Mobilní sítě
a jejich bezpečnost

L. Dostálek

Název: Mobilní sítě a jejich bezpečnost
Autor: Libor Dostálek
Obálka: Martina Hegerová

Vydal: Ústav aplikované informatiky,
Přírodovědecká fakulta Jihočeské univerzity v Českých Budějovicích
Vydáno v koedici s: Katedra informatiky a výpočetní techniky,
Fakulta aplikovaných věd Západočeské univerzity v Plzní

Rok a měsíc vydání: 2016/11
Formát: PDF
Vydání: první
Forma: elektronická, CD
Náklad CD: 500
on-line adresa: http://uai.prf.jcu.cz

ISBN 978-80-7394-606-7

1. Pár poznámek na úvod

Doba Velkých průvodců TCP/IP a PKI je již dávno pryč. I když mnohé z těchto textů by byly i dnes užitečné např. pro výuku, tak jsou ztraceny, protože jsou uzamčeny v tištěných publikacích, které dnes již téměř nikdo nečte, alespoň pokud se týká „počítačové“ literatury. To je i důvod, proč jsem si myslel, že už žádný rozsáhlejší text nevytvořím. Jenže nakonec mi to nedalo. Nedalo mi to proto, že jsem sám musel proniknout do světa mobilních sítí, které jsou postaveny na bázi protokolů TCP/IP. Na první pohled mi připadalo, že přece, když mám s protokoly TCP/IP dvacetiletou zkušenost, tak to nebude nic obtížného. Jak jsem se ale hluboce mýlil! Musel jsem začít studovat standardy pěkně od počátku. Musel jsem si začít psát poznámky, až z toho vznikla tato monografie. Bezděky tak vycházím z předpokladu, že laskavý čtenář má jisté základy TCP/IP a PKI – například v rozsahu již zmíněných Velkých průvodců [1], [2] a [3].

Před časem jsem v Českém rozhlase zaslechl rozhovor, jeho obsah není až tak podstatný, zajímavý byl ale povzdech „že ti mladí těm mobilům tak dobře rozumí“. Nedalo mi to, a na přenášce jsem se zeptal studentů, jestli znají nějaké protokoly, které se využívají pro mobilní komunikaci. Nechápali, proč by se tím měli vůbec zatěžovat, když ten mobil přece funguje. Kdežto TCP/IP je zajímá, protože počítač jim ne vždy jde připojit na internet a musí se zabývat jeho konfigurací.

Laskavému čtenáři se omlouvám, že se mi nepodařilo získat nějaký grant nebo jiné prostředky pro sazbu tohoto českého textu. Zdůvodnění mne vždy pobavilo: prý problematiku mobilních sítí není třeba podporovat z akademických peněz, je to technologie, která v Česku nemůže zajímat téměř nikoho. Konec konců ty boxy, které to zajišťují, se kupují v Číně, a když se pokazí, tak není problém koupit nový. I vzpomněl jsem si, že před mnoha a mnoha lety Československá socialistická republika vyvezla do nejmenované „rozvojové země“ traktory. Export neobsahoval žádnou opravárenskou podporu (tehdy si u nás každý opravoval traktor sám), takže pokud traktory jezdily, tak se používaly. Když přestaly jezdit, tak je odstavili a případně použily jako druhotnou surovinu pro výrobu ručních nástrojů. Tehdy jsem byl kluk a byl jsem pyšný, že my těm traktorům rozumíme. Co si asi o nás dnešní kluci v Číně myslí…

Publikace vychází v elektronické formě. Formát A4 mi připadal pro čtení na obrazovce příliš nepraktický, protože se mi zpravidla nevešla celá stránka na obrazovku. Na druhé straně jsem si říkal, že někdo si bude chtít publikaci vytisknout na běžné barevné tiskárně a svázat, tak jsem ponechal hru na sudé a liché stránky, která se používá u tištěných publikací. Při tisku na formát A4 je třeba si před vazbou nechat publikaci oříznout podle první stránky obálky.

2. Obsah

1. PÁR POZNÁMEK NA ÚVOD 3

2. OBSAH 5

3. PŘEDMLUVA 11

3.1 SÍŤOVÁ NEUTRALITA 11
3.2 REGULACE 11
3.3 KARTY 12
3.4 APLIKACE 13
3.5 ZÁKAZNICKÝ TEST 13

4. JEMNÝ ÚVOD DO MOBILNÍCH SÍTÍ 15

4.1 BUŇKY A GENERACE MOBILNÍCH SÍTÍ 16
4.2 SÍŤ OPERÁTORA JE STAVEBNICÍ 20
4.3 EPC 21
4.4 IMS 24
4.5 VEŘEJNÁ A PRIVÁTNÍ IDENTITA, IMPI A IMPU 28
4.6 DALŠÍ POUŽÍVANÉ IDENTIFIKÁTORY 30
4.7 ISIM/USIM 31
4.8 MMI 33
4.9 ZMÁČKNI A MLUV 34
4.10 5G 34

5. ROAMING 35

5.1.1 IPX 35
5.1.2 LTE roaming 35
5.1.3 VoLTE Roaming 36

6. AKA MECHANISMUS 39

6.1 FUNKCE ČIPOVÉ KARTY 42

7. EPS 43

7.1 REFERENČNÍ BOD UU 45
7.1.1 Logické kanály 47
7.1.2 Transportní kanály 47
7.1.3 Fyzické kanály 48
7.2 ÚVODNÍ PŘIHLÁŠENÍ DO SÍTĚ 50

7.3 NAS ... 52
7.3.1 EMM ... 52
7.3.2 ESM ... 53
7.4 GTP ... 54
7.5 Odvozování kryptografických klíčů ... 56
7.6 Šifrování dat mezi zařízením účastníka a eNB ... 57
7.7 Integrita dat mezi zařízením účastníka a eNB ... 58
7.8 Útoky ... 59

8. DIAMETER ... 61

8.1 Architektura protokolu Diameter ... 62
8.2 Formát zprávy ... 65
8.3 Agenti ... 69
8.3.1 Relay Agent ... 70
8.3.2 Proxy Agent ... 70
8.3.3 Redirect Agent ... 71
8.3.4 Translation Agent ... 71
8.3.5 Routing Agent ... 72
8.3.6 Edge Agent ... 73
8.4 Doména ... 74
8.5 Diameter Peer Discovery ... 75
8.6 Směrování ... 76
8.6.1 Tabulka sousedů ... 76
8.6.2 Směrovací tabulka ... 77
8.6.3 DNS směrování ... 77
8.7 Dialog protokolu Diameter ... 79
8.7.1 Dialog mezi dvěma entitami protokolu Diameter ... 79
8.7.2 Dialog zpracovávající požadavky účastníků ... 82
8.8 NAS ... 82
8.9 Účtování ... 83
8.10 Credit Control ... 85
8.11 Referenční body protokolu Diameter specifikované 3GPP ... 85
8.11.1 Gx (PCEF-PCRF) ... 88
8.11.2 S6a a S6d (MME/SGSN – HSS) ... 89
8.11.3 S13 a S13' (MME/SGSN – EIR) ... 91
8.11.4 Sd (TDF-PCRF) ... 91
8.11.5 Gxx (PCRF – SGW) ... 92
8.11.6 S9 (PCRF - PCRF) ... 93

8.11.7 Rx (AF – PCRF) ... 94
8.11.8 Cx (HSS - I-CSCF/S-CSCF) ... 95
8.11.9 Sh (HSS - AF) ... 96
8.11.10 Zh a Zn (HSS - AF) ... 96
8.11.11 Sy (PCRF – OCS) ... 98
8.11.12 SGd (MME - SMS brána) ... 99
8.11.13 Gy/Ro (Online Charging) ... 99
8.11.14 Rf (Offline Charging) ... 99
8.12 ZABEZPEČENÍ ... 99

9. SIP ... 101

9.1 SBC ... 104
9.1.1 Více rozhraní SBC ... 105
9.2 PAKET (ZPRÁVA) PROTOKOLU SIP ... 106
9.2.1 SIP URI, TEL URI a nouzová volání ... 108
9.2.2 Formát zprávy protokolu SIP ... 110
9.3 LOKALIZACE ... 128
9.4 UDÁLOSTI ... 129
9.5 SIP DIALOGY ... 130
9.5.1 Registrace a odhlášení ... 130
9.5.2 Autentizace ... 131
9.5.3 3GPP registrace s autentizací digest ... 132
9.5.4 INVITE ... 133
9.5.5 3GPP INVITE ... 137
9.5.6 Upsání se ... 138
9.5.7 REFER ... 138
9.6 PROTOKOLY NIŽŠÍCH VRSTEV ... 139
9.7 SIP ZABEZPEČENÍ ... 139
9.7.1 3GPP sítě ... 139
9.8 DNS ... 141
9.8.1 Záznam NAPTR ... 141
9.8.2 DNS ENUM ... 142
9.8.3 Překlad SIP URI ... 143
9.9 ÚTOKY PROTI SIP ... 143

10. SDP ... 149

10.1 BEZPEČNOST SDP ... 156

11. ZASÍLÁNÍ ZPRÁV V LTE A IMS 157

11.1 SIP PAGING (OBECNĚ) 158
11.2 SMS PŘES IP 158

12. MSRP 161

12.1 SRP URI 164
12.2 ÚTOKY 164

13. H.248 165

13.1 KONTEXT 167
13.2 UKONČENÍ 167
13.1 PŘÍKAZY 168
13.2 REFERENČNÍ BODY IMS 169
13.2.1 Iq a Mc 169
13.2.2 Ix 171
13.2.3 Mn 171
13.2.4 Mp 172

14. RTP/RTCP 175

14.1 RTP 175
14.2 RTCP 178
14.3 SRTP 182
14.4 SRTCP 183
14.5 BEZPEČNOST V 3GPP SÍTÍCH 183
14.6 ÚTOKY NA RTP 184

15. PHOTURIS 185

16. DTLS 186

17. SCTP 189

17.1 ASOCIACE 191
17.2 VLÁKNO (*CHUNK*) 192
17.3 MULTI- STRAMING 192
17.4 MULTI-HOMING 193
17.5 ZACHOVÁNÍ HRANIC ZPRÁV 194
17.6 OCHRANA PROTI DOS, COOKIE 194
17.7 AUTENTIZACE VLÁKEN 195
17.8 DTLS A SCTP 195

18. ČIPOVÉ KARTY 197

18.1 KONTAKTY ČIPOVÉ KARTY 200
18.2 LOGICKÉ SCHÉMA ČIPOVÉ KARTY 200
18.3 TERMINÁLY 202
18.4 ATR 203
18.5 APDU 203
18.6 USB 205
18.7 SWP 206
18.8 EMULACE ETHERNETU 206
18.9 BIP 207
18.10 WEBOVÝ SERVER 207
18.11 ZABEZPEČENÍ KOMUNIKACE S ČIPOVOU KARTOU 207
18.12 STRUKTURA DAT ULOŽENÝCH V KARTĚ 208
18.13 PERSONALIZACE A DE-PERSONALIZACE 209
18.14 ŘÍZENÍ PŘÍSTUPU 210
18.15 OTA 212
18.16 ARCHITEKTURA KARET PODLE GLOBALPLATFOM 213
18.17 REE A TEE 214
18.18 SE 215
18.18.1 Řízení přístupu aplikací 215
18.18.2 Přístup jednotlivých důvěryhodných aplikací 216
18.19 UICC 216
18.19.1 EAP 217
18.19.2 NFC 218
18.20 USIM 218
18.21 ISIM 228
18.22 EMBEDDED UICC, ESE 230

19. OBECNÁ AUTENTIZAČNÍ ARCHITEKTURA 233

19.1 REFERENČNÍ BODY 234
19.1.1 Referenční bod Ub 234
19.1.2 Referenční bod Ua 234
19.1.3 Referenční bod Zh 234
19.1.4 Referenční bod Zn 235
19.2 MECHANISMUS GBA 235
19.2.1 První fáze (autentizace vůči BSF) 237
19.2.2 Druhá fáze (Přihlášení se na web) 237

19.3 CERTIFIKAČNÍ AUTORITA 237
19.4 REFERENČNÍ BOD UT 237

20. AUTENTIZACE JEŠTĚ OBECNĚJI 241

20.1 METODY AUTENTIZACE 241
20.1.1 Kategorie „Něco ví“ 242
20.1.2 Kategorie „Něco má“ 244
20.1.3 Kategorie „Něčím je“ 245
20.2 VÍCE FAKTOROVÁ AUTENTIZACE 246
20.3 FEDERACE IDENTIT 247
20.3.1 SAML 248
20.3.2 JWT 250
20.3.3 OAuth 2.0 250
20.4 RBAC MODEL 250
20.5 OPENID CONNECT 250
20.6 AUTORIZACE 251

21. PROBLÉM AUTENTIZACE V PRAXI 253

21.1 DRUHÝ AUTENTIZAČNÍ FAKTOR 254
21.2 CÍL 255

22. POZNÁMKA K LEGÁLNÍMU ODPOSLECHU 257

23. CITOVANÁ LITERATURA 261

24. REJSTŘÍK 273

25. PŘEHLED ZKRATEK 281

3. Předmluva

Tento text se zabývá 4G i přesto, že někde za obzorem se již rýsuje 5G. Je třeba si uvědomit, že označení 4G či 5G se týkají zejména poslední míle mobilního spojení. Avšak infrastruktura mobilní sítě se skládá z mnoha dalších částí, které jsou zpravidla využívány několika generacemi. Navíc problematika poslední míle (LTE) byla do textu vložena spíše pro úplnost.

3.1 Síťová neutralita

Na internetu máme poskytovatele připojení a poskytovatele obsahu. V prvopočátcích internetu si poskytovatelé připojení představovali, že budou poskytovat i obsah. Ukázalo se, že švec se má držet svého kopyta. Bouřlivý rozvoj poskytování obsahu nastal až tehdy, když vznikli samostatní poskytovatelé obsahu. Uplynul nějaký čas a business se pomalu přesunul od poskytování připojení k poskytování obsahu. Dnes je poskytování připojení vcelku chudý business. Nedivme se proto, že poskytovatelé připojení dostali chuť si sáhnout na měšec poskytovatelů obsahu – vznikl tak termín dvojrychlostní internet. Myšlenkou bylo, že by poskytovatelé připojení za poplatek upřednostňovali některé poskytovatele obsahu. Proti tomu se zvedla vlna nevole a byla legislativně zavedena tzv. síťová neutralita, která zakazuje na internetu upřednostňovat kohokoliv.

Zajímavé je, že již 3G a 4G sítě umožňují dvojrychlostní připojení, protože z podstaty věci plyne, že pro multimediální tok („hovor“) musí být garantována šíře pásma, jinak by nebylo možné plně nahradit sítě na bázi přepínaných okruhů sítěmi paketovými. Je jen na poskytovatelích, aby jej vhodným způsobem využili. Dnes má totiž drtivá většina mobilních zařízení minimálně dvě síťová rozhraní – tzv. APN (viz obr. 4.6). Jedno do internetu a to druhé do sítě IMS. Rozhraní do IMS ve 4G zajišťuje „aby to telefonovalo“, toto rozhraní musí poskytovat nejenom garantované šíře pásma (QoS), ale musí umiňovat dokonce i upřednostňovat hovory záchranných složek v případě živelných pohrom, kdy je síť z pochopitelných důvodů přetížená. Nic tedy poskytovatelům nebrání, aby zvýhodňované služby neposkytovali jako služby internetu, ale jako IMS aplikace (přes *„dedicated bearer“* – kap. 4.2).

3.2 Regulace

Telekomunikace byly ještě vcelku nedávno záležitostí státu. Spadaly pod různá ministerstva pošt a telekomunikací. Byl to úřad. V každé obci měl nějakou nemovitost, kde nejdříve byla manuální obsluha, pak automatizovaná obsluha okolního území. Jenže dnes, pokud neuvažujeme základnové stanice a jejich spojení s jádrem, protože to může být outsoursováno pro více operátorů, tak se celá technologie sítě (tj. jádra sítě) vejde do několika málo skříní *(rack mount)*. Pochopitelně, z důvodu vysoké dostupnosti se technologie zdvojuje či ztrojuje do více geograficky vzdálených lokalit.

Konkurence mezi telekomunikačními operátory nám přinesla snižování cen za poskytované služby. Jenže za jakou cenu? Problém je v tom, že telekomunikační operátoři jsou akciové společnosti. Akciové společnosti jsou řízeny orgány, které hájí zájmy akcionářů. Akcionáři nemají přímý vhled do společností řízení společnosti

posuzují podle indikátorů, kterými je kromě vcelku logického zisku zejména podíl na trhu. Podíl na trhu lze měřit např. počtem aktivovaných SIM/USIM karet. Obchodníci vymýšlí různé triky, jak aktivovat více SIM/USIM karet. Už docílili, že počet aktivovaných SIM/USIM karet přesáhl počet obyvatelů. Avšak největší obchodní pákou zůstává cena, takže se snažili získávat nové a nové aktivované SIM/USIM karty nabídkou nižší a nižší ceny. Snižování cen má ale svou hranici, kterou je výše nákladů na poskytované služby. Obchodníci stále měli potřebu snižovat ceny, ale už nebylo kam, tak relativně zvyšovali ceny za roaming, což vadilo jen zlomku zákazníků. Jenže vysoká cena roamingu začala bránit rozvoji společného evropského trhu. Takže se nelze divit, že Evropská komise sáhla k regulaci cen za roaming. Najednou začali mít někteří telekomunikační operátoři potíže, místo, aby se reformovali, tak začaly hledat různé mantry jako dvojrychlostní internet. Místo toho, aby se začali snižovat své náklady – začali se restrukturovat

Dnešní vysoké náklady telekomunikačních operátorů jsou dány zejména tím, že se pokouší zajišťovat vše – od stožárů základnových stanic, přes základnové stanice, spojení základnových stanic s jádrem sítě, jádra sítí, vlastní telekomunikační služby, až po obchod s mobilními zařízeními. Jenže automobilky také nevyrábí pneumatiky či kličky k oknům – mají na to subdodavatelé, kteří se specializují na dílčí součástky, které pak, pokud jsou úspěšní, dodávají i více automobilkám. Stožáry základnový stanic, základnové stanice, propojení základnových stanic s jádrem sítě, jádro sítě atd. mohou dodávat specializovaní subdodavatelé, kteří pokrývají rozsáhlá území Evropské unie a samotní poskytovatelé se mohou věnovat svému businessu svým zákazníkům. Operátor může být jen virtuální, tj. dnes mu stačí, kromě ekonomických systémů, databáze zákazníků *(Customer relationship management - CRM)* a konektor na HSS *(Home Subscriber Server)* poskytovatele jádra sítě. Optimalizace se dosáhne tím, že jednotlivé technologie (např. jádro sítě) bude pokrývat více operátorů – tj. velké množství uživatelů – rozhodně více než je obyvatel ČR.

3.3 Karty

Velký úspěch mobilních technologií přišel s 2G (tj. s GSM). GSM přišlo s revoluční myšlenkou: mobilní zařízení se skládá ze dvou částí: z vlastního zařízení a SIM karty, která obsahovala osobní aktiva uživatele, která sloužila k přihlášení uživatele do sítě. Při výměně (opravě atp.) zařízení stačilo vyjmout kartu ze zařízení a vložit ji do nového zařízení a uživatel mohl mobilní síť využívat dále. Čím se mobilní zařízení začalo přibližovat osobnímu počítači, tak vznikla otázka, kam ukládat uživatelova data. Objevila se SD karta. Myšlenkou bylo, že osobní aktiva budou na SIM kartě a osobní data na SD kartě. Při výměně zařízení se vyjmou obě karty a vloží do nového zařízení. Jenže z nejrůznějších marketingových důvodů byli uživatelé přesvědčování, aby si ukládali osobní data (někdy i osobní aktiva) na lokální úložiště mobilního telefonu. Důsledkem je, že starý mobil se rozumní lidé bojí prodat nebo i dát do opravy. Když si dáte spravit peněženku, tak tam také nenecháte platební karetu. Zajímavé je, že v notebooku jsou disky stále vyjímatelné, i když se už mechanické disky prakticky nepoužívají.

Jestliže je čipová karta USIM/ISIM (viz kap. 4.7) určena pro uložení osobních aktiv, tak je jen otázkou, proč na ni neuložit platební kartu. Řešení se označuje jako „emulace platební karty USIM/ISIM kartou“. Řešení je technicky připravené – mobilní zařízení pak s terminálem obchodníka nekomunikuje přes mobilní síť, ale přímo protokolem NFC (kap. 18.19.2). Avšak nedávno jsem četl titulek v novinách „další bance se podařilo implementovat karetní operace na mobilu bez účasti operátora mobilní sítě, tj. bez uložení kryptografického materiálu platební karty na USIM/ISIM kartu“. Problém totiž není v tom, že nemáme technické řešení, že bychom na to neměli standardy atd. Problém je v tom, že zatím se nikdo příliš nepokoušel vymyslet business case, který by přinášel profit všem stranám. Business platebních karet je rozdělen mezi banku a karetní společnost. Tj. není tam místo pro mobilního operátora, takže ten není motivován takové služby zavádět.

Mobilní operátoři jsou motivování množstvím aktivovaných USIM karet. Jejich cílem je jich aktivovat co nejvíce. Vznikají tak kuriózní technická řešení jako mobilní zařízení podporující více USIM karet současně. To už je jen krůček k eUSIM kartám, kdy v mobilním zařízení je kryptografický modul ve kterém může být kryptografický materiál odpovídající řadě USIM karet. Marketing mobilních operátorů jásá a uživatel si stejně už zvykl osobní data neukládat na SD kartu, ale do lokálního úložiště mobilního zařízení, tak si zvykne i osobní aktiva ukládat do nevyjímatelného modulu mobilního zařízení. Co naplat, že eUSIM vznikl pro mobilní zrazení, která jsou součástí technologie – nikoliv pro komunikaci uživatelů. Např. pro vestavění do automobilu, který v případě havárie, informuje záchranné složky o vzniklé události (záchranné složky lze pochopitelně „volat“ i bez USIM karty).

3.4 Aplikace

V současné době, když se vysloví slovo aplikace v souvislosti s mobilními telefony, tak si každý představí tzv. mobilní aplikaci. Z pohledu osobních počítačů se jedná o „tlustého klienta“, kterého si uživatele stahují zpravidla z *up store* dodavatele operačního systému mobilního zařízení. Pro operátora mobilní sítě z tohoto businessu mohou kapat nějaké drobné.

V této publikaci pod slovem aplikace budeme rozumět „serverovou“ aplikaci umístěnou v síti (jádře) IMS. Zde budou moci poskytovatelé obsahu rozvíjet svůj business. Poskytovatelům obsahu to přinese několik výhod:

- Nejedná se o poskytování služeb přes Internet, proto mohou využívat garantovanou šíři pásma.
- Provozovatelé aplikací mohou být více chráněni proti útokům z internetu (jedná se něco jako „intranet lite“).
- Uživatelé se mohou autentizovat pomocí USIM/ISIM karty, atd.

3.5 Zákaznický test

V letošním roce se nasazuje *VoLTE (Voice over LTE)*. Docela jsem byl zvědavý, jaké jsou s tím zákaznické zkušenosti, jak se s tím vypořádali jednotliví výrobci mobilních zařízení. Když jsem

zaslechl, že zákaznický časopis dTest vydává číslo 5/2016 obsahující testování mobilních zařízení, tak jsem si jej docela komplikovaně obstaral. Byl tam výsledek testů mnoha mobilních zařízení. Byly porovnávány nejrůznější displeje, fotoaparáty – prostě vše. Jen jediná drobnost tam chyběla – nebylo tam testováno, jestli mobilní telefon vůbec telefonuje přes LTE.

4. Jemný úvod do mobilních sítí

Od počátku používání telefonu až po digitální síť GSM (2.generace mobilních sítí) se na dobu hovoru sestavoval okruh mezi volajícím a volaným. Okruh byl nejprve sestavován manuálně operátory telefonních ústředen, později byl sestavován mechanicky a nakonec elektronicky.

Zpočátku se hlasový signál moduloval analogově do sestaveného okruhu, později byl hlasový signál vzorkován a vzorky okruhem přenášeny datovými pakety. Pokud bylo třeba v těchto sítích přenášet data, pak se modulovala/demodulovala pomocí zařízení nazývaného modem do sestaveného okruhu, který byl prvotně určen pro přenos hlasu.

S příchodem 4. generace mobilních sítí se situace obrátila. Od sestavování okruhů se upustilo a vše se přenáší pomocí datových paketů rodiny protokolů TCP/IP. Zatímco 3. generace mobilních sítí se víceméně využívala pro připojení k Internetu (pro hlasové služby se souběžně využíval GSM). 4. generace přináší již takové přenosové rychlosti, že i hlasové služby je možné realizovat pomocí paketů protokolů TCP/IP, tj. bez využití přenosových okruhů.

V rodině protokolů TCP/IP se nejenom hlasové služby, ale obecně multimediální služby, implementují pomocí skupiny protokolů, z nichž nejtypičtějšími reprezentanty jsou SIP a RTP. Hlasové (resp. multimediální) služby na internetu realizované těmito protokoly se označují jako *Voice over IP* nebo zkráceně VoIP.

Čtvrtá generace mobilních sítí používá pro poslední míli mezi mobilním zařízením a sítí standard LTE. Hlasové (multimediální) služby jsou pak implementovány rovněž za využití rodiny protokolů TCP/IP (SIP, RTP apod.). Tuto komunikaci pak označujeme jako *Voice over LTE* nebo zkráceně VoLTE.

VoLTE je tedy implantováno stejnými protokoly jako VoIP. Přesto se bráním tvrzením typu: „VoLTE je v podstatě zvláštním případem VoIP“. Obojí sice vychází ze standardů RFC, ale VoLTE tyto standardy často rozšiřuje o svá specifika, některé oblasti řeší standardy 3GPP. Rozdíl je také z pohledu bezpečnosti. Zatímco účastníci VoIP jsou nejčastěji obecnými účastníky internetu, kteří se zpravidla autentizují jménem a heslem, tak účastníci LTE jsou v rámci konkrétního poskytovatele chráněnou skupinou a pro autentizaci zpravidla používají čipovou kartu USIM/ISIM.

Místo „hlasové služby“ je dnes moderní používat termín „multimediální služby“. Je tím míněno, že kromě klasických „hovoru“ je běžné implementovat např. „video hovory“, „videokonference“ apod. Je třeba ale poznamenat, že toto je jen malý výsek multimediálních možností. Někdy budu nadále používat slovo „hovor“ s mínit tím „multimediální služby“, protože mi připadá, že je pak text pro laskavého čtenáře srozumitelnější.

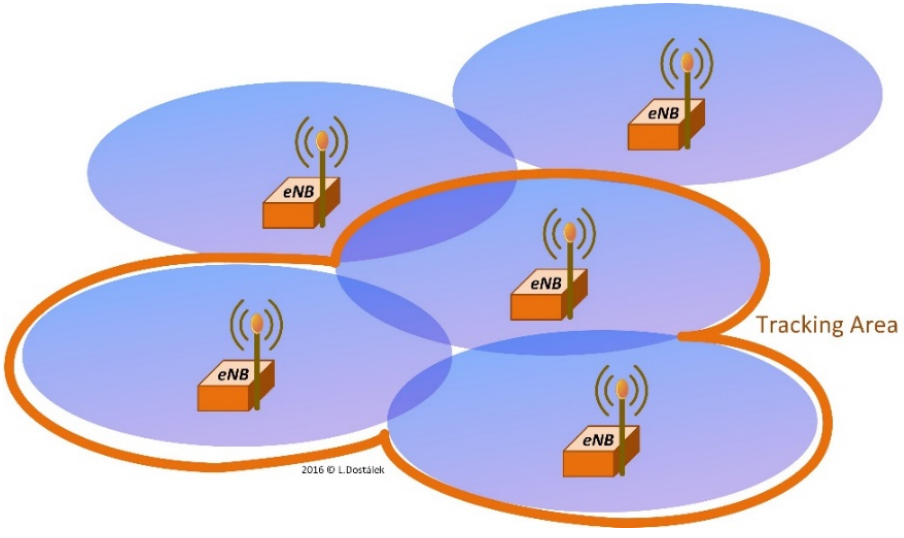
I pro znalce TCP/IP bude v následujícím textu novým termínem pojem „referenční bod“. Je to obdoba dříve používaného termínu rozhraní (*interface*) nebo v TCP/IP pojmu „protokol“. Jako referenční bod si můžeme představit sondu, kterou do síťové komunikace vložil muž uprostřed

sítě *(man in the middle)*, aby komunikaci sledoval. Na rozdíl od síťových protokolů, ale referenční bod může popisovat nejenom sítové protokoly, ale také aplikační data, protože z hlediska síťových protokolů, to co je nad aplikační vrstvou, už není síťový protokol, ale aplikace.

Celá problematika mobilních sítí je pokryta několika systémy norem, které jsou vesměs veřejně dostupné. Základem jsou normy 3GPP (*The 3rd Generation Partnership Project*), zejména roaming je specifikován v normách GSMA (*GSM Association*) a vše co se týká TCP/IP lze pochopitelně nalézt v RFC (*Requests for Comments*). Standardy ITU (*International Telecommunication Union*), kterými se standardizovaly telekomunikace v 19. a 20. století ustupují do pozadí. Je to patrně dáno zkostnatělostí této organizace (obdobně jako ISO).

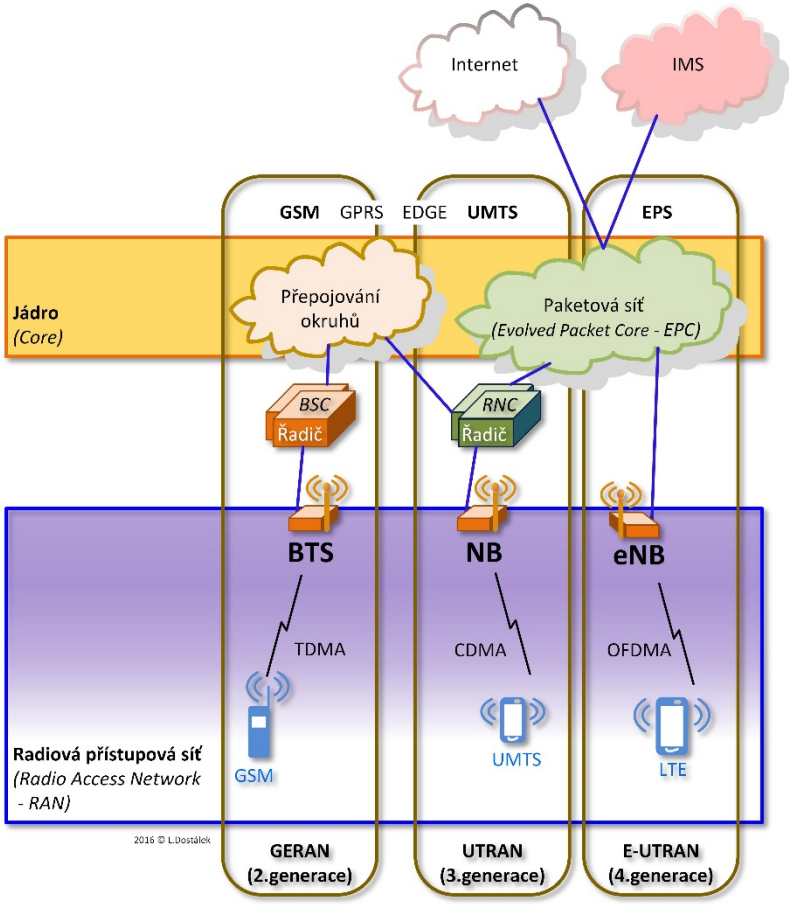
4.1 Buňky a generace mobilních sítí

Mobilní síť se snaží maximálně pokrýt obsluhované území. Pro pokrytí území využívá základnové stanice. V GSM sítích (2.generace) se základnová stanice nazývá BTS (*Base Transceiver Station*). V UMTS sítích (*Universal Mobile Telecommunication System* - 3. generace) se nazývá NB (*Node B*) v LTE (4. generace) se nazývá eNB (*evolved Node B*).



obr. 4.1 Základnové stanice a jednotlivé buňky v LTE (frekvence používané kanály konkrétní buňky se liší od frekvencí používaných kanály sousedních buněk)

Základnová stanice pokrývá území, které se nazývá buňka (*cell*). Ze základnové stanice vede připojení směrem do jádra sítě (*core*) pomocí kabelů nebo mikrovlnného spoje. Zatímco v GSM a UMTS sítích (obr. 4.2) byly skupiny základnových stanic vždy řízeny řadičem (*controller*), tak LTE již řadiče nepoužívá a základnové stanice (eNB)



obr. 4.2 Generace mobilních technologií

jsou propojeny přímo s jádrem sítě, které se nazývá EPC (*Evolved Packet Core*).

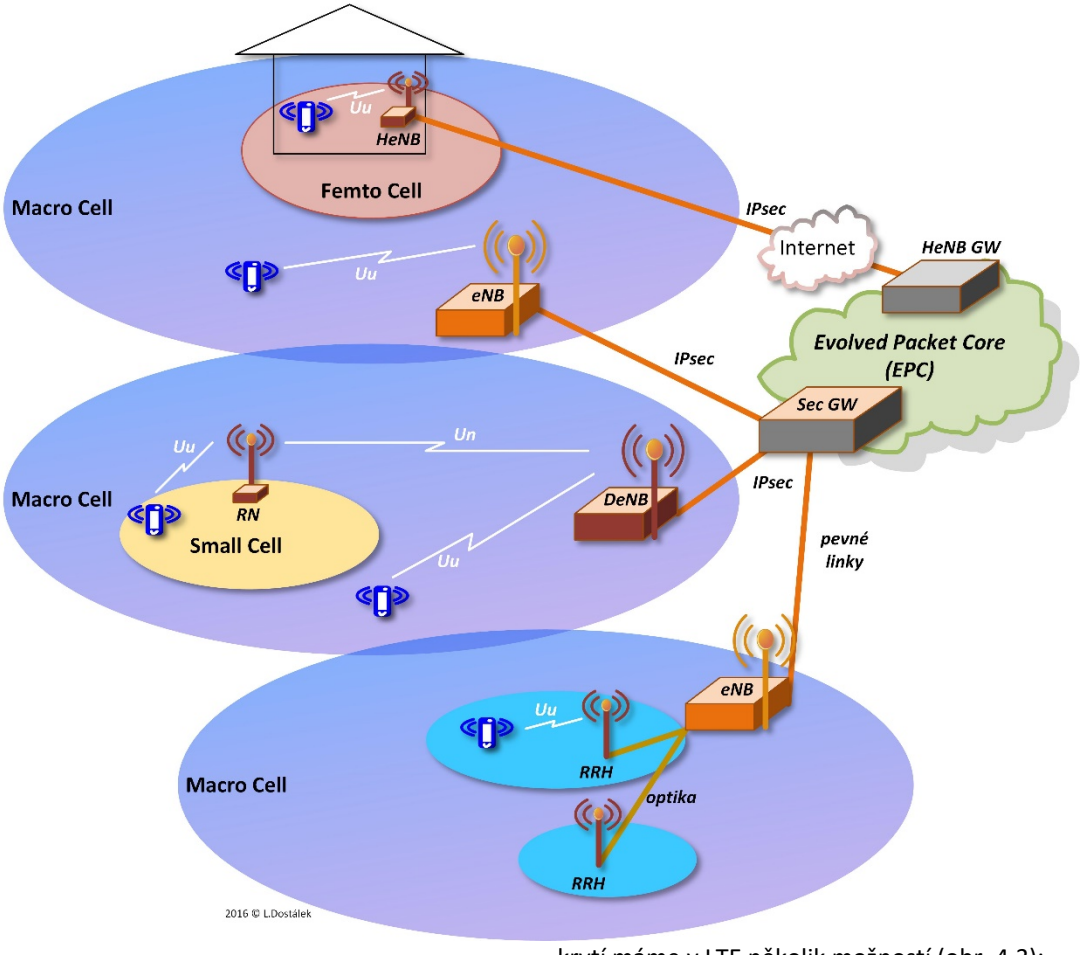
Přesto i LTE má buňky v území logicky organizováno do vyšších územních celků nazývaných *Tracking Area* (obr. 4.1). LTE síť totiž sleduje lokalizaci mobilních zařízení pohybujících se sítí i v nečinném stavu nikoliv po jednotlivých buňkách, ale právě po těchto vyšších územních celcích.

Nyní již zapomeneme na starší generace mobilních sítí (GSM a UMTS) a budeme doufat, že budou co nejdříve vypnuty, aby jejich frekvence mohly být dále využity. Jak? LTE od verze (*Release*) 10 se označuje jako *LTE Advanced*. Změna je v tom, že *LTE Advanced* využívá více frekvencí současně. Mobilní zařízení má „více antén“. Maximální přenosovou rychlost pak můžeme teore-

ticky stanovit až jako součet přenosových rychlostí v jednotlivých pásmech (není to zcela přesné, ale zato snadno pochopitelné).

Buňky mohou být různé velikosti. Hovoříme pak o různých buňkách od makro-buněk (*Macro Cell*) rozlehlých až 35 km až po mikro-buňky (*Micro cell*) pokrývající území do 200 m. Velice zajímavé jsou ještě menší buňky, které slouží k dokrývání území.

Makro-buňka sice může teoreticky pokrýt až 35 km, ale v tomto území s největší pravděpodobností, díky členitosti terénu, vznikne řada hluchý míst. Otázka je, jak dokrýt toto území. Pro dokrytí máme v LTE několik možností (obr. 4.3):



obr. 4.3 Velké, malé a nejmenší buňky LTE

- Využít tzv. *Femtocell*, tj. buněk o velikost maximálně okolo 10 m.
- Využití vykrývací základnové stanice (*Relay Node* - RN).
- Využití *Remote Radio Head* (RRH).

Asi nejpopulárnějším řešením je *Femtocell*, který je obsluhován nízko výkonovou základnovou stanicí HeNB (*Home* eNB). HeNB je často v soukromém držení účastníků. HeNB je propojena zpravidla přes Internet s jádrem sítě. Propojení je zabezpečeno IPsec tunelem, který je na straně jádra zakončen entitou *HeNB Gateway*, za kterou je již jádro sítě (EPC). *HeNB Gateway* zajišťuje též bezpečnostní oddělení jádra sítě od Internetu.

HeNB je tedy ideálním řešením např. pro chalupy, kde není pokrytí mobilní sítí, ale kde je dobré připojení k Internetu. Pomocí HeNB je též možné vykrývat různé suterénní místnosti, velíny atp.

Další variantou je vykrývací základnové stanice (RN), která je obdobou televizních vykrývacích vysílačů pro vykrývání v členitém terénu. Základnová stanice s RN komunikuje pomocí referenčního bodu (rozhraní) Un. RN pak již s mobilním zařízení ve své malé buňce komunikuje přes standardní referenční bod LTE sítí, kterým je Uu. Základnová stanice musí podporovat nový referenční bod Un. Takové základnové stanice se nazývají DeNB (*Donor eNB*).

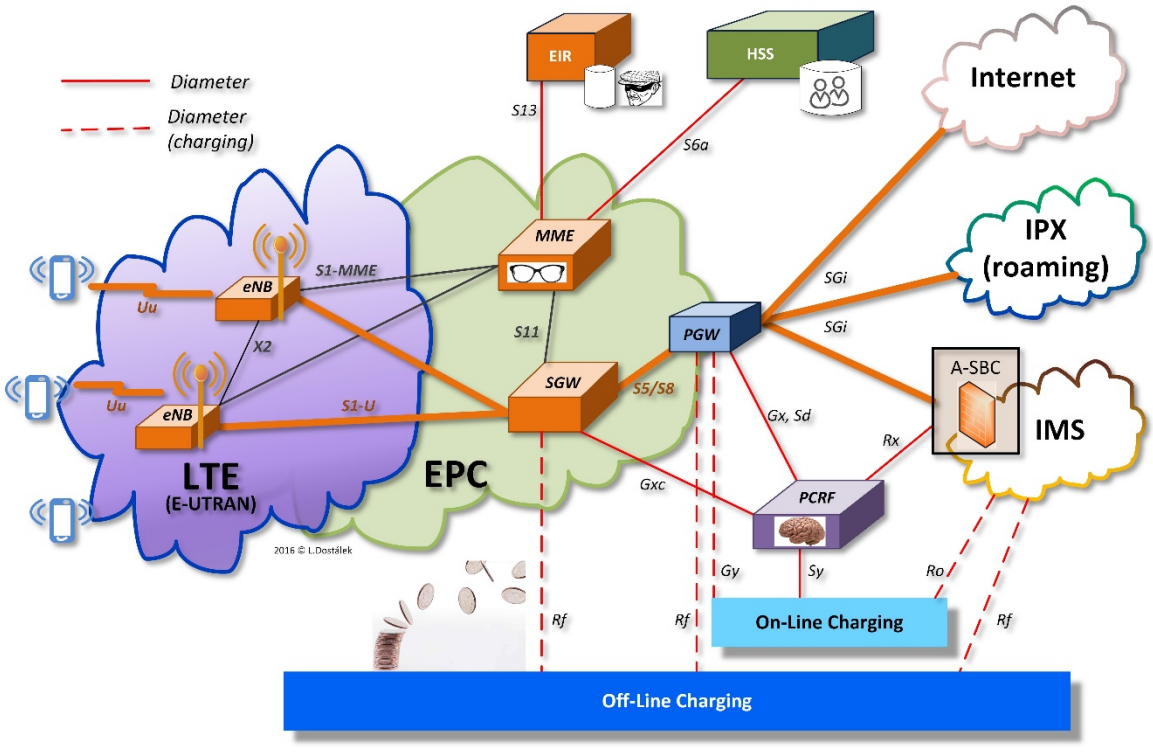
Jinou možností je *Remote Radio Head* (RRH). Klasickou představou eNB je domeček se stožárem. V domečku je veškerá elektronika včetně vysílačů. Z domečku pak vedou koaxiální kabely do antén na stožáru. V současné době se využívají tzv. distribuované eNB, kdy eNB je jen virtuální entitou. Jedna fyzická základnová stanice může obsluhovat až 3 buňky. Tj. v domečku je síťová elektronika a z ní na stožár vede optický kabel do vlastních vysílačů/přijímačů, tzv. *Remote Radio Head* (RRH), které obsluhují jednotlivé buňky. RRH je obdobou systému v letadle nebo na lodi, kdy v kokpitu je ovládání radia, které je umístěno jinde. Jestliže z domečku základnové stanice už vede na stožár optika, tak některé RRH mohou být umístěny o něco dále, na druhé budově, za rohem apod.

Základnové stanice (eNB) jsou s jádrem sítě propojeny pevnými linkami zabezpečenými IPsec tunelem. Na straně jádra sítě je pak IPsec tunel zakončen na entitě *Security Gateway*, která se specializuje právě na ukončování IPsec tunelů od základnových stanic.

Z hlediska zabezpečení cesty z mobilního zařízení do jádra sítě se cesta skládá ze dvou částí:

- Mobilní zařízení – základnová stanice (tj. poslední míle), kde LTE využívá pro generování kryptografického materiálu mechanismus AKA (kap. 6) se sdíleným tajemstvím, které je sdíleno mezi čipovou kartou USIM a tzv. domovským účastnickým serverem (HSS), který bude vysvětlen dále v textu.
- Základnová stanice – jádro sítě, kde je využit tunel IPsec.

  Uprostřed základnové stanice (a uprostřed jádra sítě) je tedy komunikace nezabezpečena, pokud se nepoužije jiný (další) mechanismus zabezpečení, což může využívat např. VoLTE, ale nemusí tak činit.



obr. 4.4 Evolved Packet System (EPS) s vyznačenými referenčními body

4.2 Síť operátora je stavebnicí

V této publikaci se soustředím pouze na síťové technologie, i když operátor musí používat i další IT systémy pro řízení sebe jako organizace (CRM, účetní systémy, fakturační systémy atd.). Na pomezí mezi síťovými technologiemi a IT technologiemi jsou zpoplatňovací systémy *(charging systems)*, které popisovat nebudu, ale zmíním se o referenčních bodech, kterými síťové technologie s těmito systémy komunikují.

Operátor má k dispozici několik technologií, ze kterých si postaví svou síť. Operátor si může zvolit jen některé technologie a jiné ponechat provozovat někým jiným. Základní technologie jsou:

- Systém EPS (*Evolved Packet System),* který účastníkům poskytuje připojení na IP vrstvě. Např. pro připojení účastníků do Internetu. EPC se skládá ze dvou částí:
    - Přístupová síť LTE, která zajišťuje poslední míli komunikace, tj. spojení mezi mobilním zařízením a základnovou stanicí.

  - Jádrem sítě - tzv. Evolved Packet Core (EPC), které řídí přístupovou síť LTE a zajišťuje účastníkům mobilní sítě komunikaci z/do Internetu a dalších sítí na bázi IP protokolu (IMS a IPX). EPC byl zaveden už s 3G sítěmi a pravděpodobně bude vyžit i v 5G sítích.

- Systém IMS (*Internet Multimedia Subsystem*), který tvoří další jádro sítě – jádro na aplikační vrstvě (protokoly SIP, RTP atd.). IMS zajišťuje, aby „to telefonovalo". IMS může provozovat jak týž operátor, který provozuje EPS, tak i jej může provozovat jiný (na operátoru EPS nezávislý) operátor.

Jak již bylo zmíněno, zatímco EPS poskytuje připojení na IP vrstvě, tak IMS poskytuje služby na aplikační vrstvě. Jedná se tedy o analogii s internetem, kde poskytovatelé internetu poskytují připojení na IP vrstvě a poskytovatelé obsahu poskytují služby na aplikační vrstvě.

4.3 EPC

Pokud budeme abstrahovat od entit sloužících pro 3G sítě a od *Security Gateway* a HeNB GW z obr. 4.3, pak EPC obsahuje tři[1] typy entit (obr. 4.4):

- MME *(Mobility Management Entity)* je klíčovou řídící entitou EPC. Zjišťuje ověření účastníků při přihlášení do sítě, sleduje pohyb nečinných účastníků, určuje SGW přes kterou poběží účastníkův datový tok atd.

- SGW *(Serving Gateway)* je zodpovědná za správu účastnických datových toků, tzv. *data bearers*. Přes tuto entitu budou procházet účastnická data.

