na to da se sve više država odluči za oporezivanje „digitalne robe“, jer to može biti odličan način za popunu budžeta, pogotovu ako se zna da je promet u elektronskoj trgovini oko 150 milijardi dolara godišnje i da ova grana spada među otpornije na krizu.

²⁶⁴ Vidas-Bubanja M.: „E – poslovanje: Menadžment, tehnologije, aplikacije“, cit.delo, str.369

²⁶⁵ Isto, str.370

3. PRAVNA REGULATIVA E-POSLOVANJA U SRBIJI

U našoj zemlji je prisutna i sve više se razvija svest o neophodnosti i velikoj koristi od primene elektronskog poslovanja. Taj novi model poslovanja obezbeđuje ekonomičnost poslovanja, lakše komuniciranje sa domaćim i inostranim partnerima i komercijalne prednosti na tržištu. U poslovnim krugovima Evropske unije i SAD-a sve je više prisutno shvatanje da se elektronskim poslovanjem zadobija značajna komparativna prednost na tržištu. Oblast elektronskih komunikacija je u savremenom svetu jedan od najznačajnijih činilaca privrednog i društvenog razvoja. Naša država, po uzoru na Evropsku uniju, mora da se postara da privredna društva u tom sektoru posluju u uslovima konkurencije i međusobne ravnopravnosti, uz uvažavanje interesa korisnika njihovih usluga. Upravo iz svih ovih razloga postoji velika potreba da se i u našoj zemlji donese Zakon o elektronskom poslovanju, čija je priprema počela 2000. godine i još uvek je u nacrtu. Zakon o elektronskom potpisu donet je 2004. godine²⁶⁶, a Krivični zakon je 2003. godine izmenjen i dopunjen sa nizom potpuno novih inkriminacija, posebno u oblasti zaštite računarskih programa, Internet mreže i protoka podataka, bezbednosti podataka na mreži, hakerskih upada i raznih zloupotreba.

Unošenjem ovih krivičnih dela u svoje zakonodavstvo Srbija je ispunila najveći deo svojih obaveza prema Direktivi EU o zaštiti računarskih programa iz 1991. godine i prema Konvenciji Saveta Evrope o sajber kriminalu iz 2001. godine. Predviđene su veoma oštre zatvorske kazne za neovlašćene upade na računare, krađu ili oštećenje računarskih programa i podataka (sa računara, Interneta, elektronskih medija), pravljenje i širenje virusa, lažno prikazivanje elektronske obrade podataka, namerno zagušenje mreže, spamovanje i ometanje funkcionisanja Interneta, neovlašćeno sprečavanje ili ometanje pristupa Internetu ili drugoj javnoj računarskoj mreži i dr.

Međutim, izrada, donošenje i implementacija Zakona o elektronskom poslovanju, u okvirima postojećeg pravnog sistema otvara mnoge probleme. Treba imati u vidu globalne okolnosti: integraciju u Evropsku uniju, odnosno činjenicu da ovaj zakon, kao i svaki drugi, treba da se uklopi u postojeći zakonski sistem, koji je na putu harmonizacije sa zakonskim sistemom Evropske unije. Posebno treba voditi računa o nizu lokalnih faktora, koji se na prvom mestu odnose na postojeće domaće zakone koji su na snazi i regulišu oblasti u tesnoj vezi sa ovom oblašću.

Na ponuđeni tekst Nacrta zakona o elektronskom poslovanju, date su značajne primedbe. Naime, Nacrt zakona se samo delimično bavi rešenjima vezanim za elektronsku trgovinu, a većina članova zakona je usmerena na regulisanje odnosa provajdera informacionih tehnologija. Zbog toga predstavnici privrednih društava koja se bave poslovima elektronskog poslovanja, smatraju boljim rešenjem da se odvojeno rade dva zakonska teksta, jedan koji će regulisati odnose u oblasti elektronske trgovine, a drugi u oblasti elektronskog poslovanja.

U Privrednoj komori Beograda, dogovoreno je da se od predstavnika zainteresovanih privrednih društava formira multidisciplinarna Radna grupa koja će, uzimajući u obzir domaća iskustva i iskustva razvijenih zemalja i zemalja u okruženju, predložiti donošenje zakonskog teksta koji će zadovoljiti potrebe kako elektronske trgovine, tako i u celini elektronskog poslovanja, vodeći računa o usklađenosti predloženih rešenja sa ostalim zakonima (Zakon o trgovini, Zakon o obligacionim odnosima i dr.).²⁶⁷

²⁶⁶ „Sl.glasnik RS“, br.135/04

²⁶⁷ Rasprava o nacrtu zakona o elektronskom poslovanju, www.internodinium.org/comment/reply/880/0

3.1. Zakon o elektronskom potpisu

U Srbiji je krajem 2004. godine donet Zakon o elektronskom potpisu, kojim se uređuje upotreba elektronskog potpisa u pravnim poslovima i drugim pravnim radnjama, kao i prava i obaveze i odgovornosti u vezi sa elektronskim sertifikatima.²⁶⁸

Osnovna uloga ovog zakona svodi se na dve stvari:

1. propisivanje uslova pod kojima je elektronski potpis pravno ekvivalentan svojeručnom potpisu i
2. propisivanje uslova koje mora da ispune sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.

Pored toga, pripremljena su i četiri podzakonska akta:

3. Pravilnik o vođenju evidencije sertifikacionih tela,
4. Pravilnik o registru sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate u Republici Srbiji,
5. Pravilnik o tehničko - tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijuma koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa i
6. Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata.

U Zakonu se na sledeći način definišu neki osnovni pojmovi i određuje njihov sadržaj i upotreba.²⁶⁹

- Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
- Kvalifikovan elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i nemogućnost naknadnog poricanja odgovornosti za njihov sadržaj;
- Potpisnik je lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica;
- Podaci za formiranje elektronskog potpisa su jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa;
- Sredstva za formiranje elektronskog potpisa su odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa;
- Podaci za proveru elektronskog potpisa su podaci kao što su kodovi ili javni kriptografski ključevi, koji se koriste za proveru i overu elektronskog potpisa;
- Sredstva za proveru elektronskog potpisa su odgovarajuća tehnička sredstva (softver i hardver) koja služe za proveru elektronskog potpisa;
- Elektronski sertifikat je elektronski dokumenat kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;
- Kvalifikovani elektronski sertifikat je elektronsko uverenje izdato od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata, kojim se jednoznačno utvrđuje identitet ovlašćenog učesnika elektronskog poslovanja;
- Korisnik je pravno lice, ili fizičko lice kome se izdaje elektronski sertifikat;

²⁶⁸ „Sl.glasnik RS“, br.135/04, Zakon o elektronskom potpisu, Član 1.

²⁶⁹ Isto, Član 2.

- Sertifikaciono telo je pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama Zakona o elektronskom potpisu.

Elektronskom dokumentu se ne moće osporiti punovaćnost ili dokazna snaga zbog toga što je u elektronskom obliku.²⁷⁰

3.1.1. Elektronski potpis i kvalifikovani elektronski potpis

Elektronski potpis je skup numeričkih podataka kojima se na kriptografski pouzdan naćin utvrćuje veza izmeću sadržaja elektronskog dokumenta i identiteta njegovog potpisnika. Elektronski potpis moće imati pravno dejstvo i moće se koristiti kao dokazno sredstvo, osim kada se posebnim zakonom zahteva da samo svojeručni potpis ima pravno dejstvo i dokaznu snagu.

Kvalifikovani elektronski potpis mora da zadovolji sledeće uslove:²⁷¹

1. da je isključivo povezan sa korisnikom,
2. da nedvosmisleno identifikuje korisnika,
3. da nastaje korišćenjem sredstava kojima potpisnik moće samostalno da upravlja i koja su isključivo pod njegovim nadzorom,
4. da je direktno povezan sa podacima na koje se odnosi,
5. da je formiran sredstvima za formiranje kvalifikovanog elektronskog potpisa i
6. da se proverava na osnovu kvalifikovanog elektronskog sertifikata korisnika.

Sredstva za formiranje kvalifikovanog elektronskog potpisa su sredstva koja moraju da obezbeće.²⁷²

1. da se podaci za formiranje kvalifikovanog elektronskog potpisa mogu pojaviti samo jednom i da je obezbećena njihova poverljivost;
2. da se iz podataka za proveru kvalifikovanog elektronskog potpisa ne mogu u razumno vreme i trenutno dostupnim sredstvima, dobiti podaci za formiranje kvalifikovanog elektronskog potpisa;
3. da kvalifikovani elektronski potpis bude zaštićen od falsifikovanja, upotrebom trenutno dostupne tehnologije;
4. da podaci za formiranje kvalifikovanog elektronskog potpisa budu pouzdano zaštićeni od neovlašćenog korišćenja.

Kvalifikovani elektronski potpis ima isto pravno dejstvo i dokaznu snagu u odnosu na podatke u elektronskom obliku, kao i svojeručni potpis i pečat u odnosu na podatke u papirnom obliku.²⁷³

3.1.2. Elektronski sertifikati i sertifikaciona tela

Elektronski sertifikat je elektronska potvrda kojim se potvrćuje veza izmeću podataka za proveru elektronskog potpisa i identiteta potpisnika. Izdaje ih ovlašćeno sertifikaciono telo.

²⁷⁰ Isto, Ćlan 3.

²⁷¹ Isto, Ćlan 7.

²⁷² Isto, Ćlan 8.

²⁷³ Isto, Ćlan 10.

Sertifikaciono telo je pravno lice koje drugim pravnim i fizičkim licima pruža usluge izdavanja elektronskih sertifikata. To može da bude svako pravno lice koje ispunjava uslove koji su predviđeni tim zakonom.²⁷⁴

Vlada određuje nadležni organ za akreditaciju i praćenje rada sertifikacionih tela koji vodi i registar akreditovanih sertifikacionih tela za elektronsko poslovanje i kontroliše njihov rad. Vlada određuje i naknadu za akreditaciju sertifikacionih tela.

Kvalifikovani elektronski sertifikat je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata i koji mora da sadrži:²⁷⁵

- oznaku da se radi o kvalifikovanom elektronskom sertifikatu;
- skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat;
- skup podataka koji jedinstveno identifikuje potpisnika;
- podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa, a koji su pod kontrolom potpisnika;
- podatke o početku i kraju važenja elektronskog sertifikata;
- identifikacionu oznaku izdatog elektronskog sertifikata;
- kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat;
- ograničenja vezana za upotrebu sertifikata, ako ih ima.

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata mora da ispunjava sledeće uslove:²⁷⁶

1. sposobnost za pouzdano obavljanje usluga izdavanja elektronskih sertifikata;
2. bezbedno i ažurno vođenje registra korisnika kao i sprovođenje bezbednog i trenutnog opoziva elektronskog sertifikata;
3. obezbeđivanje tačnog utvrđivanja datuma i vremena izdavanja ili opoziva elektronskog sertifikata;
4. da izvršava proveru identiteta i ako je potrebno drugih dodatnih obeležja licu kojem se izdaje sertifikat, na pouzdan način i u skladu sa propisima;
5. da ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za vršenje usluge izdavanja elektronskih sertifikata;
6. da koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmena i koji obezbeđuju tehničku i kriptografsku sigurnost procesa;
7. da preduzima mere protiv falsifikovanja elektronskih sertifikata, a u slučajevima u kojima generiše podatke za formiranje elektronskog potpisa, da garantuje tajnost procesa formiranja tih podataka;
8. da obezbedi finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata;
9. da obezbedi čuvanje svih relevantnih informacija koje se odnose na elektronske sertifikate u propisanom vremenskom periodu i to u izvornom obliku;
10. da ne čuva i ne kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu;
11. da obezbedi sisteme za fizičku zaštitu uređaja, opreme i podataka i sigurnosna rešenja za zaštitu od neovlašćenog pristupa;

²⁷⁴ Isto, Član 12.

²⁷⁵ Isto, Član 17.

²⁷⁶ Isto, Član 18.

12. da informiše lica koja traže izdavanje kvalifikovanog elektronskog sertifikata o tačnim uslovima izdavanja i korišćenja tog sertifikata;
13. da koristi pouzdan sistem upravljanja elektronskim sertifikatima u obliku koji omogućava njihovu proveru.

Nadležni organ vodi Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji. Registar i evidencija sertifikacionih tela dostupni su javnosti.

3.1.3. Prava, obaveze i odgovornosti korisnika i sertifikacionih tela

Elektronski sertifikat se može izdati korisniku na njegov zahtev, o čemu se zaključuje poseban ugovor. Korisnik može koristiti usluge sertifikacije jednog ili više sertifikacionih tela.

Kvalifikovani elektronski sertifikat se može izdati svakom licu na njegov zahtev, na osnovu utvrđenog identiteta i ostalih podataka o licu koje je podnelo zahtev.²⁷⁷

Korisnik je dužan da čuva sredstva i podatke za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe i da dostavi sertifikacionom telu sve potrebne podatke i informacije o promenama koje utiču na tačnost utvrđivanja identiteta potpisnika.

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata dužno je da:²⁷⁸

1. obezbedi da svaki izdati kvalifikovani elektronski sertifikat sadrži sve potrebne podatke;
2. izvrši potpunu proveru identiteta korisnika za koga vrši usluge sertifikacije;
3. obezbedi tačnost i celovitost podataka koje unosi u evidenciju izdatih sertifikata;
4. unese u svaki sertifikat osnovne podatke o svom identitetu;
5. omogućiti svakom zainteresovanom licu uvid u identifikacione podatke sertifikacionog tela i uvid u rešenje za izdavanje kvalifikacionih elektronskih sertifikata;
6. vodi ažurnu, tačnu i bezbednim merama zaštićenu evidenciju izdatih elektronskih sertifikata koja mora da bude javno dostupna;
7. vodi tačnu i bezbednim merama zaštićenu evidenciju nevažećih elektronskih sertifikata;
8. obezbedi vidljiv podatak o tačnom datumu i vremenu izdavanja, odnosno opoziva elektronskih sertifikata ;
9. postupa po odredbama zakona i drugim propisima kojima je uređena zaštita ličnih podataka.

Sertifikaciono telo dužno je da čuva kompletnu dokumentaciju o izdatim i opozvanim elektronskim sertifikatima, radi dokaznog materijala i verifikacije u sudskim, upravnim i drugim postupcima, najmanje deset godina po prestanku važenja kvalifikovanih elektronskih sertifikata.²⁷⁹

Elektronski sertifikati koje izdaje strano sertifikaciono telo, ravnopravni su sa domaćim elektronskim sertifikatima.

²⁷⁷ Isto, Član 24

²⁷⁸ Isto, Član 28

²⁷⁹ Isto, Član 31.

Sertifikaciono telo je dužno da u cilju sprovođenja nadzora omogući ovlašćenim licima pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika i primenjenoj računskoj opremi i uređajima.²⁸⁰

Znači za obavljanje elektronskog poslovanja učesnici moraju da poseduju kvalifikovane elektronske sertifikate i računsku opremu (hardver i softver): za kreiranje i čuvanje elektronskih dokumenata, za slanje i prijem elektronskih poruka (personalni računar i odgovarajući sistemski i komunikacioni softver) i za generisanje i verifikaciju elektronskih potpisa (hardver i softver za generisanje i verifikaciju elektronskog potpisa).

²⁸⁰ Isto, Član 41.

ŠESTI DEO

ELEKTRONSKO BANKARSTVO U SRBIJI

1. OPŠTE STANJE

Kada se ocenjuje stanje e-bankarstva u Srbiji, značajno je upoređivanje sa situacijom u ovoj oblasti sa razvijenim zemljama, sa jedne strane i sa stanjem u drugim oblastima u zemlji, sa druge strane. U ekonomski razvijenim zemljama procenat učešća e-bankarstva u platnom prometu je veoma visok (npr. u Francuskoj 70 i 80%), dok je u Srbiji znatno niži, posebno kada su u pitanju fizička lica, ali sa tendencijom ubrzanog razvoja.²⁸¹ Da bi Srbija dostigla ekonomski razvijene zemlje, neophodno je da se u elektronski sistem poslovanja uključi što veći broj firmi, sve državne institucije, trgovine i građani. U odnosu na druge segmente u zemlji, e-bankarstvo je relativno dobro razvijeno i što je još značajnije, pokazuje tendenciju daljeg intenzivnog razvoja. Nekada je Srbija bila u velikom zaostatku za ovakvim načinom poslovanja, ali danas to više nije tako. U „poplavi“ banaka, danas u Srbiji, kvalitet e-bankinga koji neka banka pruža, je jedan od faktora koji odlučuje kojoj će se banci klijent prikloniti.

Smatra se da su koreni relativno dobre osnove za razvoj e-bankarstva postavljeni u ranijoj tehnološkoj i organizacionoj infrastrukturi Zavoda za obračun i plaćanja (ZOP-a), kao i u stečenim navikama korišćenja nekih servisa ZOP-a za poslovne banke i preduzeća. Integrisani sistem banaka naspram NBS i samih korisnika, trenutno funkcioniše putem nekoliko veza sa centralnom bankom. Osnovna veza se odnosi na platni promet (sve banke su povezane u realnom vremenu, tj. imaju mogućnost da u svakom momentu procesiraju zahteve za izvršavanje platnog naloga). Druga bitna veza se odnosi na platni promet u širem smislu, odnosno prenos novca i hartija od vrednosti u kupoprodajnim transakcijama preko Centralnog registra.²⁸²

Značajnije unapređenje postojećih i uvođenje novih finansijskih servisa u e-bankarstvo Srbije, vezano je za promene u makroekonomskom ambijentu koje su se odigrale u prethodnim godinama. Usvajanje novog Zakona o platnom prometu 1. januara 2003. godine, jednim delom imalo je za cilj zamenu postojećeg monopolskog sistema plaćanja tržišnim sistemom, a drugim delom stvaranje institucionalnih uslova za razvoj elektronskog bankarstva. Njegov uticaj na razvoj e-bankarstva proizilazi, kako iz direktnih efekata na sam sistem plaćanja, tako i iz stvaranja preduslova za radikalnu transformaciju modela poslovanja banaka i njihovih klijenata.

Glavni problem je što postojeća informaciona – komunikaciona infrastruktura nije na zadovoljavajućem nivou. Cilj je da se ostvari međusobna elektronska povezanost svih učesnika u elektronskim transakcijama i da banke prošire asortiman usluga koje nude elektronskim putem.

Prelaskom platnog prometa u poslovne banke i gašenjem ZOP-a u januaru 2003. godine, stvoreni su svi uslovi da domaće banke ponude nešto novo našem tržištu. To su bile bezgotovinske transakcije (virmanska plaćanja) putem Interneta. U to vreme na teritoriji Srbije su postojale samo tri kompanije koje su obezbeđivale softver za e-banking i ujedno predstavljale sertifikaciona tela. Ni danas ih nema mnogo više – tek šest registrovanih u zemlji. Krajem 2003. godine, pošto je servisiran pravni sektor, banke u Srbiji su bile spremne za još jedan veliki skok – e-banking za fizička lica. Četiri godine kasnije, banke promovišu da je procenat ukupnog platnog prometa elektronskim putem čak 65%.²⁸³

²⁸¹ Vuksanović E.: „Elektronsko bankarstvo“, cit. delo, str. 237

²⁸² Isto, str. 237

²⁸³ www.emagazin.co.yu/clanak.asp

Transformacijom platnog sistema i prelaskom platnog prometa u banke otvorena je nova oblast poslovanja banaka – rad sa klijentima elektronskim putem, koji se popularno naziva e-banking. Bankarstvo je postalo lider u oblasti elektronskog poslovanja u Srbiji. Razvoj elektronskog bankarstva neophodan je uslov za opstanak banaka na finansijskom tržištu. Sve veći broj građana plaća račune i proverava devizni kurs putem Interneta, ili mobilnog telefona.

Ovakav način poslovanja brzo su prihvatile gotovo sve banke, a neke postižu i da čak 50% ukupnog broja naloga dolazi do banke elektronskim putem. Po obimu poslovanja u ovoj oblasti ne zaostajemo za zemljama u regionu.²⁸⁴ Prema nekim ocenama, nismo daleko od Rumuna, Makedonaca i Bugara, a za razliku od Hrvata i Slovenaca, kod nas je brže obavljen prelazak platnog prometa iz ZOP-a u banke. Veoma je važno obrazovanje što većeg broja građana da koriste računar i da se upoznaju sa IT tehnologijama.

Elektronsko poslovanje i njegova automatizacija prisutna u našim bankama je na veoma naprednim tehnološkim osnovama. Domaća softverska rešenja su često efikasnija, integrisanija i savremenija nego inostrana. Problem predstavlja uklapanje u evropske standarde i propise koji se razlikuju od naših, ali na tom približavanju bankari svakodnevno rade. Domaće softverske kompanije brzo i uspešno implementiraju sva rešenja iz oblasti bankarske tehnologije. Sa uvođenjem novih regulacionih tela, institucija i kriterijuma, Srbija se postepeno integriše u savremene svetske tokove poslovanja. U elektronskom bankarstvu, Srbija ne zaostaje za zemljama u regionu, ali u okviru drugih oblika elektronskog poslovanja, e-trgovine, ili B2B (engl. *business to business*) poslovanja, još je na početku.²⁸⁵

Banke su se uspešno uključile u nove sisteme međubankarskih obračuna po svetskim principima: RTGS za prioriteta plaćanja i plaćanja velikih vrednosti i neto sistem za mala plaćanja. Organizovale su preuzimanje tiro računa preduzeća i obavljanje poslova platnog prometa, pružajući viši nivo i kvalitet usluga, uz afirmaciju koncepta „u susret klijentu“. Postojeće osnovne informacione sisteme (engl. *core-banking*) sada nadograđuju sa novim slojem aplikacija za podršku elektronskom poslovanju sa privredom i stanovništvom.

Trenutna IT infrastruktura nije nerazvijena. Većina banaka „zasipa“ svoje trenutne i potencijalne korisnike reklamama u kojima su baš oni lideri na polju e-bankarstva, pri čemu svaka potencira svoje najbolje rešenje za e-bankarstvo. Tendencije idu ka tome da u budućnosti svi subjekti budu elektronski povezani, da banke proširuju asortiman usluga koje pružaju elektronskim putem uz optimalnu dinamiku promena. Opšta konkurencija podstiče pojedinačne banke u nastojanju da ponude što više pogodnosti za svoje klijente.

Veoma je izražena podrška vladinih programa u oblasti platnih kartica (kartičarstvo). Vlada ima direktan interes da pruži ovu podršku, zbog toga što svaka ovakva transakcija predstavlja legalan tok gotovine koji sa sobom nosi fiskalni račun i naplatu poreza.²⁸⁶

Asortiman ponude e-bankarstva se drastično širi u kratkom vremenskom periodu. Banke svojim klijentima omogućavaju: uvid u stanje računa, pregled prometa, pregled izvoda promena na računu, prijem i slanje ličnih poruka, plaćanje obaveza platnim nalogima sa tekućim datumima i datumima unapred. Pojavljuju se mogućnosti korišćenja usluga platnog

²⁸⁴ Pregled Press Clippinga za klijenta Politika-Ekonometar str.6-Mobilno plaćanje

²⁸⁵ Isto, str.6

²⁸⁶ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.238

prometa putem bankomata, platnih kartica, POS terminala banaka, Call Centra i mobilnih telefona (SMS).

Suština nuđenja servisa e-bankarstva (posebno kada su u pitanju građani) jeste da se njima obezbedi dostupnost preko celog dana, bez posete banci i ograničenja radnog vremena. Velike firme su u većem broju korisnici usluga e-bankarstva, što je dobrim delom rezultat stečenih iskustava korišćenjem „udaljenog ulaza“ preko terminala iz svojih poslovnih prostorija kad su radile preko ZOP-a. Za male firme e-bankarstvo postaje sve atraktivnije, jer baš zato što su male one mogu niz poslova da obavljaju ne napuštajući svoje radne prostorije, a imaju neprekidno uvid u stanje svog računa.

Banke će u narednom periodu ulagati mnogo više u promociju elektronskog bankarstva u radu sa stanovništvom. Naši građani su već prihvatili sisteme elektronskog plaćanja jer štedi vreme, dostupan je 24 časa sa bilo kog mesta ili uređaja, a stanovništvo rado prihvata sve što olakšava svakodnevni život. Građane je ipak potrebno obrazovati u primeni elektronskog bankarstva, što će doprineti popularnosti e-bankinga, a uz snižavanje tarife elektronskih transakcija u odnosu na šalterske transakcije učiniće se da on postane preovlađujuć način plaćanja građana. Treba da težimo da budemo lideri u ovoj oblasti i da se poredimo sa savremenim svetom, jer je tu prostor za napredovanje ogroman.²⁸⁷

Iako su mnogi ljudi u Srbiji i dalje izuzetno skeptični kada je u pitanju sigurnost pri korišćenju elektronskog bankarstva, za šest godina, koliko se ovaj sistem koristi u našoj zemlji, nije zabeležen ni jedan slučaj prevare. Neophodno je, ipak, obrazovati korisnike, napominju bankari, kako se ne bi desilo da lako upadnu u hakerske zamke kojih će u budućnosti neminovno biti.

Paralelno sa ekspanzijom upotrebe elektronske banke „razvila“ se i mogućnost prevara u ovom domenu poslovanja. Banke u Srbiji su sa određenim kašnjenjem startovale sa ponudom ove vrste servisa, ali su to iskoristile kao prednost i poučene iskustvom banaka sa Zapada, uvele prilično sigurne sisteme zaštite za servise elektronske banke. U Srbiji su trenutno u primeni metode korisničke autentifikacije i transakcione autorizacije pri korišćenju elektronske banke, kojima je u startu sprečena mogućnost prevare.

Najrasprostranjenija i skoro stopostotna zaštita je SSL (engl. *Secure Socket Layer*) protokol, koji obezbeđuje šifrovan prenos podataka, kako korisnika tako i servera.

I pored toga broj ljudi u Srbiji koji koriste prednosti elektronskog bankarstva, poput detaljnog uvida u sopstveni bankovni račun i mogućnost plaćanja računa preko Interneta, još uvek je mali. Ekspanzija plaćanja putem elektronskog bankarstva tek se očekuje.

