SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Mile Šikić

Modeli naplate sadržaja u mobilnim paketskim mrežama

MAGISTARSKI RAD

Zagreb, 2002.

Magistarski rad je izrađen u:

Zavodu za električne sustave i obradbu informacija i Zavodu za telekomunikacije
Fakulteta elektrotehnike i računarstva
Sveučilišta u Zagrebu,
Connect Austria u Beču.

Mentor:

Prof.dr.sc. Mladen Kos

Rad ima 118 listova

Povjerenstvo za ocjenu rada:

1. prof.dr.sc. Branko Jeren, Fakultet elektrotehnike i računarstva
2. prof.dr.sc. Mladen Kos, Fakultet elektrotehnike i računarstva
3. doc.dr.sc. Antun Carić, Ericsson Nikola Tesla

Povjerenstvo za obranu rada:

1. prof.dr.sc. Branko Jeren, Fakultet elektrotehnike i računarstva
2. prof.dr.sc. Mladen Kos, Fakultet elektrotehnike i računarstva
3. doc.dr.sc. Antun Carić, Ericsson Nikola Tesla

Rad je obranjen 19. rujna 2002.

Sadržaj

1 Uvod

Razvoj mobilnih komunikacija u području prijenosa podataka u zadnjih nekoliko godina pred sustav naplate u mobilnoj telefoniji je stavio nove zahtjeve na koje postojeći sustav naplate nije mogao odgovoriti.

Tema ovog rada je izrada modela naplate sadržaja u mobilnim paketskim mrežama, što uključuje definiranje modela, opis njegovih elemenata te opis tehnologija koje se pri tome mogu koristiti. Osim općeg modela koji podražava uz naplatu sadržaja, naplatu usluga za uporabu dobivanog sadržaja te naplatu prijenosa, prikazan je i sustav za kupovinu sadržaja, tzv. platforma za m-trgovinu (engl. *m-commerce platform*). Na kraju rada je opisan eksperimentalni model koji se može koristiti za URL utemeljenu naplatu WAP sadržaja.

Osnovni model treba omogućiti povećanje vrijednosti Internet usluga za korisnike mobilnih telefona kroz veći izbor cijene i kvalitete, te reduciranju zagušenja kroz načine tarifiranja uporabe pojedinih usluga i uporabom podataka dobivenih praćenjem uporabe. Za mobilnog operatera treba povećati fleksibilnost, poboljšati postojeći sustav naplate usluga, smanjiti kompleksnost upravljanja te povećati dobiti od pružanja usluga. Osnovnim modelom se omogućava davatelju sadržaja naplatu uporabe sadržaja i aplikacija u suradnji sa mobilnim operaterom.

Kako je model naplate sadržaja usko vezan i uz uporabu i naplatu uporabe i kvalitete mrežnih usluga i prijenosa, kod izrade modela vodilo se računa o skalabilnosti sustava.

Osim osnovnog modela prikazan je model kupnje sadržaja preko platforme za m-trgovinu. Iako ovaj sustav ne pokriva sav sadržaj kao osnovni model, njegova jednostavnost i mogućnost brze implementacija su razlog njegovog razmatranja.

Kako područje skupljanja, obrade i naplate usluga i sadržaja u telekomunikacijskim sustavima u Hrvatskoj nije leksički obrađeno, u radu se koriste stručni izrazi iz ovog područja na engleskom jeziku posebno naglašeni kurzivom.

1.1 Osnovni pojmovi

Donji popis pojmova poredan abecednim redom definira pojmove bitne za razumijevanje modela sustava naplate objašnjenih u ovom radu:

- **Accounting**
  Sumiranje informacija zavisno o uporabi usluga od strane korisnika. Izražava se u izmjerenim vrijednostima uporabe resursa, aplikacije, pozive, sadržaje i bilo koji tip veze.

- **Autentifikacija (engl. *Authentication*)**
  Autentifikacija definira potvrdu identiteta subjekta

- **Autorizacija (engl. *Authorization*)**
  Autorizacija se definira kao verifikacija ima li subjekt dozvolu obavljanja pojedine radnje na objektu ili ne.

- **Korisnik (engl. *User*)**
  Osoba koja koristi mrežnu uslugu korištenjem aplikacija.

- **Medijacija (engl. *Mediation*)**
  U većini slučajeva podaci koji su skupljeni mjerenjem su tehnički podatci. Medijacija pretvara te podatke u oblik koji može biti korišten ta spremanje i daljnje procesiranje.

- **Middleware**
  Software koji posreduje između klijentskih i poslužiteljskih usluga u distribuiranim sustavima. Omogućava središnji nadzor nad mrežom unificira skup aplikacijskih programskih sučelja (npr. WAP *gateway*).

- **Mikro plaćanje (engl. *Micropayment*)**
  Transakcije vrlo niske vrijednosti. Obično se definira da su to transakcije ispod 5 EUR-a.

- **Mjerenje (engl. *Metering*)**
  Određivanje pojedinog korištenja resursa između krajnjih sustava ili sustava između na tehničkoj razini, uključujući QoS, upravljanje i mrežne parametre.

- **M-trgovina (engl. *M-commerce*)**
  Transakcija s monetarnom vrijednošću koristeći mobilnu telekomunikacijsku mrežu.

- **Naplata (engl. *Charging*)**
  Sveukupni izraz naplata koristi se za sveukupni proces mjerenje resursa, *accounting*,

postavljanje odgovarajuće cijene, izračun naplate i omogućavanje fino granuliranih skupova detalja traženih od sustava obračuna. Obračun nije uključen u ovu definiciju.

- **Obračun (engl. *Billing*)**
  Skupljanje naplatnih zapisa, sumiranje njihovih naplatnih sadržaja i isporuka računa uključujući opcionalnu listu detaljnih troškova za korisnika

- **Politika (engl. Policy)**
  Politika je skup pravila za administriranje, upravljanje i kontrolu pristupa resursima.

- **Sadržaj (engl. *Content*)**
  Fizička ili elektronička dobra.

- **Tarifiranje (engl. *Rating*)**
  Specifikacija i postavljanje cijena za dobra, specifične mrežne resurse te usluge.

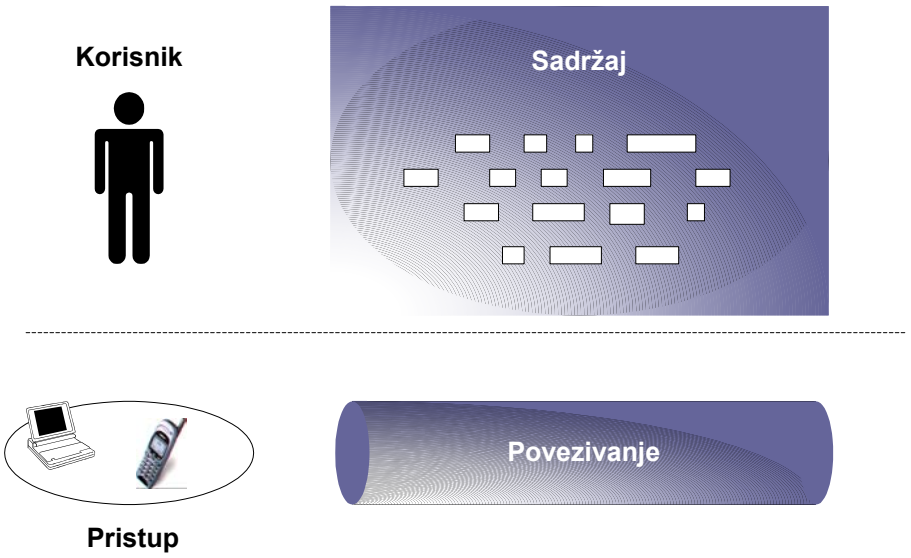
- **Usluga (engl. *Service*)**
  Usluga uključuje autonomno i mrežno zavisne zadatke potrebne za izvršenje aplikacije. Jedna aplikacija obično zahtijeva nekoliko distribuiranih usluga za uspostavu potpune funkcionalnosti

1.2 Pregled rada

Ovaj rad je organiziran na slijedeći način. Vrste sadržaja i usluga u mobilnim mrežama i mogućnosti naplate se razmatraju u drugom poglavlju. Postojeći sustav naplate u mobilnim mrežama i njegovi nedostaci su prikazani u trećom poglavlju. Dizajn modela sustava naplate koji obuhvaća sveukupnu naplatu prijenosa sadržaja i usluga sa osnovnim elementima je prikazan u četvrtom poglavlju. Detaljniji prikaz pojedinih elemenata, modela iz četvrtog poglavlja te neke njihove izvedbe nalazi se u petom poglavlju. šesto poglavlje se bavi kupnjom preko mobilnih uređaja i platformom za M-trgovinu. Sedmo poglavlje prikazuje osnovne principe eksperimentalnog modela za naplatu URL temeljenih WAP sadržaja. Zaključak rada se nalazi u osmom poglavlju. Na kraju rada nalazi se popis korištene literature, popis kratica te priloženi programi i struktura zapisa.

2 Vrste sadržaja i usluga u mobilnim mrežama i mogućnosti naplate

U trenutku kada je naplata pristupa mreži pod velikim pritiskom cijena, mobilni operatori moraju naći nove produkte koje mogu ponuditi pretplatnicima. Ponuda i naplata sadržaja je novi način kako povećati profite. Nove tehnologije poput GPRS-a, EDGE-a i UMTS omogućuju nove mogućnosti i usluge. U ovom poglavlju su prikazani sadržaji i usluge koje se mogu ponuditi korisnicima. Razvoj sadržaja dovesti će do povećanja prometa u pristupnim mrežama.



Slika 2-1: Sadržaj i povezivanje

Podjela sadržaja i povezivanja je vrlo važna zbog toga što korisnik mora znati koliko mora platiti za specifičan sadržaj, a koliko za kvalitetu usluge. Korisnik je zainteresiran za sadržaj, no isto tako za njegovu kvalitetu i vrijeme potrebno da ga dobije. Ukupna cijena mora biti najbolja ponuda koju može dobiti za to. Neki sadržaji neće se naplaćivati, ali korisniku će biti naplaćeno povezivanje. Zbog toga je sadržaj koji se ne naplaćuje jednako važan za operatera.

Osim naplaćivanja za sam pristup, korisniku se može naplatiti sadržaj i kvaliteta usluge prenošenja sadržaja.

2.1 Vrste sadržaja

Industrijska organizacija GBA (engl. *Global Billing Association*) pravi razliku između najmanje tri vrste sadržaja [16]:

- *Streaming*,
- Transakcije,
- Interaktivni sadržaji.

U tablici 2-1 su prikazani primjeri i karakteristike naplate za GBA klase sadržaja.

Tablica 2-1: Vrste sadržaja

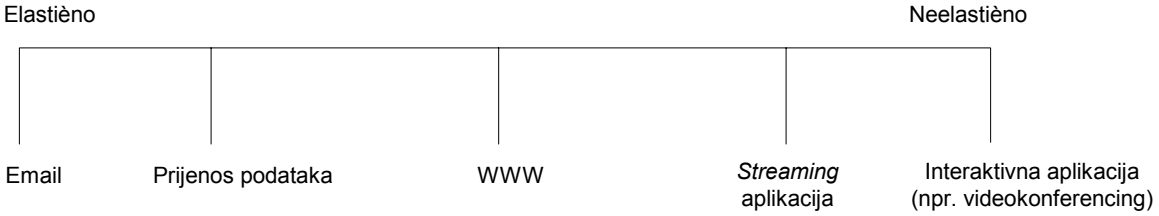
Sadržaj	Opis	Karakteristike naplate
Streaming	Skidanje cijelog sadržaja s mreže ili prenošenje "u živo" (npr. uporaba real playera). Primjeri ovakvog sadržaja su glazba, video, melodije poziva, crtani filmovi, aplikacije,...	Cijena može biti postavljena za cjelokupan sadržaj (npr. mp3 datoteke) ili njegove manje dijelove (npr. 10 minuta prijenosa). Vrijednosti mogu biti relativno niske po dijelovima ili velike za cjelokupan sadržaj. U ovom slučaju je jako bitna i kvaliteta same usluge (QoS) čija cijena ulazi u sveukupnu vrijednost.
Transakcije	Kupovina elektroničkih ili fizičkih dobara (m-/e-*trgovina*). Primjeri su kupovina kino karata, knjiga, CD-a ili burzovnih dionica.	Vrijednost leži u kupovini elektroničkih ili fizičkih dobara. Cijena samog pristupa je manje više nebitna.
Interakcija	*Push/pull* usluge. Primjeri su igre, traženje informacija, usluge lociranja korisnika, reklame vezane uz profil/karakteristike korisnika.	Ove usluge uključuju velik broj mogućnosti naplate kao npr. uporaba određivanja lokacije korisnika kao jednog od parametara. Oglašivači plaćaju za svoje reklame, dok korisnik može čak biti plaćen kroz nagradne bodove ili popuste za gledanje reklama.

2.2 Usluge prijenosa sadržaja

Mobilne paketske mreže imaju svoje zakonitosti vezane uz svoje specifičnosti (veličina ekrana, mobilnost, personalizacija), no čvrsto su vezane za razvoj usluga i sadržaja na Internetu.

Naplata usluga se na Internetu uglavnom temeljila na "*flat fee*" modelu naplate pristupa i dobivanja usluga koje nisu garantirane i koje uključuju varijabilno kašnjenje. Međutim, različite aplikacije imaju sasvim različite zahtjeve za prijenosnim uslugama. Neke usluge (npr. e-mail) mogu tolerirati značajna kašnjenja bez narušavanja kvalitete same usluge, dok druge kao što su audio i video *streaming,* značajno gube na kvaliteti već pri malim kašnjenjima. S drastično različitim zahtjevima potreba za kategorizacijom na Internetu se pokazala nužnom. Uz potrebu za postizanjem performansi javlja se i potreba određivanja cijene za različite klase usluga. Koristeći ovu ideju moguće je za korisnika da postavi prioritete za svoje aplikacije i isto tako zahtjeva prihvatljivu razinu QoS-a za pojedinu uslugu. U ovoj situaciji korisnik ima mogućnost platiti veću cijenu za veću kvalitetu.

Ovisno o vrsti prometa i njegovim zahtjevima za minimalnim kašnjenjem možemo definirati elastičnost pojedinog prometa. Na slici 2-2 je prikaz različitih prometa i njihove relativne elastičnosti u odnosu na druge promete.



Slika 2-2: Relativna elastičnost prometa

Iako su korisnici normalno pripremljeni na kašnjenje u slučaju uporabe elastičnih aplikacija, zato što očekuju da se prenesu kasnije tokom dana, netko može poslati hitan e-mail koji se može tretirati kao neelastična aplikacija (npr. e-mail kojim se obavještava nekoga da se hitno priključi video-konferenciji) [1].

3 Postojeći sustav naplate u mobilnim mrežama

Postojeći sustav naplate u mobilnim mrežama je temeljen na sustavu koji je bio predviđen za skupljanje i naplatu usluga u govornoj mobilnoj telefoniji. Osnova ovog sustava je praćenje trajanja i vrste telefonskih poziva obradom zapisa CDR-a (engl. *Charging Data Record*) dobivenih s komutatora. U sustav su naknadno dodani: SMSC (SMS središte) za razmjenu SMS poruka i kreiranje zapisa o poslanim porukama, inteligentna mrežna IN (engl. *Inteligent network*) platforma za obradu *prepaid* korisnika te GSN (engl. *GPRS switch node*) čvorovi i CG za praćenje i obradu informacija u GPRS mreži.

3.1 Arhitektura postojećeg sustava naplate

Arhitektura postojećeg sustava naplate sastoji se od sljedećih gradivih blokova:

- Autentifikacije i autorizacije korisnika,
- Mrežnih elemenata koji prate, komutiraju promet i kreiraju zapise (CDR-ove) o obavljenom prometu,
- Sustava medijacije koji prikuplja CDR-ove, provjerava njihovu ispravnost, te ih korelira i agregira na korisničkoj osnovi. Tako obrađene zapise preformatira u oblik pogodan za sustav tarifiranja i sprema ih u datoteke (engl. *batch*),
- Sustava tarifiranja koji uzima podatke iz medijacije i određuje cijenu pojedine usluge zavisno o vrsti usluge i korisničkom profilu,
- Sustava obračuna koji uzima podatke iz tarifiranja i konsolidira ih na korisničkoj osnovi i agregirane na vremenskoj osnovi (npr. unutar jednog kalendarskog mjeseca) šalje ih sustavu za izdavanje računa (engl. *invoicing*) koji ih isporučuje korisnicima (tarifiranje i obračun se najčešće realiziraju u istom uređaju),
- *Prepaid* platforme za naplatu usluga u realnom vremenu za korisnike koji unaprijed kupe određeni broj impulsa,
- *Prepaid* sustava koji služi za obradu korisničkih informacija u realnom vremenu.

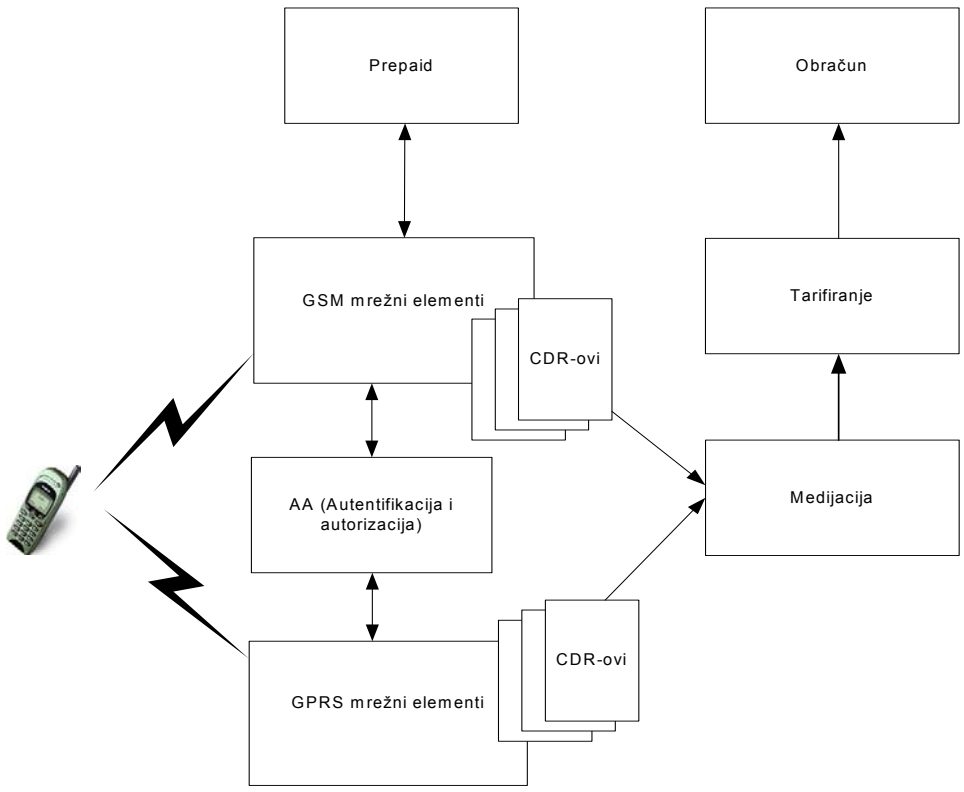
Slika 3-1 prikazuje tipičan sustav naplate, s osnovnim gradivim blokovima, u današnjim mobilnim mrežama. Takav sustav obuhvaća naplatu razgovora, spajanja na Internet preko

GSM mreže (komutacijom kanala), spajanja na Internet preko GPRS mreže (komutacijom paketa), WAP prometa i SMS poruka.

Iako su bazne stanice i kontroleri GSM i GPRS mreža fizički zajednički, mreže su prikazane odvojeno radi lakšeg promatranja sustava.

Bitan detalj na slici je povezivanje *prepaid* platforme samo na GSM mrežu, ne i GPRS. Većina današnjih operatera ovaj problem nije efikasno riješila ili su rješenja nepraktična. Stoga se u ovom radu pretpostavlja da taj problem nije riješen.

Implementacija GPRS sustava naplate u postojeći GSM sustav se provodi povezivanjem CG i postojećeg sustava medijacije. Na taj način CG, koji je i sam sustav medijacije, predstavlja dodatni izvor CDR-ova za postojeći sustav medijacije.



Slika 3-1: Postojeći sustav naplate u mobilnim mrežama i osnovni gradivi blokovi

Autentifikacijski i autorizacijski sustav prepoznaje korisnika koji se spaja na mrežu ili zahtjeva određenu uslugu, pa mu zavisno o njegovom profilu dodjeljuje različita prava (npr. uporaba VPN-a kod GPRS-a). Te se informacije spremaju u mrežne elemente koji zavisno o načinu uporabe i vrsti usluga generiraju CDR-ove. CDR–ovi se dalje prosljeđuju u sustav medijacije. U medijaciji se CDR-ovi provjeravaju, koreliraju i agregiraju na bazi korisnika i pripadajuće sesije te preformatiraju u format prilagođen sustavu tarifiranja. Sustav tarifiranja, zavisno o korisničkom profilu i tarifi za pojedine usluge, dodjeljuje cijenu za pojedinu sesiju, te preformatira podatke za sustav obračuna. Sustav obračuna agregira podatke, odnosno cijenu za pojedinog korisnika na vremenskoj osnovi (obično mjesec dana). Tako dobiveni podaci šalju se sustavu za izdavanje računa (npr. ispis računa na uplatnice).

Prepaid funkcionira na drugačiji način od klasičnog obračuna. Korisnik unaprijed od operatera zakupljuje sumu novca/vremena koja se sprema na korisnikov račun. Kada korisnik zatraži određenu uslugu mrežni element postavlja zahtjev *prepaid* platformi da mu dodijeli određenu količinu novca, odnosno vremena kod telefonskog poziva. *Prepaid* platforma dodjeljuje određeni iznos. Ukoliko usluga traje dulje mrežni element traži dodatnu količinu vremena/novca. Ako korisnik nema više novca na računu veza se automatski prekida. Ukoliko je ostalo novca na računu, mrežnom elementu se dodjeljuje nova suma novca/vremena. Komunikacija između *prepaid* platforme i mrežnog elementa je kod GSM komutatora vrlo brza i korisnik ne može koristiti uslugu ako više nema novca na računu.

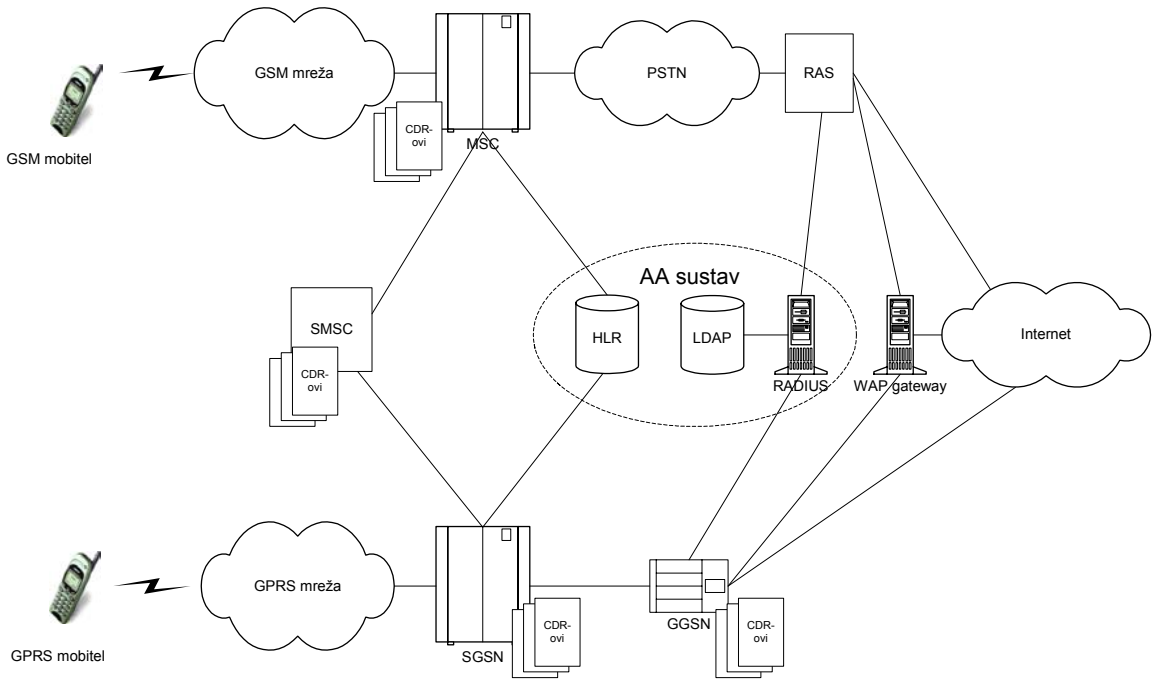
Način na koji su gradivi blokovi sustava naplate postojećih mobilnih mreža izvedeni i implementirani u sustav prikazano je na slikama 3-2 i 3-3, gdje slika 3-2 prikazuje jezgru mobilne mreže i njeno povezivanje s Internetom i javnom telefonskom mrežom (engl. PSTN – *public switched telephone network*), dok slika 3-3 prikazuje naplatu i obračun u postojećim mobilnim mrežama.

3.1.1 Jezgra mobilne mreže

Jezgru mreže čine elementi za autentifikaciju i autorizaciju (AA), te mrežni elementi za komutiranje prometa i stvaranje CDR-ova.

Autentifikacija i autorizacija se obavlja na dva mjesta. Prvo mjesto je HLR u kojem se nalazi korisnički profil prema kojem MSC, odnosno SGSN omogućuju korisniku spajanje u mrežu i uporabu određenih usluga zajamčene kvalitete (privatna IP adresa i QoS kod GPRS-a). Drugo mjesto je RADIUS server, koji dodjeljuje korisniku IP adresu i razinu usluge (npr. VPN)

prilikom spajanja na Internet. Korisnički profil se sprema u LDAP. Za uporabu telefonije i slanje SMS poruka dovoljan je korisnički profil smješten u HLR-u.



Slika 3-2: Jezgra mobilne mreže i način njezinog spajanja na Internet i javnu telefonsku mrežu

Za komutiranje prometa i generiranje CDR-ova koriste se slijedeći uređaji:

- **MSC**

  Komutator GSM prometa i generator CDR-ova vezanih uz govorne usluge, prijenos podatkovnih paketa upotrebljavajući WAP preko GSM mreže.

- **SMSC**

  Centar za slanje i primanje SMS poruka i generator CDR-ova vezanih uz SMS poruke.

- **SGSN i GGSN**

  Komutatori GPRS prometa i generatori CDR-ova vezanih uz GPRS promet u mreži.

WAP *gateway* služi kao *proxy* između WAP preglednika na korisnikovom mobitelu i HTTP poslužitelja na kojem se nalaze WML stranice. WML stranice su stranice prilagođene WAP preglednicima. WAP *gateway* ima mogućnost kreiranja vlastitih CDR-ova, ali se ovo rješenje danas uglavnom ne koristi.

RAS (engl. *Remote Access Server*) isto kao i GGSN predstavlja izlazni usmjerivač prema Internetu, Intranetu ili privatnim mrežama korisnika.

Kod uporabe mobilne telefonije MSC generira CDR-ove za svaku uspješno uspostavljenu vezu. Osnove informacije u MSC CDR-ovima su korisnički ID, vrsta usluge, trajanje i jedinstveni broj svake sesije.

SMSC generira CDR za svaku uspješno poslanu SMS poruku. Osnovne informacije u SMS CDR-ovima su korisnički ID i vrsta usluge.

Prilikom spajanja na Internet korisnik se može spojiti na nekoliko načina. Zavisno o njima nastati će CDR-ovi vezani uz uporabu te usluge. Korisnik se može spojiti na Internet na sljedeće načine:

- Uporabom prijenosa podatkovnih paketa u GSM mreži,
- GPRS mrežom,
- WAP-om preko GSM mreže,
- WAP-om preko GPRS mreže.

U prva dva slučaja korisnik za spajanje koristi računalo spojeno na mobilni uređaj dok se u trećem i četvrtom koristi WAP preglednik ugrađen u mobilni aparat.

Spajanje na Internet prijenosom podatkovnih paketa u GSM mreži

Prijenos komutiranih podatkovnih paketa CSD (engl. *Circuit Switch Data*) se razlikuje od prijenosa glasa u GSM mreži. Razlika je u načinu kodiranja. Korisnik mora imati tu uslugu omogućenu u svom korisničkom profilu pohranjenom u HLR-u. Danas se koristi i HSCSD (engl. *High Speed Circuit Swith Data*) koji omogućava uporabu više vremenskih odsječaka za prijenos podataka. Ovim načinom korisnik zove fiksni telefonski broj i preko RAS-a (engl. *Remote Access Server*) se povezuje na Internet. Za autentifikaciju i autorizaciju korisnika koristi se RADIUS server povezan s LDAP-om. CDR–ovi se generiraju na MSC-u i sadrže informacije o trajanju i vrsti usluge.

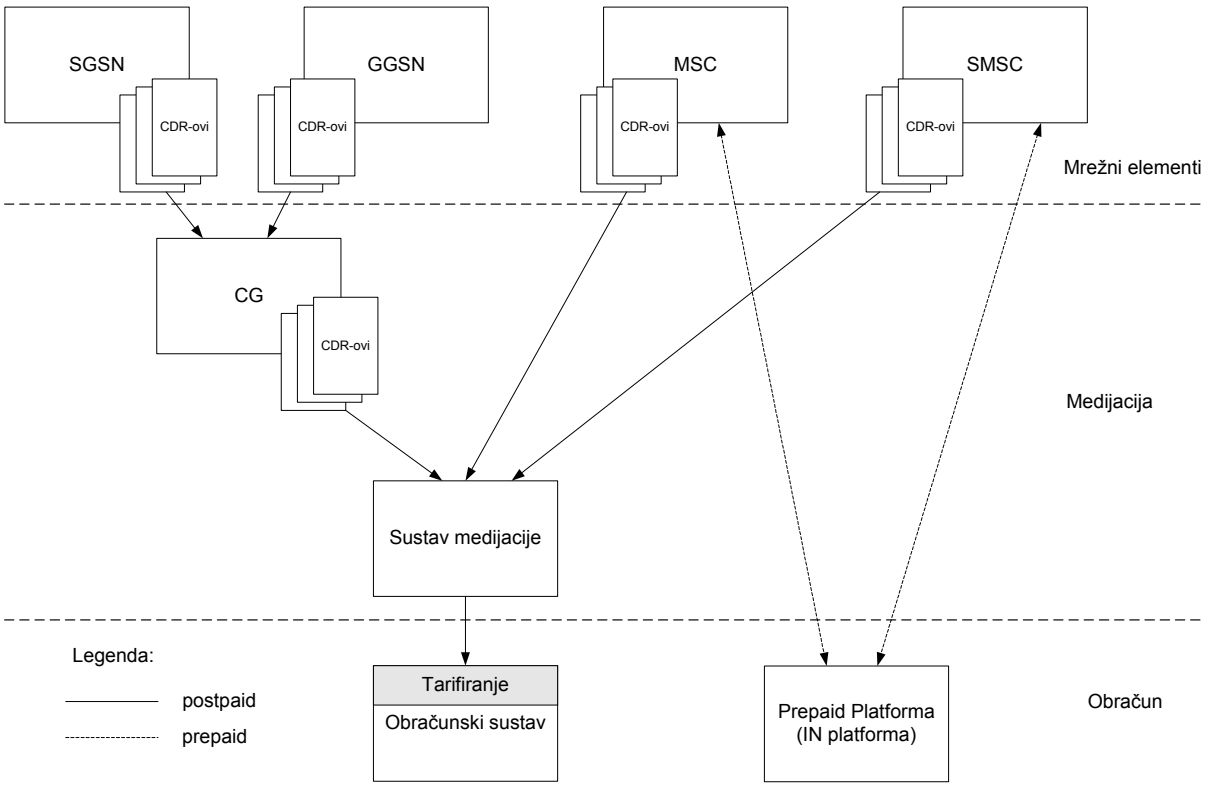
Spajanje na Internet preko GPRS mreže

Kao i kod GSM-a, da bi se korisnik mogao spojiti na samu GPRS mrežu potrebno je izvršiti autorizaciju i autentifikaciju preko HLR-a. Kada korisnik zatraži spajanje na Internet preko APN-a definiranog za tu uslugu, SGSN šalje zahtjev GGSN-u za otvaranje usluge (tzv. *PDP Context*). GGSN zahtjeva AA od RADIUS servera koji, zavisno o korisničkom profilu i vrsti APN-a, korisniku dodjeljuje IP adresu i prava. Npr. može se definirati da je korisniku omogućen samo HTTP protokol, čime se na GGSN-u, koji je u stvari usmjerivač, stvara pristupna lista s korisnikovom adresom i pravima. CDR-ovi se generiraju i na SGSN i GGSN–u te sadrže informacije o volumenu prenesenih podataka, vremenu trajanja, dogovorenom QoS-u i vrsti usluge.

Bitnih razlika između spajanja na Internet preko računala spojenog na mobilni uređaj i preko WAP-a nema. Jedina razlika je što se na izlazima iz GSM, odnosno GPRS mreže, korisnikov promet preusmjerava direktno na WAP *gateway*. Generiranje CDR-ova se obavlja na istim mjestima, uz razliku da su tarife za WAP uslugu drugačije.

3.1.2 Izvedba sustava naplate u današnjim mobilnim mrežama

Slika 3-3 prikazuje način na koji je sustav naplate izveden u današnjim mobilnim mrežama. Prikazani su mrežni elementi koji stvaraju CDR-ove, te način na koji su izvedeni medijacija, tarifiranje, obračun, te *prepaid* sustav. Sveukupan proces praćenja i mjerenja prometa u mrežnim elementima, generiranje CDR–ova, njihova medijacija i tarifiranje naziva se naplata.



Slika 3-3: Naplata i obračun u postojećim mobilnim mrežama

Kako većina postojećih sustava obračuna u sebi sadrži i tarifiranje, tako se tarifiranje na slici 3-3 nalazi u sklopu sustava obračuna.

Nakon što se CDR-ovi generiraju u mrežnim elementima, oni se prebacuju u sustav medijacije koji ih provjerava, agregira i korelira ovisno o korisniku i pojedinoj sesiji. Na kraju se formira zapis prilagođen sustavu obračuna u kojem je svaka sesija pojedinog korisnika prikazana jednom linijom zapisa.

Kod GPRS-a se podaci u realnom vremenu odmah nakon nastanka prebacuju u CG (engl. *Charging gateway*). CG koji ima funkciju medijacije za GPRS sustav, korelira podatke dobivene iz SGSN-a i GGSN-a u jedinstveni izlazni format CDR-a, koji se dalje prosljeđuje u medijaciju.

Razlog zbog kojeg se izlaz iz CG spaja direktno u medijaciju je dobivanje jedinstvenog sučelja prema sustavu obračuna.

Sustav obračuna uzima podatke iz medijacije, dodjeljuje cijenu ovisno o usluzi i agregira ukupnu cijenu na mjesečnoj osnovi.

Osim prebacivanja podataka iz GPRS čvorova u CG, koje je u realnom vremenu, svi ostali zapisi se spremaju u izlazne datoteke (engl. *batch*) koje naknadno sljedeći sustav uzima u pravilnim vremenskim razmacima najčešće koristeći FTP protokol.

Prepaid sustav može komunicirati direktno s mrežnim elementima bez medijacije. On također u sebi sadrži i tarifiranje. Većina današnjih *prepaid* sustava se bazira na IN platformi. Komunikacija između *prepaid* sustava i mrežnih elemenata se odvija SS7 protokolom.

3.2 Naplata sadržaja i usluga u postojećim mobilnim mrežama

Postojeći sustav naplate u mobilnim mrežama je fokusiran na naplatu pristupa u mreži. Pristup, ovisno o nosiocu, možemo podijeliti na:

- GSM telefoniju,
- GSM prijenos podataka,
- WAP preko GSM-a,
- SMS,
- GPRS,
- WAP preko GPRS-a.

Problem nastaje kod dodavanja novih nosioca. Kako je postojeći sustav medijacije prilagođen mobilnoj telefoniji, svako dodavanje novog nosioca iziskuje promjene i dodavanje novih mogućnosti u sustav medijacije. Time sustav medijacije postaje nefleksibilan i težak za održavanje i praćenje.

Dodatni problem predstavlja *prepaid* platforma koju je također potrebno nadograditi ili zamijeniti. Upravo taj problem je rezultirao da je samo nekoliko operatera do sada integriralo *prepaid* u GPRS sustav što je iziskivalo nabavu novog rješenja. SS7 protokol, koji se koristi u tradicionalnim telekomunikacijskim sustavima za povezivanje IN platforme sa MSC-om i SMSC-om, nije pogodan za uporabu zajedno s paketskim IP mrežama.

Iako GPRS sustav ima mogućnost uporabe QoS usluge, zbog problema s postojećom opremom kao i zbog nedostatka usluga s posebnim QoS zahtjevima, ova usluga se ne koristi u mobilnim mrežama. Oprema koja će podržavati QoS se očekuje krajem 2002 godine.

Većina postojećih sustava podržava jedino naplatu uporabe sadržaja koji se prenose SMS porukama. Sadržaji se većinom odnose na "skidanje" pojedinih slika, dojava poziva, izvještaja o stanju na računu. Ove usluge se obično naplaćuju po mjesečnoj pretplati. SMS omogućuje i kupovinu fizičkih dobara kao što su bezalkoholna pića na automatima, karte za kino i kazališne predstave, naplatu pojedinih usluga (npr. naplata parkiranja), itd.

WAP sadržaji poput pojedinih WML stranica, aplikacija i igara nemaju mogućnost naplaćivanja u većini postojećih sustava.

3.3 Zaključak

Kako su postojeći sustavi ograničeni samo na naplatu pristupa mreži, te prenošenje sadržaja preko SMS poruka, potrebno je napraviti novi sustav.

Novi sustav mora omogućiti naplatu kako postojećeg pristupa mreži, usluga i sadržaja, no isto tako mora odgovarati potrebama u budućnosti.

