INTERNACIONALNI UNIVERZITET TRAVNIK
INTERNATIONAL UNIVERSITY OF TRAVNIK

FAKULTET INFORMACIONIH TEHNOLOGIJA
INFORMACIONE TEHNOLOGIJE

SVIJET U MOBILNOM BANKARSTVU

Predmet: **Završni rad**
Mentor: Prof. Dr. Mladen Radivojević

Student:
Imran Kasumović
FIT-02/16-I

Travnik, juli 2019.

Sadržaj

1. Uvod 4
2. Historija mobilnog bankarstva 6
3. Mobilno bankarstvo 7
   3.1. Tehnički elementi mobilnog bankarstva 8
   3.2. Pristup potrošača mobilnim telefonima 10
   3.3. Trendovi korištenja i plaćanja putem mobilnog bankarstva 11
4. Kanali za tradicionalne i postojeće distribucije 12
   4.1. Tradicionalni kanali 12
   4.2. Emergant kanali 13
5. Tehnologije i standardi za multikanalno bankarstvo 14
6. Multikanalna bankarska arhitektura 16
   6.1. Korisnički uređaji 16
   6.2. Distributivna mreža 17
   6.3. Gateways 18
   6.4. Kontrole pristupa 18
   6.5. Aplikacije specifične za kanal 18
   6.6. Integracijske usluge 19
   6.7. Core banking platforme 19
7. Analiza arhitekture: Interakcije sistema 19
   7.1. Korisnik prenosi sredstva na drugu banku koristeći Web kanal 20
   7.2. Klijent se prijavljuje za povećanje limita kreditne kartice pomoću kanala za mobilne uređaje 21
   7.3. Kupac vrši kupovinu koristeći eWallet koristeći Point of Sale Channel 21
8. Opcije implementacije platforme za mobilno bankarstvo 23
   8.1. Arhitektura visokog bankarskog kanala 23
   8.2. Nivoi implementacije platformi mobilnog bankarstva 24
   8.3. Platforma za mobilno bankarstvo Arhitektura visokog nivoa 25
9. Tehnologije mobilnog bankarstva za prijenosne tehnologije 26
   9.1. SMS bankarska rješenja 27
   9.2. Interaktivni glasovni odgovor (IVR) 28
   9.3. Podaci o nestrukturiranoj dopunskoj usluzi (USSD) 29
   9.4. Wireless aplikativni protokol (WAP) 30
   9.5. SIM bazirane aplikacije 30

10. Aplikacija za mobilno bankarstvo i sigurnost podataka 31
10.1. Opcije sigurnosti tradicionalnog bankarstva 32
10.2. Opcije sigurnosti mobilnog bankarstva 34
10.3. Sigurnosne karakteristike Androida i iOS-a 36
11. Zaključak 38
12. Literatura 40

1. Uvod

Bankarstvo igra ključnu ulogu u našoj ekonomiji i postalo je sastavni dio naših života. Danas mobilni korisnici mogu provoditi osnovne bankovne transakcije kao što su provjera stanja, plaćanje računa i prijenos novca s bilo kojeg mjesta u bilo koje vrijeme. Mobilni telefoni se ne koriste samo u komunikacijske svrhe, oni se koriste za bankarske transakcije. Mobilno bankarstvo (ili m-banking) je rastuća grana elektronskog ili internetskog bankarstva. To je aplikacija mobilne trgovine koja se temelji na bežičnim mrežama i mobilnim uređajima. Sastoji se od banaka, telekomunikacijskih firmi i mobilnih uređaja. Koristi softver takozvanu aplikaciju koji se može preuzeti na mobilni uređaj.

Budući da aplikacije obrađuju osjetljive osobne podatke, njihova je sigurnost važna. Mobilni korisnik povezan je s mobilnom mrežom putem SIM kartice ili preko wi-fi mreže. Mobilno bankarstvo ima jedinstvenu konkurentsku prednost u odnosu na tradicionalno bankarstvo jer korisnicima omogućuje obavljanje bankovnih transakcija bez obzira na mjesto i vrijeme. Prednosti mobilnog bankarstva za banke i klijente uključuju jednostavan pristup bilo gdje, kontrolu nad svojim novcem, dostupnost na 24-satnoj osnovi i smanjenje troškova rukovanja bankovnim transakcijama. Ne morate imati internetsku vezu, sve što je potrebno za mobilnu vezu.

Mobilno bankarstvo je i dalje nedovoljno iskorišteno, uprkos njegovim prednostima (kao što su sveprisutnost i neposrednost) i značajna ulaganja u njega. Stopa usvajanja je niža od očekivane. Istraživači i praktičari su zainteresovani za faktore koji odlažu ili čak sprečavaju njegovo široko usvajanje. Koji faktori utiču na odluku korisnika o korištenju mobilnog bankarstva? Potencijalne prepreke za usvajanje mobilnog bankarstva uključuju percepciju korisnika o njegovoj korisnosti, jednostavnosti upotrebe, pripadajućim troškovima, e-pismenosti i kulturi. Sigurnost, privatnost, povjerenje i rizik također izazivaju zabrinutost zbog usvajanja. Mobilno bankarstvo treba da bude sigurno, zgodno i konkurentno u troškovima[1]. Povjerenje je važno u lojalnosti kupaca jer ne postoji interakcija licem u lice u mobilnom bankarstvu i uključene su osjetljive osobne informacije. Starost je također važan faktor u ponašanju usvajanja. Studije pokazuju da mlađi ljudi imaju tendenciju da koriste mobilno bankarstvo nego stariji ljudi[2].

[1] A. S. Yang, "Exploring adoption difficulties in mobile banking services," Canadian Journal of Administrative Sciences, vol. 26, 2009, pp. 136-149.
[2] A. A. Shaikh and H. Karjaluoto, "Mobile banking adoption: a literature review," Telematics and Informatics, vol. 32, 2015, pp. 129-142.

Mobilno bankarstvo u zemljama u razvoju i dalje je ograničeno. Faktori koji imaju direktan uticaj na usvajanje i upotrebljivost mobilnog bankarstva uključuju kulturne razlike, praktičnost i pismenost. Korisno je i zgodno pristupiti banci na dohvat ruke dok ste u pokretu. Nepismeno stanovništvo ne može da radi sa složenim uređajima kao što su pametni telefoni i lični digitalni asistenti (PDA). Faktori koji ometaju njegovo usvajanje, uključuju uočeni sigurnosni rizik i nedostatak povjerenja. Tehnološka anksioznost utječe na korištenje samouslužnih tehnologija. To sprečava kupce da savladaju nove tehnologije. Pošto mobilno bankarstvo ne uključuje interakciju licem u lice, teško je izgraditi povjerenje. Kada pružaoci usluga imaju povjerenje kupaca, oni spremno zadovoljavaju kupce.

Postoje neki jedinstveni izazovi sa kojima se suočava mobilno bankarstvo. Jedan od problema je sprečavanje prevare. Banka mora osigurati da zahtjeve za transakcije napravi legitimni mobilni korisnik. Lični identifikacioni broj (PIN) se obično koristi za autentifikaciju korisnika. Ne postoji univerzalni standard za mobilno bankarstvo. Bankarske strukture i sistemi variraju od zemlje do zemlje. Uprkos prednostima mobilnog bankarstva, u većini zemalja u razvoju to nije uspjelo. Niska stopa penetracije može biti posljedica nedostupnosti pametnih telefona i banaka u ruralnim područjima tih zemalja. Sigurnost i povjerenje su glavne prepreke mobilnom bankarstvu[3].

Uočen je izazov interoperabilnosti između aplikacija za mobilno bankarstvo zbog nedostatka zajedničkih standarda. Postoje različite platforme pametnih telefona: Andrios, iOs i Windows telefon. Većina mobilnih uređaja ima manje veličine ekrana i ograničene mogućnosti softvera i hardvera. Iz tog razloga, mobilne aplikacije treba da budu dizajnirane tako da omoguće korisnicima da imaju efektivnu interakciju.

[3] W. M. To and L. S. L. Lai, "Mobile banking and payment in China," IT Pro, May/June 2014, pp. 22-27. [4] "Mobile banking,"

2. Historija mobilnog bankarstva

Mobilno bankarstvo je poznato kao M-banking ili SMS bankarstvo. Evropska kompanija pod nazivom PayBox, finansijski podržana od strane Deutsche Bank, 1999. godine započela je mobilno bankarstvo. SMS je najranija ponuđena usluga mobilnog bankarstva. To je oblast u nastajanju u segmentu bankarstva. Međutim, stariji telefoni su imali ograničenu funkcionalnost. Mobilni telefoni, dlanovnici i PDA uređaji nisu imali podršku za hardver i softver. Veći troškovi planova podataka i usporena brzina mreže takođe su bili ograničavajući faktori u rastu mobilnog bankarstva. Poboljšana je unapređenjem tehnologije, hardvera i softvera. Cijena mobilnih uređaja je drastično smanjena i još uvijek se smanjuje. Brzina mreže je mnogo bolja nego ranije, a planovi podataka nisu skupi. Sve ove promjene pružile su neophodne sirovine za rast mobilnog bankarstva, a broj korisnika mobilnog bankarstva raste iz dana u dan. Korisnici koji su koristili računare / laptope za online bankarstvo, kreću se ka mobilnom bankarstvu zbog jednostavnosti upotrebe i brzog pristupa. U SAD, mobilno bankarstvo je 2006. godine uvela Wachovia banka. U septembru 2007, Aite grupa je predvidjela da će korisnici mobilnog bankarstva u Sjedinjenim Američkim Državama doseći 1,6 miliona do kraja 2007. godine i da će se brzo povećati na 35 miliona do 2010. godine. za mobilno bankarstvo.

Međutim, bezbijednosna pitanja su glavna briga pružalaca usluga mobilnog bankarstva i korisnika. Kako sistemi mobilnog bankarstva sazrijevaju, više će korisnika početi koristiti mobilno bankarstvo, što će privući pažnju hakerske zajednice na korisnike mobilnog bankarstva uglavnom za finansijsku dobit. Bezbijednost i bezbijednost ličnih i finansijskih informacija koje se čuvaju i upravljaju u uređajima su ključni faktori za korisnike, bankarsku organizaciju i bezbijednosnu zajednicu. Svrha ovog rada je da stekne osnovna znanja o mobilnom bankarstvu, objasni različite vrste arhitekture koje se koriste u mobilnom bankarstvu i identificira različite sigurnosne napade i njegove protumjere.

3. Mobilno bankarstvo

Mobilno bankarstvo se može definisati kao sposobnost obavljanja bankovnih transakcija putem mobilnog uređaja, ili šire - za obavljanje finansijskih transakcija putem mobilnog terminala[4]. Ova definicija je pogodna za rad jer uključuje ne samo osnovne usluge, kao što su izjave o bankovnim računima i transferi sredstava, već i elektronske opcije plaćanja, kao i finansijske usluge zasnovane na informacijama (npr. Upozorenja o ograničenju računa ili saldo računa, pristup brokerskom poslovanju).

Da li postoji potreba za mobilnim bankarstvom? Odgovor je čvrst "da". Iako potražnja potrošača za više sofisticiranim mobilnim uslugama nije bila tako jaka, potražnja za osnovnim mobilnim bankarstvom je izraženija u odnosu na opću potražnju za uslugama mobilne trgovine[5]. Broj korisnika bežičnih digitalnih uređaja širom svijeta je premašio 0,5 milijardi do 2003. godine, prema nekim projekcijama[6], a procijenjeni broj od 40 miliona korisnika bežične veze imat će pristup mobilnim financijskim uslugama u istom periodu potrošiti na razvoj i marketing bežičnih uređaja (oko 40 miliona USD u 2003. godini).

Mnogi predviđaju da će mobilno bankarstvo biti najvažnija aplikacija za mobilnu trgovinu. Promatrano kao dodatni kanal za poboljšanje upravljanja odnosima s klijentima, mobilno bankarstvo omogućava i financijskim institucijama i operaterima telekomunikacijskih mreža da ojačaju svoje odnose s postojećim klijentima, prošire svoju opću korisničku bazu i istovremeno usmjere na specifične, unosnije tržišne segmente[7].

Pružanje mobilnog bankarstva oslanja se na mobilni uređaj krajnjeg korisnika. Trenutno postoje dva osnovna tipa mobilnih krajnjih korisnika - mobilni telefon i prenosni ručni računar poznat kao Personal Digital Assistant (PDA).

Mobilno bankarstvo može inicirati mobilno plaćanje, koje se dijele u dvije kategorije: mikro i makro plaćanja. Mikroplaćanja su prvi oblik mobilnog plaćanja, koja su fokusirana na male transakcije. Micropayments obično se sastoje od plaćanja malih usluga i roba kao što su karte za javni prijevoz, automati za prodaju, plaćanje kioska i druge usluge na licu mjesta. Appleove iTunes kupovine su također jedan od ranih primjera mikroplata. Najznačajnija karakteristika

[4] Drexelius, K. & Herzig, M., "Mobile Banking and Mobile Brokerage – Successful Applications of MobileBusiness?", International management & Consulting , Vol.16, No. 2 (2001): 20-23.
[5] Bansai, P., "Mobile Banking Steps up a Gear", The Banker , Vol. 151, No.905 (2001): pp 121-122
[6] Kiesnoski, K., "Wireless Banking", Bank Systems & Technology, Vol. 37, No.2 (2000): 40-43
[7] Horton, V., "Cash and Carry Mobile Banking". Unix& NT News, No. 141 (2001): 42-43

mikroplaćanja je da se bankovni račun korisnika ne koristi direktno za transakcije. Macropayments su slične sa kupovinama koje se obično obavljaju platnom karticom. Primjeri makropakcija su e-trgovina, igre, e-karte, restorani i maloprodaja.

