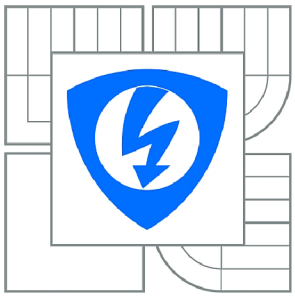
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

AUTENTIZÁCIA, AUTORIZÁCIA A ÚČTOVANIE PAKETOVÝCH PRENOSOV V MOBILNÝCH SIEŤACH

AUTHENTICATION, AUTHORIZATION AND ACCOUNTING OF PACKET ORIENTED TRANSMISSION IN MOBILE NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

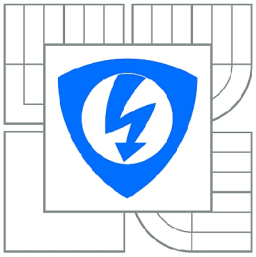
AUTOR PRÁCE — PETER TKÁČ

AUTHOR

VEDOUCÍ PRÁCE — Ing. RADKO KRKOŠ

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Peter Tkáč ***ID:*** 154895
Ročník: 3 ***Akademický rok:*** 2014/2015

NÁZEV TÉMATU:

Autentizácia, autorizácia a účtovanie paketových prenosov v mobilných sieťach

POKYNY PRO VYPRACOVÁNÍ:

Popíšte problematiku autentizácie, autorizácie a účtovania v mobilných sieťach so zameraním na paketové prenosy a paketovo realizované dátové, hlasové a multimediálne služby v mobilných sieťach štvrtej generácie. Detailne analyzujte architektúru mobilnej siete z pohľadu autentizácie, autorizácie a účtovania, popíšte zainteresované prvky, rozhrania a potrebné procedúry. Navrhnite plán implementácie uvedenej funkcionality do experimentálnej mobilnej siete UTKO FEKT VUT, kde výstupom bude vysokoúrovňový popis a tiež prislúchajúce podrobne komentované konfiguračné súbory pre jednotlivé zariadenia.

DOPORUČENÁ LITERATURA:

[1] 3GPP TS 23.203. Policy and charging control architecture. 13.1.0. 3GPP, 2014-09. Dostupné z: http://www.3gpp.org/ftp/Specs/archive/23_series/23.203/23203-d10.zip
[2] 3GPP TS 32.251. Telecommunication management; Charging management; Packet Switched (PS) domain charging. 12.7.0. 3GPP, 2014-09. Dostupné z: http://www.3gpp.org/ftp/Specs/archive/32_series/32.251/32251-c70.zip
[3] HUAWEI. Product Technical Specification: Experimentální LTE-EPC-IMS-WiFi síť UTKO FEKT VUT v Brně. 2012-2014.

Termín zadání: 9.2.2015 ***Termín odevzdání:*** 2.6.2015

Vedoucí práce: Ing. Radko Krkoš
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

ABSTRAKT

Práca sa zaoberá princípmi autentizácie, autorizácie a účtovania v paketových mobilných sieťach. V práci je popísaný vývoj mobilných sietí štvrtej generácie, architektúra týchto sietí a funkcie jednotlivých častí siete. Ďalej sa práca venuje opisu funkcií riadenia zásad a účtovania. Detailne sú vysvetlené postupy, ktoré zaisťujú bezpečnosť používateľa v sieti, procesy pri jeho autentizácii a autorizácii. Práca tiež popisuje postupy pri účtovaní v mobilnej sieti a všetky možností účtovania v systéme experimentálnej mobilnej siete.

KĽÚČOVÉ SLOVÁ

LTE, mobilná sieť, autentizácia, autorizácia, účtovanie

ABSTRACT

Concern of this thesis is priciples of authentication, authorisation and charging in packet oriented mobile networks. In thesis is description of evolution of fourth generation mobile networks, architecture of these networks and function of each part in network. Next part of the thesis decribes functions of policy and charging control. Procedures, which provide security of user in network, authentication and authorization of user, are explained in detail. Thesis describes procedures of charging in mobile networks and all options of charging in system of experimental mobile network.

KEYWORDS

LTE, mobile network, authentication, authorization, charging

TKÁČ, Peter *Autentizácia, autorizácia a účtovanie paketových prenosov v mobilných sieťach*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 54 s. Vedúci práce bol Ing. Radko Krkoš.

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Autentizácia, autorizácia a účtovanie paketových prenosov v mobilných sieťach“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som sa poďakoval vedúcemu bakalárskej práce pánovi Ing. Radkovi Krkošovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popísaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Cieľom tejto práce je popísať problematiku autentizácie, autorizácie a účtovania v mobilných sieťach. Práca sa zameriava na siete štvrtej generácie. V práci je popísaná architektúra týchto sietí a procesy, ktoré sú potrebné na realizáciu dátových, hlasových a multimediálnych služieb v mobilných sieťach.

V prvej časti práce je popísaný vývoj mobilných sietí štvrtej generácie. Je tu vysvetlené rozdelenie na prístupovú sieť a transportnú sieť. Vysvetľuje sa princíp fungovania prístupovej siete a jej výhody. Ďalej sa popisuje vývoj systému, ktorý umožňuje vyššiu kapacitu a vyššie rýchlosti prenosov. Nachádza sa tu zjednodušený popis princípov, ktoré umožňujú vyššiu kapacitu a rýchlosť siete.

V druhej kapitole práce je podrobne popísaná architektúra prístupovej siete. Vysvetľuje sa rozdelenie siete a sú tu podrobne popísané jednotlivé prvky v sieti. Vysvetľuje sa ich význam a funkcia. V ďalšej časti sa popisuje architektúra politiky kontroly a účtovania. Táto časť obsahuje opis jednotlivých prvkov a rozhraní medzi nimi.

Tretia časť práce opisuje jednotlivé funkcie riadenia zásad a účtovania. Vysvetľujú sa postupy pri vytváraní väzieb, vykonávaní niektorých udalostí, autorizácia pravidiel riadenia zásad a účtovania. Sú tu popísané princípy zaisťovania kvality služieb a akcie pri riešení konfliktov, ktoré vznikajú pri zaisťovaní kvality služieb.

Štvrtá kapitola rieši bezpečnosť používateľa pri pripájaní sa k prístupovej sieti. Opisujú sa funkcie a postupy pri zaisťovaní bezpečnosti používateľa. Je tu vysvetlený proces autentizácie a autorizácie používateľa pri získavaní prístupu k sieti a k multimediálnym službám, ktoré sieť poskytuje.

Posledná časť práce vysvetľuje procesy pri účtovaní prenosov v systéme mobilnej siete od spoločnosti HUAWEI. Nachádza sa tu detailný opis jednotlivých procesov a možné spôsoby účtovania služieb v tomto systéme.

1 VÝVOJ LTE

1.1 LTE

Sieť LTE (*The Long Term Evolution of UMTS*) alebo aj E-UTRAN (*Envolved Universal Terrestrial Radio Access Network*), predstavená projektom 3GPP (*The 3rd Generation Partnership Project*) pod vydaním *Release 8*, je prístupovou časťou EPS (*Evolved Packet System*). LTE bolo posledným krokom vo vývoji systému UMTS (*Universal Mobile Terrestrial System*). Hlavnými vlastnosťami novo predstavenej prístupovej siete boli vysoká spektrálna účinnosť, vysoké prenosové rýchlosti dát a krátka doba trvania obojsmerných prenosov [12].

Systém EPS je založený na prenose paketov. Dátové služby a prenosy v reálnom čase pracujú na protokole IP (*Internet Protocol*). Nové riešenie prístupu k sieti je založené na OFDMA (*Orthogonal Frequency Division Multiple Access*) a v kombinácii s moduláciou vyššieho rádu a priestorovým multiplexom môžu byť dosiahnuté veľké prenosové pásma. Najvyššie teoretické prenosové rýchlosti môžu dosiahnuť až 75 Mb/s pre uplink a 300 Mb/s pre downlink.

Prístupová sieť LTE je sieť základňových staníc eNodeB (*Evolved NodeB*), ktoré majú vlastné riadenie. Nenachádza sa v nej centrálny prvok, ktorý by riadil základňové stanice. Jednotlivé eNodeB sú medzi sebou prepojené rozhraniami X2 a voči nosnej sieti EPS pomocou rozhraní S1. Podstatou rozdelenia riadenia medzi základňové stanice eNodeB je zvýšenie rýchlosti vytvárania spojení s koncovými zariadeniami a zníženie času potrebného na vykonanie handoveru [1] medzi jednotlivými stanicami, napríklad kvôli presunu účastníka z oblasti pokrytej určitou stanicou. K zvýšeniu rýchlosti komunikácie napomáha aj rozdelenie riadenia medzi základňové stanice na úrovni spojovej vrstvy OSI modelu (*Open Systems Interconnection*), čo umožňuje vykonávanie procesov na tejto vrstve na jednotlivých staniciach a nie centrálne.

[1] tento termín označuje proces výmeny riadenia relácie medzi základňovými stanicami

1.2 LTE-Advanced

LTE-Advanced je ďalším krokom vo vývoji komunikačnej technológie LTE. Projekt 3GPP prišiel s riešením, ktoré obsiahli vo vydaní *Release 10.* LTE-Advanced zabezpečuje vyššie prenosové rýchlosti v cenovo efektívnej miere, kompletne spĺňajúc podmienky zadané organizáciou ITU (*International Telecommunication Union*) na systémy štvrtej generácie[13]. V systéme LTE-Advanced je možné dosiahnuť najvyššie prenosové rýchlosti až 500 Mb/s pre uplink a 1 Gb/s pre downlink pre statického účastníka.

Najpriamejšou cestou zvýšiť prenosovú kapacitu je pridanie šírky pásma. Kvôli zachovaniu spätnej kompatibility s Release 8 a Release 9 sa zvýšenie šírky pásma realizuje zlúčením nosných frekvencií R8/R9. Maximálne 5 nosných frekvencií smie byť agregovaných a maximálna možná šírka pásma je 100 MHz.

Najľahším spôsobom ako zariadiť agregáciu nosných frekvencií je použitie susedných frekvenčných kanálov pracujúcich v rovnakom frekvenčnom pásme. Toto však nie je vždy možné, kvôli alokáciám frekvencií. Je možné použiť aj nosné frekvencie, ktoré nie sú susediace vo frekvenčnom pásme, bude medzi nimi však frekvenčná medzera. Taktiež je možné na agregáciu použiť aj frekvencie z rôznych frekvenčných pásiem [13].

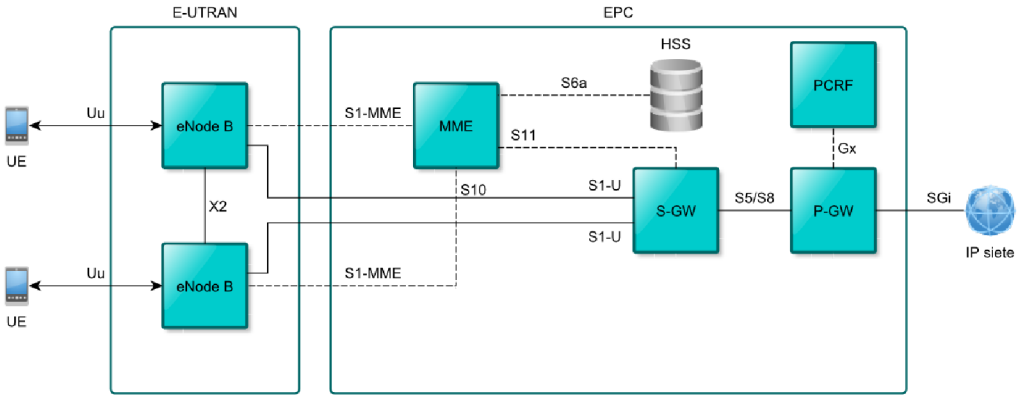
Zvyšovanie prenosovej rýchlosti pri prenose dvoch a viac dátových tokov zabezpečuje technika multiplexu MIMO (*Multiple In Multiple Out*). Tento typ multiplexu využíva vysielanie a príjem na dvoch alebo viacerých anténach, čo umožňuje využitie priestorového multiplexu. MIMO vylepšuje vlastnosti prenosového kanálu, zlepšuje odstup signálu od šumu SNR (*Signal to Noise Ratio*).

V LTE-Advanced je možné efektívne plánovať pokrytie sieťou využitím veľkých a malých buniek. Toto je zabezpečené pomocou prvkov RN (*Relay Nodes*). RN sú nízko-výkonové základňové stanice, ktoré zabezpečujú rozšírené pokrytie. Ich výhodou je možnosť pripojenia k vzdialeným oblastiam bez použitia káblov. Pripojenie k DeNodeB (*Donor eNodeB*) je riešené rádiovým rozhraním. Toto rozhranie môže pracovať na rovnakej alebo odlišnej frekvencii, ako rozhranie na ktorom prebieha komunikácia medzi používateľom a základňovou stanicou [13].

2 ARCHITEKTÚRA

2.1 Architektúra LTE

Systém LTE je čisto paketový systém, takže nevyužíva prenos na základe prepínania okruhov ako tomu bolo v minulosti. Systém pracuje na základe protokolu IP (*Internet Protocol*). Medzi výhody tohto systému patrí hlavne omnoho vyššia prenosová rýchlosť v sieti [12]. Architektúra tohoto systému je znázornená na obrázku 2.1.



