Sistem nestrukturiranih podataka dodatnih usluga

Perčić, Ivan

POLITEHNIKA PULA

VISOKA TEHNIČKO-POSLOVNA ŠKOLA

S PRAVOM JAVNOSTI

IVAN PERČIĆ

SISTEM NESTRUKTURIRANIH PODATAKA DODATNIH USLUGA

ZAVRŠNI RAD

Pula, Rujan 2014.

POLITEHNIKA PULA

VISOKA TEHNIČKO-POSLOVNA ŠKOLA

S PRAVOM JAVNOSTI

IVAN PERČIĆ

Matični broj: 0690, izvanredni student

SISTEM NESTRUKTURIRANIH PODATAKA DODATNIH USLUGA

Završni rad

Kolegij: Elektrotehnika

Mentor: prof.dr.sc. Luciano Delbianco

Pula, studenog 2014

IZJAVA O SAMOSTALNOSTI IZRADE ZAVRŠNOG RADA

Izjavljujem da sam završni rad na temu SISTEM NESTRUKTURIRANIH PODATAKA DODATNIH USLUGA („USSD – UNSTRUCTURED SUPPLEMENTARY SERVICES DATA“) izradio potpuno samostalno, koristeći se internim materijalima tvrtke Infobip d.o.o te pod voditeljstvom mentora prof.dr.sc. Luciana Delbianca. Rad je pisan u duhu hrvatskog jezika.

U Puli, ……..

Student:

Zahvala

Ovom se prilikom zahvaljujem profesorima i asistentima Politehničkog studija u Puli na predanosti i zalaganju za prenošenje znanja koje je, kao što i sam slogan Politehnike govori, primjenjivo odmah. Posebno se zahvaljujem mentoru prof. dr. sc. Lucianu Delbiancu na strpljenju i uloženom trudu kako bi ovaj rad bio uspješno priveden kraju.

Sažetak:

Kroz ovaj rad ću koristeći se svojim znanjem stečenim kroz radni odnos u Infobip d.o.o predočiti trenutno stanje USSD protokola („Unstructured supplementary service data“ - „Sistem nestrukturiranih podataka dodatnih usluga“), načine korištenja te eventualne probleme na koje bi mrežni operateri trebali obratiti pozornost u svrhu poboljšanja usluge. Pritom ću se osvrnuti na tehnologije pomoću kojih je omogućena komunikacija između korisnika, komponenata u lancu i aplikacijskog servera sve u svrhu jednostavnog prijenosa i obrade podataka, te prikupiti mišljenje auditora o USSD uslugama kroz jednostavnu USSD anketu.

Samim protokolom se ostvaruje veza (sesija) u realnom vremenu između mobilnog uređaja i mrežne stanice te se koristi za transparentni prijenos podataka u oba smjera. Komunikacija se ostvaruje preko radio veze putem signalnih kanala kratkim tekstualnim interakcijama između uređaja i mobilne stanice.

Summary:

Through this graduate work, and with using knowledge from my Infobip d.o.o employment I will present current stage of USSD protocol („Unstructured supplementary service data“ - „Sistem nestrukturiranih podataka dodatnih usluga“), methods of use and eventual problems which mobile operators should pay attention to, in order to improve the service. At the same time, I'll go through all of the technologies which are empowering communication between end users, components in chain, and application server while paying attention on simple data process and transfer. At the end, I'll gather auditors thoughts about USSD service, through simple USSD questionnaire.

Protocol is being used to establish a connection (session) in real time between mobile device and network station, and its transparent transfer of data in both directions. Coomunication is being done through radio connection, using signal channels with short textual interactions between device and mobile station.

Sadržaj

1 Uvod

Kroz ovaj rad ću koristeći se svojim znanjem stečenim kroz radni odnos u Infobip d.o.o predočiti posebnosti USSD[1] usluga te opisati interakciju svih komponenata u lancu koje omogućuju korištenje USSD usluga u svakodnevnom životu. Osvrnuti ću se i na upotrebu protokola kroz različite sektore te ga prezentirati kroz jednostavnu USSD anketu.

1.1 Sistem nestrukturiranih podataka dodatnih usluga

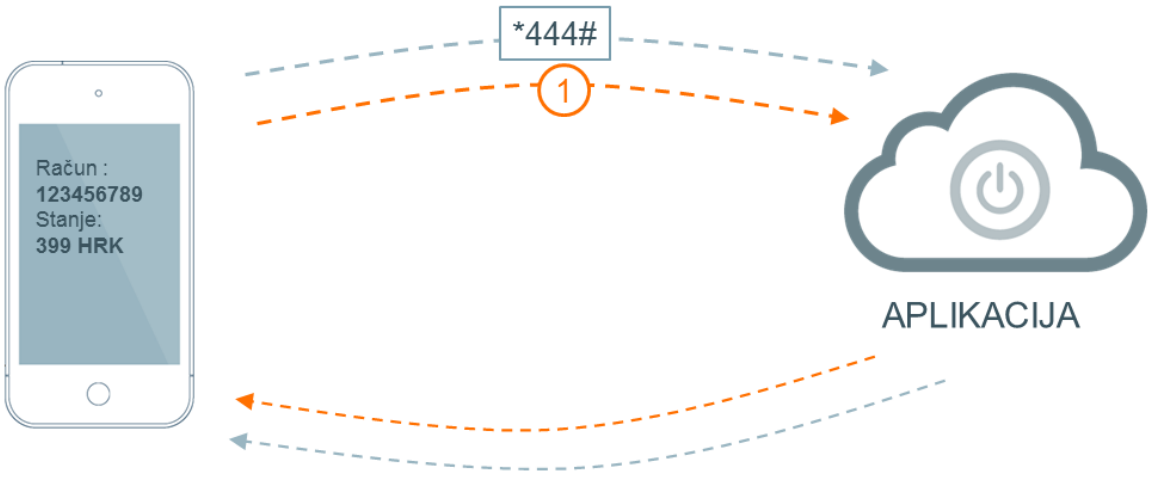
Jednostavnim prijenosom informacija putem radijske mreže (unutar Telekomunikacijkog sustava), SS7[2] protokola te komunikacijom sa aplikacijskim serverom kreiramo podlogu za razvoj brzih i dinamičnih servisa neovisno o korištenoj mobilnoj tehnologiji i trenutnoj lokaciji korisnika usluge, takav skup komponenata nazivmo USSD.

Protokolom se ostvaruje veza (u daljnjem tekstu sesija) u realnom vremenu između mobilnog uređaja i mrežne stanice te se koristi za transparentni prijenos podataka u oba smjera. Komunikacija se ostvaruje preko radio veze putem signalnih kanala kratkim tekstualnim interakcijama između uređaja i mobilne stanice.

[1] USSD - „Unstructured supplementary service data“ ili „Sistem nestrukturiranih podataka dodatnih usluga“

[2] SS7 - „Signalling System #7“ ili „Signalizacijski sistem #7“

Slika 1. Primjer iniciranje USSD usluge zvanjem na kratki broj *444#



Slika 2. Primjer interakcije kroz USSD uslugu

1.1.1 Karakteristike

Protokolom se prenose kratke tekstualne poruke, dužine do 182 znaka ovisno o mreži na koju je mobilna stanica prijavljena. Za razliku od SMS-a (Sistem kratkih poruka), USSD poruke predstavljaju interakciju u realnom vremenu za vrijeme trajanje sesije. Sesija ostaje aktivna sve dok je krajnji korisnik ne prekine što omogućava trenutnu i neograničenu razmjenu podataka. Navedene odlike pružaju krajnjim korisnicima širi spektar mogućnosti naspram korištenja SMS-a.

Protokol čine kombinacija DTAP[3] i MAP SS7[4] protokola koji su zaduženi za prijenos informacija između mobilnog uređaja, mrežne bazne stanice, servisa za obradu kratkih poruka i aplikacijskog servera.

Mobilni uređaj nakon pozivanja USSD servisa zaprima poruku u tekstualnom obliku koja se kroz proces ne sprema na niti jednu komponentu u lancu, što je od izričite važanosti kod prijenosa povjerljivih informacija kao što nije slučaj sa SMS porukama. Tokom trajanja sesije između aplikacijskog servera i mobilnog uređaja svi podatci su enkriptirani kako bi se osigurala sigurna i transparentna razmjena podataka.

Navedene sigurnosne stavke sve više prepoznaju klijenti koji raspolažu povjerljivim informacijama, gdje za primjer možemo uzeti bankarski i marketinški sektor.

[3] DTAP - ''Direct Transfer Application Part'' ili ''Direktni prijenos Aplikacijskog segmenta''

[4] MAP SS7 - ''Mobile Application Part SS7'' ili 'Mobilni aplikacijski segment SS7''

1.1.2 Prednosti

Ključne stavke zbog kojih je USSD opće prihvaćen su:

- Komunikacija sa krajnjim korisnikom kroz sesiju
- Sigurnost u prijenosu informacija između svih komponenata u lancu
- USSD interakcija se ne pohranjuje na mobilnom uređaju
- U većini zemalja USSD usluge su besplatne za krajnjeg korisnika
- Interakcija u realnom vremenu
- Do tri puta brži u usporedbi sa SMS-om, informacije dolaze do mobilnog uređaja kroz dvije sekunde od pozivanja usluge.

1.1.3 Nedostatci

- USSD sesije koriste više telekomunikacijskih resursa u usporedbi sa SMS porukama iz razloga što operater nakon zaprimanja USSD poziva mora sesiju održavati aktivnom sve dok ne zaprimi odgovor od krajnjeg korisnika. U slučaju da korisnik ne odgovori kroz 30 sekundi operater vraća poruku greške čime se sesija zatvara.
- Ovisno o operateru USSD sesije mogu biti vremenski ograničene gdje je trajanje sesije u većini slučajeva ograničeno na 120 sekundi. Vremenske jedinice se mogu razlikovati ovisno o mrežnom operateru i internim postavkama.
- Mreža mora imati dovoljno resursa za provedbu svih USSD sesija, u protivnom dolazi do zagušenja mreže i otežanog pristupanja USSD uslugama.

1.1.4 Primjena

USSD usluge svjesno i nesvjesno koristi većina današnje populacije gdje je općepoznat primjer nadoplate sredstava na mobilni račun, takozvani „bonovi“.

Zvanjem *123***UnikatniBrojBona**# pozivate USSD uslugu za nadoplatu bonova na matičnoj mreži gdje kao povratnu poruku zaprimate informaciju o uspješnosti nadoplate bona.

Napredniji primjeri korištenja USSD usluga mogu se pronaći u marketinškom i bankarskom sektoru, gdje marketing agencije provode upitnike za prikupljanje podataka dok banke nude e-banking usluge pomoću kojih možete transparentno raspolagati sredstvima na računu te provoditi plaćanja, nadoplatu bonova, pregled stanja računa neovisno o Vašoj trenutnoj lokaciji te mougućnosti pristupa internetu.

