Primjena informatičke tehnologije u bankarstvu

Kovačević, Dario

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEK

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Preddiplomski studij računarstva

PRIMJENA INFORMATIČKE TEHNOLOGIJE U BANKARSTVU

Završni rad

Dario Kovačević

Osijek , 2016.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 28.09.2016.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Dario Kovačević
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	3354, 13.10.2015.
OIB studenta:	29308415538
Mentor:	Izv.prof.dr.sc. Dominika Crnjac Milić
Sumentor:	
Naslov završnog rada:	Primjena informatičke tehnologije u bankarstvu
Znanstvena grana rada:	**Informacijski sustavi (zn. polje računarstvo)**
Predložena ocjena završnog rada:	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 Postignuti rezultati u odnosu na složenost zadatka: 3 Jasnoća pismenog izražavanja: 3 Razina samostalnosti: 2
Datum prijedloga ocjene mentora:	28.09.2016.
Datum potvrde ocjene Odbora:	05.10.2016.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 17.11.2016.

Ime i prezime studenta:	Dario Kovačević
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	3354, 13.10.2015.
Ephorus podudaranje [%]:	2%

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena informatičke tehnologije u bankarstvu**

izrađen pod vodstvom mentora Izv.prof.dr.sc. Dominika Crnjac Milić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ:

1. UVOD

Svrha ovog rada je pobliže objasniti primjenu informatičke tehnologije u bankarskom sustavu.Kada pitate nekoga ili ako pokušate sami istražiti koju ulogu ima informatika u bankarstvu, uglavnom će te naići na odgovor ili informaciju da su to elektroničko bankarstvo, bankomati, mobilno bankarstvo, itd. Bankarstvo se prije temeljilo na depozitu i štednji. S razvojem tehnologije i uslužnog segmenta bankarstva, banke su u svojim bankarskim sustavima počele sa primjenom novih distribucijskih kanala (bankomati, mobilno bankarstvo, e – bankarstvo, POS uređaji, itd) odnosno s primjenom informatičke tehnologije. U današnje vrijeme suvremena banka ne može poslovati ukoliko u svom sustavu nema implementiran informatički sustav. Najbolji pokazatelj toga su ulaganja bankarskih sustava u tehnologiju. Uz primjenu informatičke tehnologije u bankarstvu dolazi i do određenih rizika prilikom poslovanja banaka. Zato postoje određene protumjere i zaštite, od mogućih napada na korisničke podatke, kojih se banke moraju pridržavati. Kao uvod u završni rad dotaknuti ću se razvoja Internet bankarstva u svijetu i u Republici Hrvatskoj gdje ću opisati tko su bili začetnici uvođenja Interneta u poslovanje banaka i kakav je utjecaj razvoj tehnologije imao na bankarski sustav u Republici Hrvatskoj. Nakon uvoda dolazimo do razrade teme ovog rada. Za početak obraditi ću arhitekturu informacijskog sustava i način na koji funkcionira. Kroz nekoliko primjera objasniti ću primjenu informatičke tehnologije u svakodnevnom radu bankarskih sustava, njihovu izvedbu i arhitekturu, te opisati njihove prednosti i nedostatke. Na kraju ovog rada biti će objašnjen jedan vrlo bitan dio prilikom korištenja Interneta u bankarstvu, a to je sigurnost Internet bankarstva gdje će biti objašnjena primjena raznih sigurnosnih mehanizama za zaštitu podataka.

1.1 Zadatak završnog rada

Zadatak ovog završnog rada je objasniti primjenu informatičke tehnologije u bankarstvu, te na temelju primjera pokazati način rada određenih tehnologija. Pokazati mogućnosti koje je informatička tehnologija donijela u sektoru poslovanja banka i na koji način funkcionira suvremena banka. Posebnu pažnju posvetiti sigurnosti informatičkih sustava koji se koriste prilikom Internet bankarstva i na zaštitu samog korisnika kao bitnog člana cjelokupnog procesa Internetabankarstva.

2. POVIJESNI RAZVOJ

2.1. Povijesni razvoj informacijske tehnologije u bankarstvu u svijetu

Ideja o Internet bankarstvu se razvija 1980.-ih godina. Razvojem World Wide Weba sukladno se razvija i Internet bankarstvo. Programeri koji rade na razvoju baza podataka dolaze do ideje nuđenja bankovnih transakcija putem Interneta.

Godine 1983. Nottingham Building Society NBS pruža prvu uslugu Internet bankarstva u Velikoj Britaniji. Ova usluga smatra se temeljem razvoja Internet bankarstva i vodilja razvoja za većinu usluga koje su slijedile. Sustav Internet bankarstva bio je nedovoljno razvijen, postojala su ograničenja u vidu broja transakcija i funkcija koje su klijenti putem Internet bankarstva mogli obavljati. Šira upotreba Internet bankarstva započela je 90-ih godina prošlog stoljeća

1994. počinje razvoj Internet bankarstva u današnjem obliku kada je financijska institucija, Stanford Federal Credi Union ponudila prvu uslugu Internet bankarstva u Sjedinjenim Američkim Državama. Nakon toga 1995. godine u gradu Pinevillu, je osnovana banka imenom Security First Network Bank. Security First Network Bank je bila prva banka koja je osnovana samo za poslovanje putem Interneta.

Vrlo bitnu ulogu u razvoju Internet bankarstva imala je i tvrtka Apple. 2007. godine kada je Apple lansirao svoj prvi pametni telefon iPhone koji je imao mogućnost Internet bankarstva. Od tada Internet bankarstvo postaje mnogo mobilnije i smanjuje vrijeme čekanja i gužve u poslovnicama.

Od 90-ih godina prošlog stoljeća pa sve do današnjeg doba počeo je strahovit razvoj tehnologije koja je potrebna za Internet bankarstvo pa samim time se i povećava broj korisnika koji shvaćaju prednosti ove vrste bankarstva. Prema podacima Online Banking Reporta u travnju 1996. godine bilo je milijun korisnika Internet bankarstva u Sjedinjenim Američkim Državama a već 1997. godine zabilježeno je 4,2 milijuna korisnika Internet bankarstva. Već 2001. godine 19 milijuna američkih domaćinstava koristi neki oblik Internet bankarstva [1].

2.2. Povijesni razvoj informacijske tehnologije u Republici Hrvatskoj

S razvojem Interneta, Internetske tehnologije i banke u Republici Hrvatskoj su počele koristiti Internet ali u početku je Internet imao manju ulogu nego što je ima danas. Na početku su banke koristile Internet kao marketinški medij, koji je služio za oglašavanje i iznošenje ponuda koje banke nude svojim postojećim i novim korisnicima. Internet bankarstvo u Republici Hrvatskoj, onakvim kakvim ga danas smatramo, formiralo se postepeno i s nekoliko godina zaostatka u odnosu na Sjedinjene Američke Države i Europu. „Začetnikom" Internet bankarstva u Republici Hrvatskoj možemo smatrati Varaždinsku banku koja je 1997. godine uvela opciju uvida u stanje računa .Vrlo jednostavna opcija u kojoj su korisnici spomenute banke mogli pristupiti svom računu sa svog računala bez da odlaze do poslovnice i gube vrijeme na čekanje u redovima. Dvije godine kasnije na istu se opciju odlučila i Međimurska banka. Prvi poniri u „modernom Internet bankarstvu" su bile manje banke, dok su današnji lideri u svijetu bankarstva bili sporiji u uvođenju ovih promjena, tako su Raiffeisen banka i Privredna banka Zagreb uvele Internet bankarstvo 2000. godine dok 2001. godine to isto čini i Hypo Alpe Adria Bank.

Razlog zaostatka za Sjedinjenim Američkim Državama i Europom od nekoliko godina je bio nedostatak zakonske regulative u državi i nizak postotak korisnika Interneta. Zakon o platnom prometu u zemlji je omogućio nagli razvoj Internet bankarstva. Nakon donošenja Zakona o platnom prometu dolazi do porasta korištenja Interneta i banke koriste tu situaciju za privlačenje korisnika na Internet bankarstvo. Danas u Republici Hrvatskoj prema posljednjim dostupnim podatcima Hrvatske Narodne Banke, na datum 24. srpnja 2014, broj korisnika Internet bankarstva možemo vidjeti prema Tablici 2.1. [2]

Tab 2.1 *Broj korisnika prema platno prometnim servisima – 2014. godina.[2]*

HRVATSKA NARODNA BANKA
Sektor platnog prometa
Direkcija za nadzor platnog prometa

Zagreb, 24.07.2014.

BROJ KORISNIKA PREMA PLATNO PROMETNIM SERVISIMA - 2014. godina

	na dan 31.01.		na dan 28.02.		na dan 31.03.		na dan 30.04.		na dan 31.05.	
	Transakcijski račun	Drugi platni račun	Transakcijski račun	Drugi platni račun	Transakcijski račun	Drugi platni račun	Transakcijski račun	Drugi platni račun	Transakcijski račun	Drugi platni račun
POTROŠAČ										
Internet	1.142.037	17.165	1.147.517	17.438	1.155.822	18.020	1.161.394	17.969	1.167.606	18.150
Telebanking										
Mobilni telefon	392.245	3.779	403.250	4.042	415.003	4.333	425.179	4.519	435.780	4.768
E-račun	10.438		10.430		10.242		10.644		10.815	
Trajni nalog	1.005.778	1.223	1.027.315	1.233	1.042.018	1.271	1.034.704	1.179	1.001.022	1.111
Izravno terećenje	939.715	720	942.625	720	938.427	726	928.805	735	944.604	733
Ostalo	495.760	232.774	489.633	231.626	468.091	223.036	477.908	227.973	466.208	226.132
NEPOTROŠAČ										
Internet	198.612	307	199.567	294	201.374	297	204.552	301	204.467	301
Telebanking	3.101		3.119		3.139		258		258	
Mobilni telefon	17.050		17.293		17.647		18.064		18.434	
E-račun			3		3		3		3	
Trajni nalog	25.309		25.463		24.962		25.382		25.803	
Izravno terećenje	1.818		1.582		1.562		1.565		1.546	
Ostalo	9.802	72	9.746	73	9.603	71	9.417	74	7.836	75

3. INFORMATIČKA TEHNOLOGIJA U BANKARSTVU

Zbog informatičke tehnologije, u današnje vrijeme možemo izvršavati bankovne transakcije ili obaviti plaćanje računa bez napuštanja udobnosti svog doma. Prednosti „kućnog bankarstva“ su brojne – izbjegava se mukotrpno stajanje i čekanje u redu u poslovnicama banke, stanje na računima može se provjeriti svakodnevno, putem osobnog računala,tableta ili pametnog telefona, jednostavnom prijavom preko aplikacije na svoj korisnički račun koji ustvari predstavlja korisnikov bankovni račun.