Obr. 2.1: Architektúra systému LTE

Mobilná sieť LTE sa delí na dva základné bloky, a to:

- **E-UTRAN** - časť systému E-UTRAN sa nazýva aj prístupová časť siete. Zabezpečuje spojenie medzi koncovými zariadeniami v sieti, označovanými ako UE (*User Equipment*) a paketovou časťou siete EPC. V prístupovej časti siete sa nachádzajú základňové stanice eNodeB, ktoré plnia taktiež funkciu riadiacej jednotky. Zabezpečujú rádiové zdroje, pokrytie oblasti signálom a prideľujú rádiové prostriedky v sieti. Jedna eNodeB môže obsluhovať viacero UE, avšak jeden UE môže byť vždy pripojený iba k jednej eNodeB [9].
- **EPC (*Evolved Packet Core*)** - je časť systému, ktorá je nosnou časťou siete. EPC tvorí jadro siete a slúži na vysoko-rýchlostný prenos dát používateľov[9] [1]. Obsahuje tieto bloky:
  - **MME** (*Mobility Management Entity*) - prvok správy mobility je hlavným riadiacim prvkom v sieti. Jedno MME môže obsluhovať niekoľko eNodeB k nemu pripojených. Kontroluje prístup k sieti a vykonáva overenie totožnosti užívateľa. Pri autentizácii používateľa si vyžiada informácie od servera pre správu používateľov HSS (*Home Subscriber Server*) a porovná ich s informáciami od UE. Počas doby pripojenia určitého UE si uchováva

jeho používateľský profil získaný z HSS. Ak sa UE premiestni z oblasti správy daného MME a pripojí sa k inému, zašle sa kópia používateľského profilu novému prvku pre správu mobility MME a vlastná kópia sa zmaže.

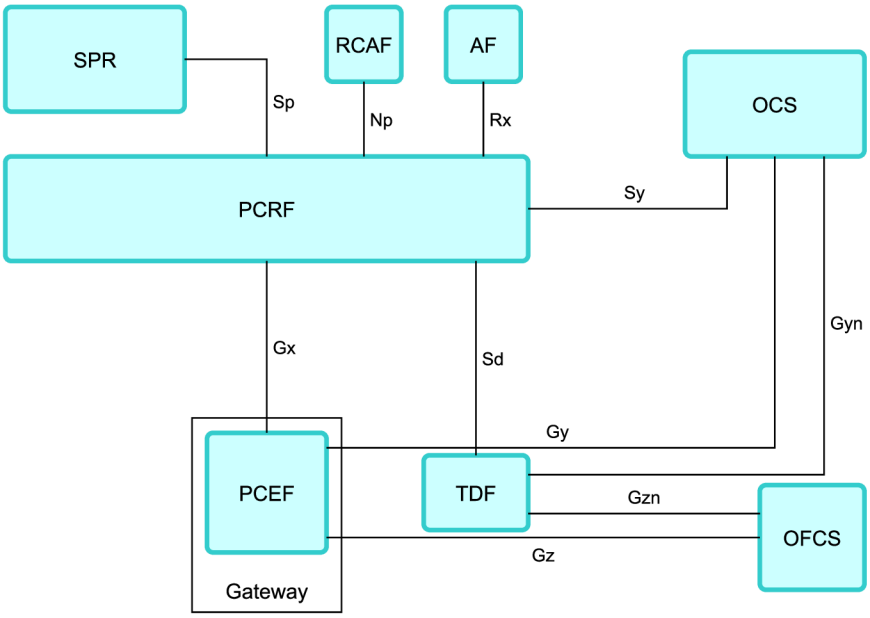
- **HSS** - je databáza informácii o všetkých účastníkoch v sieti. Obsahuje informácie o službách poskytovaných jednotlivým užívateľom. Databáza HSS je prepojená so všetkými MME v sieti. Každé MME dostáva od HSS kópie používateľských profilov všetkých UE obsluhovaných v sieti. Server pre správu používateľov obsahuje overovacie kľúče slúžiace na overenie totožnosti používateľa.
- **S-GW** (*Serving Gateway*) - primárnou funkciou oblusžnej brány je spravovanie dátových tokov medzi jednotlivými eNode B a paketovou bránou PDN-GW (*Packet Data Network Gateway*). Z funkčného hľadiska je to vstupný bod dátového toku do paketovej časti siete EPC.
- **PDN-GW** - je vlastne smerovač medzi paketovou časťou siete EPC a externými paketovými sieťami. Zabezpečuje prideľovanie IP adries, filtrovanie paketov.
- **PCRF** (*Policy and Charging Rules Function*) - prvok siete dozerajúci na vykonávanie riadenia zásad a kontoroly účtovania. Riadenie zásad a kontrola účtovania sa označuje skratkou PCC (*Policy and Charging Control*). Prvok riadenia zásad a kontroly účtovania PCRF sleduje jednotlivé dátové toky a vyhodnocuje, či poskytované služby zodpovedajú jednotlivým užívateľským profilom a im prideleným triedam QoS. Dohliada na vyúčtovanie poskytovaných služieb.

2.2 Architektúra PCC

Vlastnosti riadenia zásad a účtovania PCC zabezpečujú vykonávanie kontroly pravidiel operátora, účtovanie prenosov dát a dynamickú kontrolu nad garanciou kvality služieb QoS. Vykonáva sa kontrola vstupov do siete, využívajú sa rôzne modely účtovania závislé na viacerých faktoroch, medzi ktoré patrí napríklad objem prenesených dát, lokalita zariadenia, či typ poskytovanej služby [3]. Architektúra prvkov riadenia zásad a kontroly účtovania PCC je zobrazená na obrázku 2.2.

Kontrolu riadenia zásad a účtovania vykonávajú tieto prvky:

- **PCRF** - prvok riadenia zásad a kontroly účtovania zabezpečuje kontrolu vykonávania pravidiel a rozhodovanie o účtovaní na základe tokov dát;
- **PCEF** (*Policy and Charging Enforcement Function*) - prvok vykonávania riadenia zásad a kontroly účtovania je implementovaný v paketovej bráne PDN-GW, zabezpečuje detekciu tried QoS pre jednotlivé toky dát a ich meranie



Obr. 2.2: Architektúra PCC [3]

kvôli potrebnému účtovaniu a komunikuje s prvkom riadenia zásad a kontroly účtovania PCRF;

- **OCS** (*Online Charging System*) - systém online účtovania vykonáva spravovanie prostriedkov na účte podľa času, objemu prenosu a udalostí, ktoré si vyžadujú účtovanie v reálnom čase;
- **OFCS** (*Offline Charging System*) - systém offline účtovania zaznamenáva udalosti z PCEF a generuje účtovacie záznamy pre fakturačný systém;
- **AF** (*Application Function*) - sieťový element podporujúci aplikácie, ktoré vyžadujú dynamickú kontrolu riadenia zásad a účtovania. Vykonáva účtovanie poskytovaných služieb v reálnom čase. Prenáša do PCRF informácie o dynamických reláciách;
- **SPR** (*Subscription Profile Repository*) - register profilov používateľov obsahuje informácie o používateľoch, ktoré sú potrebné pre vykonávanie rozhodnutí prvkom PCRF o riadení zásad a kontrole účtovania. Obsahuje informácie o službách, ktoré má konkrétny používateľ aktivované, prioritu povolených služieb, informáciu o garantovanej šírke pásma, podmienky účtovania a kategóriu používateľa.
- **TDF** (*Traffic Detection Function*) - prvok rozpoznávania dát je prvok vykonávajúci detekciu aplikácii a podávanie informácii o aplikáciach a službách prvku riadenia zásad a kontroly účtovania PCRF. TDF má za úlohu informovať o spustení a ukončení aplikácií. PCRF môže vyžiadať od TDF monitorovanie

účtovania a využitia prostriedkov siete. Narozdiel od prvku PCEF, ktorý pracuje pomocou pravidiel PCC, využíva prvok TDF pravidlá ADC (*Application Detection and Control*) a komunikácia prebieha na rozhraní Sd;

- **RCAF** (*RAN* [1] *Congestion Awareness Function*) - je element, ktorý zasiela RAN User Plane Congestion Information (*RUCI*) cez rozhranie Np do prvku PCRF, aby ten mohol rozhodovať o riadení zásad. RUCI nesie informácie o úrovni zahltenia pripojenia používateľa.

Rozhrania používané v architektúre PCC [3]:

- **Rx** – toto rozhranie zabezpečuje prenos informácii o reláciách medzi AF a PCRF. Správa na tomto rozhraní obsahuje informáciu o IP adrese na identifikáciu dátového toku kvôli riadeniu zásad a potrebe účtovania. Ďalej obsahuje informáciu o potrebnej šírke pásma kvôli garantovaniu kvality služby;
- **Gx** – zabezpečuje PCRF dynamickú kontrolu nad riadením zásad a účtovaním. Toto rozhranie signalizuje rozhodnutia o riadení zásad a zabezpečuje tieto funkcie:
  - vytvorenie relácie medzi prvkami PCRF a PCEF;
  - žiadosť o rozhodnutie ohľadom riadenia zásad a účtovania;
  - poskytnutie rozhodnutia od PCRF;
  - ohlasovanie spustení a ukončení detekovaných aplikácií, prenos identifikátorov spustených aplikácií;
- **Sp** – umožňuje PCRF požiadať o informácie ohľadom pravidiel od SPR na základe užívateľovho ID alebo identifikátora siete. Rozhranie umožňuje zasielať notifikácie prvku PCRF, keď nastane zmena v popisných informáciach. Tieto notifikácie sa zasielajú len ak si to PCRF vyžiada;
- **Sd** – toto rozhranie využíva prvok TDF na komunikáciu s PCRF. Umožňuje využívať dynamické riadenie zásad a detekciu aplikácii;
- **Np** – umožňuje prenos RUCI informácii zasielaných prvkom RCAF o vybraných používateľoch;
- **Gy** – zabezpečuje online kontrolu kreditu pre účtovanie na základe poskytnutej služby a informácie zasiela prvku PCEF;
- **Gz** – umožňuje prenos informácií o offline účtovaní na základe poskytnutej služby;
- **Sy** – zabezpečuje prenos informácií o stave riadenia zásad pre konkrétneho používateľa;
- **Gyn** – umožňuje online kontrolu kreditu v prípade účtovania na základe ADC pravidiel;
- **Gzn** – prenos informácii pri offline účtovaní v prípade použitia ADC pravidiel.

[1] *Radio Access Network* – prístupová sieť využívajúca rádiové pripojenie používateľov

3 POPIS FUNKCIÍ PCC

Architektúra PCC pracuje na úrovni dátového toku služieb. Zabezpečuje funkcie riadenia zásad a kontroly účtovania pre jednotlivé dátové toky poskytovaných služieb.

3.1 Proces vytvárania väzieb

Mechanizmus vytvárania väzieb je proces, pri ktorom sa priraďuje konkrétny dátový tok služby k nosiču IP-CAN (*IP - Connectivity Access Network*) [1]. Proces vytvárania väzieb by mal vytvoriť väzbu medzi nosičom IP-CAN a reláciou dátového toku, ktorý vyžaduje dynamické riadenie zásad prvkom AF [3]. Proces vytvárania väzby vykonáva tieto tri kroky:

1. Vytvorenie relácie – znamená to spojenie informácií o dátovom toku, ktorý si vyžaduje dynamickú kontrolu riadenia zásad prvkom AF, a jednej IP-CAN relácie. Vytvorená väzba obsahuje IP adresu používateľa, identitu používateľa a informáciu o dátovej sieti, ku ktorej sa používateľ pripája.
2. Autorizácia pravidiel riadenia zásad a vytvorenie pravidiel pre triedy QoS – prvok PCRF vykoná autorizáciu pravidiel riadenia zásad a účtovania pre všetky dynamické pravidlá AF relácie. Dynamické pravidlá riadenia zásad môžu byť autorizované, aj keď nie sú kompletné na základe inštrukcií AF.
3. Vytvorenie väzby nosiča – je to asociácia pravidla riadenia zásad a pravidla triedy kvality služby k nosiču IP-CAN. Táto funkcia sa vykonáva v prvku PCEF.

3.2 Spravovanie kreditu

Spravovanie kreditu sa uplatňuje iba pri online účtovaní. Prvok vykonávania riadenia zásad a kontroly účtovania PCEF inicializuje jednu reláciu spravovania kreditu so systémom online účtovania OSC pre každú reláciu na nižšej vrstve IP-CAN. Pri TDF relácii sa inicializuje relácia spravovania kreditu prvkom TDF. Nezávislá kontrola kreditu pre individuálne služby či aplikácie môže byť dosiahnutá pridaním jedinečného kľúča účtovania v príslušnom pravidle riadenia zásad.

PCEF (prípadne TDF) si vyžiada hodnotu kreditu pre každý kľúč účtovania nachádzajúci sa v pravidle riadenia zásad a kontroly účtovania PCC (prípadne v ADC

[1] transportná sieť na nižšej úrovni, ktorá poskytuje konektivitu pomocou IP protokolu a umožňuje transparentné poskytovanie multimediálnych služieb bez bližšej znalosti danej siete

pravidle). Záleží od konfigurácie operátora, či si prvok PCEF (TDF) vyžiada hodnotu kreditu pri aktivácii pravidla riadenia zásad (ADC pravidla), alebo keď sa detekuje prvý paket konkrétnej relácie či aplikácie. OCS môže poskytnúť informáciu o hodnote kreditu, ale žiadosť o informáciu ohľadom stavu kreditu môže aj zamietnuť [3].