Prihvatanjem prakse e-poslovanja, Srbija mora da iskoristi nove ekonomske mogućnosti koje se otvaraju sa ciljem da:²⁸⁸

- Promoviše privredni rast i socijalni razvoj,
- Unapredi poslovnu efikasnost i produktivnost,
- Smanji troškove poslovanja,
- Omogući domaćim kompanijama lakšu reintegraciju u evropsko i svetsko tržište.

²⁸⁷ Pregled Press Clippinga za klijenta Politika-Ekonometar str.6-Mobilno plaćanje

²⁸⁸ www.conopljanews.net/ebankarstvo.html

Primenom e-bankinga u različitim sektorima nacionalne privrede povećava se povezanost i mećuzavisnost računarskih mreća privatnih i javnih organizacija ukljućenih u domaće i mećunarodne ekonomske aktivnosti. Na ovaj naćin, nacionalna privreda se kreće iz faze interaktivnog delovanja autonomnih subjekata ka fazi integrisanog sistema za upravljanje informacionim tokovima u privredi, što joj daje karakteristike e-ekonomije, ili društva zasnovanog na informacijama (informacionog društva). U savremenoj eri globalnog razvoja svetske privrede i društva, e-poslovanje postaje pokretać svetskog privrednog porasta. Izostanak primene e-poslovanja vodi ogranićavanju razvoja nacionalne privrede.

2. MEĆUBANKARSKI PLATNI SISTEM U SRBIJI

Poćetkom januara 2003. godine realizovan je jedan od najvećih sistemskih projekata u Srbiji. Platni promet je iz Zavoda za obraćun i plaćanja prenet u poslovne banke. Novi sistem platnog prometa u celini ispunjava svih deset osnovnih principa poslovanja, koje je u dokumentu *Core Principles for Systemically Important Payment Systems*, ustanovila Banka za mećunarodna pravnanja (BIS).²⁸⁹

Elektronski platni promet u Srbiji se obavlja razmenom elektronskih poruka kroz informacione sisteme ućesnika u transakciji plaćanja. Elektronska poruka je informacija, koja je elektronski generisana, proverena, poslata, primljena i saćuvana elektronski. Elektronski prenos novćanih sredstava izmeću ućesnika u platnom prometu, smatra se elektronskom platnom transakcijom. Elektronski nalog za plaćanje mora da sadrţi elemente utvrćene odlukom kojom se urećuju oblik, sadrţina i naćin korišćenja jedinstvenih instrumenata platnog prometa, kao i elemente za proveru autentićnosti i taćnosti tih naloga i autentićnosti njihovih podnosilaca.

U elektronskom platnom prometu izmeću Narodne banke Srbije i banaka koje ućestvuju u mećubankarskom obraćunu, NBS obezbećuje elektronsku razmenu podataka i njihovu zaštitu. Narodna banka Srbije, usluge elektronskog platnog prometa vrši preko informatićeke infrastrukture za obavljanje platnog prometa Republike Srbije. Elektronska platna transakcija smatra se okonćanom kad krajnji subjekt primi elektronsku poruku. Elektronska poruka se smatra primljenom kada pošiljalac primi potvrdu o njenom prijemu.

Validna elektronska poruka je svaka elektronska poruka propisanog formata, koja je overena elektronskim potpisom i primljena, za koju se utvrdi da sadrţi podatke koji nisu menjani od trenutka slanja te poruke – ako je njen pošiljalac registrovani ućesnik u elektronskom platnom prometu, odnosno ovlašćeno lice tog ućesnika. Ućesnik u elektronskom platnom prometu, obaveze preuzima na osnovu validne elektronske poruke, odnosno na osnovu njene izmene ili opoziva.

Domaći platni promet obuhvata:²⁹⁰

- Mećubankarski platni promet – koji se obavlja izmeću ućesnika u RTGS (engl. *Real Time Gross Settlement*) i kliring sistemu NBS i
- Interni platni promet – koji se obavlja izmeću klijenata koji imaju otvorene raćune kod iste banke.

²⁸⁹ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.137

²⁹⁰ Isto, str.137

Obračun u realnom vremenu po bruto principu (RTGS) obavlja Narodna banka Srbije – za učesnike u RTGS sistemu.

Učesnici u RTGS sistemu su:

1. Narodna banka Srbije,
2. banka koja poseduje dozvolu za rad Narodne banke Srbije i upisana je u sudski registar,
3. Republika Srbija (ministarstvo nadležno za poslove finansija, učestvuje preko konsolidovanog računa trezora koji se vodi kod Narodne banke Srbije),
4. Centralni registar, depo i kliring hartija od vrednosti,
5. Udruženje banaka Srbije.

RTGS sistem (obračun u realnom vremenu po bruto principu) podrazumeva prijem i izvršavanje pojedinačnih naloga u najkraćem mogućem vremenu od momenta njihovog prijema i to do visine pokrića na računu. U RTGS-u se mogu izvršavati svi nalozi za plaćanje, s tim što se obavezno izvršavaju nalozi za plaćanje koji glase na iznose veće od 200.000 dinara („velika plaćanja“), a što je utvrđeno operativnim pravilima za RTGS i kliring. Navedena plaćanja realizuju se u realnom vremenu, porukama SWIFT formata MT103 (klijent jedne banke – klijentu druge banke) i MT202 (banka - banci). Realizacijom RTGA transakcije u realnom vremenu se menja stanje na računu banke, odnosno drugog učesnika RTGS i kliring sistema.²⁹¹

Pod kliringom, odnosno neto obračunom, podrazumeva se prijem pojedinačnih naloga za plaćanje, ili grupa naloga za plaćanje, uz koje se dostavlja specifikacija pojedinačnih naloga, radi obračuna multilateralnih neto iznosa na obračunskim računima. Nakon toga, za svakog učesnika u kliringu se utvrđuje neto pozicija, čije se poravnanje vrši preko njegovog čiro računa. Plaćanja u kliringu („mala plaćanja“) su nalozi čiji je iznos do 200.000 dinara i „pakuju“ se u poruke SWIFT formata MT102. U jednoj poruci MT102 može biti do 100 naloga za plaćanje. Plaćanja u kliringu izvršavaju se u procesu neto poravnanja u tri klirinška ciklusa svakog radnog dana (u 11⁰⁰, 13³⁰ i 16¹⁵ časova).

Učesnici u RTGS i kliring sistemu NBS povezani su u jedinstvenu celinu u kojoj se platne transakcije razmenjuju porukama, zasnovanim na SWIFT standardu, kroz privatnu komunikacionu mrežu NBS.

NBS je operator i vlasnik RTGS i kliring sistema, konfigurisanih kao jedan sistem, na jednoj platformi. Sistem je fleksibilan u smislu postojanja mogućnosti razdvajanja RTGS-a i kliringa na odvojene sisteme, na dve platforme.

NBS je od januara 2005. godine učesnicima ponudila novi servis – izvršavanje „malih, klirinških plaćanja“ u RTGS sistemu, po Tarifi za klirinška plaćanja. To je omogućilo bankama sa boljom likvidonosnom pozicijom da izvršavaju plaćanja putem RTGS sistema, ne čekajući klirinški ciklus, a po toj Tarifi. Servis je doživio uspeh i široko je prihvaćen od strane učesnika u sistemu. Ilustrativan je podatak da je tokom prvog meseca udeo navedenih plaćanja u ukupnim plaćanjima iznosio 7%, da bi ga vremenom sve veći broj banaka počeo koristiti, tako da je 2008. godine učešće ovih plaćanja u ukupnom broju transakcija iznosilo

²⁹¹ Isto, str.138

56,82%. To je, naravno, uticalo i na učešće klirinških plaćanja u ukupnom broju plaćanja koje je sa 51,92%, koliko je iznosilo u 2007. godini, palo na 43,18% u 2008.godini.²⁹²

WAN mreža NBS pokriva teritoriju Republike Srbije. Kao prenosni putevi se koriste resursi domaćeg telekomunikacionog provajdera. Na teritoriji Republike Srbije se nalaze četiri mreža na čvora koja nude različite tehnologije pristupa (*frame relay*, *ISDN*, *lise line* i *dial-in*). Poslovne banke se uključuju u mrežu u NBS posredstvom najbližeg mrežnog čvorišta. U mreži se koristi *TCP/IP* komunikacioni protokol. Podaci u platnom prometu se šifruju, a zatim transportuju kroz mrežu. *SWIFT* mreža može služiti kao *back up* *WAN* mreži i NBS i obratno, jer je *SWIFT* format poruka primenjen i u *WAN* mreži i NBS. Poruke kojima se izvršavaju plaćanja u RTGS sistemu su *SWIFT* poruke: MT103 (klijent banke-klijentu banke), MT202 (učesnik-učesniku) i MT102 („mala plaćanja“ u RTGS-u). Odmah posle izvršenja transakcije, sistem upućuje pošiljaocu odgovarajuću poruku o izvršenom obračunu, nakon čega se transakcija smatra konačnom. Učesnici elektronskog platnog prometa dužni su da elektronsku poruku čuvaju najmanje 5 godina posle isteka godine u kojoj je izvršena elektronska platna transakcija, kao i podatke i sredstva za verifikaciju autentičnosti te poruke. Za proveru autentičnosti elektronskih poruka i ispravnosti prenosa tih poruka kroz mrežu u NBS, koristi se tehnologija javnih ključeva. NBS vrši sertifikaciju javnih ključeva i učesnici svoje javne i tajne ključeve generišu softverom koji im obezbeđuje NBS. Banke i njihovi klijenti ugovorom uređuju način i uslove međusobne razmene elektronskih poruka. NBS je donela Odluku o elektronskom načinu obavljanja platnog prometa,²⁹³ a donet je i Zakon o elektronskom potpisu²⁹⁴ i Zakon o elektronskom dokumentu.²⁹⁵

Arhitekturu informacionog sistema platnog sistema NBS čine:²⁹⁶

1. Centralni računar (engl. *Cluster Site*);
2. Računar za razvoj (engl. *Test Site*);
3. Računar za podršku (engl. *Disaster Recovery Site*), čije je korišćenje predviđeno za vanredne situacije (elementarne nepogode i sl.).

Platni sistem, sa stanovišta logičke i funkcionalne organizacije, čine četiri celine:

1. Produkcioni sajt (engl. *Main Site*);
2. Hot Backup Site;
3. Remote Backup Site (engl. *Cold Backup Site*);
4. Test site.

Na ovakvoj funkcionalnoj arhitekturi NBS zasniva *Business Continuity* plan platnog sistema, u kojem su definisane procedure koje, zajedno sa implementiranim tehnologijama, obezbeđuju da kritični radni procesi ostanu raspoloživi, ili da se veoma brzo vrate u funkciju, u slučajevima poremećaja koji uzrokuju neraspoređivost dela informacione infrastrukture ili celog računskog centra (vanredne okolnosti, kao što su prirodne katastrofe i sl.).

²⁹² www.nbs.rs

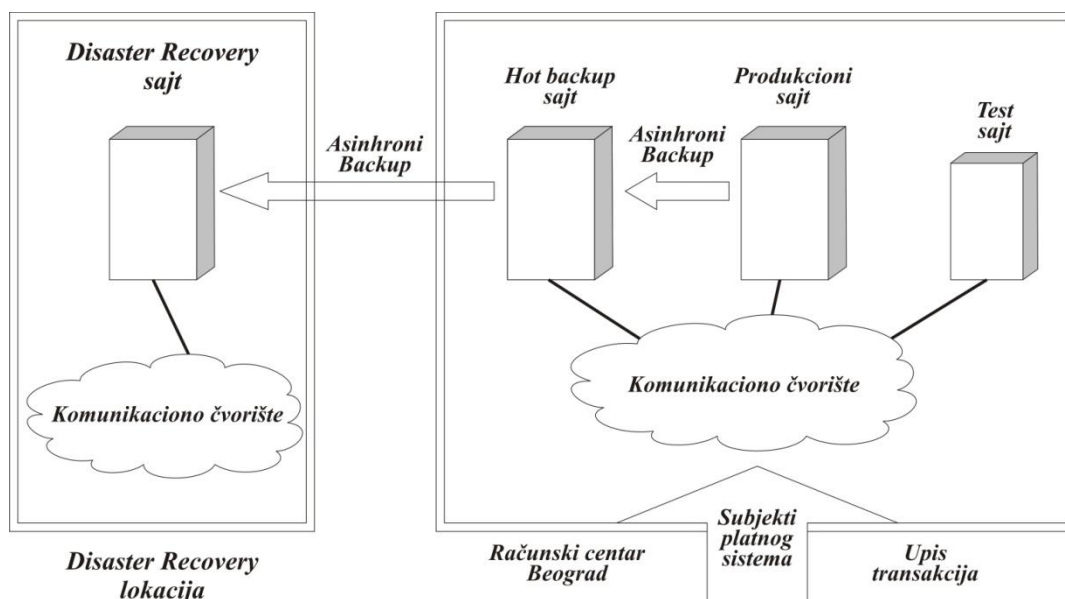
²⁹³ „Sl. glasnik RS“ br.57/04

²⁹⁴ „Sl. glasnik RS“ br.135/04

²⁹⁵ „Sl. glasnik RS“ br.51/09

²⁹⁶ Stankić R.: „Elektronsko poslovanje“, cit.delo, str.13

Slika 6: Arhitektura informacionog sistema platnog sistema NBS



3. KREDITNI BIRO

U okviru Udruženja banaka Srbije osnovan je 2004.godine Kreditni biro, sa ciljem praćenja boniteta fizičkih lica – bankarskih klijenata na nacionalnom nivou.

Potreba organizovanja poslova praćenja boniteta bankarskih klijenata kod nas je postala realnost, s obzirom na to da stepen finansijske discipline neposredno utiče na nivo likvidnosti banaka, a ima i uticaja na visinu aktivnih kamatnih stopa u smislu njihovog smanjenja.

Krajnji cilj koji se postiže organizovanjem poslova praćenja, otkrivanja i suzbijanja finansijske nediscipline se ogleda u povećanju stepena urednosti i izmirivanju obaveza građana prema bankama, jer se na ovaj način deluje preventivno na savest klijenata, sprečava se njihovo seljenje iz banke u banku, a sudsko gonjenje prestaje da bude osnovno sredstvo zaštite bankarskog kapitala.

Osnivanje ove institucije je sastavni deo priprema za primenu Bazela II i usklađivanja sa direktivom Evropskog parlamenta i Saveta za harmonizaciju u vezi sa potrošačkim kreditima. Koncept organizovanja Kreditnog biroa bazira se na zapadnoevropskim modelima, a posebno Nemačke („Shoufa“), sa neznatnim razlikama. Takva organizacija treba da omogući razvoj saradnje sa drugim evropskim institucijama za zaštitu kredita. Tehničko-tehnološku i organizacionu infrastrukturu izradila je firma *BELIT*, a sama rešenja se baziraju na Majkrosoftu.²⁹⁷

Celokupan sistem odnosa između Kreditnog biroa, kao institucije za zaštitu kredita i banaka, funkcioniše na principu uzajamnosti. Kreditni biro Udruženja banaka Srbije obavlja sledeće poslove:

²⁹⁷ Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.240

- Prikupljanje podataka o bankarskim klijentima (fizičkim licima) o njihovoj kreditnoj zaduženosti i o njihovoj urednosti u izmirivanju obaveza prema bankama i ostalim poveriocima,
- Vođenje jedinstvene baze podataka o bonitetu klijenata,
- Analiziranje zloupotreba od strane bankarskih klijenata i predlaganje mera za sprečavanje tih zloupotreba i
- Davanje izveštaja o bonitetu bankarskih klijenata bankama i drugim kreditorima članicama Kreditnog biroa.

Korišćenje izveštaja o bonitetu fizičkih lica prilikom zaključivanja ugovora o kreditu je obaveza svake banke kreditora. Ova obaveza proizilazi iz predloga direktive Evropskog parlamenta i Saveta o harmonizaciji propisa zemalja članica u vezi sa potrošačkim kreditima.

Izveštaj sadrži četiri grupe podataka:

- Identifikacione podatke o licu na koji se izveštaj odnosi (ime i prezime, adresa stanovanja, JMBG, broj lične karte, socijalni status),
- Iznose ukupnih zaduženja po kreditima kod banaka i drugih kreditora,
- Iznose nedozvoljenog prekoračenja po tekućim računima građana i platnim karticama i iznosu dospelog, a neplaćenog kredita,
- O bankama i drugim kreditorima koji su tražili izveštaj.

Na osnovu Izveštaja dobijenog od Kreditnog biroa, odnosno podataka sadržanih u Izveštaju, banka donosi odluku o tome da li će konkretnom podnosiocu zahteva pružiti traženu uslugu.

Konekcija banaka sa Kreditnim biroom je moguća putem računarskog dijaloga UBS (KBDA) ili Kreditni biro UBS online (prilaz Internetom), preuzimanjem, poštom, faksom i telefonom. Bezbednost sistema podržana je sistemom elektronskih sertifikata na smart kartici, odnosno na nivou kriptografske SSL zaštite, koja omogućava potpunu bezbednost prenosa podataka, kao i pristup bazi podataka samo ovlašćenim licima (dvostepena autorizacija i identifikacija). U skladu sa tim mehanizmom, elektronska dostava u realnom vremenu vrši se samo onim korisnicima koji su sertifikovani od udruženja. Dokumenti za razmenu podataka između banaka i IS Kreditnog biroa su u XML formatu, elektronski potpisani sa elektronskim sertifikatima na smart kartici. Za dalje razvijanje tržišta zajmova biće značajno automatizovanje procesa prijavljivanja za zajmove i njihovo dobijanje, u skladu sa svetskom praksom. Time bi se obezbedilo da banke brže procesiraju zahteve i prate izvršenje, a klijenti dobijaju bolji prikaz onoga što je u ponudi i šta mogu da biraju.²⁹⁸

Upravljanje i razvoj ovih poslova je u nadležnosti Saveta, čiji članovi su iz banaka članica Udruženja banaka, čime su obezbeđene potrebne pretpostavke da se taj razvoj odvija u skladu sa interesima, pre svega banaka.

Podršku za organizovanje ovih poslova dali su Narodna banka Srbije i Ministarstvo finansija.

²⁹⁸ Isto, str.240

4. PLATNE KARTICE

Prva platna kartica u Srbiji bila je „Diners“ i izdata je još 1969. godine. Sve do 1990. godine naša zemlja je po broju korisnika platnih kartica bila blizu razvijenim zemljama. Bivša Jugoslavija imala je daleko veći broj korisnika plastičnog novca, nego Grčka i tadašnje zemlje istočnog bloka. Međutim, u periodu od 1992. godine do 1996. godine u Srbiji nije bilo nijedne izdate kartice. „Diners club international“ ponovo počinje da izdaje kartice 1996. godine, a 2000. godine upotrebu internacionalnih Master kartica uvele su *Societe general* i tadašnja *Delta banka* i broj korisnika kartica u našoj zemlji od tada se ubrzano uvećava.

Upotreba platnih kartica u našoj zemlji bila je prilično skromna do 2002. godine, odnosno do uvođenja svih platnih transakcija u regularne novčane tokove – banke. Danas je ovaj način plaćanja uveliko popularizovan i omasovljen. Bez kartice ne može se ni zamisliti kupovina, putovanje ili kupovina na odloženo (popularni revolving), ili pak podizanje gotovine na bankomatima, ili plaćanje robe i usluga putem Interneta.

Tržište platnih kartica u Srbiji razvija se znatno brže nego bilo koje tržište u regionu (prema oceni predstavnika MasterCard-a). Za tri godine dostignut je razvoj za koji je u drugim delovima regiona bilo potrebno deset godina. Danas je broj izdatih kartica 12 puta veći od broja izdatih kartica pre četiri godine. Ovakva situacija daje nade da će biti u relativno kratkom vremenu nadoknađeno desetogodišnje nazadovanje u ovoj oblasti.

Praktično sve banke izdaju po nekoliko vrsta inostranih i domaćih platnih kartica. Od međunarodnih platnih kartica najzastupljenija je VISA koja je, nakon povratka posle desetogodišnjeg odsustva, za 3 godine dostigla milion izdatih kartica u Srbiji (upoređenja sa drugim zemljama pokazuju da je brži rast zabeležen jedino u Kini). Od ostalih platnih kartica po značaju zatim dolaze MasterCard i Diners i nešto manje American Express. Na domaćem terenu veoma intenzivno se razvija sistem DinaCard.²⁹⁹

Nacionalni „DinaCard“ sistem je osnovan u 2003. godini, u saradnji Narodne banke Srbije sa poslovnim bankama. Cilj njegovog pokretanja bio je ubrzani razvoj bezgotovinskog načina plaćanja, smanjenje gotovine u novčanoj masi i suzbijanje sive ekonomije.

Korišćenje platnih kartica u Srbiji od 2004. godine prosto je eksplodiralo. Nakon intenzivnog razvoja u 2005. i 2006. godini, poslovanje banaka sa platnim karticama u Srbiji u 2007. i 2008. godini je karakterisalo nešto umereniji, ali stabilan rast. Ukupan broj izdatih kartica u 2008. godini iznosio je 5,72 miliona. Od ukupnog broja izdatih kartica 79,4% čine debitne, 18,9% kreditne i 1,7% poslovne kartice.³⁰⁰

Cenovne i druge pogodnosti omogućile su znatnu difuziju sistema DinaCard, tako da je danas ona na drugom mestu po broju izdatih kartica, odmah iza internacionalne VISA kartice. Na tržištu platnih kartica u zemlji, DinaCard sistem je sa preko 24 miliona ostvarenih transakcija i preko 67 milijardi dinara prometa zadržao visoko učešće. Po ukupnom broju transakcija, DinaCard sistem zauzima trećinu tog tržišta, dok učešće DinaCard sistema u broju međubankarskih transakcija iznosi čak 42% u poslednjem tromesečju 2008. godine. Sistem je kraj 2008. godine dočekao sa 2,5 miliona izdatih kartica, što predstavlja 44% svih izdatih kartica u zemlji.³⁰¹

²⁹⁹ Isto, str.241

³⁰⁰ www.dinacard.nbs.rs/sr/news.html

³⁰¹ Isto

Broj platnih kartica svakodnevno raste, pa se na osnovu prakse zemalja sličnih Srbiji, zaključuje da postoji potencijal za izdavanje čak 14 miliona platnih kartica. Danas polovina građana Srbije starijih od 18 godina poseduje bar jednu platnu karticu. Pre dve godine taj procenat je iznosio oko 36%, a 2004. godine samo 7% stanovništva koristilo je ovaj oblik plaćanja. Razvoju tržišta platnih kartica svakako doprinosi i jaka konkurencija banaka koje se bore za svakog novog klijenta, kako neprekidnim inovacijama po pitanju proizvoda, tako i sve većim pogodnostima kada je reč o cenama.

Platne kartice u Srbiji postaju sve zastupljeniji način plaćanja, iako gotovina i dalje čini najveći deo prometa. Udeo kartica u prometu sve više se povećava. U strukturi transakcija karticama najveće učešće su imale debitne kartice 82,3%, dok kreditne kartice učestvuju sa 14,4%, a poslovne sa 3,3%. Prema podacima Narodne banke Srbije, promet transakcija platnim karticama izdatim u Srbiji u 2008. godini iznosio je 312,0 milijardi dinara.

Potrošačke navike u Srbiji se izjednačavaju sa navikama mnogih evropskih suseda, gde se većina transakcija platnim karticama obavlja na prodajnim mestima. Građani Srbije postaju sve aktivniji korisnici platnih kartica: imaju više kartica, koriste ih češće nego pre nekoliko godina i platne kartice ih asociraju na pozitivne stvari. Istraživanje „Master Index“ koje je kompanija „MasterCard“ sproveda u Srbiji u ovoj godini, pokazalo je da 11% korisnika platnih kartica koristi svoje kartice svakodnevno, dok ih 24% koristi nekoliko puta nedeljno. Skoro 50% vlasnika platnih kartica ima i debitnu i kreditnu karticu. Platne kartice preuzimaju ulogu plaćanja i kreditiranja. Sa povećanjem broja transakcija, dolazi do povećanja prihoda banaka, ali i preduzeća koja ih obrađuju.

Bezbednost plaćanja karticama u Srbiji je na istom nivou kao bilo gde u svetu. Sve „MasterCard“ i „Maestro“ platne kartice u Srbiji imaju najnoviju CHIP-EMV tehnologiju, koja obezbeđuje najviši nivo bezbednosti.

„MasterCard“ je lansirao „PayPass“ tehnologiju za beskontaktno plaćanje u partnerstvu sa „Intesa bankom“ i „Delta City“ šoping centrom u decembru 2008. godine. Maestro®PayPass™ gift kartica je prva kartica u ovom regionu koja ima ugrađenu inovativnu „PayPass“ tehnologiju za beskontaktno plaćanje i takođe je prva dopunjiva gift kartica u Srbiji. „PayPass“ omogućava korisnicima plaćanje manjih suma, uglavnom ispod 25 evra, bez potrebe da se izvrši autorizacija unošenjem PIN-a ili potpisivanjem. Ovo značajno ubrzava transakcije, što je veoma korisno kada su u pitanju mesta gde je broj transakcija veliki kao što su sportski stadioni, restorani brze hrane ili javni prevoz.

Čip tehnologija je sve zastupljenija u savremenom korišćenju platnih kartica. U Srbiji je ova tehnologija počela da zauzima značajno mesto u bankarskom kartičarstvu od 2003. godine. Zanimljivo je da je te godine izdata prva serija čip platnih kartica na Balkanu i to baš u Srbiji, od strane Vojoćanske banke. Čip tehnologija omogućava maksimalnu sigurnost plaćanja, jer čipovi garantuju daleko veću zaštitu od bilo kakvog pokušaja zloupotrebe.

Visoka međubankarska konkurencija dovela je do znatnog snižavanja kriterijuma za izdavanje platnih kartica, posebno debitnih. Izdavanje debitne kartice, banke po pravilu vezuju za posedovanje tekućeg računa i daju ih besplatno (bez naplate troškova izrade i članarine).