Kroz ovaj rad objasnit ću osnovne pojmove koji obuhvaćaju informatičku tehnologiju u bankarstvu, a to su: informacijski sustav, bankomati (eng. Automated Teller Machine, ATM), elektroničko bankarstvo (eng. e-banking), Internet bankarstvo, mobilno bankarstvo (eng. m-banking).

Kako bih pobliže objasnio pojedine usluge, tehnologiju izrade, upotrebu i njihove funkcionalnosti, koristit ću se uslugama Privredne banke Zagreb, jedne od vodećih banaka na hrvatskom tržištu, te ujedno jednoj od prvih banaka koja je u svoje poslovanje uvela Internet.

3.1. Informacijski sustav (IS)

Informacijski sustav (IS) je sveobuhvatnost infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz, distribuciju informacija i raspolaganje njima [2].

S obzirom na to da je korištenjem informatičke tehnologije u svim aspektima bankarskog poslovanja stvorilo veliku ovisnost o informacijskoj tehnologiji, velika važnost se posvećuje upravljanju informacijskim sustavom kao sastavnim dijelom upravljanja bankom u cjelini. Prema odluci o primjerenom upravljanju informacijskim sustavom (Hrvatska Narodna Banka, 2010.), komponente informacijskog sustava banke su:

1. Softverske komponente:
    - Aplikacijski softver,
    - Sistemski softver
    - Baze podataka
    - Softverski razvojni alati
    - Uslužni programi te ostali softveri.

2. Hardverske komponente:
    - Računala i računalna oprema,
    - Komunikacijska oprema,
    - Mediji za pohranu podataka,
    - Ostala tehnička oprema koja podržava rad IS- a.

3. Informacijska imovina:
    - Podaci u bazama podataka,
    - Datoteke s podacima,
    - Programski kod,
    - Sistemska i aplikacijska dokumentacija i slično.

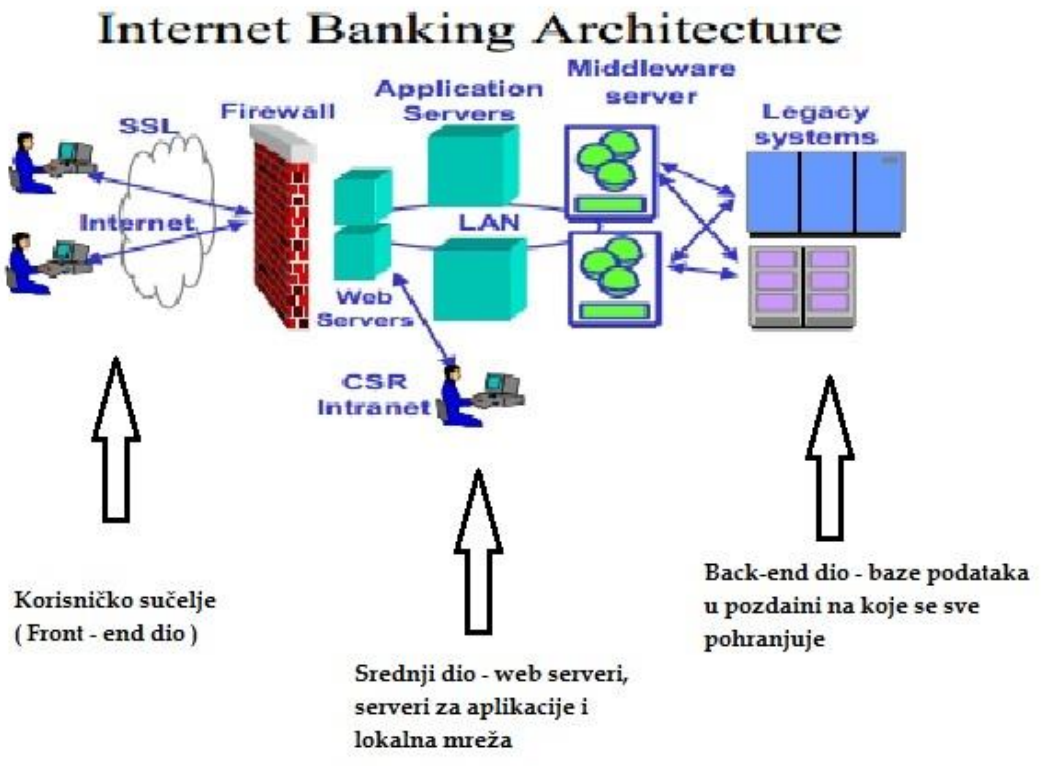
3.1.1. Arhitektura softverskog dijela IS-a

Arhitektura softverskog dijela IS-a sastoji se od tri glavna dijela (tzv. troslojna arhitektura) [3]:

1. Korisničko sučelje (eng. user interface, Front-end sustav) - predstavlja korisničko sučelje aplikacija, dio kojim klijenti vide i koriste prilikom autentikacije i korištenja financijskih usluga.Tehnologija koja se koristi prilikom pravljenja korisničkog sustava su najčešće programski jezici HTML, CSS, XHTML, JavaScript i PHP.U Današnje vrijeme je najvažnija izrada sučelja pri kojem se posebna pažnja daje vizualnom izgledu sučelja i izradi sučelja za mobilne aplikacije.

2. Srednji dio sustava (eng. Middleware) - u srednjem dijelu sustava nalaze se programi koji djeluju kao aplikacijski posrednik između više aplikacija, između aplikacije i baze podataka, ili između nekoliko baza podataka. Aplikacije međusobno komuniciraju putem sustava za razmjenu poruka (eng. messaging – GET i PUT poruke, poruke koje služe za učitavanje podataka koje korisnik unese i za prijenos između aplikacija).

3. Centralizirana obrada podataka u pozadini sustava (Back-end sustav) - u ovom dijelu sustava prikupljaju se transakcije u različitim oblicima, nakon toga se zahtjevi prevode u oblik koji će stroj razumjeti i izvršiti. Zahtjeva veliku računalnu snagu, dodatne mjere sigurnosti i napredne tehnike programiranja. Jezgra back-end sustava su baze podataka.



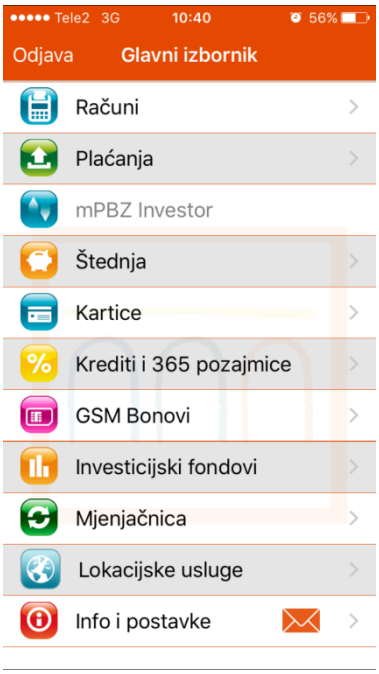
Sl 3.1. *Arhitektura sustava Internet bankarstva[3]*

SSL (eng. Secure Socket Layer) je standardna sigurnosna tehnologija za uspostavu enkriptirane veze između poslužitelja i klijenta, obično web servera i Internet stranice. Točnije, SSL je sigurnosni protokol. Određuje varijable šifriranja za vezu i podatke koji se prenose tom vezom
Vatrozid (eng. Firewall) je mrežni sigurnosni sustav koji sprječava neovlašteni pristup prema ili s neovlaštene privatne mreže. Može biti implementiran hardverski, softverski ili kombinacija oba.
Web poslužiteljeng. Web server) je program koji koristi HTTP (eng. Hypertext Transfer Protocol) za distribuciju informacija koje čine Internet stranice za korisnike, kao odgovor na njihove zahtjeve koji us proslijeđeni od strane HTTP klijenta s korisničkog računala.
Aplikacijski poslužitelj (eng. Application server) je vrsta poslužitelja dizajnirana za podršku web poslužitelju prilikom rukovanja dinamičkog sadržaja. Aplikacijski poslužitelj osluškuje rad web poslužitelja i automatski presreće sve korisničke zahtjeve za dinamičkim sadržajem. Web poslužitelj i dalje šalje statičke web stranice i grafičke datoteke kao i prije, ali sada s aplikacijskim poslužiteljem može kreirati dinamički sadržaj miješanjem podataka s predlošcima, pokretati programe ili pristupiti bazama podataka.
LAN (eng. Local Area Network) računalna mreža na unutar određenog prostora, kao što su škole, poslovni prostori. Sastoji se od međusobno povezanih računala, baza podataka i drugih uređaja.
Srednji dio sustava (eng. Middleware) je softverski sloj koji povezuje dvije inače zasebne aplikacije. Na primjer, postoji niz slojeva koji povezuju sustav baze podataka na web poslužitelju. To omogućuje korisnicima da traže podatke iz baze podataka, koristeći oblike prikazane na Internet pregledniku i omogućuje web poslužitelju vraćanje dinamičke stranice na osnovu korisnikovih zahtjeva.

3.1.2 Korisničko sučelje (Front-end sustav)

Prilikom izrade korisničkog sučelja banke bi se trebale pridržavati određenih smjernica:

- Napraviti korisničko sučelje prilagođeno svim dobnim skupinama, tako da ono bude atraktivnog izgleda i lako za korištenje mladim generacijama isto kao i onim starijim
- Slijediti preporuke dobrog dizajna i navigacije kroz aplikacije kojih na Internetu ima poprilično mnogo
- Najvažnije od svega potrebno je koristiti sigurnosne protokole za zaštitu korisnikovih podatak

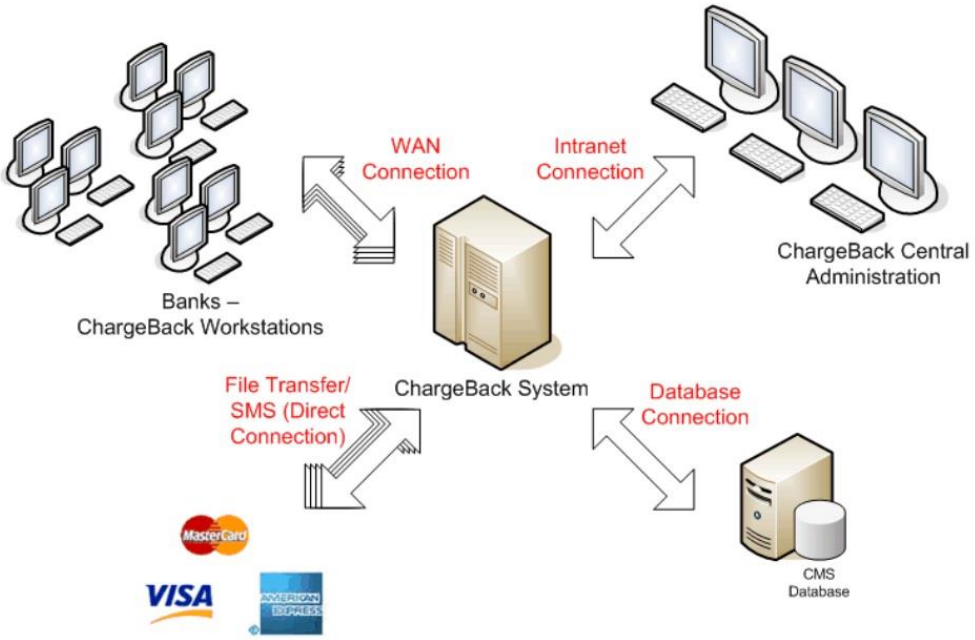


Sl 3.2. *Mobilno korisničko sučelje[13]*

3.1.3 Front – end sučelje za mobilne aplikacije

Davatelji usluga bi trebali putem mobilnih aplikacija klijentima pružiti mogućnost stalnog informiranja o promjenama stanja na računima i omogućiti transakcije. Korisničko sučelje treba biti isprogramirano koristeći tehnologije za mobilni web, za operativne sustave IOS, Android i Windows itd.