Budućnost mobilne telefonije, kao i ostalih paketskih IP mreža, je integracija u jednu mrežu u koju će korisnik moći pristupiti s bilo kojeg mjesta i koja će mu omogućiti jednaka prava bez obzira gdje se spojio.

 av naplate sadržaja i usluga mora moći podržati takvu mrežu sa sljedećim specifičnim zahtjevima:

- globalna autentifikacija i autorizacija korisnika,
- skupljanje podataka o uporabi pojedinog pristupa, usluge i sadržaja,
- naplata uporabe,
- agregacija skupljenih podataka,
- povećanje efikasnosti mreže načinom tarifiranja i uporabom skupljenih podataka o stanju prometa u mreži,
- mogućnost uporabe različitih metoda naplate (telefonski račun, *prepaid*, bankovni račun itd.),
- sigurnost sustava.

4 Model sustava za naplatu prijenosa, sadržaja i usluga u mobilnim paketskim mrežama

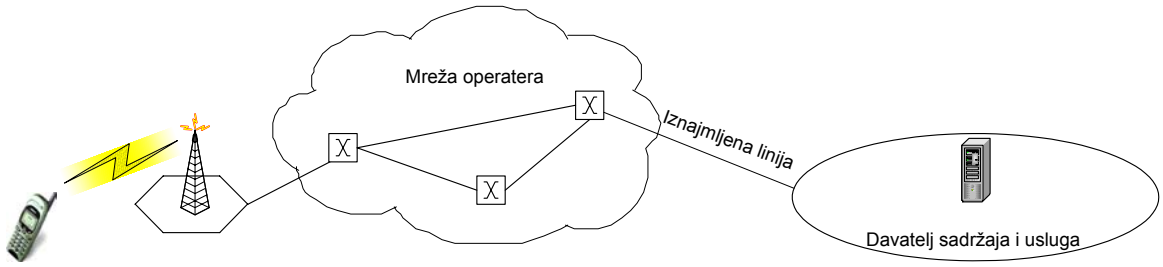
Kako je model naplate sadržaja povezan s naplatom prijenosa i usluga, model opisan u ovom poglavlju je integralan i sadrži sva tri dijela ukupne naplate (prijenos, usluga, sadržaj).

Za funkcioniranje i arhitekturu sustava koji korisnicima omogućava uporaba određenih sadržaja i usluga vrlo je bitno gdje će se ti sadržaji i usluge nalaziti i kako će biti povezani s mrežom operatera. Postoje tri načina na koje operater mobilne telefonije omogućava svojim korisnicima pristup sadržajima i uslugama:

- zatvoreni sustav,
- otvoreni sustav,
- poluzatvoreni.

Zatvoren sustav

Zatvoren sustav u kojem sadržaju mogu pristupati samo korisnici unutar mreže (u stručnoj terminologije se još naziva i "*walled garden*"). U tom slučaju sadržaj se nalazi unutar same mreže operatera ili je davatelj sadržaja povezan iznajmljenim ili VPN vezama s operaterom. Slika 4-1 pokazuje primjer zatvorenog sustava.



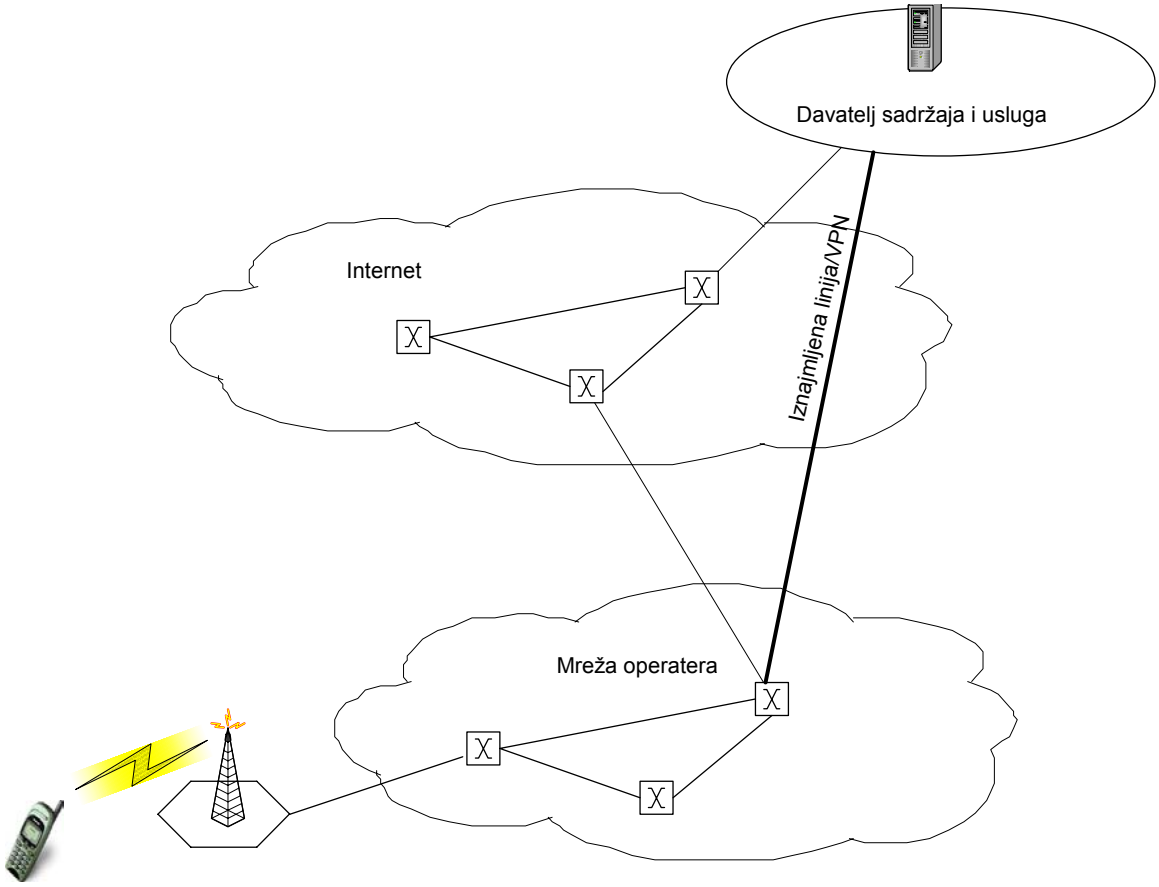
Slika 4-1 Zatvoreni sustav pristupa sadržajima i uslugama

Prednost zatvorenog sustava je u tome što operater ima potpunu kontrolu nad sadržajem i njegovom naplatom. U tom sustavu autorizacija i autentifikacija kao i skupljanje podataka bitnih za naplatu i način tarifiranja se može vršiti s centralnog mjesta. Primjer ovakvog sustava je postojeći sustav naplate usluga i sadržaja prenošenih preko SMS poruka.

Mana zatvorenog sustava je u tome što je korisnik ograničen samo na usluge i sadržaje koje mu nudi operater, dok je sve ostalo izvan njegovog dosega.

Otvoreni sustav

Otvoreni sustav je sustav gdje je korisnik povezan preko vanjskih ISP na sadržaje i usluge koje se nalaze diljem Interneta. Operator ima zasebnu iznajmljenu vezu ili VPN s kojom se povezuje s davateljem sadržaja/usluga. Preko te linije se obavlja AAA. Slika 4-2 prikazuje taj sustav.



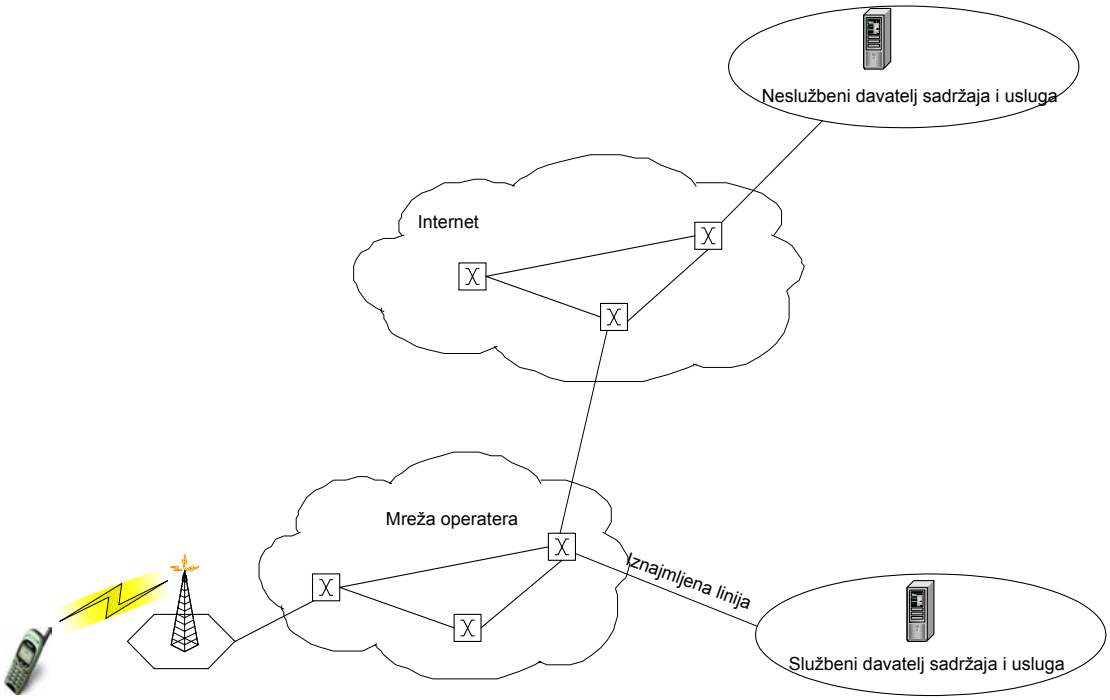
Slika 4-2 Otvoreni pristup sadržajima i uslugama

Prednosti otvorenog sustava su mogućnost korisniku da pristupi svim dostupnim uslugama i sadržajima na Internetu. Isto tako, svi na mreži imaju pristup stranicama koje se ne naplaćuju.

Nedostatak ovakvog sustava je potreba za jedinstvenom autorizacijom i autentifikacijom korisnika na različitim mjestima (npr. mreža operatera i sadržaj koji se nalazi negdje na Internetu), te skupljanje podataka bitnih za naplatu na prostorno udaljenim lokacijama.

Poluzatvoreni sustav

Polu-zatvoreni sustav (koristi ga japanska telekomunikacijska tvrtka NTT DoCoMo) je međurješenje između otvorenog i zatvorenog sustava. U tom sustavu postoje dvije vrste sadržaja odnosno stranica, službene i neslužbene. Službene stranice su one koje su direktno povezane s operaterom, za koje on jamči kvalitetu za korisnike i naplatu za davatelje sadržaja i usluga. Pristup stranicama je direktan preko portala.



Slika 4-3 Poluzatvoreni pristup sadržajima i uslugama (NTT DoCoMo sustav)

Korisnik ima mogućnost pristupa neslužbenim informacijama na način kao i kod uporabe Interneta, odnosno unošenjem adrese stranice. Operater ne daje nikakvu garanciju kvalitete ovih stranica, te ne omogućava naplatu sadržaja i usluga. Autorizacija i autentifikacija korisnika te skupljanje podataka se obavlja centralno i korisniku se naplaćuje jedino pristup pojedinoj usluzi.

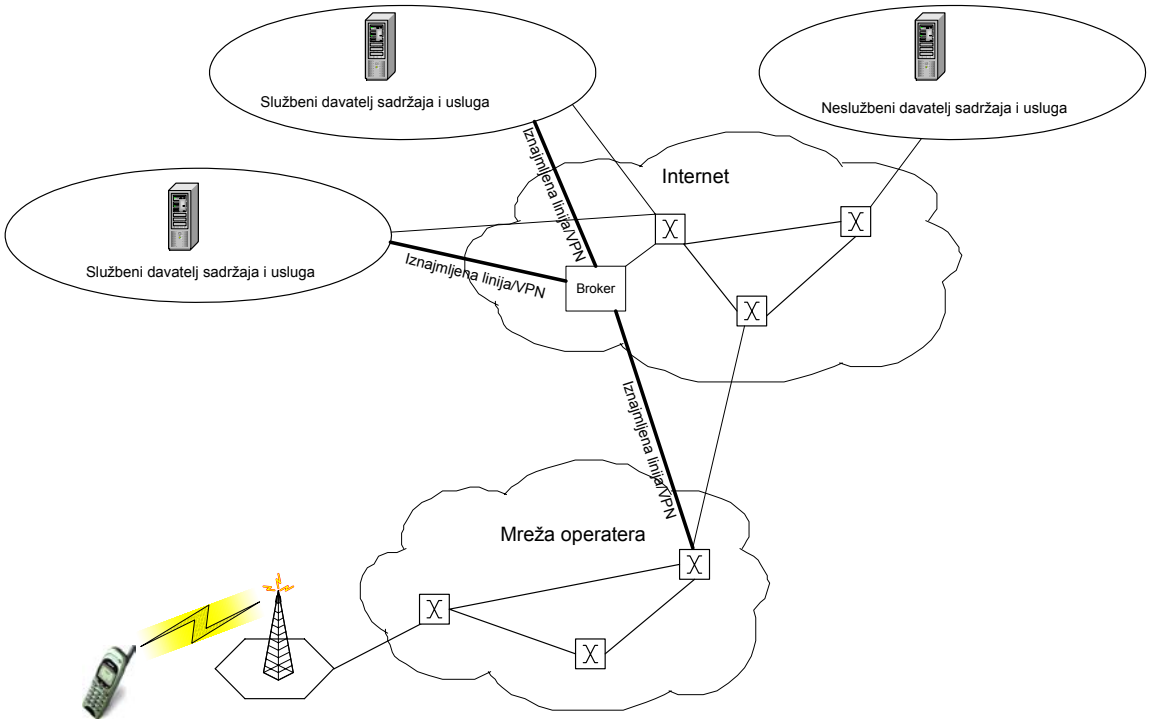
Prednost ovog sustava je u tome što korisnik pristupa svim dostupnim sadržajima na Internetu, dok se naplaćuju samo pojedine stranice odnosno sadržaji. U ovakvom sustavu autentifikacija i autorizacija korisnika se obavlja na jednom mjestu što umanjuje složenost sustava.

Nedostatak sustava je vezan uz davatelje sadržaja i vezu između operatera i davatelja sadržaja. Operater mora imati ugovor sa svakim davateljem pojedinačno, te isto tako, ako davatelj želi pružiti svoj sadržaj većem broju korisnika mora uspostaviti vezu s nekoliko operatera posebno.

Drugi primjer poluzatvorenog sustava, prikazan na slici 4-4, je uporaba brokera odnosno agencije koja se bavi skupljanjem davatelja sadržaja i usluga te nuđenja toga operateru. Ostali sadržajima koji se ne naplaćuju su direktno dostupni korisniku. Broker skuplja informacije o uporabi pojedinih sadržaja i usluga, a operater skuplja informacije o uporabi pristupa u mrežu. Autentifikacija i autorizacija se obavlja u suradnji između brokera i operatera. Podaci o uporabi usluga se šalju operateru odnosno njegovom sustavu obračuna.

Prednost ovakvog sustava je u odnosu na NTT DoCoMo model je u tome što operater vodi računa jedino o vezi prema brokeru dok broker uspostavlja veze prema davateljima sadržaja i usluga.

U ovom slučaju sadržaj mogu koristiti samo korisnici čiji operateri koji imaju ugovor s brokerom.



Slika 4-4 Poluzatvoreni pristup sadržajima i uslugama (broker sustav)

Nedostatak ovog sustava je u tome što operater ovisi o brokeru i njegovim partnerima.

U ovom radu će biti opisan model koji se temelju na kombinaciji otvorenog i poluzatvorenog sustava (broker sustava). Ova kombinacija omogućava operatoru kako dogovor s pojedinim davateljima usluga i sadržaja, tako i povezivanje s njima preko brokera.

4.1 Zahtjevi sustava za naplatu sadržaja i usluga

Internet će u budućnosti predstavljati jednu mrežu na koju će se korisnik povezivati preko različitih pristupnih mreža te gdje će korisnik dobivati jedinstveni račun bez obzira od kuda se spajao te koje je usluge koristio. Sustav mora osiguravati maksimalnu sigurnost, fleksibilnost i pouzdanost korisniku. Za razliku od postojećih GSM sustava korisnik će koristiti istovremeno nekoliko usluga, odnosno sadržaja koje će se posebno naplaćivati (npr. naplata pristupa u mrežu i praćenje *videostreaming* prijenosa). U tom slučaju sustav će pratiti istovremeno nekoliko tokova informacija bitnih za naplatu. Sustav mora imati mogućnost jednostavnog i efikasnog upravljanja u mreži, kao i mogućnost ograničenja uporabe komunikacije u mreži.

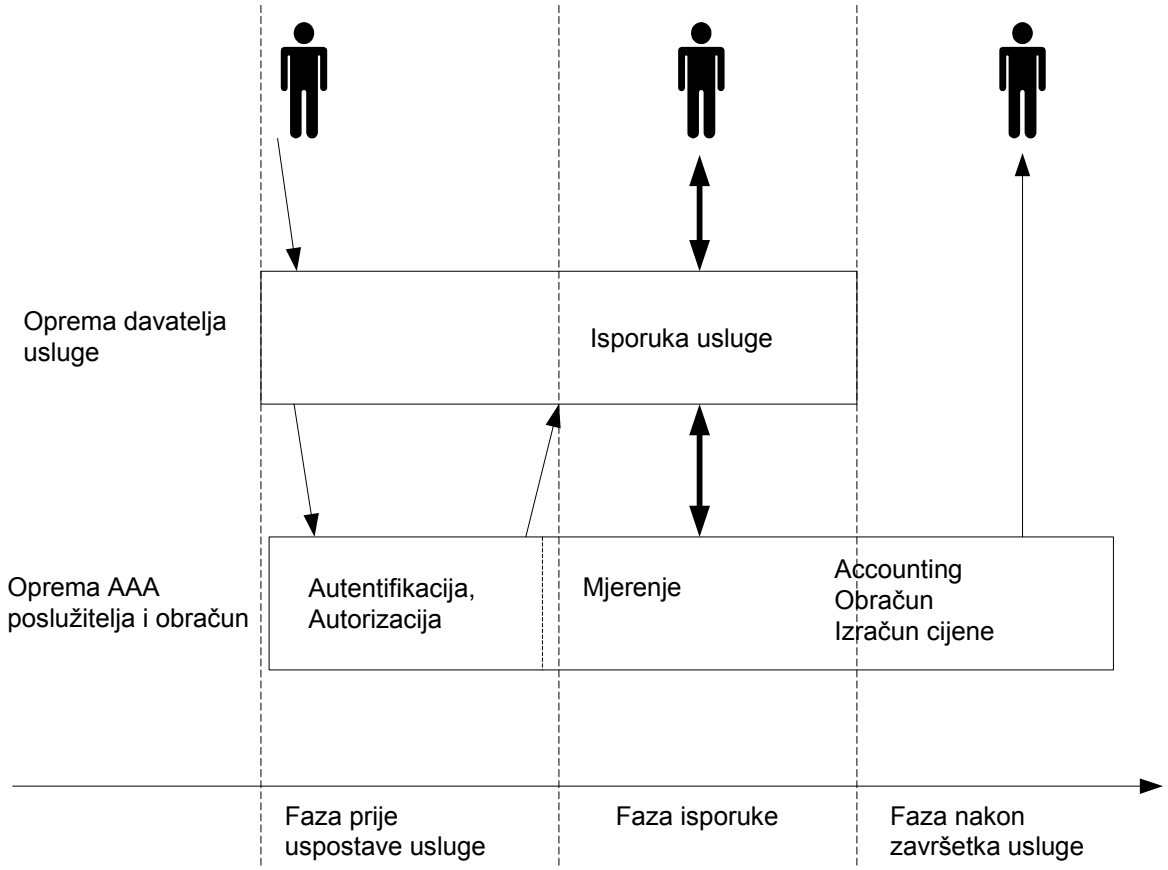
4.1.1 Sigurnost, fleksibilnost, pouzdanost i dostupnost

Da bi se to moglo omogućiti potrebno je definirati prošireni AAA sustav (Autentifikacija, Autorizacija i *Accounting*) [7]. U dodatku tradicionalnom AAA sustavu, prošireni sustav dodaje usluge kao što su podrška za politike, naplata, tarifiranje i *auditing*.

Pojednostavljen primjer logičke uspostave usluge/sadržaja prikazan je na slici 4-5.

U prvoj fazi, korisnik traži određenu uslugu. Oprema kojoj se šalje zahtjev za uslugom (npr. čvor u mreži, web poslužitelj), šalje zahtjev za autorizacijom i autentifikacijom AAA opremi (npr. AAA poslužitelj).

Ako je korisniku omogućena usluga AAA oprema šalje potvrdan odgovor opremi koja omogućuje uslugu i kreira zapis o uporabi usluge. Za vrijeme isporuke usluge, usluga se mjeri zavisno o primijenjenim politikama i mehanizmima.



Slika 4-5 Primjer uspostave usluge/sadržaja

Accounting, tarifiranje usluge i obračun se vrši u tijeku ili nakon isporuke usluge.

4.1.2 Upravljanje bilancom

Korisnik u postojećim GSM mrežama koristi istovremeno samo jednu uslugu koja se prati i naplaćuje. U budućnosti će korisnik koristiti nekoliko usluga i sadržaja koji će se pratiti odvojeno. Cjelokupni sustav mora u realnom vremenu pratiti promet i količinu novca koje je korisnik potrošio.

Praćenje potrošnje u realnom vremenu je posebno bitno u slučajevima kada korisnik ima limite na sredstva koja može potrošiti.

Primjeri limita potrošnje su slučajevi u kojima:

- korisnik postavi limite na potrošnju,
- koristi kao sredstvo plaćanja kreditne kartice limitom mjesečne potrošnje,
- korisnik zakupljuje određenu količinu usluga/sadržaja unaprijed (*prepaid*).

U ovom slučaju kada korisnik prijeđe limit automatski gubi daljnje pravo uporabe ne samo te specifične usluge nego svih usluga. Kada korisnik zatraži uslugu/sadržaj za koju nema dovoljno novca na računu, zahtjev se odbija, no ukoliko ima dovoljno novca za uporaba drugih usluga/sadržaja one su mu i dalje omogućene.

Ono što je korisniku potrebno je praćenje njegovog stanja na računu i usluga koje koristi i za koje šalje zahtjev. Sustav koji to vrši u literaturi se naziva upravljanje bilancom BM (engl. *Balance management)*.

4.1.3 Upravljanje mrežom

Sustav naplate integriran u cjelokupni sustav mobilnih paketskih mreža potrebno je nadzirati i upravljati. Općenito u IP paketskim mrežama upravljanje se najčešće koristi SNMP-om (engl. *Simple Network Management Protocol*).

Od početka devedesetih, preporuča se upotreba politika u području nadzora mreža [28]. Šira upotreba politika unutar Internet svijeta je vezana za QoS upravljanju u *Integrated* i *DiffServ* arhitekturama.

Politike definiraju moguć pristup ograničenja uporabe komunikacije u mreži i upravljanja mrežom. Uporaba politike za upravljanje mrežom ima razne prednosti pred, npr. manualnoj (uporaba komandne linije) konfiguraciji ili upravljanju preko SNMP-a [7].

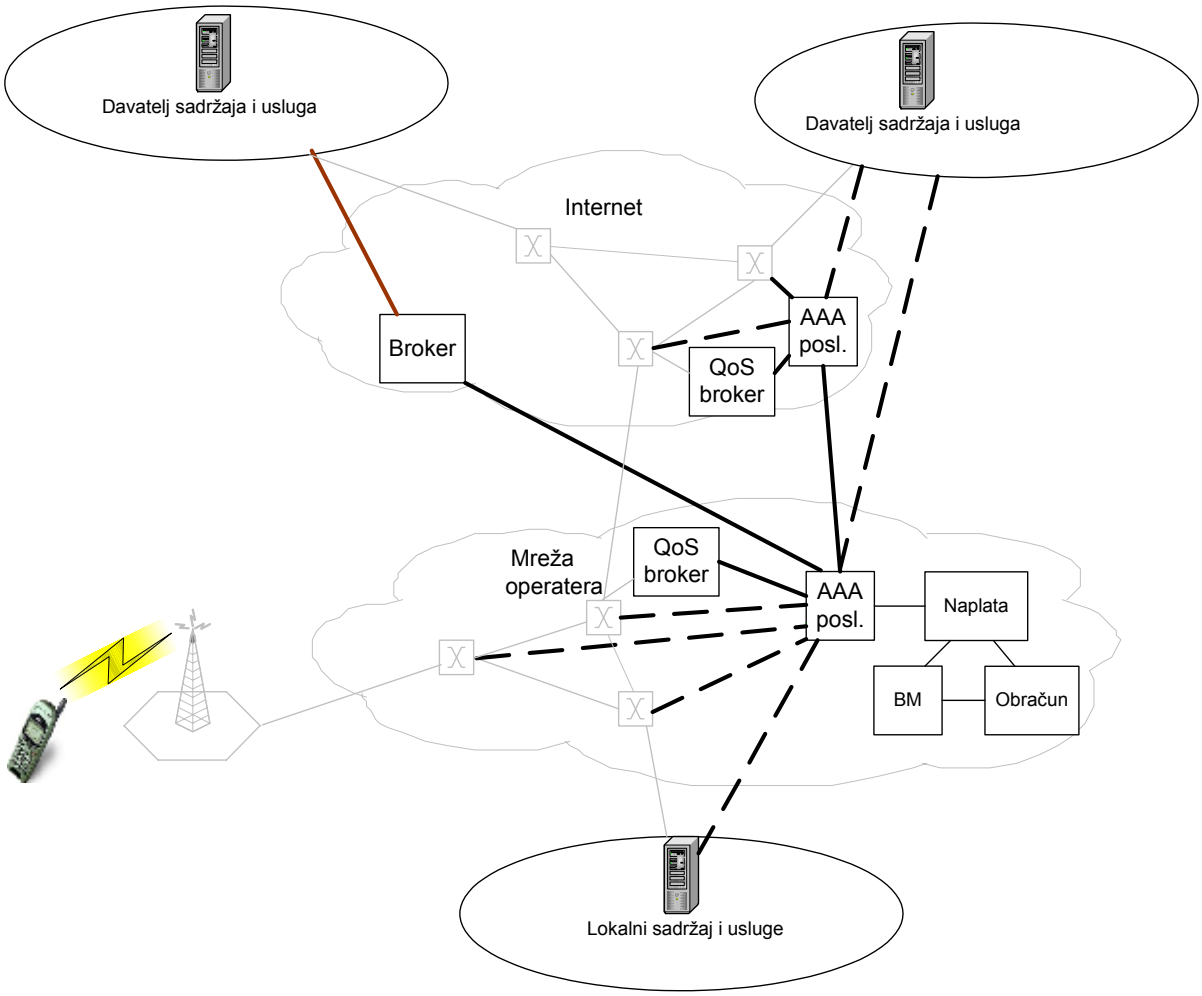
Arhitekture za uporabu politika su trenutno u diskusiji, no većina arhitektura koristi kao osnovu elemente poput točke donošenja politike PDP (engl. *Policy Decision Point*), točke provođenja politike PEP (engl. *Policy Enforcement Point*) i Spremišta politika PR (engl. *Policy* Repositiory) [10].

4.1.4 Omogućavanje QoS-a i njegove naplate

Usluge i sadržaji u mobilnim paketskim mrežama, kao što su video na zahtjev ili video konferencija zahtijevaju određenu kvalitetu usluga. Zavisno o njoj korisnik će dobiti lošiju ili bolju usluga. Proporcionalno kvaliteti usluge treba biti i njena cijena. Sustav mora omogućavati definiranje potrebnog QoS za pojedinu uslugu i njegovo tarifiranje.

4.2 Arhitektura sustava naplate sadržaja i usluga

Arhitektura sustava koji zadovoljava gore navedene zahtjeve je prikazana na Slici 4-6



Slika 4-6 Arhitektura sustava naplate sadržaja i usluga u mobilnim paketskim mrežama

Sustav naplate sadržaja i usluga je integriran u mobilnu paketsku mrežu operatera. Glavne elemente sustava čine:

- Mrežna oprema (čvorovi u mobilnoj i fiksnoj paketskoj mreži),
- Oprema za AAA,
- Tarifiranje,
- Upravljanje bilancom,
- Sustav obračuna,
- Sustav naplate,

- Broker,
- QoS broker,
- Davatelj usluge.

Svojom građom ovakva arhitektura je pogodna za različite scenarije naplate i pružanja sadržaja i usluga. Ovakva struktura je pogodna i za druge načine spajanja korisnika na zajedničku mrežu, Internet. Time se dobiva jedinstven sustav u kojem se korisnika jedinstveno autentificira i omogućuje mu se pristup određenim sadržajima, neovisno od kuda i kojim se načinom spajao (npr. ADSL-om, bežičnim LAN-om, UMTS-om...). U takvim heterogenim mrežama ključnu ulogu ima AAA sustav. AAA sustav omogućava korisniku autentifikaciju, pregovaranje i dobivanje određenih sadržaja/usluga, te praćenje i skupljanje informacija bitnih za naplatu uporabe. Ovakav sustav mora ispunjavati postavljene zahtjeve za AAA navedene u poglavlju 4.1.1.

Kako u komunikaciji između korisnika i sadržaja/usluge postoje nekoliko operatera (mobilni operater za pristup u mrežu, operater fiksne mreže, davatelj sadržaja/usluge), AAA sustavi svakog od njih moraju biti povezani. Na taj način korisnik ima jedinstveni indentifikcijski broj pod kojim se prijavljuje u mrežu. Ukoliko korisnik zatraži određeni sadržaj/uslugu od davatelja, davatelj kontaktira zadnji korisnikov AAA sustav koji mu javlja korisnikov identifikacijski broj i vrstu korisnika. Davatelj usluge prije uspostave same usluge može dobiti informaciju da li korisnik ima dovoljno novca na računu za tu uslugu. Ukoliko nema, korisnikov zahtjev se odbija. U cijelom sustavu je bitno da nitko osim krajnjeg AAA sustava (matičnog korisnikovog sustava) ne zna potpune podatke nego je predstavljen isključivo identifikacijskim brojem čime se ne narušava privatnost korisnika.

Potreba za razmjenom podataka između raznih AAA sustava je bitna iz dva razloga:

- *Roaming*,
- Višestruka autentifikacija i autorizacija.

U slučaju *raominga* korisnik se ne nalazi u svojoj mreži te AAA sustav mreže u kojoj se nalazi mora kontaktirati domicilni sustav korisnik.

Primjer višestruke autentifikacije i autorizacije su translacija korisnikove adrese (NAT) i spajanje korisnika preko WAP *gatewaya*. Ukoliko se korisnik spaja na pojedinu uslugu preko npr. WAP *gatewaya* koji se ne nalazi unutar mreže njegovog operatera, AAA sustavi izmjenjuju informacije tako da se korisnikov MSISDN pridružuje adresi WAP *gatewaya* i portu s kojeg se korisnik spaja na WAP sadržaje.

Ovakav sustav omogućava spajanje korisnika na sve dostupne sadržaje na Internetu te naplative sadržaje davatelja koji su direktno ili preko brokera povezani s mobilnim operaterom. Broker je agencija koja preuzima na sebe kontakte s davateljima sadržaja i skupljanje podataka o uporabi pojedinih sadržaja i usluga te određivanje cijene, popusta, raspored prihoda između različitih davatelja usluga. Ukoliko se broker koristi kao agregator sadržaja, on šalje skupljene podatke operateru na naplatu. U ovom slučaju operater ima ulogu izvršitelja naplate (engl. *payment provider*) te za tu uslugu dobiva određenu naknadu, komisiju. Osim toga operater naplaćuje i naknadu korisniku za uporaba pristupa u mrežu.

Za provjeru trenutnog korisnikov stanja na računu služi upravljanje bilancom. Ukoliko korisnik više nema novca na računu, odnosno nema dovoljno za traženu uslugu/sadržaj, upravljanje bilancom izdaje zahtjev AAA za onemogućivanje pristupa u mrežu ili pojedinom sadržaju.

Pojedine usluge zahtijevaju određeni QoS. Kako operater može traženi QoS omogućiti isključivo u svojoj mreži AAA sustav šalje zahtjev QoS brokeru koji komunicira s QoS brokerima ostalih mreža i dogovara QoS. Cijena usluge ovisi o trenutnom, a ne dogovorenom QoS-u.

4.2.1 Politika

Iako je arhitektura za uporabu politika još uvijek u nastajanju zbog njihovih karakteristika politike su odabrane za upravljanje sustavom.

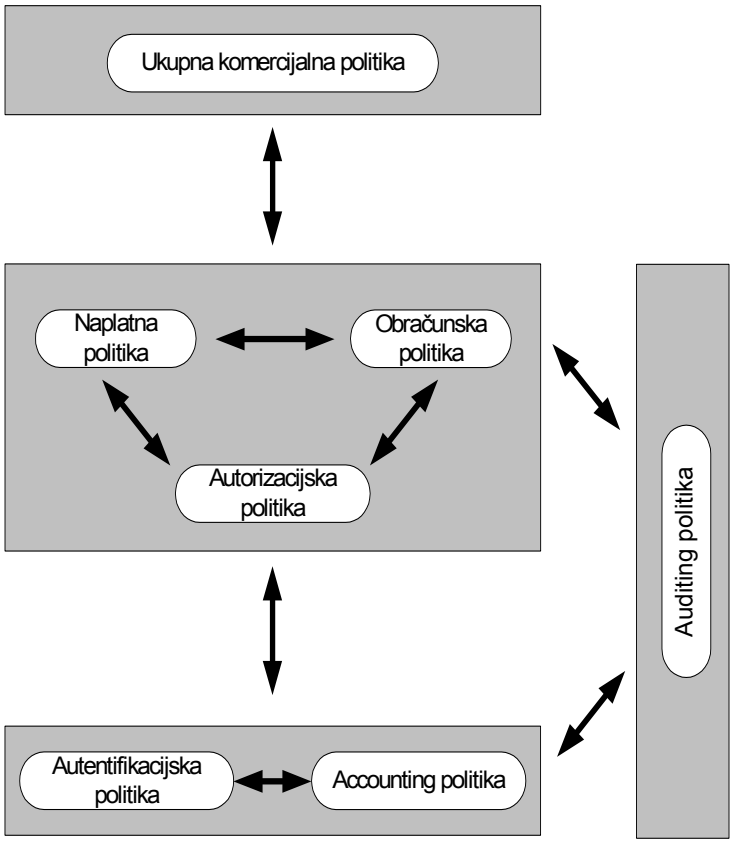
Politike definiraju cilj, put ili metodu radnje za vođenje i određivanje sadašnje i buduće odluke. Politike se u mrežnom okruženju mogu definirati kao skup pravila za administriranje, upravljanje i kontrolu pristupa mrežnim resursima.

Za izradu infrastrukture sustava, pristup zasnovan na pravilima politika je predložen od strane IRTF AAAArch istraživačke grupe. U skladu sa zahtjevima sustava proširene AAA usluge postaju nužne. Proširene AAA usluge prvenstveno zahtijevaju operateri i davatelji usluga za

ponudu transportnih usluga kao i informacijskih usluga u komercijalnom okružju. Stoga AAA usluge se mogu vrlo razlikovati, npr. zavisno o vrsti podataka koji se skupljaju ili koja shema naplate treba biti podržana. Pristup temeljen na politici nudi mogućnost odvajanja opisa usluga u formi politika od mehanizama i sistemski specifičnih informacija. Nadalje, politika omogućuju konstrukciju međudomenskih AAA usluga primjenjivih u više domenskom Internetu.

Objašnjenje veze između proširenog AAA sustava temeljenih na politici i njihovih mehanizama implementiranje usluga, grafički prikaz je prikazan na slici 4-7. Na grafu su prikazane razlike između različitih politika. Ovdje postoje dva pristupa. Jedan počinje na vrhu i prati prema dnu grafa, definirajući sustavni pristup, gdje gornja razina politike zahtjeva skup mehanizama za svoje provođenje. Npr. (1) ukupna komercijalna politika davatelja usluga/sadržaja je provedena obračunskim, naplatnim i autorizacijskim mehanizmima ili (2) naplatna politika zahtjeva provođenje mehanizam *accounting-a*. Svaki od ovih mehanizama sadrži politiku, određujući koji interni algoritam treba primijeniti. Npr. u slučaju *accounting* mehanizma, koristi se *accounting* zapis kao što je na primjer CDR ili IPDR (engl. *Internet Protocol Data Record*). O vrsti zapisa više informacija se nalazi u poglavlju 5.2.4.2. Zbog gore navedenih razloga politike nisu nezavisne.

Drugi pristup počinje od dna i prati prema vrhu grafa definirajući operacionalni pristup. *Accounting* mora biti napravljen prije naplate, a autentifikacija prethodi autorizaciji temeljenoj na autentifikaciji. *Auditing* je usluga podrške i nije neophodna za omogućavanje usluge, ali može se zahtijevati radi legalnih i regulacijskih razloga.



Slika 4-7 Model politika

Mehanizmi

Za potpunu sliku, tradicionalni AAA mehanizmi [7] i njihova poboljšanja se opisuju zasebno.

Autentifikacija

Autentifikacija definira potvrdu identiteta subjekta. Mehanizmi autentifikacije mogu se klasificirati na slijedeći način:

- Autentifikacija temeljena na poznavanju koja se zasniva na poznavanju dijeljenih tajni, kao što su PIN-ovi (engl. *Personal Identification Number*) i zaporke,
- Autentifikacija temeljena na kriptografiji koja uključuje digitalne potpise, zahtjev-odgovor mehanizme i kodove autentifikacije poruke. Korisnik ima privatni ključ kao karakteristiku,
- Autentifikacija temeljena na uporabi biometrijskih informacija kao što su otisak prsta, glas, karakteristika šarenice oka,

- Autentifikacija temeljena na sigurnim žetonima (engl. *token*) koji povezuju korisnika s pojedinim vlasništvom, npr. vlasništvo *smart card.* Ova metoda se najčešće kombinira s kriptografskim mehanizmima za prijenos informacija s žetona na autentifikator.

Autentifikacijska politika opisuje da li autentifikacija mora biti napravljena i koji autentifikacijski mehanizmi i algoritmi trebaju biti korišteni uslijed pojedinih ograničenja.