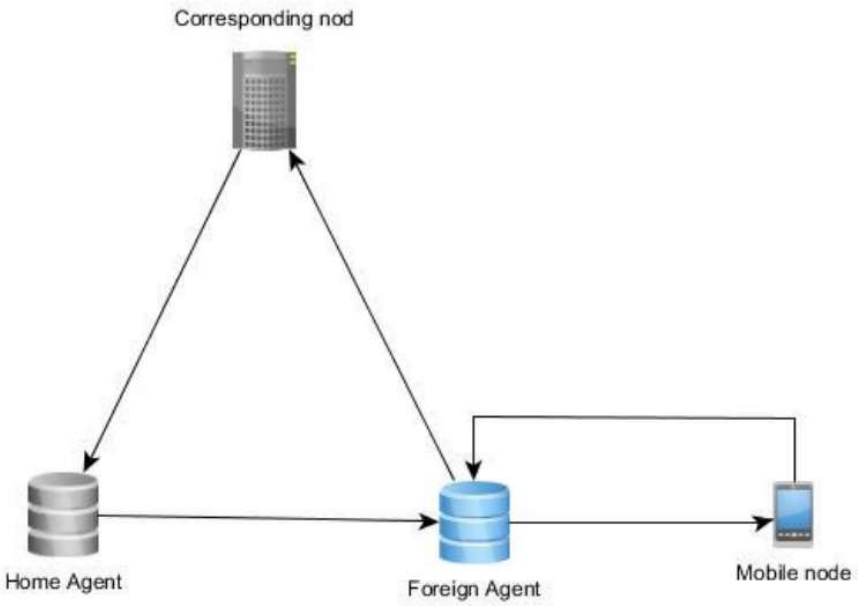
Istraživanja su pokazala da se od 2000. godine interes za mobilno plaćanje povećao. Ovo je uočeno kada je broj publikacija i konvencionalnih novinskih članaka o mobilnom bankarstvu stalno rastao. Tvrdi se to mobilno bankarstvo će na kraju postati uobičajena praksa. Mobilno bankarstvo kao trend se nije brzo razvio zbog tehničkih ograničenja. Istraživanje na to ukazuje.

Značajno interesovanje za mobilno bankarstvo izazvano je kada je računarstvo i mrežne mogućnosti uređaja adekvatnije podržavali akcije plaćanja i činile ih pogodnijim za korisnike.

3.1. Tehnički elementi mobilnog bankarstva

U nastavku će biti objašnjeno kako mobilno bankarstvo radi na tehničkom nivou. Po istraživanju će se raspravljati i modelirati sigurnosni detalji poglavlje rezultata. Ideja je da se pruži slika tehničkih elemenata šta je to potrebno za rad mobilnog bankarstva. Ucrtani model se zasniva na istraživanju izdao je Chung et. al. (2005). Njihov prijedlog nudi opći okvir model i razumijevanje arhitekture mobilnog bankarstva. Korištenje mobilnog bankarstva zahtijeva mogućnost korištenja mrežne veze u pokretu. U idealnom slučaju, korisnik ne bi ni primijetio kada je mreža promijenjena.

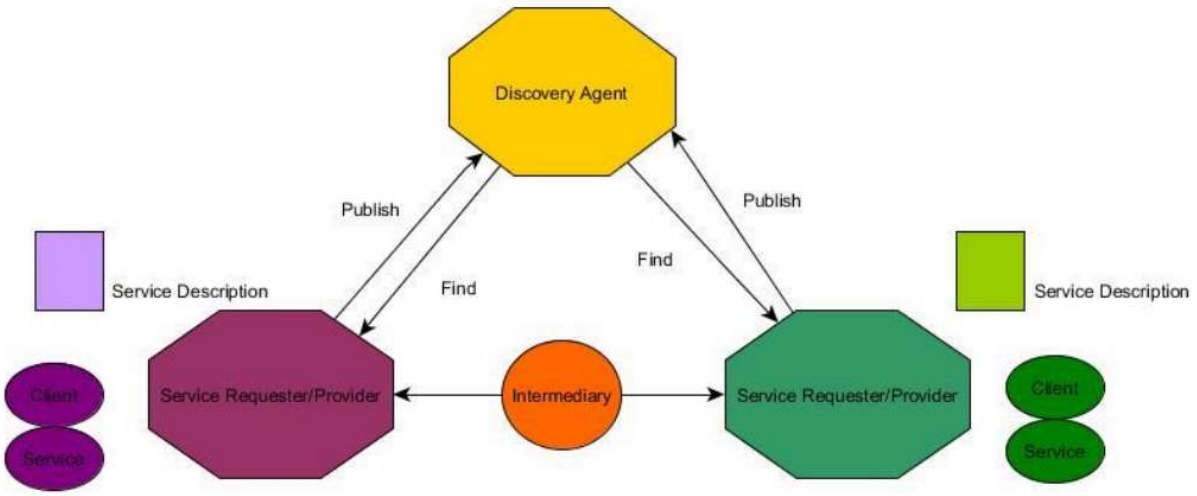
Mobilni uređaji mogu pristupiti internetu korištenjem mobilnog IP mehanizma. Kada Koristeći mobilni IP, uređaj prima jednu IP adresu bez obzira na mrežu uređaj je bio prisutan. IP adresa mobilne telefonije dolazi iz kućne mreže, koja je zove se Home Agent (HA). Kada uređaj posjeti novu mrežu, zove se Foreign Agent (FA). Uređaj pretražuje svoj HA pomoću FA i kada je to nađeno, uspostavljena je veza između HA i FA. Čineći ovo, svi paketi podataka će proći kroz HA i tako održati svoju IP adresu isto, čak i u novoj mreži.



Slika 1. Mobile IPv4

Web Service je standardizovani model za povezivanje aplikacija sa upotrebom postojeće infrastrukture. Svrha Web usluga je rješavanje tehničkih pitanja inter-aplikacijske interakcije i interoperabilnosti. U osnovi, usluge se objavljuju i pronalaze pomoću agenta za otkrivanje. Ako je usluga neke aplikacije

Zahtjev će biti poslan agentu za otkrivanje i ako su usluge objavljene u uslužnom agentu. Model ima i posredničke funkcije, koje pružaju funkcije kao što su usmjeravanje i sigurnost itd.



Slika 2. Arhitektura web servisa

3.2. Pristup potrošača mobilnim telefonima

Od novembra 2015. 87% stanovništva SAD-a starosti 18 i više godina je imalo ili ima redovan pristup na mobilni telefon. Dok je procenat odrasle osobe populacija sa mobilnim telefonima ostala je konstantna tokom prethodne tri godine, a sve veći udio posjeduje pametni telefon: ovo istraživanje je 77 posto stopa vlasništva nad pametnim telefonima među onima koji imaju mobilni telefon. Telefoni su značajan porast u odnosu na 71 posto stopa prijavljena u 2014. godini, 61 posto u 2013. godini, 52 posto stopa u 2012. godini i stopa od 44% u 2011.[8]

Stope korištenja mobilnih telefona ostaju visoke i konzistentne u svim demografskim i socioekonomskim grupama. Prevalenca mobilnih telefona pokazuje koliko su postali ukorijenjeni u modernoj kulturi. Upotreba mobilnog telefona u istraživanju 2015. godine više među mlađim starosnim grupama: 91% za osobe od 18 do 44 godine, 90 posto za osobe od 30 do 44, i 89 posto za osobe od 44 do 59 godina

Upotreba telefona se donekle smanjuje, na 81 posto osobe starosti 60 i više godina. Usvajanje pametnih telefona je slično viši kod mlađih generacija, razlike su izraženije među godinama grupe: 91 procenat onih od 18 do 29 godina i 88 procenata onih starosti od 30 do 44 godine koji poseduju mobilni telefon imaju pametni telefon, dok je 72 posto mobilnog telefona vlasnici od 45 do 59 godina i 56 posto mobilnih telefona vlasnici u dobi od 60 i više godina imaju pametni telefon.

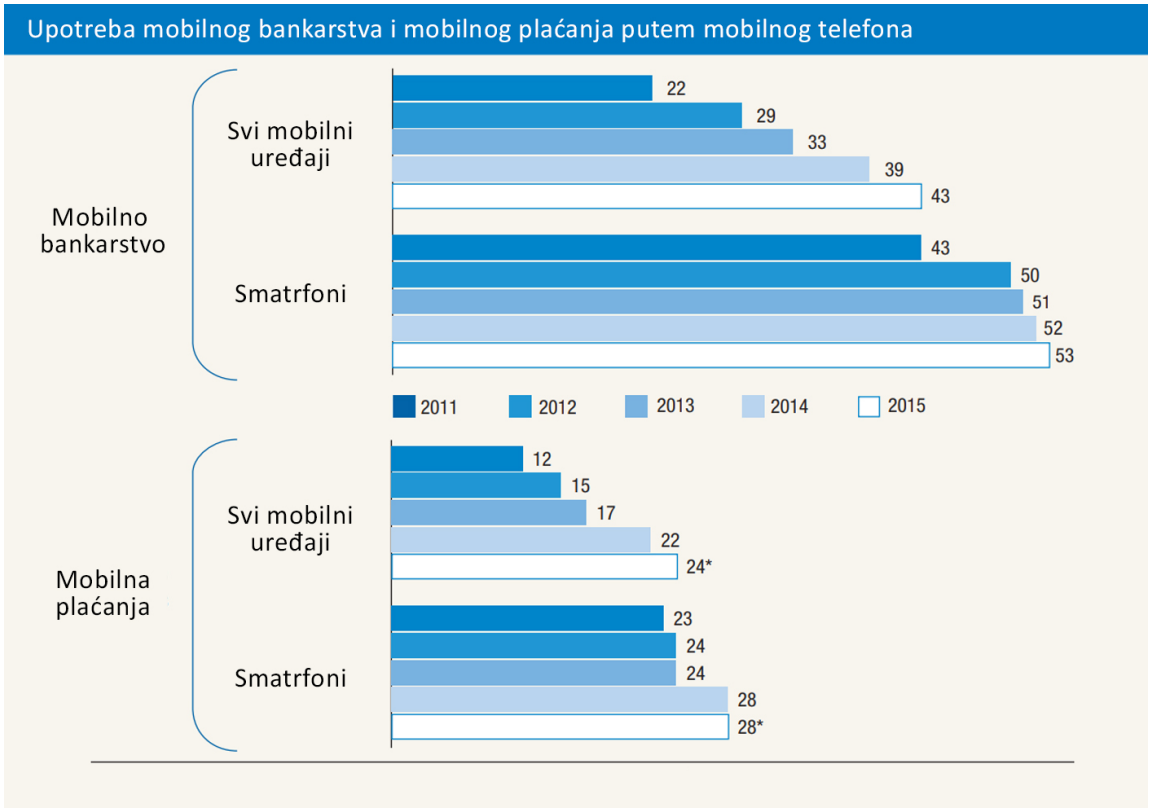
Upotreba mobilnih telefona i pametnih telefona varira u zavisnosti od toga nivo prihoda domaćinstva. U domaćinstvima koja zarađuju manje od 25.000 dolara godišnje, 76% odraslih ima neke vrste mobilnih telefona, i 58 posto njih sa mobilnim telefonima imaju pametni telefon. Upotreba oba, mobilnih telefona i pametnih telefona raste sa prihodima. Među odraslima u domaćinstvima koja zarađuju više od 100.000 dolara godišnje, 96 procenata ima mobilni telefon, i 86% onih sa mobilnim telefonima imaju pametni telefon.

[8] www.pewinternet.org/files/2015/10/PI_2015-10-29_device-ownership_FINAL.pdf

3.3. Trendovi korištenja i plaćanja putem mobilnog bankarstva

Usluge koje omogućavaju potrošačima da dobiju finansijska sredstva informacije o računu i obavljanje transakcija njihove finansijske institucije ("mobilno bankarstvo") i koji omogućuju potrošačima da vrše plaćanja, transfer novca, ili plaćanje za robu i usluge („mobilna plaćanja") postaju sve više preovlađujući. Iznad proteklih nekoliko godina ove usluge su postale dostupne u širem krugu institucija i tipova usluga koje se nude i dalje se razvijaju.

Sa povećanom diseminacijom tehnologije i širenje niza opcija, usvajanje od strane potrošača mobilne finansijske usluge su porasle. U istraživanju iz 2011. godine, na primjer, 22 posto korisnika mobilnih telefona sa bankovnim računima i 43% pametnih telefona korisnici sa bankovnim računima koji su koristili mobilno bankarstvo u prethodnih 12 mjeseci.[9] Ove proporcije su se povećale u svakoj godini istraživanja. U istraživanju 2015. godine, prisutnost mobilne telefonije bankarstvo je nastavilo da raste, dostižući 43 odsto korisnici mobilnih telefona sa bankovnim računima i 53% korisnika pametnih telefona sa bankovnim računima od interesa za ove usluge među dijelom stanovništva.



[9] Ovdje su podaci o mobilnom bankarstvu u istraživanju iz 2011. Godine izraženo kao procenat korisnika mobilnih telefona sa bankom računi.

To je rekao, udio koji ne zna da li je mobitel bankarstvo dostupno iz njihove banke je smanjen od 28% u 2013. i 22% u 2014. godini. Dionica koja kaže da njihova banka ne nudi uslugu pokazalo je manje promjena - 6 procenata u 2013, 4 procenata u 2014, i 5 procenata u 2015. godini, udio odgovora "ne znam" može sugerirati povećanje svijesti potrošača o mobilnom bankarstvu usluge u posljednjih nekoliko godina. Kao takav, to može biti indikacija da finansijske institucije povećavaju njihov marketing postojećih mobilnih usluga kao i da više njih nudi te usluge. Zabrinutost oko sigurnosti mobilnog bankarstva i često se prisutne tehnologije mobilnog plaćanja navode kao razloge zbog kojih potrošači nisu odlučili da usvoje ove tehnologije.

4. Kanali za tradicionalne i postojeće distribucije

U ovom dijelu opisujemo i tradicionalne i nove bankarske kanale, istražujući poslovni pokretač i korisnički scenariji interakcije kao osnova za zahtjeve.

4.1. Tradicionalni kanali

Poslovnica banke (branch) je kanal distribucije fondacija za bankarstvo, koji se transformiše mnogo puta sa svakom tehnološkom revolucijom. Danas mnoge grane pružaju otvoreniji planski stil koji je sličan modernom danu kupovine za kupce.

Prodajni predstavnici (predstavnik) i mobilni i na poslovnicama banaka će nastaviti da se formiraju dio osobnog iskustva koje korisnici mogu dobiti. Na mnoge načine ovi kanali predstavljaju ogranak mobilne banke sa pristupom mnogim alatima i sistemima za obradu obrazaca i zahtjeva kupaca.