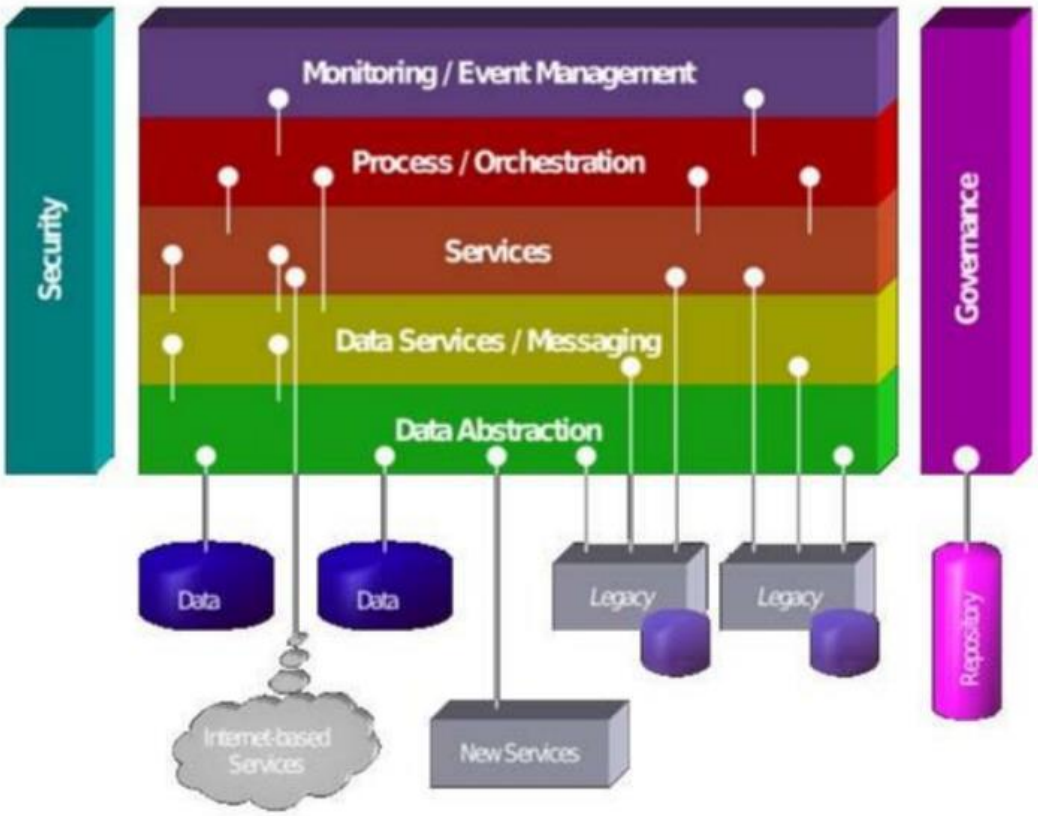
Centralizirana obrada podataka u pozadini sustava (Back-end sustav)



Sl 3.3. *Back-end sustav – modul za naplatu putem kreditnih kartica[3]*

3.1.4 Service Oriented Architecture (SOA) – povezivanje aplikacija

Tehnologija koja se pokazala učinkovitom u povezivanju velikih i nezavisnih dijelova aplikacija kako bi se uspostavila učinkovita funkcionalnost sustava je Service Oriented Architecture (SOA). U e-bankarstvu SOA se pokazala kao učinkovita tehnologija u povezivanju front-end i back-end sustava. SOA se može koristiti za interakciju aplikacija na Internet mreži, ali i s jedne radne stanice na drugu (pomoću PPP protokola i EDI (Electronic Data Interchange) mreže). SOA se sastoji od programskih usluga (eng. Software services) koje su nezavisna jedna od druge i izvršavaju se ponekad na različitim platformama (najčešće su .NET ili Java). Programske usluge mogu upravljati memorijom, kreirati poveznice između programskih komponenti i kreirati mapiranje podataka (organiziranje podataka tako da ih aplikacije mogu obraditi). SOA se može koristiti na različitim platformama: operacijskim sustavima Windows, Linux / Unix i dr.



Sl 3.4. *Prikaz SOA modela i njegove komponente[4]*

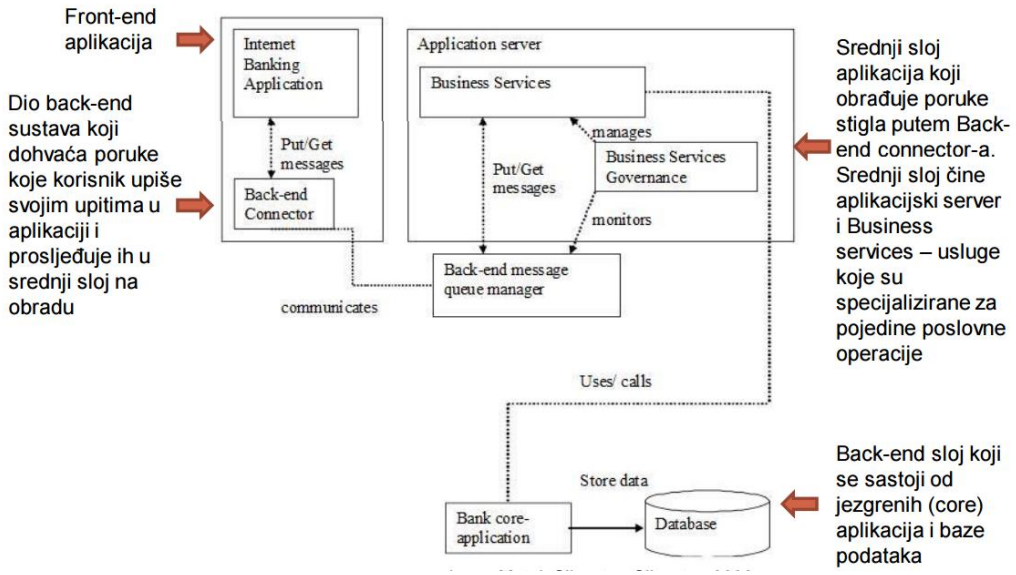
3.1.5 Integracija front-end aplikacija s backend-om

Aplikacija Internet bankarstva je kao crna kutija kojoj korisnik vidi samo one podatke koje unosi, te krajnji rezultat upita. Komunikacija između front-end sustava i back-end sustava je asinkronog tipa – što znači da ne moraju raditi oba sustava u isto vrijeme (ako zbog prekida Internet veze front-end ne radi, back-end i dalje nastavlja raditi, i obrnuto). Back-end gleda na front-end kao niz usluga s velikom granularnošću, čime se omogućuje integracija različitih aplikacija putem SOA protokola.

Dva dijela back-end sustava osiguravaju tijek poruka u sustavu:

- Back-end konektor
- Back-end upravljač porukama u repu čekanja

Primjer sustava koji radi na taj način: IBM Websphere Message Queue Manager or JMS standard (Java Message Service) for Java application servers. U njemu su usluge koje rade na aplikacijskom poslužitelju Websphere ili .NET grupirane u Business Service layer (IBM).



Sl 3.5. *Integracija front-end aplikacija sa back-end-om[13]*

3.2. Bankomat (eng. Automated teller machine, ATM)

Bankomat je računalni telekomunikacijski uređaj koji omogućuje klijentima neke financijske institucije uvid u stanje tekućeg ili žiro računa te izdavanje gotovine s istih, također noviji modeli bankomata imaju mogućnost i uplata na račune, cijeli proces se odvija elektroničkim putem bez angažiranja službenika. Štedi vrijeme, smanjuje gužve i troškove na bankovnim šalterima. Može se koristiti 24 sata na dan, a postavlja ga financijska institucija u svojim poslovnicama ili na otvorenom. Unutar svakog bankomata nalazi se računalni sklop (u većini slučajeva PC), čija je osnovna funkcija spojiti se na bankovnu ATM mrežu i za traženog klijenta pristupiti informacijama o njegovom računu. Operacijski sustavi koji se koriste za rad računala u bankomatu mogu biti Windowsi, Unix (Linux) ili drugi.

Sl 3.6. *Uplatno – isplatni bankomat[5]*

Sastavni dijelovi bankomata su:

- Procesor (računalo) – „mozak“ bankomata koji kontrolira korisničko sučelje i uređaje za transakciju
- Čitač kartice (magnetske i/ili čip) – sadrži sve informacije o klijentu i služi za identifikaciju klijenta
- Tipkovnica – klasična tipkovnica slična onoj koja se koristi na kalkulatorima
- Funkcijske tipke – koje se nalaze s lijeve i desne strane zaslona i služe za odabir ponuđenih opcija na samom zaslonu
- Pisač – služi za ispis potvrda o obavljenoj ili neuspjeloj transakciji, ispis stanja računa
- Kućište i svod kućišta – u njega se ugrađuju strojni dijelovi i mehanizmi za obradu koji zahtijevaju autorizirani pristup
- Razni senzori i indikatori

Prilikom korištenja bankomata korisniku je jako bitno da su njegovi podaci cijelo vrijeme zaštićeni i da nitko drugi nema mogućnost na bilo koji način doći do korisnikovih podataka ili novca unutar bankomata. Kako bi se osigurali korisnikovi podaci i sam novac, postoji dvostruka razina sigurnosti na bankomatima:

1. Osiguranje korisnikovih podataka

   – čitač kartice koji je opremljen kriptoprocesorom visoke razine sigurnosti koji osigurava informacije koje korisnik upisuje (npr. PIN broj)

   - u bankomatima je prema zakonu obavezna enkripcija osobnih podataka korisnika (broja kartice i PIN broja), ti podaci se obično kriptiraju koristeći DES sustav kriptiranja, u novije vrijeme se koristi Triple DES

