



UNIVERZITET SINGIDUNUM

FAKULTET ZA POSLOVNU EKONOMIJU

Beograd, Danijelova 32

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

- *Master rad* -

***Metodološko tehnološke osnove elektronskog
bankarstva***

E- BANKING

Profesor:

Docent, dr Gojko Grubor

Student:

Boško Purić

Beograd, jun 2011.

SADRŽAJ

1. METODOLOGIJA ISTRAŽIVAČKOG RADA.....	- 3 -
1.1. Uvodne napomene	- 3 -
1.2. Predmet istraživanja.....	- 3 -
1.3. Ciljevi istraživanja	- 4 -
1.4. Hipotetički okvir.....	- 4 -
1.5. Metode istraživanja.....	- 5 -
2. METODOLOŠKO TEHNOLOŠKE OSNOVE ELEKTRONSKOG BANKARSTVA.....	- 6 -
2.1. Uvod.....	- 6 -
2.1.1. Nastanak Interneta	- 6 -
2.1.2. Značaj računarskih komunikacija za strateško pozicioniranje preduzeća.....	- 9 -
2.1.3. Računarske mreže u poslovnim komunikacijama	- 9 -
2.1.4. Primena ISDN-a u poslovnim komunikacijama.....	- 11 -
2.1.5. Komunikacioni protokoli.....	- 13 -
2.1.6. Značaj informacione tehnologije za razvoj poslovnih komunikacija	- 15 -
2.1.7. Uloga tehnologije u formiranju mrežnog okruženja.....	- 16 -
2.1.8. Internet i intranet	- 18 -
2.1.9. Ekstranet	- 19 -
2.2. Internet bankarstvo	- 21 -
2.2.1. On-line bankarstvo	- 22 -
2.2.2. Internet bankarstvo banaka	- 22 -
2.2.3. Razvoj internet bankarstva.....	- 23 -
2.2.4. Vrste i načini primene internet bankarstva	- 23 -
2.2.5. Osnovi pojmovi u primeni Internet bankarstva.....	- 23 -
2.2.6. Internet protokol IPV6.....	- 24 -
2.2.7. Predstavljanje adresa u IPV6	- 26 -
2.2.8. IPv6 tipovi adresa.....	- 28 -
2.2.9. Identifikovanje IPv6 tipova adresa.....	- 29 -
2.2.10. Sigurnost.....	- 33 -
2.2.11. Podrška mobilnim sistemima	- 34 -
2.3. Ključni protokoli za potporu internet bankarstva http (Hypertext Transfer Protocol)	- 34 -
2.3.1. Autentifikacija i sigurnost HTTP protokola.....	- 35 -
2.3.2. SSL (Secure Sockets Layer)	- 36 -
2.3.3. Vrste SSL potvrda	- 36 -
2.3.4. Opšti prikaz SSL protokola.....	- 37 -
2.3.5. Slabosti i ranjivosti SSL protokola.....	- 39 -
2.3.6. On-line plaćanje kreditnim karticama	- 39 -
2.3.7. S-HTTP i SSL	- 44 -
2.3.8. SSL protokol u primeni	- 45 -
2.3.9. Zaštita informacija B2B E-Bank Sistema	- 46 -
2.3.10. Problemi poverenja pri plaćanju kreditnom karticom	- 47 -
2.4. WEB servisi	- 48 -
2.4.1. Karakteristike Web servisa	- 48 -

2.4.2. Praktična strana WEB servisa	- 50 -
2.4.3. SOAP	- 51 -
2.4.4. Prednosti Web servisa u odnosu na "klasične" Web aplikacije.....	- 52 -
2.4.5. Primeri upotrebe web servisa	- 52 -
2.4.6. Potencijali u domaćim uslovima	- 53 -
2.5. Elektronsko bankarstvo	- 54 -
2.5.1. Model E-BANK	- 56 -
2.5.2. SWIFT sistem	- 57 -
2.5.3. Elektronski platni promet i sistemi plaćanja	- 59 -
2.5.4. Elektronski novac (E-novac).....	- 59 -
2.5.4.1. Karakteristike e-novca	- 60 -
2.5.4.2. E-novac u kompjuteru korisnika (eCoins)	- 60 -
2.5.4.3. E-novac za mikroplaćanja (Qpass)	- 61 -
2.5.4.4. P2P plaćanje.....	- 61 -
2.5.5. Elektronski čekovi (E-čekovi).....	- 61 -
2.5.6. Elektronske (plastične/platne) kartice.....	- 62 -
2.6. Distributivne mreže elektronskog bankarstva	- 65 -
2.6.1. ATM sistemi (bankomati).....	- 66 -
2.6.2. POS sistemi.....	- 67 -
2.6.3. Telefonsko bankarstvo.....	- 68 -
2.6.4. PC bankarstvo	- 69 -
2.6.4.1. Video bankarstvo.....	- 71 -
2.6.4.2. SMS bankarstvo	- 71 -
2.6.5. INTERNET bankarstvo	- 72 -
2.6.6. Mobilno bankarstvo.....	- 75 -
3. CASE STUDY U EURO BANCI.....	- 77 -
3.1. Istorijat bankarstva – Eurobanka	- 78 -
3.2. Eurobanka o Bazel III.....	- 79 -
3.3. Pristupi upravljanja bankarskim rizicima u skladu sa Bazel II	- 82 -
3.3.1. Tržišni rizik.....	- 83 -
3.3.2. Operativni rizik	- 84 -
3.3.3. Value at Risk.....	- 85 -
3.4. Osnovni pojmovi vezani za sigurnost podataka Euro banke.....	- 87 -
4. DISKUSIJA (KOMENTAR ISTRAŽIVANJA)	- 88 -
5. ZAKLJUČAK.....	- 90 -
6. LITERATURA	- 94 -

1. METODOLOGIJA ISTRAŽIVAČKOG RADA

1.1. Uvodne napomene

Razvoj internet bankarstva vezan je za sve širu primjenu računarske i telekomunikacione tehnologije u procesu obrade i prenosa podataka i informacija. Ove tehnologije dovode do krupnih promjena 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 reinženjeringa poslovnih procesa u bankama, već i do reinženjeringa 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 zamjenjuju automatizovanom proizvodnjom i isporukom usluga. Troškovi velikih transakcija se smanjuju, a bankarske i finansijske usluge depersonalizuju.

Usled ubrzanog širenja internet bankarskih sistema dolazi do velikih preokreta u suštini samog internet 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 reinženjering.

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

1.2. Predmet istraživanja

Primjena računara i novih tehnologija u postojećim djelatnostima ubrzala je dolazak do novih znanja, otkrivanje novih i poboljšanje postojećih tehnologija, odnosno pojavu novih ili usavršenih proizvoda zasnovanih na korišćenju takvih tehnologija. Internet poslovanje predstavlja tendenciju ekonomsko-političkog preuređenja sveta, jer neke države ekonomskom snagom prerastaju svoje geografske granice i slede strategiju proširenja. Masovnost upotrebe elektronskog novca dovela je i do novog pojma u bankarstvu, *elektronsko bankarstvo* (*electronic banking, e-banking*), koje se ogleda u kompjuterizaciji odnosno elektronskom prenosu sredstava, kako u okvirima platnog prometa tako i u obavljanju pojedinačnih bankarskih poslova sa komitentima i klijentima u privredi i sa građanima.

Predmet istraživanja rada je:

- analiza informacionih tehnologija, računarskih mreža i protokola u cilju unapređenja poslovne komunikacije;
- primjena internet bankarstva i opis sistema sigurnosti i zaštite poslovanja banaka na internetu;
- autentifikacija i sigurnost ključnih protokola za potporu internet bankarstva (*Hypertext Transfer Protocol, Secure Sockets Layer*);
- upotreba web servisa i njeni potencijali u domaćoj privredi.

1.3. Ciljevi istraživanja

Tehnološki razvoj, a naročito informatika omogućili su bankama da ponude nove proizvode i usluge, pomjere prostorne i vremenske granice svog poslovanja, dopru do svakog svog klijenta ma gdje se on nalazio. Proces transfera novčanih sredstava je time znatno pojednostavljen. Primjenom kompjuterskog procesiranja podataka dolazi do znatnog razvoja internet bankarstva.

Glavni cilj rada je analiza informacionih tehnologija i elektronskog poslovanje sa svim aspektima i mogućnostima primene u cilju što bržeg i efikasnijeg povezivanja klijenata i tokovi informacija. Tajna uspješnog savremenog informacionog sistema je fleksibilna infrastruktura bazirana na personalnim računarima, modernim računskim mrežama i Internetu prije svega.

Naučni cilj ovog istraživanja jeste primjena savremenih računarskih mreža i protokola u internet bankarstvu, prednosti korišćenja ovih tehnika, njegova komparacija sa tendencijama koje odlikuju najznačajnije bankarske sisteme u svijetu danas; naučni opis promjena u našem internet bankarstvu na institucionalnom i funkcionalnom planu, iz ugla nove strukture banaka i novih proizvoda koje one nude.

Društveni cilj izrade ovog rada je doprinos proučavanju i razumijevanju savremenih tendencija tehnološkog razvoja svjetskog internet bankarstva, kako bi se dalji razvoj bankarstva kod nas odvijao u skladu sa sistemskim promjenama na socijalnom, političkom i ekonomskom planu, a njegove korelacije sa integracionim procesima u svijetu vodile dostizanju najvišeg kvaliteta bankarskih usluga.

1.4. Hipotetički okvir

Osnovni efekat razvoja informacione tehnologije jeste povećanje konkurencije na finansijskom tržištu, iz razloga što je značajno olakšan pristup informacijama, koje nude davaoci korisnicima usluga. 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.

Hipotetički okvir istraživanja sastoji se od sledećih pretpostavki:

H1: Uvođenje informacionih tehnologija u bankarski sektor je neophodno, s obzirom na to da je u ovom sektoru konkurencija sve više izražena.

Generalnu hipotezu operacionalizujemo preko sledećih posebnih hipoteza:

- Primjena savremenih informacionih tehnologija u elektronskom bankarstvu utiče na brže i efikasnije povezivanje klijenata i tokova informacija.
- Bankarsko tržište kao jak kontrolni mehanizam bankarskog upravljanja, intenzivno promoviše upotrebu elektronskog bankarstva radi ostvarenja boljih poslovnih i finansijskih performansi banaka.
- Od ekonomske snage banke direktno zavisi uvođenje novih tehnologija.

1.5. Metode istraživanja

Metodološki pristup istraživanja koji će se primenjivati u izradi ovog istraživanja postavljen je veoma kompleksno i zahtijeva primjenu:

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

2. METODOLOŠKO TEHNOLOŠKE OSNOVE ELEKTRONSKOG BANKARSTVA

2.1. Uvod

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja. Glavni cilj je postao da se bez obzira na geografske distance što brže i efikasnije povežu klijenti i tokovi informacija. U uslovima vrlo jake konkurencije gdje postepeno nestaju razlike između banaka, investicionih banaka, brokerskih firmi i osiguravajućih kompanija, finansijske organizacije su pod stalnim pritiskom da zadrže korisnike svojih usluga, smanje troškove, upravljaju rizikom i koriste tehnologiju kao izvor konkurentne prednosti. Model globalne organizacije i jake konkurencije zahtijeva novu koncepciju pristupa banaka u njihovom poslovanju, o čemu svedoče sve veća ulaganja u specijalizovanu i prema klijentu orijentisanu tehnologiju. Internet je jedna od tih tehnologija.

Banke su prvobitno imale odbojnost prema inovacijama koje donosi poslovanje na Internetu, ali su tokom vremena uvidjele da to nije prolazni fenomen nego sve više dio poslovne stvarnosti sa još većom perspektivom u budućnosti. Danas postoji preko 1000 svetskih banaka koje nude klijentima mogućnost obavljanja bankarskih transakcija direktno iz kuće, posredstvom Interneta.

Elektronsko bankarstvo predstavlja segment digitalne ekonomije u sferi elektronskog platnog prometa i transfera novčanih sredstava, a u međuvremenu se razvilo na sve vidove poslovanja banaka, kako unutar njene organizacije tako i na njene komitente. Institucionalno bankarstvo i finansijska tržišta imaju za poslovno okruženje sve privredne i poslovno aktivne subjekte, koji su najdirektnije upućeni na međusobnu poslovnu saradnju. Preko usluga koje bankarski sektor obavlja za svoje komitente i klijente, i preko finansijskih inovacija koje je neophodno nuditi u tržišnim uslovima, sve više dolazi do izražaja poslovna saradnja, zasnovana na savremenim informacionim i telekomunikacionim tehnologijama, što ima za rezultat transformaciju načina rada i poslovne saradnje ka elektronskom poslovanju i digitalnoj ekonomiji.

2.1.1. Nastanak Interneta

Internet je zajedničko ime za grupu informacionih resursa rasprostranjenih širom sveta. Internet se još naziva i mreža svih mreža jer su u nju povezane mreže obrazovnih i vladinih institucija kao i komercijalnih organizacija skoro svih zemalja sveta. Međutim, bila bi greška razmišljati o Internet-u samo kao o računarskoj mreži, ili čak o grupi međusobno povezanih računarskih mreža. Lepota i upotrebna vrednost Interneta leži u stvari u informacijama koje se na njemu nalaze. Internet omogućuje milionima ljudi širom sveta da komuniciraju i dele informacije. Može se komunicirati bilo slanjem i primanjem elektronske pošte, bilo uspostavljanjem veze sa nečijim računarom i razmenjivati interaktivne poruke. Internetov predek je ARPANET što je skraćenica od *Advanced Research Project Agency*, prva mreža širokog područja (*Wide-Area Network*,

WAN). Originalno je razvijena u ranim sedamdesetim, pod nadzorom Agencije za napredne istraživačke projekte odbrane (DARPA) Ministarstva odbrane SAD.

Taj projekat je podrazumevao niz eksperimenata kojima je trebalo otkriti metode umrežavanja računara, radi povezivanja Ministarstva odbrane sa ugovorenim stranama u vojnim istraživanjima, na univerzitetima na kojima su se obavljala istraživanja koje je finansirala vojska. Usled zabrinutost o opstajanju komunikacionih linija u slučaju nuklearnog napada, vazduhoplovne snage SAD-a su morale imati osiguranje da će i dalje komunicirati sa svojim snagama. Korporacija RAND predložila je sistem bez centralizovane komande, jer bi svaki centralizovani sistem mogao biti meta napada. Predloženi sistem, razvijen je od strane Paul Baran-a, predlagao je decentralizovani sistem koji bi još uvek bio operativan bez obzira da li je neki deo sistema uništen.

Sve međusobne veze u mreži mogu da šalju i primaju poruke, šalju ih do drugih međusobnih tačaka (zvanih čvorovi - node), sve dok poruka ne stigne do njene destinacije.

Informacije bi bile slane u malim paketima. Paketi bi putovali od čvora do čvora, svaki paket bi odlučivao kako će poslati paket do sledećeg dostupnog čvora. Iako bi neki čvorovi bili uništeni, poruka bi bila poslata alternativnim čvorom (nodom). Na ovaj način, mreža bi se održala u slučaju nuklearnog napada. Najznačajniji rezultat razvoja ARPANET jeste TCP/IP protokol koji je definisan 1983. godine i koji predstavlja način za razmenu podataka između različitih računara i mreža. Povezivanje računara je bilo interesantno i za komercijalne organizacije pa se javljaju brojne mreže koje povezuju računare različitih organizacija, zatim se javljaju pokušaji povezivanja tih mreža prvo na nacionalnom principu a potom i na globalnoj osnovi. Kao rezultat tih napora nastao je INTERNET.

Internet je skup povezanih mreža, sastavljen od dve ili više manjih mreža od kojih svaka koristi Internet protokol (IP) za međusobno komuniciranje. Internet je ubedljivo najveća mreža na svetu. Internet i njemu pridružene tehnologije menjaju se brže nego što to iko može da prati i predvidi, on predstavlja najznačajniji tehnološki fenomen na kraju XX veka.

Internet nema vlasnika, tj. niko nema vlast nad njegovom celinom niti ima mogućnosti da uvodi pravila. Svako je zapravo vlasnik samo svog računara, neke firme su vlasnici zajedničkih komunikacijskih kanala i opreme. Takva "savremena anarhija" na mreži bez nekih većih problema odlično funkcioniše. Međutim, telekomunikacione kompanije održavaju njihove linkove koje nose sve postojeće informacije koje se razmenjuju između host kompjutera. Zatim, imamo vladajućih tela koja kontrolišu ili nadgledaju izvesne delove Interneta. Jedan od primera je dodeljivanje domena i IP adrese.

Internet je sopstveni najbolji izbor softvera (programa) i skoro sav softver koji se može dobiti na Internetu je besplatan. Doduše većina softvera je besplatna za probu, ali nije uvek besplatna za upotrebu. Danas Internet postaje svetski virtuelni računar. Troškovi pristupa Internetu se svode na troškove zakupa vremena provedenog na Internetu koje plaćamo provajderu i na troškove zauzetosti telefonske linije, s obzirom da se Internetu obično pristupa preko telefonske linije.

Nastanak Interneta doveo je do naglog zaokreta i novih pravila ponašanja u informatičkim delatnostima i nauci. Ogromno tržište, velike uštede u marketingu (reklamiranje, prezentacije), naterale su mnoge institucije da se priključe na mrežu svih mreža-Internet.

Elektronsko poslovanje je nova tehnologija, nastala osamdesetih godina, čiji je razvoj onemogućavao nedostatak bezbednosti u vršenju monetarnih transakcija. Međutim, nastankom prvog kriptografskog sistema koji koristi javni ključ 1983. godine, počinje ekspanzija ove tehnologije. Donedavno, nedostatak bezbednosti u vršenju ovakvih transakcija je onemogućavao njihov razvoj, međutim danas, PKI (Public Key Infrastructure - infrastruktura javnog ključa) i smart ("pametne") kartice nude pouzdano rešenje. Klijentima je omogućeno da pomoću jednog rešenja mogu pristupiti svojim računima u svim bankama koje koriste rešenje E-Bank kao samostalno, ili putem EBB Beograd, što pruža obostrane uštede u poslovanju.

Smanjenje troškova, ušteda vremena i povećanje produktivnosti su potencijalne prednosti koje elektronsko poslovanje može doneti u poslovnim odnosima. Kada dve strane elektronski povežete, direktnom linijom ili virtualno preko elektronskog prodajnog mesta, vi elektronski spajate prodavce i kupce i tada ih stavljate u istu grupu korisnika - korisnika elektronskog poslovanja (*e-business*) preko Interneta,. Samim tim raste i važnost elektronskog poslovanja. Nova mesta za elektronsku kupovinu se brzo šire u svim vidovima industrije od poljoprivrede do automobilske industrije, bankarstva i dalje. Direktno elektronsko poslovanje između kompanija zauzima oko 85% ukupnih *e-commerce* transakcija, dok analitičari predviđaju još brži rast. Do 2010. prema predviđanjima *Forrester Research-a*, tržište će iznositi oko 2.500 milijardi \$ naspram 55 milijardi \$ u 1999.

Ali najveća prepreka usvajanju Internet poslovanja je nedostatak bezbednosti i poverenja.

Elektronsko poslovanje između kompanija i potrošača se zasniva na sigurnim plaćanjima, ali poslovanje između kompanija je mnogo zahtevnije. Ono zahteva sistem bezbednosti ne samo za finansijske transakcije nego i elektronske poruke, izdavanje naredbi, ugovora, prenosa govora i drugih poverljivih dokumenata. PKI je rešenje koje najviše obećava, zato je to osnova za obezbeđivanje poslovnih transakcija između kompanija. Da bi se koristila veza između korisnika i njegovog digitalnog potpisa PKI zahteva poverljivu treću stranu ili sertifikaciono telo. Uloga sertifikacionog tela je da izdaje digitalni sertifikat, elektronski ekvivalent identifikacionoj kartici, koji se sistematski koristi u svakoj transakciji.

Inače, elektronsko bankarstvo podrazumeva postojanje četiri modula: Centralnog, Internog, Korisničkog i Kontrolnog. Preduslov je da klijent poseduje računar na koji se instalira SW, potom se priključuje na izabranu elektronsku banku preko interneta, pozivnih linija i putem iznajmljenih linija. Elektronska banka je povezana sa Centralnim modulom. Izuzetno pozitivan efekat, odnosno značajne prednosti ovog vida bankarskog poslovanja, donose istom leadersku poziciju u odvijanju platnog prometa. Međutim, nove tehnologije se velikom brzinom nameću, sa sve primamljivijim servisima, te ko želi da ostane u trci na sve zahtevnijem tržištu, mora svoje poslovanje kontinuirano unapređivati.

2.1.2. Značaj računarskih komunikacija za strateško pozicioniranje preduzeća

Veoma ubrzan razvoj poslovnih sistema, tokom poslednjih nekoliko decenija doveo je do široke upotrebe komunikacionih mreža u cilju njihovog međusobnog povezivanja. Tokom 50-ih godina računarski sistemi su koristili grupnu obradu sa diskretnim datotekama, a korisnici su nosili fizički svoju papirnu dokumentaciju do računara, na obradu. Tokom 60-ih godina računarske komunikacije preko telefonskih linija su postale pogodnije - koristili su se terminali za unošenje podataka koji će se obrađivati; komunikacija je predstavljala prenos signala (poruka) od terminala do računara i nazad do korisnika. Kasnih 60-ih i 70-ih godina, razvijeni su *online real-time* sistemi sa ciljem da se pređe sa grupne obrade na pojedinačnu obradu, transakciono usmerenu. Tada su postale neophodne računarske komunikacione mreže.

Sedamdesetih godina upravljački sistemi baza podataka su zamenili starije diskretne sisteme datoteka. Takođe, bili su razvijeni integrisani sistemi, na primer, kod on-line sistema, kad korisnik iz odeljenja nabavke unese podatak koji označava kupovinu 100 stolica, sistem može da inicira tri relacione transakcije - jedna može da ide u sistem plaćanja, druga u sistem računovodstva i treća u magazin za prijem robe.

Osamdesete godine obeležava ekspanzija primene mikro-računara. U početku, oni su služili samo za razmenu podataka između različitih miniračunara i između miniračunara i centralnih mainframe računara. Mikroračunari su se veoma brzo razvili u veoma moćne sisteme, lake za korišćenje, sa dosta jeftinog i dostupnog softvera - danas oni imaju veću snagu nego mainframe računari 70-ih godina. Kako se približavao kraj veka, najvažnija oblast vezana za računare postaje umrežavanje. Klijent/server računarstvo je dramatično promenilo način interakcije profesionalaca sa informacionim sistemima i korisnika sa računarima. Kancelarija budućnosti, koja treba da spoji kopir aparate, faksove, opremu za videokonferencije, mikroračunare i drugu opremu, postaviće značajne zahteve razvoju računarskih komunikacionih mreža. Ove mreže već imaju veliki uticaj na vođenje poslova.

2.1.3. Računarske mreže u poslovnim komunikacijama

Elektronske poslovne komunikacije možemo definisati kao prenos poslovnih informacija (podataka, a u poslednje vreme, i zvuka, video zapisa, dokumenata, slika) sa jedne na drugu tačku, preko računarskih komunikacionih mreža.

Uopšte, ove mreže su stvorene da sakupljaju podatke od udaljenih tačaka (obično terminala ili mikroračunara) i prenose ih u centralnu tačku, opremljenu jačim mikroračunarom ili mainframe računarom, ili da izvršavaju suprotan proces. Ove mreže omogućavaju efikasniju upotrebu centralnih računara i poboljšanje svakodnevne kontrole poslovanja, jer ubrzavaju tok informacija. One takođe poseduju servise za transfer poruka koji omogućavaju korisnicima da "razgovaraju" međusobno preko elektronske pošte. One nude bolju i pravovremenu razmenu poslovnih podataka između većeg broja korisnika. Ciljevi stvaranja računarskih komunikacionih mreža su:

- Smanjenje vremena, napora i troškova koji su potrebni za izvršenje različitih poslovnih zadataka;
- Čuvanje poslovnih podataka u njihovom izvoru i njihovo brzo širenje;
- Podržavanje poboljšane menadžment kontrole organizacije.

Postoje dva osnovna cilja razvoja tehnologije za komunikacije računarskim mrežama:

1. Preneti bitove što brže;
2. Preneti bitove što jeftinije.

Pošto su računarske mreže i telekomunikacije usko povezane moramo osim definisanja pojma računarskih mreža definisati i pojam telekomunikacije. U literaturi se srećemo sa brojnim definicijama ovog pojma, a ovde ćemo navesti neke: "Pod telekomunikacijama se podrazumeva daljinsko komuniciranje posredstvom elektronskih sredstava - telekomunikacionih sistema."¹ Takođe treba navesti i tvrdnju da "Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja. Glavni cilj je postao da se bez obzira na geografske distance što brže i efikasnije povežu klijenti i tokovi informacije."²

U skladu sa nevedenim citatom je i Tabela 1 koja pokazuje glavne trendove (kretanja) u poslovnim telekomunikacijama. Sto je prikazano u tabeli 1.

Trendovi u industriji	Kretanje prema komparativnim prednostima, udruživanju i alijansama i umrežavanju, ubrzano deregulacijom i rastom Interneta i World Wide Web-a
Trendovi u tehnologiji	Prema ekstenzivnoj upotrebi Interneta, digitalnim fiber-optičkim i bežičnim tehnologijama da bi se kreirala visoko-brza lokalna i globalna mreža za prenos zvuka, podataka, slika, audio i video fajlova.
Trendovi u primeni	Prema što većoj upotrebi Interneta, intranetova u preduzećima i interorganizacionim ekstranetovima u cilju bržeg i sigurnijeg e-Commerce-a i e-Business-a, saradnje među firmama, i strateškog pozicioniranja na lokalnom i globalnom tržištu

Tabela 1. Ključni trendovi u poslovnim telekomunikacijama³

¹ Balaban N., Ristić Ž., Đurković J., Trninić J.: Informacioni sistemi u menadžmentu, Beograd, 2005., str. 175

² Stankić R.: Poslovna informatika, Beograd, 2003., str. 218

³ James O'Brien: Management Information Systems - managing Information Technology in the Business Enterprise, 6th edition, McGraw Hill, 2004. str. 104

2.1.4. Primena ISDN-a u poslovnim komunikacijama

Međunarodna organizacija za standarde u oblasti telekomunikacija CCITT je 1984. godine definisala ISDN (Digitalna mreža integriranih usluga) kao mrežu koja obezbeđuje digitalnu komunikaciju od kraja do kraja uz podržavanje širokog spektra govornih i negovornih servisa kojima korisnici pristupaju preko standardnih više namenskih interfejsa. Dakle, ISDN predstavlja nadgradnju odnosno viši stepen postojeće javne komutirane telefonske mreže i u sebi sublimira dva značenja:

1. sistem digitalnih komunikacionih linija,
2. međunarodni mrežni standard.

Objasnićemo suštinu ISDN u oba značenja. ISDN (*Integrated Services Digital Network*) tehnologija se zasniva na prenosu podataka kroz bakarne provodnike, tako što se propisuje vrsta signala koji se prenose. Korišćenjem ISDN tehnologije mogu se povezati svi računari, u privatnim kućama i u institucijama, tako da se transfer podataka obavlja digitalnim prenosom podataka kroz bakarne provodnike. Vodeće kompanije u SAD-u koje koriste (iznajmljuju) ISDN linije su *U.S. West, Ameritech, Bell South, Southwestern Bell* idr.

Prema zahtevima ISDN tehnologije potrebno je uspostaviti potpunu digitalizaciju telefonskih mreža na određenom regionu, da bi se izvršilo konvertovanje analognih signala (koji se još uvek koriste u telefonskim komunikacijama) u digitalne signale. Analogne petlje, koje se nalaze na krajevima telefonskih veza (lokalne petlje), generatori su šuma koji se stvara u procesu telefoniranja; digitalizacijom signala i korišćenjem digitalnih petlji izbegava se nastanak šuma, a potrebna jačina signala se ostvaruje pojačavanjem signala na usputnim stanicama.

Upotreba lokalnih digitalnih petlji zahteva korišćenje digitalnih telefonskih adaptera kojima se analogni signal pretvara u digitalni. Ovakav sistem podrazumeva i lokalno napajanje, uz digitalni telefonski aparat, jer ukoliko nije instaliran alternativni izvor energije u slučaju nestanka struje dolazi do prestanka rada telefona. U poređenju sa modemskom komunikacijom, ISDN tehnologija omogućava znatno brži transfer podataka (48 kilobita u sekundi za komunikaciju sa upotrebom klasičnog modema, a 140 kilobita u sekundi sa ISDN-modemom).

Pomenimo i jednu malu ali svima vama poznatu prednost digitalnih linija. Naime, pored prednosti u pogledu većeg propusnog obima, ISDN pruža mogućnost da se pre uspostavljanja komunikacije sa drugim korisnikom, prikaže telefonski broj korisnika koji želi da uspostavi komunikaciju (ovaj broj se pokazuje na LCD displeju koji se ugrađuje na ISDN telefonske aparate).



Ilustracija 1: Primer ISDN na jednom računarskom sistemu

ISDN predstavlja i digitalni međunarodni mrežni standard za transmisiju: glasa, pokreta i/ili video zapisa preko telefonskih linija, odnosno javnih mreža. Korisnici u preko 160 zemalja putem ISDN-a imaju pristup značajnom setu višenamenskih korisničkih interfejsa.

U svakom servisu su sjedinjene sledeće osobine:

- kompletna konekcija glasa, podataka i video zapisa bilo gde u svetu,
- kompletna digitalna povezanost sa drugim digitalnim uređajima,
- simultana upotreba glasa, video zapisa i digitalnih uređajima,
- potpuna sloboda spajanja uređaja i ljudi bez ponovnog uvezivanja žicom struktura ili specijalnih kablova i sa jednim fizičkim standardom,
- korisnički kontrolisano definisanje, video, digitalnih i data linija. Npr. linija za digitalni personalni servis može biti korišćena jedan sat, zatim se naredni sat ista telefonska linija može ponovo konfigurisati u 800-vatnu liniju, a naredni sat linija može biti redefinisana u linijskog provodnika video slika s video konferencijske sesije.

Prema tipu razlikujemo sledeće servise:

- noseći (*bearer*) servisi (prenos multimedijalne informacije u realnom vremenu),
- teleservisi (prenos i obrada svih tekstualnih, audio i video informacija),
- dopunski (*supplementary*) servisi (dodatne usluge - za svaki tip teleservisa).

Očigledno je da ISDN obezbeđuje funkcionalnu mrežu za prenos (i obradu) digitalnih informacija, bez obzira na izvor ili destinaciju, sa izuzetno velikom perspektivom daljeg razvoja

2.1.5. Komunikacioni protokoli

Protokol predstavlja skup pravila odnosno procedura po kojima se ostvaruje prenos podataka i paketa u mrežnom okruženju. Svaki protokol sadrži specifikaciju:

1. formata podataka koji se razmenjuju,
2. proceduru transfera,
3. kontrolu transfera podataka.

Područje	Standard ili referentni model	Opis
Umrežavanje	OSI, TCP/IP, SNA	Komunikacije između kompjutera
Digitalna javna priključna mreža transmisija	ISDN	Transmisija glasova, videa i podataka preko javne telefonske linije
Fibrozna optička transmisija	FDDI	100 Mbps transmisija podataka preko dualnog fibrozno optičkog prstena
Elektronska pošta	X.400	Dopušta e-mail operativnim sistemima koji rade na različitim hardverima
Uključeni paket	X.25	Dopušta različitim međunarodnim i nacionalnim mrežama da komuniciraju
EDI	X.12 Edifact (Europe)	Standardizirano transakciono formatiranje
Grafički korisnički interfejs	X Windows	Grafički opis višeg nivoa za standardizirani Window menadžment
Operativni sistem	UNIX / Windows	Softver prenosiv na različite hardver platforme

Ilustracija 2. Međunarodni standardi⁴

Sve funkcije protokola raspoređene su po tzv. slojevima koji odgovaraju hijerarhijskom karakteru komuniciranja kao višeslojnog procesa. Treba imati u vidu da komunikacija može trajati vrlo kratko (upit-odgovor) ili vrlo dugo (prenos datoteka), o čemu vodi računa poseban vremenski brojač ("tajmer") protokola koji se uključuje istovremeno sa slanjem poruke i isključuje nakon potvrde prijema poruke.

Razvoj komunikacionih protokola je, razumljivo, pratio razvoj hardvera i softvera u mrežnom okruženju. U tom smislu 70 i 80-te godine prošlog veka obeležile su lokalne LAN mreže relativno zatvorenog tipa koje su onda i pratili protokoli tzv. mrežnog nivoa:

- *Ethernet*
- *Token ring*
- *ATM (Asynchronous Transfer Mod)*
- *FDDI (Fiber Distributed Data Interchange)*

Već 90-tih godina takva zatvorena LAN okruženja ustupaju mesto tzv. otvorenim sistemima koji su savremena platforma na koju se mogu priključiti svi standardni računari. Inicijative korisnika u ovom pravcu uobličio je i ozvaničio tada IEEE (*Institute of Electrical*

⁴ Krsmanović S.: "Informacioni sistemi u mrežnom okruženju", Univerzitet "Braća Karić", Beograd, 2003., str.138

and Electronics Engineers) serijom međunarodnih standarda. Za to je danas nadležna međunarodna organizacija za standardizaciju (ISO), a što je rezultiralo protokolima za otvorene -WAN arhitekture, kao protokolima višeg nivoa:

- SNA (*System Network Architecture*)
- TCP/IP (*Transmission Control Protocol/Internet Protocol*).