1.2 Opis problema

U suvremenom svijetu mogućnost za jednostavan i brz prijenos informacija pravo je svakog čovjeka. Redovitim održavanjem svih zavisnih komponenata, unapređivanjem i dodavanjem resursa te implementacijom novih USSD tehnologija mrežni operateri osiguravaju neprestani pristup te implementaciju novih servisa pružajući krajnjim korisnicima širok spekatar usluga neovisno o trenutnoj lokaciji ili dostupnosti interneta.

Ovim radom osvrnuti ćemo se na tehnologije pomoći kojih je omogućena komunikacija između korisnika, komponenata u lancu i aplikacijskog servera sve u svrhu jednostavnog prijenosa i obrade podataka.

1.3 Cilj i svrha

Predočiti trenutno stanje USSD protokola, načine korištenja te eventualne probleme na koje bi mrežni operateri trebali obratiti pozornost u svrhu poboljšanja usluge.

1.4 Polazna hipoteza

USSD je protokol s neiskorištenim potencijalom kojim se vrši interakcija s mobilnim uređajima, neovisno o njihovim tipovima operacijskih sustava. Da bi se široki spektar korisnika upoznao sa mogućnostima ove usluge, potrebno je administracijsko sučelje kojim se može jednostavno kreirati aplikacije, neovisno o vrsti klijenata.

1.5 Metode istraživanja

U ovom završnom radu korištene su sljedeće metode :

- Metoda opisivanja
- Grafička metoda
- Metoda analize i sinteze

1.6 Struktura završnog rada

- Definicija problema
- Detaljna razrada
- Zaključak na osnovu ostvarenih rezultata
- Primjer
- Literatura

2 Metode pozivanja usluge

2.1 Uvod

Pozivatelj aplikacije je krajnji korisnik koji pozivom na unikatni kratki broj inicira proces koji je zaslužan za generaciju sadržaja koji se USSD protokolom isporučuje na broj pozivatelja, takav tok informacija nazivamo „Pull“[5] metodom ili metodom povlačenja informacija od strane pozivatelja. Metoda povlačenja je trenutno najrasprostranjenija, najjednostavnija i najbrža metoda za pristup i interakciju sa USSD uslugama samim time što je definirana u inicijaloj fazi USSD protokola te je dostupna na svim modelima mobilnih uređaja isporučenih nakon definiranja USSD MAP1[6] protokla.

Uz navedenu i sveopće korištenu metodu povlačenja informacija postoji i „Push“[7] metoda slanja čija je zadaća da pošalje informacije sa aplikacijskog servera kroz SS7 protokol prema krajnjem korisniku usluge.

Razlika između dvije navedene metode je u procesu pozivanja istih, gdje u metodi povlačenja je krajnji pretplanik zadužen za slanje zahtjeva dok u „Push“ metodi slanja je zathjev iniciran na strani operatera ili pružatelja usluga. Problem potonje metode je u odazivu krajnjeg korisnika na sesiju iniciranu od treće strane, iz razloga što „Pull“ metodom krajnji korisnik ima u naumu doći do informacija dok se „Push“ metodom informacije šalju krajnjem korisniku neovisno o tome dali ih isti očekuje, što rezultira slabijim odazivom kranjih korisnika.

Za korištenje „Push“ metode mrežni operater mora podržavati drugu fazu USSD protokola (MAP2[8]) , što u većini slučajeva predstavlja problem kod implementacije iste u slučaju kada mrežni operater ne raspolaže infrastrukturom za pružanje usluge.

[5] Pull Metoda – Metoda povlačenja

[6] MAP1 (Mobile Application Part 1 – Mobilni aplikacijski segment broj 1)

[7] Push Metoda – Metoda prosljeđivanja, guranja

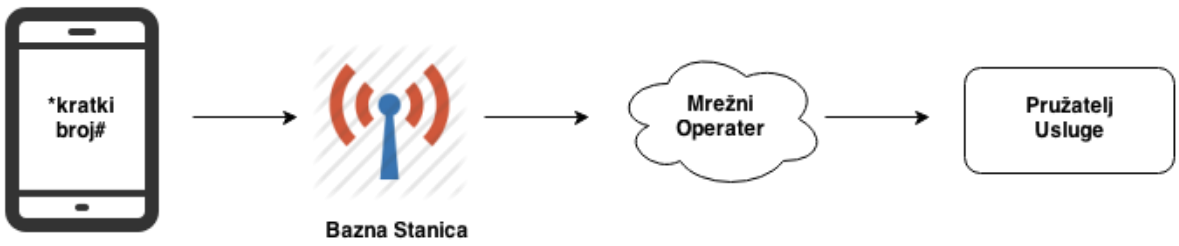
[8] MAP2 (Mobile Application Part 2 – Mobilni aplikacijski segment broj 2)

MAP2 protokol podržava 99.9% mobilnih uređaja dok je za ostatak potrebno ažurirati software[9] na uređaju.

2.2 Metoda povlačenja „Pull“

2.2.1 Interakcija pozivanjem kratkog broja „Short code“

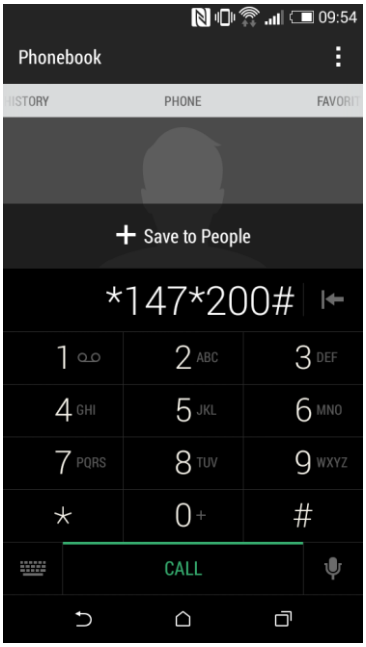
U namjeri da se krajnjem korisniku omogući pristup informacijama korištenjem USSD protokola potrebno je definirati metodu pozivanja usluge gdje krajnji korisnik ovisno o usluzi kojoj pristupa mora unijeti kratki kod koji predstavlja pozivanu uslugu u formatu ***123**#, gdje 123 može biti bilo koji kratki broj definiran od strane operatera.



Slika 3. Primjer metode povlačenja „Pull“

Nakon pozivanja istog, a ovisno o vrsti kratkog broja korisnikov mobilni račun može biti terećen za određeni iznos koji je pružatelj usluge ugovorio sa mrežnim operaterom.

[9] Software – program, aplikacija



Slika 4. Primjer pozivanja usluge korištenjem metode povlačenja „Pull“ kroz sučelje moblinog uređaja

U svrhu osiguranja transparentnosti informacija na razini države formulira se regulatorno tijelo čija je osnovna zadaća kontrolirati registraciju kratkih brojeva.
Prilikom registracije kratkog broja potrebno je podnjeti dokumentaciju kojom pružatelj usluga dokazuje da posjeduje pravo pružanja usluga kratkim brojevima gdje se za svaki kratki broj podnosi opis usluge uključujući sve akcije koje krajnji korisnik može izvršiti korištenjem kratkog broja.

Pružatelj usluga od regulatornog tijela zaprima potvrdu o registraciji kratkog broja koju prilaže mrežnim operaterima unutar države djelovanja u svrhu povezivanja na mrežu operatera s ciljem isporuke usluge krajnjim korisnicima.

Prilikom integracije svaki mrežni operater može zatražiti dodatne provjere sadržaja koji će biti dostupan na mreži kako bi svojim krajnjim korisnicima isporučili provjeren i kvalitetan USSD sadržaj.

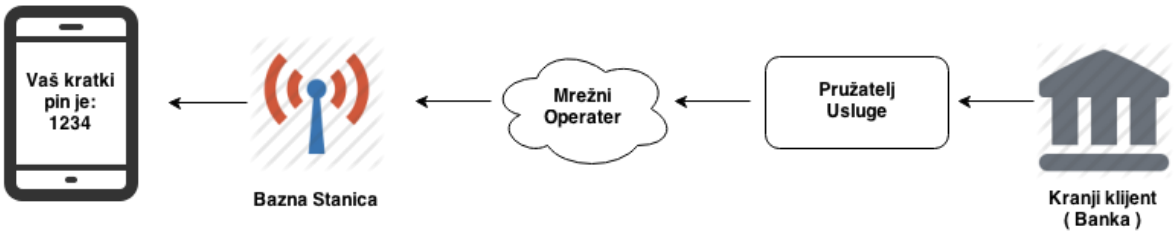
Pružatelj usluge pri svakom oglašavanju kratkog broja mora navesti tarifu naplate krajnjem korisniku gdje za primjer možemo spomenuti Južno-Afrički model od 0.20Randa[10] (11 lipa) za svakih 20 sekundi korištenja usluge, gdje je maksimalna dužina trajanja sesije limitirana na 120 sekundi u svrhu zaštite krajnjeg korisnika.

[10] Rand – novčana valuta Južnoafričke Republike

Pružatelj usluge u suradnji sa mrežnim operaterima može odrediti tarifu naplate kratkog broja gdje se pri svakom pozivu na kratki broj kranjem pozivatelju naplaćuje dogovoreni iznos. Navedeni iznos se prema dogovoru sa operaterom djeli između pružatelja usluge i mrežnog operatera. U slučaju kada pružatelj usluga želi osigurati besplatno korištenje USSD servisa za pozivatelja usluge sa mrežnim operaterom dogovara se "reverse"[11] model korištenja, gdje se svi pozivi na kratki broj naplaćuju pružatelju usluge.

2.3 Metoda slanja „Push"

Omogućuje dostavu informacija korištenjem interneta gdje je krajnji klijent zadužen za pokretanje sesije i generaciju sadržaja. Za primjer možemo uzeti pružatelja usluge i krajnjeg klijenta (banka) gdje krajnji klijent vrši dostavu jednokratnih pinova[12] koristeći „Push" metodu.



Slika 5. Primjer metode slanja „Push"

Promet generiran „Push" metodom nije reguliran od strane regulatornog tijela unutar države već istog kontroliraju mrežni operateri uz strogo propisana pravila o sadržaju kojeg je dozvoljeno dostavljati na mobilni uređaj pretplaćenog korisnika. Pravila definirana od strane mrežnog operatera prihvaćena su od pružatelja usluga prilikom potpisivanja ugovora o pružanju USSD usluga.