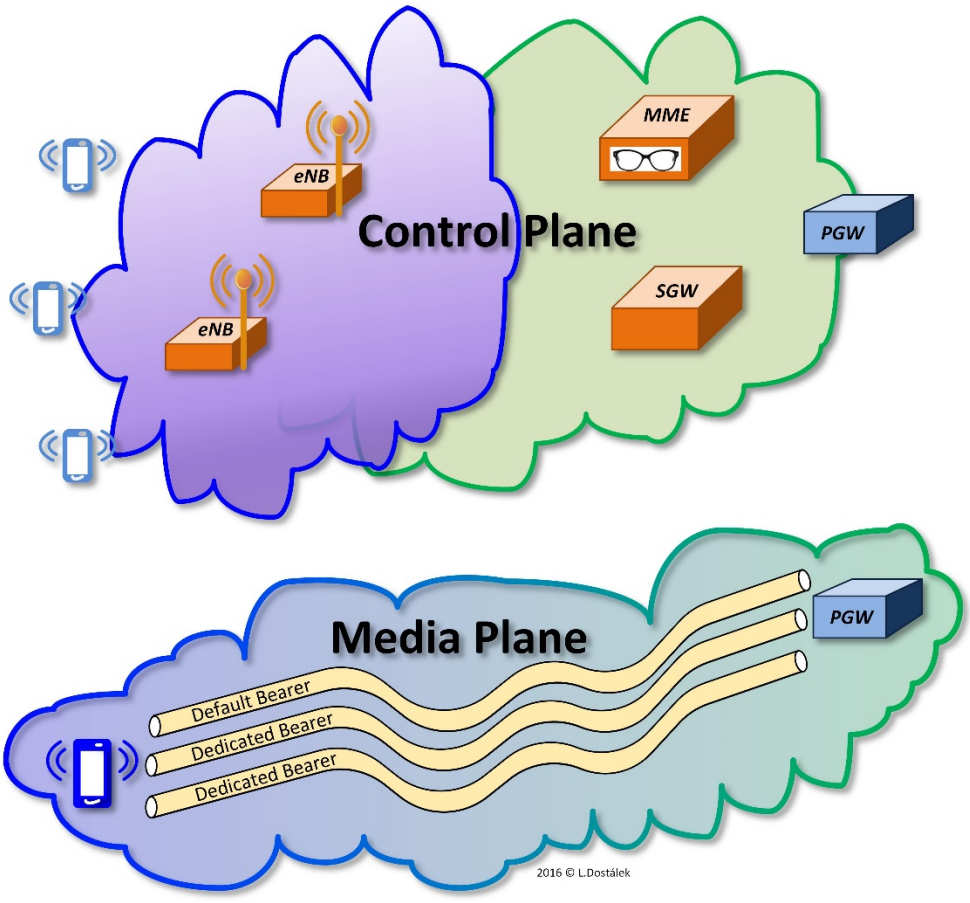
- PGW (PDN GW, *Public Data Network Gateway*) je bránou účastníkových datových paketů do externích sítí. Externí sítí může být Internet, IMS (viz kap. 4.4), nebo i IPX v případě roamingu. Účastníci spíše znají termín APN (*Access Point Name*) což si zjednodušeně můžeme představit jako identifikaci vnějšího rozhraní PGW (obr. 4.6).

Kromě zmíněných entit, které slouží výhradně pro EPC, tak případný operátor musí mít k dispozici ještě minimálně tři další entity a pochopitelně zpoplatnění (*charging*):

- EIR (*Equipment Identity Register*) – Registr zcizených zařízení. Součástí přihlašovací procedury účastníka je předání hardwarové identifikace mobilního zařízení (*International Mobile Equipment Identity* - IMEI). MME pak v rámci přihlašování zkontroluje v registru zcizených zařízení EIR, jestli mobilní zařízení není kradené.

- HSS - (*Home Subscriber Server*) - Domovský účastnický server. Entita HSS obsahuje

[1] V 3G sítích EPC využíval entity GGSN (*Gateway GPRS Support Node*) a SGSN (*Serving GPRS Support Node*). Těmito entitami s v této publikaci blíže nezabývám.



obr. 4.5 Dva pohledy na EPS

údaje o jednotlivých účastnících sítě. U každého účastníka, vedeného v HSS pod interní identitou tzv. IMSI (*International Mobile Subscriber Identity*), se vedou údaje o něm, o jím nasmlouvaných službách, a pak také sdílené tajemství K, které HSS sdílí s účastníkovou čipovou kartou USIM. Sdílené tajemství K slouží pro autentizaci účastníka do sítě a pro generování kryptografického materiálu pro zabezpečení jeho komunikace s mobilní sítí. (K je pochopitelně jiné pro každý USIM.)

- Neméně důležitou entitou je PCRF (*Policy and Charging Rules Function*), která v reálném čase určuje pravidla (politiky) sítě. Automaticky vytváří pravidla pro každého účastníka přihlašujícího se do sítě. Skrze referenční bod Sd (obr. 4.4) může PCRF moni-

torovat provoz účastníků a na základě monitorování změnit jeho síťová pravidla (politiky). V případě příchozích hovorů VoLTE (příchozích z IMS) může PCRF skrze referenční body Rx a Gxc požádá SGW o alokaci příslušného datového nosiče (*Data Bearer*) pro příchozí hovor.

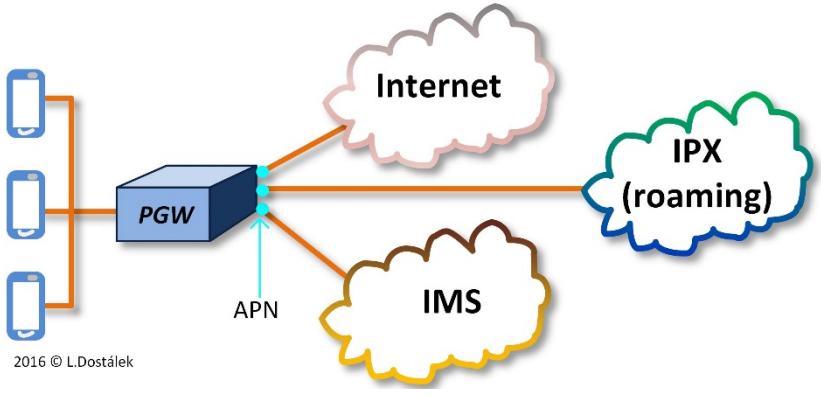
Na EPS se můžeme podívat i z většího odstupu (obr. 4.5) a uvidíme, že se skládá ze dvou vrstev (*plane*):

- Vrstvy řízení (*Control Plane*), která zajišťuje, aby to celé fungovalo. Z hlediska účastníka sítě tato vrstva není vidět. Někdy se neříká vrstva řízení, ale vrstva „signalizace sítě“, což je převzato z archaických telekomunikačních protokolů.
- Vrstvy přenosu medií (*Media Plane* nebo také *User Plane*), která zajišťuje přenos účastníkových paketů z mobilního zařízení do externích paketových sítí (Internet, IPX, IMS atp.). Tato vrstva pro každého účastníka vytvoří jeden implicitní datový nosič *(Default Bearer)* a případně jeden nebo několik vyhrazených datových nosičů *(Dedicated Bearer)* určených pro konkrétní datovou službu. Datové nosiče jsou různých kategorií. Např. pro přenos audia budeme požadovat nosič určité garantované šířky pásma. Pro přístup do Internetu zase garanci přenosového pásma nebudeme vyžadovat atd.

Nesmíme zapomenout ještě na zpoplatnění *(charging)*. Pokud by účastníci měli jen smlouvy s operátorem a operátor jim na konci měsíce posílal fakturu, pak bychom vystačili s Off-line zpoplatňováním. Se zavedením předplatných kupónů (tj. kreditních kupónů) muselo být zavedeno i On-line zpoplatnění, aby bylo možno v reálném čase zjistit, jestli účastník má na požadovanou službu dostatečný kredit.

Z hlediska externího účastníka se celé LTE s EPC jeví, jakoby všichni účastníci LTE „seděli“ na lokální sítí za PGW (obr. 4.6). Podobně jako doma účastníci sedí za xDSL modemem. Tj. LTE pro mobilního účastníka zajišťuje připojení do internetu – tj. neřeší hlasové (multimediální) služby – ty jsou řešeny na aplikační vrstvě, tj. pomocí IMS. To, přes které externí rozhraní PGW uživatel komunikuje se specifikuje pomocí tzv. APN (*Access Point Name*). Na jednotlivá APN může mít poskytovatel nastaveny různé tarify.

Poznámka na závěr: EPC vzniklo už se sítí UTRAN (tj. 3G). V těch dobách EPC poskytovalo některé služby na bázi přepínaných okruhů *(Circuit Switched)* a jiné na bázi přepínaní paketů *(Packet Switched)*. Hovořilo se, že EPC je rozděleno do dvou domén: doména přepínaných okruhů *(Circuit Switched)* a domény přepínaných paketů *(Packet Switched)*. I když eUTRAN (LTE) je již výhradně postavena na přepínání paketů, tak se v mnoha standardech s tímto terminologickým dělením stále setkáváme. Je to mj. dáno tím, že je stále vyžadována interoperabilita se zastaralými sítěmi, které používají přepínání okruhů.



obr. 4.6 Pohled na EPS z externích sítí (vztah APN k roamingu je na obrázku zjednodušen)

4.4 IMS

Máme dva světy: jedním je EPS (LTE s EPC) a druhým je IMS (*Internet Multimedia Subsystem*). Zatímco LTE s EPC umožní připojit mobilní zařízení do sítě protokolem IP, tak IMS nám umožní, aby to „telefonovalo“, tj. např. implementuje VoLTE (*Voice over LTE*). Tj. EPS poskytuje služby na IP vrstvě, IMS na aplikační vrstvě.

IMS (obr. 4.7) se skládá ze čtyř typů entit:

- SBC (*Session Border Controller*), které bezpečně oddělují IMS od ostatních sítí. IMS zpravidla využívá dva typy SBC: A-SBC (*Access SBC*) na který přistupují účastníci a I-SBC (*Interconnect SBC*), kterým je propojena s ostatními operátory nebo zastaralými sítěmi. Blíže viz kap. 9.1.
- CSCF (*Call Session Control Function*), která je zodpovědná za zpracování požadavků protokolu SIP. CSCF obsahuje řadu SIP proxy, které jsou popsány dále.
- *Aplikační služby*, které jsou nadstavbovými službami nad IMS. Jednotlivé aplikační funkce (AF) mohou být realizovány i servery třetích stran. Příklady aplikačních funkcí jsou prezentační služby, konferenční servery, servery pro rychlé zasílání zpráv (*Instant Messaging*), severy zajišťující služby „zmáčkni a mluv“, konverze zpráv do SMS a předání SMS centru atd.
- *Media resource*, který zajišťuje zvuková hlášení, případně mixáž multimediálních toků.

Např. pro *Session control* může např. poskytovat audio: „Volaný účastník je dočasně nedostupný“.

Vedle těchto entit IMS vyžívá již zmíněné entity PCRF a HSS (viz též odstavec 4.2). HSS opět obsahuje informace o účastnících, jejich službách a též sdílené tajemství K, které sdílí s účastníkovou čipovou kartou USIM/ISIM. Na základě tohoto tajemství se účastník autentizuje vůči P-CSCF, která tento požadavek předá S-CSCF, která je vyřídí za pomocí HSS. Je třeba upozornit, že EPC může využívat jiné HSS (jinou databázi účastníků) než IMS. Tj. účastník může mít jiné K pro LTE a jiné pro IMS. Prakticky na čipové kartě tak může mít dvě struktury: USIM s K pro LTE a ISIM s K pro IMS.

Jádrem IMS je entita S-CSCF, která vyřizuje požadavky, ale neobsahuje žádné bezpečností funkce. Předpokládá se, že je chráněna SBC (tj. zejména A-SBC). Pokud by útočník dostal pod svou moc S-CSCF, pak si se sítí může dělat cokoliv. Entita E-CSCF zajišťuje nouzová volání (např. „112“).

Pokud se volaný nenachází v téže síti (v témž IMS), tak je požadavek předá dále na entitu BGFC, která zjistí, jestli je volaný účastníkem jiného poskytovatele IMS, pak požadavek předá entitě IBCF. Pokud je účastníkem zastaralé sítě, pak požadavek předá entitě MGFC.

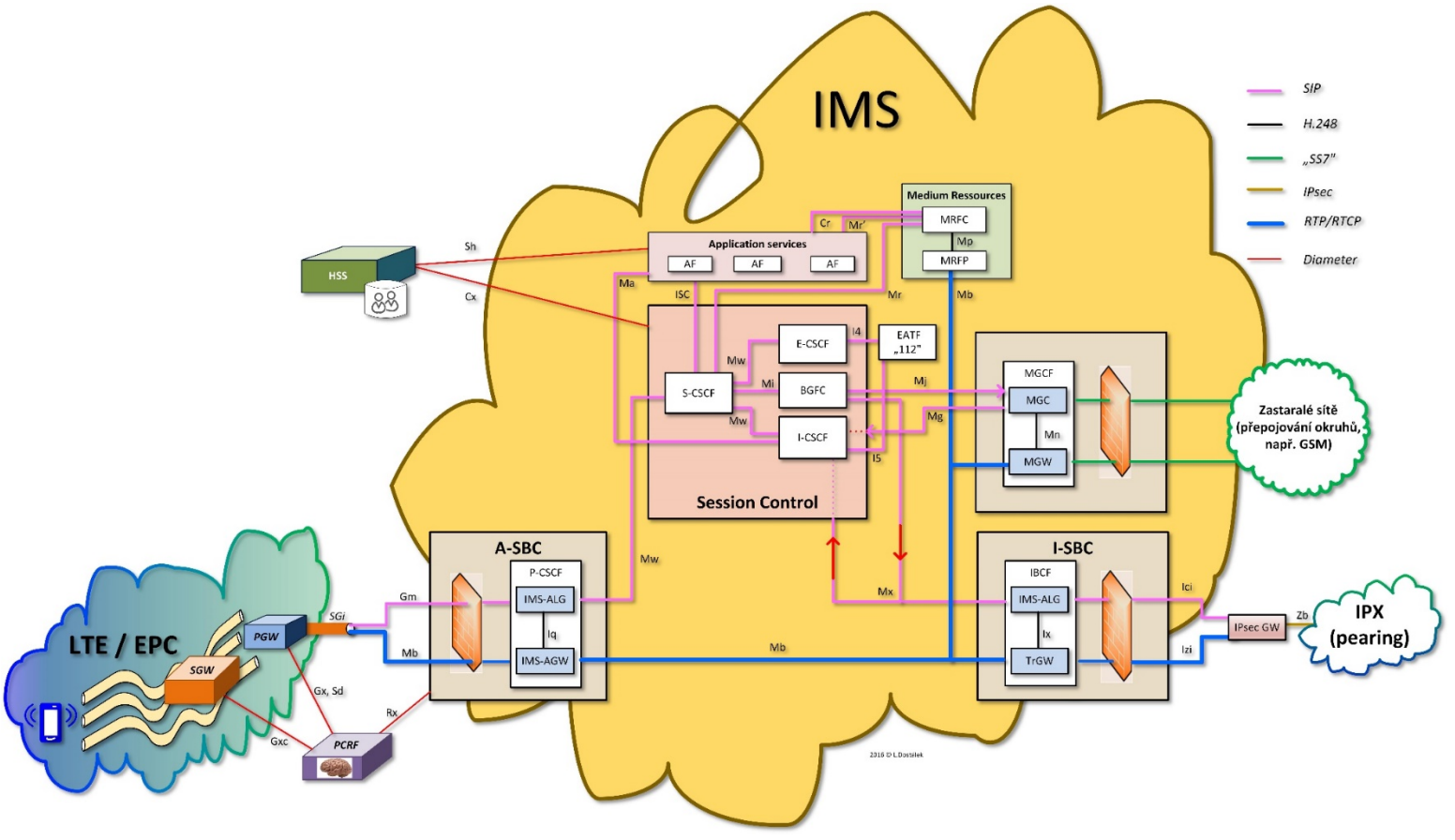
Na obr. 4.7 není znázorněna entita SLF *(Subscriber Location Function)*, zpoplatnění a DNS.

V případě, že v síti existuje vice HSS (databází účastníků), tak před tím, že se síť dotáže HSS, tak se musí dotázat SLF, kterého HSS se má dotazovat. Více HSS se může použít např. v případě, že síť sdílí více operátorů.

Ve VoLTE se účastníci primárně neadresují klasickým telefonním číslem a tzv. SIP URI připomínajícím e-mailovou adresu. DNS je proto důležité pro nalezení SIP serveru domény do které se volá.

Pokud se používají klasická telefonní čísla, pak je nutné využít DNS ENUM pro převod telefonního čísla na SIP URI volaného. Pomocí záznamů v DNS ENUM se rovněž řeší přenositelnost telefonních čísel. K DNS ENUM je třeba dodat, že DNS v IMS bude používat kořenové DNS servery sítě IPX (viz kap. 5.1.2), nikoliv kořenové DNS servery Internetu.

Ještě existuje DNS ENUM v Česku spravovaný NIC.CZ pro VoIP, který ale používá kořenové servery internetu (tento ENUM je internetová databáze, v níž majitelé telefonních čísel zveřejňují způsob, jak jim ostatní mohou na toto číslo volat přes internet, VoIP). Jelikož IPX a Internet jsou dva nezávislé světy, tak i prostory telefonních čísel v obou světech jsou nezávislé. V minulosti existovaly pokusy o rozdělení prostoru telefonních čísel tak, aby se ani pomyslně nepřekrývaly.



obr. 4.7 IMS (Internet Multimedia Subsystem) – popis jednotlivých entit obsahuje následující tabulka

CSCF	*Call Session Control Function* (CSCF) entity máme: Proxy CSCF (P-CSCF), *Serving* CSCF (S-CSCF), *Emergency* CSCF (E-CSCF) a *Interrogating* CSCF (I-CSCF)
P-CSCF	Je první entitou IMS, kterou kontaktuje účastníkovo mobilní zařízení. I když má v názvu „Proxy“, tak se z hlediska protokolu SIP jedná o B2BUA.
S-CSCF	Zpracovává požadavky a udržuje stav relací. Zprostředkovává autentizaci účastníků (jménem P-CSCF) za využití HSS. V HSS rovněž vyhledává účastníky, kterým je voláno atd.
E-CSCF	Zpracovává tísňová volání, která předává skrze EATF do integrovaného záchranného systému („linka 112“).
I-CSCF	Je kontaktním bodem pro příchozí volání z cizích sítí.
MGCF	*Media Gateway Control Function* je branou do sítí založených na jiných protokolech než SIP (GSM apod.). Zajišťuje zejména konverzi formátu komunikace a konverzi formátu media (*transcoding*).
BGCF	*Breakout Gateway Control Function* (BGCF) je dispečerem odchozích požadavků. Rozhoduje, do jaké externí sítě má být požadavek předán: jestli do sítí na bázi protokolu SIP nebo do zastaralých sítí (přepínání okruhů) na bázi SS7.
IBCF	*An Interconnection Border Control Function* provádí případné modifikace SIP/SDP požadavků mezi sítěmi různých operátorů. Může se jednat o převod IPv4 a IPv6, skrytí topologie operátora, generování zpoplatňovacích údajů (*charging*) atd.
TrGW	*Transition Gateway* provádí překlad IP adres/portů, převod mezi IPv4 a IPv6 atd. Za jistých okolností může též provádět konverzi formátu media (*transcoding*).
EATF	*Emergency Access Transfer Function* je branou do integrovaného záchranného systému. Požadavky přijímá jak od vlastní sítě (z E-CSCF), tak i z cizích sítí (z I-CSCF).
IMS-ALG	IMS *Application Level Gateway* provádí úpravy na úrovni SIP/SDP. Např. účastník se autentizuje vůči P-CSCF. Takže pro komunikaci s dalšími entitami už může být označen, jako důvěryhodný což se odrazí v příslušné hlavičce protokolu SIP. Provádí překlad IPv4 adres, konverzi IPv4 a IPv6 atd.

IMS-AGW	IMS *Access Gateway* provádí překlad IP adres/portů, převod mezi IPv4 a IPv6 atd. Za jistých okolností může též provádět konverzi formátu media (*transcoding*).
SEG (IPsec GW)	*Security Gateway* ukončuje IPsec tunely.
AF	Aplikační funkce – entita, která umožňuje vytvářet konkrétní aplikace na protokoly SIP/RTP, které přinášejí další přidanou hodnotu.
MRFC, MRFP	Viz kap. 13.2.4
SLF	*Subscriber Location Function* – v případě, že v síti existuje vice HSS, tak před tím, že se síť dotáže HSS, tak se musí dotázat SLF, kterého HSS se má dotazovat. Více HSS se může použít např. v případě, že síť sdílí více operátorů.

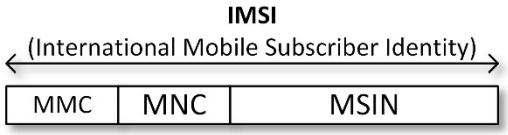
4.5 Veřejná a privátní identita, IMPI a IMPU

Účastník (*subscriber*) je veden v databázi operátora pod jeho interní identitou, která se označuje MSIN (*Mobile Subscription Identification Number*). Přidáním identifikace operátora a identifikace země, kde operátor operuje, vznikne IMSI (obr. 4.8).

Ve VoLTE se od této identity odvozuje, tzv. Privátní identita účastníka (*IP Multimedia Private Identity* - IMPI) tak, že převede do „doménového tvaru“ domény sítě IPX (obr. 4.9). Privátní identita nesmí opustit síť operátora – je určena jen pro komunikaci v rámci jeho sítě.

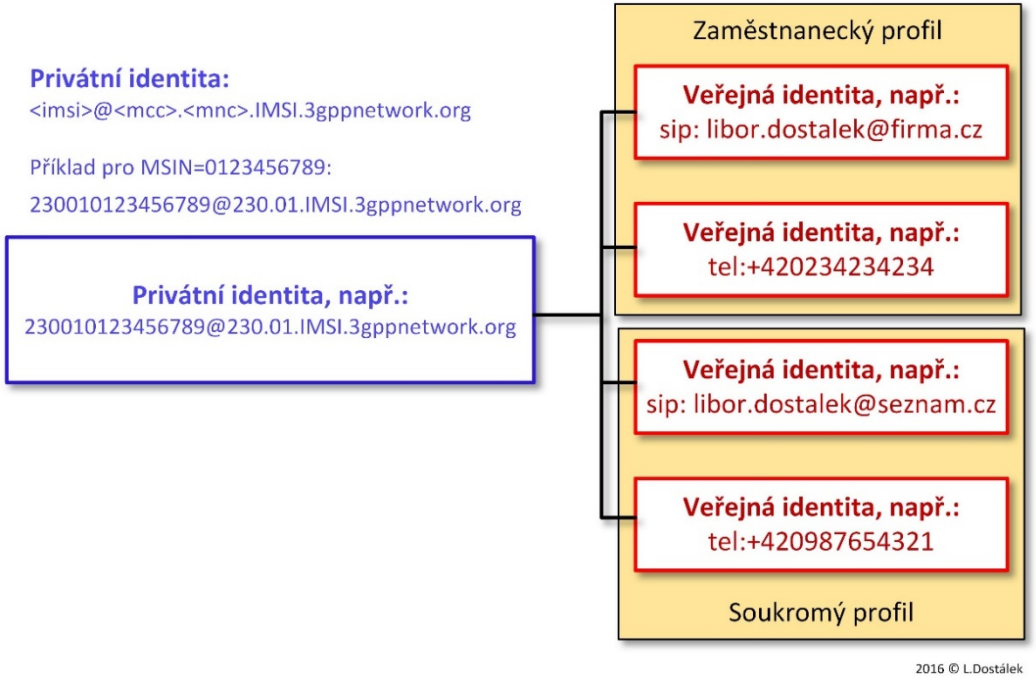
Pro veřejnou komunikaci se používá tzv. veřejná identita (*IP Multimedia Public Identity* - IMPU). Veřejnou identitou ve VoLTE je SIP URI nebo TEL URI. Přičemž účastník si může vytvořit řadu profilů, které obsahují jednu nebo více veřejných identit a nechat si např. v HSS nastavit, že v pracovní době má být kontaktován na jeden profil a mimo pracovní dobu na jiný profil. Na obr. 4.9

jsou tyto profily demonstrativně pojmenovány „Zaměstnanecký“ a „Soukromý“.



- **MMC** (Mobile Country Code)
  ČR: MCC=230
- **MNC** (Mobile Network Code)
  MNC=01 (T-Mobile)
  MNC=02 (O2)
  MNC=03 (Vodafone)
- **MSIN** (Mobile Subscription Identification Number - interní identifikace účastníka sítě)

obr. 4.8 IMSI



obr. 4.9 Veřejná a privátní identita účastníka

4.6 Další používané identifikátory

Spíše pro zajímavost, dále uvádím další používané identifikátory pro komunikaci v síti (obr. 4.10):

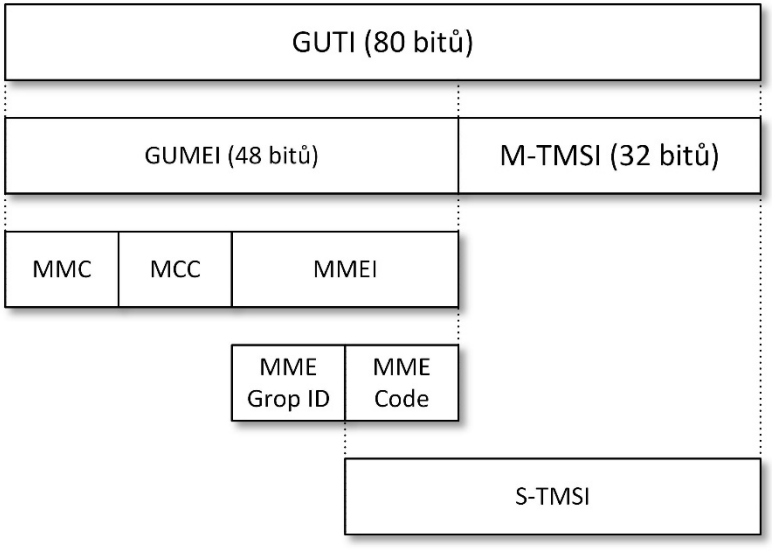
- GUTI *(Globally unique Temporary Identity)* – tento dočasný identifikátor alokuje MME pro mobilní zařízení. Skládá se z GUMMEI *(Globally unique MME Identifier)*, který identifikuje MME, a M-TMSI *(MME Temporary Mobile Subscriber Identity)*, který dočasně idenfitikuje mobilní zařízení v rámci konkrétního MME. GUMEI se skládá z:
  - MMC a MNC – viz obr. 4.10.
  - MME Group ID – identifikace skupiny MME.
  - MME Code – identifikace konkrétního MME.
- S-TMSI *(Serving –Temporary Mobile Subscriber Identity)*, který slouží pro skrytí (nevyzrazení) IMSI během úvodního přihlášení do sítě, které je nezabezpečené.
- IP adresa (IPv4 nebo IPv6) mobilního zařízení.
- C-RNTI *(Cell-Radio Network Temporary Identifier)*, který je používán v rámci buňky eNB pro identifikaci mobilního zařízení

Základnová stanice eNB používá následující identifikátory:

- Macro eNB Identifier (20 bitů)
- HeNB Identity (28 bitů)

Buňka má následující identity:

- PCI (Physical Cell Identity) – identifikace buňky na fyzické vrstvě. Zajímavé



obr. 4.10 Další používané identifikátory

je, že v síti může být pouze 504 těchto identit, tj. každá buňka musí mít identitu z jedné z těchto 504 identit.

- E-CGI (eUTRAN Cell Global Identity) - globální identifikace buňky používaná protokoly vyšších vrstev.

Tracking area má následující identitu:

- TAI (Tracking Area Identity).

Jednotlivé entity (obr. 4.7) jsou zpravidla identifikovány svými IP adresami. Používání DNS však není zcela běžné. Pokud se použije, tak každé jádro sítě zpravidla mívá vlastní kořenové DNS servery. Teoreticky je možné využít i DNS z IPX. Síť IPX má, na rozdíl od internetu, předepsanou tvorbu DNS jmen (viz kap. 8.4).

4.7 ISIM/USIM

Každý účastník má jednu privátní identitu (IMPI) a jednu nebo více veřejných identit (IMPU). V USIM je uložena pouze privátní identita (IMPI). Veřejné identity (IMPU) umožňuje udržovat až ISIM. Přičemž veřejné identity mohou být v ISIM spravovány i přes mechanismus OTA (*Over The Air*) – kap. 18.15. V případě, že není implementován ISIM, pak je možné využít pouze TEL URI jako veřejnou identitu, protože mobilních sítích je zakázáno přenášet privátní identitu do cizí sítě. SIP URI odvozené od privátní identity tak není možné přenášet do cizích sítí, tj. není pomocí něj možné komunikovat mimo domovskou síť

Pro mechanismus AKA účastníkova čipová karta obsahuje sdílené tajemství K. Čipová karta (kap. 18) se oficiálně označuje UICC (*Universal Integrated Circuit Card*) a byla zavedena v GSM síti pod označením SIM (*Subscriber Identification Module*). Byl to velký přínos k bezpečnosti, protože se oddělil hardware mobilního zařízení od hardware s identifikačními údaji účastníka sítě. Pro potřeby GSM jsou na SIM kartě dvě aplikace (dva adresáře) GSM a TELECOM. Autentizační mechanismy GSM jsou dnes považovány za slabé, ale objektivně se musí říci, že před 20 lety čipové karty ani hardware mobilního zařízení náročnější algoritmy ani neumožňovaly. I tak to byl pokrok, protože např. dodnes používané pevné analogové linky nemají zabezpečení vůbec žádné.

S příchodem UMTS (3. generace sítí) byl zaveden mechanismus AKA a na čipové kartě („SIMce“) se objevila další aplikace (adresář) USIM a sdílené tajemství K. Tyto čipové karty se již nenazývají SIM karty, ale USIM karty.

A s příchodem IMS se může objevit na kartě jedna nebo více aplikací (adresářů) ISIM.

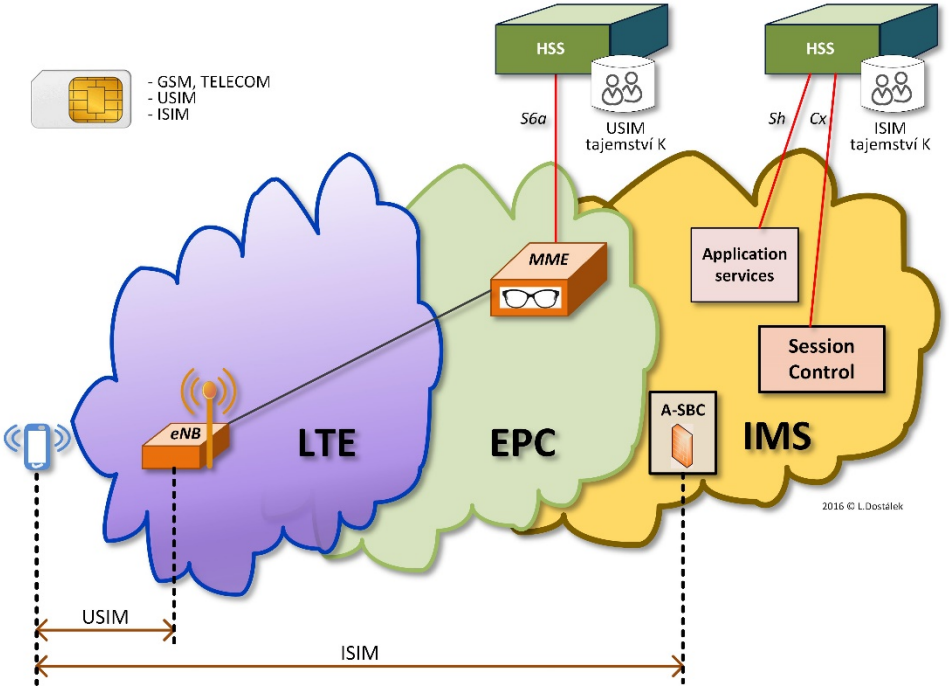
Důležité je, že sdílených tajemství K můžeme mít na kartě více. Jedno pro aplikaci USIM a další pro jednotlivé aplikace ISIM. V případě, že je na kartě více aplikací ISIM, pak každá má své K. K nejsou umístěny přímo v aplikaci (tj. v souboru v adresáři USIM/ISIM), ale v oblasti, která se nazývá bezpečný prvek (*secure element*) a slouží právě k úschově soukromých klíčů, tajných klíčů a dalšího citlivého kryptografického materiálu účastníka. Bezpečný prvek byl zaveden zejména v souvislosti s NFC, aby uspokojil bezpečnostní nároky společností vydávajících platební karty.

ISIM kromě sdíleného tajemství K obsahuje zejména veřejné identity účastníka.

Na obr. 4.11 je znázorněno, že aplikace USIM slouží k autentizaci v LTE síti a k zabezpečení komunikace mezi mobilním zařízením a základnovou stanicí eNB (zabezpečení na IP vrstvě). Zatímco aplikace ISIM složí pro zabezpečení a k autentizaci do IMS (zabezpečení na aplikační

Na obr. 4.11 si ještě všimněte dvou HSS. Jedno pro EPC a druhé pro IMS. Je to z toho důvodu, že obecně EPC a IMS mohou provozovat dva různé subjekty. Pokud obojí provozuje týž subjekt, pak může použít jedno HSS (nebo je replikovat).

Otázkou je, jestli se může provozovat VoLTE i



obr. 4.11 Zabezpečení (šifrování a integrita) pomocí USIM a ISIM

vrstvě) - konkrétně zabezpečení komunikace protokolem SIP mezi mobilním zařízením a hranou sítě IMS (A-SBC). Pozor ale, nezabezpečuje médium (RTP). Pokud chceme zabezpečit i médium, tj. použít protokol SRTP (*Secure RTP*), pak se příslušný kryptografický materiál pro toto zabezpečení přenese v SIP zprávě (protokol SDP) a následně se zabezpečení komunikace RTP/RTCP (tj. médium).

bez ISIM. Ano, ale musíte být operátorem jak LTE (včetně EPC), tak i IMS. Pak nevadí, když se využije stejný (nebo replikovaný) HSS. Další nevýhodou je, že na čipové kartě v aplikaci USIM nejsou uloženy veřejné identity. Důsledkem je, že se SIP URI účastníka uloží do konfigurace mobilního zařízení. Pak si jej ale účastník může libovolně měnit. Nebo se může účastníkům sdělit, že budou používat jen TEL URI. Tím se ale ochudí o

možnost mít telefonní kontakt ve tvaru „mailové adresy“.

4.8 MMI

Standard [4] specifikuje tzv. MMI *(Man-Machine Interface)* pro mobilní zařízení. Zjednodušeně řečeno: specifikuje, co zadává uživatel na klávesnici mobilního zařízení. Konkrétně uživatel zadává:

- Řízení hovorů, které se dělí na:
  - Mobilním zařízením iniciovaná volání.
  - Mobilním zařízením iniciovaná nouzová volání. Tato eventualita odlišuje sítě mobilních operátorů od internetového volání (VoIP), protože mobilní operátoři jsou zpravidla ze zákona povinni zajistit nouzová volání, což jim kompiluje architekturu sítě mj. přidáním entity E-CSCF (obr. 4.7). Avšak na úrovni EPS jsou díky implementaci nouzového volání komplikace ještě podstatnější – musí například zajistit autentizaci do sítě „s vytaženou USIM kartou“.
    - Příchozí volání (zobrazení, přijetí, odmítnutí příchozího volání atd.)
- Doplňkové služby, tj. zadávání řetězců, které obsahují znaky # a *.

Doplňkové služby se interpretují:

- Mobilním zařízením, např. *#06# (zobrazí IMEI).
- UICC (tj. USIM), např. **04*OLD_PIN*NEW_PIN*NEW_PIN# (změna PIN).
- Sítí, tj. odesílají se na MME. Jedná se o příkazy, které se pomocí protokolu NAS (obr. 7.1) přenesou do entity MME, která je provede. Patří sem příkazy pro blokování odchozích hovorů (*Service Code* 33), blokování odchozích mezinárodních hovorů (*Service Code* 331), blokování příchozích SMS, přesměrování hovorů atd. Jakmile však použijeme slovo hovor, tak nám to automaticky evokuje sítě na bázi přepínaných okruhů. Jedná se tedy o interoperabilitu se zastaralými sítěmi (2G, ISDN atp.). Tj. pokud si takto zablokujeme např. příchozí SMS (*Service Code* 35), pak zablokujeme SMS přicházející přes referenční bod SGc, ale pravděpodobně nikoliv SMS přicházející přes SIP (pokud to operátor nějak bokem neošetří – např. v rámci příkazu SIP REGISTER).

tab. 4.1 Syntaxe doplňkových služeb

Operace	**kód**
Aktivace	*SC*SI#
Deaktivace	#SC*SI#
Zjištění stavu	*#SC*SI#
Registrace	*SC*SI# a **SC*SI#
Zrušení	##SC*SI#
SC=*Service Code*, SI=parametr	

4.9 Zmáčkni a mluv

Již zmíněná služba „Zmáčkni a mluv“ (*Push to talk over Cellular*) umožňuje polo-duplexní komunikaci v rámci skupiny účastníků. Hodí se např. pro záchranný tým, kdy je nutné, aby celá skupina byla na příjmu a pouze jeden po zmáčknutí tlačítka mohl mluvit, a to k celé skupině (tzv. skupinové volání).

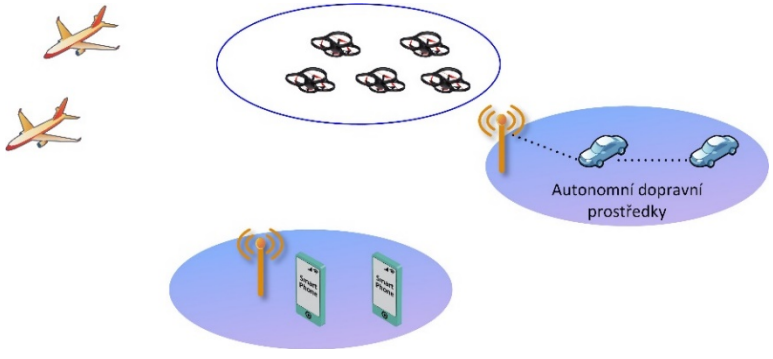
Pro profesionální záchranný systém se obecně používají specializované mobilní sítě TETRA (*Terrestrial Trunked Radio*) nebo Tetrapol. Oba systémy vycházejí z dnes již zastaralého systému GSM. Závisí na volbě konkrétního státu, jestli zvolí TETRA nebo Tetrapol. Jedná se o mobilní sítě, které zpravidla platí daňový poplatník. Pokrytí území státu základnovými stanicemi a vybudování příslušné infrastruktury je velice nákladná záležitost, takže ne vždy se dostatečně pokryje území. Účastnické stanice (slovo mobil asi není to pravé) jsou proto často kombinovány s vysílačkami, aby se eliminoval problém s pokrytím.

Obdobného efektu lze dosáhnout i aplikační funkcí IMS, která se nazývá „Zmáčkni a mluv“ (*Push to talk over Cellular)*. Stačí jeden aplikační server, který realizuje příslušnou aplikační funkci (AF) …

4.10 5G

Stále více se hovoří o sítích 5G. Před pátou generací stojí nové výzvy. Každý očekává ještě vyšší přenosové rychlosti, využívání frekvenčních pásem 27-45 GHz atd. To je ale jen pokračování trendů započatých předchozími generacemi mobilních sítí.

Zcela novou výzvou je přejít od buněk pokrývajících plochu území k buňkám, které by byly rozvrstveny vertikálně (prostorově). Měli bychom tak buňky např. pro komunikaci dronů nebo pro letový provoz. Např. v buňkách pro drony by drony komunikovaly také mezi sebou, aby si organizovali provoz (aby se vyhýbali jeden druhému a optimalizovali si dráhu letu). Další výzvou je v2v *(vehicle to vehicle)* komunikace, tj. komunikace mezi vozidly. Jak u dronů, tak i u vozidel se v buňce předpokládá jednak komunikace se základnovou stanicí, tak i komunikace mezi účastníky vzájemně. Uvidíme, co nám 5G všechno přinese …



obr. 4.12 5G (drony, autonomní dopravní prostředky atp.)

5. Roaming

Roamingem se myslí situace, kdy nemáme v dosahu svou domovskou síť, ale jsou dostupné cizí sítě, které nám umožňují se do nich přihlásit. V případě, že se připojíme do cizí sítě, pak tato síť se označuje jako „navštívená síť“. Účastníci českých mobilních sítí mohou t. č. navštívit cizí sítě jen v zahraničí.

Zajímavé je, že roaming máme jak na IP vrstvě, tzv. LTE roaming, tak roaming můžeme mít i na úrovni SIP protokolu, tzv. VoLTE roaming. Na úrovni VoLTE, máme kromě roamingu ještě volání do cizích sítí. Tím se míní, že volaný účastník je domovským účastníkem cizí sítě.

5.1.1 IPX

Pro potřeby roamingu byla vytvořena síť IPX (*IP eXchange*). Jedná se o celosvětovou síť, která je paralelní sítí k Internetu a nemá s ním přímé propojení (doufejme). Obdobně jako Internet, je i IPX postavena na protokolech TCP/IP, má vlastní kořenové DNS servery a tvorbu doménových jmen, vlastní autonomní systémy atd. Obdobně jako Internet je poskytována poskytovateli, se kterými operátoři uzavírají smlouvy o poskytování IPX.

5.1.2 LTE roaming

Cizí účastník, který navštíví síť LTE se nejprve potřebuje přihlásit. Přihlašovací proceduru zahájí s entitou MME navštívené sítě, která musí získat údaje o účastníkovi včetně kryptografického materiálu z HSS. Avšak nikoliv z HSS navštívené sítě, ale skrze IPX se dotáže HSS v domovské síti účastníka a pokračuje v přihlašovací proceduře. Nakonec umožní účastníkovi přístup do své sítě. Nyní máme dvě možnosti (obr. 5.1): *Home Routed LTE Roaming* a *Local Break Out*.

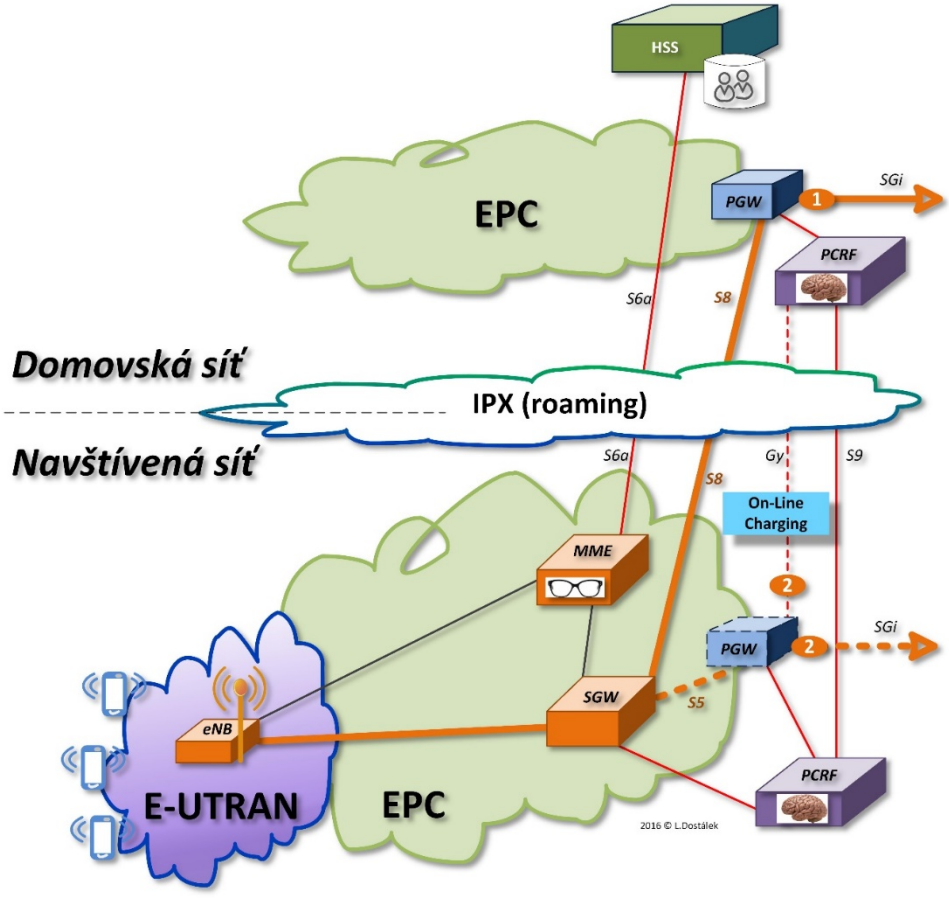
Home Routed LTE Roaming

SGW vytvoří účastníkovi datový nosič (*bearer*), ale pozor ten je tunelován od účastníka v navštívené síti skrze síť IPX na PGW domovské sítě! A teprve pak do Internetu. Tento typ LTE roamingu se nazývá *Home Routed LTE roaming*. Na obr. 5.1 šipka č. 1. Výsledkem je, že si operátoři nechají tučně zaplatit za tunelované pakety skrze IPX.

Local Break Out LTE

Druhou možností, je že by operátor navštívené sítě účastníkovy pakety přímo pouštěl do Internetu skrze jeho vlastní PGW. Tento typ LTE roamingu se nazývá *Local Break Out*. Na obr. 5.1 šipka č. 2.

Běží ale o zpoplatnění. Pokud jsou pakety tunelovány do domovské sítě, pak domovský operátor má zpoplatnění úplně pod svou kontrolou. Jenže pokud by byly pakety přímo vypouštěny do Internetu navštívenou sítí tak, by navštívená síť posílala do domovské sítě jen účtovací údaje (skrze referenční bod Gy). Lze však považovat tyto účtovací údaje za důvěryhodné opravdu od každé sítě? To je pro každého operátora otázkou, na kterou je jasná odpověď: jistota je si měřit účtovací údaje sám.



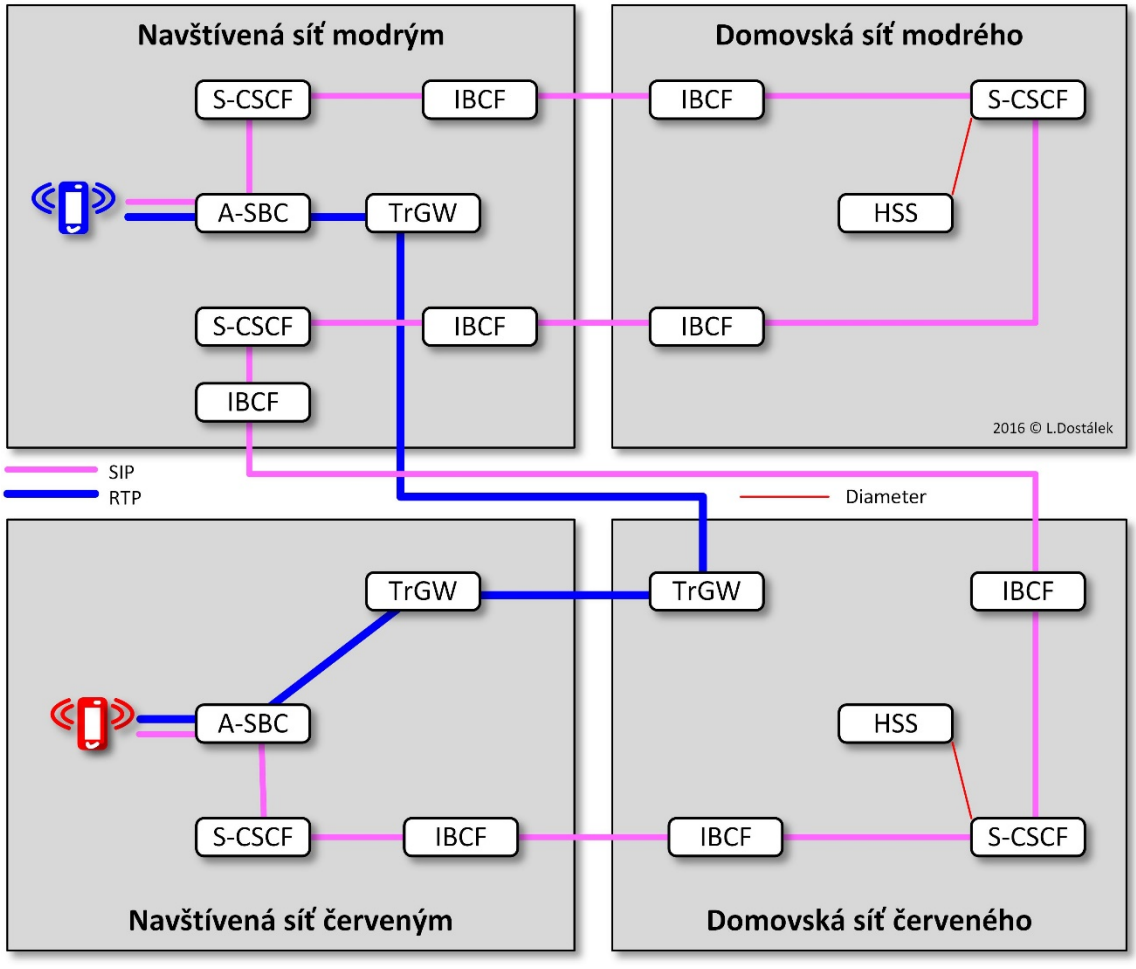
obr. 5.1 LTE roaming

Problém v EU spočívá v tom, že drahý (rozuměj skrze IPX tunelovaný) roaming ztěžuje a prodražuje spolupráci na společném trhu EU. Cílem je tedy regulovat (snížit) cenu. Jenže cílem regulace bude muset být i zakotvení důvěry mezi evropskými operátory, aby používali *Local Break Out*.

