Aleksandar Nešković
Irena Janković

IMS -IP MULTIMEDIA SUBSYSTEM

INTEGRACIJA INTERNETA
SA JAVNIM MOBILNIM ĆELIJSKIM SISTEMIMA

Akademska misao
Univerzitet u Beogradu - Elektrotehnički fakultet
Beograd, 2010.

SADRŽAJ

1. UVOD U IMS (*IP MULTIMEDIA SUBSYSTEM*)

1.1 RAZLOZI UVOĐENJA IMS-a

Jedan od ciljeva koji je trebalo ostvariti tokom evolucije mreža treće generacije (3G) je spajanje dve najrazvijenije oblasti u svetu telekomunikacija: javnih mobilnih sistema i Interneta. IP *Multimedia Subsystem* predstavlja ključni element 3G arhitekture koji omogućava da se korisnicima obezbedi mobilni pristup svim servisima koje Internet pruža. IMS je zapravo podsistem koji omogućava "surfovanje" omiljenim *web* stranicama, slanje *e-mail* poruka, gledanje video sadržaja ili učestvovanje na videokonferencijima i to gotovo u bilo kojoj tački planete, jednostavnim korišćenjem mobilnog 3G terminala.

IMS tehnologija je nastala na osnovama uspešnih principa javnih mobilnih mreža i Interneta, pri čemu su stečena iskustava iz obe tehnologije kombinovana kako bi se otišlo korak dalje u razvoju savremenih bežičnih IP mreža. U tekstu koji sledi biće ukratko izložene dobre karakteristike javnih mobilnih sistema i Interneta, kao i karakteristike IMS podsistema kao nove integrišuće tehnologije.

Poznato je da je Internet svoj dramatični razvoj, od male univerzitetske do globalne svetske mreže, doživeo zahvaljujući pružanju brojnih izuzetno korisnih servisa (WWW, e-*mail*, ...) koji su zadobili naklonost miliona korisnika. Ponuda velikog broja popularnih servisa posledica je činjenice da Internet za njihovo kreiranje koristi tzv. otvorene ("*open*") protokole koji su javno dostupni bilo kom zainteresovanom kreatoru servisa, pri čemu su metode i tehnike kreiranja servisa opisane u mnogobrojni knjigama, a predaju se i na mnogobrojnim univerzitetima i školama. Rasprostranjenost znanja o Internet protokolima implicirala je da u praksi servise najčešće kreiraju eksperti za odgovarajuću oblast kojoj je servis namenjen (naravno, koji ujedno poseduju i potreban nivo znanja o Internet protokolima koje treba implementirati).

Takođe, poznato je da javne mobilne telefonske mreže danas obezbeđuju servise za preko dve milijarde korisnika korisnika širom sveta. Moderne mreže svakako više nisu ograničene samo na osnovni telefonski servis, već sada uključuju i servise prenosa podataka, od jednostavnog slanja tekstualnih poruka (npr., SMS...) do multimedijalnih poruka, surfovanja Internetom i utvrđivanja lokacije određenog korisnika u mreži. Ipak, svoju popularnost javne mobilne mreže ne duguju širini palete svojih servisa, već mogućnosti da korisniku obezbede korišćenje servisa u gotovo bilo kojoj tački, tj. praktično svuda. Uz sve manju veličinu terminala,

korisniku postaje izuzetno atraktivna mobilnost pri korišćenju servisa koja sve manje poznaje razliku između teritorije sela, grada ili neke inostrane zemlje.

Na osnovu prethodnog izlaganja može se zaključiti da je najatraktivnijim Internet servisima već moguće pristupiti pomoću tehnologije javnih mobilnih telefonskih mreža, pa se postavlja pitanje zašto je neophodan IMS podsistem (u daljem tekstu će se kao sinonim koristi i termin „sistem") i u čemu je njegova posebnost?

Postoje tri nova koncepta bazirana na komutaciji IP paketa (PS – *Packet Switching*) koja je IMS uveo u 3G mreže. To su:

- **Kvalitet servisa (*Quality of Service - QoS*)** kojim je u okviru IMS-a eliminisan nedostatak PS domena koji funkcioniše na tzv. principu "najboljeg pokušaja" (*best effort*) i u skladu sa tim ne garantuje korisniku vrednost protoka koji će imati na raspolaganju tokom uspostavljene konekcije, niti maksimalnu vrednost kašnjenja koje se javlja pri prenosu paketa. Na taj način, nekonzistentnost kvaliteta konekcije koji je posebno bitan u slučaju multimedijalnih servisa koji se realizuju u realnom vremenu (npr., videokonferencijske veze, VoIP konekcije itd.), uzrokuje povremene probleme ili pak dovodi do potpune nemogućnosti korišćenja servisa. Nasuprot tome, IMS brine o sinhronizaciji uspostavljene konekcije (sesije) i održava zahtevani QoS čime se korisnicima omogućava korišćenje odgovarajućih multimedijalnih servisa.
- **Tarifiranje (*Charging*)** u okviru IMS-a uvodi novine u pogledu adekvatnog tarifiranja multimedijalnih sesija. Pre uvođenja IMS-a, prilikom tarifiranja servisa, 3G operatori nisu mogli da razlikuju kom servisu pripadaju podaci koji se prenose, pa se u skladu sa tim nametao princip tarifiranja na osnovu prenetog broja *byte*-ova. IMS pak, omogućava operatorima da imaju uvid u to koji tip servisa korisnik aktivira i da u skladu sa tim primenjuju alternativne metode tarifiranja. Na primer, na taj način, operator može primenjivati fiksnu tarifu pri prenosu tekstualnih poruka bez obzira na njihovu dužinu, tarifirati multimedijalne servise na bazi trajanja sesije, primenjenog QoS ili mogu implementirati posebno kreirane poslovne modele tarifiranja. Suština je da koncept tarifiranja kakav obezbeđuje IMS, donosi izuzetne pogodnosti korisnicima (naravno i operatorima).
- **Integrisanje različitih servisa** predstavlja treći glavni razlog za uvođenje IMS-a. Iako su veliki proizvođači telekomunikacione opreme i operatori zainteresovani za razvoj određenih multimedijalnih servisa, oni nastoje da se ne ograniče isključivo na te servise. Naime, operatori žele da implementiraju i servise koje su razvile neke druge kompanije – tzv. *third parties* (dakle, ne operatori, kao ni veliki proizvođači telekomunikacione opreme), da ih kombinuju i integrišu sa već postojećim servisima i na taj način obezbede nove, atraktivne kombinacije svojim korisnicima. Na taj način je recimo moguće da operator koji raspolaže servisom govorne pošte, kupi od nekog drugog proizvođača servis konverzije teksta u govor (*text-to-speech service*) i kombinovanjem obezbedi servis govorne interpretacije tekstualnih poruka, a koji bi bio namenjen korisnicima sa vizuelnim invalididetom. Velika sloboda pri integrisanju različitih servisa i mogućnost saradnje operatora sa raznovrsnim proizvođačima, ostvarena je zahvaljujući tome što su u okviru IMS-a definisani standardni interfejsi za kreiranje servisa bazirani na Internet protokolima.

Konačno, treba još jednom napomenuti, da osnovni cilj IMS-a nije da obezbedi nove servise, već da pruži korisnicima sve, kako aktuelne tako i buduće, Internet servise. Pri tome, korisnicima treba da su na raspolaganju jednake mogućnosti i u matičnoj mreži i u slučaju *roaming*-a. U skladu sa navedenim ciljevima, IMS obezbeđuje da se multimedijalne sesije odvijaju ravnopravno između dva IMS korisnika, jednog IMS i jednog Internet korisnika ili pak između dva Internet korisnika, a da su pri tome realizovane korišćenjem istih Internet protokola.

1.2 IMS STANDARDIZACIJA

U prethodnom poglavlju više puta je napomenuto da IMS koristi Internet protokole. Praktično, podrazumeva se da kada je IMS-u neophodan protokol za obavljanje odgovarajućeg zadatka (npr., za uspostavljanje multimedijalne sesije), regulatorna tela odgovorna za standardizaciju IMS-a, preuzimaju adekvatan Internet protokol i specificiraju način njegove primene u okviru IMS-a. Proces izbora odgovarajućeg Internet protokola često nije jednostavan. Ponekad odabranom Internet protokolu manjkaju esencijalne funkcionalnosti, a ponekad željeni tip protokola jednostavno ne postoji. U tim slučajevima su regulatorna tela za IMS standardizaciju zadužena da u saradnji sa regulatornim telima zaduženim za standardizaciju Interneta kreiraju odgovarajuće rešenje.

1.2.1 RELACIJE IZMEĐU REGULATORNIH TELA ZADUŽENIH ZA IMS STANDARDIZACIJU

Dva osnovna regulatorna tela zadužena za standardizaciju IMS-a su: 3GPP (*Third Generation Partnership Project*) i 3GPP2 (*Third Generation Partnership Project* 2). Oba tela su aktivno učestvovala na izradi ITU (*International Telecommunication Union*) IMT-2000 (*International Mobile Telecommunications-2000*) globalnog standarda za mobilne mreže treće generacije koji je imao za cilj realizovanje pristupa telekomunikacionim servisima korišćenjem radio-veza, uključujući zemaljske i satelitske.

Iako veoma slični, 3GPP i 3GPP2 poseduju razlike i u skladu sa tim su standardizovali posebne IMS (IP *Multimedia Subsystem*) podsisteme. Najbitnija sličnost između 3GPP i 3GPP2 IMS podsistema jeste što oba koriste Internet protokole koji su tradicionalno standardizovani od strane IETF *(Internet Engineering Task Force).* Posledično, i 3GPP i 3GPP2 sarađuju sa IETF-om na razvoju protokola koji bi odgovarali njihovim specifičnim IMS potrebama.

Kao dodatak prethodno istaknutim regulatornim telima od važnosti za IMS standardizaciju, treba istaći OMA (*Open Mobile Aliance*) alijansu koja ima zadatak razvoja posebnih IMS servisa.

U narednim poglavljima biće predstavljena 3GPP, 3GPP2 i IETF standardizaciona tela, kroz opise njihovih osnovnih struktura i funkcija.

1.2.2 *INTERNET ENGINEERING TASK FORCE* - IETF

IETF predstavlja veliku, samostalno organizovanu, međunarodnu grupu dizajnera mreža, operatora, proizvođača opreme i istraživačkih institucija čija je glavna preokupacija evolucija Internet arhitekture i efikasno funkcionisanje Interneta.

IETF je zadužen za donošenje Internet Standarda (*Internet Standards*) u okviru kojih su specificirani protokoli, procedure i konvencije koje se koriste za realizaciju Interneta, a koje su poznate pod nazivom *Request for Comments* (RFC). Treba napomenuti da se IETF ne bavi standardizacijom mreža, arhitektura koje kombinuju različite protokole, internim funkcionalnostima mrežnih elemenata niti API (*Application Programming Interfaces*) interfejsima. IETF jednostavno predstavlja "fabriku" protokola baziranih na IP-u. To je telo za standardizaciju koje je razvilo najveći broj protokola koji su trenutno u upotrebi u okviru Interneta. Interesantno je primetiti da je IETF standardizaciono telo kome može pristupiti bilo koji zainteresovan individualac.

1.2.2.1 Struktura IETF-a

IETF funkcioniše potpuno drugačije u odnosu na druge organizacije koje se bave standardizacijom (npr., kakve su 3GGP i 3GPP2). Posao u okviru IETF-a raspodeljen je na tzv. Radne grupe (*Working Groups)*, koje su odgovorne za obavljanje specifičnih zadataka i donošenje preciznog seta dokumenata. U skladu sa principima IETF-a, Radne grupe ne poseduju unapred definisano članstvo već je pristup individualan i dobrovoljan. Iako pripadnici grupa samostalno obavljaju svoje zadatke, svaka grupa poseduje od jednog do tri nadređena, koji se staraju da grupa svoje zadatke blagovremeno obavi.

Vek trajanja Radne grupe je ograničen trenutkom okončanja poslova neophodnih za donošenje potrebnih dokumenata, nakon čega Radna grupa dobija nove zadatke, biva reformisana ili prestaje da postoji. Trenutno postoji više od sto aktivnih Radnih grupa čija je kompletna lista dostupna na *site*-u: www.ietf.org/html.charters/wg-dir.html. Treba istaći da se Radnim grupama dodeljuje akronim koji identifikuje uži ili širi domen problema koji obrađuju (npr., AAA što odgovara domenu "*Authentication, Autorization and Accounting*").

Dalje uređenje IETF-a podrazumeva organizaciju Radnih grupa u skladu sa tehničkim i tehnološkim oblastima kojima pripadaju, odnosno njihovo grupisanje u tzv. Oblasti (*Areas*). Kako pomenutim Oblastima upravljaju direktori poznati kao *Area Directors*, u upotrebi je još i naziv *Area Directorate*. *Area Directors* zajedno sa čelnikom IETF-a formiraju tzv. *Internet Engineering Steering Group* (IESG) zadužen za koordiniranje posla u okviru različitih oblasti. Aktuelne oblasti IETF-a su:

- *Applications Area,*
- *General Area,*
- *Internet Area,*
- *Operations and Management Area,*
- *Real-time Applications and Infrastructure Area,*
- *Routing Area,*
- *Security Area* i
- *Transport Area.*

Posebno telo, poznato kao *Internet Architecture Board* (IAB) obezbeđuje tehnički aspekt liderstva i obrađuje podnesene primedbe ukoliko postoje (www.iab.org).

1.2.2.2 Funkcionisanje radnih grupa – *Working Group Operations*

Predlog o kreiranju Radne grupe može biti iniciran od strane bilo kojeg pojedinca koji u tom slučaju predlaže tzv. BOF (*Birds of a Feather*). BOF esencijalno predstavlja grupu ljudi zainteresovanu za diskutovanje da li je potrebno ili ne kreirati novu Radnu grupu u određenoj oblasti IETF-a. Zadatak BOF-a je takođe da definiše ciljeve i radne okvire za predloženu grupu i da ispita stepen zainteresovanosti za njen dalji rad. Ukoliko postoji jasan konsenzus učesnika diskusije za kreiranje grupe, čelnik BOF-a će prezentovati rezultate direktoru oblasti uz zahtev za odobrenje. Za konačno formiranje grupe neophodno je da odobrenje izdaju i dva glavna tela: IESG i IAB.