Funkciou prvku OSC je vytvárať zásobníky kreditu pre viacero účtovacích kľúčov. Je možné vytvoriť viacero zásobníkov kreditu pre jeden IP-CAN nosič, či jednu TDF reláciu. Úlohou OSC je kontrolovať rozhodnutia ohľadom týchto zásobníkov. OSC môže zaslať výzvu na vykonanie opakovanej autorizácie kreditu, a to zvlášť pre každý kľúč účtovania. Ak sa vyskytnú udalosti, ktoré nie je možné monitorovať prvkami PCEF či TDF, poskytnú sa informácie prvku PCRF. V prípade detekovania takejto udalosti, PCEF (TDF) vyžiada autorizáciu kreditu prvkom OSC. Prehľad týchto udalostí sa nachádza v tabuľke 3.1.

Tab. 3.1: Udalosti, ktoré môžu spustiť vykonanie autorizácie kreditu [3]

Udalosť	**Popis**	**Použité v**
Vypršanie platnosti autorizácie	OSC má obmedzenú platnosť kreditu, ktorý vyprší v stanovenom čase.	PCEF, TDF
Dlhá nečinnosť	Dátový tok služby identifikovaný pravidlom PCC alebo aplikácia identifikovaná ADC pravidlom boli nevyužívané stanovený čas.	PCEF, TDF
Zmena PLMN	UE sa presunulo do siete iného operátora.	PCEF, TDF
Zmeny QoS	Nastane zmena QoS daného IP-CAN nosiča.	PCEF
Zmena v type IP-CAN	Zmení sa typ IP-CAN relácie.	PCEF, TDF
Zmena polohy (obsluhujúca bunka)	Obsluhujúca bunka daného UE bola zmenená.	PCEF, TDF
Zmena polohy (sledovaná lokalita)	Zmení sa lokalita daného UE.	PCEF, TDF
Zmena polohy (obsluhujúca eNodeB)	Zmení sa základňová stanica daného UE.	PCEF, TDF

3.3 Spúšťacia udalosť

Funkcia ERF (*Event Reporting Function*) vykonáva detekciu spúšťacích udalostí. Ak ERF zaznamená vykonanie niektorej zo spúšťacích udalostí, oznámi danú udalosť prvku riadenia zásad a kontroly účtovania PCRF. Funkcia ERF je súčasťou prvku vykonávania riadenia zásad a kontroly účtovania PCEF, prípadne v TDF pre hlásenie udalostí pri vyžiadaných aplikáciach [3].

Spúšťacie udalosti definujú podmienky, kedy sa má ERF znovu ohlásiť po zostavení IP-CAN relácie. Udalosti, ktoré sú potrebné pri prebiehajúcich procesoch musia byť nepodmienečne ohlásené PCRF. Prvok PCRF reaguje na nové udalosti poskytnutím pravidla riadenia zásad a účtovania alebo ADC pravidla. Spúšťacie udalosti určujú, kedy má ERF signalizovať, že došlo k zmene IP-CAN nosiča.

3.4 Riadenie zásad

Riadenie zásad a kontrola účtovania v sebe zahŕňa tieto funkcie [3]:

- Vytváranie väzieb – vytváranie združení medzi dátovými tokmi služieb a nosičmi dátových tokov IP-CAN;
- Kontrola brány – blokovanie alebo povoľovanie prístupu paketom, ktoré patria k dátovým tokom služieb;
- Ohlasovanie udalostí – zasielanie notifikácií ohľadom nových udalostí;
- Kontrola QoS – autorizácia a zabezpečenie prostriedkov v sieti pre maximálnu možnú dohodnutú kvalitu poskytovaných služieb;
- Smerovanie – riadenie smerov paketov podľa špecifických smerovacích adries;
- Zriadenie nosičov IP-CAN pre IP-CAN siete.

V prípade agregácie viacerých dátových tokov sú informácie ohľadom kvality služieb jednotlivých dátových tokov poskytované ako autorizovaná kvalita služieb. Potreba zabezpečenia autorizovanej kvality služieb pre IP-CAN nosič môže viesť k degradácií alebo vylepšeniu nosiča vyžadovaného prvkom PCEF ako časť používateľom inicializovaného prenosu. Zabezpečenie autorizovanej QoS, v závislosti od politiky operátora a kapacít siete, môže viesť k sieťou inicializovanej zmene či vytvoreniu IP-CAN relácie. Zabezpečenie kvality služieb pre jednotlivé dátové toky a individuálne pravidlá riadenia zásad a účtovania vykonáva prvok PCRF.

Informácie o autorizovanej QoS môžu byť poskytované dynamicky prvkom PCRF alebo môžu byť preddefinované ako pravidlo riadenia zásad a účtovania v prvku PCEF. V prípade dynamického poskytovania týchto pravidiel sa v nich môžu zahrnúť aj informácie ohľadom autorizovanej kvality služieb. Pri preddefinovaných pravidlách riadenia zásad a účtovania v PCEF sa autorizovaná kvalita služieb zabezpečuje pri aktivovaní daného pravidla. PCEF spracuje informácie o autorizovanej QoS, informácie získané od PCRF a informácie o preddefinovaných pravidlách riadenia zásad a účtovania. PCRF by mal vedieť o informáciách ohľadom autorizovanej kvality služieb v preddefinovaných pravidlách. Toto zabezpečí, že bude poskytovaná kvalita služieb bez ohľadu na to, či budú pravidlá riadenia zásad a účtovania vykonávané dynamicky alebo budú preddefinované.

3.5 Služby s prioritou a riešenie konfliktov

Pridelenie priorít jednotlivým službám umožňuje prvku PCRF riešiť konflikty, keď aktivácia všetkých vyžadovaných PCC pravidiel vedie k nahromadeniu požiadaviek na zabezpečenie QoS a následne k prekročeniu garantovanej šírky pásma [3].

Napríklad pri poskytovaní sieťou kontrolovanej kvality služby, PCRF môže aktivovať službu s prioritou, ktorá spôsobí prekročenie garantovanej šírky pásma poskytovanej používateľovi. V takomto prípade PCRF môže určiť či deaktivácia jedného alebo viacerých dátových tokov umožní aktiváciu služby s vyššou prioritou pri zachovanej garantovanej šírke pásma. PCRF teda vyrieši konflikt deaktiváciou vybraných dátových tokov s najnižšou prioritou a akceptuje informácie o službe s prioritou od AF.

3.6 Štandardizované charakteristiky QoS

Každý dátový tok služby je spojený s jediným QCI (*QoS Class Identifier*), ktorý udáva triedu QoS pre daný dátový tok. V jednej IP-CAN relácií môže byť zlúčených viacero dátových tokov s rovnakým QCI. QCI je hodnota, ktorá určuje ako sa bude zaobchádzať s daným paketom na jednotlivých uzloch siete. Napríklad podľa váh prideleným ku QCI a následným zaraďovaním do front. Tieto nastavenia zabezpečuje operátor, ktorý konkrétny uzol vlastní [3].

QCI hodnoty sú špecifikované štandardizovanými charakteristikami. Medzi tieto charakteristiky patria:

1. Typ prostriedkov – GBR (*Guaranteed Bit Rate*) alebo nie GBR – určuje či sú prostriedky siete trvalo pridelené danej službe;
2. Priorita – čím nižšia hodnota tým vyššia priorita;
3. Rezerva oneskorenia paketov – určuje hornú hranicu možného oneskorenia pri doručovaní paketov medzi UE a PCEF;
4. Pomer chybných paketov – určuje hornú hranicu pomeru neúspešne doručených paketov k celkovému počtu odoslaných paketov.

Parameter *typ prostriedkov* udáva či sieťové prostriedky pridelené službe s určitou hodnotou GBR sú permanentne alokované. Zlúčeným dátovým tokom sú sieťové prostriedky typicky prideľované na požiadanie, čo vyžaduje dynamické riadenie zásad a dynamické účtovanie.

Hornú hranicu oneskorenia pri doručovaní paketov medzi UE a PCEF určuje rezerva oneskorenia paketov PDB (*Packet Delay Budget*). Účelom PDB je podporovať triedenie paketov pri zaisťovaní QoS.

Každý identifikátor QCI je spojený s triedou QoS. Najnižšia trieda QoS znamená najvyššiu prioritu. Trieda QoS by sa mala využívať na rozdelenie dátových

tokov od jedného UE, ale aj na rozdelenie tokov viacerých koncových používateľov. Rozdeľovanie dátových tokov by malo byť primárne založené na PDB. Ak však ciele stanovené PDB nemôžu byť už dlhšie dosiahnuté pre niektorý z dátových tokov, v takomto prípade nastane rozdeľovanie podľa priority služby.

Jedným z parametrov kvality služieb je parameter ARP (*Allocation and Retention Priority*). ARP obsahuje informácie o triede QoS. Trieda QoS definuje potrebnú časť z kapacity sieťových zdrojov. Toto umožňuje rozhodnúť, či budú poskytnuté prostriedky na naviazanie spojenia, prípadne zmenu aktuálneho spojenia alebo žiadosť bude zamietnutá kvôli obmedzenej kapacite zdrojov. ARP môže byť tiež použité pri rozhodovaní, ktorý zo spustených prenosov bude ukončený.

3.7 Akcia ukončenia relácie

Akcia ukončenia relácie môže byť použitá iba pri online účtovaní. Túto akciu vykonáva PCEF alebo TDF ak pre reláciu nie je viac dostupných prostriedkov na účte (kreditov). Paket korešpondujúci s niektorým PCC či ADC pravidlom, ktoré má kľúč účtovania s vyčerpaným kreditom, je predmetom akcie ukončenia [3]. Definované ukončovacie akcie zahŕňajú:

- povolenie prechodu paketov,
- zahadzovanie paketov,
- štandardná ukončovacia akcia podľa PCEF alebo TDF,
- presmerovanie paketov na aplikačný server.

Štandardná akcia ukončenia relácie pre všetky účtovacie kľúče, ktoré nemajú definovanú vlastnú špecifickú akciu ukončenia, by mala byť predkonfigurovaná na prvku PCEF alebo TDF podľa riadenia zásad operátora. Systém online účtovania OCS zabezpečuje akcie ukončenia relácie pre každý účtovací kľúč rozhraním Gy. Všetky predošlé akcie ukončenia relácie získané z iných zdrojov ako z OCS môžu byť systémom pre online účtovanie prepísané.

3.8 Autorizácia ADC pravidiel

Autorizácia pravidiel detekovania aplikácií a ich kontroly ADC sa odvodzuje od rozhodnutí prvku riadenia zásad a kontroly účtovania PCRF. PCRF rozhoduje, ktoré preddefinované a dynamické ADC pravidlá budú aktivované pre konkrétnu TDF reláciu. Môže to aj zahŕňať výber parametrov pre ADC pravidlá, ktoré budú aplikované pri detekcii dátového toku. Nastavenia používateľského profilu, ktoré určujú či môže byť zapnutá detekcia a kontrola aplikácií, je využívaná prvkom PCRF pri rozhodovaní o autorizácii ADC pravidiel [3].

3.9 Presmerovanie

Presmerovanie dátového toku aplikácie je možnosť, ktorú môže využiť prvok rozpoznávania dát TDF použitím ADC pravidiel alebo prvok vykonávania riadenia zásad a kontroly účtovania PCEF využitím pravidiel riadenia zásad a účtovania PCC [3]. PCRF kontroluje presmerovanie poskytovaním a upravovaním dynamických ADC pravidiel pre TDF alebo pomocou pravidiel riadenia zásad pre PCEF. PCRF riadi presmerovanie, povoľuje presmerovanie, ukončuje presmerovanie, prípadne mení cieľ presmerovania pomocou pravidiel riadenia zásad PCC alebo pomocou pravidiel ADC.

4 AUTENTIZÁCIA A AUTORIZÁCIA V MOBILNÝCH SIEŤACH 4G

V tejto kapitole sú popísané dôvody, kvôli ktorým je potrebné vykonávať autentizáciu používateľov a zabezpečiť utajenie ich identity v sieti. Nachádza sa tu popis jednotlivých procesov potrebných na zabezpečenie utajenia a bezpečného prístupu k sieti.

4.1 Bezpečnosť identity používateľa

Na zabezpečenie utajenia identity používateľa sa využívajú tieto bezpečnostné funkcie [6]:

- utajenie identity používateľa – zabezpečuje, že trvalá identita IMSI (*International Mobile Subscriber Identity*) používateľa, ktorému je služba poskytovaná, nemôže byť odpočúvaná na rádiovej prístupovej sieti,
- utajenie lokality používateľa – vlastnosť, ktorá zabezpečuje, že prítomnosť alebo príchod používateľa do určitej oblasti nemôže byť zistená odposluchom na rádiovej prístupovej sieti,
- zamedzenie sledovania používateľa – zabezpečuje, že narušiteľ nedokáže určiť, či rôzne služby sú poskytované rovnakému používateľovi.

Na dosiahnutie týchto podmienok sa využíva identifikácia používateľa dočasnou identitou. Pomocou dočasnej identity je používateľ identifikovaný v sieti, ktorou je práve obsluhovaný. Na zamedzenie možnosti sledovania používateľa, by používateľ nemal byť identifikovaný rovnakou dočasnou identitou na dlhý čas. Aby bolo možné dosiahnuť tieto bezpečnostné ciele je nutné, aby akákoľvek signalizácia či dáta používateľa, ktoré môžu odhaliť jeho identitu, boli šifrované v rádiovej prístupovej sieti.