   - za zaštitu prijenosa poruka od bankomata do financijske institucije putem mreže koristi se *Message Authentication Code* (MAC) ili *Partial MAC*

   - čitač kartica također zadržava karticu ako je kartica predugo u bankomatu bez aktivnosti ili ako se više puta uzastopno unese krivi pin

2. Fizičko osiguranje novca

   - sef unutar kućišta bankomata koji se sastoji od više ladica s novčanicama koji je osiguran sa spremnicima boje ili dima kako bi onesposobili novčanice ako im se pokuša nasilno pristupiti

3.2.1 Bankomat – način rada

Karticu lagano umetnuti u otvor bankomata(slika 3.6. broj 2), tako da se čip koji se nalazi na poleđini kartice okrenut prema dolje, iz razloga što se mehanizam za očitavanje čipa nalazi na donjoj strani mehanizma za umetanje kartica . Kad je kartica uvučena, na ekranu će se pojaviti poruka: 'Molimo zaštitite svoj PIN prilikom unosa'. Unesite svoj PIN na tipkovnici za unos zaklanjajući unos drugom rukom zbog sigurnosnih razloga. Na ekranu bankomata će se umjesto svake znamenke upisanog PIN-a pojaviti znak X. Na ekranu bankomata će se pojaviti popis transakcija koje je moguće obaviti. Na bankomatu je moguće obaviti transakcije: isplatu, uplatu (na tekući i žiro račun na određenim bankomatima), upit u stanje računa, kupnju GSM bonova, kupnju zrakoplovnih karata Croatia Airlines itd [5]. Za isporuku novca korisniku aktiviraju se mehanizmi koji biraju potrebne novčanice te iste i isporučuju. Posebni čitači se koriste za očitavanje potrebnih novčanica koje je korisnik zatražio. Također postoje i čitači koji detektiraju je li korisnik uzeo novac. Ako se desi situaciju u kojoj je čitač uzeo više novaca nego je korisnik zatražio novac će se staviti sa strane u poseban pretinac ili ako nema dovoljno novaca korisniku će se na ekranu ispisati poruka koja ga upozorava da u bankomatu nema dovoljno novaca za traženu transakciju. Još jedan bitan mehanizam unutar bankomata je i pisač koji služi za ispisivanje potvrda i raznih izjava korisniku.

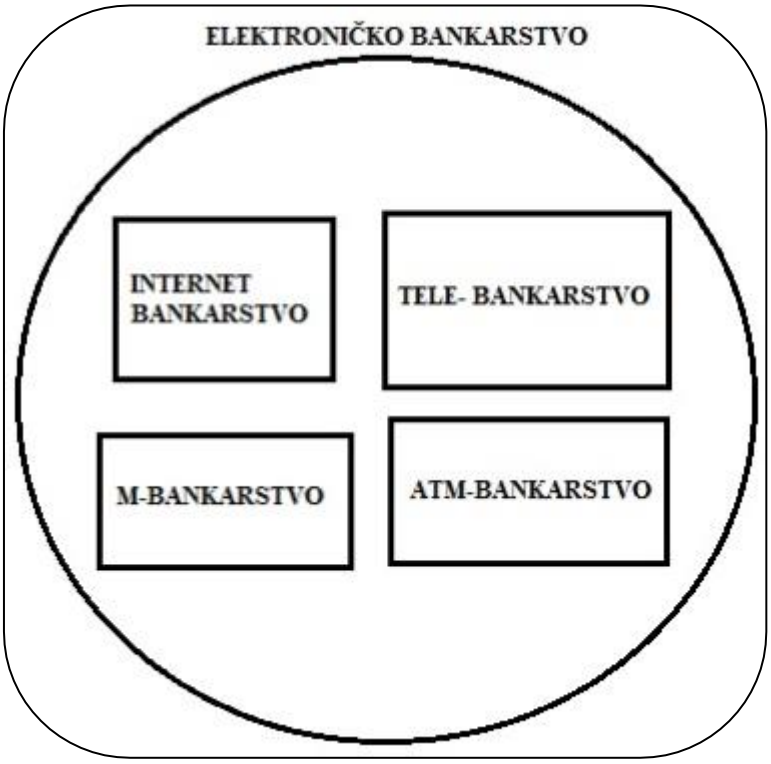
Sl 3.7. *Korisničko sučelje bankomata[13]*

Nakon što korisnik obavi što je htio bankomat „izbacuje“ karticu, na monitoru obavještava korisniku da uzme svoju karticu i ispisuje potvrdu o odrađenoj transakciji ako je opcija ispisa potvrde odabrana od strane korisnika.

3.3. Elektroničko bankarstvo

Elektroničko bankarstvo (e-bankarstvo, eng. e-banking) je najraširenij pojam od navedenih pojmova, jer uključuje pristup bankovnim računima i obavljanje transakcija uporabom informatičke tehnologije koja ne mora nužno koristiti Internetski pristup

E-bankarstvo je automatska isporuka novih i tradicionalnih bankovnih proizvoda i usluga direktno klijentima putem elektroničkih interaktivnih komunikacijskih kanala (FFIEC, 2003) [6] E-bankarstvo obuhvaća i Internet bankarstvo, i telebankarstvo, i m-bankarstvo, i bankarstvo putem bankomata (eng. Automated Teller Machine (ATM)). Klijenti mogu pristupati uslugama e-bankarstva putem elektronskog uređaja, npr. osobno računalo (eng. Personal Computer), bankomat (eng. Automated Teller Machine) ili pametnog telefona.



Sl 3.8. *Opseg elektroničkog bankarstva[13]*

3.4. Internet bankarstvo

Internet bankarstvo je usluga banke koja korisniku omogućava pristup svom korisničkom računu i obavljanje financijskih poslova s bilo kojeg mjesta na kojem postoji računalo, ili bilo koji drugi uređaj, povezan na Internet. Provodi se putem preglednika za pristup sigurnom web mjestu banke na kojem klijent uz pomoć sigurnosnih podataka koje je dobio od banke pristupa svom korisničkom računu.

Internet bankarstvo korisniku omogućava:

- Uvid u stanje računa
- Prijenos novca između računa,
- Izvršavanje pologa na račun,
- Kupovanje deviza i druge aktivnosti.

3.4.1. Preduvjeti za Internet bankarstvo

Uvjete koji su potrebni za funkcioniranje Internet bankarstva možemo podijeliti na preduvjete za banku i na preduvjete za klijente.

Preduvjeti za banku su:

- Postojanje internetske veze, računala poslužitelja i programa web poslužitelja
- Postojanje odgovarajućih programskih web aplikacija (korisničko sučelje)
- Pridržavanje odgovarajućih sigurnosnih protokola i certifikata, te zakonskih propisa o e-dokumentima i e-potpisu

Preduvjeti za klijenta – kako bi klijent mogao koristiti uslugu Internet bankarstva željene banke, potrebno je potpisati ugovor s bankom u kojem se dogovara mjesečna naknada, nakon toga korisnik dobija svoj korisnički broj i PIN broj (ili uređaj koji generira PIN broj iz sigurnosnih razloga), čime se klijentu omogućava korištenje Internet bankarstva te banke.

3.4.2. PBZ365@NET

Internetsko bankarstvo PBZ365@NET namijenjeno je svim klijentima Privredne banke Zagreb koji su vlasnici ili opunomoćenici tekućega računa u kunama, tekućega računa u stranoj valuti, žiroračuna u kunama, žiroračuna u stranoj valuti ili transakcijskoga računa obrtnika.

Korisniku omogućuje pristup bankovnim računima 24 sata dnevno s bilo kojeg mjesta gdje postoji pristup Internetu te, među ostalim, nudi sljedeće funkcionalnosti:

- Pregled stanja i prometa
- Plaćanje financijskih obveza
- Prijenos sredstava s jednog računa na drugi
- Mogućnost zadavanja naloga u najavi, te pregled svih izvršenih naloga
- Ugovaranje police osiguranja
- Uplatu rate kredita, itd...

Za korištenje usluge Internetskog bankarstva PBZ365@NET potrebno je:

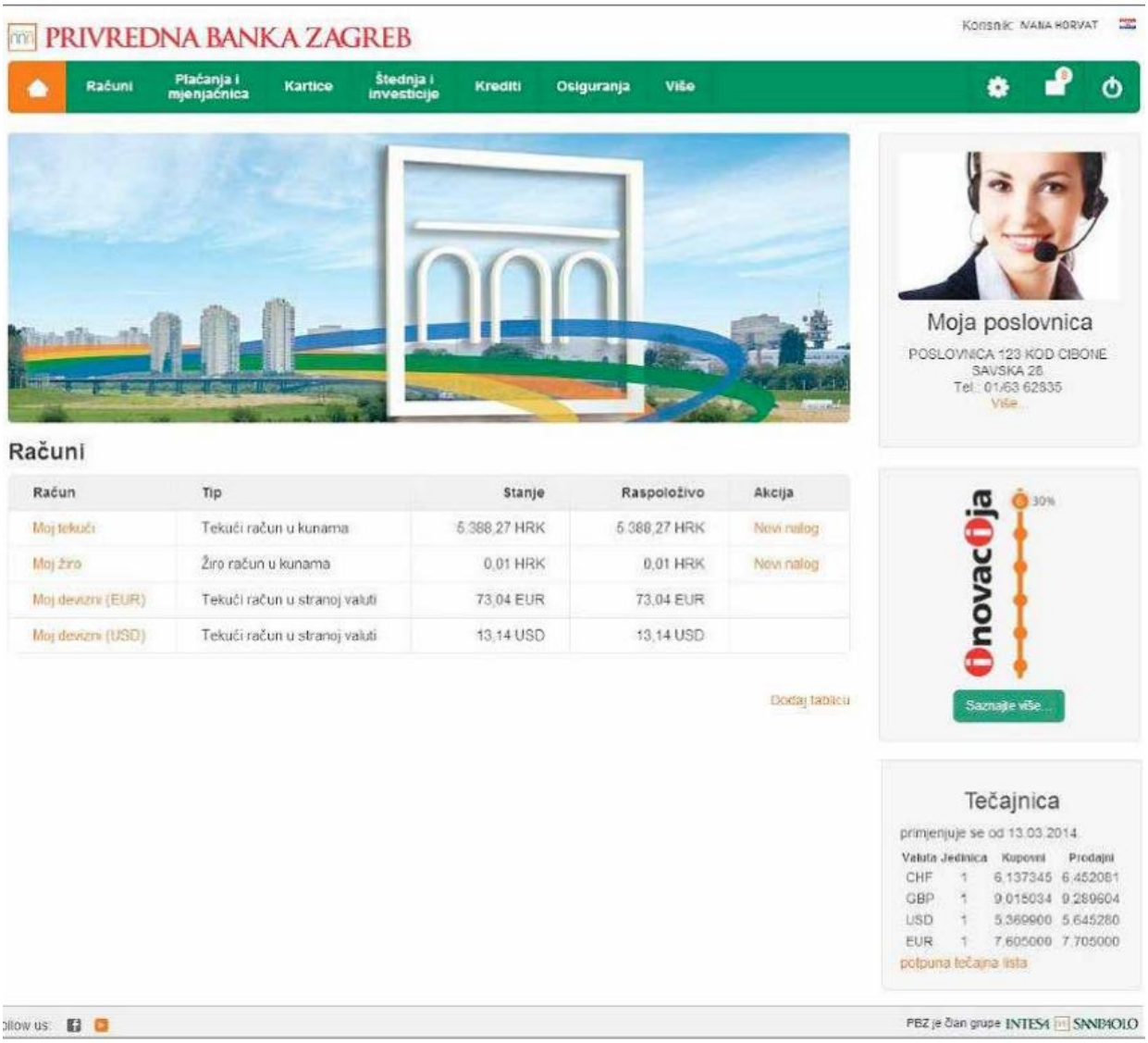
- potpisati Ugovor o korištenju u bilo kojoj poslovnici Privredne banke Zagreb
- preuzeti autorizacijski uređaj
- osigurati minimalne tehničke uvjete, uključujući i pristup Internetu [7].