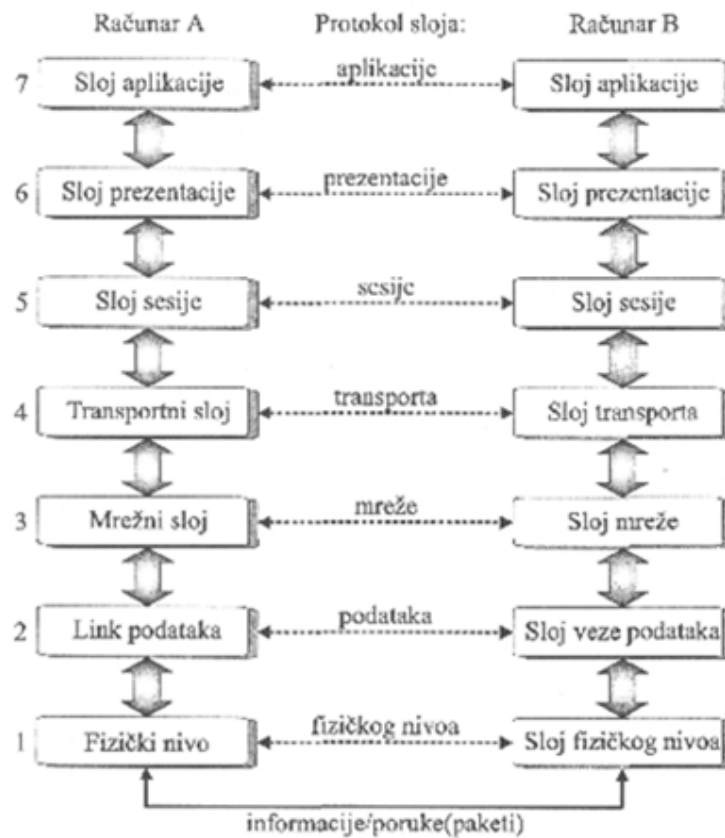
SNA protokol je prvi telekomunikacioni protokol razvijen od strane IBM-a još 70-80-tih godina koji je mogao podržati komunikaciju između inteligentnih terminala i računara, transfer fajlova, on-line procesiranje itd. SNA mreže mogle su (kasnije) prenositi i određene video signale, ali je njihova konceptijska orijentacija na mreže velikih i minikompjutera vremenom postala prevaziđena.

TCP/IP protokol je pokrenut i razvija se u SAD (od strane Ministarstva odbrane SAD) sa ciljem da univerzalno poveže različite kompjuterske sisteme. Njegov razvoj se produžava sa razvojem Interneta i što je još važnije i po konceptu i po svojoj četvoroslojnoj arhitekturi vrlo je sličan, a danas čak i kompatibilan sa OSI modelom. U okviru ovog protokola postoje posebne IP adrese koje jedinstveno, na svetskom nivou, određuju mrežni priključak bilo kog računara.

ISO/OSI protokol je danas referentni međunarodni model pa ćemo ga zato izložiti detaljnije. Definisan je pomoću sedam diskretnih slojeva na način koji je prikazan na Slici 3.2. Problem komuniciranja se hijerarhijski razlaže na manje zaokružene celine. Svaki niži sloj, obavljajući svoju funkciju, prenosi rezultat svoje usluge višim slojevima preko posebne dodirne površine, odnosno interfejsa koji postoje između svih slojeva. Osnovne funkcije pojedinih slojeva u ISO/OSI protokolu su:

1. Sloj fizičke veze je najniži nivo OSI protokola i bavi se fizičkim prenosom signala koji su bitni za uspostavljanje veze između dva računara. Specifičan: napon, fizički obim, brzinu modulacije i slično.
2. Sloj veze podataka je sloj zadužen za odgovarajuće pakovanje podataka, proveru eventualnih grešaka i njihov transfer u obliku paketa podataka na označenu adresu.
3. Mrežni sloj obezbeđuje fizičko usmeravanje podataka (ruta) kroz mrežu, proveravajući njenu topologiju i optimalni put u datom trenutku.
4. Transportni sloj uspostavlja i upravlja transportom podataka kroz mrežu i obezbeđuje sigurnu predaju poruke računaru primaocu.
5. Sloj sesije identifikuje korisnika i njegova prava pristupa kao i aplikaciju koja prima podatke - paket. Koordinira komunikaciju između u različitim aplikacija i obaveštava o eventualnim greškama.
6. Prezentacioni sloj ima za cilj da otkloni razlike u predavljanju podataka između različitih računara ili arhitektura. Ako je potrebno, vrši i konverziju kodova da bi prenešeni program, slika, glas i sl. bili razumljivi primaocu.

7. Aplikativni sloj je završni tj. nivo korisnikove aplikacije. To je, dakle, deo protokola koji se javlja kao interfejs između korisnika i njegovog računara i obezbeđuje interpretaciju podataka u formatu koji zahteva aplikacija⁵.



Ilustracija 3: ISO/OSI referentni model

2.1.6. Značaj informacione tehnologije za razvoj poslovnih komunikacija

Krajnje korisnike nema smisla pitati o opravdanosti investicija u informacione tehnologije, pošto oni objektivno nisu u stanju da sagledaju kreativne i inovativne mogućnosti koje nova tehnologija pruža. Ključno pitanje koje određuje (ne)uspeh svake tehnologije je imaginacija menadžment tima. Jedan broj poslovnih ljudi koji su zaduženi da donose ključne odluke nije u stanju da razume nove trendove zbog toga što se suština onoga što oni znaju o poslovanju u svetu uspešnih više ne primenjuje (a niko se nije potrudio da ih dovoljno ubedljivo obavesti o tome). Nasuprot popularnom mišljenju, e-poslovanje nije sinonim za e-trgovinu. Termin e-trgovina

⁵ Krsmanović S.: "Informacioni sistemi u mrežnom okruženju", Univerzitet "Braća Karić", Beograd, 2003., str.140

se fokusira isključivo na poslovne transakcije -kupovinu i prodaju proizvoda i usluga, korišćenjem mrežnih tehnologija da bi se ove transakcije izvele brže, bolje i jeftinije. S druge strane e-poslovanje - sa ili bez prefiksa "e" - podrazumeva mnogo više od jednostavne kupovine i prodaje. Zbog toga, e-trgovina nije u stanju da pruži celovitu sliku, iako je nesporno da je to važan aspekt e-poslovanja. Njen deo slike pokazuje kako novac prelazi iz ruke u ruku. E-poslovanje je pojmovno mnogo šire i sem fokusiranja samo na transakciju ono potencira korišćenje Mreže u kombinaciji sa ostalim mrežnim tehnologijama i formama elektronske komunikacije sa ciljem da omogući bilo koji oblik poslovanja.

Zbog toga su termini B2C (poslovanje – sa - korisnicima) i B2B (poslovanje - sa poslovanjem) koji se odnose na e-trgovinu takođe ograničeni u svojim definicijama pošto se fokusiraju samo na brže, bolje i po mogućnosti jeftinije obavljanje poslovnih transakcija. Uspešno poslovanje podrazumeva mnogo više od transakcije - ono komunicira, sarađuje, uči, stvara, inovira, planira, vrbuje nove poklonike... Sve su to važni poslovni procesi koji itekako mogu da profitiraju od primene tehnologija e-poslovanja.

Takođe treba znati da i na Mreži vladaju određena pravila ponašanja i ophođenja, koja, ako preduzeće želi poslovati kao ozbiljan privredni subjekt, mora poštovati. "Oko bontona na Mreži, ili kako se popularno kaže *Netiquete*, vlada veoma podeljeno mišljenje. Ne toliko oko njene primene na svim sistemima, jer se podrazumeva da vlasnici privatnih sistema mogu da nametnu svoja pravila, ali se ogorčeno vode rasprave oko pravila komuniciranja na Internetu, koji je po mnogima jedini medijum van nečije kontrole i cenzure."

⁶

2.1.7. Uloga tehnologije u formiranju mrežnog okruženja

U zadnjoj deceniji PC tehnologija je toliko napredovala da su se top modeli po snazi izjednačili sa miniračunarima. U oblasti RISC mikroprocesora su ih i prevazišli približavajući se superračunarima. Istovremeno, na polju računarskih komunikacija, došlo je do pojave novih protokola sa velikom propusnom moći po relativno niskoj ceni (xDSL, ISDN, T1/E1). Lokalne mreže prelaze na brzine 100 Mbs. Ovaj trend razvoja hardvera je omogućio da skoro sve aplikacije pređu na grafičko okruženje. Velika procesorska snaga i ogroman kapacitet memorija i diskova su omogućili prelazak na novi operativni sistem Microsoft-a: Windows NT. NT server je doneo snagu i pouzdanost VMS-a na PC platformu sjedinjujući je sa lakoćom instalacije i održavanja koju pruža grafičko okruženje. Masovno korišćenje računara u prethodnoj deceniji dovelo je do nagomilavanja ogromne količine informacija i dokumenata koji su zapisani, u po pravilu, različitim formatima korišćenjem različitih programskih paketa. *Middleware* komponente kao što je ODBC (*Open DataBase Connectivity*) omogućuju da se ovi problemi u dobroj meri prevaziđu omogućavajući međupovezivanje klijentskih aplikacija bez potrebe da se menja baza podataka ili postojeće aplikacije. Stekle su se i potrebe i uslovi da se sva ta ogromna količina opreme i podataka poveže

⁶ Pantić S.: Računarske komunikacije, Kompjuter biblioteka, Čačak, 1996.

u jedinstvenu celinu, kako na nivou pojedinih preduzeća tako i globalno. Januara 1995. godine zvanično je startovao WWW.

Ogroman broj računara i korisnika, kao i raznovrsnost korišćenih programa i njihovih verzija prouzrokovala je da se troškovi održavanja računara i lokalnih mreža enormno povećaju pa čak i višestruko nadmaše početnu cenu opreme i softvera. Rešavanjem ovog problema najviše se bave Oracle i SUN sa jedne i Microsoft sa druge strane svojim konceptima NC (Network Computer), odnosno NetPC. Ono što je zajedničko za obe koncepcije je:

1. udaljeno administriranje,
2. udaljena distribucija softvera
3. tretiranje svih resursa na mreži ravnopravno sa lokalnim (*network is computer*) je slogan SUN-a)

Očigledno je da se razvoj odvijao u dva pravca: usitnjavanje i povezivanje. Usitnjavanje u smislu da sve manji računari mogu da urade sve više posla, čime se eliminiše potreba za nabavkom velikih računara i povezivanje svih računara u lokalnu mrežu i međusobno povezivanje lokalnih mreža u jedinstvenu celinu. Koncepti koji su pomenuti prate taj globalni trend pokušavajući da sjedine dobre strane velikih i srednjih računara sa prednostima koje nude mikroračunari.

Model relacionih baza podataka je verovatno najznačajnije dostignuće u oblasti informacionih sistema. Dizajnirao ga je Dr. E.F. Codd 1970. godine za smeštanje, pristupanje i manipulaciju podacima na način koji je lakši i jednostavniji nego kod hijerarhijskih i mrežnih baza podataka. Hijerarhijske i mrežne baze podataka su teške za rad iz više razloga.

Fizička i logička definicija smeštaja podataka se vrši korišćenjem posebne sintakse (*cryptic definition language syntax*). Dalje, teškoće sa definisanjem podataka potiču od činjenice da se različiti tipovi internih pokazivača, numeričkih referenci ka lokacijama podataka, moraju smeštati u bazu podataka. Pokazivači se koriste za direktan pristup podacima. Za bilo kakvu izmenu u strukturi ili organizaciji podataka u bazi mora da se napiše netrivialni program koji će to da obavi.

U relacionom modelu podaci se referenciraju kao da su smešteni u dvodimenzionalnu tabelu. Aktuelno fizičko smeštanje, iako bitno za vreme potrebno za smeštanje, pristup ili promenu, nebitno je sintaksički za referenciranje. DBMS (*DataBase Managment System*) se stara o fizičkom smeštaju, a podaci se logički tretiraju kao da su u tabeli. Oslanjajući se na relacioni model IBM je sredinom sedamdesetih razvio SQL (*Structured Query Language*), jezik za rad sa relacionim bazama podataka. Rezultat ovog razvoja je DB/2 DBMS i danas jedan od najpopularnijih relacionih DBMS. Kasnije su se pojavili i drugi isporučioici sa svojim relacionim DBMS-ovima, kao što su: *Oracle, Informix, Progres, Sybase, MS SQL Server* i dr. Napisani su za sve značajnije operativne sisteme MVS, VMS, Unix i NT, dakle od mainframe računara pa do PC platformi.

Promene u oblasti programskih jezika, softverskih tehnika i razvojnih alata, nisu tema ovog rada i neće biti dalje razmatrane. Brzina kojom je unapređivana računarska tehnologija nezabeležena je i neuporediva sa bilo čime u istoriji ljudske civilizacije. Jedino što je ostvarilo brži rast su potrebe korisnika za informacijama serviranim na sve slikovitije i raznovrsnije načine. Glavni kriterijum za određivanje stepena informatizacije društva nije ni broj računara ni količina novca koji se na njih utroši, već procenat informacija potrebnih za odlučivanje do kojih se dolazi elektronskim putem. Treba konstatovati i da se razvoj informacionih sistema ne svodi na puko nabavljanje opreme i pisanje programa, već i na celokupnu organizaciju preduzeća, efikasno prikupljanje podataka i njihovu pouzdanost i tačnost kao i laku i jednostavnu dostupnost informacijama onima kojima su potrebne i njihovo predstavljanje u pogodnom obliku.

2.1.8. Internet i intranet

Internet je kolekcija mreža, uključujući *Arpanet*, *NSFnet*, regionalne mreže, lokalne mreže, univerzitetske mreže, koje su međusobno povezane u skladu sa skupom protokola i servisa nazvanih "*Internet protocol suite*". Veoma često se ovaj skup skraćeno naziva TCP/IP protokol, što je pogrešno jer su TCP i IP posebni protokoli, a na Internet-u se koriste i drugi protokoli kao što su UDP i ICMP. Zbog široke prihvaćenosti naziva, TCP/IP će se koristiti kao sinonim za sve internet protokole i servise. Među najznačajnijim servisima su *ftp*, *telnet*, *gopher*, *finger*, *remote login*, *computer mail*, *network file systems*, *remote printing*, *remote execution*, *name servers*, *terminal servers* i dr. Do nedavno se tehnologija koja je omogućila širenje fenomena Interneta, primenjivala uglavnom na globalnom nivou. Međutim, težište primene se sve više pomera ka lokalnim mrežama koje koriste prednosti TCP/IP protokola da bi se delile informacije i resursi unutar izolovanog sistema. Ovakve mreže su poznate pod nazivom intranet i veruje se da će u sledećih nekoliko godina razvoj i primena intraneta u velikoj meri zaseniti globalni Internet. "Razvoj mreže računara unutar jedne organizacije naziva se Intranet."⁷

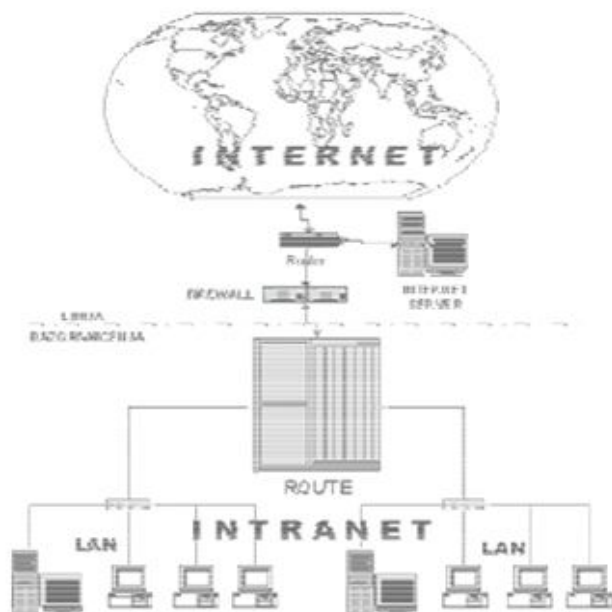
Intranet i internet mogu da se povežu preko firewall-a čija je uloga da sa Interneta selektivno propušta (filtrira) samo bezbedni saobraćaj kao i da mapira privatne IP adrese sa intraneta na javne koje se koriste na Internetu (slika 10.1). Ispred firewall-a može da se postavi internet server kome može da se slobodno pristupi preko nekog od Internet servisa. Osnovna razlika između Interneta i intraneta je između javnosti i privatnosti. Da bi bio siguran, intranet obično ima veći propusni opseg, pouzdaniji skup korisnika (koji su se, potpisujući ugovor o zasnivanju radnog odnosa, obavezali na čuvanje poslovnih tajni), čvršće mere bezbednosti i strože definisana prava pristupa podacima.

Preduzeće može da koristi Web kao jednostavan i efektan način da zaposlenima omogući pristup podacima kao što su: interni telefonski imenik, rasporedi dežurstava, cenovnik restorana i letovališta, plan godišnjih odmora, plan stručnog usavršavanja i obuke kadrova, interna akta i sl. Da li bi ovakve informacije trebalo da budu javno dostupne? Svakako ne. U ovakvim slučajevima jasno je da je prednost na strani intraneta. Neki podaci na intranetu mogu

⁷ Balaban N., Ristić Ž., Đurković J., Trninić J.: Informacioni sistemi u menadžmentu, Beograd, 2005., str. 309

da budu dostupni samo užem krugu korisnika; npr. Poslovno rukovodstvo može da ima interaktivni pristup informacijama bitnim za donošenje poslovnih odluka. Opšti podaci o preduzeću, cenovnik usluga, adrese i telefoni predstavništava, potrebe za radnom snagom i sl. su sa druge strane prirodni kandidati za Internet.

Firewall štiti intranet propuštajući samo bezbedan saobraćaj i mapira interne IP adrese u javne, dodeljene od pružaoca Internet usluga (*Internet service provider*). Lokalne mreže su međusobno povezane preko rutera korišćenjem istih protokola koji se koriste na Internetu.⁸



Ilustracija 4: Povezivanje intraneta i interneta.

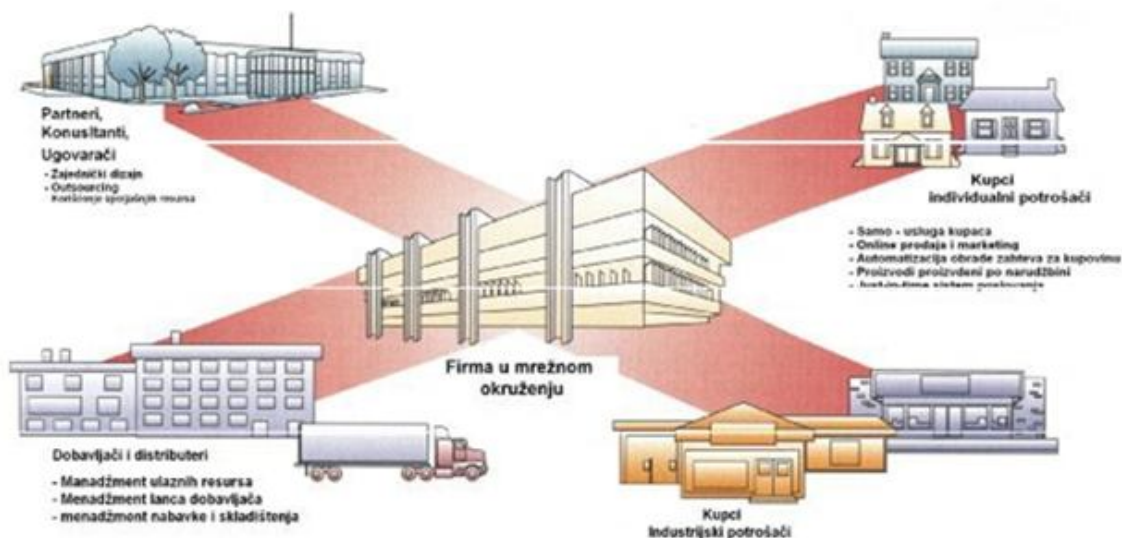
2.1.9. Ekstranet

Ekstranet je privatna mreža koja koristi Internet protokole i javne telekomunikacione sisteme za distribuciju poslovnih informacija, podataka, za rad sa dobavljačima, distributerima, proizvođačima ili kupcima. Ekstranet se može posmatrati kao spoljni deo kompanijskog intraneta ili prošireni intranet.

Ekstranet se odnosi na grupu Web sajtova koji pripadaju nezavisnim celinama i koji se kombinuju da bi informacije bile dostupne autorizovanim korisnicima. Ovo je suprotno intranetu koji je privatni sajt i kome pristupaju samo zaposleni kompanije. Ekstranet se koristi u lancu snabdevanja da bi se obezbedila delotvornija komunikacija duž lanca snabdevanja. Ekstranet zamenjuje posebne, nestandardne privatne mreže firme koje su značajno skuplje za postavljanje i

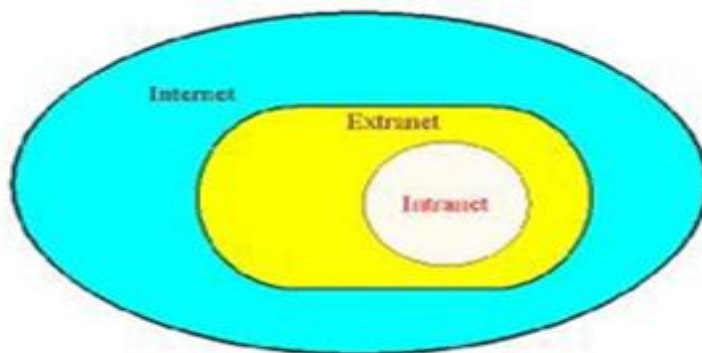
⁸ www.znanje.org

održavanje. U širem smislu, ekstranet se može opisati kao stanje poslovne svesti u kome se Internet prepoznaje kao način poslovanja sa ostalim kompanijama, paralelno sa procesom prodaje preko Interneta krajnjem kupcu. Ekstranet spaja firmu u mrežnom okruženju sa kupcima- Individualnim potrošačima, kupcima industrijskim potrošačima, dobavljačima i svim drugim poslovnim partnerima. Jedan takav odnos firme u mrežnom okruženju sa poslovnim partnerima je predstavljen na slici 4.



Ilustracija 5: Poslovanje firme u mrežnom okruženju

Ekstranet se može pojmovno odrediti i kao mehanizam utemeljen na Internet i Web tehnologijama za saobraćanje i privatno i selektivno sa mušterijama i poslovnim saradnicima.



Ilustracija 6: Hijerarhijski položaj extraneta

Ekstranet zahteva sigurnost i privatnost, obezbedjuje se primjenom firewall servera, kontrolisanog Web objavljivanja, upotreba digitalnih sertifikata ili sličnih sredstava za verifikaciju identiteta korisnika (*user authentication*), šifrovanje poruka i korišćenje virtuelnih

privatnih mreža (VPN), koje šifruju podatke IPsec zaštitnim protokolom i tuneliranjem kroz javne mreže.

Kompanije mogu koristiti ekstranet za sledeće:

1. Razmena velikih količina podataka upotrebom standarda *Electronic Data Interchange* (EDI)
2. Stavljanje na uvid kataloga velikoprodaji i ljudima iz biznisa robne razmene
3. Saradnja sa drugim kompanijama i ulaganje združenih napora u razvojnim projektima
4. Združeni razvoj i upotreba programa obuke sa drugim kompanijama
5. Obezbeđivanje ili pristupanje uslugama, koje pruža jedna kompanija, grupi kompanija. Primer pomenutih usluga je *online banking* aplikacije kojima rukovodi jedna kompanija po dogovoru s (afiliranim) bankama
6. Stavljanje na uvid novosti koje su od interesa sa partnerske kompanije
7. Bitna odlika ekstraneta je skalabilnost - ekstranet se može jednostavno uvećavati i po obimu i po funkciji, a time se racionalizuje početna investicija (mala ulaganja u prvoj fazi implementacije) i opreznije ulazi u obimnije projekte (razvoj korak-po-korak kroz male kontrolabilne implementacione faze).

Inicijativa za IT kompatibilnost:

Netscape, Oracle i Sun Microsystems su objavili alijanse koje treba da osiguraju da njihovi proizvodi za ekstranet rade u saglasnosti. Predlažu se standardi za *JavaScript i Common Object Request Broker Architecture* (CORBA). Microsoft podržava *Point-to-Point Tunneling Protocol* (PPTP) i radi sa *American Express* i drugim kompanijama na standardu *Open Buying on the Internet* (OBI). *Lotus Corporation* promoviše svoj proizvod za rad mrežnih grupa, *Notes*, koji se takođe može primeniti za ekstranet.

2.2. Internet bankarstvo

Internet bankarstvo se definiše kao sistem za direktnu upotrebu bankarskih usluga od kuće. Omogućava neposredan transfer sredstava, informacija i naloga putem informacijsko-komunikacijske mreže, dakle bez pisanja pratećih dokumenata. Cilj ovih sistema je približiti uslugu klijentima i omogućiti im komunikaciju s bankom ili drugom finansijskom institucijom od kuće, bez dodatnih napora u smislu odlaska na šalter banke, te bez posredne komunikacije.

Često se pravi pogreška pri izjednačavanju pojmova internet bankarstva i on-line bankarstva, oba pojma označavaju obavljanje bankarskih transakcija iz kuće, i asortiman bankarskih usluga im je gotovo identičan, kao i sistemi zaštite, međutim, razlike među njima znatno su veće. Osim usluga internet bankarstva i on-line bankarstva koje pružaju banke, u poslednjih nekoliko godina sve prisutnija je web trgovina (internet trgovina), kao i portala za obavljanje novčanih transakcija. U svim ovim načinima plaćanja preko interneta neophodan faktor je sigurnost i poverljivost podataka.

2.2.1. On-line bankarstvo

On-line bankarstvo predstavlja obavljanje bankarskih transakcija direktnom vezom klijenta i banke uz pomoć specijalnog programa. Potreban je poseban program instaliran na klijentovom računalu s kojega se jedino i mogu obavljati transakcije i na kojem će se nalaziti podaci o izvršenim promjenama. Pri obavljanju bankarskih transakcija u on-line bankarstvu potreban je poseban program (*Microsoft Money, Manage Your Money...*) koji se instalira na računar klijenta. Klijent je ograničen na obavljanje transakcija s tog računala, klijent posluje s dvije strane: s bankom i programerskom tvrtkom koja instalira i održava program. Pri obavljanju bankarskih transakcija u on-line bankarstvu klijentovi podaci o bankarskim transakcijama ostaju na čvrstom disku i nisu otporni na eventualne napade iz okruženja (mogućnost pljačke, ubacivanje kompjuterskih virusa...). Potreban je novac za kupovinu programa, potrebno je vrijeme za instalaciju programa, kao i vrijeme za savladavanje programa.

Usluge koje su 24 sata dnevno dostupne su pristup stanju na tekućem računu i kreditnim karticama, plaćanje računa, planirano i zakazano plaćanje za određeni termin koje će se izvršiti automatski, prijenos novca s računa na račun i usluge vođenja financija, za što je potreban dodatni program.

Nedostaci on-line bankarstva su ograničenja za obavljanje transakcija sa samo onog računala na kojem je instaliran skup program, potrebno vrijeme za obuku za rad, kao i nezaštićenost podataka na čvrstom disku korisnika na napade iz okruženja. Iz tih svih razloga veliki broj korisnika prebacio se na internet bankarstvo.

2.2.2. Internet bankarstvo banaka

Internet bankarstvo ili web bankarstvo predstavlja obavljanje bankarskog poslovanja direktno iz kuće, posredovanjem interneta. Pri obavljanju bankarskih transakcija u internet bankarstvu nije potreban poseban program i ne postoje podaci spremljeni na klijentovom čvrstom disku, pa je veća sigurnost pri obavljanju transakcija. Pri obavljanju bankarskih transakcija u internet bankarstvu pristup banci i računu je moguć s bilo kojeg mesta na svetu, pod uvjetom da na tom mjestu postoji računar priključeno na internet.

Pri transakcijama u internet bankarstvu banka brine o održavanju vlastitog hardverskog i programskog sistema zaštite, moguće je i obavljanje on-line transakcija. Predviđanja su da će se ovaj vid bankarstva razvijati velikom brzinom. Internet bankarstvo je najjeftiniji oblik bankarskih usluga, dostupan 24 sata dnevno, praktično bez prostorne i vremenske ograničenosti. Glavni ograničavajući faktori, koji uslovljavaju pristanak potrošača na ovu vrstu tehnologije, su sigurnost i privatnost. S tehničke tačke gledišta, ovaj problem su neke banke već rešile, ali ostaje činjenica da je ponašanje potrošača vođeno pre potrošačkom percepcijom nego tehničkim činjenicama. Neprihvatanje da se bankarske transakcije obavljaju preko interneta postoji pre svega iz straha da ključne finansijske informacije budu otkrivene.

Jasno su vidljive razlike između internet bankarstva i on-line bankarstva. Osnovna razlika je u ugradnji specijalnih programa, koji ograničavaju korisnika na obavljanje usluga isključivo sa računarom na koji je instaliran odgovarajući program. Razlike su i u stupnju sigurnosti pri obavljanju transakcija, zatim u novcu potrebnom za kupovinu i instalaciju programa i vremenu potrebnom za obuku korisnika. Spomenuti razlozi jasno ukazuju da je internet bankarstvo praktičniji, ekonomičniji i jednostavniji način obavljanja bankarskog poslovanja direktno iz kuće.

2.2.3. Razvoj internet bankarstva

Brže, sigurnije, lakše i jednostavnije poslovanje na internetu, ciljevi su koje pred banke i druge financijske institucije postavlja sve zahtevnije financijsko tržište. Da bi se ovi ciljevi ispunili, u svetu se drastično povećava obim ulaganja u informacijske tehnologije. Uporedno s razvojem i poboljšanjem usluga banaka na internetu ide i razvoj web trgovina te portala za posredovanje novcem.

2.2.4. Vrste i načini primene internet bankarstva

Internet bankarstvo spada u širu grupu transakcija "direktnim kanalima", zajedno s telefonskim bankarstvom, korišćenjem bankomata i ostalim načinima obavljanja finansijskih usluga bez dolaska u poslovnicu. Ponuda svih banaka koje su uvele ovu uslugu i za građane i za kompanije zaista je široka i prilično ujednačena. Osetljivo područje na kojem klijenti osećte razlike su kvaliteta pruženih usluga i individualna briga za korisnika, što bankari nazivaju "*customer care*".

2.2.5. Osnovi pojmovi u primeni Internet bankarstva

Smart Card "pametna kartica" je plastična kartica veličine kreditne kartice s ugrađenim čipom na koju su pohranjena dva jedinstvena "ključa", od kojih je jedan javni, a drugi tajni. Javni ključ prenosi se u posebnoj formi, nazvanoj digitalni certifikat, koji sadrži osnovne podatke o korisniku. Privatnim ključem korisnik potpisuje svaku zadanu transakciju. Za upotrebu ove kartice potreban je čitač koji se priključi na računar. Prije početka rada kartica se umeće u čitač i unosi se PIN (*Personal Identification Number*), čime počinje proces identifikacije. Mogućnost primene pametne kartice višestruka je; osim u kartičnom poslovanju, sve se masovnije upotrebljavaju i u javnom životu, kao osobne ili zdravstvene legitimacije te različite članske kartice.

Čitač kartice je uređaj koji omogućava pristup pametnoj kartici; priključuje se na računar i služi za čitanje podataka s čip kartice, na sličan način kao što CD ROM jedinica služi za čitanje CD-ova. Čitač kartice priključuje se na jedan od ulaza na računaru, zavisno od toga koji je slobodan - serijski ulaz ili USB (*Universal Serial Bus*) ulaz.

Token je osobnom lozinkom (PIN-om) zaštićen uređaj koji korisnicima jamči da nije moguć neovlašćen pristup njihovim računima. Pri svakom uključanju generira jednokratnu lozinku OTP

(*One Time Password*). Kod se za pristup usluzi upotrebljava token, nije potrebno instalirati dodatnu programsku podršku, jer se klijenti služe postojećim aplikacijama na svome računaru.

PIN je lični identifikacijski broj odnosno šifra pomoću koje se osigurava zaštita od neovlaštenog korištenja smart kartice ili tokena. Poznat je samo korisniku koji ga jedini može i menjati.

TAN (*Transaction Athorization Number*) kartica je identifikacijska kartica veličine kreditne kartice, na čijoj je poleđini serijski broj i tablica s transakcijskim brojevima (TAN-ovima). Pri svakoj prijavi s tablice se upisuje drugi broj, a sistem na prijavnom ekranu precizira na kojem je mestu broj u tablici.

Elektronski potpis je skup podataka koji potvrđuje izvornost, autentičnost i neporecivost slanja i primanja dokumenata u elektronskom poslovanju, a ima potpuno jednaku vrednost kao vlastoručni potpis u pravnom okruženju.

PKI (Public Key Infrastructure) autentifikacija je tehnologija "javnog ključa", odnosi se za osiguranje podataka na putu između računara, klijenta i servera elektroničkog bankarstva upotrebom enkripcije pri aktiviranju smart kartice. U javnom životu certifikat bi predstavljao ekvivalent ličnoj karti i u tom smislu u komunikaciji preko interneta osigurava međusobnu identifikaciju strana koje komuniciraju. *User ID* (korisnički ID) jedinstveni je broj korisnika usluge, koji su se dodeljuje kod ugovaranja usluge. U kombinaciji s PIN-om služi za registraciju korisnika.

2.2.6. Internet protokol IPV6

Internt Protokol verzije 4 je stvoren početkom 70-ih godina u okviru projekta ARPANET, i razvijen zarad komunikacije Američke Vojske i Univerziteta. Kroz mnogobrojne izmene, i tehnička poboljšanja, IPv4 je danas osnov globalne mreže – Internet. IPv4 se nalazi i u mnogim rešenjima koja nisu vezana samo za Internet. Današnja rasprostranjenost upotrebe IPv4 se nije mogla predvideti u godinama kada je projektovan. Pojavljuju se nove upotrebe Internet Protokola u mobilnoj telefoniji, pejdžing sistemima, ručnim i prenosivim računarima. Usložnjavaju se postojeći problemi usmeravanja saobraćaja (*routing*).

Povećava se potreba za adresnim prostorom kojeg je sve manje. Radio i video emitovanja imaju potrebu za garantovanim kvalitetom usluge protoka podataka (QoS). Postoji potreba za kriptovanjem sadržaja na IP nivou (IPSec). Neke od navedenih potreba će imati i upotrebe Interneta koje se tek naziru, primera radi to su:

- upravljanje kućnim uređajima,
- kontrola napajanja.