4.2 Autentizácia entity

Na zabezpečenie autentizácie entity sú použité tieto bezpečnostné funkcie:

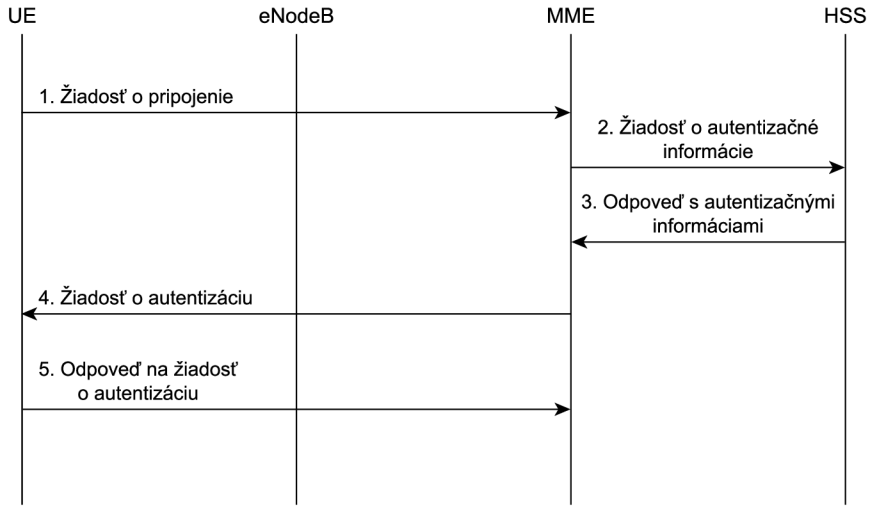
- autentizácia používateľa – obslužná sieť potvrdzuje identitu používateľa,
- autentizácia siete – používateľ potvrdzuje, že je pripojený k obslužnej sieti, ktorá je autorizovaná aby mu poskytovala garantované služby. To zahŕňa aj garanciu toho, že autorizácia je aktuálna.

Aby boli dosiahnuté tieto podmienky, musí sa pri každom zostavovaní spojenia medzi používateľom a sieťou vykonať autentizácia entity. Autentizácia sa vykonáva

mechanizmom, ktorý využíva autentizačný vektor [1] doručený obslužnej sieti serverom pre správu používateľov daného používateľa [6]. Tento proces by mal byť vykonaný obslužnou sieťou pri prvej registrácii používateľa v danej sieti a pri žiadostiach o poskytnutie služby, aktualizáciu polohy, pripojenie k sieti, odpojenie od siete a pri žiadosti o obnovenie spojenia. Proces autentizácie a zostavenia autentizačného kľúča je popísaný v nasledujúcej kapitole.

4.3 Autentizácia a autorizácia používateľa

Pri autentizácii používateľa sa vykonáva proces autentizácie a zostavenia kľúča AKA (Authentication and Key Agreement). Priebeh procesu AKA môžeme vidieť na obrázku 4.1. Tento proces je vykonávaný postupne počas týchto krokov:



Obr. 4.1: Popis AKA procesu [11]

1. Používateľské zariadenie UE odošle žiadosť o pripojenie k prístupovej sieti prvku eNodeB, ktorý správu automaticky prepošle prvku správy mobility MME.
2. Prvok správy mobility MME odošle žiadosť o autentizačné informácie serveru pre spravovanie používateľov HSS. Táto žiadosť obsahuje identitu používateľa IMSI, identifikátor obslužnej siete a jej typ [2]. Podrobný popis tejto správy sa nachádza v tabuľke 4.1.

[1] obsahuje údaje potrebné na dočasnú autentizáciu používateľa a zostavenie kľúča
[2] práca je o autentizácii v sieťach 4. generácie, takže sa jedná o typ siete E–UTRAN

3. Na základe informácii z žiadosti od MME, server pre spravovanie používateľov HSS vypočíta kľúč šifrovania CK (*Ciphering Key*), kľúč integrity IK (*Integrity Key*) a autentizačný kľúč K_{ASME}. Do odpovede s autentizačnými informáciami HSS vloží vypočítaný kľúč K_{ASME}, náhodné číslo RAND (*Random Number*), autentizačný token AUTN (*Authentication Token*), ktorý obsahuje kľúče CK a IK a očakávanú odpoveď od používateľa XRES (*Expected Response*). Podrobný popis tejto správy sa nachádza v tabuľke 4.2. HSS odošle správu prvku správy mobility MME. Ak správa obsahuje viacero autentizačných vektorov, zoradia sa na základe sekvenčného čísla. HSS nastaví separovaný bit v poli AMF (*Authentication Management Field*) na hodnotu 1. Je to prvý bit v poli AMF, ktoré je súčasťou autentizačného tokenu AUTN.
4. Prvok správy mobility MME uloží očakávanú odpoveď XRES a kľúč K_{ASME} a používateľskému zariadeniu UE odošle žiadosť o autentizáciu. Po prijatí správy modulom USIM (*Universal Subscriber Identity Module*) [3] by sa malo overiť, či autentizačný token AUTN môže byť akceptovaný. Tým sa dokáže, že autentizačný vektor nie je zastaralý. Mobilné zariadenie skontroluje počas autorizácie či separovaný bit v poli AMF je nastavený na hodnotu 1.
5. Modul USIM na základe kľúča náhodného čísla RAND a autentizačného vektora AUTN vypočíta odpoveď RES (*Response*). Tú potom odošle v odpovedi na žiadosť o autentizáciu prvku správy mobility MME. MME porovná odpoveď od používateľa RES s očakávanou odpoveďou XRES od servera pre správu používateľov. Ak sa zhodujú, autentizácia prebehla úspešne. Modul USIM taktiež vypočíta na základe autentizačného vektora AUTN a náhodného čísla RAND aj kľúče CK a IK. Z týchto kľúčov a identifikátora obslužnej siete používateľské zariadenie následne vypočíta kľúč K_{ASME}.

Pre vykonanie procesu autentizácie používateľa je potrebné získať jeho používateľský profil zo servera pre správu používateľov HSS. Získaním profilu používateľa je vykonané overenie jeho autorizácie - bez používateľského profilu by nebolo možné poskytnúť danému používateľovi zazmluvnené služby [10].

[3] jedná sa o rozšírenú verziu SIM kariet, ktorá sa začala používať s príchodom sietí UMTS

Tab. 4.1: Žiadosť o autentizačné údaje z HSS [5]

Informácia	**Kategória**	**Popis**
IMSI	Povinné	Toto pole obsahuje trvalú identitu používateľa IMSI.
Podporované funkce	Voliteľné	Obsahuje zoznam funkcií podporovaných zdrojovým prvkom.
Autentizačné informácie	Podmienené	Informácie potrebné k autentizácii v sieti E-UTRAN.
Identifikátor siete	Povinné	Obsahuje identifikátor obslužnej siete.

Tab. 4.2: Odpoveď s autentizačnými údajmi [5]

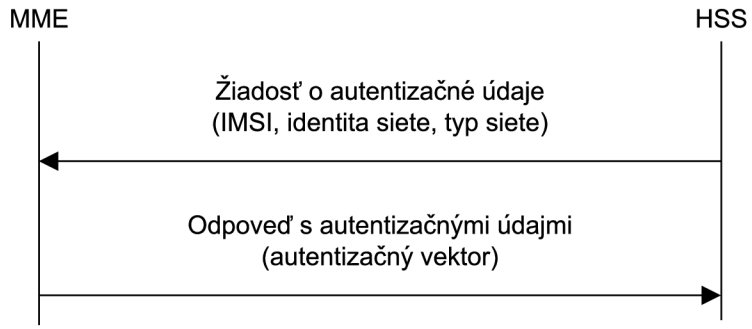
Informácia	**Kategória**	**Popis**
Výsledok	Povinné	Obsahuje výsledok operácie.
Identifikátor chyby	Voliteľné	V prípade, že HSS nepozná používateľa, oznamuje chybu.
Podporované funkcie	Voliteľné	Obsahuje zoznam funkcií podporovaných zdrojovým prvkom.
Autentizačné informácie	Podmienené	Obsahuje autentizačné vektory.

4.4 Prenos autentizačných údajov z HSS

Účelom tohto procesu je poskytnutie autentizačných vektorov prvku MME z databázy profilov HSS daného používateľa.

Autentizačný vektor je vypočítaný v HSS pomocou funkcie derivácie kľúča KDF (*Key Derivation Function*), ktorá pre výpočet vyžaduje šifrovací kľúč CK, kľúč integrity IK a identifikátor siete [7].

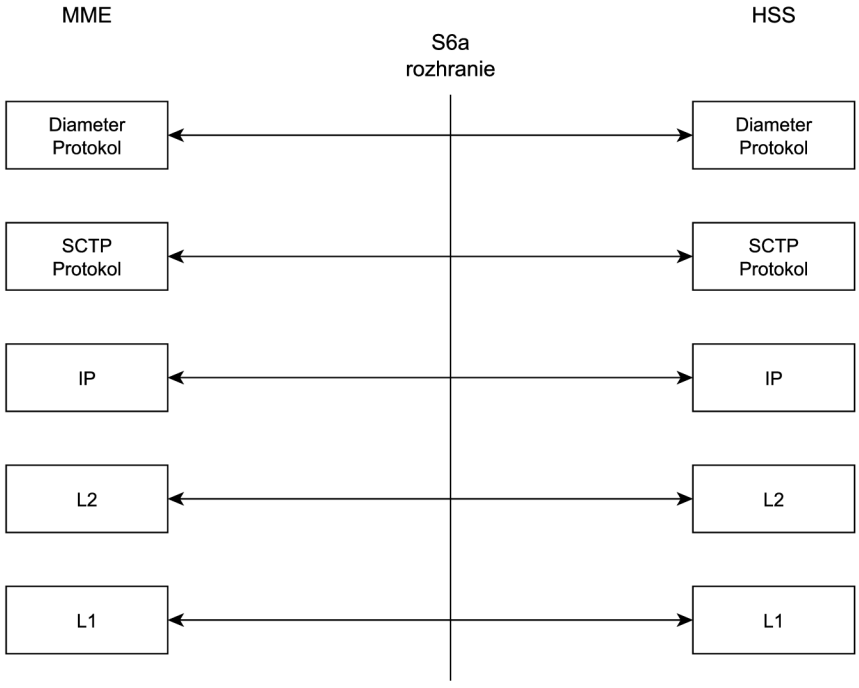
Žiadosť o autentizačné údaje by mala obsahovať identifikátor používateľa IMSI, identifikátor obslužnej siete a typ siete. Databáza HSS pošle odpoveď s autentizačnými údajmi späť prvku MME. V prípade vyžiadania viacerých autentizačných vektorov sú zoradené podľa sekvenčných čísel.



Obr. 4.2: Žiadosť HSS o údaje potrebné k autentizácii používateľa

4.5 Rozhranie S6a

Toto rozhranie sa nachádza medzi prvkom správy mobility MME a serverom pre správu používateľov HSS. Úlohou tohto rozhrania je prenos autentizačných informácii a informácií o používateľoch (ich používateľské profily) medzi prvkami MME a HSS. Rozhranie S6a je zobrazené na obrázku 4.3.

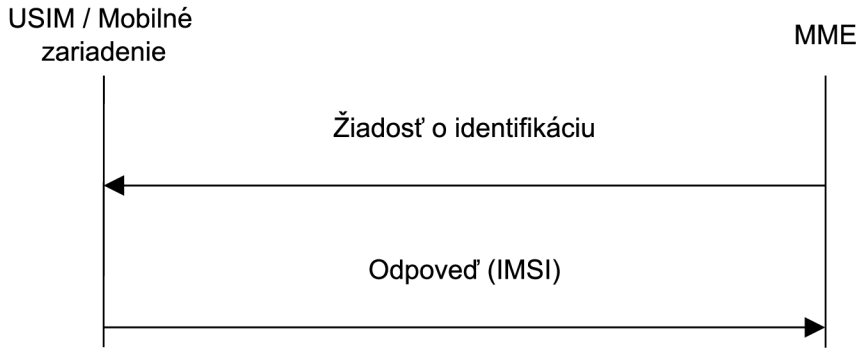


Obr. 4.3: Rozhranie S6a

Protokol Diameter zabezpečuje prenos autentizačných dát a informácií o používateľoch medzi HSS a MME. Protokol SCTP (*Stream Control Transmission Protocol*) slúži na prenos signalizačných správ medzi MME a HSS [2].

4.6 Identifikácia používateľa trvalou identitou

Tento spôsob identifikácie používateľa by mal byť vyžiadaný obslužnou sieťou vždy, keď nie je možná identifikácia používateľa dočasnou identitou GUTI (*Globally Unique Temporary Identity*). Proces identifikácie je inicializovaný prvkom MME, ktorý vyžiada od používateľa jeho trvalú identitu IMSI [7]. Priebeh je popísaný na obrázku 4.4.



Obr. 4.4: Identifikácia používateľa trvalou identitou IMSI

Odpoveď od používateľa obsahuje IMSI v nešifrovanom texte. Toto potvrdenie predstavuje slabinu v zabezpečení utajenia identity používateľa.