5.1.3 VoLTE Roaming

VoLTE roaming je roaming na úrovni protokolu SIP (tj. IMS). Roaming je v IMS možné řešit dvěma způsoby:

1. Vyžije se *Home Routed LTE roaming*. Účastník ač v navštívené síti přímo kontaktuje P-

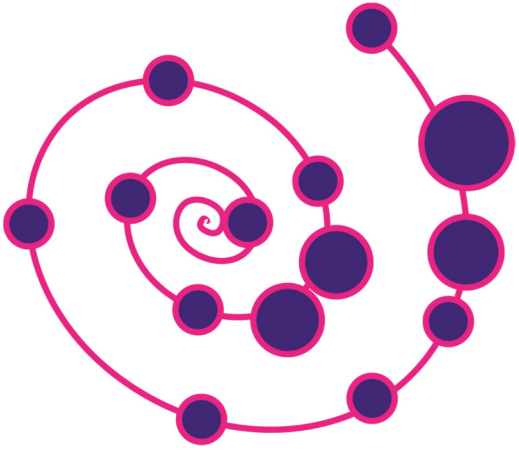


obr. 5.2 VoLTE roaming

CSCF (A-SBC) domovské sítě. Tím se přenese IP komunikace z navštívené sítě do domovské sítě a nic se na úrovni protokolu SIP nemusí řešit.

2. Účastník kontaktuje P-CSCF (A-SBC) navštívené sítě a komunikace s domovskou sítí se provede skrze referenční body Ici/Izi do IPX (obr. 4.7).

Opět je tu otázka, jestli by to nešlo nějak zlevnit. Při představě, že jak volaný, tak volající, jsou v roamingu, tak datový tok půjde skrze IPX třikrát, což volání prodraží. Na obr. 5.2 je znázorněná představa VoLTE roamingu podle normy GSMA IR.65 [5]. V tomto případě by médium *(bearer)* neprocházelo domovskou sítí volajícího, tj. sítí IPX by se procházelo jen dvakrát.



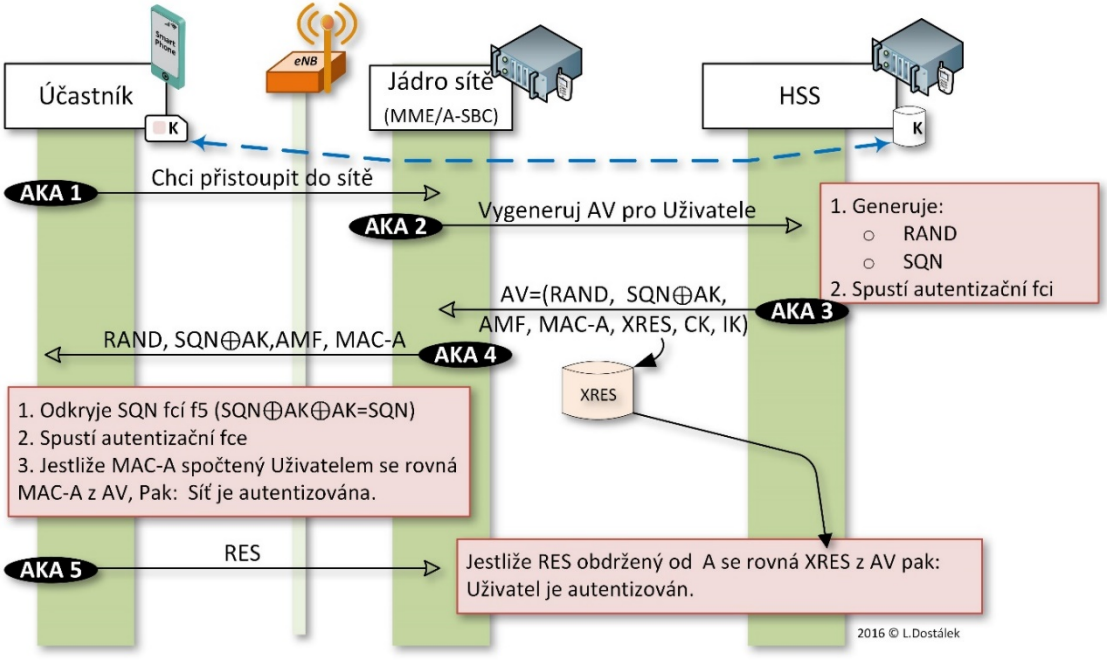
6. AKA mechanismus

Kryptografický mechanismus AKA (*Authentication and Key Agreement*) je využíván v UMTS [6], tak v LTE [7], tak i v IMS (VoLTE) [8]. Dále existuje standard pro autentizaci mechanismem AKA v protokolu HTTP [9].

AKA mechanismus slouží k oboustranné autentizaci účastníka a sítě, dále ke generování kryptografického materiálu pro zabezpečení komunikace mezi mobilním zařízením účastníka a eNB (v LTE), resp. A-SBC (v IMS).

Předpokládáme, že:

- Účastník má na USIM/ISIM uloženo sdílené tajemství, které sdílí s HSS. (Ve své podstatě je HSS jen fornt-end, za kterým se skrývá entita Autentizační centrum (AuC), které spravuje sdílená tajemství účastníků.)
- HSS i zařízení účastníka eviduje číslo *SEQ*, které se s každou autentizací zvětšuje o 1.
- Mechanismus AKA má definovány jednocestné funkce f1 až f2 [10], [11].



obr. 6.1 AKA (Authentication and Key Agreement)
eNB pouze mechanicky předává komunikaci

Funkce	**Význam**
f1 až f5	Jednocestné funkce
K	Sdílené tajemství mezi účastníkovou čipovou kartou USIM/ISIM a sítí (HSS)
RAND	Náhodné číslo generované HSS pro každou autentizaci
SQN	Pořadové číslo autentizace (udržuje síť i klient)
AK	Anonymizační klíč k SEQ (skryje SEQ během přenosu sítí)
AMF	*Authentication Management Field* (předem známý řetězec)
MAC-A	Jednorázové heslo pro autentizaci sítě
XRES	Očekávané jednorázové heslo pro autentizaci klienta
CK	*Cypher Key* - šifrovací klíč
IK	*Integrity Key* - sdílené tajemství pro zajištění integrity přenášených dat
AUTN	$AUTN = SQN \oplus AK \,//\, AMF \,//\, MAC$

- Máme definován známý řetězec *AMF* (změnou řetězce *AMF* může autentizaci provádět jiná aplikace).

AKA mechanismus (obr. 6.1) zajišťuje:

- Autentizaci sítě vůči účastníkovi pomocí jednorázového hesla *MAC-A*, které vygeneruje síť a účastník si jej nezávisle na tom vypočte. Pokud se rovnají, pak je **síť** autentizována.
- Autentizace účastníka vůči síti pomocí jednorázového hesla *XRES*, které vygeneruje síť a předá jej MME (resp. A-SBC). Účastník vygeneruje *RES* a zašle jej MME (resp. A-SBC). Pokud *RES* je shodné s *XRES*, pak je **účastník** autentizován.
- Šifrovací klíč *CK* a sdílené tajemství *IK*, které slouží pro zajištění integrity přenášených dat

Mechanismus je jednoduchý (obr. 6.1):

AKA 1. Mobilní zařízení se chce autentizovat, tak zašle síti (tj. MME, resp. A-SBC) svou privátní identitu.

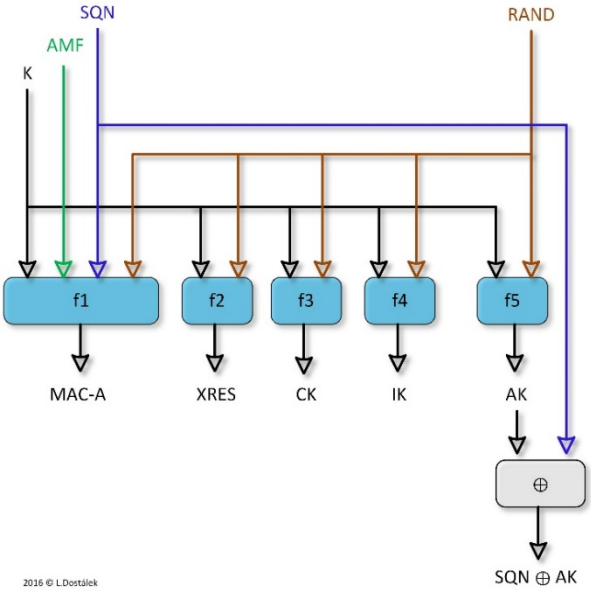
AKA 2. Síť požádá HSS o vygenerování tzv. autentizačního vektoru *AV* pro danou privátní identitu.

AKA 3. HSS následně (skrze AuC):

- Generuje náhodné číslo *RAND*.
- Uložené číslo *SEQ* zvětší o jedna.
- Spustí jednocestné funkce f1 až f5 (obr. 6.2). Do výpočtu vstupuje sdílené tajemství K a předem známý řetězec *AMF*.
- Výsledkem je autentizační vektor $AV=(RAND,\ SQN \oplus AK,\ AMF,\ MAC\text{-}A,\ XRES)$, který předá síti.

AKA 4. Síť vyzobne z *AV* jednorázové heslo *XRES*, které si uloží a zbytek pošle účastníku.

AKA 5. Zařízení účastníka nejprve spustí funkci f5, aby získalo *SEQ*, které



obr. 6.2 AKA autentizační funkce f1 až f5

porovná s jim udržovaným *SEQ*. Poté spustí zbylé jednocestné funkce a získá *MAC-A, XRES* a kryptografický materiál *IK, CK*.

Zařízení porovná jim spočtené *MAC-A* s *MAC-A* z jim přijatého autentizačního vektoru, pokud se rovnají, pak je síť autentizována. Zařízení odešle spočtené *XRES* jako *RES*.

Síť porovná *XRES* s *RES*. Pokud jsou stejné, pak je účastník autentizován.

Nyní máme obě strany autentizovány a navíc máme k dispozici kryptografický materiál *IK* (*integrity key*) a *CK* (*ciphering key*). Nejprve (ve 3G) se opravdu jeden používal k ochraně integrity a druhý k šifrování, později se přešlo na to, že se oba klíče společně derivují (obr. 7.7) a teprve výsledkem jsou šifrovací klíče, resp. klíče pro ochranu integrity.

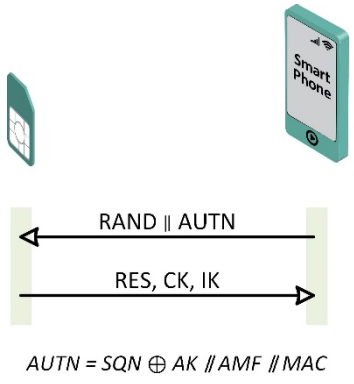
Prakticky se tato autentizace používá pro autentizaci účastníka a sítě na celou dobu jeho přihlášení k síti. Kdykoliv síť potřebuje re-autentizaci, tak už bez zadávání PIN se autentizace zopakuje. (Např. při překročení státní hranice nemusíme zadávat PIN.) Praktickou nevýhodou je, že takto má smysl zpoplatňovat jen laciné služby. Pokud bychom chtěli podat např. bankovní příkaz, pak je velkým rizikem zcizení zařízení, nebo umístění zlomyslného kódu do účastníkova zařízení, který by autorizoval příkazy automatizovaně na pozadí.

V kap. 19 se setkáme aplikaci mechanismu AKA i pro jiné případy než jen ke klasické autentizaci účastníka do mobilní sítě.

6.1 Funkce čipové karty

Sdílené tajemství K je na straně uživatele (tj. mobilního zařízení) udržováno zpravidla v interních souborech čipové karty USIM, tj. v souborech které nejsou „viditelné“ mimo operační systém čipové karty – blíže viz kap. 18.

Jelikož sdílené tajemství K neopouští čipovou kartu USIM, tak výpočty mechanismu AKA musí provádět čipová karta USIM. Na obr. 6.3 je znázorněn příklad komunikace mobilního zařízení s USIM. V tomto případě USIM vrací kromě odpovědi RES i kryptografický materiál CK a IK. V případě ISIM kryptografický materiál CK a IK zůstává v čipové kartě, která sama provádí příslušné kryptografické operace. To je možné proto, že ISIM provádí pouze autorizaci, kdežto USIM generuje kryptografický materiál na zabezpečení toku dat. Zabezpečení celého toku dat by bylo pro čipovou kartu příliš náročné.



obr. 6.3 AKA mechanismus zpravidla počítá čipová karta USIM (nikoliv mobilní zařízeni)

7. EPS

EPS (= LTE + EPC) zajišťuje „jen“ připojení mobilních zařízení k IP síti, přesto je EPS výrazně komplikovanější než připojení domácího počítače k poskytovateli internetu.

EPS se skládá z řady entit. Entita **MME** je zodpovědná za správu komunikace mezi mobilním zařízením a sítí, za alokaci datových nosičů *(data bearers)*, za přihlášení účastníka do sítě, během kterého se ustanoví kryptografický materiál atd. Zajímavé je, že mezi mobilním zařízením a MME je základnová stanice **eNB**. Základnová stanice, tak mechanicky předává požadavky mezi mobilním zařízením a MME. Výjimkou je zejména prvotní přihlášení účastníka do sítě (obr. 7.5), na jehož počátku je komunikace mezi mobilním zařízením a eNB. Teprve, až když je alokován radiový nosič *(Radio Bearer)*, tak eNB začne předávat data mezi mobilním zařízením a MME. Pro předávání těchto dat slouží protokol NAS *(Non-Access Stratum)*.

Entita **SGW** je zodpovědná za přenos dat z/do IP sítě. Někdy se říká, že SGW je, z hlediska účastníka, kotvou v mobilní síti, protože ať se účastník pohybuje v sítí kdekoliv, tak jeho paket prochází přes SGW. SGW totiž zajišťuje datové nosiče (*data bearers*) pro přenos uživatelských dat.

Entita **PGW** je pak branou do IP sítě. Máme tři typy IP sítí, do kterých se předávají IP pakety: internet, IPX pro roaming a IMS pro poskytování aplikačních služeb (pro „telefonování“).

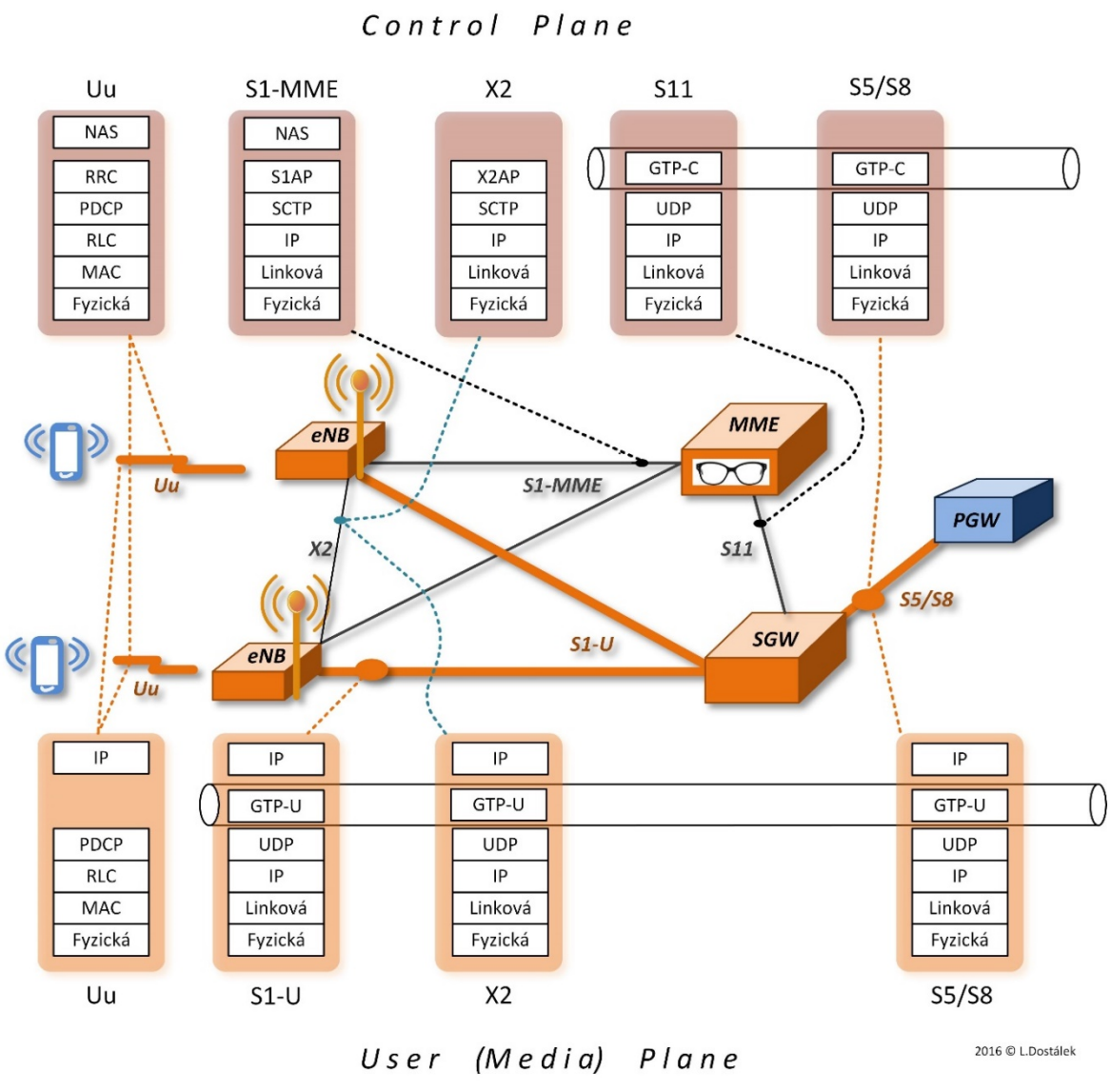
Dále máme entity **PCRF** a **HSS**, které už stojí trochu mimo EPS. Entita PCRF zodpovědná za QoS *(Quality-of-Service)* a za zpoplatnění. Entita HSS zase spravuje databázi informací o uživatelích.

Zmíněné entity jsou logickými entitami, tj. fyzicky mohou být např. MME, SGW a PGW integrovány do jednoho uzlu. Dokonce díky vizualizaci sítí mohou být mnohé zmíněné entity technicky realizovány jedním výpočetním systémem, který pochopitelně může být i zdvojen kvůli dosažení vysoké dostupnosti.

Spojení mezi jednotlivými entitami se popisuje pomocí referenčních bodů. Jednotlivé referenční body EPC a jejich síťové modely jsou znázorněny na obr. 7.1. (Nejsou zde uvedeny referenční body protokolu Diameter, ty jsou popsány v kap. obr. 8.13)

Referenční body EPC tvoří dvě skupiny:

- *Control Plane* – tyto referenční body zajišťují signalizaci sítě. Zajišťují komunikaci mezi jednotlivými entitami. Jedná se o referenční body:
  - S1-MME (někdy označovaný též jako S1-C). Tento referenční bod přenáší data mezi eNB a MME. Jako aplikační protokol je zde definován protokol S1AP.
  - S11, který zajišťuje komunikaci mezi MME a SGW,
  - Část referenčního bodu X2 určená pro signalizaci sítě, která zajišťuje vzájemnou komunikaci mezi jednotlivými eNB. Jako aplikační protokol je zde definován protokol X2AP.
  - Část referenčního bodu S5/S8, která zajišťuje signalizaci sítě.



obr. 7.1 Referenční body EPC

- Referenční body protokolu Diameter (viz kap. obr. 8.13) zajišťující komunikaci s HSS, EIR a PCRF.

- *User (Media) Plane* – referenční body zajišťující přenos účastnických dat (účastnikových IP datagramů). Tyto referenční body

využívají pro komunikaci mezi entitami protokol TCP/IP, který nese pakety tunelovacího protokolu GTP-U. GTP-U pak tuneluje účastníkovy IP datagramy. Jedná se o tunelování IP nad IP. Tunelovat lze i do cizích sítí, což se využívá v roamingu.

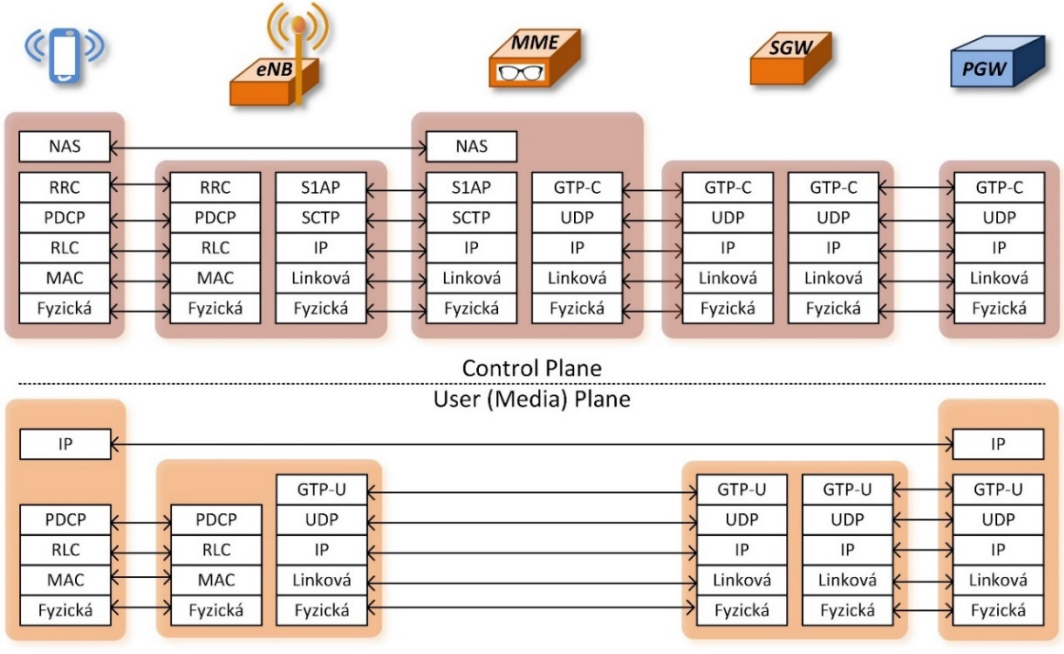
„Spodní“ IP je komunikací v rámci EPC, nemusí ani využívat DNS (resp. může využívat DNS z IPX). „Horní“ IP je pak uživatelova komunikace. Z hlediska bezpečnosti je důležité, že „spodní“ IP zabezpečuje komunikaci pomocí IPsec. Jedná se o referenční body:

- S1-U, který slouží pro popis přenosu dat mezi eNB a kotvou SGW.
- Část referenčního bodu X2 určená pro přenos uživatelských dat, která zajišťuje vzájemnou komunikaci mezi jednotlivými eNB.
- Část referenčního bodu S5/S8, která zajišťuje přenos uživatelských dat. Pokud se referenčním bodem S5/S8 přenáší uživatelova data, pak se použije protokol GTP-U.

Zvláštním případem je referenční bod Uu, který zajišťuje komunikaci mezi mobilním zařízením a eNB. Referenční bod Uu nepoužívá pro transport dat, na rozdíl od ostatních referenčních bodů, protokoly rodiny TCP/IP

7.1 Referenční bod Uu

Referenční bod Uu má jeden síťový model pro *Control Plane* a jiný pro *User (Media) Plane*. *Control Plane* využívá protokol RRC (*Radio Resource Control*) [12]. *User Plane* pak protokol IP. Společně pak využívají protokoly: PDCP (*Packet Data Convergence Protocol*) [13], RLC (*Radio*



obr. 7.2 Síťový model EPC

Link Control) [14] a MAC (*Medium Access Control*) [15].

RRC mj. zajišťuje:

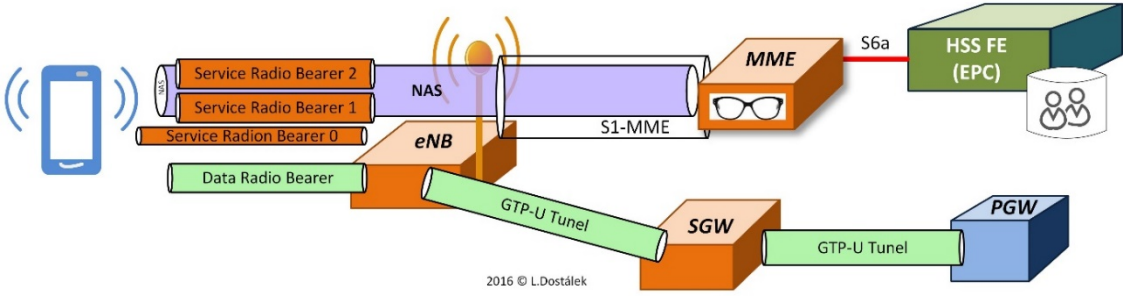
- Sestavování, správu a ukončování RRC spojení.
- Sestavování, správu a ukončování radiových signalizačních a datových nosičů.
- Přenos paketů protokolu NAS.

PDCP zajišťuje mj.:

- Kompresi IP záhlaví, aby se redukovalo množství dat přenášených radiovým rozhraním. Používá se algoritmus ROHC *(Robust Header Compression)* [16].
- Šifrování a ochranu integrity přenášených dat (viz kap. 7.6 a 7.7).
- Zamezení duplikace přenášených paketů a doručování paketů ve správném pořadí.
- Pro každý radiový datový nosič je jedna entita PDCP v rámci mobilního zařízení.

RLC zajišťuje mj.:

- Segmentaci/slučování přenášených paketů.
- Retrasmise ztracených datových paketů, detekce duplikovaných paketů a doručování paketů ve správném pořadí. Tento mechanismus může provádět i MAC.
- Pro každý radiový datový nosič je jedna entita RLC v rámci mobilního zařízení.
- Velikost datového paketu je variabilní, závisí na přenosové rychlosti. Se zvyšující se přenosovou rychlostí se zvětšuje velikost paketu, aby se snížila režie přenosu.



obr. 7.3 Radiové datové nosiče

MAC zajišťuje mj.:

- Multipex logických kanálů
- Prioritizaci logických kanálů.
- Retrasmisi ztracených datových paketů, detekce duplikovaných paketů pomocí hybrid ARQ protokolu [17].

PHY *(Physical Layer)* provádí:

- Kódování/dekódování

- Modulování/demodulování
- Multi-antena mapping atd.

Mezi mobilním zařízením a základnovou stanicí eNB Vznikne sada radiových datových nosičů:

- *Signalling Radio Bearer* 0 (SRB0), který slouží ke komunikaci mobilního zařízení a základnové stanice. Přenáší úvodní komunikaci (*RRC Connection Request, RRC Connection Setup* atd.)
- *Signalling Radio Bearer* 1 (SRB1), který přenáší pakety protokolu NAS dříve než je aktivováno zabezpečení přenosu.
- *Signalling Radio Bearer* 2 (SRB2), který přenáší pakety protokolu NAS po aktivaci zabezpečení.
- *Data Radio Bearer* – slouží k vytvoření datových nosičů (*bearer*).

Tyto radiové datové nosiče se vkládají do logických kanálů, ty do transportních kanálů. Nakonec se transportní kanály vloží do fyzických kanálů (obr. 7.4).

7.1.1 Logické kanály

BCCH *(Broadcast Control Channel)* - tímto kanálem síť šíří informace o sobě. Mobilní zařízení tyto informace může použít k přihlášení do sítě.

PCCH *(Paging Control Channel)*, používá síť pro výzvu mobilnímu zařízení, když síť nezná jeho polohu (v jaké buňce se nachází) nebo když mobilní zařízení je ve stavu nečinné. Může se šířit současně v několika buňkách.

CCCH *(Common Control Channel)*, jedná se o obousměrný kanál, který se používá při navazování a opětovném navazování spojení pomocí protokolu RRC.

DCCH *(Dedicated Control Channel)*, jedná se o oboustranný kanál, který se používá pro přenos řídících informací během RRC spojení. Tj. přenáší:

- SRB1 *(Service Radio Bearer 1)* používaný pro přenos zpráv protokolu RRC
- SRB2 *(Service Radio Bearer 2)* používaný pro přenos zpráv protokolu NAS

DTCH *(Dedicated Traffic Channel)*, oboustranný datový kanál pro přenos uživatelských dat.

MCCH *(Multicast Control Channel)* a **MTCH** *(Multicast Traffic Channel)* jsou kanály určené pro MBMS *(Multimedia Broadcast/Multicast Service)*.

7.1.2 Transportní kanály

BCH *(Broadcast Channel)* je určen pro vysílání tzv. MIB *(Master Information Block)* logického kanálu BCCH. Tento blok informací obsahuje základní informace pro volbu a navázání spojení se sítí konkrétního operátora (přenosové rychlosti, konfigurace buněk atd.).

PCH *(Paging Channel)* je určen pro přenos PCCH kanálu, podporuje tzv. přerušovaný příjem *(discontinuous reception - DRX)* v předem daných časových okamžicích při nečinném mobilním zařízení, což umožňuje šetřit zdroj mobilního zařízení.

DL-SCH *(Downlink Shared Channel)* je hlavním transportním kanálem LTE.

UL-SCH *(Uplink Shared Channel)* je obdobou DL-SCH pro Uplink.

MCH *(Multicast Channel)* je určen pro podporu MBMS. MBMS může využívat i kanál DL-SCH, tj. tento kanál nemusí být používán.

RACH *(Random-Access Channel)* je určen pro náhodný přístup, nenese žádná transportní data.

7.1.3 Fyzické kanály

PDSCH *(Physical Downlink Shared Channel)* je to hlavní kanál pro komunikaci s konkrétním mobilním zařízením (unicast). Nese jak uživatelská data, tak i řídící informace.

PBCH *(Physical Broadcast Channel)* šíří informace o síti, které může následně využít mobilní zařízení pro přihlášení se do sítě.

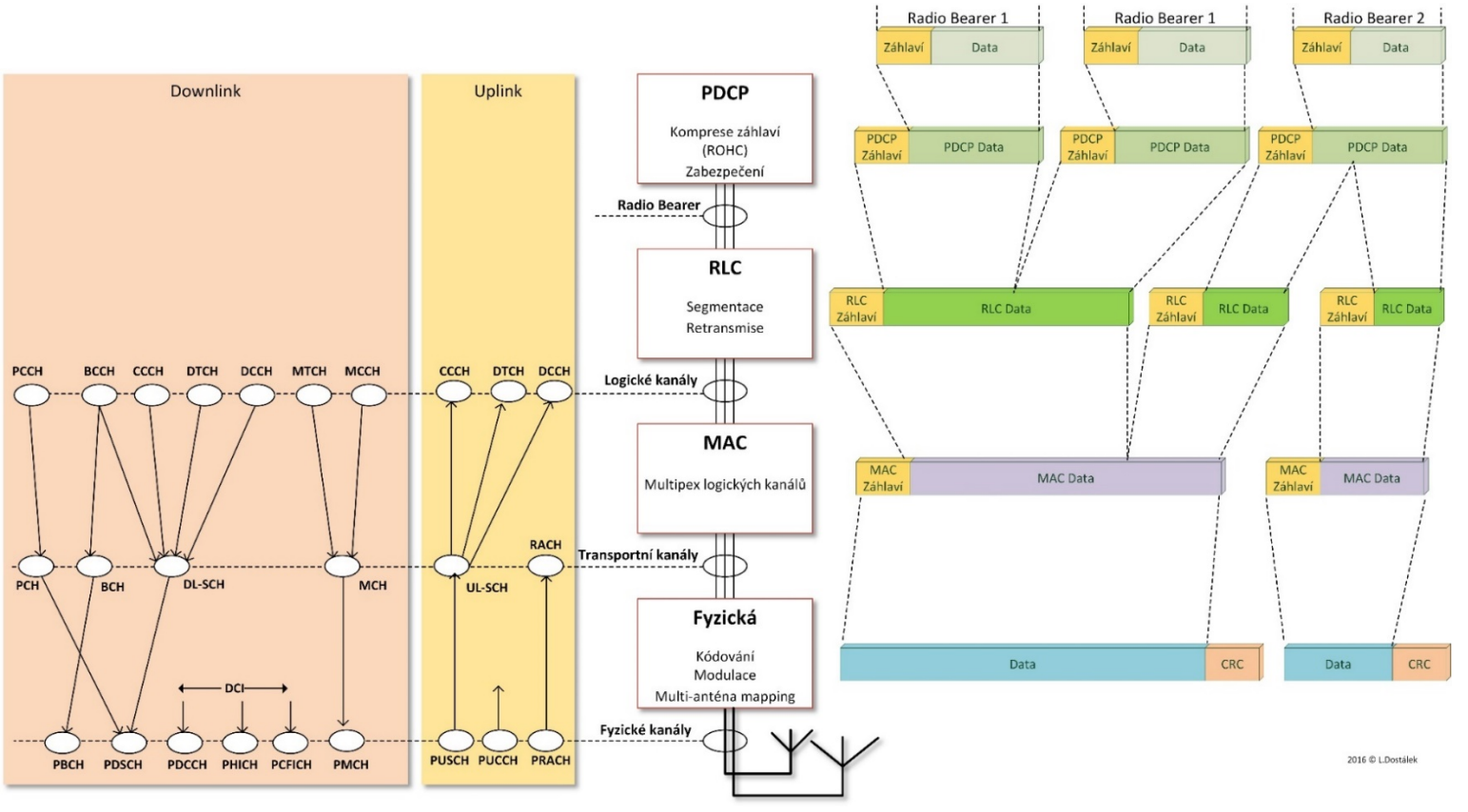
PMCH *(Physical Multicast Channel)* kanál určený pro MBMS (viz výše).

PDCCH *(Physical Downlink Control Channel)*, **PHICH** *(Physical Hybrid-ARQ Indicator Channel)* a **PCFICH** *(Physical Control Format Indicator Channel)* jsou kanály pro řízení Fyzické a MAC vrstvy *(downlink control information - DCI)*. Poskytují pro správné přijímání a dekódování přijímaných datových paketů.

PUSCH *(Physical Uplink Shared Channel)* je obdobou PDSCH pro Uplink.

PUCCH *(Physical Uplink Control Channel)* poskytuje eNB informace o situaci v mobilním zařízení, které jsou důležité např. pro protokol hybrid-ARQ.

PRACH *(Physical Random-Access Channel)* - používá se při navazování spojení mobilního zařízení se sítí.



obr. 7.4 Logické, transportní a fyzické kanály využívané referenčním bodem Uu

7.2 Úvodní přihlášení do sítě

Na obr. 7.5 je zjednodušeně znázorněno schéma přihlášení účastníka do sítě. Nejprve účastník vyhledá síť a začne komunikovat se základnovou stanicí. Nejprve mobilní zařízení kontaktuje eNB na kanálu RACH/PRACH s náhodným přístupem. V dalším kroku dojde k vytvoření spojení na úrovni protokolu RRC (konkrétně pomocí SRB0). Tato komunikace je nezabezpečená, lze tedy odchytit identifikaci účastníka, pod kterou se hlásí do sítě, proto se IMSI skrývá až do zabezpečené komunikace – použije se S-TMSI.

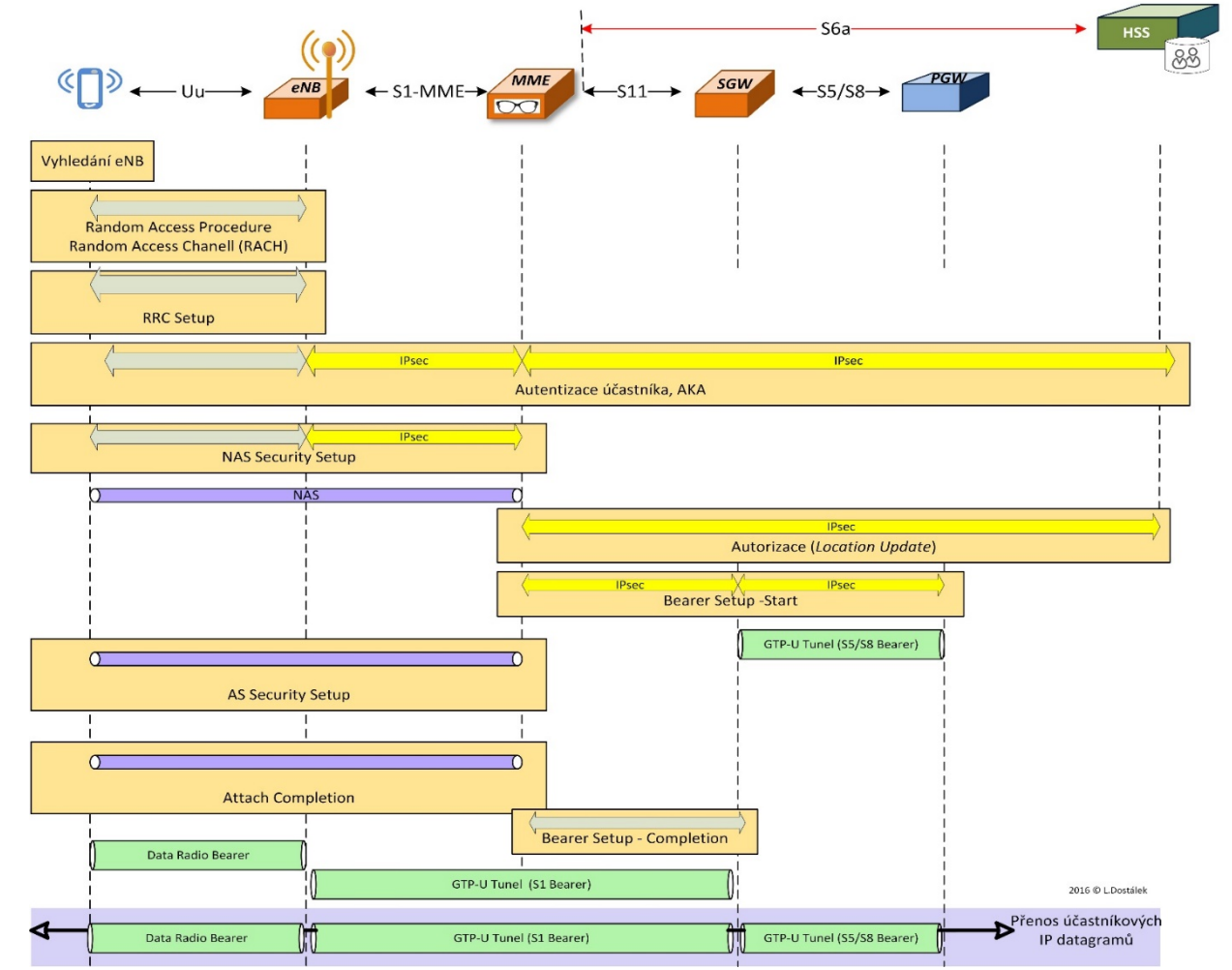
Následně dochází k autentizaci účastníka. V tomto kroku vstupuje do hry entita MME (eNB bude jen mechanicky předává pakety protokolu NAS mezi účastníkovým zařízením a MME). K autentizaci je použit mechanismus AKA (obr. 7.6). Výsledkem je autentizace účastníka a autentizace sítě. Dále byl ustanoven kryptografický materiál IK a CK, který bude následně použit pro zabezpečení komunikace (viz odstavec 7.5).

Nyní máme vytvořen bezpečný kanál mezi mobilním zařízením a MME. Může být provedena autorizace účastníka (SRB2), tj. MME jsou odeslány lokalizační údaje a vráceny jsou specifikace nasmlouvaných služeb. Byly získány veškeré údaje pro vytvoření části datového nosiče mezi SGW a PGW (*S5/S8 Bearer*).

Nyní je třeba vytvořit datový nosič. Obdobně, jako při zabezpečení protokolu NAS, dojde k vytvoření šifrovacích klíčů a tajemství po zajištění integrity datového přenosu pro datový nosič (*AS Security Setup*).

Poté dojde k potvrzení vytvoření spojení a vzniknou tři části datového nosiče: *Data Radio Bearer*, S1 Bearer a S5/S8 Bearer. Napojením těchto datových nosičů vznikne datový nosič (defaultní).

Zatímco *Data Radio Bearer* je zabezpečen na bázi mechanismu AKA, tak S1 Bearer a S5/S8 Bearer se zpravidla zabezpečuje pevným IPsec tunelem mezi entitami.



obr. 7.5 Přihlášení do sítě

7.3 NAS

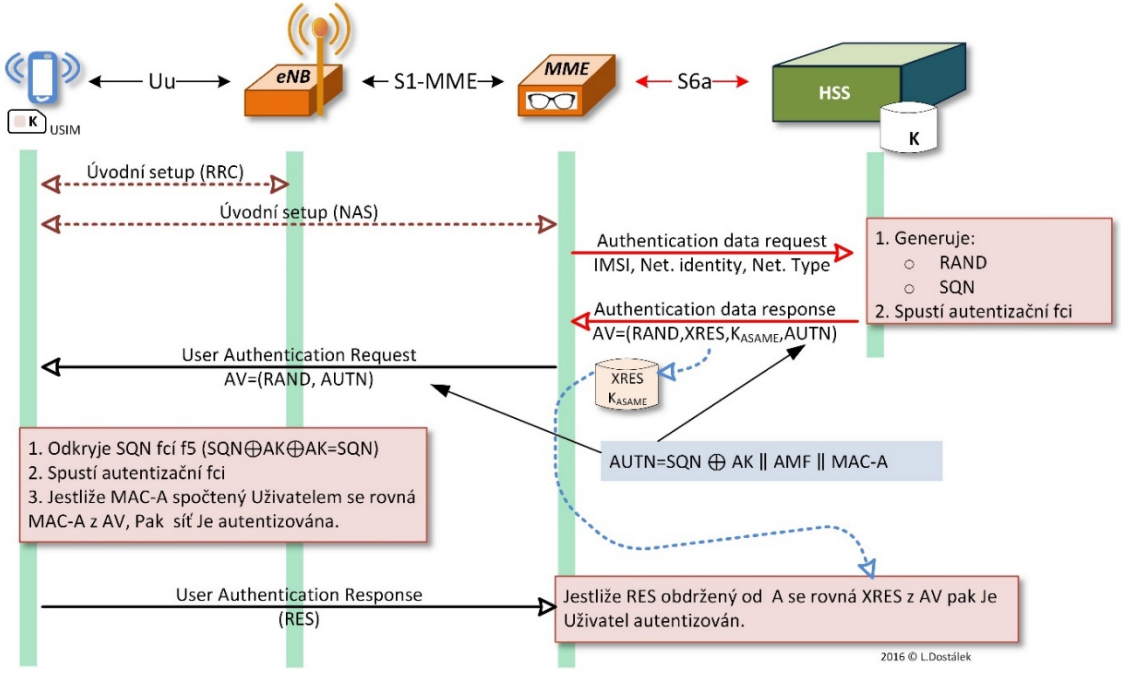
Protokol NAS (*Non Access Stratum*) [18] se skládá ze dvou částí: EMM (*EPS Mobility Management*) a ESM (*EPS Session Management*).

7.3.1 EMM

EMM spravuje stav připojení mobilního zařízení v síti. Zařízení je nejprve ve stavu vypnuto, pak probíhá registrace, jejímž výsledkem je stav připojeno. Po určitém stavu nečinnosti se zařízení dostane do stavu nečinné (*idle*). Z tohoto stavu může přejít do stavu připojeno a z něj de-registrací do stavu vypnuto.

Ve stavu nečinné je síti známa poloha zřízení v oblasti nazývané *tracking area*. V případě, že se zařízení přesune do jiné *tracking area*, tak zařízení přejde po stavu připojeno a zařízení odešle zprávu TAU (*Tracking Area Update*). Kromě zprávy TAU je definována celá řada dalších zpráv, které zajišťují jednotlivé procedury. Např.:

- *Attach* – procedura používaná k připojení k EPS.
- *Datach* – procedura pro odpojení od EPS.
- *Authentication* – procedura pro autentizaci AKA mechanismem (obr. 7.6).



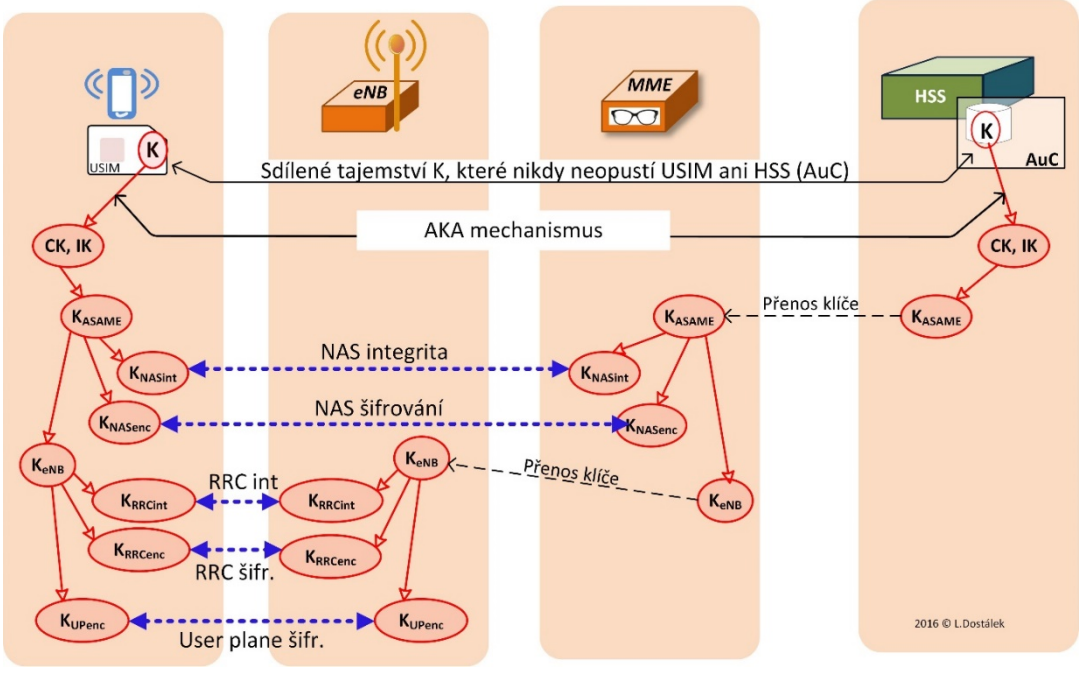
obr. 7.6 AKA mechanismus implementovaný EMM protokolu (IC a IK jsou obsaženy v K_{ASAME})

- *Identity request* – procedura, kterou síť žádá účastníkovo zařízení o identifikaci (IMSI a IMEI).
- *Security mode* – přechod do zabezpečeného přenosu.
- *NAS transport* – procedura pro přenos SMS zpráv přes NAS protokol (viz kap. 7.3).