Interaktivni sistemi glasovnog odziva (IVR) dva ključna cilja, i) djeluju kao filter prometa za upućivanje telefonskih poziva klijentima odgovarajućem predstavniku pozivnog centra, i ii) oni će obezbjediti automatizovani glasovni bankarski sistem za obavljanje nekoliko finansijskih transakcija.

Korištenje pošte (mail) je i dalje vitalni dio marketinškog kanala za bankarstvo i koristi se i za distribucija identifikatora i kartica vezanih za kupca. Kupci mogu koristiti poštu za povratak informacije, ali često se to obavlja lično u filijali ili sa modernijim kanalima kao što je on-line bankarstvo.

Servisiranjem svih oblika zahtjeva od strane kupaca, moderni dnevni pozivni centar (call center) ima predstavnike opremljene pristupom on-line i core bankarskim sistemima za obavljanje svih potrebnih funkcija u obradi zahtjeva kupaca.

Automatske blagajne (ATM) su možda prvi distribucijski kanal koji je obezbijeđen klijentima sa automatizovanim tehnološkim sistemom za interakciju sa bankom za gotovinu povlačenja. Ovi sistemi još uvijek čine osnovu za bankarstvo klijenata i sada su dopunjeni s nekoliko novijih on-line sistema.

4.2. Emergant kanali

Sistemi na prodajnim mjestima (POS), kao što je elektronski prijenos sredstava, već duže vrijeme predstavljaju glavni kanal, međutim, oni su nedavno doživjeli promjenu i omogućili kupcima korištenje prodajnog mjesta kao sredstva za podizanje gotovine. Zbog toga se ovdje vidi kao noviji kanal za bankarstvo.

Elektronska pošta (email) je prvobitno korištena kao novi kanal za distribuciju, ali s obzirom na značaj spama i zlonamjernog napada za dobivanje korisničkih vjerodajnica, ovaj oblik komunikacije se u velikoj mjeri odbacuje od velike upotrebe. U većini slučajeva banke pružaju vlastiti oblik poruka, umjesto e-pošte, koji je dostupan klijentima koji koriste online račune.

Pojava **Interneta** ima i nastavlja da transformiše njihov način poslovanja. Kanal Internet bankarstva sve više postaje centralni bankarski kanal za obavljanje svih oblika finansijskih transakcija, sa mnogim funkcijama koje su dostupne u nekoliko formata kako bi se zadovoljili osobni računari, mobilni uređaji i druge nove tehnologije.

On-line chat se često smatra proširenjem internetskog kanala, međutim, to se dovoljno razlikuje da bi se omogućilo individualno razmatranje. Tekstualna chat poruka omogućava korisnicima i bankarskom osoblju interakciju u realnom vremenu kako bi se pozabavili trenutnim pitanjima bez potrebe za glasovnim pozivom u pozivni centar. Ovo osigurava korisničku podršku koja je svjesna konteksta za on-line bankarske aktivnosti.

Mobilno bankarstvo je kanal koji obuhvata interakcije putem mobilnog uređaja, uključujući internet, SMS i glasovne pozive. Značajni napredak u mobilnoj tehnologiji omogućit će bogate korisničke scenarije koji obuhvaćaju višestruke načine interakcije (tj. Glas i podatke istovremeno), kao i podršku za računalne uređaje bazirane na tabletima, budući da oni postaju široko prihvaćeni kao dodatna oprema za većinu korisnika.

5. Tehnologije i standardi za multikanalno bankarstvo

Sa sve većom ovisnošću o trendovima uređaja, potrošač je prihvatio niz informacione i komunikacione tehnologije, kao i povezani standardi, postali su centralne komponente za bankarstvo i, što je još važnije, multikanalna distribucija. Najnovija Tehnologije se odnose na web omogućavanje, međutim pojavu i brzo usvajanje mobilnih uređaja i mreže mijenjaju tehničko okruženje za mnoge finansijske institucije. Sljedeća tabela (Tabela 1) ukratko sažima neke od istaknutih tehnologija i standarde u upotrebi.

ICT	Opis
Internet tehnologije	Internet tehnologije kao što su web serveri, on-line chat, autentifikacija serveri, gateway-i za razmenu poruka i proksiji, omogućavaju pristup on-line bankarstvu korisnika putem Interneta.
Mobilne mreže	Tradicionalne mobilne 3G i 4G mobilne mreže i bežične tehnologije podršku mobilnosti. Ovi sistemi se uglavnom koriste za proširenje Interneta pristupačnost.
RFID i NFC	Bežična komunikacija Near Field Computing (NFC) zasnovana na radiju Identifikacija frekvencije (RFID), koja se koristi za beskontaktno plaćanje od strane velikih institucije kreditnih kartica.
SOA	Servisno orijentisana arhitektura je pristup za definisanje potrošenih usluga IT aplikacijama; koje se mogu interno dijeliti ili pristupiti izvana preko Interneta.
TOGAF	Open Group Architecture Framework određuje i proces i okvir za definisanje arhitekture preduzeća i sistema
BIAN	Mreža arhitekture bankarske industrije definira skup IT usluga na servisno orijentisanoj arhitekturi.
NLU / NLP	Proširene su tehnologije za razumijevanje i obradu prirodnog jezika konvencionalno prepoznavanje glasa sa prirodnim govorom. Tradicionalni IVR je usmereni govor i restriktivni, dok NLU tehnologija podržava neograničeno (ljudski) razgovorna interakcija
eWallet	Pojava korišćenja mobilnih telefona kao uređaja za plaćanje, uz korišćenje ugrađeni SIM (modul identifikacije pretplatnika) čip za pametne kartice, gdje je Primjenjuje se aplikacija eWallet.

Tabela 1. Tehnologije i standardi za višekanalno bankarstvo[10]

Sada razmatramo neke od najnovijih uređaja i tehnologija koje se mogu pojaviti zahtijevaju strateško razmatranje. Neke od ovih inovacija ne moraju nužno postati usvojeni pristup, ali daje perspektivu o potencijalu za napredak u tehnologiji koji može zahtijevaju određenu podršku.

[10] International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.5, October 2013

Kako je tehnologija mobilnih uređaja diversifikovala, pojavila se potreba za razvojem specifične **mobilne aplikacije** za različite operativne sisteme i uređaje na tržištu. Kao takva složenost povezana sa razvojem i implementacijom više aplikacija, (npr. Flash, Java, itd. Postala je sve veći izazov za bankarske tehnologe.

Sposobnost da se prilagodi mnogo većoj formi kao i korisnici opremljen u budućnosti sa mogućnošću uređaja da u početku pristupi web lokaciji na mobilnoj jedinici i kada kod kuće to može prenijeti na televizor, koristeći ručne gestove za prebacivanje kontrole drugog uređaja. Mogućnost prenosa između uređaja će takođe zahtijevati dodatnu sigurnost mjere za sprječavanje zlonamjernih pothvata.

Ugrađeni uređaji za komunikaciju vozila mogu se možda smatrati daljnjim proširenjem na mobilne uređaje sa nekoliko ključnih razlika. Postoji povećana zavisnost od glasovnih korisničkih interfejsa, olakšana prirodnim jezikom govorne tehnologije, koje pružaju superiorno glasovno iskustvo u odnosu na tradicionalni IVR ili glas sistemi prepoznavanja[11]. Ovo je čvrst zahtjev, s obzirom na ograničenja korištenja uređaja sprečavanje ometanja rada vozila u tranzitu. Faktor forme je vjerovatno sličan tabletu, ali može biti prožeta i glavnim prikazima (HUD).

Uređaji kao što su mobilni telefoni se postavljaju kao alternativa kreditne kartice sa više učesnika trećih strana na tržištu finansijskih transakcija. Iako neke mogućnosti su proširenje postojećeg mobilnog uređaja, postoje dodatne interakcije sa trećim stranama koje može biti vlasnik računa u ime korisnika, izlažući potrebu za mogućim dijeljenjem sigurnosti šeme šifriranja za omogućavanje transakcija. Ovo takođe može biti nepoželjno za bankarske institucije, jer može olakšati eroziju tržišta transakcija konkurentnim snagama.

Mali uređaji za ručni zglob (sat) će vjerovatno primijeniti protokole poruka kao što su SMS-u će biti potrebni profili malog form faktora za prikazivanje informacija baziranih na webu. Tehnologija se verovatno oslanja i na inteligentne glasovne interfejse zbog ograničenja za faktor forme i komandu za izlaz i ulaz.

Uređaji sa ekranima za gledanje kao što su head-up ekrani i ekrani transparentne proširene stvarnosti pružit će dodatne informacije kao gledanje objekata i entiteta. Neka nedavna ispitivanja su uključila dodatne informacije o klijentima prikazuju se gazdarima koji koriste

[11] UML contribution in a virtual banking environment", ECIS 2000 Proceedings. Paper 21. pp. 883-888. [13] S. Mitchell, C.J. Pavlovski, et al. "Multimodal Natural Language Platform Supporting Cellular Phones", The ACM Journal of Mobile Computing and Communications Review (MC2R), ACM Sigmobile, Vol.10, Iss.3, pp. 34-45, 2006

okare i lokatore grana koristeći mobilne uređaje. Teško je međutim, predvidjeti da li će takvi uređaji postati mainstream, važno je to razmotriti. Raznolikost u tehnologiji će se vjerovatno nastaviti i stoga svaka predložena višekanalna arhitektura zahtijeva fleksibilan okvir da bi mogao podržavati nove uređaje i kanale kako se pojavljuju.

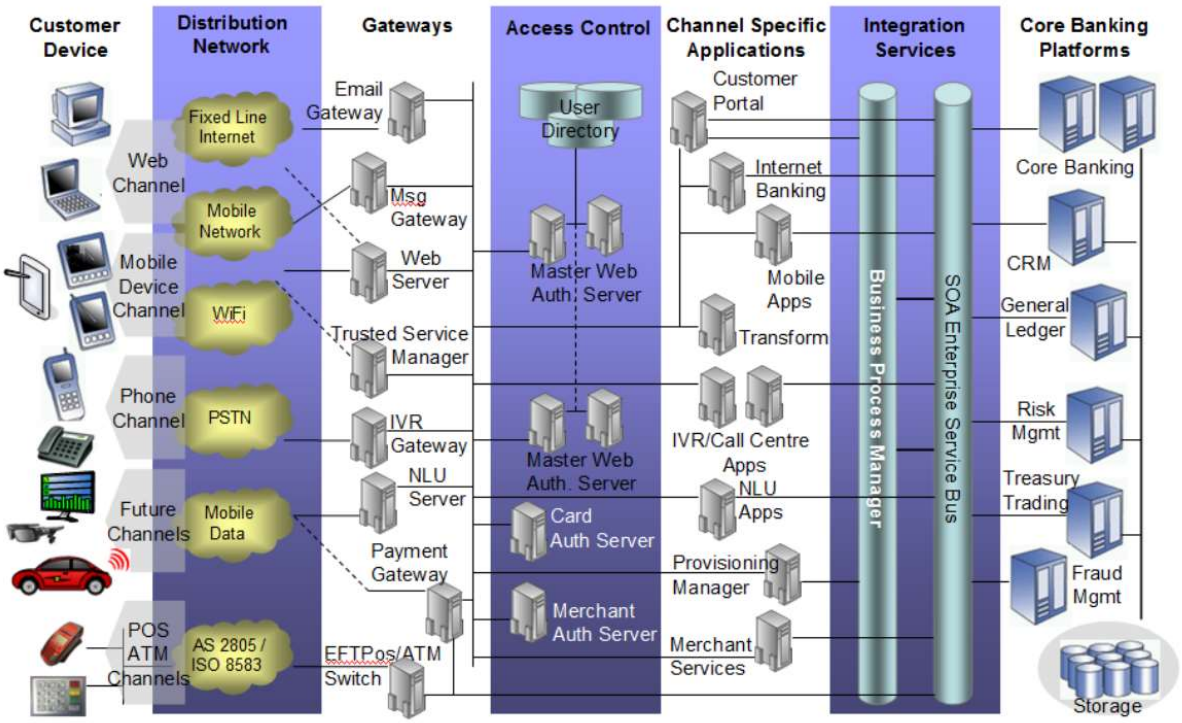
6. Multikanalna bankarska arhitektura

Oslanjajući se na tehnologije i definisane kanale distribucije prethodnih sekcija, i iskustva u primjeni povezanih koncepata kanala u široj industriji, sada predstavljamo višekanalnu arhitektura za bankarstvo. Arhitekturu fokusiramo na one kanale distribucije koji imaju tehnološki interfejs koji direktno koristi klijent u bankarstvu, pa stoga izostavljamo kanale kao što su ogranci i predstavnici koji koriste interne sisteme za obavljanje funkcija u ime klijenta. Predložena arhitektura je prikazana na slici 1, ilustrujući a slojeviti okvir u kojem se klijentski uređaji koriste za pristup finansijskim uslugama putem skupa mreže i mrežni prolazi koji usmjeravaju zahtjeve za usmjeravanje određenih aplikacija i usluga.

Aplikacije specifične za kanale koriste zajedničke osnovne bankarske funkcije putem oglašene SOA usluge i poslovni procesi integracijskog sloja. Slojeviti pristup za razdvajanje servisnih mogućnosti zajedno sa upotrebom zajedničkih usluge na sloju integracije olakšavaju implementaciju novih kanala i usluge kada se pojave. Sada opisujemo svaku od komponenti unutar definiranih slojeva i u sljedećem odjeljku 4, ilustriranje kako ova arhitektura sustava funkcionira s nekoliko scenarija interakcije koji demonstriraju ove komponente u radu kako bi se ispunili financijski zahtjevi koju je napravio kupac.