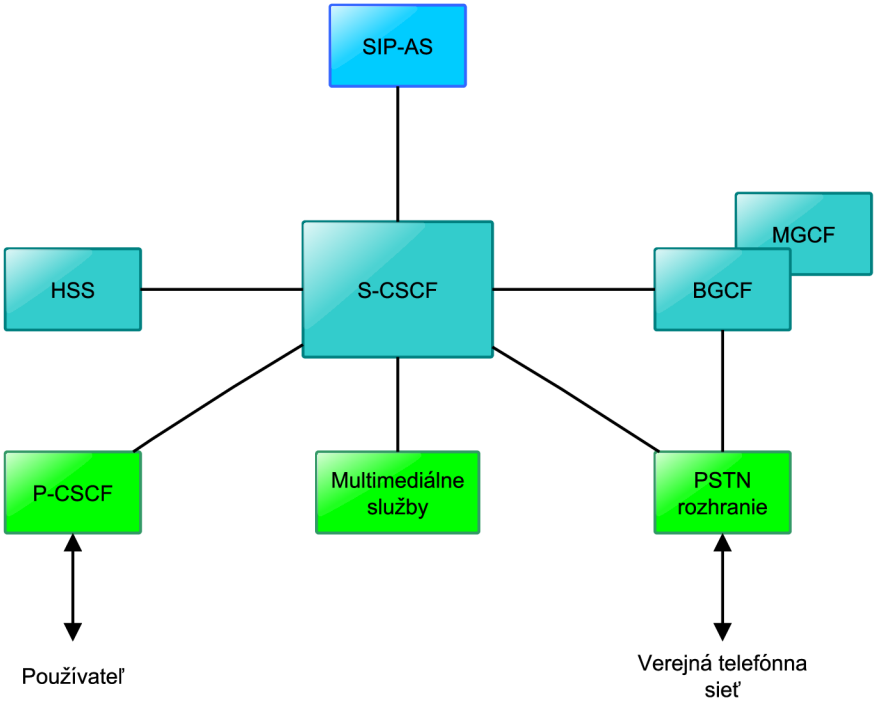
4.7 Identifikácia používateľa dočasnou identitou

Dočasná identita GUTI sa priradí mobilnej stanici kvôli zabezpečeniu utajenia identity používateľa. Trvalá identita IMSI sa používa iba po zapnutí mobilnej stanice. Následne prvok MME priradí mobilnej stanici dočasnú identitu GUTI. Po tomto procese sa na overenie identity používateľa používa iba dočasná identita GUTI. Často sa používa aj skrátená verzia dočasnej identity - S – TMSI (*S – Temporary Mobile Subscriber Identity*). Umožňuje efektívnejšie signalizačné procesy v rádiovej sieti [7].

4.8 Charakteristika systému IMS

IP Multimedia Subsytem je systém, ktorý zabezpečuje poskytovanie multimediálnych služieb v sieťach využívajúcich prepínanie paketov. Architektúra systému IMS je zobrazená na obrázku 4.5. IP multimediálne služby sú založené na protokoloch IETF (*Internet Engineering Task Force*). Systém IMS umožňuje operátorom verejných sietí ponúkať ich používateľom multimediálne služby založené na internetových aplikáciach, službách a protokoloch. IMS ponúka možnosť prístupu k hlasovým službám, video službám, dátovým prenosom, chatovacím službám či webovým technológiám [4].

Komplexné riešenie pre podporu IP multimediálnych služieb pozostáva z terminálov a špecifických funkčných prvkov IMS systému. IMS je nezávislý na okruhovo prepínanej doméne. To znamená, že nie je potrebné zriadiť doménu prepínaných okruhov, aby mohla fungovať sieť založená na IMS. Prenos signalizácie v systéme IMS pracuje na protokole SIP (*Session Initiation Protocol*). Tento protokol je detailne popísaný v dokumente RFC 3261 [15]. Protokol SIP je protokolom aplikačnej vrstvy OSI modelu a slúži na zostavovanie a riadenie relácií multimediálnych prenosov.



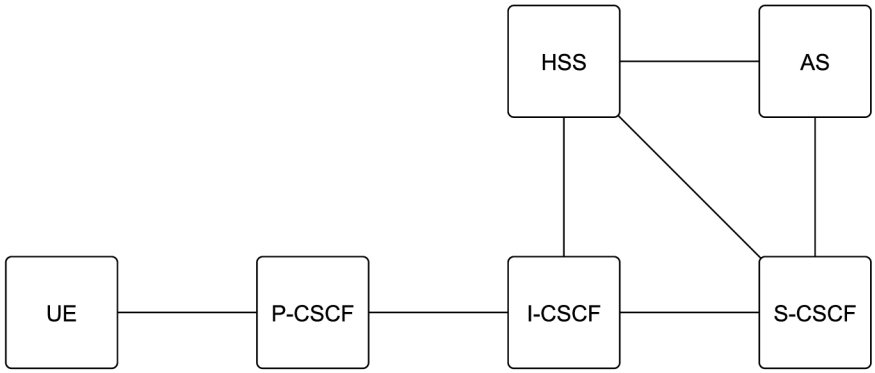
Obr. 4.5: Zjednodušená architektúra IMS [14]

Architektúra systému IMS sa skladá z niekoľkých hlavných prvkov [14]:

- CSCF – *Call Session Control Function*: zabezpečuje registráciu koncových zariadení, poskytuje smerovanie signalizačných správ protokolu SIP a podporuje poskytovanie kvality služieb QoS. CSCF je rozdelený na niekoľko ďalších celkov:
  - S-CSCF (*Server – CSCF*) – kontrolný prvok relácií pre koncové zariadenia a spravuje stav relácií;
  - P-CSCF (*Proxy – CSCF*) – táto časť je vstupným bodom zariadení do IMS, zasiela SIP správy do domáceho P-CSCF používateľa. Podporuje taktiež riadenie kvality služieb;
  - I-CSCF (*Interrogating – CSCF*) – je súčasťou S-CSCF, riadi smerovanie žiadostí HSS a S-CSCF. Je to kontrolný prvok pre zariadenia, ktoré spravujú stav relácií;
- HSS – *Home Subscriber Server*: prvok v IMS systéme, ktorý uchováva informácie o používateľoch v sieti;
- BGCF – *Breakout Gateway Control Fucntion*: tento prvok vyberá sieť, v ktorej sa komunikácia pripojí na verejnú telefónnu sieť PSTN (*Public Switched Telephone Network*);
- MGCF – *Media Gateway Control Function*: táto časť IMS prevádza SIP signalizáciu a riadi distribúciu relácií cez viacero brán;
- SIP-AS – *Session Initiation Protocol – Application Server*: platforma vykonávajúca služby, ktoré sú v sieti poskytované.

4.9 Autorizácia v IMS

Autorizácia je proces, pri ktorom si používateľ vyžiada prístup k službám, ktoré sú poskytované sieťou. Na základe entity, ktorá inicializuje proces autorizácie, môžeme autorizáciu rozdeliť na *základnú autorizáciu* a *autorizáciu pre tretiu stranu*. Základná autorizácia je inicializovaná zo strany používateľa. Po jej vykonaní má používateľ povolený prístup k základným službám siete. Pri autorizácií pre tretiu stranu je autorizácia inicializovaná prvkom S-CSCF po žiadosti používateľa o služby poskytované aplikačným serverom AS. Prvky potrebné pri autorizácií a ich vzájomné usporiadanie je zobrazené na obrázku 4.6.

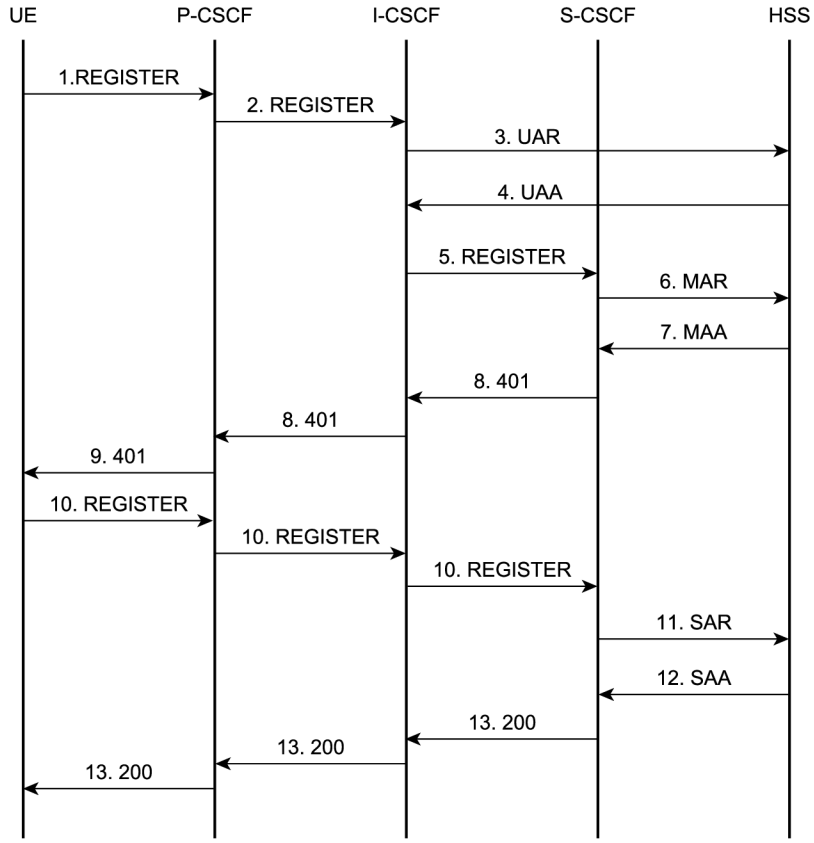


Obr. 4.6: Prvky systému IMS vykonávajúce autorizáciu [11]

4.9.1 Základná autorizácia

Procesy pri vykonávaní základnej autorizácie 4.7:

1. Autorizácia je inicializovaná zo strany používateľa zaslaním správy typu **REGISTER** prvku P-CSCF. Táto správa obsahuje identitu používateľa IMPU (*IP Multimedia Public Identity*) a adresu používateľa.
2. Prvok P-CSCF odošle správu REGISTER prvku I-CSCF, do jej hlavičky však pridá informáciu o svojej IP adrese. Tým zabezpečí, že správy určené pre používateľa budú smerované cez P-CSCF. Taktiež je pridaná informácia o názve prístupovej siete.
3. Po prijatí správy REGISTER I-CSCF získa adresu prvku P-CSCF. Získanú IP adresu porovná so svojimi záznamami. Ak danú adresu nájde vo svojich záznamoch, znamená to, že je dôveryhodná a autorizácia môže byť vykonaná. V takomto prípade I-CSCF odošle prvku HSS žiadosť o autorizáciu používateľa UAR (*User Authorization Request*), aby získal IP adresu prvku S-CSCF. Ak však IP adresa P-CSCF nie je dôveryhodná, I-CSCF odošle späť odpoveď *403 Forbidden* - server správe rozumel, no odmieta ju splniť.
4. Po prevzatí žiadosti o autorizáciu používateľa UAR server HSS určí, či je daný používateľ definovaný v jeho databáze. Odošle späť odpoveď na autorizáciu používateľa UAA (*User Authorization Answer*), ktorá obsahuje IP adresu prvku S-CSCF.
5. Na základe zaslanej IP adresy od HSS prvok I-CSCF odošle správu REGISTER danému S-CSCF.
6. S-CSCF odošle žiadosť o autentizáciu multimédií MAR (*Multimedia Authentication Request*) serveru pre správu používateľov HSS, aby získal autentizačný vektor a zároveň tým informuje HSS, že obsluhuje daného používateľa.
7. HSS odošle odpoveď na autentizáciu multimédií MAA (*Multimedia Authentica-*



Obr. 4.7: Procesy pri základnej autorizácii [11]

tion Answer), ktorá obsahuje očakávanú odpoveď XRES, náhodnú postupnosť RAND, autentizačný token AUTN, kľúč integrity IK a šifrovací kľúč CK.

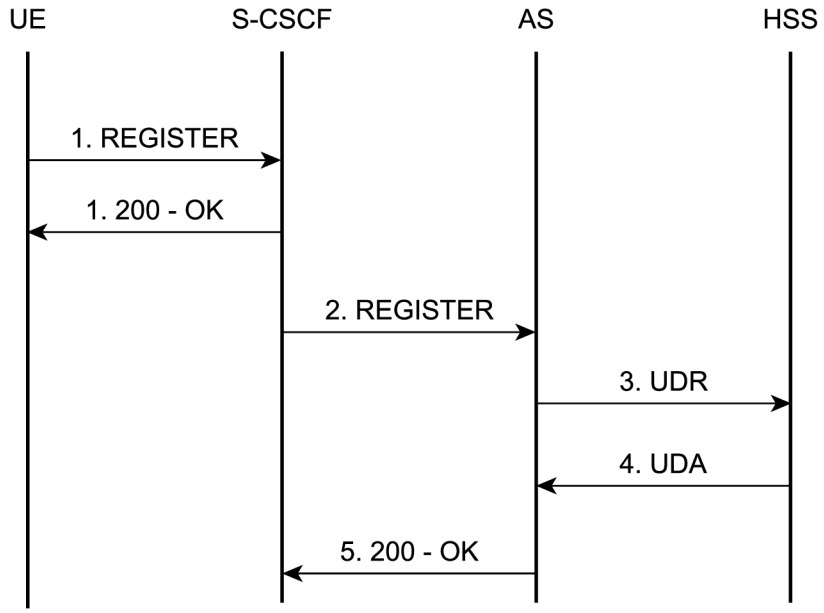
8. S-CSCF si uloží očakávanú odpoveď XRES. XRES slúži na overenie autentizácie. Následne S-CSCF odošle správu *401 - Unauthorized* - žiada sa autorizácia používateľa. Táto správa obsahuje ostatné autorizačné elementy, ktoré potrebuje P-CSCF na vykonanie autorizácie.
9. P-CSCF si zo správy uloží kľúč integrity IK a šifrovací kľúč CK a ostatné autorizačné elementy (náhodnú postupnosť RAND a autorizačný token AUTN) odošle používateľovi.
10. Po prijatí správy *401 - Unauthorized* používateľské zariadenie vypočíta odpoveď RES na základe prijatého autentizačného tokenu AUTN a náhodnej postupnosti RAND. Vytvorí novú správu REGISTER, ktorá obsahuje odpoveď RES a odošle ju S-CSCF.
11. Po prijatí správy S-CSCF porovná odpoveď od používateľa RES s očakávanou

odpoveďou XRES. V prípade zhody bola autentizácia vykonaná úspešne. S-CSCF odošle žiadosť o pridelenie servera SAR (*Server Assignment Request*) prvku HSS aby získal profil používateľa.