Sl 3.9. *Ulazna stranica Internet bankarstva PBZ365@NET* [7]

Nakon toga potrebno je uz pomoću korisničkog broja i PIN broja, kojeg korisnik dobija od banke prilikom potpisivanja ugovora, prijaviti se u sustav. Osim prijave preko mToken aplikacije moguća je i prijava uz pomoć čitača kartice. Čitač kartice (Slika 3.10) je identifikacijski uređaj veličine ljudskog dlana koji se sastoji od malog ekrana i tastature s funkcijskim tipkama (isti princip kao i kod džepnog kalkulatora). Radi na principu očitavanja čipa koji se nalazi na korisnikovoj kartici. Kada se kartica umetne u čitač, čitač radi prepoznavanje čipa i na ekranu traži od korisnika da upiše svoj pin, te nakon unosa pina generira i ispisuje na ekranu korisniku jednokratnu zaporku koju korisnik unosi na web stranici Internet bankarstva.

Sl 3.10. *Čitač kartica* [20]

Nakon završetka prijave pojavljuje se glavni izbornik na kojem su prikazani podatci o imenu i prezimenu korisnika, barometar Inovacije,
tečajna lista, aktivni računi te izbornici s dostupnim funkcionalnostima.



Sl 3.11. *Glavni ekran PBZ365@NET usluge* [7]

Pod opcijom računi korisnik ima uvid u sve svoje otvorene račune u toj banci, tipu računa o kojem se radi, te informaciju o raspoloživom iznosu na pojedinom računu ako ih ima više kao što je to prikazano na slici 3.11. Sljedeća opcija je plaćanje i mjenjačnica u kojoj korisnik može obavljati sve platne transakcije, korisnik kreira nalog za plaćanje popunjava potrebna polja u kreiranom nalogu i jednostavnim klikom miša plaća svoje račune. U mjenjačnici korisnik ima mogućnost kupnje i prodaje valute bez odlaska u mjenjačnicu. Pod izbornikom kartice korisnik ima detaljan uvid u svoje kreditne kartice, korisni ima detaljan uvid vezan uz svoju karticu i može vršiti uplatu odabranu karticu. Na kartici štednja i investicija korisniku se omogućava uvid u stanje već napravljeni štednja, oročenja ili investicija ili mu se pruža mogućnost otvaranje nove štednje ili oročenja. U izborniku Krediti moguće je pregledavati detalje, promete, anuitet,

dospjeli dug i ukupno zaduženje kredita i brzih pozajmica, ako ih korisnik ima. Također je moguće pregledavati detalje već otplaćenih kredita i pozajmica te obavljati isplatu sredstava i prijevremenu definitivnu otplatu kratkoročnih i dugoročnih pozajmica, ako ih korisnik ima.
Pod opcijom osiguranje korisnik je u mogućnosti ugovoriti:

- Dopunsko zdravstveno osiguranje
- Potpuno zdravstveno osiguranje
- Osiguranje imovine
- Obvezno osiguranje od automobilske sigurnosti

Ako je korisnik napravio sve što je htio, na kraju rada treba se odjaviti iz aplikacije internetskog bankarstva odabirom ikone za odjavu u gornjem desnom kutu.

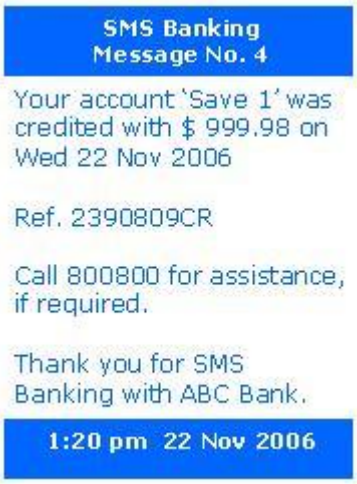
3.5. Mobilno bankarstvo

Mobilno bankarstvo je bankarstvo koje za pristupanje bankovnim uslugama ostvaruje putem pametnih telefona ili tableta. Obično se koriste aplikacije koje su svojim izgledom korisničkog sučelja i načinom autorizacije klijenata prilagođene dimenzijama i tehnološkoj platformi koju nudi klasičan suvremeni pametni mobilni telefon. To znači da će informacije, meniji i sve ostalo što čini uslugu samostalnog bankarstva na ekranu biti prikazane na najkraći mogući način, ali i da će autorizacija biti kudikamo jednostavnija nego na Internetu, obzirom da je mobitel, to jest SIM kartica koja je u njemu - svojim jedinstvenim pozivnim brojem - na neki način već identificiran s vlasnikom. Ako korisnik želi pristupiti svom računu preko mobilnog bankarstva njegov pametni telefon mora biti povezan na neku vrstu Interneta, najčešće su to bežične mreže (WiFi) ili mobilne mreže (3G, 4G) .

3.5.1. SMS bankarstvo

SMS bankarstvo je jedan tip mobilnog bankarstva koje omogućava klijentima obavljanje ograničenog broja usluga putem mobilnog telefona korištenjem SMS sustava poruka. SMS (Short Message Service) je sustav za razmjenu kratkih poruka (duljine do 160 znakova) putem mobilnih i fiksnih telefona koristeći standardne telefonske protokole (GSM) . SMS bankarstvo koristi PUSH I PUL poruke. Pod PUSH poruke spadaju informacije koje banka šalje klijentu bez da je klijent poslao upit (mobilni marketing, novosti banke ili jednokratna zaporka koja se koristi kao zaštita od prijevara, pri čemu se korisniku svaki put kada pristupa SMS bankarstvu šalje nova jednokratna lozinka). PULL poruke su poruke koje klijent šalje banci koristeći

mobilni uređaj i tražeći informacije ili prilikom obavljanja transakcije (kada klijent želi vidjeti stanje svog računa ili valutni tečaj i dr.) .



Sl 3.12. *Primjer poruke u SMS bankarstvu* [13]

3.5.2. Bankarstvo na dlanu - mPBZ

mPBZ mobilno bankarstvo je usluga koja omogućuje, putem mobilnog uređaja, brz i jednostavan pristup informacijama vezanim uz usluge i proizvode koje klijent ima u PBZ-u uz mogućnost provođenja financijskih transakcija. Usluga je namijenjena svim klijentima Privredne banke Zagreb koji su vlasnici ili opunomoćenici tekućeg ili žiro računa.

Usluga mPBZ koristi se putem mPBZ programske podrške instalirane na mobilni uređaj. Unutar programske podrške implementiran je token koji služi za identifikaciju korisnika i autorizaciju naloga zadanih putem mPBZ usluge.

Preduvjeti za korištenje mPBZ usluge:

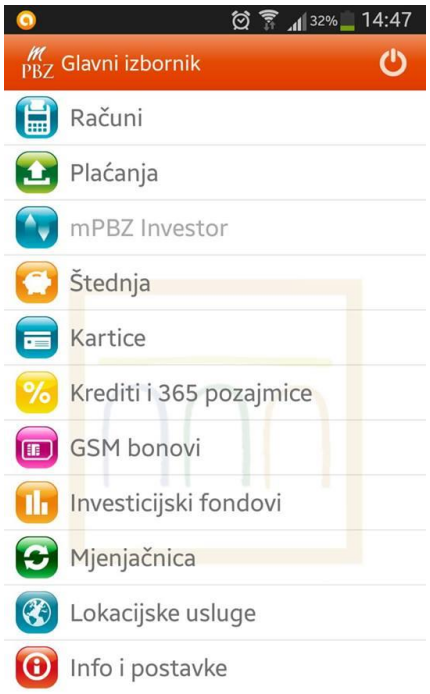
- Mobilni telefon koji podržava Java2 Mobile Edition (J2ME) verzije MIDP 2.0 i CLDC 1.1
- Dovoljno memorije za spremanje programske podrške na mobilni uređaj (oko 300 kB slobodno memorijskog prostora za pohranu svih datoteka koje dolaze s aplikacijom i njezinim instaliranjem na uređaj, a to uključuje sve datoteke koje nastaju prilikom programiranja takvih aplikacija i prilikom njihovog izvršavanja na samom uređaju)
- Korisnik mora imati omogućen GPRS pristup Internetu s mobilnog uređaja (ispravno konfigurirane postavke za spajanje na Internet) [8]

Prilikom pokretanja mPBZ aplikacije na zaslonu ekrana vašeg mobilnog uređaja će se pojaviti identifikacijski ekran., koji od korisnika traži unos token PIN-a, pomoću kojeg korisnik pristupa samoj aplikaciji i svom korisničkom računu.

Java Platform, Micro Edition (JME ili J2ME) je platforma bazirana na javi koja pruža fleksibilno okruženje za aplikacije na mobilnim i drugim uređajima.
Mobile Information Device Profile (MIDP) omogućava pisanje aplikacija i usluga za mobilne mrežno-spojne uređaje, koja u kombinaciji s CLDC-om čini java okruženje za mobilne uređaje i omogućuje pokretanje java orijentiranih aplikacija.
Connected Limited Device Configuration (CLDC) definira osnovni skup sučelja za programiranje aplikacija za mobitele a u kombinaciji s MIDP, ona pruža čvrstu Java platformu za razvoj aplikacija koje će se pokretati na uređajima s ograničenom memorijom, procesorskom snagom i grafičke mogućnosti.

General Packet Radio Services (GPRS) je stariji standard bežične komunikacije koji je dostupan mobilnim uređajima druge i treće generacije koji koriste GSM (*eng. Global System for Mobile communications*). Komunikacija (mreža) se ostvaruje prospajanjem paketa, što omogućuje kvalitetniju iskoristivost mreže zato što se resursi zauzimaju samo onda kada su stvarno potrebni. Zbog svoje kvalitete, brzine i pouzdanosti omogućio je razvoj korisničkih aplikacija raznovrsnih sadržaja.