Nakon formiranja grupe, njeni akteri započinju sa radom na glavnom cilju, a to je donošenje odgovarajućih tehničkih dokumenata i utvrđivanje odgovarajućih Internet standarda.

Neophodno je istaći, da se sva tehnička dokumenta koja predlaže Radna grupa ili njeni individualni članovi označavaju kao *Internet-Drafts*, sve dok su u procesu aktivne izrade. *Internet-Drafts* predstavljaju privremena dokumenta čija važnost ističe i prestaje da postoji šest

isključivo u okviru sesija iniciranih od strane IMS terminala i adresiranih na korisnika u mreži na bazi komutacije kola, kakve su PSTN i PLMN (*Public Land Mobile Network*). Glavni zadatak BGCF-a je:

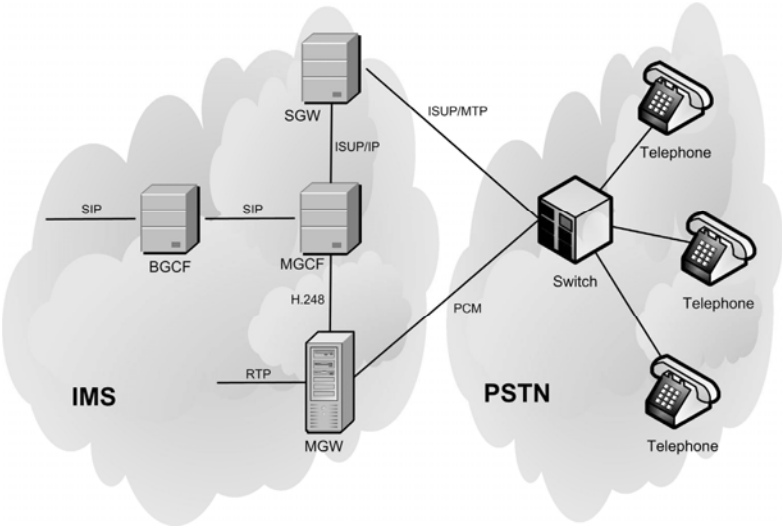
- izbor odgovarajuće mreže gde se može obaviti povezivanje sa CS (*circuit-switched*) domenom, i
- izbor adekvatnog PSTN/CS *gateway*-a, ukoliko se međupovezivanje realizuje u istoj mreži gde se nalazi i BGCF.

1.4.6 PSTN/CS *GATEWAY*

PSTN *gateway* obezbeđuje interfejs ka mreži na bazi komutacije kola i pri tome omogućava IMS terminalima da upućuju i primaju pozive iz/ka PSTN mreže (ili bilo koje druge CS mreže). PSTN *gateway* sačinjavaju:

- **SGW (*Signaling Gateway*) –** obezbeđuje interfejs ka signalizacionoj ravni CS mreže (tipično, signalizacija No. 7). SGW obavlja konverziju nižih protokola.
- **MGCF (*Media Gateway Control Function*) –** predstavlja centralni deo PSTN/CS *gateway*-a. MGCF poseduje mehanizam za konverziju protokola i obavlja mapiranje SIP protokola, zaduženog za kontrolu sesije na IMS strani u jedan od protokola za kontrolu poziva na CS strani, ISUP/IP ili BICC/IP. Kao dodatak konverziji protokola za kontrolu poziva, MGCF kontroliše resurse MGW (*Media Gateway*) komponente. Na relaciji između MGCF i MGW komponenti, u upotrebi je H.248 protokol.
- **MGW (*Media Gateway*) –** obavlja ulogu interfejsa ka ravni prenosa PSTN ili druge CS mreže. Sa jedne strane MGW može da šalje i prima IMS multimedijalne poruke, korišćenjem RTP (*Real-Time Protocol*, RFC 3550) protokola. Na drugoj strani, MGW koristi jedan ili više PCM (*Pulse Code Modulation*) veza za komunikaciju sa CS mrežom. Dodatno, MGW obavlja transkodovanje u slučajevima kada IMS terminal ne podržava koder koji se koristi na CS strani.

Slika 1.4 ilustruje PSTN *gateway* kao vezu ka CS mreži.



Slika 1.4: PSTN *gateway* ka CS mreži

1.5 IDENTIFIKACIJA U OKVIRU IMS-a

U svakoj mreži, neophodno je da postoji jedinstvena identifikacija korisnika. Mogućnost identifikacije korisnika zapravo omogućava pravilno usmeravanje poziva do odredišnog korisnika. Najpoznatiji je svakako način identifikacije, odnosno numeracije u PSTN mrežama, gde redosled cifara određuje korisnika (tj., njegovu lokaciju). Dodatno, specifičnim skupom cifara (najčešće karakterističnim prefiksom) mogu se identifikovati i posebni servisi.

IMS sistem takođe primenjuje mehanizme za identifikaciju korisnika i servisa, a njihove karakteristike će biti izložene u poglavljima koja slede.

1.5.1 JAVNI KORISNICKI IDENTITETI – *PUBLIC USER IDENTITIES*

U IMS-u je definisan deterministički način identifikacije korisnika koji zadužuje operatora matične mreže da korisniku dodeli jedan ili više tzv. javnih korisničkih identiteta (*Public User Identities*). *Public User Identities* su javno dostupni (štampaju se i na vizit-karticama, na primer), a koriste se u okviru IMS-a za rutiranje SIP signalizacije. Ukoliko uporedimo IMS sa GSM sistemom, *Public User Identity* u IMS-u predstavlja isto što i MSISDN (*Mobile Subscriber ISDN Number*) u GSM sistemu.

Javni korisnički identiteti (*Public User Identities*) mogu biti definisani kao SIP URI (SIP *Uniform Resource Identifier*) ili TEL URL (*Telephone Uniform Resource Locator*).

Kada *Public User Identity* sadrži SIP URI, definisan u okviru RFC 3261, on poseduje formu:

sip:ime.prezime@operator.com

Pri tome, IMS operatori zadržavaju pravo da izmene šemu adresiranja u skladu sa svojim potrebama. Dodatno, SIP URI forma može uključivati i telefonski broj kada dobija novi format. Na primer:

sip:+1-212-555-02983@operator.com; user=phone.

Prethodno navedeni format je neophodan zato što SIP protokol zahteva da URI prilikom registracije bude SIP URI. Stoga u SIP-u nije moguće registrovati TEL URL (RFC 3966), ali je moguće registrovati SIP URI koji uključuje i telefonski broj.

TEL URL predstavlja drugi format koji *Public User Identity* može da ima. Naveden je primer TEL URL-a koji reprezentuje telefonski broj u internacionalnom formatu:

tel:+1-212-555-02983.

TEL URL formati su neophodni za uspostavljanje poziva od strane IMS terminala ka PSTN korisniku, zato što su PSTN brojevi prezentovani isključivo pomoću cifara. Na drugoj strani, TEL URL-ovi su takođe neophodni ukoliko PSTN pretplatnik želi da pozove IMS korisnika, jer on isključivo raspolaže ciframa.

Predviđeno je da operatori dodele najmanje jedan SIP URI i jedan TEL URL po korisniku. Postoje posebni razlozi za dodelu više od jednog javnog korisničkog identiteta korisniku. Na primer, potreba razdvajanja sopstvenih privatnih identiteta, na one koji su poznati prijateljima od onih namenjenih poslovnim saradnicima i sl.

IMS zapravo uvodi interesantan koncept: set implicitno registrovanih javnih korisničkih identiteta (*a set of implicitly registered public user identities*). Pri standardnim SIP operacijama,

svaki identitet je neophodno posebno registrovati. Međutim, u okviru IMS-a, postoji mogućnost registracije više identiteta u okviru jedne poruke u cilju uštede vremena i protoka (detaljniji opis postupka registracije biće dat u okviru poglavlja 2).

1.5.2 PRIVATNI KORISNIČKI IDENTITETI – *PRIVATE USER IDENTITIES*

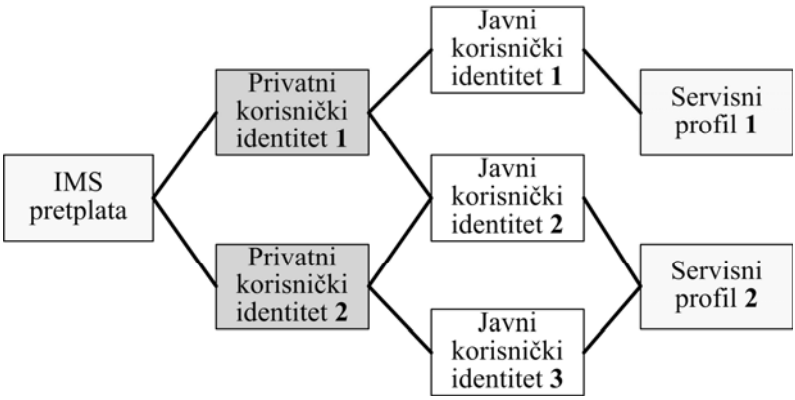
Svakom IMS korisniku biva dodeljen privatni korisnički identitet, *Private User Identity*. Za razliku od javnih identiteta, privatni korisnički identiteti nemaju SIP URI ili TEL URL formu, već poseduju format NAI (*Network Access Identifier,* speecificiran u RFC 4282) identifikatora za pristup mreži. NAI format je **username@operator.com.**

Private User Identities se isključivo koriste za identifikaciju korisničkog naloga i za potrebe autentifikacije, ali se ne koriste za potrebe rutiranja SIP zahteva. *Private User Identity* obavlja sličnu funkciju u IMS sistemu, kao IMSI (*International Mobile Subscriber Identifier*) u GSM-u. Korisnik ne mora da poznaje svoj privatni korisnički identitet jer on može biti smešten na kartici, na isti način na koji je IMSI uskladišten na SIM (*Subscriber Identity Module*) kartici.

1.5.3 RELACIJA IZMEĐU JAVNIH I PRIVATNIH KORISNIČKIH IDENTITETA

U okviru IMS sistema standardizovanog u okviru 3GPP *Release* 5, podrazumevano je da se IMS korisniku dodeljuje jedan privatni korisnički identitet, *Private User Identity,* i nekoliko javnih odnosno, *Public User Identities.*

3GPP *Release* 6 je proširio navedene relacije, i uspostavio odnose između privatnih i javnih identiteta kao što je prikazano na slici 1.5. Uočava se da je IMS korisniku moguće dodeliti više privatnih identiteta. U slučaju UMTS-a, isključivo jedan *Private User Identity* može biti smešten na SIM kartici, ali korisnici mogu posedovati više SIM kartica u zavisnosti od broja privatnih identiteta koji im je neophodan. Međutim, u okviru IMS-a, moguće je koristiti jedan javni korisnički identitet u kombinaciji sa više privatnih, kao što je slučaj sa npr., *Public User Identity#2* prikazanim na slici 1.5. U praksi bi navedeni primer značio da dva različita IMS terminala koriste isti *Public User Identity#2*, ali su na njihovim karticama zapisana dva različita privatna identiteta, u ovom slučaju: *Private User Identity#1 i Private User Identity#2.*



Slika 1.5: Relacija između javnih i privatnih korisničkih identiteta definisana u okviru 3GPP R5

1.5.4 JAVNI IDENTITETI SERVISA – *PUBLIC SERVICE IDENTITIES*

Koncept javnih identiteta servisa, PSIs (*Public Service Identities*) predstavljen je u okviru 3GPP *Release-a* 6.

Specifičnost PSI-a je u tome što se ne dodeljuje IMS korisniku već servisu smeštenom na odgovarajućem aplikacionom serveru. Kao i javni korisnički identitet, PSI može imati SIP URI ili TEL URL format, ali se u odnosu na njega razlikuje time što nije ni u kakvoj vezi sa privatnim korisničkim identitetima. Razlog tome je što se privatni identiteti koriste za potrebe autentifikacije korisnika, a PSI nije primenjiv na IMS korisnike.

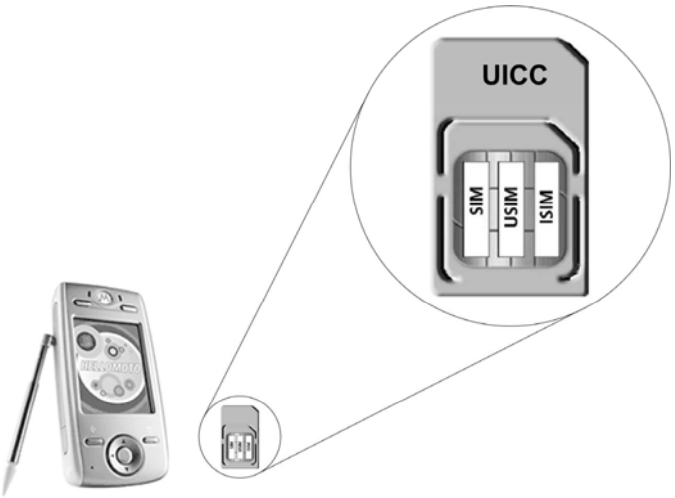
1.6 SIM, USIM I ISIM PREMA 3GPP SPECIFIKACIJAMA

Suštinu u dizajnu 3GPP terminala predstavlja prisustvo UICC (*Universal Integrated Circuit Card*) kartice. UICC predstavlja inteligentnu (i sa stanovišta terminala zamenljivu) karticu koja sadrži limitiranu količinu podataka. UICC se upotrebljava, između ostalog, za skladištenje informacija o pretplatničkom nalogu, autentifikacionih ključeva, imenika i poruka.

GSM i 3GPP specifikacije podrazumevaju prisustvo UICC kartice u terminalu kako bi on ispravno funkcionisao. Ukoliko UICC nije prisutan u terminalu, korisnik će moći da realizuje isključivo tzv. hitne pozive.

UICC je opšti termin koji definiše fizičke karakteristike inteligentne kartice (na primer, broj i raspored pinova, naponske nivoe, itd.). Pri tome, interfejs između UICC-a i terminala je takođe standardizovan.

