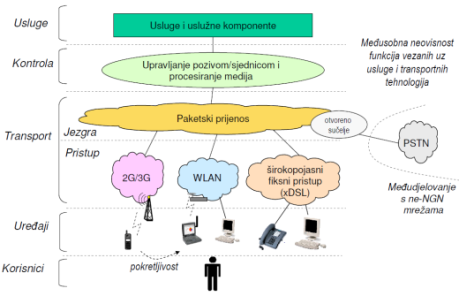
**Konvergencija u sljedećoj generaciji mreže**: potreba za novim uslugama koristeći širokopojasni pristup (povećanje prihoda operatora); pristup uslugama u svakom trenutku (pokretljivost korisnika); povezivanje različitih vrsta usluga; pojednostavljenje mrežne arhitekture

**3 gledišta konvergencije**: **konvergencije usluga** (npr. triple play, jedinstven broj, jedinstven spremnik); **konvergencije korisničke opreme** (npr. WLAN <-> 2G/3G); **konvergencije mreže** (horizontalna arhitektura, *all IP* informacije)

**NGN**: slojevita arhitektura (pristupna mreža, prijenos i komutacija, upravljanje, usluge); slojevi međusobno neovisni (neovisnost upravljanja i prijenosa; neovisnost usluga i prijenosa: dobro definirana sučelja između upravljanja i usluga); paketski prijenos; širokopojasni prisup, kvaliteta s kraja na kraj; uniformne karakteristike iste usluge; interoperabilnost i suživot s postojećim mrežama

****

**Uslužni stratum**: dio NGN koji omogućuje prijenos podataka na razini usluge, te kontrole uslužnih resursa (UA, UI, *Service Admission Control*); **sastoji od** (IMS s podrškom za xDSL *AN* i PSTN/ISDN simulaciju; PSTN/ISDN emulacija zamjenjuje TDM opremu i podržava postojeće terminale)

**Upravljačke funkcije**: koriste se prije izvođenja same usluge, a vezane uz korisnike (naplata);

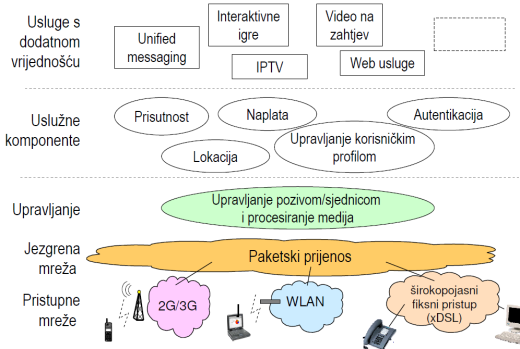
**Transportni stratum**: omogućuje prijenost podataka i kontrolu transportnih mrežnih resursa (*Network Admission Control, Dynamic Connectiviti Provision*); **sastoji od** (*Network Attachment Subsystem* – dinamičko pridjeljivanje IP adresa; autentifikacija i autorizacija korisnika; upravljanje pokretljivošću; konfiguracija pristupne mreže na temelju korisničkih profila)(*Resource Admission Control Functions* – autorizacija QoS zahtjeva i definiranje zahtjeva koje mrežni elementi moraju zadovoljiti; upravljanje sjednicom)

**Vrste usluga**:

**Usluge za masovno tržište**: standardizirane; osigurana interoperabilnost u različitim mrežama; skalabilnost, dostupnost, istovjetnost

**Posebne usluge za definiranje grupe korisnika**: specifične usluge prema trenutnim zahtjevima i potrebama korisnika; fleksibilnost u oblikovanju usluga, brzo kreiranje i dostupnost usluga; integracija

**Uslužna arhitektura NGN**



**Usluge za NGN**: usluge za komunikaciju; temeljene na digitalnom sadržaju; kombinirane usluge...

**Višemedijska tel. usluga**: zamjena za postojeće pokretne i fiksne; podrška za višemedijsku sesiju

**Višemedijska konferencija**: razmjena višemedijskog sadržaja; sadržaj prilagođen karakteristikama uređaja; signalizacija i rukovanje medijima