6.1. Korisnički uređaji

Uređaji i tehnologija koju koriste kupci značajno su se razvili od prvog raspoređivanja samouslužnih bankomata. Mainstream bankarstvo se u velikoj mjeri oslanja na Internet kanal sa novijim trendovima koji pokazuju migraciju upotrebe na mobilne uređaje. Dakle, ključni kanalni uređaji ovog sloja uključuju Web i mobilne uređaje. Tradicionalne usluge sa telefona, bankomata i EFTP-a se stalno proširuje novim transakcijama i sposobnostima. Važno razmatranje kod korisničkih uređaja je da je ovo veoma nestabilan sloj sa, na primer, novim mobilnim uređajima koji se izdaju svakih 12 do 18 mjeseci. Ovo ima ometanja efekata nizvodno na komponente naknadnih slojeva koji su potrebni za podržavanje rada tih uređaja.



Slika 3. Nacrt za višekanalnu bankarsku arhitekturu

6.2. Distributivna mreža

Distributivne mreže su u velikoj mjeri namijenjene da budu besprijekorna komponenta unutar skupa infrastruktura koja sadrži višekanalni sistem. Distributivne mreže uključuju fiksnu liniju mreže podataka koje podržavaju internet, mobilne podatkovne mreže za mobilne telefone, vruće točke i WiFi mreže i tradicionalnije mreže kao što je javna komutirana telefonska mreža (PSTN) i EFTPos / ATM mreže bazirane na ISO8583 (AS2805 u Australiji). Podržane mreže i u velikoj mjeri određeni popularnim uređajima koji su dostupni na tržištu i zahtijevaju kanale koji podržavaju kanal za distribuciju finansijskih usluga. Buduće mreže se pojavljuju, međutim, vjerovatno će to biti proširenja postojećih mrežnih tehnologija s povećanjem u opsegu podataka kako bi se podržale složenije interakcije korisnika. Svijest o mreži je važna razmatranje dizajna za višekanalnu arhitekturu, jer postoji kritični zahtjev osiguravanje osjetljivih financijskih sadržaja preko sve javne mreže.

6.3. Gateways

Komponente koje čine Gateway sloj uključuju mrežne gateway-e povezane s webom, kao što je slanje poruka (SMS, MMS), e-pošta i HTTP Web servera; ovi čvorovi će servisirati web saobraćaj od kanala fiksne ili mobilne mreže. Integrisani gejtveri za glasovni odgovor se koriste kao web orijentisani serveri koji pretvaraju ulazni i izlazni govor u odgovarajući tekst za aplikacijski poslužitelj na sloju specifičnog kanala. Budući kanali kao što su ugrađeni uređaji unutar automobila će biti više ovisna o govornim sučeljima i najnovijim tehnologijama kao što je razumijevanje i obrada prirodnog jezika vjerovatno će pružiti neophodne konverzija jezika kako bi se korisnicima omogućila bolja interakcija. Komponente na ovom sloju su također odgovorane za uspostavljanje šifriranog kanala za osiguravanje svih komunikacija između njih kupca i banke. Tekuće tehnologije također se nalaze u ovom sloju, kao što je EFPOS / ATM prekidači, za transakcije usmjeravanja i provjeru kartica, i gateways za plaćanje za HTTP plaćanje automobila.

6.4. Kontrole pristupa

Ključne komponente koje čine sloj kontrole pristupa uključuju Master Authentication Server za kanale povezane s Internetom i poslužitelja Merchant Authentication za račun trgovca usluge autentifikacije. Glavni web autentikacijski server pruža identitet i pristup mogućnosti upravljanja, kao funkcija jedinstvene prijave, za korisnike koji pristupaju finansijskim uslugama sa web, mobilnih i telefonskih kanala. Kao noviji kanali pojavljuju se dodatni klasteri raspoređenih kako bi zadovoljili povećanje posla autentifikacije. Merchant Authentication Servers omogućiti pristup trgovinskim uslugama kao što su prikupljanje sredstava, izvještavanje, naknada za račun i transakcije upravljanje.

6.5. Aplikacije specifične za kanal

Nakon toga slijedi uvid u potrebu da se podrži tržište uređaja koji se brzo mijenja su protočni efekti i na gateway-ove i na kanale specifične aplikacije. Štaviše, podržavajući pristupnici i aplikacije zahtijevaju sličnu agilnost u podržavanju novog uređaja mogućnosti, koje zahtijevaju reviziju i nadogradnju u skladu s novim mogućnostima koje pružaju ovi uređaji; gdje se koriste karakteristike uređaja putem distributivnog kanala. U nekim ovo može biti prilagođavanje faktora forme, za gledanje finansijskih usluga, do novih mobilnih aplikacija koje podržavaju nove web tehnologije (npr. Flash, Java, Javascript). Kao novije pojavljuju se alati (tj. NLU),

aplikacije koje podržavaju zahtjeve mogu biti postavljene na ovom sloju prema budućim kanalima distribucije.

6.6. Integracijske usluge

Ključni princip podržan predloženom slojevitom arhitekturom je taj da on pruža oblik apstrakcija specifičnih zahtjeva uređaja iz preostalih slojeva sistema. Dakle, promjene u sposobnostima uređaja su smještene prije i na sloju specifičnog kanala, sa svim dodatnim funkcijama koje isporučuju pristupnici. To znači procese i jezgro bankarski sistemi mogu funkcionirati u relativno stabilnom okruženju bez utjecaja ove promjene. Ovo je dodatno olakšano upotrebom poslovnog busa i poslovnog servisa reklamne sposobnosti upravnika procesa za uzlazne i nizvodne sisteme.

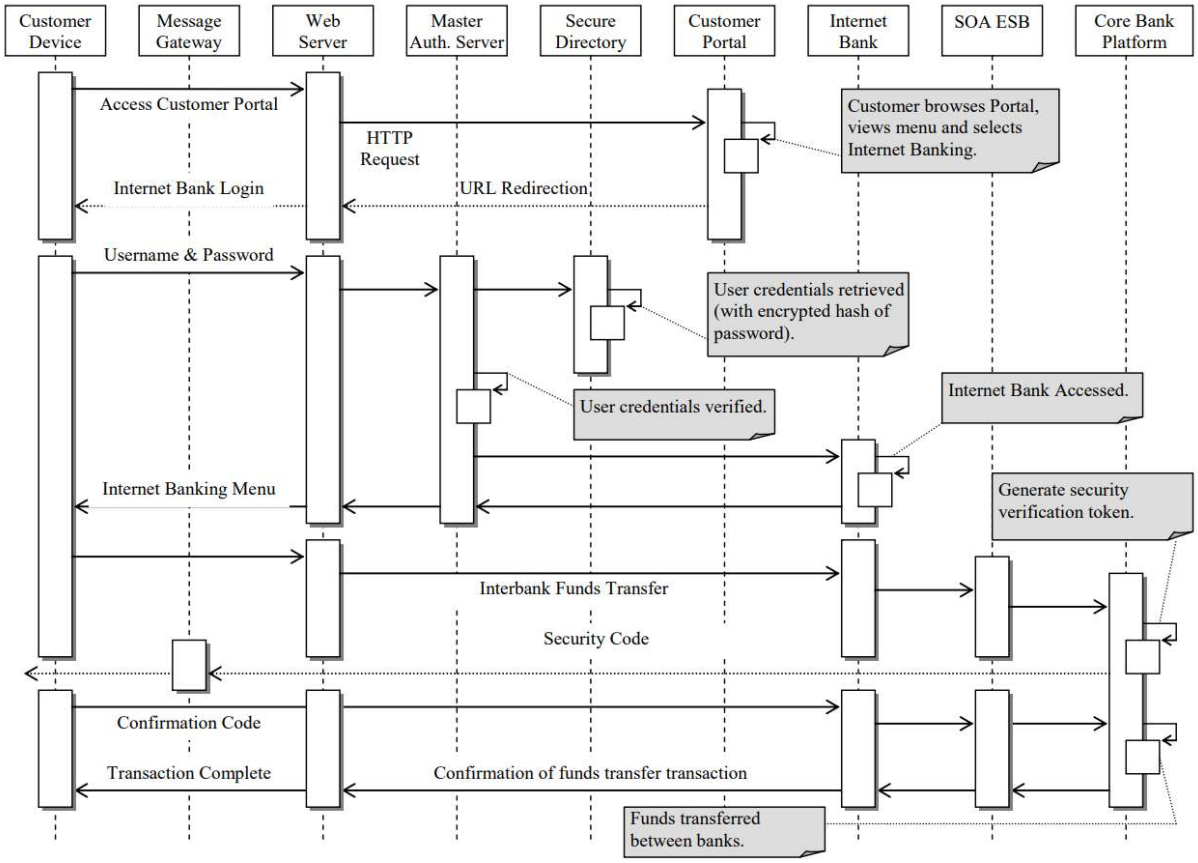
6.7. Core banking platforme

Jezgro bankarskih platformi osigurava stabilno i sigurno okruženje za izvršenje velikih obima finansijskih transakcija i funkcija operativne podrške kojima upravlja banka. Iako se broj i vrsta osnovnih bankarskih sistema razlikuje među institucijama, ključ ilustrovani sistemi se koriste za podršku najčešćih finansijskih aktivnosti. To uključuje centralne bankarske platforme za račune, zajmove, sredstva; odnos sa klijentima sistem upravljanja (CRM); glavna knjiga za upravljanje obavezama, potraživanjima, itd; rizik upravljanje za procjenu računa klijenata i transakcija; trezorske i trgovinske sisteme; I sistemi za upravljanje prevarama na svim finansijskim aktivnostima. Na samom kraju multikanala spektar, slojeviti pristup je namijenjen da olakša stabilnost od promjena, kao što je to jezgro bankarske platforme pružaju osnove za veće vremensko razdoblje u odnosu na aplikacije i uređaje koji su u neposrednoj blizini kupca i koji su podložniji promjenama.

7. Analiza arhitekture: Interakcije sistema

Sada analiziramo predloženu višekanalnu arhitekturu ilustrirajući kako su različiti Komponente nacrta međusobno djeluju kada je zahtjev pokrenuo korisnik putem jednog od definisanih kanala. Dijagrami interakcije su UML bazirane interakcije sistema koje su korisne u mapiranju komponentnih funkcija na određene platforme, to može pomoći u komercijalnom proizvodu odabir prilikom izgradnje višekanalne platforme.

7.1. Korisnik prenosi sredstva na drugu banku koristeći Web kanal



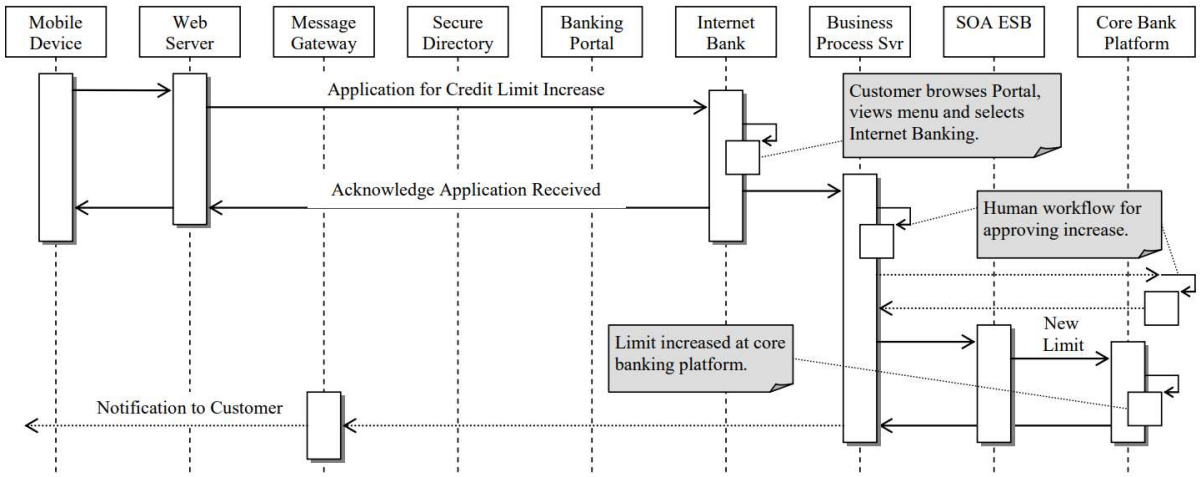
Slika 4. Interakcija web kanala

Dijagram interakcije prikazan na slici 4 ilustrira kako su komponente predložene okvir interakcije prilikom obrade zahtjeva klijenta za prijenos sredstava u drugi vlasnika računa u drugoj finansijskoj instituciji. Korisnik u početku pristupa klijentu bankarski portal i podnosi zahtjev za pregled njihovih bankovnih računa. Nakon unosa korisničkog imena i lozinke, vjerodajnice se prosljeđuju na poslužitelj Web Master Authentication i verifikovani prema bezbijednosnom imeniku korisnika. Nakon autentifikacije, podaci o bankovnom računu se vraćaju klijentu. Prenos sredstava onda može biti iniciran od strane korisnika, sa posrednikom izazov autentifikacije korisniku koji se vraća kako bi potvrdio traženi transfer sredstava; sa obezbeđenjem kod koji se šalje (na primer) mobilnom telefonu korisnika. Kupac odgovara na transakciju izazov i transfer sredstava vrši centralna bankarska platforma.

7.2. Klijent se prijavljuje za povećanje limita kreditne kartice pomoću kanala za mobilne uređaje

Izostavljajući prva dva koraka prikazana u prethodnom primjeru (koji su isti) sada opisujemo interakcije sistema kada klijent podnese zahtjev za povećanje limita kreditne kartice pomoću mobilnog telefona U ovom primjeru korisnik pristupa stranici Internet bankarstva koristeći mobilni uređaj, podnošenje on-line obrasca ili zahtjeva za uvećanjem jednog od odabranih platne kartice. Zatim se zahtjev prosljeđuje upravitelju poslovnih procesa, koji inicira automatizirani poslovni proces za odobravanje i postavljanje revidiranog limita kreditne kartice u jezgri bankarska platforma.

Nakon odobrenja povećanja limita, korisnik može biti obaviješten koristeći niz metoda. S obzirom na porast zlonamjerne e-pošte preko interneta, takve obavijesti ili se šalju na mobilni telefon, fizička pošta poštom ili se mogu pojaviti kao poruka direktno na računu Internet bankarstva za pregled od strane klijenta kada slijede pristup svojim računima.