Da bi se produžila upotreba IPv4, i rešili stečeni problemi, preduzimale su se razne mere. Prelazi se na CIDR (*Classless Inter Domain Routing*) zarad povećanja iskorišćenosti IPv4 adresnog prostora. Usložnjava se procedura zauzimanja novih Internet adresa. Sve je veća upotreba privatnih mreža koje su vezane kroz proxy na Internet. Sve češće se koristi NAT (*Network*

Address Translation), koji smanjuje zauzeće IPv4 adresnog prostora, ali ima i ozbiljne nedostatke. Vremenom je IPv4 dobio razne mogućnosti koje su mu nedostajale ali je nemoguće istovremeno koristiti više njih, primera radi *IPSec*, *QoS* i *MobileIP*.

Postojeće mere kojima se štedi Internet prostor, mogu da produže životni vek, ali ne mogu da pruže rešenja za nove potrebe i već postojeće probleme. Umesto da razne industrije i kompanije razviju svoja rešenja koja bi pružila potrebne mogućnosti ali bila ograničena na mala tržišta i neusaglašena sa IPv4, traženo je zajedničko rešenje. Od ranih devedesetih godina postoji dokumentovana potreba za Internet Protokolom nove generacije.

Kroz desetine dokumenata IETF-ovih (*Internet Engineering Task Force*) radnih grupa među, kojima su bitniji rfc-1380, rfc-1543, rfc-1550, rfc-1710⁹ uobličen je današnji izgled Internet Protokola nove generacije. Problem iscrpljivanja adresa IPv4 je prepoznat u ranim devedesetim, kada su razni eksperti pravili projekcije pokazujući da ako se nastavi povećanja tražnja za IPv4 adresa, celokupni adresni prostor će biti potrošen za samo par narednih godina. Nova IP verzija, u razvojnoj fazi poznatija pod imenom *IP Next Generation*, pod imenom IPv6 je bilo predloženo rešenje. Ali se isto tako znalo da će razvoj novog standarda potrajati, i da je potrebno kratkoročno rešenje kako bi se sprečilo potpuno iscrpljivanje adresa tipa IPv4 do pojave novog tipa adresa.

To kratkoročno rešenje je bilo Network Address Translation (NAT), koje omogućuje da više hostova dele jednu ili par javnih IP adresa. Iza NAT uređaja, koriste se privatne IP adrese. NAT je bio toliko uspešan u usporavanju iscrpljivanja IPv4 adresa i postao toliko standardni deo većine mreža, da do ovog dana mnogi dovode u pitanje potrebu za novom IP verzijom. Ali široko korišćenje NAT-a je promenio otvoreni, transparentni, peer-to-peer Internet u nešto što više liči na veliki skup klijent-server mreža. Korisnici se vide kao da su povezani iza "ivice" Interneta, a servisi protiču do njih. Retko da korisnici doprinose celokupnom bogatstvu Interneta.

Gledano sa ekonomske perspektive, Internet korisnici su postali samo potrošači, a ne proizvođači. Iako je IPv6 standard završen pre nekoliko godina, tek nedavno se pojavio ozbiljniji interes za prelazak sa IPv4 na IPv6. Postoje dva osnovna razloga za ovaj čin. Prvi je vizija aplikacija koje koriste koncepte kao što je mobilni IP, garantovanje kvaliteta usluge, *end-to-end* bezbednost i sl. Drugi razlog je ubrzana modernizacija vrlo naseljenih zemalja, kao što su Indija i Kina.

IPv6 menja 32-bitne IPv4 adrese sa 128-bitnim adresama, čime imamo na raspolaganju 340 trilion trilion triliona IP adresa. Ovaj broj bi zadovoljio zahteve za javnim IP adresama i odgovorio na potrebe pomenuta dva razloga, bar u za nas vidljivoj budućnosti. IPv6 adrese se ne razlikuju od IPv4 adresa samo po dužini. "Stenografija" za njihovo pisanje je drugačija, imaju značajno drugačiji format, a i njihova funkcionalna organizacija je drugačija.

⁹ Internet Engineering Task Force / RFC dokumenti http://www.ietf.org/iesg/1rfc_index.txt

2.2.7. Predstavljanje adresa u IPV6

Već nam je poznato da su 32-bitne IPv4 adrese predstavljene odvajanjem na četiri 8-bitna segmenta i pisanjem svakog od ovih segmenata decimalno između 0 i 255, odvajajući ih tačkama. 128-bitne IPv6 adrese se predstavljaju odvajanjem na osam 16-bitnih segmenata. Svaki segment se piše heksadecimalno između 0x0000 i 0xFFFF, odvojenih dvotačkama. Primer pisanja IPv6 adrese¹⁰:

3ffe:1944:0100:000a:0000:00bc:2500:0d0b

Pamćenje više od nekoliko takvih adresa je praktično nemoguće, a ni njihovo pisanje nije ništa mnogo zabavnije. Na sreću, postoje dva pravila u smanjenju veličine pisanih IPv6 adresa. Prvo pravilo je

- Početne nule u bilo kom 16-bitnom segmentu ne moraju biti pisane; ako bilo koji 16-bitni segment ima manje od četiri heksadecimalna broja, pretpostavlja se da su nedostajući brojevi početne nule.

U primeru prethodne adrese, treći, četvrti, peti, šesti i osmi segment ima početne nule. Upotrebom pravila kompresije adrese, adresa može biti napisana kao:

3ffe:1944:100:a:0:bc:2500:d0b

Primećujemo da se mogu izostaviti samo početne nule; ostale nule ne mogu, jer bi na taj način segmenti bili nejasni, jer ne bi mogli reći da li se nedostajuće nule nalaze pre ili posle napisanih brojeva. U primeru adrese, peti segment ima sve nule, a napisan je samo sa jednom. Mnoge IPv6 adrese imaju duge stringove nula u sebi. Uzmimo za primer ovu adresu:

ff02:0000:0000:0000:0000:0000:0000:0005

Ova adresa se može smanjiti na:

ff02:0:0:0:0:0:0:5

Ipak, korišćenjem drugog pravila ova adresa se može još više smanjiti:

- Bilo koji susedni string jednog ili više 16-bitnih segmenata koji u sebi ima sve nule se može predstaviti dvostrukom dvotačkom.
-

Koristeći ovo pravilo, prethodna adresa se može predstaviti ovako:

ff02::5

¹⁰ S. Deering, R. Hinden, RFC 1883: Internet Protocol, Version 6 (IPv6) Specification, December 1995.

Pogodnost pisanja ovakve adrese je očigledna. Ali primetimo da pravilo kaže da samo jedan susedni string segmenata sa svim nulama može biti predstavljen sa dvostrukom dvotačkom. Korišćenjem dvostruke dvotačke više od jedanput u IPv6 adresi može stvoriti pometnju. Uzmimo, na primer, sledeću adresu:

2001:0d02:0000:0000:0014:0000:0000:0095

Bilo koja od sledećih redukcija adrese je tačna jer koriste dvostruku dvotačku samo jednom:

2001:d02::14:0:0:95

Ali sledeća redukcija nije validna jer koristi dvostruku dvotačku dva puta:

2001:d02::14::95

Nije validna jer je dužina dva stringa sa svim nulama dvosmislena; može predstavljati bilo koju od sledećih IPv6 adresa:

2001:0d02:0000:0000:0014:0000:0000:0095

2001:0d02:0000:0000:0000:0014:0000:0095

2001:0d02:0000:0014:0000:0000:0000:0095

Za razliku od IPv4, u kome je prefiks mrežnog dela adrese identifikovan decimalama sa tačkama ili heksadecimalnom maskom adrese ili *bitcountom*, IPv6 prefiksi se uvek identifikuju *bitcountom*. Tj., posle adrese se kuca “/” i decimalni broj koji indicira koliko je prvih bitova adrese prefiks bitovi. Na primer, prefiks sledeće adrese su prva 64 bita:

3ffe:1944:100:a::bc:2500:d0b/64

Kada se upisuju samo IPv6 prefiksi, postavljaju se svi host bitovi na 0 na isti način kao i sa IPv4 adrese. Na primer,

3ffe:1944:100:a::/64

IPv6 adresa koja se sastoji od svih nula se može napisati samo sa dvostrukom dvotačkom. Postoje dva slučaja gde se koriste adrese sa svim nulama. Prva je podrazumevana adresa, gde je adresa sa svim nulama a dužina prefiksa je nula:

::/0

Druga IPv6 adresa sa svim nulama je nespecificirana adresa, koja se koristi u nekim procedurama *Neighbor Discovery Protocol* - a. Neodređena adresa je dodatak, indicirajući odsustvo prave IPv6 adrese. Kada se piše takva adresa, razlikuje se od podrazumevane adrese po dužini prefiksa:

::/128

2.2.8. IPv6 tipovi adresa

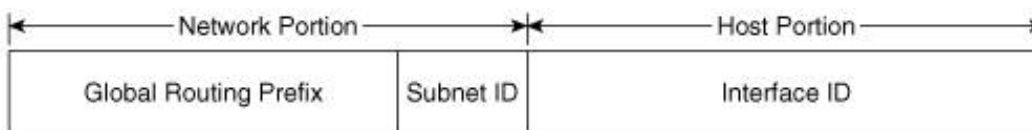
Postoje tri tipa IPv6 adresa:

- *Unicast*,
- *Anycast*,
- *Multicast*.

Za razliku od IPv4, ne postoji IPv6 *broadcast* adresa. Ipak, postoji "*all nodes*" *multicast* adresa, koja prvenstveno služi za istu svrhu kao i *broadcast* adresa.

Globalne unicast adrese:

Unicast adresa je adresa koja identifikuje jedan uređaj. Globalna *unicast* adresa je adresa koja je globalno jedinstvena. Opšti format IPv6 unicast adrese je prikazana na slici 5. Ovaj format je zastareo i uprošćava raniji format koji je podelio IPv6 unicast adresu u *Top level Aggregator* (TLA), *Next-Level Aggregator* (NLA) i druga polja.



Ilustracija 7: Opšti format IPv6 unicast adrese

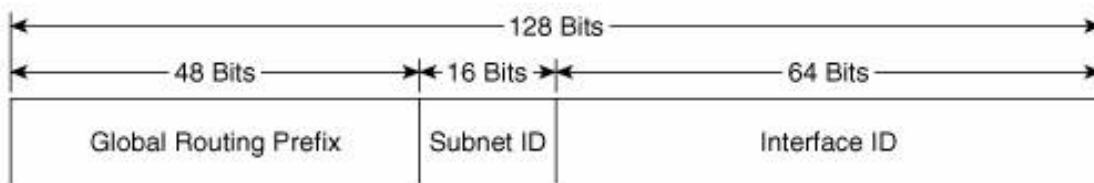
Host deo adrese se naziva *Interface ID*. Razlog za ovo ime leži u tome da host može imati više od jednog IPv6 interfejsa, pa tako adresa ispravnije identifikuje interfejs na hostu nego host sam sebe. Ali ta veština ne ide mnogo daleko: Jedan interfejs može imati više IPv6 adresa, i može imati dodatnu IPv4 adresu, u kom slučaju je Interface ID samo jedan id nekoliko identifikatora interfejsa.

Možda je najveća razlika između IPv4 i IPv6 adresa, osim dužine, lokacija *Subnet* (podrežnog) identifikatora kao deo mrežnog dela adrese, a ne host dela. Nasledstvo od arhitekture IPv4 adrese je da se *subnet* deo IPv4 adrese uzima od host dela adrese. Kao rezultat, host deo IPv4 adrese varira ne samo po svojoj klasi, već i brojem bitova koji se koriste za subnet identifikaciju.

Prva vidljiva korist ugrađivanja IPv6 Subnet ID polja u mrežni deo adrese je taj da Interface ID može biti iste veličine za sve IPv6 adrese, uprošćavajući rasčlanjivanje adrese. Pravljenjem Subnet ID kao mrežnog dela pravi jasno razlikovanje funkcija: Mrežni deo daje lokaciju uređaja do specifičnog linka podataka, a host deo daje identitet uređaja na linku podataka.

Interface ID globalne IPv6 adrese je, sa vrlo malo izuzetaka, dužine 64 bita. Takođe sa vrlo malo izuzetaka, polje Subnet ID je dužine 16 bita. 16-bitno Subnet ID polje daje prostor za 65536

odvojenih *subnetova*; čini se da je korišćenje fiksne Subnet ID veličine kao ova, kada u većini slučajeva kapacitet neće biti ni blizu popunjen, nepotrebno. Ali sa datom celokupnom veličinom IPv6 adresnog prostora, i sa datim prednostima lake dodele adrese, dizajna, upravljanja i rasčlanjivanja koje proizilazi iz korišćenja fiksne veličine, ova veličina je opravdana.



Ilustracija 8: Standardna veličina polja globalne unicast IPv6 adrese

2.2.9. Identifikovanje IPv6 tipova adresa

Prvih par bitova adrese određuju tip adrese. Na primer, prva tri bita svih trenutnih globalnih unicast adresa je 001. Kao rezultat, prepoznavanje heksadecimalnog predstavljanja globalne unicast adrese je lako: Svi počinju sa 2 ili 3, u zavisnosti od vrednosti četvrtog bita u prefiksu globalnog rutiranja. Tako, na primer, trenutno alocirani prefiksi koji se koriste u 6Bone (javna IPv6 istraživačka mreža) počinje sa 3ffe, a IPv6 adrese koje su trenutno alocirane od strane RIR-a počinju sa 2001.

Za binarni broj 001 u globalnim <i>unicast</i> adresama se očekuje da bude dovoljno za neko buduće vreme; par drugih kombinacija bitova se dodeljuju drugim definisanim tipovima adresa. U tabeli 3. su prikazane trenutno alocirane kombinacije vodećih bitova. TIP adrese	<i>High-Order Bitovi</i> (binarno)	<i>High-Order Bitovi</i> (Hex)
<i>Unspecified</i>	00...0	::/128
<i>Loopback</i>	00...1	::1/128
<i>Multicast</i>	11111111	FF00::/8
<i>Link-Local Unicast</i>	1111111010	FE80::/10
<i>Site-Local Unicast</i> (Deprecated)	1111111011	FFC0::/10
<i>Global Unicast</i> (Trenutno alocirani)	001	2xxx::/4 or 3xxx::/4

Za binarni broj 001 u globalnim <i>unicast</i> adresama se očekuje da bude dovoljno za neko buduće vreme; par drugih kombinacija bitova se dodeljuju drugim definisanim tipovima adresa. U tabeli 3. su prikazane trenutno alocirane kombinacije vodećih bitova. TIP adrese	<i>High-Order Bitovi</i> (binarno)	High-Order Bitovi (Hex)
<i>Reserved</i> (Buduće global unicast alokacije)	Sve ostalo	

Ilustracija 9. Bitovi visokog reda IPv6 tIPa adrese

Zaglavlje internet protokola IPv6 je u odnosu na zaglavlje IPv4 protokola dosta pojednostavljeno. Naime, od njega zadržava samo 3 polja (verzija, izvorišna adresa i odredišna adresa) i uvodi dodatnih 5 polja

bit 0-3	4-11	12-15	16-23	24-31
Verzija	Tip prometa	Oznaka toka		
Dužina podatka		Sledeće zaglavlje	Ograničenje skoka	
Izvorišna internet adresa (128 bita)				
Odredišna internet adresa (128 bita)				
Podatak (TCP segment ili UDP datagram)				

Ilustracija 10. Verzija internet protokola, vrednost je 6.

- Tip prometa (DS/ECN) (8 bita): Ovo polje se odnosilo na polje *Traffic Class* i bilo je rezervisano za upotrebu od strane početnih čvorova i/ili prosleđujućih rutera da bi se identifikovalo i razlikovalo između različitih klasa prioriteta IPv6 paketa. Prvih šest bita polja Klasa Saobraćaja sada se odnose na polje DS (*differentiated services*), a ostalih 2 bita su rezervisana za polje ECN (*explicit congestion notification*).
- Oznaka toka (20 bita): Može biti korišćeno od strane hosta da obeleži one pakete sa kojima ruteri treba da posebno postupaju u okviru mreže.
- Dužina podataka (16 bita): Dužina ostatka IPv6 paketa koji prati zaglavlje, u oktetima. Drugim rečima, ovo je kompletna dužina svih produženih zaglavlja plus dužina PDU-a transportnog nivoa.
- Sledeće zaglavlje (8 bita): Identifikuje tip zaglavlja koje prati IPv6 zaglavlje. Ovo može biti i IPv6 produženo zaglavlje ili zaglavlje višeg sloja, kao što je TCP ili UDP.
- Ograničenje skoka (8 bita): Preostali broj dozvoljenih skokova za ovaj paket. Ograničenje skokova je postavljeno na željenu maksimalnu veličinu od strane izvorišta i dekrementira se od strane svake tačke koja prosleđuje paket. Paket se odbacuje kada vrednost ovog polja postane nula. Ovo je pojednostavljen postupak u odnosu na postupak koji treba da se obavi sa poljem dužine života kod IPv4. Saglasnost je bila da dodatni napor u obračunu vremenskih intervala u IPv4 nije doneo nikakvu značajnu vrednost protokolu. U stvari, IPv4 ruteri, kao glavno pravilo, tretirali su TTL polje kao polje ograničenja skoka.
- Izvorišna adresa (128 bita): Adresa pošiljaoca paketa (uređaja predajne strane).
- Odredišna adresa (128 bita): Adresa određenog primaoca paketa. Ovo ne mora, u suštini, da bude krajnja odredišna adresa ako je prisutno zaglavlje rutiranja.

IPv6 protokol obezbeđuje tri metode za konfiguraciju:

- *Stateless Auto-Configuration;*
- *Stateful Auto-Configuration;*
- *Manual Configuration.*

Auto-konfiguracija i rekonfiguracija koje se ovde spominju omogućuju laku modifikaciju mrežne arhitekture. Npr., auto-konfiguracija obezbeđuje hostu u mreži generisanje jedinstvene adrese za sopstvenu upotrebu na osnovu mrežne topologije i ostalih uređaja u mreži. Proces auto-konfiguracije uključuje formiranje lokalne link-adrese, verifikaciju njene jedinstvenosti na linku i utvrđivanja koje informacije trebaju biti auto-konfigurisane.¹¹

Za dobijanje određenih parametara klijent (host) šalje odgovarajuću *Request* poruku serveru direktnim ili indirektnim putem. Naime, klijent formira adresu lokalnog linka koju koristi za kreiranje adresnog interfejsa i dobijanje dodatnih parametara za konfiguraciju. Nakon toga server šalje odgovor u vidu *Reply* poruke koja sadrži zahtijevane parametre, s tim da ova poruka može

¹¹ Convergence Technologies for 3G Networks, Second edition by Jeffrey Banister, Paul Mather and Sebastian Coope, John Wiley & Sons, Ltd, 2004.

sadržavati i status informaciju koja opisuje te parametre.¹² *Manual Configuration* je tehnika koja je zavisna od implementacije i ovde neće biti razmatrana.¹³

To je tehnika koja se koristi kada se ne zahtijeva manuelna (engl. Manual) konfiguracija, kako hostova tako i servera. Ona se koristi kada određeni sajt nema jasno definisane adrese hostova i to sve dok su te adrese jedinstvene i rutabilne. Osnovna prednost ove tehnike je u tome što mali sajtovi koji se sastoje od nekoliko mašina spojenih na jedan link, ne zahtijevaju postojanje odgovarajućeg adresnog servera za konfiguraciju. Takođe, isti slučaj je i sa velikim sajtovima koji se sastoje od nekoliko mreža.

U ovom slučaju IPv6 čvor samostalno kreira IPv6 adresu za vlastitu upotrebu ne zahtijevajući manuelno konfigurisan adresni server. Pored toga *Stateless* auto-konfiguracija omogućuje čvorovima konfiguraciju sopstvenih adresa koje su rutabilne. Pri tome je neophodno da ovi čvorovi komuniciraju sa lokalnim IPv6 ruterima. Naime, čvor kombinuje adresu od 48 ili 64 bita sa mrežnim prefiksom koji dobija od lokalnog rutera. Zahvaljujući prednostima ove tehnike može se smanjiti cijena koja se ulaže za mrežnu podršku tako što se ne mora vršiti manuelna konfiguracija neke radne stanice prije njene upotrebe.¹⁴

Situacija u današnjim mrežama je takva da uz male administrativne cijene, kao i malu cijenu mrežnih interfejsa, mogu biti kreirane nove tržišne mogućnosti za kontrolu i nadgledanje instaliranih kompjuterskih sistema. Ova činjenica postaje važna ako se ima u vidu da mreže u pojedinim dijelovima grada predstavljaju bitan dio tržišta. IPv4 često koristi DHCP protokol da smanji napore za manuelno dodijeljivanje adresa krajnjim čvorovima. DHCP sadrži statičke tabele pomoću kojih vrši dodijeljivanje adresa novim čvorovima u vezi. *Stateful* auto-konfiguracija je definisana tako da svaki host sadrži konfiguraciju adresnog interfejsa i parametre dobijene od servera. Kod ove tehnike host generiše identifikator interfejsa koji vrši identifikaciju interfejsa u podmreži. Ovakva konfiguracija se koristi kada sajt zahtijeva strožiju kontrolu nad dodijeljenim adresama. Radi predostrožnosti zahtijeva se testiranje jedinstvenosti adrese prije njene upotrebe. Kombinacijom lokalnih informacija i onih dobijenih od rutera (npr. prefiks za identifikaciju podmreže združene sa linkom) formira se adresa koja se dodijeljuje hostu.¹⁵

Postupak auto-konfiguracije omogućava niz prednosti korisnicima mreže na svim nivoima. Tako npr., prilikom nove dodjele adresa zbog određenih poboljšanja u mreži, ovaj postupak će omogućiti dodjelu novih prefiksa hostovima bez zahtijevanja manuelne rekonfiguracije radnih

¹² Is IPv6 Finally Gaining Ground ?, George Lawton, Industry Trends, August 2001.

¹³ A Scenario-Based Review of IPv6 Transition Tools, Michael Mackay, Christopher Edwards, Martin Dunmore, Tim Chown and Graca Carvalho, IEEE Internet Computing, May-June 2003.

¹⁴ Convergence Technologies for 3G Networks, Second edition by Jeffrey Banister, Paul Mather and Sebastian Coope, John Wiley & Sons, Ltd, 2004.

¹⁵ IPv6 Transition Tools, Michael Mackay, Christopher Edwards, Martin Dunmore, Tim Chown and Graca Carvalho, IEEE Internet Computing, May-June 2003.

stanica. Takođe ova tehnika omogućuje dodjelu novih adresa mobilnim uređajima bez obzira na njihovu lokaciju, odnosno mesta gde su povezani na mrežu.¹⁶

2.2.10. Sigurnost

Sigurnost je složeno i veoma važno pitanje transporta podataka na Internetu. U novim mrežama prenoše se veoma osjetljivi podaci (npr. kreditne kartice) koji su namijenjeni samo krajnjim (dodijeljenim) korisnicima. Tehnika koja se koristi u funkcije sigurnosti zavisi od operativnog sistema, različitih procedura i kompjuterskih algoritama. IPv6 protokol koristi IPsec paket sigurnosti. Taj paket se koristi kao standardna funkcija u IPv6 verziji, a ne kao opciona za stari protokol. Ideja ovog koncepta se sastoji u tome da krajnji sistemi podrže osnovne nivoe sigurnosti koji odgovaraju IPsec arhitekturi. Cilj ovakve realizacije je taj da definisanjem operacija sigurnosti na IP sloju budu obezbijeđene iste za sve IP aplikacije, uključujući i one koje ne podliježu zaštiti. IPsec servisi su realizovani na bazi mehanizama koji se nazivaju *security associations* (SA).

Ovi mehanizmi su jedinstveno određeni sljedećim elementima:

- SPI indeks (engl. *Security Parameter Index*) koji može biti pridružen algoritmima za enkripciju i autentifikaciju;
- odredišnom IP adresom;
- identifikatorom upotrijebljenog protokola.

Korišćenje IPsec paketa sigurnosti podrazumijeva upotrebu AH (engl. *Authentication Header*) i ESP (engl. *Encapsulating Security Payload*) protokola.

AH protokol obezbjeđuje integritet podataka, autentifikaciju izvorišne adrese i zaštitu od ponavljanja. Takođe, on omogućava autentifikaciju na višim slojevima, kao i autentifikaciju nekih polja IP zaglavlja. Ovaj protokol može biti korišten samostalno i u kombinaciji sa ESP protokolom.

ESP protokol se koristi za realizaciju pouzdane konekcije upotrebom enkripcije. Pored toga koristi se i za potrebe autentifikacije. Ove funkcije su opcione i jedna od njih mora biti izabrana.

Određeni problemi se javljaju pri korišćenju IPsec operacija u kombinaciji sa prelaznim rešenjima na novi protokol. Naime, problem je u tome što prilikom translacije paketi mogu ostati bez autentifikacije usled korištenja prevodilaca i releja. U ovakvim situacijama IPsec operacije ne mogu biti upotrebljene s kraja na kraj nekog sistema. Ovaj problem se može rešiti korišćenjem višestrukog broja IPsec sekcija između krajnjih sistema i prevodilaca, odnosno releja, omogućujući tako kraj-kraj (engl. *end-to-end*) operaciju sigurnosti. Kao posledicu

¹⁶ Perkins, Charles E., "Dynamic Host Configuration Protocol for IPv6", Internet Engineering Task Force, May 5, 2000.

ovakvog rešenja imamo dodatno procesiranje na prevodiocima i relejima, te odgovarajuće upravljanje šiframa.¹⁷

Inkapsulacijom IPv6 paketa unutar IPsec operacije, kao i dodatnom inkapsulacijom unutar IPv4 paketa znatno se povećava veličina paketa, što za posledicu ima degradiranje performansi. Kao alternativa za ove i druge probleme može se koristiti hijerarhijsko tuneliranje unutar prelaznih rešenja kada je sigurnost neophodna.

2.2.11. Podrška mobilnim sistemima

Jedan od nedostataka IPv4 protokola je smanjena mogućnost upravljanja u mobilnim komunikacijama. Naime, IPv4 ne može lako obezbediti sledeće funkcije:

- dodeljivanje novih adresa prilikom promene mreže od strane mobilnih stanica;
- laku autentifikaciju koju zahteva rutirajuća infrastruktura prilikom promene lokacije mobilnog korisnika;
- utvrđivanje istovetnosti mreža pri promeni istih;
- obaveštavanje sagovornika o promeni lokacije (mreže).

Ovi nedostaci mogu lako biti prevaziđeni upotrebom nove (IPv6) verzije protokola. IPv6 protokol koristi 128 bita za adresiranje hostova i mreža. Ovako definisan adresni prostor daleko prevazilazi današnje potrebe. Međutim, današnja tendencija razvoja mobilnih mreža je takva da svaka mobilna stanica dobije vlastitu IP adresu, što značajno povećava potrebe za raspoloživim adresnim prostorom. S druge strane, razvoj mobilnih sistema je usmeren tako da obezbedi uvođenje IP protokola u sve delove sistema (engl. *all-IP network*). Ta činjenica takođe potvrđuje potrebu za proširenim adresnim prostorom i implementacijom novih funkcija. *All-IP network* su mreže nove generacije gde se svi korisnički podaci, uključujući govor i video signal, prenose pomoću IP paketa.

2.3. Ključni protokoli za potporu internet bankarstva http (Hypertext Transfer Protocol)

HTTP (*Hypertext Transfer Protocol*) je protokol koji se koristi pri radu s *world wide web*-om. HTTP protokol je implementiran kao protokol po principu zahtev/odgovor. Klijent šalje zahtev za prijenos sa stranice web servera na njegovo računar. Web server na taj zahtev odgovara slanjem tražene stranice, protokol radi u aplikacijskom sloju. Klijent šalje zahtev HTTP serveru, HTTP server interpretira zahtev i šalje odgovarajući odgovor klijentu. Komunikacija je zapravo tipa uspostavljanja konekcije, bez zadržavanja stanja. Nakon odgovora HTTP servera na klijentov zahtev, veza se prekida sve do sledećeg zahteva. Jedini izuzetak od ovog scenarija je u slučaju kada klijent primeni HTTP metodu keep-a-live koja je podržana u verziji HTTP 1.1. U

¹⁷ Realizing the Transition to IPv6, Daniel G. Waddington and Fangzhe Chang, Bell Research Laboratories, IEEE Communications Magazine, June 2002.

ovom slučaju, klijent održava vezu svo vrijeme. Kod HTTP zahteva postoji nekoliko metoda koje se koriste:

- GET metoda
- HEAD metoda
- POST metoda
- PUT metoda
- DELETE metoda
- TRACE metoda

Metoda GET se koristi za preuzimanje informacija u HTTP zahtevu. GET dozvoljava dodatnu fleksibilnost preko upotrebe IF iskaza. Ovime se može doći do takozvanih kondicionalnih GET metoda. Ukoliko je ispunjen zahtev IF iskaza, podaci se prenose. Ovime se postiže da se spremljene kopije web stranica ažuriraju efikasnije, te se dobiva bolja iskorištenost propusnog opsega na mreži. Metoda HEAD je vrlo sličan GET metodi s tom razlikom da se tijelo poruke ne vraća klijentu. Ova metoda se koristi radi utvrđivanja da li je link još aktivan ili je izmijenjen u odnosu na prethodno stanje. Izmijenjeno stanje se testira uspoređivanjem informacija poslanih u REQUEST zaglavlju s odgovorima dobivenim u RESPONSE zaglavlju.

Metoda POST se koristi za zahtev HTTP serveru da prihvati priključene podatke kao novu »isporuku« HTTP serveru. Ova metoda se može koristiti za slanje poruka u *news* grupe, slanja HTML (*Hyper Text Markup Language*) formulara HTTP serveru ili dodatnih zapisa podataka bazi podataka koja se nalazi na HTTP serveru.

Metoda PUT se koristi za zahteve da se podaci poslani u zahtevu smjeste na izvor koji je naveden u REQUEST poruci. Ovo se razlikuje od POST metode u kojoj se može specificirati odredište za podatke. Ako podaci već postoje, smatra se da su to izmjene pojedinih podataka.

Metoda DELETE se koristi za zahtev HTTP serveru da izbriše izvor koji je naveden u REQUEST poruci. Ova metoda može biti obustavljena intervencijom korisnika ili podešavanjem određenih sigurnosnih parametara na HTTP serveru. Odgovor o uspješnosti se šalje jedino kada server ima namjeru izvršiti brisanje. Metoda TRACE se koristi radi osiguranja da su primljeni podaci od HTTP servera ispravni. TRACE odgovor je zapravo HTTP zahtev koga prima HTTP server. Ovime se omogućava testiranje i pronalaženje pogrešaka kod HTTP zahteva.

2.3.1. Autentifikacija i sigurnost HTTP protokola

Većina web servera takođe može pružiti neke osnovne sigurnosne opcije. Ovo se pokazuje u slučaju kada se korisniku neke stranice prikaže dijalog u kojem treba unijeti korisničko ime i lozinku pre odobravanja pristupa web stranici. Glavni problem s ovim vidom autentifikacije je to što se podaci za korisničko ime i lozinku prenose preko mreže u formi čistog teksta. Svako ko poseduje program za "prisluškivanje" prometa na mreži (*network sniffer*) može doći u posed ovih informacija i kasnije te podatke iskoristiti za neovlašten pristup preko tog računara. Sve web

stranice koje su osigurane sa SSL-om (*Secure Sockets Layer*) imaju HTTPS:// u svojoj URL (*Universal Resource Locator*) adresi. Ukoliko ne vidite HTTPS:// za ono za što se tvrdi da je osigurana web prezentacija, nije poželjno unositi poverljive informacije kao što je broj kreditne kartice. Takođe, potrebno je videti i neke dodatne indikatore koji ukazuju da je uspostavljena sigurna veza i kod *Netscape*-a i *Internet Explorer*-a. Kod *Netscape*-a, ključ koji se pojavljuje na dnu prozora, a kod *Internet Explorer*-a, indikacija je lokot koji se takođe pojavljuje na dnu prozora.

2.3.2. SSL (*Secure Sockets Layer*)

SSL (*Secure Sockets Layer*) je protokol za sigurno slanje poruka (komunikaciju) putem interneta, koji omogućava slanje poverljivih podataka (npr. broj kreditne kartice) putem interneta u šifriranom i sigurnom obliku. SSL protokol ostvaruje poseban komunikacijski sloj, koji je smešten na pouzdani transportni sloj. Od aplikacijskog sloja prima poruku koju treba poslati, rastavi je u manje delove prikladne za šifriranje, dodaje kontrolni broj, šifrira, eventualno kompresira, a zatim te delove pošalje. Primalac primi delove, dekompresira, dešifrira, proveriti kontrolne brojeve, sastavi delove poruke, pa ih preda aplikacijskom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mrežu. Ukoliko su klijent i server neaktivni duže vreme ili razgovor s istim atributima zaštite potraje predugo, atributi se menjaju.

SSL protokol je dizajniran i napravljen u kompaniji *Netscape Communications*, za upotrebu s *Netscape Navigator*om. Prva verzija, 1.0, je razvijena 1994. godine, međutim, to je bila samo probna verzija korištena unutar ove kompanije. Verzija 2.0 je bila prva koja je izdana u javnost i koja je isporučivala s *Netscape Navigator*om, verzijama 1 i 2. Poslije verzije SSL 2.0, Microsoft je izdao svoju verziju ovog protokola, koja je imala naziv PCT (*Private Communications Transport*). Najnovija verzija SSL 3.0, je uključila sva poboljšanja Microsoft-ovog PCT-a, i time uklonila slabosti verzije SSL 2.0. U to vreme je, IETF (*Internet Engineering Task Force*) grupa, koja je osnovana 1996. godine, napravila otvoreni standard za šifriranje zasnovan na SSL-u 3.0. Ovaj protokol je nazvan TLS (*Transport Layer Security*) verzija 1.0, i objavljen je 1999. godine na RFC (*Request For Comments*) 22461. Očekuje se da će TLS protokol biti standardiziran od strane IETF-a, i može se reći da se on razlikuje od SSL-a u nekoliko detalja. On je adaptiran od strane korisnika i projekatnata mobilnih radio uređaja, koji su prilagodili ovaj protokol bežičnim komunikacijama, i nazvali ga WTLS (*Wireless Transport Layer Security*).