***Unified messaging***: više različitih komunikacijskih medija u jedinstvenu uslugu (e-mail, sms, mms, IM); usluga se prilagođava karakterisikama uređaja i željama korisnika; zajednički pretinac; usluga o prisutnosti

**IPTV**: paketski prijenos strujećeg audia i videa; širokopojasne tehnologije xDSL; QoS za multicast i unicast radi QoE

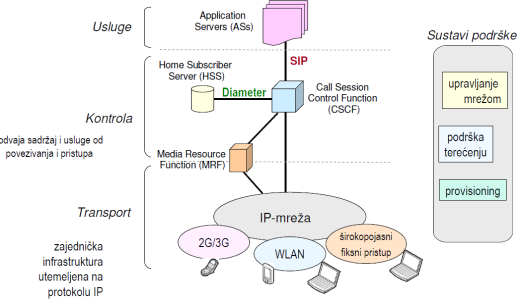
**VOD**: *Content Distribution Network*; upravljanje mrežnim opterećenjem

**Kombinirane usluge**: kombinacija kanalne domene za govor i paketsku domenu za druge sadržaje

**IMS**: standardizirana NGN-arhitektura; 3GPP; usmjerena ka višemedijskim uslugama; neovisnost o pristupnoj mreži; konvergencija mreže prema *all-IP* arhitekturi (fiksno i pokretno; komutacija kanala i komutacija paketa); obuhvaća sve elemente jezgrene mreže za pružanje višemedijskih usluga

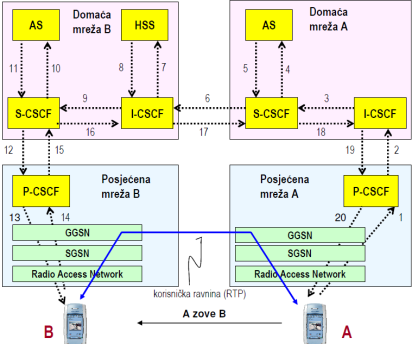
**Glavne značajke**: osnovni mrežni protokol IP; signalizacijski protokol SIP; AAA protokol *Diameter*; podrška za pokretljivost svega i svačega; podrška za QoS s kraja na kraj

**Tehnički razlozi**: isporuka raznih usluga; podrška za kvalitetu usluge; međudjelovanje s paketskim i kanalnim mrežama; prelaženje; upravljanje signalima; standardizirane uslužne komponente; podrška za razne AN



**Preduvijeti korištenja IMS usluga**:**1.** uspostava ugovora s IMS-operatorom; **2.** IP pristup; **3.** otkrivanje adrese P-CSCF čvora; **4.** registracija na IMS putem SIP-a

**Poziv s IMS-uslugom**



**QoS**: sveukupni učinak performansi usluge koji određuje stupanj zadovoljstva korisnika

**Mreže s komutacijom kanala**: relativno ograničen prostor za varijaciju kvalitete usluga; mrežni terminal, prijenosna mreža; **zaključci** – poboljšanje usluga (bolje kodiranje informacije; optimizacija prijenosnog puta); sama tehnologija vrlo robusna

**Delay**: ključni faktor QoS-a u mrežama s komutacijom signala; kašnjenje na mrežnim poveznicama (određeno karakteristikama prijenosnog puta)

**Mreže s komutacijom paketa**: IP, problemi (*packet loss, queuing delay*);

**Mjere za QoS**: *available capacity; delay; delay jitter; packet loss rate*

**UMTS QoS klase**: *conversational* (<80ms); *streaming* (<250ms); *interactive* (par sec); *background* (bez ograničenja)

**QoE**

**Mjerenje QoE**: korisničkim testovima (1-5; MOS); instrumentalno (algoritmi simuliraju korisničke reakcije na različit QoS);; mjerenje u skladu s visokim znanstvenim standardima

**Svojstva opreme za testiranje mobilnih aplikacija**: prenosivost; raznovrsnost i točnost dobivenih informacija; efikasnost rukovanja; mogućnost zaprimanja informacija neovisno o kontekstu; prirodna interakcija korisnika s aplikacijom; mogućnost testiranja svih relevantnih aplikacija za mobilne uređaje