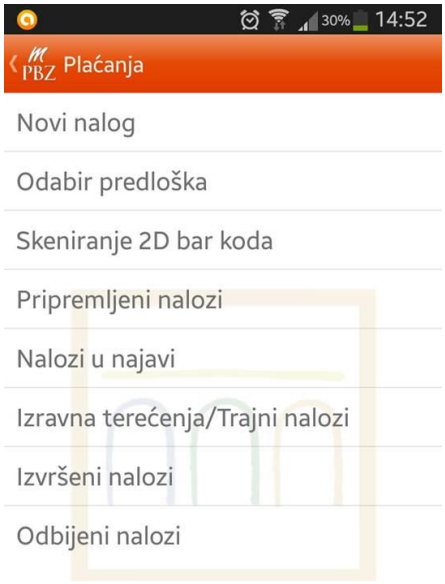
Sl 3.13. *Identifikacija korisnika[13]*



Sl 3.14. *Glavni izbornik mPBZ[13]*

Nakon odrađene identifikacije, koja je puno jednostavnija u odnosu na Internet bankarstvo, dolazimo do glavnog izbornika koji se sastoji od nekoliko opcija, kao što je prikazano na slici 3.14.Odabiremo opciju računi i na zaslonu nam se pojavljuje novi ekran s popisom svih otvorenih računa u banci. U nastavku možemo, ukoliko nas to zanima, odabrati jedan od računa i vidjeti detaljan ispis prometa koji je napravljen za taj račun.

Sl 3.15. *Pregled računa [13]*



Sl 3.16. *Opcije plaćanja[13]*

Pod opcijom plaćanje ulazimo u dio koji je namijenjen za brzo i jednostavno plaćanje račun, odabirom stavke skeniranje 2D bar koda, pametni telefon pomoću svoje ugrađene kamere skenira 2D bar kod s računa i na zaslonu kreira već ispunjen nalog za plaćanje jedino što korisniku preostaje je potvrditi plaćanje naloga ponovno upisujuću svoj token PIN.
Korisnik ima mogućnost i sam ispuniti nalog odabirom opcije novi nalog, gdje je formiran prazan obrazac naloga koji korisnik ispunjava, po završetku također je potrebna autentifikacija upisivanjem token PIN-a.

3.6. Telefonsko bankarstvo

Telefonsko ili tele-bankarstvo je usluga financijske institucije preko koje je klijentima omogućeno obavljanje financijskih transakcija putem fiksnog telefona, bez potrebe za posjećivanjem banke ili bankomata. Ako je ipak potrebno angažiranje službenika banke putem telefona, tada se ona može obaviti u radno vrijeme službenika, koje može biti i duže od redovitog radnog vremena poslovnice banke.
Prednosti:

- Raspoloživost i nakon radnog vremena poslovnice
- Smanjuje troškove obavljanja transakcije, jer klijent ne mora doći u poslovnicu

Nedostaci:

- Ako radno vrijeme službenika nije 24/7 tada tele-bankarstvo nije moguće stalno kao Internet bankarstvo
- Neke banke ne omogućavaju pristup svim računima putem tele-bankarstva

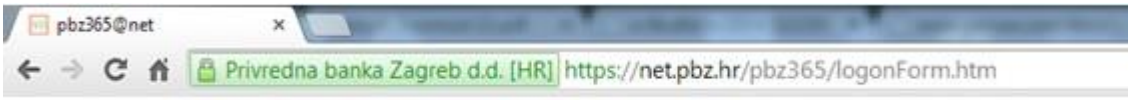
Postupak provođenja telefonskog bankarstva:

1. Klijent treba biti registriran za ovu uslugu kod banke, dobiti lozinku za autorizaciju (lozinka za tele-bankarstvo u pravilu je različita od one za Internet bankarstvo) i korisnički broj
2. Banka mora imati mogućnost alocirati brojeve telefona klijenta
3. Za pristup tele-bankarstvu, klijent treba sa svog telefona nazvati poseban telefonski broj banke koji dobiva od banke za tu svrhu.
4. Pomoću korisničkog broja i lozinke klijent može pristupiti svom računu (tekućem, kreditnom, štednom, kreditnoj kartici i dr.). Neke banke imaju i dodatne korake za autorizaciju (npr. Korištenje i numeričke i glasovne lozinke, ili odgovaranje na nekoliko sigurnosnih pitanja koja postavlja službenik banke).

4. SIGURNOST INTERNET BANKARSTVA

Sigurnost i zaštita Internet bankarstva je problem kojem treba posvetiti najviše pažnje, jer je korisniku ispred svega najvažnije da je njegov novac u banci siguran. Danas je briga o sigurnosti puno više od nabavke sigurnih sefova za novac. Razvojem e-bankarstva, sigurnost postaje više softverski problem (Al-Khatib, 2012) [3]

Kada se radi o Internet bankarstvu i poslovanju preko Interneta pojavljuju se rizici i može doći do narušavanja sigurnosti. Internet poslovanje se uglavnom odvija putem internetske mreže. Internet je javni medij, komunikacija na njemu je otvorena i nema formalnih mehanizama kontrole. Rizici kod korištenja Internet bankarstva obično se odnose na pokušaje prevare od strane trećih lica ili različitim pogreškama u obradi informacija. Razina sigurnosti za obavljanje transakcija putem Internet bankarstva utječe i na sustav internet bankarstva kojim se banka služi.
U Internet poslovanju banke se koriste različitim algoritmima za siguran protok podataka kroz internetsku stranicu. Banke koje posluju na području Republike Hrvatske se koriste SSL algoritam (eng. Secure Socket Layer). Prilikom ulaska na korisničko sučelje za prijavu na Internet bankarstvo ulazimo u sigurno zonu koju možemo prepoznati tako što u adresnoj traci Internet preglednika umjesto http piše https i pokraj se nalazi slika lokota.



Sl 4.1. *Secure Socket Layer(SSL) web korisničkog sučelja[7]*

Postoje dva osnovna područja na kojima bi banke trebale štiti podatke:

1. Mreža - napadi na komunikacijsku mrežu banke najčešće su u obliku upada haker-a i krađe podataka pri njihovom prijenosu mrežom. Mjere prevencije su koristiti jake sustave enkripcije onih podataka koji se prenose putem mreže
2. Hardverska i softverska oprema - napadi na hardver i softver banke mogu biti s ciljem onemogućavanja njihovog funkcioniranja (tzv. Denial of Service – DoS napadi) ili s ciljem logiranja kao uljez koji će neovlašteno obaviti neku transakciju ili postaviti virus kako bi se urušio sustav. Mjera prevencije za ove napade su vatrozidi (eng. Firewalls) na točkama gdje se oprema banke spaja s mrežom.

Rizici narušavanja sigurnosti su veliki, ali postoje metode zaštite koje banke primjenjuju da se ti rizici smanje što je više moguće. Potrebno je napraviti strategiju upravljanja sigurnošću, dokument u kojem tvrtka, u ovom slučaju banka, detaljno razrađuje postupke za očuvanje sigurnosti Cilj strategije je omogućiti neometano i sigurno odvijanje svih dijelova poslovanja.
Prilikom razradnje strategije potrebno je pripaziti na nekoliko detalja:

1. Potrebno je isplanirati sigurnosne sustave za svaki dio poslovanja, svi dijelovi poslovanja su važni
2. Stalno ulagati u nove sigurnosne sustave, što uključuje financijska ulaganja u sustave i stručno usavršavati osoblje zaduženo za održavanje sustava

Načini na koje se može ugroziti sigurnost poslovanja su:

- Krađa hardvera digitalnog sadržaja ili softvera
- Intenzivnim napadima na ranjiva područja (pretrpavanje poslužitelja nebitnim zahtjevima koje izaziva pad sustava)
- Pokretanje virusa ili malicioznih programa kojima se napada software ili hardware
- Neovlašteno pristupanje (skrivanje IP adresa, probijanje lozinki)

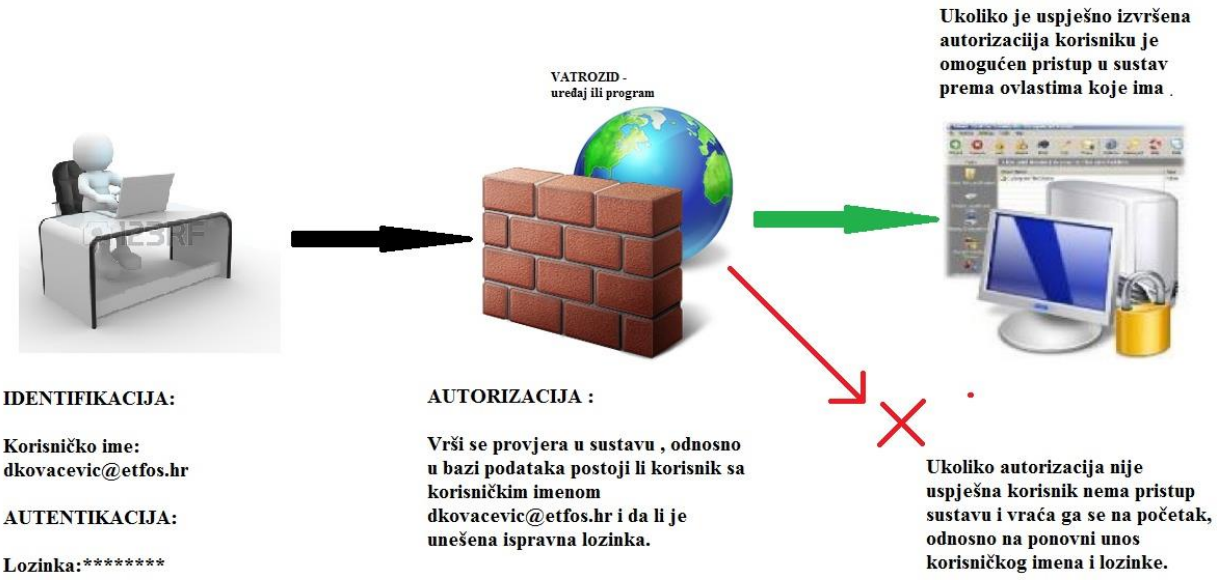
Zbog gore navedenih načina ugrožavanja sustava postoje određeni mehanizmi i tehnike zaštite kako bi se spriječili bilo kakvi pokušaji napada na sustav.

Prvi od mehanizama je identifikacija, autentikacija i autorizacija:

- Identifikacija je postupak prilikom kojeg se od korisnika traži upisivanje imena i prezimena, identifikacijskog broja ili korisničkog imena koje je dobio od banke
- Autentikacija je postupak povezan s identifikacijom, a dokazuje da li je osoba koja se pokušava ulogirati na stranicu zaista ta osoba za koju se predstavlja, za autentifikaciju se koriste tri najčešća načina:
    1. nešto što korisnik zna (lozinka, PIN itd)
    2. nešto što korisnik ima (pametna kartica, TAN tablica, stick i sl.)
    3. nešto što korisnik jeste (biometrija – otisak prsta, rožnica oka, rukopis i sl.)