Sa logičkog aspekta, UICC može sadržati više logičkih aplikacija kao što su: SIM (*Subscriber Identity Module*), USIM (*Universal Subscriber Identity Module*) i ISIM (IP *multimedia Services Identity Module*). Primer takve UICC kartice prikazan je na slici 1.6.



Slika 1.6: SIM, USIM i ISIM na UICC kartici 3GPP IMS terminala

1.6.1 SIM (*SUBSCRIBER IDENTITY MODULE*)

U SIM modulu upisan je skup parametara koji su od suštinskog značaja za funkcionisanje terminala u GSM mrežama (to su npr., informacije o korisničkom nalogu, parametri neophodni za autentifikaciju, informacije o privilegijama dodeljenim korisniku, itd.). Iako se termini UICC i SIM često na isti način interpretiraju, UICC se odnosi na fizičku karticu, dok SIM predstavlja jednu od aplikacija implementiranu na UICC-u. SIM je u širokoj upotrebi u mrežama druge generacije (2G) kao što su to npr., GSM mreže.

SIM aplikacija je standardizovana u ranim fazama razvoja GSM-a. 3GPP je nasledio ranije usvojene specifikacije, a trenutno je SIM specificiran u okviru 3GPP TS 11.11 i 3GPP TS 51.011.

1.6.2 USIM (*UNIVERSAL SUBSCRIBER IDENTITY MODULE*)

USIM (standardizovan u okviru 3GPP TS 31.102) predstavlja još jedan primer aplikacije implementirane na UICC karticama treće generacije. USIM obezbeđuje set parametara (sličan po prirodi, a opet različit u odnosu na SIM parametre) koji uključuje informacije o korisničkom nalogu, autentifikaciji korisnika, metodama tarifiranja itd. USIM se upotrebljava za pristup UMTS (*Universal Mobile Telecommunication*) mrežama koje predstavljaju 3G evoluciju GSM-a.

USIM je neophodan ukoliko terminal na bazi komutacije kola ili komutacije paketa želi da funkcioniše u okviru mreže treće generacije. SIM i USIM mogu da koegzistiraju, tako da terminali koji poseduju neophodne karakteristike, mogu da koriste istovremeno GSM i UMTS mreže.

Parametri koje skladišti USIM raspoređeni su u okviru sledećih polja:

- **IMSI (*International Mobile Subscriber Identity*),** polje u kome je sadržan identitet koji se posebno dodeljuje svakom od korisnika. IMSI identitet je vidljiv mreži, a ne samom korisniku, i koristi se za potrebe autentifikacije. Kako je napomenuto u poglavlju 1.5.2, predstavlja ekvivalent *Private User Identity-u* u IMS-u.
- **MSISDN (*Mobile Subscriber ISDN Number*),** polja koja sadrže jedan ili više brojeva dodeljenih korisniku. Kako je napomenuto u poglavlju 1.5.1, predstavlja ekvivalent *Public User Identity-u* u IMS-u.
- **CK (*Ciphering Key*) i IK (*Integrity Key*),** polja koja sadrže ključeve neophodne za zaštitu integriteta podataka koji se prenose radio-interfejsom.
- ***Long term secret,*** polje koje sadrži šifru koja se koristi za potrebe autentifikacije korisnika i proračun CK i IK ključeva korišćenih na relaciji terminala i mreže.
- **SMS (*Short Message Service*),** polja u okviru kojih USIM skladišti kratke poruke i njima pridružene podatke (npr., pošiljalac, primalac, status poruke…).
- **SMS (*Short Message Service*) *parameters,*** polja u koja USIM smešta parametre neophodne za konfiguraciju SMS servisa, kao što je adresa odgovorajućeg SMS centra i lista protokola koji su podržani.
- **MMS (*Multimedia Message Service*) *user conectivity parameters,*** polja USIM-a koja sadrže konfiguracione podatke neophodne za MMS servise, kao što su adrese MMS servera ili MMS *gateway*-a.
- **MMS (*Multimedia Message Service*) *user preferences,*** polja koja sadrže posebna podešavanja vezana za funkcionisanje MMS servisa.

1.6.3 ISIM (IP *multimedia SERVICES IDENTITY MODULE*)

Treća aplikacija koja može biti prisutna u okviru UICC-a jeste ISIM (standardizovan u okviru 3GPP TS 31.103). ISIM aplikacija ima posebnu važnost za IMS sistem, jer sadrži set parametara koji se koriste za identifikaciju korisnika, njegovu autentifikaciju i konfiguraciju terminala, kada je terminal aktivan u okviru IMS-a. ISIM može da koegzistira u okviru jedne UICC kartice sa SIM ili USIM aplikacijama pojedinačno, ili sa obe aplikacije istovremeno.

U relevantne parametre koje ISIM skladišti ubrajamo:

- ***Private User Identity****,* isključivo jedan privatni korisnički identitet (detaljno pojašnjeno u poglavlju 1.5.2).
- ***Public User Identities****,* jedan ili više javnih korisničkih identiteta u SIP URI formatu (detaljno pojašnjeno u poglavlju 1.5.1).
- ***Home Network Domain URI,*** naziv domena matične mreže u SIP URI formatu. Navedeni parametar je jedinstven i upotrebljava se tokom procedure registracije u cilju utvrđivanja adrese matične mreže.
- ***Long-term secret,*** dugotrajnu šifru koja se koristi za potrebe autentifikacije korisnika i proračun CK (*Ciphering Key*) i IK (*Integrity Key*) ključeva korišćenih na relaciji terminala i mreže. IMS terminal upotrebljava IK ključ u cilju zaštite integriteta SIP signalizacije koja se razmenjuje između IMS terminala i P-CSCF servera. Ukoliko je signalizacija šifrovana, IMS terminal dodatno koristi CK ključ za potrebe enkripcije i dekripcije SIP signalizacije na relaciji IMS terminala i P-CSCF servera.

Sva prethodno navedena polja su dostupna isključivo za čitanje, što znači da korisnik ne poseduje mogućnost izmene parametara.

Pristup 3GPP IMS mreži se zasniva na prisustvu ISIM ili USIM aplikacije u okviru UICC-a pri čemu se preferira ISIM aplikacija koja je posebno namenjena i prilagođena IMS sistemu. USIM aplikacija zapravo omogućava korišćenje IMS-a (uz izvesna ograničenja) onim korisnicima koji nisu stigli da implementiraju IMS specifičnosti na svoje stare UICC kartice.

Kako SIM aplikacija poseduje niži stepen sigurnosti, pristup 3GPP IMS mreži nije moguće ostvariti pomoću SIM aplikacije.

2. SIGNALIZACIONA RAVAN U OKVIRU IMS-a

Signalizaciona ravan predstavlja nezavistan deo IMS-a u okviru koga se sprovodi prenos i procesiranje signalizacionih SIP poruka. Kroz mnogobrojne koncepte i procedure implementirane u okviru signalizacione ravni, realizuje se uspostavljanje i upravljanje IP multimedijalnim sesijama, aktivira se mehanizam pune kontrole servisa (između ostalog i kontrola kvaliteta, QoS - *Quality of Service*) i obezbeđuje zaštita u IMS-u.

Svaki aspekt funkcionisanja signalizacione ravni biće posebno razmotren.

2.1 UPRAVLJANJE SESIJOM

Upravljanje sesijom svakako predstavlja jedan od osnovnih zadataka signalizacione ravni, a najvažniju ulogu pri realizaciju ove funkcije ima protokol za kontrolu sesije. U okviru IMS sistema, definisanog od strane 3GPP-a i 3GPP2-a, signalizacija i upravljanje sesijama bazirane su na SIP (*Session Initiation Protocol*) protokolu.

Kako je ranije pojašnjeno u okviru poglavlja 1.2.3.1, SIP protokol je inicijalno dizajniran od SIP radne grupe u okviru IETF-a kao signalizacioni protokol Interneta. Kasnije je SIP, zbog svojih dobrih karakteristika postao ujedno i bazičan protokol IMS sistema. Pri tome, zbog specifičnosti koncepcije IMS sistema i zahteva koje treba u okviru njega da ispuni, dizajnirana su mnoga dodatna rešenja koja su naknadno uključena u posebne SIP specifikacije.

Radi kompletnog razumevanja načina upravljanja sesijom u IMS-u, u narednim poglavljima će najpre biti izložene osnovne karakteristike i mehanizmi SIP protokola, a potom će biti objašnjene specifične procedure uspostavljanja i kontrole sesije u signalizacionoj ravni IMS-a.

2.1.1 FUNKCIONALNOSTI SIP PROTOKOLA

SIP (*Session Initiation Protocol*) predstavlja protokol aplikativnog sloja pomoću koga se ostvaruje uspostavljanje, modifikovanje i prekidanje multimedijalnih sesija preko Interneta. Poznato je da jednu multimedijalnu sesiju čini više učesnika između kojih se mogu realizovati i višestruki tokovi razmene podataka. Na primer, sesija može imati oblik telefonskog poziva koji se odvija između dva korisnika, ali i konferencijske veze tokom koje se novi učesnici mogu

uključivati na SIP poziv. SIP sesije su specifične po tome što mogu sadržati opise sesija koji omogućavaju korisnicima da pregovaraju o tipovima medija koji se prenose, kao i o parametrima sesije. SIP protokol obezbeđuje svoje sopstvene mehanizme za pouzdanu kontrolu sesije, a može funkcionisati preko različitih transportnih protokola kao što su TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*) i SCTP (*Stream Control Transmission Protocol*). SIP je takođe kompatibilan sa IPv4 i IPv6 protokolima.

Tokom kontrole sesije SIP je zadužen za sledeće aktivnosti:

- utvrđivanje trenutne lokacije odredišnog korisnika,
- utvrđivanje da li je korisnik voljan da učestvuje u sesiji,
- određivanje karakteristika korisničkog terminala,
- uspostavljanje sesije i
- upravljanje sesijom što uključuje modifikaciju parametara sesije, aktiviranje funkcija za obezbeđivanje servisa tokom sesije i okončanje sesije.

U daljem tekstu detaljnije će biti objašnjeni najbitniji aspekti SIP protokola:

- identifikacija i adresiranje u okviru SIP-a,
- SIP entiteti,
- tipovi SIP poruka,
- opisivanje sesije pomoću SDP (*Session Description Protocol*) protokola,
- tipovi SIP transakcija,
- uspostavljanje i kontrola sesija (objašnjenje će biti uključeno u razmatranje procedure uspostavljanja IMS sesije u poglavlju 2.1.3).

2.1.1.1 Identifikacija i adresiranje u okviru SIP-a

Svaki SIP korisnik se na jedinstven način identifikuje pomoću SIP URI-a (SIP *User Resource Identifier*). SIP URI predstavlja identifikator koji ima formu sličnu *e-mail* adresi i najčešće se sastoji od korisničkog imena (*username*) i naziva domena (*domain name*). Pored ova dva osnovna parametra SIP URI može sadržati i više dodatnih parametara. Radi sticanja opšteg uvida u format SIP URI identifikatora navodi se nekoliko primera:

sip:Petar@mts.telekom.com; transport=tcp
sip:Alice.Smith@domain.com
sip:tao@research.telecordia.com

Prema standardu, opšta forma jednog SIP URI identifikatora ima sledeću formu:

sip:user:password@host:port;uri-parameters?headers

Prvi deo očigledno označava da je u pitanju SIP protokol. Na istoj vodećoj poziciji može se naći i oznaka *sips* u slučaju kada SIP koristi poseban protokol za enkripciju poruka u cilju zaštite njihovog integriteta, što je najčešće TLS (*Transport Layer Security*).

Sledeće polje (tzv. korisničko polje) sadrži opcione informacije o korisniku u vidu korisničkog imena i lozinke u formi: *user:password@.* U slučaju izostavljanja korisničkog polja, SIP URI identifikuje resurs odredišnog *host*-a. U suprotnom, kada se korisničko ime ne izostavlja, identifikuje se konkretan korisnik *host*-a. Iako SIP dozvoljava prisustvo lozinke pri identifikaciji, korišćenje *password* polja se ne preporučuje s obzirom da se SIP poruke prenose nezaštićene. Treba naglasiti da je jedino korisničko polje *case sensitive* ukoliko se navedeno svojstvo eksplicitno ne zahteva u slučaju drugih polja.

2.5 UPRAVLJANJE PRISTUPOM

2.5.1 UPRAVLJANJE PRISTUPOM U OKVIRU INTERNETA

Mehanizmi koji će u ovom poglavlju biti opisani razmatraju da li je korisnik autorizovan da šalje i prima određeni tip servisa, i ako jeste, sa kojim kvalitetom servisa.

Poznato je da se generalno pravila pristupa jednom domenu implementiraju od strane rutera. Kako ruteri ne raspolažu informacijama sadržanim u korisničkom profilu koje su neophodne za donošenje odluke, oni moraju da kontaktiraju entitet koji tim informacijama raspolaže. SIP *proxy* server predstavlja entitet koji autentifikuje korisnike i dobija njihove korisničke profile, neposredno pre uspostavljanja sesije. Stoga, SIP *proxy* proverava informacije o korisniku i daje instrukcije ruteru da li da prihvati ili odbije medij korisnika.

Za komunikaciju između rutera i SIP *proxy* severa koristi se COPS (*Common Open Policy Service Protocol*) pomoću koga se prenose informacije neophodne za regulisanje pravila pristupa, a čije će osnove biti izložene u narednom poglavlju.

2.5.1.1 COPS protokol

COPS protokol predstavlja *request/response* protokol koji se koristi između servera za regulisanje pristupa, koji se u okviru COPS-a označavaju kao PDP (*Policy Decision Point*), i njihovih klijenata označenih kao PEP (*Policy Enforcement Point*).

COPS podržava različite PEP tipove, koji su identifikovani vrednošću polja *Client-Type.* Dva karakteristična primera PEP-ova su ruter sa RSVP funkcionalnošću i GGSN u 3G mreži. Informacije koje oni razmenjuju sa PDP serverima su različitog karaktera, ali oba tipa koriste COPS. Pri tome, *Client-Type* polje zapravo definiše sadržaj poruka koje se razmenjuju između PDP i PEP entiteta.