**Budućnost QoSa**: pragmatični razvoj mreže i usluga; omogućavanje velikih brzina i volumena u pristupnoj mreži

**Sigurnosni zahtjevi**

**Sigurnost**: *security*; sposobnost mreža, sustava, usluga i aplikacija da se suprotstave neočekivanim slučajnim događajima i zlonamjernim aktivnostima koje mogu narušiti i kompromitirati raspoloživost, vjerodostojnost, cjelovitost i povjerljivost informacije i komunikacije

**Prijetnja u mrežnom okružju**: *network threat*; okolnost, stanje ili događaj koji može naškoditi osoblju ili mrežnim računalnim resursima u obliku uništavanja, razotkrivanja ili modifikacije podataka, uskrate usluge, prijevare i zlouporabe

**Autentičnost**: *authenticity*; utvrđivanje i potvrda identiteta korisnika

**Cjelovitost**: *integrity*; informacija odaslana, primljena ili pohranjena u izvornom i nepromijenjenom obliku; modifikacija dopuštena ovlaštenim korisnicima

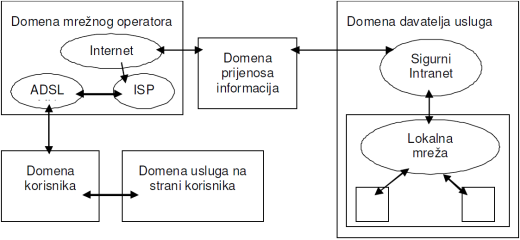
**Povjerljivost**: confidentiality; zaštita komunikacije ili pohranjene informacije od neovlaštenog presretanja; preduvjet za privatnost

**Neporecivost**: *non-repudiation*; sudionici ne mogu poreći aktivnost u kojoj su sudjelovali

**Kontrola pristupa**: *access control*; ograničavanje pristupa infromacijama i provođenja aktivnosti; dodjela ovlasti korisnicima

**Raspoloživost**: *availability*; informacije moraju biti raspoložive, a sustavi u operativnom stanju usprkos mogućim neočekivanim događajima

**Sigurnosni model**

****

**Domena mrežnog operatora**: nesmetano funkcioniranje mreže (raspoloživost svih mrežnih komponenti i sustava; cjelovitost svih mrežnih komponenti i sustava)

**Domena korisnika**: autentičnost – raspoloživost; ovise o (sigurnosti računala i korisničke mrežne opreme; sigurnost korištenih usluga; ponašanje korisnika)

**Sigurnost na nivou mrežne komunikacije**: sigurnost se može ostvariti postupcima uvedenim na razini sloja, pri čemu se sigurnosne usluge u n-tom sloju pružaju svim višim slojevima

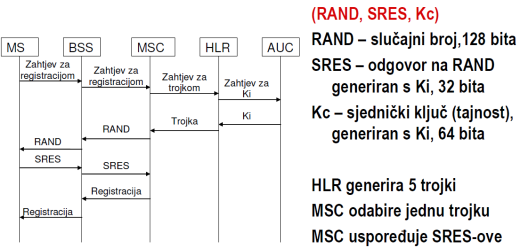
**Sigurnost na nivou aplikacije**: sigurnost se može ostvariti postupcima uvedenim za pojedinu uslugu ili aplikaciju u najvišem sloju, sa ili bez sigurnosnih usluga nižih slojeva

**Ipsec**:mrežni sloj; siguran prijenos cijelog paketa ili dijela paketa putem dvosmjerne sigurnosne asocijacije te simetričnih algoritama za zaključavanje;različiti modaliteti prijenosa (AH i ESP; tunelski način i transportni način); **nedostaci** – složenost Ipsec protokola; potreba za podrškom na razini mrežnog stoga u OS

**SSL/TLS**: transportni sloj; sigurnosni mehanizmi pridružuju se transportnom protokolu kojim je moguće ostvariti pouzdan prijenos TCP; dvoslojni protokol koji se postavlja iznad protokola TCP da bi pružio sigurnosne usluge aplikacijskom protokolu

**Aplikacijski sloj**: u potpunosti različita rješenja za različite aplikacije; **prednosti** – sigurnost ne mora ovisiti o nižim slojevima; jednostavno korištenje UDPa za komunikaciju u realnom vremenu; **nedostaci**: veća složenost izrade aplikacije; povećana vjerojatnost ugrožavanja sigurnosti pogreškama u programiranju