12. HSS odpovie zaslaním profilu používateľa v odpovedi na pridelenie servera SAA (*Server Assignment Answer*).
13. Po odpovedi S-CSCF používateľovi správou *200 - OK* autorizácia prebehla úspešne.

4.9.2 Autorizácia pre tretiu stranou

Autorizácia pre tretiu stranu prebieha rovnako ako základná autorizácia, no je doplnená o ďalšie potrebné procesy. Zmena oproti základnej autorizácii nastáva od kroku 10. kroku pri procesoch popísaných v predchádzajúcej kapitole.



Obr. 4.8: Procesy pri autorizácii pre tretiu stranu [11]

Procesy pri autorizácií pre tretiu stranu sú zobrazené na obrázku 4.8:

1. Prvok S-CSCF vykoná základnú autorizáciu používateľa, ktorá je popísaná v predchádzajúcej podkapitole na obrázku 4.7.
2. Na základe používateľského profilu prijatého zo servera pre správu používateľov HSS prvok S-CSCF určí, či existujú počiatočné filtrovacie kritéria iFC (*Initial*

Filter Criteria). Tieto kritéria špecifikujú podmienky poskytovania jednotlivých služieb a určujú, na ktorých aplikačných serveroch sú dané služby poskytované. Na základe údajov získaných z používateľského profilu odošle S-CSCF žiadosť o autorizáciu konkrétnemu aplikačnému serveru AS.

3. Aplikačný server detekuje pokus o autorizáciu používateľa a odošle žiadosť o údaje o používateľovi UDR (*User Data Request*) serveru pre správu používateľov HSS.
4. HSS odpovie správou UDA (*User Data Answer*), ktorá obsahuje údaje o používateľovi, ako jeho identitu a poskytované služby.
5. Aplikačný server AS na základe prijatých údajov vykoná autorizáciu používateľa. V prípade úspešnej autorizácie si uloží prijaté údaje vo svojej lokálnej databáze vráti odpoveď *200 - OK* prvku S-CSCF, ktorá potvrdí úspešný priebeh autorizácie pre tretiu stranu.

4.10 Návrh implementácie funkcie autentizácie

Funkcia autentizácie identifikuje používateľov a zabezpečuje synchronizáciu kľúčov potrebných pri procese autentizácie AKA. Kontrolovaním identity používateľov prvok USN9810 zabezpečuje, že sieť poskytuje služby iba autorizovaným používateľom. Prvok USN9810 je riešením od firmy HUAWEI, ktorý integruje funkcie prvku SGSN (*Serving GPRS Support Node*) [4] a prvku správy mobility MME.

Aktiváciu funkcie autentizácie je potrebné vykonať pomocou systému na obsluhu a údržbu (*HUAWEI Operation & Maintenance System*). Aktivácia sa vykonáva v príkazovom riadku tohto systému pomocou príkazu ***MOD S1USRSECPARA***. Tento príkaz má mnoho voliteľných parametrov. Ich detailný popis sa nachádza v tabuľkách 4.3 a 4.4.

V tabuľke 4.3 je popis základných parametrov, ktoré je potrebné nastaviť vždy. Ak je v parametri **OPTIONAL** nastavená hodnota **YES**, aktivuje sa možnosť nastavenia pokročilých funkcií. Ich prehľad a detailný popis sa nachádza v tabuľke 4.4.

[4] zabezpečuje prenos dát k mobilným staniciam v systéme GPRS

Tab. 4.3: Parametre príkazu na aktiváciu autentizácie

Parameter	**Názov parametra**	**Popis**
USRRANGE	Rozsah používateľov	Tento parameter udáva rozsah používateľov. Hodnota: - **DEFAULT** - modifikácia nastavení bezpečnosti pre všetkých používateľov, - **SPECIAL** - modifikácia nastavení bezpečnosti pre používateľov špecifikovaných IMSI sériami.
IMSIPRE	IMSI prefix	Tento parameter špecifikuje prefix IMSI. Používa sa len v prípade, keď je hodnota **USRRANGE** nastavená na **SPECIAL**.
SECPLC	Riadenie bezpečnosti	Tento parameter špecifikuje či budú vykonané procesy autentizácie a dohoda zabezpečenia. Hodnota: - **NEVER** - funkcia autentizácie je vypnutá, - **AUTHONLY** - vykonávaná je iba autentizácia, - **AUTHANDPROTECTED** - vykonávané obe funkcie, doporučené nastavenie.
SUPTINTAGTH	Algoritmus integrity	Špecifikuje algoritmus integrity podporovaný systémom. Tento parameter je platný iba v prípade, keď je parameter **SECPLC** nastavený na hodnotu **AUTHANDPROTECTED**. Hodnota: - **EIA0** - bez šifrovacieho algoritmu, - **EIA1** - založený na štandarde SNOW, - **EIA2** - založený na štandarde AES.
SUPTCIPHAGTH	Šifrovací algoritmus	Špecifikuje šifrovací algoritmus podporovaný systémom. Tento parameter je platný iba v prípade, keď je parameter **SECPLC** nastavený na hodnotu **AUTHANDPROTECTED**. Hodnota: - **EEA0** - bez šifrovacieho algoritmu, - **EEA1** - založený na štandarde SNOW, - **EEA2** - založený na štandarde AES.
OPTIONAL	Pokročilé funkcie	Tento parameter je platný iba v prípade, keď je parameter **SECPLC** nastavený na hodnotu **AUTHONLY** alebo **AUTHANDPROTECTED**. Hodnota: - **YES**, - **NO**.

Tab. 4.4: Pokročilé parametre príkazu na aktiváciu autentizácie

Parameter	**Názov parametra**	**Popis**
AUTHEVENT	Autentizačná udalosť	Špecifikuje udalosti, pri ktorých je potrebná autentizácia. Hodnota: - **ATTACH**, - **INTRA_TAU**, - **INTER_TAU**, - **DETACH**, - **SERVICE_REQUEST**, - **PROD_TAU**, - **SYSTEM_CHANGE_TAU**
AUTHPERIOD	Autentizačná perióda	Tento parameter nastavuje periódu autentizácie. Hodnota: **0 - 24 hodín** Ak je nastavená hodnota **0**, periodická autentizácia je vypnutá.
AUTHEVENT-THRESHOLD	Hraničná hodnota	Špecifikuje horný limit, pred ktorého prekročením sa nevykonáva autentizácia pri udalostiach uvedených v **AUTHEVENT**.Keď celkový počet udalostí špecifikovaných v **AUTHEVENT** dosiahne tento limit, začne sa vykonávať autentizácia týchto udalostí. Hodnota: - **0** - funkcia je vypnutá, - **1 - 1023** - celkový počet udalostí.
AUTHSETS-NUMBER	Počet autentizačných vektorov	Špecifikuje počet autentizačných vektorov. Hodnota: **1 - 5**
PREGET-AUTHSETS	Dopredné získavanie autentizačných vektorov	Tento parameter špecifikuje, či prvok MME získava autentizačné vektory z HSS pred inicializáciou samotného procesu autentizácie. Hodnota: - **NO**, - **YES**.

Na obrázku 4.9 sa nachádza prostredie systému na obsluhu a údržbu od firmy Huawei. V hornej časti okna sa nachádza detailný popis zadávaného príkazu. Uprostred sa nachádza okno, do ktorého je možné zadať príkaz v textovej forme. Na obrázku je zobrazený návrh príkazu, ktorý môže byť implementovaný do daného systému. V spodnej časti okna sa nachádza formulár, ktorý umožňuje pohodlnejšie zadávanie potrebných príkazov.

Návrh príkazu ***MOD S1USRSECPARA*** má tieto parametre:

- *Rozsah používateľov* = **DEFAULT** - príkaz platí pre všetkých používateľov;
- *Riadenie bezpečnosti* = **AUTHANDPROTECTED** - vykonávať sa bude autentizácia aj dohoda zabezpečenia;
- *Algoritmus integrity* = **EIA0-1 & EIA1-1 & EIA2-1** - povolené sú všetky algoritmy, systém zvolí algoritmus na základe dohody s mobilným zariadením;
- *Šifrovací algoritmus* = **EEA0-1 & EEA1-1 & EEA2-1** - povolené sú všetky algoritmy, systém zvolí algoritmus na základe dohody s mobilným zariadením;
- *Pokročilé funkcie* = **YES** - pokročilé funkcie sú zapnuté;
- *Autentizačná udalosť* = **ATTACH-1** - autentizácia sa vykonáva pri pripojení používateľa;
- *Autentizačná perióda* = **1** - autentizácia sa vykonáva periodicky každú hodinu;
- *Hraničná hodnota* = **10** - autentizácia sa začne vykonávať až po 10 udalostiach špecifikovaných v poli Autentizačná udalosť;
- *Počet autentizačných vektorov* = **2** - počet zasielaných autentizačných vektorov;
- *Dopredné získavanie autentizačných vektorov* = **YES** - dopredné získavanie autentizačných vektorov z HSS je povolené.

Obr. 4.9: Zadanie príkazu MOD S1USRSECPARA

5 ÚČTOVANIE V SYSTÉME HUAWEI

Účtovanie je v mobilných sieťach štvrtej generácie implementované za účasti prvkov S-GW, P-GW a PCRF. Paketová brána **UGW9811** je riešením od spoločnosti HUAWEI a v závislosti na type dátovej siete môže pracovať ako prvok GGSN (*Gateway GPRS Support Node*) [1] alebo ako kombinácia prvkov S-GW a P-GW. Prvok PCRF je v systéme od spoločnosti HUAWEI označovaný ako **UPCC** (*Unified Policy and Charging Controller*).

Prvok PCRF ani jeho technická dokumentácia však neboli zatiaľ spoločnosťou HUAWEI dodané do systému experimentálnej mobilnej siete UTKO FEKT VUT, preto nebolo možné vytvoriť návrh konkrétnej implementácie účtovania v mobilnej sieti. Táto časť práce preto obsahuje popis všetkých možností účtovania v tomto systéme bez konkrétnych riešení. Popis priebehov účtovania a jednotlivých funkcií sa nachádza v technickej dokumentácií paketovej brány UGW9811 [11].

5.1 Účtovací režim

Účtovacie systémy sú nastavované poskytovateľmi pripojenia tak, aby boli aplikované žiadané účtovacie pravidlá za využívanie prostriedkov siete. UGW9811 podporuje online a offline účtovanie. Spolupracuje pritom cez rozhranie Gy so systémom online účtovania OCS, ktorý podporuje online účtovanie a pomocou rozhrania Ga komunikuje s účtovacou bránou CG (*Charging Gateway*), ktorá implementuje offline účtovanie.

Pri využívaní dátových služieb rôznymi používateľmi UGW9811 získava charakteristiky jednotlivých dátových tokov, ako sú objem prenesených dát či doba poskytovania služby. UGW9811 komunikuje s OCS a CG a zo získaných údajov generuje záznamy o účtovaní CDR (*Charging Data Records*).

Popis procesu:

1. Používateľ inicializuje žiadosť o poskytnutie služby. Prvok správy mobility MME odošle správu prvku PDN-GW, ktorá nesie informácie o používateľovi, vrátane charakteristiky účtovania a názve prístupového bodu APN (*Access Point Name*). PDN-GW rozhodne, ktorý účtovací režim je použitý (online alebo offline účtovanie).
2. PDB-GW pomocou názvu APN a informácií o používateľovi získa jeho používateľský profil. PDN-GW zistí, či je profil viazaný k účtovacím pravidlám a či je pre daného používateľa aktivované *normálne účtovanie* alebo *účtovanie na základe dátového toku FBC (Flow-Based Charging)*. Účtovacie pravidlá sú

[1] paketová brána v dátovej sieti GPRS

uložené v databáze zásad v pamäti prvku PDN-GW. Tieto pravidlá môžu byť doručené prvkom PCRF alebo vytvorené v paketovej bráne.

3.
   - V prípade spracovania dátových tokov od používateľa, ktorý podlieha *normálnemu účtovaniu*, P-GW zaznamenáva objem prenesených dát a dobu trvania relácií. Tieto informácie vymieňa s OCS a generuje záznamy o účtovaní.
   - Ak P-GW spracuje dáta od používateľa, ktorý podlieha *účtovaniu na základe dátového toku*, paketová brána analyzuje charakter prenášaných dát a výsledky porovnáva s pravidlami účtovania v databáze zásad. Následné informácie vymieňa s účtovacou bránou CG a generuje záznamy o účtovaní.