PDP i PEP razmenjuju COPS saobraćaj preko TCP konekcije koja je uvek inicirana od strane PEP-a. Sa sigurnosnog aspekta, TCP konekcija može biti podržana korišćenjem IPsec-a ili TLS (*Transport Layer Security*) protokola. Posebno treba napomenuti da kada nijedan od ovih sigurnosnih mehanizama nije na raspolaganju, sam COPS obezbeđuje zaštitu integriteta.

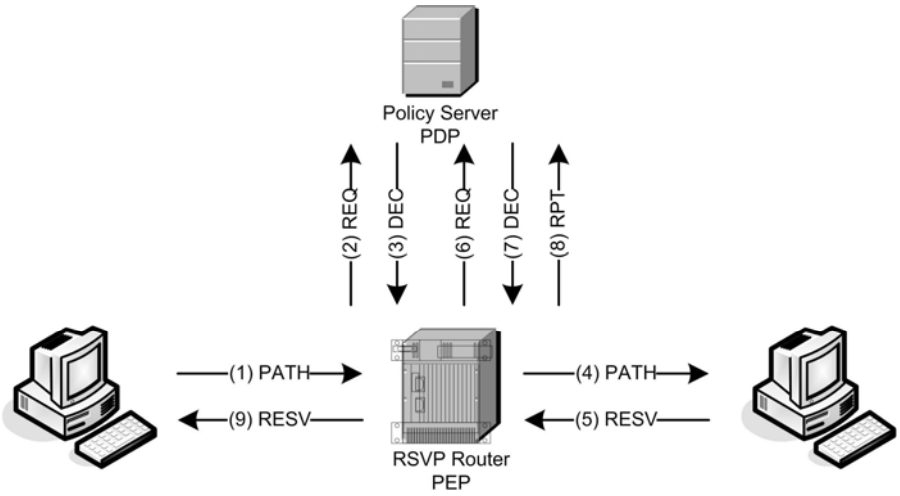
COPS podržava dva modela za kontrolu pristupa: *outsourcing* i *provisioning* modele kontrole.

***Outsourcing* model**

U okviru *outsourcing* modela PEP kontaktira PDP svaki put kada treba doneti odluku o upravljanju pristupom. Korišćenje COPS protokola za RSVP predstavlja primer *outsourcing* modela.

Ruteri koji poseduju RSVP funkcionalnost, koji imaju ulogu PEP-a i koriste COPS *Client-Type* 1, šalju upit PDP-u po prijemu RSVP poruke. Ruter (PEP) specificira koja RSVP poruka je primljena (npr., PATH ili RESV), pri čemu se očekuje od rutera da deluje (npr., da rezerviše resurse za određeni tok podataka). PDP odlučuje da li se zahtev za rezervacijom može prihvatiti ili ne, prema pravilima domena, i šalje svoju odluku PEP-u (ruteru). Takođe, PDP može slati povremene instrukcije PEP-u.

Na slici 2.51 prikazan je primer u kome RSVP ruter komunicira sa serverom za kontrolu pristupa pomoću COPS protokola.



Slika 2.51: Primer korišćenja COPS protokola za potrebe RSVP-a

Kada ruter primi PATH poruku (1) on će informisati server za upravljanje pristupom slanjem REQ poruke (2). Server autorizuje ruter da prosledi PATH poruku slanjem DEC poruke (3). Kada ruter primi RESV poruku on će proslediti serveru još jednu REQ poruku (6) tražeći dozvolu za rezervaciju resursa. Nakon što dobije dozvolu (7) i rezerviše resurse, ruter šalje serveru RPT poruku - izveštaj (8). Konačno, ruter prosleđuje RESV poruku inicijatoru prethodne PATH poruke (9).

***Provisioning* model**

Provisioning model (COPS-PR) upravljanja pristupom omogućava PEP-u da na osnovu pravila o upravljanju koje je dobio od PDP-a samostalno odlučuje. Navedena pravila se uključuju u dokumenta poznata kao PIB (*Policy Information Bases*).

PIB sadrži više PRC-eva (*Provisioning Classes*) koje se dalje sastoje od tzv. instanci označenih kao PRI (*Provisioning Instances*). PRC-ovi se mogu predstaviti kao tabele u kojima je definisana odgovarajuća tema (npr., karakteristike PEP-a), dok se PRI-ovi mogu shvatiti kao pojedini redovi tabele koji sadrže konkretne vrednosti.

Kada COPS-PR klijent kontaktira server, on mu ne prosleđuje informacije o konkretnom događaju, kao u slučaju *outsourcing* modela, već informacije o samom sebi (klijentu). Na osnovu njih, server odlučuje koje instrukcije da pošalje klijentu. Jednom kada klijent preuzme instrukcije, on stiče mogućnost donošenja individualnih odluka bez kontaktiranja servera. To čini COPS-PR skalabilnim protokolom.

2.5.2 UPRAVLJANJE PRISTUPOM U OKVIRU IMS-a

IMS koristi COPS protokol za prenos informacija vezanih za upravljanje pristupom, ali pri tome ne koristi samo jedan model. Umesto toga, koristi se kombinacija prethodno opisanih COPS *outsourcing* i *provisioning* (COPS-PR) modela. Format poruka i korišćenje PIB-ova (*Policy Information Bases*) preuzeto je iz *provisioning* modela. Sa druge strane, prenos *policy* odluka u realnom vremenu potiče iz *outsourcing* modela.

2.5.2.1 SIP procedure

Postoje dva tipa ograničenja koja se mogu primeniti na tipove sesija koje terminal može da uspostavi u IMS mreži:

- *User-specific limitations*: ograničenja definisana za određenog korisnika. Primer specifičnih korisničkih ograničenja predstavlja npr. "*audio-only*" vid pretplate na IMS servise koji onemogućava uspostavljanje video sesije.
- *General network policies*: opšta pravila upravljanja pristupom koja su definisana na nivou cele mreže i koja se podjednako primenjuju na sve korisnike. Primer predstavlja slučaj kada IMS mreža ne dozvoljava korišćenje G.711 audio kodera velikih protoka.

Definisana ograničenja se moraju uzeti u obzir prilikom *offer/answer* razmene koje terminal obavlja u IMS sistemu. S-CSCF i P-CSCF sprečavaju neautorizovanu *offer/answer* razmenu. Pri tome, P-CSCF je zadužen za tretiranje opštih pravila, dok S-CSCF opslužuje oba tipa ograničenja.

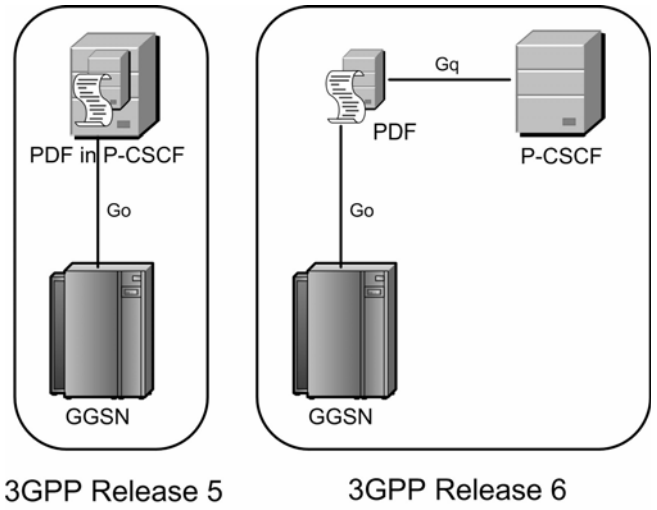
P-CSCF i S-CSCF koriste isti mehanizam kako bi sprečili korisničke agente da ostvaruju neautorizovane *offer/answer* razmene. Pri tome se oslanjaju na mogućnost pristupa SDP telu poruka koje se razmenjuju. Ukoliko ponuda sadrži informacije suprotne pravilima pristupa (npr., nedozvoljeni tip kodera) CSCF šalje 488 (*Not Applicable Here*) odgovor sa kompletnim ili delimičnim SDP opisom pravila.

2.5.2.2 Autorizacija medija

Kada dva korisnička agenta realizuju *offer/answer* razmenu prihvatljivu CSCF serverima zaduženim za kontrolu, oni mogu da razmenjuju medij. Pri tome, mreža mora da uputi GGSN-u adekvatne instrukcije za autorizaciju korisničkog sadržaja medija sve dok je on u saglasnosti sa prethodno autorizovanom *offer/answer* razmenom.

***Policy Decision Function* - PDF**

IMS koristi COPS protokol na relaciji između PDF noda u mreži i GGSN-a. Pri tome, GGSN deluje kao PEP, a PDF kao PDP. U okviru 3GPP *Release*-a 5, PDF predstavlja logički entitet koji može biti kolociran sa P-CSCF serverom ili realizovan kao samostalna jedinica, pri čemu je protokol između njih *proptietery* tipa. Standardizacija protokola između PDF-a i GGSN-a uvedena je u okviru 3GPP *Release*-a 6. Na slici 2. 52 data je ilustracija obe arhitekture.



Slika 2.52: Arhitektura za autorizaciju medija u okviru 3GPP *Release*-a 5 i *Release*-a 6

Interfejs između GGSN i PDF komponenti (označen kao Go interfejs) baziran je na COPS protokolu. Interfejs između PDF-a i P-CSCF-a označen je sa Gq, a proces njegove standardizacije je još uvek u toku.

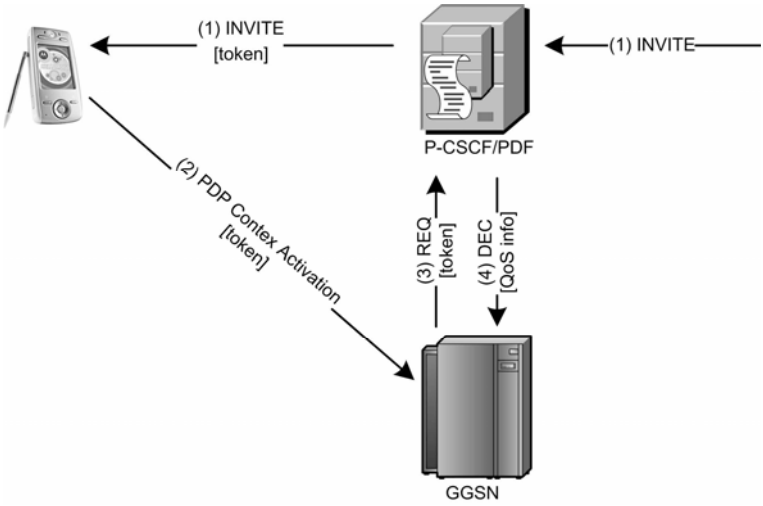
Uloga PDF-a se sastoji u informisanju GGSN-a o karakteristikama sesije za čije uspostavljanje je korisnik u određenom trenutku autorizovan. GGSN koristi navedene informacije u cilju instaliranja filtara za pakete u logiku rutiranja. Stoga, ukoliko korisnički agent pokuša da ostvari neku neautorizovanu radnju, paket će biti odbačen.

Go interfejs nije obavezan u IMS mreži, ali se očekuje da bude implementiran u svim ozbiljnim IMS mrežama, jer operatoru obezbeđuje mnoge korisne funkcionalnosti.

Media Authorization Token

3GPP obezbeđuje mehanizam u mreži kojim se autorizuje uspostavljanje tokova medija. Mehanizam je poznat kao SBLP (*Service-Based Local Privacy*), a zasniva se na uvođenju tzv. koncepta "žetona" za autorizaciju medija koji IMS terminali vraćaju mreži kada zahtevaju uspostavljanje sesije, odnosno razmenu medija.

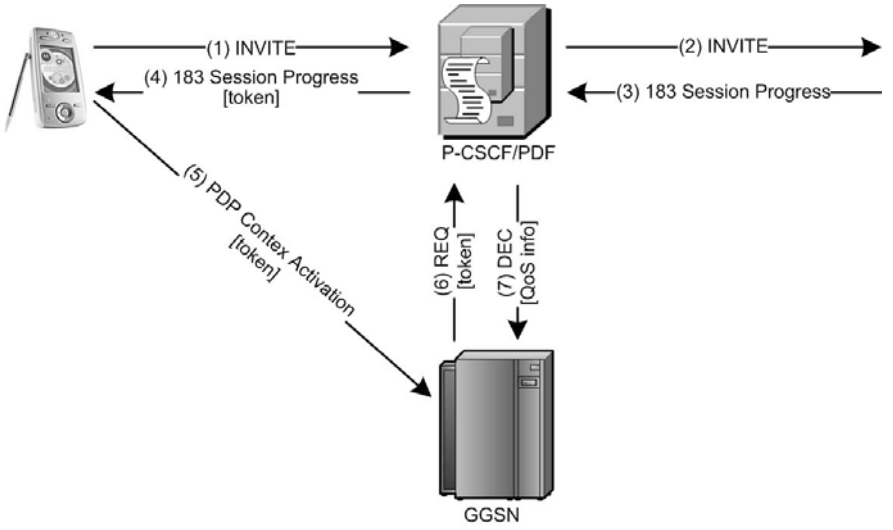
Na slici 2.53 prikazan je tok poruka u slučaju kada različiti entiteti razmenjuju žetone za autorizaciju medija.



Slika 2.53: Prenos žetona za autorizaciju u okviru INVITE zahteva

Slika 2.53 prikazuje PDF kako generiše žeton za autentifikaciju koji P-CSCF priključuje INVITE zahtevu u polje zaglavlja obeleženo kao "P-Media-Authorization". Potom, terminal dodaje žeton (čiji format definiše RFC 3520) u poruke koje šalje za rezervaciju resursa. Kako je u primeru prikazana GPRS pristupna mreža, GGSN će izdvojiti žeton iz primljene poruke i proslediti ga zajedno sa identifikatorom toka, PDF entitetu koji koristi COPS. PDF šalje nazad karakteristike sesije za koje je terminal autorizovan. Ove informacije su označene kao SBLP pristupne informacije.

Na slici 2.54 prikazan je slučaj u kome se žeton razmenjuje prilikom slanja SIP odgovora.



Slika 2.54: Prenos žetona za autorizaciju u okviru SIP odgovora

napredniji koderi kao što je npr., H.264. Posebno treba primetiti da je H.263 koder zahtevani koder za veći broj servisa definisanih 3GPP specifikacijama kao što su: MMS (*Multimedia Messaging Service*), PSS (*Transparent end-to-end Packet-switched Streaming Service*) i IMS. H.263 standard je pretrpeo i nekoliko proširenja (H.263v2 i H.263v3) pre nego što je standardizovan novi H.264 koder.