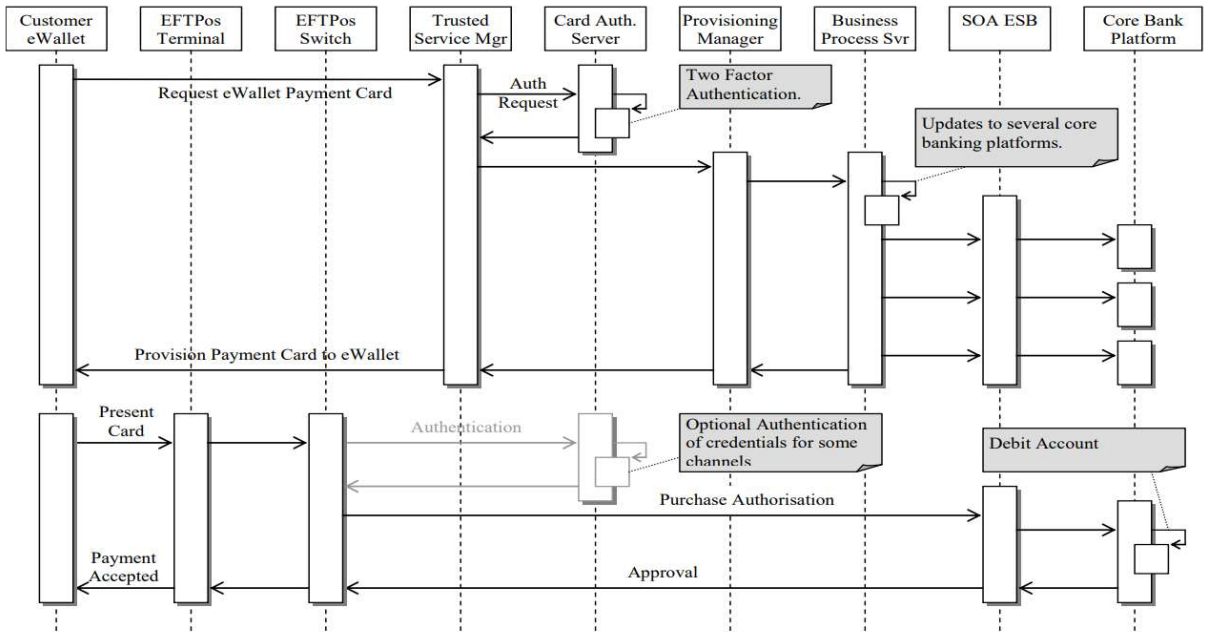


Slika 5. Interakcija mobilnog kanala

7.3. Kupac vrši kupovinu koristeći eWallet koristeći Point of Sale Channel

Konačni primjer interakcije sažima kako komponente surađuju pri obradi a zahtjev za plaćanje putem mobilnog uređaja, s ugrađenim eWallet-om, preko prodajnog mjesta trgovački terminal. Banka će prvobitno dostaviti podatke o platnoj kartici klijentu pametna kartica (SIM) na svom mobilnom telefonu, to uključuje zahtjev putem Upravitelja pouzdanih usluga (TSM) banci i kada se autentificiraju odgovarajući podaci o računu su sigurno mobilnom telefonu koristeći banku Provisioning Manager. Postoji nekoliko entiteta koji mogu upravljati i implementirati

upravitelja pouzdane usluge[12], međutim pretpostavljamo da banka ima implementirati ovu komponentu kako bi maksimizirali nekoliko prednosti koje su razmatrane. Kada je eWallet kartica Ovo je također aktivirano na odgovarajućoj platformi jezgre bankarstva, pogledajte sliku 4.



Slika 6. Interakcija eWallet i Eftpos kanala

Kada je kupac spreman da kupi predmet, premješta svoj mobilni telefon u neposrednoj blizini do EFTPos terminala koji podržava beskontaktni komunikacijski sistem u blizini polja. Plaćanje Zahtjev za autorizaciju se šalje preko EFTPos finansijske mreže i prosljeđuje se na odobrenje (opcionalno, vjerodajnice se provjeravaju putem usluge provjere autentičnosti platne kartice za neki web kanala). Usluga SOA ESB-a (to obično može biti dio osnovne bankarske platforme za povećanje performansi) se poziva da se verifikuje i zatim obradi zahtjev za autorizaciju kupovine; to je da se utvrdi da li su na raspolaganju dovoljna sredstva sa naknadnim zaduženjem na računu osnovna bankarska platforma. Potom se odobrenje vraća korisničkom uređaju. Hvatanje fondova je obrađuje se u kasnijoj fazi korištenjem konvencionalnih serijskih transakcija preuzimanja trgovaca. Deployment ključnih tehnologija kao što je TSM unutar banke, pomažu da se omogući ovaj tip distribucije Kanal koristi nove tehnologije na način koji je besprijekoran za korisnika.

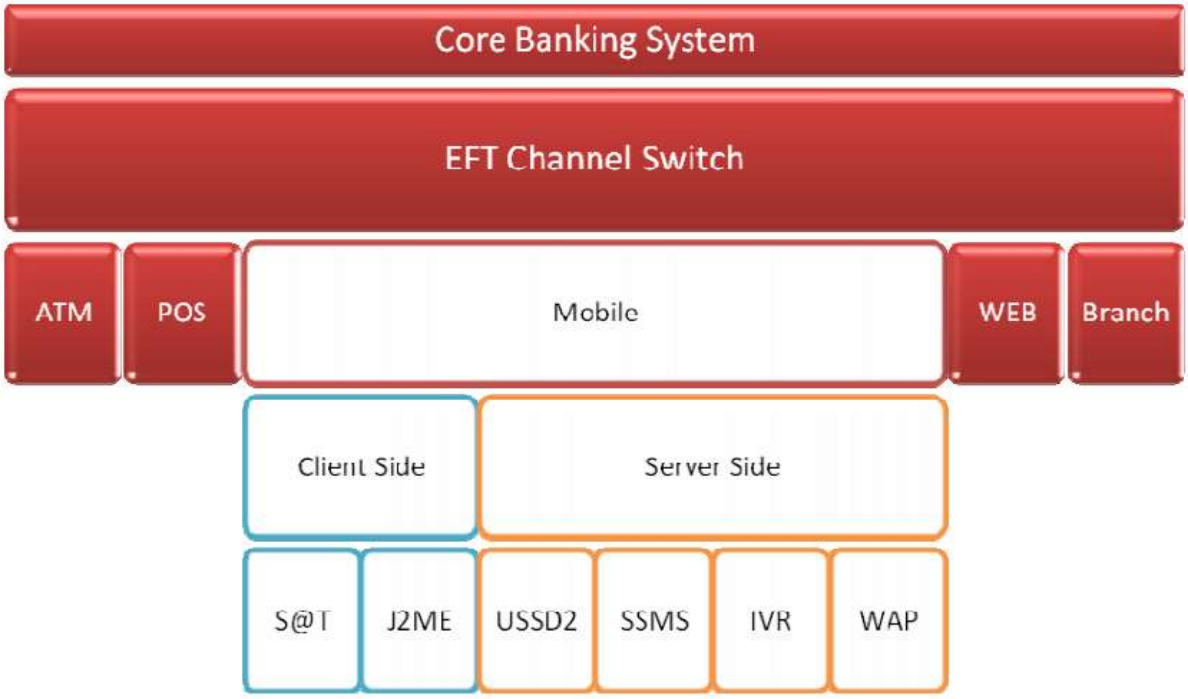
[12] D. Worthington, "Five Reasons Why Banks Should be their own TSMs", BellId, 2012. http://www.bellid.com/media1/blog/view/17-5-reasons-why-banks-should-be-their-own-tsms

8. Opcije implementacije platforme za mobilno bankarstvo

8.1. Arhitektura visokog bankarskog kanala

Mobilno bankarstvo predstavlja proširenje postojeće infrastrukture plaćanja banke na mobilne telefone kao kanal za pokretanje mobilne mreže i njenog dometa, za isporuku bankarske usluge za potrošače.

Infrastruktura mobilnog bankarstva tako je u sličnom tehničkom okruženju kao i banke Ponude bankomata, POS, podružnica i internet bankarstva. Osnovni bankarski sistem banke, sistem koji sadrži račun potrošača i koji se odnosi na njega upravljanje transakcijama i istorija, zahtijevaju sredstva za prevođenje bankarskih instrukcija, od potrošača, preko jednog od bankovnih kanala kao što su bankomati ili internet, u a format koji jezgro bankarskog sistema može obraditi. Ovaj prevod se obično izvodi od strane EFT channel switch[13]. EFT prekidač kanala bi prebacivao transakcije iz kanala u odgovarajuću oblast unutar jezgrenog bankarskog sistema.



Slika 7. Mobilno bankarstvo u ukupnoj bankarskoj arhitekturi.

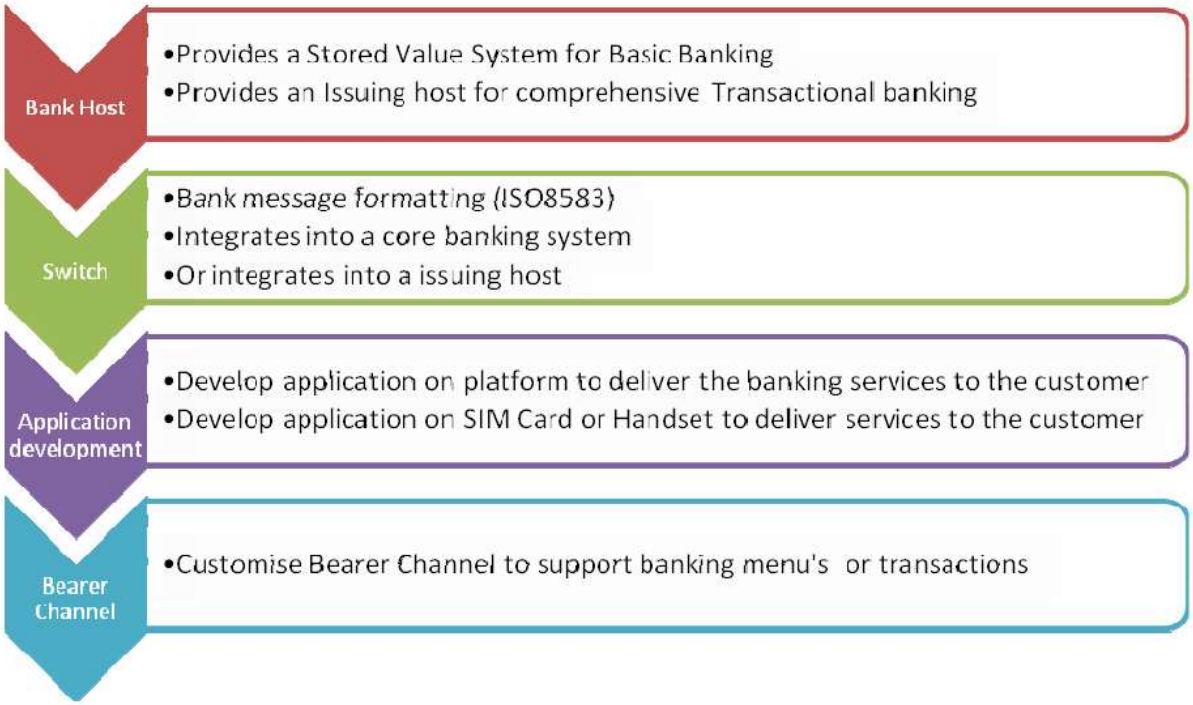
[13] An Electronic Funds Transfer, EFT, or Financial Switch accepts, translates and forwards transactions from multiple channels to the bank's core systems. This can sit within the bank or the bank's third party processor.

Kanal mobilnog bankarstva može se dostaviti potrošaču preko dva nosioca ili aplikacijska okruženja. Aplikacije na strani klijenta su aplikacije koje se nalaze na SIM kartici potrošača ili na njihovoj stvarnoj mobilni telefon. Tehnologije na strani klijenta uključuju J2ME i S @ T. Aplikacije na strani servera razvijaju se na serveru dalje od mobilnog telefona potrošača ili SIM kartica.

Tehnologije na strani servera uključuju USSD2, IVR, SSMS i WAP. Banka bi samo trebala odabrati jedan od ovih kanala bearer[14], ili strategije kanala nositelja, za implementaciju. Međutim, na nekim tržištima bilo bi pametno provesti više od jednog kanala nosioca kako bi se upravljalo potrošačima i rizik povezan sa nepoduzimanjem specifične tehnologije. Izabrani kanal nosioca ne utječe na mjesto gdje bi trebala biti smještena platforma mobilnog bankarstva.

8.2. Nivoi implementacije platformi mobilnog bankarstva

Produženje franšize plaćanja na mobilne može biti jednostavno kao bankovni kanal omogućavanje ili kao kompleksno kao kompletna implementacija bankarskog sistema u zavisnosti od toga šta infrastruktura već postoji, i ona koja se može ponovo koristiti kao dio implementacije.