UGW9811 podporuje viacero účtovacích režimov, ktoré môžu byť klasifikované na niekoľkých úrovniach 5.1:

1. úroveň - v závislosti, či je účtovanie implementované v reálnom čase sa účtovacie režimy delia na online alebo offline účtovanie;
2. úroveň - v závislosti, či je účtovanie špecifikované poskytovanou službou sa účtovacie režimy delia na normálne a na základe dátového toku (*FBC - Flow Based Charging*);
3. úroveň - v závislosti na podmienkach účtovania sa účtovanie rozdeľuje na základe doby trvania prenosu, na základe objemu prenesených dát a na základe uskutočnenia udalosti.

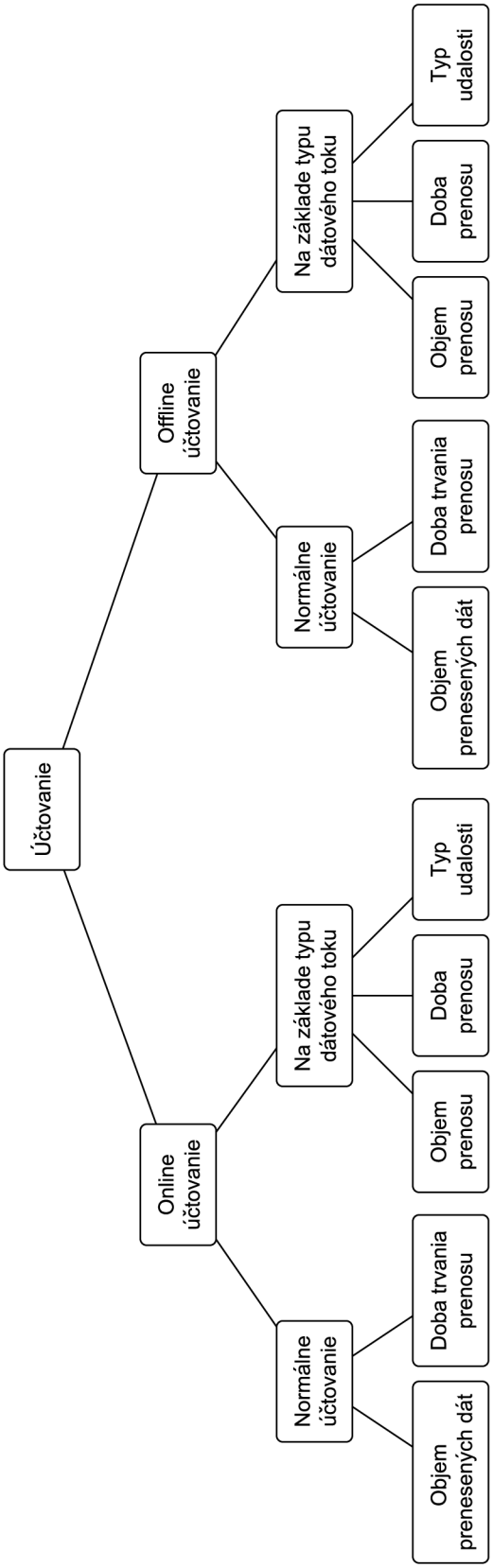
Tieto možností účtovacích režimov sa vždy prekrývajú na daných úrovniach. To znamená, že každý dátový tok podlieha niektorej možnosti účtovania na jednotlivých úrovniach.

Charakteristika účtovania špecifikuje podrobnosti spôsobu účtovania poskytovaných služieb. Charakteristika účtovania môže byť doručená zo servera pre správu používateľov alebo nakonfigurovaná priamo v paketovej bráne UGW9811. Pri výbere charakteristiky účtovania má vyššiu prioritu charakteristika doručená prvkom MME z HSS, ak nie je manuálne priorita priradená lokálne nakonfigurovaným charakteristikám. Online alebo offline účtovací režim môže byť doručený prvkom na kontrolu riadenia zásad a účtovania PCRF alebo nakonfigurovaný priamo v UGW9811.

5.2 Funkcie účtovania v systéme HUAWEI

Offline účtovanie

Funkcia offline účtovania umožňuje prvku UGW9811 implementáciu účtovania pre používateľov nie v reálnom čase. Pri offline účtovaní sa monitoruje využívanie prostriedkov siete a generujú sa účtovacie záznamy CDR. Prvok UGW9811 môže genero-



Obr. 5.1: Možností účtovania na jednotlivých úrovniach [11]

vať niekoľko rôznych typov účtovacích záznamov CDR. V prípade experimentálnej siete UTKO, kde prvok UGW9811 kombinuje funkciu paketovej brány PDN-GW a obslužnej brány S-GW je však možné generovať iba záznamy typu PGW-CDR.

Paketová brána PDN-GW odosiela účtovacie záznamy účtovacej bráne CG. Účtovacia brána môže byť nakonfigurovaná lokálne alebo špecifikovaná prvokom pre riadenie a kontrolu zásad PCRF.

Paketová brána generuje účtovacie záznamy CDR, ktoré obsahujú informácie o používateľovi, ako jeho identitu IMSI, názov prístupového bodu, objem prenosu či dobu trvania spojenia. Pri účtovaní na základe dátového toku taktiež obsahujú názov účtovacieho pravidla, objem dát danej služby a dobu poskytovania danej služby.

Okamžitá fakturácia (*Hot Billing*)

Tento spôsob účtovania je špeciálnym typom offline účtovania. Účtovacia brána CG prioritne spracuje účtovacie záznamy CDR s príznakom okamžitej fakturácie. Funkcia účtovania okamžitou fakturáciou vyžaduje vysokú rýchlosť generovania účtovacích záznamov CDR.

Proces účtovania okamžitou fakturáciou:

1. Pri pripojení sa používateľa k paketovej sieti pomocou paketovej brány PDN-GW sa začnú generovať záznamy účtovania CDR.
2. Paketová brána a účtovacia brána CG si vymenia potrebné správy pre kontrolu spojenia.
3. Pri využívaní dátových služieb používateľom paketová brána zaznamenáva účtovacie údaje, ako sú objem prenesených dát či doba prenosu. Po ukončení podmienky pre účtovanie služby sa vygeneruje záznam CDR, ku ktorému sa pridá príznak účtovania okamžitou fakturáciou. Tento záznam CDR sa následne odošle účtovacej bráne CG.
4. Po ukončení spojenia používateľa sa vygeneruje posledný účtovací záznam CDR a odošle sa účtovacej bráne CG.

Výhodou účtovania okamžitou fakturáciou je zvýšenie rýchlosti generácie účtovacích záznamov CDR a zníženie rizika nepreplatených faktúr.

Základné účtovanie na základe dátového toku

Táto funkcia umožňuje aplikáciu rôznych tarif pre rôzne služby. Pri tomto spôsobe účtovania musí paketová brána PDN-GW analyzovať dátové toky aby bolo možné identifikovať jednotlivé typy poskytovaných služieb. Funkciu základného účtovania na základe dátového toku je možné použiť pri online aj offline účtovaní. Pri použití základného účtovania na základe dátového toku musí byť povolená funkcia online alebo offline účtovania.

Pri použití účtovania na základe dátového toku je v mobilných sieťach 4. generácie možné použiť iba záznamy o účtovaní paketovej brány PGW-CDR. Štatistiky o jednotlivých službách pri účtovaní na základe dátového toku sú uložené v týchto záznamoch. Súčasťou týchto záznamov je aj identifikátor služby SID (*Service ID*) a hodnotiaca skupina RG (*Rating Group*).

Pre možnosť účtovania na základe dátového toku musí byť v systéme aktivovaná funkcia na rozpoznávanie dátových tokov. Táto funkcia pracuje na 3., 4. a 7. vrstve OSI modelu a umožňuje paketovej bráne analyzovať dátové toky na základe účtovacích charakteristík definovaných pravidlami riadenia zásad a účtovania PCC.

Online účtovanie

Funkcia online účtovania umožňuje implementáciu účtovania v reálnom čase za využívanie prostriedkov paketovej siete. Pri pripojení používateľa k dátovej sieti systém online účtovania OCS určí, či je možné poskytnúť danému používateľovi služby na základe jeho účtovacích charakteristík a stavu prostriedkov na konte. Pri využívaní dátových služieb používateľom systém OCS monitoruje využívanie prostriedkov predplatených používateľom a upravuje ich stav na konte používateľa. V prípade vyčerpania prostriedkov je poskytovanie služieb zamedzené.

Online účtovanie implementuje funkcie prvku uplatňovania riadenia zásad a účtovania PCEF. Paketová brána PDN-GW komunikuje rozhraním Gy pomocou Diameter protokolu so systémom pre online účtovanie OCS, čím umožňuje vykonávanie online účtovania s kontrolou kreditu.

Účtovanie služieb na základe doby prenosu

Táto funkcia účtovania umožňuje účtovanie služieb používateľom na základe doby poskytovania danej služby. Pri aplikovaní tohoto spôsobu účtovania musí byť v systéme povolená funkcia rozlišovania poskytovaných služieb. Funkcia účtovania služieb na základe doby prenosu môže byť implementovaná pri online aj offline účtovaní.

- Pri online účtovaní paketová brána PDN-GW využíva reláciu kontroly kreditu na účtovanie poplatkov v reálnom čase. Paketová brána komunikuje so systémom pre online účtovanie OCS, ktorý rozhoduje o účtovaní na základe doby trvania prenosu.
- Pri offline účtovaní paketová brána odosiela účtovacie záznamy CDR účtovacej bráne CG. Účtovacie záznamy obsahujú informácie o dobe trvania prenosov. Účtovacia brána rozhoduje o účtovaní pre jednotlivé poskytované služby.

Prideľovanie zdrojov kreditu *Credit Pooling*

Pri online účtovaní kontrolou kreditu dochádza k rezervácií jednotiek, čo spôsobuje ich fragmentáciu. Pri aktivácií niektorej služby účastníkom, OCS rezervuje určitú časť prostriedkov na účte pre danú službu. Pri aktivácií viacerých služieb môže nastať situácia, že že aktivácia služby bude zamietnutá kvôli nedostatku prostriedkov na účte, aj keď nebudú vyčerpané, no budú rezervované prebiehajúcimi službami. Funkcia prideľovania zdrojov kreditu zamedzuje tejto fragmentácii pri online účtovaní viacerých služieb súčasne. Systém pre online účtovanie OCS priraďuje viacerým službám zdroj kreditu, pričom tento zdroj je medzi nimi navzájom zdieľaný.

Funkcia prideľovania zdrojov kreditu podporuje účtovanie na základe doby prenosu a objemu prenesených dát, no neumožňuje účtovanie na základe udalostí. Zdroj prideleného kreditu však nemôže byť zdieľaný medzi účtovaním na základe doby prenosu a objemu dát. Povolený je vždy iba jeden spôsob.

Účtovanie na základe typu udalosti

Funkcia účtovania na základe typu udalostí umožňuje účtovanie služieb používateľom na základe počtu využití daných služieb. Tento spôsob účtovania môže byť použitý pri online aj offline účtovaní.

Prvok UGW9811, ktorý vykonáva funkciu paketovej brány umožňuje účtovanie na základe typu udalosti pre tieto služby:

- HTTP (*HyperText Transfer Protocol*) - poskytovanie prístupu k obsahu webových stránok. Účtovanie je založené na počte prístupov k službe.
- RTSP (*Real Time Streaming Protocol*) - táto služba poskytuje prístup k multimediálnym dátovým tokom. Účtovanie sa nevykonáva na základe doby trvania prenosu či objemu prenesených dát ale na počte prístupov k službe.
- WAP (*Wireless Application Protocol*) - umožňuje prístup k jednoduchým webovým stránkam vytvoreným pre mobilné zariadenia. Účtuje sa počet pripojení k službe.
- MMS (*Multimedia Messaging Service*) - umožňuje prenos krátkych správ s multimediálnym obsahom. Účtovanie prebieha vzhľadom na počet použití služby.

5.3 Návrh implementácie funkcie účtovania

Prvok siete PCRF potrebný pre implementáciu účtovania zatiaľ nebol spoločnosťou HUAWEI dodaný do systému experimentálnej mobilnej siete UTKO FEKT VUT. Z dôvodu absencie samotného prvku PCRF a jeho technickej dokumentácie nebolo možné vytvoriť návrh implementácie účtovania do systému experimentálnej siete, preto tento návrh nie je súčasťou práce.

6 ZÁVER

V práci je popísaná a vysvetlená architektúra mobilných sietí štvrtej generácie. Vysvetľujú sa princípy a postupy pri vykonávaní riadenia zásad a kontroly účtovania. Popisuje sa problematika riešenia konfliktov pri zaisťovaní poskytovaných služieb.

Práca popisuje princípy zaisťovania bezpečnosti používateľa v sieti a ochrany siete pred prístupom neautorizovaných používateľov. Rieši sa prideľovanie dočasných identít a zamedzenie sledovania používateľa. Práca opisuje procesy pri autentizácii a autorizácii používateľa a vytvorení šifrovacích kľúčov pre komunikáciu. Súčasťou tejto časti práce je návrh implementácie autentizácie a autorizácie používateľov pri pokuse o prístup k sieti a detailný popis potrebných príkazov.