H.264 standard definiše koder koji je tehnički identičan sa prethodno spomenutim MPEG-4 koderom. Razlog tome je činjenica da su standard zajedničkim naporima razvijali VCEG i MPEG grupe. U praksi se pored ova dva naziva korisi i treći - AVC (*Advanced Video Coding*).

3.1.3. KODIRANJE TEKSTA

Tekst sam po sebi predstavlja digitalnu informaciju, tako da nema potrebe za A/D i D/A konverzijama koje su neophodne u slučaju kodiranja audio i video signala. Postoje dva vida tekstualne komunikacije: *instant* poruke i tekst koji se prenosi u realnom vremenu.

Instant poruke sadrže kompletnu poruku. Pošiljalac kreira kompletnu poruku i šalje je kao celinu, tako da primalac dobija konačnu verziju poruke.

Tekst koji se prenosi u realnom vremenu zapravo podrazumeva prenos informacija o pritiscima na tipke tastature, umesto stvarnog teksta. Ukoliko korisnik koji kuca tekst pogreši i obriše deo sadržaja, korisnik na prijemu će moći da registruje ove modifikacije. To je iz razloga što se na prijemu dobija lista slova i komandi, po redosledu kucanja. Najčešće korišćeni format za prenos teksta u realnom vremenu jeste T.140 (ITU-T *Recommendation* T.140).

3.1.4. OBAVEZNI KODERI KOJI SE KORISTE U IMS-u

Poželjno je da svi IMS terminali podržavaju iste kodere kako bi mogli direktno da komuniciraju, bez potrebe za uvođenjem transkodera. Ipak, 3GPP i 3GPP2 nisu mogli da se dogovore oko usvajanja obaveznih kodera za implementaciju u IMS terminale. Stoga, audio i video sesije između 3GPP i 3GPP2 IMS terminala obično iziskuju transkodere. 3GPP i 3GPP2, svaki zasebno definišu tipove kodera koje moraju podržati njihovi IMS terminali.

Svi 3GPP IMS terminali podržavaju AMR govorni koder i H.263 video koder. 3GPP IMS terminali koji obezbeđuju širokopojasne servise podržavaju AMR-WB audio koder, a terminali koji obezbeđuju prenos teksta u realnom vremenu podržavaju T.140.

3.2. PRENOS MEDIJA

Sa aspekta prenosa medija razlikujemo dva tipa medija: medij koji toleriše izvesni gubitak paketa i medij koji gubitke ne toleriše uopšte. Primer prvog tipa medija predstavljaju audio i video servisi, a kao primere drugog tipa navodimo *web* stranice i *instant* poruke. Ukoliko se izgubi nekoliko paketa tokom audio prenosa primalac može primetiti degradaciju u kvalitetu zvuka, ali će razumeti njen sadržaj. Suprotno tome, ukoliko se ne prenesu izvesni delovi *instant* poruke, njen sadržaj i smisao se mogu sasvim pogrešno protumačiti.

Protokol transportnog nivoa za specifični medij se bira na osnovu tipa medija. Tradicionalno, TCP (*Transport Control Protocol*) protokol se koristi za pouzdan prenos medija,

a UDP (*User Datagram Protocol*) za prenos koji ne garantuje pouzdanost. Ipak, UDP protokol nije pogodan za prenos velikih količina podataka, jer ne poseduje mehanizme za kontrolu zagušenja. Kako bi rešio ovaj problem, IETF je razvio poseban novi protokol nazvan DCCP (*Datagram Congestion Control Protocol*).

3.2.1. POUZDANI PRENOS MEDIJA

Postoje dva transportna protokola koja omogućavaju pouzdani prenos korisničkih podataka. To su:

- TCP (*Transport Control Protocol*) protokol kojim se isporučuje niz *byte*-ova i
- SCTP (*Stream Control Transmission Protocol,* specificiran u RFC 2960) protokol, kojim se isporučuju podaci u vidu poruka.

TCP najbolje funkcioniše u slučajevima kada korisnik, koji prima podatke, ne mora da sačeka sve podatke da pristignu da bi počeo sa procesiranjem. Čitači Internet stranica su najbolji primeri za navedeni slučaj. Kada korisnik zatraži sadržaj izvesne stanice pomoću HTTP-a, Internet čitač prima navedeni sadržaj tokom nekoliko TCP konekcija, ali se korisniku u svakom trenutku prikazuju do tada pristigle informacije. Na ovaj način, korisnik ne mora da čeka kompletan sadržaj stranice da bi počeo sa čitanjem.

SCTP protokol predstavlja bolji izbor u odnosu na TCP, kada su aplikacije zainteresovane za prijem svih podataka odjednom. SCTP aplikaciji isporučuje poruke umesto niza *byte*-ova. Poruka može na primer, sadržati kompletnu *instant* poruku ili fajl koji se prenosi između korisnika. SCTP takođe obezbeđuje funkcionalnosti koje nisu sadržane u TCP protokolu, kao što su bolja zaštita od DoS (*Denail of Service*) napada, *multi-homing*, višestruki nizovi podataka po SCTP asocijaciji (konekcije u SCTP-u su označene kao asocijacije).

Iako SCTP pruža izvesne prednosti, TCP je i dalje najrasprostranjeniji pouzdani protokol.

Mnogi protokoli uspostavljaju TCP konekcije kako bi prenosili i kontrolne poruke i korisničke podatke. Primer predstavljaju HTTP, SMTP i Telnet protokoli. U okviru ovih protokola, klijent šalje zahtev serveru preko TCP konekcije, a server preko iste konekcije šalje natrag zatražene podatke. Klijenti uspostavljaju ove konekcije preko poznatih portova identifikovanih protokolom. Na primer, *web* čitač, koji sadrži HTTP klijent, šalje zahteve serverima na port broj 80, poznatiji kao HTTP port.

SIP protokol ima mogućnost uspostavljanja TCP konekcija ili SCTP asocijacija bez korišćenja poznatih portova. Naime, SDP opis sesije definiše tip podataka koji se prenose i protokol koji se koristi što uslovljava da se pouzdani i nepouzdani tipovi konekcije uspostavljaju na isti način. Na slici 3.2 prikazan je primer SDP opisa sesije za TCP konekciju koja treba da prenosi slike u T.38 formatu (format koji se koristi za slanje faks poruka). *Passive direction* atribut ukazuje da će primalac ovog SDP-a biti aktivni deo sesije i da će on inicirati TCP konekciju.

```
v = 0
o = Alice 2890844526 2867842807 IN IP4 192.0.0.2
s = I will send you a fax
c = IN IP4 192.0.0.2
t = 0 0
m = image 20000 TCP t38
a = direction:passive
```

Slika 3.2: TCP konekcija u ramu SDP opisa sesije

3.2.2. NEPOUZDANI PRENOS MEDIJA

UDP predstavlja protokol za nepouzdani prenos podataka. Korisnik koji šalje UDP pakete se nada da će većina njih stići na prijem kako bi primalac poruke bio u stanju da je razume.

Iako je veoma rasprostranjen, UDP protokol poseduje veliki nedostatak kada je reč o prenosu velikih količina podataka. Naime, UDP ne obezbeđuje bilo kakav mehanizam kontrole zagušenja. Korisnici koji uspostavljaju UDP konekcije neće usporiti sa slanjem podataka, čak ni kada u mreži vlada ozbiljno zagušenje i time će situaciju učiniti još gorom. Iako se kontrola zagušenja obavezno implementira na nivou aplikacionog sloja, praktikuje se njeno prisustvo u većini drugih slojeva.

Porast broja aplikacija koje koriste UDP za nepouzdani prenos bio je indikacija IETF-u da postoji potreba za protokolom transportnog nivoa koji bi uključio mehanizam kontrole zagušenja u mreži. Prvi predlog je bio da se kreira SCTP ekstenzija za nepouzdani prenos. Ipak, mehanizmi SCTP-a za kontrolu zagušenja nisu prikladni za neke tipove multimedijalnog saobraćaja. DCCP (*Datagram Congestion Control Protocol*) protokol, specificiran u okviru RFC-a 4340 podržava različite tipove mehanizama za kontrolu zagušenja i dizajniran je sa ciljem da odgovara multimedijalnom saobraćaju.

3.2.2.1. DCCP protokol

DCCP predstavlja nepouzdani protokol transportnog nivoa koji omogućava uspostavljanje i okončanje konekcije, kao i pregovaranje o algoritmima za kontrolu zagušenja koji će se koristiti tokom konekcije.

DCCP konekcije se uspostavljaju dijalogom u tri faze (*three-way handshake*), tokom kojeg se pregovara o karakteristikama konekcije. Posebno treba istaći dogovor DCCP aktera o algoritmu za kontrolu zagušenja koji će koristiti. U opštem slučaju algoritmi se razlikuju po CCID-u (*Congestion Control Identifier*) koji im se dodeljuje. Trenutno postoje tri CCID-a koja se mogu odabrati kao oznake za specifični tip kontrole zagušenja:

- ***Sender-based,***
- ***TCP-like*** i
- ***TRFC (TCP-Friendly Rate Control).***

TRFC algoritam (specificiran u RFC-u 5348) je posebno pogodan za multimedijalni saobraćaj, jer izbegava grube izmene u protoku podataka i na fer način deli dostupni protok sa TCP protokolom.

DCCP još uvek predstavlja novi protokol, pa u skladu sa tim nije veoma zastupljen.

3.2.2.2. RTP protokol

RTP (*Real-time Transport Protokol,* specificiran u RFC-u 3550) omogućava prenos medija koji se prenose u realnom vremenu, kao što su audio i video sadržaji, pomoću nepouzdanih protokola kao što su UDP i DCCP. Upotrebljava se uvek zajedno sa RTCP (RTP *Control Protocol*) protokolom koji obezbeđuje statistiku kvaliteta servisa i informacije za uspostavljanje sinhronizacije unutar medija.

Glavni zadatak RTP-a jeste da omogući prijemnicima da generišu adekvatan takt pri emitovanju medija, jer IP mreže nisu u stanju da potpuno sačuvaju vremenske relacije podataka koji se prenose, odnosno unose tzv. *jitter*. Na primer, ukoliko se na istu destinaciju pošalju dva IP paketa u razmaku od 10ms, ne postoji garancija da će drugi paket stići na odredište 10ms nakon prvog. Štaviše, postoji mogućnost da drugi paket pristigne u isto vreme kad i prvi, mnogo kasnije ili čak pre prvog paketa. To za posledicu ima da prijemnici ne mogu da se oslone na vreme pristizanja paketa prilikom uspostavljanja redosleda paketa u ramu medija. U tu svrhu koriste se RTP vremenske oznake.

RTP paketi se na prijemu smeštaju u bafer po redosledu koji diktiraju vremenske RTP oznake na paketima. Ukoliko je paket sa specifičnom oznakom neophodan za emitovanje, a još uvek nije stigao, koriste se tehnike interpolacije kako bi se popunila praznina (npr., u slučaju audio medija moguće je emitovati poslednji paket u dužem vremenskom periodu). Ukoliko paket koji je nedostajao stigne na odredište nakon emitovanja biće odbačen.

Pored vremenskih oznaka, RTP paketi sadrže i sekvencijalne brojeve. Oni se upotrebljavaju na prijemu kako bi se utvrdilo koliko je paketa izgubljeno u mreži tokom prenosa. Ukoliko se u mreži gubi suviše paketa izvesno vreme, učesnici u konekciji mogu da odluče da promene postojeći koder i upotrebe tip kodera koji obezbeđuje bolji kvalitet u lošijim uslovima.

RTP paketi takođe nose binarne identifikatore pošiljaoca i tip sadržaja koji se prenosi. Identifikatori pošiljaoca se koriste tokom konferencijskih veza u cilju identifikacije govornika, a tip sadržaja identifikuje način kodiranja i format prenosa podataka RTP paketa. Tip sadržaja predstavlja numeričku vrednost koja označava određeni koder koji je odabran tokom pregovaranja prilikom uspostavljanja sesije i sadržan je u SDP opisu sesije. Statički tipovi sadržaja su brojevi koji uvek odgovaraju istom koderu. Na primer, tip sadržaja 0 odnosi se na G.711 μ-*law* audio koder.

Dinamički tipovi sadržaja se određuju tokom pregovora korišćenjem *offer/answer* modela. Oni identifikuju određeni koder u ramu konkretne sesije. Na slici 3.3 prikazan je SDP opis sesije koji sadrži audio sadržaj koji može biti kodiran korišćenjem G.711 μ-*law* (statički tip sadržaja 0) ili korišćenjem 16-bitnog linearnog stereo kodera sa frekvencijom odabiranja 16KHz (dinamički tip sadržaja 98, specificiran je u redu a=rtpmap:98 L16/16000/2). Primalac audio sadržaja će primiti RTP pakete čiji tipovi sadržaja mogu imati vrednosti 0 ili 98 i na osnovu opisa sesije će ih dekodirati.

```
v = 0
o = Alice 2890844526 2867842807 IN IP4 192.0.0.2
s = Let's talk!
c = IN IP4 192.0.0.2
t = 0 0
m = audio 20000 RTP/AVP 0 98
a = rtpmap:98 L16/16000/2
```

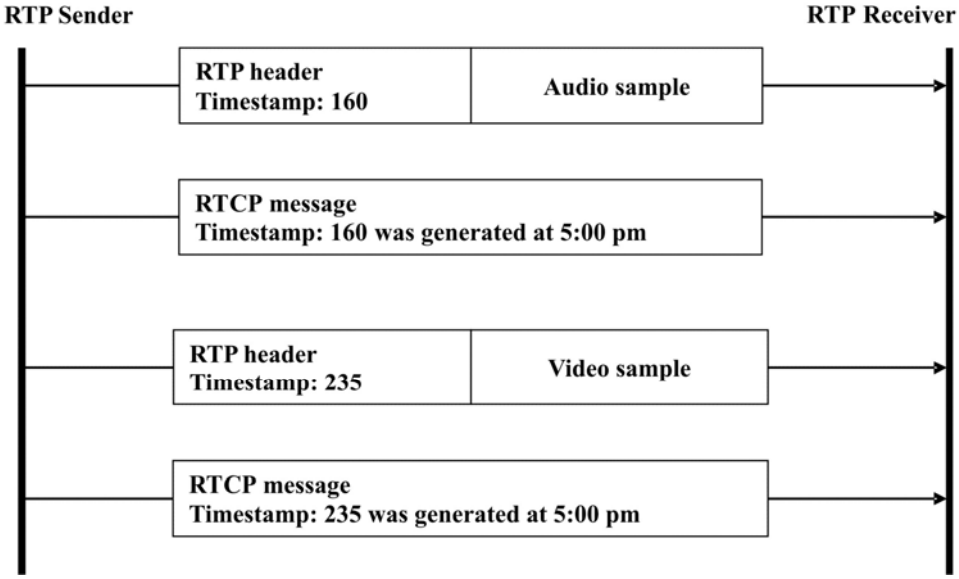
Slika 3.3: SDP opis sesije sa statičkim i dinamičkim tipovima sadržaja

3.2.2.3. RTCP protokol

RTCP (RTP *Control Protocol*) predstavlja protokol koji se uvek koristi zajedno sa RTP-om. On obezbeđuje statistiku kvaliteta servisa, informacije neophodne za uspostavljanje sinhronizacije unutar medija i realizuje mapiranje između RTP binarinih identifikatora pošiljaoca i naziva čitljivih od strane korisnika. RTCP poruke šalju i RTP pošiljaoci i RTP primaoci paketa.