7.3.2 ESM

Tento protokol je určen pro aktivaci, správu a deaktivací datových nosičů (*Bearers*). Během EMM procedury *Attach* (obr. 7.5) vznikne tzv. defaultní datový nosič (*EPS Default Bearer*). Další tzv. dedikované datové nosiče je možné vytvářet pomocí procedur protokolu ESM. Máme např. procedury:

- *Activate Default Bearer* – aktivuje defaultní datový nosič.
- *Activate Dedicated Bearer* – aktivuje dedikovaný datový nosič.
- *Modify EPS Bearer* – modifikuje vlastnosti datového nosiče.
- *PDN Connectivity* – aktivace připojení s externí sítí (např. do internetu)
- *PDN Disconnect* – de-aktivace připojení k externí síti.



obr. 7.7 Hierarchie klíčů v EPS

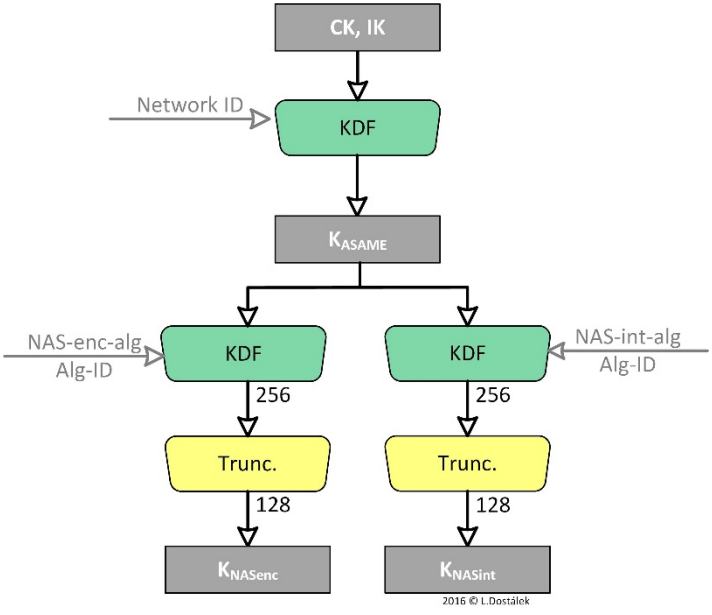
7.4 GTP

Na obr. 7.1 je také vidět využití protokolů GTP-C *(GPRS Tunnelling Protocol for Control Plane)* [19] a GTP-U *(GPRS Tunnelling Protocol User Plane)* [20]. Jedná se o tunelovací protokoly, které tunelují IP přes IP. Z hlediska architektury EPS je jejich význam zásadní. Mj. umožňují:

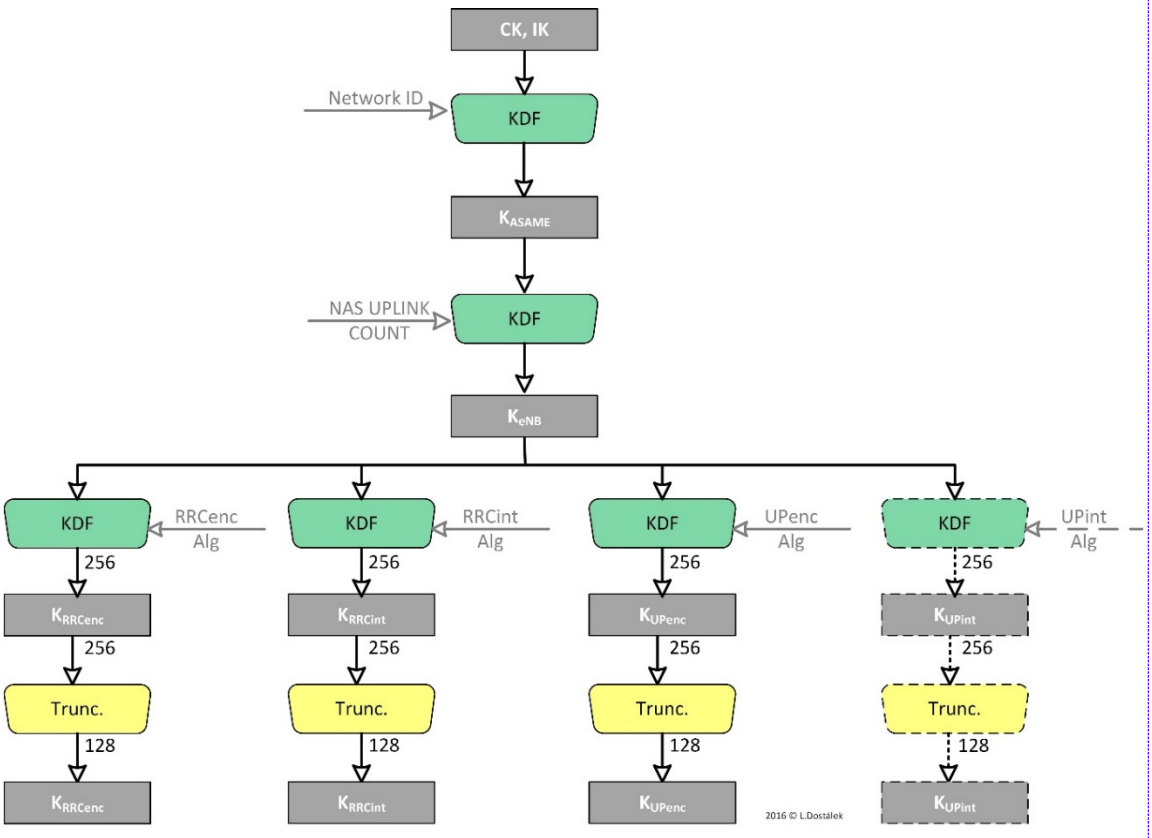
- Tunelovat IP datagramy skrze EPC na PGW, odkud se předávají dále do sítě (internet, IMS apod.). Jenže na obr. obr. 7.1 je znázorněna jedna síť, ale protokoly GTP umožňují tunelovat IP datagramy i do cizích sítí v případě roamingu. Tj. tunelují IP datagramy na PGW nikoliv navštívené sítě, ale domovské sítě.
- Umožňují oddělit „spodní“ UDP/IP komunikaci mezi entitami EPC od „horní“ IP komunikace (tunelovaná přes GTP-U), která přenáší účastnická data. Z hlediska DNS bude „spodní“ IP komunikace používat vlastní DNS, tj. vlastní kořenové DNS servery, nebo kořenové servery IPX (nebo DNS vůbec nebude používat). „Horní“ IP komunikace bude používat kořenové DNS sítě, do které příslušný datový nosič (tj. APN) míří: DNS servery internetu, DNS servery IPX nebo DNS servery IMS (pokud nepoužívají servery IPX).

Jak již bylo zmíněno, GTP protokoly (*GPRS Tunnelling Protocol*) jsou dva:

- GTP-C (*GPRS Tunnelling Protocol or Control plane (GTPv2-C))* [19].



obr. 7.8 Odvození K_{ASAME}, K_{NASint} a K_{NASenc}
(Trunc. značí odříznutí šifrovacího bloku na požadovanou délku)



obr. 7.9 Odvození K_{eNB}, K_{RRCenc}, K_{RRCint}, K_{UPenc} a K_{UPint}
(Trunc. značí odříznutí na požadovanou délku šifrovacího bloku)

- GTP-U (*GPRS Tunnelling Protocol User Plane (GTPv1-U)*) [20].

Zatímco GTP-U zajišťuje vlastní tunelování IP přes IP, tak GTP-C zajišťuje zřizování, správu a monitorování tunelů. Jako je např.:

- *Create Session Request.*
- *Create Session Response.*
- *Create Bearer Request.*
- *Create Bearer Response.*
- *Bearer Resource Command.*

K monitorování dostupnosti používá příkazy:

- *Echo Request.*
- *Echo Response,* atd.

Nevýhodou těchto, protokolů je, že to, jako jedny z mála dále popisovaných protokolů, nejsou standardy IETF RFC – jsou to „jen" standardy 3GPP. Pokud se v budoucnu přejede na roaming typu „*Local breakout*" (viz kap. 5.1.2), tak se jejich význam ještě sníží. Navíc se jedná o značně

komplikované protokoly, které řeší i některé problémy transportní vrstvy. Dalším netriviálním problémem je přechod účastníka např. mezi 4G a 3G beze změny IP adresy účastníka (pokud navštívené buňce např. není 4G pokrytí). Důsledkem je, že aktuální verze těchto protokolů implementuje jen několik málo dodavatelů.

7.5 Odvozování kryptografických klíčů

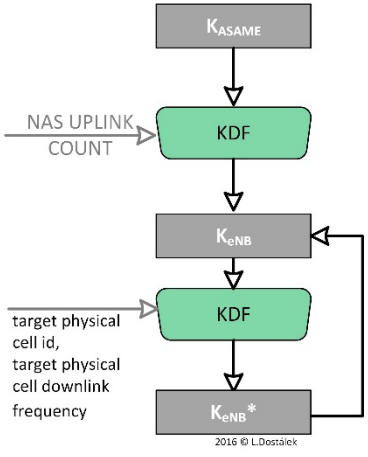
Po úspěšné autentizaci AKA mechanismem je jak na straně HSS, tak i na straně účastníkova zařízení připraven kryptografický materiál CK a IK. Z tohoto materiálu se odvozují šifrovací klíče a klíče pro zajištění integrity.

Asi překvapivé je, že CK a IK nejsou sdíleny mezi účastníkovým zařízením a MME, jak jsem doposud pro zjednodušení uváděl. V případě EPS se nepoužívají přímo CK a IK, ale od nich odvozený klíč K_{ASAME}. Teprve z něj se odvozuje další kryptografický materiál (obr. 7.7).

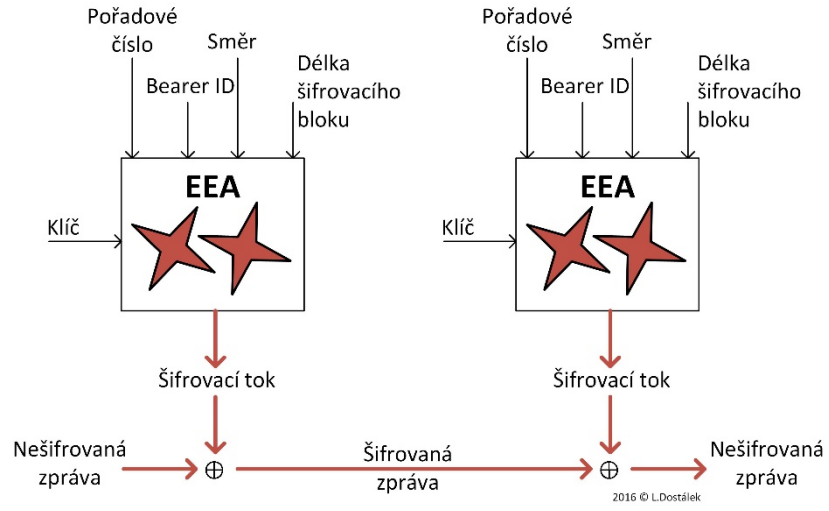
Důležité je, že mechanismus musí podporovat i pohyb účastníků mezi buňkami. Tj. změnu komunikace s jiným eNB.

Pro zabezpečení komunikace mezi účastníkovým zařízením a eNB budeme odvozovat následující klíče:

- **K_{NASint}** – Klíč po zajištění integrity komunikace protokolem NAS mezi účastníkovým zařízením a MME.
- **K_{NASenc}** – Klíč po šifrování komunikace protokolem NAS mezi účastníkovým zařízením a MME.
- **K_{RRCint}** - Klíč po zajištění integrity komunikace protokolem RRC mezi účastníkovým zařízením a eNB.
- **K_{RRCenc}** - Klíč po šifrování komunikace protokolem RRC mezi účastníkovým zařízením a eNB.



obr. 7.10 Odvození kryptografického materiálu pro další navštívený eNB



obr. 7.11 EPS Encryption Algorithm (EEA)

- **K_{UPenc}** - Klíč po šifrování datového nosiče mezi účastníkovým zařízením a eNB.
- **K_{UPint}** – Volitelný klíč pro zajištění integrity datového nosiče mezi účastníkovým zařízením a eNB.

Klíče se odvozují funkcí KDF [21] [22]:

```
Odvozený klíč = KDF (Klíč, S) =
     HMAC-SHA-256 (Klíč, S)
```

Jednocestná funkce `HMAC-SHA-256` je popsána v [22], řetězec `S` obsahuje zřetězení parametrů a jejich délek:

```
S = FC ‖ P0 ‖ L0 ‖ P1 ‖
   L1 ‖ P2 ‖ L2 ‖ P3 ‖
   L3 ‖... ‖ Pn ‖ Ln
```

Kde:

`FC` je předem známý bajt odlišující různé instance použití algoritmu.

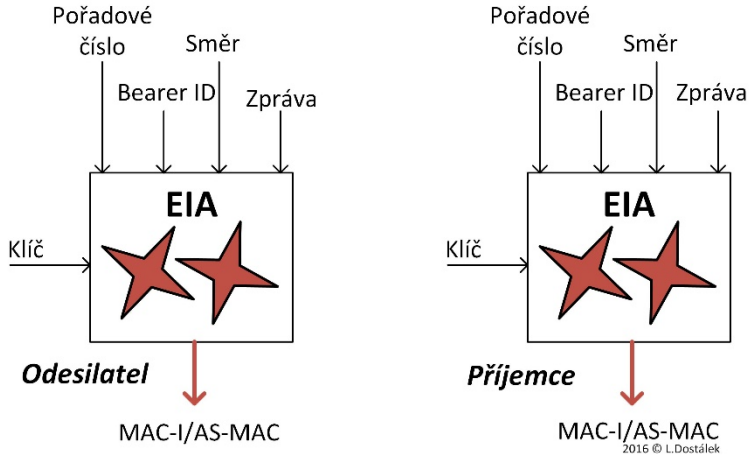
`P0` až `Pn` obsahuje vstupní parametr

`L0` až `Ln` obsahuje délku vstupního parametru.

Při přechodu do jiné buňky se musí pro základnovou stanici této buňky (eNB) odvodit nový **K_{eNB}** (obr. 7.10).

7.6 Šifrování dat mezi zařízením účastníka a eNB

Šifrování se provádí proudovou šifrou označovanou jako EEA (*EPS Encryption Algorithm*) [7]. Je generován šifrovací tok, který se operací XOR *(eXclusive OR)* aplikuje na vstupující data. Týž šifrovací proud se aplikuje na šifrovaná data, čímž se získají původní (nešifrovaná) data. Viz obr. 7.11, kde:



obr. 7.12 EPS Integrity Algorithm (EIA)

- Klíč je 128 bitů dlouhý klíč odvozený v předchozím odstavci.
- 32 bitové Pořadové číslo (*count*) je pořadové číslo, které musí být použito pouze jedno pro daný klíč $\mathbf{K_{eNB}}$. Táž číselná sekvence může být použita, jak pro šifrování, tak pro zajištění integrity.
- 5 bitová identifikace datového nosiče (*Bearer ID*)
- 1 bitový směr určuje, jestli se jedná o přenos dat z účastníkova zařízení do eNB (*uplink*) – hodnota 0, nebo o opačný směr (*downlink*) – hodnota 1.

Tč. jsou podporovány následující EEA algoritmy:

- EEA – nulový algoritmus
- 128-EEA1 – založený na algoritmu SNOW 3G.
- 128-EEA2 – založený na algoritmu 128-bit AES v CTR módu.
- 128-EEA3 – založený na algoritmu ZUC.

7.7 Integrita dat mezi zařízením účastníka a eNB

Obdobně se postupuje i v případě výpočtu kryptografického kontrolního součtu (MAC), který zajišťuje integritu přenášených dat (obr. 7.12) protokolem EIA (*EPS Integrity Algorithm*).

Tč. jsou podporovány následující EIA algoritmy:

- 128-EIA1 – založený na algoritmu SNOW 3G
- 128-EIA2 – založený na algoritmu 128-bit AES v CMAC módu
- 128-EIA3 – založený na algoritmu ZUC.

7.8 Útoky

Signalizační bouře	Signalizační bouře je obdobou *black out* v energetických sítích. Vychází z předpokladu, že linky, které zajišťují *Control Plane* jsou nejméně o řád méně kapacitní, než linky, které zajišťují *User (media) Plane*. Vygenerováním silného provozu, který může být případně multiplikován, dojde k zahlcení *Control Plane,* a tím i výpadku celé sítě (byť *User Plane* má dostatek kapacity). Veřejné známé signalizační bouře byly způsobeny chybou software, která příslušný sítový provoz vygenerovala. Došlo k výpadku jedné entity, který způsobil výpadek dalších entit, až celé sítě. Pravděpodobně stejného účinku by šlo dosáhnout i zlomyslným generováním např. zpráv *Tracking Update* (viz 7.3.1) apod.
Útoky z IPX	V současné době je síť IPX více či méně považována za důvěryhodnou. Je třeba tento předpoklad opustit, když zejména dnes víme, že DDoS útoky v internetu organizují přímo státy nebo jimi podporované organizace.
DDoS Internet, IPX	V současné době je nejvíce DDoS útoků vedeno pakety protokolu DNS, protože jsou dopravovány přes nepotvrzované UDP, tj. útočník má volnou ruku v generování paketů. Problém je, že protokoly SIP, RTP atp. využívají též UDP, tj. lze očekávat DDoS útoky obdobného rozsahu i na tyto protokoly.
Veřejná IP adresa	Se zavedením IPv6 dostávají účastnická zařízení veřejnou adresu. Tj. jsou přímo dostupné z internetu. Stačí si uvědomit, že pouhým odesíláním „ping“ z internetu na tuto adresu se čerpá kredit.
Prolomení se do „spodního“ IP	Mezi „spodním“ a „horním“ IP je protokol GTP. Tj. z veřejného internetu nelze adresovat rozhraní entit EPC. Otázkou je, jestli v budoucnu (např. chybou SW) nedojde k útokům touto cestou (tj. jestli se útočník z internetu nedostane do spodního IP). Útočník by mohl paralyzovat celou síť. V minulosti takové útoky byly málo časté, protože telekomunikační infrastruktura běžela na jiném protokolu (SS7). Avšak i do této infrastruktury jsou známy útoky.

Útoky na eNB	Útoky ne eNB jsou značně náročné – podstatně jednodušší je útočit v teple domova na HeNB.
HeNB	HeNB je zpravidla ve vlastnictví účastníka. Zatímco radiová komunikace je dostatečně zabezpečeně, tak „uvnitř“ HeNB je dešifrována a převáděna na IPsec tunel. HeNB je přitom zpravidla ve vlastnictví účastníka, tj. potencionálního útočníka.
Útoky na jádro sítě	Jelikož EPC patří do kritické infrastruktury, tak potencionálními útočníky mohou být i orgány cizích států, které mohou mít dostatek prostředků na útoky na jádro sítě. Což je pro běžného útočníka neproveditelné.
Útoky na mobilní zařízení	Útoky na účastníkovo zařízení zlomyslným kódem budou asi nejběžnějším typem útoku.

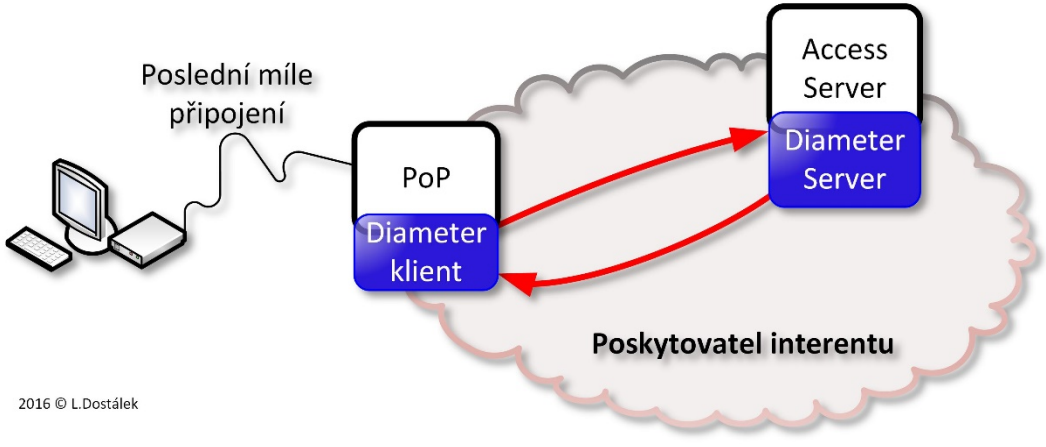
8. Diameter

Protokol Diameter (*Diameter Base Protocol*) [23] je protokolem nove generace pro autentizaci (*Authentication*), autorizaci (*Authorization*) a účtování (*Accounting*). Někdy s proto označuje také jako protokol AAA.

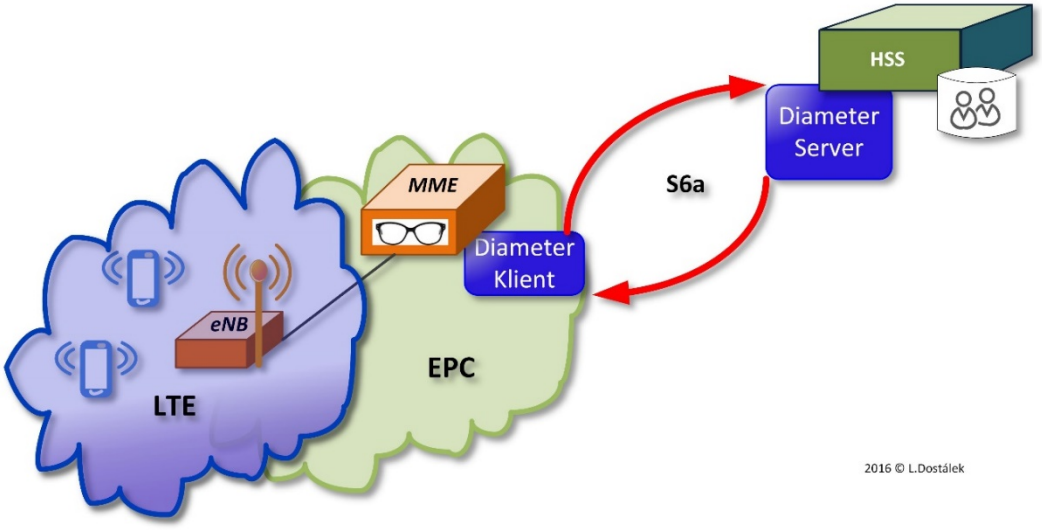
Jestliže něco označíme, jako novou generaci, pak je otázkou, co je tou předchozí generací. Za předchozí generaci je považován protokol RADIUS (*Remote Authentication Dial In User Service*) [24]. RADIUS (česky poloměr) je tedy předchůdcem protokolu Diameter (česky průměr). Tím ale podobnost mezi těmito protokoly končí. Neexistuje tu zpětná kompatibilita. Později bude zmíněno, že pro komunikace mezi entitou protokolu RADIUS a entitou protokolu Diameter je nutné mezi tyto entity vložit entitu *Diameter Translation Agent*, tj. jakýsi překladač z jednoho protokolu do druhého.

Problémů protokolu RADIUS byla celá řada. Asi největším problémem bylo výhradní využití protokolu UDP [25] na síťové vrstvě. V době vzniku protokolu RADIUS byl jedinou alternativou k protokolu UDP, protokol TCP [26]. Využití TCP by ale nebylo šťastné, protože by došlo k frontování např. autentizačních požadavků do „roury“ protokolu TCP, což by vedlo zvětšení prodlevy při autentizaci. Tyto problémy byly odstraněny využitím protokolu SCTP (kap. 17) na síťové vrstvě.

Protokol Diameter je protokolem typu klient/server. Jeho typické nasazení je nasazení na hraně poskytovatele sítě (např. Internetu, IMS apod.). Na obr. 8.1 je znázorněno využití protokolu Diameter mezi PoP (*Point of Presence*) poskytovatele internetu a jeho serverem pro řízení přístupu (*Access Server*). Na obr. 8.2 je zase znázorněno využití protokolu Diametr pro autentizaci účastníků LTE, tj. referenční bod S6a. V obou případech klient protokolu Diameter je součástí uzlu sítě, který nemá lokálně k dispozici



obr. 8.1 Využití protokolu Diameter pro autentizaci zákazníků poskytovatele internetu



obr. 8.2 Využití protokolu Diameter pro autentizaci účastníků LTE

autentizační informace. Požadavky na autentizaci předá klientu protokolu Diameter, který komunikuje se serverem protokolu Diameter a za jeho pomocí zprostředkuje připojení účastníka do sítě. Podobně jako o autentizační informace může klient protokolu Diameter žádat o server o autorizační, účtovací, kreditní nebo jiné informace.

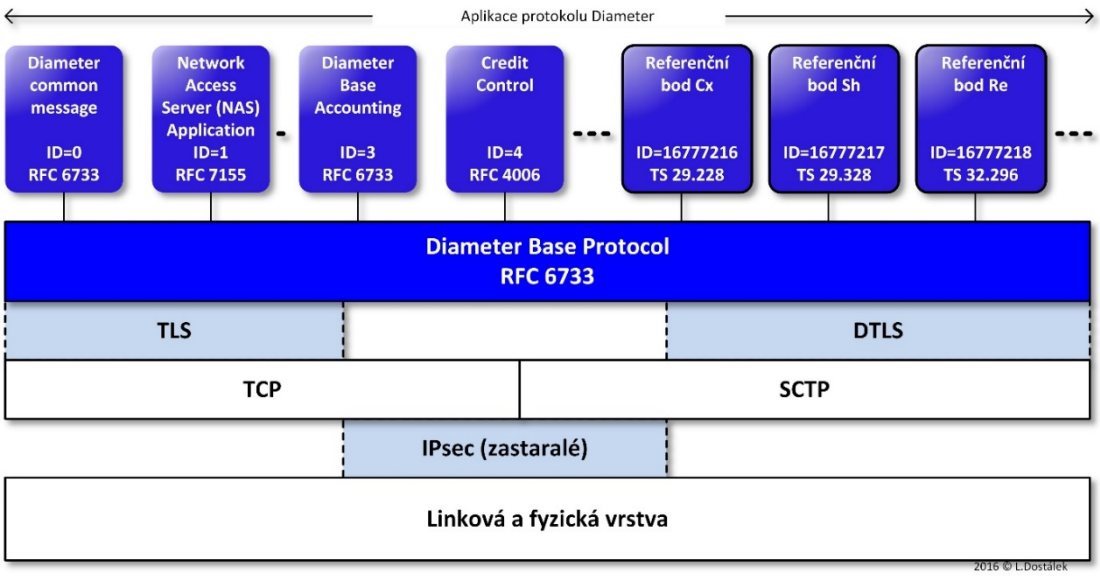
Uzly protokolu Diameter mohou participovat i ve složitější sítové topologii. Některé uzly mohou procovat jako agenti, tj. pro některé požadavky mohou pracovat jako servery, pro jiné zase jako klienti. Protokol Diameter umožňuje i serverem iniciované zprávy. Pomocí těchto zpráv je možné např. ukončit relaci konkrétního účastníka.

Kromě již zmíněné autentizace může protokol Diameter zajišťovat např.:

- Účtování využití síťových zdrojů za určité období. Např. *Diameter Base Accounting* – specifikovaný v [23], resp. *Off-line Charging* (kap. 8.11.14).
- Sledování výše kreditu u předplacených služeb. Např. *Diameter Credit Control Application* [27], resp. *On-line Charging* (kap. 8.11.13).

8.1 Architektura protokolu Diameter

Jelikož protokol Diameter je aplikačním protokolem, tak to, co leží nad aplikační vrstvou, již jsou aplikace, hovoříme tak o aplikacích protokolu Diameter, nebo o AAA aplikacích. Mnohé AAA aplikace definují své vlastní standardy, které jsou rozšířením protokolu Diameter. Aplikační protokol se oficiálně nazývá *Diameter*



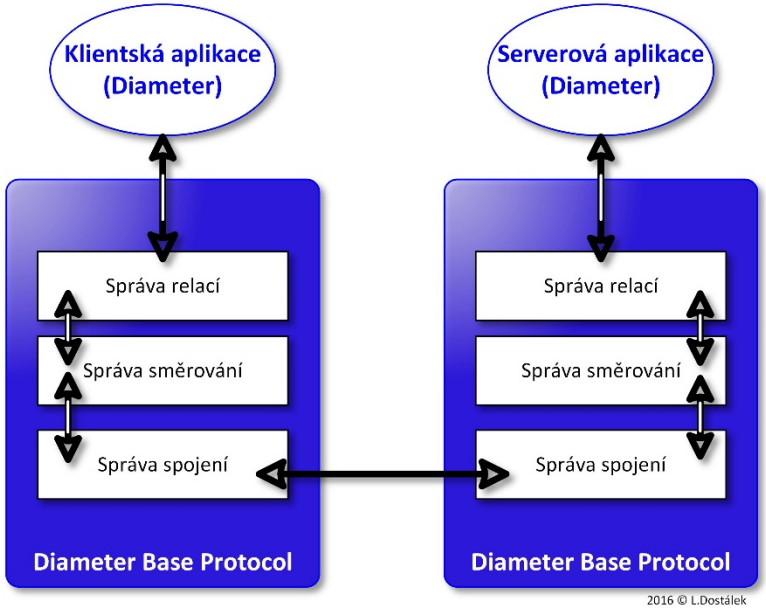
obr. 8.3 Síťový model protokolu Diameter

Base Protocol [23], a standardy, které jej rozšiřují, jsou „aplikace“ (obr. 8.3). Pro ty, kteří si pod pojmem „aplikace“ představující již aplikační program, tak je to trochu zvláštní, protože, jak uvidíme později, programy jsou ještě výše nad tím. Navíc, tyto programy jsou často součástí firmware síťových boxů.

Jako protokoly nižších vrstev se používá buď SCTP (kap. 17) nebo TCP [26]. Zajímavé je zabezpečení protokolu Diameter. V dřívějších verzích protokolu Diameter bylo podporováno zejména zabezpečení pomocí IPsec [28]. To bylo přehodnoceno a vyžadovaným zabezpečením je dnes TLS [29] nebo DTLS (kap. 16) a teprve v případě, že tyto mechanismy není možné využít, tak je přípustný IPsec [28]. Komunikace bez zabezpečení by neměla být implementována vůbec. To pochopitelně nepoužijeme, když jde např. o komunikaci dvou aplikací v rámci jednoho operačního systému.

V protokolu Diameter spolu nemusí komunikovat pouze sousední entity. Mezi klienta a server mohou být v protokolu Diameter vkládány další entity - mezilehlé entity, které označujeme termínem agent. Později budou popsány např. proxy agent, redirect agent, translation agent atd. Mezilehlé entity mohou pro některé aplikace vystupovat jako agent, pro jiné jako server.

Entita protokolu Diameter provádí následující funkčnosti (obr. 8.4):

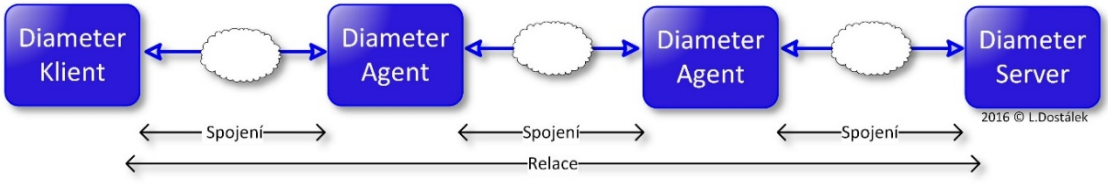


obr. 8.4 Architektura protokolu Diameter

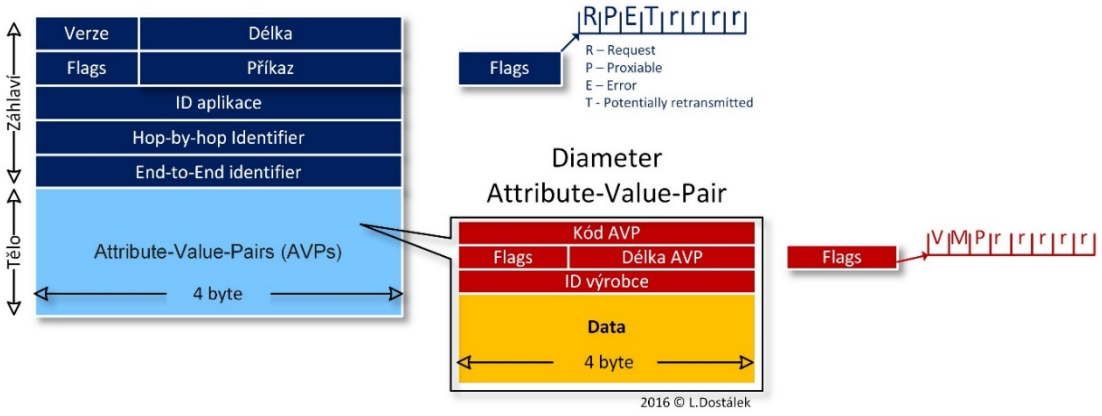
- Správu spojení mezi sousedními entitami protokolu Diameter.
- Správu směrování paketů protokolu Diameter.
- Správu relací mezi koncovými entitami relace.

Rozdíl mezi spojením a relací je vidět na obr. 8.5. Relace se zabývá řešením konkrétního aplikačního problému (např. autentizace klienta). Každá aplikace by měla stanovit zásady, kdy relace začíná a kdy končí. Pakety patřící téže relaci obsahují shodný identifikátor *Session-Identifier*.

Tzv. stavový agent protokolu Diameter udržuje stavovou informaci relace (nezaměňovat s dále zmíněným stavem transakce). Stav relace je považován za aktivní, dokud to není změněno, nebo dokud nevyprší.



obr. 8.5 Spojení a relace v protokolu Diameter



obr. 8.6 Zpráva (příkaz) protokolu Diameter

Relace se skládá z transakcí. Transakce se skládá z dotazu a odpovědi na něj. Protokol Diameter vyžaduje, aby agenti vždy udržovali stav transakce (nezaměňovat se stavem relace, ten udržují jen stavoví agenti). Provádí se to pomocí identifikátoru *Hop-by-Hop Identifier,* který slouží k párování dotazu a odpovědi mezi sousedními agenty: Požadavek, který dorazí na agenta, obsahuje jedinečný *Hop-by-Hop Identifier.* Agent si jej uloží a nahradí jej novým jedinečným identifikátorem a dotaz předá dále. Pokud se vrátí odpověď, pak obsahuje týž identifikátor. Agent podle toho zjistí, že na dotaz dorazila odpověď. Identifikátor obnoví uloženou hodnotou a odpověď předá dále. I bezsatovývý agent udržuje stav transakce – neudržuje stav relace.

Relace se může skládat z jedné nebo vice transakcí. To závisí na konkrétní aplikaci protokolu Diameter. Např. Referenční bod S6a zřizuje pro každou transakci relaci.

8.2 Formát zprávy

Zpráva v protokolu Diameter se nazývá příkazem. Příkaz se skládá ze Záhlaví a Těla příkazu (obr. 8.6). Záhlaví obsahuje položky. Tělo příkazu pak obsahuje jednu nebo více dvojic atribut a jeho hodnota (*Attribute-Value-Pair* - AVP). *Diameter Base Protocol* [23] definuje základní sadu příkazů a AVP. Jednotlivé aplikace protokolu Diameter (*Diameter Applications*) pak definují další nové příkazy a AVP.

Položka	Význam
Verze	Tato položka musí osahovat hodnotu 1.
Délka	Obsahuje délku zprávy včetně záhlaví a výplňkových AVP. Pole je dlouhé 3B.
Flags	8 bitů – viz obr. 8.6 (r = rezervováno pro budoucí využití)
Příkaz *(Command Code)*	Kód příkazu, tj. o jaký příkaz se jedná. Kódy příkazů protokolu Diameter jsou přidělovány IANA [30].
ID aplikace *(Application ID)*	Kód aplikace protokolu Diameter. Identifikuje aplikaci, které příkaz patří. Viz obr. 8.3. Hodnoty *Application ID* jsou přiřazovány IANA [30].
Hop-by-Hop Identifier	Identifikátor *Hop-by-Hop* slouží sousedům (sousedním agentům) k párování dotazu a odpovědi na něj.
End-to-End Identifier	Identifikátor *End-to-End* slouží k párování dotazu a odpovědi mezi konci relace.
AVP	AVP (*Attribute and Value Pairs*) nese aplikační informace zprávy protokolu Diameter

Položka	Význam
Kód AVP *(AVP Code)*	Kód AVP, tj. o jaký AVP se jedná.
Délka AVP (AVP Length)	Obsahuje délku AVP (včetně všech polí záhlaví AVP). Pole je dlouhé 3B.
Flags	8 bitů – viz obr. 8.6 (r = rezervováno pro budoucí využití) • P – rezervováno pro end-to-end bezpečnost • M (*Mandatory*) – Příjemce příkazy musí tomuto AVP rozumět, pokud ne, tak musí odpovědět chybou. • V (*Vendor-Specific*) – indukuje, jestli volitelné pole *Vendor-Specific* je v záhlaví AVP nebo nikoliv.

ID výrobce (Vendor ID)	Toto pole je určeno pro kód výrobce. Hodnotu si výrobci registrují u IANA jako tzv. "*SMI Network Management Private Enterprise Codes*" [31]. Pole je volitelné, je použito, pouze pokud je nastaven bit V.

tab. 8.1 Položky záhlaví protokolu Diameter

Diameter Base Protocol [23] zavádí základní sadu příkazů protokolu Diameter (tab. 8.2) další příkazy si pak specifikuji a u IANA registrují jednotlivé aplikace protokolu Diameter (*Diameter Application*).

Příkaz	**Zkratka**	**Kód**	**Flag R(equest)**
Abort-Session-Request	ASR	274	1
Abort-Session-Answer	ASA	274	0
Accounting-Request	ACR	271	1
Accounting-Answer	ACA	271	0
Capabilities-Exchange-Request	CER	257	1
Capabilities-Exchange-Answer	CEA	257	0
Device-Watchdog-Request („Diameter Echo Request“)	DWR	280	1
Device-Watchdog-Answer („Diameter Echo Reply“)	DWA	280	0
Disconnect-Peer-Request	DPR	282	1
Disconnect-Peer-Answer	DPA	282	0
Re-Auth-Request	RAR	258	1
Re-Auth-Answer	RAA	258	0
Session-Termination-Request	STR	275	1
Session-Termination-Answer	STA	275	0

tab. 8.2 Základní sada příkazů protokolu Diameter

Zajímavostí je, že součástí základní sady příkazů nejsou příkazy pro navázání relace. Ty jsou totiž závislé na konkrétní aplikaci protokolu Diameter (*Diameter Application*). Na druhou stranu příkazy pro ukončení relace pro obnovení autentizace (*re-authentication*) jsou součástí základní sady příkazů.Diameter Base Protocol [23] dále zavádí základní sadu AVP (tab. 8.3). Další AVP si pak registrují u IANA jednotlivé aplikace protokolu Diameter (*Diameter Application*)

tab. 8.3 Základní sada AVP

AVP	Kód	Význam
Vendor-Id	266	Identifikace dodavatele software
Host-IP-Address	257	Odesilatelova IP adresa
Auth-Application-Id	258	Identifikace aplikace protokolu Diameter (viz obr. 8.3). Aplikace orientované na autentizaci (včetně *Credit Control*) používají AVP *Auth-Application-Id,* Aplikace orientované na účtovaní používají AVP *Acct-Application-Id.* Hodnoty jsou registrovány v [30].
Acct-Application-Id	259	
Inband-Security-Id	299	Nabízí podporované metody zabezpečení
Result-Code	268	Výsledkový kód požadavku. Protokol Diameter používá následující notaci: • 1xxx (Informativní odpověď) • 2xxx (Úspěšná odpověď) • 3xxx (Chyba protokolu) • 4xxx (Dočasná chyba) • 5xxx (Trvalá chyba)
Auth-Request-Type	274	Informuje o tom, jestli účastník má být autorizován, autentizován nebo obojí.
Session-Id	263	Identifikátor relace
User-Name	1	Účastnické jméno
Origin-Host	264	Identifikace koncového bodu, který inicioval zprávu (*Diameter message*)

Origin-Realm	296	Identifikace domény koncového bodu, který inicioval zprávu (*Diameter message*)
Destination-Host	293	Identifikace uzlu, kterému je zpráva určena (*Diameter message*)
Proxy-Host	280	Obsahuje identitu uzlu, který toto AVP do zprávy přidal
Route-Record	282	Každý agent, který předává zprávu, vkládá do tohoto AVP svou identitu. Před předáním zprávy je agent povinen zjisti, jestli zpráva neobsahuje jeho identitu v AVP *Route-Record*, aby se zamezilo cyklení zpráv.
Destination-Realm	283	Identifikace domény bodu, kterému je zpráva určena (*Diameter message*)
Proxy-Info	284	Obsahuje identitu uzlu, který toto AVP do zprávy přidal
Proxy-State	33	Obsahuje stav entity, která toto AVP vytvořila
Origin-State-Id		Slouží k detekci zpráv z řádně neukončených relací (např. po restartu entity protokolu Diameter). Entita protokolu Diameter zvyšuje hodnotu tohoto AVP vždy po svém restartu.

8.3 Agenti

Agenti zajišťují předávání zpráv protokolu Diameter včetně směrování zpráv. [23] definuje následující typy agentů protokolu Diameter:

- Relay Agent
- Redirect Agent
- Proxy Agent
- Translation Agent

Další typy agentů definují 3GPP a GSMA:

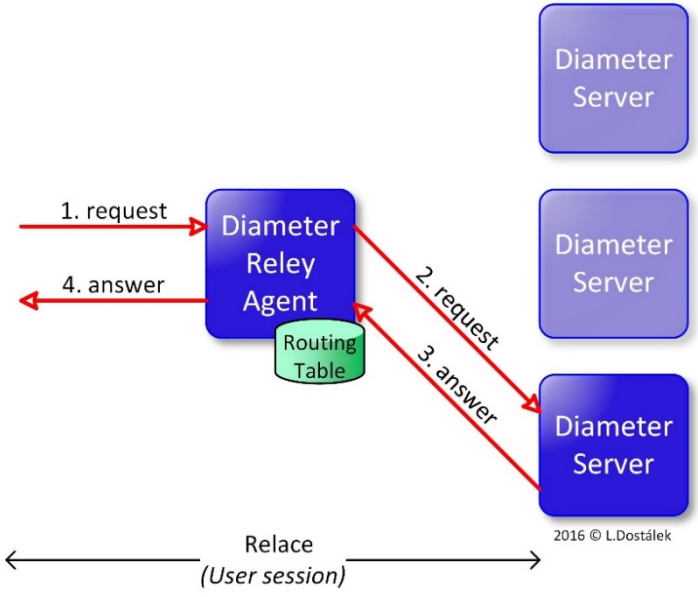
- Diameter Routing Agent [32].
- Diameter Edge Agent [33].

8.3.1 Relay Agent

Relay Agent akceptuje požadavek a směruje jej dále k jejich cíli. Ke směrování využívá doménovou směrovací tabulku (*Realm Routing Table* - viz 8.6.2). Je třeba zdůraznit, že se jedná o směrovaní na aplikační vrstvě (nezaměňovat se směrováním IP protokolu!).

8.3.2 Proxy Agent

Proxy Agent obdobně jako Relay Agent předává, za využití doménové směrovací tabulky, zprávy směrem k jejich cíli. Navíc však může modifikovat celý obsah zprávy. Může např. vynucovat specifickou politiku (*policy enforcement).* Politikou lze vynucovat např. přístup k síti, poskytnutí

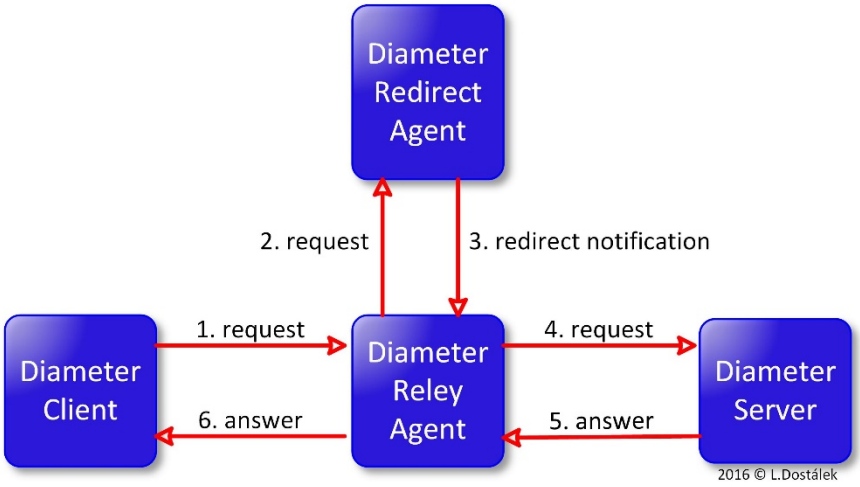


obr. 8.7 Diameter Relay / Proxy Agent

Relay Agent modifikuje, vkládá nebo ruší směrovací informace. Avšak nemění žádné další částí zprávy (příkazu) protokolu Diameter.

Důležité rovněž je, že Relay Agent nemusí podporovat (předávat) libovolné aplikace protokolu Diameter, podporuje jen konkrétní nabízené služby (předává jen pakety s konkrétním *Applicatio-ID*).

určitých zdrojů sítě (např. datového nosiče zaručené šířky pásma) atd. To samozřejmě vyžaduje, že Proxy Agent musí být stavový, tj. musí udržovat stav relace a samozřejmě, že musí udržovat i stavy transakcí.



obr. 8.8 Přesměrovávání zpráv protokolu Diameter

8.3.3 Redirect Agent

Redirect Agent je užitečným nástrojem pro centralizaci směrovacích informací protokolu Diameter. Rediract Agent nepředává zprávy, ale vrací odpovědi s informacemi jak má Diameter Agent předat zprávu dále k cíli. Redirect agent nemodifikuje aplikační část zprávy a jelikož jím neprochází odpověď, tak nemůže být stavovým agentem.