Autorizacija

Autorizacija se definira kao verifikacija ima li subjekt dozvolu obavljanja pojedine radnje na objektu ili ne. Autorizacijski mehanizmi mogu se kategorizirati u dvije glavne klase:

- Autentifikacijski temeljeni mehanizmi koji zahtijevaju autentifikaciju subjekta kao preduvjet za autorizaciju. Informacija za autorizacijsku odluku se smješta kod sustava objekta, kao što su npr. takozvane *Access* liste operacijskih sustava oblika "korisnički S ima dozvolu obavljanja radnje R na objektu O". Drugi primjer je datotečni sustav koji unaprjeđuje osnovnu listu uvjetima temeljenim na atributima objekta. "Korisniku S je dozvoljeno obavljanje akcije R na objektu O što zadovoljava uvjete C".

- Vjerodajnički temeljeni mehanizmi koji koriste vjerodajnice koje su povjerljive informacije koje korisnik drži kod sebe u autorizacijskom procesu. Vjerodajnički mehanizmi se široko koriste u M-biznisu, npr. u formi mikro plaćanja.

Autorizacijske politike definiraju koje radnje subjekta su dozvoljene za obavljanje na objektu. Autorizacijska politika može biti pozitivna (omogućavanje) ili negativna (zabranjivanje).

Formalno, autorizacijska politika može biti definirana na slijedeći način:

skup objekata O
skup subjekata S
skup tipova radnji R
Autorizacijsko pravilo: trojka (s, o, r) gdje

$s \in S, o \in O, r \in R$

$f: S \times O \times R \rightarrow$ (istina, laž)

"ako f(s, o, r) = istina", autorizacijska odluka je pozitivna. Inače subjektu se odbija autorizacija.

Ova osnovna definicija se proširuje radi uključivanja ograničenja u politikama. Ova ograničenja mogu biti postojeća stanja objekata ili univerzalni uvjeti. Ovo označava, da odluka o politici može ovisiti o vrijednosti atributa objekta ili univerzalnim uvjetima poput vremena.

Ovdje jasno postoji velika sličnost između politika i mehanizama za autentifikacijski temeljenu autorizaciju. Za vjerodajnički temeljene mehanizme vjerodajnica ima sličnu formu kao politika, gdje skup objekata ima samo jedan element koji je zapravo korisnik (može biti anoniman) koji ima vjerodajnicu.

Accounting

Accounting sustav ima dva glavna zadatka: skupljanje podataka iz sustava mjerenja (engl. *metering*) i distribuiranje podataka korisnicima *accounting* zapisa. Zbog toga, dvije vrste politika pripadaju skupljanju i distribuiranju.

Korisnik *accounting* zapisa može, zavisno o svojoj neovisnosti, specificiranoj kroz *accounting* politiku, čije informacije on treba u kojem vremenu od *accounting* sustava. Ova politika može biti događaj potaknut unutarnjim događajem, zahtjevom sustava obračuna za *accounting* zapisom ili vanjskim događajem poput završetka tekućeg mjeseca.

Za zadatak skupljanja politika mjerenja opisuje koje informacije su mjerene sustavom mjerenja i prenesene *accounting* sustavu. Jasno je da *accounting* politika utječe na politike mjerenja ili su potaknuti kroz politike mjerenja.

Naplata

Naplata uključuje najzamršenije politike i mehanizme istodobno. Dok politika naplate definira koji prometi i parametri su primijenjeni u mehanizmima naplate, mehanizmi naplate omogućuju infrastrukturu za izračun konačnih troškova za uporaba usluga s obzirom na informacije dobivene od *accounting*-a. Radi toga izraz izračun naplate (engl. *charge calculation*) se koristi samo za mehanizme. Pretpostavljajući da sveukupne komercijalne politike postoje, specifične politike pokreću davatelje usluga da zarade novac i ostanu na tržištu. U tom stadiju naplata postaje neophodna. Radi toga sama naplata se smatra politikom. Dok politike određuju koja radnja se uzima ili odgovara na događaj, naplata se smatra kao striktna politika koji omogućava davatelju dobivanje naknade za uporaba usluge, sadržaja odnosno mrežnih resursa.

Auditing

Auditing se definira kao nezavisan pregled *accounting* zapisa ili logova sustava. Korišteni mehanizmi ovise o cilju *auditing*-a. *Auditing* za naknadnu provjeru korištenih resursa i troškova korisnika se obavlja zahtjevom za zapisom loga i zapisima o statusu sesije, od strane davatelja ili treće povjerljive strane (engl. *trusted third party*).

Jednostavan mehanizam za *auditing* ispravnosti sistemskih logova je usporedba zapisa u logovima kooperativnih poslužitelja. *Auditing* u cilju detektiranja povreda sigurnosti se radi uporabom *audit* traka, neprekinutih kronoloških logova aktivnosti i događaja koji sadrže informaciju tko je to uradio, što, kada, gdje i kako. Korisnici ili subjekti uključeni u te aktivnosti mogu biti korisnici (ljudska bića), sklopovlje (usmjerivači, korisnički uređaji) ili programska podrška (operacijski sustavi, aplikacije). Pretraga može biti u formi kontinuiranog ili periodičkog u realnom vremenu praćenja traka i trenutnog odgovora odnosno reakcije, ako se dogodi neočekivani događaj ili radnja. Pretragu je moguće raditi i naknadno, ali to može umanjiti šanse za izbjegavanjem povreda sigurnosti. *Auditing* politika u ovom slučaju opisuju koji događaji radnje trebaju biti zapisani na *audit* traku i kako se one provjeravaju.

Obračun

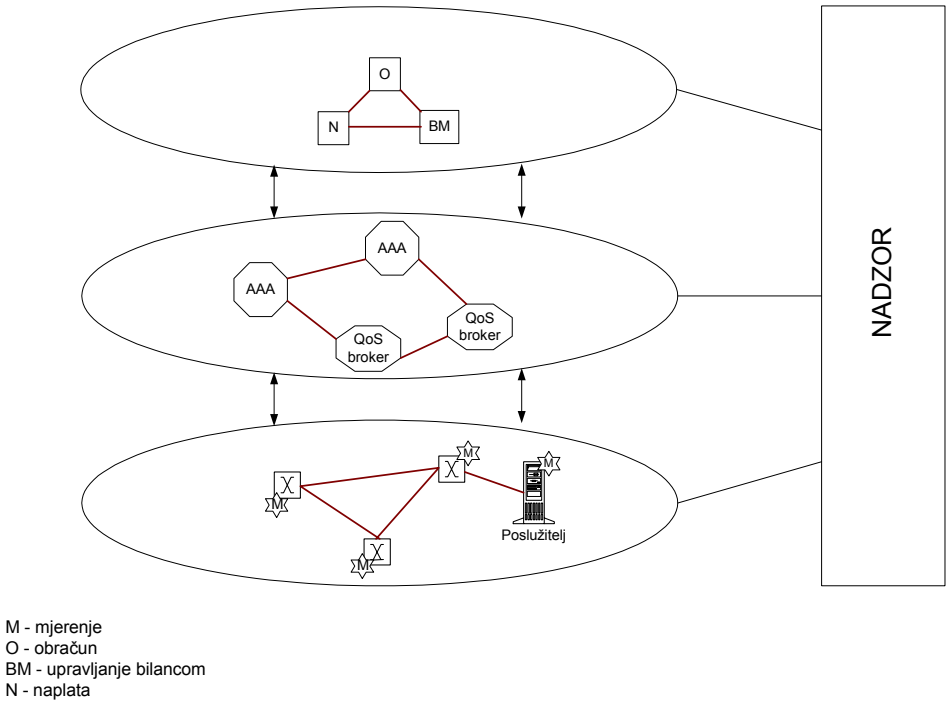
Obračun označava proces transformiranja skupljenih korisnikovih naplatnih informacija na njegov račun. On uključuje proces gdje sve naplatne informacije skupljene u vremenskom periodu, npr, jedan mjesec, za korisnika su popisane na jedan račun. Račun pokazuje količinu potrebnu za platiti, identificira metodu plaćanja odabranu ili selektiranu i prenosi se elektronički ili na papiru korisniku.

Politike obračuna se bave načinom naplate usluge/sadržaja za pojedinog korisnika, popustima, limitima potrošnje koje postavlja korisnik ili operater.

5 Gradivi blokovi sustava naplate prijenosa, sadržaja i usluga

Sustava naplate sadržaja prikazan na slici 4-6 može se podijeliti na dva dijela. Jedan dio predstavlja mreža operatera i na nju direktno spojeni ISP-i i davatelji sadržaja i usluga, dok drugi dio predstavlja broker. Broker sustav predstavlja posrednika između operatera ili između operatera i davatelja usluga/sadržaja. Broker je građen od samo nekih ili svih ostalih gradivih blokova koji se stoga u ovom modelu nazivaju i osnovnim. Tokom opisa osnovnih blokova objašnjena je i primjena pojedinih izvedbi broker sustava. Općenito o broker sustavima se govori u poglavlju 5.4. Gledajući funkcijski i po osnovnim gradivim blokovima sustav se može podijeli u četiri razine:

- Mrežni elementi i poslužitelji te sustav za mjerenje prometa i uporabe sadržaja i usluga,
- Sustav za AAA zajedno sa QoS brokerom koji omogućuju korisniku pristup na mrežu sukladno njegovim pravima i praćenje njegove uporabe sadržaja i usluga,
- Sustav za određivanje cijene, praćenje stanja računa, obračunavanje i metode plaćanja,
- Nadzor sustava (politike).



M - mjerenje
O - obračun
BM - upravljanje bilancom
N - naplata

Slika 5-1 Razine sustava za naplatu sadržaja i usluga

5.1 Mrežni elementi, poslužitelji i sustav mjerenja

5.1.1 Mrežni elementi

Mrežne elemente čine elementi mobilne paketske mreže (GPRS/UMTS čvorovi) te elementi fiksne paketske mreže (komutatori, usmjerivači, itd.). Za dizajn sustava naplate nije bitno da li su mrežni elementi dio mobilne ili fiksne mreže. Zbog toga se u arhitekturi sustava posebno ne označavaju. Kroz njih prolaze podaci između krajnjeg korisničkog uređaja i mrežnog poslužitelja ili drugog korisničkog uređaja. Njihova uloga je prenošenje tih podataka s unaprijed dogovorenom kvalitetom i vrstom prometa. Dogovor se odvija između korisnika i AAA sustava prije početka prijenosa ili je već ranije statički utvrđen. Mrežni elementi su npr.: GGSN, SGSN, usmjerivači, ATM i *Ethernet* komutatori i vatrozidi.

5.1.2 Poslužitelji

Poslužitelji su uređaji koji sadrže podatke bitne za komunikaciju u samoj mreži ili podatke i usluge zanimljive samom korisniku.

Prva skupina poslužitelja služi kao servis mrežnim elementima omogućavajući pristup korisnika u mrežu i prebacivanje jezika razumljivog korisniku na jezik mreže. U tu skupinu ulaze npr. DNS poslužitelji, DHCP, NAS.

Druga skupina poslužitelja sadrži podatke i usluge zanimljive samom korisniku. U toj skupini se nalaze HTTP, *e-mail*, FTP, *streaming* audio i video, te aplikacijski poslužitelji.

Postoji i vrsta uređaja odnosno programa koji se nalaze između ove dvije skupine. Uloga ove vrste uređaja je pomoć korisniku pri traženju i dobivanju određenog sadržaja ili usluge s poslužitelja iz gore navedene druge skupine. Takvi uređaji odnosno programi nazivaju se u stručnoj terminologiji *proxy* i *midleware.*

Proxy uređaji imaju ulogu smanjenja prometa u mreži na način da sami dohvaćaju sadržaj umjesto korisnika i isti predaju korisniku te za svaki slijedeći dohvat jedino provjeraju da li je na poslužitelju došlo do promjene sadržaja. Ukoliko nije, prethodno dohvaćeni i memorirani sadržaj isporučuju korisniku. Primjer *proxy*-a su HTTP *proxy* i real audio *proxy*.

Midleware pomaže korisniku dohvaćanjem i prilagođavanjem sadržaja do kojeg korisnik sam ne bi mogao doći zbog opreme koju ima. Dobar primjer za objašnjenje *midleware*-a je WAP *gateway*. WAP *gateway* vrši transakciju prometa između korisničkog uređaja s ugrađenim

WAP pretraživačem i HTTP poslužitelja na kojemu se nalaze korisniku zanimljive informacije. Kako WAP pretraživač ne može direktno komunicirati s HTTP poslužiteljem, on šalje svoj zahtjev WAP *gateway-u* koji taj zahtjev preoblikuje u zahtjev koji HTTP poslužitelj razumije, a rezultate zahtjeva vraća korisničkom uređaju. Primjer *midleware*-a su: WAP *gateway*-u, programi za lokaciju korisnika, platforme za M-trgovinu, itd.

5.1.3 Sustav mjerenja

Sustav mjerenja ima zadatak mjeriti vrstu i količinu prometa u mrežnim elementima, vrstu i trajanje usluge, sadržaja te uporabu usluga *midleware*-a.

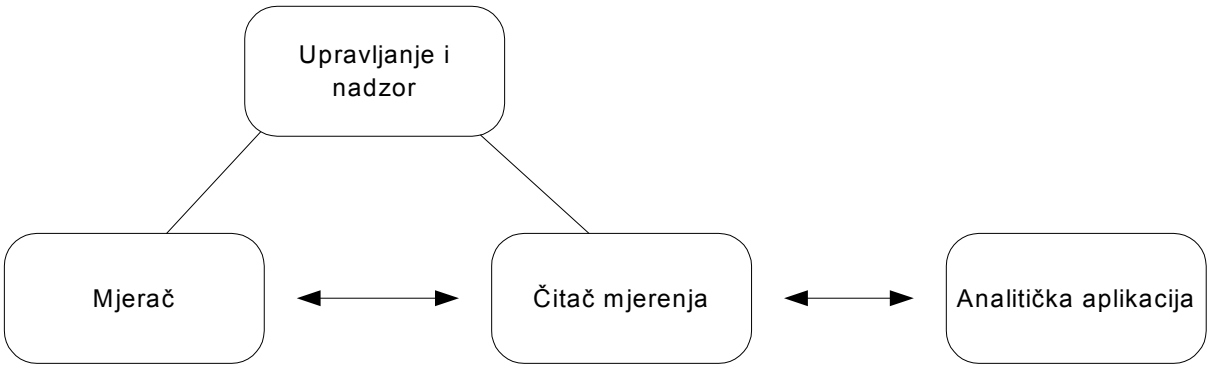
Izvedba mjerača ovisi o tome što se mjeri. Osnovna podjela načina mjerenja je slijedeća:

- mjerenje po događaju,
- mjerenje toka.

Mjerenja po događaju je mjerenje kod kojeg se prati da li se neki događaj dogodio i koliko puta. U tom slučaju nije bitno kada se dogodio, koliko je trajao i kakve je kvalitete bio. Primjeri ovakvog načina mjerenja su mjerenje koliko je puta korisnik učitao pojedinu stranicu, koliko je glazbenih brojeva "skinuo" s poslužitelja, koliko je poruka poslao, koliko je razina određene igre prešao i koliko je puta korisnik koristio uslugu određivanja lokacije.

Kod mjerenja toka je bitno koja se vrsta toka mjeri, koliko je određeni tok trajao, koja mu je kvaliteta bila, koliko je paketa preneseno, u koje se vrijeme odvijao, itd. Primjeri ovog mjerenja su mjerenje dužine praćenja određenog VoD, QoS usluge, količine podataka u Kbyte-ima, duljina trajanja uporabe pojedine informacije.

Najčešće korišteni model sustava mjerenja se sastoji od četiri elementa kako je to prikazano na slici 5-2 [31]. Primjer takvog sustava je NeTraMet [32].



Slika 5-2 Sustav mjerenja NeTraMet

- **Mjerač:** Mjerač broji stalne atribute (npr. broj byta, broj događanja, broj sekundi) i klasificira ih po pripadnosti određenim entitetima koristeći druge atribute (kao što su izvorišna i odredišna IP adresa, MSISDN, korisnička oznaka). Entitet je netko (ili nešto) tko je odgovoran za neku aktivnost na mreži ili na poslužitelju. To može biti korisnik, krajnji sustav, mreža, zavisno o granularnosti specificiranoj u konfiguraciji mjerača. Vrlo važan aspekt mjerača je agregiranje, transformacija i daljnje procesiranje snimljene aktivnosti prije nego su podaci spremljeni. Procesirani i spremljeni podaci se nazivaju "podaci o uporabi".

- **Čitač mjerača:** Čitač mjerača prenosi podatke o uporabi od mjerača tako da su oni dostupni analitičkoj aplikaciji odnosno *accounting* sustavu.

- **Upravljanje:** Upravljanje mjerenja predstavlja aplikacija koja konfigurira mjerače i kontrolira čitače mjerača. Za određivanje odgovarajuće konfiguracije za svaki mjerač i ispravnog ponašanja svakog čitača mjerača ono koristi podatkovne zahtjeve analitičke aplikacije. Često se uloge čitača mjerača te upravljanja integriraju zajedno. Informacije o konfiguraciji mjerača i čitača mjerača se dobivaju konvertiranjem *accounting* politike koja sadrži relevantne tokove, atribute i instrukcije čitaču za skupljanje podataka.

- **Analitička aplikacija:** Analitička aplikacija obrađuje podatke o uporabi na način da iz njih izvede informaciju i zapis koristan za dobivanje informacije o stanju u mreži. Na taj se dobivaju informacije koje se mogu koristiti za upravljanje mrežom, otklanjanja zagušenja i slično.

Drugi primjer sustava za mjerenje je Cisco NeTFlow. Ovaj sustav se sastoji od mjerača i kolektora toka [8].

Kod poslužitelja većina mjerača je integrirana u same aplikacije. Aplikacije spremaju periodički ili potaknute nekom promjenom podatke u svoje logove. Problem prilikom uzimanja podataka za *accounting* je u tome što svaka aplikacija ima svoj format spremanja podataka u log. Zbog toga je potrebno napraviti SDK za razvoj aplikacija. Na taj način prilikom izrade aplikacije log će biti definiran u skladu s zahtjevima *accounting* sustava. Ukoliko davatelj usluge sadržaja/usluge ne želi imati "stranu" aplikaciju na svom uređaju potrebno je instalirati program koji će npr. preko otvorenog *socket*-a komunicirati s uređajem na kojem se nalaze logovi i na taj način dolaziti do izmjerenih podataka.

5.2 AAA sustav i QoS broker

AAA sustav i s njim povezani QoS broker (u literaturi još se naziva i *bandwidth* broker) pripada središnjoj razini (Slika 5-1) sustava za naplatu sadržaja i usluga objašnjenom u ovom radu. Ova razina ima zadatak identificirati korisnika, omogućiti mu garantirane ili dogovorene usluge i sadržaje, skupiti podatke o uporabi pojedinih usluga/sadržaja, agregirati ih zavisno o korisniku i poslati slijedećoj razini koja je zadužena za naplatu.

AAA sustav korišten u ovom radu, kako je to napomenuto u poglavlju 4.1.1, ne predstavlja tradicionalni AAA sustav već prošireni AAA sustav objašnjen u radovima IETF-a. Kako je IETF namijenjen prvenstveno fiksnoj IP mreži u ovom radu AAA sustav se implementira sa HSS (engl. *Home Subscribing System*) sustavom na način kako je to predloženo u 3GPP standardima. HSS predstavlja prošireni HLR u UMTS sustavu koji služi za autorizaciju, autentifikaciju i lociranje korisnika u mobilnim mrežama.

5.2.1 Osnovna AAA arhitektura

Pretpostavka za ovu arhitekturu je višedomenska Internet topologija. U svakoj administrativnoj domeni potrebno je da se nalazi najmanje po jedan AAA poslužitelj koji komunicira s AAA poslužiteljima u drugim domenama preko standardnog protokola. Protokol mora imati mogućnost podržavanja potreba širokog spektra aplikacija koje zahtijevaju AAA funkcionalnost.

Korisnik će osim u "svojoj" mreži morati imati mogućnost uporabe usluga u mrežama drugih operatera. Tipičan primjer u mobilnim komunikaciji je *roaming*. Osim toga ponekad će se

između korisnika i davatelja sadržaja nalazi nekoliko domena. Zbog ovoga protokol mora imati mogućnost funkcioniranja i u multi-domenskom okružju.

Kako će razne aplikacije imati različite specifične zahtjeve i funkcije potrebno je postaviti specifične aplikacijske module ASM (engl. *Aplication Specific Modules*) koji mogu ponijeti jedinstvenu funkcionalnost zahtijevanu od strane svake aplikacije.

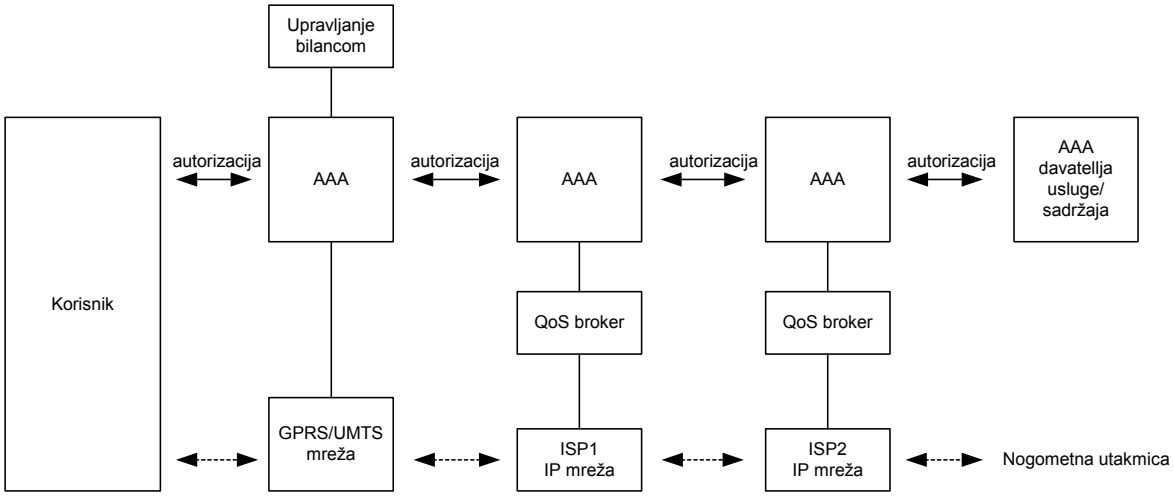
S obzirom da podaci zahtijevani od svake pojedine aplikacije za autentifikacijom, autorizacijom i *accounting*-om mogu imati jedinstvenu strukturu, standardni AAA protokol mora omogućiti enkapsulaciju nevidljivih jedinica Specifične aplikacijske informacije ASI (engl. *Application Specific Information*). Ove jedinice počinju sa standardnim zaglavljem radi omogućavanja njihovog prosljeđivanja u infrastrukturi. Kada dođe na odredište AAA poslužitelj propušta ASI jedinicu kroz svoje programsko sučelje prema odgovarajućem ASM-u za specificiranu aplikaciju.

Osnovni element AAA sustava predstavlja AAA poslužitelj koji ima mogućnost autentifikacije korisnika, rukovanje sa autorizacijskim zahtjevima i skupljanje *accounting* podataka. Poslužitelj se povezuje s ASM-om zaduženim za resurse za koje je tražena autentifikacija.

5.2.1.1 Komponente AAA poslužitelja

Autorizacijsko evaluacijsko pravilo

Prvi korak u autorizacijskom procesu je korisnikovo slanje zahtjeva za autorizacijom. AAA poslužitelj koji zaprima zahtjev ima pravila po kojima ispituje zahtjev i na osnovu kojih donosi odluku. AAA poslužitelj na osnovu zahtjeva treba imati pravilo koje će prepoznati osnovnu informaciju u zahtjevu, ali neće znati ništa o ASI-u osim gdje informacija treba biti evaluirana. Bitno je kreirati pravila koja će upućivati na elemente koji nisu podrazumijevani u trenutku kada je aplikacija bila kreirana.



Slika 5-3 Primjer poslužiteljskog zahtjeva preko više domena

Primjer za ovo je zahtjev korisnika za gledanje nogometne utakmice s udaljenog poslužitelja. Zahtjev će biti uspješan jedino u slučaju da ako je to omogućeno korisniku njegovim APN-om, ako postoji dostupna širina prijenosnog pojasa i ako ima dovoljno novca za platiti uslugu (Upravljanje bilancom, platforma za M-trgovinu). Širina prijenosnog pojasa definira se dogovorom između QoS brokera.

Aplikacijski specifični modul (ASM)

Na strani davatelja usluge/sadržaja ASM upravlja resursima i konfigurira opremom za omogućavanje autoriziranih usluga/sadržaja.

Korisnikov mobilni operator također treba ASM-ove za obavljanje specifičnih funkcija. Jedan od primjera je i povezivanje upravljanja bilancom s AAA sustavom.

U ovom sustavu ASM modul predstavlja odvojenu komponentu od AAA poslužitelja. Kao takav on mora imati mogućnost adresiranja odnosno mora biti dio globalnog imeničkog prostora.

Autorizacijski log

Za potrebe *auditing*-a poslužitelj mora imati bazu podataka u kojoj periodički sprema logove događaje. Ova baza može se koristiti i za *accounting* zahtjeva za autorizacijom.

Spremište politika

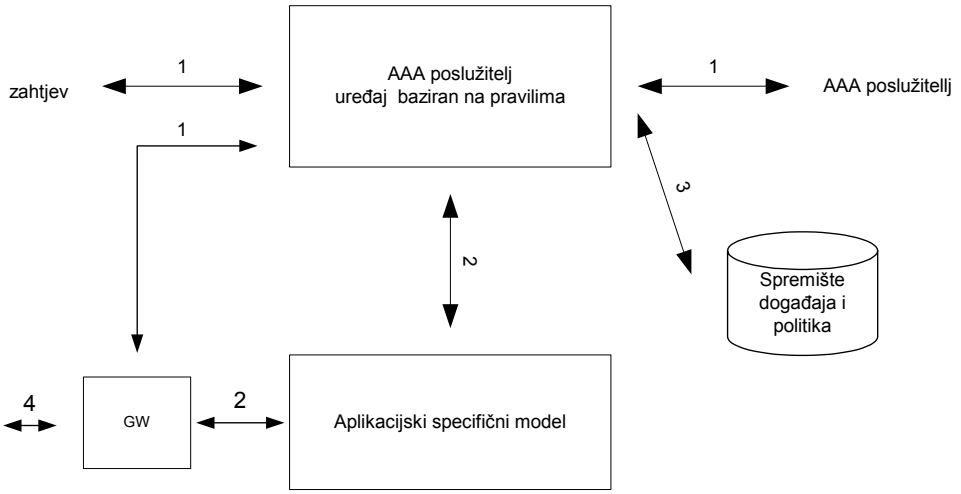
Spremište politika predstavlja bazu podataka koja sadrži dostupne usluge i resurse o autorizacijskim odlukama i politika pravilima koje ih proizvode. Kako usluge i resursi moraju imati svoju adresu i na taj način dostupni drugim AAA poslužiteljima potreban je za njih imenički prostor koji se također nalazi u ovom spremištu.

Zahtjev za prosljeđivanjem

Prosljeđivanje poruka između AAA poslužitelja se vrši zbog višedomenske prirode AAA sustava. Kako je svaki AAA poslužitelj zadužen za svoju domenu u ovom sustavu svi poslužitelji su jednako važni kao i protokol koji se komunicira između njih na istoj razini.

5.2.1.2 Osnovni model AAA poslužitelja

Slika 5-4 prikazuje model AAA poslužitelja povezanog s gore navedenim komponentama.

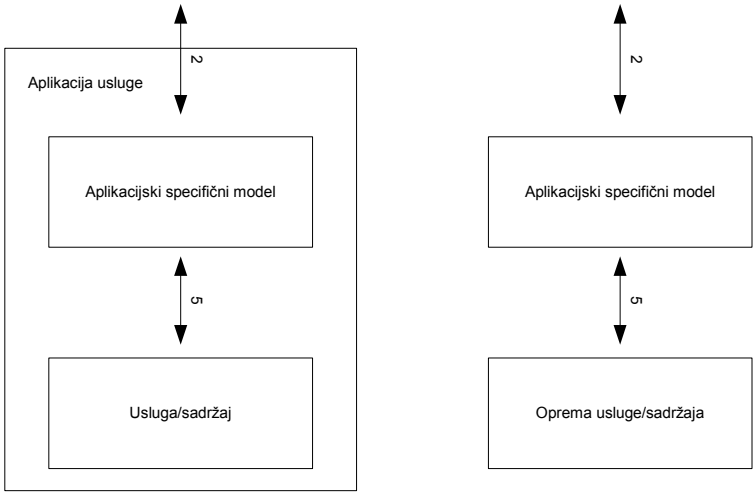


Slika 5-4 Komunikacija AAA poslužitelja

U ovom modelu korisnik slijedećeg AAA poslužitelja kontaktira AAA poslužitelj radi dobivanja autorizacije, a poslužitelj komunicira s uslugama. Zahtjev se šalje AAA poslužitelju koristeći protokol "1". Poslužitelj komunicira s uslugom koristeći protokol "2". Protokol "3" se koristi za komunikaciju sa spremištem. Protokoli "2" i "3" podržavaju globalni imenički prostor za specifične aplikacije. Za protokol "3" se najčešće koristi LDAP ili ODBC. U slučaju da se koristi postojeći protokol koji nije u skladu sa AAA komunikacijom izvodi se g*ateway* između entiteta koji šalje zahtjev i ASM-a, odnosno AAA poslužitelja. *Gateway* ima funkciju translacije protokola.

Komunikacija između ASM i usluga

Na strani davatelja usluga/sadržaja, ASM i programska podrška koja omogućuje uslugu mogu biti povezani u pojedinu servisnu aplikaciju. U ovom slučaju sučelje između njih je sučelje programske podrške. Ako se usluga nalazi u opremi izvan ASM, kao što je na primjer usmjerivač u QoS broker aplikaciji, tada ASM komunicira s uslugom koristeći isti protokol. Ove dvije mogućnosti su prikazane na slici 5-5. U oba slučaja komunikacija između ASM-a i usluge je označena brojem 5. Točan protokol ovisi o vrsti usluge.

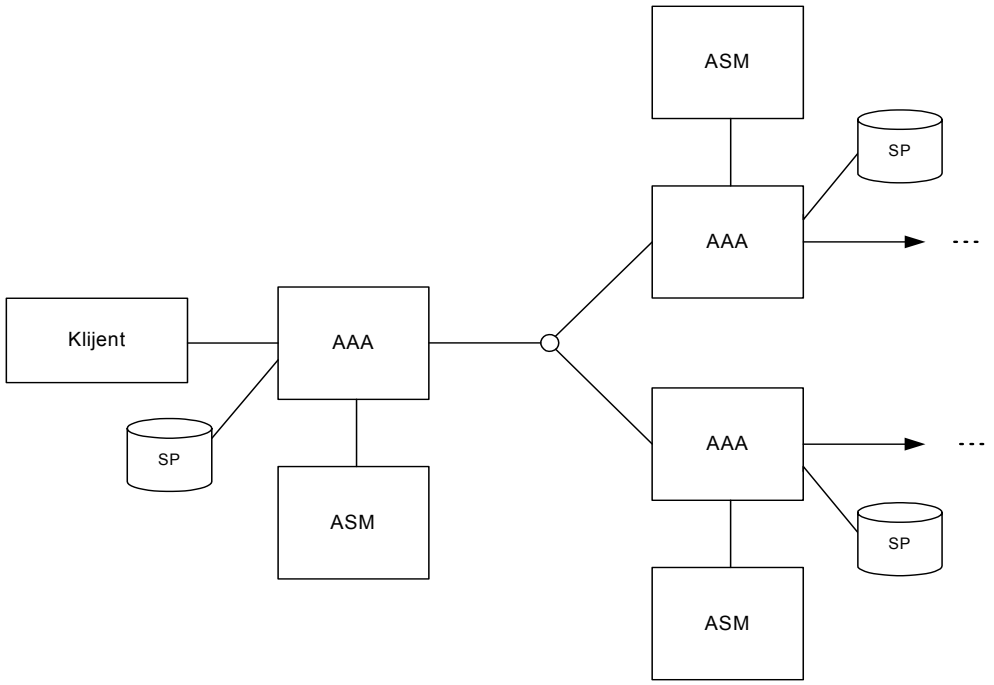


Slika 5-5 ASM - usluga komunikacija

Multi-domenska arhitektura

Moduli AAA poslužitelja mogu koristiti tip "1" komunikacije za međusoban kontakt za izvršavanje dijelova zahtjeva.

Slika 5-6 prikazuje mrežu AAA poslužitelja u različitim administrativnim domenama koji komuniciraju koristeći tip "1" komunikacije.



ASM - Aplikacijski specificirani modul
SP - Spremište politika

Slika 5-6 Multi-domenska arhitektura

5.2.2 AAA mobilnog IP-a

Ideja mobilnog IP-a specificirana u [5] je u tome da korisnik bez obzira na promjenu fizičkog boravišta zadržava svoju IP adresu. Mobilni uređaj mora komunicirati moći s drugim uređajima nakon promjene točke sloja povezivanja kojom se povezuje na Internet, bez promjene svoje IP adrese. Mobilne paketske mreže i njihovi uređaji se odlično uklapaju u ovu ideju. Na ovaj način svaki korisnik bio u svojoj mreži ili u *roamingu* koristi istu IP adresu. AAA sustav ima ulogu da mu to omogući. Zbog primjenjivosti u mobilnim paketskim mrežama u ovom radu pobliže objašnjavamo princip mobilnog IP te njegovo povezivanje s AAA sustavom.

Elementi mobilne IP arhitekture su slijedeći:

Mobilni čvor

Krajnji uređaj ili usmjerivač koji mijenja točku svog pristupa s jedne mreže ili podmreže u drugu. Mobilni čvor može promijeniti svoju lokaciju bez promjene IP adrese te nastaviti komunicirati s drugim Internet čvorovima.

Domaći agent

Usmjerivač u matičnoj mreži mobilnog čvora koji tunelira pakete radi prijenosa do mobilnog čvora koji se trenutno nalazi izvan matične mreže i održava trenutne lokacijske informacije za mobilni čvor. Slično ulozi HLR-a u mobilnim paketskim mrežama.

Strani agent

Usmjerivač ili mobilni čvor posjećene mreže koji omogućava usluge usmjeravanja mobilnom čvoru prilikom registriranja. Strani agent uzima tunelirane podatke i predaje ih mobilnom čvoru kojem su podaci njegovog domaćeg agenta bili namijenjeni. Za pakete koje je poslao mobilni čvor, strani agent može služiti kao predodređeni usmjerivač za registrirane mobilne čvorove.

Primalac

Čvor dizajniran da omogući servisno sučelje između klijenta i lokalne domene.

Strana domena

Administrativna domena, koju posjećuje mobilni IP klijent i koja sadrži potrebnu AAA infrastrukturu za provođenje neophodnih radnji koje omogućuju mobilnu IP registraciju. Iz kuta stranog agenta strana domena je lokalna domena.

Lokalna domena

Administrativna domena koja sadrži AAA infrastrukturu izravnog interesa za mobilnog IP klijenta kada se on nalazi izvan svoje domaće domene.

Mobilni čvor dobiva dugotrajnu IP adresu u svojoj domaćoj mreži. Ova adresa se administrira na isti način kao fiksna adresa pridjeljenja stacionarnom uređaju. Kada se nalazi udaljen od svoje domaće mreže "briga o adresi" mu se pridjeljuje i predstavlja trenutnu točku pristupa mobilnog čvora.

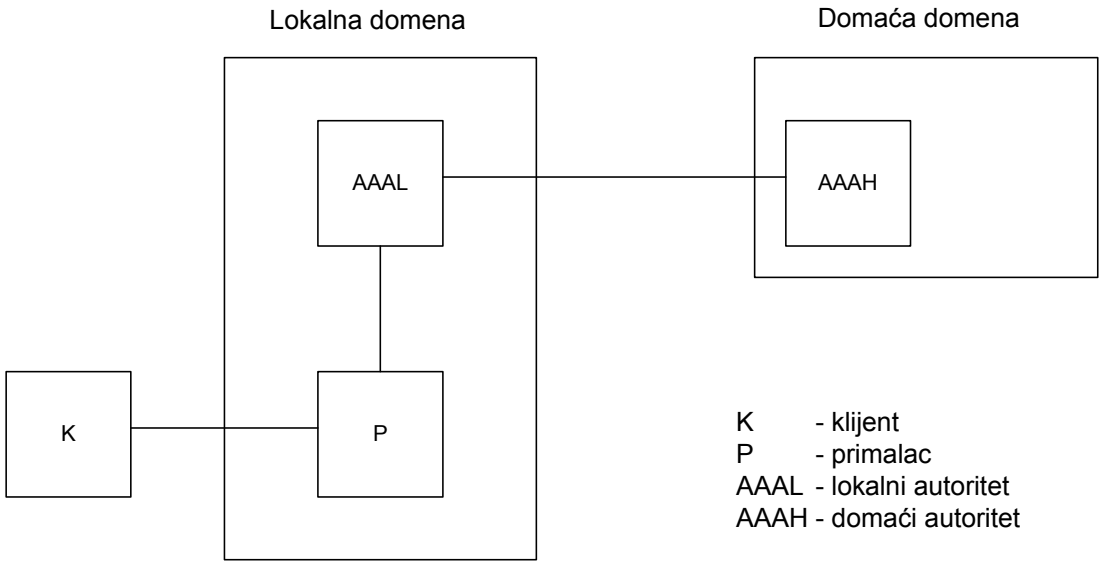
Priključna točka tunela prema mobilnom čvoru za pakete proslijeđene mobilnom čvoru dok se nalazi izvan domaće mreže se naziva briga o adresi. Protokol može koristiti dva različita tipa brige o adresi: "briga o adresi stranog agenta" koja je adresa stranog agenta s kojom je

mobilni čvor registriran i "ko-locirana briga o adresi" koja je izvana dobivena lokalna adresa kojoj je mobilni čvor priključen jednim od svojih mrežnih sučelja.