2.3.3. Vrste SSL potvrda

Postoji više vrsta potvrda. Potvrde je moguće koristiti i u drugim situacijama, ne samo u okviru SSL protokola, ali njihova upotreba izlazi izvan okvira ovog rada.

- Klijentske SSL potvrde ; Koriste se za identifikaciju klijenta putem SSL protokola. Uobičajeno je poistovjećivanje identiteta klijenta s osobom. Osim za identifikaciju osoba kod pristupa serveru, klijentska potvrda se može koristiti i u druge svrhe, npr. za digitalno potpisivanje digitalnih formulara. Primjer: 1. Banka daje korisniku klijentsku SSL

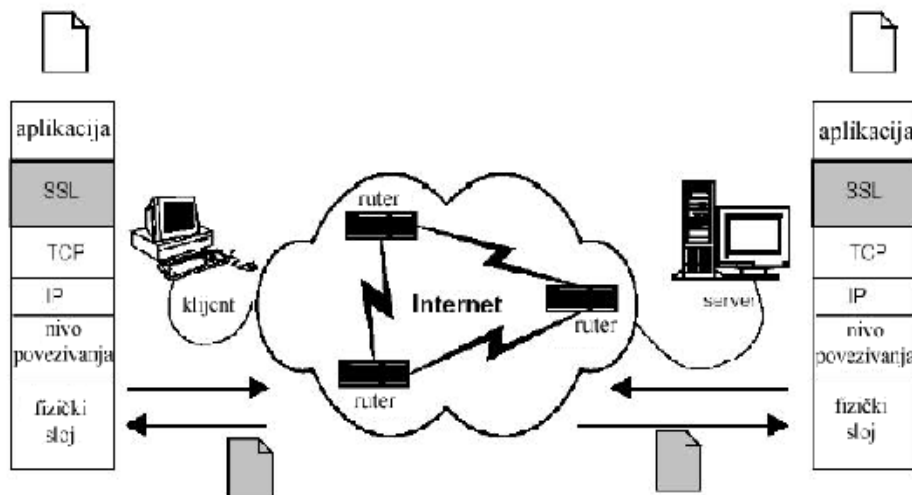
potvrdu koja omogućava serveru banke identifikaciju korisnika i dozvoljava korištenje bankovnog računa. 2. Preduzeće može dati svakom novom zaposlenom klijentsku SSL potvrdu, kojom je moguće dobiti pristup serveru poduzeća.

- Serverske SSL potvrde; Koriste se za identifikaciju servera od strane klijenta putem SSL protokola. Identifikacija servera je obavezna u SSL protokolu za ostvarivanje zaštićenog prijenosa podataka dok identifikacija klijenta nije. Primer: Internet poslovanje, npr. on-line prodavaonice, najčešće koriste identifikaciju servera preko serverskih SSL potvrda kako bi uspostavili zaštićenu SSL vezu i uverili korisnika da je to odgovarajuće preduzeće s kojim korisnik želi poslovati. Šifrirana SSL veza osigurava da osetljivi podaci koji se šalju kroz mrežu, kao što su brojevi kreditnih kartica, budu zaštićeni.

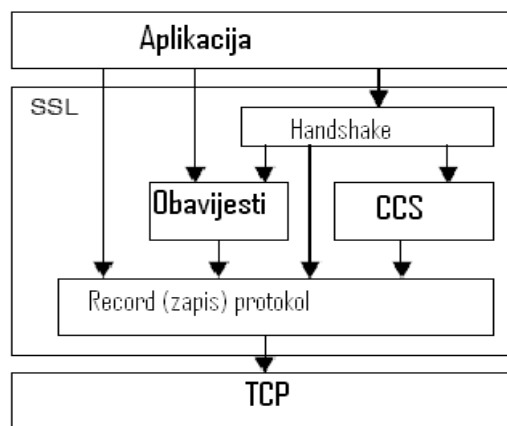
2.3.4. Opšti prikaz SSL protokola

SSL omogućava razmenu informacija između klijenta i servera, na transparentan način. Ovaj protokol nalazi se između aplikacijskog i transportnog sloja ISO/OSI (*International Standard Organization's Open System Interconnect*) referentnog modela. Koristeći ovaj pristup, moguće je identificirati SSL protokol kao dio sloja za prezentaciju. Na slici br. 8 se može videti mesto SSL-a u okviru TCP/IP protokola.

Međutim, SSL ne funkcioniše na vrhu *User Datagram* protokola, zato što ne nudi pouzdan prenos podataka, što može dovesti do gubitka IP paketa. Zbog toga, SSL ne može pružiti zaštitu za sledeće protokole: SNMP (*Simple Network Management Protocol*), NFS (*Network File System*), DNS (*Domain Name Service*) kao i za protokol VOIP (*Voice Over Internet Protocol*). SSL se sastoji od dva pod-nivoa: *SSL Record* i *SSL Handshake*, te koristi još 4 podprotokola: 1) *SSL Record*, 2) *SSL Handshake*, 3) *Change Cipher Spec*, i 4) *Alert*. *SSL Record* sloj je odgovoran za prenos blokova informacija, između dva računara. *SSL Handshake* protokol upravlja razmenom ključeva, obaveštenja i promene lozinki. Ovi nivoi se nalaze na vrhu sloja za prenos podataka, koji je obično TCP sloj. Na slici br. 9 vidi se veza između pod-protokola, kao i njihova lokacija i ostali slojevi SSL-a.



Ilustracija 11: SSL u okviru TCP/IP protokola



Ilustracija 12: Prikaz veza potprotokola

Handshake protokol je odgovoran za identifikaciju subjekata u komunikaciji, posredovanje algoritama za šifriranje i kontrolu, razmjenu PreMasterSecret, koja se koristi za generiranje identifikacijskih i šifriranih ključeva kroz *MasterSecret*. Funkcija CCS (*Change Cipher Spec*) protokola, je da obavijesti *Record (zapis) protokol* o promenama u sigurnosnim parametrima. Protokol za obaveštavanja, *Alert*, otkriva pogreške koje su se dogodile tokom proveravanja poruke, kao i svih neslaganja koje se mogu dogoditi tokom "handshake-a". Na kraju, *Record* protokol prihvata sve razmenjene sigurnosne parametre između dva subjekta, koja su se spojila zahtevajući sigurnost, i štiti podatke koji dolaze iz aplikacijskog sloja, kao i poruke iz nekog od ostala tri pod-protokola. Bitno je reći da SSL razlikuje vezu (eng. *connection*) i razgovor (eng. *session*). Veza je usluga koja se koristi za prenos, dok je razgovor niz veza s istim šifriranim parametrima koji se razmenjuju tokom "handshake-a". Razgovor (eng. *session*) može sadržavati više veza (eng. *connections*). Identifikacija se utvrđuje za svaki od razgovora, a sledeći parametri

ostaju nepromenjeni tokom razgovora: 1. redni broj razgovora (ID), 2. potvrda, 3. algoritam za kompresiju, 4. algoritmi za šifriranje i potpis, i 5. *MasterSecret* koji se razmenjuje između klijenta i servera. Za svaku novu vezu u razgovoru, *handshake* postavlja sledeće parametre: dva slučajna broja, jedan za klijenta a drugi za server, parametre *hashing* algoritma na klijentskoj strani i serverskoj strani, blok šifriranih ključeva za klijenta i servera, inicijalni vektor za blok šifriranja na obje strane. Niz brojeva je specifičan za svaku vezu, i on se inicijalizira poslije poruke *Change Cipher Spec*. Kad god se klijent spoji na server, novi razgovor je pokrenut. Ako se isti klijent spoji na drugi server, novi razgovor će biti pokrenut bez prekida prethodnog. Ako se klijent kasnije vrati na prvi server, i poželi sačuvati izabrane sigurnosne parametre koji su već napravljeni, klijent će zatražiti od servera da nastavi stari razgovor umesto pokretanja novog. SSL dokumentacija sugerise da se dužina razgovora limitira na 24 sata, ali stvarna dužina razgovora je obično određena na serveru. Record protokol koristi parametre tokom procesa povezivanja da bi ih prosledio transportnom sloju. U biti, ovaj protokol je odgovoran za deljenje podataka na blokove i njihovo slanje na strani pošiljaoca, kao i za deljenje na strani primaoca. Druge funkcije uključuju kompresiju, kao i šifriranje i dešifriranje poruka.

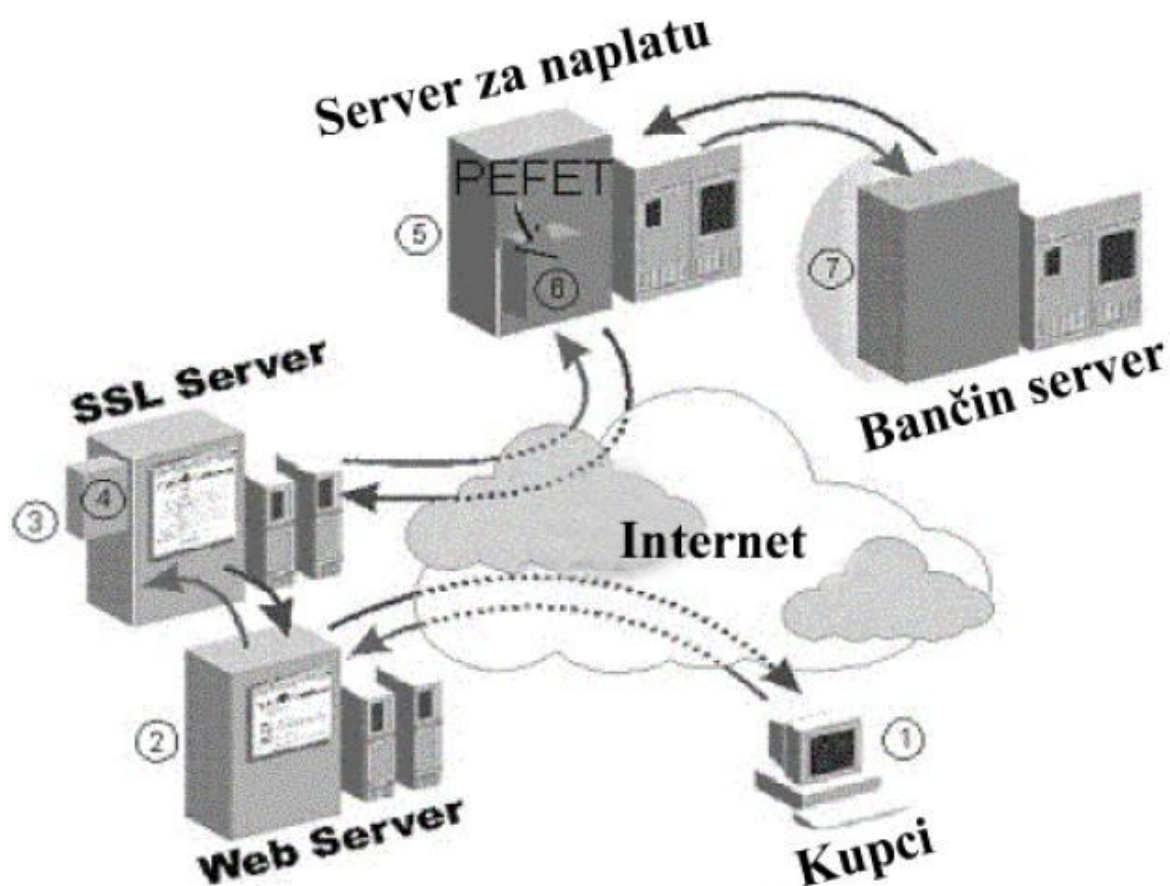
2.3.5. Slabosti i ranjivosti SSL protokola

Rast i popularnost SSL aplikacija upućuje na opasnost od otkrivanja i iskorištavanja sigurnosnih "rupa" u protokolu, koji bi mogli ugroziti sigurnost podataka koji se štite. Popularnost interneta, i njegovih korisnika je u porastu svaki dan, i broj korisnika koji koriste elektronske transakcije raste isto tako. SSL je vrlo jeftin za implementaciju, i razvijen je kao brza opcija za potrebe sigurnosti u web aplikacijama, koje rade sa poverljivim podacima. To objašnjava više implementacija ovog protokola na internetu. Međutim, kao i svaki drugim sistem, SSL nije u potpunosti siguran. SSL je dizajniran da osigura sledeće; poverljivost, integritet i proveru identiteta. Deo koji se odnosi na poverljivost je takav, da zlonamerna osoba može presresti osetljive informacije, u trenutku dok se šalju, ali se ti podaci ne mogu dešifrirati. Deo sa proverom identiteta je dizajniran da oseti mogući napad nazvan "čovek u sredini", gde su poverljivi podaci preusmereni od strane zlonamerne osobe. Servis za proveru identiteta je dobro implementiran kroz potvrde, iako može postati žrtva napada.

2.3.6 On-line plaćanje kreditnim karticama

Rast interneta i world wide web-a je uticao na sve veću komercijalizaciju prodaje roba i usluga putem mreže. Danas, kreditne kartice predstavljaju osnovno sredstvo plaćanja za on-line kupovinu. Oko 90% on-line kupovina je učinjeno putem kreditne kartice. Na većini stranica koje omogućavaju elektronsku trgovinu, za korisnike je najjednostavnije kupiti neki proizvod samo time što će uneti broj kreditne kartice i dan isteka kartice. Ali postavlja se pitanje koliko je siguran prenos takvih informacija do internet stranice e-trgovca. Postoje dva osnovna sigurnosna protokola za zaštitu on-line plaćanja; Već spomenuti SSL (*Secure Sockets Layer*) i SET (*Secure Electronics Transaction*).

SSL šalje šifrirane podatke direktno između korisnika i internet stranice na kojem se proizvod (usluga) kupuje. Najnovije verzije poznatih web preglednika, uključujući *Netscape Communicator 7.1*, omogućavaju korisnicima šifrirani prenos podataka u 128 - bitnom SSL razgovoru. Kada kupac poželi kupiti nešto na internetu od prodavača koristeći SSL vezu, takav proces se može podeliti u dva koraka. U prvom koraku, dvije strane uspostavljaju razgovor, a u drugom koraku se razmjenjuju informacije između klijenta i servera kroz SSL vezu. Tada klijent popunjava karticu za kupovinu i bira opciju za plaćanje. Općenito, ovaj klijent mora unijeti neke bitne osobne informacije, kao što su broj kreditne kartice, dan isteka kartice, ime, i adresu. Sve te informacije unijete na serveru se šifriraju ponovo u SSL serveru, pa se onda šalje zahtev za naplatu kroz internet. Na kraju se od banke traži provjera identiteta. SSL server dobiva ili dozvolu ili odbijanje za transakciju kroz server za plaćanje, i šalje rezultate kupcu i prodavaču. Sigurnost ovakvog načina plaćanja se može vidjeti na slici br. 10



Ilustracija 13. Prikaz plaćanja ON LINE kreditnim karticama

1. Kupac;
2. Server za e-poslovanje;
3. SSL server koji sadrži stranicu sa uplatom;
4. Administrativni alati koje koristi prodavac;
5. Server za naplatu (plaćanja);
6. Podsistem za prevare;
7. Bančin server.

Ovakve transakcije moraju se izvršiti na siguran način, tako da informacije o plaćanju ne mogu biti izmijenjene tokom prijenosa. Međutim, korisnik želi biti siguran da su informacije o njegovoj kreditnoj kartici sigurne. Prodavač želi biti siguran da će plaćanje biti obavljeno bez ometanja. Koristeći SSL vezu, pružena je odgovarajuća sigurnost za zaštitu od ovakvih rizika, prije svega što SSL pruža šifriranje podataka, identifikaciju servera, integritet poruke, i identifikaciju klijenta preko TCP/IP protokola.

Kada se kupuje preko Interneta korišćenjem kreditne kartice potrebne su procedure za bezbjednu komunikaciju radi dokazivanja autentičnosti umješanih strana, da obezbede poverljivi prenos naružbine i informacije o plaćanju kao i da zaštiti integritet transakcije. Trenutni pristup postizanju bezbene komunikacije je da se koristi SSL protokol koji je razvila firma Netscape, a koji je trenutno najčešće korišćen metod za obavljanje sigurnih transakcija na mreži. Podržava ga većina Web servera kao i klijenata uključujući *Microsoft Internet Explorer* i *Netscape Navigator*. Transakcija korišćenjem SSL protokola uključuje sledeće aktivnosti:

- server šalje svoj digitalni sertifikat klijentu
- klijent proverava da li je sertifikat izdat od strane CA
- klijent i server razmenjuju javne ključeve
- klijent generiše tajni ključ koji se koristi samo u započetoj transakciji.
- klijent šifrue generisani tajni ključ, korišćenjem serverovog javnog ključa i šalje ga serveru.

U daljem toku transakcije server i klijent koriste isti tajni ključ metodom simetričnog kriptovanja. U verziji 2.0 SSL podržava samo proveru autentičnosti servera, dok je u novoj SSL v3.0 uključena i podrška za proveru autentičnosti klijenta. On obavlja dokazivanje autentičnosti servera i, opciono dokazivanje autentičnosti klijenta. Sa SSL-om poverljive informacije su zaštićene putem enkripcije, a i korisnik je uveren kroz dokazivanje autentičnosti servera da komunicira sa željenim web site-om, a ne sa nekim lažnim web sajtom. Pored toga SSL obezbeđuje integritet podataka, tj. zaštitu protiv bilo kog pokušaja da se izmene podaci koji se prenose tokom jedne komunikacione sesije. Glavne razmene u toku SSL sesije su prikazane na slici 11.

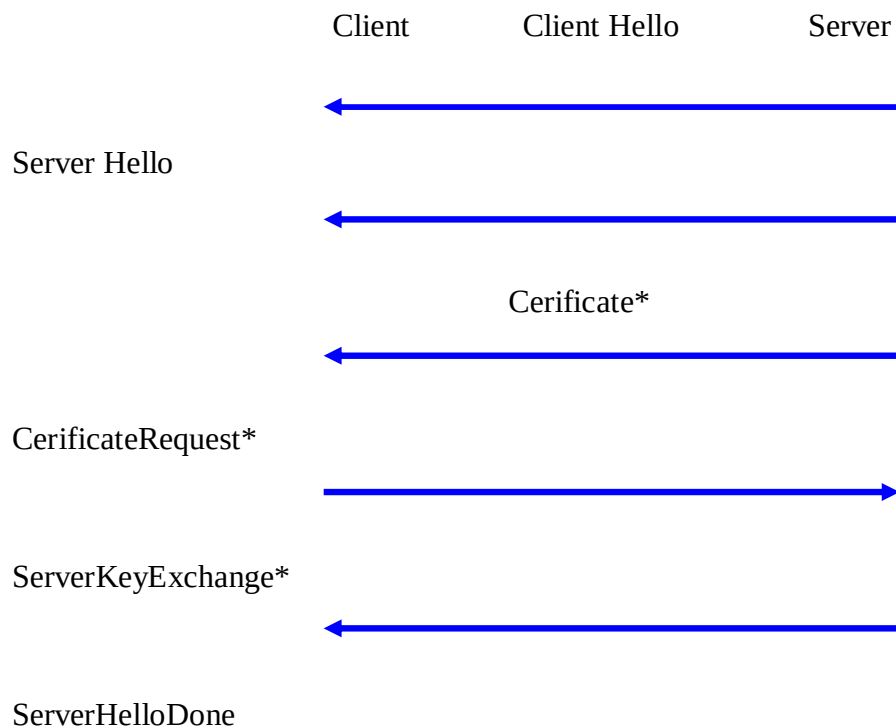
Transakcija putem kreditne kartice ima pet glavnih učesnika: kupca, prodavca, banku prodavca, izdavača i nabavljača. Prodavac ima ugovor sa svojom bankom kojim omogućuje da prihvati plaćanje kreditnom karticom putem Interneta. Izdavač je finansijska institucija, kao što je banka, koja izdaje kreditnu karticu kupcu. On je odgovoran za plaćanje duga vlasnika kartice.

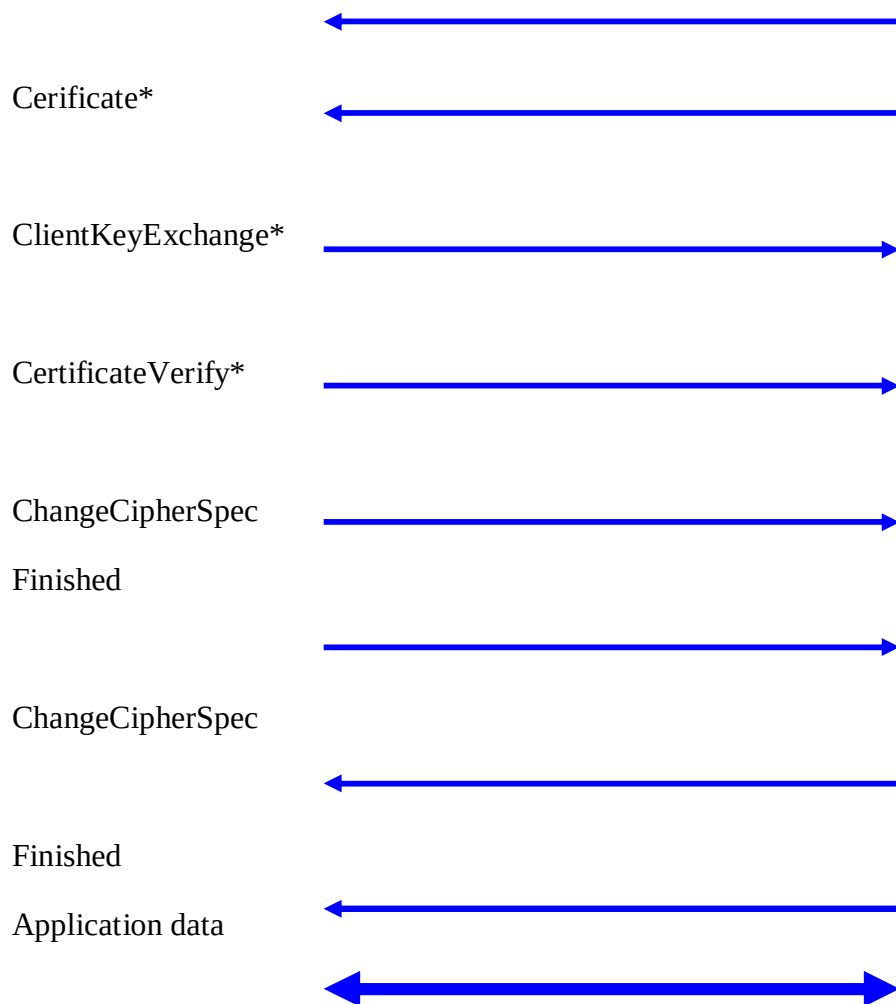
Nabavljač, sa druge strane, dobija transakcije kreditnih kartica od prodavaca i procesira ih za plaćanje. Nabavljač obezbeđuje autorizaciju prodavcu da je dati račun aktivan i da predložena kupovina ne prelazi kreditni limit vlasnika kartice. Nabavljač takođe vrši plaćanja na prodavčev račun, a onda je refundiran od strane izdavača. Banka prodavca može da funkcioniše kao nabavljač.

Da bi se uspostavila SSL sesija između SSL servera i klijenta, oni treba da se dogovore oko verzije SSL protokola koji će se koristiti, izaberu kriptografske algoritme, opcionalno potvrde autentičnost jedno drugoga i koriste tehnike enkripcije sa javnim ključevima u cilju generisanja i razmene tajnih podataka. Glavne razmene između klijenta i servera u toku uspostavljanja SSL sesije su sledeće:

ClientHello i *ServerHello* poruke: Ove dve poruke se koriste za uspostavljanje naprednih bezbednosti mogućnosti između servera i klijenta. One sadrže podatke o:

- Verziji protokola
- Identifikaciji sesije
- Listu kriptografskih opcija
- Metodu kompresije
- Slučajnom broju





Ilustracija 14. Glavne razmjene izmedju klijenata i servera

Server certificate: Server šalje svoj sertifikat, ako treba da dokaže svoju autentičnost. Format sertifikata prati standard X.509.v3

Server key exchange poruka: Ona je opcionalna. Neophodna je u nekim okolnostima, kao npr. Ako server ne poseduje sertifikat ili je njegov sertifikat samo za potpisivanje. U njoj se nalazi algoritam razmene ključeva i povezani parametri .

ServerHelloDone poruka: Ova poruka označava da je pozdravna faza uspostavljanja veze završena. Nakon slanja ove poruke, server će biti u modu čekanja za klijentov odgovor. Klijent verifikuje da je server pružio validan sertifikat ako je potrebno i proverava da li su ServerHello parametri prihvatljivi.

Client key exchange poruka: Ona ima različite formate, u zavisnosti od toga koji je algoritam javnih ključeva izabran između ClientHello i ServerHello poruka. Još jednom, slično istoj poruci servera, ona sadrži algoritam razmene ključeva i povezanih parametara.

Finished poruka: Ova poruka se uvijek šalje odmah nakon *ChangeCipherSpec* poruke da bi se potvrdilo da su razmena ključeva i proces potvrde autentičnosti obavljeni uspešno.

Sada ćemo opisati korake pri plaćanju kreditnom karticom preko Interneta. Transakcija započinje kada kupac odluči da naruči online sa prodavčevog web site-a. Prodavčeva prodajna aplikacija pita kupca za detalje plaćanja (kao što su broj kreditne kartice, identifikacioni broj vlasnika kartice i datum važnosti) pored drugih informacija kao što su adresa slanja robe. Kupac tada unosi informacije u obrazac osiguran korišćenjem SSL-a. U ovakvom obrascu, informacije o plaćanju su zaštićene dok se šalju prodavcu

Po prijemu porudžbine, prodavčev server šalje informacije o plaćanju nabavljačevom procesoru za autorizaciju, korišćenjem posvećenih i sigurnih linija. Autorizacija je zahtev da se zadrže sredstva za plaćanje. Nabavljač će potvrditi da kreditna kartica ima dovoljno sredstava da pokrije iznos transakcije. Nabavljač ili autorizuje određeni iznos novca ili odbija transakciju. Autorizacija samo smanjuje raspoloživi kredit, ona ne tereti račun kupca, niti prenosi sredstva prodavcu. Nakon što je transakcija autorizovana, prodavac tereti kreditnu karticu kupca za autorizovanu sumu. Ovo se naziva i "potvrđivanje". Po pravilima banaka koje izdaju kartice, prodavac ne sme potvrditi transakciju dok roba nije spremna za slanje, tako da može postojati vremenska pauza između autorizacije i potvrđivanja. Ako kupac poništi narudžbinu prije potvrđivanja, generiše se poništavanje.

"Potvrđivanja" se skupljaju i poravnavaju automatski u određenim vremenskim intervalima, npr. na kraju svakog dana. Poravnanje se prikazuje kao transakcija između nabavljača i prodavca. Kada se procesiraju skupljena "potvrđivanja", web server preko koga se vrše plaćanja, povezuje se nabavljačem da završi transakcije i prenese odgovarajuće sume novca na prodavčev račun u banci. Izdavač šalje mesečni račun vlasniku kartice za kupovine koje je obavio od poslednjeg računa.

2.3.7. S-HTTP i SSL

Sigurni hiper - tekst transfer protokol (S-HTTP) je sigurnosni podsistem HTTP-a, a razvila ga je *Enterprise Integration Technologies* kompanija. Oba, S-HTTP i SSL pružaju mogućnost sigurne komunikacije sa web serverima, i oba se mogu koristiti da bi se obezbedila poverljivost, identifikacija, i integritet (nepromenljivost) podataka. Međutim, ovi pristupi se razlikuju u sledećim elementima:

- SSL šifruje celu Internet vezu na nižem sloju, između aplikacijskih protokola, kao što su HTTP i TCP/IP slojevi. Ali S-HTTP radi na istom sloju kao HTTP. On osigurava razgovor obuhvatajući podatke unutar sigurnosnog paketa.
- SSL koristi specijalni "handshake" da bi uspostavio parametre za sigurnu vezu. S-HTTP definiše sigurnost razmenom zaglavlja za pakete poslate tokom web razgovora. Ova razmena zaglavlja paketa se može definisati kao vrsta sigurnih tehnologija koje se koriste u vezi.

S-HTTP podržava širok spektar opcija za obezbeđivanje sigurnih parametara. Opcije koje podržava prave od S-HTTP-a fleksibilan sistem, ali i sistem koji je vrlo težak za konfigurisanje na web sajtu. SSL takode pruža veliki broj opcija koji garantuju sigurnosne parametre i ove opcije su pre-konfigurisane u *browseru* i serverima, što čini da SSL bude lakši za korišćenje.

Ove funkcionalnosti današnjih *web browsera* pružaju mogućnost SSL-u da bude dominantna tehnologija za sigurne web veze. Kao rezultat toga, on-line plaćanja kreditnim karticama se većinom izvode uz pomoć SSL veza.

2.3.8. SSL protokol u primeni

SSL protokol je stvoren kao odgovor rastućim zahtevima za zaštićeni prenos podataka na Internetu. Zbog pravovremenog nastanka, te zbog tržišne uloge preduzeća *Netscape Communications*, stvaraoca ovog protokola, SSL je postao vrlo rasprostranjen. SSL, osim što je odobren kao standard od strane *www consortiuma* (www.w3.org) postao je *de facto* standardom. Uz SSL razvijala su se i druga rešenja koja ostvaruju zaštićeni prenos podataka kroz mrežu. Uspešnost SSL-a dodatno je naglašena nedostatkom drugih dovoljno dobrih rešenja koji bi ga zamenili. Ovde su dati kraci pregledi nekih od rešenja.

S-MIME Secure-MIME protokol je razvila RSA i dodatak je već postojećem MIME protokolu. Koristi sistem javnih ključeva kao osnovu za proveru ispravnosti i šifrovanje. Algoritmi za šifrovanje i rad sa potvrdama identični su onima korišćenim u SSL-u, tako da se iste potvrde mogu koristiti i u ovom protokolu. Korisnicima MIME-a, S-MIME omogućava zaštitu identičnu u ovom radu opisanoj zaštiti koju pruža SSL.

S-HTTP Secure HTTP je dodatak HTTP-u, on deluje u aplikacijskom sloju ISO/OSI modela. Za razliku od SSL-a koji ima zadatak da ostvari zaštićeni kanal između klijenta i servera, S-HTTP ima za cilj zaštićeno preneti pojedinačnu poruku. Takođe, omogućava proveru ispravnosti pošiljaoca poruke, te šifrovanje poruke kao i SSL. Razlog nerasprostranjenosti ovog protokola je neuspešan marketing koji ga je pratio, iako zadovoljava većinu zahteva traženih na tržištu.

SSH Secure Shell se koristi za spajanje na udaljeni računar. Stvara zaštićeni kanal između dva računara, a identifikacija se vrši **pomoću** lozinke, koju pre slanja kroz mrežu šifruje. Ne omogućava identifikaciju pomoću potvrda.

PEM (*Private Enhanced Mail*) omogućava zaštićeni prenos e-mail poruka koristeći proveru ispravnosti potvrdama, zaštitu sistemom javnih ključeva i proveru integriteta pomoću kontrolnog broja. PEM nije vezan za neki određeni operativni sistem ili vrstu korisnika, pa ga podržava veliki broj softverskih proizvoda. Ograničenje koje postavlja PEM je mogućnost slanja samo tekstualnih poruka.

PCT - *Private Communication Technology* je proizvod *Microsofta* koji je nastao kao reakcija na SSL verziju 2. Ta verzija SSL-a je imala probleme u situacijama kada je došlo do nasilnog prekida veze, čime je napadač dobio priliku da se uključi u razgovor bez identifikacije. PCT je

obuhvatio sve prednosti SSL-a, i rešio uočene probleme. Čim se pojavila SSL verzija 3, gde su rešeni postojeći problemi i dodate druge mogućnosti, PCT je prevaziđen i retko se koristi.

SHEN je zamena za postojeći HTTP. Razvijen je u CERN-u, gde i sam HTTP, zbog čega je zapažen, ali nije zaživeo pa je danas teško pronaći informacije o njemu.

PGP - *Pretty Good Privacy* je proizvod koji pruža mogućnost identifikovanja privatnim ključem, proveru integriteta i šifrovanje. Ne podržava proveru ispravnosti pomoću potvrda. Za njegovu upotrebu korisnik je primoran da dosta toga samostalno napravi, pa zna biti nespretan.

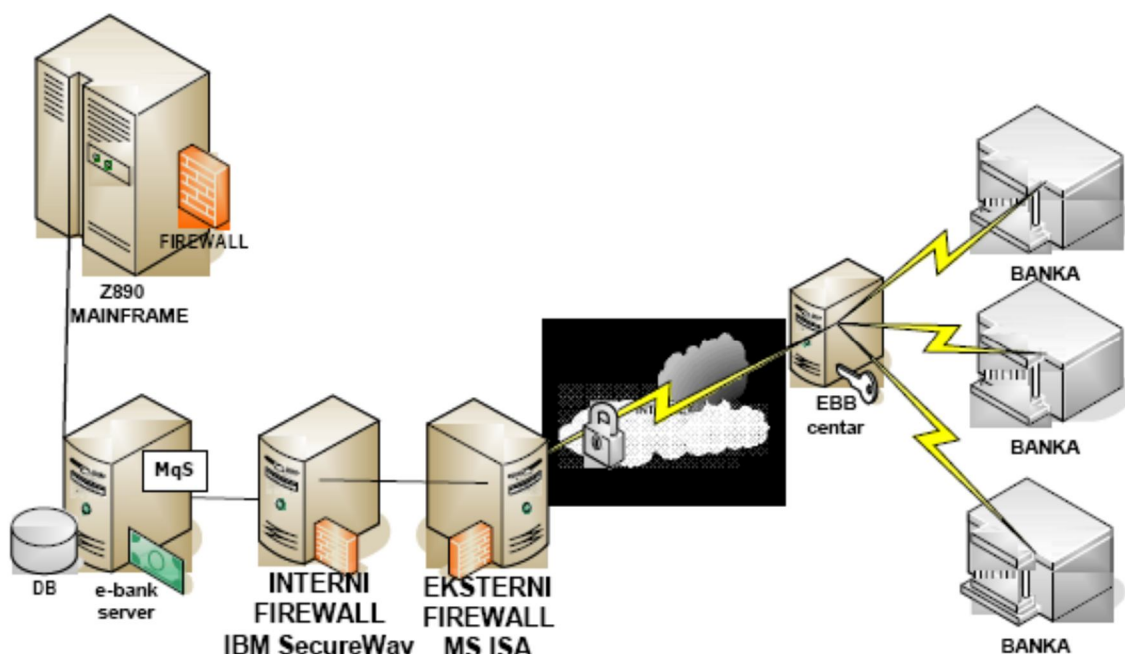
2.3.9. Zaštita informacija B2B E-Bank Sistema

Kao što je u uvodu naznačeno, paralelno sa razvojem elektronskog poslovanja u porastu je kriminal i zloupotreba IT resursa. Sve informacije koje egzistiraju u sistemu E-bank, po teoriji klasifikacije informacija, spadaju u klasu 4, u tajne informacije. Ovo znači da neautorizovan spoljašnji ili unutrašnji pristup ovim informacijama bi mogao biti kritičan za kompaniju. Prilikom osmišljavanja zaštite sistema polazi se od uobičajenih pretpostavki:

- potencijalni napadač ima potpun pristup komunikacionom kanalu (Internet) između pošiljaoca i primaoca;
- potencijalni napadač poseduje potrebno znanje o algoritmima šifrovanja.