Za kreiranje statistike o kvalitetu servisa, RTP korisnici izveštavaju (korišćenjem RTCP protokola) jedni druge o broju RTP paketa koje su poslali, odnosno primili. Na taj način jednostavno je utvrditi broj izgubljenih paketa tokom sesije.

Prilikom slanja paketa, RTP koristi RTCP kako bi obezbedio mapiranje između vremenskih oznaka svojih medijskih sesija i prave vremenske satnice. Na taj način, na prijemu je moguće sinhronizovati različite tokove podataka. Primer interne sinhronizacije predstavlja audio-video sinhronizacija, tzv. sinhronizacija usana (*lip synch*). Na slici 3.4 pokazano je kako RTCP mapiranje omogućava prijemniku da ostvari sinhronizaciju usana .

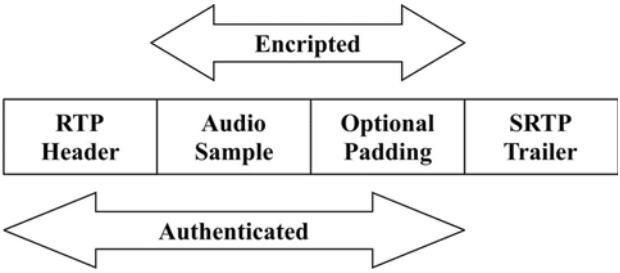


Slika 3.4: Korišćenje RTCP-a za potrebe *lip synch* sinhronizacije

Kao što je već navedeno, RTCP poruke takođe obezbeđuju mapiranje između RTP binarnih identifikatora pošiljaoca i naziva razumljivih korisniku. Navedeni tip mapiranja je jako koristan u slučaju konferencijskih veza kada se medij istovremeno prima od strane različitih korisnika na istoj adresi. RTCP omogućava korisnicima da budu u svakom trenutku informisani ko govori.

3.2.2.4. SRTP protokol

SRTP (*Secure RTP*, specificiran u RFC-u 3711) obezbeđuje poverljivost, autentifikaciju poruka i zaštitu od reprodukcije RTP i RTCP saobraćaja. Na slici 3.5 ilustrovano je koji delovi RTP paketa podležu autentifikaciji, a koji delovi bivaju enkriptovani.



Slika 3.5: SRTP protekcija

Pri korišćenju SRTP-a za razmenu medija, od mehanizama zaštite koristi se *key management* protokol za generisanje *master* i *session* ključeva. Ključevi za zaštitu sesije, *session keys*, periodično se osvežavaju kako zlonamerni napadači ne bi imali pristup velikim količinama podataka enkriptovanih istim ključem.

3.2.3. PRENOS MEDIJA U IMS-u

IMS najčešće koristi RTP protokol preko UDP-a za nepouzdani prenos medija. DCCP će se možda koristiti u budućnosti, ali trenutno nije dovoljno rasprostranjen da bi se koristio u okviru IMS-a.

Sa aspekta sigurnosti, IMS ne obezbeđuje nikakav tip zaštite na nivou sloja medija. Pretpostavlja se da je saobraćaj enkriptovan na nižim slojevima pri pristupu radio mreži, kao i da IMS predstavlja pouzdanu mrežu.

Kada je reč o pouzdanim protokolima transportnog nivoa, logičan izbor je TCP. TCP predstavlja stabilan protokol i veoma je rasprostranjen. Kao dodatak, koriste se ekstenzije dizajnirane da omoguće mehanizme za kontrolu tokova koji su pogodniji za radio-veze.

4. REALIZACIJA SERVISA U OKVIRU IMS-A

Nakon što su razmotreni tehnologije i mehanizmi koje IMS koristi (poglavlja 2 i 3), može se pristupiti razjašnjavanju na koji način IMS ostvaruje svoj osnovni cilj: pružanje servisa.

Za sada su poznate procedure uspostavljanja i kontrole multimedijalnih IMS sesija, kao i bogatstvo različitih karakteristika koje sesija može da ima, posebno sa aspekta medija koji se prenosi. Takođe, prikazano je da neki servisi (npr., servis govorne pošte) ne zahtevaju posebnu standardizaciju, već ih je moguće obezbediti uz pomoć osnovnih mehanizama.

Ipak, treba istaći da postoje servisi koji zahtevaju posebnu standardizaciju i oni će biti predmet razmatranja u ovom poglavlju. Odabrani su neki od najznačajnijih servisa, inicijalno podržani od strane IMS-a. To su *Presence* servis, *Instant-messaging* i *Push-to-Talk*.

Treba napomenuti da se ovom grupom ne iscrpljije lista servisa koje IMS može da obezbedi. Mnogi novi i inovativni servisi će u budućnosti biti razvijeni u okviru IMS infrastrukture i standardizovani.

4.1. *PRESENCE* SERVIS NA INTERNETU I U OKVIRU IMS-a

Presence, (u grubom prevodu na naš jezik znači prisutnost), predstavlja jedan od osnovnih servisa za koje se očekuje da će u budućnosti biti svuda zastupljeni. U okviru svog osnovnog zadatka, *presence* servis treba da obezbedi znatnu količinu poručenih informacija određenoj grupi korisnika. Pored toga, *third-party* servisi će imati mogućnost da čitaju i analiziraju *presence* informacije kako bi modifikovali servis koji pružaju korisniku u skladu sa njegovim potrebama i željama sadržanim u *presence* informacijama.

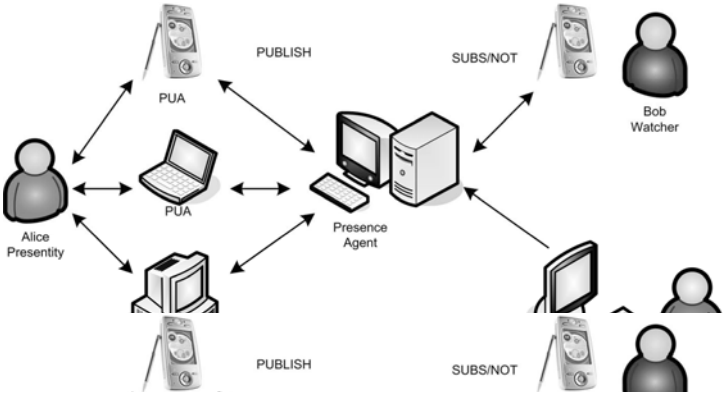
Presence servis je definisan od strane IETF-a i inicijalno razvijen u okviru Interneta. Kasnije je podržan i u okviru odgovarajuće IMS arhitekture koja je omogućila različite primene *presence* servisa u IMS-u.

4.1.1. *PRESENCE* SERVIS NA INTERNETU

4.1.1.1. Osnovne karakteristike *Presence* servisa

Presence predstavlja servis koji omogućava korisniku da se informiše o dostupnosti, raspoloživosti i želji za komunikacijom nekog drugog korisnika. *Presence* ustvari daje indikaciju da li su odabrani korisnici aktivni ili ne, kao i to da li su slobodni za komunikaciju ili su pak, zauzeti (npr., prisustvuju nekom poslovnom sastanku ili razgovaraju telefonom) u slučaju kada su aktivni. Dodatno, *presence* servis omogućava korisnicima da informišu druge korisnike o komunikacionim uređajima kojima raspolažu, kao i njihovim karakteristikama (npr., da li poseduju audio ili video karakteristike itd.).

Presence koncept definiše različite aktere i njihove uloge, prikazane ne slici 4.1.



Slika 4.1: SIP *Presence* arhitektura

Osoba koja obezbeđuje informacije *presence* servisu naziva se *presentity*, skraćeno od *presence entity*, što bi se moglo prevesti kao prisutni entitet. Na slici 4.1 *Alice* ima *presentity* ulogu. *Presentity* pruža *presence* informacije (set atributa koji karakterišu *presentity*-ja) kao što su npr., status, adresa za komunikaciju itd. Određeni *presentity* može imati više uređaja označenih kao *Presence User Agents* (PUAs) koji su zaduženi za pružanje njegovih *presence* informacija.

Na slici 4.1 prikazana su tri PUA-a: jedan IMS terminal, jedan *laptop* i jedan *desktop* računar. Svaki od njih sadrži izvesne informacije o *Alice*, kao *presentity*-u. Oba kompjutera mogu znati da li je *Alice* ulogovana ili ne. IMS terminal poznaje status registracije koji *Alice* ima, kao i to da li je ona uključena u neku od multimedijalnih sesija. Spektar informacija može biti dopunjen satnicom kada će se *Alice* vratiti sa ručka ili indikacijom da li je *Alice* dostupna za videokonferenciju. Svi PUA-ovi šalju informacije koje poseduju nadređenom entitetu koji se zove *Presence Agent* (PA). PA je zadužen za prikupljanje svih informacija i kreiranje kompletne slike za *presence* skup informacija koja pripada *Alice*.

Presence Agent je najčešće integrisan u tkz. *Presence Server* (PS). PS predstavlja funkcionalni entitet koji deluje ili kao PA ili kao *proxy* server za SUBSCRIBE zahteve.

Na slici 4.1 prikazane su još dve osobe akteri u *presence* servisu. U pitanju su *Bob* i *Cynthia* koji imaju ulogu tzv. "posmatrača" (*watcher*-a). *Watcher* je entitet koji potražuje *presence* informacije o određenom *presentity*-u ili *watcher* informacije o njegovim drugim

posmatračima. Pri tome, postoji više tipova *watcher*-a. *Fetcher* je posmatrač koji od PA-a dobija aktuelne *presence* informacije na zahtev. Sa druge strane, *subscribed watcher* je posmatrač koji želi da bude obaveštavan o izmenama (budućim) *presence* informacija *presentity*-a.

Većina aplikacija kombinuje *presentity* i *watcher* funkcionalnosti u okviru jednog softverskog paketa, skrivajući time od krajnjeg korisnika razliku koja postoji između procesa objavljivanja *presence* informacija i njihovog preuzimanja. U skladu sa učešćem u različitim procedurama, navedene funkcije će tokom izlaganja biti tretirane zasebno.

Presence servis zapravo predstavlja posebnu aplikaciju izgrađenu na vrhu SIP koncepta za notifikaciju o događajima. Navedeni koncept omogućava PUA entitetu da korišćenjem SIP REQUEST transakcija preuzme (*fetch*) postojeće ili da se prijavi (*subscribe*) da prima buduće izmene *presence* informacija o *presentity*-u. U drugom slučaju, status pretplate PUA-a se čuva u okviru PA-a, koji se sa aspekta SIP notifikacionog koncepta odnosi kao tzv. *notifier*. Naime, PA korišćenjem SIP NOTIFY transakcija, obaveštava sve pretplaćene PUA entitete kada god nastanu promene *presence* informacija.

Sve SUBSCRIBE/NOTIFY transakcije sadrže SIP *Event* polje u zaglavlju poruke koje identifikuje aktuelni događaj na koji se prijava (*subscription*) ili notifikacija odnose. *Internet Draft* „*A Presence Event Package for the Session Initiation Protocol* (SIP)“ definiše „*presence*“ tip događaja u okviru SUBSCRIBE ili NOTIFY zahteva pomoću vrednosti *presence* u *Event* polju zaglavlja.

Presence servis kao i *e-mail* ili AAA funkcije, može biti identifikovan tzv. “*pres* URI“ adresom. *Pres* URI ne specificira koji protokol se koristi za pristup resursima ovog servisa. Ipak, preporučuje se korišćenje *sip* ili *sips* URI-a, kada god je to moguće. Primer *pres* URI-a je: *pres:Alice@example.com*.