8.3.4 Translation Agent

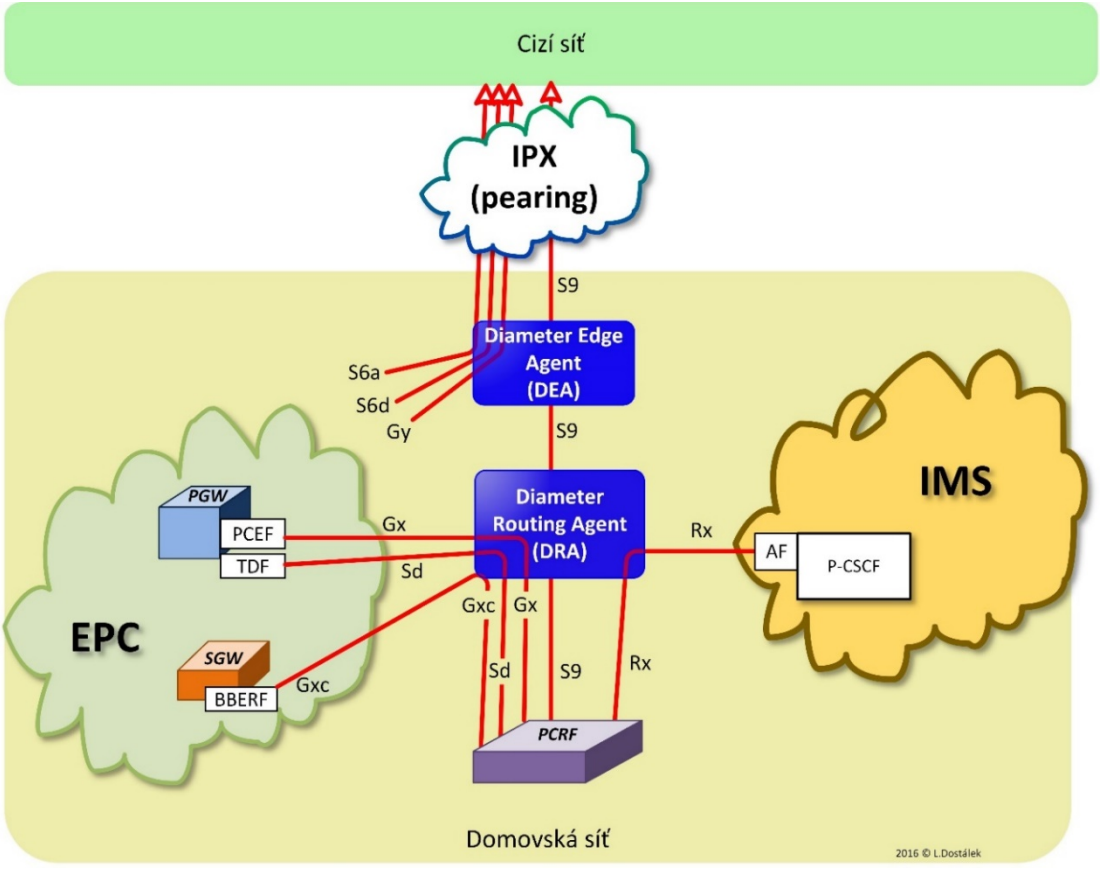
Translation Agent (obr. 8.9) je entita, která převádí (transformuje) komunikaci aplikačního protokolu Diameter do/z jiného aplikačního protokolu (např. RADIUS nebo TACACS+).

obr. 8.9 Příklad: Diameter Translation Agenta

8.3.5 Routing Agent

Diameter Routing Agent (DRA) je specifický Diameter agent pro EPC (viz kap. 7). Je specifikován v 3GPP TS 29.213 [32].

protože umožňuje komunikaci protokolem Diameter převést z propojení každého uzlu EPC jádra s každým na hvězdicovou architekturu. Další výhodou (kromě centralizace) je možnost modifikace zpráv protokolu Diameter. Stává se totiž,



obr. 8.10 Diameter Routing Agent

DRA může být implementován buď jako Proxy nebo jako Redirect Agent. Jeho cílem je centralizovat komunikaci protokolem Diameter v EPC *(core)*. Někdy se označuje jako *Diameter hub*, že zařízení různých výrobců mají problém se vzájemnou kompatibilitou protokolu Diameter, kterou lze opravit jednoduchou transformací zpráv na DRA. Nevýhodou DRA je, že se může stát "*single point of failure*", proto se DRA zpravidla zdvojují a výpadek jednoho DRA se ošetřuje na

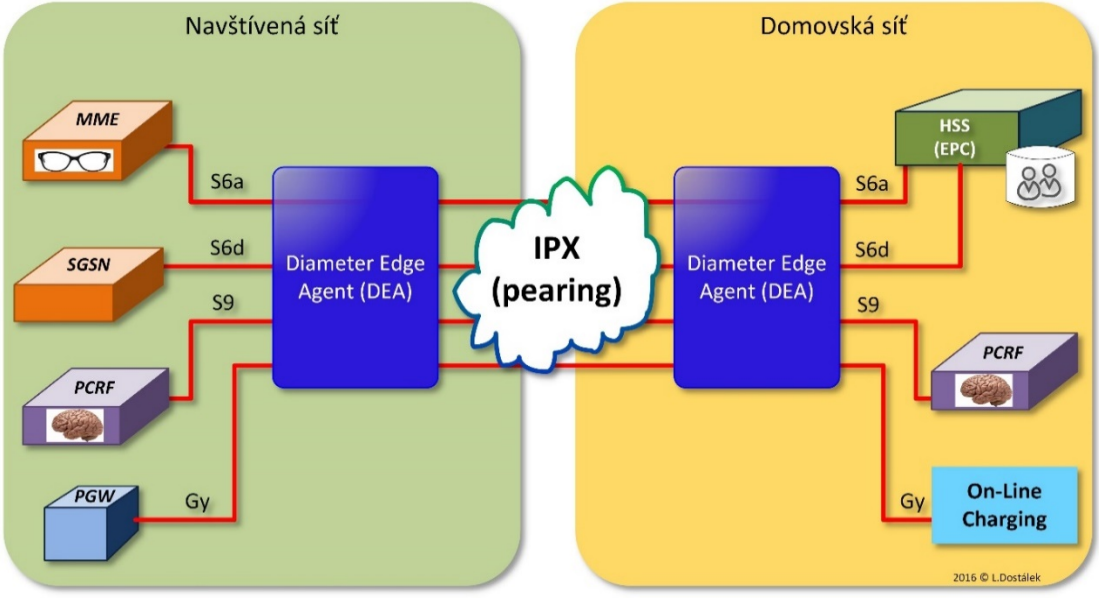
úrovní protokolu SCTP (protokol nižší síťové vrstvy).

Kromě zmíněné sítové argumentace o smyslu DRA je ještě podstatnější argumentace aplikační. V případě, že máme více než jedno PCRF, tak se využití DRA považuje za nutné. DRA totiž může v případě výpadku nebo přetížení jednoho PCRF směrovat požadavky na jiné PCRF. Proto se můžeme setkat s názorem, že v případě použití jen jednoho PCRF není implementace DRA nutná.

DRA je považováno za zbytečné. Stejně tak referenčních bodů pro účtování (Rf, Gy a Ro). Důvod může být i praktický, protože tyto referenční body jsou často na jiných virtuálních sítích než DRA.

8.3.6 Edge Agent

Diameter Edge Agent (DEA) je uváděn ve standardu GSMA IR.88 [33]. Podobně jako, DRA, je i DEA specifickým agentem pro využití v EPC *(core)*.



obr. 8.11 Diameter Edge Agent

DRA zpravidla podporuje referenční body: Gx, Gxc, Sd, S9 a Rx. Avšak výrobci DRA boxů zpravidla podporují větší škálu referenčních bodů, protože tytéž boxy dodávají i jako DEA. Napojení referenčních bodů S6a (HSS) a S13 (EIR) skrze

DEA se umísťuje na hranici EPC zpravidla mezi síť operátora a IPX (nebo sítěmi ostatních operátorů) mj. pro bezpečné oddělení sítě operátora od ostatního světa. DEA lze tedy přirovnat k specializovanému firewallu pro protokol Diameter.

Jeho cílem je též skrýt topologii sítě operátora před okolním světem. Žádná komunikace protokolem Diameter vně sítě operátora by neměla běžet mimo DEA.

DEA může pro některé aplikace běžet jako Proxy Agent, který přidává, modifikuje nebo odebírá AVP z předávaných zpráv protokolu Diameter. Pro jiné může běžet jen jako Relay Agent. Je třeba ale mít na paměti, že jedna instance DEA může běžet buď jako proxy nebo jako relay. Prakticky se však DEA zpravidla konfiguruje tak, že pro externí sítě se tváří jako relay (nabízí *Relay application ID*), pro vnitřní sítě se nabízí jako proxy (nabízí *Proxy ID*).

Zatím jsme předpokládali, že DEA je ve vlastnictví a správě mobilního operátora. Je však obecně možná i strategie, že DEA je poskytována poskytovatelem IPX. Nicméně standard GSMA IR.88 [33] vyžaduje, aby v případě veřejných mobilních operátorů byla DEA implementována (buď operátorem nebo IPX) a kromě předávání zpráv prováděla kontrolu přístupu, vynucování politik přístupu a zpracovávání speciálních AVP.

GSMA IR.88 [33] specifikuje, aby DEA podporovala následující referenční body:

- S6a mezi MME navštívené sítě a HSS domovské sítě.
- S6d mezi SGSN (3G sítě) navštívené sítě a HSS domovské sítě.
- S9 mezi PCFR navštívené sítě a PCRF domovské sítě. S9 není vyžadováno, pokud PCRF navštívené sítě je konfigurované statickými politikami pro účastníky z cizích sítí (účastníky v roamingu).
- Gy mezi PGW a OCS (Online charging) domovské sítě. Podpora Gy je volitelná, ale je užitečná v případě *home routed roaming* (viz kap. 5.1.2).

8.4 Doména

Doména (*Realm*) je velice důležitým pojmem v protokolu Diameter. Lze ji přirovnat k doméně (*realm*) protokolu Kerberos, avšak je to jen přirovnání – nejedná se o domény v stejném významu.

V počítačových sítích se obecně používá síťový přístupový identifikátor (*Network Access Identifier* - NAI). Např. `pepa@firma.eu`. Doménou pak označujeme vše, co následuje za znakem '@'. Doménová jména se spravují pomocí DNS. Můžeme také říci, že doména nám určuje, jestli požadavek má být směrován lokálně nebo do cizí sítě.

Zatímco v Internetu jsme zvyklí doménová jména si registrovat téměř libovolně, tak v IPX jsme svázáni striktními pravidly. Standard 3GPP TS 23.003: "Numbering, addressing and identification" [34] 3GPP definuje zásady odvozování DNS jmen pro EPC (*Evolved Packet Core*). Na jednu stranu připouští obecná jména tvaru `operator.com`, ale podstatně užitečnější budou DNS jména odvozená od IMSI (viz odstavec 4.5). Pro EPC standard 3GPP TS 23.003 [34] definuje následující formát DNS jména účastníkovy domovské sítě:

epc.mnc<MNC>.mcc<MCC>.3GPPnetwork.org

Příklad:

Mějme např. IMSI=230010999999999, tj.

MMC=230 (České republika)

MNC=01 (T-Mobile)

MSIN=0999999999

Pak plně kvalifikované DNS jméno EPC pro jeho domovskou doménu je:

epc.mnc001.mcc230.3GPPnetwork.org.

V předchozím příkladu uvedená doména „epc“ je důležitá např. pro referenční bod S6a. Pro jiné referenční body jsou zajímavé další domény. GSMA IR.67 [35] zavádí další subdomény domény 3gppnetwork.org:

- ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- ics.mnc<MNC>.mcc<MCC>.3gppnetwork.org
- unreachable.3gppnetwork.org

8.5 Diameter Peer Discovery

Zásadním problémem je, jak nalézt další uzel, na který předat zprávu protokolu Diameter, tak aby postupně doputovala až ke svému adresátu. Tj., jak nalézt souseda, kterému požadavek předat. Musíme si uvědomit, že jsme na aplikační (nikoliv IP) vrstvě, tj. soused může být i velmi vzdálen. Protokol Diameter podporuje následující mechanismy:

- Statická (ruční) konfigurace
- Využití DNS

Postup je pak následující. Rozhoduje se podle názvu domény, do které má požadavek zaslat:

1. Diameter hledá příslušného souseda v statické konfiguraci, pokud tam najde vhodného souseda, tak mu zprávu předá.
2. V DNS hledá pro příslušnou doménu NAPTR větu. Pokud existuje, pak provede překlad (zpravidla přes SRV záznam), až se dostane na A (resp. AAAA) záznam souseda, kterému zprávu předá.
3. Pokud příslušný NAPTR záznam v DNS nenajde, pak v DNS hledá následující SRV záznamy:
   - "_diameter._tcp.*doména*" pro Diameter přes TCP,

- "_diameters._tcp.*doména*" pro Diameter přes TLS,
- "_diameter._sctp.*doména* " pro Diameter přes SCTP,
- "_diameters._sctp.*doména* " pro diameter přes DTLS.

8.6 Směrování

Protokol Diameter je aplikační protokol typu klient/server. Avšak mezi klienta a server je možné vkládat již zmíněné agenty, kteří předávají zprávy protokolu Diameter. Tuto strategii používají i jiné síťové protokoly, jako např. HTTP, který vkládá mezi klienta a server např. HTTP proxy.

Relace protokolu Diameter může být navázána pouze mezi koncovými body (klient/server). Z pohledu účastníka se pak relace může jevit jako řetězec spojení. Důležité je, že každé spojení (téže relace) může používat jiný transportní protokol (TCP, SCTP).

Směrování v protokolu Diameter jen zdánlivě připomíná směrování IP protokolu. Zásadní rozdíl mezi těmito směrováními je v tom, že IP protokol směruje na základě IP adresy, kdežto protokol Diameter směruje na základě názvu domény (*realm*). Avšak používáme obdobnou terminologii, jako je směrovací tabulka, máme zde i termín implicitní směr (*default route*) atd.

Směrování v protokolu Diameter využívá dvě tabulky:

- Tabulka sousedů (*Diameter Peer Table*), která obsahuje uzly, na které máme přímé spojení transportním protokolem (TCP, SCTP).
- Směrovací tabulka (*Realm Routing Table*), která obsahuje „*next hop*“ pro cílové domény, kam chceme směrovat požadavek.

8.6.1 Tabulka sousedů

Tabulka sousedů obsahuje pro každého souseda následující položky:

- **Identita souseda** *(Host Identity)*, která se získá od souseda v rámci dialogu *Capabilities Exchange* (příkazy CER/CEA), kdy soused ji uvádí v AVP *Origin-Host*.
- **Stav** *(Status)*. Názvy stavů často začínají buď prefixem „I-“ pro iniciátora spojení nebo „R-“ pro toho kdo očekává požadavek (*responder*). Máme např. stavy: R-Open, I-Open, Wait-I-CEA, Wait-Conn-Ack, Closed, Closing. Příslušný stavový stroj popsán v [23].
- **Statický nebo dynamický** – specifikuje, jestli položka do tabulky sousedů byla vložena staticky nebo byla vytvořena dynamicky (např. pomocí DNS směrování).
- **Doba expirace** *(Expiration time)* – specifikuje pro dynamicky vložené položky čas, do kterého musí být položka obnovena nebo vyprší.
- **Podpora TLS** *(TLS/TCP and DTLS/SCTP Enabled)* – specifikuje, jestli je možné se sousedem zabezpečit komunikaci pomocí TLS
- **Další informace,** např. odkazy na kryptografický materiál zabezpečující komunikaci.

8.6.2 Směrovací tabulka

Jednotlivé záznamy směrovací tabulky obsahují následující položky:

- **Jméno cílové domény** *(Realm Name)* – používá se jako primární klíč při vyhledávání ve směrovací tabulce. Implementace protokolu Diameter často nehledají jen přesnou shodu, ale pokud se jim ji nepodaří nalézt, pak vyhledávají záznam, který se zprava nejvíce shoduje.
- **Identifikátor aplikace protokolu Diameter** *(Application Identifier)* – používá se jako sekundární klíč ve směrovací tabulce. Musíme si uvědomit, že různé aplikace protokolu Diameter v téže doméně mohou běžet na různých serverech.
- **Akce** *(Local Action)* – specifikuje, jak se má naložit s požadavkem směrovaným dle tohoto záznamu. Akce máme:
  - LOCAL – Zpráva bude zpracována lokálně, tj. nebude směrována na jiný server.
  - RELAY – zpráva bude předána, aniž by byly modifikovány jiné AVP než ty, které složí ke směrování. Tj. předávající entita se zachová jako *Relay Agent.*
  - PROXY – zpráva bude předána, ale může být modifikována. Tj. předávající entita se zachová jako *Proxy Agent.*
  - REDIRECT – Předávající entita se zachová jako Redirect Agent.
- **Identifikátory serverů** *(Server Identifier),* kam má být zpráva předána v případě akce RELAY nebo PROXY. V případě akce REDIRECT pak obsahuje identifikace serverů, kam má být přesměrována.
- **Statický nebo dynamický** – specifikuje, jestli položka do směrovací tabulky byla vložena staticky nebo byla vytvořena dynamicky (např. pomocí DNS směrování).
- **Doba expirace** *(Expiration time)* – specifikuje pro dynamicky vložené položky čas, do kterého musí být položka obnovena nebo vyprší

8.6.3 DNS směrování

Aplikační směrování na základě DNS známe z elektronické pošty, které je směrována pomocí MX záznamů. MX záznamy jsou specifické záznamy pro elektronickou poštu. Později byly zavedeny obecné záznamy pro DNS směrování na aplikační vrstvě, které se nazývají NAPTR [36]. Ty ovšem jsou zase tak obecné, že pro protokol Diameter byla jejich obecnost omezena na záznam typu S-NAPTR [37].

Pokud chceme nalézt spojení na entitu protokolu Diameter, pak můžeme rovněž použít DNS. Hledáme např. Diameter server v konkrétní doméně. Doménu můžeme dedukovat např. z názvu domény v NAI (*Network Access Identifier* [38]) v AVP (*attribute-value pair*), z *User-Name* nebo z *Destination-Realm*. V mobilních sítích budeme doménu odvozovat nejspíše od IMSI (viz příklad na konci odstavce).

Připomeňme, že DNS je v IPX nezávislé na DNS v internetu, tj. IPX provozuje vlastní kořenové DNS servery. Poskytovatelé IPX nebo i operátoři pak provozuje „*slave*“ servery k těmto serverům. Někteří operátoři si však z kořenové zóny

vyberou jen některé domény, nebo dokonce je nepoužívají a konfigurují si vlastní kořenové DNS servery.

Z hlediska vyhledání Diameter serverů pomocí DNS máme dvě strategie:

- Klasická strategie protokolu Diameter (*Diameter Base Protocol*) [23].
- Novější strategie, která využívá S-NAPTR.

Klasická strategie využívala záznam NAPTR se službou o hodnotě "AAA+D2x", kde písmeno x odpovídalo transportnímu protokolu (např. D2S pro SCTP). Nevýhodou tohoto řešení je fakt, že lze tak vyhledat obecný Diameter server pro doménu. Prakticky je třeba ale hledat server pro konkrétní Diameter aplikaci (např. vyhledat HSS vzdálené sítě, tj. nalézt server pro referenční bod S6a apod.). Proto nověji byl v RFC-6408 [37] zaveden pro protokol Diameter záznam typu S-NAPTR (*Diameter Straightforward-Naming Authority Pointer*). Sám S-NAPTR byl zaveden již před tím v RFC-3958 [39].

S-NAPTR není žádným novým typem DNS záznamu. Je naopak jen podmnožinou záznamu typy NAPTR – jedná se o NAPTR záznamy, které mají příznak (*flag*) nuď „S“ nebo „A“ (ostatní nejsou přípustné).

RFC 6408 [37] specifikuje některé služby pro záznamy typu NAPTR (tab. 8.4.):

tab. 8.4 Některé služby pro záznamy typu NAPTR

NAPTR Tag	Diameter Application
aaa+ap1	NASREQ [40]
….	
aaa+ap3	Base Accounting [23]
aaa+ap4	Credit Control [27]
….	
aaa+ap16777251	3GPP S6a [41]
…	
aaa+ap16777267	3GPP S9 [42]

Vraťme se k našemu hypotetickému příkladu (nemá žádnou souvislost se skutečností):

Mějme např. IMSI=230010999999999, tj.

MMC=230 (České republika)

MNC=01 (T-Mobile)

MSIN=0999999999

Pak plně kvalifikované DNS jméno pro jeho domovskou doménu EPC je:

`epc.mnc001.mcc230.3GPPnetwork.org.`

Nyní potřebujeme v této doméně nalézt HSS (tj. Diameter server pro referenční bod S6a). Aby to bylo možné, pak v DNS musí být např. následující záznamy:

```
$ORIGIN epc.mnc001.mcc230.3gppnetwork.org.
;                order    pref     falg    service
;                regexp   replacement
 IN      NAPTR   50       50       "s"     "aaa+ap16777251:diameter.tls.tcp"
                 ""       _diameter._tls._tcp.server
```

```
 IN      NAPTR    50       51       "s"    "aaa+ap16777251:diameter.sctp"
                  ""       _diameter._sctp.server

;
;                                    Prior. Weight    port     Target

_diameter._tls._tcp.server IN SRV   0      1        3868     server1
_diameter._sctp.server     IN SRV   0      1        3868     server2

server1                    IN     AAAA     ….server2
IN       A        ….
```

Na závěr je třeba jen uvést, že vyhledávání Diameter serveru pomocí DNS je užitečné pokud hledáme server mimo naší vlastní síť. Uvnitř sítě mnohdy stačí využít prosté IP adresy serveru a DNS se vůbec nemusíme nezabývat.

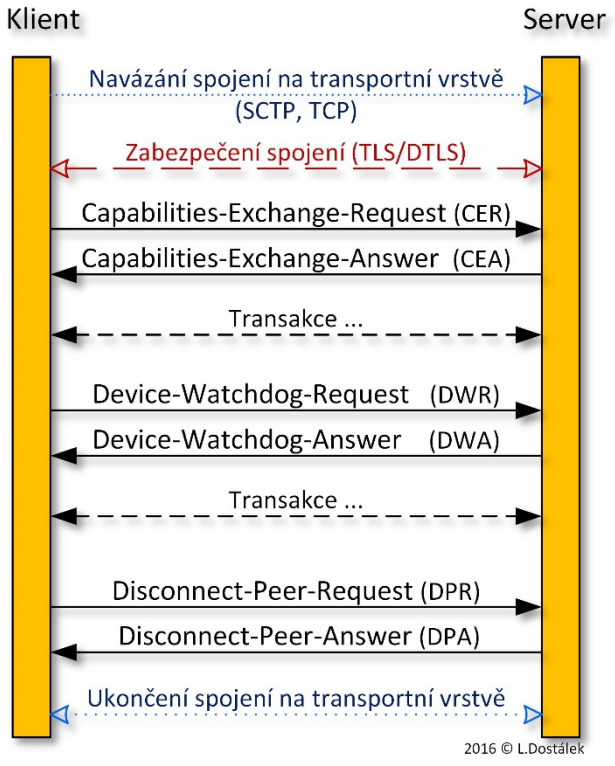
8.7 Dialog protokolu Diameter

V protokolu Diameter máme dva základní dialogy:

- Dialog, kterým se navazuje spojení mezi dvěma entitami protokolu Diameter.
- Dialog, kterým se vyřizují konkrétní požadavky konkrétních účastníků. Tento dialog je závislý na konkrétní aplikaci protokolu Diameter.

8.7.1 Dialog mezi dvěma entitami protokolu Diameter

Když dva uzly protokolu Diameter naváží spojení na transportní vrstvě (např. protokolem SCTP – viz kap. 17) a případně zabezpečí komunikaci pomocí TLS/DTLS, pak jsou povinni provést transakci *Capabilities Exchange*, tj. Vzájemně se informovat o svých schopnostech (podporovaných verzích protokolu, podporovaných aplikacích, podporovaných bezpečnostních mechanismech



obr. 8.12 Dialog mezi sousedy

atp.). Teprve poté mohou do komunikace vstoupit aplikace.

Uzel sítě smí odesílat příkazy na sousední uzel je těch Diameter aplikací, které mu sousední uzel nabídl během *Capabilities Exchange*.

Příjemce příkazu *Capabilities-Exchange-Request* (CER) musí určit průnik mezi jím podporovanými aplikacemi a aplikacemi uvedenými v přijatém příkazu CER (tj. AVP *Application-Id*) a výsledek uvede do odpovědi *Capabilities-Exchange-Answer* (CEA). Obdobně to provede i s AVP: *Auth-Application-Id* a *Acct-Application-Id*.

Současný standard protokolu Diameter [23] vyžaduje, aby po navázání transportního spojení (TCP, resp. SCTP) došlo vždy k zabezpečení komunikace pomocí TLS (resp. DTLS). Starší verze standard umožňovaly v rámci *Capabilities Exchange,* aby se sousední uzly pomocí AVP *Inband-Security* dohodly na zabezpečení. A teprve pak došlo k zabezpečení komunikace. Tento postup již dále není doporučován.

CER a CEA nesmí být předávány dále pomocí proxy, redirect ani relay agentů. Výjimkou jsou pouze příkazy CER s AVP*: Auth-Application-Id* nebo *Acct-Application-Id*.

Na obr. 8.12 je znázorněn klasický dialog protokolem Diameter:

1. Navázání transportního spojení
2. Zabezpečení komunikace
3. Dialog *Capabilities Exchange*
4. Nyní mohou přijít ke slovu jednotlivé aplikace
5. V pravidelných intervalech je pomocí příkazu DWR testována dostupnost druhé strany. Pokud druhá strana odpovídá příkazem DWA, pak je dostupná („aplikační ping“).
6. Příkazem DPR se vyžaduje ukončení spojení. Spojení je ukončeno po přijetí DPA.

tab. 8.5 Příklad výpisu zprávy protokolu Diameter pomocí programu Wireshark

```
Transmission Control Protocol, Src Port: 5698, Dst Port: 3868, Seq: 1, Ack: 1, Len: 170
Diameter Protocol
    Version: 0x01
    Length: 170
    Flags: 0x80  (Request)
    Command Code: 257 Capabilities-Exchange
    ApplicationId: 0
    Hop-by-Hop Identifier: 0x6a5b2c5d
    End-to-End Identifier: 0x7f6b5d8f
    AVP: Origin-Host(264) l=12 f=-M- val=pop.firma.cz
    AVP: Origin-Realm(296) l=23 f=-M- val=diameterserver.firma.cz
    AVP: Host-IP-Address(257) l=14 f=-M- val=10.18.158.5
    AVP: Vendor-Id(266) l=12 f=-M- val=0
    AVP: Product-Name(269) l=21 f=- val=Open Diameter
    AVP: Origin-State-Id(278) l=12 f=-M- val=5685321575
    AVP: Auth-Application-Id(258) l=12 f=-M- val=Diameter NASREQ Application (1)
    AVP: Auth-Application-Id(258) l=12 f=-M- val=Diameter EAP (5)
    AVP: Inband-Security-Id(299) l=12 f=-M- val=NO_INBAND_SECURITY (0)
```

8.7.2 Dialog zpracovávající požadavky účastníků

Představme si, že Diameter klient je na hranici poskytovatele internetu jako součást PoP (obr. 8.1). Tento klient má navázán dialog protokolem Diameter s jedním nebo více servery protokolu Diameter (např. pro každou aplikaci protokolu Demeter jiným). Mezi klientem a serverem protokolu Diameter tikají příkazy *Device-Watchdog-Request* a *Device-Watchdog-Answer* …

Nyní na PoP dorazí požadavek účastníka o poskytnutí připojení do internetu. Nejjednodušším příkladem je, že PoP podporuje aplikace *Network Access Server* (NAS) [40] a *Diameter Base Accounting* [23]. (Obě aplikace protokolu Diameter jsou též zmíněny v následujících odstavcích.)

PoP nejprve provede aplikací NAS autentizaci/autorizaci klienta (v tomto případě pomocí jména účastníka a hesla). Na základě úspěšné autentizace/autorizace se vytvoří relace, která získá svůj identifikátor: *Session-Id*. Pokud má být aktivováno účtování, tak v tomto okamžiku je klientem (tj. PoP, resp. jeho součást NAS) odeslán příkaz *Accounting-Request* s START_RECORD. Pokud tento příkaz selže, pak je odeslán EVENT_RECORD se důvodem selhání. V případě, že příkaz neselhal, vytvoří se účtovací relace, která získá jedinečný identifikátor: *Acct-Session-Id*.

Ukončení relace (*Session*) může nastat z několika důvodů, např.:

- Účastník vypnul své zařízení. Z tohoto důvodu aplikace protokolu Diameter zpravidla vyžadují pravidelné obnovování relace (*re-authentication*), aby zjistily, jestli účastníkovo zařízení je stále aktivní.
- Účastník sám žádá o odpojení. K tomu se použijí příkazy ze základní sady příkazů protokolu Diameter (*Session-Termination-Request, Session-Termination-Answer*).

Diameter server žádá PoP (resp. jeho součást NAS) o ukončení relace příkazem protokolu Diameter Abort-Session-Request.

- Účastníkovi vypršel kredit. To by bylo v případě, že PoP by podporoval aplikaci protokolu Diameter označovanou jako CC (Credit-Control Application).

8.8 NAS

NAS [40] je příkladem aplikace protokolu Diameter sloužící pro autentizaci/autorizaci klientů přistupujících do sítě. Dále pak bude popsána jiná aplikace protokolu Diameter - referenční bod S6a, který rovněž slouží pro autentizaci/autorizaci účastníků přistupujících do mobilní sítě.

NAS je klientem protokolu Diameter, který komunikuje se serverem protokolu Diameter.

Účastníkův požadavek na připojení do sítě je převeden klientem protokolu Diameter (NAS) na příkaz *AA-Request*, který žádá Diameter server o autentizační/autorizační informace. Diameter server vrací požadované informace příkazem

AA-Answer. V případné úspěšné autentizace/autorizace je vytvořena relace pro tohoto účastníka.

Obnovování autentizace provádí klient protokolu Diameter zopakováním původní příkazu *AA-Request*.

Toto obnovování probíhá pravidelně, ale vždy v kratším intervalu než, který je uveden v AVP *Authorization-Lifetime* (tab. 8.3) příkazu *AA-Answer*. Navíc NAS může mimo pravidelné obnovování autentizace požádat o obnovení autetnizce explicitně příkazem *Re-Auth-Answer.*

V případě, že NAS zjistí, že se účastník odpojil, pak příkazem *Session-Termination-Request* (tab. 8.2) ukončí relaci. Klient ukončení potvrdí příkazem *Session-Termination-Answer.* Diameter server může příkazem *Abort-Session-Request* vydat příkaz k ukončení relace. NAS pak ukončení potvrdí příkazem *Abort-Session-Answer*.

tab. 8.6 Příkazy aplikace Diameter NAS

Příkaz	Zkratka	Kód	Flag R(equest)
AA-Request	AAR	265	1
AA-Answer	AAA	265	0
Re-Auth-Request	RAR	258	1
Re-Auth-Answer	RAA	258	0

8.9 Účtování

Účtování (*Diameter Base Accounting*) je dalším příkladem aplikace protokolu Diameter specifikovaným v RFC 6733 [23].

Představme si, že již proběhla autentizace/autorizace klienta do sítě, tj. je vytvořena relace. Cílem je měřit čerpání služeb za účelem vyúčtování služby poskytnuté během relace. Za tímto účelem se zřizuje tzv. účtovací relace, která sleduje čerpání zdrojů tak, aby toto čerpání mohlo být následně vyúčtováno. Jedné relaci může odpovídat více účtovacích relací.

Klient (např. NAS) posílá příkazy ACR (*Accounting-Request*) na Diameter účtovací server (*Accounting Server*) účtovací příkazy, ve kterých zaznamenává informace o poskytovaných službách. Diameter účtovací server odpovídá příkazem ACA (*Accounting-Answer*). Diameter účtovací server z přijatých příkazů ACR vytváří účtovací záznamy, které se dále slouží pro vyúčtování služeb (*billing*) zákazníkovi.

Máme dva typy záznamů:

- Jednorázová událost (záznam typu EVENT_RECORD).
- Čerpání služby, které začíná záznamem START_RECORD, stvrzuje pokračování čerpání záznamy typu INTERIM_RECORD a zaznamená ukončení čerpání záznamem typu STOP_RECORD. Účtování (*Billing*), pak musí z těchto záznamů určit délku čerpání služby, která je následně vynásobena cenou služby (z ceníku) a postoupena k fakturaci.

tab. 8.7 Příkazy aplikace Diameter Base Accounting

Příkaz	Zkratka	Kód	Flag R(equest)
Accounting-Request	ACR	271	1
Accounting-Answer	ACA	271	0

tab. 8.8 AVP aplikace Diameter Base Accounting

AVP	Kód	Význam
Accounting-Record-Type	480	Typ účtovacího záznamu: • Událost (EVENT_RECORD) – hodnota 1 • Začátek plnění (START_RECORD) – hodnota 2 • Plnění pokračuje (INTERIM_RECORD) – hodnota 3 • Plnění ukončeno (STOP_RECORD) – hodnota 4
Acct-Interim-Interval	85	Toto AVP zasílá server klientu. Klient pak v tomto intervalu zasílá INTERIM_RECORD (viz AVP *Accounting-Record-Type*).
Accounting-Record-Number	485	Pořadí účtovacího záznamu v rámci relace. *Session-Id*. *Accounting-Record-Number* jedinečně identifikuje účtovací záznam. Cože je možné využít např. i k zjišťování duplicit.
Acct-Session-Id	44	Identifikuje účtovací relaci
Acct-Multi-Session-Id	50	Používá se v případě, že jedné *Session-Id* odpovídá více účtovacích relací, aby vyjádřilo, že patří téže *Session-Id*.
Accounting-Sub-Session-Id	287	Používá se v případě, že účtovací relace je třeba dělat na sub-relace.

8.10 Credit Control

RFC 4006 [27] specifikuje mechanismus řízení kreditu (např. získaného z předplatného kupónu). Zatímco účtování (*Diameter Base Accounting*) zaznamenává čerpání služby po jejím čerpání, tak autorizace kreditu (*Credit Control*) autorizuje kredit před tím, než je služba poskytnuta.

Je třeba připomenout, že čerpání služby přímo nevyjadřuje cenu služby, ta se musí získat oceněním např. doby poskytování služby, či množství přenesených atp. Vše musí probíhat v reálném čase.

Autorizace kreditu může použít jeden ze dvou následujících modelů:

- Rezervace finanční částky na účtu, která je po poskytnutí služby teprve vyúčtuje. Během čerpání služby je udržována kreditní relace. V případě, že není služba čerpána v předpokládaném rozsahu, tak se z účtu odečte jen adekvátní částka.
- Přímou debetní operací (odečtením z účtu). Jedná se o jednorázovou akci, tj. kreditní relaci není třeba udržovat.

Kromě autorizace kreditu, řízení kreditu (*Credit Control*) zajišťuje ještě další služby, jako je: nabíjení kreditu, zjišťování výše kreditu, změna tarifu atd.

tab. 8.9 Příkazy aplikace Diameter Credit Control (CC)

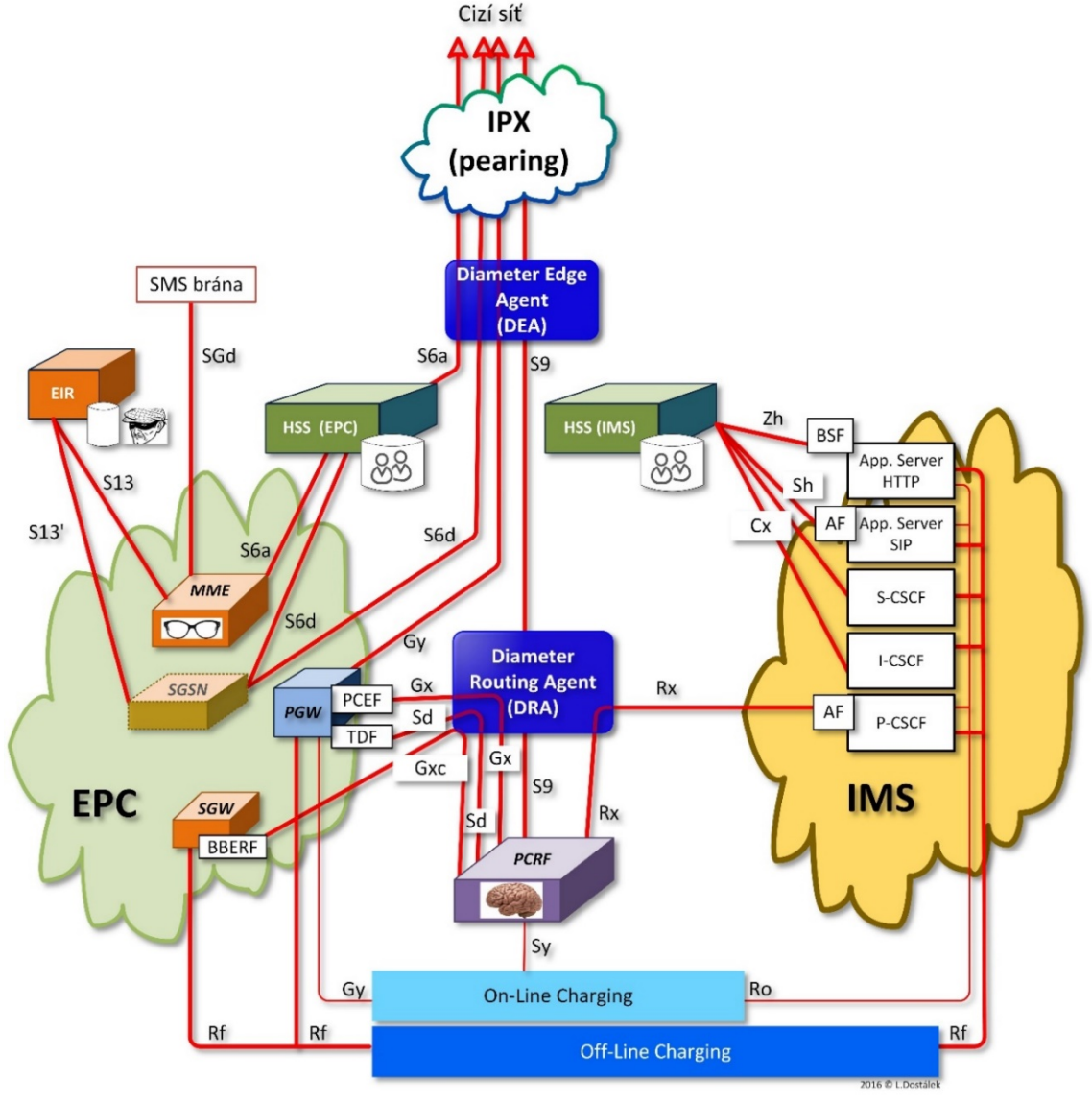
Příkaz	Zkratka	Kód	Flag R
Credit-Control-Request	CCR	272	1
Credit-Control-Answer	CCA	272	0

tab. 8.10 AVP aplikace Diameter Credit Control (CC)

8.11 Referenční body protokolu Diameter specifikované 3GPP

Konsorcium 3GPP si u IANA zaregistrovalo pro referenční body mobilních aplikací identifiká-

tory aplikací [30]. Některé z nich, včetně ID aplikací protokolu Diameter a standardů, které je specifikují, jsou uvedeny v tab. 8.11 .



obr. 8.13 Referenční body protokolu Diameter specifikované 3GPP

<table>
<tr><th colspan="2">S6a</th><th>S6d</th><th>S13</th><th>S13’</th><th>Gx</th><th>Sd</th><th>Gxa</th><th>Gxc</th><th>Rx</th><th>S9</th><th>Gy</th><th>Ro</th><th>Rf</th><th>Sy</th><th>Cx</th><th>Sh</th><th>Zh</th><th>Zn</th><th>SGd</th></tr>
<tr><td colspan="2">ID=16777 251</td><td colspan="2">16777 252</td><td>16777 224</td><td>16777 303</td><td colspan="2">16777 266</td><td>16777 236</td><td>16777 267</td><td>4</td><td>4</td><td>3</td><td>16777 302</td><td>16777 216</td><td>16777 217</td><td>16777 221</td><td>16777 220</td><td>16777 313</td></tr>
<tr><td colspan="2" rowspan="2">3GPP TS 29.272 [41] (Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN))</td><td colspan="3" rowspan="2">3GPP TS 29.212 [43] (Policy and Charging Control (PCC))</td><td colspan="3" rowspan="2">3GPP TS 29.214 [44] (Policy and Charging Control over Rx)</td><td rowspan="2">3GPP TS 29.215 [42] (Policy and Charging Control (PCC) over S9)</td><td colspan="3">3GPP TS 32.240 [45]</td><td rowspan="2">3GPP TS 29.219 [46] (Spending Limit Reporting over Sy)</td><td rowspan="2">3GPP TS 29.228 [47] (IP Multimedia (IM) Subsystem Cx and Dx)</td><td rowspan="2">3GPP TS 29.328 [48], 3GPP TS 29.329 [49] (Sh Interface based on the Diameter protocol)</td><td colspan="2" rowspan="2">3GPP TS 33.220 [21]
3GPP TS 33.221 [50]
3GPP TS 33.222 [51]
3GPP TS 33.223 [52]
3GPP TS 33.224 [53]

Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)</td><td rowspan="2">3GPP 29.338 [54] (Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs))</td></tr>
<tr><td>3GPP TS 32.251 [55]</td><td>3GPP TS 32.260 [56]</td><td rowspan="2">3GPP TS 32.295 [57]</td></tr>
<tr><td colspan="5" rowspan="2">IETF RFC-4006 [27] (Diameter Credit-Control Application)</td><td colspan="2">3GPP TS 32.296 [58]</td><td rowspan="2">3GPP TS 29.229 [60]</td></tr>
<tr><td colspan="3">3GPP TS 32.299 [59]</td></tr>
<tr><td colspan="20">Diameter Base Protocol [23]</td></tr>
<tr><td colspan="20">TLS, DTLS</td></tr>
<tr><td colspan="20">TCP, SCTP</td></tr>
<tr><td colspan="20">IPv4, IPv6 (+ IPsec)</td></tr>
<tr><td colspan="20">Linková vrstva</td></tr>
<tr><td colspan="20">Fyzická vrstva</td></tr>
</table>

tab. 8.11 Síťový model referenčních bodů protokolu Diameter specifikovaných 3GPP

8.11.1 Gx (PCEF-PCRF)

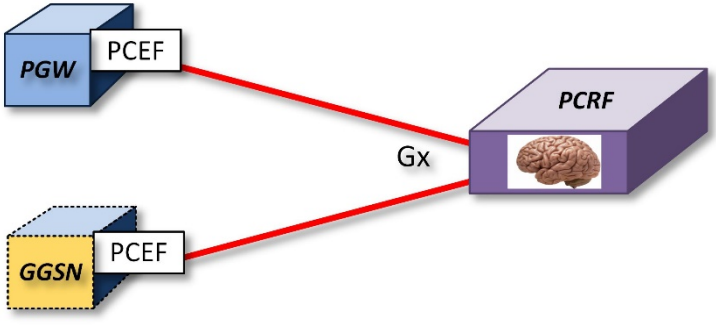
Referenční bod Gx (obr. 8.14) leží mezi PCRF (*Policy and Charging Rules Function*) a PCEF (*Policy and Charging Enforcement Function*). PCEF si nepředstavujeme jako samostatný box, ale jednu z funkčností PGW (resp. GGSN), která provádí řízení toku účastnických dat, tj. řízení *user (media) plane*. PCEF vynucuje politiky toku dat v závislosti na způsobu účtování (*charging*). Pravidla pro řízení a pravidla pro účtování se označují jako pravidla pro PCC (*Policy and Charging Control*).

V případě off-line účtování zjišťuje, jestli účastník splňuje příslušná pravidla, v případě on-line účtování, zjišťuje, jestli má dostatečný kredit atd.

Pomocí referenčního body Gx entita PCRF zasílá nebo ruší pravidla PCC na PCEF a dále mocí tohoto referenčního bodu může PCEF zasílat PCRF informace o událostech týkající se toků účastnických dat. Rovněž tento referenční bod může být využit pro řízení toku dat a řízení účtování.

Referenční bod Gx zjišťuje následující procedury:

- Žádost o pravidla PCC
- Poskytnutí pravidel PCC
- Obsluha chyb pravidel PCC (*PCC Rule Error Handling*)
- Nastavení zasílání asynchronních událostí (*Provisioning of Event Triggers*)
- Aktivování/deaktivování sledování (*Trace activation/deactivation*)
- Zasílání asynchronních událostí (*Provisioning of Event Report Indication*)
- Poskytování účtovacích informací o datové relaci (*Reporting Accumulated Usage*)
- Vykazování nasbíraných účtovacích informací
- Poskytování autorizovaných QoS toků dat
- Indikace ukončení alokace datového nosiče (*bearer*)
- Indikace ukončení datové relace



obr. 8.14 Referenční bod Gx

- Požadavek na ukončení datové relace
- Výběr módu datového nosiče (*bearer*)
- Podpora procedur prováděných v určitou hodinu (*Time of the day procedures*)
- Podpora nouzového volání (*IMS Emergency Session Support*)
- Podpora obnovení volání (*IMS Restoration Support*)
- Podpora prioritních relací, tj. např. prioritního volání (*Multimedia Priority Support*)
- Požadavky na monitorování (*Requesting Usage Monitoring Control*)
- Sponzorované připojení (*Sponsored Data Connectivity*)
- Výpadek a obnova PCRF (*PCRF Failure and Restoration*)
- Vykazování přístupu do sítě (*Reporting Access Network Information*)

tab. 8.12 Příkazy aplikace Diameter Gx

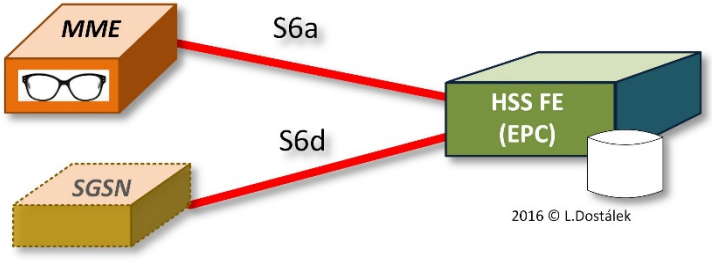
Příkaz	Zkratka	Kód
Credit-Control-Request	CCR	272
Credit-Control-Answer	CCA	272
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258

8.11.2 S6a a S6d (MME/SGSN – HSS)

Referenční bod S6a (obr. 8.15) je určen pro přenos informací o účastníkovi mezi MME a HSS. Obdobně, referenční bod S6d je určen pro přenos informací o účastníkovi mezi SGSN a HSS (SGSN je entita 3G sítě, dále v tomto textu nezmiňována).

Referenční body S6a a S6d zajišťují následující procedury:

- Vyžádání autentizačních informací (*Authentication Information Retrieval Procedure*), kdy MME (resp. SGSN) žádá HSS o informace (tzv. autentizační vektor – viz



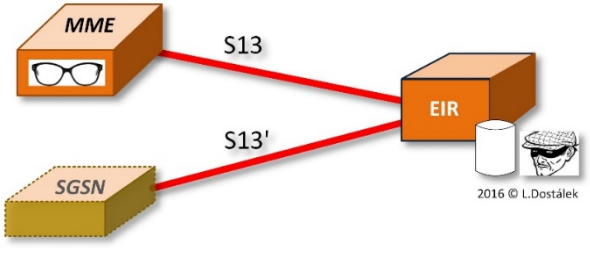
obr. 8.15 Referenční body S6a S6d

kap. 6), pomoci kterých bude moci autentizovat účastníka.

- Přechod do jiné buňky (*Update Location Procedure*), kdy MME (resp. SGSN) mění v HSS informace o lokalizaci účastníka. Tato procedura se používá v následujících případech:
  - Informování HSS o identitě MME (resp. SGSN), která aktuálně obsluhuje účastníka.
  - Předat MME (resp. SGSN informace o účastníkovi).
  - Poskytnout HSS informace o schopnostech mobilního zařízení účastníka.
- Výměna informací o účastníkovi (*Subscriber Data Handling Procedures*) – používá se mezi HSS a MME (resp. SGSN) pro změnu, zrušení nebo vyžádání informací o účastníkovi.
- Obnova pro výpadku (*Fault Recovery Procedures*) – používá HSS, aby informoval MME (resp. SGSN) o svém restartu.
- Notifikace: např. změn konfigurace mobilního zařízení, změna APN, dostupnost mobilního zařízení atd.

tab. 8.13 Příkazy aplikací Diameter S6a a S6d

Příkaz	Zkratka	Kód
Update-Location-Request	ULR	316
Update-Location-Answer	ULA	316
Cancel-Location-Request	CLR	317
Cancel-Location-Answer	CLA	317
Authentication-Information-Request	AIR	318
Authentication-Information-Answer	AIA	318
Insert-Subscriber-Data-Request	IDR	319
Insert-Subscriber-Data-Answer	IDA	319
Delete-Subscriber-Data-Request	DSR	320
Delete-Subscriber-Data-Answer	DSA	320
Purge-UE-Request	PUR	321
Purge-UE-Answer	PUA	321
Reset-Request	RSR	322



obr. 8.16 Referenční body S13 a S13'

Reset-Answer	RSA	322
Notify-Request	NOR	323
Notify-Answer	NOA	323

8.11.3 S13 a S13' (MME/SGSN – EIR)

Referenční bod S13 (obr. 8.16) slouží pro komunikaci mezi MME a registrem ukradených zařízení, který se nazývá EIR (*Equipment Identity Register*). Tj. v rámci autentizace účastníka je zjišťováno, jestli zařízení není registrováno v EIR. Obdobně referenční bod S13' slouží pro komunikaci SGSN (3G) a EIR. Význam registru EIR je velice omezený.