Izdavanje kreditnih kartica je slobodnije i nosi sobom plaćanje članarine, troškova održavanja računa i kamate na korišćeni kredit (koji se najčešće javlja u varijantama revolving kredita). Za izdavanje kreditne kartice, radi se analiza klijenta i njegove kreditne sposobnosti.

Trenutno su u opticaju dileme o realnim mogućnostima masovnog korišćenja kreditnih kartica, zbog materijalnog nivoa većeg dela stanovništva, posebno ako se ima u vidu da se kamate najčešće kreću na mesečnom nivou od 1,95% - 2,20%. Međutim, dok materijalni nivo stanovništva i visina kamate mogu delovati ograničavajuće, nivo postojeće kreditne zaduženosti deluje suprotno. Visina zaduženosti stanovništva je znatno ispod proseka zaduženosti u regionu (posmatrano po stanovniku, ona u Srbiji iznosi 100 evra, u Hrvatskoj 2.000 evra, a u Sloveniji 3.000 evra).³⁰²

Kod izvesnog broja analitičara prisutan je strah od nekontrolisane kreditne ekspanzije, po osnovu korišćenja kreditnih kartica u narednom periodu. Sa druge strane, ekspanzija kreditnih zaduženja vrši se pod adekvatnom kontrolom, zahvaljujući funkcionisanju Kreditnog biroa, kod koga je evidentirano ukupno pojedinačno zaduženje svakog pojedinca. Prema postojećoj odluci Centralne banke, dozvoljeno kreditno zaduženje svakog korisnika je 30% mesečnih prihoda, a Kreditni biro ima zadatak da spreči probijanje limita propisanih odlukom Centralne banke.

Kreditni biro osnovan je pri Udruženju banaka Srbije i raspolaže informacijama o kreditnoj istoriji svakog pojedinca (podaci o ranijim kreditima, korišćenju tekućeg računa, poslovanju sa debitnim i kreditnim karticama, lizingu, pa čak i ižirantima). Procedura izdavanja kreditne kartice podrazumeva, davanje saglasnosti banci za pribavljanje pomenutih informacija od Kreditnog biroa, pri podnošenju zahteva za dobijanje kreditne kartice. Inače, sve ove informacije korisnici mogu dobiti i na lični zahtev, radi ličnog uvida u svoju kreditnu poziciju.

Difuzija kreditnih kartica je počela u januaru 2006. godine, kada su one zamenile upotrebu čekova za realizaciju odloženog plaćanja. Država je imala poseban interes za ponovnim svođenjem upotrebe čekova na funkciju instrumenata plaćanja i prenošenje kreditiranja na kreditne kartice, u kontekstu borbe protiv sive ekonomije i legalizacije novčanih tokova, sa svim pozitivnim ekonomskim efektima koje oni sobom nose.

Udruženje banaka Srbije zajedno sa još 12 banaka osnovalo je jula 2004. godine „čip card“ centar koji pruža usluge izdavanja platnih kartica, autorizacije, obrade transakcija, povezivanje sa POS terminalima i ATM, procesuiranje domaćih i stranih platnih kartica. Kada podatke o korisniku kartice banka unese u svoj sistem i prenese „čip card-u“, ovaj centar poseduje sve podatke o korisniku kartice i njegovim pravima. Ako korisnik izgubi karticu u centru se i o tome vodi evidencija, kao i roku trajanja platne kartice.

U Centru postoje podaci o svim transakcijama koje korisnik obavlja platnom karticom (kupovinama ili podizanju gotovine). Centar rešava i probleme sa eventualnim reklamacijama, pronalazi sve obavljene transakcije i otkriva moguće greške prilikom obavljanja plaćanja. Procesing, u stvari, podrazumeva dnevne obrade transakcija, rešavanje reklamacija, unos i ažuriranje podataka korisnika kartica, bankomata i POS terminala. Centar kontroliše rad i nadgleda bankomate i radi odobrenja za transakcije na osnovu limita ili stanja na računu korisnika kartice. Centar je dobio licencu procesora Visa za rad sa karticama sa magnetnom pistom.

Centar je sa domaćim bankama povezan *on line* vezama, jer sa izdavanjem brojnih kartica postoji mogućnost da korisnik računa zloupotrebi uslugu banke, pa isti novac može da

³⁰² Vuksanović E.: „Elektronsko bankarstvo“, cit.delo, str.242

podigne na bankomatu, a zatim na šalteru banke. Transakcija obavljena na bankomatu dolazi u Čip card, koji je kroz zaštićene kanale šalje do zaštićene aplikacije i vraća do banke. U bankarskoj aplikaciji se rezerviše taj novac i rezervacija se prikazuje na bankomatu pa korisnik ne može više da ga podiđe. Blokira se mogućnost zloupotreba i dizanje istog novca dva puta. Smanjenju zloupotreba doprineće i kartice sa čip tehnologijom, koje od 2006. godine izdaje nekoliko domaćih banaka.

Na kraju 2007. godine bankama u DinaCard sistemu je omogućeno da svojim korisnicima ponude uslugu prijema novca iz inostranstva. U ovom trenutku, tu uslugu nudi pet banaka, a očekuje se da i ostale banke u sistemu uskoro u svoju ponudu uvrste servis prijema novca. Planirano je da se uskoro korisnicima omogući da putem mobilnog telefona plaćaju račune - pre svega postpejd račune za mobilne telefone, a nakon toga i račune za fiksne telefone, struju, komunalije, bežični Internet i slično.³⁰³

U cilju dalje difuzije, vode se pregovori za kobrendovanje ove kartice za njeno delimično korišćenje u inostranstvu. Planirano je da se u narednom periodu sprovedu aktivnosti na omogućavanju njihovog korišćenja preko Interneta.

5. TRGOVINA NA INTERNETU

Kupovina i prodaja robe preko Interneta, koja je uobičajena u svetu, u Srbiji još nije zaživela u punoj meri. Uprkos raznim pogodnostima i popustima koje elektronska trgovina pruža kupcima, broj korisnika ovog načina trgovanja u Srbiji je skoro zanemarljiv. Oko 135.000 građana Srbije, odnosno manje od dva procenta, je tokom 2007. godine kupovalo robu i usluge preko Interneta. U odnosu na 2006. godinu, broj onih koji su kupovali putem Interneta, povećao se samo za 30.000, iako je takav način transakcija u svetu odavno prepoznat i primenjen, kao vrlo praktično rešenje za plaćanje roba i usluga. U Nemačkoj je, primera radi, prošle godine preko Interneta platilo neku uslugu ili robu, čak 30 miliona građana, odnosno 41 procenat. U okruženju je situacija slična kao i u Srbiji.

Uzrok male tržišne tražnje za ovakvom vrstom usluga je to što u Srbiji mali broj stanovnika koristi Internet (oko 1,7 miliona korisnika), ali i to što nisu sve kartice ovlašćene za Internet kupovinu, pa je proizvode koji se nude na sajtovima moguće platiti samo popunjavanjem uplatnice u banci ili pošti. Jedan od glavnih razloga je zastarela i neadekvatna zakonska regulativa, nespremnost banaka da preuzmu rizik poslovanja preko Interneta, ali i nedovoljna informisanost građana i preduzeća o e-trgovini. Svega nekoliko desetina domaćih kompanija nudi kupovinu i prodaju preko Interneta.

Za plaćanje putem Interneta u Srbiji, korisnici se mogu opredeliti za Visa, Master i American Express kartice koje izdaje banka Intesa ili Visa virtuelnu karticu koju izdaje Raiffeisen banka. Te kartice su u svetu priznate kao sredstvo plaćanja, pa je kupovina u stranim Internet trgovinama umnogome olakšana njihovom pojavom.

Banka Intesa je postala zvanična banka „akvajerer“ za Srbiju, što znači da ima licencu da izdaje Visa i Master kartice namenjene upravo plaćanju preko Interneta. Kada korisnik kupuje nešto na nekom od dvadesetak domaćih sajtova koji sa Intesom imaju zaključen ugovor, sa sajta trgovca, kupac biva preusmeren na sajt banke gde ostavlja lične i podatke o kartici, posle

³⁰³ www.nbs.rs

čega nastavlja proceduru na sajtu trgovca. Reč je o sigurnoj tehnologiji koja omogućuje bezbednost novčanih transakcija na Internetu.

Glavna prepreka široj upotrebi kartica za plaćanje na Internetu u Srbiji, je strah ljudi od prevare. Međutim, ukoliko se korisnici pridržavaju uputstava stručnjaka, znatno će se smanjiti rizik da budu prevareni prilikom plaćanja na Internetu. Najvažnije je proveriti kredibilitet sajta sa koga naručujete robu ili usluge. Prvo treba proveriti kakvi kontakti postoje na sajtu. Ukoliko nema kontakata, koji ukazuju na to da firma zaista fizički postoji, ne treba kupovati na tom sajtu. Korisnik vrlo lako može zaključiti da li je sajt bezbedan i po tome da li su poverljivi podaci korisnika šifrovani. Naime, ukoliko vam se kada popunjavate formular za kupovinu neke robe na sajtu, u donjem desnom uglu pojavi mali katanac, to znači da su podaci koje ostavljate šifrovani i samim tim bezbedni. Takođe, klikom na taj katanac pojaviće se digitalni sertifikat sajta, kao dokaz njegove sigurnosti, jer se u sertifikatu nalaze svi podaci firme čiji je taj sajt.

Preporučuje se kupovina na renomiranim Internet prodavnicama, koje su prepoznate kao pouzdane i iza kojih je jasno da stoje kompanije koje su u stanju da ispune objavljene uslove kupovine i naručivanja i time garantuju isporuku prodate robe ili usluga. Znači, treba izbegavati manje i nepoznate Internet prodavnice koje nemaju izgrađenu reputaciju. Posebno treba obratiti pažnju na objavljene uslove kupovine i opšte uslove sa kojima se korisnik saglasi pre obavljanja plaćanja. Najvažnije je obučiti ljude, objasniti im kako da postupaju prilikom upotrebe kartica na Internetu.

Kupovina preko Interneta, dakle nije „balk“ niti je toliko nebezbedna koliko se inače misli. Tome u prilog govori sve veći broj ljudi u svetu, ali i u našem okruženju koji se za to opredeljuju. Mnogo više prevara se dogodi prilikom klasičnih trgovinskih aranžmana, nego onih preko Interneta. Dakle, treba biti oprezan i isprobati nešto ekonomičniji način kupovine preko Interneta.

Firme, banke i specijalizovane kompanije neprestano unapređuju bezbednosne tehnologije na ovom polju, jer se i *on-line* poslovanje vrlo brzo širi. Visa i Master-card su nedavno osmislili program zaštite pod nazivom „3D sekjur“. Oni koji žele da plaćaju preko Interneta, učlane se na sajt tih kompanija besplatno i tom prilikom dobiju jedinstvenu šifru, koju će znati samo oni i koju će morati da unesu u formular prilikom svake *on-line* transakcije koju obavljaju pomoću Visa ili Master kartica. Ovakve usluge polako počinju da se primenjuju i u Srbiji.

Građanima u Srbiji nedostaju informacije o prednostima, sigurnosti, ali i o opasnostima elektronskog poslovanja. Neophodno je građane uputiti na mogućnosti raznih pronevera koje se čine u stranim zemljama kada koriste usluge plaćanja putem Interneta. Od izuzetne važnosti je i da zaštite elektronski potpis. Naši građani tek treba da steknu naviku plaćanja iz fotelje, dok firme imaju znatno više informacija i češće koriste usluge e-bankinga. Većina preduzeća plaća robu i usluge putem Interneta.

Naša država treba da pomogne i da se uključi u sveobuhvatnije obrazovanje građana u elektronskom plaćanju, poput Rumunije koja je primenila kompletan program na nivou države za omasovljavanje i uvođenje računara kod građana, jer to je početni korak bez kojeg se ne može govoriti o e-bankingu. Kod nas je do sada osnovano preko 100 test centara u kojima je preko 7.000 građana Srbije steklo informatičku obuku po široko rasprostranjenom

evropskom modelu informatičke pismenosti: ECDL – *European Computer Driving Licence*. Informatičko obrazovanje je premisa, odnosno neophodni uslov daljeg razvoja zemlje.³⁰⁴

Za razvoj elektronskog poslovanja u Srbiji neophodno je usvojiti i dopuniti pravnu regulativu koja uređuje ovu oblast. Među poslednjim zemljama u Evropi doneli smo Zakon o elektronskom potpisu, što je dodatno otežalo rad banaka. U firmama za projektovanje i razvoj informacionih sistema kažu da je Srbiji neophodan i zakon koji bi uredio odnose i odgovornosti u složenim relacijama e-trgovine, gde je u igri više strana, trgovac, kupac, isporučilac i njihove banke. Procenjuje se da bi ovakav zakon doprineo napretku domaćeg elektronskog poslovanja.

6. STUDIJA SLUČAJA U JEDNOJ DOMAĆOJ BANCI

6.1. Primena elektronskog bankarstva u Komercijalnoj banci a.d. Beograd

Komercijalna Banka a.d. Beograd, sa izuzetno visokim rejtingom i imidžom u bankarskim krugovima u Srbiji, od samog početka je vrlo ozbiljno shvatila elektronsko poslovanje i sve što ono donosi, jasno uvidevši perspektive daljeg razvoja jednog ovakvog rešenja i benefite koje ono sa sobom nosi, čime je i postala predvodnik svim ostalim bankama na tržištu.

Osluškujući permanentno potrebe klijenata kao i uvažavajući njihove želje, Banka je konstantno modifikovala i unapređivala svoja rešenja i postavljala uvek nove i više standarde u ovoj oblasti poslovanja. Banka trenutno na tržištu ima najsavremenije elektronske servise iz oblasti korporativnog e-bankarstva i najobuhvatnije web rešenje namenjeno fizičkim licima koje predstavlja rezultat zajedničkog rada na razvoju između banke sa jedne i vendara – proizvođača softvera sa druge strane, što svakako predstavlja pozitivan primer kvalitetnog strateškog partnerstva.

Svesna svoje pozicije na tržištu, kao i činjenice da svojim potezima utiče i na aktivnosti svih ostalih banaka u Srbiji, Banka brižljivo bira svoje poteze i punu pažnju posvećuje edukaciji svojih klijenata i kompletnog okruženja, čime stvara povoljnu klimu za veću primenu elektronskih servisa u odnosu na klasičan oblik bankarskog poslovanja. Lica zadužena za elektronsko bankarstvo u ekspoziturama Banke, u neposrednom kontaktu, upoznaju klijenta – potencijalnog korisnika servisa, sa prednostima korišćenja e-bankinga, a svojim stručnim savetima treba da pomognu klijentima da se odluče za ovaj vid komunikacije sa Bankom.

Kao novitet, Komercijalna banka a.d. Beograd je u svojim ekspoziturama (za sada u eksperimentalnoj fazi u nekoliko beogradskih ekspozitura) uvela specijalizovana mesta nazvana „Kutak za E-banking“, gde će se svi klijenti Banke moći u potpunosti informisati o svemu vezanom za elektronsko poslovanje, kako pravnih, tako i fizičkih lica i gde će ujedno moći sami kreirati svoj web nalog i izmiriti neke svoje obaveze uz asistenciju posebno obučених ljudi koji opslužuju ova radna mesta. Ovako direktan pristup pokazao je odlične rezultate u vrlo kratkom vremenskom periodu, jer kvalitetnim i jasnim odgovorima koje klijenti dobijaju na svako postavljeno pitanje vrlo brzo uviđaju sve prednosti ovakvog načina poslovanja i razbijaju predrasude koje su eventualno imali, a koje su bila posledica neinformisanosti.

³⁰⁴ www.poslovnimagazin.biz/magazin/srbija

Sve je veći broj klijenata koji umesto odlaska na bankarski šalter, plaćanje računa obavljaju, elektronskim putem, koristeći prednosti i pogodnosti koje pruža *on line* bankarstvo. Da bi stimulisala plaćanje preko Interneta, Banka je smanjila proviziju za transakcije koje se vrše online.

Komercijalna banka a.d. Beograd ima elektronske servise iz oblasti:

- 1) e-bank za pravna lica,
- 2) e-banka za fizička lica,
- 3) SMS servis.

6.1.1. E-bank za pravna lica

Elektronsko bankarstvo namenjeno pravnim licima omogućava brže, jeftinije i sigurnije poslovanje – uz brojne pogodnosti:

- Pristup sredstvima sa bankovnih računa i mogućnost obavljanja novčanih transakcija od strane klijenta sa Komercijalnom bankom a.d. Beograd, sa bilo koje lokacije, u zemlji ili u inostranstvu, 24 časa neprekidno, 7 dana u nedelji, bez odlaska u Banku i ograničenja radnim vremenom;
- Značajnu uštedu vremena – vreme plaćanja iznosi samo 1-3 minuta;
- Uštedu novca: usluga obavljena putem E-bank-a jeftinija je i do 50% nego usluga putem klasične metode, na šalteru Banke.

Uslov koji klijent treba da ispuni je da ima otvoren račun u Komercijalnoj banci a.d. Beograd i da poseduje savremenu računarsku opremu.

Za obavljanje elektronskog platnog prometa za pravna lica, Komercijalna banka a.d. Beograd nudi dva programska rešenja:

- 1) HAL E-bank i
- 2) FX Client.

HAL E-bank

Hal E-Bank je savremeni programski proizvod za podršku elektronskom bankarstvu. Hal E-Bank podržava rad sa više računa u više banaka i za više preduzeća. Sa Hal E-Bank možete sve bezgotovinske poslove, koje inače obavljate preko bančnih šaltera, bilo kada obaviti sa radnog mesta ili od kuće. Hal E-Bank ne poznaje granice, kao što ih poznaju bančni šalteri, koji su otvoreni samo u određenom vremenskom periodu u toku dana.

Program Hal E-Bank se instalira na računar korisnika. Za svoj rad zahteva još čitač pametnih kartica, pametnu karticu i modem ili stalnu Internet konekciju za povezivanje sa bankom. Zaštita podataka se u Hal E-Bank temelji na upotrebi pametne kartice i danas, u svetu, predstavlja najviši stepen zaštite na komercijalnom području. Razvijena je posebno za zaštitu podataka, šifrovanje i overavanje. Čitač pametnih kartica se priključuje na personalni računar. Rad sa pametnom karticom je sličan radu sa ostalim karticama na bančnim automatima. Za ulaz u program Hal E-Bank potrebno je staviti pametnu karticu u čitač i ukucati svoj lični (PIN) broj. Provera identiteta, šifrovanje podataka i elektronsko potpisivanje svih naloga se

izvodi u samoj pametnoj kartici. Ako izgubite karticu i nepošteni pronalazač pokuša da je zloupotrebi ona će se sama zaključati nakon tri uzastopna pokušaja unosa pogrešnog ličnog broja (PIN-a). Overa korisnika, elektronski potpis i celovitost podataka svih naloga koji se elektronski šalju u banku temelje se na principu dvojnih ključeva (tajnih i javnih), nazvanim RSA i šifrovanju podataka na principu standardizovanog algoritma DES.

Prednosti Halcom-ovog sistema:

- Korisnici imaju svoje „Bankovne šaltere” na monitoru računara, kod kuće ili na radnom mestu. „Bankovni šalter” omogućava poslovanje 24 časa, 7 dana u nedelji, 365 dana godišnje. Korisnici imaju uštedu u vremenu i novcu, jer nema više potrebe da lično idu u banku, a provizije na elektronske naloge su niže;
- Dodatna funkcija nazvana „remote” ili mobilna autorizacija omogućava vam da autorizujete (potpisujete) naloge za plaćanja sa neke druge lokacije ili u toku putovanja;
- Korisnici nemaju potrebu da primaju izvode sa bankovnog računa, jer iste mogu da dobiju svakog trenutka, preko svog računara;
- Kreiranje naloga se obavlja u off-line režimu, tako da nema dugotrajnog zauzeća telefonske linije;
- Transfer podataka između korisnika i banke je veoma brz.

Instalacijom ovog sistema na raspolaganju su sledeće usluge:

- Upit o stanju računa u realnom vremenu;
- Pripremu naloga za plaćanje, kao i mogućnost valutacije naloga unapred;
- Preuzimanje izvoda;
- Mogućnost Import-a (uvoza) naloga za plaćanje, kao i Export-a (izvoza) prispelih izvoda u txt formatu, radi povezivanja knjigovodstvene aplikacije korisnika sa E-bankom;
- Čuvanje pripremljenih naloga za plaćanje za veći broj upotreba (regularna ili pojedinačna mesečna plaćanja);
- Potvrde o izvršenim plaćanjima, promenama na računu i sl.

Ukoliko klijent ima neki poseban zahtev u okviru E-bank servisa (grupno potpisivanje naloga za prenos, udaljeno potpisivanje naloga za prenos, corporate e-bank servis, B2B servis, prijem izvoda u xml formatu, paket za knjigovodstvene agencije i slično) potrebno je da se obrati Službi e-bankarstva za pravna lica.

Grupno potpisivanje naloga se odnosi na firme kojima nije dovoljan jedan potpisnik na nalogu za prenos. Ukoliko želi ovu uslugu klijent mora popuniti HAL E-bank pristupnicu za grupno potpisivanje.

Udaljeno potpisivanje naloga za prenos mogu vršiti klijenti koji na jednoj lokaciji rade pripremu naloga, a na drugoj lokaciji im se nalazi potpisnik, a pritom njihovi računari ne moraju biti umreženi. Za ovu uslugu potrebno je popuniti pristupnicu za korišćenje WEB E-bank servisa za pravna lica.

Klijent Banke, pravno lice, pored domaćeg platnog prometa može obavljati i platni promet sa inostranstvom. Da bi obavio platni promet sa inostranstvom, klijent koji već poseduje karticu za elektronsko poslovanje u domaćem platnom prometu, dovoljno je da popuni samo HAL E-

3. Na prikazanom meniju izaberite Nalog za prenos ili Kompenzacija. Na ekranu se prikazuje slika naloga za prenos ili kompenzacije sa već upisanim Vašim podacima (ime i sedište nalogodavca, broj računa na strani koja se zadužuje, kod kompenzacije još ime i račun primaoca).

Nalog za prenos

NALOG ZA PRENOS
1000000RY7G3VGL

dužnik - nalogodavac
TEST KOMITENT 2 D.O.O.
Proizvolna 222, Novi Sad

svrha plaćanja

poverilac - primalac

pečat i potpis nalogodavca
Pripremljen: 15.08.2003
mesto i datum prijema
obrazac br. 3

šifra plaćanja
31 ? CSD

iznos

račun dužnika-nalogodavca
205-000000100027110

model i poziv na broj(zaduženje)

račun poverioca-primaoca

model i poziv na broj(odobrenje)

datum valute
15.08.2003

hitno

Pripremio: Potpisao: Potvrdi Opozovi

Kompenzacija

NALOG ZA PRENOS(kompenzacija)
1000000RY7G3VGL

dužnik - nalogodavac
TEST KOMITENT 2 D.O.O.
Proizvolna 222, Novi Sad

svrha plaćanja

poverilac - primalac
TEST KOMITENT 2 D.O.O.
Novi Sad

pečat i potpis nalogodavca
Pripremljen: 15.08.2003
mesto i datum prijema
obrazac br. 3

šifra plaćanja
31 ? CSD

iznos

račun dužnika-nalogodavca
205-000000100027110

račun poverioca-primaoca
205-000000100027110

model i poziv na broj(zaduženje)

model i poziv na broj(odobrenje)

datum valute
15.08.2005

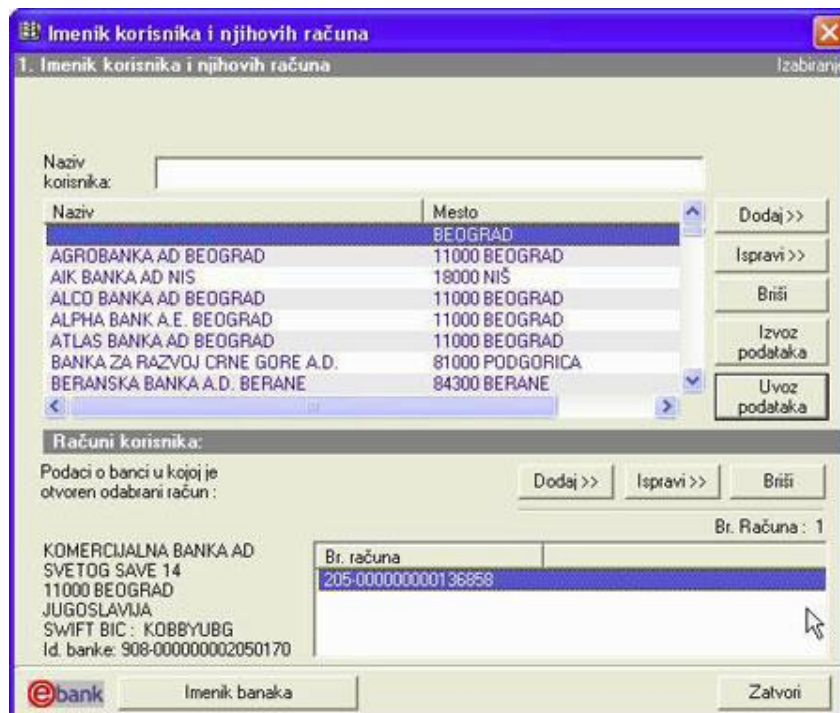
hitno

Pripremio: Potpisao: Potvrdi Opozovi

Pored tih podataka automatski se upišu još predloženi datum željene valute i unapred definisane šifre. Šifru morate, s obzirom na svrhu plaćanja, izabrati sami. Pri tome se možete poslužiti klikom miša na strelicu desno uz polje za unos šifre, koje vam u padajućem spisku prikaže sve dozvoljene mogućnosti. Možete se poslužiti Šifarnikom vrste posla, koji se prikazuje klikom na dugme ? desno od polja za unos šifre.

4. U polje svrha *plaćanja* doznake upišite svrhu.

5. U polje *poverilac - primalac* upišite ime vlasnika računa. Kad promenite sadržaj u polju *poverilac - primalac*, koje sadrži naziv primaoca, otvori se Imenik korisnika i njihovih računa. Upisom početnog dela naziva u polje Naziv korisnika ograničavate listu prikazanih korisnika (primaoca).