Ovisno o mrežnom operateru vrsta sadržaja se kategorizira kao:

- Transakcijski sadržaj

[11] Reverse model korištenja – Obrnut model korištenja

[12] Pin – kratki broj, zaporka

- Marketing sadržaj

Generiranje prometa za oba dozvoljena je samo ukoliko se krajnji korisnik pretplatio na primanje USSD sesija. Akcija aktiviranja pretplate za neku od usluga nosi naziv „opt-in“[13] te se odrađuje direktno preko USSD menu-a (pozivom na kratki broj) ili slanjem SMS poruke na dedicirani kratki broj. Ukoliko krajnji korisnik zaprimi USSD sesiju bez da se samovoljno prijavio može se objaviti regulatornoj agenciji ili mrežnom operateru čija je zadaća istražiti slučaj te blokirati sve daljnje USSD sesije prema prijavljenom broju.

Sesije generirane „Push“ metodom naplaćuju se isključivo pružatelju usluge od strane mrežnog operatera iz razloga što kranji korisnik ne može utjecati na broj generiranih USSD sesija prema vlastitom pretplatničkom broju.

2.3.1 Protokoli za interakciju

Pružatelj usluge dužan je krajnjem klijentu osigurati pristup servisima za pokretanje sesija „Push“ metodom gdje krajnji klijent ovisno o poslovnoj logici pretplaćenim korisnicima šalje dinamično generirani sadržaj.

Ovisno o infrastrukturi pružatelja usluge, najčešće korišteni protokoli za interakciju sa aplikacijom kreiranom od strane klijenta su:

- HTTP
- SOAP
- SMPP

Krajnji klijent od pružatelja usluge pri aktivaciji korisničkog računa zaprima instrukcije o slanju „Push“ USSD sesija kao i naputke o sadržaju kojeg je dozvoljeno slati na brojeve pretplatnika.

[13] Opt-in – lista kontakata koju klijent (npr. Banka) ima ažuriranu kod sebe, te sadrži popis svih krajnjih korisnika koji su pretplaćeni za primanje obavijesti. Sadrži i detalje o načinu na koji su kontakti prikupljeni. Postoji i „Opt – out“ lista, te sadrži popis svih adresata koji su izrazili potrebu za prekidanjem primanja obavijesti. Obavijesti prema takvim korisnicima nisu dozvoljene.

2.3.1.1 HTTP

HTTP ili punim imenom „HyperText Transfer Protocol“ je generalno korištena metoda ili aplikacijski protokol za prijenos i prikazivanje informacija na internetu.
U komunikaciji sudjeluju klijent i server gdje u većini slučajeva je klijent zaslužan za iniciranje komunikacije, gdje za primjer klijenta možemo uzeti web preglednik te za server neku od poznatih web stranica.

HTTP je protokol zasnivan na principu zahtjeva i odgovora, gdje nakon što je odgovor zaprimljen klijent prekida komunikaciju sa serverom. Klijent automatski uspostavlja komunikaciju sa serverom na portu 80, ukoliko nije drugačije specificirano.

Također postoji i sigurnija verzija protokola „HTTPS“ ili punim nazivom „„HyperText Transfer Protocol Secure“ koji na portu 443 omogućava kriptiranu komunikaciju između klijenta i servera tako da se u adresu web preglednika unese „https://domena.ext“ umjesto „http://domena.ext“.
Kako bi domena mogla koristiti kriptiranje podatka , certifikat mora biti zakupljen od ovlaštenog certifikatora. Samo domene koje imaju zakupljen ovlašteni certifikat se smatraju sigurnim za prijenos osjetljivih informacija.

HTTPS kao i njegov manje napredniji pratioc HTTP podržavaju četri metode poziva :

- GET
- POST
- PUT
- DELETE

GET[14] metoda je generalno korištena u svim web preglednicima i služi za povlačenje informacija sa servera te prikaz istih unutar web preglednika. Postoje slučajevi kada se GET metodom mogu u sklopu web adrese poslati dodatni parametri koji

[14] GET – prikupljanje, povlačenje

omogućavaju serveru generiranje dinamičkog sadržaja. Veoma je važno ne koristiti GET metodu kada se šalju informacije od velikog značaja kao korisničko ime ili zaporka iz razloga što su isti vidljivi te ostaju kasnije pohranjeni u memoriji web preglednika.
Primjer kako ne koristiti GET metodu je :
http://primjer.com/?korisnik=ivan&zaporka=percic.

POST[15] metoda služi za slanje informacija prema serveru gdje isti obrađuje podatke te generira dinamički sadržaj ovisno o zaprimljenim informacijama.
U usporedbi sa GET metodom, zahtjevi slani POST metodom se nikad ne pohranjuju u memoriji web preglednika te nemaju limit na veličinu informacija koja se šalje (ovisno o serveru koji zaprima zahtjev).

PUT[16] metoda se koristi u slučajevima kada na serveru već postoji sadržaj koji treba biti ažuriran, tada web klijent šalje novi ažurirani sadržaj PUT metodom. U slučaju da sadržaj nije prethodno definiran na serveru postoji mogućnost kreacije novog sadržaja.

DELETE[17] metoda je korištena u slučajevima kada je potrebno izbrisati sadržaj na poslužitelju. Kao i kod POST I PUT metoda unutar URL-a se specificira identifikator sadržaja koji služi za raspoznavanje sadržaja u bazi.

[15] POST – objaviti

[16] PUT - postaviti

[17] DELETE - izbrisati

2.3.1.2 SOAP

„Simple object access protocol“ je baziran na HTTP protokolu te kao sredstvo razmjene informacija koristi XML „Extensible markup language“[18].
Jedna od najvećih karakteristika SOAP protokola je da je neovisan o programskom jeziku i lako proširljiv čineći integraciju jednostavnom.

Zbog navedenih prednosti SOAP se koristi u integracijama između klijenata i pružatelja usluge gdje je jedini uvjet kojeg obje strane moraju zadovoljiti upotreba HTTP protokola kao podloge za prijenos informacija.
Pružatelj usluge je dužan dostaviti klijentu SOAP specifikaciju prema kojoj klijent sastavlja zahtjev koji se šalje prema pružatelju usluge, isti je dužan poslati odgovor unaprijed definiran u SOAP specifikaciji.

2.3.1.3 SMPP

SMPP ili „Short Message Peer-to-Peer“[19] je standadizirani protokol korišten u telekomunikacijskoj industriji koji služi za prijenos kratkih poruka između pozivatelja usluge i centra za razmjenu kratkih poruka.

Protokol je baziran na TCP[20] podlozi gdje krajnji korisnik koristeći korisničko ime, zaporku, ip adresu servera i port šalje zahtjev za prijavu na SMPP server.
Uspješnom prijavom ostvaruje se sesija između klijenta i servera koja se održava slanjem kratkih poruka tzv. „PDU“[21] paketa.

Postoje različiti PDU paketi ovisno o akcijama koje klijent želi izvršiti prema serveru, neki od najčešće korištenih PDU paketa su :

[18] Extensible markup language – Jednostavan jezik za označavanje

[19] Short Message Peer-to-Peer – „Kratka poruka točka-na-točku“

[20] TCP - Transmission Control Protocol – „Transmisijski protokol za kontrolu“

[21] PDU – „Protocol Data Units“ ili „Jedinice podatkovnog protokola“

Ime paketa	Objašnjenje
Bind	Koristi se za inicijalno uspostavljanje sesije sa serverom. U ovom paketu klijent šalje korisničko ime i zaporku. Postoje tri vrste bind paketa : Transmitter (samo slanje paketa), Transciever (primanje i slanje paketa), Receiver (primanje paketa) gdje je za USSD obavezno korištenje Transciever načina ili kombinacija Transmitter i Receiver moda pri spajanju kako bi se omogućilo slanje menu-a krajnjem korisniku i zaprimanje odgovora.
Bind_resp	Server odgovara bind_resp paketom koji sadrži informaciju dali se klijent uspješno prijavio na sustav.
Submit_sm	Paket kojeg klijent koristi kako bi serveru poslao novu poruku. Unutar polja *destination_addr* klijent specificira primatelja poruke dok u polju *msg* specificira USSD poruku koju želi dostaviti primatelju.
Submit_sm_resp	Server odgovara submit_sm_resp paketom koji sadrži informaciju o zaprimanju submit_sm paketa.
Deliver_sm	Paket koji server šalje klijentu. Isti sadrži odgovor kojeg je krajnji korisnik unjeo na mobilnom uređaju.
Deliver_sm_resp	Paket koji klijent šalje serveru kao potvrdu zaprimljenog deliver_sm paketa. Nakon zaprimanja paketa server očekuje novi submit_sm paket kako bi kranjem korisniku na mobilni uređaj dostavio novi USSD menu.
Unbind_sm	Paket može biti poslan od strane servera prema klijentu ili obrnuto te označava zahtjev za prekid tekuće SMPP sesije.
Unbind_sm_resp	Strana koja je zaprimila Unbind_sm odgovara unbind_sm_resp paketom kao potvrdom za prekidom komunikacije.

Primjer USSD „Push“ sesija kroz SMPP komunikaciju :

Komunikacija	Objašnjenje
(bindreq: (pdu: 0 9 0 [65725854]) USERNAME PASSWORD USSD 52)	Klijent šalje zahtjev za spajanjem na SMPP server
(bindresp: (pdu: 17 80000009 0 65725855))	SMPP server odgovara dajući klijentu do znanja da je uspješno prijavljen na SMPP server.
(submit: (pdu: 244 4 0 65729145) (addr: 1 1 38599123456789) (addr: 1 1 38599123456789) (sm: msg: Moja Banka 1.Stanje računa 2.Plaćanja 3.Krediti 4.Pomoć 9.Izlaz))	Klijent šalje USSD „Push“ sesiju prema mobilnom broju 38599123456789.
(submit_resp: (pdu: 44 80000004 0 65729145) 123458121891312), No Error	Server odgovara klijentu paketom koji potvrđuje da je sesiju zaprimio, te generira unikatni id „123458121891312" koji služi za evidenciju sesije.
(deliver: (pdu: 119 5 0 70160488) (addr: 1 1 38599123456789) (addr: 1 1 38599123456789) (sm: msg: 0))	Korisnik koji je zaprimio sesiju na broj 38599123456789 odgovara brojem 1. Isti odgovor je se proslijeđuje klijentu , čija je zadaća potvrditi primku odgovora te poslati novi USSD menu.
(deliver_resp: (pdu: 17 80000005 0 70160488))	Klijent potvrđuje primku odgovora generiranog od strane korisnika mobilnog uređaja
(submit: (pdu: 244 4 0 65729145) (addr: 1 1 38599123456789) (addr: 1 1 38599123456789) (sm: msg: Račun : 123456789	Klijent zadnjim paketom salje informaciju o stanju računa korisnika.