4.1.1.2. Presence Information Data Format - PIDF

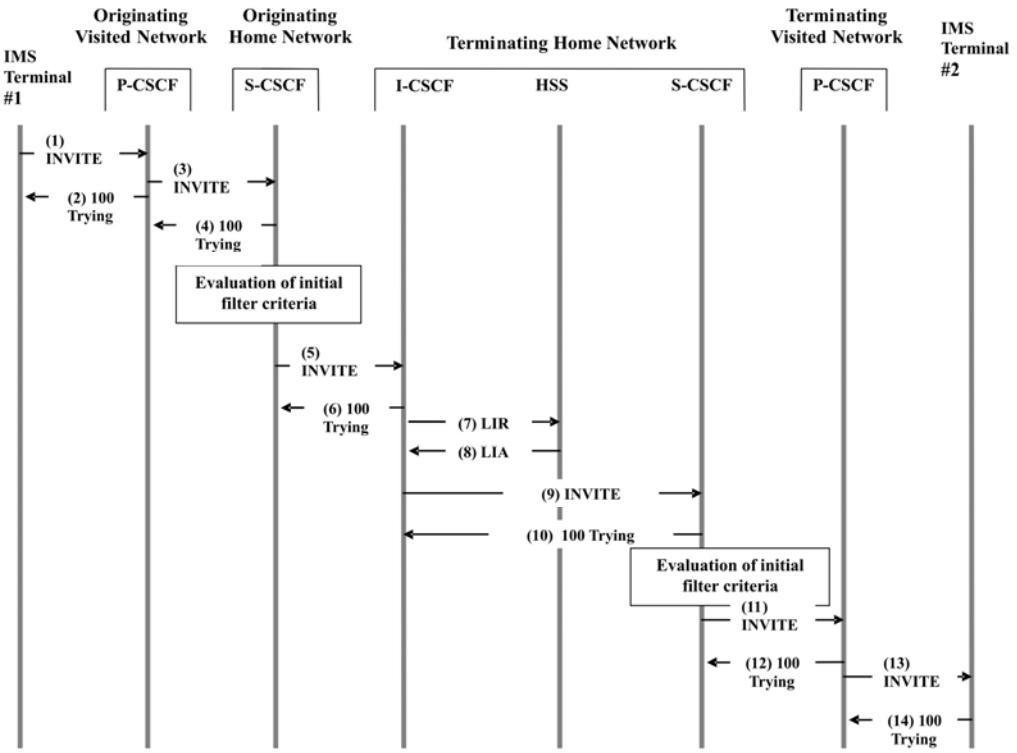
PIDF (specificiran u *Internet Draft*-u „*Presence Information Data Format* (PIDF)“) je format prenosa semantičkog sadržaja *presence* informacija između dva *presence* entiteta. PIDF predstavlja zajednički profil tako da i drugi protokoli, pored SIP-a, imaju mogućnost prenosa *presence* informacija.

PIDF je osmišljen tako da uključi minimalni broj podataka pomoću kojih se mogu zadovoljiti osnovne potrebe servisa. Navedeni minimalistički pristup garantuje upotrebljivost PIDF-a od strane različitih protokola. Dodatno, PIDF u velikoj meri podržava kreiranje ekstenzija kada postoji potreba za proširenjem osnovnog modela.

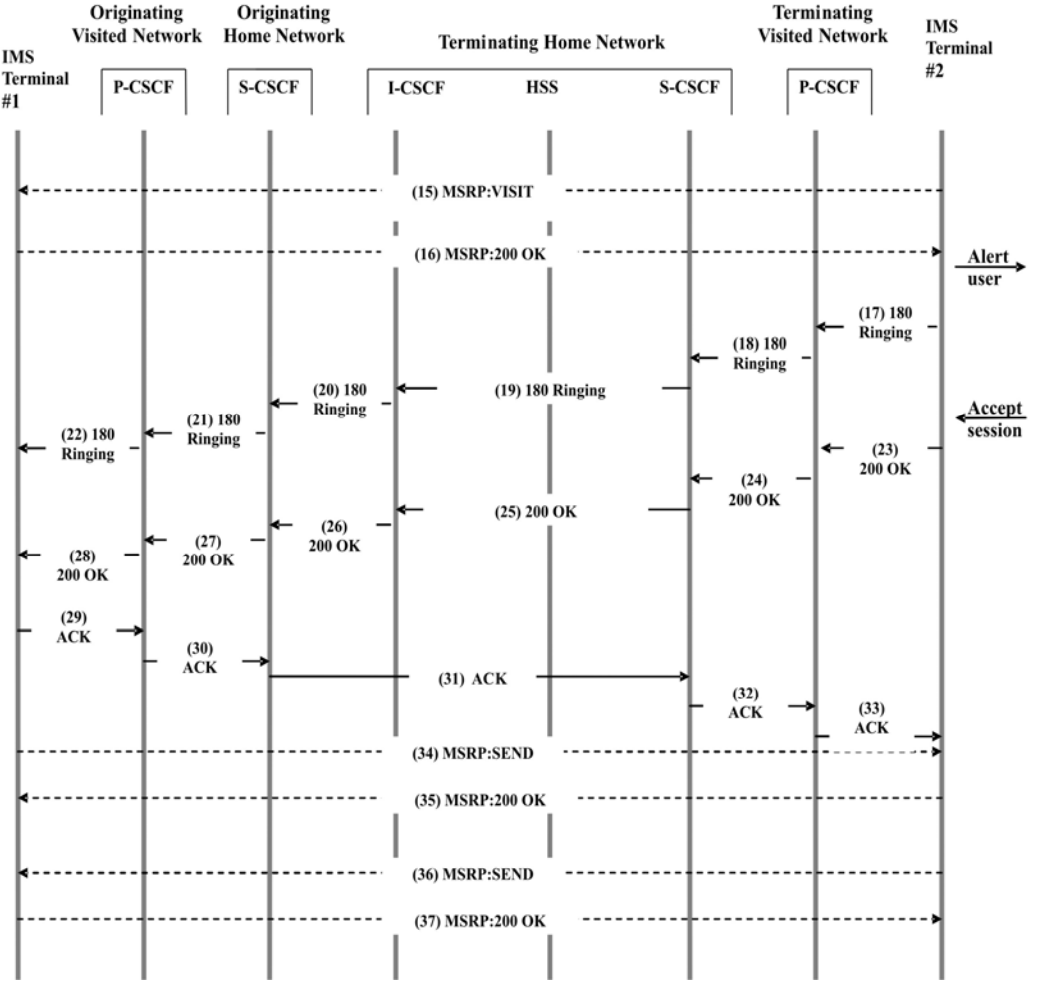
PIDF kodira *presence* informacije u formu XML (*Extensible Markup Language*) dokumenta koji se može prenositi u okviru PUBLISH ili SUBSCRIBE/NOTIFY transakcija. PIDF dokument sadrži *presence* informacije o *presentity*-u. Navedene informacije se sastoje od većeg broja elemenata, od kojih se svaki označava kao segment (engl. *tuple*). Svaki segment sadrži više standardnih elemenata:

- ***status*:** status *presentity*-a označen kao *open* ili *closed,* što bi bilo ekvivalentno terminima *online* i *offline*, respektivno;
- ***contact:*** opcioni element koji obezbeđuje URI za kontaktiranje *presentity*-a;
- ***note, timestamp*** i druge opcione elemente.

Kako *open* i *closed* statusi nisu dovoljni za mnoge aplikacije, PIDF dozvoljava da ekstenzije definišu nove statuse, kao što su na primer, „*at home*“, „*on the phone*“, „*away*“ itd.



Slika 4.15a: *End-to-end* MSRP sesija



Slika 4.15b: *End-to-end* MSRP sesija

Prethodno opisani scenario može uključivati MRFC i MRFP komponente IMS-a kao posrednike. Ovakav slučaj može biti posledica želje operatora da realizuje tarifiranje na osnovu veličine poruka ili na osnovu nekog dodatnog kriterijuma naznačenog u MSRP SEND porukama. Dodatno, MRF može imati ulogu konferencijske jedinice za razmenu poruka između više strana, poznatije kao tzv. "*chat server"*.

4.3. *PUSH-TO-TALK* SERVIS

Push-to-Talk servis predstavlja prvi IMS servis koji su svojim korisnicima pružili mnogi operatori zato što ne zahteva implementaciju novih radio-tehnologija. Za realizaciju *Push-to-Talk* servisa na nivou transportnog sloja mogu se čak koristiti i linkovi malog protoka i velikih kašnjenja. Navedeni tipovi linkova bi bili krajnje neprikladni za opsluživanje drugih tipova servisa kakav je npr., prenos govora.

Push-to-Talk predstavlja *walki-talkie* tip servisa. Korisnici pritisnu i drže taster kada žele nešto da objave, ali ne otpočinju sa konverzacijom sve dok im terminal ne ukaže na to, najčešće emitovanjem zvučnog signala (*beeping*). U ovom stadijumu, korisnici servisa izraze sve što su želeli i označe kraj govora i sesije, oslobađanjem tastera koji su držali pritisnut.

Za razliku od regularnih govornih poziva koji funkcionišu u *full-duplex* režimu, *Push-to-Talk* predstavlja *half-duplex* režim. To znači da u određenom trenutku, samo jedan od korisnika može da govori.

4.3.1. *PUSH-TO-TALK* STANDARDIZACIJA

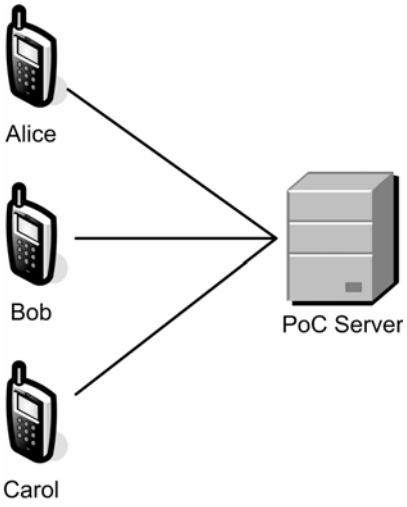
Trenutno postoji više nekompatibilnih *Push-to-Talk* specifikacija. Mnoge od njih nisu bazirane na IMS-u, već sadrže licencirana rešenja implementirana od strane pojedinih proizvođača. Kao rezultat toga, postojeća *Push-to-Talk* rešenja generalno nisu interoperabilna sa opremom drugih proizvođača.

Mnogi operatori zainteresovani za obezbeđivanje *Push-to-Talk* servisa, nisu se osećali komforno u prethodno opisanoj situaciji na tržištu i tražili su od nekih proizvođača da realizuju standardizovano rešenje bazirano na IMS-u. Kao posledica toga, grupa proizvođača (*Ericsson, Motorola, Nokia* i *Siemens*) se udružila i razvila otvoreni *Push-to-Talk* industrijski standard zvani PoC (*Push-to-Talk over Cellular*). Rezultat navedene saradnje bio je set javno dostupnih PoC specifikacija.

OMA trenutno radi na razvoju *Push-to-Talk* standarda baziranog na IMS-u. OMA je kao početnu tačku u razvoju preuzeo PoC specifikacije od navedenog tima proizvođača. U isto vreme IETF radi na izgradnji određenih blokova koji nedostaju SIP arhitekturi kako bi se obezbedio *Push-to-Talk* servis sa kompletnim karakteristikama. Verovatno je da će i OMA iskoristiti rad IETF-a i uključiti ga u svoje konačno *Push-to-Talk* rešenje.

4.3.2. *PUSH-TO-TALK* ARHITEKTURA

Na slici 4.16 prikazana je PoC arhitektura. Svi korisnici su povezani na isti PoC server koji opslužuje i signalizaciju i medij. Sa strane IMS jezgra, PoC server se vidi kao bilo koji drugi aplikacioni server, pri čemu su njegovi servisi implementirani poštujući standardne IMS procedure.

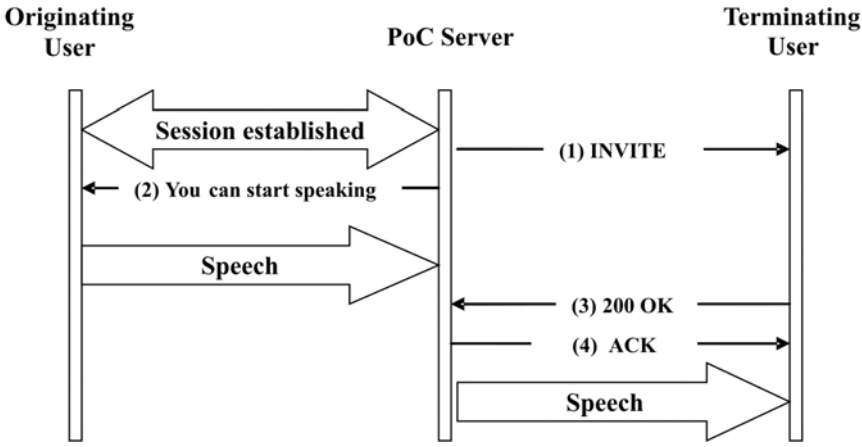


Slika 4.16: PoC arhitektura

Jednom kada se uspostavi PoC sesija korišćenjem SIP protokola, PoC server obavlja kontrolu toka i distribuciju medija. *Push-to-Talk* servis funkcioniše tako što terminali zahtevaju od PoC servera da im dodeli pravo govora (*floor*), što im PoC odobrava, redom jednom po jednom. Terminal koji dobije pravo govora, šalje medij PoC serveru koji ga dalje distribuira do odgovarajućih korisnika. Za transport paketa govora koristi se RTP protokol, dok je RTCP protokol zadužen za kontrolu dodele prava govora korisnicima.

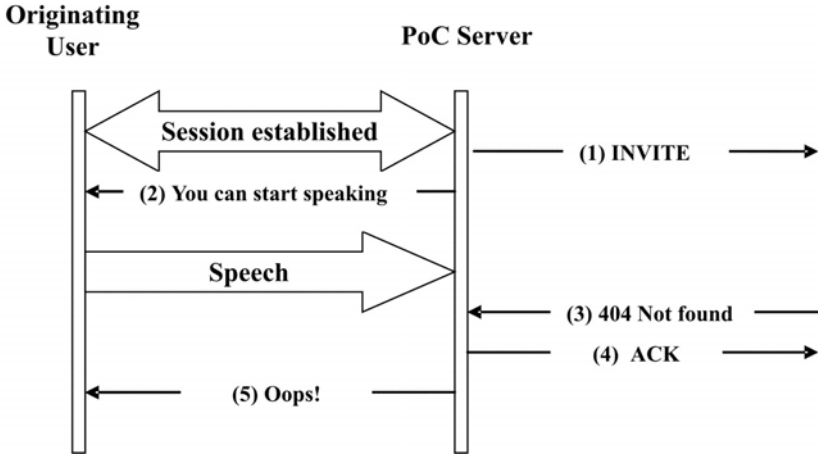
Putanja kojom se medij šalje uvek prolazi kroz PoC server, čak i kada je reč o scenariju između dva aktera. Na taj način, jednostavno je dvočlanoj sesiji priključiti nove aktere.