Korišćenjem miša i klizača na desnoj strani izaberite u gornjem spisku željenog korisnika (primaoca), a zatim u donjem spisku jedan od njegovih računa, u slučaju da ih ima više. Naziv izabranog korisnika (primaoca) i izabrani broj računa je prikazan u drugoj boji. Izbor potvrdite klikom na dugme Izaberi. Podaci o izabranom korisniku (primaocu) i računu će se prepisati u odgovarajuća polja na nalogu: *poverilac - primalac*, račun *poverioca - primaoca*. Ako u imeniku nema korisnika (primaoca) s nazivom, čiji se početak slaže sa unesenim nizom reči, oba spiska su prazna. Nakon pritiska na dugme *Dodaj>>* na listi korisnika (primalaca) otvori se interaktivni prozor, koji omogućava unos podataka novog korisnika (primaoca). Posle unosa podataka o korisniku (primaocu) morate uneti još podatke o njegovom računu, na koji nameravate izvršiti plaćanje. Uneseni podaci se čuvaju u imeniku. Imenik možete osvežavati istovremeno pri unosu naloga, ili pak podatke o korisnicima (primaocima) i njihovim računima unesite u imenik unapred.

6. U polje *model i poziv na broj (zaduženje)* upišite odgovarajući svoj pozivni broj zaduženja.

7. U polje *datum valute* upišite željeni datum valute. Predefinisano se u to polje upiše prvi mogući datum valute s obzirom na današnji (sistemski) datum. Ako vam datum odgovara, pritisnite *<Enter>*, u protivnom korigujte datum. Pri unosu datuma uzmite u obzir praznike i neradne dane.

8. U polju *šifra plaćanja* unesite odgovarajuće vrednosti tako, da je izaberete sa padajućih spiskova. Pozovite je tako, što kliknete na strelicu nadole pored ekrančića. Ako želite detaljniji opis pojedinih šifara, kliknite dugme s upitnikom. Otvoriće se ekran sa

detaljnim opisom šifara. Šifru možete takođe jednostavno uneti u odgovarajuća polja. Program pri takvom načinu neće dozvoliti unos šifara, kojih nema u spisku.

9. U polje *CSD* upišite željeni iznos (decimalno razgraničenje je zarez a ne tačka!).

10. Polje *model i poziv na broj (odobrenje)* služi unosu pozivnog broja odobrenja. Kod doznake sredstava fizičkom licu u banci (doznaka plate na tekući račun, ulog na štednu knjižicu) potrebno je u poziv na broj odobrenja upisati individualni broj računa (u polje broja žiro računa unosite broj žiro računa banke). Pozivni sadrži takođe modul koji omogućava proveravanje pravilnosti unešenog broja. Platne naloge s greškom u tom polju nije moguće preneti u banku.

11. Ako želite nalog obraditi sa prioritetom, označite ga kao hitan. Kliknite na kvadratić pored natpisa „hitno“. U njemu se prikaže kvačica. Takav nalog nosi oznaku „N“ u pregledima naloga i u prozoru za otpremu.

12. Kad ispunite sva potrebna polja, kliknite na dugme *U redu*. Podaci iz naloga se prenesu u mapu *Nalozi*. Novi nalog se dodaje na kraj mape, a interaktivni prozor sa slikom novog naloga je pripremljen za unos sledećeg platnog naloga. Za prekidanje unosa kliknite na dugme *Opozovi* ili pritisnite taster <Esc>.

Potpisivanje

Kad budete želeli potpisati pripremljene platne naloge, uradite sledeće:

1. Otvorite mapu *Priprema* naloga tako, da u levom delu ekrana, kliknete na *Priprema* i zatim ispod nje na *Nalozi*. Na ekranu se prikaže spisak platnih naloga. Pripremljeni nalozi bez grešaka, koje jedino možete potpisati, su prikazani zelenom bojom.

2. Potražite željeni nalog, prikazan u zelenoj boji, i kliknite na njega levim dugmetom miša. Izabrani nalog mora biti prikazan naglašeno. Samo u tom slučaju je označen. Možete označiti takođe i više naloga i potpisati ih grupno ili pojedinačno.

3. Levim dugmetom miša kliknite na dugme *Potpisi*. Na ekranu se prikaže izabrani nalog. Pre potvrđivanja potpisa još možete promeniti podatke u poljima čiji sadržaj je prikazan u crnoj boji. Sadržaj polja prikazanih u sivoj boji ne možete promeniti.

4. Potpis naloga potvrdite sa *U redu*, ako želite izabrani nalog potpisati. Ako prikazani nalog ne želite potpisati, kliknite na *Opozovi* ili pritisnite taster <Esc>. Potpisani platni nalozi će promeniti boju u crveno. Te naloge možete poslati na isplatu u banku.

Napomena: Podatke na potpisanim nalogima nećete moći više menjati. Ako želite promeniti podatke na već potpisanom nalogu, morate ga najpre otključati.

Slanje

1. Ako radite s više računa, izaberite onaj, za koji želite poslati dokumente u banku. Otvorite mapu *Slanje* tako, da u levom delu ekrana kliknete na *Slanje*. Na ekranu se prikaže spisak proverenih platnih naloga i poruka, koji su pripremljeni za otpremu (slanje u banku).

2. Izaberite dokumente, koje želite poslati u banku i kliknite na dugme *Pošalji*. Program će započeti uspostavljanje veze sa bankom. Kad je veza uspešno uspostavljena, izabrani dokumenti se prenose na računar banke. Pri toj vezi će se sa računara banke na vaš računar preneti i svi obračuni nalozi i podaci o najnovijim stanjima na vašim računima. Nakon uspešnog slanja naloga i čitanja mogućeg prometa veza se automatski prekida, da bi se vreme komunikacije skratilo na najmanju meru. Ako je na strani banke na raspolaganju nova verzija programa E-Bank, primićete meću poslatim dokumentima (nalozi, poruke) o tome odgovarajuće obaveštenje.

3. Kad se prenos završi prikazaće se prozor sa detaljima o poslatim i primljenim dokumentima.



4. Prozor zatvorite klikom na dugme *Zatvori*. Ako se veza sa serverom banke ne uspostavi uspešno, platni nalozi se ne prenesu. U tom slučaju se na ekranu prikaže odgovarajuća poruka.

Uspešno poslati nalozi se iz mape *Priprema* naloga prenose u mapu *Arhivirani nalozi*, gde dobiju status "poslat". Uspešno poslatih dokumenata nema više u mapi *Slanje*.

Pregled prometa

Ako želite pregledati prometne stavke u mapi *Pregled* izaberite *Promet*. Prikazaće se lista prometnih stavki za izbrani račun i vremenski period:

Razlike boje prometnih stavki označavaju:

- Crvena - Knjiženi odliv;
- Pink - Tekući dnevni promet (svi tipovi);
- Siva - Odbijen, opozvan i storniran nalog;
- Plava - Knjiženi priliv;
- Narandžasta - Provizija banke;
- Crna - Storno.

U prozoru se prikazani osnovni podaci o stanju, tekućem prometu i nalogima na čekanju. Detalji o prometu na izabranom računu dobijate klikom na dugme *Promet*.

Personal E-Bank 10.2.2.2 Copyright © HALCOM Informatika d.o.o. 1997-2005

Datoteka Pogled Komunikacija Alati Pomoć

Vlasnik računa: **BATA METALOPRERAĐIVAČKA RADNJA BR.** Račun: **325-00000000453207 BATA METALOPRERAĐIVAČKA RADNJA BR.**

Ispis podataka za: **PODESI** | 01.12.2004 | 02.12.2005

Pregled stanja i prometa na računima

Knjigovodstveno stanje: **=19.461,00**
Datum promene knjigovodstvenog stanja: **2005-11-25-14.46.05**

On-line promet | Promet za naloge u čekanju u banci za danas | Promet za naloge u čekanju u banci za ubuduće

Datum knjiženja	Datum valute	Iznos na teret	Iznos u korist	Iznos odbijeno/drugo	Naziv	Sviha
02.12.2005	02.12.2005	=225,00			ALPHA BANK A.E. BE...	PLAĆILO PREDRAČUN...
02.12.2005	02.12.2005	=561,00			ATLAS BANKA AD BE...	PLAĆILO STANARINE
02.12.2005	02.12.2005	=701,00			CACANSKA BANKA A...	PLAĆILO VODOVODA
02.12.2005	02.12.2005	=727,00			CONTINENTAL BANK...	PLAĆILO TV NAROČNI...
02.12.2005	02.12.2005		=780,00		ATLAS BANKA AD BE...	PLAĆILO STANARINE
02.12.2005	02.12.2005		=920,00		CONTINENTAL BANK...	PLAĆILO TV NAROČNI...

Evid. stanje | Otvori

Pripremljen ... | Br. ozn. zapisa: 1 | Zbir: =0,00 CSD | 02.12.2005 09:15 | NUM | SCRL

Podaci su podeljeni u tri celine, a svaku od njih možete videti klikom na odgovarajući jezičak. Detalje o određenoj prometnoj stavki možete videti tako što je izaberete i kliknete na dugme *Otvori*.

Izvodi

Izvide banka šalje za svaki račun posebno, a možete ih videti u mapi *Pregled/izvodi*. Izborom ove opcije otvoriće se spisak izvoda za izabrani račun i vremenski interval:

Personal E-Bank 10.2.2.2 Copyright © HALCOM Informatika d.o.o. 1997-2005

Datoteka Pogled Komunikacija Alati Pomoć

Vlasnik računa: **SMS TEST Beograd Ulica mladosti 12** Račun: **205-000123456789082 SMS TEST**

Ispis podataka za: **PODESI** | 01.12.2004 | 02.12.2005

Izvodi

Knjigovodstveno stanje=**56.090,00**

Br. izvoda	Datum izvoda	Staro stanje	Br. naloga na teret	Ukupni promet na teret	Br. naloga u korist	Ukupni promet ...	Nc
6066	14.11.2005	1.000,00	1	1.013,00	0	0,00	
6063	25.11.2005	1.000,00	1	86.727,00	3	106.188,00	
✓ 4763	14.11.2005	1.000,00	0	0,00	1	1.450,00	
4685	17.11.2005	1.000,00	0	0,00	1	52.156,00	
1366	16.11.2005	1.000,00	1	2.303,00	0	0,00	
✓ 1164	14.11.2005	1.000,00	0	0,00	1	5.800,00	

Otvori | Izvoz | Pregled | Štampaj

Pripremljen ... | Br. ozn. zapisa: 1 | Zbir: =0,00 CSD | 03.12.2005 08:03 | NUM | SCRL

Izvođe možete detaljnije pregledati. To uradite tako da iz liste odaberete izvod (samo naglašeni izvod je izabran) i pritisnete dugme *Otvori*. Otvori se vam ekran *Detalji izvoda*, kako je to prikazano na donjoj slici. Na vrhu ekrana ispisani su detalji izvoda, kao što su broj izvoda, za dan,...A na sredini ekrana možete pregledati promet tog izvoda. Pregled prometa možete sortirati na način, da mišem kliknete na zaglavlje kolone. Sortiran izvod možete da izvozite i štampate.

Detalji izvoda

Detalji izvoda

Izvod br.	814	Br. zaduženja:	16
Za dan:	02.12.2005	Ukupan promet na teret:	968.566,00
Datum prethodnog izvoda:			
Staro stanje:	1.000,00	Br. odobrenja:	29
Novo stanje:	3.447.970,00	Ukupan promet u korist:	4.415.536,00

Pregled prometa

Datum knjiženja	Datum val...	Iznos na teret	Iznos u korist	Iznos odbijeno/d...	Naziv	Svrha
02.12.2005	02.12.2005	=701,00			CACANSKA BA...	PLAĆ
02.12.2005	02.12.2005	=727,00			CONTINENTAL ...	PLAĆ
02.12.2005	02.12.2005		=780,00		ATLAS BANKA ...	PLAĆ
02.12.2005	02.12.2005		=920,00		CONTINENTAL ...	PLAĆ
02.12.2005	02.12.2005	=1.201,00			AGROBANKA A...	PLAĆ
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=2.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=22.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005	=22.587,00			EBB BEOGRAD...	PL. Č
02.12.2005	02.12.2005		=27.892,00		DDOR BANKA ...	PLAĆ
02.12.2005	02.12.2005		=27.892,00		DDOR BANKA ...	PLAĆ

Otvori Izvoz Pregled Štampaj

halebank

Zatvori

6.1.2. E-bank za fizička lica

Korisnik WEB E-Bank servisa za fizička lica u Komercijalnoj banci a.d. Beograd, može postati svako fizičko lice koje u Banci ima otvoren račun i ako poseduje neophodnu opremu za korišćenje servisa elektronskog bankarstva za fizička lica. Za korišćenje WEB E-Bank servisa za fizička lica neophodan je pristup Internetu preko računara ili drugog uređaja sa WEB pretraživačem tipa MS Internet Explorer, Mozilla Firefox, Netscape ili slični.

Web E-Bank servis za fizička lica predstavlja najbrži i najlakši način plaćanja, koji je namenjen građanima za obavljanje elektronskog bankarstva, preko Interneta, 24h neprekidno, 7 dana u nedelji. Prednosti ovog servisa su:

- Obavljanje transakcija bez provizije;
- Ne postoji vremenska i prostorna ograničenost;

- Brzina, kvalitet i sigurnost poslovanja;
- Jednostavna upotreba.

Usluge koje su dostupne korisniku su:

- Uvid u stanje i promet po računima, platnim karticama i kreditima;
- Prenos sredstava sa jednog na drugi dinarski račun i izmirivanje obaveza po kreditnim karticama, kreditima i namenskim novčanim računima za trgovanje hartijama od vrednosti;
- Plaćanje na predefinisane račune, račune prijavljene zahtevom ili plaćanje bez ograničenja u zavisnosti od prijavljivanja na aplikaciju;
- Menjačke poslove sa deviznog računa na dinarski račun i obrnuto, koje vlasnik i/ili ovlašćeno lice poseduje u Banci;
- Dopuna kredita za mobilni telefon u realnom vremenu;
- Dopuna Internet sati u realnom vremenu;
- Devizna štednja;
- Dinarska štednja;
- Nerealizovani čekovi;
- Kreditni kalkulator;
- Kursna lista;
- Konvertor valuta;
- Informacije o kamatnim stopama;
- Pregled namenskih računa za hartije od vrednosti;
- Štampanje potvrde o izvršenom plaćanju.

Kod plaćanja računa i prenosa sredstava, nalozi se izvršavaju saglasno zakonskim propisima i važećim aktima Banke. Za korišćenje usluge obavljanja transakcija, Banka će korisniku automatski zaračunati naknadu po izvršenom pojedinačnom nalogu, zaduživanjem njegovog tekućeg računa saglasno važećoj tarifi Banke.

Korisnici WEB E-Bank servisa za fizička lica mogu koristiti različita sredstva autentifikacije koja u skladu sa bezbednosnom politikom korisniku daju različita ovlašćenja prilikom plaćanja. Korisnici se mogu prijaviti na aplikaciju jednim od navedenih načina autentifikacije:

- Korisničkim imenom i lozinkom
- Sertifikatom na USB flash memoriji.

Korisnici koji se prijavljuju korisničkim imenom i lozinkom mogu vršiti plaćanje samo na račune sa liste predefinisanih računa ili račune koje korisnik prijavi popunjavanjem zahteva za registraciju novih primalaca.

Sertifikat na *USB flash* memoriji kojim se koristi za autentifikaciju izdaje sertifikaciono telo KOBB CA. Korisnici koji se prijavljuju na ovaj način mogu vršiti plaćanje na bilo koji račun. Korisnici koji poseduju sertifikat mogu se prijaviti na aplikaciju i upotrebom korisničkog imena i lozinke, ali plaćanje mogu vršiti samo na predefinisane račune.

U slučaju potrebe klijenta da mu se izda dokaz o izvršenom plaćanju, iz arhive naloga WEB aplikacije može se odštampati izvršeni nalog i isti doneti u ekspozituru radi overe od strane odgovornog radnika Banke. Uvidom u promet po tekućem računu klijenta, odgovorni radnik proverava da li je nastala finansijska promena evidentirana i izvršena od strane Banke i da li

je u opisu označena kao *Web plaćanje*. Ukoliko je sve navedeno ispunjeno, odgovorni radnik Banke potpisuje i overava nalog klijenta.

Podršku klijentu u vezi korišćenja WEB E-Bank servisa pružaju odgovorni radnici na šalteru i radnici E-bankarstva stanovništva.

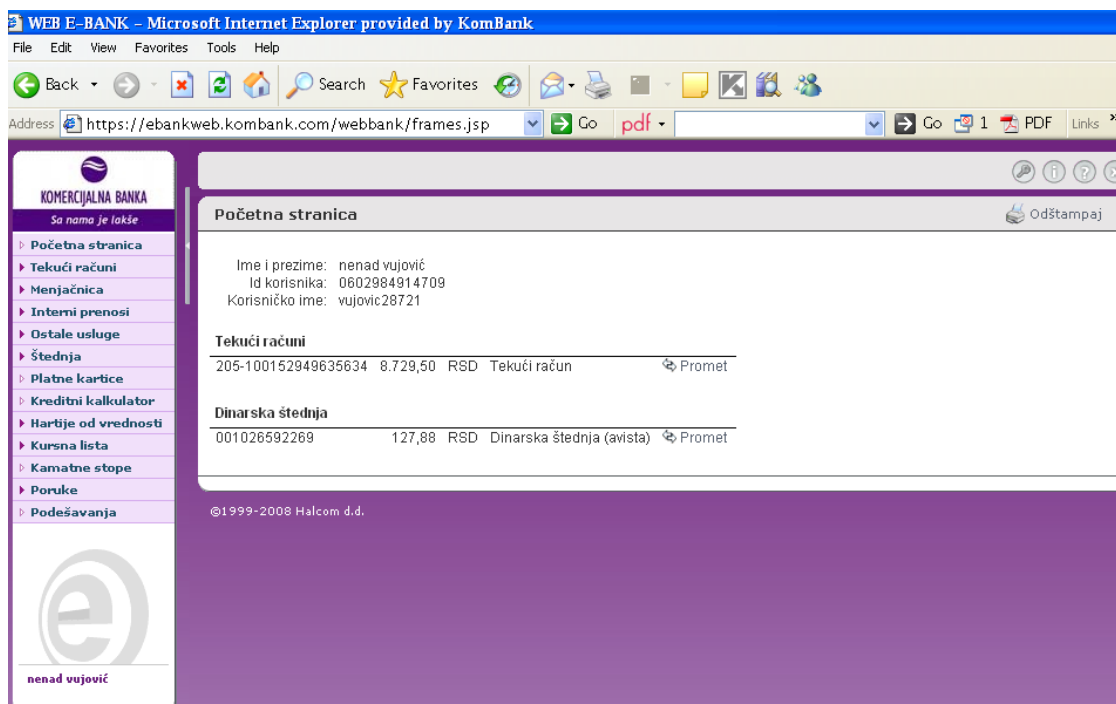
Klijentima se pruža telefonska podrška u vezi sa :

- Korišćenjem aplikacije;
- Realizacijom naloga za plaćanje.

kao i elektronska podrška vezana za odgovore na pitanja klijenata upućena na e-mail adresu Službe E-bankarstva stanovništva e-bank-web@kombank.com

6.1.2.1. Osnovne funkcije Web E-bank servisa za fizička lica

WEB E-Bank je zamišljen tako da korisniku sa jednog mesta, na što jednostavniji način omogući rad. Na sledećoj slici prikazano je radno okruženje WEB E-Bank servisa za građane.



Sa leve strane, uz samu ivicu pretraživača nalazi se glavni meni. Na vrhu se nalazi gornji okvir gde se prikazuju ikone nezavisne od izbora korisnika. U centralnom delu nalazi se radna površina čiji izgled zavisi od izabrane opcije iz glavnog menija.

Tekući računi

Izborom opcije tekući računi iz glavnog menija prikazuju se podopcije vezane za rad sa tekućim računima.

Osnovni podaci o tekućim računima

Izborom opcije *Tekući računi* > *Pregled* prikazuju se sledeći podaci:

- Vlasnik računa;
- Broj računa;
- Stanje na računu;
- Limit (dozvoljeno prekoračenje);
- Rok važenja limita (rok važenja dozvoljenog prekoračenja);
- Status računa (Aktivan, Blokirano ili Sporan).

Detaljan pregled stanja

Račun **205-100152682020297**
Vlasnik računa **TEST TEST**

Knjigovodstveno stanje (Datum) **40.006,39 RSD**
Današnji promet(odobrenje) (broj) 0,00 RSD (0)
Današnji promet(zaduženje) (broj) 0,00 RSD (0)
Tekuće stanje **40.006,39 RSD**

Iznos naloga u obradi (broj) **27.030,00** (41)
Iznos naloga na čekanju (broj) **0,00** (0)

Iznos limita (rok važenja limita) 58.600,00 RSD (04.02.2007)

Nazad

Promet po tekućem računu

Za informacije o prometu po tekućem računu iz glavnog menija izaberite *Tekući računi* > *Promet*.

KOMERCIJALNA BANKA
Sa nama je lakše

Pregled
Promet
Čekovi
Primaoci
Priprema naloga
Imenik naloga
Arhiva naloga
Menjačnica
Interni prenosi
Štednja
Platne kartice

Pregled prometa

Račun: 205-100152682020297
TEST TEST

Stanje: **40.006,39 RSD**

Prikaz prometa za: **mesec**

Datum knjiženja	Na teret	U korist	Odbijeno/Drugo	Primalac/Nalogodavac	Svrha doznake	
07.04.2007	1,00			KOMERCIJALNA BANKA	PRE PAID	Prikaži
18.03.2007	500,00			KOMERCIJALNA BANKA	PRE PAID 500	Prikaži
18.03.2007	500,00			KOMERCIJALNA BANKA	PRE PAID 500	Prikaži
12.03.2007	33,00			KOMERCIJALNA BANKA	GFGGFF	Prikaži
Ukupno:	1.034,00	0,00				

Nazad

Za detaljnije informacije o određenoj transakciji kliknite na link *Detalji*.

Pregled nerealizovanih čekova

Za informacije o nerealizovanim čekovima potrebno je da iz glavnog menije izaberete opciju *Tekući računi* > *Čekovi*.

Spisak nerealizovanih čekova

Odšampaj

Račun:


205-100152682020297
TEST TEST

Stanje:
40.006,39RSD

Broj čeka	Datum izdavanja
0000600062	07.11.2003
0005351307	29.12.2004
0005351307	16.08.2005
0006262049	09.05.2005

Ukupno čekova: 4

Nazad

- Broj čeka – serijski broj čeka
- Datum izdavanja – datum kada je ček izdat
- Ukupno čekova – ukupan broj nerealizovanih čekova

Primaoci

U podopciji koja se nalazi u okviru opcije *Tekući računi* možete imati uvid u sve primaoce. Za informaciju o ličnim primaocima potrebno je iz glavnog menija izabrati opciju *Primaoci*.

Registrovani primaoci

Odšampaj

Račun:


205-100152976036124
IRENA GAJIĆ

Stanje:
35.478,20 RSD

Račun	Primalac	Status		
160-513020012639327	BANKA INTESA DEVIZNI RACUN	REGISTROVAN	 Detalji	 Obriši
205-100152976032535	DRACHE CHE	REGISTROVAN	 Detalji	 Obriši
160-510010017663059	IRENA GAJIĆ	REGISTROVAN	 Detalji	 Obriši
205-100152976058210	MARIJA STOJANOVIĆ	REGISTROVAN	 Detalji	 Obriši
205-100152976056591	MILOŠ NIKOLIĆ	REGISTROVAN	 Detalji	 Obriši
205-100152866584331	MILOŠ VASOVIĆ	REGISTROVAN	 Detalji	 Obriši
205-100152949635634	NENAD VUJOVIĆ	U REGISTRACIJU	 Detalji	 Obriši
170-000000000288007	SBB PJ TELEFONIJA KDS BEOGRAD	REGISTROVAN	 Detalji	 Obriši
205-100152976058337	SRĐAN GUČEVAC	REGISTROVAN	 Detalji	 Obriši
205-100152983357393	VLADA VETERINAR	REGISTROVAN	 Detalji	 Obriši

Registracija novog primaoca

©1999-2008 Halcom d.d.

Ukoliko želite da registrujete novog primaoca potrebno je da kliknete na dugme *Registracija novog primaoca* (*Tekući računi>Moji primaoci*). Nakon registracije primaoca potrebno je da prikazani obrazac odštampate, potpišete i odnesete u najbližu ekspozituru Banke radi verifikacije (samo za korisnike koji koriste korisničko ime i lozinku kao sredstvo autentifikacije). Primaoca takođe možete registrovati u najbližoj ekspozituri Banke popunjavanjem Zahteva za registraciju novog primaoca. Ukoliko želite da obrišete registrovanog primaoca kliknite na *Obriši*.

Priprema naloga

Ukoliko želite da izvršite plaćanje, potrebno je kliknuti na opciju *Tekući računi>Priprema naloga*, kako bi se na radnoj površini prikazao formular za pripremu naloga. Ukoliko vam je dostupno korišćenje više računa, u polju za izbor računa izaberite račun sa kojeg želite da vršite plaćanje. Sa desne strane se prikazuje tekuće stanje za izabrani račun.

1
2
3

Priprema naloga

Odštampaj

Račun:

205-100152949635634
NENAD VUJOVIĆ

Stanje:
8.729,50 RSD

Nalog za prenos
Status:
Oznaka:

Dužnik - Nalogodavac

NENAD VUJOVIĆ
MILIĆA RAKIĆA 9/94
BEOGRAD

Svrha plaćanja

Poverilac - Primalac

Šifra plaćanja

89
?

RSD

Račun dužnika - nalogodavca

205-100152949635634

Model i poziv na broj (zaduženje)

Račun poverioca - primaoca

Model i poziv na broj (odobrenje)

Datum valute

18.11.2008

Hitno

Sredstva za povraćaj

mesto i datum prijema

Obr. ver. 1

Priprio:
Datum prijema:
Potpisao:

Izaberi primaoca
Odaberi nalog iz imenika
Pošalji

©1999-2008 Halcom d.d.