Stanje: 399,49 HRK))	
(submit_resp: (pdu: 44 80000004 0 65729145) 123458121891312), No Error	SMPP server potvrđuje primku USSD menu-a i istog prosljeđuje korisniku mobilnog uređaja

Prednost SMPP protokola u usporedbi sa protokolima baziranim na HTTP-u je u činjenici što je SMPP standardiziran SMS protokol te kako je baziran na principu aktivne sesije omogućava brži prijenos podatka između dvije strane.

Broj sesija koje klijent može ostvariti definira se na SMPP serveru a služe postizanju bržeg prijenosa podataka.

2.3.2 Interakcija zvanjem telefonskog broja

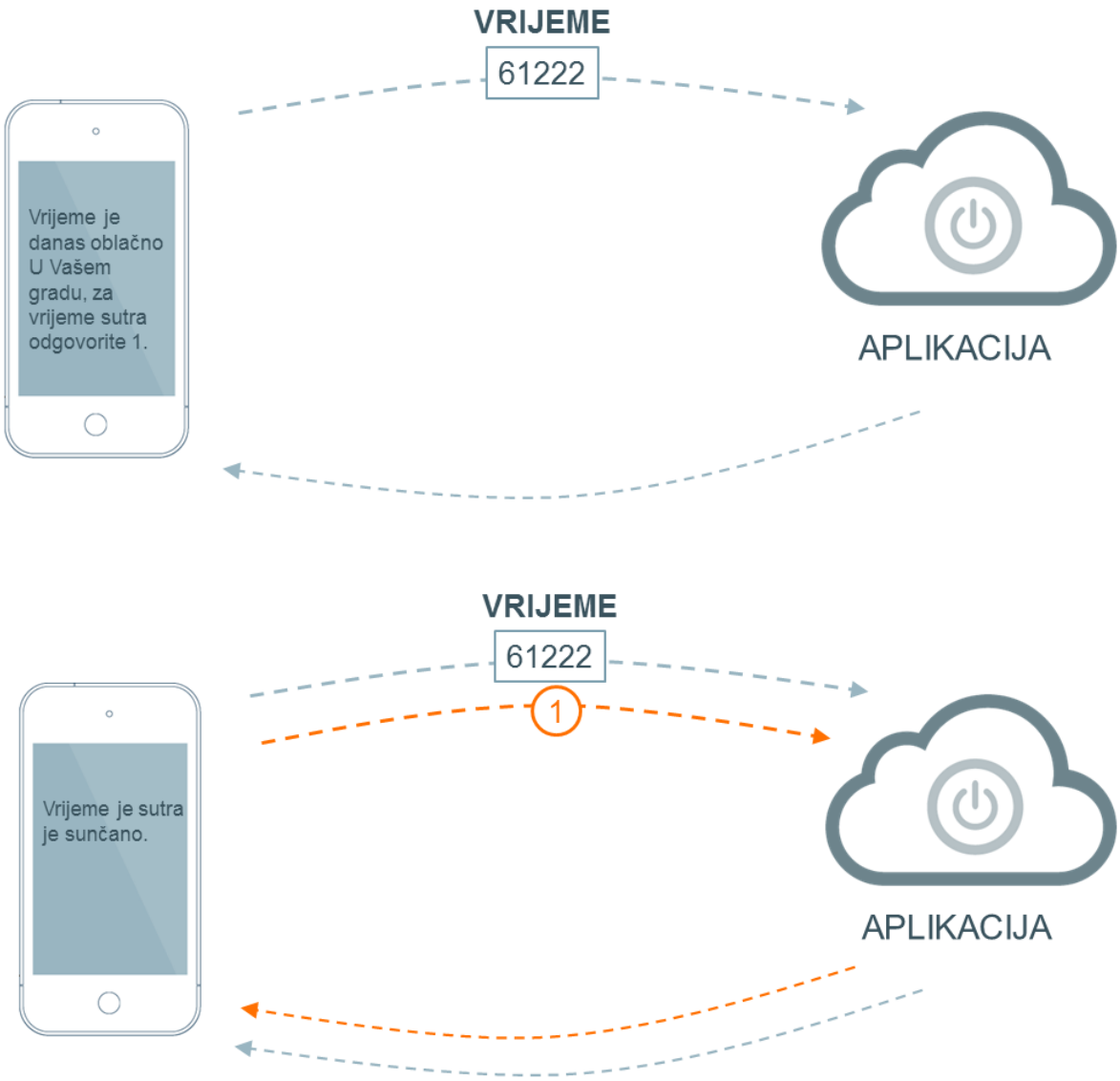
U situacijama kada kratki broj nije dostupan za registraciju kao alternativa za pozivanje usluge može se upotrijebiti fiksni telefonski broj u formatu 01/123456789. Prednost ove metode nad registracijom kratkih kodova leži u činjenici da je fiksni telefonski broj javno dostupan neovisno o mrežnom operateru koji se koristi za pozivanje usluge.
Krajnji korisnik pozivom na fiksni telefonski broj zaprima ton koji označava zauzeće telefonske linije. S prekidom komunikacije krajnji korisnik na mobilni uređaj zaprima USSD sesiju.

Ovaj način interakcije besplatan je za krajnjeg korisnika iz razloga što se pozivi prema fiksnom telefonskom broju koji odgovara zauzećem linije ne naplaćuju od strane mrežnih operatera, samim time pružatelj usluge snosi sve proizašle troškove.
Nedostatak navedene interakcije je što zahtjeva podršku „Phase 2“[22] USSD tehnologije što u slabije razvijenim zemljama predstavlja nezaobilazni problem u implementaciji.

2.3.3 Interakcija slanjem SMS (kratke) poruke

Slanjem SMS poruke na kratki broj pokreće se proces baziran na sadržaju zaprimljene poruke koji je zaslužan za dinamično generirane USSD sesije.
Za primjer se može uzeti slanje poruke sadržaja „VRIJEME“ na kratki broj 61222 gdje krajnji korisnik 10-tak sekundi nakon slanja SMS poruke zaprima USSD sesiju sa informacijama o trenutnim vremenskim prilikama i opcijama za daljnju navigaciju.

[22] Phase 2 – „Faza 2“



Slika 6. Primjer interakcije slanjem SMS (kratke) poruke specificiranjem sadržaja

Ovakav način interakcije prvenstveno pruža mogućost implementacije različitih servisa ovisno o sadržaju SMS poruke. Implementacija dodatnih servisa je jednostavan proces za pružatelja usluge samim time što se sastoji od jednog koraka : registracije nove riječi koja predstavlja novu uslugu za kranjeg pretplatnika.

Ova vrsta interakcije kao i „interakcija zvanjem telefonskog broja“ dijele isti problem, gdje mrežni operateri unutar države moraju podržavati „Phase 2“ USSD kako bi korištenje usluge bilo moguće.

3 Prijenos, sigurnost i obrada podatka

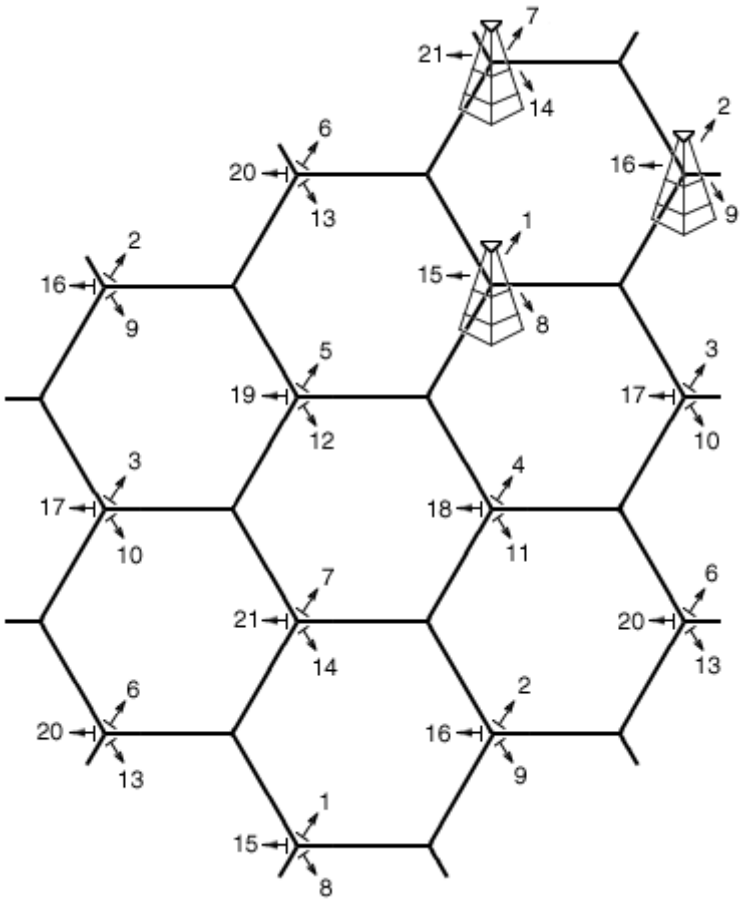
Prilikom prijenosa podataka između krajnjeg pozivatelja, pružatelja usluge te mrežnog operatera koriste se sljedeći protokoli / segmenti:

- Radijska mreža
- SS7 protokol
- IP/VPN Protokol

Ovo poglavlje opisuje osnove protokola korištenih u USSD procesu, te sam protok informacija od pozivatelja usluge do aplikacijskog servera zaduženog za kreiranje sadržaja.