Da bi se e-bank sistem obezbedio od zloupotreba primenjena je IT zaštita na više nivoa i to:

1. Zaštita na nivou aplikativnog i transakcionog softvera
2. Zaštita na nivou operativnog sistema
3. Hardverska kontrola
4. Antivirusna zaštita
5. Zaštita na nivou mrežne infrastrukture
6. Proceduralna i operaciona zaštita
7. Fizička zaštita



Ilustracija 15. Zaštita informacija B2B E-Bank Sistema

2.3.10. Problemi poverenja pri plaćanju kreditnom karticom

Pitanje poverenja u procesu plaćanja je jedan od najkritičnijih aspekata koji određuju prihvatljivost metode plaćanja. Jasno je da ako strane koje učestvuju u transakciji ne mogu biti sigurne u tačnost transakcije, onda je veoma verovatno da se ona neće uopšte desiti.

Kod ovih transakcija, poverenje se produbljuje kroz sledeće garancije:

Kupac mora biti siguran da :

- Transakcija će uzrokovati da on plati tačno određenu sumu i da će biti opterećen samo za stvari koje je kupio i to po dogovorenoj ceni.
- Njegove informacije o plaćanju neće biti ukradene i zloupotrebene za vršenje nedozvoljenih plaćanja pomoću njih.
- Da će primiti robu koju je kupio
- Da u slučaju spora ima dovoljno dokaza da dokaže da li se plaćanje desilo ili ne.

Prodavac mora biti siguran:

- Da će se transakcijom njemu platiti tačno dogovorena suma.
- Da u slučaju spora ima dovoljno dokaza da dokaže da li se plaćanje desilo ili ne.

Dobar protokol za plaćanje postiže ove stvari i za kupca i za prodavca . Njih je lako postići pri transakcijama kreditnom karticom u običnim prodavnicama. Budući da se posao obavlja licem u

lice, prodavac može uporediti potpis kupca sa potpisom na poledini kartice takođe se na licu mesta utvrđuje suma novca i roba o kojoj se radi u datoj transakciji. Ne postoji opasnost da se informacije o plaćanju ukradu ako kupac radi sa poverljivim trgovcem. U slučaju spora, svaka strana ima potpisanu kopiju priznanice koja se može iskoristiti kao dokaz da se transakcija desila.

Pitanje poverenja postaje mnogo komplikovanije kada se plaćanja kreditnom karticom vrše preko Interneta. Korišćenjem SSL-a ne ispunjavaju se svi preduslovi za poverenje spomenuti gore. Najčešći razlozi za zabrinutost su da neki od tradicionalnih načina garancije integriteta plaćanja mogu biti ugroženi.

2.4. WEB servisi

Pod Web servisom se podrazumeva bilo koja softverska aplikacija koja je dostupna preko mreže (Internet ili intranet) i koja koristi standardizirani XML sistem poruka za razmenu podataka. Razmena funkcioniše tako da korisnik poziva Web servis slanjem upita u XML formatu, a poslužitelj u istom formatu vraća rezultat obrade.

2.4.1. Karakteristike Web servisa

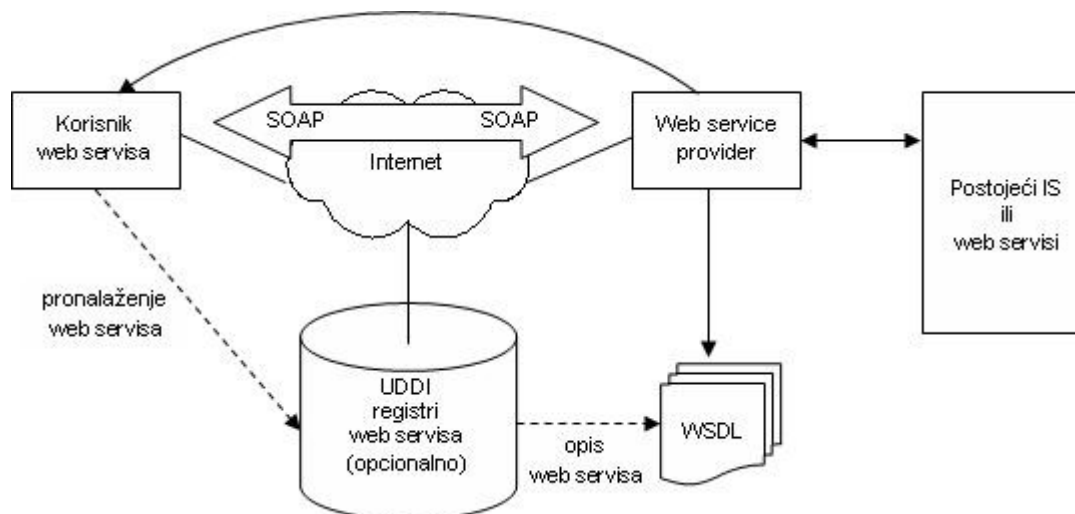
Budući se sva komunikacija odvija uz pomoć XML-a, Web servisi nisu vezani ni za jedan operacijski sistem ili razvojno okruženje, čime se zaobilazi nekompatibilnosti među postojećim softverima. Karakteristike infrastrukture Web servisa:

- Web servis poslužitelj i korisnik Web servisa su spojeni na Internet, te mogu komunicirati međusobno i s drugim servisima
- način komunikacije mora odgovarati nekom široko prihvaćenom standardu - obično su to SOAP poruke, a mogu i biti HTTP-GET ili HTTP-POST zahtevi
- rad Web servisa ne zavisi o operacijskom sistemu, objektnom modelu niti o programskom jeziku, sve dok se Web servisi i korisničke aplikacije pridržavaju otvorenih standarda

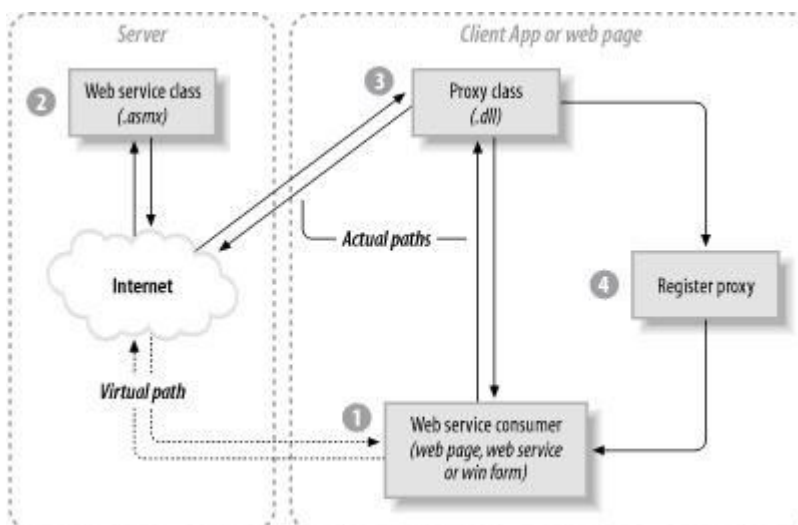
Pošto Web server i CGI aplikacija moraju da razmene podatke kroz proces razmene, komunikacija između njih je znatno usporena.

Karakteristike infrastrukture Web servisa:

- Web servis poslužitelj i korisnik Web servisa su spojeni na Internet, te mogu komunicirati međusobno i s drugim servisima
- način komunikacije mora odgovarati nekom široko prihvaćenom standardu - obično su to SOAP poruke, a mogu i biti HTTP-GET ili HTTP-POST zahtevi
- rad Web servisa ne zavisi o operacijskom sistemu, objektnom modelu niti o programskom jeziku, sve dok se Web servisi i korisničke aplikacije pridržavaju otvorenih standard.



Ilustracija 16. Karakteristike infrastrukture Web servisa



Ilustracija 17. Princip rada web servisa

Korisnik Web servisa(1) šalje upit prema poslužitelju (2). Korisnik ima privid da komunicira preko Interneta direktno sa Web servisom, a u stvari komunicira sa *proxy* klasom(3), koja je lokalna korisniku. Zadatak *proxy*-a je da obavi sve komunikacijske pojednosti nižeg nivoa potrebne za slanje podataka preko Interneta do poslužitelja. Proxy isto tako prima rezultate i

prezentira ih korisniku. Sve je to moguće uz uvet da je *proxy* prethodno registriran kod korisničke aplikacije(4).¹⁸

2.4.2. *Praktična strana WEB servisa*

XML (*Extensible Markup Language*)

Standardizovani jezik za opis podataka, koji omogućava programerima razvoj sopstvenih tipova podataka, u cilju identifikacije informacija u dokumentima, te njihovom stavljanju u odgovarajući kontekst.

SOAP (*Simple Object Access Protocol*)

predstavlja protokol koji opisuje način na koji jedna aplikacija treba da komunicira sa web servisom. SOAP omogućava korišćenje web servisa za finansijske transakcije na Internetu, kao što je recimo autorizacija kreditnih kartica.

UDDI (*universal description, discovery and integration*)

sistem sličan “*yellow pages*” sistemu, na kome su izlistani web servisi, a koji dopušta softverskim aplikacijama da “prelistaju” dostupne web servise i opisuje način kako da se “zakače” za njih.

WSDL (*Web services description language*)

jezik koji služi za definisanje pojedinačnih web servisa. WSDL jezikom opisuju se sve vrste aktivnosti koje može da odradi neki web servis.

Praktično gledano, web servis predstavlja bilo koju softversku aplikaciju koja je dostupna preko mreže (Internet ili intranet) i koja koristi standardizovan XML sistem poruka. XML se koristi za formatiranje svih oblika komunikacije ka web servisima. Na primer, klijent poziva web servis slanjem poruke u XML formatu, zatim čeka na odgovarajući XML odgovor. Pošto se sva komunikacija formatira uz pomoć XML standarda, web servisi nisu vezani ni za jedan operativni sistem ili razvojno okruženje - jednostavno, Java aplikacije mogu da “komuniciraju” sa *Perl* aplikacijama, dok recimo Windows programi mogu da razmenjuju podatke sa programiranjem koji rade u Unix okruženju.

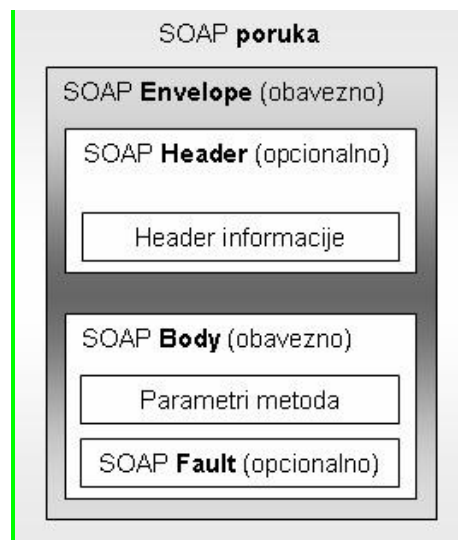
Web servisi sasvim prevazilaze nekompatibilnosti skupom softverskih standarda kao što su XML, SOAP (*simple object access protocol*), UDDI (*universal description discovery and integration*) i WSDL (*Web services description language*). Ovi standardi omogućuju definisanje, pakovanje, pristupanje i izvršavanje podataka i programa preko Interneta, bez potrebe za vođenjem računa o pojedinačnim implementiranim tehnologijama.

¹⁸ http://spvp.zesoi.fer.hr/seminari/2004/xml_web_servisi-isorsa/2.htm

2.4.3. SOAP

SOAP je jednostavan protokol za razmenu informacija u decentraliziranom, distribuiranom okruženju. Baziran je na XML message protokolu koji je standardiziran od strane *World Wide Web Consortium* (W3C). Pomoću SOAP-a se može implementirati RPC stil komunikacije u kojem SOAP poruka sadrži pozivajuću funkciju i parametre koje prosljeđuje funkciji. Uobičajeno je da takvu poruku šalje korisnik, a poslužitelj vraća poruku s rezultatom pokrenute funkcije. SOAP takođe podržava "dokumentni stil" aplikacije u kojima je SOAP samo omotač oko XML dokumenta. Takve aplikacije su veoma fleksibilne i zato se danas koristi ta prednost prilikom kreiranja Web servisa.

SOAP dokument se sastoji od obavezne SOAP envelope, opcionalnog SOAP zaglavlja (*header*) i obaveznog SOAP tela (*body*).



Ilustracija 18. Soap protokol

SOAP *Envelope* sadrži *encodingStyle* atribut koji definira korištena pravila serijalizacije u dotičnoj SOAP poruci. Taj se atribut može pojaviti u bilo kojem elementu i prenosi se na sve podređene elemente (*child elements*) koji ne sadrže vlastiti atribut.

SOAP *Header* je prvi podređeni element SOAP *envelope* elementa. Podređeni elementi *header* elementa (*child elements*) moraju biti identificirani sa *namespace* (obično se koristi URI) i lokalnim imenom. Svaki element može sadržavati atribut *mustUnderstand* kojim se primatelju naznačuje da je obavezno procesiranje zaglavlja (vrijednost atributa =1). SOAP poruka koja putuje do određene destinacije obično na svom putu prolazi kroz skup posrednika. Za tu svrhu postoji poseban atribut *actor* koji definira kojim je sve posrednicima namijenjena poruka. SOAP *Body* element je podređeni element SOAP *envelope* elementa koji se koristi za prenos parametara metoda i (opcionalno) poruka o grešci. SOAP je iznimno lako povezati s HTTP

protokolom, koji je podržan od skoro svih operacijskih sistema. Infrastruktura za nadgledanje i sigurnost unutar HTTP-a je također već razvijena.

2.4.4. Prednosti Web servisa u odnosu na "klasične" Web aplikacije

Fleksibilniji su. Klasične Web aplikacije se mogu koristiti samo uz pomoć *Web browser*-a, pri čemu korisnik nema nikakvog uticaja na to kako će rezultat izgledati na njegovom ekranu, osim ako ne napravi program koji će da iz dobijenog HTML-a "izvlači" interesantne podatke i prikazuje ih na željeni način. Web servise mogu da koriste najrazličitiji programi: počev od drugih Web servisa, preko Web aplikacija, GUI programa ili čak tzv. aplikacija komandne linije. Recimo servis za prevod teksta koji smo pomenuli kao primer, može da koristi Altavista.com, program za obradu teksta kao što je MS Word, može se napraviti i programčić u Unix tradiciji koji bi radio u stilu *"ttx -ef mytextfile"* (prevod sadržaja fajla mytextfile sa engleskog na francuski), a mogao bi da bude korišćen i sa npr. mobilnih telefona ili ručnih računara koji imaju vezu sa Internetom. Svi ovi različiti "klijenti" bi koristili jedan isti Web servis i autori tog servisa ne bi morali ni da znaju kakve sve različite aplikacije ga koriste. Štedljiviji su po pitanju opterećenja mreže i resursa servera. Ako opet pogledamo primer sa *Systran*-ovom Web aplikacijom, videćemo da ona najpre mora da pošalje korisniku HTML sa formom za unos teksta, a posle prevoda šalje mu ne samo prevedeni tekst, već i HTML kod koji opisuje kako taj tekst treba da bude prikazan. Web servis bi primio jedan zahtev sa originalnim tekstom i poslao jedan odgovor sa prevedenim tekstom - nikakav dodatni HTML.

Lakši su za razvoj, testiranje i održavanje. Kod Web aplikacije je neophodno odraditi ne samo funkciju programa, već i dizajn i sve to dobro istestirati sa raznim browserima i platformama. Ko je probao da uskladi da Web aplikacija izgleda dobro na različitim *browserima* zna kakva je to muka (pitajte autora ovog sajta), a kad se napravi neka izmena, proces testiranja ide iz početka. Sa Web servisima svega toga jednostavno nema. Autor servisa brine o funkciji - prikaz je na klijentima. Znači li to da će Web servisi zameniti Web aplikacije koje rade sa HTML-om? Ne, osim u retkim slučajevima. Web servisi imaju svoj spektar primene koji je mnogo širi od onog koje pokrivaju Web aplikacije. Međutim, u mnogim slučajevima je još uvek bolje raditi sa HTML prikazom nego praviti specijalizovane programe koji će tumačiti podatke dobijene od servera. ES je primer Web aplikacije koja treba da ostane u ovom obliku, mada nije nemoguće dodati i Web servis.

2.4.5. Primeri upotrebe web servisa

Kao jedan od najjednostavnijih primera upotrebe web servisa možemo uzeti aukcijski endžin poznate Interneta aukcijske kuće *eBay* [www.ebay.com]. Zainteresovane firme i pojedinci mogu se jednostavno pretplatiti na korišćenje *eBay*-evih web servisa, tako da ne moraju investirati u razvoj sopstvenih. Sve što je potrebno je da u svoje web aplikacije implementiraju nekoliko redova programskog kôda kako bi inkorporirali eksterne web servise. Na taj način je praktično omogućeno da druge kompanije (koje u osnovi nisu aukcijske kuće) imaju funkcionalnost jedne aukcijske kuće, te mogu da organizuju privatne instant-aukcije na sopstvenim web sajtovima.

Dodatno ovaj web servis može biti potpomognut servisima drugih kompanija koje se bave procesiranjem plaćanja, isporuke i logistike, tako da zainteresovane firme (pojedinci) mogu da kreiraju aukcijske portale bez sopstvenih resursa, a u saradnji sa brojim provajderima različitih web servisa.

Još jedan vrlo plastičan primer upotrebe web servisa je kompanija CUNA Mutual [www.cuna.org], koja se bavi pružanjem finansijskih usluga kreditnim ustanovama. Ova kompanija koristi web servise za transfer podataka iz *back-end* aplikacija za upravljanje finansijskim servisima na web stranice. Većina ovih softverskih aplikacija je urađena pre više godina, kada se još nije naslućivao veliki potencijal Interneta. U kompaniji su procenili da nije isplativo ponovo razvijati iste aplikacije koje bi nudile dodatne dinamičke sadržaje. Umesto toga, odlučili su da kreiraju web servise koji automatski formatiraju podatke iz pozadinskih aplikacija tako da vrlo jednostavno mogu (preko *content-management* sistema) da se prikažu na web stranicama.

2.4.6. *Potencijali u domaćim uslovima*

Kao što je gore navedeno, web servisi, njihov razvoj i upotreba, mogu biti najzanimljiviji finansijskom sektoru, tj. domaćim bankama, štedionicama, kreditorima, brokerskim kućama i sličnim ustanovama. Upotreba ove nove tehnologije još više dobija na značaju prelaskom platnog prometa u poslovne banke. Kreiranjem odgovarajućih web servisa i usaglašavanjem komunikacije između poslovnih partnera shodno XML standardima povećava se efikasnost i operativnost, smanjuju se troškovi i ojačava se veza između poslovnih partnera i klijenata.

Banalni primer opravdanosti uvođenja web servisa odnosi se na kreiranje i distribuciju izveštaja o stanju na računima klijenata, popularnim "izvodima". Trenutno, domaće banke ove izveštaje nude u raznoraznim oblicima, a najčešće u štampanom obliku ili u obliku tekstualnih datoteka različitih formata. Ovako formirane informacije se vrlo teško unose u informacione sisteme klijenata, što uvećava troškove i kompleksnost. Rešenje bi bilo formiranje web servisa koji bi opsluživao klijente podacima koji su standardizovanog formata. Ovim bi takve poruke mogle, bez dodatnih transformacija i konverzija, da ulaze u poslovne informacione sisteme klijenata. U perspektivi, poslovni partneri između sebe i u komunikaciji sa bankama, bi trebali da razviju sopstvene web servise kako bi standardizovali komunikaciju, te povećali efikasnost i konkurentnost. Sa web servisima, poslovanje se premešta sa mreže koja je oslonjena na ljudski faktor, na mrežu koja se oslanja na aplikacije (aplikativno-orijentisane mreže gde međusobno komuniciraju aplikacije). Ovo ne znači da se iz priče izbacuje ljudski faktor, već da se samo omogućava direktna konverzacija između aplikacija, kao što to sada imamo u pojednostavljenom obliku između *web browser*-a i web servera (zahtev-odgovor).

2.5. Elektronsko bankarstvo

Pod elektronskom tehnologijom podrazumevamo kombinovanu upotrebu informacionih tehnologija i telekomunikacija. Pod uticajem primene elektronskog poslovanja reorganizuju se skoro sve delatnosti i tako danas imamo e-trgovinu, e-bankarstvo, e-upravu i sl.

Elektronsko poslovanje ima sledeće prednosti:

- smanjenje troškova poslovanja, i to prevashodno vezane za izradu papirnih dokumenata,
- smanjenje grešaka, pogotovo gde je tačnost informacija od značaja,
- ušteda vremena, posebno u prenosu informacija,
- smanjenje obima ljudskoga rada,
- pristupačnost i razmenljivost informacija.

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 preduslovi:

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

Kod poslovnih sistema koji su uveli elektronsko poslovanje se mogu uočiti određene prednosti. Primena elektronskog poslovanja je dovela do smanjenja troškova poslovanja, i to prevashodno troškova vezanih za izradu papirnih dokumenata, kao na primer, smanjenje troškova izrade papirnih obrazaca. Vezano za smanjenje troškova je i smanjenje obima ljudskoga rada koji je vezan za papirnu dokumentaciju, kao na primer sortiranje, zavođenje dokumenata, štampanje, itd. Pored toga smanjen je i obim posla na unošenju podataka u računar iz primljene dokumentacije, kontrola unosa, i drugo. Smanjenje grešaka, pogotovo gde je tačnost informacija od značaja, je od velike važnosti. To se postiže automatskim prikupljanjem, otpremom i prijemom poruka, gde se izbegava uticaj ljudskih grešaka. Elektronsko poslovanje omogućuje uštedu vremena, posebno u prenosu informacija, a to je bitna prednost jer obezbeđuje pravovremenu informaciju koja može biti od suštinske važnosti za donošenje odluka. Pored pomenutih prednosti koje elektronsko poslovanje nudi, obezbeđuje i pristupačnost informacija i njihovu razmenu. Informacije je lako sortirati, lakše im je pristupiti i vršiti dalju obradu.

Sa druge strane, sprečavanje zloupotreba informacija paralelan je zadatak zadatku razvoja elektronskog bankarstva. Danas, možemo konstatovati da postoji nekoliko sistema i nivoa zaštite podataka, počevši od najjednostavnijih kao što je lozinka, koji danas sam po sebi više ne predstavlja dovoljan sistem zaštite i mora se kombinovati sa određenim dodacima (na primer, PIN kodovi), preko TAN kartica pa sve do savremenih sistema enkripcije podataka koji za sada onemogućavaju zloupotrebu informacija. Naravno, osnovni zadatak pružalaca usluga elektronskog poslovanja, svakako jeste zaštita podataka, s obzirom na sve veći broj mogućnosti i načina da se zaobiđu klasični sistemi zaštite i da se dođe u posed informacija.

Ipak, najveću odgovornost za sprečavanje zloupotrebe informacija iz elektronskog bankarstva snosi sam korisnik, jer se u njegovom posedu nalaze pojedinačni elementi zaštite sistema. Prema tome, korisnik usluge (npr. fizičko lice) poseduje korisničko ime i lozinku za pristup sistemu, dok korisnik (pravno lice) smart karticu i PIN. Ukoliko bi došlo do sistemskog proboja koje bi imalo efekta na sve korisnike usluge, tada bi eventualna banka trebala da pruži obeštećenje svojim korisnicima u cilju održavanja buduće saradnje.

Radi lakšeg shvatanja pojma elektronskog bankarstva i njegovog funkcionisanja potrebno je objasniti nekoliko bitnih pojmova vezanih za navedenu materiju, radi njenog što potpunijeg shvatanja. Ti pojmovi su: bankomat, POS terminal i bankarske kartice.

Bankomat je inteligentni interaktivni računarski terminal, dislociran i povezan u bankarsku mrežu i koji je na raspolaganju 24 časa za obavljanje pretežno rutinskih bankarskih operacija (podizanje i ulaganje gotovine, polaganje depozita, transfer sredstava, postavljanje upita i dobijanje informacija i korišćenje kredita). Bankomati se danas postavljaju na svim frekventnim mestima poslovanja, kretanja i života klijenata, obrazujući tako brojne „x-terminale“ mreže sa izuzetno niskim troškovima.

POS terminal ili POS sistem, predstavlja elektronski transfer koji povezuje maloprodaju i bankarsko finansijske institucije. Sa stanovišta hardvera i povezivanja koncept je sličan bankomatima, uz drugačiju funkciju terminala koji ovde ima ulogu registar kase. Jedna od bitnih razlika i pretpostavki za razvoj POS sistema čija je međunarodna standardizacija identifikaciono-klasifikacionih šifara svih artikala, simbolizovana danas u poznatom BAR kodu. Standardni BAR kod za jedinstvenu identifikaciju artikala sastoji se iz 13 cifara predstavljenih tankim i debelim linijama različitog međusobnog razmaka. Svaka decimalna brojka kodira se sa dve tamne i dve svetle vertikalne linije. Danas je u svetu standardizovano osamnaest (18) format BAR kodova (npr. kod sa 20 znakova koji se koristi u avio-saobraćaju, kod sa 39 znakova koji se koristi za špediciju, carinu itd.).

Bankarske kartice su plastične kartice, slične kreditnim karticama, s tom razlikom što su aktivne za podizanje gotovine samo do momenta pozitivnog stanja na računu banke koja je istu izdala. Namenjene su neposrednom korišćenju kao ključ za prilaz ATM uređaju i obavljanje odgovarajućih transakcija.

Kao izdavaoci kreditnih kartica se pojavljuju banke i druge finansijske institucije, kao i velike firme. Zbog toga postoje izvesne razlike u tretiranju pojedinih kartica i njihovom prihvatanju prilikom plaćanja. Prilikom korišćenja bankarske kartice identifikuje se šifra izdavaoca kartice i šifra vlasnika kartice, a kod savremenih tj. „pametnih“ ili „inteligentnih“ kartica (*smart card*) moguće je obezbediti i lozinku pristupa (*password*).

Ovakve kartice u uslovima elektronskog bankarstva omogućavaju:

1. Bezgotovinski platni promet u realnom vremenu i
2. Kreditiranje vlasnika kartice.¹⁹

Njihovu osnovu čine mikroprocesorski čip sa različitim veličinama RAM, ROM i PROM memorijom. U skladu sa tim mogućnostima i funkcijama uobičajena je podela kartica na tri generacije:

1. **Standardna ili kontaktna pametna kartica**, je istih formata i debljine kao i konvencionalne plastične kartice, ali sadrži posebno ugrađenu memoriju i procesor, i 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.
2. **Bezkontaktne kartice sa čipom**, tretiraju se kao četvrta generacija finansijskih transakcionih kartica ili druga generacija kartica sa čipom. One su se tehnološki usavršavale uporedo sa usavršavanjem same tehnologije čipa. Prva tehnološka rešenja zasnivala su se na korišćenju više od jednog čipa i zahtevale su upotrebu posebnih mera za obezbeđenje sigurnosti. Novije kartice se zasnivaju na korišćenju samo jednog čipa, jeftinije su i imaju duži vek trajanja.
3. Najrevolucionarniji koncept kartice sa čipom predstavljaju **kartice koje su snabdevene sa displejom i tastaturom**, a koje su poznate pod nazivom „super pametne kartice“ (*Super Smart Card*). Nazivaju se još i aktivnim ili samoautorizujućim pametnim karticama. Kako je kod njih udružena logika s kalkulatorom, najveće koristi pomoću njih mogu se postići i multiplikacijom njihovih funkcija. I displej i tastatura su integralni delovi kartice, čija veličina po ISO standardima odgovara veličini obične kreditne kartice.²⁰

2.5.1. Model E-BANK

U sistemu međunarodnog bankarstva postoje brojni primeri specijalizovanih institucija elektronskog bankarsko-finansijskog poslovanja koji koristeći Internet i intranet arhitekturu i standarde omogućavaju kompletne usluge korisnicima.

E-bank sistem pruža niz usluga kako prodajnim mestima, tako i vlasnicima platnih kartica. Plaćanje na internetu može se obaviti na dva načina. Prvi način je ukoliko se zna iznos uplate i

¹⁹ Đurković, Ivan, „MEĐUNARODNO BANKARSTVO“, Univerzitet „Braća Karić“, Beograd, 2008., str. 134.

²⁰ Ibid. str. 134.

račun na koji se uplaćuje, vlasnik kartice može da se korišćenjem broja kartice i lozinke prijavi na e-bank sajtu i tu direktno izvrši uplatu. Kao dodatnu pogodnost, prema dogovoru sa prodajnim mestom, na sajtu mogu da se drže podaci o mesečnim zaduženjima pretplatnika prodajnog mesta. Na taj način, vlasnici kartica mogu da vide koliko duguju i da zatim predu na automatski popunjenu uplatnicu.

Drugi način je da se plaćanje može obaviti i kao završni korak na nekom drugom sajtu. Kupcu se po završetku izbora robe na sajtu prodajnog mesta prezentira završni račun. Ovaj dokument u sebi sadrži iznos koji treba da se plati, identifikatore transakcije i prodajnog mesta. Po obavljenoj vizuelnoj proverbi završnog računa kupac prelazi na e-bank sajt na kome se popunjavanjem podataka o kartici kompletira uplata.

Ovakav način uplate ne zahteva od prodajnog mesta nikakvu specijalnu zaštitu podataka. Svi poverljivi podaci se unose na bezbednom e-bank sajtu. Sigurnost sajta obezbeđuje SSL protokol, koji je jedan od najčešće korišćenih protokola za transfer poverljivih podataka na internetu. Prodajno mesto i vlasnik kartice su o obavljenoj autorizaciji transakcije obavešteni odmah, a mogu opciono da zahtevaju i da im se kao potvrda pošalje e-mail.

Korisnici kartice mogu na *e-bank* sajtu da pristupe podacima o svojim prethodnim uplatama, u tabelarnoj formi. Na sličan način, prodavci mogu da pristupe podacima o uplatama na svom prodajnom mestu. Sistem ima troslojnu arhitekturu, koja je tipična za aplikacije na internetu. Ovakva arhitektura obezbeđuje veću sigurnost sistema. Takođe, implementacija pojedinih delova sistema je lakša jer manje zavisi od specifičnosti implementacije ostalih delova sistema. Korisnici pristupaju sistemu preko interneta pomoću svojih *browser*-a. Korisničke zahteve obrađuje aplikacioni server. Obrada podrazumeva i konsultovanje baze podataka. U slučaju uplate, aplikacioni server se obraća *BankWork* aplikaciji koja obavlja autorizaciju transakcija. Odgovor aplikacionog servera se vraća korisniku u formi dinamički generisane HTML strane.

2.5.2. SWIFT sistem

SWIFT (*Society for World Wide Interbanking Financial Telecommunication*) je svetsko udruženje za interbankarske finansijske telekomunikacije. SWIFT je istovremeno sinonim za WAN mrežu. Osnovan je 1973. godine sa ciljem da postavi standard u automatskom transferu podataka između banaka, a od 1987. godine je proširen delokrug i na transfer podataka između finansijskih, nebankarskih organizacija (investicione institucije, brokerske i dilerske kompanije, berze itd. Danas SWIFT predstavlja svetskog lidera u transferu podataka banaka i ostalih finansijskih organizacija.

Mreža ima dve centrale koje se nalaze u Americi i Holandiji. Centri za podršku postoje na tri kontinenta i oni su na raspolaganju korisnicima 24 časa dnevno. Pored toga SWIFT mreža ima svoja regionalna predstavništva u svim većim zemljama sveta. Početkom 2000. godine to je brojalo oko 7000 korisnika SWIFT-a iz čak 190 zemalja sveta. SWIFT je vlasništvo banaka i finansijskih institucija članica, a korišćenje mreže se plaća kvartalno prema obimu korišćenja.

Visok stepen sigurnosti u SWIFT mreži utiče i na procese ulaska novih korisnika u mrežu. Proces je dugotrajan, i zna da traje i po nekoliko godina, ali njegovim završavanjem se garantuje visoka obučenost i osposobljenost kadrova novog korisnika i sigurnosti starih korisnika. Ulaskom novog korisnika u SWIFT mrežu on postaje punopravan član i korisnik mreže. Svakih tri meseca se starim članovima SWIFT mreže šalju tzv. „big“ fajlovi koji sadrže podatke o svim novim korisnicima, odnosno članovima mreže. Takav način organizovanja i vođenja mreže ju je učinio najboljom i najsigurnijom mrežom ove vrste u svetu i skoro sav promet u međunarodnom bankarstvu i finansijama se odvija preko ove mreže.