AAA poslužitelji identificiraju korisnike koristeći NAI (engl. *Network Access Indentifier*) [2]. Mobilni čvor može identificira sam sebe uključujući NAI zajedno s mobilnim IP registracijskim zahtjevom [35]. NAI ima oblik korisnik@područje, (engl. user@realm).

5.2.2.1 Osnovni model

Unutar Interneta, klijent koji pripadna jednoj administrativnoj domeni (domaća domena) često treba sadržaje i usluge koje omogućuje druga administrativna domena (strana domena) [31]. Agent u stranoj domeni što zaprima (primalac) korisnikov zahtjev traži klijenta vjerodajnice da ga može autentificirati prije nego mu omogući pristup resursima. Vjerodajnice mogu biti nešto što strana domena razumije, ali u većini slučajeva one su razumljive jedino domaćoj domeni te mogu biti korišteni za postavljanje sigurnih kanala s mobilnim čvorom.



Slika 5-7 AAA poslužitelji u domaćoj i lokalnoj domeni

Kako u većini slučajeva primalac nema dovoljno podataka potrebnih za završetak transakcije, on se konzultira s autoritetom (obično u istoj stranoj domeni) radi dobivanja dokaza o valjanosti klijentovih vjerodajnica. Kako se primalac i autoritet nalaze u istoj domeni, očekuje se da imaju uspostavljen siguran komunikacijski kanal.

Ako lokalni autoritet (AAAL) nema dovoljno informacija za verifikaciju vjerodajnica on pregovora oko verifikacije s vanjskim autoritetom. Između njih također je potreban siguran

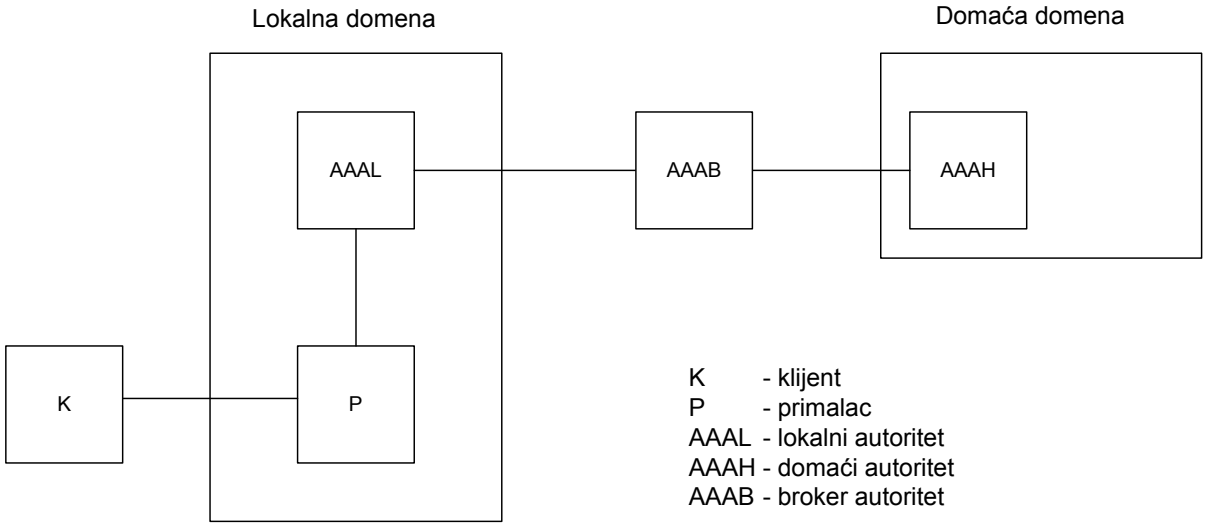
komunikacijski kanal zbog sigurnog pregovaranja o autorizaciji koja bi korisniku omogućila pristup nekim ili svim uslugama. Autorizacija određenih usluga i sadržaja najčešće zavisi o sigurnoj autentifikaciji korisnikovih vjerodajnica.

Kada lokalni autoritet odobri autorizaciju pojedinih usluga i obavijesti o tome primaoca o uspjehu pregovora, primalac može omogućiti korisniku pristup traženim resursima.

Kako vjerodajnice mobilnog čvora moraju ostati zapamćene primalac, lokalni autoritet ili bilo koji drugi čvor prema domaćem autoritetu ne smije imati mogućnost učenja bilo koje informacije koja mu može omogućiti rekonstrukciju ili ponovnu uporabu vjerodajnica.

5.2.2.2 Broker model

Slika 5-7 prikazuje konfiguraciju u kojoj lokalni i domaći autoritet dijele povjerenje. U slučaju veze s velikim brojem domena i AAA autoriteta, broj potrebnih sigurnih veza između njih raste kvadratnom progresijom. Zbog toga se pristupa uporabi brokera koji funkcionira kao *proxy* između njih. Na taj način svaki autoritet treba imati samo jednu vezu prema AAA brokeru.



Slika 5-8 Povezivanje AAA poslužitelja koristeći broker

AAAB na slici 5-8 predstavlja broker poslužitelj. Broker omogućuje sigurnosnu i središnju točku kontakta za mnoge operatere.

5.2.3 Politika u AAA okruženju

U ovom poglavlju će biti objašnjeno uporaba politika u AAA okuženju te njihov utjecaj na odvijanje transakcije. AAA poslužitelj upravlja spremištem politika. Da li će zahtjev biti prihvaćen ili odbijen ovisi o procjeni pokretačke politike (engl. *Driving policy*). Općenito AAA poslužitelj mora komunicirati s drugim AAA poslužiteljima u cilju potpunog prihvaćanja ili odbijanja zahtjeva. Ovo se događa kada je politika koja se procjenjuju distributivna politika.

5.2.3.1 Definicija AAA politika

Politike su skup pravila za administriranje, upravljanje i kontrolu pristupa mrežnim resursima [22]. U osnovnoj AAA strukturi politike se objašnjavaju kao pravila politika. Jednostavno pravilo politike sastoji se politike stanja i politike radnje. Politika stanja se procjenjuje i zavisno je o da li je politika radnje poduzeta ili ne. Stroj temeljen na pravilu RBE (engl. *Rule Based Engine*,) evaluira politiku stanje radi donošenja odluke o politici. Ovisno o izlazu će RBE izvršiti politiku radnje.

Osim politika potrebno je definirati zahtjev i stroj temeljen na pravilu:

- **Zahtjev**

  Zahtjev je bilo koja vrsta poruke koja traži uslugu. Postoji mnogo zahtjeva i načina slanja zahtjeva usluzi kao što su npr. *push*, *pull* ili agent model objašnjeni u [23] Zahtjev će izvršiti neku akciju i vratiti odgovor.

- **Stroj temeljen na pravilu**

  Stroj temeljen na pravilu može biti sposoban procesirati pravila danih tipova s malo ili bez znanja o aplikaciji. U drugim slučajevima stroj temeljen na pravilu može biti specificiran za pojedinu aplikaciju. Generički uređaj može pozvati pomoć ASM-a za procjenu pojedinih politika.

  Politika odluke može rezultirati kao istina ili laž, što naknadno rezultira radnjom koja označava vrijednost atributa, pretrage ili generira slijedeću politika ili poziva specifičnu funkciju. Ako je rezultat pravilo politike, onda njegovo stanje treba utvrditi za određivanje slijedeće radnje. Ovo pravilo može biti parsano lokalno ili može biti proslijeđeno drugoj AAA usluzi.

Lokacija politika se može podijeliti u tri kategorije:

- Distribuirane politike,
- Lokalne politike,
- Udaljene politike.

Tipovi politika

Osim osnovnih politika sustava navedenih u poglavlju 4.2.1 kao što su: autentifikacijska, *accounting*, obračunska, naplatna, *auditing;* za osnovnu AAA arhitekturu bitne su:

- **Konfiguracijska politika**

  U mnogo slučajeva pravila politika i atributi moraju biti predstavljeni u aplikacijskom formatu da mogu bit procesirani na drugom uređaju. Konfiguracijska politika određuje kako se rezultati jedne politike evaluacije se translatiraju u aplikacijski specifičnu formu tako ih servisna oprema može evaluirati.

- **Pokretačka politika**

  Prva politika koja se zahtjeva i pretražuje u spremištu politika nakon primitka zahtjeva.

- **Registracijska politika**

  Registracijska politika rukuju s načinom kako su korisnici i drugi entiteti registrirani u mreži i kako se vjerodajnice kreiraju i distribuiraju. Primjer registracijske politike je politika zaporke: kako često se zaporka obnavlja, koliko znakova mora imati, postoji li rječnička provjera itd.

- **Sigurnosna politika**

  Sigurnosni politika upravlja zahtjevima za sigurnu transakciju. Ovaj tip politika kreira dodatne zahtjeve za gore navedene politike. Npr. može zahtijevati da se stroga autentifikacija uvijek koristi i da svi podaci koji putuju mrežom moraju biti kriptirani.

- **Politika dodjeljivanja usluge**

  Jedan od uvjeta autorizacije za uslugu može zavisiti o trenutnoj uporabi ili dostupnosti usluge.

- **Politika specificiranja usluge**

  Ovaj tip politika specificiran od strane korisnika i određuje koja usluga/sadržaj je određena pod kojim uvjetima. Npr. korisnik može postaviti zahtjev da gleda prijenose nogometnih utakmica samo ako njihova cijena ne prelazi 10 kn.

Komponente politika

Politike su napravljene od nekoliko komponenata. Ono što definitivno pripada bilo kojoj politici je:

- **Politika radnja**

  Nešto što efikasno govori nekom uređaju da uradi nešto. Ovo može biti parametar koji je promijenjen ili naredba dana ASM-u.

- **Atribut politike**

  Bilo koji podatkovni element koji može biti procesiran politika pravilom.

- **Politika stanje**

  Boolov izraz kao što je npr. "(cijena_skijanje < 10) AND disciplina=slalom"

- **Politika pravilo**

  Gotovo sve što može biti opisano s if…then…else uvjetom.

5.2.3.2 AAA poslužitelj i pokretačka politika

U ovom poglavlju je prikazan detaljnije AAA poslužitelj objašnjavajući pokretačku politiku. Prikaz osnovnog modela AAA poslužitelja nalazi se na slici 5-4. Kada procesira AAA transakcije, AAA poslužitelj ne zna koju specifičnu uslugu korisnik želi. Informacije se

nalaze u pokretačkim politikama. Općenito postoji jedna pokretačka politika po usluzi za svaki tip poruke koji može biti primljen preko bilo kojeg sučelja.

Slika 5-9 prikazuje detaljniji prikaz osnovnog AAA poslužitelja i njegove veze s drugim entitetima kao što su ASM-ovi, spremište politika i log događaja.

Komunikacija između AAA poslužitelja i drugih entiteta, objašnjena je u poglavlju 5.2.1.2.

Središnji dio AAA poslužitelja je kontrolni modul. Kontrolni modul procesira AAA transakcije. Transakcije nastaju zahtjevom poruke komunikacijskog tipa "1" od strane drugog AAA poslužitelja ili tipa poruke tipa "2" od ASM-a. Poruke komunikacijskog tipa 1 se procesiraju na razini protokola generičkim pokretačem AAA protokola. Poruke tipa 2 se procesiraju modulom "ASM sučelje".

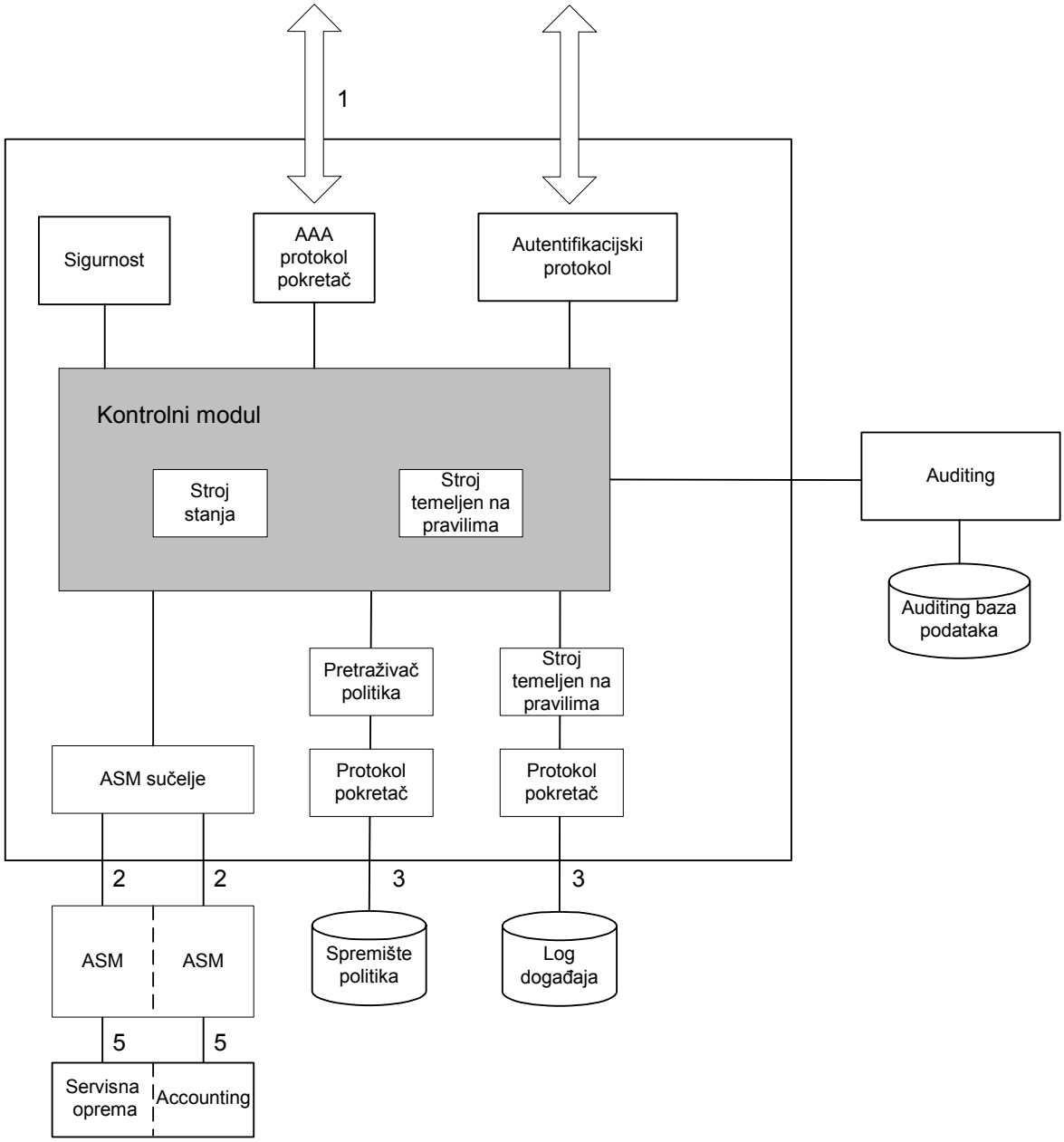
Kada kontrolni modul primi poruke tipa 1 i 2 što pripadaju novoj transakciji, on procesira poruku u skladu sa pravilima u pokretačkoj politici.

AAA poslužitelj je između ostalog i politika uređaja. Politike koje se evaluiraju mogu biti primljeni preko generičkog AAA protokola ili zahtijevani preko politike pretraživača. Politike se nalaze u spremištu politika. Pretraživač politika koristi pretraživačke protokole za pretraživanje i zahtijevanje politika koje mogu biti baza podataka ili imenički servis.

Sigurnosni mehanizmi se obavljaju pomoću biblioteke sigurnosnih funkcija koje omogućuje sigurnosni modul.

Kada procesira AAA transakcije, AAA poslužitelj ne zna koju specifičnu uslugu korisnik želi. Informacije se nalaze u pokretačkim politikama. Općenito postoji jedna pokretačka politika po usluzi za svaki tip poruke koji može biti primljen preko bilo kojeg sučelja.

Funkcionalni blok dijagram AAA poslužitelja je prikazan na slici 5-9.



Slika 5-9 Funkcionalni blok dijagram AAA poslužitelja

Pokretačka politika specificira ponašanje AAA poslužitelja. Pokretačka politika u SP i ASM-ovima imaju zavisnu relaciju, zbog toga što politike mogu upućivati na ASM radi rješavanja dijela politika. Ovo znači da sadržaj PS-a i ASM-a određuju ponašanje AAA poslužitelja. Djelomična zamjena sadržaja PS-a i ASM-a rezultirati će drugačijim AAA poslužiteljem. Ova mogućnost treba biti dinamički podržana dajući tako mogućnost administratoru da prilagodi ponašanje AAA poslužitelja bez potrebe za ponovnim kompiliranjem AAA poslužitelja.

5.2.4 Accounting

Accounting opisuje skupljanje podataka o uporabi pojedinih resursa. Ovo uključuje kontrolu prikupljanja podataka (mjerenje), prijenos i spremanje *accounting* podataka. Za slijedeći korak, podaci izmjereni za naplatu moraju biti pridruženi korisniku koji je inicijator toka i kupcu koji je odgovoran za plaćanje. Za pokretanje *accounting*-a, korisnik ili udaljeni operator moraju biti autentificirani i autorizirani. Accounting proces se konfigurira *accounting* politikom.

Većina postojećih *accounting* sustava je usko specijalizirana uz određeno područje, kao što je npr. skupljanje informacija o duljini trajanja pojedinog GSM telefonskog razgovora, količina prenesenih podataka u GPRS ili fiksnoj mreži, broj prenesenih SMS poruka. Osim toga većina informacija poput uporabe WAP usluge ili spajanja na Internet biranom linijom naplaćivali su se mjerenjem vremena uporabe usluga definiranjem specijalnog broja na kojeg je korisnik zvao za dobivanje tražene usluge. Ovakav sustav zbog svoje nefleksibilnosti ne može odgovarati zahtjevima naplate pojedinih sadržaja i usluga u mobilnim paketskim mrežama.

Zadnjih godina većina operatera za naplatu sadržaja se okrenula rješenjima M-trgovina kojima korisnik kupuje određene sadržaje, no ovo rješenje nije efikasno u području naplate *streaming* tipova sadržaja, QoS i sličnih usluga za koje se ne može unaprijed odrediti cijena.

Drugo rješenje koje se koristi je tzv. IP medijacija.

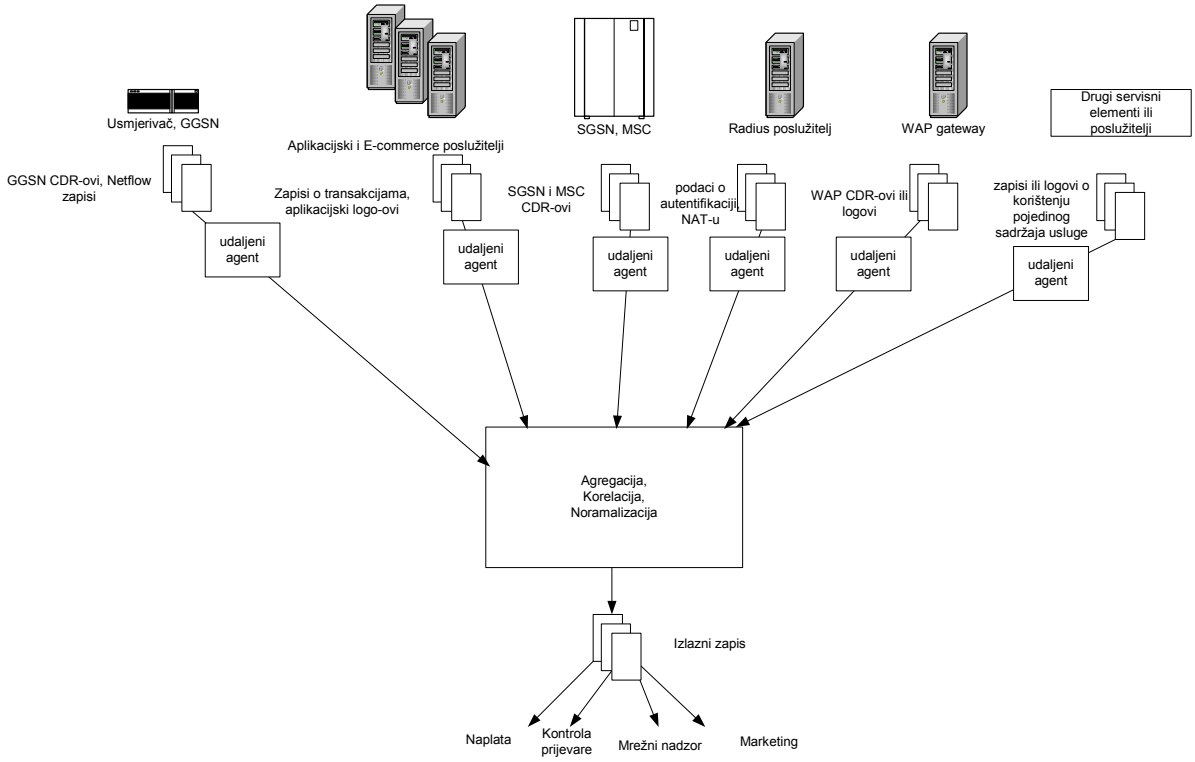
5.2.4.1 IP medijacija

IP medijacija (engl. *IP mediation*) je sustav u kojem se skupljaju podaci s raznih uređaja unutar mreže te zajedno koreliraju i obrađuju u oblik prikladan za naplatu i obračun.

Slika 5-10 prikazuje način na koji funkcionira IP medijacija. IP medijacija se sastoji od dva glavna dijela:

- Udaljenog agenta koji prikuplja podatke od raznih mrežnih elemenata i poslužitelja,
- Centralnog sustava koji podatke korelirira, agregira i zapisuje u izlaznom formatu koji je prikladan za dalju obradu. Osim toga centralni sustav i nadzire rad agenta.

Izlazni zapis se prenosi sustavu naplate, sustavu za nadzor prevare, sustavima za praćenje stanja prometa u mreži, marketingu i ostalim elementima koji zapisi mogu koristiti. Zapise i logove stvara sustav mjerenja koji se razlikuje od tipa do tipa opreme te proizvođača. IP medijacije su modularno razvijene na način da većinom podržavaju glavne formate (Npr. G-CDR-ovi, S-CDR-ovi, MOC-ovi, *Netflow* podaci, itd.), a za specifične se prilagođavaju prilikom implementacije. Agenti su većinom SDK rješenja koja se direktno ubacuju u rubne mrežne elemente (npr. na prijelazima prema drugim domenama) i poslužitelje i koja uzimaju informacije iz logova ili zapisa sustava mjerenja. Agenti su u nekim slučajevima i sami dio sustava mjerenja.



Slika 5-10 IP medijacija

Drugi način je da se instalira stroj koji je povezan s uređajem na kojem se nalaze podaci. Između ta dva stroja se obično otvora *socket* i "push" metodom se podaci prebacuju agentu koji se nalazi na instaliranom stroju. Prednost ovog rješenja je sigurnost davatelja usluge/sadržaja.

Glavna uloga centralnog sustava je koreliranje informacija u cilju dobivanja potpune identifikacije korisnika i količine uporabe pojedine usluge. Primjer za koreliranje je kada korisnik prati *streaming* video. Iz informacija od *streaming* poslužitelja, usmjerivača, RADIUS poslužitelja koji je korisniku dodijelio IP adresu i GGSN čvorova može se saznati o

kojoj je usluzi riječ, koji ju je korisnik koristio (translacija IP adrese u MSISDN i obratno), koliko dugo, koliku količinu podataka i s kojim QoS je prenio. Kako se agenti nalaze fizički udaljeni od centralnog sustava veza s njima se uspostavlja iznajmljenim ili VPN linijama. Za upravljanje agentima se koriste protokoli za udaljeni rad poput CORBA-e i RMI-a.

IP medijacija je pasivni sustav koji isključivo skuplja i obrađuje podatke, kao takav funkcionira samo u jednom smjeru, od usluge/sadržaja prema naplati odnosno sustavu obračuna. On u sustavu naplate sadržaja i usluga ne može funkcionirati samostalno zbog nemogućnosti kontrole pristupa ovisno o informacijama o korisniku koje ima operater. Na taj način sustav ne daje povratnu informaciju davatelju usluge o npr. tome da li korisnik ima još dosta novca na računu za uporabu usluge/sadržaja.

Većina sustava za IP medijacija koje sam upoznao tokom rada na ovom projektu podrazumijevaju dobivanje korisničke informacije isključivo koreliranjem informacija. U tu skupinu ulaze sustavi renomiranih proizvođača sustava medijacije poput: Intec, OpenNet, HP-a. Primjer za ovakvu korelaciju je sustav u kojem se korisnik spaja na sadržaj udaljenog davatelja usluge preko GPRS sustava operatera uz uporaba NAT-a. Pretpostavimo da IP adresu korisnika dodjeljuje GGSN iz svoga skupa adresa. U ovom slučaju od osnovne MSISDN ili IMSI informacije po kojoj operater prepoznaje korisnika imamo nekoliko transformacija do konačne IP adrese s koju davatelj usluga vidi kao adresu s koje mu je upućen zahtjev. Za povezivanje ove dvije informacije potrebno je korelirati G-CDR (GGSN CDR koji zna IMSI i IP adresu koju je dodijelio korisniku) i informaciju dobivenu s NAT-ova koji su vršili translaciju adresa. Nakon što se sve te informacije međusobno koreliraju sustav zna točno o kojem se korisniku radi. Na ovaj način dok se ustanovi o kojem je korisniku riječ on može koristiti dio usluga bez provjere stanja na njegovom računu.

Ovaj problem se rješava upotrebom AAA sustava koji prije međusobno komunicirajući znaju ID korisnika i kojem operateru pripada. Na taj način davatelj usluge/sadržaja upitom AAA sustavu dolazi do informacije da li je korisnik autoriziran za uporaba tražene usluge. Nakon toga uporabi resursa dodjeljuje korisnikov ID. Ovu informaciju imaju i ostali uređaji u mreži koji prate uporabu usluga. Primjer IP medijacija koje podržavaju ovo rješenje su: Tertio i Telensciences koji ima i vlastito rješenje AAA poslužitelja.

5.2.4.2 IPDR

IPDR (engl. IP Data Protocol) je jedan od formata zapisa informacije o uporabi pojedine usluge koji predstavlja izlazni format *accounting* sustava. Ovaj format zapisa je nastao kao težnja ipdr.org neprofitne organizacije koja pokušava specificirati format podataka koji će imati fleksibilnu strukturu i moći opisati atribute uporabe skupljenih sustavom medijacije i zahtijevanim od strane sustav obračuna.

Osim kao izlaz iz sustava medijacije ovaj format se može koristiti kao izlazni zapis o uporabi pojedinih usluga u pojedinim mrežnim elementima.

IPDR zapis [19] mora moći karakterizirati bilo koji tip korištenja koji može biti skupljen od strane IP mreže, odnosno aplikacijskog poslužitelja. Postoji 5 zajedničkih atributa u tipičnom IPDR zapisu. Te komponente su "tko, što, gdje, kada i zašto" vrijednosti koje opisuju pojedino uporaba određene usluge. Kako se u engleskom ove komponente prevode kao "*who*, *what*, *where*, *when*, *why*" često se naziva i 5w. Svaka od njih je dolje ukratko objašnjena:

- Tko – odgovornost za uporaba usluge
  Korisnikov ID,

- Kada
  Vrijeme završetka ili vrijeme događaja,

- Što
  Usluga,
  Mjerenja uporabe/kvanti
  Npr: Bytevi, paketi, tok, klikovi, transakcije, vrijeme trajanja itd.
  QoS mjerenja
  Informacija o stanju
  Druge informacije o stanju transakcije ili trenutnom stanju (Start vrijeme)

- Gdje
  Kontekst
  Identifikator izvora
  Identifikator odredišta
  Identifikator servisnog elementa na kojem je zapisan,

- Zašto
  Triger tip (npr. razlog zašto mreža i servisni elementi izdaju ovaj podatak)

U dodatku na "5w" definiranih gore, svaki zapis može uključiti referente točke na druge IPDR zapise koji sadrže određene informacije o uporabi ili sadrže informaciju o uporabi koja je korištena za kreiranje danog zapisa.

5.2.4.3 Accounting politike

Accounting politike opisuju pravila za generiranje, transport i spremanje podataka o *accounting*-u. One se mogu izmjenjivati između AAA instanci. *Accounting* politike konfiguriraju *accounting* proces. Politike za definiranje mjerenja su izvedene iz *accounting* politika. *Accounting* politika se ne koriste za konfiguriranje naplate ili procesa obračuna.

Accounting politike se nalaze u AAA poslužitelju (lokalne politike) ili su primljene od drugih AAA poslužitelja ili korisnika. Može se odvojiti dva različita modela dobivanja *accounting* politike: *push* i *pull* model.

Push model

U *push* modelu *accounting* politike su dobivene od drugog AAA poslužitelja ili korisnika radi uspostave politika u lokalnoj *accounting* infrastrukturi. Primanje i evaluacija ovih politika ne smije biti obavljeno bez specijalnih sigurnosnih uvjeta.

Pull model

U *pull* modelu AAA poslužitelj zahtjeva politike od udaljenog AAA poslužitelja ili korisnika šaljući zahtjev za *accounting* politikama. Udaljeni AAA poslužitelj šalje odgovor u kojem potvrđuje da ima odgovarajući politiku.

Accounting politike se provode mrežnim elementima koji su konfigurirani u skladu s politikama. Oni utječu na slijedeće postavke u *accounting* arhitekturi:

- Konfiguraciju mjerača,
- Skupljanje podataka i agregacija,
- Distribucija i smještaj *accounting* zapisa.

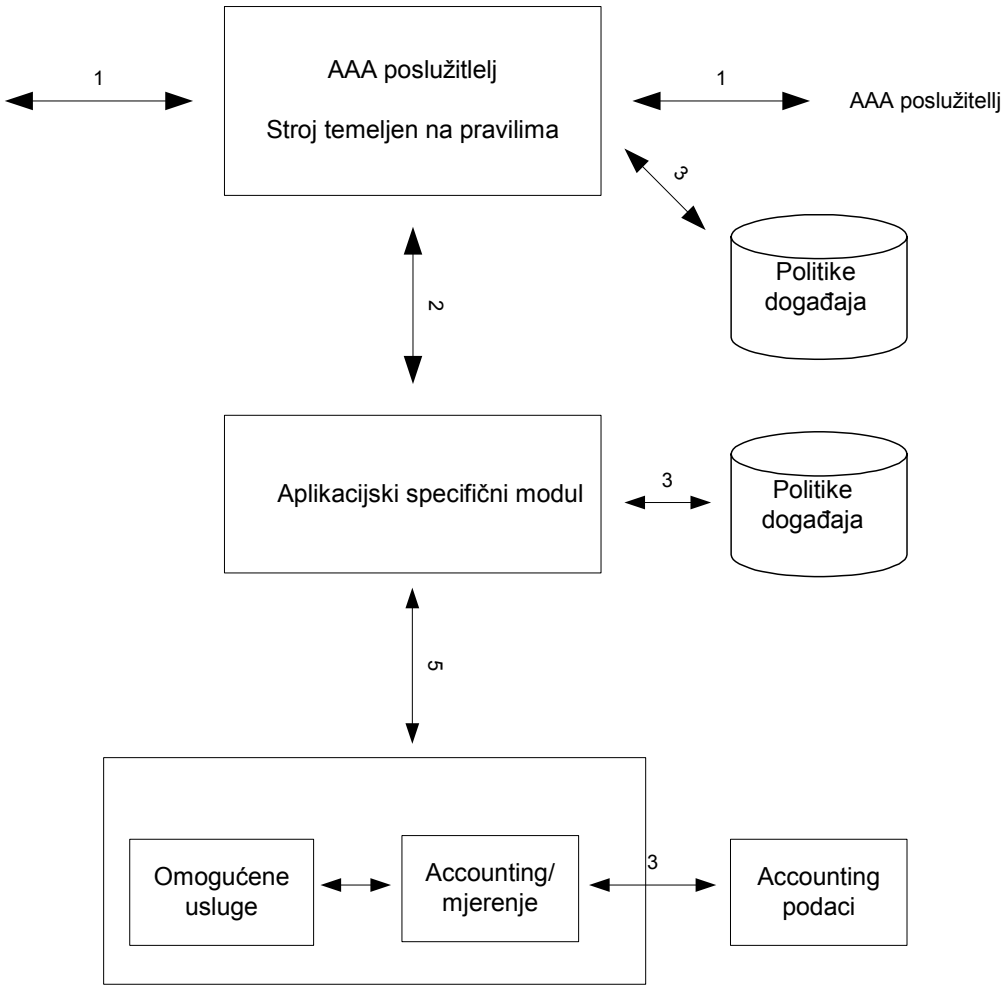
5.2.4.4 Accounting usluge

Accounting se može gledati kao proces (integrirani *accounting*) ili kao odvojena usluga (zasebni accounting).

Integrirani accounting

U integriranom *accounting* modelu *accounting* je dio omogućene usluge. Ovo znači da se nalazi zajedno s specificiranom uslugom. Na ovaj način *accounting* proces je pridružen specifičnoj usluzi i može skupljati *accounting* informacije direktno. Konfiguracija *accounting* arhitekture je napravljena kao dio konfiguracije servisne opreme na kojoj se nalazi. *Accounting* politike su definirane kao dio dogovora oko omogućavanja usluge. ASM konvertira instrukcije od AAA poslužitelja u odgovarajuće konfiguracije servisne opreme uključujući postavke za *accounting* arhitekturu.

Podaci o uporabi resursa šalju se natrag AAA poslužitelju preko ASM-a. *Accounting* proces unutar usluge pretvara izmjerene podatke u *accounting* zapise koji se šalju AAA poslužitelju. Za generiranje konverzije *accounting* zapisa, može se obaviti agregiranje i filtriranje podataka.

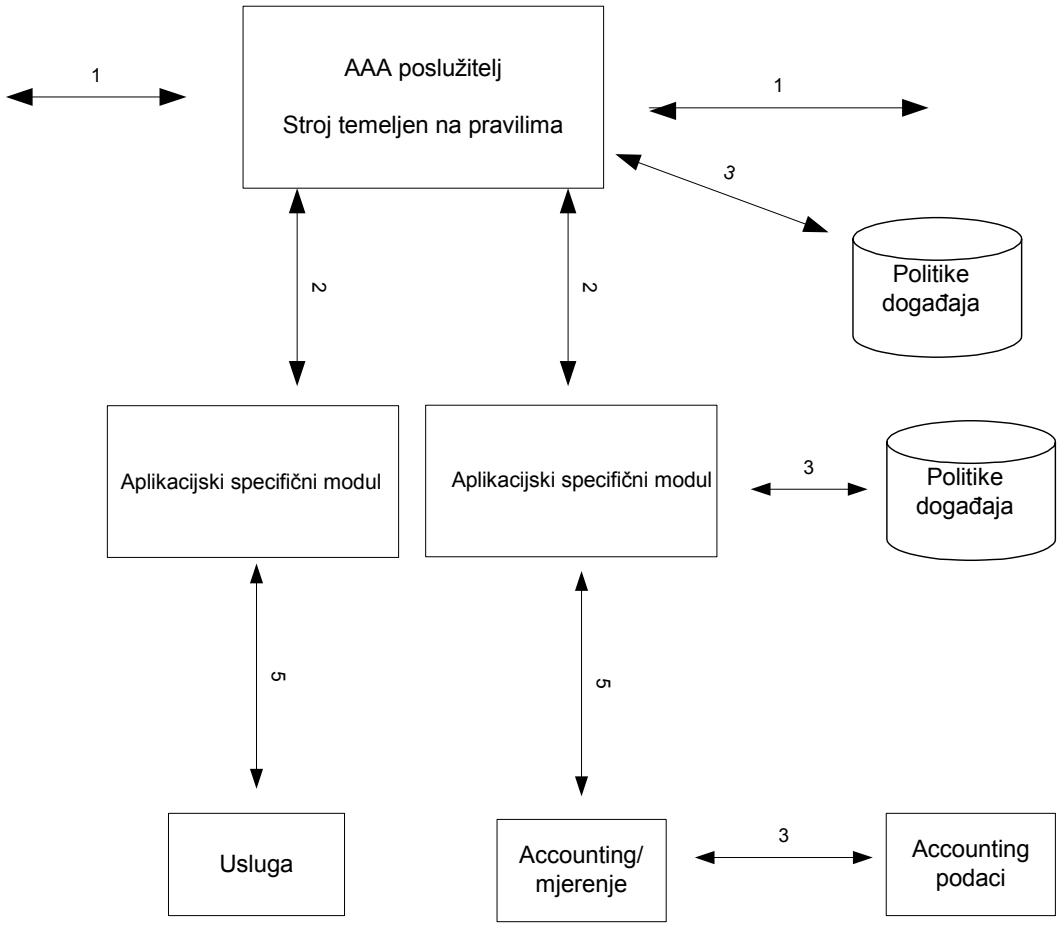


Slika 5-11 AAA poslužitelj s integriranim accounting-om

Zasebni *accounting*

Accounting proces može biti odvojen od same usluge. U ovom slučaju *accounting* se ne nalazi integriran u samoj usluzi. *Accounting* usluga je omogućena općim *accounting* sustavom koji je sposoban skupljati informacije o uporabi različitih usluga. Ako je *accounting* odvojen proces jedan operator može obavljati *accounting* za nekoliko davatelja usluga. Dobar primjer je sustav opisan u ovom radu u kojem operater vrši *accounting* i za davatelje usluga/sadržaja s kojima je povezan iznajmljenom linijom ili VPN-om.

Davatelj usluga koji nema vlastitu uslugu *accounting*-a zahtjeva ovu uslugu od davatelja *accounting* usluge.



Slika 5-12 AAA poslužitelj s zasebnim *accounting-om*

5.2.5 Protokoli u AAA sustavu

Postoji nekoliko protokola koji mogu podržavati AAA. U ovom poglavlju dan je osvrt na njih i njihovu upotrebljivost u AAA sustavu u skladu s rezultatima IETF AAA radne skupine [11].