Práca zjednodušene vysvetľuje architektúru a fungovanie systému pre podporu multimediálnych služieb IMS. Tento systém umožňuje poskytovanie multimediálnych služieb v paketovo orientovaných sieťach.

V poslednej časti práce sú popísané postupy pri účtovaní v systéme mobilnej siete od spoločnosti HUAWEI. Keďže do systému experimentálnej mobilnej siete zatiaľ nebol dodaný prvok siete potrebný pre implementáciu účtovania a ani jeho technická dokumentácia, práca návrh implementácie účtovania neobsahuje. V práci sú však popísané všetky možnosti účtovania v takomto systéme.

LITERATÚRA

[1] 3GPP TS 23.002. *Technical Specification Group Services and System Aspects; Network architecture*. 8.7.0. 3GPP, 2010–12. Dostupné z URL: <http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-870.zip>.

[2] 3GPP TS 23.401. *LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*. 11.3.0. 3GPP, 2012–11. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/11.03.00_60/ts_123401v110300p.pdf>.

[3] 3GPP TS 23.203. *Policy and charging control architecture*. 13.1.0. 3GPP, 2014–09. Dostupné z URL: <http://www.3gpp.org/ftp/Specs/archive/23_series/23.203/23203-d10.zip>.

[4] 3GPP TS 23.228. *LTE; IP Multimedia Subsytem (IMS)*. 12.6.0. 3GPP, 2014–09. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/123200_123299/123228/12.06.00_60/ts_123228v120600p.pdf>.

[5] 3GPP TS 29.172. *LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol*. 9.9.0. 3GPP, 2012–01. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/129200_129299/129272/09.09.00_60/ts_129272v090900p.pdf>.

[6] 3GPP TS 33.102. *3G security; Security architecture*. 12.2.0. 3GPP, 2015–01. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/133100_133199/133102/12.02.00_60/ts_133102v120200p.pdf>.

[7] 3GPP TS 33.401. *LTE; 3GPP System Architecture Evolution (SAE); Security architecture*. 12.13.0. 3GPP, 2015–01. Dostupné z URL: <http://http://www.etsi.org/deliver/etsi_ts/133400_133499/133401/12.13.00_60/ts_133401v121300p.pdf>.

[8] 3GPP TS 32.251. *Telecommunication management; Charging management; Packet Switched (PS) domain charging*. 12.7.0. 3GPP, 2014–09. Dostupné z URL: <http://www.3gpp.org/ftp/Specs/archive/32_series/32.251/32251-c70.zip>.

[9] FIRMIN, Frédéric. *The Evolved Packet Core* [online]. [cit. 15. 11. 2014]. Dostupné z URL: <http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core>.

[10] FORSBERG, Dan; GÜNTHER, Horn; WOLF-DIETRICH, Moeller a VALTTERI, Niemi. *LTE Security*. Druhá edícia. Hoboken: John Wiley, 2013, 345s. ISBN 978-111-8355-589.

[11] HUAWEI. *Product Technical Specification: Experimentální LTE-EPC-IMS-WiFi síť UTKO FEKT VUT v Brně*. 2012–2014.

[12] NOHRBORG, Magdalena. *LTE* [online]. [cit. 15. 11. 2014]. Dostupné z URL: <http://www.3gpp.org/technologies/keywords-acronyms/98-lte>.

[13] WANNSTROM, Jeanette. *LTE-Advanced* [online]. 2013, [cit. 15. 11. 2014]. Dostupné z URL: <http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced>.

[14] POOLE, Ian. *IMS architecture* [online]. [cit. 2. 12. 2014]. Dostupné z URL: <http://http://www.radio-electronics.com/info/telecommunications_networks/ims-ip-multimedia-subsystem/ims-architecture.php>.

[15] ROSENBERG, J.; SCHULZRINNE, H.; CAMARILLO, G.; ai. *RFC 3261 - SIP: Session Initiation Protocol (SIP)*. Technická správa, Internet Engineering Task Force, 2002.

ZOZNAM SKRATIEK

3GPP	projekt, ktorý spája organizácie zaoberajúce sa vývojom štandardov v telekomunikáciách – The 3rd Generation Partnership Project
ADC	funkcia, ktorá detekuje dátové toky aplikácií a vykonáva ich riadenie– Application Detection and Control
AF	prvok, ktorý vykonáva dynamickú kontrolu pravidiel riadenia zásad – Application Function
AKA	proces autentizácie používateľa a zostavenia kľúča – Authentication and Key Agreement
AMF	pole v autentizačnom tokene, ktorý informuje o počte autentizačných vektorov – Authentication Management Field
APN	názov prístupového bodu – Access Point Name
ARP	parameter QoS, obsahuje informácie o úrovni priority – Allocation and Retention Priority
AUTN	autentizačný token – Authentication Token
CK	šifrovací kľúč – Ciphering Key
BGCF	prvok v architektúre IMS, ktorý rozhoduje o pripojení k verejným telefónnym sieťam – Breakout Gateway Control Function
CDR	záznamy o účtovaní – Charging Data Records
CG	účtovacia brána, implementuje offline účtovanie – Charging Gateway
CSCF	prvok systému IMS, ktorý riadi komunikačné relácie – Call Session Control Function
DeNode B	základňová stanica eNode B, ku ktorej sú rádiovým rozhraním pripojené Relay Nodes – Donor eNode B
eNode B	inteligentná základňová stanica prístupovej siete – Evolved Node B
EPC	dátové jadro mobilných sietí – Evolved Packet Core
EPS	mobilná sieť pracujúca na princípe prepínania paketov – Evolved Packet System

ERF	funkcia, ktorá má za úlohu vykonávať detekciu spúšťacích udalostí – Event Reporting Fuction
E-UTRAN	rádiová sieť slúžiaca na pripojenie mobilných zariadení – Envolved Universal Terrestrial Radio Access Network
FBC	účtovanie na základe dátového toku – Flow Based Charging
GBR	určuje garantovanú šírka pásma pre danú službu – Guaranteed Bit Rate
GGSN	hraničné zariadenie medzi sieťou GPRS a vonkajšou paketovou sieťou – Gateway GPRS Support Node
GSM	štandard vyvinutý pre mobilné digitálne siete 2. generácie – Global System for Mobile Communications
GUTI	dočasná identifikácia používateľa – Globally Unique Temporary Identity
HE	umožňuje používateľovi previesť svoje poskytované služby do iných sietí – Home Environment
HSS	obsahuje databázu informácii o účastníkoch v sieti – Home Subscriber System
HTTP	zabezpečuje prenos obsahu webových stránok – HyperText Transfer Protocol
I-CSCF	kontrolný prvok pre zariadenia, ktoré spravujú stav relácií – Interrogating Call Session Control Function
IETF	organizácia, ktorá vytvára a podporuje internetové štandardy – Internet Engineering Task Force
iFC	špecifikujú počiatočné filtrovacie kritéria pri poskytovaní služieb – Initial Filter Criteria
IK	kľúč integrity – Integrity Key
IMS	systém využívajúci paketovo orientované siete na prenos multimediálnych služieb – IP Multimedia Subsystem
IMSI	jedinečné číslo pridelené operátorom, ktoré slúži na identifikáciu používateľa – International Mobile Subscriber Identity

IP	komunikačný protokol pracujúci na sieťovej vrstve ISO modelu – Internet Protocol
IP-CAN	transportná sieť na nižšej úrovni, ktorá zabezpečuje konektivitu pomocou IP protokolu– IP Connectivity Access Network
ITU	medzinárodná organizácia, ktorá je súčasťou OSN a má na starosti rozvoj a spoluprácu krajín v oblasti telekomunikácií – International Telecommunication Union
KDF	funkcia derivácie kľúča pomocou ktorej HSS vypočíta autentizačný vektor – Key Derivation Function
LAI	identifikátor slúžiaci na určenie polohy používateľov – Location Area Identification
LTE	prístupová časť dátovej siete – The Long Term Evolution of UMTS
MAA	odpoveď na žiadosť o autentizáciu multimédií – Multimedia Authentication Answer
MAC	protokol zabezpečujúci fyzické adresovanie na spojovej (linkovej) vrstve ISO modelu – Media Access Control
MAR	žiadosť o autentizáciu multimédií – Multimedia Authentication Request
MGCF	riadi SIP signalizáciu a distribúciu relácií cez viacero brán – Media Gateway Control Function
MIMO	priestorový multiplex využívajúci prenos pomocou viacerých vysielačov a prijímačov – Multiple In Multiple Out
MME	prvok správy mobility, zabezpečuje riadenie komunikácie – Mobility Management Entity
MMS	umožňuje prenos krátkych správ s multimediálnym obsahom – Multimedia Messaging Service
OCS	zabezpečuje účtovanie v reálnom čase– Online Charging System
OFCS	zabezpečuje offline účtovanie – Offline Charging System
OFDMA	metóda kódovania dát na niekoľko nosných frekvencií – Orthogonal Frequency Division Multiple Access

OSI	vrstvový model štruktúry komunikačných dátových sietí – Open Systems Interconnection
PCC	súbor pravidiel riadenia zásad a kontroly účtovania – Policy and Charging Control
PCEF	súčasť PDN-GW, prvok vykonávania riadenia zásad a kontroly účtovania – Policy and Charging Enforcement Function
PCRF	prvok dozerajúci na kontrolu pravidiel riadenia zásad a kontroly účtovania – Policy and Charging Rules Function
P-CSCF	zasiela SIP správy, podieľa sa na podpore QoS – Proxy Call Session Control Function
PDB	určuje hornú hranicu času pri možnom oneskorení paketov – Packet Delay Budget
PDN-GW	smerovač medzi EPC a vonkajšími paketovými sieťami – Packet Data Network Gateway
PLMN	sieť, ktorá je spravovaná jedným operátorom – Public Land Mobile Network
PSTN	verejná telefónna sieť – Public Switched Telephone Network
QCI	identifikátor, ktorý prideľuje váhy jednotlivým paketom pri riadení kvality služieb – QoS Class Identifier
QoS	zabezpečuje poskytovanie rôznych priorít pre jednotlivé služby – Quality of Service
RAI	identifikátor LAI doplnený o kód smerovacej oblasti – Routing Area Identification
RAND	128 bitové pole náhodných čísiel využívané v autentifikačných a šifrovacích procesoch – Random Challenge
RCAF	prvok, ktorý zasiela informácie o stave spojenia používateľov prvku PCRF – RAN Congestion Awareness Function
RES	hodnota získaná od koncového zariadenia, ktorá sa porovnáva s očakávanou hodnotou pri autentizácii – Response
RG	hodnotiaca skupina v záznamoch o účtovaní – Rating Group

RN	základňové stanice, ktoré slúžia na rozšírenie pokrytia – Relay Nodes
RTSP	zabezpečuje prenos multimediálneho obsahu v reálnom čase – Real Time Streaming Protocol
RUCI	nesie informácie o indikácii zahltenia jednotlivých používateľov – RAN User Plane Congestion Information
SAA	žiadosť o pridelenie servera – Server Assignment Answer
SAE-GW	zabezpečuje prenos užívateľských dát – System Architecture Evolution Gateway
SAR	odpoveď na žiadosť o pridelenie servera – Server Assignment Request
S-CSCF	kontrolný prvok, spravuje relácie v IMS – Server Call Session Control Function
SCTP	slúži na prenos signalizačných údajov – Stream Control Transmission Protocol
SGSN	podporuje dátové prenosy v sieti druhej generácie – Serving GPRS Support Node
S-GW	spravuje dátové toky – Service Gateway
SID	identifikátor služby – Service ID
SIP	signalizačný protokol, používaný na kontrolu multimediálnych komunikačných relácií v IP sieťach – Session Initiation Protocol
SIP-AS	platforma, na ktorej sú nasadené multimediálne služby poskytované v sieti – Session Initiation Protocol Application Server
SNR	vyjadruje odstup signálu od šumu – Signal to Noise Ratio
SPR	zaznamenáva o užívateľoch informácie, ktoré sú potrebné na vykonávanie rozhodnutí o PCC – Subscription Profile Repository
S – TMSI	skrátená verzia dočasnej identity používateľa – S – Temporary Mobile Subscriber Identity
TDF	vykonáva detekciu dátových tokov a podáva informácie o aplikáciach a službách prvku PCRF – Traffic Detection Function
TMSI	dočasná identita používateľa používaná na rádiovej prístupovej sieti – Temporary Mobile Subscriber Identity

UAA	odpoveď na žiadosť o autorizáciu používateľa – User Authorization Answer
UAR	žiadosť o autorizáciu používateľa – User Authorization Request
UDA	odpoveď na žiadosť o údaje o používateľovi – User Data Answer
UDR	žiadosť o údaje o používateľovi – User Data Request
UE	koncové zariadenia v sieti – User Equipment
UMTS	mobilná sieť 3. generácie – Universal Mobile Terrestrial System
UPCC	označenie prvku PCRF v systéme od spoločnosti HUAWEI – Unified Policy and Charging Controller
USIM	modul, ktorý umožňuje komunikáciu v UMTS sieťach – Universal Subscriber Identity Module
VLR	databáza používateľov, ktorí boli pripojení k danej oblasti – Visited Location Register
WAP	umožňuje prenos jednoduchých mobilných stránok určených pre mobilné zariadenia – Wireless Application Protocol
XRES	hodnota, ktorú sieť očakáva na overenie autentizácie – Expected Response