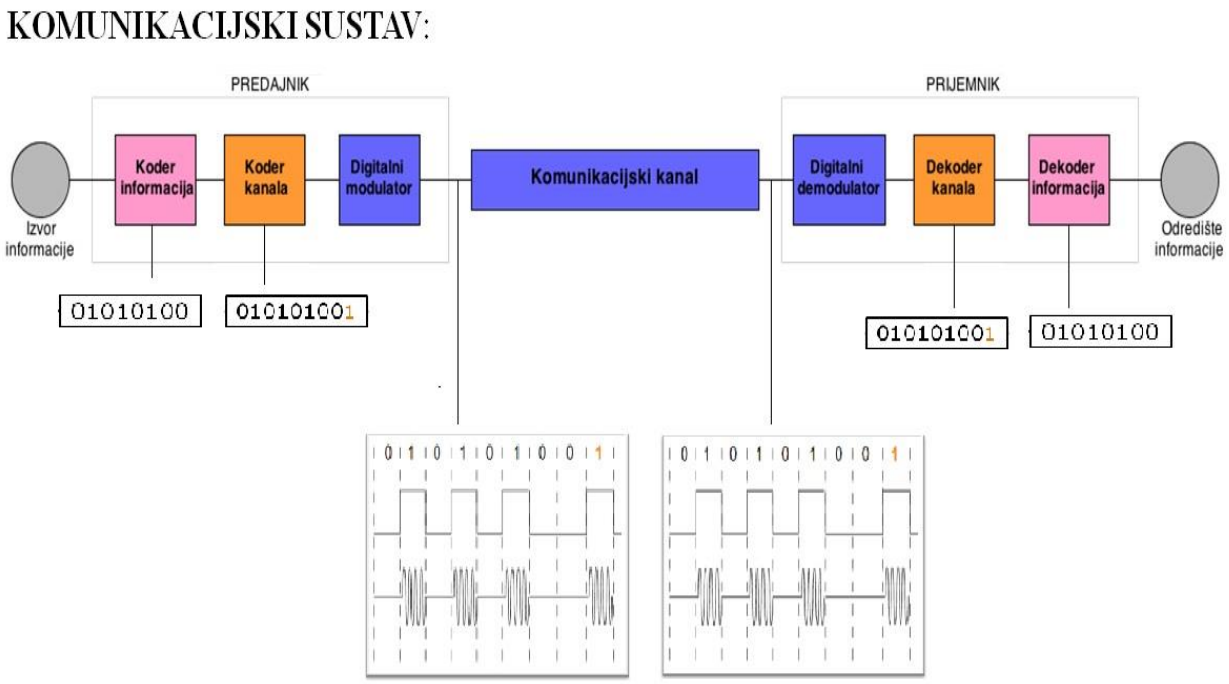
    - prilikom autentikacije najvažnije je podatke koje korisnik upisuje zaštiti pri prijenosu kako korisnik ne bi postao meta napada i iskorištavanja
- Autorizacija je postupak provjere sustava u kojoj se provjerava da li osoba koja se predstavila sustavu ima ovlasti pristupanja samom sustavu (provjera s unaprijed pohranjenim podacima unutar sustava)

Autentikacija i identifikacija se može provesti na dva načina. Prvi je pomoću fizičke mjere gdje korisnik posjeduje nekakav predmet, najčešće su to identifikacijske kartice, pametne kartice, token uređaj. Drugi način je pomoću logičke mjere koja se odnosi na lozinku, koju bi samo korisnik trebao znati.



Sl 4.2. *Identifikacija, autentikacija i autorizacija[13]*

Drugi mehanizam se odnosi na zaštitu tajnosti prilikom prijenosa podataka. Prilikom zaštite tajnosti podatak koji se prenose računalnim mrežama koriste se metode šifriranja (kriptografija, kriptoanaliza). Kriptografija je postupak kojim se originalna poruka napravi nerazumljiva osobama koje nisu sudionici komunikacije, a zatim se kriptoanalizom radi obrnuti postupak, odnosno primalac poruke uz pomoć pronalaženja tajnog ključa enkriptirane poruke vidi njezin sadržaj, tj. originalnu poruku.



Sl 4.3. *Kriptiranje podataka i kriptoanaliza[12]*

Treći mehanizam je obrana od virusa. Mjere zaštite protiv virusa mogu se podijeliti u dvije skupine:

- Mjere preventivne zaštite – korisniku se preporučuje izbjegavanje upotrebe sumnjivih programa, otvaranje poruka nepoznatog podrijetla, redovito spremanje sigurnosnih kopija svojih datoteka i programa i upotreba antivirusnih programa za detektiranje virusa
- Mjere za već nastalu štetu – pokušati spasiti podatke i programe poslovanja, koristiti antiviruse za čišćenje virusa (ako je potrebno obrisati zaražene datoteke i njihov sadržaj)

Najkorišteniji antivirusni programi koji mogu obaviti gore navedene zadaće su AVG, McAfee Antivirus, Esset NOD32, BitDefender, F-prot, HouseCall. Ako dođe do zaraze virusom postoji mogućnost nekontroliranog slanja mail poruka (eng. spam), šalje se veliki broj poruka velikom broju korisnika u jako malom vremenskom razdoblju. Korisnik nije ni svjestan operacija koje se dešavaju jer virus sam obavlja slanje spam poruka. Kako bi se spriječilo slanje spam poruka korisnik bi treba koristiti anti spam programe kao što su AddAware, StopZilla, Panda Titanium Antivirus + Antismap i dr.

4.1. Sigurnost Internet bankarstva u Republici Hrvatskoj

Podaci iz 2006. godinu pokazuju da je 2/3 transakcija izvršeno kroz elektroničke kanale - bankomate, mobitele, Internet, itd. U tom vremenskom periodu otkako se Internet korisit u poslovanju banaka nije zabilježen niti jedan incident ili pokušaja krađe podataka . To znači da bankarski sustav u cijeloj Republici Hrvatskoj nije radio nikakve kompromise po pitanju sigurnosti, pogotovo ne na Internetu .

Nasuprot tome, imamo primjere iz Velike Britanije i Slovačke i drugih zemalja gdje su banke oštećene napadom na sustave Internet bankarstva metodama poput phishinga, jer su koristile najslabiju metodu autorizacije, a to su: korisničko ime i zaporka (eng. *user name & password*). Većina banaka u Republici Hrvatskoj koristi najsuvremenije i najsigurnije sigurnosne tehnologije, a to su PKI pametne kartice ili tehnologija jednokratnih zaporki (eng. one time password) pomoću ručnih kripto uređaja tzv. Tokena [11].

Uz sve vrste zaštita koje banke posjeduju ipak dolazi do proboja sigurnosti, te tako imamo novije primjere kao što su hakiranje stranica Karlovačke banke kao i Samoborske banke iz 2012. godine. Hrvatska Narodna Banka je sredinom 2014. godine upozorila građane na hakerske napadaje koji su s bankovskih računa građana i poslovnih subjekata uzimali veće količine sredstava.

Najčešći oblici prevara koje se mogu susresti na našim prostorima su upotreba zlonamjernih programa (virusa, trojanaca i sličnih) koji se šalju korisnicima na njihove e-mail adrese. Sadržaji tih e-mail poruka su većinom linkovi koji preusmjeravaju korisnike na lažne Internetske stranice njihovih banaka i traže autorizacijske podatke od korisnika, stranice koje izgledaju autentično izvornim stranicama. Prevaranti su u mogućnosti napraviti identične stranice zato što su stranice pisane HTML-om (opisni jezik za izradu web stranica) i njegov kod je dostupan svima. Glavni cilj prevaranata je korištenje podataka koje su im korisnici nesvjesno proslijedili je otuđivanje novčanih sredstava korisnika. Ovakvim metodama se posebno ciljaju poslovni korisnici koji najviše koriste Internet za autoriziranje transakcija s karticama ili nekim drugim metodama spomenutim u ovom radu. Korisnike se informira ukoliko primijete bilo kakve nepravilnosti iste odmah prijave svojim bankama.

```
53
54 <style>
55 .sirius-hidden {
56     display: none;
57 }
58
59 .sirius-visible {
60     visibility: visible;
61 }
62 </style>
63 </head>
64 <body class="logon-body">
65
66     <input type="hidden" value="/pbz365" id="ctx" />
67     <input type="hidden" value="" id="showCardExpiration" />
68     <input type="hidden" value="" id="errors" />
69     <input type="hidden" value="" id="enteredUsername" />
70     <input type="hidden" value="" id="selectedTab" />
71     <input type="hidden" value="/pbz365" id="ctx" />
72     <input type="hidden" value="https://investor.pbz.hr/PbzInvestorWeb/logon/logonPbzInvestor.html" id="investorLogonUrl" />
73     <input type="hidden" value="PROD" id="deploymentLocation" />
74     <input type="hidden" value="8.23.8" id="version" />
75     <input type="hidden" value="true" id="minifiedJs" />
76     <input type="hidden" value="false" id="consoleLog" />
77
78     <div class="container">
79         <noscript>
80             <style type="text/css">.no-js { display: none; }</style>
81             <div class="dialog dialog-danger" style="text-align:left;">
82                <div class="span1" style="margin-top:10px">
83                    <i class="fui-cross" style="color: red; text-shadow: 1px 1px #000000;"></i>
84                </div>
```

Sl 4.4 *HTML kod autorizacijske stranice za pristup računim[7]*

5. ZAKLJUČAK

Razvoj informacijskih i telekomunikacijskih tehnologija direktno utječe na razvoj društva i na globalizaciju, veliki utjecaj imao je i u napredovanju Internet bankarstva u relativno kratkom vremenskom razdoblju. Od pojave informatičke tehnologije u bankarstvu, bankarstvo je napravilo golemi napredak prema naprijed u svom poslovanju, ne samo u uslužnom pogledu nego i u cjelokupnom sustavu koji čini suvremenu banku.