5.2.5.1 Autentifikacijski protokoli na sloju povezivanja

Autentifikacijski protokoli se široko koriste u uspostavi veze na sloju podatkovnog povezivanje. U PPP PAP (engl. *Password Authentication Protocol*) autentifikacija je temeljena na paru korisničko ime i lozinka. PPP CHAP (engl. *Challenge Handshake Authentication Protocol*) podržava mehanizam zahtijevanog odgovora koji kontrolira autentifikator. U mehanizmu zahtijevanog odgovora lozinka ne smije biti prenesena preko veze. PPP EAP (engl. *Extensible Authenitication Protocol*) podržava autorizaciju zasnovanu na različitim mehanizmima, temeljene na identitetu i zahtjevu, ali također koristi jednokratne lozinke ili generičke žetone. Ovi protokoli su često integrirani u protokole prijenosnog sloja, koji implementiraju autentifikacijski zasnovani autorizaciju.

5.2.5.2 RADIUS

RADIUS (engl. *Remote Authentication Dial In User Service*) protokol je dizajniran za prijenos autentifikacije, autorizacije i nekih konfiguracijskih podataka između NAS-a, koji je RADIUS klijent i pojedinog RADIUS poslužitelja, koji drži informacije za autentifikaciju i autorizaciju korisnika. RADIUS poslužitelj može također funkcionirati kao klijent drugim RADIUS poslužiteljima. Originalno RADIUS je definiran da podržava povezivanje biranom linijom, no danas se koristi u mnogo više scenarija. RADIUS koristi različite gore nabrojane autentifikacijske protokole. Definirana [6] su proširenja za predaju *accounting* informacija RADIUS *accounting* poslužitelju. Postoji veliki broj razloga zašto RADIUS nije prihvaćen kao tipičan AAA protokol [11].

5.2.5.3 DIAMETER

DIAMETER protokol je definiran kao nasljednik RADIUS-a, koji uklanja znane RADIUS nedostatke. DIAMETER se sastoji od osnovnog protokola [34] koji definira format zaglavlja i sigurnosna proširenja te zahtijevane naredbe i AVP-ove [engl. *Attribute Value Pairs*]. Osnovni protokol je sesijski orijentiran, te zasnovan na modelu ravnopravnih razina. DIAMETER funkcionira preko SCTP (engl. *Stream Control Transmission Protocol*] kao transportnog protokola. Informacije se izmjenjuju prema AVP-ovima.

Različita proširenja osnovnog protokola dopuštaju uporaba različitih pristupnih tehnologija definirajući specijalne naredbene kodove i AVP-ove. NASREQ (*Network Access Server Requirements*) proširenja [36] pokrivaju podrški RADIUS autentifikacijskih protokola, PPP EAP, i autorizacije potrebne od NAS usluga. Proširenja vezana uz mobilni IP definiraju AVP-ove tako da podržavaju mobilni IP preko različitih administrativnih domena [35]. S ovime DIAMETER poslužitelj je sposoban autentificirati, autorizirati i skupiti *accounting* informacije za usluge zahtijevane od mobilnog čvora. *Accounting* proširenje [27] definira skup generičkih AVP-ova što mogu biti korišteni za sve usluge i podržavaju *accounting* u realnom vremenu. DIAMETER ispunjava osnovne uvjete za prihvaćanje kao opći AAA protokol [11].

5.2.5.4 COPS

COPS protokol [29] (engl. *Common Open Policy Service*) je protokol za izmjenu informacija o politikama između PEP-ova (engl. *Policy Enforcement Point*) i PDP-a (engl. *Policy*

Decision Point). COPS je jednostavni zahtjev i odgovor protokol u klijent/poslužitelj modelu. PEP-ovi su klijenti, a PDP funkcionira kao poslužitelj.

COPS je originalno specificiran za odobravanje autorizacije RSVP (engl. *Resource Resrvation Protocol*) zahtjeva u mrežama koje podržavaju integriranu uslugu. Ali protokol je dizajniran da bude primjenjiv u mnogo širem kontekstu. COPS se smatra prihvatljivim za AAA protokol zahtjeve definirane od strane AAA radne grupe [11].

5.2.5.5 SNMP

SNMP v3 (engl. *Simple Network Management Protocol Version* 3) preporuča novi model upravljanja. Ovaj model omogućava dizajn i razvoj sofisticiranih aplikacija upravljanja te također AAA aplikacija. *Accounting* je posebno podržan prijenosnim i smještajem *accounting* zapisa u SNMP upravljačku informacijsku bazu MIB (engl. *Management Information Base*). Ipak SNMP ne može biti prihvaćen kao opći AAA protokol [11], zato što je ograničen na upravljačku shemu pristupa bazama niske učestalosti.

5.2.5.6 Ostali protokoli

Ostali protokoli mogu se koristiti za autentifikaciju i autorizaciju; neki su aplikacijski ovisni poput DHCP-a i DNS-a, dok su neki integrirani u aplikaciju za autorizaciju uporabe aplikacije. Slijedeća lista nije potpuna, no pokazuje da se AAA zadatak ne obavlja samo na razini spajanja i transporta.

- **DHCP**

  DHCP ne omogućuje metode za autentifikaciju klijentski zahtijevanih konfiguracija. U mehanizmima autentifikacije izvor i sadržaj DHCP poruka su dodani, što također omogućava autorizaciju klijenata.

- **DNS**

  Reverzni DNS zahtjevi za izvorišnom IP adresom mogu biti korišteni za kontrolu pristupa. DNS ime pridruženo IP adresi se koristi u cilju upravljanja pristupom.

- **LDAP**

  LDAP se može koristiti za objavljivanje različitih informacija, općenito informacija o politikama te isto tako informacija o kontroli pristupa, npr. u formi pristupnih

kontrolnih lista. Kako pristup LDAP informacijama može biti autentificiran, LDAP se može smatrati kao protokol što podržava AAA.

- **HTTP autentifikacija**
  Dio HTTP protokola [37] se bavi osnovnom shemom autentifikacije. [21] se bavi osnovnom i sažetom shemom autentifikacije. Koristeći ove mehanizme, pristup web stranica može biti autoriziran.

- **SSL**
  SSL protokol se nalazi iznad transportnog sloja i nudi aplikacijama poput FTP-a i HTTP-a autentifikaciju poslužitelja i klijenta i izgradnju sigurnog povezivanja koje omogućava povjerljivost, integritet i autentičnost. SSL je dio TLS-a (engl. *Transport Layer Security*) [41].

- **Sistem kreditnih kartica**
  Utipkavanje broja kreditnih kartica u HTML formu u cilju kupovine pristupa sadržaju na WWW-u i prijenos ovog broja preko HTTP-a definira princip autorizacijskog pristupa korištenog za usluge sadržaja.

5.2.6 Integracija HSS i AAA u mobilnim paketskim mrežama

Kao nadogradnja za HLR u UMTS mreži, HSS (engl. *Home Subscriber System*) je glavna baza podataka korisnika. U njemu se nalaze informacije vezane uz pretplatnika koje podržavaju rukovanje pozivima/sesijama. Iako predstavlja budućnost UMTS mreža HSS je još uvijek u fazi razvoja i definiranja.

Mreža pojedinog operatera može imati jednog ili više HSS-a, što ovisi o broju mobilnih pretplatnika, kapacitetu opreme i organizaciji mreže.

HSS je odgovoran za držanje slijedećih korisnički orijentiranih informacija:

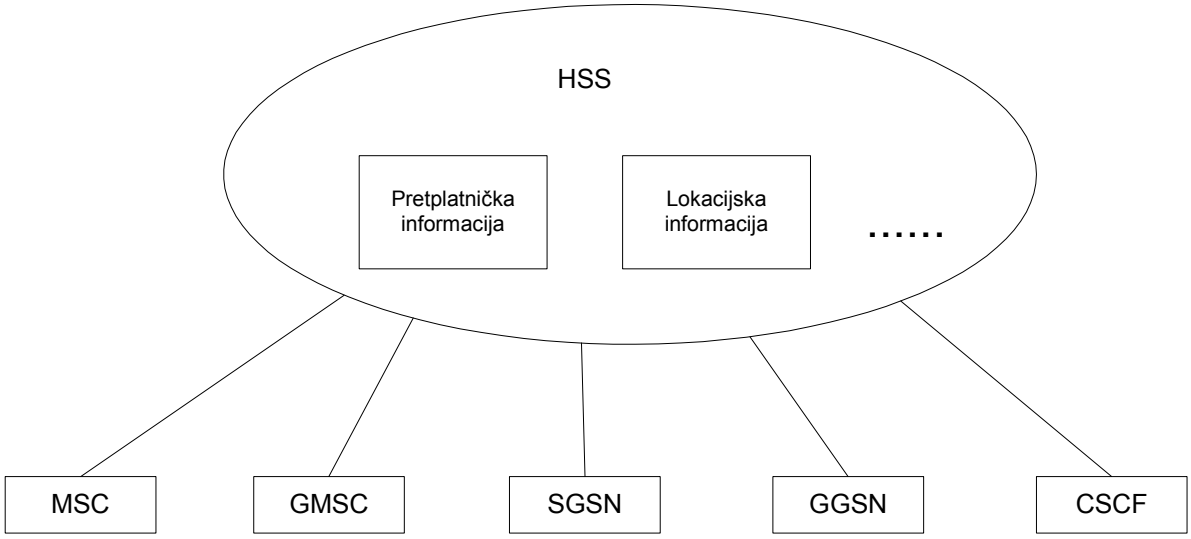
- Identifikacije korisnika, informacije o broju i adresi,

- Sigurnosne korisničke informacije: informacije kontrole pristupa mreži za autentifikaciju i autorizaciju,

- HSS podržava korisničku registraciju i lokacijske informacije na razini sustava povezanih operatera,

- Informacije o korisničkom profilu.

Na osnovu ovih informacija HSS je odgovoran za podržavanje kontrole poziva i upravljanje sesijom različitih domena i podsistema operatera kako je to prikazano na slici 5-14.

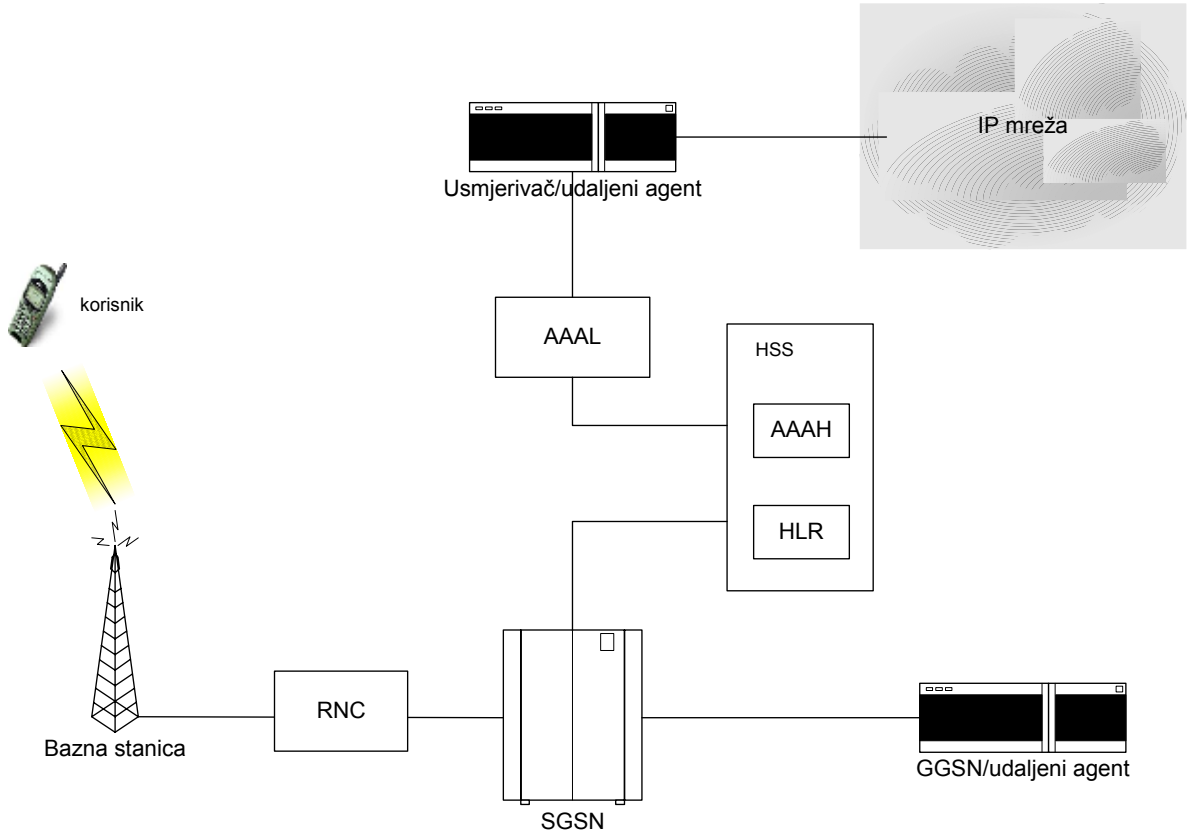


Slika 5-13 Primjer generičke HSS strukture

HSS se sastoji od slijedećih funkcionalnosti:

- IP multimedija funkcionalnost za omogućavane podrške kontrolnoj funkciji IM podsistema kao što je CSCF,
- Podskup HLR/AUC funkcionalnosti zahtijevanih od PS domene,
- Podskup HLR/AUC funkcionalnosti zahtijevanih od CS domene.

Iako postoji nekoliko prijedloga rješenja kojima se povezuje AAA poslužitelj kojeg definira IETF i HSS koje definira ETSI, rješenje na slici 5-14 je odabrano u ovom radu za tu integraciju [13]. Ovakvo rješenje omogućava potpunu integraciju mobilnih paketskih mreža s fiksnim paketskim mrežama na razini AAA.



Slika 5-14 UMTS R5 sistemska arhitektura između mobilnih i fiksnih mreža.

Autentifikacija se obavlja koristeći IETF-ove AAA protokole. Domaći AAA poslužitelj je dio HSS-a, dok je lokalni poslužitelj dio mreže drugog operatora (npr. WLAN ili ISP operater). Jedna od funkcija HSS-a je povezivanje različitih identitete korisnika, tako omogućavajući mreži da jednako tretira korisnika bez obzira da li se trenutno nalazi mobilnoj mreži ili možda WLAN mreži drugog operatera kao jednog i sa istim utjecajem na obračun i uporaba mrežnih usluga.

5.2.7 QoS broker

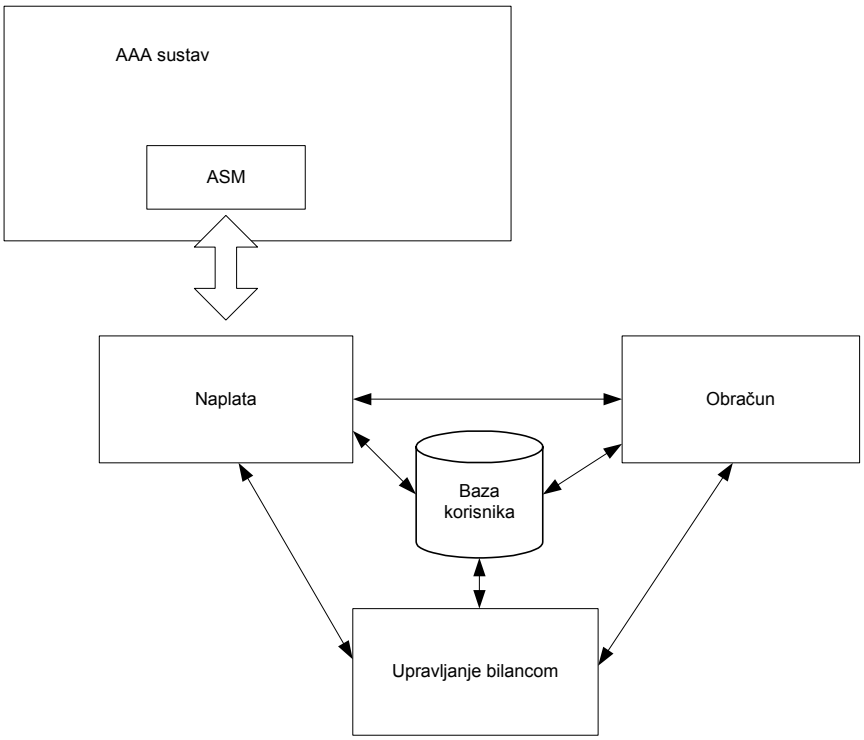
AAA arhitektura ima cilj omogućiti usluge koje zahtijevaju određeni QoS. Unutar modela *Diffserv* [39] arhitektura se koristi za omogućavanje QoS-a. AAA arhitektura mora raditi s ovom arhitekturom za omogućavanje usluga radi kontrole pristupa usluzi/sadržaju i biti sposobna obračunati osigurani QoS. Ovo znači da AAA sustav treba sučelje prema *Diffserv* arhitekturi preko specifičnih ASM-ova. U ovom radu se pretpostavlja da postavljanje QoS-a između domena obavlja QoS broker arhitekturom objašnjenom u [38]. U tom radu se QoS broker naziva *Bandwidth Broker*. QoS broker je dvoslojni model u kojem QoS broker prihvaća RAR (engl. *Resource Allocation Request*] od korisnika koji pripada njegovoj domeni

ili RAR-ove generirane od strane drugih QoS brokera iz susjednih domena. Svaki QoS broker upravlja jednom servisnom domenom i omogućuje autorizaciju zavisno o politici. RAA (engl. *Resource Allocation Answer*) potvrđuje ili odbija zahtjev ili indicira "u toku" stanje. RAR/RAA model implicira da je ovo distribuirana usluga, gdje je prva autorizacija *pull* temeljena, a ostale su ili *pull* ili agent temeljene [23].

U slučaju samo *pull* temeljene autorizacije, prvi QoS broker, zapravo servisna oprema koja prima RAR od korisnika, kontaktira lokalni AAA sustav preko ASM-a. Autorizacijski zahtjev enkapsulira podatke od RAR-a potrebne za autentifikaciju i autorizaciju. Ako QoS broker primi pozitivan odgovor od AAA sustava, prosljeđuje RAR slijedećem QoS brokeru u nizu gdje se procedura ponavlja. Nakon primitka RAA QoS broker konfigurira mrežne elemente u svojoj domeni za traženu uslugu. Ove se može učiniti preko SNMP-a, COPS-a ili komandne linije. U slučaju kada su svi osim prvog temeljeni na agent modelu AAA sustav prosljeđuje RAR preko AAA protokola do AAA sustava slijedećeg QoS u nizu koji obavlja autorizaciju. Ove se ponavlja sve dok krajnja domena nije dostignuta. Ako su sve autorizacije uspjele, RAA se propušta natrag AAA protokolom do prvog QoS brokera koji prosljeđuje RAA korisniku. U svakom AAA sustavu RAA se prosljeđuje QoS brokeru preko ASM-a. Servisna oprema (npr. QoS broker) ili odvojeni sustav trebaju biti konfigurirani da skupljaju *accounting* informacije za svaku domenu. Ovo može biti urađeno uporabom *accounting* politike [23]. U slučaju uporabe *pull* temeljene autorizacijske politike moraju biti propušteni u AAA odgovor od poslužitelja prema servisnoj opremi, dok se agentske autorizacijske politike propuštaju zajedno s konfiguracijskim zahtjevom za servisnu opremu.

5.3 Naplata, obračun i upravljanje bilancom

Uloga ove razine je određivanje cijene pojedinih usluga/sadržaja, vođenje računa o stanju na korisničkom računu te naplata. Ova razina se povezuje sa AAA sustavom preko naplate povezane sa ASM-om kako je to prikazano na slici 5-16. Upravljanje razine obavlja se politikama, odnosno pravilima ovisno o izvedbi opreme. Isto tako politike naplate se mogu nalaziti u spremištu politika AAA, ali i mogu biti interno spremljene. Politike obračuna se nalaze smještene unutar sustav obračuna.



Slika 5-15 Naplata, obračun i upravljanje bilancom te njihovo povezivanje s AAA sustavom

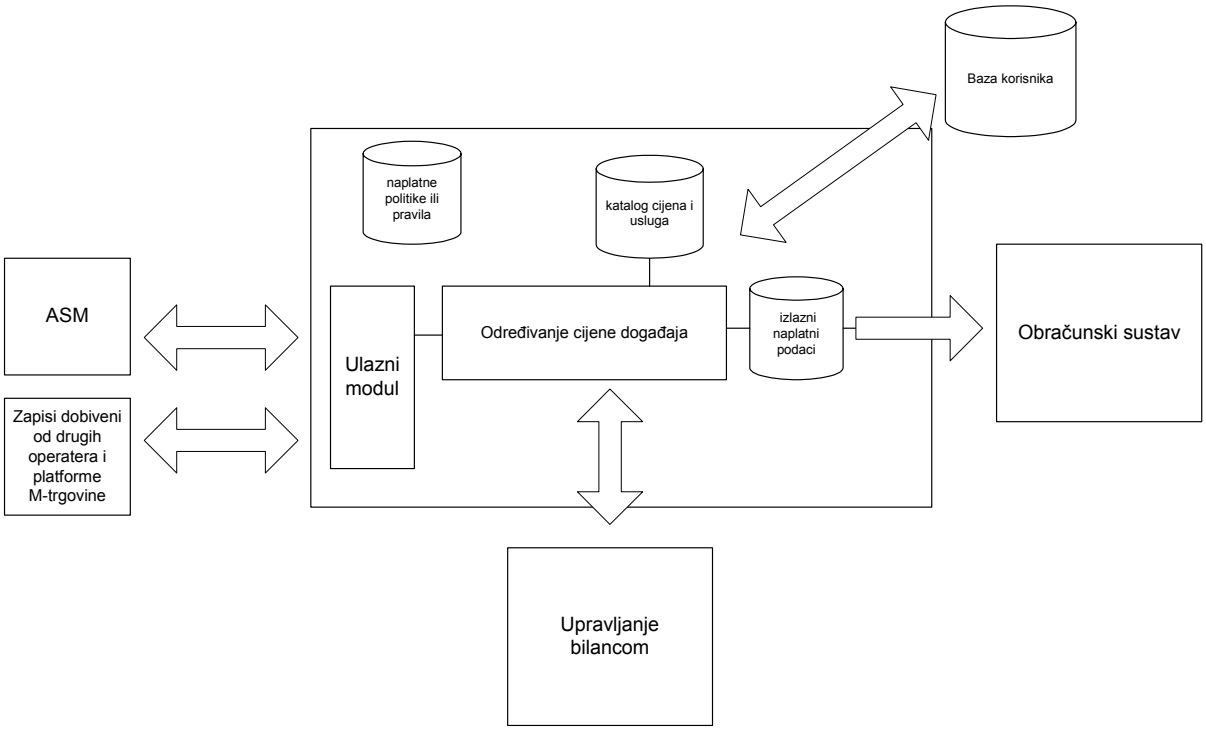
5.3.1 Naplata

Iako je naplata zapravo cjelokupni proces od skupljanja i mjerenja podataka te određivanja cijene za pojedinu uslugu, u ovom radu naplatom definiramo procesiranje podataka dobivenih iz *accountinga* preko AAA sustava, te zaračunavanje odgovarajuće naknadu za uporabu usluga i sadržaja. Usluga se zaračunava koristeći katalog cijena pojedinih usluga te moguće popuste vezano uz pojedinog korisnika.

Slika 5-16 prikazuje osnovni model naplate sustava. Osnovni moduli sustava su:

- Modul za određivanje cijene događaja, tarifiranje (engl. *Rating*),
- Ulazni modul,
- Katalog cijena i usluga,
- Baza izlaznih podataka koji se predaju sustavu obračuna.

Ovaj model naplatnog sustava ima mogućnost unošenja podataka iz AAA sustava preko ASM te unošenja podataka iz sustava drugih operatera kao što su podaci o *roaming* uslugama ili podataka iz neovisnih platformi kao što je platforma za M-trgovinu.



Slika 5-16 Model naplatnog sustava

Osnova ovog modela je određivanje cijene događaja. Modul ima mogućnost određivanja cijena različitih tipova usluga zasnovanih na događajima kao što su telefonski pristup, pristup paketskoj mreži, kupovina, URL temeljeni sadržaji. Ovakav sustava nije limitiran na pojedini tip ili klasu događaja kao što su to npr. telefonski CDR-ovi, IPDR-ovi i slično. Sustav dopušta definiranje bilo kojeg događaja. Događaji predstavljaju zbivanja nečega – kao što su telefonski razgovor, izbor filma, kupovina dobara, pristup web stranici ili druga usluga, transfer podataka, isporuku SMS poruke.

Ovakav sustav podržava koncept dodatnih tarifa obračunavanja. Na taj način za kompleksne slučajeve obično vezane uz naplatu sadržaja ne obračunava se samo vrijednost prenesenog sadržaja već i količina prenesenih podataka i QoS.

Sustav ima mogućnost pre-autorizacije naplate za pojedine događaje kao što su isporuka sadržaja ili transakcija M-trgovine. Ovi događaji mogu biti preneseni kao kompleksni događaji ili tok parcijalnih događaja. Pre-autorizacija se vrši slanjem zahtjeva sustavu upravljanja bilancom koji alocira određena sredstva.

Događaji kojima je unaprijed određena cijena se mogu unijeti u ovaj sustav. Ovi događaji mogu biti unijeti od drugih mobilnih operatera ili sustava M-trgovine. Naplatni sustav omogućava unos bilo koje kombinacije događaja kojima je određena cijena i onih kojima nije. Primjer za to je npr. gledanje prijenosa nekog događaja. Cijena prijenosa je definira od strane davatelja sadržaja, dok količina prenesenih podataka i QoS nemaju unaprijed određenu cijenu.

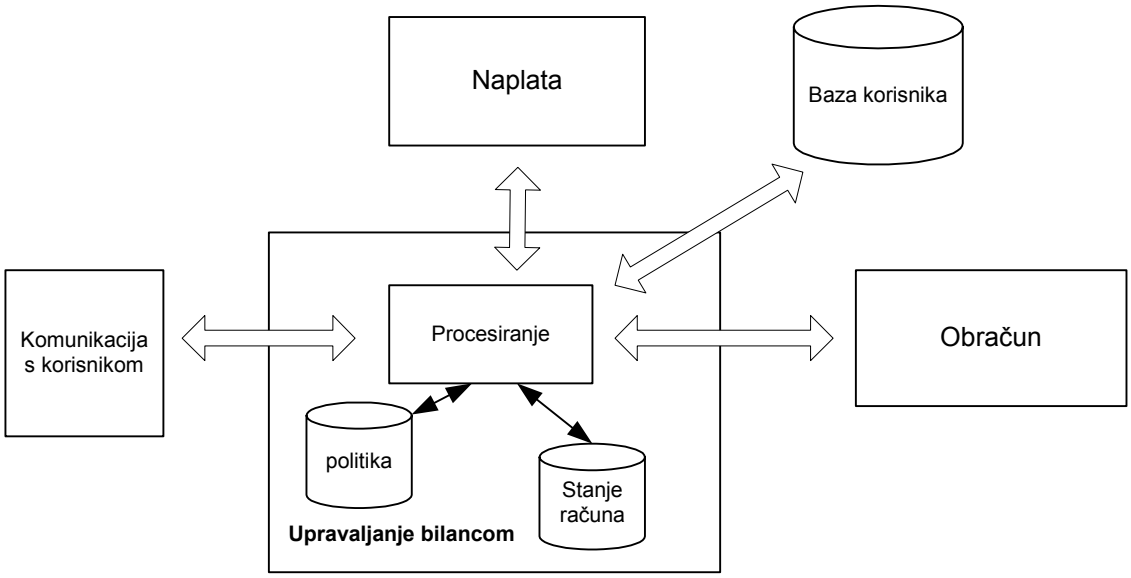
Accounting sustav može omogućiti tok parcijalnih zapisa o događaju što opisuje događaj koji je u toku. Ovi pojedini događaji su mogli biti agregirani u *accounting* sustavu ili se agregiraju u naplatnom sustavu. Parcijalni događaji koji se agregiraju unutar sustava omogućuju vođenje računa o količini novca na korisnikovom računu za vrijeme događaja koji se zbivaju korištenjem nekoliko usluga. Ovo se obavlja u suradnji s BM koji je zadužen za stanje na korisnikovom računu.

Obračunati podaci se spremaju u izlaznu bazu i prenose BM koji vodi računa o trenutnom stanju računa.

5.3.2 Upravljanje bilancom

U početku razvoja telekomunikacijskih usluga pa tako i mobilne telefonije i prijenosa podataka sva naplata se vršila naknadno bez obzira na iznos računa, tzv. *postpaid*. Mobilna telefonija je unijela novi način plaćanja, plaćanje unaprijed, tzv. *prepaid*. *Prepaid* je usluga plaćanja u kojoj korisnik unaprijed uplati određenu količinu novca za određene usluge kao što je uporaba mobilne mreže. Uporabom usluge stanje računu se smanjuje. Nakon što potroši svu količinu novca korisnik ne može više koristiti uslugu već mora uplatiti novu količinu novca. Osim ova dva osnovna načina plaćanja postoji mogućnost plaćanja kreditnim karticama, direktnog skidanja novca s korisnikovog računa. Plaćanje karticama je slično *prepaid*-u zbog mjesečnih limita. Metoda plaćanja skidanjem novca direktno s korisnikovog računa funkcionira na način da korisnik dodijeli određenu količinu novca na računu. Nakon potrošnje te količine novca korisnik može dodatno odrediti određenu količinu. Sve ovo su osjetljive i složene transakcije koje vrlo često nužno zahtijevaju direktnu vezu između operatera i novčanih institucija. Kod ovakvog načina plaćanja bitno je da korisnik u svakom trenutku je može saznati stanje na svom računu.

Upravljanje bilancom vodi računa o svemu gore navedenom. U njemu se nalaze zapisani računi korisnika i trenutno stanje na njima.



Slika 5-17 Upravljanje bilancom

Slika 5-17 prikazuje upravljanje bilancom i njegovo povezivanje s drugim sustavima. Upravljanje bilancom između ostalog je posredno povezano s korisnikom. Korisnik može preko npr. web ili WAP sučelja pratiti trenutno stanje na svom računu i u skladu s politikama odrediti limite potrošnje, zatražiti prenošenje dodatne količine novca. Nakon što dostigne limite potrošnje korisniku se šalje obavijest preko SMS-a ili web-a i onemogućava mu se daljnja uporaba usluge. Nakon što dobije zahtjev od korisnika za novim limitom šalje zahtjev sustavu obračuna koji komunicira s novčarskom institucijom i korisniku odobrava ili ne alokaciju slijedeće količine novca.

Korisnik može imati nekoliko računa. Zavisno o korisnikovim postavkama, koje se pohranjuju u bazu korisnika, nakon što se potroši novac na jednom računu mogu se dodatno alocirati sredstva s drugog računa.

BM omogućava pre-autorizaciju određene količine novca. Nakon što je alocirao traženu količinu novca, sa svakim zapisom koji dobije od naplatnog sustava, za taj događaj smanjuje alociranu količinu novca. Ukoliko je događaj završio prije nego je cijela količina novca potrošena ili je isteklo vrijeme postavljeno u skladu s politikama za traženi tip usluge, BM vraća preostale novce.

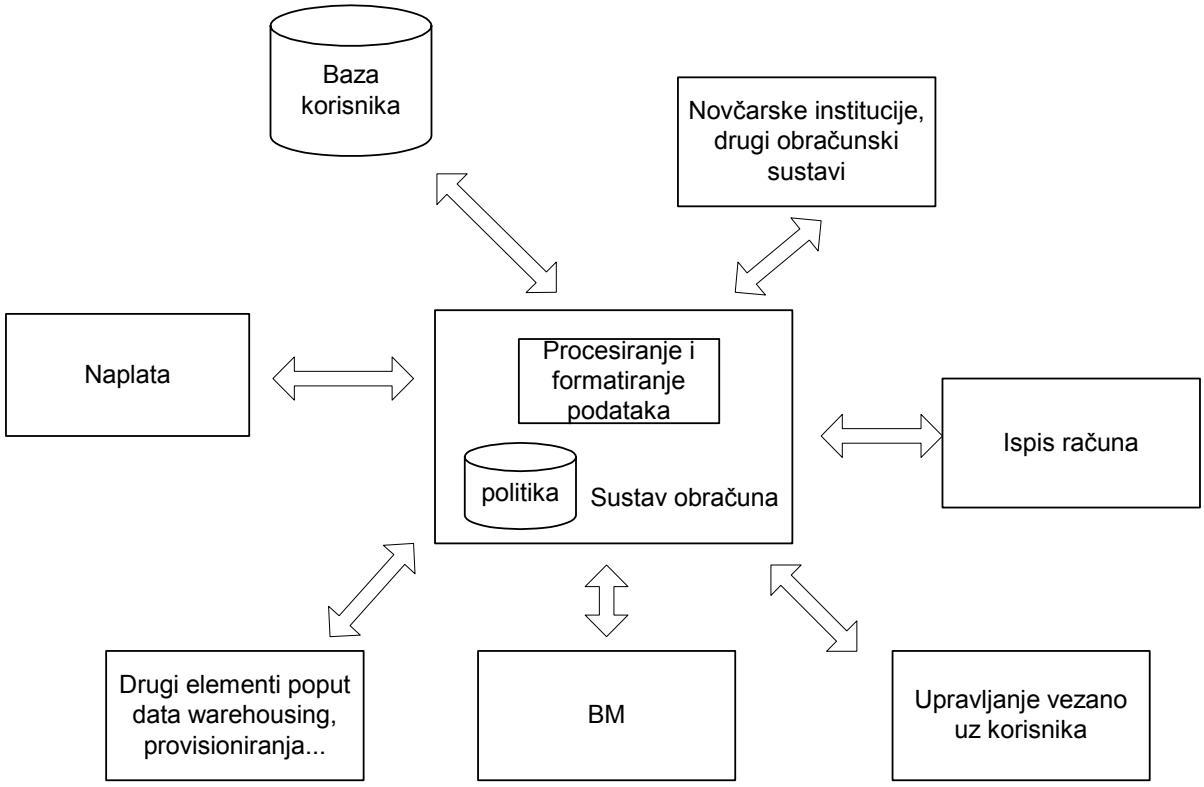
5.3.3 Sustav obračuna

Sustav obračuna povezan je s mnogo elemenata i sustava kako je to prikazano na slici 5 –19. Kako većina ovih elemenata je vezana uz brigu o korisniku i ekonomske pojmove poput

marketinga (razni popusti), dodavanje poreza, zaračunavanje kamata na neplaćene račune i sl. što ne ulazi u područje ovog rada objašnjeno je najosnovanije funkcioniranje ovog sustava. Alternativne metode plaćanja (poput kreditnih kartica ili odvojenih *prepaid* sustava) i komunikacija s njima u ovom radu pridjeljuju se sustavu obračuna.

Sustav obračuna skuplja zajedno sve podatke vezane za pojedini račun: produkte, tarife, popuste, uporaba pojedine usluge, poreze i proračune.

Podaci kojima je dodijeljena cijena u naplatnom sustavu, sustav obračuna uzima periodički, npr. svakih sedam dana i obrađuje te preformatira u oblik pogodan za ispisivanje ili pogodan za prosljeđivanje drugim sustavima.



Slika 5-18 Sustav obračuna

5.3.4 Baza korisnika

Baza korisnika sadrži sve podatke i informacije o pojedinom korisniku bitne za određivanje cijene, BM i sustav obračuna. Npr. tarifni modeli, klasa korisnika, popusti, limiti i slično.

5.3.5 Izvedbe naplatnog sustava, sustava obračuna te BM-a

Umjesto naplate u praksi, se obično koristi izrazi tarifiranje (engl. *Rating*) i vođenja (engl. *Guiding*) za cjelokupno određivanje cijene i prilagođavanje izlaznog formata podataka sustavu obračuna. Gotovo svi sustavi imaju ujedinjene funkcije obračuna, tarifiranja i vođenja u jedinstvenom sustavu obračuna. BM je novi modul koji se dodaje postojećim sustavima kao zasebni element ili se integrira kao dio jedinstvenog sustava. Od sustava pojedinih proizvođača proučavanih tokom ovog rada kao dva vrlo fleksibilna rješenja s integriranim BM-om izdvajaju se Convergys "Geneva" (od verzije 5.0) te Portalov "Infranet wireless".

5.4 Broker

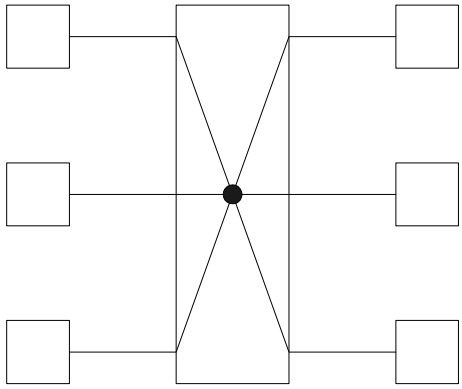
Broker u sustavu naplate predstavlja agenciju koja vrši usluge posredovanja između sustava raznih operatera i davatelja usluga/sadržaja koji nemaju direktnu međusobnu vezu. U poglavlju 5.2.2.2 prikazana je izvedba AAA brokera koji posreduje između dva AAA poslužitelja koji nemaju direktnu veza.

Modele brokera se može podijeliti u tri osnovne skupine:

- Broker između istovrsnih sustava
  U ovom slučaju broker posreduje između istovrsnih sustava i predstavlja koncentrator. Ovim rješenjem smanjuje se broj potrebnih veza između sustava i svi međusobno komuniciraju preko brokera. Primjeri ovog rješenja su komunikacija između AAA sustava preko AAA brokera, razmjena informacija između operatera o uporabi *roaming* usluga.

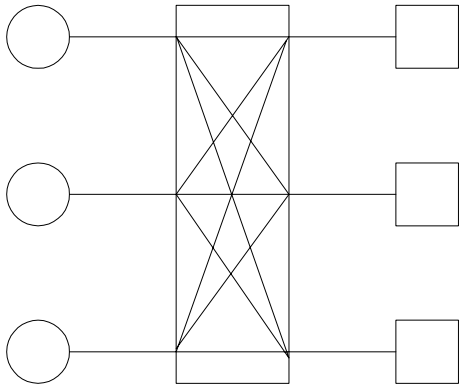
- Broker između raznovrsnih sustava u kojem istovrsni sustavi nisu povezani
  Kod ovog modela postoje dvije vrste sustava. Jedni sustavi sadrže usluge i sadržaje koje su potrebne drugim sustavima. Sustavi unutar prve i unutar druge skupine ne razmjenjuje usluge međusobno nego se isključivo preko brokera povezuju s sustavima druge skupine. Primjer ovog modela je broker koji skuplja davatelje sadržaja i nudi ih operaterima.