Klíčem v databázi EIR je IMEI (*International Mobile Equipment Identity*), což je unikátní číslo přidělené výrobcem mobilnímu zařízení.

tab. 8.14 Příkazy aplikací Diameter S13 a S13'

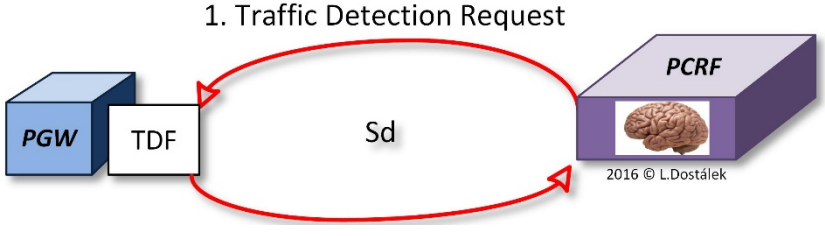
Příkaz	***Zkratka***	***Kód***
ME-Identity-Check-Request	*ECR*	*324*
ME-Identity-Check-Answer	*ECA*	*324*

8.11.4 Sd (TDF-PCRF)

Referenční bod Gx neumožňuje sledovat chování účastníků, aby je je schopen regulovat. Např. v případě jejich chování mimo stanovená pravidla. Byla proto zavedena další funkčnost PGW, která se označuje jako TDF (*Traffic Detection Function*) a referenční bod Sd, přes který PCRF umí detekovat chování účastníků. TDF monitoruje a detekuje provoz sledovaných služeb a na základě zadaných pravidel. Detekuje, např. start/ukončení sledované služby, provoz v rámci stanovených pravidel pro detekované služby.

Referenční bod Sd se umisťuje mezi PCRF (*Policy and Charging Rules Function*) a TDF. Přes tento referenční bod PCRF předává TDF pravidla pro sledování služeb (*Traffic Detection Request*) poskytovaných PGW a zpět získává hlášení o sledovaných službách (*Traffic Detection Report*). Na základě získaného hlášení, pak může (např. skrze referenční bod Gx):

- Povolit/blokovat detekované službě požadovaný datový tok
- Omezit datový tok (*Traffic Shaping*)
- Přesměrovat datový tok



obr. 8.17 Referenční bod Sd

tab. 8.15 Příkazy aplikace Diameter Sd

Příkaz	Zkratka	Kód
TDF-Session-Request	TSR	8388637
TDF-Session-Answer	TSA	8388637
Re-Auth -Request	RAR	258
Re-Auth -Answer	RAA	258

8.11.5 Gx*x* (PCRF – SGW)

Obecným označením Gx*x* se míní referenční body, které začínávají řetězcem "Gx" a to druhé "x" je zpravidla "a" nebo "c".

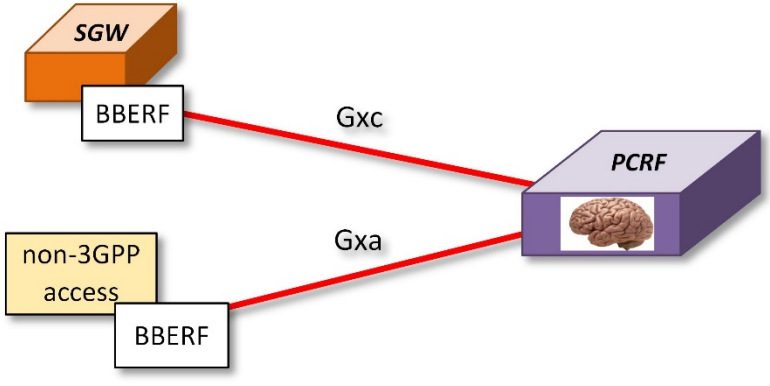
BBREF (*Bearer Binding and Event Reporting Function*) je funkce SGW nebo jiné entity pomocí které PCRF řídí datové nosiče (*bearer*). Pomocí referenčního bodu Gxc entita PCRF řídí alokaci datových toků na SGW. Pomocí referenčního bodu Gxa to lze řídit na obecné entitě blíže nespecifikované konsorciem 3GPP.

Gxc se používí pro:

- Poskytnutí/změnu/zrušení pravidel pro QoS datové toky spravované SGW.
- Odesílání událostí o datových tocích spravovaných SGW.

Procedury zajišťované skrze Gxc jsou:

- Žádost o poskytnutí QoS pravidel *(Gateway control and QoS Rules Request)*
- Poskytnutí QoS pravidel *(Gateway control and QoS Rules Provision)*
- Řízení o ukončení relace *(Gateway Control Session Termination)*
- Žádost o ukončení relace *(Request of Gateway Control Session Termination)*
- Zpracování chyb QoS pravidel *(QoS Control Rule error handling)*
- Propojení s relacemi referenčního bodu Gx *(Gateway Control session to Gx session linking)*



obr. 8.18 Referenční body Gxa a Gxc

- Podpora vice datových toků *(Multiple Bearer Binding Function support)*
- Podpora nastavení zasílání asynchronních událostí *(Provisioning of Event Triggers)*
- Volba módu datového nosiče *(Bearer Control Mode Selection)*
- Poskytování a vynucování politiky přidělování QoS toků *(Provisioning and Policy Enforcement of Authorized QoS)*
- Sledování aktivace/deaktivace *(Trace activation/deactivation)*
- Podpora procedur prováděných v určitou hodinu (*Time of the day procedures*)
- Podpora nouzového volání (*IMS Emergency Session Support*)
- Podpora prioritních relací, tj. např. prioritního volání (*Multimedia Priority Support*)
- Výpadek a obnova PCRF (*PCRF Failure and Restoration*)
- Vykazování přístupu do sítě (*Reporting Access Network Information*)

tab. 8.16 Příkazy aplikace Diameter Cxc

Příkaz	Zkratka	Kód
Credit-Control-Request	CCR	272
Credit-Control-Answer	CCA	272
Re-Auth -Request	RAR	258
Re-Auth -Answer	RAA	258

8.11.6 S9 (PCRF - PCRF)

Referenční bod S9 se používá v případě roamingu pro komunikaci mezi PCRF navštívené a PCRF domovské sítě. S9 přenáší informace o pravidlech (*policy*) pro QoS datové toky a informace o pravidlech účtování (*charging control information*) mezi navštívenou sítí a domovskou sítí. Referenční bod S9 je v případě *local breakout* volitelným. S9 realizuje následující procedury:

- Navázání, modifikace a ukončení S9 relace *(S9 Session Establishment, Termination, or Modification)* domovským PCRF
- Navázání, modifikace a ukončení S9 relace *(S9 Session Establishment, Termination, or Modification)* PCRF navštívené sítě
- Podpora nastavení zasílání asynchronních (*Event Triggers*)
- Podpora vice datových toků *(Multiple Bearer Binding Function support)*
- Poskytnutí a podpora defaultního datového nosiče *(Provisioning and validation of Default EPS Bearer authorized QoS)*
- Volba módu datového nosiče *(Bearer Control Mode Selection)*
- Vykazování přístupu do sítě (*Reporting Access Network Information*)
- Poskytnutí QoS přidělené domovskou PCRF
- Správa odložených relací *(Deferred Session Linking Handling)*

- Podpora připojení do různých sítí přes jedno APN *(Session Linking Handling When Multiple PDN Connection to a single APN is supported)*
- Žádost o pravidla (politiky) PCC *(Policy and Charging Control)* a politiky QoS
- Poskytnutí pravidel PCC a politik QoS
- *Rx over S9*
- Podpora *IP flow mobility*
- Detekce a řízení služeb *(Application Detection and Control)*

tab. 8.17 Příkazy aplikace Diameter S9

Příkaz	Zkratka	Kód
Credit-Control-Request	CCR	272
Credit-Control-Answer	CCA	272
Re-Auth -Request	RAR	258
Re-Auth -Answer	RAA	258
Trigger-Establishment-Request	TER	8388656
Trigger-Establishment-Answer	TEA	8388656

8.11.7 Rx (AF – PCRF)

Referenční bod Rx (obr. 8.19) propojuje požadavky IMS (kap. 4.4) a EPC (kap. 4.3). V případě odchozího nebo příchozího hovoru je třeba nejprve rezervovat datový tok (*bearer*) pro případ, že by byl hovor uskutečněn. Těsně před začátkem hovoru se pak datový nosič aktivuje pro příslušný hovor.

Referenční bod Rx se používá při zřizování aplikačních relací mezi PCRF *(Policy and Charging Rules Function)* a aplikační funkcí (AF). Pod aplikační funkcí si představíme např. P-CSCF (součást A-SBC).

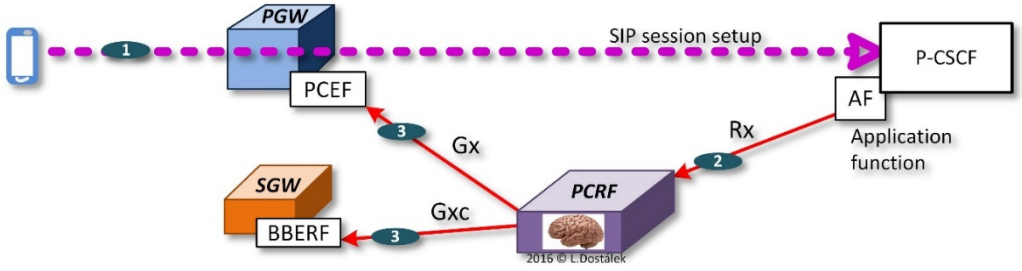
Na obr. 8.19 vidíme sestavování SIP relace (kap. 0). V případě, přijetí požadavku volaným (výsledkový kód SIP protokolu: 183 Session progress) se této výsledkový kód dostane až na P-CSCF, která jej odchytí a referenčním bodem Rx požádá PCRF zprostředkování rezervace datového média (*bearer*) v LTE síti. Poté předá výsledkový kód protokolu SIP volajícímu.

PCRF zajistí rezervaci referenčních bodů Gx a Gxc tak, že pomocí referenčního bodu Gx zašle na PGW pravidla PCC (*Policy and Charging Control)* skrze funkci PCEF. Obdobně na SGW zašle žádost o rezervaci datového toku pomocí funkce BBREF.

Analogicky, když volaný zvedne telefon, tak se medium aktivuje; v případě ukončení hovoru se zase deaktivuje.

Referenční bod Rx zajišťuje následující procedury:

- Poskytování informací o zřizované aplikační relaci (Initial Provisioning of Session Information)
- Modifikace aplikační relace (Modification of Session Information)
- Ukončení aplikační relace (AF Session Termination)



obr. 8.19 Referenční bod Rx

- Poskytování informací o otevření/uzavření datového toku RTP/RTCP *(Gate Related Procedures)*
- Poskytování informací o otevření/uzavření datového toku SIP *(Provisioning of AF Signaling Flow Information)*
- Žádání a poskytování informací statusu datového nosiče *(Subscription to Notification of Signaling Path Status)*
- Notifikování o událostech na datových nosičích *(Traffic Plane Events)*

tab. 8.18 Příkazy aplikace Diameter Rx

Příkaz	Zkratka	Kód
AA-Request	AAR	265
AA-Answer	AAA	265
Re-Auth-Request	RAR	258
Re-Auth -Answer	RAA	258
Session-Termination-Request	STR	257
Session-Termination-Answer	STA	257
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274

8.11.8 Cx (HSS - I-CSCF/S-CSCF)

Informace o účastnících poskytovaných službách jsou vedeny v HSS. V případě, že S-CSCF nebo I-CSCF potřebuje získat tyto informace (např. při registraci účastníka, při lokalizaci účastníka atp.), pak využije referenční bod Cx.

Referenční bod Cx poskytuje následující procedury:

- Výměnu lokalizačních informací účastníka
- Poskytnutí autentizačního vektor (AV) pro autentizaci účastníka metodou AKA (kap. 6)
- Výměnu autentizačních informací.

- Aktualizaci informací o účastníkovi v HSS

tab. 8.19 Příkazy aplikace Diameter Cx

Příkaz	Zkratka	Kód
User-Authorization-Request	UAR	300
User-Authorization-Answer	UAA	300
Server-Assignment-Request	SAR	301
Server-Assignment-Answer	SAA	301
Location-Info-Request	LIR	302
Location-Info-Answer	LIA	302
Multimedia-Auth-Request	MAR	303
Multimedia-Auth-Answer	MAA	303
Registration-Termination-Request	RTR	304
Registration-Termination-Answer	RTA	304
Push-Profile-Request	PPR	305
Push-Profile-Answer	PPA	305

8.11.9 Sh (HSS - AF)

Jestliže účastník již naváže relaci se SIP aplikačním serverem, pak aplikace může chtít vyhledat v HSS další informace o účastníkovi. K tomu slouží referenční bod Sh.

Procedury poskytované referenčním bodem Sh:

- Zjištění dat o účastníkovi v HSS
- Upsání se HSS (*Subscription/Notification*) k tomu, aby HSS informoval aplikační server o změnách údajů o účastníkovi v HSS.

tab. 8.20 Příkazy aplikace Diameter Sh

Příkaz	Zkratka	Kód
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307

8.11.10 Zh a Zn (HSS - AF)

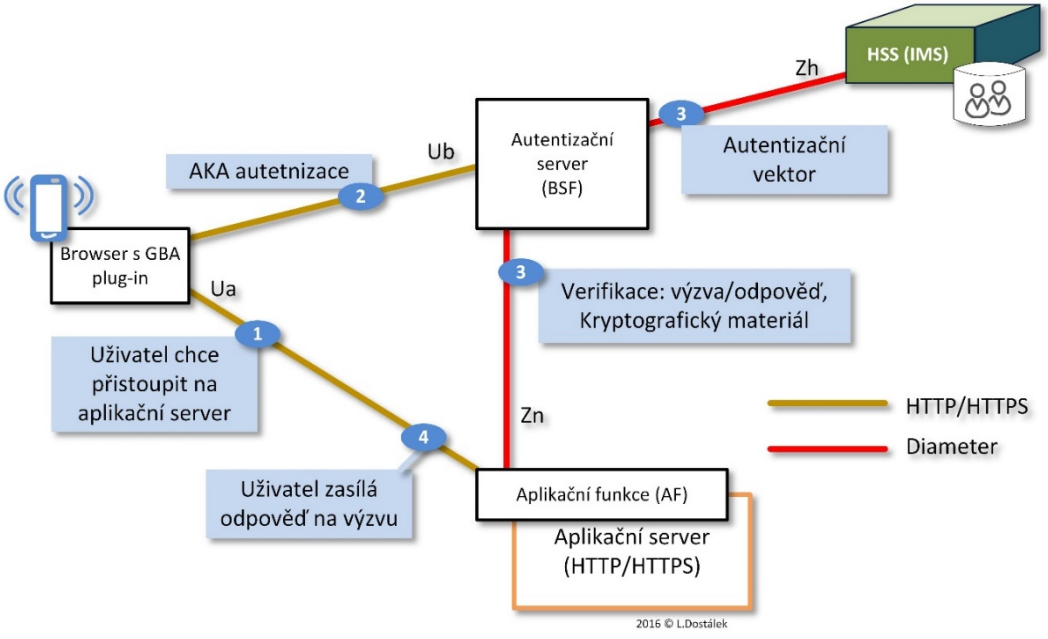
Zatímco Cx referenční bod je určen pro zjišťování informací o účastníkovi v HSS pro aplikační funkce na bázi protokolu SIP, tak referenční bod Zh je určen pro zjišťování informací o účastníkovi v HSS, který ale přistupuje do sítě přes protokol HTTP. Jinými slovy, referenční bod Zh spolu s referenčním bodem Zn umožňují využít k autetnizaci na web prostředky mobilního zařízení. Tj. umožňují se na web autentizovat pomocí USIM/ISIM.

Obezná architektura autentizace na web pomocí USIM/ISIM se nazývá GBA (*Generic Bootstrapping Architecture*). Pro autentizaci je použita metoda HTTP Digest [9] s modifikací pro AKA mechanismus (kap. 6) [21].

- Referenční bod Ua (obr. 8.20), který je pro webový přístup účastníka na obecný webový portál.

Jestliže se klient se chce autentizovat na obecný Aplikační server, pak:

1. Účastník přistoupí protokolem HTTP/HTTPS přes referenční bod Ua na aplikační server.



obr. 8.20 Referenční body Zh, Zn. Ua a Ub

Jsou definovány dva referenční body:

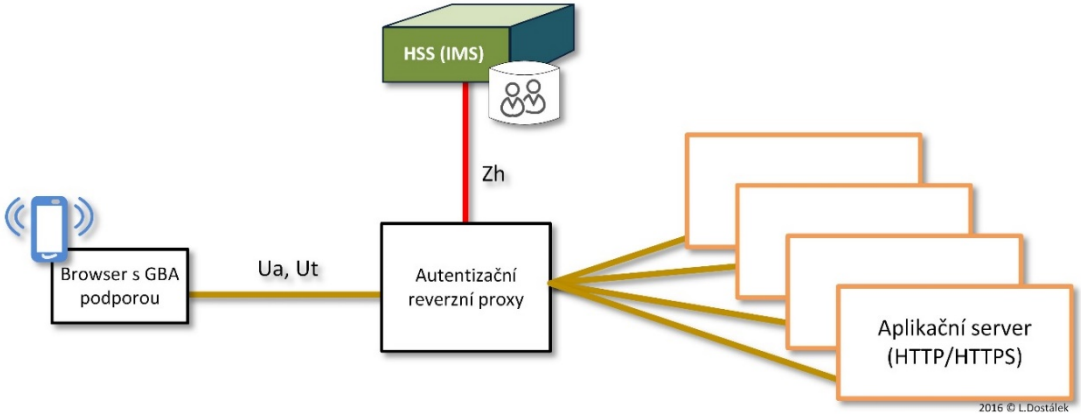
- Referenční bod Ut (kap. 19.4), který je pro webový přístup účastníka na webový portál operátora.

2. Aplikační server jej přesměruje na Autentizační server BSF.
3. Autentizace probíhá AKA mechanismem skrze referenční bod Ub:
   a. BSF požádá přes referenční bod Zh HSS o autentizační vektor a provede autentizaci účastníka mechanismem

AKA. Následně BSF předá pře referenční bod Zn aplikačnímu serveru předá kryptografický materiál pro autentizaci účastníka na aplikační server, který je odvozen od IK a CK.

b. Účastník se autentizuje vůči aplikačnímu serveru na základě kryptografického materiálu získaného přes referenční bod Ub (aplikační server získal kryptografický materiál přes referenční bod Zn).

V uvedeném modelu je oddělena funkce aplikačního serveru a autentizačního serveru, pro-



obr. 8.21 Autentizační proxy

tože každý z nich může provozovat jiný subjekt.

Jednouší architektura vyžívá Autentizační server jako reverzní proxy (obr. 8.21). Tato architektura se používá zejména pro referenční bod Ut (kap. 19.4).

8.11.11 Sy (PCRF – OCS)

Referenční bod Sy je mezi PCRF (domovské sítě) a OCS (*Online Charging System*). Referenční bod Sy umožňuje přenos vyčerpaném mužství poskytnutých zdrojů (“o snižujícím se kreditu”) z OCS do PCRF. Referenční bod Sy poskytuje následující funkce:

- PCRF zasílá OCS informace o změně množství poskytnutých zdrojů.
- OCS poskytuje PCRF informace o dosažení limitu čerpání zdrojů.
- PCRF zasílá OCS informace o zrušení hlášení o čerpání zdrojů.

tab. 8.21 Příkazy aplikace Diameter Sy

Příkaz	Zkratka	Kód
Spending-Limit-Request	SLR	8388635
Spending-Limit-Answer	SLA	8388635
Spending-Status-Notification-Request	SNR	8388636

Spending-Status-Notification-Answer	SNA	8388636

8.11.12 SGd (MME - SMS brána)

Přes tento referenční bod se předávají SMS zprávy z MME na SMS bránu (směr MO), a také v opačném směru (MT) z SMS brány na MME.

tab. 8.22 Příkazy aplikace Diameter SGd

Příkaz	Zkratka	Kód
MO-Forward-Short-Message Request	OFR	8388645
MO-Forward-Short-Message Answer	OFA	8388645
MT-Forward-Short-Message Request	TFR	8388646
MT-Forward-Short-Message Answer	TFA	8388646

8.11.13 Gy/Ro (Online Charging)

Referenční bod Ro zahrnuje funkcionality referenčního bodu Gy. Referenční bod Gy je mezi OCS (Online Charging System) a PCEF. Principiálně komunikace skrze tyto referenční body vychází z aplikace Diameter Credit Control (kap. 8.10)

8.11.14 Rf (Offline Charging)

Principiálně komunikace skrze trnyo referenční bod vychází z aplikace Diameter Účtování (kap. 8.9)

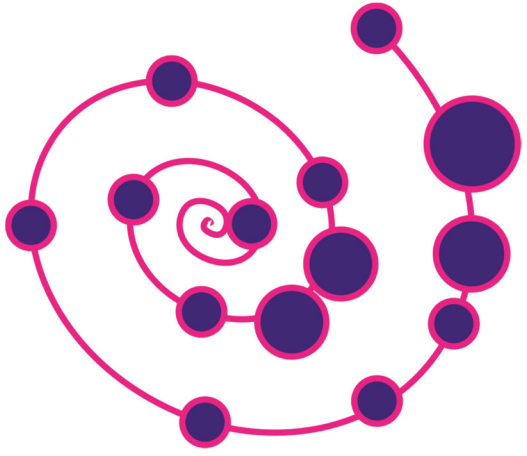
8.12 Zabezpečení

Protokol Diameter by se měl vždy zabezpečovat pomocí TLS nebo DTLS a to dříve, než začne dialog *Capabilities Exchange*. Jako alternativní (doplňková) forma zabezpečení může být použit IPsec, avšak všechny implementace by měly podporovat zabezpečení TLS/TCP a DTLS/SCTP. Kryptografický materiál pro zabezpečení protokolu Diameter (pro TLS/DTLS/IPsec) musí být zajištěn nezávisle na protokolu Diameter. [23]. Standard zakazuje komunikovat protokolem Diameter nezabezpečeně. Pochopitelně, že tato doporučení je třeba brát s rozumem a komunikaci v rámci jednoho fyzického serveru nebo vedle sebe stojících fyzických serverů v zabezpečeném prostředí je třeba zabezpečovat na základě výsledků analýzy rizik.

Zabezpečení pomocí TLS/DTLS musí být oboustranné. Tj. server se musí představit svým certifikátem veřejného o klíče, který musí být pro klienta důvěryhodným (tj. vydán důvěryhodnou certifikační autoritou) a naopak klient se musí představit svým certifikátem veřejného o klíče, který musí být pro server důvěryhodným (tj. vydán důvěryhodnou certifikační autoritou).

Pokud máme k dispozici certifikát veřejného klíče např. serveru, pak je třeba si uvědomit, že certifikováno je spojení veřejného klíče s DNS jménem (resp. IP adresou serveru). Na serveru může běžet nejenom více aplikací protokolu Diameter, ale např. webový server atp. Tj. certifikát serveru bez dalšího nic ještě nevyjadřuje o tom, jestli je určen pro autentizaci protokolu Diameter. Je určen jen pro autentizaci nějaké aplikace běžící na tomto serveru.

Řešením, jak v certifikátu vyjádřit, že certifikát je určený pro autentizaci konkrétní aplikace je např., že v certifikátu bude uvedeno jak DNS jméno z NAPTR záznamu, tak i pole *replacement* z NAPTR záznamu. Obdobně v případě SRV záznamů bude v certifikátu uvedeno jak DNS jméno ze SRV záznamu, tak i pole *target*.

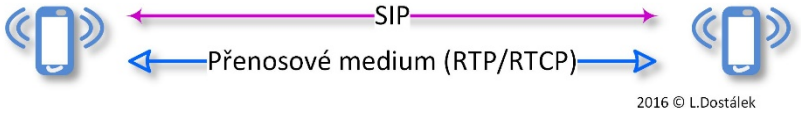


9. SIP

SIP (*Session Initiation Protocol*) [61] je aplikační protokol, pomocí kterého je možné navázat, modifikovat a ukončovat multimediální relace (telefonní hovory, telekonference apod.). Pomocí protokolu SIP mohou být přizvání další účastníci do již běžících relací (např. multimediálních konferencí). Rovněž mohou být přidány/odebrány další přenosová multimediální media.

Protokol SIP ale není integrovaným komunikačním systémem. SIP se používá společně s dalšími síťovými protokoly pro vytvoření komunikační architektury. Typicky (obr. 9.1) tato architektura dále zahrnuje protokoly jako je RTP (*Real-time Transport Protocol*) pro přenosové medium v reálném čase, SDP (*Session Description Protocol*) pro popis multimediálních relací apod.

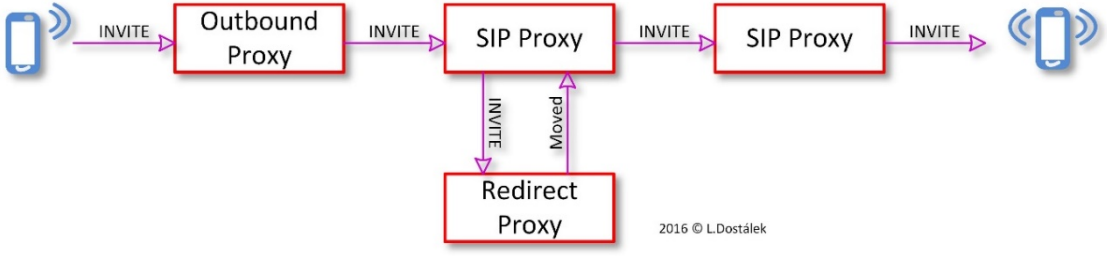
SIP je sice protokol typu klient/server, ale podobně jako v případě protokolu SMTP používáme termín SIP agent, protože většina SIP entit vystupuje jednou jako klient (zpravidla volající) a podruhé jako server (volaný). Koncový účastník často používá SIP agent v provedení SIP telefonu, který poskytuje tradiční telefonní služby jako vytáčení, odmítnutí hovoru, přijetí hovoru, pozastavení hovoru, předání hovoru atd. SIP navíc umožňuje další služby jako Rychlé zasílání zpráv (*Instant Messaging*) apod.



obr. 9.1 Protokol SIP se zpravidla používá ve spojení s dalšími protokoly

Komunikace pouze dvou koncových entit je možná, ale je trochu nepraktická zejména pro veřejné poskytovatele komunikačních služeb. V reálném světě tak spolu obvykle nekomunikují pouze dva účastníci. SIP proto zavádí několik mezilehlých entit (obr. 9.2), pomocí kterých je možné vybudovat požadovanou sítovou topologii.

Protokol SIP nenahrazuje jen klasickou telefonní komunikaci, ale volání může přenášet i video,



obr. 9.2 Příklad topologie SIP entit

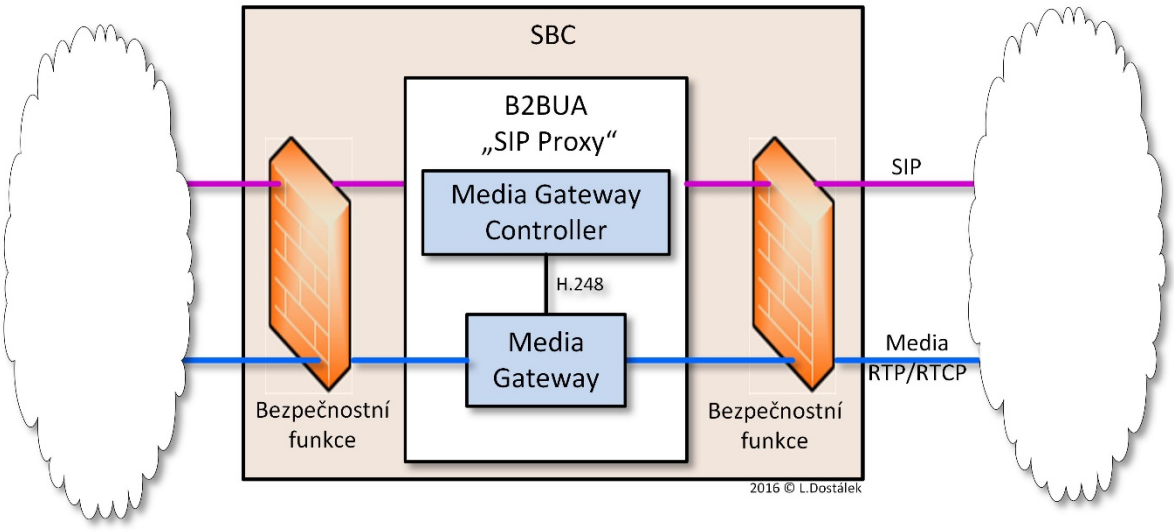
text atp. Proto se obecně nehovoří o „hovoru“, ale o „multimediálním přenosu“ – zkráceně „media“. Navíc protokol SIP otevírá možnosti další služeb, jako jsou konference (pochopitelně multimediální), dále pak např. prezentační služby, které poskytují informace o stavu účastníků (např. Online, Nepřítomny, Nerušit apod.). Prezentační služby mohu poskytovat nejenom informace o tom, jestli jsou ostatní účastníci dostupní, ale mohou poskytovány další informace o ostatních účastnících, jako jsou kontaktní informace, ale třeba i obchodní informace o nabízených službách.

Specifickou komunikací podporovanou protokolem SIP je „Zmáčkni a mluv“ (*Push to talk over Cellular*), která umožňuje polo-duplexní komunikaci v rámci skupiny účastníků. Tj. je obdobou volání „vysílačkou“. Tento způsob komunikace je výhodný např. v rámci záchranných týmů.

tab. 9.1 Entity SIP protokolu

Entita	***Význam***
User Agent (UA)	Logická entita, která může pracovat jako UAC i jako UAS. Typickým příkladem UA je „SIP telefon“.
User Agent Client (UAC)	Logická entita, která inicializuje nové požadavky (např. vytvoření multimediální relace). Role UAC trvá pouze během konkrétní relace. Jinými slovy: software, který realizuje vytvoření relace, pracuje jako UAC během této relace. Když později tento software naopak přijímá nový SIP požadavek, pak bude vystupovat v roli UAS po dobu této nové relace.
User Agent Server (UAS)	Logická entita, která generuje odpověď na SIP požadavek. Odpovědí může být přijetí, odmítnutí nebo přesměrování SIP požadavku. Role UAS trvá jen po dobu jedné transakce. Software, který realizuje UAS vystupuje jako UAS jen po dobu relace. V následující relaci může např. inicializovat nový požadavek, pak v této následující relaci bude vystupovat jako UAC.
Server	SIP server je síťový element, který přijímá SIP požadavky a odpovídá na ně. Příkladem serveru je SIP Proxy, UAS nebo Registrátor.
Proxy, Proxy Server	Proxy je mezilehlá entita, která pracuje jako server i jako klient. Serverová část proxy přijímá požadavky jiných klientů, předává je klientské části proxy, která požadavky vyřizuje jejich jménem. Proxy je důležitá pro SIP směrování, tj. předává SIP požadavky blíže k cílovému SIP serveru. Proxy může být rovněž užitečná pro vynucování bezpečnostní politiky při předávání SIP požadavku. Proxy může interpretovat a přepisovat části SIP požadavků před tím, než je předá.

Odchozí proxy (*Outbound Proxy*)	Odchozí SIP proxy přijímá požadavky klientů, i když klient není schopen rozpoznat SIP server v požadovaném SIP URI (např. není schopen provést příslušný DNS překlad). Odchozí SIP proxy se konfiguruje v UA buď ručně nebo pomocí autokonfiguračních protokolů (např. DHCP).
Back-to-Back User Agent (B2BUA)	B2BUA je logická entita, která akceptuje SIP požadavek jako UAS. Avšak její klientská část (UAC) vytvoří nový požadavek, který předá směrem k cílovému SIP serveru. Na rozdíl od SIP Proxy B2BUA akceptuje a předává multimediální dialog (např. RTP/RTCP). Příkladem B2BUA je SBC (*Session Border Controller*).
Registrátor (Register)	Registrátor je koncová SIP entita, která přijímá požadavky (metody) REGISTER od registrujících se do sítě agentů (UA). A tyto požadavky předává lokalizační službě (*location service*). Lokalizační služba spojuje jednu (nebo více) SIP URI registrujícího se agenta s jeho kontaktní adresou. Více agentů (UA) může mít zaregistrováno stejné SIP URI – všichni takto registrovaní agenti (UA) mohou přijímat hovory na toto SIP URI.
Redirect Server	Jedná se agenta, který generuje odpovědi 3xx (Redirection) na požadavky, které přijal. Přesměrovává tím požadavky na množinu alternativních SIP URI. Redirect server umožňuje SIP proxy směrovat SIP komunikaci do externích domén.
Gateway	Gateway je brána do jiných sítí. Např. do veřejných telefonních sítích založených na starších protokolech (SS7 apod.).
***Event State Compositor* (ESC)**	Jedná se o UAS, který přijímá, zpracovává a odpovídá na požadavky nesoucí metodu PUBLISH.
Policy server	Entita, která UA poskytuje Politiky komunikace (*policy*). Odchozí proxy může na zprávu UAC obsahující metodu INVITE odpovědět chybou „488 Not Acceptable Here“ s tím, součástí této odpovědi je i hlavička Policy-Contact s URI Policy serveru. UAC následně kontaktuje Policy server, který vrátí zprávu s hlavičkou Policy-ID obsahující indikaci, že Policy server byl kontaktován. Následně UAC zopakuje INVITE, ale s přidanou hlavičkou Policy-ID přijatou od Policy serveru. Tento nový požadavek INVITE už bude patrně odchozí proxy přijat.
Relay	Proxy nebo B2BUA entita, která přijímá požadavky s tím, že cílové URI překládá na jedno nebo více cílových URI. Tj. může i množit SIP požadavky na více cílů (může je „množit“).



obr. 9.3. Session Border Controller (SBC)

9.1 SBC

A SBC (*Session Border Controller)* je B2BUA entita často kombinovaná s bezpečnostními a dalšími funkcemi (obr. 9.3). Funkčnost SBC lze přirovnat k firewallu oddělujícího sítě různých bezpečnostních zón.

SBC se zpravidla skládá z:

- SIP entity B2BUA, která akceptuje nejenom SIP protokol, ale i přenosové médium. Akceptované požadavky pak předává jménem původního klienta dále k cílovému serveru.
- Bezpečnostní funkce („firewally“), které jsou zpravidla odlišné pro vstup požadavku a pro výstup požadavku.
- Další funkce (nejsou znázorněny na obrázku obr. 9.3), kterými může být např. autentizace účastníků vůči externí databázi účastníků, účtování atd. Pro tyto funkce se často využívá protokol Diameter (kap. 8).

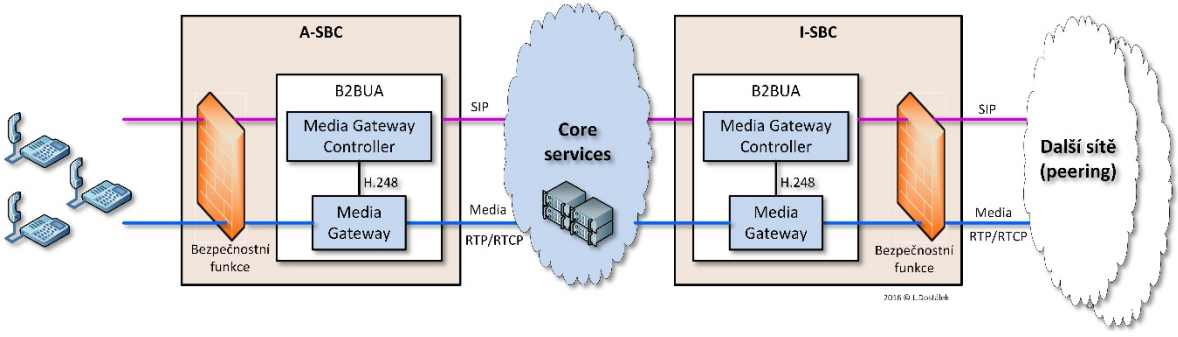
Někteří výrobci dodávají multifunkční boxy, kde lze namísto B2BUA entity konfigurovat též gateway. Topologie zůstává podobná, avšak výstupním protokolem již pak není SIP, ale např. SS7 [62].

Entita B2BUA se skládá z entit:

- MGC (*Media Gateway Controller*), který akceptuje požadavky protokolu SIP a předává je směrem k cílovému SIP serveru.

- MG (*Media Gateway*), která akceptuje a přenosové médium (RTP/RTCP).

Jelikož jádro sítě považujeme za „bezpečnou zónu“, pak může minimalizovat bezpečnostní



obr. 9.4 A-SBC a I-SBC

Důležité je, že MGC a MG se musí vzájemně domluvit, co mají akceptovat a předávat dále. K této slouží zpravidla protokol H.248 (kap. 13).

Z hlediska poskytovatelů mobilních sítí je SBC ochranným prvkem chránícím jádro (*core*) jejich sítí od ostatních aktérů mobilních sítí. Používají specializované SBC, které se označují (obr. 9.4):

- A-SBC (*Access SBC*), který je specializovaný na přístup koncových účastníků (*subscribers*). Jeho částí je zejména autentizace přistupujících účastníků, účtování a mnohdy i vytvoření IPsec tunelů mezi přistupujícími účastníky a A-SBC. A-SBC též skryje topologii jádra sítě před účastníky.
- I-SBC (*Interconnect SBC*), který propojuje poskytovatele s ostatními poskytovateli. Opět zajišťuje např. vytvoření IPsec tunelů mezi I-SBC a ostatními poskytovateli (resp. poskytovateli IPX, skrytí topologie jádra sítě atd.

funkce na rozhraních SBC směrem k jádru sítě (na obr. 9.4 nejsou vůbec znázorněny). Ovšem to neznamená, že tam nemohou být implementovány.

Komunikace protokolem SIP mezi entitami jádra sítě (*core*) se považuje za bezpečnou také v tom smyslu, že entity se mezi sebou vzájemně nemusí autentizovat. Autentizaci účastníků provede entita A-SBC a ostatní entity tomu důvěřují. To platí i v případě, že účastník byl autentizován v navštívené (cizí) síti a jeho požadavek přišel skrze I-SBC. To pravděpodobně bohužel jinak řešit nelze, ale podle mého názoru to v budoucnu přinese mnohá bezpečnostní překvapení.

9.1.1 Více rozhraní SBC

Klasické firewally ve firmách často připojujeme k více různým bezpečnostním zónám tak, že do nich vkládáme více síťových karet. V případě, že potřebujeme připojit k jádru mobilní sítě více bezpečnostních zón (např. VoIP a VoLTE na

straně A-SBC), pak se jeví dobrým nápadem vložit do SBC více síťových karet, podobně jak tak činíme v případě podnikových firewallů.

V tomto případě je třeba být ale obzvláště opatrným a zvážit rizika, protože na rozdíl od připojení firmy se zde často propojují sítě, které podléhají zákonu č. 181/2014 Sb., o kybernetické bezpečnosti. Problém je v tom, že útočník z jedné bezpečnostní zóny může např. omezit činnost celého SBC (s více sítovými kartami) a tím paralyzovat kritickou infrastrukturu. Dodavatelé SBC někdy řeší tento problém kompromisem, kterým je, že bezpečnostní funkce jsou implementovány na každé síťové kartě samostatně (tj. nezávisle na ostatních síťových kartách). Útočník pak např. DDoS útokem může omezovat jednu kartu, ale neomezí tím komunikaci na ostatních kartách.

9.2 Paket (zpráva) protokolu SIP

Protokol SIP definuje zprávy, které se vyměňují mezi SIP entitami. Jedná se např. o zprávy vedoucí k navázání, ukončení a modifikaci relací, které mohou obsahovat jeden nebo více datových toků (*media streams*).

Protokol SIP je textově orientovaným protokolem, syntakticky podobným protokolu HTTP. Podobně jako v protokolu HTTP zde máme dva typy zpráv: požadavek a odpověď. Požadavek rovněž začíná metodou (obr. 9.5) a odpověď začíná stavovým řádkem nesoucí kód odpovědi (chybový kód).

tab. 9.2. Metody protokolu SIP

Metoda	Standard	Význam
ACK	RFC3261	Potvrzuje přijetí zprávy
BYE	RFC3261	Ukončuje relaci mezi dvěma účastníky konference
CANCEL	RFC3261	Ukončuje nedokončený požadavek
INFO	RFC6086	Přenáší aplikační informace mezi koncovými body
INVITE	RFC3261 RFC6026	Vyzývá k vytvoření relace mezi účastnickými agenty (UA)
MESSAGE	RFC3428	Přenos zpráv (*Instant Messaging*)
NOTIFY	RFC6665	Metoda NOTIFY se používá k informování účastníků o změnách stavu (např. události).
OPTIONS	RFC3261	Žádá informace o schopnostech volajícího (bez zřízení relace)

PRACK	RFC3262	Metoda PRACK (*Provisional Response ACKnowledgement*) zvyšuje spolehlivost sítě přidáním „spolehlivého“ potvrzovacího mechanismu. Požadavky s metodou PRACK jsou obdobou požadavků s metodou ACK, avšak jsou odesílány jako reakce na dočasné odpovědi: Provisional (1xx).
PUBLISH	RFC3903	Publikuje stav (resp. změnu stavu) události. I když syntakticky je obdobou metody REGISTER, tak smyslem je obdobou metody NOTIFY – umožňuje vytvořit, modifikovat a zrušit událost.
REFER	RFC3515	Indikuje, aby příjemce (identifikovaný v *Request-URI*) kontaktoval třetí stranu uvedenou v tomto požadavku. Např. přesměrování hovorů.
REGISTER	RFC3261	Registruje kontaktní informace účastníku.
SUBSCRIBE	RFC6665	Odebírání zdrojů nebo hovorů pro nejrůznější zdroje nebo volání sítě.
UPDATE	RFC3311	Umožňuje UAC změnit parametry relace (např. množinu datových toků, kodeky apod.) aniž by došlo ke změně stavu relace (např. k přerušení relace).

tab. 9.3 Kódy odpovědi protokolu SIP

Kódy odpovědi	**Význam**
Provisional (1xx)	Přijatý požadavek je zpracováván (dočasná odpověď).
Success (2xx)	Požadavek byl úspěšně přijat, pochopen a akceptován.
Redirection (3xx)	Ke zpracování požadavku je třeba další akce (zpravidla klientem).
Client Error (4xx)	Požadavek je syntakticky chybný a nemůže být serverem zpracován.
Server Error (5xx)	Server zhavaroval při zpracování patrně správného požadavku.
Global Failure (6xx)	Požadavek nemůže být zpracován žádným serverem.

9.2.1 SIP URI, TEL URI a nouzová volání

Každý prvek sítě protokolu SIP je identifikován pomocí URI (*Uniform Resource Identifier*), který je obecným standardem používaným např. pro web nebo elektronickou poštu. V mobilních sítích se nejčastěji používá SIP URI nebo TEL URI.

SIP URI vždy začíná schématem „sip“ nebo „spis“ (SIP přes SSL/TLS) následovaným dvojtečkou. Obecně má tvar:

sip:username:password@doména:port;parametery

Příklady:

sip:Josef.Novak@firma.cz

sip:123456789@oeprator.cz;lr

tab. 9.4 Parametry SIP URI

Parameter	Význam
comp	SIP komprese (*Signaling Compression*).
lr	Indikuje, že tento zdroj má implementován mechanismus směrování SIP protokolu *(SIP routing mechanisms).*
maddr	Indikuje, že adresa SIP je vícesměrovou adresou (*Multicast address*).
method	Tento parametr umožňuje explicitně specifikovat metodu protokolu SIP, která má být použita.
transport	Tento parametr umožňuje explicitně specifikovat SIP transportní protokol (UDP, TCP, SCTP).
ttl	Specifikuje hodnotu parametru TTL (*time-to-live*) v UDP více směrových (*multicast*) paketech. Může se použít jen v případě více směrových (*multicast*) paketů a protokolu UDP.
user	Tento parametr umožňuje rozlišit telefonní číslo od účastnického jména mající tvar telefonního čísla. V případě, že účastnické jméno by bylo možné zaměnit za telefonní číslo, pak se uvede parametr “user=phone”.

Alternativně může být použito TEL URI, které má tvar:

```
tel:telefonní-číslo;parametry
```

Kde telefonní-číslo může být telefonní číslo formátu E.164 nebo telefonní číslo v privátním formátu. Telefonní číslo je zajímavé zejména kvůli zpětné kompatibilitě se zastaralými sítěmi. SIP agent musí nejprve telefonní číslo z TEL URI převést pomocí DNS ENUM na SIP URI a teprve pak je možné navazovat relaci protokolem SIP.

Příklad:

```
tel:+420-201-555-0123
```

URI (Uniform Resource Identifier) je obecný identifikátor, který může být:

- buď všeobecně známý URL (*Uniform Resource Locator*), který popisuje i způsob, jak se k požadovanému zdroji dostat. Příkladem jsou HTTP URI nebo SIP URI.
- nebo URN (*Uniform Resource Name*), který neřeší jak se k identifikovanému zdroji dostat.

Pro nouzová volání se používají URN (volající nechce řešit jak se záchranné službě dovolat, chce zachránit). RFC-5031 definuje následující ‘sos’ URN Sub-Services:

tab. 9.5 SIP URN

Service	**Description**
sos	Všeobecné volání o záchranu
sos.ambulance	Ambulance (záchranka)
sos.animal-control	Zvěrolékař
sos.fire	Hasiči
sos.gas	Únik plynu
sos.marine	Námořní záchranná služba
sos.mountain	Horská služba
sos.physician	Lékařská služba
sos.poison	Toxikologie
sos.police	Policie

Příklady:

```
urn:service:sos
urn:service:sos.fire
```

9.2.2 Formát zprávy protokolu SIP

Zpráva protokolu SIP (obr. 9.5) používá formát standardu "*Internet Message Format*", který byl zaveden legendárním standardem RFC-822 z roku 1982 (dnes aktuálně standardizován RFC-5322). "*Internet Message Format*" používá i většina ostatních textově orientovaných protokolů jako např. HTTP nebo SMTP.

Protokol SIP je protokol typu klient/server. A to i přesto, že koncové entity mohou jednou vystupovat jako klient a podruhé jako server – obdobně jako např. protokol SMTP. Z toho důvodu o koncových entitách (software) hovoříme jako o agentech.

V protokolu SIP klient odesílá zprávu, která obsahuje v prvním řádku záhlaví tzv. metodu (obdobně jako protokol HTTP). Server následně odpovídá zprávou, která v prvním řádku záhlaví obsahuje výsledkový kód.

Zpráva protokolu SIP (obr. 9.5) se skládá ze záhlaví a těla odděleného jedním prázdným řádkem. Záhlaví zprávy se skládá z hlaviček, které začínají klíčovým slovem odděleným dvojtečkou.