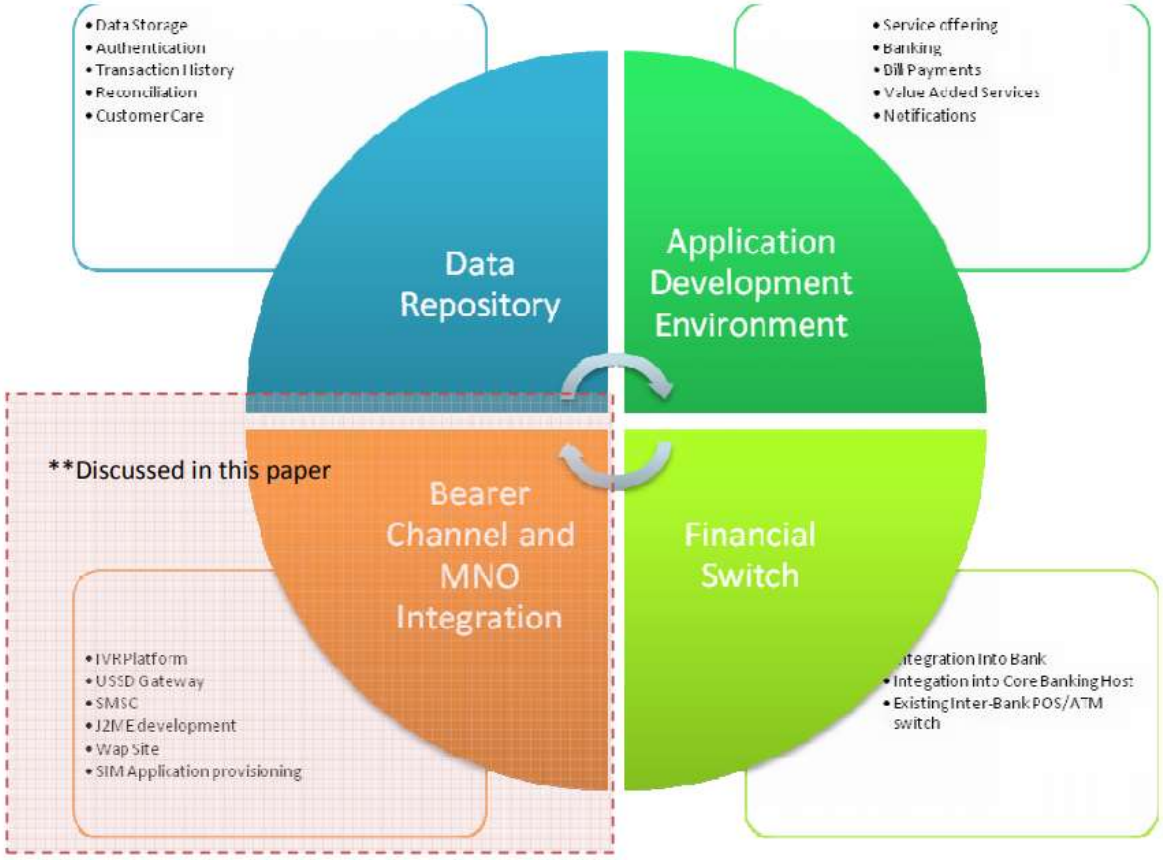


Slika 8. Mobilna bankarska rješenja zahtijevaju sljedeće slojeve u omogućavanju mobilnog bankarstva

[14] Access channel for a consumer from their mobile phone, such as SSMS, WAP, USSD2, etc.

8.3. Platforma za mobilno bankarstvo Arhitektura visokog nivoa

Ako pogledamo tipičnu banku kao onu koja već ima osnovni bankarski sistem, onda mobilni bankarska platforma koju bi banka koristila, ili koja bi se integrisala, imala bi sljedeće komponente:



Slika 9. Komponente platforme za mobilno bankarstvo

Gornji dijagram odražava tipičnu uslugu mobilnog bankarstva. Usluga bi zahtijevala integracije u MNO kako bi se olakšalo korištenje kanala nositelja mreže i kako bi se to učinilo pristupite mobilnom telefonu potrošača. Spremište podataka pohranjuje dovoljno informacija o klijentima kako bi se olakšala obrada finansijske transakcije. Spremište podataka bi također imalo dovoljno informacija autentifikaciju klijenta u svakoj transakciji. Po stambenim transakcionim i potrošačkim podacima, spremište bi također olakšalo brigu o klijentima i pomirenje određenih finansijskih transakcije koje koriste okruženje za razvoj aplikacija za izvršavanje usluga. E.g. prodaja vrijeme emitiranja bi zahtijevalo usklađivanje između obrađenih transakcija i vremena emitiranja operatera mreže.

Okruženje za razvoj aplikacija olakšava stvarni razvoj usluge potrošača, kao što su bankarski meniji i komande. Može ugroziti integraciju trećih strana u podržavanju usluga s dodanom

vrijednosti kao što su plaćanje računa ili prodaja na vrijeme. Aplikacija razvojno okruženje podstiče inteligenciju dostavljenu telefonima potrošača, bez obzira da li je klijent ili server.

Finansijski prekidač bi funkcionisao kao interfejs centralnog bankarskog sistema banke. Instrukcije sakuplja okruženje za razvoj aplikacija preko MNO interfejsa i koristi podatke iz spremišta podataka, prenose se preko financijskog prekidača u format transakcije banka može koristiti.

9. Tehnologije mobilnog bankarstva za prijenosne tehnologije

Ovaj odjeljak se bavi front-end komponentom ili Mobile Banking-om koji se suočava s korisnicima Tehnologije. Ova komponenta lanca vrijednosti do kraja mobilnog bankarstva se obično isporučuje ili prilagođuje od strane prodavca mobilnog bankarstva ili jedinice specijalizovane tehnologije unutar banaka.

Te tehnologije mobilnog bankarstva mogu se kategorizirati u dva okruženja:

Tehnologije na strani servera

Tehnologije na strani servera su one aplikacije koje su izgrađene na serveru, daleko od SIM-a potrošača ili Mobilni telefon. Primjeri tehnologija na strani servera bi bili SMS, IVR, USSD2 i WAP.

Tehnologije na strani klijenta

Tehnologije na strani klijenta su one aplikacije, rješenja i ponude usluga koje su izgrađene ili ugrađene na SIM ili mobilnu slušalicu. Primjeri aplikacija na strani klijenta su S @ T i J2ME (JAVA).

Te tehnologije sa kojima se suočavaju potrošači imaju različite karakteristike i procese.

Svaka od ovih tehnologija zahtijeva da potrošač registrira ili aktivira aplikaciju banka / MNO / prodavac koji nudi uslugu na tržištu. Ovaj proces registracije definiše davalac usluga i služi kao početna identifikacija potrošača kako bi se osiguralo stalno povjerenje i sigurnost transakcije. Oni su brojni načini registracije ili aktiviranja postojećih klijenata, od kojih svi zahtijevaju odobrenje banke koja nudi uslugu.

Registracija potrošača često stvara prepreku za usvajanje potrošača, ali služi kao neophodan korak u procesu eliminacije prevara i potencijalnih transakcionih rizika u ponudi (kao i regulatorni zahtjev).

U aplikacijama na strani poslužitelja, podaci o potrošačima koji omogućuju obradu transakcija, kao što su detalji računa / kartice, obično se čuvaju u zaštićenom okruženju, na serveru u banci ili na njihov dodijeljeni pružatelj usluga / dobavljača.

U aplikacijama na strani klijenta, podaci o potrošaču se obično pohranjuju u aplikaciji ili unose od strane korisnika, i šifrirane aplikacijom na SIM kartici ili slušalici. Svaka od aplikacija na strani poslužitelja i na strani klijenta ukratko su opisane u nastavku.

9.1. SMS bankarska rješenja

SMS (Short Messaging Service) omogućava korisnicima da šalju i primaju tekstualne poruke na mobilnom telefonu telefon pomoću numerisane tastature na slušalici za unos znakova. Svaka poruka može biti postavljena do 160 znakova i šalje se i od korisnika različitih mreža operatora. Svi mobilni danas dostupni telefoni podržavaju SMS. Doista, SMS je postao globalni fenomen, sa milijarde tekstualnih poruka poslanih širom svijeta svake sedmice. Procjenjuje se da je u svijetu ukupno 1 trilijun tekstualnih poruka poslano 2005. godine.

Pored SMS-a osoba-osoba, postoji i veliki broj tekstualnih poruka zasnovanih na sadržaju Usluge su dostupne. Većina GSM operatera korisnicima nudi mogućnost pretplate usluge koje šalju vijesti, sportske i zabavne sadržaje direktno na mobilni telefon u obrascu SMS.[15]

SMS bankarstvo zahtijeva da registrirani korisnik pokrene transakciju slanjem strukturiranog SMS (SSMS) poruka za uslugu mobilnog bankarstva.

Ovaj SSMS zahtijeva identifikator oznake riječi za upućivanje SMS gateway-a na slanje poruke ispravnu SMS aplikaciju. Riječ oznake je prva riječ u SSMS-u.

Ravnoteža SSMS-a bi sadržavala instrukcije od korisnika do Mobile Banking-a aplikacija.

Npr .: "*bank_balance_PIN*" za upit bankovnog salda na bazi SMS-a;

ili

bank_transfer_cheque_savings_100.00_PIN ’za prebacivanje sa čekovnog računa na štednju

račun u iznosu od 100,00.

[15] www.gsmworld.com

U svakom od ovih primjera SSMS će se slati kratkom SMS-u ili adresi (kraći verzija telefonskog broja). SSMS će preći sa potrošačkog telefona kroz GSM mreža za MNO SMSC (Centar za kratke poruke).

SMSC pohranjuje i prosljeđuje SSMS na SMS Gateway dodijeljen kratkom kodu koji koristi Pružalac usluga mobilnog bankarstva.

Pružalac usluga mobilnog bankarstva bi koristio broj mobilnog telefona potrošača koji je proslijedio SMSC sa SSMS-om, da identifikuje potrošača i odgovori na njegov zahtjev.

Odgovor bi slijedio isti povratni put i, u gore navedenim primjerima, bi odgovorio potrošaču SMS porukom potvrde. E.g. „Bank Balance 150.00“ ili From Prelazak sa provjere na štednju od 100,00 “.

9.2. Interaktivni glasovni odgovor (IVR)

U telefoniji, interaktivnom glasovnom odgovoru, ili IVR, je telefonska tehnologija koja omogućava osobi, obično telefonski pozivatelj, za odabir opcija iz glasovnog izbornika i interakciju s telefonom sistem. Reprodukuje se unaprijed snimljen govorni poziv i pozivaoc pritisne broj na telefonu da biste izabrali opciju, tj. "pritisnite 1 za da, pritisnite 2 za ne". Prepoznavanje govora takođe može tumačenje jednostavnog izgovorenog odgovora pozivaoca, kao što su "da", "ne" ili složenije riječi, riječi i imena preduzeća ili broj kao važeći odgovor na glasovnu poruku. DTMF signali (uneseni iz telefonske tipkovnice) i prepoznavanje govora na prirodnom jeziku interpretirati odgovor pozivaoca na glasovne upute.

IVR je najstariji oblik mobilnog bankarstva koji se suočava sa potrošačima. IVR je korišćen prije postojanje mobilnih telefona u obliku telefonskog bankarstva i još uvijek se koristi danas. IVR zahtijeva od registrovanog potrošača da pozove objavljeni broj telefona i bude odgovarao prethodno snimljenim glasom koji potrošaču predstavlja različite opcije menija.

Sistem IVR bi onda od potrošača uzimao potrebne instrukcije upisivanjem tonova odabira broja koje potrošač ulazi na tastaturu, ili putem izgovorene komande i kreira instrukciju koja se daje provajderu / banci. Davatelj usluga bi koristio broj mobilnog telefona potrošača koji je proslijedila mreža da identifikuje potrošača i kao faktor autentičnosti.

Kanal može koristiti bilo koji mobilni uređaj i bilo koji potrošač koji je u stanju da pozove. Pružalac usluga je obavezan da ima IVR sistem koji može koštati samo 7000 USD Međutim, može se povećati i da bude prilično skupa u zavisnosti od broja korisnika treba biti poslužen.

IVR sistemi su prilagođeni korisniku, ali mogu se pokazati skupim za održavanje i skupim za potrošača koji treba da napravi ono što može biti relativno dugačak poziv. Naravno, ovo zavisi o tome ko plaća, u zavisnosti od toga da li je to besplatan telefonski broj ili ne.

9.3. Podaci o nestrukturiranoj dopunskoj usluzi (USSD)

U svojoj najjednostavnijoj definiciji, USSD je forma SMS-a upravljana preko menija, gdje bi korisnik primio a meni teksta na telefonu, za razliku od niza riječi.

USSD je kanal nosioca podataka u GSM mreži. Kao SMS, prenosi male poruke od gore do 160 znakova između mobilnog telefona i mreže. Za razliku od SMS-a, koji je spremište i naprijed ', USSD je zasnovan na sesiji i može pružiti interaktivni dijalog između korisnika i određeni skup aplikacija. Drugim riječima, obe strane dijaloga se dešavaju tokom sesije dok je interakcija zasnovana na SMS porušena u svaki segment komunikacije između klijenta i usluge.

USSD1 dozvoljava jednosmjernu komunikaciju s mrežom, USSD2 omogućava dvosmjernu komunikaciju komunikacije između korisnika i mreže. Sa USSD1, interakcija između korisnik i usluga bi bili razbijeni u svaki komunikacijski segment, slično SMS-u. Sa USSD2 bi bio održan u istoj sesiji i omogućio bi tekući razgovor između korisnika i usluge. Ovo je slično e-pošti i instant porukama, e-mail čeka primaocu da čita i reaguje, dok razmjena trenutnih poruka omogućava neposredan dijalog. USSD je kao standardna značajka kao SMS i dostupan je u procijenjenih 95% uređaja danas.

USSD ne zahtijeva pre-konfiguraciju na SIM ili slušalicama potrošača i već je ugrađen većina GSM mreža. MNO, međutim, moraju komercijalizovati proizvod uspostavljanjem neophodne mogućnosti fakturisanja kanala nosioca i promovisanje upotrebe USSD-a za dodanu vrijednost usluge pored interne mreže i brige o korisnicima. E.g. od * 100 # koji bi dostavili SMS saldo vašeg prepaid računa za računanje vremena na intuitivniji meni punog servisa kao diskutovano u nastavku.

Registrovani potrošač bi pozvao broj koji uključuje * s i #s. Ovaj broj bi mogao biti sačuvan i u telefonskom imeniku potrošača kao ime banke kako bi se izbjegla konfuzija u biranju ili posjedovanju da zapamtite USSD niz.

9.4. Wireless aplikativni protokol (WAP)

WAP se najbolje opisuje kao internet na mobilnom telefonu. **WAP** je otvoreni međunarodni standard za aplikacije koje koriste **bežičnu komunikaciju**. Njegova Osnovna aplikacija je omogućavanje pristupa **Internetu** sa **mobilnog telefona** ili **PDA**. WAP pretraživač pruža sve osnovne usluge web pretraživača, ali je pojednostavljen za rad u okviru ograničenja mobilnog telefona. WAP je sada protokol za koji se koristi većina svjetskih mobilnih internet stranica, poznatih kao WAP stranice.

Mobilni internet sajtovi, ili WAP stranice, su web-stranice koje su pisane ili dinamički konvertovane u WML (Wireless Mark-up Language) i pristupa se preko WAP pretraživača. WAP ili mobilno internet bankarstvo pruža potrošaču slično iskustvo kao i internet bankarstvo.