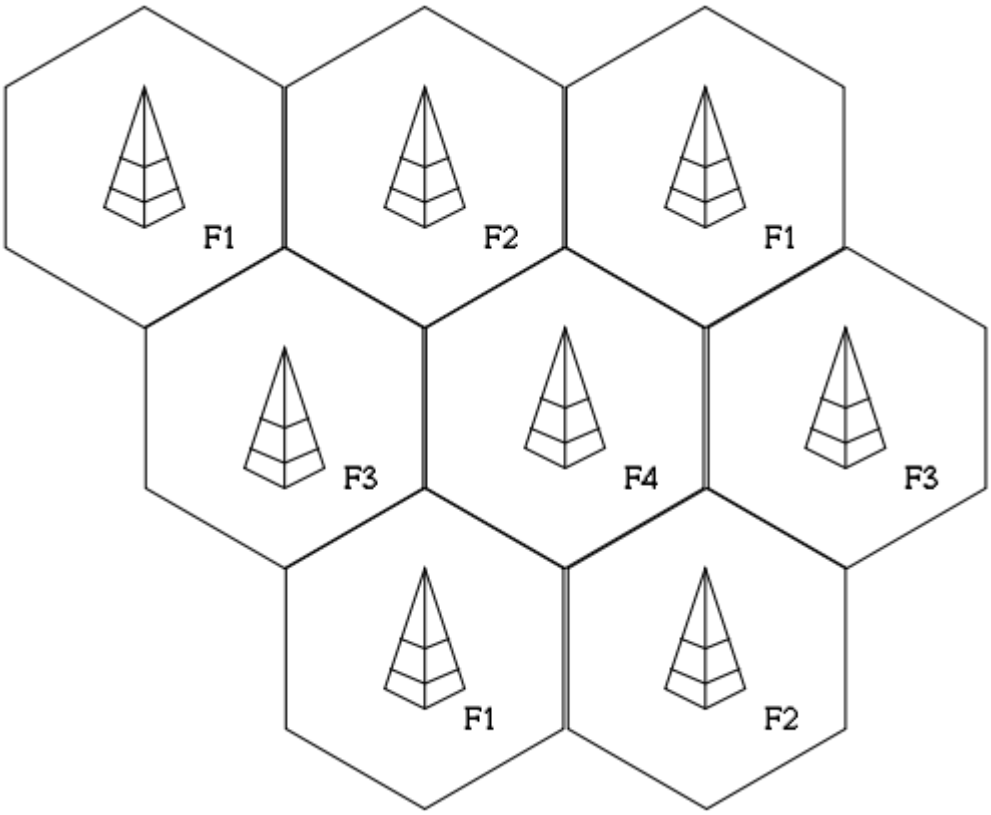
3.1 Radijska mreža

Ili mobilna mreža je bežična mreža na koju su prijavljeni mobilni uređaji u svrhu ostvarivanja komunikacije. Kako bi se komunikacija ostvarila mobilni uređaji moraju biti prijavljeni na geografski respoređene bazne stanice koje formiraju ćelije te odašilju signal kako bi omogućile pokrivenost uslugom. Ćelije se formiraju u formatu heksagona te sadrže različit broj baznih stanica koji je utvrđen na osnovu broja korisnika koji trebaju pristupiti mreži.



Slika 7. Raspored baznih stanica u formatu heksagona

Svaka od ćelija mora imati svoju zasebnu frekvenciju rada (1 do 6) kako bi korisnici mogli ostvariti nesmetanu komunikaciju. Takva frekvencija se ne smije ispreplitati sa frekvencijom susjedne ćelije ali se može ponovno koristiti u bilo kojoj drugoj ćeliji koja nije u direktnom dodiru sa prvotnom.



Slika 8. Raspodjela frekvencija po ćelijama

Kako bi se omogućila internacionalna komunikacija između uređaja na mreži, bazne stanice komuniciraju sa centralnom baznom stanicom koja prosljeđuje podatke na MSC[23] „Mobile Switching center“ zadužen za obradu podataka. MSC je zadužen za proslijeđivanje informacija prema traženim servisima (USSD, registar prijavljenih korisnika) ili drugim MSC-ovima , također direktno komunicira sa javnom telefonskom skretnicom koja sadrži infrastrukturu i logiku za spajanje mobilnih i fiksnih komunikacijskih kanala na globalnoj razini.

Bazne stanice su u većini slučajeva locirane na uzvisinama (zgrade, brda) uz gusto naseljena područja gdje su mrežne usluge najviše korištene.
U područjima slabog signala postoji mogućnost izgradnje nove bazne stanice ili uporabe antene sa reproduktorom signala koji koristeći dalekometnu antenu zaprima i reproducira signal te samim time osigurava kvalitetnu mrežnu pokrivenost.
U slučajevima kada je krajnji korisnik u pokretu postoji mogućost da prijeđe iz jedne ćelije u drugu pri čemu se mobilni uređaj prijavljuje na baznu stanicu sa najjačim

[23] MSC – Mobile switching center – „Mobilni centar za preusmjeravanje“

signalom, čime mjenja kanal komunikacije. Neovisno o tome dali je u toku poziv krajnji korisnik neće primjetiti tranziciju na novu baznu stanicu.

Nakon što krajnji korisnik pozove USSD uslugu, bazna stanica zaprima signal te ga proslijeđuje na centralnu baznu stanicu koja isti kroz „**A**ccess“[24] kanal proslijeđuje na MSC.
„**A**ccess“ kanal služi za prijenos SS7 informacija između centralne bazne stanice i MSC-a.
MSC na osnovu zaprimljenih podataka (broj pozivatelja, kratki broj) poziva USSD Gateway te očekuje povratnu informaciju.
USSD Gateway prema kratkom broju određuje USSD aplikaciju te od iste očekuje sadržaj. Isti se potom proslijeđuje na MSC i centralnu baznu stanicu, da bi potom bio dostavljen krajnjem korisniku od bazne stanice na koju je trenutno prijavljen.

3.2 SS7 protokol

„Signalling System #7“ ili „Signalizacijski sistem #7“ je standardizirani skup protokola korištenih u telekomunikacijskoj industriji radi alokacije i delokacije resursa za povezivanje i raspuštanje telefonskih razgovora, provjeru brojeva, naplatu, SMS, provjera lokacije korisnika i USSD.

Signalizacija je pojam koji opisuje prijenos kontrolnih informacija za uspostavljanje poziva ili komunikacije kroz dedicirani 56/64kbps signalni kanal (out-of-band signalling[25]). Samim prijenosom informacija kroz dedicirani kanal podiže se nivo sigurnosti u odnosu kada se isti kanal koristi za prijenos signalnih informacija i telefonskog poziva (in-band signalling[26]).

SS7 protokol se koristi za :

- Spajanje i raspuštanje poziva

[24] Access kanal – „Pristupni kanal“

[25] Out-of-band signalling – komunikacija izvan definirane telekomunikacijske frekvencijske grupe

[26] In-band signalling – komunikacija unutar definirane telekomunikacijske frekvencijske grupe

- Naplatu
- Proslijeđivanje poziva
- SMS
- USSD
- HLR
- Provjeru portabilnosti[27] brojeva
- Dostavu multimedijalnog sadržaja (melodija, slika, igara)
- Alokacija besplatnih brojeva (primjer : 08009000)

SS7 se sastoji od skupa rezerviranih ili dediciranih signalnih kanala i kanala za interkonekciju (signalling point). Postoje tri vriste kanala za interkonekciju :

- Service switching point (SSP)
- Signal transfer point (STP)
- Service control point (SCP)

3.2.1 Service switching point (SSP)

Su punktovi koji se koriste u telekomunikacijskim sistemima te su direktno spojeni na druge punktove putem „**A**ccess“ signalnih kanala. SSP koristeći svoju internu routing tablicu razmjenjuje podatke sa drugim SSP punktovima na osnovi globalne adrese (GT – „Global title“) ili u odsutnosti iste proslijeđuje zahtjev za informacijom prema Service control point (SCP).

Globalna adresa ili „Global title“ je unikatna adresa pošiljaoca prema kojoj se razaznaje promet na mreži. Svaki mobilni operater ima set globalnih adresa sa kojih šalje promet prema globalnim adresama drugih operatera. Operater koji zaprima promet prema svojoj globalnoj adresi može prema adresi sa koje pristiže promet razaznati o kojem se operateru radi. Veoma je važno napomenuti da mobilni

[27] Portabilnost brojeva – sposobnost da se mobilni broj prenese s jedne mreže na drugu, što znači da će prefiks ostati od prve mreže, ali će se sav komercijalni dio odvijati na drugoj mreži (u slučaju da je broj prenesen s mreže 1 na mrežu 2)

operateri diljem svijeta imaju ugovore o poslovanju i slanju prometa na ugovorene mreže gdje u slučaju da operater šalje poruke prema operateru s kojim nema ugovorene usluge isti može blokirati sav promet ovisno o globalnoj adresi s kojeg isti pristiže. Kako bi se osigurala redundancija i dodatni resursi postoji mogućost korištenja „**E**xtended“[28] kanala čija je osnovna zadaća preuzeti sav ili dio prometa kada su prvotni „**A**ccess“ kanali nedostupni ili u slučaju velike količine prometa.

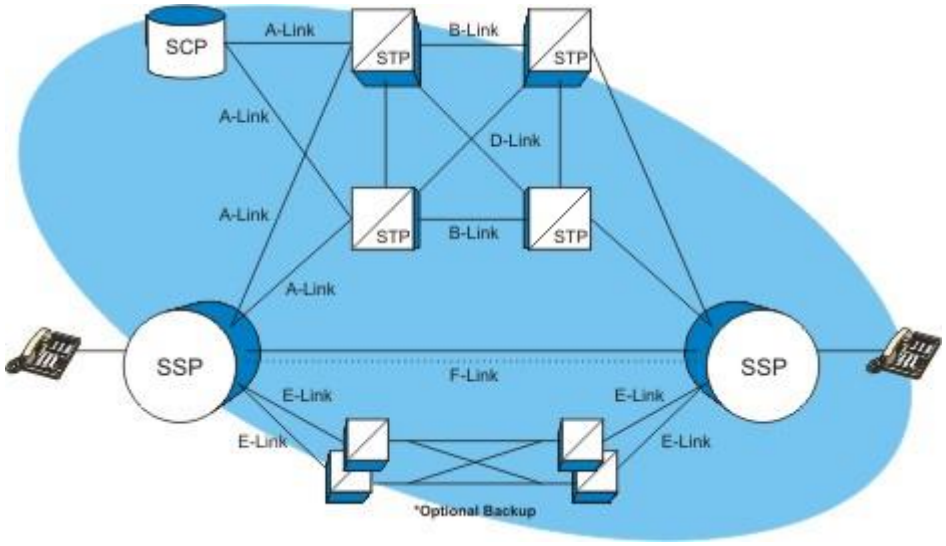
3.2.2 Signal transfer point (STP)

Služi za usmjeravanje informacija prema SSP punktovima ili drugim STP routerima putim SS7 signalnih kanala ovisno o globalnoj adresi, telefonskom broju primaoca ili prema sadržaju poruke ukoliko je riječ o SMS ili USSD porukama. Kako bi se osigurala redundancija postoji mogućost postavljanja više STP punktova te se isti poparuju „**C**ross“ kanalima. Također postoji mogućost da se dva ili više različitih mobilnih operatera direktno povežu koristeći „**B**ridge“ ili „**D**iagonal“ kanale.

3.2.3 Service control point (SCP)

Je komponenta zaslužna za pružanje informacija SSP punktovima. Prema zaprimljenim informacijama SSP punktovi znaju gdje usmjeriti pakete kako bi se uspostavio poziv , dostavila SMS poruka ili USSD menu. STP i SCP su u većini slučajeva redundantni kako bi usluga bila dostupna neovisno o potencijalnim ispadima na mreži.

[28] Extended kanali – rezervni kanali koji preuzimaju promet u slučaju da primarni nisu dostupni



Slika 9. SS7 interkonekcija između dva mobilna operatera

3.3 IP/VPN protokol

Korisnici usluge (marketinške tvrtke, banke) koje se odluče na povezivanje putem VPN[29] tehnologije razmjenjuju dvije javno dostupne internet adrese koje služe kao točke povezivanja. Prijenos podataka koristeći VPN tehnologiju zasnivan je na pojmu tuneliranja prometa. Tuneliranje predstavlja inicijalizaciju i održavanje mrežne konekcije između dvije stranke.