**Autentičnost pretplatnika**: **prijetnja** – poznavanje IMSI omogućuje krivo predstavljanje i neovlašten pristup mreži, IMSI jednoznačno povezan sa MSISDN; **zaštita** – provjera autentičnosti SIM-a prigodom registracije



**Autentičnost opreme**: **prijetnja** – gubitak ili krađa; **zaštita** – prijava gubitka ili krađe opreme mrežnom operatoru, zapisuje se u EIR (onemogućena provjera autentičnosti) i HLR (zabranjuje se pristup mreži)

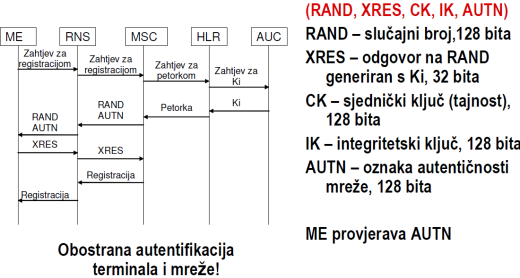
**Anonimnost pretplatnika**: **prijetnja** – dohvaćanjem IMSI na zračnom sučelju može se ustanovit pretplatnikova lokacija i pratiti kretanje; **zaštita** – privremeni identitet TMSI (lokalnog značenja); nakon provjere autentičnosti -> TMSI; VLR i MSC provode preslikavanje IMSI-TMSI

**Tajnost komunikacije**: **prijetnja** – prisluškivanje na zračnom sučelju; **zaštita** – šifriranje podataka; A5

**Slabosti sigurnosti GSMa**: sigurnosne mjere usredotočene na zračno sučelje; veza BTS-BSC potencijalno izložena napadima; signalizacijski sustav, SS7, bez kriptografske zaštite; ne štiti se integritet podataka;pristup algoritmima se kontrolira *security through obscurity*

**Osnovna svojstva sigurnosti UMTSa**: Ki se ne razmjenjuje kroz mrežu, mreža provjerava autentičnost USIMa; šifriranje signalizacijske informacije koja omogućuje otkrivanje identiteta pretplatnika; provjera autentičnosti mreže; tajnost: algoritam KASUMI; integritet signalizacijske informacije: ključ IK

**Autentičnost pretplatnika i mreže u UMTSu**



**Sigurnosne implikacije uvođenja IMSa**: nasljeđuje gotovo sve slabosti IP tehnologije; donosi nove probleme (SPIT, SPIM,SSO);

**Botnet**: mreže računala koje se posljedicom infekcije štetnim kodom nalaze pod kontrolom treće strane; napadač ima mogućnost kontrolirati mrežni složaj računala te koristiti za napade; krađa podataka i identiteta korisnika

**SMS**: duljina poruke 140B; 160 ili 70 znakova (unicode); SS7; TCAP; MAP; spec: Point-to-point, Cell Broadcast

**SME**: element koji može slati i primati kratke poruke; smješten MS, fiksnoj mreži ili uslužnom centru

**SMSC**: odgovoran za isporuku poruka od izvorišnog SME do odredišnog SME; *store-and-forward*

**Osnovne funkcije SMSa**: *submit*, *delivery*, izvještaj o poruci ako je zatražen, period valjanosti poruke

**EMS**: nadogradnja SMSa na aplikacijskom sloju; koncept informacijskih elemenata; promjene na SME

**Osnovni EMS**: formatirani tekst; monikromatske slike, animacije i monofone melodije

**Prošireni EMS**: slike i animacije s 4 nivoa sive boje; slilke i animacije u boji; vCard; vCalendar; polifone melodije; formatirani tekst u boji; URI; capability profile

**Nedostaci**: veliki broj SMS poruka čini EMS poruku (naplata po SMS poruci); prijenos signalizacijskim kanalom; razvoj MMSa zaustavlja EMS

**MMS**: multimedijske poruke; interoperabilnost s e-mailom; 2.5G i 3G; slanje poruke grupi primatelja; perzistentna komunikacija; obavjest o poruci; prilagodba sadržaja poruke