Kroz ovaj rad je napravljena analiza korištenja informatičkih tehnologija koje se pokazuju nužne za poslovanje suvremenih banaka. Bilo da se radi o infrastrukturi i fizičkim uređajima (hardverskim dijelovima) ili logičkim i programskim komponentama (softverskim dijelovima) sustava. Kroz nekoliko primjera je pobliže objašnjena funkcionalnost i izrada pojedinih tehnologija koje se koriste. Uvodom rada prikazan je kratak opis informacijskog sustava i glavnih komponenata koje ga tvore. Potom su pobliže objašnjene pojedine komponente, informacijskog sustava, odnosno hardverski i programski dijelovi sustava, kroz tekstualni opis i vizualnu predodžbu uz upotrebu slikovitog prikaza ili autohtonih slika. Kroz nekoliko primjera kroz rad je prikazana upotreba gore navedenih komponenata pomoću fizičkih uređaja, kao što su bankomati, čitači kartica, i programskih aplikacijskih, koje uključuju mobilne aplikacije i internetske stranice koje korisnicima omogućava brz i jednostavan pristup svojim korisničkim podatcima i bankovnim računima. Radom je ukazano na prednosti i nedostatke koji su prisutni primjenom informatičke tehnologije u bankarstvu poput izbjegavanja čekanja u dugačkim redovima u poslovnicama banaka, mogućnosti pristupanju korisničkim računima iz udobnosti svojeg doma, itd. Posebna pozornost pri istraživanju literature i pri pisanju ovog rada ukazana je na sigurnost u korištenju tehnologije i Interneta u bankarstvu. Zaštita podata i korisnika ima vrlo visoku važnost u modernom bankarstvu. Banke s razvojem tehnologije razvijaju i nove vrste zaštita svojih klijenata, najbolji primjeri toga su zamjena magnetskih traka na kraticama s čipovima koje je vrlo teško iskopirati ili skenirati, pristup podacima preko Interneta se provodi kroz sigurne kanale (SSH tuneliranje) uvode se višestruke jednokratne zaporke koje se generiraju na zahtjev korisnika, itd.

Primjena informatičke tehnologije u bankarstvu u današnje doba zauzima gotovo sve aspekte poslovanja. Izvjesno je da će tehnologija u nadolazećim godinama strahovito brzo napredovati, a samim time možemo očekivati napredak i inovacije u tehnologijama koje se koriste u bankama i bankarskim sustavima . Veliki napredak i modernizacija se može očekivati u načinu i tehnologiji na kojima će se u budućnosti obavljati bankarske usluge, plaćanja i interakcija između klijenta i

banke. Uz napredak izvedbe samih usluga i potrebno je obratiti pažnju i na mehanizme i tehnologiju koji će u budućnosti biti upotrijebljeni za implementaciju sigurnosti i zaštitu podataka.

LITERATURA

[1] Online Banking Report,[http://www.onlinebankingreport.com] (zadnji pristup 01.06.2015)

[2] Hrvatska Narodna Banka, [http://www.hnb.hr] (zadnji pristup 05.06.2015)

[3] Al-Khatib, A.L., E-Banking: Survey, International Journal of Advanced Research in Computer Scienceand Software Engineering, Volume 2, Issue 10, October 2012. [http://www.ijarcsse.com/docs/papers/10_October2012/] Volume 2 - V2I10-0015.pdf (zadnji pristup 02.06.2015)

[4] David S. Linthicum, Leveraging EA Concepts to Make Your SOA a Guaranteed Success [http://semanticommunity.info/@api/deki/files/7623/=EA07_Keynote_Linthicum.pdf] (zadnji pristup 02.06.2015)

[5] Privredna banka Zagreb [http://www.pbz.hr/bankomati#.VBjH-fl_uwk] (zadnji pristup 02.06.2015)

[6] Federal Financial Institutions Examination Council, [http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques] (zadnji pristup 05.06.2015)

[7] Privredna Banka Zagreb, [http://onlinebanka.pbz.hr/pbz365]

[8] Privredna Banka Zagreb, [http://onlinebanka.pbz.hr/dokumenti/Korisnicka_uputa_za_mPBZ.pdf] (zadnji pristup 15.06.2016)

[9] http://en.wikipedia.org/wiki/Telephone_banking (zadnji pristup 15.06.2016)

[10] Privredna banka Zagreb, [http://onlinebanka.pbz.hr/pbz365-tel.html#.VBHE-_l_uwk] (zadnji pristup 15.06.2016)

[11] Informatička tehnologija u poslovanju, infoTrend broj 154/101/2007 [http://arhiva.trend.hr/pdf/IT154.pdf], str. 40 – 43 (zadnji pristup 22.04.2015)

[12] Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek,

Komunikacijske mreže, auditorne vježbe, fizički sloj (1.Djelotvornost komunikacije)

[13] Izvor : autor

Dodatna literatura:

[14] http://www.combis.hr/rjesenja-i-usluge/po-vrsti/aplikativna-rjesenja/combanking

(zadnji pristup 05.06.2015)

[15] http://www.banksoft.hr/banksoft/banksoft-suvremeno-bankarsko-okruzenje

[16] https://en.wikipedia.org/wiki/SMS_banking (zadnji pristup 05.06.2015)

[17] MyBankTracker, Taking A Look Inside An ATM Machine,
http://www.mybanktracker.com/news/2010/05/12/taking-a-look-insidean-atm-machine/

(zadnji pristup 02.06.2015)

[18] Shetty, S., SMS banking, http://paladion.net/sms-banking/ (zadnji pristup 06.06.2015)

[19] Tieto, White paper: Front-end transformation,
[http://www.tieto.com/sites/default/files/files/whitepaper_front-end_1005_web.pdf]

(zadnji pristup 06.06.2015)

[20] Privredna Banka Zagreb, [http://onlinebanka.pbz.hr/citac-kartica.html#.V-vnJ_mLRpg]

(zadnji pristup 16.09.2016)

SAŽETAK

Ovim završnim radom bit će opisano i kroz primjere pokazano kako se u suvremeno informatičko doba primjenjuje informatička tehnologija u bankarskom sustavu. Samim razvojem Interneta i internetske tehnologije paralelno su se razvijale i bankarske informacijske tehnologije zato što su banke uvidjele veliki potencijala koji tehnologija pruža u njihovom radu. Kroz rad je objašnjena infrastrukturni dio (hardware) i programski dio (software) tehnologija koje se koriste u bankama. Preko fizičkih uređaja poput bankomata sve do aplikacija koje korisnicima omogućavaju obavljanje velikog broja usluga za koje bi obično morali stajati u redovima u poslovnicama banaka. Kroz primjere opisana je funkcionalnost i prednosti koje svojom upotrebom u bankarskim sustavima donosi tehnologija i njezin razvoj od samog početka pa sve do danas. Iako tehnologija zamjenjuje sve veći broj usluga koje se mogu obavljati bez odlaska u poslovnicu banke i usluga za koje je prije bio neophodan ljudski faktor, kroz istraživanje ove teme uviđa se kako će uvijek postojati potreba za ljudskim resursima u radu suvremenih bankarskih sustava. Zaštita podataka i sprječavanje njihove zloupotrebe na štetu korisnika, zauzimaju veliki dio unutar upotrebe suvremene tehnologije u bankarskim sustavima. Od enkripcije i zaštite podataka do višestrukih unosa jedinstvenih zaporki za pristup željenom sadržaju samo su neke od metoda zaštite koje se koriste. Sukladno razvoju informatičke tehnologije koja se svakodnevno primjenjuje u bankama, paralelno se razvijaju, nadograđuju i implementiraju novi načini zaštita korisnika i njihovih podataka od mogućih prijevara i štete koja eventualno može nastati ako korisnikove informacije dospiju u krive ruke.Sa daljnjim razvojem tehnologije i Interneta kao medija koji se sve više koristi u svakodnevnom radu suvremenih bankarskih sustava, postoji potreba, a i poželjno je, da se svakodnevno osmišljavaju i implementiraju nove vrste zaštita podataka i autorizacija pristupa istima koje čine upotrebu tehnologije u bankarskim sustavima zaštićenima i na vrlo visokoj sigurnosnoj razini što u konačnici za krajnjeg korisnika znači sigurno i transparentno korištenje usluga. Radom je ukazano na smjernice za detaljnija istraživanja i proširenja u području koje se progresivno razvija, te je u današnje doba nužan kao sastav i potpora u svim poslovnim sustavima, pa tako i u suvremenim bankarskim sustavima.

Ključne riječi:

Internet**,** banka, tehnologija,informacijski sustav,arhitektura, bankomat, mobilno bankarstvo, Internet bankarstvo, zaštita podataka, sigurnost internet bankarstva.

Application of information tehnology in banking

ABSTRACT

This final work will be describing and through the examples showing how information technology is applied in the banking system in the modern information age. As the Internet and Internet technologies have been developing, the banking information technology has been developing along side with it, because the banks have realized the great potential that technology offers in their everyday work. Through the paper it is explained the infrastructure (hardware) and software part of technologies used in banks. Through physical devices such as ATM's to applications that allow users to perform a large number of services that would normally required of users to stand in lines waiting to speak with bank tellers. Through several examples the paper describes and explains the functionality and advantages of its use in banking systems technology provides and its development from the very beginning until today. Although technology replaces a large number of services that can be done without going to a bank branch and services that used to be able to be completed only with a help of a bank teller, trough research of this topic it is recognized that there will always be a need for human interaction in the work of modern banking system. Data protection and the prevention of their abuse to the detriment of users, occupy a large part in the use of modern technology in the banking system. From usage of encryption and data protection to multiple entries of unique passwords, to access the desired content, are just some of the methods of protection used. In accordance with the development of information technology that is used daily in the banks,it is essential to develop, build and implements new ways to protect users and their data against possible fraud and damages that may possibly arise if the user's information gets into the wrong hands .With further development of technology and the Internet as a medium which is increasingly used in the daily work of modern banking system, there is a need, and it has become a standard for every day devising and implementation of new types of data protection and authorization access to data, in order to make use of technology in the banking system protected and on very high security level which ultimately for end-user means a safe and transparent use of services. The paper also points to the guidelines for further research and extension in an area that is progressively developing, and in modern age as a necessary structure and support in all business systems, including the sovereign banking system.

Keywords:

Internet, bank, technology, information systems, architecture, Automated Teller Machine (ATM), mobile banking, internet banking, data protection, internet banking security.

ŽIVOTOPIS

Dario Kovačević rođen je 28. ožujka 1993. godine u Sremskoj Mitrovici. Od 2007. do 2011. godine pohađao je Elektrotehničku i prometnu školu Osijek gdje je stekao zvanje Tehničara za računarstvo. Nakon završene srednje škole od 2011. godine pohađa Elektrotehnički fakultet Osijek, koji danas nosi naziv Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek. Pohađa sveučilišni preddiplomski studij smjer računarstvo. Za vrijeme studiranja sudjelovao je u programu kulturne razmjene gdje je 6 mjeseci proveo u Sjedinjenim Američkim Državama u saveznoj državi Wyoming usavršavajući znanje stranog jezika i otkrivanju novih kultura i ljudi. Trenutno je zaposlen u NTH Mediji kao Operations Manager gdje do izražaja dolaze stečena znanja iz raznih predmeta koje je slušao tijkom svog školovanja na Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, te se nada kako će se nastaviti usavršavati i ispunjavati zahtjeve i zazove koji se pred njega svakodnevno stavljaju.