Potrošač će preći na mobilni internet tako što će pristupiti WAP pretraživaču mobilnog telefona i unos adrese web lokacije. Stvarna bankarska aplikacija prebiva u banci i osiguran je i prati na isti način kao i internet sajt za bankarstvo. Mobilni telefon i nosač (GPRS) se koristi za prikazivanje ili prenosi podatke između potrošača i banke.

Potreban je potrošačev telefon da bude sposoban (funkcionalno razvijen / učitan od strane slušalice proizvođača), i imaju odgovarajuću konfiguraciju (koju obezbjeđuje MNO), kako bi podržali WAP Banking. MNO-i često ovu funkcionalnost segmentiraju samo na post-paid korisnike.

9.5. SIM bazirane aplikacije

SIM Application Toolkit (SAT / S @ T) omogućava pružatelju usluga ili banci da smjesti u okviru SIM kartice. SIM Application Toolkit (koji se obično naziva STK) je standard GSM sistema koji omogućava SIM-u da inicira akcije koje se mogu koristiti za razne usluge sa dodatnom vrijednošću.

SIM Application Toolkit se sastoji od skupa naredbi koje su programirane u SIM karticu definirajte kako SIM treba da stupi u interakciju direktno sa vanjskim svijetom i pokrene naredbe nezavisno od slušalice i mreže. Ovo omogućava SIM-u da izgradi interaktivnu razmjenu između mrežne aplikacije i krajnjeg korisnika, te pristup ili kontrola pristupa mreža. SIM takođe daje komande slušalici, kao što je „meni za prikaz“ i „traži korisnika“ ulaz “.

STK je implementiran od strane mnogih mobilnih operatera širom svijeta za mnoge aplikacije, gde je potreban pristup zasnovan na meniju, kao što je mobilno bankarstvo i pregled sadržaja.

Izazov u SIM baziranim aplikacijama je da aplikaciju već stavite na SIM karticu postoji na tržištu.

Provajder usluge ima mogućnost slanja aplikacije Over the Air (OTA), što podrazumijeva isporuku nekoliko šifrovanih SMS poruka koje sami konfigurišu aplikaciju na SIM kartici, ili, obezbjeđivanje nove SIM kartice sa aplikacijom koja je već ugrađena u SIM. Ovo drugo ima ekonomski uticaj na mrežnog operatera i postojećeg potrošača u tome potrošač bi morao nabaviti novu SIM karticu kako bi mogao koristiti aplikaciju.

Kada se aplikacija nalazi na SIM kartici, mogu se unositi uputstva potrošača, šifrirati, i prenosi se SMS-om do provajdera ili banke. Može biti poteškoća u nadogradnji ili promjeni aplikacije na SIM kartici kao potrošač bi morao ponovo pružiti prijavu u postupku sličnom opisanom gore; ili bi operater mreže morao ponovo učitati aplikaciju po zraku u svaki i svaku SIM karticu svaki put kada izvrše promjenu aplikacije.

Prednost SIM Based Applications je sposobnost mrežnog operatera ili banke da posjeduje komad nekretnina na SIM kartici. Pošto je SIM karticu obezbijedio određeni MNO, ovo osigurava prevenciju odljeva za taj MNO, i osigurava da je banka specifična aplikacija nalazi se na SIM kartici i stoga pruža slične pogodnosti banci.

10. Aplikacija za mobilno bankarstvo i sigurnost podataka

„Over-the-air“ ili „in-the-clear“ su termini koji se često koriste u finansijskoj industriji kada se odnose na bankarske transakcije koje se prenose preko nešifrovanih komunikacijskih protokola.

Vidljivo je da su kanali za mobilne nosioce „jasni“ uglavnom zbog razumijevanja da vaši podaci putuju zrakom (doslovno) i stoga ne mogu biti sigurni. Zabrinutost je da je prevarant u mogućnosti da uključi ili sluša vaš poziv, ili prenos podataka, i da snima podatke zbog zlonamjernih ili lažnih razloga.

Činjenice dokazuju drugačije. GSM sigurnost je snažna, ako ne i jača, od vaše tradicionalne fiksne komunikacije. Trebalo bi novca, vremena i truda da bi to bilo moguće zapravo prodiru u GSM mrežu, kradu podatke, a zatim je koriste na prevaru. Štaviše, ako je ovo bili su vjerovatno u mobilnom bankarstvu, prevarant bi još uvijek bio u mogućnosti pristupiti ograničenom iznosu sredstava iz potrošača računa iz dolje navedenih razloga.

Pregled onoga što bi bilo potrebno da se "čuje" na pozivu ili prenosu podataka preko GSM-a mreže slijede:

Prevarant bi morao da zna gde će klijent biti u vrijeme poziva, a takođe znati broj mobilnog telefona klijenta i moći da putuje sa najbržim putovanjem iz poziva jedna bazna stanica na drugu. Povodom izazova mobilnosti, prevarantu bi onda i dalje potrebno dešifrirati GSM enkripciju i pronaći način da se identificira određeni mobitel komunikacija, s obzirom da je identifikacija korisnika kao GSM potrošača skrivena u svrhu privatnosti.

Ako se pretpostavi da je prevarant mogao da postigne sve gore navedeno, onda bi to bilo podvrgnuti odgovarajućim provjerama brzine i transakcijskim ograničenjima koje je banka ili njihova banka naplatila platforma.

Stoga se čini da nije moguće da prevarant troši svoj novac i energiju na pokušaj slomiti sloj komunikacije. Ali još uvijek ne može biti dovoljno samo za bankarstvo pruža nešifrovane podatke putem šifrovanog kanala. U upoređivanju protokola komunikacije u nepokretnoj mreži sa mobilnim, jasna diferencijacija na zaštita prenesenih podataka se pojavljuje u nastavku.

10.1. Opcije sigurnosti tradicionalnog bankarstva

Dijagrami ispod prikazuju opcije koje su dostupne za osiguravanje podataka preko tradicionalnih fiksna telefonska komunikacija:

Nešifrovani podaci preko nekodirane fiksne komunikacijske veze:

Ovo nije idealno rješenje za bankarstvo jer ne pruža zaštitu podataka ili stvarne komunikacijske protokole, koji komunikacijsku vezu ostavlja za lako prodiranje i podatke lako pristupačne.

Nešifrovani podaci preko šifrirane fiksne komunikacijske veze:

Time bi se osigurao vanjski sloj komunikacije, što bi bilo teško bilo kome da se uključi u komunikacijski sloj kako bi se došlo do podataka koji se prenose u banku. Međutim, nešifrovani podaci su u opasnosti.

Šifrirani podaci preko šifrirane fiksne veze:

Ovo je tipično kako se podaci banke prenose od potrošača preko svojih kanala do svog domaćina. Šifrovani podaci poslani preko šifrovanog komunikacijskog sloja. Podaci su obično šifrovani na kanalu, tj. na ATM-u ili POS-u.

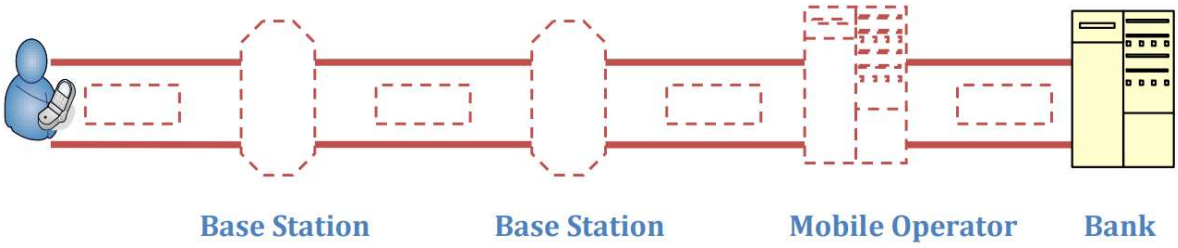
Dodatna autentifikacija i ublažavanje rizika kao dodatna mjera sigurnosti

U tradicionalnim bankarskim okruženjima imamo smanjenje rizika i autentičnost potrošača kao:

- Dva faktora autentifikacije, kao što su ATM kartica i ATM PIN osiguravaju da ste vi da biste mogli potvrditi da je korisnik od koga primate transakcije.
- Praćenje i prevencija prevare, kao što su ponašanje potrošača i geografski trošiti ponašanje.
- Brzina provjerava i troši ograničenja, sprječavajući ne više od definisanog broja transakcije se pojavljuju i sprječavaju samo određeni iznos po danu od potrošnje.

10.2. Opcije sigurnosti mobilnog bankarstva

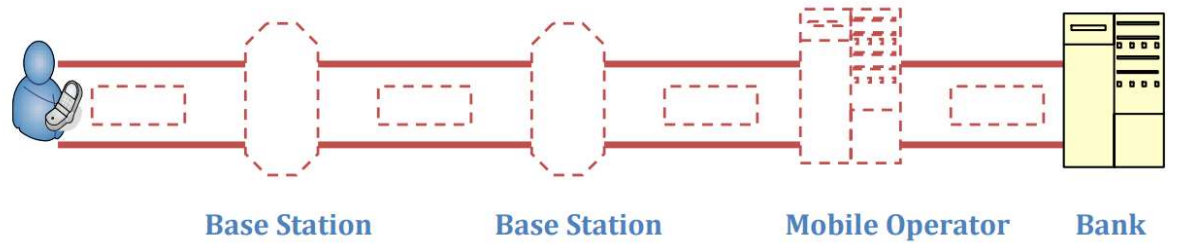
Dijagram ispod prikazuje opcije koje imate za osiguranje podataka preko GSM kanala:



Podaci koji se prenose preko mobilne mreže zaštićeni su standardnim GSM sigurnosnim protokolima na sloj komunikacije. Identitet pretplatnika je također zaštićen u ovom lancu. Rizik u prenos podataka preko GSM kanala može se naći u broju zaustavljanja podataka prije dolaska u banku. Za razliku od komunikacije u fiksnoj mreži, podaci se prenose preko mobilnog telefona mreža prelazi sa jedne bazne stanice na drugu, što znači da je lanac kriptovan komunikacija je prekinuta. Podaci su također nešifrovani kada pogodi mrežnog operatera. Tako, postoji slomljena enkripcija između potrošača i banke.

Ovo se razlikuje po kanalu nosioca ili aplikaciji koja se koristi u mobilnom bankarstvu:

Sigurnost podataka za SMS bankarstvo

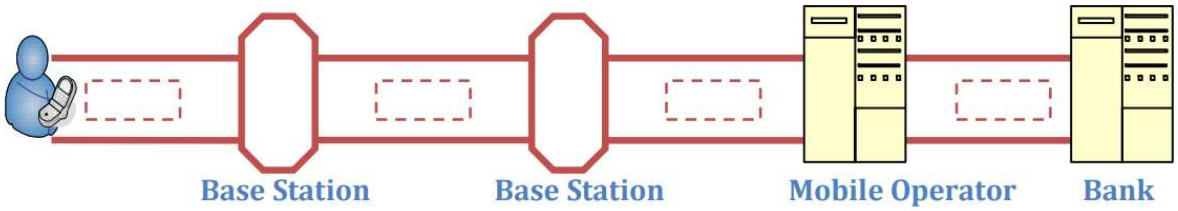


SMS bankarstvo se smatra najbezbjednijim kanalima mobilnog prenosnika. Ovo je zbog broja tačaka koje su SMS-ovi dostupni drugima u jasnom ili nešifrovanom formatu.

Potrošač bi pokrenuo transakciju slanjem SMS poruke banci putem SMS-a banke kratki kod kao završna adresa. SMS će biti automatski pohranjen na telefonu i dostupan svima koji ga vide telefon potrošača. SMS će zatim proći kroz šifrovanu GSM komunikaciju kanala, preko baznih stanica i prekida se kod operatera mobilne mreže, gdje se nalazi obično se čuvaju nešifrovane. U ovom trenutku MNO može proslijediti poruku banci procesor bežične aplikacije, SMS gateway ili procesor mobilnog bankarstva (koji može biti treći partija), gdje je pohranjena ili

kodirana ili nešifrirana. Treća strana bi onda proslijedila poruku banci preko šifrirane fiksne linije do banke gdje se obično pohranjuje u a osigurano okruženje. Kao što se može videti, postoji mnogo tačaka izlaganja.

IVR, USSD sigurnost bankovnih podataka:



IVR, kao glasovni poziv, zaštićen je i šifrovanim GSM komunikacionim slojem[16], kao i GSM zaštita pretplatničkog identiteta potrošača[17] i prenosi se preko mobilne mreže do IVR banke. Samo u ovom trenutku su unosi koje je potrošač unio u njihov telefon, pohranjeni. Ako je to u okruženju banke, trebalo bi da bude sigurno, ali ako na platformi „na pola“ nije sigurno.

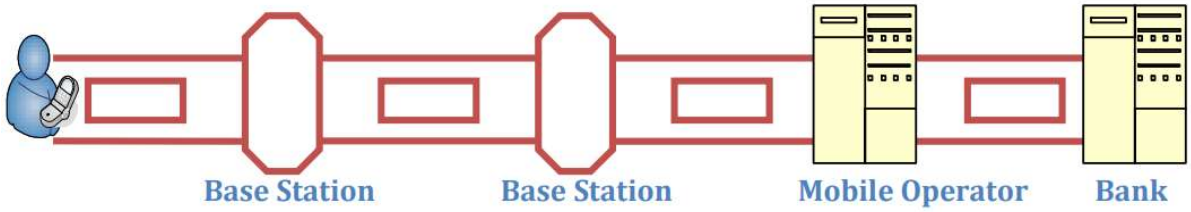
USSD2 je sličan IVR-u za sigurnost podataka tako što otvara jednu sesiju između uređaja i USSD2 aplikacija kod mrežnog operatora, procesora ili banke. Drugim riječima transakcija je završena dok je sesija otvorena i nije pohranjena za naknadni završetak.