Kako bi se zagarantirala sigurnost prijenosa podataka stranke koriste enkripcijske ključeve koji služe za enkripciju i dekripciju poslanih odnosno zaprimljenih paketa. Paketi sadrže informacije primatelja te enkriptirani sadržaj koji je nemoguće dekriptirati.

[29] VPN ili „Virtual private network“ je tehnologija koja omogućuje sigurno povezivanje između računala koristeći privatnu ili javnu mrežnu infrastrukturu. Kao medij za prijenos informacija najčešće se koristi internet dok je sekundarna i nadasve skuplja opcija privatna internet linija

VPN također koriste zaposlenici tvrtki kako bi pristupili privatnim resursima u vrijeme kada se ne nalaze na radnom mjestu. Za prijavu koriste javnu VPN adresu te korisnicko ime i zaporku. Nakon uspješne prijave zaposlenici mogu koristiti resurse koji su im dostupni dok su na radnom mjestu, time se uvelike rješava problem zaposlenika koji često putuju ili imaju potrebu raditi izvan ureda.

Karakteristike svakog VPN-a su:

- Autentikacija korisnika – provjera i dozvoljen pristup samo ovlaštenim korisnicima.
- Evidencija – evidencija događaja korisnika koji mogu imati direktni utjecaj na resurse unutar VPN konfiguracije
- Adresiranje – alokacija / delokacija privatnih adresa za korisnike koji su se uspješno prijavili
- Šifriranje – podataka kako bi se isti zaštitili od pristupa neovlaštenih korisnika
- Upravljanje ključevima – mehanizmi za generaciju i osvježavanje ključeva nužnih za enkripciju prometa između klijenta i poslužitelja.
- Podrška za različite protokole

3.3.1 Prednosti

Neke od prednosti korištenja VPN tehnologije su :

- Visoka razina sigurnosti
- Standardiziran i opće korišten protokol
- Mogućnost jednostavne implementacije neovisno o geografskoj lokaciji dviju stranaka

3.3.2 Nedostatci

Neovisno o popularnosti VPN tehnologije postoje nedostaci :

- Konfiguraciju VPN-a moraju obavljati izučeni specijalisti pritom pazeći na svaki detalj pri konfiguraciji gdje svaka pogreška može značiti gubitak povjerljivih informacija s obzirom da se kao medij prijenosa koristi javni internet.
- Performanse VPN-a nisu konstantne s obzirom da ovise o mrežnom pružatelju usluga i trenutnim kapacitetima mreže. Privatna internet linija u ovom slučaju ima zagarantirane performanse i direktnu kontrolu od strane mrežnog administratora.
- Pri konfiguraciji VPN-a stranke mogu koristiti različite modele uređaja što nekad dovodi do nekompatibilnosti te samim time oduženoj konfiguraciji.

3.3.3 Vrste VPN rješenja

Kako bi bili u mogućnosti zadovoljiti sigurnosne standarde specifičnih korisnika (npr, Banke, vladine organizacije) moramo podržavati različite VPN izvedbe.

VPN rješenja dijelimo na :

- Rješenja bazirana na vatrozidima koriste već implementirane mehanizme kako bi osigurali internu mrežu od neželjenog pristupa. Vatrozid se postavlja na točku putem koje se s interneta pristupa na internu mrežu te samim time ima mogućost kontrole dolaznog prometa te upravljanje istim.
- Sklopovski orjentirana VPN rješenja nisu zavisna o operativnom sustavu već koriste tehnologiju tuneliranja čime postižu najveću propusnost kod obrade podataka.
- Programski orjentirana rješenja su najoptimalnija za korištenje iz razloga što omogućavaju selektivno tuneliranje prometa temeljeno na mrežnim adresama i protokolima.

3.3.4 Tuneliranje

VPN tehnologija bazirana je na ideji tuneliranja prometa gdje se pod tuneliranje prometa podrazumijeva ostvarivanje i održavanje mrežne veze kroz koju se razmjenjuju enkriptirani paketi. Paketi se razmjenjuju na temelju informacija koje su pohranjene u zaglavlju svakog paketa te specificiraju pošiljatelja odnosno primaoca paketa.

Mnoštvo mrežnih protokola je definirano s namjerom da se koriste za VPN tuneliranje. Tri najpoznatija i općeprihvačena protokola su :

- IPSec
- PPTP (Point-to-Point Tunelling protocol)
- L2F (Layer 2 Forwarding)
- L2TP (Layer 2 Tunelling protocol)

3.3.4.1IPSec

IPSec[30] je standard definiran 1995 godine od strane IETF-a (Internet Enginnering task force) čiji glavni cilj je siguran prijenos informacija što je omogućeno implementacijom raznih sigurnosnih tehnologija gdje IPSec implementira šifriranja i provjeru korisnika na mrežnom sloju.
Implementacija IPSec-a zavisi na razmjeni ključeva između stranaka koje povezuju mrežne resurse kod realizacije USSD ili sličnih usluga.

Kroz rad IPSec koristi sljedeće protokole i standarde:

- Diffie-Hellman[31] metodu za razmjenu ključeva
- DES[32] ili 3DES standard za šifriranje podataka
- HMAC[33]
- Digitalna uvjerenja izdana od strane odgovarajućeg autoriteta

Kod prijenosa podataka IPSec protokol je zaslužan za definiranje zaglavlja paketa koji sadrži podatke za autentikaciju pomoću kojih primaoc podataka može provjeriti da li je paket pristigao od provjerenog pošiljatelja.

IPSec protokol podržava dva načina rada :

- Prijenos podataka
- IPSec tuneliranje podataka

[30] IPSec – Internet Protocol Security – „Protokol za sigurnost na internetu“

[31] Diffie-Hellman metoda za razmjenu ključeva – glavni ključ koji se koristi za generiranje regularnih ključeva se ne prenosi istim medijem kao i ostali podaci za spajanje

[32] DES – Data encription standard – „Enkripcijski podatkovni standard“

[33] HMAC – „Hash-based message authentication code“ – „kombinirano orijentirana autentifikacija koda“

Kod prijenosa podataka šifriraju se samo aplikacijska zaglavlja dok su IP zaglavlja dostupna za pregled routerima na mreži koji su zaslužni za usmjerivanje prometa što predstavlja potencijalni rizik gdje napadač može pratiti izvor i destinaciju paketa.

IPSec tuneliranje je poseban način tuneliranja prometa koji implementira dodatnu zaštitu na način da obje strane (klijent i poslužitelj) konfiguriraju IPSec mod kod tuneliranja prometa. Kod prijenosa prometa koriste se dogovoreni mehanizmi za enkapsulaciju i šifriranje gdje se za razliku od metode prijenosa podataka enkriptiraju kompletni IP paketi što omogućava siguran prijenos neovisno da li se koristi javna ili privatna mreža.

3.3.4.2 PPTP (Point-to-Point Tunelling protocol)

Za razvijanje PPTP protokola zaslužna je nekolicina proizvođača kao US Robotics, Ascend Communications, 3Com, ECI Telematics i Microsoft gdje je trenutno općekorištena Microsofto-va inačica protokola.

Protokol se bazira na PPP protokolu (Point-to-point protokolu) odnosno na TCP/IP[34] protokolima. Omogućava autentifikaciju te tuneliranje prometa gdje se poslani paketi enkapsuliraju prilikom slanja te dekapsuliraju na strani primaoca.

PPTP protokol koristi 40-bitnu, 56-bitnu ili 128-bitnu enkripciju te nažalost postoji mogućost eksplotacije paketa iz razloga što je proces šifriranja oslabljen upotrebom korisničkih zaporki koje su podložne brute-force napadima.

Protokol kojim se nadograđivao PPTP je L2F[35] gdje ga je u konačnici u potpunosti nadogradio L2TP[36] protokol.

[34] TCP/IP – Transmission Control Protocol / Internet Protocol – „Internetski protokol za prijenos i kontrolu podataka“

[35] L2F – Layer 2 Forwarding – protokol za tuneliranje koji koristi virtualne mreže za sigurni prijeno podataka

3.3.4.3 L2F (Layer 2 Forwarding)

L2F je protokol koji je definirao Cisco te je neovisan o prijenosnom mediju a sadrže ga svi Cisco proizvodi.
Nakon što se incira veza između dvije stranke, prva provjerava prisutnost L2F protokola te odrađuje autentifikaciju.

L2F protokol je naslijedio L2TP protokol.

3.3.4.4 L2TP (Layer 2 Tunelling protocol)

L2TP protokol je definiran 1999 godine od strane Cisc-a i Microsoft-a kroz standard RFC 2661 te je temeljen na L2T i PPTP protokolu. Za implementaciju L2TP protokola potreban je L2TP pristupni koncentrator i L2TP mrežni poslužitelji gdje mrežni poslužitelj predstavlja krajnju točku PPP[37] sjednice koja se tunelira kroz sustav korištenjem pristupnog koncentratora.
L2TP protkol ne pruža mehanizme za zaštitu podatka već ovisi o enkripcijskom protokolu na razini tunela.

L2TP protokol podržava obvezno i proizvoljno definirane tunele gdje se način rada razlikuje ovisno o izabranom modelu.

Način rada obvezno definiranog tunela uključuje sljedeće korake:

- Korisnik inicira PPP konekciju prema svom internet provideru (ISP).
- ISP prihvaca konekciju te je PPP sesija uspostavljena
- Korisnik se mora autentificirati korisničkim imenom pomoću kojeg ISP u svojoj bazi podataka može odrediti servise koje korisnik ima pravo koristiti
- Pristupni koncentrator inicira L2TP tunel prema mrežnom poslužitelju

[36] Layer 2 Tunneling Protocol – Protokol za tuneliranje koji podržava virtualne privatne mreže

[37] PPP – Point to Point Protocol – Protokol za komunikaciju od točke do točke

- Ukoliko mrežni poslužitelj prihvati spajanje pristupni koncentrator enkapsulira PPP u L2TP te proslijeđuje podatke preko tunela
- Mrežni poslužitelj koristi standardnu PPP autentifikaciju da bi utvrdio identitet korisnika te mu dodjelio IP adresu.