Što je bitno napomenuti, da pri korišćenju SWIFT-a mora da se primjenjuje: standardizovana struktura dokumenata i kriptografija, odnosno šifriranje poruka.²¹

Svaki korisnički server, preko koga se pristupa SWIFT mreži treba da bude opremljen i čitačem kartica koje će obezbediti identifikaciju korisnika, a svi PC-i korisničkoj LAN mreži moraju imati instalirane klijent – SWIFT aplikacije. Te aplikacije služe za kreiranje, čitanje, prijem i slanje poruka.

Veliku popularnost SWIFT-a kao WAN mreže koja obezbeđuje implementaciju internet tehnologija u svet finansijsko bankarskih usluga ima svoje polazište u sledećim mogućnostima (24 časa dnevno): sve vrste transfera sredstava korisnika; sve vrste transfera banaka; prenos poruke; menjački poslovi; depoziti i zajmovi; mogućnost pozajmice depozita i sredstava; plaćanje kamata; izvodi i potvrde stanja računa; postavljanje pitanja i dobijanja odgovora i korišćenje internet servisa. Procene su da se godišnje pomoću SWIFT mreže prenese oko milijardu transakcija.

Permanentno širenje međunarodne trgovine, rast važnosti kapitala i razmene informacija, znanja i dokumentacije u tom finansijskom kompleksu, postavio je pred SWIFT visoke zahteve tržišta. Ta sveukupna zaštita sistema postiže se koristeći ranije pomenute mehanizme, kao što su, kontrola pristupa, zaštita tajnosti i integriteta informacije, provera identiteta pošiljaoca i primaoca uz korišćenje svih elemenata kriptografije, šifriranje, ključevi i dešifrovanje. Bitna je i ta činjenica da SWIFT stalno usavršava postojeće i razvija nove servise u skladu sa novim zahtevima finansijsko-bankarskog poslovanja. Takva dva servisa su:

1. NET FILE ACT, kao fajl transfer servis koji podržava razmenu datoteka koje sadrže zbirna plaćanja ili pojedinačne fajlove;
2. NET INTER ACT, kao servis koji omogućava finansijskim institucijama da međusobno interaktivno komuniciraju, zatim komuniciraju sa klirinškim kućama, filijalama itd.

Ova dva servisa su novina u bankarstvu i početak njihovog korišćenja veže se za početak ovog veka.

Đurković, Ivan, „MEĐUNARODNO BANKARSTVO“, Univerzitet „Braća Karić“, Beograd, 2008., str. 135.

2.5.3. Elektronski platni promet i sistemi plaćanja

Elektronska trgovina, pogotovo ona koja u svom sistemu obuhvata potrošače i digitalne proizvode, postavlja oštre zahteve prema sistemu plaćanja. Sistemi plaćanja moraju da budu pogodni za kupovinu preko mreže, prenosivi preko mreže, dovoljno jaki da prevaziđu smetnje i jeftini za transakcije, sa ekstremno malim vrednostima. Uprkos ovoj skupini zahteva, predloženo je više desetina standarda plaćanja preko interneta. Neki od tih standarda su *Anonymous Internet Merchantile Protokols* od AT&T Bell Labs, *Conditional Acces for Europe* za EU, *Secure Electronic Transaction* kojeg je promovisao MasterCard i Visa, itd. većina softverskih proizvoda koji se nude, zasnivaju se na ovim otvorenim standardima (*CyberCash*, *DigiCashMondex* i dr.).

Sistemi elektronskog plaćanja mogu se klasifikovati u tri grupe:

1. Plaćanje preko posrednika,
2. Plaćanje koje se zasniva na prenosu elektronskih fondova i
3. Plaćanje zasnovano na elektronskoj valuti.

Glavne promene koje su ostvarene u elektronskom poslovanju su obavljanje rutinskih transakcija, kao i uvođenje elektronskog transfera novca, odnosno elektronskog plaćanja. Korišćenje Interneta kao komunikacionog kanala u oblasti plaćanja uslovalo je pojavu Internet plaćanja i odgovarajućih instrumenata kojima se ova plaćanja obavljaju. U tradicionalnom sistemu plaćanja na malo postoji nekoliko sistema za elektronski transfer novca koji se danas koriste, i to: bankomati, EFT/POS sistemi i elektronske kartice. Među novim instrumentima i transakcionim mehanizmima na Internetu tri su posebno interesantna, a to su inteligentne kartice, digitalni novac i mikro-transakcije²².

2.5.4. Elektronski novac (E-novac)

U tradicionalnoj trgovini, u osnovi poslovanja kao instrument plaćanja nalazi se novac. Svaki trgovac najviše voli plaćanje gotovim novcem, jer može odmah da ga troši čim ga primi, ne mora da plaća proviziju firmama koje izdaju kreditne kartice i druge procedure. Za banke novac je jeftin za obradu, a kada se primenjuje umesto kreditnih kartica, troškovi za banku su niži, a ipak predstavljaju sigurnije platežno sredstvo od čekova i kreditnih kartica.

Zbog izuzetno niskih troškova obrade, novac se može koristiti i za plaćanje jako malih iznosa za takozvana mikroplaćanja. Zbog sveg navedenog u e-poslovanju svi vole da koriste e-novac, odnosno elektronski novac.

Elektronski novac je bezbedan, i može se koristiti za obavljanje mikroplaćanja. U praksi, neugodnost oko preuzimanja softvera, otvaranja računa i izgradnje specijalnih sistema e-

²² Ćirović, Milutin, „BANKARSTVO“, Beograd, Bridge Company, 2001., str. 239.

trgovine, kao i poteškoća da se pridobije kritična masa korisnika, izgleda da daje prednost korisnicima e-novca. Uprkos ovim preprekama pojavljuju se sasvim nove mogućnosti e-novca, ili, alternativna plaćanja karticom. Sve pomenute varijacije mogu se grupisati u sledeće kategorije: e-novac, kartice sa deponovanim vrednostima i plaćanje tipa P2P.

2.5.4.1. Karakteristike e-novca

Elektronski novac ima sledeće karakteristike:

- Elektronski novac se sastoji od binarnog niza bitova, čije kopiranje je jednostavno,
- Pravilom „trajanje jedne novčanice jednako je jednoj transakciji“, rešava se problem višestrukog trošenja,
- Svaka ispravna novčanica nosi potpis finansijske institucije koja ju je izdala,
- Za proveravanje i dokaz ispravnosti novčanice koristi se metoda elektronskog potpisa.

Međutim, smatra se da elektronski novac ima dvije bitne karakteristike. Prva karakteristika je ta da se elektronski novac može upotrebiti za plaćanje koje se odnosi na veliki broj usluga i proizvoda. Da bi se neki novac nazivao e-novcem, on mora da bude upotrebljiv za paletu plaćanja.

Gotovinski novac iza koje stoji banka, zakonsko je sredstvo plaćanja, što nije slučaj sa sadašnjim tipovima e-novca. Ovo prouzrokuje pravne probleme, jer za razliku od gotovog novca, koji obavezno moraju da prime svi učesnici u plaćanjima, elektronski novac primaju samo oni prodavači koji su uključeni u ovaj vid plaćanja.

Druga karakteristična stvar za e-novac, jeste da on sadrži unapred uplaćenu vrednost koja je registrovana na mikročipu. Postoje dve kategorije e-novca, a razlikuju se u zavisnosti gde je registrovana unapred uplaćena vrednost. Tako da postoje:

1. E-novac u vidu smart kartica, čija je novčana vrednost unapred uplaćena i registrovana na čipu kartice,
2. E-novac koji je unapred uplaćen, pri čemu je novčana vrednost registrovana na hard diskovima kompjutera.

2.5.4.2. E-novac u kompjuteru korisnika (eCoins)

Karakteristika ovog sistema je da korisnik otvara svoj racun i prenosi specijalni elektronski novčanik na svoj kompjuter, dok se kupovina odvija uz pomoć *eCoins* kreditne kartice. Digitalni niz znakova koji vredi pet američkih centi, predstavlja jedan *eCoin*. Ovakvi *eCoins*-i se prenose sa online računara u e-novčanik.

Da bi trgovac mogao da koristi ovaj sistem, potrebno je da ima ugrađenu specijalnu *eCoin* ikonicu na svojoj stranici za plaćanje. Zadatak ovog servera je da vodi evidenciju svih korisnika i

trgovaca, da prima zahteve za plaćanje iz korisničkog novčanika i da obrađuje već ugrađene fakture za trgovce.

2.5.4.3. E-novac za mikroplaćanja (*Qpass*)

Qpass predstavlja jedan od sistema mikroplaćanja koji uspeva da izbegne određene probleme koji se pojavljuju kod ove vrste plaćanja, i tu ima dobar uspeh. Ovaj sistem se koristi za kupovinu sadržaja servisa nekih novina ili časopisa. Kod ovog sistema korisnik otvara *Qpass* račun, kreirajući korisničko ime, lozinku i specifičnu kreditnu karticu čiji će račun biti zadužen za određenu kupovinu. Posle obavljene kupovine, korisnik unosi svoje *Qpass* korisničko ime, lozinku i potvrđuje kupovinu.

Posebnost ovog sistema je da se odmah ne tereti račun kreditne kartice, već se svi troškovi sabiraju u vidu jednomesečne transakcije, koja tada ide na račun korisnikove kreditne kartice.

2.5.4.4. P2P plaćanje

Najnoviji vid plaćanja koji se sve više koristi jeste plaćanje P2P. Ovaj vid plaćanja omogućava prenos sredstava između dva pojedinca za razne namene, kao što su plaćanje artikla kupljenog na aukciji, prenos sredstava prijatelju ili slanje poklona porodici.

PayPal je jedna od prvih kompanija koja je ponudila ovaj servis i koja tvrdi da ima oko četiri miliona računa klijenata, da rukovodi sa oko 25% transakcija i da preko svojih sredstava usmerava oko dve milijarde dolara godišnje. Takođe, druge brojne kompanije pokušavaju da ponude ovaj servis korisnicima za online plaćanja.

Potrebno je izvući mišljenje ili pak činjenicu da svi navedeni serveri rade na jedan, gotovo identičan način. Ovo podrazumeva dodeljivanje korisničkog imena, lozinke, davanje podataka o e-mail adresi obezbeđenje servisa sa karticom za plaćanje ili brojem tekućeg bankovnog računa. Tek nakon ove uplate, može se vršiti prenos novca. Nakon unosa korisničkog imena i lozinke, pristupa se svom kompjuteru, a potom se unosi e-mail adresa osobe koja prima novac, zajedno sa dolarskim iznosom koji se šalje. Korišćenjem e-mail servisa poruka se šalje na unetu adresu. Poslata poruka sadrži link na Web stranici odgovarajućeg servera. Klikom miša na link primalac poruke pristupa odgovarajućem servisu. Tada primalac unosi broj računa na koji će se preneti doznačeni iznos sredstava. Ovi servisi omogućavaju primaocu da knjiži novac sa tog računa, da li na svoju karticu ili na bankovni račun, u zavisnosti od želje primaoca.

2.5.5. Elektronski čekovi (*E-čekovi*)

Elektronski čekovi su slični običnim papirnim čekovima, jer sadrže istu informaciju kao i papirni čekovi. Takođe se mogu koristiti svugdje gde se koriste i papirni čekovi, i zasnovani su na istom pravnom okviru i principu korišćenja. Osnovna ideja e-čekova je da elektronski dokument može

zameniti papirni i kriptografski potpis može da zameni ručni. Zajedničke karakteristike papirnog i e-čeka su autorizacija samog čeka, striktno poštovanje instrukcije čeka i izdaju ih iste finansijske institucije. Za razliku od papirnog čeka, e-ček ima autentifikaciju preko digitalnog potpisa i sertifikata, i njegova transakcija mora biti automatski procesuirana.

E-ček ima određene prednosti u odnosu na papirni ček. Upotrebom e-čeka smanjuje se broj papirnih čekova, što dovodi do smanjenja opreme i finansijskog segmenta potrebnih za servisiranje papirnih čekova. E-ček ima svoje sopstvene principe koji su tehnološki napredniji od papirnog i primenjuju se različite vrste plaćanja u poslovnim i drugim transakcijama.

E-čekovi su elektronski platni instrumenti koji se korišćenjem odgovarajućeg softvera izdaju i potpisuju, a putem komunikacionih sredstava upućuju korisniku plaćanja. Konceptijski, oni imaju elektronski oblik i digitalni potpis. Plaćanje e-čekovima ide na sledeći način: u prvoj fazi platilac dobija od emitenta softver i ovlašćenja za izdavanje čekova, u drugoj fazi platilac na osnovu softvera piše ček i šalje ga korisniku, u trećoj fazi korisnik šalje emitentu ček na autentifikaciju i potpis, u četvrtoj fazi, nakon autentifikacije emitent obaveštava korisnika o ispravnosti čeka, u petoj fazi vrši se plaćanje preko banke korisnika za račun korisnik, i u poslednjoj fazi banka korisnika obaveštava svog komitenta da mu je račun odobren.

2.5.6. *Elektronske (plastične/platne) kartice*

Početkom osamdesetih godina prošloga veka kartice su postale uobičajeno sredstvo plaćanja roba i usluga i dostigle su razmere masovne primene. U bankama i organizacijama koje su se bavile kartičnim poslovanjem, za potrebe kartičnog poslovanja, razvijena je tehnološka i računarska infrastruktura koja je opsluživala ovako masovno sredstvo plaćanja.

Bankomati su funkcionisali na bazi kartica, a uvodile su ih samo pojedine banke sa ciljem da smanje troškove šalterskog poslovanja, da stave na raspolaganje korisnicima mogućnost da 24 časa dnevno mogu da podižu novac i da pomoću njih produže vreme odležavanja novca na računima korisnika. U opticaju se nalazio veliki broj različitih kartica. Svaka banka je izdavala ili pokušavala da izdaje svoju karticu, ali se nekoliko svetski poznatih sistema izdvojilo i počelo naglo da se šire i nameću kao standard. To je stvorilo potrebu da se definiše svetski standard, kako bi omogućilo da se kartice jedne banke koriste na bankomatima drugih banaka. U tom periodu pojavio se Internet.

U početku, sama razmena podataka preko Interneta bila je dovoljna za akademsku mrežu i nije bilo potrebe da se bilo šta plaća. Širenjem Interneta i masovnim korišćenjem njegovih mogućnosti javila se potreba da se izvesne usluge plaćaju putem Interneta. U tom trenutku došlo je do spajanja dve različite tehnologije koje su se dopunjavale, a to su Internet i platne kartice.²³ Internet je pružio korisnicima obilje mogućnosti za poslovanje, a kartica je svojom tehnologijom omogućila da se to poslovanje finansijski zatvori i izvrši plaćanje.

²³ Ćirović, Milutin, op. cit., str. 176.

Elektronska tehnologija omogućila je upotrebu elektronskih kartica koje se koriste kao instrument bezgotovinskog plaćanja. Kao izdavaoci ovih kartica pojavljuju se banke, gde jednu karticu mogu izdavati više banaka i u tu svrhu formiraju udruženja (na primer *DinaCard*, *Visa*, *MasterCard*), nebankarske organizacije (*Diners Club*, *American Express*) i velike kompanije, pri čemu izdate kartice važe samo u internim mrežama (najčešći je slučaj da trgovac izda svoju karticu, na primer *M&S Card*, *Wall Mart Card*, *Rodic MB Card*, *C-market20*).

Elektronske kartice kao instrumente plaćanja možemo podeliti prema:

1. Tehnologiji koja je primenjena: kartice sa magnetnom trakom i inteligentne kartice (*smart cards*) sa silicijumskim mikroprocesorskim čipom,
2. Prema vremenu plaćanja i anonimnosti transakcija: debitne kartice, kreditne kartice i kartice sa unapred uplaćenim iznosima novca,
3. Lokaciji primene: nacionalne (važe u zemlji gde su izdate) i internacionalne (važe ravnopravno, kako u zemlji tako i u inostranstvu),
4. Korisniku kartice: osnovnu, dodatnu, poslovnu, i sl.

U 2003. godini i u domicilnom okruženju javljaju se kartice najvećih trgovinskih kuća, a njihova pojava prouzrokovana je ukidanjem mogućnosti korišćenja čeka kao, nezvaničnog, sredstva kreditiranja građana. U uslovima elektronskog bankarstva ove kartice omogućavaju bezgotovinski platni promet u realnom vremenu, putem debitnih kartica i kreditiranje vlasnika kartice, putem kreditne kartice.

Elektronske kartice trenutno obuhvataju dve osnovne tehnologije:

1. Kartice sa magnetnom trakom. Kod ovih kartica podaci se zapisuju na magnetnoj traci koja se nalazi na poledini (PIN vlasnika kartice, njegovo ime, broj računa i drugo). Magnetna traka nema kapacitet za čuvanje velike količine podataka. Upisani podaci podložni su spoljnim uticajima, odnosno mogu biti promenjeni, izbrisani ili oštećeni, slučajno ili namerno. Na ovim kartica moguće je čitanje i upisivanje podataka. Ipak, zbog nedovoljne sigurnosti upisivanje se gotovo ni ne koristi, tako da se ova vrsta kartice može nazvati samo memorijskom. Magnetna traka je raspoređena na tri staze na kojima se vrši upis podataka, i to: prva traka služi za upis broja kartice i imena vlasnika kartice i koristi se samo za čitanje podataka; druga traka služi za upis PIN-a i takođe se koristi samo za čitanje podataka; treća traka služi za upis i čitanje svih ostalih podataka, kontrola i ograničenja, datum važenja kartice, i dr.
2. Kartice sa mikročipom (tzv. inteligentne/pametne/smart kartice) - omogućuju korisnicima da potpuno odvojeno i bezbedno drže veći broj aplikacija na jednoj kartici. Glavna razlika između magnetne i inteligentne kartice je u tome što magnetna traka samo reprodukuje informacije, a smart kartica može da zapiše informacije u sopstvenu memoriju. *Mikročip* u kartici omogućuje automatsko izračunavanje novog stanja novca posle izvršene transakcije. Ova kartica može da služi kao kreditna kartica, debitna kartica, unapred plaćena kartica, lična karta, vozačka dozvola, zdravstvena knjižica i sl. Smart kartica ima oko 100 puta više memorijskog prostora i procesor pomoću koga su

omogućena razna izračunavanja direktno na kartici. To znači da ceo proces (npr. kriptovanje) počinje, traje i završava se na samoj kartici i nikakvi podaci ne napuštaju karticu, što je čini bezbednijom. Smart kartica predstavlja računar u malom, koji uključuje: Procesor (CPU) - pomoću kojeg se vrše izračunavanja, *Read-Only Memory* (ROM) - memorija na kojoj se nalazi operativni sistem, PIN (*Personal Identification Number*) je kod za identifikaciju u elektronskim transakcijama koji se smatra ekvivalentom potpisa klijenta. *Random Access Memory* (RAM) - memorija koja se koristi za privremeno skladištenje prilikom rada procesora, *Electrically Erasable and Programmable Read-Only Memory* (EEPROM) - memorija u kojoj su smešteni podaci (broj tekućeg računa, sertifikat, ključevi i sl), Ulazno-izlazni sklop preko kojeg se komunicira sa okolinom (čitačem).

Proces plaćanja kreditnom ili debitnom karticom uglavnom zahteva četiri strane u svakoj transakciji: vlasnika kartice, trgovca koji prodaje proizvod ili uslugu, kompanije koja vrši obradu plaćanja kreditnom ili debitnom karticom i emitenta kreditne ili debitne kartice.

U izvesnim slučajevima kompanija koja vrši obradu plaćanja kreditnom ili debitnom karticom i emitent kreditne ili debitne kartice mogu biti isti. 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.

S obzirom da klijenti ne moraju da provode puno vremena u čekanju na pružanje usluge, mogu to vreme da iskoriste za obavljanje drugih aktivnosti. Prednosti upotrebe platnih kartica klijenti mogu osetiti i pri plaćanju određenih roba i/ili usluga. Korisnici platnih kartica nemaju potrebu da nose gotovinu sa sobom, s obzirom 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, gotovo „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 autorizacioni centar koji će blokirati mogućnost upotrebe iste. To znači da bi klijenti trebali da uvek pri sebi imaju broj telefona autorizacionog centra da bi bili u mogućnosti da pravovremeno izvrše blokiranje platne kartice.

Bitno je napomenuti, da s obzirom da su platne kartice postale i identifikacione kartice u banci, u slučaju da dođe do istovremenog gubitka platne kartice i lične karte, potrebno je odmah o tome obavestiti i matičnu banku da bi se blokirao tekući račun klijenta. Razlog tome je što se putem informisanja autorizacionog centra sprečava zloupotreba platnih kartica na bankomatima i POS-ovima, dok se putem informisanja matične banke predupređuje mogućnost zloupotrebe na šalteru banke i podizanja gotovine (i dozvoljenog minusa).

Ukratko navedeno, platne kartice predstavljaju zamenu (mnogo komforniju) za gotovinski novac, koje uz obezbeđivanje preduslova od strane poslovnih banaka i pridržavanja propisanih

uslova korišćenja kartica od strane klijenta, mogu i predstavljaju izuzetno sigurno sredstvo svakodnevnog raspolaganja sredstvima na poslovnim računima banaka. U domicilnim uslovima poslovanja, kartice su po ukidanju čekova kao instrumenta kreditiranja (što nikada ček i nije smeo da bude), doživele 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 bankarske ustanove.

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 ili 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.

2.6. Distributivne mreže elektronskog bankarstva

Usled razvoja računarske i telekomunikacione tehnologije došlo je do velikih tehnoloških promena u funkcionisanju banaka, tako da se može govoriti o stvaranju i razvoju elektronskog bankarstva (*e-banking*). Kada se govori o inovacijama bankarskog poslovanja pre svega se odnosi na tehnologiju platnog prometa i transfera novčanih sredstava.

U elektronskom bankarstvu koriste se sledeće distributivne mreže kojima se ostvaruju informacioni i poslovni kontakti sa bankom:

1. ATM sistemi (bankomati),
2. POS sistemi,
3. Telefonsko bankarstvo,
4. PC bankarstvo,
5. SMS bankarstvo,
6. Internet bankarstvo,
7. Mobilno bankarstvo.²⁴

²⁴ Ćirović, Milutin, op. cit. str. 230

2.6.1. ATM sistemi (bankomati)

Prvi korak ka elektronskom bankarstvu je rezultat razvoja informacione mreže koja je omogućila automatizaciju šalterskog poslovanja putem bankomata, odnosno samouslužnih šaltera ATM i POS terminala, s ciljem povećanja kvaliteta usluga banaka i orijentacije prema klijentima.

ATM (*Automated Teller Machine*) predstavlja najrasprostranjeniju formu EFT tehnologije. ATM su mašine koje su dislocirane i povezane u bankarsku mrežu. Pogodnost za klijente je 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 gužva 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. Pored već tradicionalne usluge podizanja gotovine, bankomati omogućuju i upit u stanje računa, polaganje depozita, transfer sredstava sa računa na račun u okviru banke, plaćanje raznih računa, kupovinu prepaid bonova i sl.

Prikaz podizanja gotovine na ATM aparatu možemo dati na sledeći način (uprošćeni prikaz): korisnik aktivira ATM ubacivanjem platne kartice u aparat u deo predviđen za to, ATM traži od korisnika da izabere jezik (uglavnom srpski ili engleski), nakon izbora jezika, korisnik je obavezan da unese svoj PIN (*Personal Identification Number*) koji je vezan uz datu platnu karticu, ATM proverava ispravnost PIN-a, ukoliko je PIN prihvaćen, traži se od korisnika da odabere transakciju koju će izvršiti. U domicilnim uslovima, na bankomatima je moguće obaviti uglavnom dve operacije/transakcije, a to su: upit stanja na tekućem računu građana i isplata gotovine. 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 pokrenu dodatnu opciju za to, po unosu željenog iznosa, ATM vraća korisniku platnu karticu, ATM isplaćuje novac kroz deo predviđen za to, ATM izbacuje listić potvrde na kojem je evidentiran datum transakcije i iznos sredstava koji je klijent podigao.

U početku poslovanja putem ATM-a, posedovanje mreže bankomata bilo je pitanje prestiža među bankama, pa su se banke naprosto utrkivale u razgranavanju sopstvenih mreža bankomata. Kasnije su banke uvidele nesvrishodnost samostalnog razvoja mreža bankomata, pa su otpočeli procesi njihove integracije, pri čemu se dve ili više banaka sporazumevaju o međusobnom korišćenju svojih mreža bankomata. Bankomati su prvobitno radili u *offline* režimu, šaljući podatke o transakcijama grupno u određenim vremenskim intervalima, dok danas većina bankomata radi u on-line režimu, odnosno transakcije se izvršavaju u realnom vremenu.

2.6.2. POS sistemi

EFTPOS/POS sistem (*Electronic Fund Transfer on Point of Sale/Point of service*) je sistem za elektronski transfer novca na mestu prodaje proizvoda ili usluga, koji se ostvaruje povezivanjem maloprodajnog mesta sa mrežom i bazama 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 eminentom kartice.

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 ISDN veze, pri čemu se na licu mesta on-line proverava stanje na računu korisnika

ISDN (*Integrated Services Digital Network* - digitalna mreža sa integrisanim 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.

Povratna informacija na osnovu koje se štampa račun i to po pravilu u dva primerka, s tim što jedan primerak ostaje tražiocu usluge. Često se kod novijih POS-ova zahteva i unos PIN koda od strane kupca, korisnika kartice. U domaćim uslovima poslovanja uglavnom je prisutna vrsta POS terminala koji ne traže unos PIN koda na njima prilikom realizacije transakcije.

Proces plaćanja platnom karticom na POS-u možemo prikazati na uprošćen način:

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 (na primer, *Europlanet*), 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 centri 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,
7. Nakon obrađene transakcije, poslovna banka trgovca ili autorizacioni centar šalje šifru odobrenja (ili odbijanja) POS terminalu prodavcu. 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 emitenu 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.

Tokom zadnje decenije prošlog veka, broj POS-ova je značajno porastao. To znači da danas većina prodajnih mesta prihvataju platne kartice kojima se mogu obavljati plaćanja. 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 se brinu da li klijent ima sredstva na računu, s obzirom da je provera on-line, dok kupac ne mora da piše ček i bezbednije je da ne nosi novac sa sobom.

2.6.3. Telefonsko bankarstvo

Telefonsko bankarstvo predstavlja direktno korišćenje bankarskih usluga od kuće, pošto omogućava neposredan transfer sredstava, informacija i naloga putem telefonske mreže. Zasniva se na takozvanim pozitivnim centrima, ili sistemima kojima se pristupa preko određenih šifri, otkucanih preko tastature. Može se koristiti za proveru stanja i transakcija na računima, otplate zajmova, plaćanje unutar banke, slanje stanja računa na korisnikov fax, naručivanje čekova, plaćanje računa u zemlji i transfera novca. Za ovu vrstu usluge, radi identifikacije, pored šifre može da se koristi i token.

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 i/ili unošenjem PIN-a (lično kreirane lozinke) ostvaruje se pristup operateru. Autentifikacioni tokeni su hardverska ili softverska sredstva koja služe za generisanje jednokratnih lozinki. Hardverski tokeni su lako prenosivi mali uređaji koji proračunavaju lozinku. Korisnik pročita lozinku sa tokena i unosi ga prilikom prijavljivanja na sistem/aplikaciju. Njegova prednost je 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.

Preduslov za uključenje u sistem je da korisnik ima otvoreni 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.

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 izvodu 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).

2.6.4. PC bankarstvo

Kućno bankarstvo je takođe u sprezi sa razvojem internet tehnologije i rada računara. Ono predstavlja tehniku plaćanja koja podrazumeva upotrebu kućnih PC kompjutera koji se nalaze u stanu korisnika, za kontakt sa bankom i obavljanjem finansijskih transakcija.

Iako je u stalnom porastu broj kompjutera po glavi stanovnika, još uvek njihov nedovoljan broj, predstavlja prepreku ovom načinu plaćanja. Kućno bankarstvo je u samom početku omogućavalo dobijanje podataka o stanju na računu koji se vodi kod banke za naručivanje čekova, slanje otpremnica i sl. sa pojavom platnih kartica počele su funkcionisati usluge plaćanja unošenjem broja kartice i PIN koda (skrivenog broja). Za obavljanje plaćanja potreban je elektronski čitač takvih kartica, koji danas predstavlja standardni deo opreme potreban za kućno bankarstvo.

Da bi korisnik izdao nalog za plaćanje, podatke koji su potrebni za plaćanje unosi stavljanjem kartice u elektronski čitač, a zbog autentifikacije, unosi i svoju šifru, odnosno PIN kod. Korišćenjem tehnike kućnog bankarstva, korisnik može platiti usluge i proizvode maloprodavcu, a po potvrdi njegove poslovne banke, da je njegov račun odobren za iznos računa, maloprodavac će isporučiti robu na kućnu adresu potrošača.

Sa pojavom globalne kompjuterske mreže, razvojem interneta, tehnologija kućnog bankarstva je doživela dinamični napredak i postala osnova Internet plaćanja. On-line PC bankarstvo se sprovodi putem Intraneta i predstavlja kombinaciju karakteristika programa za lične finansije i elektronskog plaćanja računa. PC 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. Na taj način klijent može da obavlja transakcije (jedino sa datog računara). Svi podaci o izvršenim nalogima se nalaze na personalnom računaru na kome je instaliran.

Izvod sadrži podatke o obavljenom plaćanju, kao i načinu obavljenog plaćanja i služi kao dokaz o plaćanju u slučaju prigovora od strane korisnika ove usluge banke. Razvoj elektronskog bankarstva uslovio je i pronalazak softvera za lične finansije (*personal finance software*). To je softver koji omogućava da, uz pomoć računara, klijenti vode brigu o svom novcu. Prve verzije softvera za lične finansije pojavile su se još 1983. pod nazivom *Quicken*. Program je doživeo veliki uspeh, pa je brzo dobio konkurenciju u vidu drugih programa, od kojih se u poslednje vreme ističe program Money, kompanije Microsoft. Performanse ovih proizvoda su danas prilično ujednačene. Standardne mogućnosti ovih programa obuhvataju: podsetnik o neizmirenim obavezama, inteligentni registrator računa, programiranje budućih isplata, kalkulator za finansijsko planiranje, kreiranje plana otplate duga, investiranje, pregled portfelja investicija, praćenje berzanskih indeksa, kreiranje različitih vrsta finansijskih izveštaja, finansijski adresar, finansijski savetnik i sl.

Za funkcionisanje PC bankarstva koristi se direktna on-line komunikaciona veza između personalnog računara i računskog centra banke uz korišćenje modema i to preko Intraneta. PC 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 da se olakša upotreba istog postignut je zahvaljujući tome što su na tržište ušle firme kao što su *Intuit* i *Microsoft*, koje imaju 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 (na primer, *Halcom*-ovo rešenje za PC 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.

Za obavljanje bankarskih transakcija u on-line PC bankarstvu potrebno je:

1. Specijalizovan softver koji se ugrađuje na računar klijenta,
2. Klijent može obavljati transakcije samo sa svog računara,
3. Klijent posluje sa bankom koja instalira i održava softver (rede i sa softverskom kompanijom),
4. Klijentovi podaci o obavljenim transakcijama ostaju na hard disku i na bančinom serveru,
5. Neophodan je novac za kupovinu softvera,
6. Potrebno je vreme za instaliranje softvera, kao i vreme za ovladavanje programom.²⁵

²⁵ Vuksanović, Emilija, „ELEKTRONSKO BANKARSTVO“, Beograd, Beogradska bankarska akademija i Institut ekonomskih nauka, 2006., str. 182.

On-line PC bankarstvo ima i određene nedostatke. Korisnik elektronske banke je ograničen da obavlja transakcije samo sa onog računara na kojem je instaliran softver. Pored toga, promena banke zahteva i novi softver i ponovni unos podataka, kao i potrebno vreme za obuku za rad. On-line PC bankarstvo omogućava klijentu da priprema naloge u *offline* režimu, odnosno da priprema i čuva naloge koji će tek kasnije biti realizovani.

Transakcije mogu da se obavljaju neprestano, a izvršenje transakcija u internom platnom prometu je trenutno (između pravnih lica koja su deponenti banke). Moguće je vršiti prenos između svojih računa, plaćanje računa, vršiti pregled stanja na svojim računima, i sl. Putem PC bankarstva klijenti mogu da dobijaju izvode i izveštaje o promenama na računu, po dinamici koja im odgovara. Klijenti imaju mogućnost i da vrše izdavanje naloga sa valutiranjem unapred.

2.6.4.1. Video bankarstvo

Video bankarsko poslovanje iz kuće predstavlja interaktivni sistem koji nudi kvalitetnu i potpunu transformaciju bankarskih usluga. Većina video bankarskih sistema nudi više baznih servisa za plaćanje računa, proveru stanja na računima, transfer sredstava sa računa na račun i sl.

Video bankarski sistemi imaju za cilj da obuhvate kompletan spektar uslužnih servisa, da omoguće pristup ostalim uslužnim servisima, poput kućne kupovine, igre, zabave, informacije o aukcijama, sportskim događajima, informacije o sportskim, kulturnim dešavanjima i dr.

Bitan uticaj na dizajn servisa ima selekcija servisa koji su u ponudi. Da bi korisnik servisa pristupio mreži i uslužnim servisima banke potrebno je da unese PIN kod. Pored opcija koje se nude iz kategorije bankarskog poslovanja od kuće, korisnik može da izabere i druge uslužne servise (vesti, zabava i sl.).

2.6.4.2. SMS bankarstvo

Uvažavajući ubrzani tempo života, banke se opredeljuju da zadovolje potrebu svojih klijenata da bilo kada i bilo gde, brzo i diskretno dobiju korisne i tačne informacije o stanjima njihovih računa. Da bi klijent banke adekvatno mogao da upravlja svojim sredstvima, potrebna je tačna i pouzdana informacija o stanju njegovog računa u banci.

Tradicionalni model pribavljanja ovakve informacije podrazumeva odlazak do šaltera banke ili zvanje odgovarajuće ekspoziture, što iziskuje znatan utrošak vremena i novca. Rešenje za prevazilaženje prostornog i vremenskog ograničenja našlo se pri upotrebi mobilnog telefona i SMS-a. Ukoliko korisnik želi da podatke o svom računu dobija putem kratkih poruka, neophodno je da u organizacionoj jedinici banke koja pruža takvu mogućnost popuni posebnu pristupnicu u kojoj daje podatke o računu i broj mobilnog telefona sa koga će postavljati upite.