Protokol SIP (obdobně jako protokol SMTP) používá v mnoha hlavičkách tzv. Zobrazované jméno (*Display Name*). Zobrazované jméno zobrazuje software koncovým účastníkům. Kdežto skutečná technicky používaná adresa se skrývá ve špičatých závorkách:

```
To: Fantomas II. <Josef.No-
    vak@firma.cz;ttl=20>
```

Je tu však jeden naprosto zásadní rozdíl oproti protokolu SMTP, který zejména při prvním setkání s analýzou paketů protokolu SIP může činit potíže: SIP server totiž kopíruje některé hlavičky z klientovy zprávy beze změny do odpovědi. Jedná se zejména o hlavičky: To, From, Call-ID, CSeq and Via. U jiných hlaviček tak naopak nečiní (Contact, Accept-* a pod.). Prakticky je to vidět na příkladu (tab. 9.3).

obr. 9.5 Zpráva protokolu SIP

Klíčové slovo frekventovaných hlaviček protokolu SIP (tab. 9.7) má kromě dlouhého tvaru i jednopísmenný tvar (v tab. 9.7 uveden v závorce za dlouhým tvarem).

tab. 9.6 Přiklad SIP zpráv (přejat z RFC-3261)

Požadavek (zpráva od klienta)	**Odpověď serveru**

`INVITE sip:bob@biloxi.com SIP/2.0`
`…`
`To: Bob <sip:bob@biloxi.com>`
`From: Alice`
`<sip:alice@at-lanta.com>;tag=1928301774`
`Call-ID: a84b4c76e66710@pc33.atlanta.com`
`CSeq: 314159 INVITE`
`Contact: <sip:alice@pc33.atlanta.com>`
`…`
	`SIP/2.0 200 OK`
	`….`
	`To: Bob <sip:bob@biloxi.com>;tag=a6c85cf`
	`From: Alice`
	`<sip:alice@atlanta.com>;tag=1928301774`
	`Call-ID: a84b4c76e66710@pc33.atlanta.com`
	`CSeq: 314159 INVITE`
	`Contact: <sip:bob@192.0.2.4>`
	`…`

tab. 9.7 Hlavičky protokolu SIP

Hlavička	**Standard**	**Význam** `Příklad`
Accept	RFC3261	Akceptované typy obsahu. `Accept: application/sdp;level=1, text/html`
Accept-Contact (a)	RFC3841	Umožňuje, aby si UAC nastavil (specifikoval), že bude přijímat (akceptovat) pouze relace (hovory), které odpovídají (*matches*) některým nebo všem (*) hodnotám metody. `Accept-Contact: *;mobility="mobile";methods="INVITE"`
Accept-Encoding	RFC3261	Akceptovaná kódování obsahu.

		`Accept-Encoding: gzip`
Accept-Resource-Priority	RFC4412	Vyjmenovává tzv. *resource values* (r-values), které je SIP server schopen zpracovat. Blíže viz hlavička Resource-Priority. `Accept-Resource-Priority: dsn.flash-override, dsn.flash, dsn.immediate, dsn.priority, dsn.routine`
Accept-Language	RFC3261	Indikuje preferované jazyky (s vyšší hodnotou q je více preferovaným) `Accept-Language: da, en-gb;q=0.8, en;q=0.7`
Alert-Info	RFC3261	Specifikuje alternativní vyzváněcí tóny UAS `Alert-Info: <http://www.example.com/sounds/moo.wav>`
Allow	RFC3261	Vyjmenovává podporované metody protokolu SIP `Allow: INVITE, ACK, OPTIONS, CANCEL, BYE`
Allow-Events (u)	RFC6665	Obsahuje seznam balíků událostí, pro které účastník může vystupovat v roli oznamovatele (*notifier*). Tj. UA odesílá tuto hlavičku, aby propagoval, že může zpracovávat SUBSCRIBE a generovat NOTIFY pro balíky události uvedené v této hlavičce.
Answer-Mode	RFC5373	Chování UA vztahující se k akceptování nebo odmítání požadavků. `Answer-Mode: Manual;require`
Authentication-Info	RFC3261	Hlavička se využívá v rámci vzájemné autentizace metodou Digest. `Authentication-Info: nextnonce="47364c23432d2e131a5fb210812c"`
Authorization	RFC3261	Autentizační hlavička. Často následuje jako odpověď po autentizační výzvě WWW-authenicate (např. jako součást odpovědi `401 Unau-`

		thorized). Prvním parametrem je autentizační metoda (Basic, Digest apod.), dále následují parametry závislé na autentizační metodě. Např. • username – účastnické jméno autentizujícího se účastníka. • realm – autentizační doména do které se účastník autentizuje • nonce – náhodný řetězec, který se kopíruje do odpovědi • response – autentizační odpověď `Authorization: Digest username="Alice", realm="firma.cz", nonce="84a4cc6f3082121f32b42a2187831a9e", response="7587245234b3434cc3412213e5f113a5432"`
	TS 24.229	Standard 3GPPP TS 24.229 zavádí další parametr: • integrity-protected, tento parametr se předává mezi důvěřujícími si entitami (proxy, B2BUA, relay apod.). Hodnota „yes“ vyjadřuje, že účastník přistoupil na A-SBC bezpečným kanálem, tj. během registrace vznikly IPsec SA a následně pomocí IPsec byl vytvořen bezpečný kanál, který zajišťuje integritu (avšak nutně nemusí být aktivováno šifrování protokolem ESP). Výše uvedené parametry se plní v případě algoritmu AKA: • nonce=RAND+AUTN (plus je oddělovač spojení řetězců a AUTN= SQN⊕AK‖AMF‖MAC-A) • algorithm=AKAv1-MD5 • realm= DNS jméno domovské sítě. • Response=XRES
Call-ID (i)	RFC3261	Jedinečný identifikátor, který identifikuje hovor nebo všechny registrace konkrétního klienta. SIP server je povinen tuto hlavičku vždy zkopírovat do odpovědi.

		`Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@biloxi.com`
		Nebo v krátké formě:
		`i: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@192.0.2.4`

Call-Info	RFC3261	Poskytuje dodatečné informace o volajícím nebo volaném
		`Call-Info: http://wwww.example.com/alice/photo.jpg`
		`;purpose=icon`

Contact (m)	RFC3261
	RFC4596
	RFC3840
		Poskytuje URI, jehož význam závisí na typu požadavku nebo odpovědi. Ve spojení s metodou INVITE určuje přímý kontakt na iniciátora zprávy. Ve spojeni s metodou REGISTER může obsahovat řadu vlastností, které budou následně uloženy v Lokalizační databázi pro případ, že někdo bude registrovanému volat..
		Může obsahovat např. parametry:
		• `q` – priorita kontaktu (*quality*)
		• `expires` - vypršení platnosti v sekundách
		• `methods` – podporované SIP metody
		• `schemes` – URL na které může být: odeslán požadavek, přesměrována odpověď apod.
		• `mobility` – nabývá hodnot: `mobile` (mobilní telefon), `fixed` (pevná linka)
		`INVITE …`
		`m: "Pepa Novak" <sip:novak@firma.cz>;q=0.7; expires=3600,`
		`"Pepa" <mailto:pepa@firma.cz>;q=0.1`
		`REGISTER …`
		`Contact: <sip:pepa@firma.cz>`
		`;methods="INVITE,OPTIONS,MESSAGE,ACK"`
		`;language="en,cz";`
		`;schemes="http,sip,sips,tel"`
		`;mobility="mobile"`

Content-Disposition	RFC3261	Popisuje, jak má být tělo zprávy interpretováno UA: • "session" – tělo zprávy popisuje relaci, • "render" – tělo zprávy má být zobrazeno účastníku, • "icon" – tělo zprávy má být zobrazeno jako ikona reprezentující volajícího. `Content-Disposition: session`
Content-Encoding (e)	RFC3261	Indikuje, že tělo zprávy je kódováno. SIP server musí nejprve provést dekódování uvedeným algoritmem, a teprve pak obdrží zprávu ve tvaru specifikovaném hlavičkou `Content-Type`. `e: tar`
Content-Language	RFC3261	Indikuje jazyk `Content-Language: cz`
Content-Length (l)	RFC3261	Indikuje délku těla zprávy protokolu SIP `l: 173`
Content-Type (c)	RFC3261	Indikuje typ media (*media type*) posílaném v těle zprávy `c: text/html; charset=ISO-8859-2`
CSeq	RFC3261	Obsahuje pořadové číslo požadavku klienta (desítkově) a metodu. SIP server je povinen tuto hlavičku vždy zkopírovat do odpovědi. `CSeq: 4711 INVITE`
Date	RFC3261	Obsahuje datum a čas (GMT)

		`Date: Sat, 13 Nov 2010 23:29:00 GMT`

Error-Info	RFC3261	Obsahuje odkaz na dodatečné informace ohledně chybového výsledkového kódu.
		
		`SIP/2.0 404 The number you have dialed is not in service`
		`Error-Info: <sip:not-in-service-recording@atlanta.com>`

Event (o)	RFC6665 RFC6446	Indikuje jakou událost nebo třídu událostí si přejeme být informováni (*subscribing*). `Event: foo; param=abcd; id=1234`
Expires	RFC3261	Specifikuje dobu, za které zpráva vyprší `Expires: 5`
Feature-Caps	RFC6809 RFC3840	Hlavička nese vlastnosti entity, které nelze vyjádřit v hlavičce Contact (vlastnosti mají stejný formát, jako vlastnosti v hlavičce Contact). Jedná se např. o entity Registrátor, proxy, B2BUA apod.
Flow-Timer	RFC5626	Doba (ve vteřinách) po kterou server čeká, než odešle *keep-alives*, aby zjistil, jestli komunikace není mrtvá. Jako *keep-alives* se často používá zdvojené CRLF (návrat vozíku, nový řádek).
From (f)	RFC3261	Indikuje iniciátora požadavku. Parametr `tag` obsahuje náhodný řetězec, který je užitečný pro spárování s odpovědi. SIP server je povinen tuto hlavičku vždy zkopírovat do odpovědi. `f: Anonymous <sip:c8oqz84zk7z@privacy.org>;tag=hyh8`
Geolocation	RFC6442	Vyjadřuje geografickou lokaci cíle. `Geolocation: <cid:target123@atlanta.example.com>`

Geolocation-Error	RFC6442	Chyba v geografické lokaci `Geolocation-Error: 100 ; code="Cannot Process Location"`
Geolocation-Routing	RFC6442	S hodnotou “yes” se specifikuje, že golokační údaje mohou být využity pro směrování. `Geolocation-Routing: no`
History-Info	RFC7044	Zachycuje historické informace vztahující se SIP požadavku `History-Info: <sip:bob@biloxi.example.com;p=x>;np=1;index=1.1`
Identity (y)	RFC4474	Elektronický podpis identity autora požadavku. `Identity:"ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2 a1pxAr3VgrB0SsSAaifsRdiOPoQZYOy2wrVghuhcsMbHW USFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGnFVcnyaZ++yR lBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="`
Identity-Info (n)	RFC4474	Obsahuje URI, ze kterého je možné stáhnout certifikát autora požadavku. `Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1`
Info-Package	RFC6086	Přenáší aplikační informace mezi koncovými body.
In-Reply-To	RFC3261	Vyjmenovává seznam identifikátorů volání (`Call-ID`) na které tento hovor odkazuje nebo které vrací. `In-Reply-To: 70710@saturn.bell.com, 17320@saturn.bell.com`
Join	RFC3911	Logicky spojí existující SIP dialog s novým SIP dialogem. `Join: 98732@sip.example.com;from-tag=r330r;to-tag=f7ff`

Max-Breadth	RFC5393	Specifikuje maximální počet dialogů, které může tento požadavek generovat (*fork*). `Max-Breadth: 60`
Max-Forwards	RFC3261	Musí být použit s každou metodou protokolu SIP. Omezuje maximální počet proxy nebo bran (*gateway*) přes které může být požadavek předán. Doporučená hodnota je 70. Zabraňuje toulání požadavku v síti. Max-Forwards: 6
Min-Expires	RFC3261	Minimální občerstvovací interval. Min-Expires: 60
MIME-Version	RFC3261	1.0
Min-SE	RFC4028	Indikuje minimální period (ve vteřinách) ve které musí být relace protokolu osvěžována pomocí požadavku nesoucí metodu INVITE nebo UPDATE.
Organization	RFC3261	Obsahuje jméno organizace, která požadavek (resp. odpověď) vygenerovala.
P-*		Řetězcem "P-" jsou uvozeny hlavičky, které navrhlo konsorcium 3GPPP. Tyto hlavičky jsou zpravidla vytvářeny proxy (resp. B2BUA) a nesou informace, které tyto entity zjistily o volajícím nebo o volání jako takovém. Tyto hlavičky pak tuto informaci přenáší mezi důvěřujícími si entitami, tj. entitami, které se vzájemně neautentizují (např. entity v core IMS konkrétního poskytovatele).

P-Access-Network-Info	RFC3455 TS 24.229	Tato hlavička je důležitá pro sítě, které připojují své zákazníky různými technologiemi na linkové nebo síťové vrstvě. Tato hlavička pak nese informace o použité technologii, která může být následně využita pro optimalizaci poskytovaných služeb. V mobilních sítích může též např. nést identifikátor buňky nebo lokalizační identifikátor, ze kterého lze následně odvodit reálnou lokaci.
P-Answer-State	RFC4964	Tato hlavička je rozšířením pro komunikaci Zmáčeni a mluv (*Push to talk Server over Cellular* (PTT)). Při komunikaci Zmáčkni a mluv se často používá režim, kdy příchozí stram se přijímá automaticky (*Unconfirmed*) bez potvrzení volaného (aniž by cokoliv mačkal). `P-Answer-State: Unconfirmed`
P-Asserted-Identity	RFC3325	Používá se mezi důvěřujícími si entitami (vzájemně se neautentizují), aby přenesly informaci o identitě, pod kterou se účastník, který tento požadavek odeslal, autentizoval. Autentizaci provedla např. entita A-SBC a výsledek této autentizace předává dalším entitám IMS v této hlavičce.
P-Asserted-Service	RFC6050	Umožňuje důvěryhodné entitě přidat do požadavku informaci o typu požadované služby. Tuto informaci může získat např. při autentizaci účastníka. Důvodem je skutečnost, že SIP URI neumožňuje specifikovat službu (např. *Push to talk over Cellular, Video on demand*, IPTV apod.) a požadavek tak směrovat na konkrétní aplikační server. `P-Asserted-Service: urn:urn-7:3gpp-service.telephony.ver1`
P-Associated-URI	RFC3455	Umožňuje registrátoru vrátit množinu URI, které jsou registrovány pro danou IP adresu (*address-of-record*).
P-Called-Party-ID	RFC3455	Identifikace volaného v případě, že volaný má registrováno vice URI a je třeba jasně identifikovat, kam má být hovor směrován. Identification of Called Party in the case that Called Party has more registered URI and it necessary clearly identify the URI at which the call is routed.

		`P-Called-Party-ID: sip:user1-business@example.com`
P-Charging-Function-Addresses	RFC3455	Obsahuje jeden nebo vice parametru, které obsahujíc IP adresu nebo jméno zpoplatňovacího *(charging)* serveru. Parametry: • ccf - off-line charging server • ecf - on-line charging server `P-Charging-Function-Addresses:ccf=192.1.1.1; ccf=192.1.1.2`

P-Charging-Vctor	RFC3455
	TS 24.229
		Obsahuje informace pro zpoplatnění (*charging*). Např. ICID (*IMS Charging IDentifier*) apod.
		`P-Charging-Vector: icid-value=1234bc9876e;`
		`icid-generated-at=192.0.6.8;orig-ioi=home1.net`

P-DCS-*		Hlavičky začínající tímto řetězcem slouží pro potřeby tzv. *Distributed Call Signaling (DCS).* Smysl DCS si lze snadno domyslet z popisu následujících hlaviček.

P-DCS-Trace-Party-ID	RFC5503	Obsahuje reálnou identitu volajícího v případě anonymního volajícího. Používá se v případě, že telekomunikační regulátor to vyžaduje po potřeby vymáhání práva např. pomocí *Originated Trace Service*.
		`P-DCS-Trace-Party-ID: <sip:+12345678912@domain.com;`
		`user=phone>;timestamp=3434688831.2327`

P-DCS-OSPS	RFC5503	Používá se výhradně pro komunikaci mezi důvěřujícími si SIP entitami (hlavičku vytváří důvěryhodná proxy, resp. B2BUA). Může být využito pro speciální typy volání. Jako je např. nouzové volání. OSPS je zkratka *Operator Services Position System*.
P-DCS-Billing-Info	RFC5503	Přenáší účtovací (*billing*) informace mezi důvěryhodnými entitami (pro potřeby DCS).

P-DCS-LAES	RFC5503	Obsahuje adresu a port tzv. *Electronic Surveillance Delivery Function* (“odposlech”) pro směrování duplikovaného streamu a událostí spojených s tímto streamem..
P-DCS-Redirect	RFC5503	Obsahuje identifikační údaje volání pro potřeby zákonného odposlechu přesměrovaného hovoru.
P-Early-Media	RFC5009	*Early-Media* označuje audio nebo video používané volajícím přes navázáním relace. Např. vyzváněcí tón, odpovědi na IVR (*Interactive Voice Response*) apod. Hlavička má např. význam pro sdělení, že je *Early-Media* podporováno, při komunikaci s externími sítěmi. `P-Early-Media: supported`
P-Media-Authorization	RFC3313	Hlavička obsahuje jeden nebo více *authorization token* pro autorizaci datového toku. *Authorization token* zpravidla vydává Policy server. Používá se pro autorizaci toků s nastaveným QoS.
P-Preferred-Identity	RFC3325	Hlavička je vkládána do SIP zprávy účastnickým agentem (UA), aby indikovala identitu účastníka, kterou by si přál, aby důvěryhodná proxy vložila do hlavičky P-Asserted-Identity.
P-Preferred-Service	RFC6050	Je vkládána do SIP zprávy UA, aby důvěryhodné proxy indikoval služby, které by si přál mít uvedeny v hlavičce P-Asserted-Service.
P-Profile-Key	RFC5002	Pro daný profil obsahuje klíč, který má být použit pro dotaz do účastnické database.
P-Refused-URI-List	RFC5318	Odmítne zpracování přicházejícího seznamu URI. Tento mechanismus je určen pro vytváření specifického typu komunikace v rámci komunikace Zmáčkni a mluv (*Push to talk over Cellular* - PoC), která se označuje jako ad-hoc skupinová relace.
P-Served-User	RFC5502	Předává identitu obsluhovaného účastníka na referenčním bodě ISC, tj. mezi S-CSCF a aplikační funkcí (AF).
P-User-Database	RFC4457	Obsahuje adresu HSS účastníka, který vygeneroval požadavek. Tato hlavička může být přidána do požadavku směrovaného z I-CSCF na S-CSCF.

P-Visited-Network-ID	RFC3455	Sděluje registrátorovi nebo proxy v domovské síti identifikaci navštívené (*visited*) sítě. `P-Visited-Network-ID: other.net, "Visited network 1"`
Path	RFC3327	Umožňuje zaznamenávat a předávat seznam mezilehlých proxy mezi UA a SIP Registračním serverem. Je podobný Record-Route. Rozdíl oproti Record-Route spočívá v tom, že ze používá v případě zpráv obsahujících metodu REGISTER odpovědí na ní (třída odpovědí s návratovým kódem 2xx). Record-Route se naopak nesmí ve správách s metodou REGISTER používat.
Permission-Missing	RFC5360	Obsahuje URI pro jehož předání není oprávnění `Permission-Missing sip:C@example.com`
Policy-Contact	RFC6794	Obsahuje URI Policy serveru, který má být kontaktován UAC. Volitelně parametr `non-cacheable`. Specifikující, že URI Policy server nemá UAC nadále udržovat (“kešovat”).
Policy-ID	RFC6794	Obsahuje URI Policy serveru a volitelné parametry.
Priority		Indikuje urgentnost požadavku. Hlavička může nabývat hodnot: "non-urgent", "normal", "urgent", "emergency" a případně dalších definovaných hodnot. `Priority: emergency`
Priv-Answer-Mode	RFC5373	Obdobné jako Answer-Mode s tím, že je požadován administrátorský přístup, který může vyžadovat dodatečnou autetnizaci.
Privacy	RFC3323	Požaduje, aby zpracování požadavku a odpovědi proběhlo v Privacy režimu. Tj. aby např. B2BUA entita zpracovávající požadavek nepředávala informace, ze kterých by bylo možno zjistit identitu volajícího. Tj. aby nepředávala např. hlavičky From, Contact, Reply-To, Via, Call-Info, User-Agent, Organization, Server, Subject, Call-ID, In-Reply-To a Warning.
Proxy-Authenticate	RFC3261	Obsahuje autetnizační výzvu (challenge). Obdoba hlavičky WWW-authenticate pro autentizaci vůči proxy.

Proxy-Authorization	RFC3261	Autetnizační hlavička pro autentizaci vůči proxy. Je obdobou hlavičky Authorization.
Proxy-Require	RFC3261	Obsahuje rozšíření protokolu SIP podporované Proxy (viz Require).
RAck	RFC3262	Používá se v požadavcích nesoucích metodu PRACK. Obsahuje: • Hodnotu z hlavičky RSeq (ze zprávy na kterou je odpovídáno) • Hodnotu z hlavičky CSeq • Metodu
Reason	RFC3326	Důvod proč je inicializována relace (důvod volání). `Reason: SIP ;cause=200 ;text="Call completed elsewhere"`
Record-Route	RFC3261	Identita proxy - vkládáno proxy, aby si vynutila, že i následující požadavky tohoto dialogu budou směrovány skrze tuto proxy. `Record-Route: <sip:biloxi.com;lr>,<sip:big.atlanta.com;lr>`
Recv-Info	RFC6086	Indikuje, které balíky (*Packages*) si přeje odebírat pomocí požadavků se zprávou INFO.
Refer-Sub	RFC4488	Když má hodnotu „false“, tak specifikuje, že příjemce SIP zprávy s metodou REFER nemá provést implicitní upsání se (obdobně, jak to dělá metoda SUBSCRIBE). `Refer-Sub: false`
Refer-To (r)	RFC3515	Obsahuje kontakt na třetí stranu. Používá se v případě REFER. `Refer-To: <sip:c@example.com;method=INVITE>`
Referred-By (b)	RFC3892	Obsahuje identitu (tj. SIP URI) původce SIP požadavku. `Referred-By: sip:r@ref.example;cid="2UWQFN303@ref.example"`
Reject-Contact (j)	RFC3841	Obsahuje řetězec vlastností (viz hlavička Contact), které se porovnávají s příchozím požadavkem. V případě, že je podmínka splněna, pak je požadavek odmítnut. `Reject-Contact: *;actor="msg-taker";video`
Replaces	RFC3891	Používá se k logickému nahrazení jednoho dialogu druhým.

		`Replaces: 4228@phone.exa.org;to-tag=743;from-tag=672;early-only`
Reply-To	RFC3261	Obsahuje logickou hodnotu, na kterou se má odpovědět. Hodnota může být různá od hodnoty v hlavičce From. `Reply-To: Bob <sip:bob@biloxi.com>`
Request-Disposition (d)	RFC3841	Specifikuje preference volajícího, jak by měl server zpracovat požadavek. `Request-Disposition: proxy, recurse, parallel`
Require	RFC3261	Pomocí této hlavičky UAC sděluje UAS, která rozšíření SIP by měl podporovat, aby mohl požadavek přijmout. Hodnoty lze nalézt na http://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml#sip-parameters-4. Např. "100rel" vyžaduje, aby požadavky byly potvrzovány "spolehlivě" (tj. metodou PRACK). `Require: 100rel`
Resource-Priority	RFC4412	Vyjadřuje prioritu přístupu k síti (např. v případě zahlcení sítě při mimořádné události). Hlavička označuje SIP požadavek stupněm priority („důležitosti"). Stupeň důležitosti obsahuje název stupnice důležitosti a vlastní prioritu v rámci této stupnice oddělenou tečkou. Hlavička může obsahovat i více hodnot. Stupnice důležitosti jsou např. „dsn" (*The Defense Switched Networ*k), „wps" (*Wireless Priority Service*) apod. `Resource-Priority: dsn.flash, wps.3`
Retry-After	RFC3261	Může být použit s výsledkovými kódy 500 (Server Internal Error) nebo 503 (Service Unavailable) k odhadu časového intervalu po který bude služba nedostupná. Obdobně může být použit I ve spojení 404 (Not

		Found), 413 (Request Entity Too Large), 480 (Temporarily Unavailable), 486 (Busy Here), 600 (Busy) nebo s 603 (Decline). Volitelný parametr `duration` indikuje, jak dlouho poté bude služba dostupná. `Retry-After: 18000;duration=3600`

Route	RFC3261	Používá se k vynucení cesty požadavku skrze uvedené proxy.
		
		`Route: <sip:bigbox3.site3.atlanta.com;lr>,`
		`<sip:server10.biloxi.com;lr>`

RSeq	RFC3262	Používá se v mechanismu "spolehlivého" potvrzování dočasných odpovědí (metoda PRACK). Obsahuje číselnou hodnotu.

Security-Client	RFC3329	Obsahuje seznam klientem podporovaných bezpečnostních mechanismů.
		
		`Security-Client: tls`
		`Security-Client: digest`

Security-Server	RFC3329	Obsahuje seznam serverem podporovaných bezpečnostních mechanismů. `Security-Server: tls;q=0.2`
Security-Verify	RFC3329	Obsahuje serverem verifikovaný seznam bezpečnostních mechanismů `Security-Verify: tls;q=0.2`
Server	RFC3261	Obsahuje informace o software server zpracovávajícím požadavek. `Server: HomeServer v2`
Service-Route	RFC3608	Obsahuje "přednastavenou" cestu, kterou si UA přeje použít.

		`Service-Route: <sip:P2.HOME.EXAMPLE.COM;lr>,` `<sip:HSP.HOME.EXAMPLE.COM;lr>`
Session-Expires (x)	RFC4028	Vyjadřuje časový limit relace.
SIP-ETag	RFC3903	Pro každý úspěšný požadavek metody PUBLISH entita Event State Compositor (ESC) generuje identifikátor události (entity-tag), který vrací v odpovědi s výsledkovým kódem 2xx, v hlavičce SIP-ETag. `SIP-ETag: dx200xyz`
SIP-If-Match	RFC3903	Identifikuje konkrétní událost pro požadavek, který je občerstvením, změnou nebo zrušením událostí. Tato hlavička musí obsahovat identifikátor události (entity-tag), který odpověděl Event State Compositor (ESC) v hlavičce SIP-ETag.. `SIP-If-Match: dx200xyz`
Subject (s)	RFC3261	Indikuje povahu hovoru. Je užitečný I pro filtraci hovorů. `s: Tech Support`
Subscription-State	RFC6665	Indicate the status of the subscription.
Supported (k)	RFC3261	Vyjmenovává rozšíření protokolu SIP podporované UA. Použité hodnoty jsou shodné s hodnotami hlavičky Require. `Supported: 100rel`
Suppress-If-Match	RFC5839	Obsahuje identifikátor události (entity-tag). Jestliže je podmínka splněna, pak bude potlačeno buď tělo nebo celá následující notifikace. Suppress-If-Match: b4cf7
Target-Dialog	RFC4538	Sděluje příjemci že odessilatel ví o uvedeném existujícím dialogu. Příjemce pak může povolit přístup k tomuto dialogu.

		`Target-Dialog: fa77as7dad8-sd98ajzz@host.example.com;local-tag=kkaz-;remote-tag=6544`
Timestamp	RFC3261	Specifikuje kdy UAC odeslal požadavek UAS. `Timestamp: 54`
To (t)	RFC3261	Specifikuje logického adresáta požadavku. t: sip:+12125551212@server.phone2net.com
Trigger-Consent	RFC5360	Specifikuje cílové URI (může jich být vice) na které má relay směrovat (množit) požadavky. `Trigger-Consent: sip:123@relay.example.comtarget-uri= "sip:friends@relay.example.com"`
Unsupported		Obsahuje seznam nepodporovaných rozšíření protokolu SIP (viz Require).
User-Agent	RFC3261	Obsahuje informace o software UAC, který inicioval požadavek. `User-Agent: Softphone Beta1.5`
Via	RFC3261 RFC7118	Indukuje cestu vytvořenou požadavkem, která určuje cestu, kterou by měla jít odpověď. Může obsahovat parametry "maddr", "ttl", "received", "branch" apod. parametr "branch" obsahuje identifikátor transakce a je využíván proxy pro detekci smyček Hlavičky Via v odpovědi musí být s hodné s hlavičkami Via v požadavku a musí být uvedeny ve stejném pořadí. `Via: SIP/2.0/UDP 192.0.2.1:5060; received=192.0.2.207;branch=z9hG4bK77asjd`

Warning	RFC3261	Obsahuje dodatečné informace související s výsledkovým kódem odpovědi. `Warning: 301 isi.edu "Incompatible network address"`
WWW-Authenticate	RFC2617 RFC3261	Obsahuje autentizační výzvu (challenge). Viz hlavička Authorization. WWW-Authenticate: Digest realm="atlanta.com", domain="sip:boxesbybob.com", qop="auth", nonce="f84f1cec41e6cbe5aea9c8e88d359", opaque="", stale=FALSE, algorithm=MD5
	TS 24.229	TS 24.229 zavádí nové parametry pro autentizační metodu Digest: • `ik` – kryptografický materiál pro zajištění integrity (*integrity-key*) • `ck` – kryptografický materiál pro šifrování (*cipher-key*) Stávající parametry plní • `nonce=RAND+AUTN` (plus je oddělovač spojení řetězců, AUTN= SQN⊕AK‖AMF‖MAC-A • `algorithm=AKAv1-MD5` • `realm=` DNS jméno domovské sítě.

9.3 Lokalizace

Slovo „lokalizace“ se v protokolu SIP používá ve dvou různých významech:

1. Vy smyslu vyhledání kontaktních údajů účastníka, se kterým chceme např. navázat relaci („zavolat mu“). Lokalizační údaje o účastníky se vedou v tzv. Lokalizační databázi. Lokalizační databáze je databáze záznamů o adresách účastníků. Každý záznam o adrese (*address-of-record* - AOR) je ukazatel z URI účastníka na URI (IP adresu), kde je účastník dostupný. Nad lokalizační databází pak běží lokalizační služba (*Location Service*), která poskytuje vazby mezi záznamy o adrese (*address-of-record*) a kontaktními adresami.

   Lokalizační databáze může být plněna administrativně, SIP požadavkem s metodou REGISTER apod.

2. Druhým významem slova „lokalizace“ je míněna geografická lokalizace, tj. kde se fyzicky klient nachází. V tomto případě budu používat přívlastek „geografická“ nebo zakrácené geolokace. Geolokace je důležitá např. při zasílání nouzových nebo obchodních zpráv do určité lokality. Nebo v případě nouzových volání, kdy je důležitá geografická lokalizace účastníka, žádajícího o pomoc.

9.4 Události

Událost (*event*) je v protokolu SIP abstraktní pojem. Obecně se událostí míní nějaká stavová informace o konkrétní entitě udržovaná na serveru. Např. stav připojení (např. Online), dostupnost, ochota komunikovat atd.

Z hlediska protokolu SIP pak máme dvě komunikující entity:

- Pozorovatel (*watcher*), klient kterého zajímá stav entity a přeje si být informován o změně stavu.
- Prezentátor (*presentity*), který poskytuje informace o stavu své entity. Anglické slovo *presentity* vzniklo ze spojení „presence“ a „entity“.

Co si pod pojmem událost představit konkrétně? Událostí máme několik typů. Nepoužívá se zde však termín „typ událostí“, ale „balík událostí“. Máme tak např. balík „konference“ specifikující multimediální konference nebo jednoduchý balík „presence“ specifikují prezentaci stavu dostupnosti účastníků sítě.

K zasílání změn stavu události se můžeme upsat metodou SUBSCRIBE. Změna události je nám pak notifikována metodou NOTIFY. Pokud může být událost (nebo její stav) měněna více účastníky současně, pak je událost udržována na serveru nazývaném *Event State Compositor* (ESC) a účastníci změnu stavu události publikují metodou PUBLISH.

Vytvoření události závisí na konkrétním balíku událostí. Často je možné událost vytvořit metodou SUBSCRIBE. Některé události mohou být spojeny s metodou REGISTER a jiné budeme třeba vytvářet přes webové rozhraní. To je aktuální např. v případě konferencí. Kdy musíme popsat konferenci a je často pohodlnější vyplnit webový formulář než XML dokument, který přeneseme v těle zprávy s metodou SUBSCRIBE.

Balíky událostí (Event packages) jsou registrovány na http://www.iana.org/assignments/sip-events/sip-events.xhtml

tab. 9.8 Balíky událostí

Jméno balíku událostí	Standard
call-completion	[RFC6910]
certificate	[RFC6072]
credential	[RFC6072]
conference	[RFC4575]
consent-pending-additions	[RFC5362]
dialog	[RFC4235]
http-monitor	[RFC5989]
kpml	[RFC4730]
load-control	[RFC7200]
message-summary	[RFC3842]

poc-settings	[RFC4354]
presence	[RFC3856]
reg	[RFC3680]
refer	[RFC3515]
session-spec-policy	[RFC6795]
spirits-INDPs	[RFC3910]
spirits-user-prof	[RFC3910]
ua-profile	[RFC6080]
vq-rtcpxr	[RFC6035]
winfo	[RFC3857]
xcap-diff	[RFC5875]

Jednotlivé balíky jsou specifikovány standardy, které zavádí často vlastní terminologii (každý balík je svět sám pro sebe).

9.5 SIP dialogy

Máme velké množství SIP dialogů. Vedle klasických učebnicových dialogů jsou zajímavé rovněž dialogy mezi entitami mobilních sítí (3GPP).

9.5.1 Registrace a odhlášení

Po zapnutí SIP zařízení je zpravidla prvním dialogem registrace zařízení. Cílem registrace je sdělit síti, na kterém URI (resp. IP adrese) se klient nachází (obr. 9.6). Přesněji řečeno: registrací se míní vytvoření tzv. záznamu o adrese (*address-of-record* - AOR) v Lokalizační databázi.

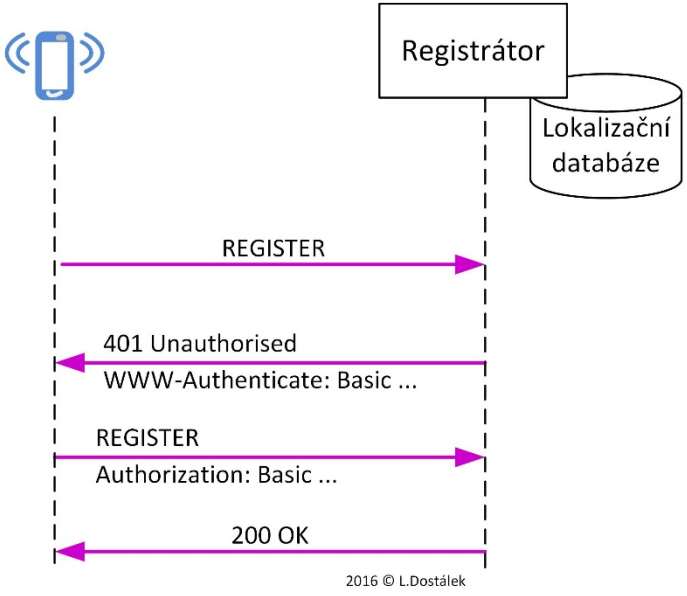
Výsledkem registrace je propojení SIP URI účastníka s počítačem (IP adresou), kde je účastník přihlášen. Registrační server následně zapíše toto propojení do lokalizační databáze. Lokalizační databáze následně poskytuje informace, které slouží proxy k nalezení volaných.

Do lokalizační databáze se zapíše URI uvedené v hlavičce „Contact“ požadavku. Např.:

```
REGISTER …
Contact: sip:pepa@firma.cz;expires=300
```

Vytvoří v lokalizační databázi záznam pro `sip:pepa@firma.cz` na dobu pěti minut.

Registrace je důležitá pro to, aby klient mohl přijímat příchozí hovory. I bez registrace může účastník kontaktovat odchozí proxy. Např. v mobilních sítích neregistrovaný účastník může volat tísňová volání (nemusí být implementováno).



obr. 9.6 SIP REGISTER

Jak je čárkovaně zobrazeno na obrázku obr. 9.12 při SIP registraci síť může vyžadovat autentizaci účastníka. Autentizační mechanismy jsou přejaty z protokolu HTTP. Blíže viz kapitola 9.5.2.

Pří registraci klient odesílá na registrační server požadavek nesoucí metodu REGISTER. Údaje, které účastník chce uvést do Lokalizační databáze, se zpravidla přenáší v hlavičce `Contact`. Požadavek s metodou REGISTER následně klient opakuje v pravidelných intervalech, dokud je přihlášený. Registrace se používá pro směrování SIP požadavku, nesouvisí ale s autorizací odchozích požadavků.

Všimněte si, že na obr. 9.6 vůbec není přenos média (RTP/RTCP). Médium se opravdu na registraci nikterak nepodílí.

Odhlášení (*deregistration*) znamená zneplatnění záznamu o adrese (*address-of-record* - AOR) v Lokalizační databázi. Odhlášení může nastat jak z iniciativy účastníka, tak i z iniciativy sítě. Odhlášení z iniciativy sítě je případ, kdy účastník své zařízení náhle vypne. Z hlediska sítě to znamená, že od účastníka přestanu chodit opakované požadavky s metodou REGISTER a po stanoveném časovém intervalu síť provede odhlášení.

Odhlášení z iniciativy účastníka se provede požadavkem s metodou REGISTER s hlavičkou „Expires: 0“. V lokalizační databázi se zneplatní URI uvedené v hlavičce „Contact:“ tohoto požadavku. Pokud by se uvedlo „Contact: * “, pak by se zneplatnily všechny URI daného účastníka.

9.5.2 Autentizace

Pro autentizaci slouží hlavičky

- WWW-Authenticate, která je výzvou pro autentizaci. SIP zpráva s touto hlavičkou je většinou spojena s výsledkovým kódem 401 Unauthorised.
- Authorization, která nese autorizační odpověď.

Protokol SIP umožňuje několik autentizačních metod, které jsou většinou převzaty z protokolu HTTP:

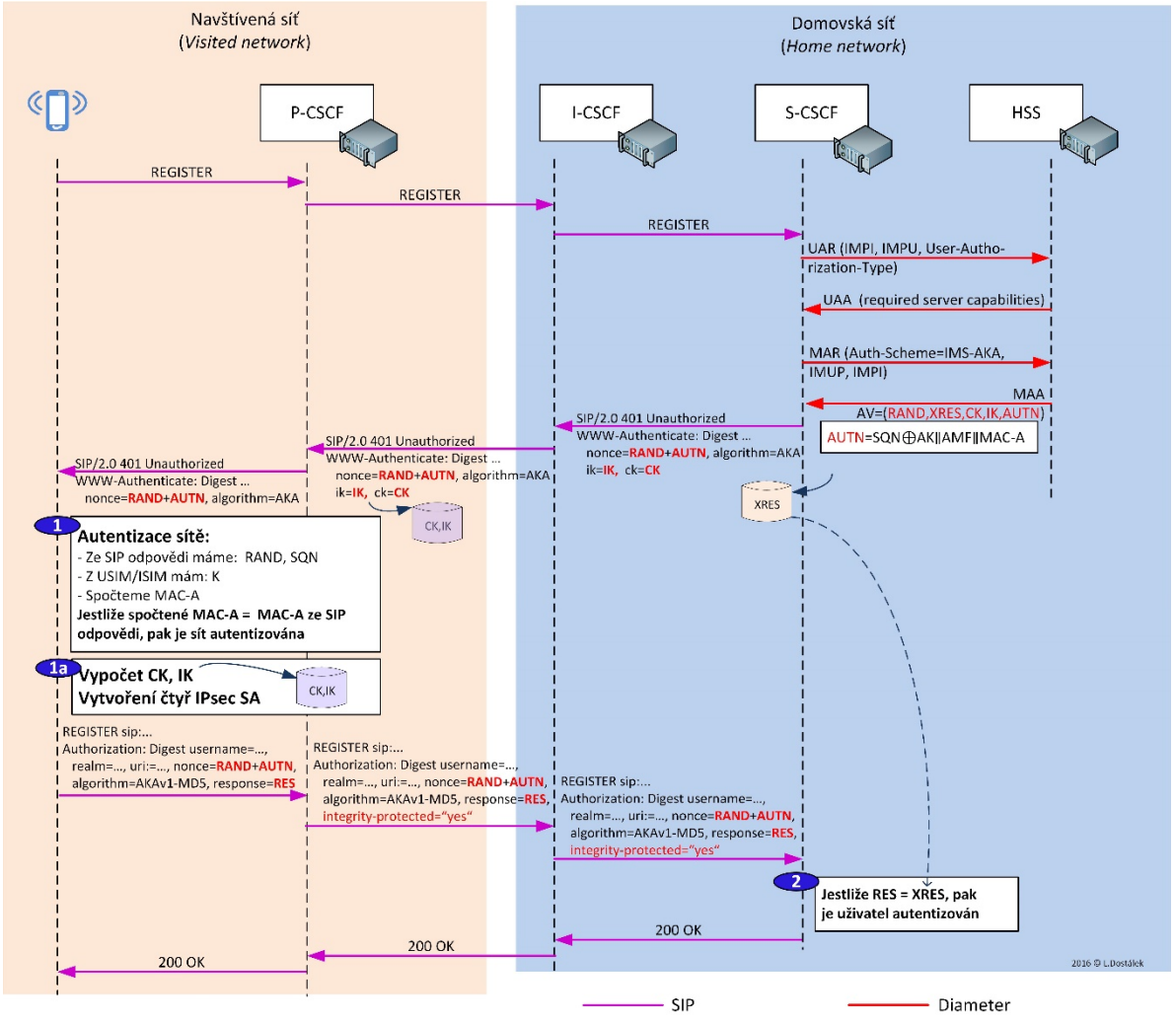
- Základní (Basic) autentizace např. pomocí účastnického jména a hesla přepravovaného jako součást URI.
- Autentizaci protokolem Kerberos, která je zajímavá zejména pro intranety, kde se používají domény Windows. Lístek protokolu Kerberos je zabalen do obálky SPNEGO (RFC-4559) a ta pak do hlavičky Authorization autentizační metody „Negotiate“. Tato metoda rovněž umožňuje autentizaci NTLM používanou ve starších sítích Windows.
- Autentizaci Digest, která rovněž používá autentizaci heslem, ale heslo není přímo přenášeno sítí (je skryto v hash). Jedná se o autentizaci typu výzva (challenge) - odpověď (response). Dotaz je umístěn v hlavičce WWW-Authenticate a odpověď v hlavičce.Authorization.
  3GPP Digest využívá hlaviček WWW-Authenticate a Authorization pro metodu Digest. Avšak tím podobnost si autentizaci Digest končí. V uvedených hlavičkách je autentizace AKA.

Zajímavé je, že metoda 3GPP Digest je originálně navržená pro SIP protokol, ale je použitelná i pro protokol HTTP. Např. pro webovou komunikaci (HTTP) z mobilního zařízení na portál operátora byl zaveden referenční bod Ut s autentizací 3GPP Digest.

9.5.3 3GPP registrace s autentizací digest

Tato registrace vychází opět z metody výzva (*challenge*) - odpověď (*response*). Na obr. 9.7 je zjednodušeně znázorněn celý proces (nejsou tam zobrazeny všechny entity, přes které běží komunikace, ale jen ty, které jsou důležité pro pochopení procesu).

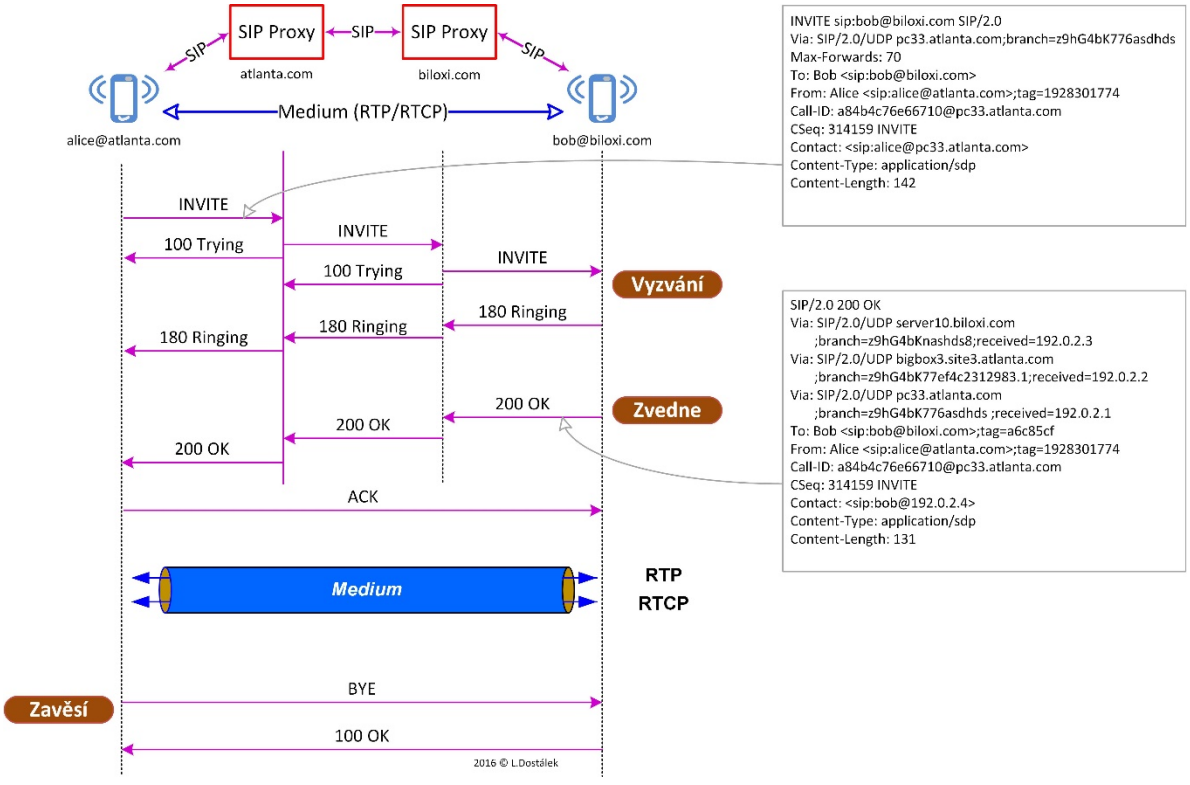
Obecně se účastník registrující se do sítě nachází v cizí navštívené síti (*visited network*). Požadavek na registraci proto posílá na P-CSCF (součást A-SBC) navštívené sítě. Tato síť nemá k dispozici kryptografický materiál pro jeho autentizaci, proto požadavek předá do domovské sítě účastníka. V domovské síti požadavek doputuje na entitu S-CSCF, která je zodpovědná za vyřízení požadavku. Tato entita požádá protokolem Diameter o příslušný kryptografický materiál entitu HSS (jedině HSS sdílí tajemství K s USIM/ISIM účastníka). HSS vygeneruje autentizační vektor AV a předá jej S-CSCF, která si z autentizačního vektoru vyzobne XRES (jednorázové heslo pro autentizaci účastníka) a zbytek předá do odpovědi.



obr. 9.7 SIP 3GPP registrace

9.5.4 INVITE

Metodou INVITE „voláme účastníkovi na jeho SIP URI (resp. TEL URI)“. Pokud známe jen jeho telefonní číslo (TEL URI), pak pomocí DNS ENUM (kap. 9.8.2) musíme nejprve přeložit telefonní číslo na jeho SIP URI. Pokud již máme SIP URI, tak pomoci DNS NAPTR zjistíme SIP server (proxy) volaného a SIP zprávu INVITE zašleme na takto zjištěný server. Server vezme ze SIP URI část před @ a vyžádá si protokolem Diameter (resp. Radius) lokalizační informace o volaném (jeho IP



obr. 9.8 SIP Lichoběžník (převzato z [61])

adresu). Na tuto IP adresu následně předá INVITE.