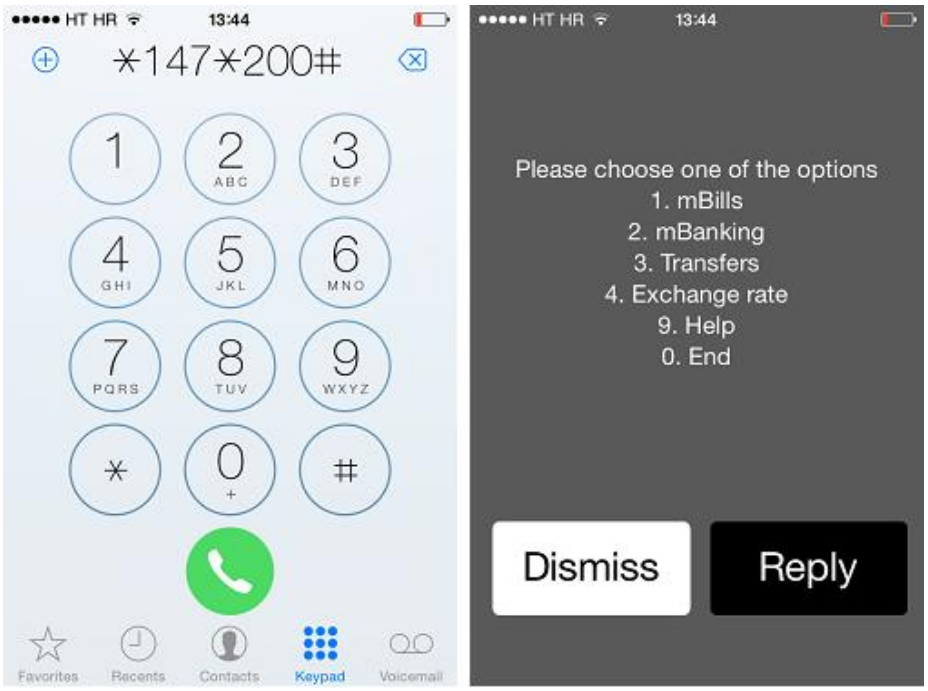
Proizvoljno definirani tunel određuju sljedeći koraci:

- Korisnik ima uspostavljenu vezu sa svojim ISP-om
- Pristupni koncentrator inicira L2TP tunel prema mrežnom poslužitelju
- U slučaju da mrežni poslužitelj prihvati zahtjev za spajanjem, pristupni koncentrator enkapsulira PPP u L2TP te proslijeđuje podatke preko tunela
- Mrežni poslužitelj koristi standardnu PPP autentifikaciju da bi utvrdio identitet korisnika te mu dodjelio IP adresu.

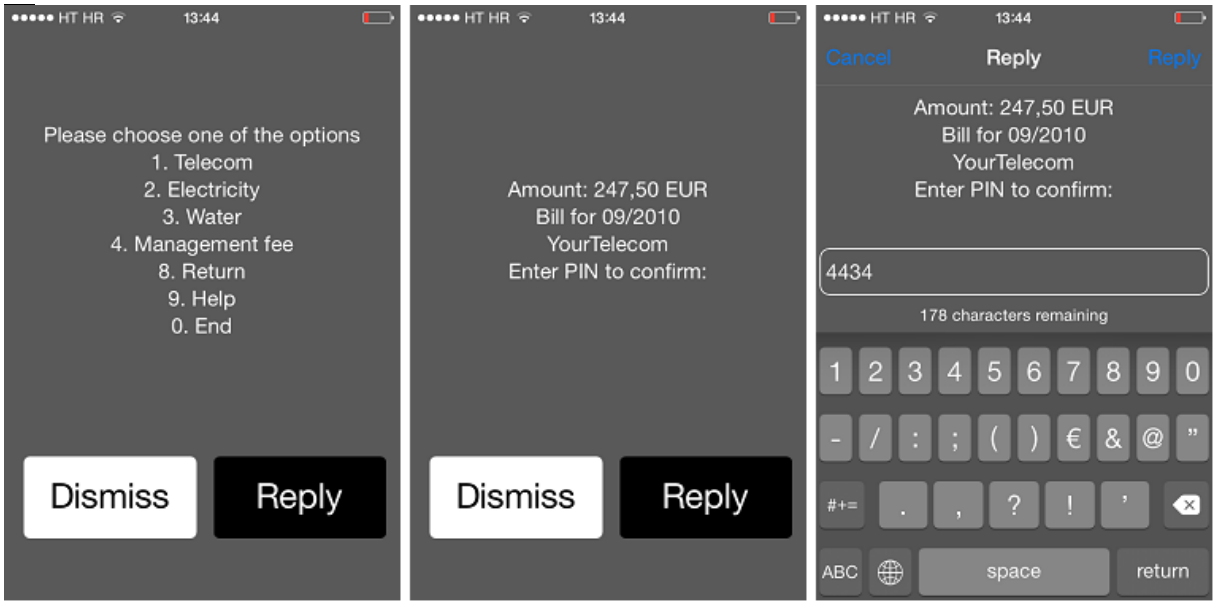
L2TP protokol podržava kontrolne i podatkovne poruke gdje se kontrole poruke koriste kod uspostave i održavanja tunela dok se podatkovne poruke koriste kod enkapsulacije PPP paketa, te se mogu ponovo poslati ukoliko dođe do gubljenja paketa.

4 USSD primjer u praksi

Pozivom na dedicirani kratki broj *147*200# sa T-Mobile mreže u Hrvatskoj korisnik pokreće jednostavnu demo USSD aplikacije koja prikazuje bankovno sučelje gdje korisnik ima mogućost plaćanja računa, prijenosa novca te uslugu.

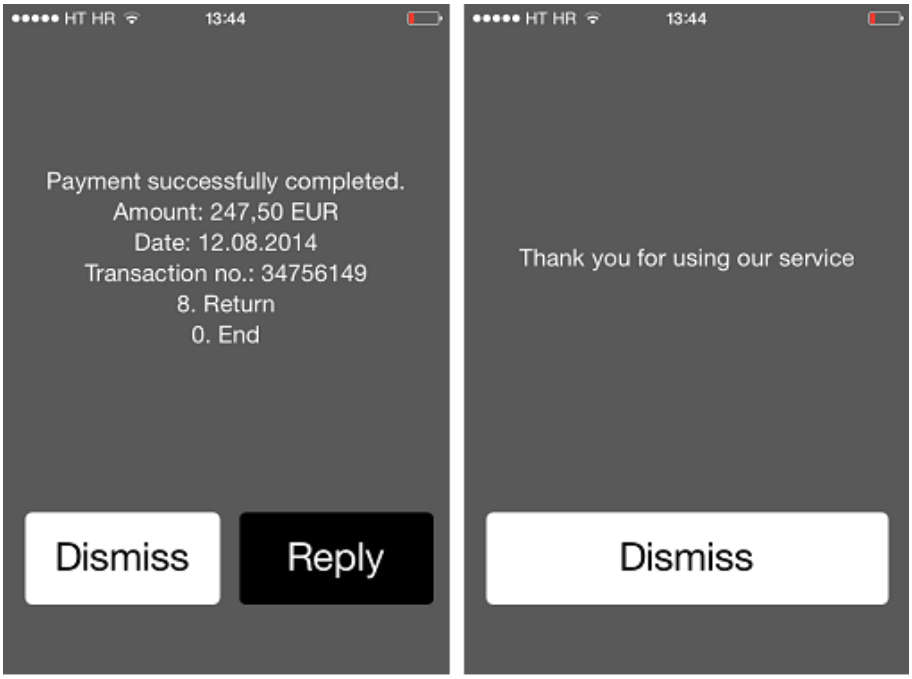


Slika 10. Pozivanje DEMO USSD aplikacije na kratkom broju *147*200#



Slika 11. Interakcija kroz uslugu , primjer plačanja računa

Korisnik nakon što je uspješno platio račun za telekomunikacije završava sesiju te zaprima pozdravnu poruku:



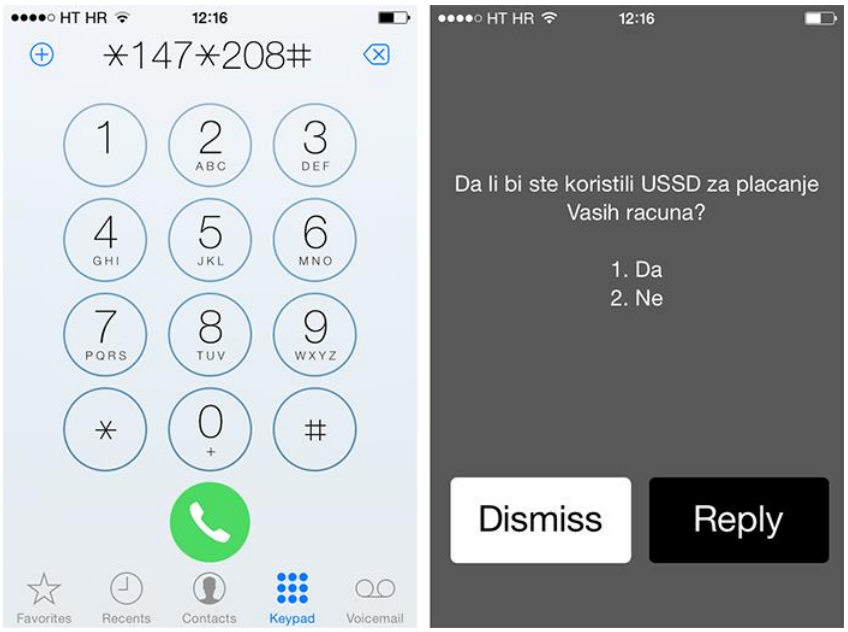
Slika 12. Korisnik zatvara sesiju nakon uspješnog plaćanja računa

Slične aplikacije izražene od strane Banaka u produkcijskom okruženju nude više mogućosti za interakciju kao što su :

- Provjera računa
- Zahtjev za prekoračenje na računu
- Zahtjev za izdavanje kredita
- Zahtjev za izdavanje kreditnih kartica
- Promjena korisničkih postavka (broj telefona,e-mail,zaporka)
- Upit korisničkoj podršci banke
- Aktivacija dodatnih usluga unutar banke
- Pregled umirovljeničkih fondova
- Burza

4.1 Pozivanje USSD usluge „Diplomski rad“

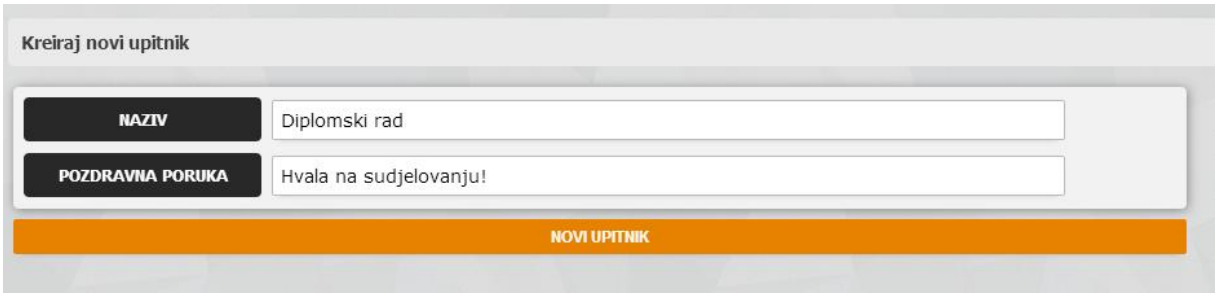
USSD aplikacija „Diplomski rad“ je kreirana uz pomoc Upitnik aplikacije a u svrhu prezentacije USSD usluge te je javno dostupna na T-Mobile mreži na dediciranom kratkom broju *147*208#.