U okviru PoC-a može da se realizuje i tzv. *early media* servis, što od PoC-a zahteva skladištenje paketa koji se prenose. *Early media* servis je kreiran u cilju smanjenja vremenskog intervala koji protekne od trenutka kada korisnik pokuša da uspostavi sesiju do trenutka kada počinje da govori. Naime, uspostavljanje sesije *early media* servisa uključuje jednu INVITE transakciju između pozivajućeg korisnika i PoC servera i još jednu INVITE transakciju na relaciji između PoC-a i pozvanog korisnika. U okviru *early media* servisa, PoC server dodeljuje pravo govora pozivajućem korisniku pre završetka druge INVITE transakcije, kao što je prikazano na slici 4.17. PoC server pretpostavlja, na osnovu informacija koje poseduje, da će pozvani korisnik biti dostupan i da će prihvatiti sesiju. Stoga, PoC skladišti sve primljene govorne pakete od pozivajućeg korisnika pre nego što pozvani korisnik pošalje odgovor. Kada pozvani korisnik prihvati sesiju PoC server mu šalje sve pakete koje je sačuvao.



Slika 4.17: *Early media* servis

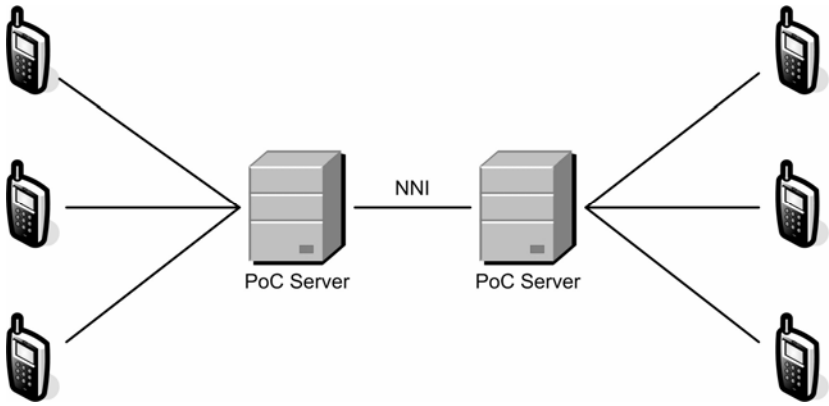
Early media servis smanjuje vremensko kašnjenje u prenosu, ali takođe može uzrokovati određene probleme. Ukoliko pozvani korisnik nije dostupan (npr., korisnik je izgubio radio-pokrivanje što mreža još uvek nije detektovala), PoC će morati da prekine pozivajućeg korisnika koji je već otpočeo učešće u sesiji. U tom slučaju PoC mora da informiše inicijatora sesije da paketi govora ne mogu biti isporučeni, na način prikazan na slici 4.18.



Slika 4.18: Problemi detektovani u slučaju *early media* servisa

4.3.3. *INTEROPERATOR SESSIONS* – SESIJE IZMEĐU OPERATORA

PoC server pretpostavlja da svi korisnici koriste isti PoC server. Ipak, ne mora uvek da bude takav slučaj (npr., kada žele da komuniciraju korisnici koji pripadaju mrežama različitih operatora). Neki od operatora insistiraju da PoC sesije u kojima učestvuje bar jedan njihov korisnik, moraju da uključe PoC server njihove mreže, jer im to olakšava mnoge operacije (npr., proces tarifiranja). Rezultujuća arhitektura koja može da udovolji ovakvim zahtevima prikazana je na slici 4.19.



Slika 4.19: *Multi-operator* arhitektura

PoC serveri iz različitih domena komuniciraju korišćenjem NNI (*Network-to-Network*) interfejsa. OMA radi na razvoju navedenog interfejsa, ali se očekuje da će se i po njegovoj konačnoj definiciji OMA susresti sa brojnim problemima vezanim za kontrolu dodele prava govora u distribuiranom okruženju.

LITERATURA

[1] Gonzalo Camarillo, Miguel A.Garcia-Martir - *"The 3G IP Multimedia Subsystem (IMS)",* (*West Sussex, England John Wiley & Sons Ltd*, Oktobar 2004).

[2] H. Schulzrinne - „RPID - *Rich Presence Extensions to the Presence Information Data Format* (PIDF)". *Internet Draft draft-ietf-simple-rpid-03, Internet Engineering Task Force*, Mart 2004. Rad je u toku.

[3] J. Rosenberg - „*A Watcher Information Event Template-Package for the Session Initiation Protocol* (SIP)". *Internet Draft draft-ietf-simple-winfo-package-05, Internet Engineering Task Force*, Januar 2003. Rad je u toku.

[4] J. Rosenberg - „*A Presence Event Package for the Session Initiation Protocol* (SIP)". *Internet Draft draft-ietf-simple-presence-10*, *Internet Engineering Task Force*, Januar 2003. Rad je u toku.

[5] J. Rosenberg - "*Interactive Connectivity Establishment* (ICE): *A Methodology for Network Address Translator* (NAT) *Traversal for Multimedia Session Establishment Protocols*" *Internet Draft draft-ietf-mmusic-ice-01, Internet Engineering Task Force*, Februar 2004. Rad je u toku.

[6] M.Lonnfors, K.Kiss - „*User agent capability presence status extension*". *Internet Draft draft-ietf-simple-winfo-prescaps-00, Internet Engineering Task Force*, Februar 2004. Rad je u toku.

[7] M.Lonnfors, K.Kiss - „*An Event State Publication Extension for the Session Initiation Protocol* (SIP)". *Internet Draft draft-ietf-sip-publish-03, Internet Engineering Task Force*, Februar 2004. Rad je u toku.

[8] V. Hilt, J. Rosenberg - "*Supporting Intermediary Session Policies in* SIP". *Internet Draft draft-hilt-sipping-session-spec-policy-00, Internet Engineering Task Force*, Oktobar 2003. Rad je u toku.

SPISAK SKRAĆENICA

3GPP	*Third Generation Partnership Project*
3GPP2	*Third Generation Partnership Project* 2
AAA	*Authentication, Authorization and Accounting*
ACA	*Accounting-Answer*
ACR	*Accounting-Request*
ADPCM	*Adaptive Differential Pulse Code Modulation*
ADSL	*Asymmetric Digital Subscriber Line*
AH	*Authentication Header*
AMR	*Adaptive Multi Rate*
AMR-WB	AMR *Wide Band*
ANSI	*American National Standards Institute*
API	*Application Programming Interface*
APN	*Access Point Name*
ARIB	*Association of Radio Industries and Business*
AS	*Application Server*
ATIS	*Alliance for Telecommunications Industry Solutions*
AVC	*Advanced Video Coding*
AVP	*Attributs Value Pair*
B2BUA	*Back-toBack User Agent*
BCP	*Best Current Practise*
BGCF	*Breakeout Gateway Control Function*
BICC	*Bearer Independent Call Control*
BOF	*Birds of a Feather*
BS	*Billing System*
CAMEL	*Customized Applications for Mobile Network Enhanced Logic*
CAP	CAMEL *Application Part*
CCF	*Charging Collection Function*
CCID	*Congestion Control Identifier*
CCSA	*China Communications Standards Association*
CDMA	*Code Division Multiple Access*
CDR	*Charging Data Record*
CGF	*Charging Gateway Function*
CGI	*Common Gateway Interface*
CK	*Ciphering Key*
COPS	*Common Open Policy Service*
CS	*Circuit-Switched*
CSCF	*Call/Session Control Function*
CSE	CAMEL *Service Environment*
DCCP	*Datagram Congestion Control Protocol*
DHCPv6	*Dynamic Host Configuration Protocol for* IPv6

DNS	*Domain Name Server*
DOI	*Domain of Interpretation*
DoS	*Denial of Service*
DSCP	*Differentiated Services CodePoint*
DSL	*Digital Subscribe Line*
ECF	*Event Charging Function*
ECUR	*Event Charging with Unit Reservation*
EDGE	*Enhanced Data rates for GSM Evolution*
ESP	*Encapsulating Security Payload*
ETSI	*European Telecommunication Standard Institute*
FMC	*Fixed/Mobile Convergence*
FQDN	*Fully Qualified Domain Name*
FTP	*File Transfer Protocol*
GERAN	*GSM EDGE Radio Access Network*
GGSN	*Gateway GPRS Suport Node*
GPRS	*General packet radio service*
GSM	*Global System for Mobile communications*
GSM-EFR	*GSM Enhanced Full Rate*
GSM-FR	GSM *Full Rate*
GSM-HR	GSM *Half Rate*
gsmSCF	*GSM Service Control Function*
HLR	*Home Location Register*
HSS	*Home Subscriber Servers*
HTTP	*Hypertext Transfer Protocol*
IAB	*Internet Architecture Board*
ICE	*Interactive Connectivity Establishment*
ICID	IMS *Charging Identity*
I-CSCF	*Interrogating*-CSCF
IEC	*Immediate Event Charging*
IESG	*Internet Engineering Steering Group*
IETF	*Internet Engineering Task Force*
IK	*Integrity Key*
IKE	*Integrity Key Exchange*
IM-MGW	IP *Multimedia Media Gateway Function*
IMS	*IP Multimedia Subsystem*
IMSI	*International Mobile Subscriber Identifier*
IM-SSF	IP *Multimedia Service Switching Function*
IMT-2000	*International Mobile Telecommunications-2000*
IOI	*Inter Operator Identifier*
IP-CAN	IP *Connectivity Access Network*
ISAKMP	*Internet Association and Key Management Protocol*
ISC	IMS *Service Control Interface*

ISDN	*Integrated Services Digital Network*
ISIM	IP *multimedia Services Identity Module*
ISUP	ISDN *User Part*
ITU	*International Telecommunication Union*
LIA	*Location-Information-Answer*
LIR	*Location-Information-Request*
LPC	*Linear Prediction Coding*
LS	*Lip Synchronization*
LTP	*Long-Term Predictor*
MAA	*Multimedia-Auth-Answer*
MAP	*Mobile Aplication Part*
MAR	*Multimedia-Auth-Request*
MEGACO	*MEdia GAteway COntrol*
MGCF	*Media Gateway Controller Function*
MGW	*Media Gateway*
MIME	*Multipurpose Internet Mail Extension*
MMS	*Multimedia Message Service*
MPEG	*Motion Picture Experts Group*
MRF	*Media Resource Function*
MRFC	*Media Resource Function Controller*
MRFP	*Media Resource Function Processor*
MSC	*Mobile Switching Center*
MSISDN	*Mobile Subscriber ISDN Number*
MSRP	*Message Session Relay Protocol*
MTU	*Message Transmission Unit*
NAI	*Network Access Identifier*
NAS	*Network Access Server*
NAT	*Network Address Translator*
NNI	*Network-to-Network Interface*
OMA	*Open Mobile Aliance*
OSA-SCS	*Open Service Access – Service Capability Server*
PA	*Presence Agent*
PCG	*Project Coordination Group*
PCM	*Pulse Code Modulation*
P-CSCF	*Proxy*-CSCF
PDA	*Personal Digital Assistant*
PDF	*Policy Decision Function*
PDP	*Policy Decision Point*
PEP	*Policy Enforcement Point*
PHB	*Per-Hop Behavior*
PIB	*Policy Information Bases*
PIDF	*Presence Information Data Format*

PLMN	*Public Land Mobile Network*
PoC	*Push-to-Talk over Cellular*
POTS	*Plain Old Telephone Service*
PRC	*Provisioning Classes*
PRI	*Provisioning Instances*
PSS	*Packet-switched Streaming Service*
PS	*Packet Switching*
PS	*Presence Server*
PSI	*Public Service Identities*
PSTN	*Public Switched Telephone Network*
PUA	*Presence User Agent*
QoS	*Quality of Service*
RAN	*Radio Access Network*
RFC	*Request for Comments*
RLS	*Resource List Server*
RPE	*Regular Pulse Excitation*
RPID	*Rich Presence Information Data Format*
RSVP	*Resource ReSerVation Protocol*
RTCP	RTP *Control Protocol*
RTP	*Real-time Transport Protokol*
SBLP	*Service-Based Local Privacy*
SC	*Steering Committee*
SCF	*Session Charging Function*
S-CSCF	*Serving*-CSCF
SCTP	*Stream Control Transmission Protocol*
SDO	*Standards Development Organization*
SDP	*Session Description Protocol*
SEG	*security gateway*
SGSN	*Serving GPRS Suport Node*
SGW	*Signaling Gateway*
SIM	*Subscriber Identity Module*
SIP	*Session Initiation Protocol*
SIP URI	SIP *Uniform Resource Identifier*
SLF	*Subscriber Location Function*
SMS	*Short Message Service*
SMTP	*Simple Mail Transfer Protocol*
SPI	*Security Parameter Index*
SRF	*Single Reservation Flow*
SRTP	*Secure RTP*
SSF	*Service Switching Function*
SVCD	*Super Video* CD
TCP	*Transmission Control Protocol*

TDM	*Time Division Multiplexing*
TEL URL	*Telephone Uniform Resource Locator*
THIG	*Topology Hiding Inter-network Gateway*
TIA	*Telecommunications Industry Association*
TISPAN	*Telecoms & Internet converged Services & Protocols for Advanced Networks*
TLS	*Transport Layer Security*
TR	*Technical Reports*
TRFC	*TCP-Friendly Rate Control*
TS	*Technical Specifications*
TSG	*Tehnical Specification Group*
TTA	*Telecommunications Technology Association*
TTC	*Telecommunications Technology Committee*
TUP	*Telephony User Part*
TURN	*Traversing Using Relay NAT*
UA	*User Agent*
UAA	*User Authentication-Answer*
UAC	*User Agent Client*
UAR	*User Authentication-Request*
UAS	*User Agent Server*
UDP	*User Datagram Protocol*
UE	*User Equipment*
UICC	*Universal Integrated Circuit Card*
UMTS	*Universal Mobile Telecommunication*
UNI	*User-to-Network Interface*
USIM	*Universal Subscriber Identity Module*
UTRAN	*UMTS Terrestrial Radio Access Network*
VCD	*Video* CD
VoIP	*Voice over* IP
WCDMA	*Wideband Code Division Multiple Access*
WiMAX	*Worldwide Interoperability for Microwave Access*
WLAN	*Wireless Local Area Network*
XCAP	XML *Configuration Access Protocol*
XML	*Extensible Markup Language*

INDEX

L

M

N

O

P

Q

R

S

T

U

V

W

X