- Broker između raznovrsnih sustava u kojem su istovrsni sustavi povezani
  U kombinaciji gornjih rješenja sustavi unutar obje skupine mogu i međusobno komunicirati. Primjer je broker sustava u kojem bi operatori osim pristupa davateljima sadržaja imali mogućnost izmjenjivati sadržaje i usluge međusobno, a isto tako bi davatelji usluga imali mogućnost izmjene nekih sadržaja čime bi upotpunili svoje ponude.



Sustav koji se koristi usluge brokera

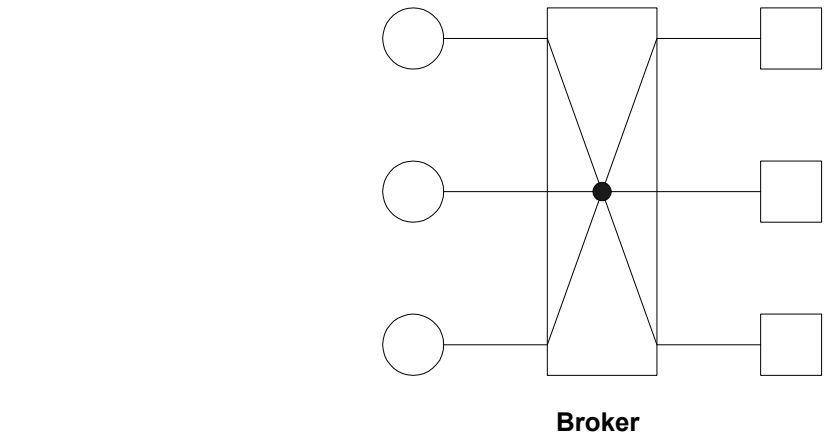
Slika 5-19 Broker između istovrsnih sustava



Tip sustava I

Tip sustava II

Slika 5-20 Broker između raznovrsnih sustava u kojem istovrsni sustavi nisu povezani



Slika 5-21 Broker između raznovrsnih sustava u kojem su istovrsni sustavi povezani

Uporaba usluga brokera umanjuje potrebe povezivanje svih sustava međusobno i na taj način donosi uštedu u potrebnim vezama prema pojedinim operaterima odnosno davateljima usluga. Loša karakteristika brokera je u tome što on predstavlja i najslabiju točku jer gubitkom veze prema brokeru gubi se veza prema drugim operatorima i/ili davateljima sadržaja. Zbog toga je vrlo važno postaviti sigurne veze prema brokerima i koristiti ih za povezivanje s operaterima odnosno davateljima sadržaja s kojima je količina razmjena informacija nedovoljna da bi ekonomski opravdala direktno povezivanje.

5.5 Zaključak

Model sustava naplate prijenosa sadržaja i usluga prikazan u ovom i prošlom poglavlju predstavlja prijedlog cjelokupnog rješenja koje bi omogućilo integriranu naplatu.

U ovom sustavu nije posebno obrađene *prepaid* usluge, ali se one uporabom BM rješenja lako integriraju.

Osnovna ideja ovog sustava je zasnovana na uporabi postojećih rješenja u područjima AAA poslužitelja, mobilnog IP-a, BM i QoS brokera. Iako će funkcioniranje ovakvog sustava doći do punog izražaja uporabom IPv6 gdje će svaki mobilni korisnik imati mogućnost uporabe vlastite IP adrese, moguća je njegova implementacija koristeći IPv4.

Sigurnost sustava temeljena je na AAA sustavu i ovisi o njegovoj implementaciji.

Prednost ovakvog sustava je u mogućnosti naplate kompleksnih slučajeva u kojima se korisniku istovremeno naplaćuje prijenos podataka, usluga garantiranja određenog prijenosnog pojasa te sam sadržaj. Osim naplate sustav i omogućava funkcioniranje gore navedenog, tj. korisniku omogućuje pristup određenim sadržajima sa garantiranom QoS te autorizaciju usluga bez obzira da li se korisnik nalazi u svojoj mreži ili u stranoj. Sustav omogućava i praćenje prometa u mreži, što zajedno sa naplatom pojedinog QoS omogućava kontrolu i otklanjanje zagušenja.

Nedostatak sustava je što komunikacijom unutar mreže unosi povećanje prometa u mrežu. No zapravo najveći problem trenutnoj implementaciji rješenja da su njegovi osnovni elementi i poput AAA sustava i njemu pridruženih protokola (DIAMETER i COPS) još uvijek u fazi razvoja.

6 Model M – trgovine

Za razliku od modela sustava objašnjenog u četvrtom i petom poglavlju, ovo poglavlje se bavi isključivo kupovinom dobara i transakcijama preko mobilnih uređaja. Ovaj sustava se naslanja na gore objašnjeni sustav da koristi pojedine njegove sastavne dijelove kao što je na primjer sustav obračuna.

Kupovina sadržaja i dobara preko Interneta poznata kao E-trgovina je široko raširena i iako postoje usponi i padovi u budućnosti će ovaj vid kupovine biti jedna od najvažnijih djelatnosti na Internetu. Kupovina preko mobilnih uređaja, poznata kao M-trgovina donosi nove mogućnosti prije svega uz svoje specifičnosti:

- mobilnost,
- trenutna pozicija korisnika,
- mobilni uređaj je vezan uz jednog korisnika.

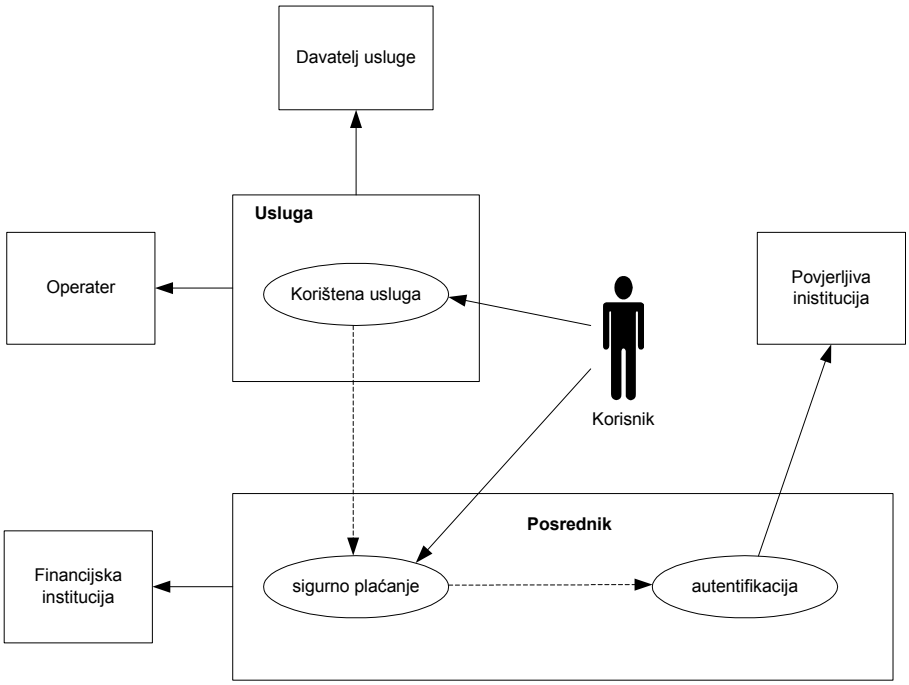
Primjer japanskog NTT DoCoMo-a pokazuje važnost ovih gore specifičnosti za uspješno lansiranje usluga koje uključuju naplatu sadržaja.

Osim kupovine glavninu transakcija M-trgovine obuhvaćaju financijske transakcije kao što su je npr. prenošenja novca na druge račune.

Kako mobilni uređaji većina današnjih mobilnih uređaja osim WAP pretraživača nemaju nikakve dodatne aplikacije za razliku od sustava e-trgovine. Sustav M-trgovine treba posrednika koji će umjesto njega komunicirati s davateljima usluga i financijskim institucijama. Općenito takvi se sustavi nazivaju *middleware*. Kod M-trgovine taj posrednik se naziva platforma za M-trgovina.

6.1 Osnovni elementi modela M-trgovina

Osnovni model M-trgovina se objašnjavaju u ovom poglavlju. Slika 6-1 prikazuje primjer uporabe usluge i sadržaja te glavne elemente modela koji sudjeluju u tome.



Slika 6-1 Način funkcioniranja sustava M-trgovine i njegovi glavni elementi

Glavni elementi ovog sustava su:

- Korisnik,
- Posrednik koji pomaže u transakciji i izmjeni informacija (platforma M-trgovine),
- Davatelj usluge,
- Operater,
- Financijska institucija,
- Povjerljiva institucija za autentifikaciju korisnika.

Korisnik prije nego što dobije zatraženu uslugu mora biti autentificiran. Nakon toga se provjerava da li ima dovoljno novca na računu za traženu transakciju. Tek nakon toga biti će autoriziran za uporaba traženog sadržaja. Autentifikacija se odvija neovisno o posredniku te se na taj način čuva privatnost npr. korisnikovog bankarskog računa. Sve veze između pojedinih dijelova sustava su kriptirane čime se postiže sigurnost transakcije.

Kako je mobilnim operaterima u interesu da što više prihoda ostane njima, tako da oni najčešće u ovom modelu predstavljaju i financijsku instituciju (potrebna im i posebna

dozvola) te povjerljivu instituciju, a platforma M-trgovine se obično nalazi unutar mreže operatera. Ovaj rad se bavi samo tim slučajem.

6.2 Sigurnost M-trgovina rješenja

Kako detaljan prikaz sigurnosnih aspekata M-trgovine prelazi okvire ovoga rada, u ovom poglavlju je dan kratak pregled mogućnosti za postizanje sigurnosti.

Tehnologije igraju važnu ulogu u sigurnosti rješenja M-trgovine. Za svaku od dolje navedenih tehnologija uključena je i njena pripadnost jednoj od pet sigurnosnih pretpostavki: tajnost, autentifikacija, integritet, neodbacivanje i autorizacija [44].

Enkripcija

Enkripcija se može koristiti za osiguranje tajnosti. Enkripcija je proces u kojem je neki tekst (npr. neko ime, broj) transformiran u podatke koji nemaju neko značenje. Ovo se postiže uporabama enkripcijskih i dekripcijskih ključeva. Razumijevanje bilo kojeg presretenog enkriptiranog podatka je praktično nemoguće.

Slijedeći mehanizmi su zasnovani na kripto sustavu javnog ključa. Kripto sustav definira kako se enkripcija i dekripcija obavljaju. U jednom kripto sustavu javnog ključa koriste se slijedeći ključevi: javni ključ, koji je javno objavljen i privatni ključ koji se drži tajnim.

Digitalni potpisi

Digitalni potpisi mogu osigurati autentifikaciju učesnika u transakciji te integritet i neodbacivanje transmisije. Digitalni potpis je podatak koji prati digitalno enkodiranu poruku. Prodavač knjiga *on-line* može koristiti digitalni potpis za verifikaciju da kupovina pojedine knjiga na ime Ivana Ivića i pripada Ivanu Iviću, a ne nekom drugom. Digitalni potpisi mogu se proizvesti enkripcijom sadržaja podataka prenesenih uporabom privatnog ključa. Ovo osigurava da digitalni potpisi ne mogu biti krivotvoreni. Matematička metoda koristi *hash* funkciju koja može biti korištena za minimiziranje veličine digitalnog potpisa.

Za verifikaciju digitalnog potpisa potrebno je imati kopiju javnog ključa potpisane strane.

Digitalni certifikat

Digitalni certifikat je skup informacija kojima digitalni potpis može biti pridjeljen od strane poznatog autoriteta i provjeren od strane zajednice certificiranih korisnika. Čest tip digitalnih certifikata su certifikati javnih ključeva koji se nedvojbeno vežu za pojedinu osobu, uređaj ili entitet za pojedini javni ključ. Digitalni certifikat sadrži četiri glavne komponente: javni ključ, informaciju koja povezuje ovaj ključ s njegovim vlasnikom, informaciju o izdavaču certifikata i njegov digitalni potpis. Certifikacijski autoritet izdaje digitalne certifikate.

PKI (engl. *Public Key Infrastructure*)

PKI je definirana od strane PKIX radne skupine kao "skup *hardware-a*, *software*-a, ljudi i procedura potrebnih za kreiranje, upravljanje, spremanje, distribuciju i opoziv certifikata zasnovanog na kriptografiji javnog ključa". Ovo je skup standarda koji kontroliraju životni ciklus digitalnih certifikata. PKI može definira autorizacijski i neodbacujući aspekt sigurnosti [25].

Gore navedene tehnologije su instrumenti u postavljanju sigurnog okružja za M-trgovina plaćanje. Primjer toga je WTLS, sigurnosni protokol u WAP arhitekturi koji uključuje enkripciju i digitalne potpise. WTLS osigurava komunikaciju između korisnikovog mobilnog uređaja i WAP *gateway*-a. Slijedeći primjer je SET (engl. *Secure Electronic Transaction*), protokol MatserCard i Visa kartičnih kuća, za podršku plaćanju bankarskim karticama. SET koristi PKI.

WAP korisnici u budućnosti će koriste moći autentificirati davateljima usluga i operaterima koristeći WTLS i WIM (engl. *Wireless Indentity Modul*) koji će spremiti reference za industrijski standard X.509 digitalnih potpisa. WIM može biti spremljen u SIM karticu. Novi model Nokia mobitela 6310 (izdan u Q4 2001) ima u sebi ugrađen WIM modul.

6.3 Metode plaćanja

O metodama plaćanja ovisi izvedba rješenja same M-trgovina platforme. Dva osnovna modela su plaćanje temeljeno na korisnikovom računu i plaćanje temeljeno na žetonima.

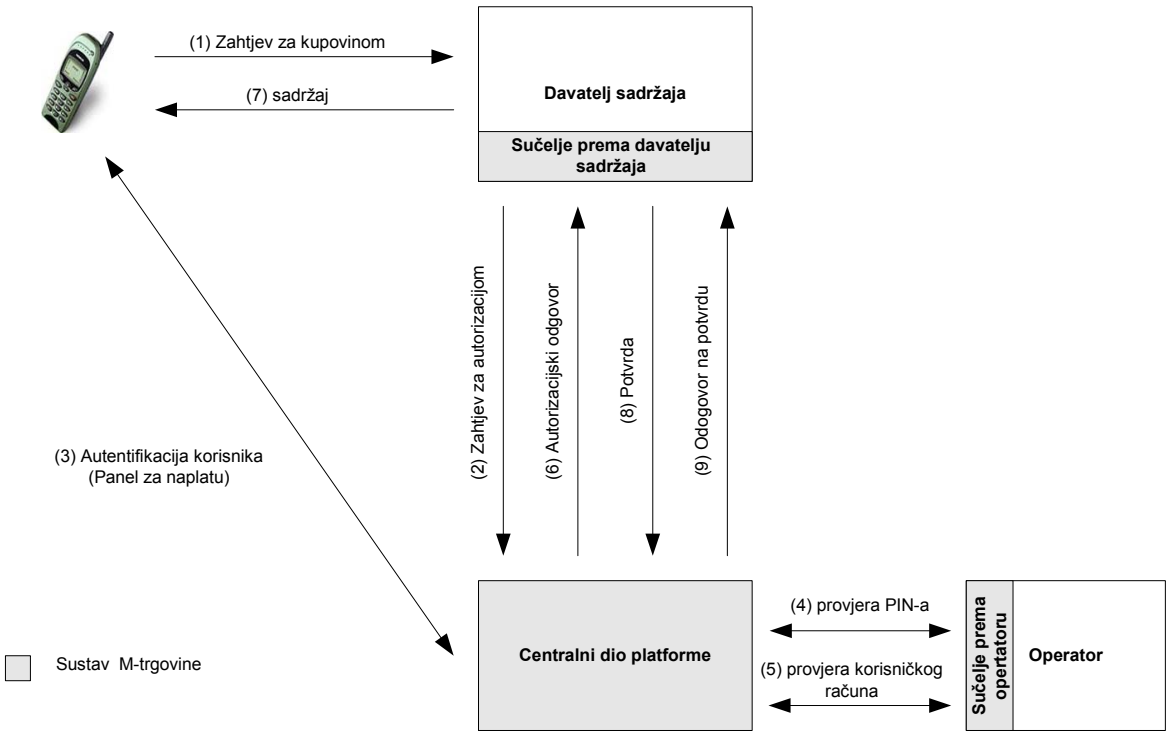
6.3.1 Plaćanje temeljeno na računu

Kod metode plaćanja temeljene na računu, svakom korisniku je pridružen specifični račun kojim upravlja platforma.

Ako se koristi *prepaid* transakcija račun se direktno povezuje s korisnikovim *prepaid* računom u postojećem sustavu obračuna operatera. Ako se koristi *postpaid* transakcija, troškovi se nalaze na korisnikovom računu. Ovi troškovi se agregiraju i periodički šalju na naplatu.

Kako tradicionalni sustav obračuna zbog visokih troškova nisu pogodni za rukovanje transakcijama vrlo niskih vrijednosti (npr. *micropayment*) zbog visokih administrativnih troškova, platforme M-trgovine imaju dio sustava obračuna koji akumuliraju ove transakcije koje mogu biti plaćene kasnije.

Na slici 6-2 je prikazano kako izgleda primjer transakcije u slučaju uporabe plaćanja temeljenog na računu.



Slika 6-2 Primjer transakcije koristeći platformu za M-trgovina s plaćanjem vezanim za račun

Primjer transakcije, u kojoj je pretpostavljeno da je korisnik unaprijed registriran, je slijedeći:

1. **Korisnik zatraži sadržaj od davatelja.** Korisnik nađe sadržaj koji ga zanima i zatraži ga koristeći (npr. wap pretraživač).

2. **Davatelj šalje zahtjev za autorizacijom korisnika platformi za M-trgovinu.** Sigurnim kanalom (obično VPN ili iznajmljena veza) davatelj usluge šalje zahtjev platformi.

3. **Upit korisniku za potvrdu.** Platforma za M-trgovinu šalje korisniku upit za potvrdu zahtjeva za sadržajem i autentifikacijom koji dobiva na zaslonu svog mobitela. Korisnik unosi svoj PIN (PIN svoje kartice) i šalje ga posredniku.

4. **Provjera korisnikove autentifikacije.** Posrednik prosljeđuje PIN operatoru koji može odobriti ili ne korisnikovu autentifikaciju.

5. **Provjera stanja korisničkog računa.** Nakon uspješne autentifikacije platforma postavlja upit Operateru o stanju korisnikovog računa. Ovo je obično neophodno u slučaju uporabe *prepaid* usluge.

6. **Odgovor na zahtjev za autorizacijom.** U slučaju da je korisnik uspješno autentificiran i da ima dovoljno novca na računu za traženu transakciju, platforma šalje potvrdu za autorizaciju uporabe sadržaja od strane korisnika.

7. **Isporuka sadržaja.** Davatelj usmjerava korisnika na stranice s traženim sadržajem.

8. **Potvrda.** Davatelj sadržaja/usluge, nakon uspješno prenesenog sadržaja, šalje platformi potvrdu o tome.

9. **Odgovor na potvrdu.** Platforma šalje davatelju usluge odgovor na primljenu potvrdu.

6.3.1.1 Arhitektura platforme za M-trgovinu za plaćanje temeljeno na računu

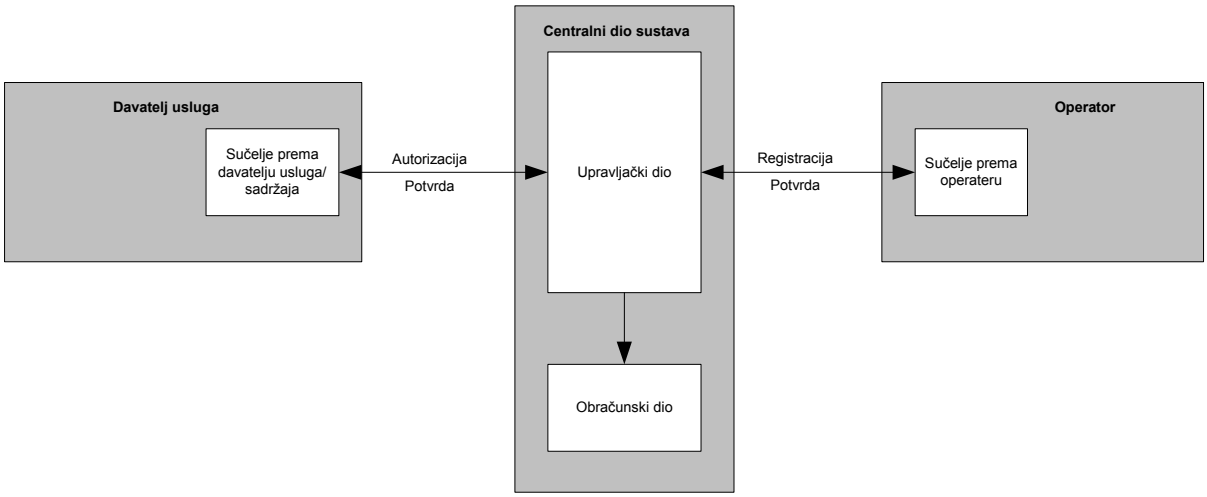
Arhitektura platforme za M-trgovinu za plaćanje temeljeno na računu se obično sastoji od četiri programske komponente:

- **Upravljački dio** koji upravlja i nadzire transakcije, poslužuje stranice koje predstavljaju sučelje prema korisniku (npr. panel za naplatu), upravlja aktivnostima korisničkih računa.

- **Obračunski dio** obavlja poslove vezane uz obradu transakcija, raspodjelu dobiti, agregaciju transakcija.

- **Sučelje prema davatelju sadržaja** je programska komponenta što povezuje davatelja sadržaja i komunicira s upravljačkim dijelom vezano uz transakcijsku informaciju.

- **Sučelje prema operateru** je veza prema operaterovom sustavu (autentifikacija, obračun).



Slika 6-3 Osnovni dijelovi platforme za M-trgovinu za plaćanje temeljeno na računu

Upravljački dio

Upravljački dio sačinjavaju upravljanje sustavom te skup web aplikacija i usluga što omogućuju osnovno procesiranje transakcija. Ovaj dio je zadužen za upravljanje, konfiguriranje aktiviranje korisnika, autorizaciju transakcija i upravljanje korisničkim računima.

Obračunski dio

Obračunski dio dobiva neobrađene transakcije od upravljačkog dijela i obavlja slijedeće zadatke:

- Obračun cijena transakcija,

- Razdjela zarade za podjelu dobiti između operatera i davatelja sadržaj,
- Agregiranje transakcija za obračun između operatera i davatelja sadržaja.

Obračunski dio se može zamijeniti postojećim sustavom obračuna ukoliko ima podržane gore navedene funkcije. Primjer takvog sustav obračuna je Convergys "Geneva".

Sučelje prema operatoru

Sučelje prema operatoru je obično Java program prilagođen integraciji u sustav operatora. Ono funkcionira kao most između upravljačkog dijela i operatora. Ovo omogućava operatoru interakciju s upravljačkim dijelom u cilju kreiranja korisničkog računa, autentifikacije, autorizacije i funkcija upravljanja računom.

Ovo sučelje zahtjeva integraciju s dijelom sustavom operatora koji vodi računa o korisničkim računima, naplati i autentifikaciji koji vrši autentifikaciju korisnika i autorizaciju transakcije.

Sučelje prema davatelju sadržaja/usluga

Sučelje prema davatelju sadržaja/usluga je program koji davatelj sadržaja/usluga instalira unutar svoje platforme za e-trgovinu cilju generiranja i interpretiranja poruka poslanih i primljenih od upravljačkog dijela. Ovo sučelje dopušta davatelju prodaju bilo kojih produkata i usluga po bilo kojoj cijeni.

Ova sučelja se obično nalaze pakirana u tzv. SDK (engl. *Software Development Kit*) ili osnovni kit. Osnovni kit je obično vrlo jednostavan za instalirati i može omogućiti transakcije vrlo brzo. Kod ovog rješenja nije potreban dodatni razvoj rješenja, nego se konfiguriraju datoteke koji opisuju produkte koje prodaje davatelj usluga/sadržaja i modificiraju njegove WML stranica koje uključuju veze na sustav M-trgovine. Ovo rješenje se koristi kod prodaja digitalnih sadržaja, odnosno dobara.

SDK predstavlja zapravo programska biblioteka za integriranje platforme za M-trgovinu u postojeću platformu e-trgovine. Ovo rješenje omogućava vrlo tijesnu integraciju s postojećom platformom E-trgovine i vrlo je fleksibilno. Najviše koristi kod prodaje fizičkih sadržaja, odnosno dobara.

Osnovni zadaci ovog sučelja su:

- Iniciranje transakcije. Ovo rezultira potvrdom ili odbijanjem autorizacije.
- Potvrda autorizacije.
- Odbijanje autorizacije.

6.3.2 Plaćanje temeljeno na žetonu

Ovo rješenje predstavlja alternativu rješenju temeljenom na računu u kojem postoji račun za svakog korisnika. Žeton se definira kao sredstvo razmjene koje predstavlja određenu monetarnu vrijednost obično pohranjenu u banci ili kod operatera. Žetoni se izmjenjuju tokom transakcije. Umjesto žetona često se rabi i izraz kupon.

U ovom načinu plaćanja korisnik treba zamijeniti određenu količinu novca u elektronički ekvivalent, žetone. Žetoni se mogu pohraniti npr. u korisnikov mobilni uređaj. Postojeće implementacije spremišta žetona uključuju zaštitu lozinkama radi osiguranja u slučaju da ako je uređaj na kojem se nalaze žetoni izgubljen ili ukraden.

Ova metoda omogućuje anonimnost korisnika.

Jedan od prednosti ove metode je u tome da je pogodna za upravljanje mikro plaćanjima (engl. *Micropayment*) zbog toga što su troškovi administriranja relativno niski u usporedbi s metodom zasnovanom na računu.

Na slici 7-4 je prikazana tipična *postpaid* transakcija po prenesenoj jedinici (npr. razina igre). Zbog pojednostavljenja nije prikazan WAP *gateway* između HTTP poslužitelja i korisnika.

1. **Korisnik zatraži sadržaj od davatelja.** Korisnik nađe sadržaj koji ga zanima i zatraži ga koristeći npr. wap pretraživač.
2. **Sučelje prema davatelju usluga prosljeđuje detalje kupovine platformi za M-trgovinu.** Sigurnim kanalom (obično VPN ili iznajmljena veza) davatelj usluge šalje zahtjev platformi za M-trgovinu.
3. **Platforma za M-trgovinu šalje nepotpisani ugovor HTTP poslužitelju davatelja usluge.** Ugovor obično sadrži detalje poput cijene, usluge koji korisnik kupuje, vrijeme, datum itd.

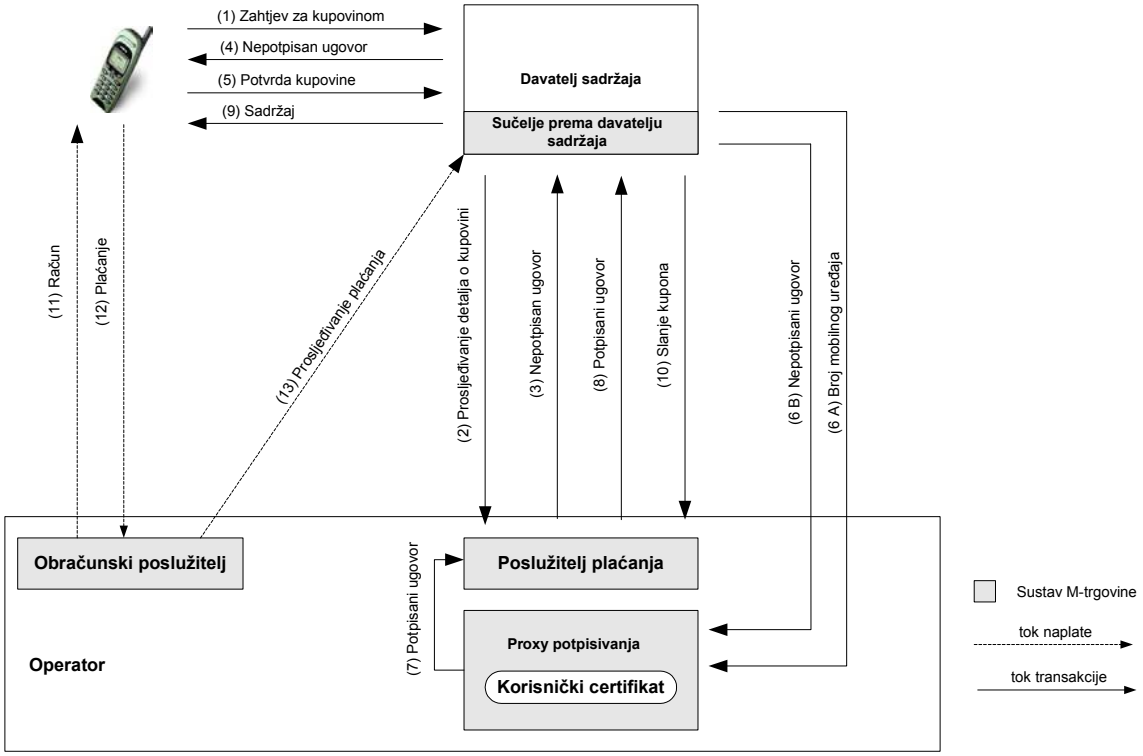
4. **Korisnik dobiva nepotpisani ugovor.** Korisnik dobiva od poslužitelja nepotpisani ugovor.

5. **Korisnik potvrđuje kupovinu.** Korisnik potvrđuje kupovinu obično pritiskom na određeni hiperlink ili gumb na zaslonu svoga aparata.

6. **Nepotpisani ugovor i broj korisnikovog mobilnog uređaja se šalju proxy-u potpisa.** Slanje se obavlja kao *cookie* u polju HTTP zaglavlja. Broj korisnikovog mobilnog aparata je dobiven od WAP *gateway*-a. Ovo se obavlja na način da WAP *gateway* u HTTP zahtjevu koji šalje poslužitelju umeće broj mobilnog uređaja koji mu je poslao zahtjev.

7. **Potpisivanja ugovora.** *Proxy* potpisivanja koristi korisnikove certifikate za potpisivanje ugovora. Korisnik treba preregistrirati svoj mobilni broj s *proxy*-em potpisivanja.

8. **Slanje davatelju usluga obavijesti o potpisanom ugovoru.** Davatelj usluga dobiva potpisani ugovor.



Slika 6-4 Primjer transakcije koristeći platformu M-trgovine s plaćanjem žetonima

9. **Slanje sadržaja korisniku.** Korisniku se omogućuje pristup traženoj usluzi.

10. **Slanje kupona.** Sučelje integrirano u aplikaciju davatelja usluge šalje kupone, gdje je svakom kuponu pridružena određena monetarna vrijednost. Kuponi mogu biti vrijeme trajanja, klik mišem, nivo igre, itd.

11. **Platforma šalje agregirani račun korisniku.** Platforma analizira kupone u cilju određivanja relevantnog podatka za naplatu i šalje agregirani račun korisniku.

12. **Korisnik vrši plaćanje.** Korisnik vrši plaćanje operatoru. Plaćanje se obično vrši kroz mjesečni račun.

13. **Slanje plaćanja davatelju usluge.** Plaćanje kupljenog sadržaja se prosljeđuje davatelju usluge/sadržaja.

6.3.2.1 Arhitektura platforme za M-trgovine za plaćanje temeljeno na žetonima

Kao što je prikazano osjenčano na slici 7-4 ova arhitektura se sastoji: *proxy*-a potpisivanja, sučelja prema davatelju usluga, poslužitelja plaćanja i obračunskog poslužitelja. Implementirana sigurnost ove arhitekture je temeljena na RSA PKI enkripciji.

Proxy potpisivanja

Proxy potpisivanja je poslužitelj koji potpisuje ugovore o kupovini u ime korisnika. On se nalazi zajedno s poslužiteljem plaćanja unutar operaterovog sustava. Sadržavajući korisnikove certifikate ovaj poslužitelj sadrži digitalne potpise koje postojeće izvedbe mobilnih uređaja ne mogu držati kod sebe.

Sučelje prema davatelju usluga

Ovo sučelje, integrirano u aplikaciju E-trgovine davatelja usluga, omogućava iniciranje sesije, autentifikaciju korisnika i slanje kupona poslužitelju plaćanja zasnovano na korisnikovom uporabi usluge. Kupon ili žeton je ime dano jedinici uporabe. Primjer je pritisak na gumb na mobilnom uređaju koji može korespondirati jednom kuponu. Ovo sučelje se obično zasniva na filozofiji objektnog dizajna temeljenog na konceptu sesije.

Poslužitelj plaćanja

Ovaj poslužitelj omogućava operateru usluge plaćanja davatelju usluge. On upravlja transakcijom i računima za operatera i davatelja usluge/sadržaja, administrira primanje kupona i održava zapis o njima.

Obračunski poslužitelj

Obračunski poslužitelj je integriran s postojećim sustav obračuna operatera ili predstavlja sustav obračuna nove generacije, koji omogućava jednostavnu obradu računa korisnika i obračunom prema davatelju usluge (zaračunavanje naknade za obračunavanje).

6.4 Zaključak

M-trgovina rješenje je rješenje koje je jednostavno implementirati u postojeći sustav naplate u mobilnim sustavima. Iako ovo rješenje prvenstveno pruža mogućnost kupovine i transakcija preko mobilnih uređaja postoji mogućnost nadogradnje naplate sadržaja kojima se unaprijed ne zna cijena. To se postiže slanjem zahtjeva za preautorizacijom određene količine sredstava za npr. 10 minuta uporabe neke usluge, nakon čega se za narednih 10 minuta šalje slijedeći zahtjev.

Kako se glavnina komunikacija odvija direktno između pojedinih dijelova sustava te zbog kriptiranja veza sigurnost informacija je velika. Informacije o samom korisniku, njegovom računu i iznosu novca na njemu ostaju nepoznate davatelju usluga.

Nova rješenja poput uporabe JavaCard i WIM će omogućiti uporaba sofisticiranih klijentskih aplikacija temeljenih na mobilnom uređaju. JavaCard specifikacije omogućuju Java tehnologiji pokretanje na karticama s limitiranom memorijom. WIM omogućava korisnicima spremanje javnih ključeva i digitalnih certifikata na njihovim uređajima. Na ovaj način će se transakcije moći obavljati brže i jednostavnije.

Od gore navedenih rješenje prvo rješenje, u kojem se naplata veže uz račun trenutno se više koristi, no mogućnosti spremanja digitalnih certifikata na mobilnim uređajima omogućiti će daljnji razvoj drugog rješenja.

7 Eksperimentalni model sustava za naplatu URL temeljenih WAP sadržaja

Sadržaji i usluge koje se nude korisnicima mobilnih paketskih mreža ograničeni su izvedbom mobilnih uređaja. Postojeći mobilni uređaji mogu primati samo sadržaj na dva načina: preko SMS poruka, preko WAP-a.

Način naplate poruka preko SMS se vrlo jednostavno rješava slanjem SMS poruka na različite ulazne brojeve čime se vrši tarifiranje pojedine poruke. Npr. korisnik koji želi platiti parkiranje šalje poruku na recimo broj "123". Sustav definira da cijena poruke koja se šalje na taj broj odgovara cijeni jednog sata parkiranja u prvoj tarifnoj zoni odnosno 4 kn/sat.

Naplata pojedinih WAP sadržaja može se vršiti sistemom kupnje (poglavlje 7), naplatom pojedinih URL stranica (naplaćuju se samo određene stranice) ili naplatom uporabe pojedinih aplikacija. U ovom radu je izrađen prijedlog jednostavnog modela naplate pojedinih stranica, tzv. URL temeljena metoda naplate.

URL temeljena naplata je proces, u kojem nakon uspješno prenesene od korisnika zahtijevane stranice, naplativi zapis će biti generiran u WAP *gateway*-u. Kako je ovaj rad temeljen na paketskim mrežama, model se bazira na uporabi WAP usluga preko GPRS mreže.

7.1 Cilj eksperimentalnog modela

Cilj ovog eksperimentalnog modela je opis načina na koji postojeći WAP CDR-ovi mogu biti korišteni za URL temeljenu naplatu sadržaja dostupnog preko WAP-a.

Model opisuje:

- Način generiranja CDR-ova,
- Njihov sadržaj,
- Način obrade u postojećem sustav medijacije,
- Model rasporeda i generiranja sadržaja na web poslužitelju.

Kao *wap gateway* se koristi Nokia Artus Messaging Platform Release 2.2 WAP.

Model ne opisuje:

- Omogućavanje i aktiviranje usluge,
- Obračunske platforme.