Polja *Dužnik* – *Nalogodavac*, odnosno *Račun dužnika* – *nalogodavca* su unapred popunjena podacima o vlasniku računa, odnosno brojem računa. U polje *Svrha plaćanja* potrebno je uneti opis transakcije. Polje *Poverilac* – *Primalac* je zajedno sa poljem *Račun poverioca* – *primaoca* povezano sa registrom primalaca. Za prikaz liste javnih i ličnih primaoca kliknite na dugme *Izaberi primaoca*. Izborom ove opcije prikazuje se novi prozor sa tabelom registrovanih primalaca.

Registrovani primaoci			
Račun primaoca:		Naziv primaoca:	
		Prikaži	Zatvori
Račun	Primalac	Vrsta	
840-00000014366634	Arhitektonski Fakultet	JAVNI	Izaberi
205-000000000962037	Avcom D.o.o.	JAVNI	Izaberi
160-513020012639327	BANKA INTESA DEVIZNI RACUN	MOJ	Izaberi
165-000000000136039	BEOCITY DOO	JAVNI	Izaberi
335-0000000001000613	DDOR Novi Sad	JAVNI	Izaberi
170-000030105558565	Delta Generali Osiguranje	JAVNI	Izaberi
160-0000000000056142	DELTA LIFE	JAVNI	Izaberi
260-019601003661647	Diners Club International	JAVNI	Izaberi
205-100152976032535	DRAGCHE CHE	MOJ	Izaberi
170-000000000047738	Dunav Osiguranje	JAVNI	Izaberi
840-000000110966673	Ekonomski Fakultet	JAVNI	Izaberi
845-000000006484935	Elektrodistribucija Užice	JAVNI	Izaberi
845-000000009884979	Elektromorava Požarevac	JAVNI	Izaberi
845-000000001484973	Elektrosrbija Kraljevo ED Kruševac	JAVNI	Izaberi
840-000000143866648	Elektrotehnički Fakultet	JAVNI	Izaberi
845-000000005284948	Elektrovojvodina	JAVNI	Izaberi
845-000000004084961	Elektrovojvodina JP NS	JAVNI	Izaberi
845-000000006084907	EPS-JP Elektrodistribucija-Beograd	JAVNI	Izaberi
250-000000424953608	EUROBANK EFG	JAVNI	Izaberi
840-000000134466669	Fakultet Organizacionih Nauka	JAVNI	Izaberi
840-000000183866635	Fakultet Političkih Nauka	JAVNI	Izaberi
165-000000000119646	Fefa Fakultet	JAVNI	Izaberi

Klikom na *Izaberi* podaci o primaocu će se iskopirati na Nalog za prenos.

U polje *Šifra* izabrati šifru 89, a ukoliko plaćate porez, takse i naknade tj. ako je primalac Vlada Republike Srbije ili Poreska uprava onda se bira šifra 53, model 97, poziv na broj odobrenja bez crtica. (Ukoliko niste sigurni koju šifru plaćanja je potrebno uneti, kliknite na znak pitanja koji se nalazi pored padajućeg menija na kome se bira sama šifra).

U polje *Datum valute* možete uneti današnji datum ili datum sa valutom unapred.

Za slanje naloga potrebno je kliknuti na dugme *Pošalji*. U radnoj površini se prikazuje popunjen nalog, u obliku kakav će biti prosleđen u Banku. Ukoliko su svi podaci u redu, potrebno je kliknuti na opciju *Potvrdi*.

Imenik naloga

Svaki nalog koji se pošalje iz WEB E-Bank može se sačuvati u imeniku naloga i služiti kao uzorak za pripremu novih naloga. Ovaj postupak je predviđen za naloge koji se periodično ponavljaju, kao što su: nalozi za plaćanje struje, telefona, infostana itd. Imeniku naloga se pristupa izborom istoimene opcije iz podmenija Tekući računi.

Imenik naloga			
Račun:		205-100152976036124 IRENA GAJIĆ	
Vrsta	Primalac	Račun	Opis
NALOG ZA PRENOS	DRAGCHE CHE	205-100152976032535	PROBA
NALOG ZA PRENOS	IRENA GAJIĆ	160-510010017663059	UPLATA NA TEKUĆI RAČUN ZA MORE
NALOG ZA PRENOS	SBB PJ TELEFONIJA KDS BEOGRAD	170-000000000288007	UPLATA FLAT HOME 256 ZA KORISNI?
NALOG ZA PRENOS	SBB PJ TELEFONIJA KDS BEOGRAD	170-000000000288007	UPLATA FLAT HOME 256 ZA KORISNI?
NALOG ZA PRENOS	TELEKOM	908-0000000002050170	PREPAID DOPUNA
NALOG ZA PRENOS	TELENOR D.O.O. BEOGRAD	265-104031000049722	USLUGE MOBILNE TELEFONIJE ZA MAR
NALOG ZA PRENOS	VLADA VETERINAR	205-100152983357393	PROBA2
Nazad			

U radnoj površini prikazuje se tabela sa spiskom naloga koji su sačuvani u imeniku.

Tabela sadrži sledeće kolone:

- Vrsta – vrsta naloga;
- Primalac – naziv primaoca;
- Račun – broj računa primaoca;
- Opis – svrha plaćanja;
- Popravi – prikazuje se postojeći uzorak koji možete promeniti;
- Obriši - uzorak će se obrisati iz Imenika naloga;
- Nova uplata - postojeći uzorak se koristi za pripremu novog naloga.

Arhiva naloga

Svi nalozi koji su poslani iz WEB E-Bank aplikacije čuvaju se u arhivi naloga. Za ulazak u arhivu naloga potrebno je izabrati istoimenu opciju iz glavnog menija. U radnoj površini se prikazuje tabela sa spiskom uplata. U slučaju da korisnik radi sa više računa, u gornjem levom uglu, u polju za izbor računa, potrebno je izabrati onaj za koji se želi pregledati arhiva. Desno od polja za izbor računa prikazano je i trenutno stanje na istom.

Arhiva naloga

Pronađi

Odštampaj

Račun:

205-100152976036124

IRENA GAJIĆ

Stanje:

35.478,20 RSD

Prikaz arhive naloga za:

Primalac:

Opis:

Iznos:

=

i

RSD

Period od:

02.01.2008

do:

17.02.2008

Prikaži

Datum valute	Primalac	Iznos	Opis	Status		
08.02.2008	TELENOR D.O.O. BEOGRAD	2.623,69	USLUGE MOBILNE TELEFONIJE	IZVRŠEN	Detalji	Nova uplata
07.02.2008	SBB PJ TELEFONIJA KDS BEOG	1.350,00	UPLATA FLAT HOME 256 ZA K	IZVRŠEN	Detalji	Nova uplata
15.01.2008	TELENOR D.O.O. BEOGRAD	1.952,57	USLUGE MOBILNE TELEFONIJE	IZVRŠEN	Detalji	Nova uplata
15.01.2008	IRENA GAJIĆ	20.000,00	UPLATA NA TEKUĆI RAČUN IN	IZVRŠEN	Detalji	Nova uplata
05.01.2008	SBB PJ TELEFONIJA KDS BEOG	1.350,00	UPLATA FLAT HOME 256 ZA K	IZVRŠEN	Detalji	Nova uplata
03.01.2008	IRENA GAJIĆ	1.000,00	UPLATA NA TEKUĆI RAČUN IN	IZVRŠEN	Detalji	Nova uplata
Ukupno:		28.276,26				

©1999-2008 Halcom d.d.

Virtuelna menjačnica

Za korišćenje Menjačnice potrebno je iz glavnog menija izabrati opciju *Menjačnica*. Pomoću Menjačnice možete vršiti otkup ili prodaju deviza. Ova opcija je omogućena klijentima koji imaju otvoren devizni račun. Konverzija valuta nije dozvoljena.

Prodaja deviza

Za prodaju deviza, potrebno je iz glavnog menija izabrati opciju *Menjačnica>Prodaja deviza*. Prodaja deviza je moguća samo sa deviznih avista računa na tekući račun. Banka ne

218

obračunava proviziju kod prodaje deviza. Prodaja se može vršiti do iznosa raspoloživih sredstava na deviznom računu sa koga vršite prodaju. Vlasnici deviznih štednih knjižica ne mogu koristiti usluge virtuelne menjačnice. Ukoliko želite da imate mogućnost kupovine i prodaje deviza u opciji virtuelne menjačnice neophodno je da postojeću štednu knjižicu prebacite u avista devizni račun što možete uraditi na vašem matičnom šalteru.

1 2 3

Prodaja deviza

Odštampaj

Na teret računa: 001249579908 (EUR)

U korist računa: 205-100152713037502 (RSD)

Prodajem: EUR

Pošalji

Odustani

- Na teret – devizni račun sa koga se vrši prodaja
- U korist – dinarski račun na koji će biti prenešen iznos u dinarskoj protivvrednosti
- Prodajem – iznos strane valute za prodaju
- Iz padajuće liste *Na teret* izaberite račun sa koga se vrši prodaja deviza a iz padajuće liste *U korist* račun na koji se vrši prenos dinarske protivvrednosti. U polje *Prodajem* potrebno je upisati iznos koji želite da prodate a zatim kliknite na dugme *Pošalji*

1 2 3

Prodaja deviza

Odštampaj

Podaci od: 04.12.2008 12:25:29.559

Na teret računa: 001249579908 (EUR)

U korist računa: 205-100152713037502 (RSD)

Prodajem: 0,05 EUR

Iznos: 4,49 RSD

Promeni

Potvrdi

Odustani

U prikazanom prozoru sa popunjenim podacima za promenu podataka kliknite na dugme *Promeni*, odnosno ukoliko želite da odustanete kliknite na dugme *Odustani*. Ukoliko ste sigurni da su podaci ispravno upisani kliknite na dugme *Potvrdi* kako bi nalog poslali u Banku.

Kupovina deviza

Za kupovinu deviza potrebno je iz glavnog menija izabrati opciju *Menjačnica>Kupovina deviza*. Kupovina deviza je moguća samo na teret tekućih računa a u korist avista deviznih računa i računa oročene devizne štednje. Kod kupovine deviza Banka obračunava proviziju u skladu sa važećim tarifama. Kupovina se može vršiti do iznosa raspoloživih sredstava po tekućem računu na čiji teret se vrši kupovina, kao i do propisanog dnevnog limita u iznosu od 1.000 evra.

1 2 3 Kupovina deviza

Odštamaj

Podaci od: 04.12.2008 12:35:03.590

Na teret računa:

205-100152713037502 (RSD)

U korist računa:

001249579908 (EUR)

Kupujem:

1,00 EUR

Provizija:

0,30% (0,28 RSD)

Iznos:

92,87 RSD

Promeni

Potvrdi

Odustani

U prikazanom prozoru sa popunjenim podacima za promenu podataka kliknite na dugme *Promeni*, odnosno ukoliko želite da odustanete kliknite na dugme *Odustani*. Ukoliko ste sigurni da su podaci ispravno upisani kliknite na dugme *Potvrdi* kako bi nalog poslali u Banku.

Interni prenos

Za Interne prenose potrebno je iz glavnog menija izabrati opciju *Interni prenos*. Pod internim prenosima se podrazumeva prenos između vlastitih računa odnosno partija korisnika (bez konverzije) kao i izmirenje obaveza po osnovu kredita, platnih kartica itd.

Priprema prenosa

Za Interne prenose potrebno je iz glavnog menija izabrati *Interni prenos > Priprema prenosa*.

1 2 3 Platnu karticu

Odštamaj

Na teret računa:

Izmirenje za:

☒ Platnu karticu
 ☐ Kredit
 ☐ Račun

U korist kartice:

4176130000011606

Iznos:

2500 RSD

Datum valute:

09.04.2007

Dalje

Nazad

- Na teret računa – račun sa koga se prenose sredstva,
- Izmirenje za: Platnu karticu – izaberite kod izmirenja obaveza po osnovu platne kartice,
- Kredit – izaberite kod izmirenja obaveza po osnovu kredita,
- Račun – izaberite kod prenosa između vlastitih računa (moguće je između računa iste vrste), uključujući i namenske račune za kupovinu/prodaju HOV.
- U korist – u zavisnosti od prethodnog izbora prikazaće se skriveni broj platne kartice, kreditna partija ili broj računa.
- Iznos – iznos sredstava koje želite da prenesete,

- Datum valute – datum kada želite da prenos bude izvršen (obratite pažnju na neradne dane).

Prenos između vlastitih računa podrazumeva prenos sa tekućeg na tekući račun, sa računa avista štednje na račun avista štednje (sredstva po vičenju) kao i prenos sa avista računa na račun oročene štednje. U padajućoj listi računa se uvek prikazuju računi za koje i sa kojih je dozvoljen prenos (namenski računi za kupovinu/prodaju HOV).

Izmirenje obaveza po osnovu kredita podrazumeva prenos sa računa na kreditnu partiju. U listi računa se uvek prikazuju računi za koje je dozvoljen prenos kao i kreditne partije na koje je dozvoljen prenos.

Izmirenje obaveza po osnovu kreditnih kartica podrazumeva prenos sa tekućeg računa na račun kreditne kartice. U listi računa se uvek prikazuju računi za koje i sa kojih je dozvoljen prenos.

Štednja

Za informacije o štednji potrebno je iz glavnog menija izabrati opciju *Štednja*. U okviru opcije *Štednja* postoje dve podopcije i to za rad sa računima *Domaća štednja* ili *Devizne štednje*.

Domaća štednja

U okviru opcije *Domaća štednja* prikazaće se svi računi dinarske štednje (po vičenju i oročeni) kojima korisnik raspolaže a podržani su kroz aplikaciju. Oznaka za dinare u platnom prometu je RSD.

Dinarski računi štednje						 XML  Excel  CSV  Odštampaj	
						Podaci od: 07.04.2007 19:18:11.501	
Jedan zapis nađen. 1							
	Račun	Vrsta	Vlasnik računa	Status	Stanje		
	001047783921	Dinarska knjižica	GORAN MARKOVIĆ	Aktivan	30,40 RSD	 Detalji	 Promet

Promet po računima dinarske štednje

Za prikaz prometa po računima dinarske štednje potrebno je u glavnom meniju izabrati opciju *Štednja>Domaća štednja*, a zatim kliknuti na link *Promet* koji se nalazi na kraju reda.

Pregled prometa

Račun:

001047783921 (RSD)

Stanje:
30,40 RSD

Podaci od:08.04.2007 09:48:44.008

Prikaz prometa za:

3 meseca

Prikazanih 3/3 zapisa. 1

Datum valute	Nateret	U koris	Primalac/Nalogodavac	Opis	Status
09.01.2007	3.000,00 RSD				Obradjeno
08.01.2007	7.600,00 RSD				Obradjeno
08.01.2007		3.000,00 RSD			Obradjeno

Nazad

U gornjem delu ekrana prikazan je broj računa i stanje, dok se u radnoj površini prikazuju:

- Datum valute – prikazuje se datum izvršenja naloga,
- Na teret – prikazuju se zaduženja,
- U korist – prikazuju se odobrenja,
- Status – prikazuje se status naloga.

Detalji o računima oročene dinarske štednje

U osnovnom delu WEB aplikacije potrebno je iz menija izabrati opciju *Štednja>Domaća štednja*, a zatim kliknuti na link *Detalji* u poslednjoj koloni.

Detalji o dinarskom oročenju		Odštampaj
Podaci od: 12.04.2007 15:11:01.010		
Račun: 001145741911		
Sinonim:	Promeni sinonim	
Status: Blokirano		
Stanje: 6.429,52 RSD		
Obračunata kamata: -188,04 RSD		
Porez: 0,00 RSD		
Iznos za likvidaciju: 6.241,48 RSD		
Promet Dospelo Nazad		

Podaci od – datum poslednjeg ažuriranja podataka

Račun – prikazan je broj računa Sinonim (drugi naziv za Vaš račun) – služi za dodeljivanje sinonima određenom računu radi lakše navigacije. Ukoliko želite da dodelite sinonim nekom računu potrebno je da u istoimeno polje upišete željeni naziv a zatim da kliknete na opciju *Promeni sinonim*. Ukoliko želite da obrišete sinonim i da se prikazuje samo broj računa, potrebno je da u polju sinonim obrišete sve karaktere a zatim kliknete na opciju *Promeni sinonim*.

- Status – prikazan je status računa,
- Stanje – prikazano je stanje na računu,
- Obračunata kamata – prikazan je iznos obračunate kamate u stranoj valuti,
- Porez – prikazan je iznos poreza u stranoj valuti,
- Iznos za likvidaciju – prikazan je iznos za likvidaciju u stranoj valuti (iznos koji se prisvaja pod identičnim uslovima štednje),
- Protivvrednost iznosa za likvidaciju – prikazan je iznos za likvidaciju preračunat u dinare Oročen na – prikazan je period na koji su sredstva oročena.

Devizna štednja

Za rad sa računima devizne štednje potrebno je iz glavnog menija izabrati opciju *Štednja>Devizna štednja*. U zavisnosti od vrste računa i perioda oročenja razlikujemo račune dinarske avista štednje i račune devizne oročene štednje.

Osnovni podaci o računima devizne štednje

Devizni računi štednje						XML Excel CSV Odštampaj		
						Podaci od: 08.04.2007 10:55:35.753		
Prikazanih 7/7 zapisa. 1								
	Račun	Vrsta	Vlasnik računa	Status	Stanje	Detalji	Promet	Dospeće
	šššššš	Devizna knjižica - oročeno na 12 mes.	SNEZANA MICOVIĆ	Aktivan	10.281,07 CHF			
	001245473293	Devizni račun	SNEZANA MICOVIĆ	Aktivan	0,12 CHF			
	001245473293	Devizni račun	SNEZANA MICOVIĆ	Aktivan	1.778,80 USD			
	001245473293	Devizni račun	SNEZANA MICOVIĆ	Aktivan	2.201,69 EUR			
	001247540528	Devizna knjižica		Aktivan	436,30 EUR			
	007046788976	Devizna knjižica - oročeno na 12 mes.	SNEZANA MICOVIĆ	Aktivan	9.751,84 USD			
	007046788976	Devizna knjižica - oročeno na 12 mes.	SNEZANA MICOVIĆ	Aktivan	50.029,19 EUR			

U osnovnom delu WEB aplikacije potrebno je iz menija izabrati opciju *Štednja>Devizna štednja*. Na ekranu će se prikazati spisak svih računa koji su podržani.

Promet po računima devizne štednje

Za prikaz prometa po računu devizne štednje potrebno je da u okviru menija izaberete opciju *Štednja>Devizna štednja* a zatim da kliknete na link *Promet* na kraju reda.

U gornjem delu ekrana prikazan je broj računa i stanje na njemu. Ukoliko ste više računa prijavili za rad posredstvom WEB E-Bank servisa, sa padajuće liste *Račun* izaberite račun za koji želite pregled prometa. Prikazani su sledeći podaci:

- Datum valute – prikazuje se datum izvršenja naloga,
- Na teret – prikazuje se iznos transakcije na teret,
- U korist – prikazuje se iznos transakcije u korist,
- Primalac/Nalogodavac,
- Opis – prikazuje se opis promene,
- Status – prikazuje se status naloga.

Detalji o računima devizne oročene štednje

U osnovnom delu WEB aplikacije potrebno je iz menija izabrati opciju *Devizni računi štednje*, a zatim kliknuti na link *Detalji* u poslednjoj koloni. Prikazuje se ekran sa podacima:

Detalji o deviznom oročenju
 Odštampaj

Podaci od: 08.04.2007 12:02:21.216

Račun: 007046788976
Sinonim:
Vlasnik računa: SNEZANA MICOVIĆ
Status: Aktivan

Stanje: 9.751,84 USD
Obračunata kamata: 56,57 USD
Protivvrednost kamate: 3.371,07 RSD
Porez: 11,31 USD
Protivvrednost poreza: 673,97 RSD
Iznos za prenos: 0,00 USD
Protivvrednost iznosa za prenos: 0,00 RSD
Iznos za likvidaciju: 9.797,10 USD
Protivvrednost iznosa za likvidaciju: 583.820,94 RSD

- Podaci od – datum poslednjeg ažuriranja podataka,
- Račun – prikazan je broj računa *Sinonim* (drugi naziv za Vaš račun) – služi sa dodeljivanje sinonima određenom računu radi lakše navigacije. Ukoliko želite da dodelite sinonim nekom računu potrebno je da u istoimeno polje upišete željeni naziv a zatim da kliknete na opciju *Promeni sinonim*. Ukoliko želite da obrišete sinonim i da se prikazuje samo broj računa, potrebno je da u polju sinonim obrišete sve karaktere a zatim kliknete na opciju *Promeni sinonim*.
- Vlasnik računa – prikazano je ime i prezime vlasnika računa,
- Status – prikazan je status računa,
- Stanje – prikazano je stanje na računu *Obračunata kamata* – prikazan je iznos obračunate kamate u stranoj valuti,
- Protivvrednost kamate – kamata preračunata u dinare (oznaka za dinare u platnom prometu je RSD),
- Porez – iznos poreza u stranoj valuti,
- Protivvrednost poreza – iznos poreza preračunat u dinare,
- Iznos za prenos – iznos za prenos u stranoj valuti,
- Protivvrednost iznosa za prenos – iznos za prenos preračunat u dinare,
- Iznos za likvidaciju – iznos za likvidaciju u stranoj valuti (iznos koji se prisvaja pod identičnim uslovima štednje),
- Protivvrednost iznosa za likvidaciju – iznos za likvidaciju preračunat u dinare.

Platne kartice

Izborom opcije *Platne kartice* iz glavnog menija prikazuju se podopcije vezane za rad sa platnim karticama.

Osnovni podaci o platnim karticama

Za prikaz osnovnih informacija o platnim karticama potrebno je iz glavnog menija izabrati opciju *Platne kartice>Pregled*.

Spisak platnih kartica						 Odštampaj	
	Broj kartice	Kartica	Stanje	Važi do	Status		
	4176*****1606	Test	43.000,00 CSD	01.11.2008	AKTIVNA	 Detalji	 Promet
	9891*****0407	KREDITNA Test1	45.000,00 CSD	01.12.2008	AKTIVNA	 Detalji	 Promet
	9891*****0107	Test1		15.09.2008	AKTIVNA	 Detalji	 Promet

- Broj kartice - prikazan je broj kartice u zaštićenom formatu tako da su vidljive samo prve četiri i poslednje četiri cifre,
- Kartica - prikazana je vrsta kartice (elektron, standard, revolving...),
- Stanje - prikazano je raspoloživo stanje i to samo za kreditne kartice,
- Važi do - prikazan je datum isteka kartice,
- Status - prikazan je status kartice (*Aktivna ili Blokirana*).

Promet po platnoj kartici

Za pregled prometa po platnoj kartici potrebno je iz glavnog menija izabrati opciju *Platne kartice>Promet*. Pregled prometa po platnim karticama moguć je i preko stranice sa osnovnim prikazom platnih kartica klikom na link *Promet*.

Platne kartice-promet

Pronađi

Odštampaj

TXT

Excel

Kartica:

VISA

4176*****1606

Test

Prikaz prometa za:

3 meseca

Datum autorizacije	Datum valute	Iznos	Valuta	Iznos u lokalni valuti	Mesto korišćenja	Status
02.02.2007	03.02.2007	1.567,67	CSD	-	KOMERCIJALNA BANKA	Detalji
13.02.2007	13.02.2007	8.000,00	CSD	100,00	MAXIMUS	Detalji

Nazad

- Kartica – prikazuje se broj kartice i ime i prezime vlasnika računa na koji se odnosi kartica. Ukoliko koristite više platnih kartica izborom željene kartice promeniće se prikaz prometa
- Stanje - prikazuje se iznos raspoloživih sredstava po kartici,
- Datum autorizacije - prikazuje se datum kada je kartica korišćena,
- Datum valute - prikazuje se datum kada vam je zadužen odgovarajući račun kartice,
- Iznos – prikazuje se iznos za koji se zadužuje račun kartice,
- Valuta – prikazuje se oznaka valute,
- Iznos u lokalnoj valuti - prikazuje se konvertovan iznos u dinarima (oznaka za dinare u platnom prometu je RSD) za koji se zadužuje račun kartice,
- Mesto korišćenja – prikazuje se mesto gde je kartica korišćena,
- Status – status transakcije (izvršen, neizvršen) prikazuje se da li je račun kartice zadužen za iznos koji je autorizovan (Izvršen) ili su sredstva rezervisana (Neizvršen).

Kredit

Izborom ove opcije iz glavnog menija prikazuju se podopcije vezane za rad sa kreditima.

Osnovni podaci o kreditima

Za prikaz osnovnih informacija o kreditima potrebno je iz glavnog menija izabrati opciju *Kredit*>*Pregled*.

Pregled kredita							XML Excel CSV Odštampaj	
Podaci od: 09.04.2007 12:57:19.936								
Prikazanih 3/3 zapisa. 1								
Partija kredita	Sinonim	Status	Iznos	Broj rata	Iznos fiksne rate	Datum puštanja u tečaj		
001646200071		Aktivan	606,10 EUR	36	20,22 EUR	10.06.2005	Detalji	Update
001645922283	šššššš	Aktivan	13.277,94 EUR	60	267,16 EUR	22.04.2002	Detalji	Update
001645822519	Moj racun	Aktivan	20.990,44 EUR	60	422,34 EUR	19.04.2002	Detalji	Update

- Partija kredita – kreditna partija (broj kredita),
- Sinonim (drugi naziv za Vaš kredit)– služi sa dodeljivanje sinonima određenom računu radi lakše navigacije.
- Status – status u kome se nalazi kredit (*Aktivan*, *Sporan* ili *Blokiran*),
- Iznos – ukupan iznos kredita,
- Broj rata – broj rata kredita,
- Iznos fiksne rate – fiksna rata,
- Datum puštanja u tečaj – datum od kada važi kredit.

Detalji o kreditu

Za prikaz detalja o kreditima potrebno je iz glavnog menija izabrati opciju *Kredit*>*Pregled* a zatim kliknite na link *Detalji*.