Tok transakcija od kraja do kraja je preko šifrovanog sloja komunikacije GSM i identitet pretplatnika je takođe skriven. Podaci se također mogu šifrirati čim se završi na USSD2 gateway sedi kod mrežnog operatera, procesora ili banke i tako sprječava bilo kakav interni rizik od zloupotrebe podataka. Stoga je jedini rizik da se podaci unesu u komunikaciju sloj nije sam kriptovan. Ako bi neko mogao da prekine GSM enkripciju, on bi imao pristup podacima.

U IVR, USSD2 i SMS bankarskim kanalima, osjetljivi podaci potrošača se obično čuvaju na a serveru, a ne na slušalici. Ovi podaci su šifrovani. Podaci unijeti u slušalicu su ograničeno na provjeru autentičnosti potrošača (PIN) i bankarske instrukcije od strane potrošača, bez unosa računa ili ličnih podataka. Prijetnja ostaje da ako telefon i SIM kartica i podaci za autentikaciju su ukradeni i korišćeni na mobilnom telefonu bankarski kanal za transakcije, onda je potrošač u opasnosti. Podaci su beskorisni bez ovih četiri elementa. Ovo je slično ATM kartici i Pin okruženju.

[16] GSM Security Standards
[17] GSM Security Standards

S@T sigurnost bankovnih podataka, J2ME i WAP



WAP omogućava otvaranje GPRS sesije između web pretraživača i weba aplikacija u banci. Ova sesija je ponovo zaštićena šifrovanim GSM-om komunikacijski sloj, a zatim može biti dodatno zaštićen enkripcijom stvarnog bankarstva web stranici kojoj se pristupa. To čini WAP bankarstvo otvorenim za slične prijetnje kao i internet bankarstva, koja je dodatno osigurana time što banka može utvrditi da je sjednica započeta od SIM-a potrošača.

J2ME koristi isti kanal nosioca kao WAP. Međutim, J2ME aplikacije mogu imati dodatnu bezbijednost oko aplikacije koja se nalazi na slušalici. Tako su podaci unijeti u Aplikaciju J2ME se može kodirati u tom trenutku i poslati preko GPRS kanala kako je opisano gore. On bi se dešifrirao samo u banci ili procesoru. J2ME je ipak otvoren za određene napade u kojima potrošač treba da utvrdi da li se aplikacija preuzima ispravan izvor i da izvor nije onaj zlonamernog pokušaja kopiranja banaka primjena u cilju dobivanja osjetljivih podataka od potrošača.

S @ T je najsigurniji način mobilnog bankarstva. Ona omogućava banci da učita svoje šifrovanje ključevi na SIM kartici sa sopstvenom aplikacijom banke. Prema tome, podaci o potrošačima mogu se pohraniti na SIM kartici, a potrošač može biti ovjeren na slušalici prije nošenje bilo kakvih podataka preko mobilne mreže. Podaci su takođe kodirani prije odlaska i dešifruje se samo pomoću bankovnih ključeva za šifrovanje u banci.

10.3. Sigurnosne karakteristike Androida i iOS-a

Bezbijednosni model Android sistema primjenjuje sandboxing aplikacija u svom sistemu. To znači da su sve aplikacije ograničene samo na određene resurse, što ih čini nesposobnim za interakciju sa resursima jednih drugih. Aplikacija ne može ometati resurse ili podatke koje čuva druga aplikacija, što ih čini imunima na viruse (ne na sam telefon). Sandboxing se podrazumijeva i za korisnika koji je ograničen na pristup root-u, čineći korisničke skinuti virus nesposoban da koristi sistemske komande u rootu. Appleov iOS operativni sistem takođe koristi sandboxing aplikacija koje su napravili drugi proizvođači.

Uprkos sandboxingu, Android aplikacije mogu međusobno komunicirati. Sve funkcionalnosti kao što su kamera, telefon i sistemski mehanizmi itd. Rade kao aplikacija. Komunikacija između Android aplikacija se vrši pomoću tzv. "Namjera". Namjera znači da će aplikacija poslati zahtjev za upotrebu dijela funkcionalnosti aplikacije, koje se nazivaju komponente. Ako aplikacija za SN želi koristiti kameru, ona mora izraziti svoju namjeru korištenja.

Međutim, aplikacija može koristiti komponentu samo ako ima dozvolu za to. Ovaj sigurnosni mehanizam zasnovan na dozvolama u osnovi kreira listu kontrole pristupa za aplikacije ako obe aplikacije imaju odgovarajuću listu prava pristupa komponenta, dozvola se daje. Obratite pažnju na to da odbijanje pristupa komponentama aplikacije se ne zasniva na imenovanju aplikacija, što bi bilo problematično jer programer ne može znati koje će aplikacije korisnik imati u telefonu. Lista kontrole pristupa se kreira tokom instalacije i kada se pokrene namjera, IPC mehanizam će provjeriti da li obje aplikacije imaju odgovarajuću sigurnosnu politiku.

U Appleovim iOS operativnim sistemima, aplikacije trećih strana mogu da komuniciraju sa korisničkim informacijama kao što su kontakt podaci i iCloud sa određenim parom ključeva, dopuštajući Appleu da zna programera koji koristi ove resurse. Ako aplikacija treće strane želi da komunicira ili koristi resurse druge treće strane aplikacija, oni moraju biti u aplikacijskoj grupi. U aplikacijskoj grupi, sve aplikacije dijele jedinstveni ključ koji im omogućava da se međusobno prepoznaju. Na taj način iOS osigurava da nijedna neželjena aplikacija ne može upravljati resursima aplikacije.

Prethodno spomenute sigurnosne značajke u Androidu i iOS-u pokazuju njihovu sposobnost da zaštite aplikacije jedni od drugih. Oba operativna sistema omogućavaju programerima da komuniciraju aplikacije koristeći TLS / SSL protokol kako bi zaštitili svoj promet podataka. Ovo i dalje ostavlja neke rupe.

Android je podijelio sve svoje funkcionalnosti u aplikacije i podrazumijevane aplikacije. Oni su u opasnosti, jer su otvoreno poznati programerima. To daje resurse malware aplikacija za rad sa mikrofonom i kamerom itd. Android sigurnosni sistemi su kreirani da zaštite aplikacije od sebe, a ne od njih čitav sistem. Android je dobio kritiku zbog toga što nije u mogućnosti da primeni crnu ili bijelu listu u sistemu. Appleovi programeri moraju biti registrovani na taj način, što čini kreiranje malware-a rizičnim jer sistem čini da se zlonamerni programer lako pronađe jer je potrebno da bude registrovan od strane stvarne osobe ili registrovana organizacija.

11. Zaključak

Finansijske institucije su povećale zavisnost od tehnoloških rješenja koja omogućavaju njihovo finansijsko poslovanje proizvoda i usluga. Proliferacija internet tehnologija, mobilnih uređaja i konkurencije, međunarodna trgovina je uvela pritisak na bankarske i finansijske institucije da to osiguraju i održava se konkurentno vođstvo. Ključni izazov za bankarstvo i finansije je kako usvojiti nove Informacione i komunikacione tehnologije (IKT) unutar organizacije na vrijeme, bez ometanja postojećih rješenja koja pružaju trenutne bankarske softvere za poslovanje.

U radu se predlaže višekanalna arhitektura za finansijske institucije kao što je bankarstvo. Arhitektura je bazirana na industrijskom iskustvu u razvoju višekanalnih rješenja u sličnim industrijama dalje se usavršavaju na osnovu naših iskustava u bankarstvu. Predložena arhitektura se može koristiti olakšati donošenje odluka o tome kako najbolje implementirati nove i nove multikanalne tehnologije unutar bankarstva, pružajući sredstva za procjenu kako osigurati učinkovito korištenje postojećih ulaganja u sisteme i tehnologije. Rješenje se može koristiti kao nacrt za razvoj bankarskih institucija višekanalne strategije; bavljenje postojećim, novim i budućim kanalima bankarske distribucije.

Kako bankarske institucije nastavljaju sa inovacijama u novim tehnologijam, postoji povećana motivacija za uspostavljanjem tehnološkog okvira za usvajanje novih kanala distribucije i tehnologije. Klijenti se dokazuju da su tehnički pametniji i stoga će imati tendenciju ka upotrebi novih uređaja za obavljanje svojih finansijskih i poslovnih aktivnosti. U ovom radu smo opisali arhitekturu višekanalnog sistema za bankarstvo, ilustrujući kako se komponenta sistema interaguje u praksi. Predloženi okvir slijedi pristup slojevite arhitekture koji olakšava primjenu novih tehnologija, s ciljem minimiziranja poremećaja u osnovnim bankarskim platformama. Tradicionalni kanali bankarstva za obavljanje trgovine suočavaju se sa povećanom konkurencijom novih učesnika koji koriste internet tehnologije za obavljanje finansijskih transakcija.

Banke koje su u mogućnosti primijeniti te nove tehnologije i podržavaju nove kanale korištenjem novih platnih instrumenata bit će u boljoj poziciji da služe klijentima slijedeći te trendove u usvajanju uređaja. Nadamo se da će predložena arhitektura i pristup biti korisni kao nacrt za druge finansijske institucije koje razvijaju svoje programe za buduće višekanalne bankarske sisteme. Postoji dalji rad na razjašnjavanju poslovnih procesa povezanih sa predloženim okvirom, uključujući poslovne aktivnosti za podršku i održavanje novih kanala o kojima se raspravljalo. Osim toga, potrebno je više rada za definiranje sigurnosnih arhitektura

potrebnih za podršku sistema za višekanalnu banku kako se nove prijetnje pojavljuju kroz korištenje novih tehnologija.

Štaviše, očekuje se da će, kada se na tržište pojave nove aplikacije i uređaji na strani klijenta, napadači će ciljati ove oblasti pokušavajući da iskoriste bezbijednosne izloženosti u ovim tehnologijama.

12. Literatura

[1] C.J. Pavlovski, “Service Delivery Platforms in Practice”, IEEE Communications Magazine, vol. 45, no. 3, March 2007, pp. 114-121.

[2] T. Kamogawa and H. Okada, “Enterprise Architecture and Information Systems - In Japanese Banking Industry”, International Symposium on Applications and the Internet. IEEE, 2008, pp. 433-436

[3] J. Sun and Y. Chen, “Building a Common Enterprise Technical Architecture for an Universal Bank”, International Conference on Management and Service Science (MASS), 2010, pp. 1-4.

[4] R. Winter and R. Fischer, “Essential Layers, Artifacts, and Dependencies of Enterprise Architecture”, Journal of Enterprise Architecture, Vol. 3, Issue 2, May 2007.

[5] K. Pousttchi and M. Schurig, “Assessment of Today’s Mobile Banking Applications from the View of Customer Requirements”, Proceedings of the 37th Hawaii International Conference on System Sciences - 2004, pp. 1-10.

[6] M.K. Harma and R. Dubey, “Prospects of technological advancements in banking sector using Mobile Banking and position of India”, International Association of Computer Science and Information Technology, 2009, pp. 291-295

[7] P. Chandrahas, D. Kumar, et. al., “Some Design Considerations for a Mobile Payment Architecture”, National Conference on Communications (NCC), 2011, pp. 1-5.

[8] S.K. Bhosale, “Architecture of a Single Sign on (SSO) for Internet Banking”, IET International Conference on Wireless, Mobile and Multimedia Networks, 2008. IET pp. 103-105.

[9] C.Narendiran, S.A. Rabara, and N.Rajendran, “Performance Evaluation on End-to-End Security Architecture for Mobile Banking System”, 1st IFIP Wireless Days, 2008, pp. 1-5.

[10] H. Reza and N. Mazumder, “A Secure Software Architecture for Mobile Computing”, 9th International Conference on Information Technology- 2012, pp. 566-571.

[11] C. Möckel, “Usability and Security in EU E-Banking Systems: Towards an Integrated Evaluation Framework”, International Symposium on Applications and the Internet, 2011, pp. 230-233.

[12] A. Carignani, M. De Marco, and C. Rosenthal-Sabroux, “Supporting a multiple channel architecture design: the UML contribution in a virtual banking environment”, ECIS 2000 Proceedings. Paper 21. pp. 883-888.

[13] S. Mitchell, C.J. Pavlovski, et al. “Multimodal Natural Language Platform Supporting Cellular Phones”, The ACM Journal of Mobile Computing and Communications Review (MC2R), ACM Sigmobile, Vol.10, Iss.3, pp. 34-45, 2006.

[14] C. Cox, “Trusted Service Manager: The Key to Accelerating Mobile Commerce”, FirstData, 2009. http://www.firstdata.com/downloads/thought-leadership/fd_mobiletsm_whitepaper.pdf

[15] D. Worthington, “Five Reasons Why Banks Should be their own TSMs”, BellId, 2012. http://www.bellid.com/media1/blog/view/17-5-reasons-why-banks-should-be-their-own-tsms

[16] Business Wire, “U.S. Bank Introduces Augmented Reality iPhone® Application to Find Branches and ATMs”, 2012. http://www.businesswire.com/news/home/20120411005193/en/U.S.-Bank-Introduces-Augmented-RealityiPhone

[17] PrivatBank, “PrivatBank ready for customer service with Google Glass”, Press Release, April 2013. http://www.privatbank.lv/en/presscenter/pressrelease/2013/news2013-04-001/.

[18] A. S. Yang, “Exploring adoption difficulties in mobile banking services,” Canadian Journal of Administrative Sciences, vol. 26, 2009, pp. 136-149.

[19] A. A. Shaikh and H. Karjaluoto, “Mobile banking adoption: a literature review,” Telematics and Informatics, vol. 32, 2015, pp. 129-142.

[20] W. M. To and L. S. L. Lai, “Mobile banking and payment in China,” IT Pro, May/June 2014, pp. 22-27. [4] “Mobile banking,”

[21] Drexelius, K. & Herzig, M., “Mobile Banking and Mobile Brokerage – Successful Applications of MobileBusiness?”, International management & Consulting , Vol.16, No. 2 (2001): 20-23.

[22] Bansai, P., “Mobile Banking Steps up a Gear”, The Banker , Vol. 151, No.905 (2001): pp 121-122

[23] Kiesnoski, K., “Wireless Banking”, Bank Systems & Technology, Vol. 37, No.2 (2000): 40-43

[24] Horton, V., “Cash and Carry Mobile Banking”. Unix& NT News, No. 141 (2001): 42-43