Za korišćenje ove usluge potreban je račun otvoren kod banke i bilo koji tip mobilnog telefona. Posle autorizacije i odobravanja pristupnice, klijent banke automatski dobija

pozdravnu poruku na svoj mobilni telefon, koja ga obaveštava da je postao aktivni korisnik ove usluge.

Aktivirana usluga omogućava klijentu u svakom momentu:

1. Proveru stanja na računu, na zahtev, dnevno ili po promeni (gde se definišu parametri priliva na račun pri kojem se dobija adekvatna SMS poruka, podaci o stanju čekova, poslednja promena/transakcija, i sl.),
2. Obavljanje platne transakcije, pri čemu se mogu vršiti plaćanja samo na unapred navedene račune,
3. Uvid u važeću kursnu listu i sl.

Možemo dati uprošćeni primer korišćenja SMS banke od strane korisnika. Primera radi, klijent banke može da vrši upit u stanje svog računa. Potrebno je da korisnik sa svog mobilnog telefona pošalje poruku, na broj servisnog centra banke, koja će sadržavati šifru za proveru stanja računa. Tražene podatke o stanju računa korisnik dobija u obliku poruke na svoj mobilni telefon. Poruka stiže u vrlo kratkom roku, koji varira u zavisnosti od stepena opterećenosti mobilne mreže, ali koji je retko kada duži od jedne minute. Sistem sigurnosti je zasnovan na povezanosti transakcionog računa i broja mobilnog telefona (neke banke koriste i PIN), kao i unapred definisanim i pohranjenim brojevima računa u korist kojih se može izvršiti plaćanje.

Veću zastupljenost SMS bankarstva kod građana možemo pronaći u nekoliko sledećih razloga. Prvi razlog tome je što u apsolutnim brojevima više ima potencijalnih korisnika fizičkih lica, u odnosu na pravna lica. Drugi razlog je što velika preduzeća koja koriste on-line bankarstvo ili Internet bankarstvo imaju on-line uvid u stanje i promene svog računa, pa im usluge ovog vida elektronskog bankarstva nisu toliko neophodne. U prilog tome govori i činjenica da su korisnici SMS banke (pravna lica) uglavnom manja preduzeća koja ne koriste druge vidove elektronskog bankarstva, a imaju potrebu da, po potrebi, provere stanje svog računa ili prate prilive i/ili odlive sa svog računa.

2.6.5. *INTERNET bankarstvo*

Internet bankarstvo predstavlja pribavljanje bankarskih informacija i realizaciju bankarskih transakcija preko Interneta. Internet bankarstvo je zasnovano na korišćenju World Wide Web31-a, gde se korisniku omogućuje direktan pristup putem *web browsera* [32]. 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. Obavljanje Internet bankarstva i pored sličnosti sa PC bankarstvom pretpostavlja određene razlike. Kod Internet bankarstva pristup računu omogućen je putem *browsersa* (pretraživača), što eliminiše potrebu za specijalnim softverom. Internet bankarstvo omogućuje pristup elektronskoj banci sa bilo kog računara u svetu, koji je na neki

način priključen za Internet. Podaci o obavljenim transakcijama nisu uskladišteni na hard disku, pa je i sigurnost veća, a banka održava zaštitu sistema. Transakcije se obavljaju on-line.

U samom početku pojavljivanja banaka na Internetu, banke su se predstavljale samo informativno, i to postojećim ili potencijalnim klijentima. 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.

World Wide Web (www/web) je globalna struktura za brz prenos informacija koja se sastoji iz sledećih elemenata:

1. *Hypertext markup language* (HTML) - za formiranje web stranica i njihovo povezivanje,
2. *Hypertext transfer protocol* (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. Web čitač/pretraživač (*web browser*) je softver za pretraživanje Interneta i čitanje strana na Internetu (npr. *Netscape-Navigator*, *Microsofts Internet Explorer*, *Opera* i dr.). Web bankarstvo ima mnogobrojne prednosti i efekte u odnosu na dosadašnji klasičan poslovni odnos banka-klijent. Prednosti novog načina poslovanja putem web banke su **Error! Reference source not found.:**

1. Mogućnost obavljanja poslova od kuće ili sa bilo koje lokacije u zemlji ili svetu,
2. Ne postoji potreba odlaska na šalter Banke,
3. Ušteda u vremenu (klijent ne traži parking) ili može u svoje slobodno vreme kreirati naloge,
4. Nije potreban specijalan softver i podaci nisu uskladišteni na klijentovom hard disku, što daje veću sigurnost pri obavljanju transakcija,
5. Prostorna neograničenost Internet bankarstva,
6. 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),
7. Nema radnog vremena, odnosno mogućnost obavljanja poslova od strane klijenata sa bankom je 24 časa dnevno,
8. Brzina obavljanja transakcija, koja traje 1-3 minute,
9. Ažurnost obaveštavanja o promenama na računu,
10. Jednostavnost priključivanja na web banku,
11. Klijentu omogućuje tajnost podataka,
12. Lakoća upotrebe.

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 doživele 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 prožima 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 trebale 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.

Kao primer Internet bankarstva u domicilnim uslovima može poslužiti web banka *Erste bank* pod nazivom *NovoNet*, koje u osnovi predstavlja *Halcom*-ovo rešenje. *Erste bank* pruža uslugu web, odnosno Internet bankarstva, koja je namenjena fizičkim licima klijentima *Erste bank*. Putem ovog savremenog vida poslovanja, *Erste bank* 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.). Klijentima *Erste bank* 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 primaocima za koje korisnici iskažu 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 neovlašćene osobe, 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 računaru postoji čitač kartice.

Pored navedenog, upotrebom smart kartice se mogu obavljati plaćanja primaocima koje nije potrebno prethodno registrovati. Jedini problem za sve korisnike web bankarstva može nastati što 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.

2.6.6. Mobilno bankarstvo

Mobilno bankarstvo omogućava transakcije putem prenosnih računara (*laptop*), digitalnih ličnih organizatora (PDA) i mobilnih telefona, koji su opremljeni specijalnim softverom za mobilni pristup Internetu, pa se mogu koristiti za obavljanje svih vrsta usluga i transakcija. Mobilna plaćanja putem mobilnih telefona (*Mobile payments/M-payments*) spadaju u grupu plaćanja na malo. Mobilni telefoni mogu biti uređaji kojima se obavlja plaćanje u sadejstvu sa drugim uređajima (na primer, kao što je slučaj kod plaćanja mobilnim telefonom na POS terminalima) ili se plaćanje može obaviti samo upotrebom mobilnog telefona²⁶. Učesnici u mobilnim plaćanjima su mobilni operateri, banke i druge finansijske institucije, trgovci i potrošači. Broj ljudi koji koriste mobilni telefon za obavljanje plaćanja se brzo povećava.

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).

Broj korisnika bežičnih načina plaćanja proporcionalno raste u svim razvijenim zemljama sveta. Sa samim razvojem usluge mobilne telefonije i njihovim pojeftinjenjem ovaj medij prevashodan za komunikaciju počinje da poprima uloge medija za transakcije i komunikaciju ne samo sa finansijskim institucijama, već i sa maloprodajnim objektima. 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 Internet-a, pristupe svom računu u banci. Konekcija sa bankom se ostvaruje putem mobilnog telefona koji u sebi ima ugrađen WAP uređaj. Da bi se mogla koristiti ova usluga bilo koje banke, korisnik mora da ima prilagođen WAP uređaj (mobilni telefon). Pri svemu tome korisnik jedino plaća utrošene impulse operateru mobilne telefonije.

²⁶ Bjelić, Predrag, „MOBILNI TELEFON KAO KANAL ELEKTRONSKOG POSLOVANJA“, *Ekonomski anali*, 2001, vol. 44, iss. 151-152, str. 95

Uskoro će se *mPay* koristiti i pri plaćanju komunalnih (režijskih) računa, kao i za kupovinu putem Interneta. Do sada je niz komunalnih preduzeća izrazilo interes za uključivanje u *mPay* uslugu. U drugoj fazi, *mPay* usluga omogućiti će i korišćenje niza bankarskih usluga putem mobilnog telefona, koristeći samo mobilni telefon.

Prednosti mobilnog bankarstva:

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 posve 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 konektuje 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.).

3. CASE STUDY U EURO BANCI

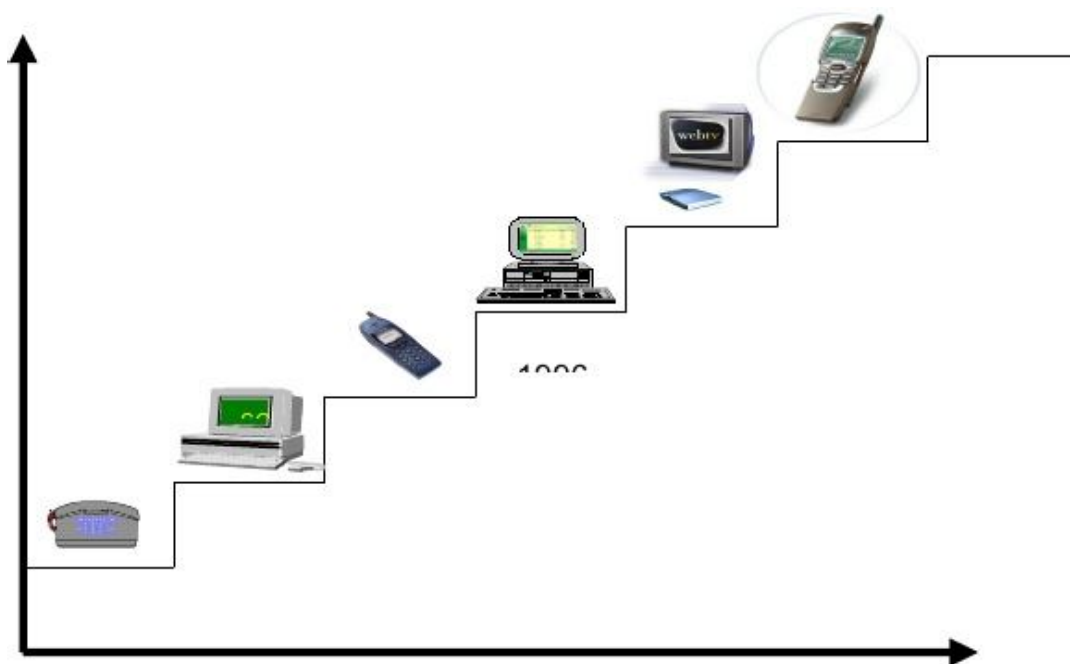
EFG Group je međunarodna bankarska grupacija, koja je u sastavu kompanije *Eurobank Financial Group EFG* (Luksemburg) SA. Grupa je sastavljena od dve i odvojene podskupine, od kojih svaka ima svoj upravni odbor, menadžment, poslovni i geografski opseg, i pod-konsolidovani regulatorni nadzor:

- EFG International, globalna privatna bankarska grupa prisutna širom sveta koja se bavi privatnim bankarstvom i upravljanjem sredstvima, sa sedištem u Cirihi, Švajcarska, koja je kotirana kao EFGN na švajcarskoj berzi (SIX Swiss exchange) i njena direktna matična kompanija *European Financial Group SA*, sa sedištem u Ženevi koju nadgleda švajcarska FINMA.
- *Eurobank EFG*, koja je jedna od najvećih bankarskih grupacija u Grčkoj, kotirana na atinsko berzi (EUROB), nudi sve vrste bankarskih proizvoda, upravljanje sredstvima, osiguranje i ostale usluge u celoj Grčkoj, ako i u centralnoj, istočnoj i jugoistočnoj Evropi, Londonu i Luksemburgu, nadgledana na konsolidiranoj osnovi od strane Banke Grčke.

Elektronsko poslovanje je posao na duge staze. Nije dovoljno samo primeniti novu tehnologiju. Potrebno je napraviti i mnoge organizacione promene, napraviti novi model poslovanja.

Elektronsko poslovanje na Internetu kreće od »Web sajta« - prezentacionog karaktera. U sledećoj fazi to je *E-business*, kupovina i prodaja, zatim se proširuje deljenjem informacija i prerasta u inteligentni *e-business »end to end«* poslovni proces.

Elektronsko poslovanje uglavnom podrazumeva poslovanje preko računara, ali daljim širenjem mobilne telefonije sve više poslovnih transakcija odvijaće se preko mobilnog telefona. Prema prognozama *Gartner Group*, 2004. Godine bar 40% B2C elektronske trgovine odvijaće se preko inteligentnih mobilnih telefona korišćenjem bežičnog aplikacionog protokola (WAP – *Wireless Application Protocol*)



Ilustracija 19 . Elektronsko poslovanje

Modeli plaćanja u Internet poslovanju

Dva osnovna modela plaćanja su:

- *Cash-like*, sistem koji podrazumeva pretplatu. U ovakvim sistemima određena suma novca se uzima od kupca pre nego što je trgovina obavljena. U ovu grupu spadaju:

- *Smart card*,
- elektronski keš i
- bankarski čekovi.

Check-like, sistem kod koga se plaćanje obavlja u trenutku kupovine (*pay-now*) ili po obavljenoj kupovini (*pay-latter*). Primer za *pay-now* grupu su bankomati (ATM – *Automated Teller Machine*), a za *pay-latter* je primer plaćanja kreditnim karticama.

3.1. Istorijat bankarstva – Eurobanka

Kompanija je osnovana 2005. godine, kao firma za pružanje konsultantskih usluga iz oblasti nekretnina. Kao članica EFG Grupe, Eurobank EFG danas predstavlja glavnog klijenta naše kompanije. EFG Property Services je uspeo da razvije značajan portfolio klijenata uključujući banke, javne institucije, investicione fondove, strane investitore, lokalne firme za realizaciju nekretnina i ostale kompanije.

EFG Property Services je prisutna u sektoru usluga nekretnina u Srbiji. Njihov tim stručno zaposlenih svojim bogatim iskustvom, pružaju celokupne profesionalne usluge visokog kvaliteta u oblasti poslova sa nekretninama, kako za Grupu Eurobank EFG, tako i za treća lica. Privredno društvo zauzima ugledno mesto među vrhunskim proceniteljima nekretnina zbog toga što realizuje preko 5,000 procena godišnje. Ta činjenica doprinosi snazi u drugim sektorima kojima se bavimo, kao na primer, posredovanje (pružamo kompletne brokerske usluge kod prometa nekretnina ili zakupa), savetodavne usluge, istraživanje tržišta, tehničko održavanje i upravljanje objektima, kao i upravljanje sredstvima. EFG Property Services izuzetno poznaje tržište nekretnina u Srbiji, kao i u drugim zemljama Nove Evrope preko lokalnih filijala.

EFG Property Services se bavi sledećim poslovima:

- Savetodavne usluge
- Istraživanje tržišta
- Procene
- Posredovanje
- Upravljanje nekretninama i objektima
- Nekretnine u privredi
- Upravljanje sredstvima u oblasti nekretnina
- Tehničke usluge
- Nekretnine Grupe

Cilj EFG Property Services je da ojača svoju vodeću poziciju u sektoru usluga u oblasti nekretnina, na liniji potpune orijentacije na svoje klijente. Osnovni princip privrednog društva je da stvara i razvija dobre dugoročne odnose sa klijentima, kako u sektoru stanovništva tako i privrede, pružanjem visoko kvalitetnih integrisanih usluga. Uspešna kompanija i njeno poslovanje stvaraju produktivnu radnu klimu gde proističu veštine, inicijative i neprestana evolucija na ličnom planu. Razne procedure i poslovi baziraju se na profesionalnom iskustvu i kvalitetu u skladu sa standardima i principima dinamične bankarske grupe EUROBANK EFG kojoj pripada.

3.2. Eurobanka o Bazel III

Bolji kvalitet kapitala Prvo, Bazel III će značajno povećati kvalitet bankarskog kapitala. Postoji tendencija da se ova ključna karakteristika zanemari jer se posmatrači uglavnom usmeravaju na nivo propisanog kapitala koje zahteva Bazel III. Svakako, sporazum postignut 12. septembra o kalibraciji novih standarda privukao je veliku pažnju i to s pravom. Ali, upravo je sporazum iz jula o projekciji okvira utro put za njegovu kalibraciju. Nova definicija kapitala je u svakom pogledu istog značaja kao povećani nivo kapitala i predstavljala je bitan korak u ovom procesu: imperativ je bio adekvatno definisati kapital pre postavljanja njegovog nivoa. Viši kvalitet kapitala znači veću moć apsorpcije gubitaka, što sa svoje strane znači da će banke biti jače, tako što će im biti omogućeno da bolje podnesu periode stresa. Koji su novi zahtevi za kapitalom? Ključni element je veća usmerenost na ono što se naziva akcionarski kapital, tj.

komponenta najvišeg kvaliteta bančinog kapitala. standardima, kao što znate, banke moraju da drže najmanje polovinu svog propisanog kapitala kao Tier 1 kapital. Ostatak čine druge stavke nižeg kapaciteta apsorpcije. Pored toga, polovina Tier 1 kapitala mora biti akcionarski kapital. Drugi deo Tier 1 kapitala je isto tako visokog kvaliteta u poređenju sa drugim elementima strukture kapitala, ali ne istog kalibra kao obične akcije i zadržana dobit. Oštrije usmerenje na akcionarski kapital znači da okvir Bazela III jače naglašava minimalni zahtev za kapitalom višeg kvaliteta. Dalje, definicija akcionarskog kapitala - poznatog i kao "jezgro kapitala" - sada je strožija. Po sadašnjem sistemu, izvesne vrste aktive spornog kvaliteta već su izuzete iz kapitalne baze (tj. Tier 1 i Tier 2). Po Bazelu III, ova izuzimanja će biti strožija jer će se primenjivati direktno na akcionarski kapital. Ovo predstavlja bitno jačanje definicije dela kapitala banaka najvećeg kvaliteta. I još korak dalje, definicija Tier 1 kapitala je isto tako pojačana da bi uključila akcionarski kapital i druge kvalifikovane instrumente na osnovu strogih kriterijuma. Jačanjem kvaliteta kapitala, Bazel III će voditi suštinskom unapređenju kapaciteta banaka za apsorpciju gubitaka. Po Bazelu II, koeficijenti za minimalne zahteve u pogledu akcionarskog kapitala i Tier 1 kapitala bili su 2% i 4%, respektivno. Prema novoj definiciji kapitala, ovi koeficijenti sada iznose oko 1% i 2%, respektivno, za prosečnu međunarodno aktivnu banku. Nova pravila znače da će, pod istim okolnostima, banke morati da povećaj svoj akcionarski kapital da bi ispunile minimalne zahteve.

Pojačani kapitalni okvir: sa Bazela II na Bazel III

U procentima od rizika ponderisane aktive	Zahtevi za kapitalom						Dodatni makroprudencijalni plašt	
	Akcionarski kapital			Tier 1 kapital		Ukupni kapital		Dodatni kapacitet za apsorbovanje gubitaka za SIFI*
	Minimum	Zaštitni amortizer	Zahtev	Minimum	Zahtev	Minimum	Zahtev	
Bazel II	2			4		8		
Memo:	Jednako oko 1% za prosečnu međunarodnu banku po novoj definiciji			Jednako oko 2% za prosečnu međunarodnu banku po novoj definiciji				
Bazel III Nova definicija i kalibracija	4,5	2,5	7,0	6	8,5	8	10,5	0-2,5 Dodatno teretanje kapitala za SIFI?

Ilustracija 20. Pojacani kapitalni okvir sa Bazela II na bazel III

Kada se ocenjuje stanje e-bankarstva u Srbiji značajno je upoređivanje sa situacijom u ovoj oblasti razvijenim zemljama, sa jedne strane, i sa stanjem u drugim oblastima u zemlji, sa druge strane. U razvijenim zemljama procenat učešća e-bankarstva u platnom prometu je veoma visok. (npr. u Francuskoj 70 i 80%), a u Srbiji je znatno niži (u celini oko 1/3 ili manje kada su u pitanju fizička lica). U odnosu na druge segmente u zemlji, e-bankarstvo je relativno dobro razvijeno, i što je još značajnije, pokazuje tendenciju daljeg intenzivnog razvoja (po vrstama proizvoda i po tehnološkom nivou mogućnosti korišćenja). Do donošenja zakona o digitalnom potpisu interna tela u bankama su vršila samostalno izdavanje odgovarajućih sertifikata zbog

toga što još uvek ne postoji nacionalno sertifikaciono telo za sve servise koji zahtevaju digitalni sertifikat.

Banke su se uspešno uključile u nove sisteme među bankarskih obračuna po svetskim principima: RTGS za prioriteta plaćanja i plaćanja velikih vrednosti i neto sistem za mala plaćanja. Organizovale su preuzimanje žiro računa preduzeća i obavljanje poslova platnog prometa, pružajući viši nivo i kvalitet usluga, uz afirmaciju koncepta "u susret klijentu". Postojeće osnovne informacione sisteme ("*core-banking*") sada nadograđuju sa novim slojem aplikacija za podršku elektronskom poslovanju sa privredom i stanovništvom.

Trenutna IT infrastruktura nije nerazvijena. Kod jednog dela populacije postoji interesovanje za proizvode e-bankarstva i e-novca. Kod drugog dela stvar je još uvek na relaciji gotovina-račun u banci uz prisustvo otpora i nepoverenja.

Asortiman ponude e-bankarstva se drastično širi u kratkom vremenskom periodu. Preko kućnog PC ili mobilnih telefona banke svojim komitentima 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 mogućnost korišćenja usluga platnog prometa putem bankomata (CDs i ATM) [7] platnih kartica, POS terminala Banaka, Call Centra i mobilnih telefona (SMS).

Sa uvođenjem ATM i POS terminala počinje primena platnih kartica sa tendencijom značajnog povećavanja u pogledu obima i asortimana. Ponuda banaka je još uvek ispred tražnje. Jedna banka ima u ponudi međunarodno važeće kartice (*Visa, Diners, Master...*), ali u ovom trenutku one u Srbiji mogu da se koriste samo za bezgotovinska plaćanja, dok za Internet plaćanja mogu da se upotrebljavaju samo u inostranstvu (nedostaju nam odgovarajući lokalni centri za procesiranje ovih transakcija). Drugi pravac aktivnosti usmeren je na razvijanje sistema i širenje prijemne mreže nacionalnih kartica (YUBA i *DinaCard*).

Suština nudjenja 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 korisnih usluga e-bankarstva, što je dobrim delom rezultat stečenih iskustava korišćenjem "udaljenog ulaza" preko terminala iz svojih kancelarija kad su radile preko ZOP-a. Za male firme e-bankarstvo postaje sve atraktivnije, jer baš zato što su male mogu niz poslova da obavljaju ne napuštaju svoje radne prostorije, a imaju neprekidno uvid u stanje svog računa.

Razlozi zbog kojih se banke pojavljuju /rade/ na Internetu su sledeći:

- Stvaranje imidža inovativne firme, koja je u stanju da svojim korisnicima ponudi najsavremenija tehnološka rešenja.
- Bolje i veće interaktivne mogućnosti. Za banku koja se u tržišnim uslovima bori za svakog svog komitenta, najvažnija je komunikacija sa njim. U klasičnim uslovima banka je mogla da komunicira samo dok je trajalo radno vreme, ili preko nekog informativnog

šaltera koji bi radio neprekidno. Ovakav način poslovanja stvarao je ograničenja u komunikaciji. Interaktivne mogućnosti komuniciranja preko Interneta su praktično neograničene i samo je pitanje do kog nivoa banka ima interesa da se angažuje.

- Mogućnost racionalizacije potencijala banke. Banka prenošenjem određenih servisa na Internet redukuje troškove poslovanja, jer ne mora— za povećanje broja komitenata, da otvara novi poslovni prostor, da ga oprema i zapošljava nove službenike. Ovo je posebno interesantno za one geografske regione gde banka nema mrežu ekspozitura ili ima mali broj komitenata. Sa Internetom banka može da pokrije znatno veći geografski prostor ne otvarajući nove ekspoziture. Veliki broj informacija koje banka može da stavi svojim korisnicima na raspolaganje u principu nisu dostupni širem krugu njenih korisnika. To se odnosi na mogućnosti plasmana i kreditiranja po najpovoljnijim uslovima, inostrana plaćanja, savetodavne funkcije i dr.
- Samouslužno bankarstvo je korisno, podjednako i za banku i za korisnika, jer korisnik ima servise 24 časa dnevno, 7 dana u nedelji, a banka bez povećanja broja zaposlenih radi 24 časa dnevno.

3.3.Pristupi upravljanja bankarskim rizicima u skladu sa Bazel II

Prema Bazel II standardima od banaka se zahteva da imaju koeficijent kapitala (KK) od 8%, minimalno, pri čemu se dati pokazatelj izračunava prema sledećoj formuli:

$$KK = \frac{\text{propisani kapital banke}}{\text{rizikom ponderisana aktiva}}$$

Kreditni rizik predstavlja najznačajniji rizik kome je banka izložena u svom poslovanju. Moglo bi se reći da je ovaj rizik star koliko i samo bankarstvo, jer pozajmljivanje novca drugoj ugovornoj strani uvek je sa sobom nosilo opasnost da pozajmljena sredstva neće biti vraćena. Još tada je prepoznata potreba za upravljanjem ovim rizikom kako bi se sprečile negativne posledice po bankarski posao, te su u skladu sa tim preduzimane različite aktivnosti. Naravno stepen složenosti mehanizama kojima se upravljalo kreditnim rizikom tada bio je daleko jednostavniji nego što je danas. Kompleksnost upravljačkih sistema nametnula se kao neophodnost u uslovima kada se finansijsko tržište razvija velikom brzinom, kada se kreiraju novi instrumenti i bankarski proizvodi itd. Cilj je da se na adekvatan način kontroliše izloženost riziku i prate sva eventualna pogoršanja kao i da se preduzmu preventivne mere kako bi se nepovoljne situacije sprečile.

Najbolji primer o tome šta se dešava kada se relaksiraju kriterijumi te samim tim poveća verovatnoća realizacije kreditnog rizika je upravo velika kriza na hipotekarnom tržištu kredita u SAD (u čijem izvoru se jednim delom nalazi i ovaj rizik) koja je poprimila ogromne srazmere i proširila se i na ostatak sveta.

Definicija

Kreditni rizik se definiše kao verovatnoća da banka neće biti u stanju da naplati svoja ukupna potraživanja od klijenta, kako po osnovu glavnice tako i po osnovu svih pripadajućih kamata.

S obzirom na konkretan izvor nastanka kreditnog rizika možemo da razlikujemo tri tipa ovog rizika: rizik naplativosti (*default risk*), rizik kreditne premije i rizik pogoršanja kreditnog rejtinga. *Rizik naplativosti* je rizik koji postoji još u trenutku kada je kredit odobren odnosno instrument emitovan, jer već tada svaki klijent/emitent ima neki kreditni rejting, a svakom rejtingu moguće je pripisati određenu verovatnoću *default*-a odnosno neizvršenja. *Rizik kreditne premije* je rizik da će se kreditna premija promeniti i uticati na pogoršanje performansi klijenta/emitenta, te potencijalno stvoriti probleme u otplati kredita. *Rizik kreditnog rejtinga* je rizik da će doći do pogoršanja kreditnog rejtinga klijenta u periodu kada je kredit aktivan tj. u periodu njegove otplate.

3.3.1. Tržišni rizik

Tržišni rizik predstavlja rizik nepovoljnih devijacija tržišnih vrednosti hartija od vrednosti u portfoliju banke koje su uzrokovane kretanjima tržišnih parametara, u periodu posedovanja hartija. Realizacija ovog rizika se ogleda u smanjenju vrednosti bankarskih pozicija. Kao što je već rečeno ključni parametri koji utiču na data kretanja su kamatne stope, indeksi, devizni kursevi, cene bazičnih roba...

Bazel II standardima tržišni rizik se definiše kao rizik gubitaka u bilansnim i van bilansnim pozicijama koji nastaje iz kretanja tržišnih cena.

Definisane su i dve grupe:

1. rizici sadržani u instrumentima vezanim za kamatnu stopu i vlasničke uloge u knjizi trgovanja
2. devizni rizik i robni rizik širom banke.

Najznačajniji faktor u upravljanju tržišnim rizikom je period držanja ili period u kom banka ima otvorenu poziciju na nekoj aktivu. Rok dospeća finansijskih instrumenata u ovom slučaju nije od naročitog značaja u postupku upravljanja rizikom iz razloga što je bilo koju hartiju od vrednosti, teoretski, moguće prodati na sekundarnom tržištu pre roka dospeća ili je moguće izvršiti hedžing. Uglavnom period držanja zavisi od tipa instrumenta. Kod deviznih kurseva radi se o periodu od jednog dana, dok je kod derivata to mnogo duže (nekad se izražava i u mesecima). Jasno je da što je to vreme duže to je i izloženost delovanju ovog rizika veća. Regulatorne vlasti imaju u svojoj nadležnosti određivanje optimalnog perioda držanja pojedinih pozicija kako bi se na adekvatan način upravljalo ovim rizikom.

Banka može biti izložena dejstvu tržišnog rizika kod sledećih pozicija:

1. obveznice sa fiksnom i fleksibilnom kamatnom stopom,
2. akcije,
3. derivati sa različitim aktivom u njihovoj osnovi - akcijama, obveznicama, fjučersima itd. i
4. transakcije koje su na neki način povezane sa deviznim kursovima.

U osnovi je moguće razlikovati dva tipa tržišnog rizika:

A. *sistematski tržišni rizik* - uzrokovan je odlukama o ekonomskoj politici neke zemlje i pogađa sve finansijske instrumente na tržištu i

B. *specifični tržišni rizik* - rizik promene vrednosti pojedinačne hartije od vrednosti, koji zavisi od poslovne aktivnosti i rezultata subjekta koji je izdao datu hartiju.

Tržišni rizik se često prepliće sa rizikom likvidnosti i operativnim rizikom. Kretanje cena hartija od vrednosti u velikoj meri zavisi od stepena likvidnosti tržišta. Ako je tržište slabo likvidno, vrlo je teško pronaći drugu ugovornu stranu i samim tim volatilnost cena je veća nego u uslovima visoke likvidnosti tržišta. Drugim rečima rečeno, na tržištima sa manjim stepenom likvidnosti tržišni rizik je izraženiji. Kada je u pitanju veza sa operativnim rizikom klasičan primer su defekti u praćenju portfolija i donošenju odluka o upravljanju portfoliom koji mogu dovesti do značajnih gubitaka. Jedan od najpoznatijih primera u istoriji bankarstva i finansijskih tržišta je slučaj Barings Bank i Nick Leeson-a. Gubici koji su nastali u ovom slučaju duguju se padu cena, ali je u pozadini svega stajalo nepoštovanje procedura.

3.3.2. Operativni rizik

Operativni rizik predstavlja rizik koji se javlja usled grešaka ili nepredviđenih događaja nastalih u toku izvršavanja poslovnih aktivnosti kompanija. Izvori ovog rizika mogu biti vrlo široki: prevara, pravni rizici, okruženje, teroristički napadi...

U menadžmentu rizika se obično govori o tri grupe rizika: kreditni, tržišni i operativni. Dok se sa prva dva rizika upravlja u okviru sektora finansija, poslednji je uglavnom vezan za centralizovano upravljanje, ali može biti i rasprostranjen na nekoliko odjeljenja poput IT odeljenja koje vodi računa o riziku informacionih tehnologija ili HR-a koji se stara o riziku ljudskih faktora.

Definicija

Prema Bazel II standardima operativni rizik se definiše kao rizik od gubitaka koji proističe iz neadekvatnih ili neuspešnih internih procesa, ljudi i sistema ili spoljnih događaja. Zakonski rizik je uključen takođe, dok strateški i reputacioni pripadaju drugoj klasi.

Bazel II standardima predloženo je sedam kategorija u koje je moguće rasporediti sve potencijalne izvore operativnog rizika. Reč je o sledećim stavkama:

1. interna obmana (pronevera aktive, izbegavanje poreza...);
2. eksterna obmana (krađa informacija, krađa trećih lica, falsifikovanje, štete tehničkih aktivnosti...);
3. pravila eksploatacije zaposlenih (*employment practices*) i sigurnost radnog mesta (diskriminacija, zdravlje i sigurnost zaposlenih...);
4. klijenti, proizvodi i poslovna praksa (tržišno manipulisanje, defekti proizvoda, nedopuštena trgovina...);
5. štete na fizičkoj aktivi (prirodne katastrofe, terorizam, vandalizam...);
6. poremećaji u poslu i radu sistema (poremećaji u radu softvera i hardvera) i
7. izvršavanje, isporuka i upravljanje procesima (greške u unosu podataka, računovodstvene greške, izostanak obaveznog izveštavanja...).

Pristupi merenju

Banke imaju obavezu da iz svog kapitala izdvajaju odgovarajuće iznose sa ciljem prevencije od potencijalnih rizika. Izračunavanje iznosa kapitala koji je obavezan za držanje se vrši prema jednom od sledećih metoda:

1. pristup osnovnog indikatora,
2. standardizovani pristup i

3. viši pristupi merenja (*Advanced Measurement Approaches* - AMA).

Bankama se predlaže da postepeno uvode različite metode u skladu sa njihovim tehničkim mogućnostima i praksom. Pri tome jasno su definisani kriterijumi pod kojima drugi i treći pristup mogu da se koriste. Ipak, od međunarodno aktivnih banaka i banaka sa značajnim izloženostima operativnom riziku se očekuje da će da koriste sofisticiranije pristupe (da će nastojati da ne koriste pristup osnovnog indikatora) koji će odgovarati profilu rizika kome pripada institucija tj. konkretna banka. Predviđeno je da banka može da koristi pristup osnovnog indikatora ili standardizovani pristup za jedan deo svojih aktivnosti, dok će za ostatak koristiti AMA pod uslovom da ispuni odedene minimalne kriterijume.