7.2 Postojeći sustav naplate WAP pristupa

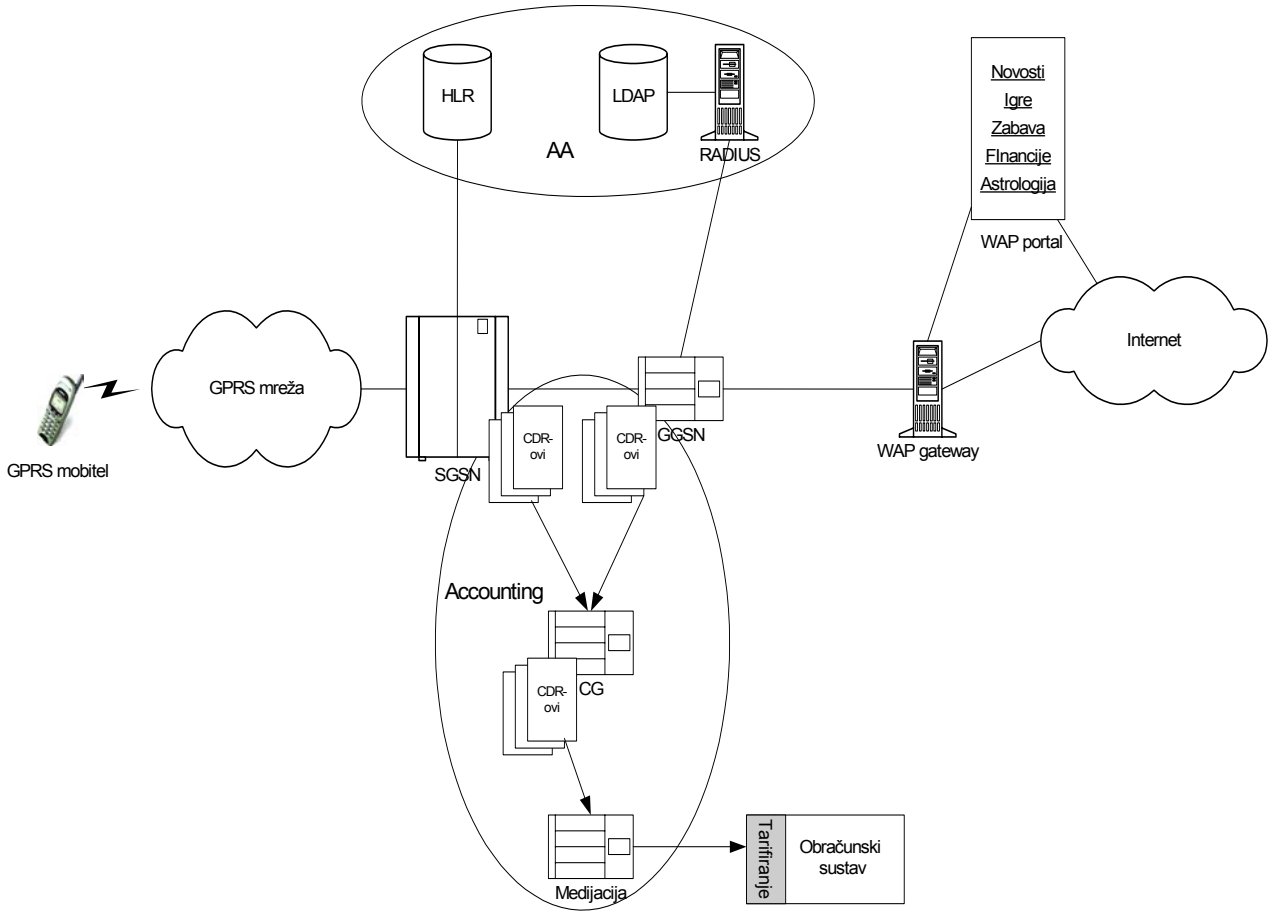
Postojeći sustav naplate uporabe WAP usluge bazira se na naplati pristupa WAP-u: GPRS, odnosno GSM. Korisnik plaća količinu prenesenih podataka (GPRS), odnosno vrijeme provedeno koristeći uslugu (GSM).

Slika 7-1 prikazuje postojeći sustav naplate u GPRS mreži. Sustav se sastoji od autentifikacije i autorizacije korisnika te generiranja i obrade CDR-ova. CDR-ovi se generiraju u GPRS čvorovima zavisno o količini prenesenog prometa. Za autentifikaciju i autorizaciju koristi se RADIUS poslužitelj povezan s GGSN-om te HLR. U HLR-u se nalazi korisnikov profil koji sadrži podatke da li korisnik ima dopuštenje uporabe pojedine usluge/APN-a.

Kada korisnik zatraži uporabu WAP-a, ukoliko ima omogućenu tu uslugu u HLR-u, njegov zahtjev se šalje GGSN-u koji prosljeđuje zahtjev RADIUS poslužitelju. RADIUS poslužitelj dodjeljuje korisniku IP adresu iz skupa adresa rezerviranih za WAP uslugu. Time se korisniku omogućava uporaba WAP usluga. Podatke o korisnikovoj IP adresi i sesiji RADIUS zapisuje u LDAP poslužitelj. CDR–ovi se generiraju u GPRS čvorovima zavisno o količini prenesenog prometa. Nakon toga se u realnom vremenu prenose u CG gdje se koreliraju. Na izlazu CG dobivamo jedinstveni CDR koji je sadrži informaciju u uporabi usluge tokom cijele sesije. Takav CDR se dalje šalje u sustav medijacije koji ga dodatno provjerava, obrađuje i šalje sustavu obračuna na naplatu

WAP *gateway* koji povezuje korisnikov mobilni uređaj na mrežu konverzijom WAP protokola u HTTP protokol također generira CDR-ove, no nema mogućnost identifikacije korisnika po njegovom IMSI-u ili MSISDN-u, zbog toga što GGSN se ponaša kao klasičan usmjerivač i jedino šalje informaciju o trenutnoj korisnikovoj IP adresi.

Ovakav sustav nema mogućnost praćenja i identifikacije spajanja korisnika na pojedine stranice, odnosno sadržaje.



Slika 7-1 Postojeći sustav naplate u GPRS mreži

7.3 Osnovne pretpostavke eksperimentalnog modela

Osnovne pretpostavke eksperimentalnog modela odnose se na polja u WAP CDR-ovima koje je moguće koristiti za naplatu sadržaja, model sustava, način dobivanja MSISDN informacije u WAP *gateway* CDR-ove, metode i scenarije naplate.

7.3.1 WAP CDR

Osnovna ideja eksperimentalnog modela je uporaba WAP CDR-ova umjesto CDR-ova koje generiraju čvorovi. CDR-ovi dobiveni s čvorova bilježe jedino uporabu WAP usluge i količinu prenesenog prometa. U njima ne postoji informacija o uporabi pojedinih sadržaja odnosno posjećivanju WAP stranica. Tu informaciju sadrže WAP CDR-ovi.

Najvažnija polja WAP CDR, WAP *gatewaya* korištenog u ovom eksperimentu prikazana su u tablici 7-1.

Tablica 7-1 Najvažnija polja WAP CDR-a

CDR polje	*Comment*
Start Transaction	Vrijeme početka transakcije
End transaction	Vrijeme kraja transakcije
MSISDN	MSISDN broj mobilnog terminala
IP-Address	IP adresa mobilnog terminala
Service ID	ID usluge za zahtijevani URL, dobiven od tarifne datoteke
Tariff Class	Informacija korištena za tarifiranje usluge dobivena od tarifne datoteke
Success Indicator	Uspjeh prijenosa
Uplink/Downlink Data Volume	Količina prenesenih podataka.
Bearer Type	Indikator *prepaid* usluge.
GGSN ID	IP adresa GGSN-a
Charging ID	Jedinstveni naplatni broj za pojedinu transakciju

URL se definira u tarifnoj datoteci i mapira se u WAP CDR kao "ID usluge". "Tarifna klasa" definira kojoj tarifnoj klasi pripada pojedina URL stranica. Na ovaj način svakoj URL stranici ili skupini njih se pridružuje informacija o kakvoj se usluzi/sadržaju radi, davatelju usluge i tarifi za tu uslugu. Ove informacije se mogu konfigurirati u tarifnoj datoteci.

Primjer uporabe ovog modela je slijedeći. Pretpostavimo da se davatelj usluge "Sportske novice" čija na web stranica nalazi na adresi www.sportske_novice.hr. Za stranice koje se naplaćuju na toj adresi definirati ćemo "ID usluge" 1xx, gdje sa jedan označavamo davatelja usluge (u našem slučaju "Sportske novice"), a sa x-evima pojedinu uslugu (npr. teniski rezultat). "Tarifna klasa" definira koliko pojedina stranica košta. Za stanice koje koštaju 0.5 kn definiramo npr. tarifnu klasu 200.

Vrlo bitno polje u tablici je polje koje definira prenesenu količinu podataka. Ova informacija omogućava uporabu samo WAP CDR-ova čime se izbjegava potreba uporabe CDR-ova dobivenih u GPRS čvorovima.

Polje MSISDN jedinstveno određuje korisnika. Kako se ova informacija ne može dobiti direktno preko GGSN potrebno je drugačiji način.

7.3.2 Model sustava

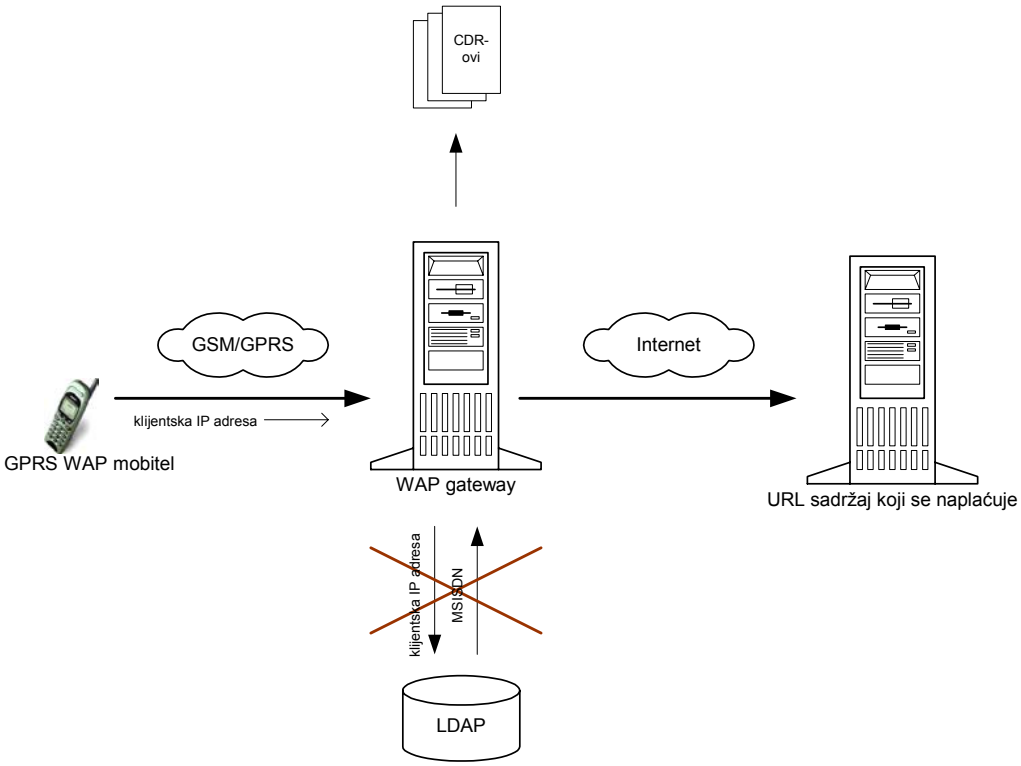
Osnovna ideja eksperimentalnog modela je u uporabi WAP portala preko kojeg korisnik može pristupati sadržajima. WAP portalu mogu pristupati jedino korisnici unutar operaterove GPRS mreže. Ovo se dobiva postavljanjem WAP *gatewaya* unutar Intranet mreže operatera.

Korisnici definiraju WAP portal kao polaznu točku za pretraživanje sadržaja. WAP portal se povezuje s davateljima sadržaja iznajmljenim/VPN linijama. Ovaj sustav koji odgovara poluzatvorenom NTT DoCoMo sustavu je najjednostavniji za implementiranje i lako se može nadograditi na sustav broker ili sustava otvorenog tipa uporabom dodatne autentifikacije korisnika.

7.3.3 MSISDN informacije u WAP gateway-u

Prilikom uspostave WAP sesije, RADIUS server dodjeljuje mobilnom terminalu IP adresu. Tom prilikom se sve bitne informacije (MSISDN, IP adresa, vrijeme uspostave sesije,...) o sesiji zapisuju u LDAP poslužitelj, u korisnički profil pojedinog korisnika.

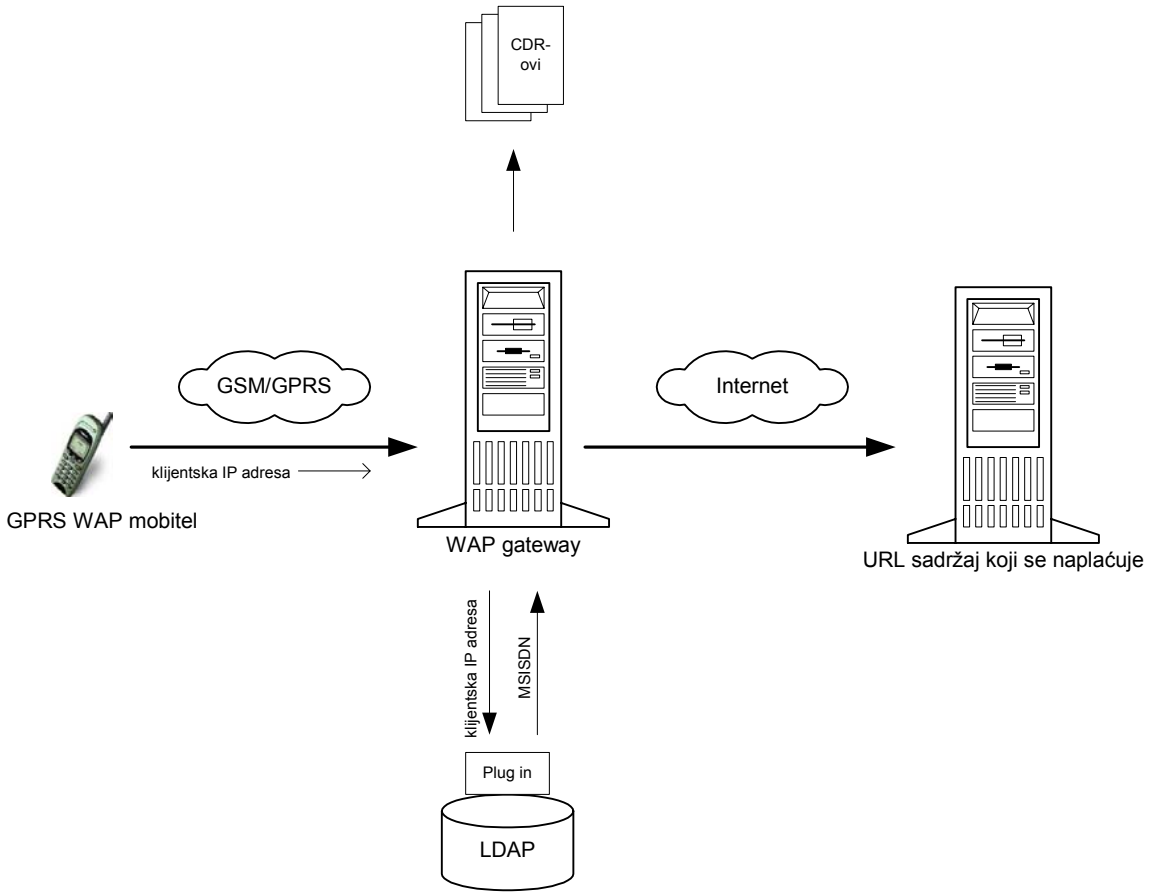
WAP *gateway* dobiva informaciju o IP adresi korisnika koji se preko njega spaja na pojedinu web stranicu. Da bi saznao MSISDN korisnika, on mora poslati upit LDAP poslužitelju. LDAP poslužitelj pronalazi trenutnog korisnika IP adrese i vraća WAP *gatewayu* korisnikov MSISDN. Pošto su korišteni LDAP poslužitelj i WAP *gateway* različitih proizvođača nije bila moguća direktna komunikacija između njih (Slika 7-2). Za potrebe eksperimenta pretpostavljena je komunikacija između LDAP i WAP *gatewaya* i postojanje MSISDN informacije u CDR-ovima.



Slika 7-2 Generiranje CDR-ova bez povezivanja s LDAP-om

Predloženo rješenje za uspostavu komunikacije sastoji se u izrade *plug in* na LDAP server koji konvertira zahtjeve na način da WAP GW može komunicirati s LDAP korisničkom bazom. Ovaj *plug in* mora biti implementiran u skladu s WAP GW LDAP specifikacijom sučelja. Slika 7-3 prikazuje arhitekturu takvog rješenja.

Uz mogućnost uporabe MSISDN broja korisnika u WAP CDR-ovima, ovim rješenjem se omogućava i slanje MSISDN broja preko WAP *gatewaya.* Na taj način će udaljeni davatelj sadržaja imati mogućnost pratiti tko pristupa njegovom sadržaju i po MSISDN broju ili nekom drugom indetifikacijom izvedenom iz njega može dopustiti korisniku uporaba sadržaja ili ne. Osnovna ideja ovog eksperimenta je bila ispitivanje mogućnosti naplate pojedinih URL sadržaja uporabom poluzatvorenog sustava NTT DoCoMo te u ovom slučaju dodatna autentifikacija nije bila potrebna.



Slika 7-3 Generiranje CDR uz uporabu LDAP *plug in*-a

7.4 Metode naplate

Osnovne dvije metode naplate su *prepaid* i *postpaid*. Radi jednostavnosti odlučeno je da se eksperiment temelji samo na *postpaid* metodi.

7.5 Scenariji naplate

Način naplate pojedinih sadržaja ovisi o željama marketinga. Za slučaj naplate sadržaja postoji nekoliko scenarija naplate. U tim scenarijima korisnik se može naplatiti:

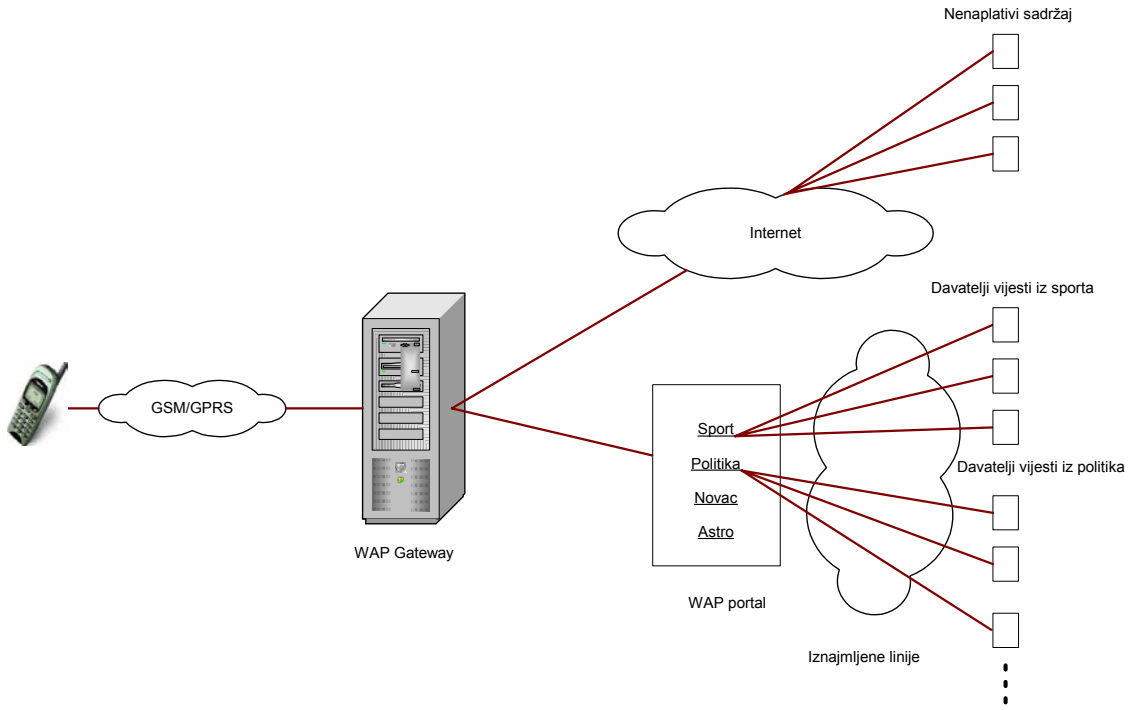
- Pristup,
- Sadržaj,
- Oboje istodobno.

Zadatak eksperimenta je bio utvrditi mogućnosti za sva tri slučaja. Najteži slučaj je onaj u kojem se naplaćuje samo sadržaj jer u tom je slučaju potrebno, kako će kasnije biti objašnjeno, oduzeti količinu prenesenih podataka u slučaju kada korisnik pregledava sadržaje koji se naplaćuju.

7.6 Arhitektura eksperimentalnog modela

Kao što je prije napomenuto u ovom modelu koristi se pristup sadržaju preko portala. Davatelj sadržaja može biti operater ili strani davatelj koji ima potpisan ugovor i iznajmljenu, odnosno VPN komunikaciju koja ga povezuje s WAP *gatewayem* operatera. Slika 7-4 prikazuje ideju načina na koji korisnik pristupa naplativim i nenaplativim sadržajima.

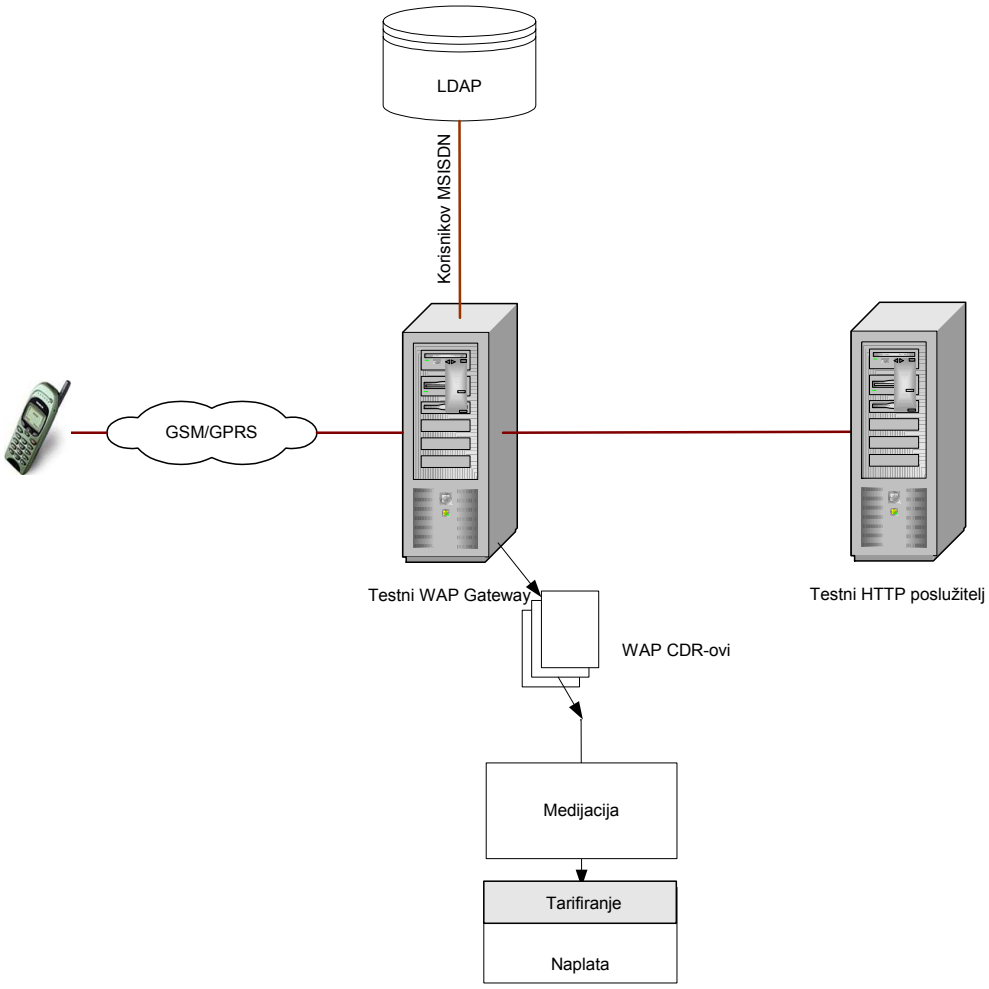
Korisnik će platiti samo za konkretne sadržaje, odnosno ne plaća za kretanje po osnovnim menijima. Npr., korisnik kojeg zanima stanje pojedinih dionica će prvo na portalu izabrati temu "Novac" na njoj rubriku stanje dionica te konačno stanje samih dionica. Prije nego zatraži stanje biti će obaviješten da se ta usluga naplaćuje. Kada potvrdi, dolazi na stranicu s informacijom. Korisniku će biti naplaćena samo informacija ne i stranice koje su joj prethodile.



Slika 7-4 Model pristupa sadržajima

Na slici 7-4 je prikazan način pristupa sadržajima koji se želio simulirati eksperimentom. Za potrebe eksperimenta umjesto odvojenog WAP portala i različitih davatelja usluga korišten je HTTP poslužitelj. Slika 7-5 prikazuje način na koji je realiziran eksperimentalni model. Za razliku od postojećeg modela naplate WAP sadržaja objašnjenog u poglavlju 7.2 naplate informacija o uporabi se više ne skuplja na GPRS čvorovima nego na WAP *gatewayu*. Na taj način se izbjegava i uporaba CG u procesu obrade WAP CDR-ova.

Za izvedbu ovog modela su dodatno izvedene prepravke u sustav medijacije kako bi se obradili CDR-ovi te na izlazu dobio format prikladan sustavu obračuna.



Slika 7-5 Arhitektura eksperimentalnog modela

7.6.1 Testna oprema

7.6.1.1 HTTP poslužitelj

Za simuliranje WAP portala i sadržaja pojedinih davatelja korišteno je osobno PC računalo.

Karakteristike računala i *software*-a:

- AMD Thunderbird radnog takta 1 GHz,
- 256 MByta DDR radne memorije,
- 40 GByta hard diska,
- RedHat 7.2 distribucija Linux operativnog sustava,
- Apache 1.3.23 HTTP poslužitelj,

- PHP v. 4.0,
- PostgreSQL v.7.0 baza podataka.

7.6.1.2 Sustav medijacije

Sustav medijacije korišten u ovom radu je Comptel MDS/ARM Release 3.6.0.

7.6.1.3 Sustav obračuna i tarifiranja

Sustav obračuna i tarifiranja korišten u ovom sustavu je Convergys Geneva v. 4.2.

7.6.1.4 Testni mobitel

Testni mobitel korišten u ovom eksperimentu je Nokia 7110 sa ugrađenom WAP 1.1. podrškom.

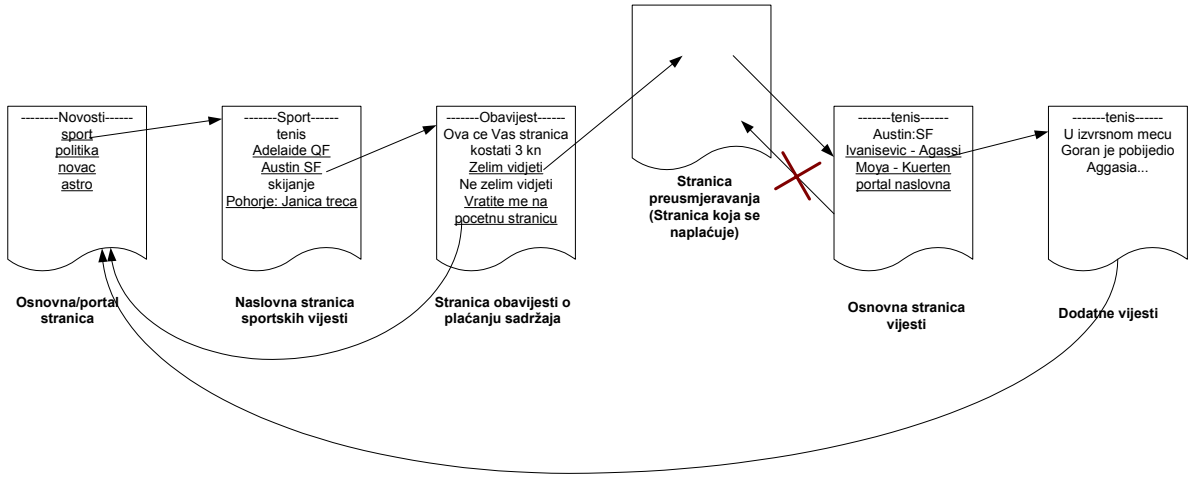
7.6.2 Osnovni model naplate pojedinih stranica i kreiranje CDR-ova

Kako WAP *gateway* ima mogućnost generiranja CDR-ova za svaku uspješnu transakciju/učitanu stranicu ta je mogućnost korištena u ovom eksperimentalnom modelu. Osnovni princip je definiranje direktorija u kojima se nalaze naplative stranice.

Za izvedbu ovog rješenja korištena je mogućnost definiranja "tarifne klase" za pojedine URL-ove. Na ovaj način će svi sadržaji koji imaju određeni URL biti naplaćeni dok drugi neće. U eksperimentalnom modelu nije korištena i mogućnost ID usluge kojom bi se moglo dodatno definirati cijena pojedinih usluga. Za potrebe eksperimenta korištena je jedinstvena cijena za sve sadržaje.

U zasebnom "tariff" datoteci je definiran URL poslužitelja i direktorij čiji sadržaj se naplaćuje (80.108.135.21/~msikic/wap/charged). Na taj način jedino sadržaji iz tog direktorija biti će naplaćeni korisniku. Dodatno se definira direktorij (80.108.135.21/~msikic/wap/temp) u kojem se nalazi dodatni sadržaji naplative informacije koji se dodatno ne naplaćuju.

Slika 7-6 prikazuje model naplate stranica.

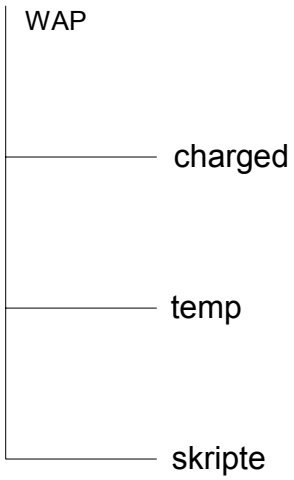


Slika 7-6 Model naplate stranica

Kada korisnik dođe do sadržaja koji se naplaćuje prvo mu se prikazuje stranica koja ga obavještava o cijeni sadržaja. Ako želi vidjeti sadržaj potvrđuje i link ga vodi na stranicu preusmjeravanja koja nakon što se učita odmah ga prebacuje na prvu stranicu traženog sadržaja. S te stranice korisnik ima pristup ostalim stranicama traženog sadržaja. Stranice preusmjeravanje se naplaćuje i spremaju u zaseban direktorij "charged", dok se stranice naplative informacije spremaju u direktorij "temp". Korisniku se ne omogućava "back funkcija" na prvoj stranici naplative informacije. Na taj način on ne plaća dodatno gledanje sadržaja već će platiti jedino u slučaju ako ponovi cjelokupan postupak. Stranice s traženim sadržajem su korisniku dostupne neko vrijeme, recimo npr. 10 minuta nakon čega se korisniku onemogućava ponovni pristup sadržaju. Ako želi ponovo vidjeti sadržaj mora ponoviti proceduru čime će mu ponovno biti naplaćeno uporaba traženog sadržaja. Na ovaj način se sprječava da korisnik spremi stranice sa sadržajem i kasnije ih ponovo učitava.

Kako bi ovo rješenje funkcioniralo potrebno je organizirati strukturu direktorija na poslužitelju. Slika 7-7 prikazuje izvedbu direktorija na HTTP poslužitelju. Stranice preusmjeravanja se spremaju u direktorij "charged", naplativ sadržaj, a skripte u direktorij pod nazivom skripte.

Sve ostale stranice, kao što su početne stranice portala, spremaju se u osnovni wap direktorij.



Slika 7-7 Organizacija direktorija na HTTP poslužitelju

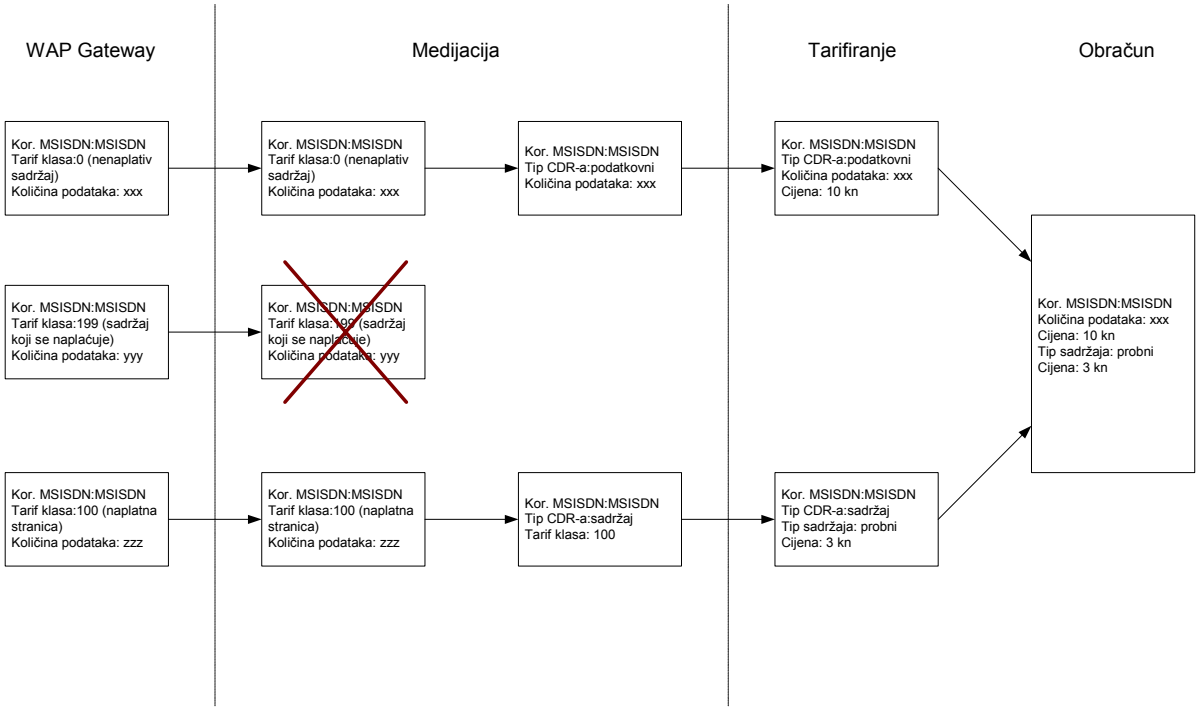
Na ovaj način u izlaznim se dobivaju CDR-ovi s tri tarifna polja. Za eksperimentalni model definiraju se sadržaji sa slijedećim tarifnim poljima:

- Nenaplativi sadržaj s vrijednošću "0" koja predstavlja predefiniranu vrijednost koju nije potrebno dodatno definirati u "tariff" datoteci,
- Naplativa, stranica preusmjeravanja s vrijednošću "100" za sve datoteke u direktoriju "charged",
- Stranice naplativog sadržaja s vrijednošću "199" za sve datoteke u direktoriju "temp".

7.6.3 Obrada CDR-ova u sustavu medijacije

Nakon što WAP *gateway* generira CDR za svaku uspješnu učitanu stranicu sprema CDR u svoj izlazni direktorij. Od tamo ga kupi sustav medijacije najčešće FTP protokolom. Sustav medijacije učitava CDR provjerava njegovu ispravnost, prilagođuje ga izlaznom formatu koji sustav obračun odnosno tarifiranja razumije.

Eksperimentalni model podrazumijeva model naplate u kojem se za naplativ sadržaj ne naplaćuje dodatno pristup u mrežu. Model naplate u kojem se naplaćuje i pristup i sadržaj se jednostavno dodaje definiranjem novog tipa CDR-a. Takav CDR bi se u sustav medijacije dijelio na dva CDR: pristupni i sadržajni.



Slika 7-8 Obrada CDR-ova

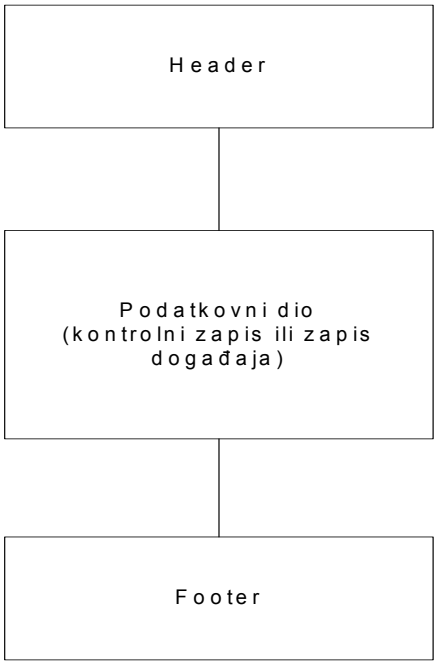
Slika 7-8 prikazuje prolaz CDR-ova kroz medijaciju tarifiranje i sustav obračuna. Sustav medijacije obrađuje pristigle CDR-ove na način da:

- CDR–ove s tarifnom klasom "0" pretvara u "podatkovne" i takve zapisuje u izlazni direktorij,
- CDR–ove s tarifnom klasom "199" odbacuje pošto stranice koje ga generiraju sadrže samo sadržaj koje je korisnik već unaprijed platio, a u ovom slučaju količina prenesenih podataka ne naplaćuje,
- CDR–ove s tarifnom klasom "100" pretvara u "sadržajne" takve zapisuje u izlazni direktorij.

Sustav tarifiranja uzima izlazne CDR-ove iz sustava medijacije, te im ovisno o tipu dodjeljuje određenu cijenu za preneseni kB odnosno, 3 kn po sadržaju. Sustav obračuna stavlja sve zapise iz tarifiranja na račun, zbraja ukupnu naknadu za uporaba sadržaja i usluga i to šalje sustavu za izdavanje računa.

7.6.4 Oblik CDR-a u izlaznom direktoriju sustava medijacije

CDR u izlaznom direktoriju sustav medijacije predstavlja ulazni format sustava tarifiranja. Format je izrađen u skladu s IPDR.org specifikacijom i korišten je isključivo za ovo testiranje. Format CDR-a odnosno datoteke se može podijeliti na tri dijela: *header*, podatkovni dio i *footer* kao što je prikazano na slici 7-9.



Slika 7-9 Opći format izlaznog medijacijskog CDR-a

- *Header* definira tipove i podtipove datoteke. Oni su linije teksta.

- Podatkovni dio sadrži sve informacije i varira zavisno o tipu. Sva polja moraju biti predstavljena iako nemaju definirane vrijednosti (engl. *null*). Svako polje unutar zapisa je odvojeno zarezom (CVS). Zapis završava karakterom nove linije (heksadecimalna vrijednost 0A). Kada je vrijednost *null* označava se zarezom.

Kako je sustav tarifiranja i obračuna predstavljao sustav obračuna "Geneva", korišten je njen format podataka uz definiciju specijalnih polja za ovo testiranje [9].