Slika 13. Pozivanje aplikacije „Diplomski rad“ kroz sučelje mobilnog uređaja

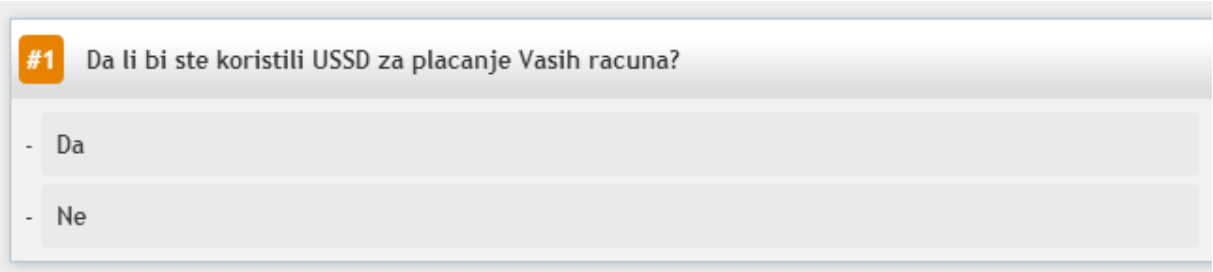
Upitnik aplikacija omogućuje krajnjim klijentima da jednostavno i brzo bez znanja o programiranju kreiraju i održavaju USSD upitnike u svrhu prikupljanja informacija od krajnjih pozivatelja usluge.

Nakon upućenog poziva na kratki broj pozivatelj zaprima sadržaj definiran u Upitnik aplikaciji te aplikacija u slučaju zaprimljenog odgovora od strane pozivatelja pohranjuje isti u bazi podataka te prema istoj prezentira podatke klijentu kroz intuativno korisničko sučelje.



Slika 14. Kreacija novog upitnika „Diplomski rad“

Nakon kreacije novog upitnika klijent može definirati pitanja i odgovore na koje pozivatelj usluge može odgovoriti a koji će biti dostupni klijentu za daljnu obradu i analizu.



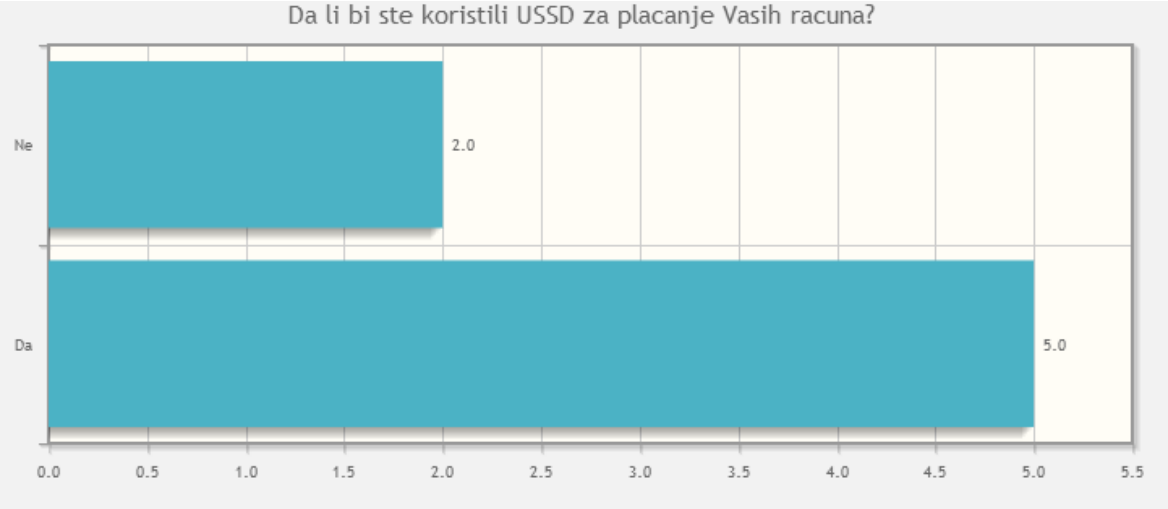
Slika 15. Definiranje pitanja i predefiniranih odgovora

4.2 Prikupljanje i analiza podataka

Sve prikupljene podatke krajnji klijent može pregledavati unutar Upitnik aplikacije kroz grafički prikaz ili preuzimanjem podataka u excel formatu.

Slika 16. Kratak pregled odgovora

Na osnovu prikupljenih podataka krajnji klijenti mogu kreirati metrike i segregirati bazu pozivatelja usluge. Primjer segregacije može biti pitanje kojim se određuje spol pozivatelja usluge, čime se ženskom ili muškom rodu mogu postaviti specifična pitanja . Muški rod će vjerojatno biti skloniji sportu dok bi ženski mogao biti skloniji modi.



Slika 17. Kratak pregled odgovora kroz grafove

Segregacijom pozivatelja usluge krajnji klijenti mogu efektivnije mjeriti prisutnost njihovih proizvoda na tržištu te prema zaprimljenim podatcima mogu preciznije plasirati svoje proizvode te samim time povećati prihode odnosno smanjiti rashode.

5 Zaključak

Prema procjenama stručnjaka do početka 2014 godine broj mobilnih uređaja iznositi će 7.3 milijardi, što je više od broja stanovnika zemlje. Saznanjem da 99.9% mobilnih uređaja nativno podržava USSD tehnologiju velike korporacije u marketinškom i bankarskom sektoru žele pružiti svojim korisnicima mogućost raspolaganjem informacija neovisno o trenutnom položaju i modelu mobilnog uređaja.

Na temelju naših saznanja, primjećuje se konstantan rast potražnje za jednostavnim i personaliziranim administracijskim sučeljem za kreaciju aplikacija što klijentima omogućuje brzo plasiranje usluge neovisno o dilatacijama tržišta bez dodatnih troškova. Infobip svojim rješenjima formira eko sustav koji pridonosi povezivanju potreba poslovnih korisnika sa već prisutnim mogućnostima operatera.
Glavni su predvodnici Afričke zemlje u kojima je USSD prihvaćen kao opći standard za komunikaciju između poslovnih subjekata upravo zbog gore navedenog razloga. S obzirom na taj model, ostaje za analizirati dali je potencijal i internacionalno primjenjiv.

6 Literatura

Interna dokumentacija tvrtke Infobip d.o.o

6.1 Internet stranice

1. http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf

7 Popis slika

8 Tumač pojmova

1. USSD“ - („Unstructured supplementary service data“ - ili „Sistem nestrukturiranih podataka dodatnih usluga“)
2. SS7 - „Signalling System #7“ ili „Signalizacijski sistem #7“
3. DTAP - ''Direct Transfer Application Part'' ili ''Direktni prijenos Aplikacijskog segmenta''
4. MAP SS7 - ''Mobile Application Part SS7'' ili 'Mobilni aplikacijski segment SS7''
5. Pull Metoda – Metoda povlačenja
6. MAP1 (Mobile Application Part 1 – Mobilni aplikacijski segment broj 1)
7. Push Metoda – Metoda prosljeđivanja, guranja
8. MAP2 (Mobile Application Part 2 – Mobilni aplikacijski segment broj 2)
9. Software – program, aplikacija
10. Rand – novčana valuta Južnoafričke Republike
11. Reverse model korištenja – Obrnut model korištenja
12. Pin – kratki broj, zaporka
13. Opt-in – lista kontakata koju klijent (npr. Banka) ima ažuriranu kod sebe, te sadrži popis svih krajnjih korisnika koji su pretplaćeni za primanje obavijesti. Sadrži i detalje o načinu na koji su kontakti prikupljeni. Postoji i „Opt – out“ lista, te sadrži popis svih adresata koji su izrazili potrebu za prekidanjem primanja obavijesti. Obavijesti prema takvim korisnicima nisu dozvoljene.
14. GET – prikupljanje, povlačenje
15. POST – objaviti
16. PUT - postaviti
17. DELETE - izbrisati
18. Extensible markup language – Jednostavan jezik za označavanje
19. Short Message Peer-to-Peer – „Kratka poruka točka-na-točku“
20. TCP - Transmission Control Protocol – „Transmisijski protokol za kontrolu“
21. PDU – „Protocol Data Units“ ili „Jedinice podatkovnog protokola“
22. Phase 2 – „Faza 2“
23. MSC – Mobile switching center – „Mobilni centar za preusmjeravanje“
24. Access kanal – „Pristupni kanal“
25. Out-of-band signalling – komunikacija izvan definirane telekomunikacijske frekvencijske grupe
26. In-band signalling – komunikacija unutar definirane telekomunikacijske frekvencijske grupe

27. Portabilnost brojeva – sposobnost da se mobilni broj prenese s jedne mreže na drugu, što znači da će prefiks ostati od prve mreže, ali će se sav komercijalni dio odvijati na drugoj mreži (u slučaju da je broj prenesen s mreže 1 na mrežu 2)
28. Extended kanali – rezervni kanali koji preuzimaju promet u slučaju da primarni nisu dostupni
29. VPN ili „Virtual private network“ je tehnologija koja omogućuje sigurno povezivanje između računala koristeći privatnu ili javnu mrežnu infrastrukturu. Kao medij za prijenos informacija najčešće se koristi internet dok je sekundarna i nadasve skuplja opcija privatna internet linija
30. IPSec – Internet Protocol Security – „Protokol za sigurnost na internetu“
31. Diffie-Hellman metoda za razmjenu ključeva – glavni ključ koji se koristi za generiranje regularnih ključeva se ne prenosi istim medijem kao i ostali podaci za spajanje
32. DES – Data encription standard – „Enkripcijski podatkovni standard“
33. HMAC – „Hash-based message authentication code“ – „kombinirano orijentirana autentifikacija koda“
34. TCP/IP – Transmission Control Protocol / Internet Protocol – „Internetski protokol za prijenos i kontrolu podataka“
35. L2F – Layer 2 Forwarding – protokol za tuneliranje koji koristi virtualne mreže za sigurni prijeno podataka

36. Layer 2 Tunneling Protocol – Protokol za tuneliranje koji podržava virtualne privatne mreže
37. PPP – Point to Point Protocol – Protokol za komunikaciju od točke do točke