Detaljni pregled kredita		Odštampaj
Podaci od: 09.04.2007 13:09:29.941		
Partija kredita: 001645822519		
Sinonim:		Promeni sinonim
Status: Aktivan		
Datum puštanja u tečaj: 19.04.2002		
Broj rata: 60		
Izkorišćeni iznos: 20.990,44 EUR		
Iznos rate: 422,34 EUR		
Datum dospeća prve rate: 20.05.2002		
Datum dospeća poslednje rate: 20.04.2007		
Nominalna kamatna stopa: 7,95%		
Nivo nominalne kamatne stope: Godišnje		
Stanje: 751,48 EUR		
Ukupno uplaćeno: 20.614,95 EUR		
Neizmirene dospele obaveze: 430,50 EUR		
Obračunata kreditna kamata: 4.041,64 EUR		
Obračunata zatezna kamata: 360,65 EUR		
Pripisana pasivna kamata: 0,29 EUR		
Učešće: 0,00 EUR		
Pregled uplata	Iznos za likvidaciju	Izmirenje obaveze
Nazad		

- Partija kredita – kreditna partija (broj kredita),
- Sinonim (drugi naziv za Vaš kredit) – služi sa dodeljivanje sinonima određenom računu radi lakše navigacije,
- Status – status kredita (može biti aktivan, sporan, blokiran),
- Datum puštanja u tečaj – datum isplate,
- Broj rata – ukupan broj rata,
- Iskorišćeni iznos – iznos kredita,
- Iznos rate – iznos rate,
- Datum dospeća prve rate – prikazuje se datum dospeća prve rate,
- Datum dospeća poslednje rate – prikazuje se datum kada treba platiti poslednju ratu, odnosno izmiriti kredit,
- Nominalna kamatna stopa – stopa po kojoj se obračunava kamata,
- Nivo nominalne kamatne stope – godišnja ili mesečna,
- Stanje – iznos iskorišćenog kredita + obračunata kreditna kamata + obračunata zatezna kamata - iznos uplata - obračunata pasivna kamata,
- Ukupno uplaćeno – zbir svih uplata po partiji,
- Neizmirene dospele obaveze – iznos dospelih obaveza (rata) + obračunata zatezna kamata – uplate,
- Obračunata kreditna kamata – kreditna kamata,
- Obračunata zatezna kamata – zatezna kamata,
- Pripisana pasivna kamata – kamata obračunata na pretplatu,
- Učešće – učešće.

Plaćanje rate kredita

Za plaćanje rate kredita potrebno je iz glavnog menija sa leve strane izabrati opciju:

1. Interni prenos – > Priprema prenosa ili
 2. Krediti – > Detalji – > Izmiranje obaveza
- U oba slučaja otvoriće vam se sledeći ekran:

The screenshot shows a web browser window with a purple header. The main content area is titled 'Priprema prenosa' with a sub-header '1 2 3'. There is a 'Na teret računa' field with a dropdown menu showing '205-100152682098382 (RSD)'. Below this is the 'Izmirenje za:' section with three radio buttons: 'Platnu karticu', 'Kredit' (selected), and 'Račun'. The 'U korist partije kredita:' field has a dropdown menu showing '001650301363 (EUR)'. The 'Iznos:' field is set to '1000 RSD'. The 'Datum valute:' field is set to '10.11.2008'. At the bottom, there are two buttons: 'Pošalji' and 'Nazad'. In the top right corner of the form, there is a 'Odštampaj' button.

Iznos za likvidaciju

Za prikaz iznosa za likvidaciju kredita potrebno je iz glavnog menija izabrati opciju *Krediti>Pregled*, kliknite na link *Detalji* kako bi se prikazala stranica sa detaljima o kreditu a zatim kliknite na opciju *Iznos za likvidaciju*. Upit na iznos za likvidaciju korisniku daje informaciju koliko je potrebno uplatiti kako bi izmirio sve obaveze i likvidirao kredit. Iako je korisnik celokupnu obavezu po kreditu izmirio davanjem elektronskog naloga kroz WEB E-Bank, to ne znači da je kredit likvidiran već je potrebno kontaktirati vašeg kreditnog referenta oko detalja.

Iznos za likvidaciju kredita		Odštampaj
Podaci od: 09.04.2007 13:21:10.430		
Datum: 09.04.2007		
Iznos u valuti: 755,75 EUR		
Iznos: 60.199,71 RSD		
Nazad		

Kreditni kalkulator

Opcija *Kreditni kalkulator* je informativnog karaktera i klijentima pruža mogućnost računanja približnog iznosa rate kredita u zavisnosti od izabrane kamatne stope i dužine perioda otplate kredita.

Komercijalna banka AD Beograd – Kamatni kalkulator :: - Microsoft Int...

| Pomoć | Štampa | Zatvori



Kalkulator za kredite građanima

Datum: 1 1 2007

Traženi kredit: 10.000,00 din.

Naknada: 0,00 din. 0 %

Učešće: 0,00 din. 0 %

Depozit: 0,00 din. 0 %

Kamata na depozit: 0 %

Rata (anuitet): din.

Interval otplate: mesečni

Period otplate: 12 meseci

Grejs period: 0 meseci

Kamatna stopa: 11,95 % 0,95 %
godišnja mesečna

[Izračunaj](#) [Obriši](#)

[Opšte informacije](#) [Anuitetski plan](#)

Opis	Iznos
Efektivna kamatna stopa:	
Povraćaj depozita:	
Iznos anuiteta (rate):	
Broj anuiteta (rate):	
Iznos kamata:	
Ukupno plaćanja:	

6.1.3. Korišćenje SMS servisa

SMS servis Komercijalne banke a.d. Beograd, omogućava korisnicima mobilnih telefona – klijentima Banke, da jednostavno, u svakom trenutku i sa bilo koje lokacije komuniciraju sa Bankom.

SMS servis mogu koristiti sva fizička i pravna lica – klijenti Banke. Da bi se klijent Banke prijavio za korišćenje servisa potrebno je:

- da poseduje mobilni telefon u mreži nekog od domaćih mobilnih operatera,
- da se u matičnoj ekspozituri Banke registruje Pristupnicom za korišćenje servisa.

Prijava za korišćenje servisa se obavlja na bazi popunjene Pristupnice u matičnoj ekspozituri klijenta i to:

- Pristupnica za korišćenje SMS servisa za fizička lica i
- Pristupnica za korišćenje SMS servisa za pravna lica.

Pristupnica za korišćenje SMS servisa za fizička lica se automatski generiše iz aplikacije za administraciju na bazi unosa JMBG klijenta, dok Pristupnicu za korišćenje SMS servisa za pravna lica, klijent predaje popunjenu i overenu od strane zakonskog zastupnika.

Nakon izvršene registracije za korišćenje servisa, korisnik može odmah početi sa korišćenjem usluga SMS servisa.

SMS poruke se šalju na broj 5622 nezavisno od mreže mobilnog operatera. SMS servis Komercijalne banke a.d. Beograd, fizičkim i pravnim licima omogućava informacije o računima koje klijent poseduje u Banci, kao i usluge automatskog obaveštavanja.

Pored usluga koje su namenjene samo korisnicima SMS servisa, postoje dve javne usluge koje su dostupne svim korisnicima mobilnih telefona u nekoj od mreža nacionalnih operatera:

- informacije o dnevnoj kursnoj listi, ili na određen dan u prethodnom periodu,
- informacije o novitetima iz ponude Banke.

SMS servis Komercijalne banke fizičkim licima omogućava informacije o:

- tekućem računu (stanje na računu, iznos poslednje promene, datum poslednje promene, limit po računu, rok važenja limita, broj nerealizovanih čekova),
- računu dinarske štednje (stanje na računu, rok oročenja),
- deviznom računu i deviznoj štednoj knjižici (informacije za prve četiri aktivne valute sa najvećim stanjem, rok oročenja).

Korisniku SMS servisa za fizička lica dostupne su i usluge automatskog obaveštavanja o:

- prilivu na tekući račun (iznos priliva, datum priliva, opis promene),
- autorizaciji platne kartice (vrsta i broj kartice, datum, vreme, iznos i mesto autorizacije).

SMS servis Komercijalne banke a.d. Beograd pravnim licima omogućava informacije o tekućem računu (stanje na računu, iznos poslednje promene, datum i vreme poslednje promene, opis promene).

Korisniku SMS servisa za pravna lica dostupna je i usluga automatskog obaveštavanja o prilivu na tekući račun (iznos priliva, datum i vreme priliva, opis promene).

Zaposleni u Odeljenju E-banke u skladu sa Instrukcijom za emitovanje SMS poruka, na bazi Zahteva za emitovanje SMS poruka koji dostavlja Sektor marketinga, a na predlog poslovnog sektora, vrše emitovanje poruka svim ili samo ciljnoj grupi korisnika.

6.2. Pokazatelji ostvarenog prometa u E-banci Komercijalne banke a.d. Beograd

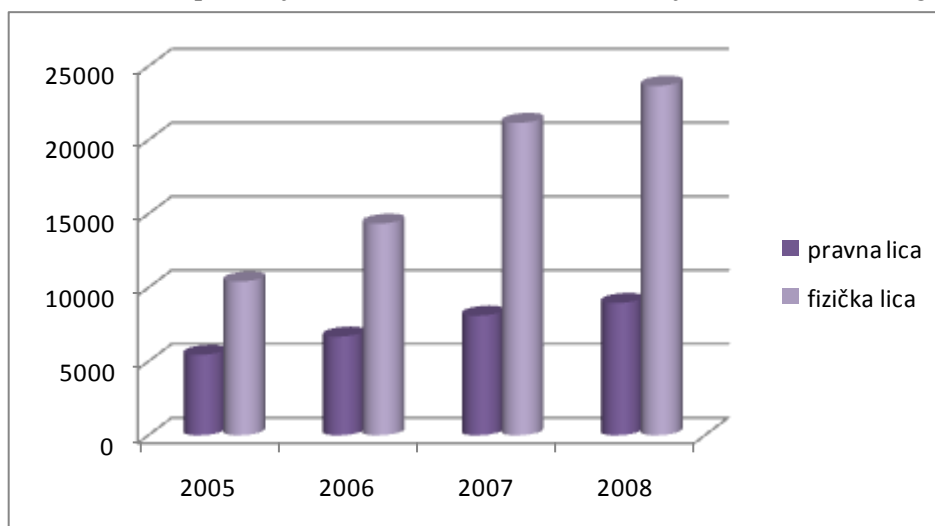
Na osnovu istraživanja koje sam sproveda u Komercijalnoj banci a.d. Beograd, u Odeljenju E-banke, došla sam do sledećih saznanja:

1. U periodu od 2005-2008. godine, broj korisnika elektronskog bankarstva u Komercijalnoj banci a.d. Beograd iz godine u godinu značajno se povećavao.

Tako je Banka na kraju 2005. godine imala 5.452 klijenta - pravna lica koji su koristili elektronsko bankarstvo, a u avgustu 2008. godine imala je 8.967 klijenata - pravnih lica, što predstavlja povećanje od 3.515 klijenata ili 64%. Povećanje u odnosu na 2007. godinu iznosi 10,58% (Grafikon 1).

Što se tiče fizičkih lica, Banka je na kraju 2005. godine imala 10.424 klijenata koji su koristili elektronsko bankarstvo, a 2008. godine imala je 23.682 klijenta, što čini povećanje od 13.258 klijenata, ili 127%. Povećanje u odnosu na 2007. godinu iznosi 11,86% (Grafikon 1).

Grafikon 1: Ukupan broj korisnika e-bankarstva Komercijalne banke a.d. Beograd

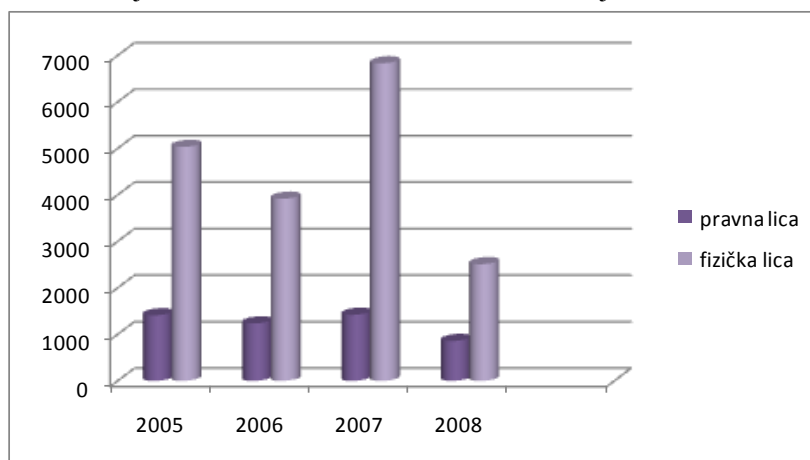


2. Broj novih korisnika elektronskog bankarstva u Komercijalnoj banci a.d. Beograd, po godinama, za pravna i fizička lica prikazan je u Grafikonu 2.

Broj korisnika e-bankarstva u 2005. godini povećan je za 1.409 pravnih lica i 5.033 fizička lica, u 2006. godini za 1.236 pravnih lica i 3.917 fizičkih lica, u 2007. godini to povećanje

iznosi 1.421 za pravna lica i 6.831 za fizička lica i u 2008. godine 858 novih pravnih lica i 2.510 fizičkih lica (Grafikon 2).

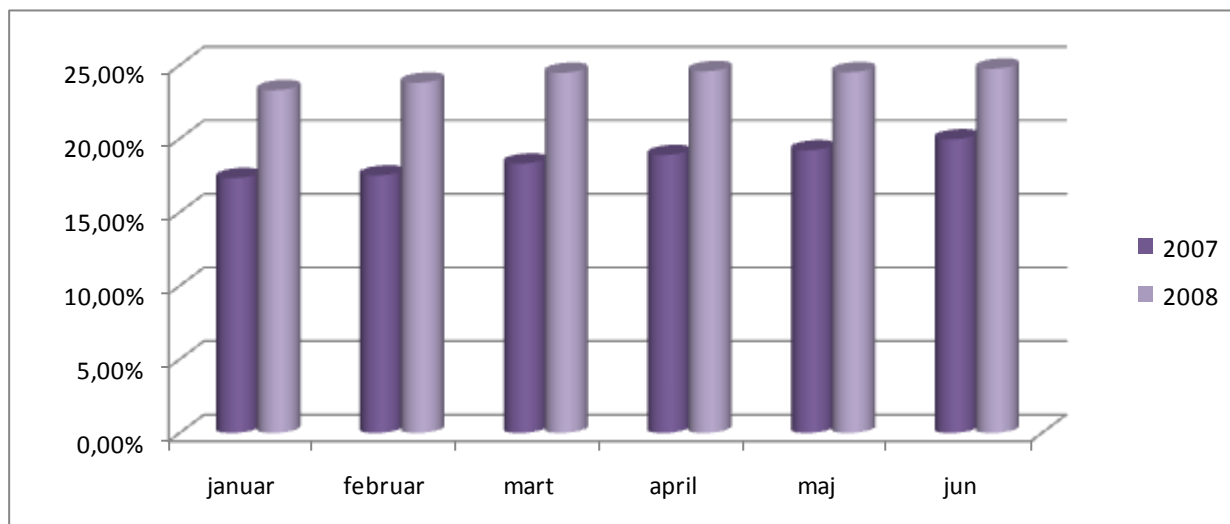
Grafikon 2: Broj novih korisnika e-bankarstva Komercijalne banke a.d. Beograd



3. Kada se posmatra procentualno učešće elektronskih naloga u odnosu na ukupan broj naloga u platnom prometu Komercijalne banke a.d. Beograd, može se konstatovati da je prisutan stalni rast prometa preko e- banke.

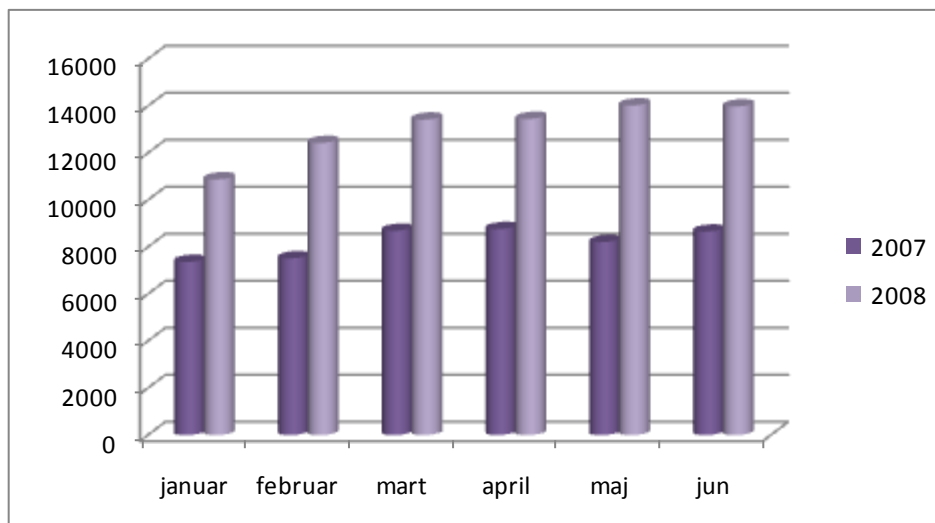
Iz Grafikona 3. vidi se porast procentualnog učešća elektronskih naloga u ukupnom broju, naloga po mesecima u 2007. i 2008. godini. Od januara 2007. godine kada je to učešće iznosilo 17,32%, procenat učešća elektronskih naloga stalno raste, da bi u junu 2008. godine iznosio 24,76% u ukupnom platnom prometu Banke.

Grafikon 3: Procentualno učešće elektronskih naloga u odnosu na ukupan broj naloga u platnom prometu



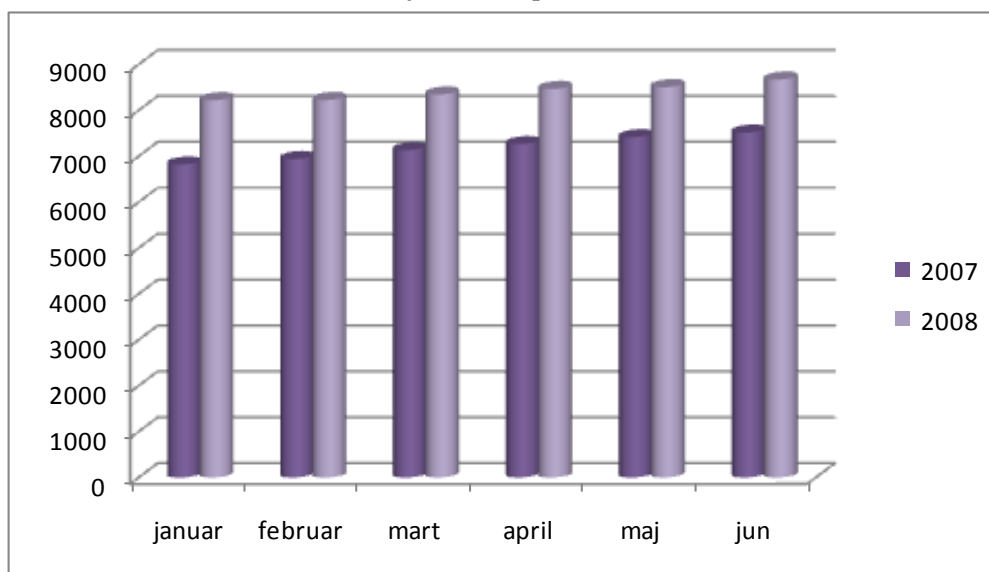
4. Ako se posmatra broj WEB naloga u Komercijalnoj banci a.d. Beograd, može se konstatovati stalni rast iz meseca u mesec. Tako je Banka u prvom polugodištu 2008. godine imala 78.189 WEB naloga, a u prvom polugodištu 2007. godine 49.213 naloga, što znači da je upoređujući ova dva perioda, promet preko e-banke povećan za 58,88% (Grafikon 4).

Grafikon 4: Broj WEB naloga u Komercijalnoj banci a.d. Beograd



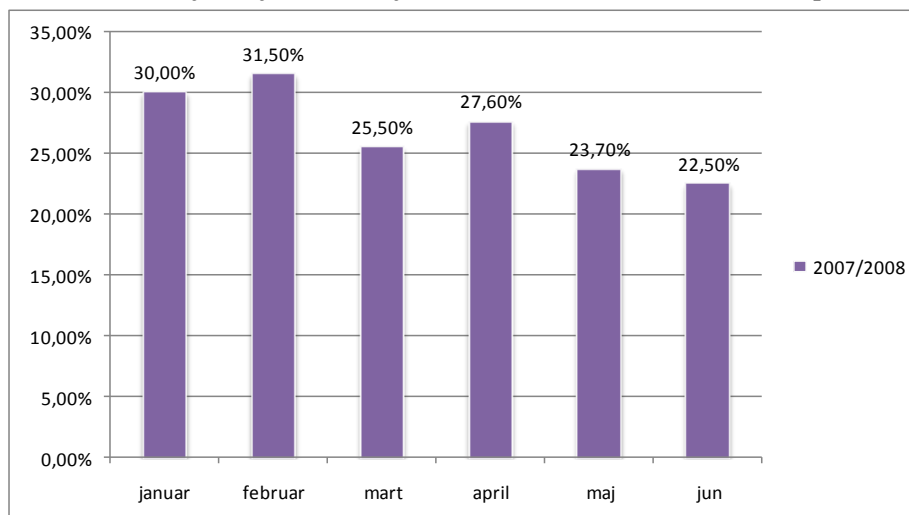
5. Kada se posmatra broj e-računa pravnih lica, može se konstatovati permanentno povećanje iz meseca u mesec i u 2007. i u 2008. godini. Tako je u januaru 2007.godine broj e-računa pravnih lica iznosio je 6.820, da bi u junu 2008. godine dostigao cifru od 8.671. Broj e-računa pravnih lica je povećan za 15,37% za period januar-jun 2007. godine/ januar-jun 2008. godine (Grafikon 5).

Grafikon 5: Broj e-računa pravnih lica



6. Broj transakcija u E-banci u svakom mesecu 2008. godine, povećan je u odnosu na isti mesec prethodne godine. To povećanje u januaru 2008. godine u odnosu na isti mesec 2007. godine iznosi 30,00%, u februaru 31,50%, u martu 25,50%, u aprilu 27,60%, u maju 23,70% i u junu 22,50% (Grafikon 6). Ukupan broj transakcija u E-banci u prvom polugodištu 2008. godine povećan je za 34,91% u odnosu na prvo polugodište prethodne godine.

Grafikon 6: Povećanje broja transakcija u e-banci u odnosu na isti mesec prethodne godine



7. U E-banci Komercijalne banke a.d. Beograd mogu se obavljati sve bezgotovinske transakcije preko računara, vršiti pregled stanja na svojim računima, štampati prometne stavke iz definisanog vremenskog perioda, slati poruke i primati obaveštenja od banke. Sve transakcije putuju direktno na server banke bez posredovanja službenika banke. Bančin službenik je obavešten samo o onim zahtevima klijenta koji zahtevaju dodatno odlučivanje ili rad u koji mora biti uključen čovek. Transakcije se obrađuju odmah, odnosno odmah kada je to moguće. Banka može vratiti (odbiti) platni nalog. U tom slučaju klijent prima obaveštenje o odbijanju izvršenja transakcije.

8. Transakcije se u elektronskoj banci izvode preko javnih komunikacionih medija i zbog toga je njihova zaštita od suštinskog značaja. Sveobuhvatnost zaštite u elektronskoj banci postignut je na način da:

- su podaci tajni i dostupni samo onome kome su namenjeni. Podaci se šifruju na strani pošiljaoca i potom dešifruju kada stignu do primaoca;
- je obezbeđena mogućnost utvrđivanja validnosti i celovitosti podataka digitalnim potpisom klijenta;
- se overava poreklo podataka. Overom se utvrđuje da li je pošiljalac pravi ili se neko pokušava lažno predstaviti. Obezbeđivanjem autentičnosti pošiljaocima je oduzeta mogućnost da se odreknu poslatih podataka ili da ih zataje. Autentičnost utvrđuju overene potvrde (sertifikati) klijenata banke;
- sa odgovarajućom zaštitom onemogućavamo upad u centralni sistem banke.

Sveobuhvatnost zaštite u elektronskoj banci je od ključnog značaja jer se u nju moraju pouzdati kako klijenti (korisnici) tako i banke. Komercijalna banka a.d. Beograd koristi zaštitu pomoću pametne kartice (engl. *Smart Card*).

Zaštita se u Hal E-Bank temelji na vrhunskoj tehnologiji identifikacije korisnika i digitalnog potpisivanja transakcija na osnovu infrastrukture tajnih i javnih ključeva (engl. *Public Key Infrastructure*).

6.3. Unaprećenje poslovanja E - bankarstva

Aplikativna rešenja vezana za elektronsko bankarstvo u Komercijalnoj banci a.d. Beograd, bilo pravnih ili fizičkih lica, odnose se isključivo na aktivnosti iz domena platnog prometa. Odnosno, klijentima se preko E-banke nudi mogućnost svih vrsta plaćanja u zemlji i inostranstvu za pravna lica i mogućnost izmirenja obaveza tj. plaćanja raznih računa za fizička lica u zemlji. Neminovnost daljeg razvoja elektronskog bankarstva, jeste dopuna osnovnog paketa usluga koji se trenutno nudi preko E-banke, pratećim servisima koji će imati za rezultat potpuno zatvaranje poslovnog procesa, odnosno mogućnost da se kompletan poslovni proces oko kredita obavi iz poslovne prostorije i od kuće bez odlaska u banku, kao i mogućnost zamene dokumentarne kontrole (trenutno obavezne u deviznom i spoljno trgovinskom poslovanju) sa elektronskim dokumentima koji su digitalno potpisani, a samim tim i potpuno validni i identični papirnim.

Osnovu daljeg razvoja elektronskih servisa svakako predstavljaju mobilna plaćanja putem mobilnih telefona tj. *Mobile payments/mPayments* rešenja, ili eventualno *mobile banking*, koji su se trenutno počeli nuditi na tržištu. Komercijalna banka a.d. Beograd planira da uskoro implementira *mPayments* rešenje. Ovo rešenje *Halcom* informatike iz Ljubljane (popularno se zove 1,2,3 Pay) je bazirano na WPKI tehnologiji (aktivni sertifikat spušten na Sim karticu-trenutno najviši oblik zaštite) i nudi osnovu za dalji razvoj i širenje usluga klijentima preko ovog servisa. Preko ovog servisa biće moguća kupovina preko Interneta tj. *E-commerce* sa potpunom zaštitom transakcije.