Na slici se nalazi format zapisa specificiran za ovo testiranje. Format se odnosi samo na podatkovni dio koji je mijenjan za potrebe ovog testiranja.

Unutar zapisa svako polje se specificira kao jedno od:

- Z – zahtijevano, mora biti definirano u,
- O - opcionalno, ako je dostupno u medijaciji definira se, inače je *null,*
- N – null, nije zahtijevano.

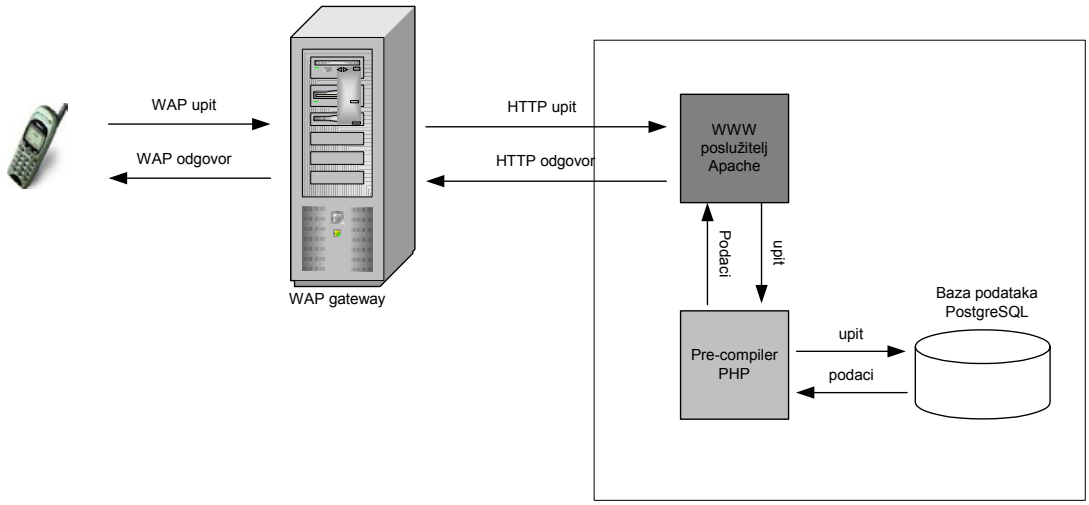
Broj atributa	Ime	Maximalna duljina	Tip	Klasa	Opis
STANDARDNA POLJA					
	Tag	6	Text	Z	
	Event Source	40	Text	Z	MSISDN
	Event Type	9	Int	Z	10 – WAP_volumen 11 – WAP_content
	Event DTM	22	DTM	Z	Vrijeme u formatu yyyy/mm/dd-hh-mm-ss.tt s vodećim nulama gdje je to potrebno
	Cost Centre	9	Int	N	Ne koristi se
	Currency code	3	Text	N	Ne koristi se
	Event Cost	10	Int	N	Ne koristi se
	Loyalty Points	9	Int	N	Ne koristi se
	Competitor cost	10	Int	N	Ne koristi se
	Internal cost	10	Int	N	Ne koristi se
	External Cost	10	Int	N	Ne koristi se
	Tax Override	9	Int	N	Ne koristi se
POLJA DEFINIRANA OD KORISNIKA					
1	Mediation Process Id	40	Text	Z	Broj specificiran od strane sustava medijacije
2	Duration	40	Text	Z	Vrijeme trajanja transakcije u formatu "hh:mm:ss"
3	Uplink and Downllink Volume	40	Text	O	Količina prenesenih podataka u bytovima. Ne koristi se u sadržajnim zapisima
4	Service Element Id	40	Text	Z	Element koji generira zapise. Uvijek "WAP_gateway"
5	GGSN Id	40	Text	O	IP adresa GGSN-a
6	Content Provider	40	Text	Z	Za sada uvijek "Test"
7	Tariff Class	40	Text	O	Moguće vrijednosti su "0" i "100"
8	Service ID	40	Text	O	Za sada se ne koristi
9	Sucess Indikator	40	Text	Z	Uvijek "1"
10	Charging Id	40	Text	O	Redni broj naplate
11	Unit Type	40	Text	O	Uvijek "Byte"
12	Content Detail	40	Text	Z	Za sada uvijek "Test"
13-24	Attributes 13 to 24	40	Text	N	Ne koristi se

Slika 7-10 Format podatkovnog dijela zapisa korišten u eksperimentu

Primjeri zapisa korištenih u ovom eksperimentu mogu se vidjeti u prilogu.

7.6.5 Način generiranja stranica na HTTP poslužitelju

Generiranje dinamičkih stranica, njihov smještaj i uklanjanje nakon definiranog vremena (10 minuta) riješeno je uporabom php jezika i postgresql baze podataka. Kao HTTP poslužitelj korišten Apache podignut na RedHat 7.2 Linux platformi. Osnovni princip generiranja stranica prikazan je na slici 7-11.



Slika 7-11 Generiranje stranica na HTTP poslužitelju

Da bi HTTP poslužitelj mogao raditi s wml stranicama dodani su formati vezani uz wml u konfiguraciju poslužitelja.

Za generiranje dinamičkih stranica korištene su php skripte scr1 i scr2. Obje ove skripte nalaze se u prilogu. Baza podataka nije bila popunjena do kraja tako da se moglo pratiti zbivanje u slučajevima kada upit ne rezultira traženim sadržajem. Za uklanjanje dinamičkih stranica starijih od deset minuta koristila se skripta za uklanjanje stranica također prikazana u prilogu.

7.7 Testiranje i rezultati

Testiranje modela se svodilo na ispitivanje da li će na izlazu sustav obračuna za svaki uspješan upit odgovarajući CDR biti kreiran.

Testiranje je pokazalo da eksperimentalni sustav funkcionira u skladu s očekivanjem. Za svaku uspješnu transakciju je kreiran WAP CDR koji je bio proslijeđen sustavu obračuna na obradu. Primjer izlaznih CDR-ova iz sustav medijacije se može vidjeti u prilogu.

Sve dinamički generirane stranice su bile smještene u pripadajuće direktorije i korisniku je generiran uvijek samo jedan CDR po informaciji s naplatnom informacijom. Tokom testiranja pokušane su "prevare" stavljanjem stranica sa sadržajem koji se naplaćuje u *bookmark*-e. Kako su te stranice obrisane nakon 10 min, nije ih bilo moguće nakon toga roka ponovo učitati.

U slučaju neuspjelih transakcija WAP *gateway,* u skladu s očekivanjima nije generirao CDR-ove.

Sustav medijacije je uspješno eliminirao CDR-ove s tarifnom klasom "199", odnosno CDR-ove sadržaja koji se naplaćuje, no pri tome se ne naplaćuje pristup u mrežu.

Kako je testni WAP *gateway* je imao dozvolu samo za dva istovremena mobilna uređaja, nije napravljen test opterećenja. No s obzirom na definirane karakteristike WAP *gatewaya* i broj korisnika koji istovremeno koristi ovu uslugu eksperimentalni sustav može uspješno funkcionirati i s povećanim opterećenjem.

7.8 Zaključak i daljnja istraživanja

Kako su rezultati testiranja potvrdili očekivanja, ovakav model se može primijeniti u sustavima gdje je potrebna naplata wap usluga po sadržaju pojedinih URL stranica. Davatelji sadržaja moraju implementirati raspored direktorija predložen u ovom istraživanju te njihove adrese moraju biti upisane u datoteku "tariff". Osnovni preduvjet za ovakav model je rješenje problema sa autentifikacijom korisnika stavljanjem LDAP *proxy* rješenja objašnjenog u poglavlju 7.3.3 Prednost ovakvog sustava su potreba za malim uloženim sredstvima i brzina implementacije. Kako su operater i korisnik povezani sigurnim vezama, mogućnost prevare je svedena na minimum, a rješenje s generiranjem CDR-ova samo u WAP *gatewayu* smanjuje zahtjeve za procesiranjem podataka i za kapacitetom veze zbog toga što između davatelja sadržaja i operatera postoji samo komunikacija koja je inicirana od strane korisnika.

Ovakvo rješenje se može koristiti kao prijelazna faza prema drugim naprednijim rješenjima. Izvedbe i realizacija je zavisila o trenutnom stanju u mreži, u kojoj se testiralo, gdje *prepaid* usluga za GPRS još nije bila podržana. U trenutku kada GPRS sustav bude imao podržan i *prepaid* sustav rješenje prikazano u ovom radu biti će potrebno nadograditi. Za buduća istraživanja potrebno je predvidjeti rješenje za druge tipove sadržaja kao što su aplikacije, igre i slični sadržaji. Osnovna ideja ovog sustava predstavlja dobar temelj za to.

8 Zaključak

U ovom radu su prikazana tri različita sustava naplate. U prvom sustavu omogućena je kompletna naplata prijenosa, sadržaja i usluga. Ovakvo rješenje je pogodno ne samo za mobilne paketske mreže nego i za općenito IP mreže kojoj će mobilna paketska mreža biti samo jedna od pristupnih mreža. Drugo rješenje je sustav M-trgovine u kojem centralno mjesto ima platforma za M-trgovinu, koja obavlja dio procesiranja koje korisnikov mobilni uređaj zbog svoje trenutnih mogućnosti nije u stanju obaviti (poput digitalnih potpisa) te istovremeno predstavlja sučelje prema davatelju usluga. Ovo rješenje, za razliku od prvog omogućava prije svega novčane transakcije i kupovine i ne omogućava korisniku garanciju kvalitete prijenosa određenih usluga i njihovu naplate već je za to potrebno imati zasebno rješenje. Treće rješenje prikazano u ovom sustavu je eksperimentalno i pokriva jedan mali segment usluga vezanih uz naplatu pojedinih stranica te prijenosa.

Uporaba pojedinih rješenja ovisi o dostupnosti pojedinih rješenja, strateškim ciljevima operatera, količini korisnika te trenutnim mogućnostima mobilnih uređaja i prilagođenosti davatelja usluga.

S obzirom da su temeljni blokovi AAA sustava još uvijek u razvoju na ovo rješenje treba računati u budućnosti i implementirati ga korak po korak. Ono što je sigurno potrebno je nabaviti sustav koji pokriva naplatu zasnovan na pojedinom događaju, obračun i upravljanje bilancom. Ovakvi sustavi su obično integrirani i postoje već na tržištu i prodaju se kao sustavi obračuna. Slijedeći korak treba biti implementacija i nadogradnja opreme koja će u budućnosti moći omogućiti uporaba AAA sustava (npr. usmjerivači, komutatori, vatrozidi, RADIUS i LDAP poslužitelji). Budući da je ovakav sustava temeljen na budućim uslugama poput VoD, koje nije moguće koristiti sa sadašnjim karakteristikama mreže i mobilnih aparate, potrebno je pojedina rješenja integrirati postepeno. Jedan od slijedećih koraka je integracija MMS sustava.

Sustav M-trgovine je rješenje koje se jednostavno i brzo implementira u postojeći sustav, iako ne pokriva naplatu pristupa i pojedinih sadržaja i usluga, gotovo u potpunosti zahtjeva postojeće zahtjeve, mogućnosti mreže i mobilnih mreža. Ovo rješenje omogućava operateru i ispitivanje reagiranja korisnika na pojedine sadržaje te koliko promatranje u sustavu koliko će to utjecati na njegove mrežne kapacitete. Potrebna je integracija ovog rješenja s već

spomenutom novom generacijom sustava obračuna na način da dio funkcija platforme za M-trgovinu preuzme sustav obračuna.

Treće eksperimentalno rješenje je vrlo jednostavno i najlakše ga je implementirati. Ovo rješenje je fleksibilno i lako se može nadograditi te koristiti za istraživanja. Prednost ovog rješenja je da ne utječe na povećanje prometa u mreži između davatelja usluga i operatera. Ovim rješenjem mogu se provjeriti i mogućnosti uporabe postojećih AAA rješenja poput RADIUS-a i LDAP-a.

Na temelju iskustva u radu postojećih sustava naplate u budućnost će se koristiti nadogradnja prvog rješenja koje će preuzeti prednosti jednostavnosti uporabe M-trgovine.

9 Popis literature

[1] A. Bouch, M.A. Sasse, H. DeMeer: *A user-centered Approach to Managing Quality of Service*; University College London, 2000.

[2] B. Aboba, M. Beadles: *The Network Access Identifier*; Internet Engineering Task Force, RFC 2486, Siječanj 1999.

[3] C. de Laat, G. Gross, L. Gommans, J.Vollbrecht, D. Spence: Generic *AAA Architecture;* Internet Engineering Task Force, RFC 2903, Kolovoz 2000.

[4] C. de Laat, D. Spence: *Structure of a Generic AAA Server;* Internet Draft, draft-irtf-aaaarch-generic-struct-00.txt, Veljača 2001.

[5] C. Parkins: *IP Mobility Support for Ipv4;* Internet Engineering Task Force, RFC 3220, Siječanj 2002.

[6] C. Rigney: *RADIUS Accounting;* Internet Engineering Task Force, RFC 2866, Lipanj 2000.

[7] Christoph Rensing, Hasan, Martin Karsten, Burkhard Stiller: *A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond A*^{x}; ETH TIK-Report Nr. 111, Svibanj 2001.

[8] CISCO: *NetFlow Services and Applications*; Cisco Systems 1999.

[9] Convergyes, Geneva dokumentacija v4.2 i v5.0; 2001

[10] D. Levi, P. Meyer, B. Stewart: *SNMP Applications*; Internet Engineering Task Force, RFC 2573, Travanj 1999.

[11] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, B. Wolff: *Authentication, Authorization, and Accounting: Protocol Evaluation*; Internet Engineering Task Force, RFC 3127, Lipanj 2001.

[12] ETSI: *Broadband Radio Access Networks BRAN; HIPERLAN Type 2; Requirements and Architecture for Interworking between HIPERLAN/2 and 3 rd Generation Cellular systems;* ETSI TR 101 957 v1.1.1, Kolovoz 2001.

[13] ETSI: *Internet Protocol (IP) based Networks*: *Parameters and Mechanisms for Charging*; ETSI TR 101 734 V1.1.1, Rujan 1999.

[14] Fredric Hacklin: *Master thesis - A 3G Convergence Strategy for Mobile Business Middleware Solutions;* Helsinki University of Technology, Rujan 2001.

[15] G. Carle, S. Zander, T. Zseby: *Policy-based Accounting*; Internet Draft, draft-irtf-aaaarch-pol-acct-04.txt, Veljača 2002.

[16] Global Billing Association, *Billing for Content dokumentacija,* http://www.globalbilling.org/

[17] Hasan, Jürgen Jähnert, Sebastian Zander, Burkhard Stiller: *Authentication, Authorization, Accounting, and Charging for the Mobile Internet*; ETH TIK-Report Nr. 114, Lipanj 2001.

[18] Hewlett-Packard: SIU dokumentacija; 1999.

[19] IPDR Organisation: *Network Data Management – Usage (NDM-U) For IP-Based Services, v3.0*, Studeni 2001.

[20] J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry: *The COPS (Common Open Policy Service) Protocol; Internet Engineering* Task Force, RFC 2748, Siječanj 2000.

[21] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart: *HTTP Authentication: Basic and Digest Access Authentication*; Internet Engineering Task Force, RFC 2617 Lipanj 1999.

[22] J. Salowey, G. Sliepen, A. Taal, D. Spence: *Policies in AAA;* Internet Draft, draft-irtf-aaaarch-aaa-pol-01.txt, Ožujak 2001.

[23] J.Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Framework;* Internet Engineering Task Force, RFC 2904, Kolovoz 2000.

[24] J.Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Application Examples;* Internet Engineering Task Force, RFC 2905, Kolovoz 2000.

[25] Jalal Feghhi, Jalil Feghhi, and Peter Williams: *Digital Certificates*; Addison-Wesley Publishing Company, 1999.

[26] Jan Gerke, Placi Flury, Burkhard Stiller: *The Design of a Charging and Accounting System for the Internet*; ETH TIK-Report Nr. 91, Kolovoz 2000.

[27] Jari Arkko, Pat R. Calhoun, Glen Zorn, Patel: *DIAMETER Accounting Extension;* Internet Draft, draft-calhoun-diameter-accounting-08.txt, IETF work in progress Rujan 2000.

[28] M. Sloman: *Policy Driven Management for Distributed Systems*, Plenum Press Journal of Network and Systems Management, Vol. 2, No. 4, str. 333-336, Prosinac 1994,

[29] M. Sloman: Politicy Driven Management For Distributed Systems, Plenum Press Journal of Network and Systems Management, Vol. 2, No. 4, Prosinac 1994, pp 333-316

[30] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan: *Authentication Methods for LDAP*; Internet Engineering Task Force, RFC 2829, Svibanj 2000.

[31] N. Brownlee, C. Mills, G. Ruth: *Traffic Flow Measurement: Architecture*; Internet Engineering Task Force, RFC 2722, Listopad 1999.

[32] N. Brownlee: *Traffic Flow Measurement: Experiences with NeTraMet*; Internet Engineering Task Force, RFC 2123, Ožujak 1997.

[33] P. Calhoun, C. Perkins: *Mobile IP Network Access Identifier Extension for IPv4*; Internet Engineering Task Force, RFC 2794, Ožujak 2000.

[34] Pat R. Calhoun, Jari Arkko, William Bulley, Erik Guttman, Glen Zorn, David Spence, John Loughney: *Diameter Base Protocol*; Internet-Draft, draft-ietf-aaa-diameter- 09.txt, Ožujak 2002.

[35] Pat R. Calhoun, Tony Johansson, Charles E. Perkins: *Diameter Mobile IPv4 Application*; Internet-Draft, draft-ietf-aaa-diameter-mobileip 09.txt, Ožujak 2002.

[36] Pat R. Calhoun, William Bulley, Allan C. Rubens, Jeff Haag, Glen Zorn, David Spence: *Diameter NASREQ Application*; Internet-Draft, draft-ietf-aaa-diameter-nasreq-09.txt, Ožujak 2002.

[37] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: *Hypertext Transfer Protocol -- HTTP/1.1; Internet Engineering* Task Force, RFC 2616, Lipanj 1999.

[38] R. Neilson, Jeff Wheeler, Francis Reichmeyer, Susan Hares: *A Discussion of Bandwidth Broker Requirements for Internet2 Qbone Deployment v0.7*; Internet2 Qbone BB Advisory Council, Kolovoz 1999.

[39] S. Blake, D. Black,M. Carlson, E. Davies, Z. Wang, W. Weiss: *An Architecture for Differentiated Service*; Internet Engineering Task Force, RFC 2475, Prosinac 1998.

[40] S. Glass, T. Hiller, S. Jacobs, C. Perkins: *Mobile IP Authentication, Authorization, and Accounting Requirements;* Internet Engineering Task Force, RFC 2977, Listopad 2000.

[41] T. Dierks, C. Allen: *The TLS Protocol Version 1.0*; Internet Engineering Task Force, RFC 2246, Siječanj 1999.

[42] T. Hiller, P. Walsh, X. Chen, M. Munson, G. Dommety, S. Sivalingham, B. Lim, P. McCann, H. Shiino, B. Hirschman, S. Manning, R. Hsu, H. Koo, M. Lipford, P. Calhoun, C. Lo, E. Jaques, E. Campbell, Y. Xu, S. Baba, T. Ayaki, T. Seki, A. Hameed: *CDMA2000 Wireless Data Requirements for AAA*; Internet Engineering Task Force, RFC 3141, Lipanj 2001.

[43] TeleManagement Forum: *Telecom Operation Map, v2.1*, March 2000.

[44] Yu Chye Cheong, Cheng-Lin Tan: *Payments in Mobile Commerce*; Cap Gemini Ernest&Young, 2001.

10 Popis kratica

A	Accounting
AA	Authentication Authorization
AAA	Authentication Authorization Accounting
APN	Access Point Name
ATM	Asynchronous Transfer Mode
BM	Balance Management
CDR	Charging Data Record
CG	Charging Gateway
CHAP	Challenge Handshake Authentication Protocol
COPS	Common Open Policy Service
CS	Circuit Switch
CSCF (3G)	Call Server Control Function
DHCP	Dynamic Host Configuration Protocol
ERP	Enterprise Resource Planning
FA	Foreign Agent
GBA	Global Billing Association
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSN	GPRS Support Node

HA	Home Agent
HLR	Home Location Register
HSCSD	High Speed Circuit Switch Data
HSS	Home Subscribing System
HTTP	Hypertext Transfer Protocol
IM (3G)	IP Multimedia
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
LDAP	Lightweight Directory Access Protocol
MSC	Mobile Switching Center
MSISDN	Mobile Systems International Subscriber Identity
NAI	Network Access Identifier
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PKI	Public Key Information
PR	Policy Repository
PS	Packet Switch
QoS	Quality of Service

RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Server
RFC	Request For Comment
SDK	Software Development Kit
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System
VoD	Video on Demand
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WML	Wireless Mobile Language
XML	Extensible Markup Language

11 Zahvala

Zahvaljujem se djevojci Ivani i majci Ivanki na strpljivosti za vrijeme izrade ovoga rada. Tokom izrade ovoga rada veliku pomoć sam imao u očuhu Juri Šonje koji mi je pomogao u prevođenju stručnih engleskih izraza na hrvatski. Većina ovoga rada, izrađena je tokom boravka u Connect Austria. U tom razdoblju sam imao veliku pomoć i podršku od voditeljice "Mediation" odjela Diane Šepetanc, kojoj za to želim posebno zahvaliti.

Prilog A Primjer podatkovnog WAP CDR-a na izlasku iz sustava medijacije

```
Geneva: text_data_transfer_file
Format: 1
Character_set: ASCII8
File_type: event_file
File_subtype: GPRS_WAP_volume
File_group_number: 1
File_in_group_number: 1
Total_files_in_group: 1
Source_ID: WAP
Tag: GPRS -v8
# GPRS WAP volume record
Event: "004369911662777","10","2001/09/24-16-45-06.00","001_20010424171512
22009",,,,,,,,"00:00:05","0000000500","WAP_gateway",,"Test","0",,"1",,"Byte","Test",,,,,,,,,,,
,,
Footer: text_data_transfer_file
AuditValue_1: 0
AuditValue_2: 0
End: text_data_transfer_file
Lines: 1
Characters: 100
Checksum:
Security_checksum:

End_of_file:
```

Prilog B Primjer WAP CDR-a, kojim se naplaćuje sadržaj, na izlasku iz sustava medijacije

```
Geneva: text_data_transfer_file
Format: 1
Character_set: ASCII8
File_type: event_file
File_subtype: GPRS_WAP_content
File_group_number: 1
File_in_group_number: 1
Total_files_in_group: 1
Source_ID: WAP
Tag: GPRS -v8
# GPRS WAP content record
Event: "004369911662777","11","2001/09/24-16-47-06.00","001_20010424171512
22010",,,,,,,,"00:00:04",,"WAP_gateway",,"Test","100",,"1",,"Byte","Test",,,,,,,,,,,,
Footer: text_data_transfer_file
AuditValue_1: 0
AuditValue_2: 0
End: text_data_transfer_file
Lines: 1
Characters: 100
Checksum:
Security_checksum:
End_of_file:
```

Prilog C Skripta 1

```
<?php
//send wml headers
header("Content-type: text/vnd.wap.wml");
header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");                    // expires in the past
header("Last-Modified: " . gmdate("D, d M Y H:i:s") . " GMT");     // Last modified, right now
header("Cache-Control: no-cache, must-revalidate");          // Prevent caching, HTTP/1.1
header("Pragma: no-cache");                                  // Prevent caching, HTTP/1.0
echo("<?xml version=\"1.0\"?>");?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD wml 1.2//EN"
"http://www.wapforum.org/DTD/wml_1.2.xml">
<wml>
<?php
$database = pg_connect ("host=localhost dbname=content_charging user=postgres password=bazaipo");
if (!$database)
{
      #print "ne mogu se spojiti na bazu";
      exit;
}

$result=pg_exec($database,"SELECT tabla1.tip,
                              tabla1.podtip,
                              tabla2.link_100,
                              tabla1.kljuc1,
                              tabla2.kljuc2
                        FROM tabla1,tabla2
                        WHERE tabla1.tip='$var' and tabla2.kljuc1=tabla1.kljuc1");

print "<head>
<meta forua=\"true\" http-equiv=\"Cache-Control\" content=\"max-age=0\"/>
</head>
<template>
<do type=\"prev\" name=\"m0\" label=\"Natrag\"><prev/></do>
</template>
<card id=\"$var\" title=\"$var\">
";

for ($i = 0; $i < pg_NumRows($result); $i++)    # loop through all rows returned
{
      $polje = pg_fetch_array($result,$i);          # print the value returned
      $podtip[]=$polje["podtip"];
      $link_100[]=$polje["link_100"];
      $kljuc2[]=$polje["kljuc2"];
}

for ($i=0;$i<pg_NumRows($result); $i++)
{
      if ($i==0)
      {
                  print "<p>".$podtip[$i]."</p>";
      }
      else
      {
            if ($podtip[$i]!=$podtip[$i-1])
                  print "<p>".$podtip[$i]."</p>";
      }
```

```
        print "<p><a href=\"scr2.wml?var=$kljuc2[$i]\">".$link_100[$i]."</a></p>";
}
print "</card>";

?>
</wml>
```

Prilog D Skripta 2

```
<?php
//pokreni random generator i generiraj neku vrijednost
srand((double)microtime()*1000000);
$file_ext = rand(1,99999999);

$database = pg_connect ("host=localhost dbname=content_charging user=postgres password=bazaipo");
if (!$database)
{
print "<p>ne mogu se spojiti na bazu</p>";
exit;
}

//ubaci sifru u bazu uz provjeru jedinstvenosti kljuca
//prvo izvadi sve sifre iz baze
$sve_sifre=pg_exec($database,"SELECT sifra FROM kljucevi2");
//zatim provjeri svaki element polja $sve_sifre
$i = 0;
while ( $i<pg_NumRows($sve_sifre) )
{
	$polje_sifri = pg_fetch_array($sve_sifre,$i);
	if ($file_ext == $polje_sifri["sifra"])
	{
		//cijela while petlja se pokrece ispocetka s time da generiram novi kljuc
		$i = 0;
		$file_ext = rand(1,99999999);
	}
	else
		$i++;
}
//generirana sifra nije jednaka nijednoj u bazi; mozemo novu sifru ubaciti u bazu
$rezultat=pg_exec($database,"INSERT INTO kljucevi2 VALUES ($file_ext)");

//generiraj charge stranicu
create_charge($file_ext);

//generiraj podizbornik vijesti
$par2=& create_submenu($file_ext,$database,$var);

$rjesenje=count($par2);

//generiraj sve stranice vijesti
create_all_news($file_ext,$database,$par2);

//funkcija za kreiranje charge stranice
function create_charge($file_ext)
{
	//sa charge stranice se radi redirect na vijesti
	$charge_page="<?php
header(\"Location: http://80.108.135.21/~msikic/wap/temp/".$file_ext."/index.wml\");
header(\"Content-type: text/vnd.wap.wml\");
?>";
	//zapisi fajl na hard
	$novo_ime=$file_ext.".wml";
	$direktorij="/home/msikic/public_html/wap/charged/";
	write_file($charge_page,$novo_ime,$direktorij);
```

```
}

function &create_submenu($file_ext,$data,$var)
{
	$new_file_ext="s".$file_ext.".wml";
	$tekst_submenu=zaglavlje();
	$result=pg_exec($data,"SELECT tabla1.podtip,
				tabla3.link_200,
				tabla3.kljuc3,
				tabla3.kljuc2,
				tabla2.link_100
			FROM tabla3,tabla1,tabla2
			WHERE tabla3.kljuc2='$var' and tabla2.kljuc2=tabla3.kljuc2 and tabla1.kljuc1=tabla2.kljuc1");
	$tekst_submenu.="";

	for ($i=0;$i<pg_NumRows($result); $i++)
	{
		$polje = pg_fetch_array($result,$i);		# print the value returned
		$podtip[]=$polje["podtip"];
		$link_100[]=$polje["link_100"];
		$link_200[]=$polje["link_200"];
		$kljuc3[]=$polje["kljuc3"];

	}

	for ($i = 0; $i < pg_NumRows($result); $i++)	# loop through all rows returned=0
	{
		if ($i==0)
		    $tekst_submenu.="<card id=\"$podtip[$i]\" title=\"$podtip[$i]\"><p>$link_100[$i]</p>";
		$tekst_submenu.="<p><a href=\"vijest".$i.".wml\">".$link_200[$i]."</a></p>";
	}
	$tekst_submenu.="
	<p><a href=\"../../portal.wml\">portal naslovna</a></p>
	</card></wml>";
	$comand1="/home/msikic/public_html/wap/temp/".$file_ext;
	mkdir($comand1,0777);

	//upisi index.wml u novostvoreni direktorij
	$novo_ime="index.wml";
	$direktorij="/home/msikic/public_html/wap/temp/".$file_ext."/";
	write_file($tekst_submenu,$novo_ime,$direktorij);
	return $kljuc3;
}

function create_all_news($file_ext,$data,&$query_args)
{
	$num_rows=count($query_args);

	for ($j = 0; $j < $num_rows; $j++)
	{
		$result=pg_exec($data,"SELECT tabla3.vijest, tabla2.link_100, tabla1.podtip
			FROM tabla3,tabla2,tabla1
			WHERE tabla3.kljuc3='$query_args[$j]' and tabla2.kljuc2=tabla3.kljuc2 and
tabla1.kljuc1=tabla2.kljuc1");

		$polje = pg_fetch_array($result,0);		// print the value returned
		$vijest=$polje["vijest"];
		$link_100=$polje["link_100"];
		$podtip=$polje["podtip"];
```

```
            $tekst_news_page = zaglavlje();
            $tekst_news_page.="
            <template>
            <do type=\"prev\" name=\"m1\" label=\"atrag\"><prev/></do>
            </template>
            ";
            $tekst_news_page.="<card id=\"$podtip\" title=\"$link_100\">
            <p>$vijest</p>
            <p><a href=\"../../portal.wml\">portal naslovna</a></p>
            </card></wml>";

            //definiraj parametre za zapisivanje vijesti
            $novo_ime="vijest".$j.".wml";
            $direktorij="/home/msikic/public_html/wap/temp/".$file_ext."/";
            write_file($tekst_news_page,$novo_ime,$direktorij);
      }

}
//funkcija za kreiranje zaglavlja
function zaglavlje()
{
      $tekst_zag="<?php header(\"Content-type: text/vnd.wap.wml\");
      header(\"Expires: Mon, 26 Jul 1997 05:00:00 GMT\");
      header(\"Last-Modified: \" . gmdate(\"D, d M Y H:i:s\") . \" GMT\");
      header(\"Cache-Control: no-cache, must-revalidate\");
      header(\"Pragma: no-cache\");
      echo (\"<?xml version=\\\"1.0\\\"?>\");?> ";
      $tekst_zag=$tekst_zag."<!DOCTYPE wml PUBLIC \"-//WAPFORUM/DTD wml 1.2//EN\"
\"http://www.wapforum.org/DTD/wml_1.2.xml\">
      <wml>
      <head>
      <meta forua=\"true\" http-equiv=\"Cache-Control\" content=\"max-age=0\"/>
      </head>
      ";
      return $tekst_zag;
}

//funkcija za zapisivanje fajla na hard
function write_file($tekst,$ime,$dir)
{
      $lokacija=$dir.$ime;
      $fp=fopen("$lokacija","w");
      fwrite($fp,$tekst);
      fclose($fp);
}


//Sada slijedi ispis onoga sto vidi korisnik nakon pozivanja scr2.wml skripte
header("Content-type: text/vnd.wap.wml");
header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");                    // expires in the past
header("Last-Modified: " . gmdate("D, d M Y H:i:s") . " GMT");     // Last modified, right now
header("Cache-Control: no-cache, must-revalidate");          // Prevent caching, HTTP/1.1
header("Pragma: no-cache");                                  // Prevent caching, HTTP/1.0
echo("<?xml version=\"1.0\"?>");?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD wml 1.2//EN"
"http://www.wapforum.org/DTD/wml_1.2.xml">
<wml>

<head>
</head>
```

```
<card id="Obavijest" title="Obavijest">

<?php
if ($rjesenje!=0)
{
	print "<p>Ove vijesti Vas kostaju 3 kune
	<br/>
	<a href=\"../charged/".$file_ext.".wml\">Zelim vidjeti</a> <br/>
	Ne zelim vidjeti. <br/>
	<a href=\"../portal.wml\">Vratite me na pocetnu stranicu</a> <br/>
	<template>
	<do type=\"prev\" name=\"m0\" label=\"Natrag\"><prev/></do>
	</template>";
}
else
{
	print "
	<p>Nema nikakvih vijesti u ovoj kategoriji
	<template>
	<do type=\"prev\" name=\"m0\" label=\"Natrag\"><prev/></do>
	</template>";
}
?>
</p>

</card>
</wml>
```

Prilog E Skripta za brisanje dinamičkih stranica

```
<?php
//uzimam vrijeme epohe u sekundama
$sada=time();

//brisati cu fajlove starije od 10 minuta odnosno 600 sekundi
$erase_criteria=$sada-600;

$database = pg_connect ("host=localhost dbname=content_charging user=postgres password=bazaipo");

if (!$database)
{
	print "<p>ne mogu se spojiti na bazu</p>";
	exit;
}

$result=pg_exec($database,"SELECT * from kljucevi2");
print "Izvadjeno je: ".pg_NumRows($result)."redova\n";
for ($i = 0; $i < pg_NumRows($result); $i++)
{

	$polje=pg_fetch_array($result,$i);
	$file_name="/home/msikic/public_html/wap/charged/".$polje["sifra"].".wml";
	//$file_name1="/home/msikic/public_html/wap/temp/r".$polje["sifra"].".wml";
	$last_time_written=filectime($file_name1); //filectime je funkcija koja vraca kada je $file_name bio zadnji
puta zapisan

	if ($last_time_written < $erase_criteria)
	{
		unlink ($file_name);
		//unlink ($file_name1);
		$komanda="rm -rf /home/msikic/public_html/wap/temp/".$polje["sifra"]."/";
		system ($komanda);

		//moraju se obrisati i stare sifre
		$query="DELETE from kljucevi2 where sifra=".$polje["sifra"];
		$new_result=pg_exec($database,$query);

	}
}

?>
```

ŽIVOTOPIS

Rođen sam 18. studenog 1972. godine u Zagrebu. Srednju Tehničku školu "Ruđer Bošković" završio sam 1991. godine u Zagrebu. Diplomirao sam 1996. godine na Fakultetu elektrotehnike i računarstva u Zagrebu, smjer Radiokomunikacije i profesionalna elektronika. Od 1997.godine sam zaposlen na Zavodu za elektroničke sustave i obradu informacija na poslu zavodskog suradnika. Tokom rada sudjelovao sam i vodio više desetaka projekata u području LAN, WAN mreža te učionica za udaljena predavanja. U tijeku 2000, 2001 te 2002 u dva navrata radio sam po 5 mjeseci u austrijskom GSM operateru "Connect Austria" na poslovima testiranja sustava medijacije i obračuna te razvoja sustava naplate sadržaja u mobilnim paketskim mrežama. Autor sam nekoliko radova u časopisu "Mreža" u područjima Linux-a i GPRS mreža.

SAŽETAK

Modeli naplate sadržaja u mobilnim paketskim mrežama

Razvoj mobilnih paketskih mreža GPRS-a i UMTS-a, mobilnim operaterima daje mogućnost pružanja korisnicima novih usluga i sadržaja. Budući da cijena pristupa mrežama pada operateri moraju naći nove načine naplate. Postojeći sustav obrađen u prvom dijelu rada omogućava naplatu jedino pristupa te sadržaja prenesenih preko SMS-a kao nosioca. U drugom dijelu rada prikazana su tri modela koja omogućavaju naplatu sadržaja i usluga koji nisu obuhvaćeni u postojećim sustavima.

Prvo je objašnjen model koji omogućava cjelovitu naplatu pristupa, sadržaja i usluga. Ovaj model je temeljen na principu korištenja AAA sustava, mobilnog IP-a, QoS brokera, te upravljanja bilancom. Opisane su osnove ovih sustava te njihova integracija u cjelokupni model. Ovakav model osim naplate pruža mogućnost praćenja prometa i pružanja korisniku određenih usluga i sadržaja.

Drugi model je model sustava M-trgovine koji omogućava prodaju fizičkih i elektronskih sadržaja. Opisane su osnovne komponente ovog sustava te dva osnovna modela sustava M-trgovine: sustav s plaćanjem vezanim za račun i sustav s plaćanjem temeljenim na žetonima.

Treći model je eksperimentalni model koji omogućava naplatu URL temeljenih WAP sadržaja. Opisane su osnovne komponente, način funkcioniranja modela te prikazana praktična implementacija ovog modela.

Izloženi modeli mogu poslužiti kao predložak za rješavanje problema naplate sadržaja u mobilnim paketskim mrežama.

Ključne riječi

naplata, obračun, tarifiranje, politika, mobilne mreže, UMTS, sadržaj, usluge, AAA, mobilni IP, M-trgovina

SUMMARY

Content charging models in mobile packet networks

Development of mobile packet networks GPRS and UMTS created additional ways of delivering new services and contents to mobile users. Since the network access cost must be decreased, mobile network operators have to find new ways of content charging. In the first part of this thesis a short overview of the currently used charging system is given. This system supports only access charging and content charging for the content over the SMS bearer. In the second part of this document, three models that enable content and service charging, not supported in currently used systems, are described.

A model that supports content, service and access charging is explained firstly. This model is based on using the AAA system, mobile IP, the QoS broker system and the balance management system. An overview of these systems and their integration into the whole model is described. This model, besides charging, also supports a traffic monitoring and gives provision for access to specific contents and services.

Second model described in this thesis is an M-commerce model, which supports trading of physical and non-physical (i.e. digital contents) items. An overview of basic building blocks and a description of two basic M-commerce models, the account-based model and the token-based model, is given.

Finally, an experimental model for WAP URL based content charging is described. This section gives a description of basic components and the model functionality. It also provides an example of practical implementation in recent charging models.

Models presented in the thesis can be used as a pattern for content charging solution in the mobile packet networks.

Keywords

charging, billing, rating, policy, mobile networks, UMTS, content, services, AAA, mobile IP, M-commerce