Jednom odabran prelazak na napredniji način merenja kapitalnih izdvajanja ne dozvoljava vraćanje na jednostavniji način bez prethodne dozvole supervizora. Naprotiv, supervizor ima pravo da zahteva od banke da se vrati na jednostavniji metod merenja ukoliko ustanovi da više nisu ispunjeni kvalifikujući kriterijumi. Ovaj zahtev ostaje na snazi sve dok se ponovo ne steknu uslovi za povratak banke na prethodno korišćen metod.

3.3.3. *Value at Risk*

Value at Risk (VaR) je mera rizika koja se danas najčešće koristi za potrebe izražavanja tržišnog rizika. U novije vreme je susrećemo i kao moguću metodu kod merenja operativnog rizika, mada u ovom segmentu još uvek nije zaživela u potpunosti.

U ranijem periodu upravljanje rizicima se svodilo na jednostavno postavljanje limita npr. u pogledu broja otvorenih pozicija ili dozvoljenog gepa u ročnosti finansijskih instrumenata. Vremenom je ovakav način kontrole postao neefikasan na više polja. Naime, granice su tehnički stvarale mogućnost smanjenja rizika na jednoj strani, ali povećanje na drugoj. Takođe, nekada je poželjan rizik eliminisan iz razloga probijanja dozvoljenih limita. Smatra se da je najveći problem bio u tome što nije postojala konzistentna politika po pitanju određivanja limita i iznosa potencijalnog gubitka koji se toleriše. Ustanovljeno je da za potrebe menadžmenta nije bitna struktura pozicija kojima se raspolaže već samo gubitak koji bi mogao biti rezultat sastava konkretnog portfolija, kao i verovatnoća nastanka tog gubitka. Drugim rečima rečeno, od ključnog značaja za menadžment je raspored verovatnoće gubitaka u knjizi trgovanja. U nastojanju da se obezbedi adekvatna mera koja bi na neki način uvažavala raspored verovatnoće, nastala je ideja o *Value at Risk* modelima.

VaR kao mera predstavlja ocenu mogućeg gubitka u portfoliju sa fiksnim učešćem pozicija u određenom vremenskom periodu sa određenim stepenom poverenja. Pri tumačenju prethodne definicije treba biti vrlo obazriv i obratiti pažnju na nekoliko stvari:

1. VaR je samo *ocena* mogućeg gubitka, što znači da se utvrđuje na bazi statističkih metoda i modela, uz postavljanje određenih pretpostavki o stohastičkim procesima kojima se opisuje kretanje veličina na tržištu kao i o rasporedu verovatnoće prinosa finansijskih instrumenata;
2. učešće pozicija u portfoliju je *fiksno*, što znači da nam VaR daje mogućnost samo da procenimo potencijalni gubitak ukoliko struktura portfolija ne bude menjana;
3. VaR se uvek računa s obzirom na neki vremenski period i onda nam sama vrednost govori o potencijalnom gubitku u datom vremenskom horizontu;
4. budući da je u pitanju ocena koja se računa sa određenim stepenom poverenja o procenjenom gubitku možemo govoriti samo kao o potencijalnom, nikako ne možemo reći da je to cifra koja nam pokazuje koliki je maksimalno moguć i to siguran gubitak.

Dakle, pogrešno je tvrditi da ako dnevni VaR iznosi € 1 milion (uz postavljeni stepen poverenja od 95%) onda je maksimalno mogući gubitak u narednom danu konkretne institucije upravo € 1

milion. Maksimalno mogući gubitak je ukupna vrednost portfolija date institucije, samo što je verovatnoća nastanka takvog događaja zanemarljivo mala. Jedino što možemo tvrditi na bazi dobijene mere jeste da u 95% slučajeva gubitak institucije narednog dana neće premašiti iznos od € 1 milion. Ako je model koji je usvojen za računanje korektan to znači da je moguće da se u 5 od 100 dana desi gubitak veći od vrednosti dnevnog VaR-a.

Kao što se može primetiti koncept VaR-a počiva na nekoliko pretpostavki, čije ispunjenje je diskutabilno i na čiji račun se odnosi većina kritika ovog pristupa. Pojasnićemo neke od njih.

Prva pretpostavka se odnosi na oblik stohastičkog procesa za koji verujemo da se nalazi u osnovi kretanja ključnih vrednosti na finansijskim tržištima tj. cena i/ili prinosa. Utvrđivanje oblika stohastičkog procesa i određivanje njegovih parametara nije jednostavno. Cilj je doći do modela koji najbliže opisuje realno stanje stvari. Pojedine varijante modela polaze od pojednostavljenih pretpostavki koje u praksi nisu zadovoljene (analitički metod pretpostavlja da su prinosi normalno raspoređeni).

Druga pretpostavka se odnosi na fiksna učešća finansijskih instrumenata u portfoliju za koji se računa VaR. Ovo je moguće tvrditi samo u slučaju kratkih vremenskih intervala, dok je sa produženjem horizonta za koji se VaR računa ova pretpostavka praktično nezadovoljena. U takvim situacijama mora se dodatno definisati tretman pozicija koje u zadatom vremenskom periodu dospevaju kao i pravila trgovanja.

Modeli za merenje VaR-a

Postoji više modela koji mogu biti primenjeni kako bi se došlo do ocene VaR-a, a tri osnovna su:

1. Analitički model ,
2. istorijski model i
3. *Monte Carlo* simulacija.

Pored navedenih varijanti postoji veliki broj mogućih prilagođavanja kako bismo što bolje postavljenim modelom opisali stvarno stanje. Na primer, jedno od mogućih prilagođavanja jeste uvođenje pretpostavke varijanse prinosa (ovo znači da varijansa nije konstantna tokom vremena, već se menja na određeni način). Upravo u zavisnosti od toga kako utvrdimo zakonitost koju prati ovaj parametar postojaće više varijanti na koje se možemo osloniti pri izračunavanjima VaR-a.

U izgradnji znanja koja se vezuju za ovu oblast krenućemo najpre od jednostavih modela za koje je bitno uočiti suštinu kako bismo lakše mogli razumeti naprednije tehnike koje se koriste. Stoga počinjemo sa analitičkim modelom.

Stub 1 Bazel-a II definiše minimalne kapitalne zahteve za kreditni, tržišni i operativni rizik.

Ovaj stub pokušava da odgovori na glavno pitanje koje je cela Bazel II standardizacija postavila ispred sebe: kako računati stopu minimalne adekvatnosti kapitala banke?

Stopa minimalne adekvatnosti kapitala banke je zapravo količnik ukupnog kapitala i rizikom ponderisane aktive i razlog je razvijanja novih načina za preciznije merenje rizika.

Stub 1 Bazela II postavlja standarde za izračunavanje brojioca (struktura kapitala koja se priznaje kao adekvatna) i imenioca (ponderi rizika koji se primenjuju na sve bankarske plasmane).

Pre pojave Bazela II gotovo svi plasmani su se smatrali jednako rizičnim. HOV najvišeg i najmanjeg rejtinga su posmatrane kroz istu prizmu, što je dovodilo do arbitraže. U okviru istog pondera rizičnosti, javljale su se više i niže rizične HOV. Posledica toga je reanžiranje portfolia aktive banke u korist rizičnijih plasmana jer one, po pravilu, donose viši prinos za jednake troškove kapitala.

Bazel II podstiče umesto jednoobraznog, kakav je do sada bio, **fleksibilan** način izračunavanja kreditnog rizika, na osnovu čega bi svaka banka koristila metod koji odgovara njenom portfoliju, preferencijama rizika i tržištima koje zauzima.

Aktivna strategija upravljanja portfolijom dovodi do biranja najprofitabilnijih plasmana za zadati nivo rizika, i shodno tome, nivo adekvatnosti kapitala. Što napredniji pristup banka koristi za merenje rizika (AIRB), imaće manje kapitalne zahteve uz nesmanjeni prinos.

Neka istraživanja su pokazala da bi potpuna primena Bazel II standarda zasnovana na procenama konkretnih rizika plasmana, dovela do pada minimalne zahtevane stope kapitala u proseku za 1,2%, što definitivno ide u prilog razvijanju složenijih internih modela praćenja rizika.

Stub 2 Bazela II postavlja kvalitativne uslove za upravljanje rizicima i izračunavanje adekvatnosti kapitala. Bazira se na sledećim principima:

1. princip interne procene adekvatnosti kapitala (ICAAP),
2. princip supervizije (SREP),
3. kapital iznad minimalnog nivoa i
4. intervencija supervizora.

Proces upravljanja rizikom treba da bude kontinuiran i sveobuhvatan. Od supervizora se očekuje da proceni u kojoj meri banke dobro ocenjuju svoje potrebe za kapitalom.

Posle procene, ukoliko je neophodna, sledi intervencija. Naravno, ona je pre svega usmerena na jačanje internih kontrola, preispitivanje procedura i metoda za upravljanje rizikom. Znači, uloga supervizora ide mnogo dalje od postavljanja pravila i sankcija za nepoštovanje istih. Supervizor i banka treba da kontinualnom saradnjom i komunikacijom omoguće prevenciju pada kapitala ispod potrebnog nivoa. Zajedno, uz poštovanje unapred utvrđenih pravila.

Konstantnim nadzorom, supervizor će se vremenom intenzivnije fokusirati na one banke i/ili konkretne delove banaka sa rizičnijim profilom rizika.

Supervizor će svakako obrati pažnju i na faktore rizika koji nisu u celini obuhvaćeni pri računanju stope adekvatnosti kapitala. To su, uglavnom, faktori koji su eksterni za banku, a tiču se opšteg stanja privrede: cikličnost privrede, poslovni rizik, rizik kretanja kamatne stope. Za upravljanje eksternim rizicima, standardizacija kroz pravila i procedure je limitirana. Zato će se na njih obratiti posebna pažnja, kako u smislu sankcija, tako i u smislu davanja smernica kako da banke "predvide nepredvidivo", i svedu rizik na najmanju moguću meru.

3.4. Osnovni pojmovi vezani za sigurnost podataka Euro banke

"Smart" kartica

Ukoliko klijent želi da vrši plaćanje sa računa firme neophodno je da u okviru *e-banking* paketa poseduje tzv. "smart" karticu koja služi za elektronsko potpisivanje naloga.

"Smart" kartica je iste veličine i oblika kao i bilo koja kreditna kartica (Master, Diners, Dina itd.), ali umesto magnetne trake koja sadrži podatke o vlasniku kartice, a koja se nalazi na poleđini kreditne kartice, poseduje utisnut mikroprocesor (čip) radi uskladištenja i obrade elektronskih podataka ili aplikacija. "Smart" kartice predstavljaju trenutno najviši oblik tehnološkog razvoja i bezbednosti u kartičarstvu.

"Smart" kartica se dostavlja korisniku pripremljena da se na nju upiše digitalni sertifikat, neophodan kod elektronskog potpisivanja naloga za plaćanje.

Digitalni sertifikat

Digitalni sertifikat se kreira korišćenjem matematičkih funkcija, šifrovan je i predstavlja sažetu verziju originalnih podataka.

To je vrsta "elektronske" lične karte koju dodeljuje nezavisno sertifikaciono telo kojim se potvrđuje identitet korisnika smart kartice, sa ciljem da se licu koje prima poruku omogući da dešifruje sadržaj poruke.

Svrha korišćenja digitalnog sertifikata jeste obezbeđivanje sigurnosti kod plaćanja.

Digitalni sertifikat se "upisuje" na karticu na način opisan u uputstvu koje korisnik dobija na mini CD-u u okviru paketa za *e-banking*.

Digitalni potpis

Digitalni potpis predstavlja elektronski potpis koji se koristi za autentifikaciju identiteta pošiljaoca poruke, ili potpisnika dokumenta. Takođe se koristi kao dokaz da originalni sadržaj poruke ili dokumenta nije izmenjen od trenutka kada je dokument potpisan. Njime se obezbeđuje autentičnost poruke, njena neporecivost i integritet podataka.

Mere predostrožnosti:

Ukoliko se posumnja da je sertifikat vlasnika kartice na bilo koji način kompromitovan, to može da znači da postoji realna opasnost od falsifikovanja potpisa na dokumentima (nalog za plaćanja itd).

4. DISKUSIJA (KOMENTAR ISTRAŽIVANJA)

U današnjem svijetu povećane globalizacije tržišta i ekonomske regionalizacije poslovanje ne može biti uspješno bez upotrebe moderne informacione tehnologije. Umrežavanje preduzeća i javne administracije i razvoj Interneta doveli su do velikih promjena u načinu i efikasnosti rada poslovnih sistema. Omogućena je jednostavna i brza komunikacija, gotovo trenutno prenošenje velikih količina podataka na velike udaljenosti, jednostavno objavljivanje i ažuriranje multimedijalnih dokumenata i njihova kontinuirana globalna dostupnost, digitalna isporuka dobara i usluga, direktno plaćanje putem Interneta, stvaranje virtuelnih organizacija itd. Sve to predstavlja elemente novog oblika poslovanja, tzv. elektronsko poslovanje (*electronic business*).

Elektronsko poslovanje je opšti koncept koji obuhvata sve oblike poslovnih transakcija ili razmjene informacija koje se izvode korišćenjem informacione i komunikacione tehnologije i to: između preduzeća, između preduzeća i njihovih kupaca, ili između preduzeća i javne administracije.

Elektronsko poslovanje uključuje i elektronsko trgovanje dobrima i uslugama. Elektronsko poslovanje može se posmatrati sa više stanovišta. Sa aspekta komunikacija elektronsko poslovanje je elektronska isporuka informacija, proizvoda i u usluga i elektronsko plaćanje korišćenjem računarskih i drugih komunikacijskih mreža. Sa poslovnog aspekta to je primjena tehnologije u svrhu automatizacije poslovnih transakcija i poslovanja.

Elektronsko poslovanje ima korjene u sedamdesetim godinama prošlog vijeka, nastankom elektronskog prenosa gotovine (EFT, *Electronic fund transfer*) koji se odvija između banaka putem sigurnih privatnih mreža. Osamdesetih godina razvijena su dva nova oblika elektronskog poslovanja: elektronska razmjena podataka (*Electronic data interchange* - EDI), elektronska pošta.

Obje tehnologije su doprinjele znatnom smanjenju količine papira u upotrebi i povećanju automatizacije poslovanja. Elektronska razmjena podataka omogućila je preduzećima slanje i prijem poslovnih dokumenata u standardnom elektronskom obliku, i to putem sigurnih privatnih mreža. Međutim, EDI je skupa tehnologija i nju uglavnom koriste velika preduzeća. Mala i srednja preduzeća su umjesto privatnih mreža koristila on-line servise mreža sa dodatom vrednošću (*value added networks*, VAN), koje posjeduju programe koji omogućavaju elektronsku razmjenu podataka. Tokom devedesetih godina, pojavom *World Wide Web*-a u okviru Interneta, prvi put je omogućen jednostavan rad na mreži i jednostavno i jeftino objavljivanje i širenje informacija. Omogućeni su raznovrsni oblici poslovanja, a samo poslovanje je postalo jeftinije, pa su i mala preduzeća dobila mogućnost korišćenja elektronskog poslovanja. Demokratizacija poslovanja približila je globalno tržište malim i srednjim preduzećima. Korišćenje računara i mreža nije više privilegija velikih i bogatih preduzeća, već se u trku na globalnom tržištu mogu uključiti i najmanja preduzeća. Rizik neblagovremenog uključivanja u savremeno poslovanje je zaostajanje i gubljenje pozicija na tržištu.

Pojam elektronskog poslovanja prvi je definisao IBM, opisujući ga kao djelatnost koja omogućava izgradnju i primjenu poslovnog modela u kome su promjene katalizator rasta, a organizaciona struktura se mijenja zavisno od poslova. Model odlikuju dinamički, kompjuterizovani odnosi sa partnerima, elektronska vremena reagovanja, virtuelne strukture i visok nivo automatizacije, što sve doprinosi optimizovanju poslovnih procesa i sticanju prednosti nad konkurencijom. Elektronsko poslovanje zasniva se na primjeni Interneta, intraneta i aplikacija za grupni rad.

5. ZAKLJUČAK

Iz svega što je izneseno u radu možemo zaključiti sledeće:

Informacione tehnologije predstavljaju veoma važan faktor (resurs) u procesu strateškog pozicioniranja preduzeća. Proces tranzicije koji u sebi sadrži i procese globalizacije i integracije tržišta obezbeđuje preduzećima sa našeg područja da izlaze na inostrano tržište, ali istovremeno i otvara granice naše zemlje za priliv stranog kapitala, investicija i proizvoda. U takvom okruženju preduzeća se, kao i sama zemlja i privreda, moraju transformisati. Veliki broj informacija mora se obezbediti menadžment timu preduzeća da bi se procesi u preduzeću odvijali na optimalnom nivou.

Segment poslovanja preduzeća koji predstavlja predmet ovog istraživanja su informacione tehnologije i elektronsko poslovanje sa svim aspektima i mogućnostima primene.

Brzina, globalizacija, unapređenje produktivnosti, dolaženje do novih klijenata i deoba znanja među organizacijama i institucijama u cilju ostvarivanja konkurentne prednosti - jesu termini koji određuju elektronsko poslovanje. Ukratko, sinonim za savremeno poslovanje jeste elektronsko poslovanje!

IBM je 1997. godine prvi počeo sa korišćenjem termina "*e-business*", da bi napravio konceptualnu razliku sa do tada upotrebljavanim terminom "*e-commerce*" (elektronska trgovina), koji je izjednačavao elektronsko poslovanje sa elektronskom trgovinom. U drugoj polovini ove godine, međutim, i dalje ne postoji opšteprihvaćena definicija elektronskog poslovanja, pri čemu čak i velike enciklopedije poput Britanike definišu pojam *e-commerce* kao pojam *e-business*.

Elektronsko poslovanje, *e-business*, je skup poslovnih aktivnosti koje se odvijaju posredstvom informaciono-komunikacionih tehnologija, a posebno Interneta, i koje podrazumevaju:

- optimizaciju poslovnih procesa (proizvodnja, marketing, veleprodaja, distribucija, prodaja, naplata, isporuka, dopuna zaliha);
- unapređenje odnosa sa ciljnim javnostima (klijentima, zaposlenima, dobavljačima, distributerima) i
- unapređenje ostalih poslovnih servisa podrške (banke, advokatske agencije, računovodstvene agencije, zakonodavstvo i vladine agencije).

Sa druge strane, elektronska trgovina, *e-commerce*, predstavlja komponentu elektronskog poslovanja, koja opisuje procese kupovine, prodaje i razmene dobara, usluga i informacija, putem računarskih mreža koje uključuju i Internet.

Osnovni oblici elektronskog poslovanja vezani su za upotrebu Informacionih tehnologija (IT) u poslovanju i to:

- internu upotrebu- primena Intraneta, *Extraneta* (mreža poslovnih partnera nastala objedinjavanjem korporacijskih intranetova), *Business to Employee* - B2E (plate, odmori, bolovanja, odsustva, utrošak radnog vremena).
- *Business to Business* (B2B) - potpuno automatizovani sistem koji je podržan *E-Commerce* i ekstranetom i omogućuje trgovinu između firmi preko Interneta, sa nizom pratećih aktivnosti.
- *Business to Customer* (B2C) se odnosi na mnogo širi deo privrede: online bankarstvo, turizam i saobraćaj, online aukcije, zdravstvene informacije, nekretnine.

Za razliku od B2B sistema, koji je složeniji jer firme obično žele da pregovaraju o cenama, rokovima isporuke, strukturi proizvoda, garanciji, tehničkoj i materijalnoj podršci, B2C trgovina zasniva se, najčešće, na izboru proizvoda iz kataloga sa predefinisanim cenama od strane kupca. B2B sistemi zahtevaju integraciju informacionih sistema firmi koje međusobno posluju, dok B2C sistemi ne zahtevaju takvu integraciju (arhitektura sistema "običnih kupaca" može se najčešće ignorisati).

Electronic Commerce (EC), u prevodu elektronska trgovina, jeste poznati komunikacioni koncept vezan za trgovinu proizvodima, uslugama i informacijama pomoću Informacionih tehnologija.

Osnovne primene EC tehnologije potrošačke orijentacije su u sledećim oblastima: oglašavanje, marketing i trgovina, tržište i istraživanje proizvoda, podrška kupcima, prodajni katalogi, aukcije, trgovina hartijama od vrednosti, tržište zapošljavanja i elektronski *shopping* prostor (*Cyber Marketplace*).

Business-to-business orijentisana EC pokriva skup komunikacionih aktivnosti između kompanija i/ili korporacija. Može se reći da je ova vrsta elektronskog poslovanja izazvala fundamentalne transformacije sistema poslovanja. Internet je omogućio sledeće tri prednosti u među korporacijskoj trgovini:

- distribuciju informacija svim partnerima
- i interfejs za EDI sistem
- i veliku propusnu moć informacija između kompanija bez namenskih privatnih linija.

Međutim, ova vrsta EC je bila zastupljena i pre popularizacije Interneta, a zasnivala se na *Electronic Data Interchange* (EDI) sistemu. Često se pojam *business-to-business* elektronskog poslovanja pogrešno poistovećuje sa EDI. U aktuelnoj teorijskoj literaturi (Keneth Laudon, Efraim Turban i dr.) i u praksi preduzeća u na zapadu u poslednjih nekoliko godina popularno je koristiti popularne termine koji poč inju sa slovom "e" (*buzzwords*) i koji označavaju različite nove tehnike i tehnologije poslovanja na Internetu. Indikativno je da se pojmovi sa slovom "e" (*electronic* - elektronsko), uključujući i termin elektronsko poslovanje, u poslednje vreme isključivo vezuju za primenu Informacionih tehnologija u poslovanju i za Internet terminologiju. *e-Commerce* (*Electronic Commerce*, EC - elektronska trgovina) je kupovina ili prodaja

dobara ili usluga putem Interneta, naročito putem servisa *World Wide Web*. U praksi se ovaj termin često koristi umesto novijeg termina *e-business*, što znači poslovanje putem Interneta. Termin *e-Commerce* može se definisati i kao proces upravljanja online finansijskim transakcijama od strane pojedinaca ili kompanija. Ovaj proces uključuje kako maloprodajne, tako i veleprodajne transakcije.

Termin *Online* je sinonim za Internet (biti na liniji = biti na Internetu). Fokus *e-Commerce*-a je u sistemima i procedurama pomoću kojih dolazi do razmene različitih finansijskih dokumenata i informacija. Ovi sistemi uključuju transakcije kreditnim karticama, *e-cash* (elektronska gotovina), *e-billing* (elektronsko plaćanje), *e-cheques* (elektronski čekovi), *electronic invoices* (elektronski računi), narudžbine i finansijske izjave. *e-Commerce* praktično omogućuje nastavak korišćenja tehnologije elektronskih razmena podataka (EDI). *Electronic Data Interchange* (EDI) je razmena poslovnih podataka gde se koristi razumljivi format ovih podataka. Ovaj sistem razmene podataka je prethodio pojavi Interneta i obično se koristio u razmeni podataka između korisnika. Kao što se može videti iz prethodnih definicija, pojam elektronskog poslovanja je mnogo širi od definicija najčešće korišćenog njegovog sinonima *e-Commerce*. Mnogo prikladniji termin za elektronsko poslovanje jeste *e-Business*.

Electronic Business (EB - elektronsko poslovanje) jeste vođenje poslova na Internetu, što ne podrazumeva samo kupovinu i prodaju, nego i brigu o klijentima i poslovnim partnerima, kao i organizacija poslovanja u sopstvenoj firmi online i organizacija prema klijentima.

Elektronska trgovina je moderna poslovna metodologija koja organizacijama, trgovcima i kupcima omogućuje smanjenje troškova, uz unapređenje kvaliteta roba i usluga i povećanje brzine njihove isporuke. Broj elektronskih transfera raste više od 15% godišnje, što je skoro tri puta više od ukupnog godišnjeg porasta poslovnih transakcija.

Primena elektronske trgovine je počela još sedamdesetih godina, ali je uglavnom bila ograničena na velike korporacije i veoma mali broj korisnika. Komercijalizacijom Interneta, primena elektronskog poslovanja je rapidno porasla. U poslednjih pet godina su se pojavile mnoge inovativne primene ove tehnologije, kao što su oglašavanja, aukcije i druga iskustva virtuelne realnosti.

Primena Informacionih tehnologija u poslovanju, kako ćemo videti u radu, je zasigurno opravdana i neophodna, ali i kao takva nailazi na određene otpore.

Način poslovanja privrednika, preduzetnika i menadžera, na prostorima SCG pre svega, vrlo se malo zasnivao i zasniva na upotrebi informacionih tehnologija. Informacione tehnologije se u nekim slučajevima smatraju samo troškom a ne investicijom i tretiraju se kao luksuz a ne kao neophodnost.

Neki segmenti informacionih tehnologija zahtevaju i određene uslove, kako materijalne (digitalne telefonske centrale, brz protok podataka kroz mrežu, kompjutere određenog kvaliteta i performansi) tako i nematerijalne (zakonska regulativa, usklađenost propisa i tehnika...), i na taj

način iako firma ima nameru da investira u informacione tehnologije kako bi na poboljšala svoju poziciju na tržištu, u startu je onemogućena materijalnim ograničenjima ili zakonskom regulativom.

Elektronsko bankarstvo predstavlja elektronske sisteme za transfer novca, zapisa i dokumenata bez papira baziranog na integraciji računarske i komunikacione tehnologije.

U osnovi elektronskog bankarstva nalazi se EFT (*Electronic Funds Transfer*) odnosno transfer sredstava iz dela finansijskih aktiva u okviru jednog ili više transaktora, i to elektronskim putem. Takav prenos novca i zapisa bez papira obavlja se uz primenu odgovarajućih programskih paketa i aplikacija.

Pod elektronskom tehnologijom podrazumevamo kombinovanu upotrebu informacionih tehnologija i telekomunikacija. Pod uticajem primene elektronskog poslovanja reorganizuju se skoro sve delatnosti i tako danas imamo e-trgovinu, e-bankarstvo, e-upravu, i sl.

Brz razvoj Interneta i tehnologije, pomognut stalnim ljudskim naporima, razvijanje elektronskog bankarstva dobija rapidni porast, tako da se kompjuterizovanjem pojedinaca iz dana u dan podiže nivo u razvoju ove oblasti. Mnoge su prednosti elektronskog bankarstva u odnosu na ranije oblike poslovanja i komunikacije. Kroz rad su prikazane prednosti, ali najbitnije su ušteda vremena i povećanje produktivnosti, koje predstavljaju potencijalne vrednosti koje pruža elektronsko bankarstvo.

Svrha E-bankarstva je u ostvarenju nekoliko ciljeva, a koji su: smanjenje čekovnog plaćanja i drugih oblika bezgotovinskog plaćanja i plaćanja gotovinom, obezbeđenja mogućnosti automatskog depozita i podizanja novca preko udaljenih terminala (bankomat), omogućavanja kompjuterizovanog plaćanja usluga, razvijanja transakcije deponovanja, uvođenja sistema elektronskog plaćanja računa klijenata svih vrsta bez korišćenja čekova i gotovine, razvijanje lepeze usluga i kreiranja novih prihoda i proširenja postojećih tržišta i obima klijenata. Dakle, početna hipoteza je dokazana.

6. LITERATURA

1. Balaban N., Ristić Ž., Đurković J., Trninić J.: *Informacioni sistemi u menadžmentu*, Beograd, 2005., str. 309
2. Bjelić, Predrag, *MOBILNI TELEFON KAO KANAL ELEKTRONSKOG POSLOVANJA*“, *Ekonomski anali*, 2001, vol. 44, iss. 151-152, str. 95
3. Ćirović, Milutin, „*BANKARSTVO*“, Beograd, Bridge Company, 2001.
4. *Convergence Technologies for 3G Networks*, Second edition by Jeffrey Banister, Paul Mather and Sebastian Coope, John Wiley & Sons, Ltd, 2004.
5. Curry, J., *The Customer Marketing Method*, *The Customer marketing Institute* BV, 2000.
6. Đurković Ž., J., Trninić J.: *Informacioni sistemi u menadžmentu*, Beograd, 2005., str. 175
7. Đurković, Ivan, „*MEDUNARODNO BANKARSTVO*“, Univerzitet „Braća Karić“, Beograd, 2008.
8. Filipović Vinka, Milica Kostić, *Marketing menadžment Teorija i praksa*, *FON - Menadžment*, Beograd, 2001.
9. Hadžić, Miroljub, „*BANKARSTVO*“, Cicero print, Beograd, 2007.
10. Imber, Jane and Betsy-Ann Toffler : *Dictionary of Marketing terms*, *treće izdanje*, *Barrond Business Dictionaries*, 2000.
11. Ivković Miodrag, Milošević Slađana, Subić Zoran, Dobrilović Dalibor: *Elektronsko Poslovanje*, Tehnički fakultet, Zrenjanin, 2005.
12. James O'Brien: *Management Information Systems - managing Information Technology in the Business Enterprise*, 6th edition, McGraw Hill, 2004. str. 104
13. Kotler, P., *Marketing Menagement*, 11th edition, *Prentice Hall*, 2003.
14. Krsmanović S.: „*Informacioni sistemi u mrežnom okruženju*“, Univerzitet “Braća Karić”, Beograd, 2003., str.138
15. Krstić Ž. Borko, „*BANKARSKI MENADŽMENT*“, Ekonomski fakultet Niš, Niš, 2004.
16. Mattison Rob: *Winning Telco Customers Using Marketing Database*, *Artech House*, *Boston – London*, 1999.
17. Miljević Milan, „*SKRIPTA IZ METODOLOGIJE NAUČNOG RADA*“, Univerzitet u Istočnom Sarajevu, Filozofski fakultet, Pale 2007.
18. Mishkin S. Frederic, „*MONETARNA EKONOMIJA, BANKARSTVO I FINANSIJSKA TRŽIŠTA*“, VII izdanje, Data Status, Beograd, 2006.
19. Mohammed R., Fisher R. J., Jaworski B. J., Paddison G. : *Internet Marketing: Building Advantage in a Networked Economy*, McGrawe – Hill College, 2001.
20. Pantić S.: *Računarske komunikacije*, *Kompjuter biblioteka*, Čačak, 1996.
21. Perkins, Charles E., “*Dynamic Host Configuration Protocol for IPv6*“, Internet Engineering Task Force, May 5, 2000.
22. Radovanović, Predrag, „*TEHNOLOGIZACIJA BANKARSTVA*“, *Naša reč*, Leksovac, 2000.
23. *Realizing the Transition to IPv6*, Daniel G. Waddington and Fangzhe Chang, Bell Research Laboratories, IEEE Communications Magazine, June 2002.
24. S. Deering, R. Hinden, RFC 1883: *Internet Protocol, Version 6 (IPv6) Specification*, December 1995.
25. Smith, M.L. , *One to One : Put the customer in the information driven seat and building better relationships*, *direct marketing*, *Hoke Communication, Inc.* , 1998.
26. Stankic dr Rade *Elektronsko poslovanje*, , Ekonomski fakultet Beograd

27. Stankić R.: *Poslovna informatika*, Beograd, 2003., str. 218
28. Varagić Dragan: *Kultura komunikacije na Internetu i njen odnos sa Internet marketingom* seminar Netforum, Beograd, 1998.
29. Varagić Dragan: *Vodič kroz raj i pakao Internet marketinga*, Novi Sad, 2002.
30. Vuksanović, Emilija, „ELEKTRONSKO BANKARSTVO“, Beograd, Beogradska bankarska akademija i Institut ekonomskih nauka, 2006.
31. Zimmerman, J., *Marketing on the Internet*, Maximum Press, 2000.
32. Živković, Aleksandar, Stankić, Rade, Krstić, Borko, „*Bankarsko poslovanje i platni promet*“, Ekonomski fakultet Beograd, 2004.

WEB IZVORI

33. www.wikipedia.org
34. www.zaba.hr
35. www.poslovniforum.hr
36. www.znanje.org
37. Internet Engineering Task Force / RFC dokumenti http://www.ietf.org/iesg/1rfc_index.txt
38. http://www.spvp.zesoi.fer.hr/seminari/2004/xml_web_servisi-isorsa/2.htm

POPIS SKRAĆENICA:

PIN – Personal Identification Number - Osobni identifikacijski broj
USB – Universal Serial Bus - Univerzalno serijsko sučelje
OTP – One Time Password - Jednokratna lozinka
TAN – Transaction Authorization Number - Broj autorizacije transakcije
PKI – Public Key Infrastructure - Infrastruktura javnog ključa
HTTP – Hypertext Transfer Protocol - Hipertekstualni prijenos podataka
HTML – HyperText Markup Language - Hipertekstualni označni jezik
SSL – Secure Sockets Layer - Protokol za prijenos zaštitno kodiranih podataka
PCT – Patent Cooperation Treaty - Ugovor o suradnji na području patenata
IETF – Internet Engineering Task Force - Inženjerska radna skupina za internet
TLS – Transport Layer Security - Transportni sigurnosni sloj
WTLS – Wireless Transport Layer Security - Bežični transportni sigurnosni sloj
ISO/OSI – International Standard Organization's / Open System Interconnect - Međunarodna organizacija za standarde / model otvorenih komunikacija
SNMP – Simple Network Management Protocol - Protokol za upravljanje mrežom
NFS – Network File System - Mrežni datotečni sustav
DNS – Domain Name System - Sistem imena server
VoIP – Voice over Internet Protocol - Program za razgovor putem internet
SET – Secure Electronics Transaction - Osigurana elektronička transakcija
S-HTTP – Secure Hypertext Transfer Protocol - Sigurni hipertekstualni prijenos podataka
S-MIME – Secure Multipurpose Internet Mail Extensions - Sigurni standard za proširenje funkcija elektronske pošte
MIME – Multipurpose Internet Mail Extensions - Standard za proširenje funkcija elektronske pošte
SSH – Secure Shell – Sigurnosni program za komunikaciju s operacijskim sustavom
PEM – Private Enhanced Mail - Elektronska pošta sa šifriranjem
PGP – Pretty Good Privacy - Standard za zaštitu na internet
DOD – Department of Defense - Očela za obranu
UDP – User Datagram Protocol - Korisnički protokol za paketne mreže bez spajanja
SMTP – Simple Mail Transfer Protocol - Jednostavni protokol za razmjenu pošte
WAN – Wide Area Network - Mreža širokog dosega