Bez obzira na to koje će rešenje koristiti neka banka, svakako će osnova daljeg razvoja E-bankarstva biti na mobilnom telefonu. Potrebno je klijentima omogućiti da putem mobilnog telefona plaćaju račune - pre svega postpejd račune za mobilne telefone, a nakon toga i račune za fiksne telefone, struju, komunalije, bežični Internet i slično.

Sledeće što je neophodno jeste da se građanima Srbije omogući korišćenje *PayPal* i drugih servisa za sigurno plaćanje na Internetu. Aktuelnim podzakonskim aktima o deviznom poslovanju nije obuhvaćena mogućnost *on line* plaćanja proizvoda i usluga na Internetu. *PayPal* je najpoznatiji od nekoliko servisa koji omogućavaju sigurno *on line* plaćanje i transfer sredstava putema Interneta tzv. elektronskim novcem. Da bismo mogli da koristimo *PayPal*, on mora biti registrovan i zvanično odobren u našoj zemlji. Sve je više vebajtova koji, iz razloga sigurnosti, podržavaju isključivo elektronski novac, pa su građani Srbije uskraćeni za jednu veoma korisnu pogodnost. Zato je neophodno da Ministarstvo za telekomunikacije i informatičko društvo preduzme mere, kako bi građani Srbije što pre mogli da uživaju u prednostima plaćanja elektronskim novcem.

Za dalji razvoj i veće korišćenje prednosti e-bankarstva i informacionih tehnologija, potrebno je da postoji odgovarajuća infrastruktura, mogućnost širokopojasnog pristupa mreži i kritična masa korisnika računara i Interneta.

Ključni preduslov za rast e-bankarstva je obrazovanje stanovništva. U Srbiji oko 30% domaćinstava koristi Internet, ali uglavnom za slanje mejla, a za e-bankarstvo manje. I banke i telekomunikacione kompanije i država treba da rade na edukaciji kako bi se procenat korišćenja e-bankinga povećao. Naša država treba da pomogne i da se uključi u sveobuhvatnije obrazovanje građana u elektronskom plaćanju, jer to je početni korak bez kojeg se ne može govoriti o e-bankingu. Informatičko obrazovanje je premissa, odnosno neophodni uslov daljeg razvoja zemlje.

Za razvoj elektronskog poslovanja u Srbiji neophodno je usvojiti i dopuniti pravnu regulativu koja uređuje ovu oblast. Među poslednjim zemljama u Evropi doneli smo Zakon o elektronskom potpisu, što je dodatno otežalo rad banaka. U firmama za projektovanje i razvoj informacionih sistema ističu da je Srbiji neophodan i zakon koji bi uredio odnose i odgovornosti u složenim relacijama e-trgovine, gde je u igri više strana, trgovac, kupac, isporučilac i njihove banke. Procenjuje se da bi ovakav zakon doprineo napretku domaćeg elektronskog poslovanja. Postojeća zakonska regulativa i rešenja koje ona nude trenutno onemogućavaju brži razvoj elektronskih servisa i predstavljaju određenu kočnicu daljem razvoju, jer pravno nisu uređene oblasti iz kompletnog domena E-poslovanja koje bi omogućile brži i dinamičniji razvoj elektronskih servisa.

ZAKLJUČNA RAZMATRANJA

Pri izradi ove doktorske disertacije, pošlo se od potreba banka u Srbiji da ulažu u nove tehnologije radi ostvarenja konkurentne prednosti i veće efikasnosti u cilju generisanja većeg profita. Nove tehnologije pomažu bankama da smanje troškove obavljanja rutinskih transakcija, smanje pritisak na filijale, a samim tim i broj zaposlenih u filijalama, kao i broj potrebnih filijala. Sa druge strane, omogućava im da ostvare prihode od klijenata koji koriste sisteme elektronskog bankarstva. Takođe, banke sada lakše sakupljaju informacije o svojim korisnicima i njihovim preferencama u pogledu servisa koje banka nudi, što vodi uspostavljanju čvršćih veza i dugoročnih odnosa sa klijentima.

Istraživanja u ovom doktorskom radu, kako iz teorijskih izvora, tako i iz prakse u međunarodnom bankarstvu, a posebno u srpskom bankarstvu, nedvosmisleno potvrđuju postavljenu hipotezu rada: „*Primena savremenih informacionih tehnologija u elektronskom bankarstvu utiče na brže i efikasnije povezivanje klijenata i tokova informacija*“.

Analogno navedenom, respektujući redosled do sada prikazane sistematike izlaganja, moguće je donošenje sledećih bitnih zaključaka:

1. Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja banaka tj. do uvođenja novih kanala distribucije bankarskih usluga, odnosno elektronskog bankarstva. Informacione tehnologije omogućavaju smanjenje troškova obrade podataka i komunikacije, što utiče na smanjenje cene usluga krajnjim korisnicima. Pored navedenog, informacione tehnologije omogućavaju nastanak virtuelnih banaka (koje nemaju fizičkih filijala i kod kojih su potrebe za brojem zaposlenih minimalne) i sve veće korišćenje elektronskog novca. Osnovni efekat razvoja informacione tehnologije jeste povećanje konkurencije na finansijskom tržištu, iz razloga što je olakšan pristup informacijama, koje nude davaoci korisnicima usluga.

Nikada u istoriji bankarskog poslovanja nisu učinjene tako velike i korenite promene kao za poslednjih tridesetak godina. Pojava plastičnog i digitalnog novca učinili su preokret ka potpunoj dematerijalizaciji i virtuelizaciji novca. Internet, e-bankarstvo i mobilno bankarstvo su doveli do toga da je banka izašla iz svojih prostorija. Danas banka dolazi u kuću korisnika ili na njegovo radno mesto.

2. Najznačajnije promene koje su do sada ostvarene u domenu elektronskog bankarstva odnose se pretežno na domen rutinskih transakcija u bankama, i to pre svega u platnom prometu. Sistemi za elektronski prenos sredstava (engl. *Electronic Funds Transfer System - EFTS*) predstavljaju prve manifestacije uvođenja tehnoloških inovacija na bazi primene informacione i komunikacione tehnologije (*ITC*), tako da za ranu fazu e-bankarstvo praktično znači uvođenje informacione i komunikacione tehnologije u sistem plaćanja. Platni promet doživljava suštinsku promenu sa uvođenjem elektronskog prenosa novca (engl. *Electronic Funds Transfer - EFT*) koji rešava mnoge probleme prethodnih sistema plaćanja.

Pored platnog prometa, EFT je našao značajnu primenu i u drugim rutinskim operacijama koje banke vrše za svoje klijente, kao što su polaganje novca na transakcione i štedne račune, transfer novca sa jednog računa na drugi, upitima stanja na računima, transakcijama na deviznom i novčanom tržištu, kupovini i prodaji vrednosnih papira i itd.

Tehničko-finansijske inovacije vode intenzivnoj globalnoj utakmici sa bankarskim okruženjem. Dolazi ne samo do reinženjeringa u bankama, već i do reinženjeringa u procesima između samih banaka, banaka i njihovih klijenata i između klijenata i trećih lica međusobno. Sa prelaskom na novu tehničko-tehnološku osnovu stvara se nova filozofija poslovanja koja sa sobom nosi prilagođavanje softverskih rešenja korisničkim potrebama, promenu strategije nastupa banaka, načina i metoda upravljanja rizicima itd.

One banke koje ne uspeju da održe korak sa razvojem informacione tehnologije, mogle bi da izgube deo svojih klijenata, smanje svoje poslovanje i ostanu bez većeg profita. Banke moraju ne samo da prate razvoj i ulažu u novu tehnologiju, već i da koordiniraju i kombinuju pružanje svojih usluga koristeći veći broj različitih kanala distribucije. Adekvatna primena savremene informacione tehnologije i informacionih sistema u bankarstvu, a naročito korišćenje Interneta, obezbeđuje bankama konkurentnu tržišnu poziciju i dugoročnu poslovnu egzistenciju.

Najveće tehnološko dostignuće u razvoju bankarstva je pojava elektronskog novca. Elektronski novac se može definisati kao informacija o monetarnoj vrednosti koju je moguće transferisati kroz računarske mreže. Da bi zamenio „klasičan novac“, elektronski novac mora biti univerzalno prihvaćen, što znači da može da se daje iz „ruke u ruku“, ali i da funkcioniše u računarskim mrežama. Transakcije obavljene elektronskim novcem moraju biti jeftinije od klasičnih transakcija, izdavanje (emitovanje) novca, njegovo servisiranje i korišćenje moraju biti jeftinije od rada klasičnim novcem. Uopšteno govoreći, elektronski novac mora pružati znatne prednosti kako bi od korisnika bio široko prihvaćen. Za sada elektronski novac samo u određenim segmentima uspešno zamenjuje klasičan, ali tamo gde je prihvaćen obezbeđuje veliku brzinu protoka novca. Prihvatljivost iz „ruke u ruku“ nije postignut u zadovoljavajućem nivou. Razlog za manju prihvatljivost elektronskog novca je u tome što mora da se izvrši provera stanja na računu ili kreditne sposobnosti onoga ko nudi elektronski novac, što nije slučaj kod klasičnog novca.

Činjenica je da elektronski novac sve više dobija na značaju. Internet kao ogromni poslovni potencijal zahteva elektronski novac i uopšte nije sporno da će se njegova upotreba sve više širiti. Da bi zadovoljio korisnike mora da ispunji neke uslove. Mora biti lako prenosiv, da troškovi njegovog kreiranja i rukovanja budu mali ili bar niži od klasičnog novca, mora da omogućava promet bez posrednika, to jest da se sa njim mogu raditi „off line“ transakcije. Posebno mora da obezbedi anonimnost učesnika u transakciji.

Razvoj e-bankarstva tesno je povezan sa razvojem elektronskih kartica kao sredstva koje omogućava aktiviranje terminala za masovno korišćenje bankarskih usluga na različitim mestima.

Prednosti upotrebe platnih kartica su nesumnjive i to kako za klijente, tako i za banke. Klijentima banke se pruža komoditet u obavljanju poslova sa bankom kod podizanja gotovine na bankomatima, bez potrebe čekanja na šalterima i u bilo koje vreme nezavisno od radnog vremena banke. Prednosti upotrebe platnih kartica klijenti mogu osetiti i pri plaćanju određenih roba ili usluga. Korisnici platnih kartica nemaju potrebu da nose gotovinu sa sobom, s obzirom na to da su sve radnje obavezne da primaju platne kartice. To znači da korisnici platnih kartica mogu izvršiti plaćanje jednostavnim prezentovanjem iste. Sa druge strane, odobrena kreditna kartica omogućava korisnicima jednostavnu, pogotovo „impulsnu“ kupovinu proizvoda ili usluga. I na kraju, imaocima kartica pruža sigurnost u odnosu na gotov

novac, jer u slučaju gubitka iste potrebno je samo pozvati autorizovani centar koji će blokirati mogućnost upotrebe iste.

Platne kartice sve više dobijaju na značaju kao metod obračuna za plaćanja na malo pri kupovini određenih proizvoda ili usluga. Najveće kompanije koje posluju sa kreditnim i debitnim karticama organizovale su zasebne elektronske klirinške i obračunske sisteme. MasterCard i VISA imaju svoje sopstvene mreže koje se koriste za verifikaciju transakcija širom sveta. Elektronski terminali na mestu prodaje, EFT/POS terminali, omogućavaju da se podaci sa kartice provere za manje od 15 sekundi u okviru mreže koja povezuje prodavce širom sveta sa centrom za obradu kreditnih ili debitnih kartica i emitentom kartica.

Smart kartice se sve više koriste za potrebe e-poslovanja, zbog toga su veoma moćno sredstvo za poboljšanje sigurnosti elektronskih transakcija. Najveća snaga Smart Card tehnologije je u raznovrsnosti mogućih primena. Na bazi nje moguće je razvijanje većeg broja različitih sigurnosnih aplikacija u oblasti zaštite pristupa računaru ili mreži, identifikacije, mobilne telefonije, elektronskog novca, digitalnog potpisa.

Mobilno bankarstvo je najnoviji trend u razvoju elektronskog bankarstva. Prognozira se da će mobilno bankarstvo doći i snajm se ekspanziju od Internet bankarstva u narednih tri do pet godina, s obzirom na to da broj korisnika mobilnih telefona daleko prevazilazi broj korisnika Interneta.

Mobilno bankarstvo omogućava transakcije putem prenosnih računara (lap-top), digitalnih ličnih organizacija (PDA) i mobilnih telefona, koji su opremljeni specijalnim softverom za mobilni pristup Internetu, što znači da korisnik može pristupiti svojoj finansijskoj instituciji pomoću mobilnog telefona i izvršiti željene transakcije. Mobilna plaćanja putem mobilnih telefona spadaju u grupu plaćanja na malo.

3. Elektronska plaćanja podrazumevaju transfer novca i izvršenje plaćanja primenom elektronske tehnologije. Elektronska plaćanja velikih vrednosti se obavljaju upotrebom privatnih informacionih mreža. Korisnici ovih mreža su banke i druge finansijske institucije. Ovakve mreže se koriste i za obavljanje međunarodnih plaćanja (kao što je mreža S.W.I.F.T. organizacije) i za unutrašnji platni promet (primer američke mreže FEDWIRE).

Plaćanja malih vrednosti se elektronski obavljaju uglavnom primenom platnih kartica. Najsavremeniji vid platnih kartica su platne kartice sa elektronskim očitavanjem informacija i one omogućavaju elektronska plaćanja, uglavnom primenom elektronskog prenosa sredstava sa mesta prodaje (engl. *electronic funds transfer at point-of-sale - EFTPOS*). Korišćenje Interneta kao komunikacionog kanala i u oblasti plaćanja, je uslovilo pojavu Internet plaćanja i odgovarajućih instrumenata kojima se ova plaćanja obavljaju i to: elektronske gotovine, elektronskih čekova i Internet platnih kartica. Dok su maloprodajna plaćanja osvojila Internet, međubankarska plaćanja još nisu počela da se obavljaju preko ove mreže, zbog još uvek prisutne nesigurnosti, kada se radi o velikim iznosima transfera.

Nastanak novih zaštitnih sistema će pomoći da se razvije kompletno bankarsko-finansijsko poslovanje na Internetu, jer se kao motiv pojavljuju znatno niži troškovi poslovanja. Sistem zaštite ne sme suviše povećavati troškove poslovanja, kako ne bi postalo neracionalno da se posluje na Internetu, ali u isto vreme troškovi sigurnosnog sistema su mali kada se ima u vidu potencijalna šteta nastala neovlašćenim upadom u sistem banke.

Aktuelna kretanja na finansijskim tržištimā ukazuju na to da je danas teško naći tržiste, koje nije u fazi zamene klasičnog trgovanja, elektronskim trgovanjem, ili koje ne planira ovakav poduhvat. Globalizacija berzanskog poslovanja, podrazumeva automatizaciju postojećih sistema i povezivanje sa berzama. Na ovakav način omogućava se realizacija ponude usluga svim potencijalnim korisnicima, ma gde se nalazili. Elektronski način trgovanja akcijama jeftiniji je i fleksibilniji od dosadašnjeg načina trgovanja akcijama i idealna je solucija za rastuće potrebe korisnika za trgovanjem bez vremenskog ograničenja.

Elektronske berze, kao tehnološki napredniji modalitet organizacije ovog poslovanja, baziraju se na primeni informacionih tehnologija, a posebno mrežne ekonomije. U tom kontekstu posebnu ulogu ima Internet kao multimedijaska svetska mreža, zbog toga što omogućava transformaciju samog berzanskog poslovanja, primenu njegovog modela, oblikovanje drugačijih odnosa između učesnika i doprinosi promenama u strukturi. Berze su sve manje fizičke institucije, a sve više virtuelne institucije koje omogućavaju pojednostavljen i uprošćen pristup informacijama, kao i funkcionisanje po principu rada na daljinu. Prodiranje informacione tehnologije u berze i njihovo poslovanje predstavlja jedan od najznačajnijih fenomena u ovoj oblasti.

4. Primena informacione tehnologije u bankarstvu donosi, sa jedne strane, snažan porast organizacionih i ekonomskih potencijala, a sa druge strane, otvara prostor za pojavu novih oblika rizika. Znači, brzi razvoj potencijala e-bankinga nosi i rizike i koristi. Zbog toga se adekvatno obezbeđenje sigurnosti, pojavljuje kao poseban kritičan faktor u funkcionisanju elektronskog bankarstva. Sve ovo zahteva razvijanje posebnih metoda kontrole i nadzora, a to je funkcija koju banke moraju da razvijaju do maksimuma kako bi zadržale visok nivo poverenja i sigurnosti svojih korisnika.

Od borda direktora i top menadžmenta očekuje se da donesu eksplicitnu i dokumentovanu stratešku odluku u pogledu toga kako će banka da pruža usluge e-bankinga. Inicijalna odluka treba da obuhvati specifičnu odgovornost, politiku i kontrolu za bavljenje rizicima, uključujući rizike koji nastaju u prekograničnom kontekstu. Efektivan upravljački nadzor treba da obuhvati revidovanje i odobrenje ključnih aspekata bančinog procesa kontrole sigurnosti, kao što su razvoj i održavanje infrastrukture kontrole sigurnosti koja valjano štiti sisteme e-bankinga i podatke za upravljanje rizicima povezanim sa povećanom složenošću i povećanim oslanjanjem na odnose autorsinga i zavisnošću od treće strane u obavljanju kritičnih funkcija e-bankinga.

Mada je bord direktora odgovoran da obezbedi odgovarajuće procese kontrole sigurnosti za e-banking, suština ovih procesa zahteva specijalnu pažnju menadžmenta zbog pojačanih pretnji sigurnosti koje donosi e-banking. Ovo treba da uključi postavljanje odgovarajućih mera poverljive autorizacije i autentifikacije, logičke kontrole i kontrole fizičkog pristupa, adekvatnu infrastrukturu sigurnosti za održavanje odgovarajućih ograničenja i restrikcija za aktivnosti internih i eksternih korisnika i integritet podataka o transakcijama, arhive i informacija. Pored toga, treba obezbediti postojanje jasnih dnevnika, jer sve transakcije e-bankinga treba da su obezbeđene i mere za obezbeđenje poverljivosti ključnih informacija e-bankinga treba da odgovaraju osetljivosti tih informacija.

Da bi se banke zaštitile od poslovnog, pravnog i reputacionog rizika, usluge e-bankinga moraju da se daju konzistentno i blagovremeno, u skladu sa visokim očekivanjima klijenata u pogledu stalne i brze raspoloživosti, ali i u skladu sa potencijalno visokom tražnjom za transakcijama. Banke moraju da budu sposobne da pružaju usluge e-bankinga svim krajnjim

korisnicima i da budu u stanju da održe takvu raspoloživost u svim okolnostima. Efektivni mehanizmi za reagovanje na incidente su, takođe, od ključnog značaja za umanjenje operativnog, pravnog i reputacionog rizika koji nastaju kao posledica neočekivanih događaja, uključujući interne i eksterne napade, koji mogu da ugroze pružanje e-banking sistema i usluga. Da bi se odgovorilo očekivanjima klijenata, banke moraju da imaju efektivni kapacitet, poslovni kontinuitet i planove za svaku eventualnost. Banke treba da razviju odgovarajuće planove za reagovanje na incidente, uključujući komunikacione strategije, koje obezbeđuju kontinuitet poslovanja, kontrolu reputacionog rizika i limitiranje obaveza po osnovu poremećaja u njihovim uslugama e-bankinga.

5. Za zaštitu elektronskih poruka su razvijeni brojni bezbednosni mehanizmi za koje se koriste jedna ili više metodologija zaštite.

Nivo zaštite razmenljivih elektronskih poruka izuzetno je značajan element na osnovu kojeg se korisnici opredeljuju za ili protiv primene e-transakcija. To je posebno karakteristično u slučajevima kada gubitak, izmena, neovlašćeni uvid ili neke druge pretnje elektronskim dokumentima mogu da izazovu značajne pravne i finansijske posledice po učesniku u *online* transakciji. Naime, u e-poslovanju i razmeni elektronskih dokumenata učestvuju brojni partneri i svi moraju da imaju odgovarajući nivo zaštite.

Smanjivanje rizika u elektronskom poslovanju kompleksan je postupak, koji obuhvata nove tehnologije, organizacione politike i procedure, nove zakone i industrijske standarde na osnovu kojih će se dati ovlašćenja nadležnim organima da gone i kažnjavaju počinioce sajber – kriminalnih radnji. Međutim, potpuna sigurnost ne postoji. Ali, trajna sigurnost u informatičkoj eri nije ni potrebna. Podaci obično imaju vrednost u određenom vremenskom periodu, tako da se prema potrebi zaštite jedan dan, ili mesec, ili godinu.

Kriptografija se bavi čuvanjem tajnosti informacija, što ima poseban značaj kada se poverljivi podaci prenose, odnosno smeštaju u bilo kakav elektronski sistem. Da bi se obezbedila sigurnost poruka koje se šalju preko Interneta, koriste se različite tehnologije kriptografije. Ova tehnologija bazira se na dva podprocesa: najpre se vrši šifrovanje poruke koja se šalje, a zatim njeno dešifrovanje nakon prijema, pomoću odgovarajućih algoritama, korišćenjem tzv. ključa. Šifrovanjem, poruka treba da se zaštiti tako da je ne može pročitati niko osim njenog pošiljaoca i primaoca. Sigurnost prenosa šifrovane poruke zavisi od tajnosti ključa.

Upotreba računara i telekomunikacija dovele su do potrebe uvođenja digitalnog potpisa kao zamene za funkciju svojeručnog potpisa (engl. *written signature*) u uslovima tradicionalnog bankarskog poslovanja. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca) i da obezbedi garantovanje identiteta pošiljaoca poruke. Ovakav potpis se može u pravnim postupcima i radnjama smatrati digitalnim ekvivalentom svojeručnog potpisa na papirnom dokumentu. Digitalni potpis se smatra najvišim stepenom zaštite.

Od razrešenja problema zaštite elektronskih podataka zavisi će i razvoj poslovanja na Internetu. Elektronsko poslovanje nesporno je donelo mnoge „blagodeti“, ali i brojne opasnosti. Što je njegov rast i zastupljenost veća, to su i posledice zloupotrebe teže.

6. Rast koji je u nekoliko poslednjih godina doživelo elektronsko poslovanje, u odnosu na klasične tipove poslovanja, dovelo je do promene pravila poslovanja i njegove regulacije.

S obzirom da elektronsko poslovanje omogućava izvršavanje klasičnih poslovnih zloupotreba kao što su prevare, finansijske malverzacije, ili izbegavanje plaćanja poreza na nov način, potrebno ga je posebno regulisati, jer se pravila i kontrolni mehanizmi klasičnog poslovanja ne mogu primeniti. Međutim, to nije tako jednostavno, prvenstveno zato što je ovo nova oblast poslovanja koja je u stalnim i brzim promenama. Pored toga, tehnologija koja se primenjuje nije ograničena samo na jedan region, ili zemlju. Izlaz je pokušao da se nađe u međunarodnim organizacijama i telima kao što su Ujedinjene nacije, Svetska trgovinska organizacija, ili u okviru regionalnih ekonomskih integracija, kao što je Evropska unija. Sporost u dogovaranju koja je posledica usaglašavanja stavova između zainteresovanih država, prouzrokuje relativnu neefikasnost ovih tela. Pored toga, njihove odluke su obavezne samo za one države koje su se izjasnile da ih prihvataju. Međutim, potrebe za smanjenjem troškova poslovanja i želja za povećanjem tržišta koja je sublimirana u elektronskom poslovanju, dovela je do toga da mnoge razvijene zemlje ubrzano pristupaju njegovom regulisanju.

Regulisanje pravnih aspekata elektronskog poslovanja je veoma značajno, jer ovaj vid poslovanja direktno dovodi u pitanje funkcionisanje tradicionalnih pravnih režima koji su zasnovani na pravilima pismene evidencije, postojanju originalnih potpisanih dokumenata i sličnim faktorima koji nemaju svoje ekvivalente u domenu elektronskog poslovanja.

Potpuno adekvatna zakonska regulativa za elektronsko poslovanje praktično još uvek ne postoji ni u većini razvijenih zemalja najvećih korisnika informacionih tehnologija, a da se zemlje u razvoju i zemlje u tranziciji još uvek nalaze na samom početku izgradnje legislative u ovom domenu. Razvijene zemlje, kao najveći korisnici elektronskog poslovanja, sigurno su i najaktivnije u svim oblastima razvoja i podrške uvođenju elektronskih transakcija, pa i u izgradnji pravnog okvira.

Sigurno je da će još dosta vremena proći dok se ne usaglase zakonske regulative vezane za poslovanje pojedinaca i preduzeća na Internetu. Do tada, nedostatak zakonske regulative onemogućavaće određene segmente poslovanja, dok će sa druge strane omogućavati primenu širokog spektra nezakonitih aktivnosti u poslovanju pojedinaca i preduzeća na Internetu.

Razvoj elektronske trgovine u EU zavisi od kreiranja takvog legalnog okvira koji će obezbediti značajne pravne garancije za komercijalne transakcije koje se realizuju elektronski i koji će omogućiti slobodno kretanje elektronskih usluga. Pristup EU u ovom domenu balansira između potrebe regulisanja e-trgovine i opasnosti preterane regulacije koja može ugroziti dalji razvoj ovog novog sektora.

U našoj zemlji je prisutna i sve više se razvija svest o neophodnosti i velikoj koristi od primene elektronskog poslovanja. Naša država, po uzoru na Evropsku uniju, mora da se postara da privredna društva u tom sektoru posluju u uslovima konkurencije i međusobne ravnopravnosti, uz uvažavanje interesa korisnika njihovih usluga. Upravo iz svih ovih razloga postoji velika potreba da se i u našoj zemlji donese Zakon o elektronskom poslovanju, čija je priprema počela 2000. godine i još uvek je u nacrtu. Zakon o elektronskom potpisu donet je 2004. godine, a 2009. donet je Zakon o elektronskom dokumentu. Krivični zakon je 2003. godine izmenjen i dopunjen sa nizom potpuno novih inkriminacija, posebno u oblasti zaštite računarskih programa, Internet mreže i protoka podataka, bezbednosti podataka na mreži, hakerskih upada i raznih zloupotreba.

Međutim, izrada, donošenje i implementacija Zakona o elektronskom poslovanju, u okvirima postojećeg pravnog sistema otvara mnoge probleme. Treba imati u vidu globalne okolnosti: integraciju u Evropsku uniju, odnosno činjenicu da ovaj zakon, kao i svaki drugi, treba da se uklopi u postojeći zakonski sistem, koji je na putu harmonizacije sa zakonskim sistemom Evropske unije. Posebno treba voditi računa o nizu lokalnih faktora, koji se na prvom mestu odnose na postojeće domaće zakone koji su na snazi i regulišu oblasti u tesnoj vezi sa ovom oblašću.

7. U Srbiji razvoj elektronske banke počinje tek sa reformama bankarskog sektora i prelaskom platnog prometa u bankarski sistem. Do tog trenutka banke su jedini vid elektronskog poslovanja ostvarivale u domenu deviznog sektora tj. poslovnih odnosa sa inostranstvom i to putem SWIFT-a. Domaće banke u domenu elektronskog bankarstva, vide svoju šansu razvoja, te dolazi do ulaganja značajnog iznosa finansijskih sredstava i kupovine savremene informaciono-komunikacione tehnologije, koja omogućava početak poslovanja banaka u elektronskoj sferi. Danas se može konstatovati da većina banaka ima razvijen sistem elektronskog poslovanja koji podrazumeva saradnju banke i sa pravnim i sa fizičkim licima kao klijentima, ali i saradnju banaka sa nacionalnim regulatornim institucijama pre svega sa NBS.

Primenom e-bankinga u različitim sektorima nacionalne privrede povećava se povezanost i međuzavisnost računarskih mreža privatnih i javnih organizacija uključenih u domaće i međunarodne ekonomske aktivnosti. Na ovaj način, nacionalna privreda se kreće iz faze interaktivnog delovanja autonomnih subjekata ka fazi integrisanog sistema za upravljanje informacionim tokovima u privredi, što joj daje karakteristike e-ekonomije, ili društva zasnovanog na informacijama. U savremenoj eri globalnog razvoja svetske privrede i društva, e-poslovanje postaje pokretač svetskog privrednog porasta. Izostanak primene e-poslovanja vodi ograničavanju razvoja nacionalne privrede.

Elektronsko bankarstvo u Srbiji je još daleko od dostizanja svog zenita, ali sa svakodnevnim povećanjem učešća elektronskog poslovanja polako, ali sigurno dostižemo razvijene zemlje Zapadne Evrope. Postojeća zakonska regulativa i rešenja koje ona nude trenutno onemogućavaju brži razvoj elektronskih servisa i predstavljaju određenu kočnicu daljem razvoju, jer pravno nisu uređene oblasti iz kompletnog domena e-poslovanja koje bi omogućile brži i dinamičniji razvoj elektronskih servisa.

Razvoj elektronskog bankarstva u Srbiji svakako su obeležila i društveno politička dešavanja na ovim prostorima u ne tako davnoj prošlosti, što ima za rezultat skromnije poslovne pokazatelje u odnosu na zemlje u okruženju. Trenutno, u Srbiji elektronsko bankarstvo koristi mali broj klijenata i, za sada se, ne može predvideti kojim će tempom ta primena rasti, što nameće potrebu ulaganja značajnih sredstava banke u razvoj, marketing i obrazovanje klijenata. Ključni preduslov za rast e-bankarstva je obrazovanje stanovništva. U Srbiji oko 30% domaćinstava koristi Internet, ali uglavnom za slanje *e-maila*, a za e-bankarstvo manje. I banke i telekomunikacione kompanije i država treba da rade na edukaciji kako bi se procenat korišćenja e-bankinga povećao.

Snižavanjem tarife elektronskih transakcija u odnosu na šalterske transakcije učiniće da elektronska plaćanja postanu preovlađujući način plaćanja građana.

Aplikativna rešenja vezana za elektronsko bankarstvo, bilo pravnih, ili fizičkih lica, odnose se isključivo na aktivnosti iz domena platnog prometa, odnosno klijentima se preko E-banke

nudi mogućnost svih vrsta plaćanja u zemlji i inostranstvu za pravna lica i mogućnost izmirenja obaveza tj. plaćanja raznih računa za fizička lica. Neminovnost daljeg razvoja elektronskog bankarstva u Srbiji, jeste dopuna osnovnog paketa usluga koji se trenutno nudi preko E-banke, pratećim servisima koji će imati za rezultat potpuno zatvaranje poslovnog procesa, odnosno mogućnost da se kompletan poslovni proces obavi iz poslovne prostorije i od kuće bez odlaska u banku, kao i mogućnost zamene dokumentarne kontrole (trenutno obavezne u deviznom i spoljno trgovinskom poslovanju) sa elektronskim dokumentima koji su digitalno potpisani, a samim tim i potpuno validni i identični papirnim.

U uslovima globalne finansijske krize, kada je neophodno sniziti troškove poslovanja u smislu smanjenja broja filijala ili agenata, elektronska komunikacija sa klijentima predstavlja pravo rešenje. Treba da težimo da postanemo lideri u ovoj oblasti i da se poredimo sa savremenim svetom, jer je tu prostor za napredovanje ogroman.

Komercijalna banka a.d. Beograd, u poređenju sa ostalim domaćim bankama, ima najsavremenije elektronske servise iz oblasti korporativnog e-bankarstva i najsveobuhvatnije web rešenje namenjeno fizičkim licima koje predstavlja rezultat zajedničkog rada na razvoju između banke sa jedne i vendara – proizvođača softvera sa druge strane, što, svakako, predstavlja pozitivan primer kvalitetnog strateškog partnerstva.

Svesna svoje pozicije na tržištu, kao i činjenice da svojim potezima utiče i na aktivnosti svih ostalih banaka u Srbiji, Komercijalna banka a.d. Beograd brižljivo bira svoje poteze i punu pažnju posvećuje obrazovanju svojih klijenata i kompletnog okruženja, čime stvara povoljnu klimu za veću penetraciju elektronskih servisa u odnosu na klasičan oblik bankarskog poslovanja.

Sve je veći broj klijenata koji, umesto odlaska na bankarski šalter, plaćanje računa obavljaju elektronskim putem, koristeći prednosti i pogodnosti koje pruža *online* bankarstvo.

U periodu od 2005-2008. godine broj korisnika elektronskog bankarstva u Komercijalnoj banci a.d. Beograd se znatno povećao. Broj pravnih lica koja su koristila e-bankarstvo u ovom periodu je povećan za 3.515, ili 64%, a fizičkih lica za 13.258 ili 127%.

Konstantno se povećava broj elektronskih naloga u odnosu na ukupan broj naloga u platnom prometu Banke. U prvom polugodištu 2008. godine promet preko E-banke je povećan za 56,18% u odnosu na isti period 2007. godine.

Osnovu daljeg razvoja elektronskih servisa svakako predstavljaju mobilna plaćanja putem mobilnih telefona tj. *Mobile payments/mPayments* rešenja, ili eventualno *mobile banking*, koji su se trenutno počeli nuditi na tržištu. Komercijalna banka a.d. Beograd planira da uskoro implementira *mPayments* rešenje. Ovo rešenje *Halcom* informatike iz Ljubljane (popularno se zove 1,2,3 Pay) je bazirano na WPKI tehnologiji (aktivni sertifikat spušten na Sim karticu-trenutno najviši oblik zaštite) i nudi osnovu za dalji razvoj i širenje usluga klijentima preko ovog servisa. Preko ovog servisa biće moguća kupovina preko Interneta tj. e-commerce sa potpunom zaštitom transakcije.

8. Neminovnost daljeg razvoja elektronskog bankarstva, jeste dopuna osnovnog paketa usluga koji se trenutno nudi preko E-banke, pratećim servisima koji će imati za rezultat potpuno zatvaranje poslovnog procesa, odnosno mogućnost da se kompletan poslovni proces oko kredita obavi iz poslovne prostorije i od kuće bez odlaska u banku, kao i mogućnost zamene

dokumentarne kontrole (trenutno obavezne u deviznom i spoljno trgovinskom poslovanju) sa elektronskim dokumentima koji su digitalno potpisani, a samim tim i potpuno validni i identični papirnim.

Za dalji razvoj i veće korišćenje prednosti e-bankarstva i informacionih tehnologija u Srbiji, potrebno je da postoji odgovarajuća infrastruktura, mogućnost širokopojasnog pristupa mreži i kritična masa korisnika računara i Interneta.

LITERATURA

1. Backstrom Hans, Peter Stenkula: „ELECTRONIC MONEY – RISKS, QUESTIONS, POTENTIAL“, Sveriges Riksbank Quarterly Review No.1, 1997.
2. Backstrom Hans: „EU, EMU AND THE PAYMENT SYSTEM“, Sveriges Riksbank Quarterly Review No.4, 1995.
3. Bjelica, V,: „BANKARSTVO“, Stilos, Novi Sad, 2001.
4. Bjelić, P,: „ELEKTONSKO TRGOVANJE“, Institut za međunarodnu politiku i privredu, Beograd, 2000.
5. Bjelić, P,: „MOBILNI TELEFON KAO KANAL ELEKTRONSKOG POSLOVANJA“, Ekonomski anali br.151-2, oktobar 2001-mart 2002.
6. Brewer, M,: „INTERNET BANKING“, A S Pratt, 1999.
7. Burton, M, Lombra, R: „THE FINANCIAL SYSTEM AND THE ECONOMY: Principles of Money & Banking“, Thomson/South-Western, 2006.
8. Chaffey, D,: „E-BUSINESS AND E-COMMERCE MANAGEMENT“, Prentice Hall, London, 2002.
9. Chen, S,: „STRATEGIC MANAGEMENT OF E-BUSINESS“, ohn Wiley & Sons, West Sussex, 2005.
10. Claessens, S, Glaessner, T, Klingebiel, D: „ELECTRONIC FINANCE: A New Approach to Financial Sector Development“, World Bank, 2002.
11. Cronin, M,: „BANKING AND FINANCE ON THE INTERNET“, SCN Education B.V, 2001.
12. Ćirović, M,: „BANKARSTVO“, Naučno društvo Srbije, Beograd, 2007.
13. Ćirović, M,: „ELEKTRONSKE MREŽE INTERBANKARSKIH PLAĆANJA“, Poslovni krug, Beograd, 1997.
14. Daniel, Elizabeth, Chris Storey: „ON LINE BANKING: Strategic and Management Challenges“, Elsevier Science Long-Range Planning, No.6., 1997.
15. Deitel, H.M, Deitel, P.J, Steinbuhler, K,: „E-BUSINESS AND E-COMMERCE FOR MANAGERS“, Prentice Hall, New Jersey, 2001.
16. Dinić, S, Pantović, V, Starčević, D,: „SAVREMENO POSLOVANJE I INTERNET TEHNOLOGIJE“, Energoprojekt-Ingraf, Beograd, 2007.
17. Erik Banks: „E-FINANCE: The Electronic Revolution“, Wiley, 2001.
18. Ford, W., M.S.Baum,: „SECURE ELECTRONIC COMMERCE“, Prentice Hall PTR, 2001.
19. Frederic S. Mishkin: „MONETARNA EKONOMIJA, BANKARSTVO I FINANSIJSKA TRŽIŠTA“, prevod, Data status, Beograd, 2006.
20. Gkoutzinis Ath Apostolos: „INTERNET BANKING AND THE LAW IN EUROPE: Regulation, Financial Integration And Electronic Commerce“, Cambridge Univ Pr, 2006.
21. Hadžić, M,: „BANKARSTVO“, Fakultet za finansijski menadžment i osiguranje, Beograd, 2007.
22. Ivković, M, Milošević, S, Subić, Z, Dobrilović, D,: „ELEKTRONSKO POSLOVANJE“, Tehnički fakultet Mihajlo Pupin, Zrenjanin, 2005.
23. Jayaram Kondabagil: „RISK MANAGEMENT IN ELECTRONIC BANKING: Concepts and Best Practices“, Wiley, 2007.
24. James W. Kolari and Benton E. Gup: „COMMERCIAL BANKING: THE MANAGEMENT OF RISK“, John Wiley & Sons, 2004.
25. Jonathan Coppel: „E-COMMERCE: IMPACTS AND POLICY CHALLENGES“, OECD, 2000.
26. Joshi C. Vasant: „E-FINANCE“, Sage Pubns, 2004.

27. Jošanov, B, Perić, D,: „ELEKTRONSKO POSLOVANJE: pogled iz Srbije“, monografija, Prometej, Novi Sad, 2005.
28. Kalkota, R, Robinsnon, M,: „E-POSLOVANJE“, Mate, Zagreb, 2002.
29. Kaufman, C., Perlman, R. and Speciner, M,: „NETWORK SECURITY“ (Private Communication in a Public World), 2nd edition, Prentice Hall 2002.
30. Kotlica, S,: „INFORMACIONO TEHNOLOŠKA PARADIGMA I EKONOMSKI RAZVOJ“, Institut ekonomskih nauka, Beograd, 1996.
31. Laudon, C.K.et.all: „E-COMMERCE: Business, Technology, Society“, Addison Wesley, Boston, 2001.
32. Lutovac ,M, Tošić, D,: „BIZNIS PLAN ZA ELEKTRONSKO POSLOVANJE“, Viša elektrotehnička škola, Beograd, 2007.
33. Lutovac, M, Tošić, D, Pocajt, V: „OSNOVI ELEKTRONSKOG POSLOVANJA“, Viša elektrotehnička škola, Beograd, 2007.
34. Mahmood Shah and Steve Clarke: „E-BANKING MANAGEMENT: Issues, Solutions, and Strategies“, Information Science Publishing, 2008.
35. Marić, S, Novaković, I,: „ELEKTRONSKO POSLOVANJE (E-BUSINESS)“, Kvarak, Kraljevo, 2006.
36. Marković, M, Simić, R,: „POSLOVNO BANKARSTVO I ELEKTRONSKO POSLOVANJE“, Beogradska poslovna škola, Beograd, 2004.
37. Marković, M, Simić, R, Todorović, M,: „INFORMACIONI SISTEMI U BANKARSTVU“, Beogradska poslovna škola, Blace,2001.
38. Marković, M, Simić, R, Todorović, M,: „ELEKTRONSKO POSLOVANJE“, Beogradska poslovna škola, Blace, 2003.
39. Miller, J,: „ELECTRONIC BANKING“, SCN Education B.V, 2001.
40. Miller, J,: „E-BANKING: Integrating and Managing Your Banks Electronic Services“, A S Pratt, 1999.
41. Novaković, I,: „MENADŽMENT ELEKTRONSKOG POSLOVANJA“, Kvarak, Kraljevo, 2006.
42. Novaković, J,: „ELEKTRONSKO POSLOVANJE“, Megatrend, Beograd, 2005.
43. Oppliger, R,: „INTERNET AND INTRANET SECURITY“, ARTECH HOUSE, 1998, ISBN 0-89006-829
44. Oppliger, R,: „SECURITY TECHNOLOGIES FOR THE WORLD WIDE WEB“, Artech House, 2000, ISBN 1-58053-045-1.
45. Orr, Bill: „E-BANKS OR E-BRANCHES?“, ABA Banking Journal, 1999.
46. Plant, R,: „E-COMMERCE FORMULATION OF STRATEGY“, Prentice Hall, 1999.
47. Pleskonjić, D, Đorđević, B, Maček, N, Carić, M,: „SIGURNOST RAČUNARSKIH MREŽA“, Viša elektrotehnička škola, Beograd, 2006.
48. Pocajt, V,: „ELEKTRONSKO POSLOVANJE I KAKO USPETI U NJEMU“, Zbornik radova Info-Teh, Vrnjačka Banja, 2003.
49. Radojević, T,: „MEĐUNARODNA I DOMAĆA REGULATIVA PROTIV PRANJA NOVCA“, časopis „Spoljnotrgovinski savetnik“ br.3/2007, Poslovni biro, Beograd, str.15-28
50. Radojević, T,: „REGULATIVA EU IZ OBLASTI BANKARSTVA, FINANSIJA I POSLOVANJA HARTIJAMA OD VREDNOSTI“, časopis „Spoljnotrgovinski savetnik“ br.5/2007, Poslovni biro, Beograd, str.51-59
51. Radojević, T,: „ELEKTRONSKO PODNOŠENJE DOKUMENATA CARINI“, časopis „Spoljnotrgovinski savetnik“ br.12/2007, Poslovni biro, Beograd, str.45-54
52. Radojević, T,: „OKVIRNA DIREKTIVA EU O MREŽAMA I USLUGAMA ELEKTRONSKIH KOMUNIKACIJA“, časopis „Spoljnotrgovinski savetnik“ br.6/2008, Poslovni biro, Beograd, str.27-30

53. Radojević, T.: „DIREKTIVA EU O PRAVNOJ ZAŠTITI BAZA PODATAKA“, časopis „Spoljnotrgovinski savetnik“ br.6/2008, Poslovni biro, Beograd, str.31-36
54. Radojević, T.: „KAPITALNI POSLOVI SA INOSTRANSTVOM“, časopis „Finansijske, Bankarstvo, Revizija i Osiguranje“ br. 02/2007, Fakultet za finansijski menadžment i osiguranje, Beograd, str. 56-69
55. Radojević, T, Stakić, B.: „FINANSIJSKI I DEVIZNI MENADŽMENT U TURIZMU“, Univerzitet Singidunum, Beograd, 2009.
56. Rimpi Jatana and R. K. Uppal: „E-BANKING IN INDIA: CHALLENGES AND OPPORTUNITIES“, New Century Publications, 2007.
57. Robson, Mark: „ELETRONIC MONEY: PUBLIC POLICY ISSUES“, Bank of England, Financial Stability Review, 1996.
58. Rose S. Peter, Sylvia C. Hudgine.: „BANKARSKI MENADŽMENT I FINANSIJSKE USLUGE“, prevod, Data status, Beograd, 2005.
59. Rose S. Peter: „MENADŽMENT KOMERCIJALNIH BANAKA“, Prevod, Mate, Zagreb, 1999.
60. Rose S. Peter: „COMMERCIAL BANK MANAGEMENT“, 5th Edition, McGraw-Hill Irwin, Boston 2002.
61. Schneier, B.: „APPLIED CRYPTOGRAPHY“, John Wiley & Sons, Inc., 1996.
62. Sharma M.K., Gupta S.K., Verma S.B.: „E - BANKING AND THE DEVELOPMENT OF BANKS“, Deep and Deep Publications Pvt. Ltd., 2008.
63. Sheppard, David: „PAYMENT SYSTEMS“, Handbook in Central Banking No. 8. London: Bank of London, 1996.
64. Stankić, R.: „ELEKTRONSKO POSLOVANJE“, Ekonomski fakultet, Beograd, 2007.
65. Starčević, D: „PERMANENTNO OBRAZOVANJE KAO PREDUSLOV USPEŠNOG RAZVOJA E-POSLOVANJA“, Privredna komora Beograda, Beograd, 2004.
66. Strauss, J, El-Ansary, Frost, R.: „E-MARKETING“, Pearson Prentice Hall, New Jersey, 2006.
67. Subramani N., Gamesan V., and Anbalagan D.: „E-COMMERCE AND E-BANKING“, Abhijeet Publications, 2008.
68. Suman C. Jain : „E – BANKING“, RBSA Publishers, 2006.
69. Turban, Efram Jea Lee, David King, H. Micheal Chung: „ELETRONIC COMMERCE: A managerial perspective“, Printice Hall, 2000.
70. Hufl, SL, Wade, M, Schneberger, S.: „CASES IN ELETRONIC COMMERCE“, McGraw Hill, Boston, 2000.
71. Uroš, T.: „ELEKTRONSKO POSLOVANJE“, Beogradska poslovna škola, Beograd, 2006.
72. Uroš, T.: „ELEKTRONSKO BANKARSTVO“, Beogradska poslovna škola, Beograd, 2008.
73. Varagić, D.: „RAJ I PAKAO INTERNET MARKETINGA“, Prometej, Beograd, 2002.
74. Vasković, V.: „SISTEMI PLAĆANJA U ELEKTRONSKM POSLOVANJU“, Fakultet oragizacionih nauka, Beograd, 2007.
75. Vidas-Bubanja, M.: „E-POSLOVANJE: Menadžment, tehnologije, aplikacije“, Beogradska poslovna škola, Beograd, 2005.
76. Vujović, S.: „ELEKTRONSKO POSLOVANJE I POSLOVNA INTELIGENCIJA“, Univerzitet Braća Karić, Beograd, 2005.
77. Vujović, T.: „ELEKTRONSKO BANKARSTVO I ELEKTRONSKI NOVAC: poslovanje sa elektronskim novcem, rizici i uticaj na monetarnu politiku“, Jugoslovensko bankarstvo, br. 9-10/2002.

78. Vuković, D,: „PRINCIPI UPRAVLJANJA RIZIKOM ZA ELEKTRONSKO BANKARSTVO – prevod“, Jugoslovenski pregled, Beograd, 2007.
79. Vuksanović, E,: „ELEKTRONSKO BANKARSTVO“, Fakultet za bankarstvo, osiguranje i finansije, Institut ekonomskih nauka, Beograd, 2006.
80. Vuksanović, E,: „MEHANIZMI I INSTRUMENTI PLAĆANJA U USLOVIMA ELEKTRONSKOG PRENOSA SREDSTAVA“, u knjizi „Elektronski prenos novca“, SAM Konsalting, Beograd, 1994.
81. Vunjak, N,: „FINANSIJSKI MENADŽMENT“, Proleter Bečej, Subotica, 2005.
82. Vunjak, N, Kovačević, Lj,: „POSLOVNO BANKARSTVO“, Proleter Bečej, Subotica, 2002.
83. Vunjak, N, Kovačević, Lj,: „BANKARSTVO (Bankarski menadžmet)“, Subotica, 2006.
84. Tivanović, B,: „KUĆNO BANKARSTVO (TOKENI U ELEKTRONSKOM BANKARSTVU) HOMEBANKING“, Zbornik radova E-trgovina, Palić 2004.
85. Welch, B,: „ELECTRONIC BANKING AND TREASURY SECURITY“, Woodhead, Abington, 2005.
86. William Stallings: „NETWORK SECURITY ESSENTIALS“, Prentice, Third Edition, 2007.

NEAUTORIZOVANI IZVORI:

1. Zakon o elektronskom potpisu („Sl. glasnik RS“, br. 135/2004)
2. Zakon o elektronskom dokumentu („Sl. glasnik RS“, br. 51/2009)
3. Zakon o bankama („Sl. glasnik RS“, br. 107/2005)

ELEKTRONSKI IZVORI

www.kombank.com
www.nbs.rs
www.etrgovina.org
www.emagazin.rs
www.ogledalo.rs
www.emportal.rs
www.ebb-bg.com
www.pexim.com
www.24x7.com
www.bankerinter.net
www.eccf.su.ac.yu
www.psee.edu.cg.yu
www.bis.org
www.towergroup.com
www.austin.tex.ac
www.swift.com
www.visabs.com
www.wapforum.com
www.mobeyforum.com
www.mobiletransaction.org
www.openmobilealliance.org
www.corporate.visa.com
www.ieee.org
www.europe.eu.int
www.rsa.com
www.europay.com
www.visa.com
www.mastercard.com
www.digsigtrust.com
www.otp.org
www.pkiforum.com
www.saferpay.com
www.lucent.com
www.newyorkfed.org
www.arraydev.com
www.cybercash.com

SKRAĆENICE

ACH – Automated Clearing House
ALM - Asset liability management
ATM – Automated teller machine
CHIPS – Clearing House Inter-Bank Payments System
CRM – Customer Relationship Management
ECBS – European Committee for Banking Standard
ECHO – European Clearing House
ECN - Electronic communication network
EDAT – Electronic direct access trading
EDI – Electronic Data Interchange
EDIFACT - Electronic Data Interchange For Administration, Commerce and Transport
EEPROM - Electrically erasable programmable read-only memory
EFT – Electronic funds transfer
EFTPOS – Electronic funds transfer at point of sale
EFTS – Electronic Funds Transfer System
FEDI - Financial electronic data interchange
FTP – File Transfer Protocol
FVCM – Financial Value Chain Management
GSTPA – Global Straight Through Processing Association
HB – Home banking
HTTP - Hypertext Transfer Protocol
IBOS – International Banking One Solution
ISO - International Organization for Standardization
ITC - Information Technology and Communication
MATIF - Marché à Terme International de France
NASDAQ - National Association of Securities Dealers Automated Quotations
OTPP – On line Third Party Processors
PDA - Personal digital assistant
PIN – Personal Identification Number
PKI – Public Key Infrastructure
POS – Point of sale
PPTP – Point to Point Tunneling Protocol
PROM - Programmable Read-Only Memory
RAM – Random Access Memory
ROM – Read Only Memory
RTGS – Real Time Gross Settlement
SEEM - *Single* European Electronic Market
SEPA – Single European Payment Area
SET – Secure Electronic Transaction
S-HTTP – Secure Hypertext Transfer Protocol
SIP - Session Initiation Protocol
SMTP – Standard Mail Transfer Protocol

SSL – Secure Socket Layer

STP – Straight Through Processing

SWIFT - Society for Worldwide Interbank Financial Telecommunication

TAN – Transaction access number

TARGET - Trans-European Automated Real-time Gross settlement Express Transfer System

TCP/IP – Transmission Control Protocol/Internet Protocol

UNCITRAL - United Nations Commission on International Trade Law

UNCTAD – United Nations Conference on Trade and Development

URL - Uniform Resource Locator

VPN – Virtual Private Network

WAP - Wireless Application Protocol

WIPO - The World Intellectual Property Organization

WTO - The World Trade Organization