Typickým příkladem (převzatým z RFC-3261) je sestavení hovoru mezi dvěma účastníky (Alicí a Bobem). V tomto případě Alice používá SIP aplikaci na zařízení "smartphone". Komunikace běží skrze dvě mezilehlé proxy. Tato komunikace se často označuje jako SIP lichoběžník (obr. 9.8).

První řádek prvního požadavku obsahuje metodu INVITE následovanou dalšími řádky záhlaví (hlavičkami):

- `Via` obsahuje IP adresu Alice (pc33.atlanta.com) na které Alice očekává odpověď na tento požadavek. Parametr obsahuje `branch` identifikátor transakce.
- `To` obsahuje zobrazované jméno (Bob) a SIP URI (sip:bob@biloxi.com) volaného (tj. toho komu je tento požadavek určen).
- `From` obsahuje zobrazované jméno (Alice) a SIP URI (sip:alice@at-

lanta.com) volajícího (tj. toho, kdo inicioval tento požadavek). Parametr tak obsahuje náhodný řetězec (1928301774), který se používá pro identifikaci požadavku.

- `Call-ID` obsahuje globálně jednoznačný identifikátor volání, který se vytvoří z náhodného řetězce jména počítač nebo jeho IP adresy. Kombinace: `To`, `From` a `Call-ID` jednoznačně určuje dialog mezi Alicí a Bobem.

- `CSeq` (*Command Sequence*) obsahuje pořadí (celé číslo) a metodu. CSeq je s novým požadavkem (v rámci dialogu) zvyšováno po jedné.

- `Contact` obsahuje SIP URI pro přímý kontakt účastníka. Rozdíl mezi `Via` a `Contakt` spočívá v tom, že `Via` specifikuje entitu, které se má odpovědět na tetno požadavek, tak `Contact` specifikuje entitu pro další komunikaci.

- `Max-Forwards` specifikuje maximální počet mezilehlých entit (“hopů”) přes které může být požadavek předáván. Mezilehlé entity snižují hodnotu tohoto parametru.

- `Content-Type` specifikuje typ obsahu těla zprávy.

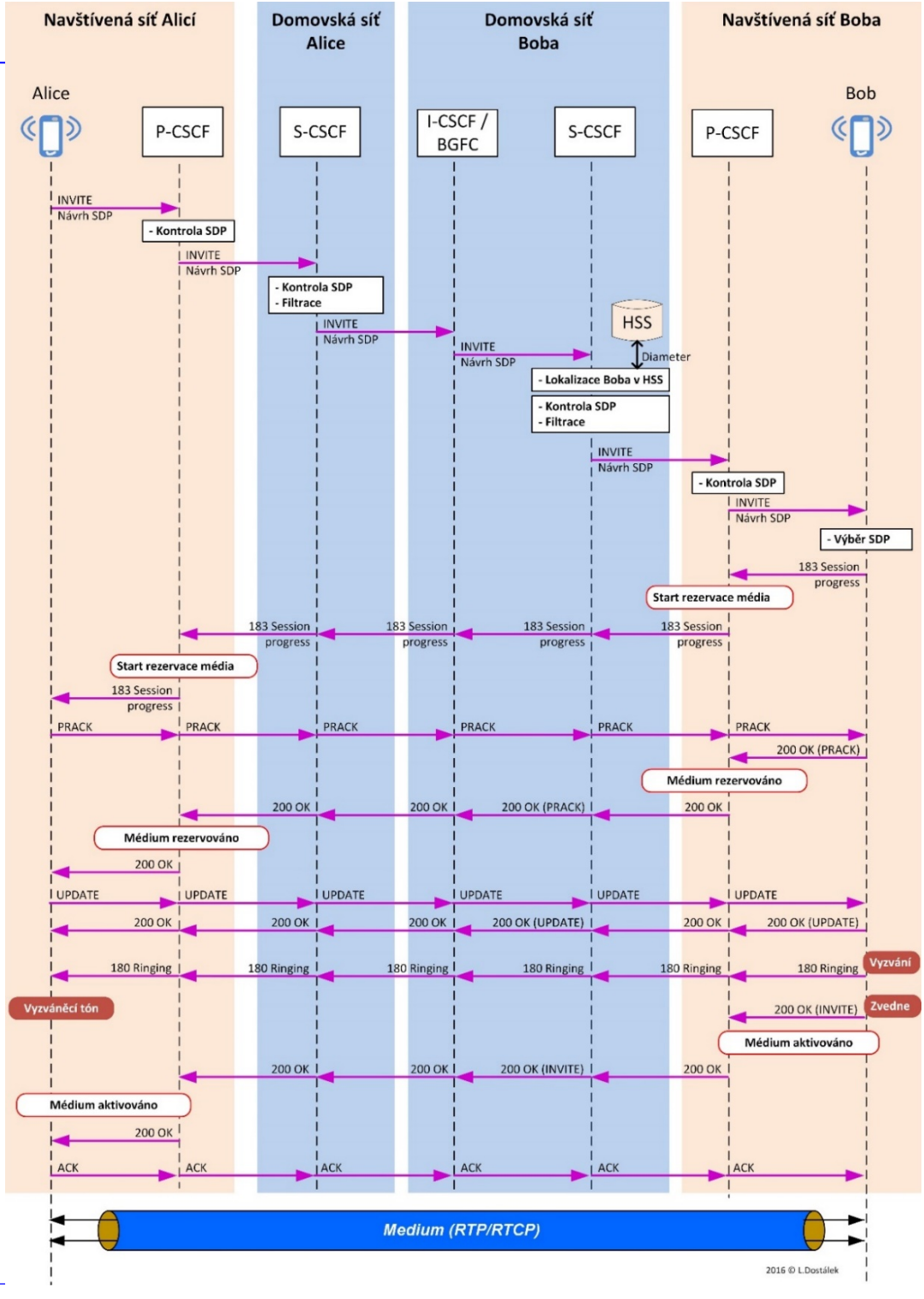
- `Content-Length` obsahuje délku těla zprávy.

Jelikož telefon Alice nezná IP adresu Boba, tak odesílá INVITE odchozí proxy atlanta.com. Adresa odchozí proxy bývá zpravidla získávána pomocí DHCP protokolu.

atlanta.com je SIP proxy server. Proxy server přijme požadavek a jménem žadatele jej předá dále. V našem případě proxy server nejenom přijme požadavek INVITE, ale také odešle odpověď 100 (Trying) zpět. Odpověď 100 (Trying) indikuje, že požadavek INVITE byl přijat a proxy jej předává dále. Tato odpověď má stejný obsah hlaviček To, From, Call-ID, CSeq včetně parametru branch v hlavičce Via jako přijatý požadavek INVITE.

Proxy atlanta.com nalezne pomocí DNS proxy biloxi.com (blíže viz kapitola 9.8), která obsluhuje doménu biloxi.com. Výsledkem je získání IP adresy proxy serveru biloxi.com, na který je dále předán požadavek INVITE. Před předáním požadavku vloží proxy do SIP zprávy další hlavičku `Via` se svou identifikací. Proxy biloxi.com přijme zprávu INVITE a zpět odpoví 100 (Trying) čímž sdělí, že zpráva byla přijata a bude předána dále. Proxy se následně dotáže Lokalizační database, aby získala IP adresu Boba. Nakonec přidá do zprávy další hlavičku `Via` se svou identifikací a předá požadavek INVITE Bobovu počítači.

Bobův počítač přijme zprávu INVITE a začne vyzvánět. Zpět indikuje vyzvánění odpovědí 180 (*Ringing*), která je předávána přes mezilehlé proxy až k volajícímu. Každá mezilehlá proxy z hlavičky Via pozná kam má zprávu předat (vždy vymaže hlavičku Via se svou identifikací).



obr. 9.9 3GPP INVITE

Když telefon Alice přijme odpověď 180 (*Ringing*), tak spustí vyzváněcí tón a zobrazí tuto informaci na displeji telefonu. Když bob zvedne telefon, tak SIP telefon vygeneruje odpověď 200 (OK) signalizující zvednutí telefonu. Tato odpověď obsahuje v těle zprávy protokolem SDP specifikaci přenosového media pro uskutečňovanou relaci. Jedná se o SDP odpověď na SDP zprávu ve zprávě INVITE.

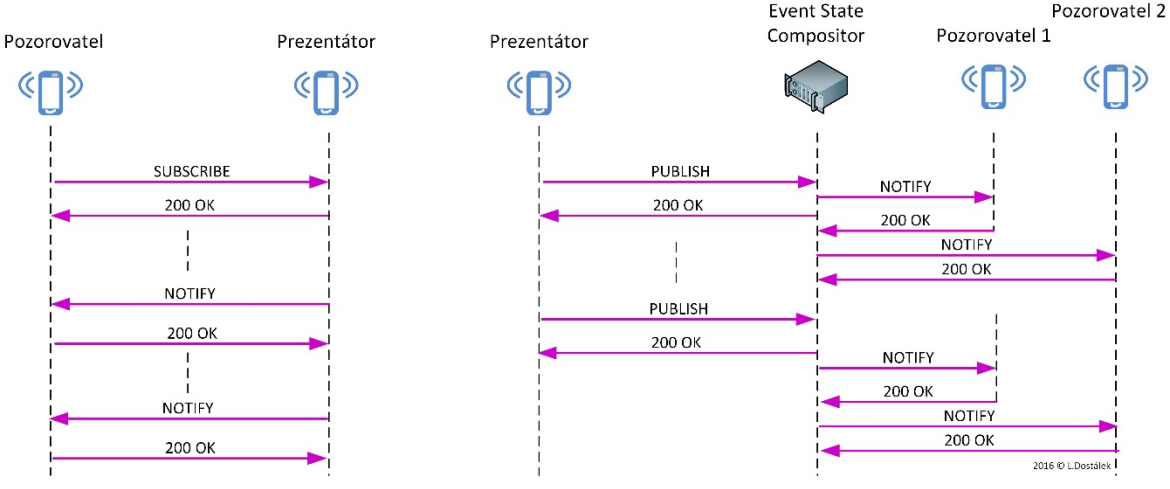
Nakonec Alice odešle zprávu s metodou ACK. Může ji odeslat již přímo (bez účasti mezilehlých proxy) za využití informací z hlaviček `Contact`. Nyní může dojít k sestavení kanálu pro přenos média (RTP/RTCP).

9.5.5 3GPP INVITE

Na obr. 9.9 je znázorněno zjednodušené schéma metody INVITE v 3GPP sítích. V mobilních sítích je to složitější o to, že je třeba v LTE síti aktivovat příslušný datový nosič (*bearer*), který bude garantovat kvalitu přenosu. Přitom dopředu nevíme, jestli síť volaného v daném okamžiku je schopna alokovat odpovídající datový nosič (*bearer*). Kdybychom totiž úspěšně navázali relaci protokolem SIP a datový nosič by nebylo možné alokovat, pak relace by byla „hluchá" – byl by to „fantomický hovor" a účastník by si nejspíše myslel, že se jedná o poruchu.

V okamžiku vyzvánění už síť musí mít potvrzeno, že medium je po celé cestě od volajícího k volanému alokováno. K potvrzení startu rezervace média se používá metoda PRACK a potvrzení, že médium je alokováno, se provede metodou UPDATE, která může ještě modifikovat parametry relace.

Důležité je si uvědomit, že P-CSCF (součást A-SBC) musí zpracovávat procházející SIP zprávy a



obr. 9.10 Upsání se metodami SUBSCRIBE a PUBLISH

na referenčním bodu Rx (protokol Diameter) nejprve rezervovat příslušné přenosové médium a posléze jej aktivovat (na obrázku to není znázorněno).

9.5.6 Upsání se

Upisujeme se čertu či členství v konferenci. Zpravidla se upisujeme k odebírání informací o změně stavu nějaké entity (např. účastník se připojil do sítě). Účastníci se zde vyskytují ve dvou rolích:

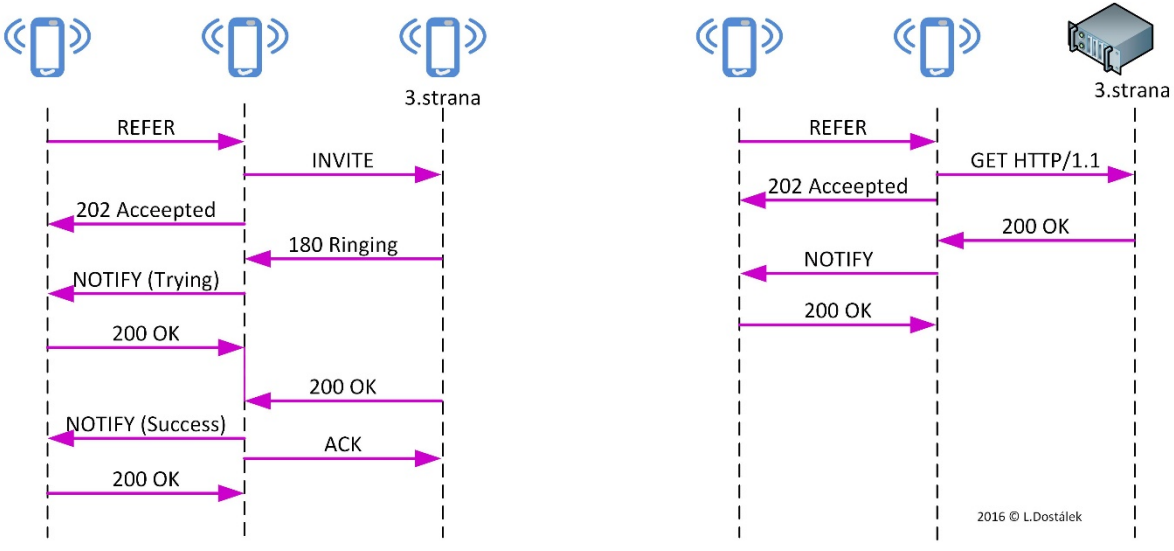
- Prezentátor, tj. ten, kdo chce zveřejňovat informace.
- Pozorovatel, tj. účastník, který chce být informován o změně stavu. Tyto informace jsou zasílány pozorovateli SIP zprávy s metodou NOTIFY.

Upisujeme se zpravidla metodou SUBSCRIBE (obr. 9.10 vlevo). K zasílání informacích o změně stavu události, které nám (upsaným) budou zasílány metodou NOTIFY. Upisovací požadavek by měl obsahovat hlavičku Expires, která specifikuje délku upsání. Tato doba může být prodloužena nebo zkrácena zopakováním požadavku s metodou SUBSCRIBE.

V případě, že událost může aktualizovat více účastníků, pak se událost zpravidla vede na *Event State Compositor* (ESC) a účastníci pak změnu stavu události publikují metodou PUBLISH (obr. 9.10 vpravo).

9.5.7 REFER

SIP požadavkem s metodou REFER sdělujeme jinému UA, aby kontaktoval třetí stranu dle instrukcí uvedených v požadavku. Např. aby navázal relaci na v SIP požadavku referované URI (obr. 9.11 vlevo), aby se přihlásil do konference, aby si zobrazil zajímavou webovou stránku (obr. 9.11 vpravo) atd.

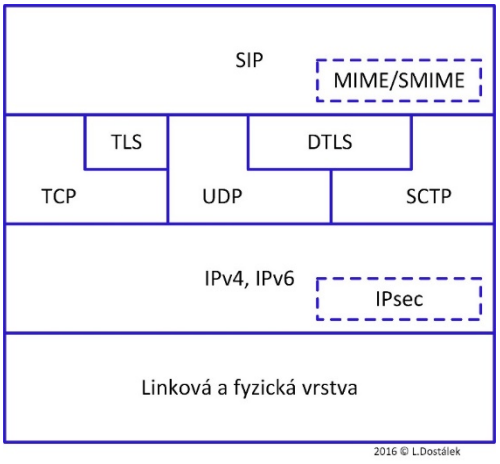


obr. 9.11 Metoda REFER

9.6 Protokoly nižších vrstev

Protokol SIP může využívat několik protokolů nižších vrstev (obr. 9.12). Klasické použití je využití protokolu TCP nebo UDP na portech 5060 (nešifrováno) a 5061 (přes TLS).
Avšak pro vzájemnou komunikaci mezi SIP proxy a SIP B2BUA se stále častěji používá protokol SCTP (blíže viz kap. 17).

Dříve se deklarovalo, že nepotvrzované protokoly jako UDP nebo SCTP v nepotvrzovaném módu nelze zabezpečit pomocí TLS. S nasazováním DTLS (blíže viz kap. 16) však i tato omezení pominula. V případě, že nelze použít TLS ani DTLS, pak pro zabezpečení máme vždy ještě k dispozici IPsec.



obr. 9.12 SIP a protokoly nižších vrstev

9.7 SIP Zabezpečení

Protokol SIP může být zabezpečen několika způsoby:

- IPsec zabezpečuje komunikaci na IP vrstvě. Např. certifikát veřejného klíče koncového bodu IPsec tunelu obsahuje zpravidla jméno ne IP adresu síťového rozhraní (obdobně jako certifikát webového server běžícím na témže počítači). Nebezpeční spočívá v tom, že např. soukromý klíč a certifikát pro webový server běžící na témže počítači může být zneužit pro IPsec tunel protokolu SIP a obráceně. Řešením je používat specializované servery pro každý účel zvlášť. Např. SBC je takovým specializovaným počítačem.

- S/MIME zabezpečuje jen tělo zprávy (nikoliv hlavičky, které nesou "lokalizační údaje") mezi koncovými body. Využití tohoto zabezpečení v sítích na bázi protokolu SIP je velice omezené.

- TLS/DTLS se jeví jako nejvýhodnější zabezpečení, protože zabezpečuje celou zprávu na aplikační vrstvě. Z důvodů uvedených u IPsec není příliš vhodné kombinovat na témže rozhraní komunikaci TLS/DTLS a IPsec.

Často kladenou otázkou je, proč je třeba zabezpečovat tělo SIP zprávy. Důvodem je fakt, že často v SIP zprávě přenášíme kryptografický materiál pro zabezpečení media (protokoly RTP/RTCP). Médium (RTP/RTCP) může pak být zabezpečeno protokolem SRTP (kap. 14.3).

9.7.1 3GPP sítě

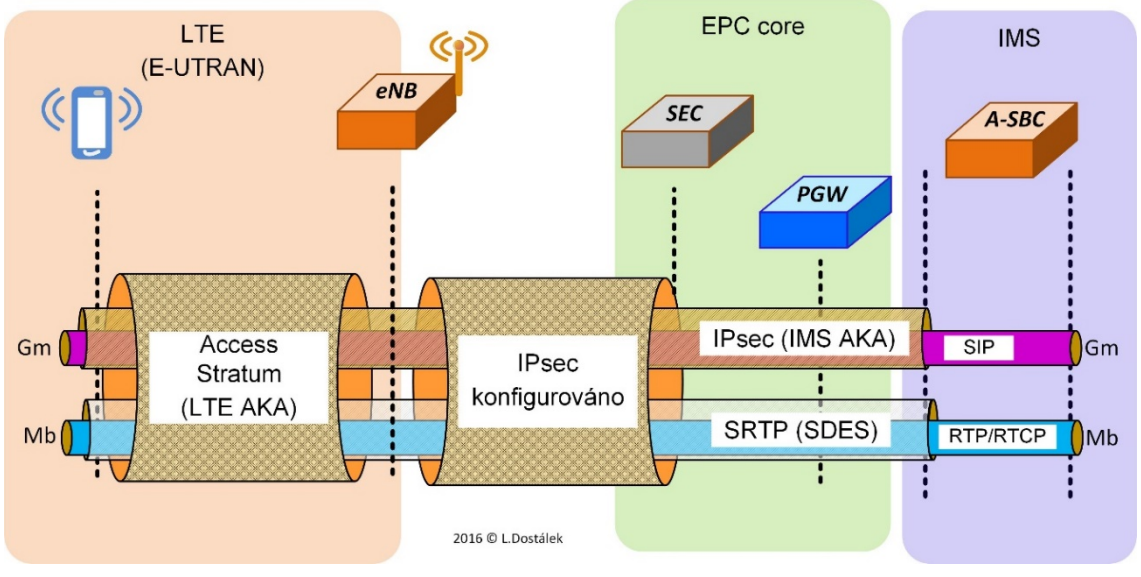
Architekturu zabezpečení v 3GPP sítích specifikuje 3GPP TS 33.203 [8]. V 3GPP sítích se používá

zabezpečení protokolu SIP pomocí IPsec (je přípustné i zabezpečení na aplikační vrstvě pomocí TLS/DTLS nebo i jiných mechanismů). IPsec se používá jak zabezpečení mezi účastníkem a A-SBC (referenční bod Gm), tak i k zabezpečení mezi I-SBC a poskytovateli sítě IPX (referenční body Ici a Izi se zabezpečí IPsec a vznikne referenční bod Zb), avšak to je jiná kapitola.

Na obr. 9.13 je schématický vyjádřeno zabezpečení celé cesty mezi účastníkem a A-SBC. Vidíme, že A-SBC plní dvě role: portál IPsec tunelu a B2UA agent. Zabezpečení je provedeno ve dvou vrstvách:

1. Protokol SIP (referenční bod Gm) je zabezpečen pomocí IPsec na celé cestě od účastníka až do A-SBC. Médium (referenční bod Mb) je zabezpečeno zpravidla metodou SDES protokolu SRTP rovněž po celou cestu mezi účastníkem a A-SBC (viz kap. 9.1). Jedná se tedy o zabezpečení na celé cestě mezi účastníkem a A-SBC.
   Pokud by v protokolu IPsec na referenčním bodu Gm nebylo aktivováno šifrování a kryptografický materiál pro SDES se přenášel v SDP paketu v těle protokolu SIP, pak aktivace SRTP postrádá smysl, neboť kryptografický materiál by se přenášel nezabezpečenou cestou.
2. Zabezpečení LTE komunikace mezi účastníkem a základnovou stanicí eNB (radiové rozhraní mobilní sítě). Využívá se zde rovněž mechanismus AKA, který sdílí tajemství K mezi USIM účastníka a HSS.

   Zabezpečení EPC, tj. zabezpečení komunikace mezi eNB a jádrem sítě EPC. Zde se zpravidla konfiguruje IPsec tunel



obr. 9.13 Zabezpečení cesty mezi účastníkem a A-SBC (SRTP někteří nevyužívají, což považuji za riziko)

9.8 DNS

Protokol SIP používá zejména dva typy URI:

- TEL URI, např. tel:+420-603-533-825, kde se ignorují tzv. vizuální separátory (pomlčka, lomítko a tečka) a výsledek se pomocí DNS ENUM převede na SIP URI
- SIP URI, např. sip:novak@firma.cz;transport=udp

Tyto URI musíme pomocí DNS přeložit až na IP adresy, transportní protokoly a jejich porty. K tomu nám v DNS slouží záznamy NAPTR. Jeho použití je na první pohled trochu komplikované, ale snadno se pochopí na příkladech.

9.8.1 Záznam NAPTR

Záznam NAPTR (*Name Authority Pointer*) je typ DNS záznamu (RR věty) – podobně jako A nebo CNAME. Má obecně formát:

```
Doména TTL  IN NAPTR pořadí preference příznak  služba výraz nahrazení
```

Kde:

`Doména` – obsahuje plně kvalifikované DNS jméno.

`TTL`, `IN` – má standardní význam.

`Pořadí` – určuje pořadí, v jakém musí být záznamy NAPTR (stejné domény) zpracovávány. Nižší čísla jsou zpracovávány před vyššími. Jakmile se zpracuje záznam s konkrétním pořadím, pak už se další záznamy neprohledávají.

`Preference` – určuje pořadí v jakém budou NAPTR záznamy zpracovávány pokud mají shodnou položku pořadí (obdoba MX záznamu).

`Příznak` – máme příznaky "S", "A", "U" a "P". Příznak sděluje co má být dalším krokem v DNS překladu:

- "S" míní SRV větu, tj. výsledkem překladu PTR záznamu je DNS jméno odkazující na SRV záznam.
- "A" míní A ,AAAA nebo A6 větu, Tj. výsledkem překladu NAPTR záznamu je DNS jméno odkazující na A ,AAAA nebo A6 záznam.
- "U" – výsledkem je absolutní URI.
- "P" – aplikačně specifický záznam.

`Služba` – nejčastěji specifikuje protokoly nižších vrstev. Položka může obsahovat prázdný řetězec.

Pro DNS ENUM jsou registrovány služby konstruované následujícím způsobem:

```
E2U+enumservice:typ-podtyp
```

Např.:

`E2U+email` – telefonní číslo má být transformováno na adresu elektronické pošty

`E2U+SIP` – telefonní číslo má být transformováno na SIP URI.

Pro protokol SIP jsou registrované následující služby:

tab. 9.9 NAPTR parametr Služba

Služba	Aplikační protokol	Zabezpečení	Transportní protokol	Standard
SIP+D2T	SIP		TCP	RFC3263
SIPS+D2T	SIP	TLS	TCP	RFC3263
SIP+D2U	SIP		UDP	RFC3263
SIP+D2S	SIP		SCTP	RFC3263
SIPS+D2S	SIP	TLS	SCTP	RFC4168
SIP+D2W	SIP		WS	RFC7118
SIPS+D2W	SIP	TLS	WS	RFC7118

Kde:

- WS = protokol WebSocket [RFC6455], který je transportní vrstvou nad TCP, volitelně může být zabezpečen TLS.
- Využití protokolu DTLS tč. nebylo registrováno.

`Výraz` – regulární výraz, který se použije na DNS dotaz.

`Nahradit` – čím se má výsledek nahradit.

9.8.2 DNS ENUM

DNS ENUM (*tElephone NUmber Mapping*) je systém pro překlad telefonních čísel na SIP URI. Byla zaregistrována doména e164.arpa. pro překlad telefonních čísel dle standardu E.164 na SIP URI.

Příklad: Telefonnímu číslu: +420 123 45 67 89 odpovídá následující plně kvalifikované DNS jméno:

```
9.8.7.6.5.4.3.2.1.0.2.4.e164.arpa.
```

V DNS pak může mít záznam:

```
$ORIGIN 9.8.7.6.5.4.3.2.1.0.2.4.e164.arpa.
       IN NAPTR 100 10 "u" "E2U+sip"  "!^.*$!sip:user@firma.cz!"  .
```

Příznak `"u"` znamená, že výsledkem bude absolutní URI. `"E2U+sip"` znamená, že absolutní URI bude protokolu SIP. Regulární výraz `"!^.*$!sip:user@firma.cz!"` se skládá ze dvou částí (oddělených !): první část `^.*` znamená vezmi celý vstup (celé telefonní číslo) a nahraď jej druhou částí: `sip:user@firma.cz.` Poslední tečka už jen říká, že je vše hotovo. Tj. volání na telefonní číslo +420 123 45 67 89 bylo transformováno na volání na SIP URI `sip:user@firma.cz.`

9.8.3 Překlad SIP URI

Nakonec se ještě musí `sip:user@firma.cz` přeložit na informace vedoucí k nalezení příslušného SIP serveru. V DNS máme např.:

```
$ORIGIN firma.cz.
 IN NAPTR 100 10 "S" "SIP+D2U"                                   ""
_sip._udp.firma.cz.
 IN NAPTR 102 10 "S" "SIP+D2T" "!^.*$!sip:helpdesk@firma.cz!"
_sip._tcp.firma.cz.
```

Nejprve se zpracovává záznam s pořadím 100. Ten říká, že SIP server volaného je dostupný transportním protokolem UDP a má SRV záznam `_sip._udp.firma.cz.` Pokud tento záznam selže, pak se přejde na další záznam a SIP URI `sip:user@firma.cz` se přepíše na `sip:helpdesk@firma.cz` a protokolem TCP se naváže spojení na server, který má v DNS záznam SRV: `_sip._tcp.firma.cz.`

9.9 Útoky proti SIP

Útok	Popis
Převzetí kontroly nad účastníkovým zařízením	Převzetí kontroly může být důsledkem: • Slabiny operačního systému (stará verze, neaplikované záplaty atp.) • Chybné zacházení se zařízením (implicitní heslo, neaktivovaná antivirová ochrana atp.) • Zlomyslný kód (virus, botnet atp.)
Muž uprostřed	Útočník zachytává SIP komunikaci, modifikuje ji a posílá dále. Tento způsob útoku je základem pro mnoho dále zmíněných útoků: maškaráda, uniregistrar útok, únos registrace, odposlech atd. Nabízí se i možnost odposlechu toku dat uprostřed HeNB, pokud není použit protokol SRTP.
Pozměnění zprávy	Obecný typ útoku muže uprostřed. Obecně je možné pozměnit: • Záhlaví SIP zprávy. To je užitečné pro útoky typu Únos registrace. • Tělo SIP zprávy. Útoky jsou v tomto případě zajímavé např. i na metody typu MESSAGE („pozměnění SMS“) nebo SUBSCRIBE.
Maškaráda	Muž uprostřed se podvrhne za jiného účastníka ze zachycené komunikace. Může pak např. přesměrovat komunikaci atp.

Unregister útok	Muž uprostřed podvrhne zprávu REGISTER s nulovou hodnotou v hlavičce Expire a tím ukončí relaci oběti.
Únos registrace	Klasickou metodou je modifikace zprávy s metodou REGISTER. V této zprávě útočník vymění v hlavičce Contact IP adresu za svou IP adresu. Registruje se tak na místo původního účastníka, kterého po zbytek registrace odstaví od komunikace např. DoS útokem.
Falešný únos registrace	Muž uprostřed sleduje příchozí hovory a snaží se je uzavřít.
Odposlech	Slovo „Odposlech“ má v souvislosti se SIP protokolem dva významy: • Odposlech paketů (*Sniffing*), jak je používán v datových sítích (např. programem Wireshark). Z datových paketů protokolu SIP je pak možné zjistit např. kryptografický materiál pro zabezpečení média (SRTP) či jiné zajímavé informace. Zajímavé informace je také možné získat díky přihlášení se do konference. • Nezákonný odposlech (*Eavesdropping*) multimediální relace. Programem Wireshark má na sledování multimediálních relací dnes celé menu. Zachycenou relaci je následně i možné uložit a přehrávat. V mobilních sítích, které nepožívají šifrování média (používají pouze IPsec AH) je nejjednodušší si upravit HeNB (*Femto Cell*) pro *sniffing* a následně fyzicky HeNB dopravit do blízkosti odposlouchávaného. V lokálních sítích musíme pro *sniffing* často použít navíc útok *„ARP poisoning”*. • Zákonný odposlech (*Lawful interception*) specifikovaný standardy TS 33.102 až TS 33.108.
*Podvržený server (*Impersonating a Server*)*	Jedná se o útok používaný vůči webovým serverům. Cílem útoku je z účastníka vylákat jeho heslo. Útočník podvrhne např. SIP Odchozí server za svůj upravený SIP Redirect server (nebo SIP proxy), který z požadavků vyzobává jména účastníků a jejich hesla. Požadavek následně předá dále na SIP Registrátora. Tento útok je jednodušší než obdobný útok proti webovým serverům, protože Registrátor (na rozdíl od webového serveru) není třeba vyřazovat dodatečným útokem z provozu. Např. správce firemního SIP Odchozího serveru může bez jakýchkoliv problémů získat hesla všech účastníků, aniž by si toho kdokoliv všimnul.

Útok je možný často i v případě zabezpečení pomocí TLS/DTLS. Důvodem je skutečnost, že mnohá účastnická zařízení jsou konfigurována tak, aby neověřovala, zdali certifikát UAS byl vydán důvěryhodnou certifikační autoritou. V takovém případě je použití TLS/DTLS spíše škodlivé, protože účastníka udržuje ve falešném přesvědčení, že jeho komunikace je bezpečná. Tento typ útoku není možný v případě, že je účastník autentizován pomocí USIM/ISIM.

Zboření relace (Tearing Down Sessions)

- Muž uprostřed odešle metodu BYE.
- DDoS útokem se znemožní pravidelné odesílání REGISTER a síť odhlásí účastníka, protože se domnívá, že vypnul zařízení bez odhlášení.

DDoS

V Internetu jsou útoky DDoS velice běžné. Poskytovatelé Internetu se proti těmto útokům brání pomocí DDoS praček. Nejznámějším dodavatel DDoS praček na svém webu http://www.arbornetworks.com zveřejňuje *Digital Attack Map,* kde jsou vizualizovány DDoS útoky na úrovni států.

Pro útočníky je v současné době nejjednodušší provádět DDoS útoky pomocí DNS protokolu, protože ten používá nepotvrzovaný protokol UDP. A právě protokol SIP může rovněž využívat UDP, což je spíše v jeho neprospěch. Protokoly DTLS a SCTP proto pro nepotvrzovanou komunikaci implementovaly protokol Photuris (kap. 15).

Při DDoS útoku je důležitá jeho potencionální amplifikace, tj. kolik paketů vygeneruje v průměru jeden paket útoku.

Např. útočník může na Registrátor poslat v jednom požadavku dlouhý seznam URI, které chce registrovat. Registrátor následně protokolem Diameter nebo Rádius vygeneruje pro každé URI jeden paket.

Útočník zašle na SIP Relay požadavek, který vygeneruje řadu požadavků.

DDoS a botnety

Na rozdíl od Internetu Botnet může v SIP síti způsobit jednoduše zahlcení. Může totiž vygenerovat tak silný provoz na síti, že síť nebude schopna rezervovat datová média. K tomu stačí, aby je generoval množství „prozvonění“, které podle obr. 9.9 provádí rezervaci média.

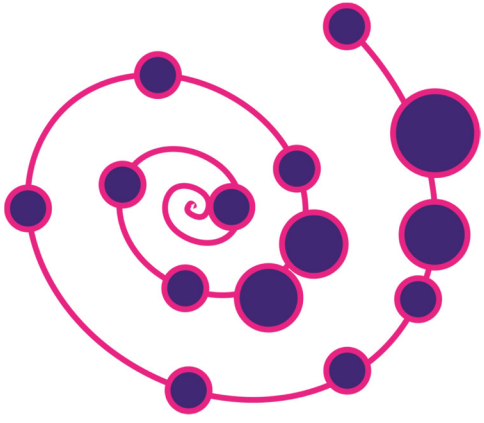
Obdobně, když botnet odešle z milionů zařízení SMS zprávu, tak rovněž může dojít až k výpadku sítě.

VoIP spam, Spam over IP telephone (SPIT)	Zasílání nechtěných zpráv.
Vishing	*Vishing* (*Voice phishing*) je vylákávání osobních informací pomocí hovoru.
Defraudace poplatku (Toll fraud)	Nekorektní využívání systému např. pro mezinárodní hovory účtované za lokální sazbu. Neúčtování volání na barevné linky apod.
Invite Replay Billing Attack	Neautorizované volání pomocí zopakování odchyceného požadavku s metodou INVITE. Tyto útoky byly v minulosti možné zejména díky chybám v software A-SBC provádějícím autentizaci.
Fake Busy Billing Attack	Útočník jakoby převezme hovor, ale udržuje jen relaci. Hovor je sice z pohledu účastníků ukončen, ale relace trvá a je účtována po celou dobu, co ji útočník udržuje.
Bye Delay Billing Attack	Útočník záměrně pozdržuje BYE zprávu, aby prodloužil účtovací dobu.
Bye Drop Billing Attack	Útočník prodlužuje účtovací dobu zahozením zprávy BYE
SIP Authentication Attack	Jedná se o útok hrubou silou na pobočkovou ústřednu, která má SIP konektor. Útočník se snaží slovníkovým útokem prolomit administrátorské heslo ústředny. Ovládne-li ústřednu, pak může útočit dále do SIP infrastruktury.
Leveraging Forking to Flood a Network	Malý počet oprávněných požadavků generuje masivní provoz mezi SIP entitami. Může to být způsobeno chybnou konfigurací nebo i chybou software. Pokud ovšem útočník má přístup k dostatečnému množství zdrojů, pak může generovat ohromný síťový provoz. Množení požadavků může být omezeno mechanismem (hlavičkami) `Max-Breadth`, avšak ani tento mechanismus není dokonalý. Ochranou je jedině detekce útoků a monitorování síťového provozu.
Obejití P-CSCF	Poté co se zlomyslný účastník úspěšně registruje do sítě, může se pokoušet obcházet P-CSCF a posílat SIP zprávy přímo S-CSC. Tj. může se vyhnout i IPsec tunelu mezi účastníkem a P-CSCF. Má to za následek, že: 1. Účastník se vyhne zpoplatnění.

2. Účastník se může podvrhnout jako jiný účastník (maškaráda) a jeho jménem posílat INVITE, BYE a pod.

Doporučuje se následující opatření:

- Přístup k S-CSCF omezit pouze na entity, které přístup potřebují.
- Zamezení možnosti předstírat P-CSCF jinou IP adresu účastníka (IP spoofing). Např. pouze na entity z IMS core.



10. SDP

SDP (*Session Description Protocol*) [63] předává požadované vlastnosti na médium v multimediální relaci. Např. transportní adresy, frekvenci vzorkování multimédia, kodeky a další metadata relace. Může rovněž nést kryptografický materiál pro zabezpečení média, tj. zabezpečení RTP/RTCP. Zpráva protokolu SDP zpravidla tvoří tělo zprávy protokolu SIP (kap. 9), tj. přímo se nevkládá do transportního protokolu. Dalo by se i říci, že „transportními protokoly" pro SDP zprávu jsou aplikační protokoly, jako SIP, RTS (*Real Time Streaming Protocol*) [64], HTTP (*Hypertext Transport Protocol*) [65], elektronická poštu s MIME zprávou [66] atp.

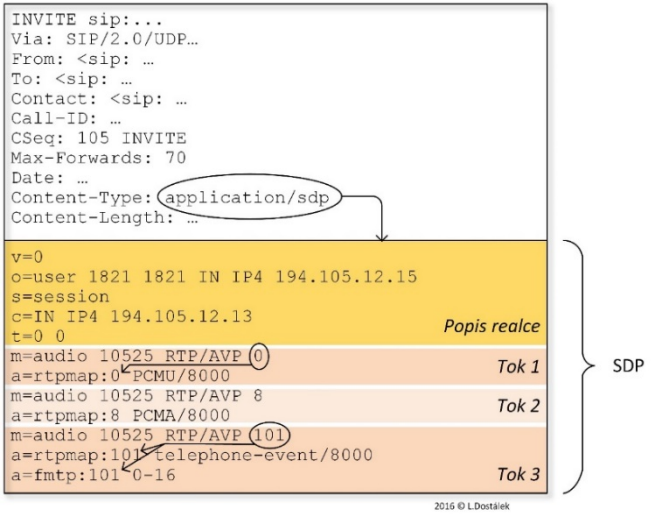
SDP popisuje parametry multimodální relace pomocí dvojic (typ parametru a jeho hodnota):

```
<type>=<value>
```

Každá dvojice je vždy na samostatném řádku. Typ parametru (`<type>`) je tvořen jedním písmenem a hodnota (`<value>`) závisí na typu parametru, zpravidla se jedná o řetězec v kódování UTF-8.

SDP zpráva se skládá vždy ze dvou částí:

- Popisu relace (začíná vždy „`v=`"), který obsahuje parametry společné pro celou relaci (tj. pro všechny multimediální toky relace). SDP zpráva musí obsahovat popis relace.
- Popis žádného, jednoho nebo více multimediálních toků. Popis každého jednotlivého multimediálního toku začíná vždy „`m=`".



obr. 10.1 Příklad SDP zprávy vložené do SIP zprávy

tab. 10.1 Některé parametry protokolu SDP

<type>=	**Povinný**	**Relace (S), Tok (M)**	**<value>** **příklad**
v= *(protocol version)*	ano	S	v=0
o= *(originator and session identifier)*	ano	S	o=<username> <sess-id> <sess-version> <nettype> <addrtype> <unicast-address> Specifikuje původce relace a identifikátor relace: <username> - účastnické jméno původce, v případě, že jej nelze určit, pak se použije hodnota „-“. <sess-id> - globálně jednoznačný identifikátor relace <sess-version> - verze tohoto popisu relace <nettype> - typ sítě, která je použita <addrtype> - typ adresy, která je dále použita <unicast-address> - adresa původce relace. `o=pepa 1234567890 9876543210 IN IP4 172.17.1.45`
s= *(session name)*	ano	S	s=<session name> Název relace (textově)
i= *(session information)*	Ne	S,M	i=<session description> Textová informace o relaci
u=	Ne	S	u=<uri>

(uri)			Obsahuje HTTP URI, kde lze nalézt bližší údaje o relaci
e= (e-mail)	Ne	S	e=<email-address> Specifikuje kontaktní informace osoby zodpovědné za konferenci.
p= (phone number)	Ne	S	p=<phone-number> Specifikuje kontaktní informace osoby zodpovědné za konferenci.
c= (connection data)	Ne	S,M	SDP zpráva musí obsahovat jeden řádek “c=” buď v části Popis relace, nebo pro každý Tok zvlášť. c=<nettype> <addrtype> <connection-address> Specifikuje adresu, na kterou se má relace připojit: <nettype> - typ sítě, která je použita <addrtype> - typ adresy, která je dále použita <connection-address>/ttl/počet – adresa připojení, hodnota parametru TTL (parametr TTL se používá jen v případě multicastových adres) a počet adres za sebou na které je možné se připojit `c=IN IP4 224.2.1.1/127/3` Značí, že je možné se připojit na adresy 224.2.1.1, 224.2.1.2 a 224.2.1.3 a hodnota TTL má být nastavena na 127.
b= (bandwidth)	Ne	S,M	b=<bwtype>:<bandwidth> Specifikuje požadovanou šířku pásma. Parametr <bwtype> upřesňuje co, se šířkou pásma míní. Např. hodnota CT (*Conference Total*) vyjadřuje, že se jedná o šíři pásma pro celou konferenci."
z= (time zones)	Ne	S	z=<adjustment time> <offset> <adjustment time> <offset> .... Plánuje opakování relace. Obsahuje posloupnost dvojic: Čas opakování ve formátu *NTP time* [67], tj. kdy se má relace opakovat. Posun letního času vůči *NTP time* v době, kdy relace má být opakována. Posun se ale počítá od času plánování konference.

			Např. v předchozím létě bylo naplánováno opakování konference, pak máme: `z=3633120000 -1h 3644697600 0`
k=* (encryption keys)	Ne	S,M	Obsahuje kryptografický materiál, použití tohoto parametru není doporučeno.
t= (timing)	Ano	time	t=<start-time> <stop-time> Specifikuje začátek a konec relace.

r=
(repead times)
	Ne	time	r=<repeat interval> <active duration> <offsets from start-time>
			Specifikuje pravidelné opakování relace. Např. konference má být plánována od pondělí 4.5.2015 od 10:00 (*NTP time*: 3639722400) do středy 10. června 2015 (*NTP time*: 3642926400) vždy po dobu jedné hodiny (1h). Má se opakovat vždy v pondělí od 10:00 a ve středu od 11:00. Pak dostaneme:
			`t=3639722400 3642926400`
			`r=7d 1h 0 49h`
			(<offsets from start-time> obsahuje počátky konferencí v rámci opakování (7d). Od pondělí 10:00 do středy 11:00 je 49 hodin)

m=
(medium)
	Ano	M	m=<media> <port> <proto> <fmt> ...
			Specifikuje typ media, formát media a transportní adresu
			<media> - typ média
			<port> - transportní port
			<proto> - protokol
			RTP/AVP: RTP přes UDP.
			RTP/SAVP: SRTP přes UDP.
			<fmt> - ukazatel na popis formátu (řádek začínající “a=”).
			`c=IN IP4 224.2.1.1/127/2`
			`m=video 49170/2 RTP/AVP 31`
			`a=rtpmap:31 L16/16000/2`

			Adresa 224.2.1.1 je použita s porty 49170 a 49171 a adresa 224.2.1.2 je použita s porty 49172 a 49173. Ukazatel 31obsahuje detailnější popis média pomocí a= type. Je použito kódování L16 se vzorkovacím kmitočtem 16.000 Hz, 2 kanály.
a=	Ne	S,M	Atribut relace, složí pro rozšíření protokolu SDP. Zpráva protokolu může obsahovat žádný, jeden nebo více atributů. Atributy se mohou vyskytovat jak popisu relace, tak v popisu toku. Příklady atributů: a=rtpmap:<fmt> <encoding name>/<clock rate> [/<encoding parameters>] Slouží pro bližší specifikaci media využívající RTP protokol, jako je vzorkovací kmitočet, kodek atp. Příklad viz m=. Význam jednotlivých parametrů: <fmt> - číselná hodnota ukazatele z řádku m= <encoding name> - typ přenášených dat RTP protokolem [68] <clock rate> - vzorkovací kmitočet <encoding parameters> - další parametry a=fmtp:<fmt> <format specific parameters> Obecně definuje parametry specifické pro medium. a=ptime:<packet time> Specifikuje čas (v milisekundách) dopravovaného RTP paketu a=maxprate :<packet-rate> Specifikuje maximální rychlost paketů [69]. a=crypto:<tag> <crypto-suite> <key-params> [<session-params>] Specifikuje kryptografický materiál pro zabezpečení toku [70]. Může obsahovat nezabezpečený kryptografický materiál! <tag> - číselný identifikátor jedné kryptografické sady (skupiny kryptografických algoritmů)

			<crypto-suite> - kryptografická sada
			
			<key-params> - kryptografický materiál. Je ve tvaru <key-method> : <key-info>. V případě, že je použita metoda “inline”, pak přímo následuje kryptografický materiál v nezabezpečeném tvaru. Příklad:
			
			`m=audio 49170 RTP/SAVP 0`
			`a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:`
			`PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:32`
			
			a=ecn-capable-rtp: <attribute>
			
			Notifikaci o zahlcení sítě (*Explicit Congestion Notification (ECN)*) pro RTP over UDP [71].
			
			a=3ge2ae:requested
			a=3ge2ae:applied
			
			Pomocí těchto atributů [72] se sděluje, jestli má být (resp. je) aplikováno zabezpečení media mezi mobilním zařízením a A-SBC – tzv. *end-to-access-edge media protection* (viz též kap. 14.5).
			
			a=path: URI
			
			Indikuje v MSRP protokolu (kap. 12) URI na které si původce přeje přijímat zprávy
			
			`m=message 7654 TCP/MSRP *`
			`a=accept-types:text/plain`
			`a=path:msrp://atlanta.example.com:7654/jshA7weztas;tcp`
			`a=max-size:2500`
			
			a=accept-types
			
			Indikuje typ media, který je akceptovatelný pro původce zprávy.
			
			a=max-size
			
			Indikuje maximální velkost zprávy (v bajtech), kteoru je původce ochoten akceptovat.

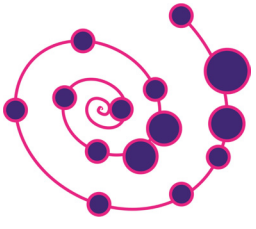
10.1 Bezpečnost SDP

Pokud je SDP přenášeno v nezabezpečeném tvaru, pak je jednoduché paket odchytit a případně změnit.

Zabezpečení je možné:

- Mezi konci relace (*end-to-end*) je zprávu možné zabezpečit např. pomocí S/MIME [73]. To je ovšem těžko použitelné, protože pak není možné, aby se mezilehlé entity dostaly k obsahu SDP zprávy, což často vyžadují, aby mohly např. provést trans-kódování (převod z jednoho kódování do jiného) zprávy.
- Mezi mobilním zařízením a A-SBC (*end-to-access-edge*) [72]. To je možné zabezpečit např. pomocí IPsec.

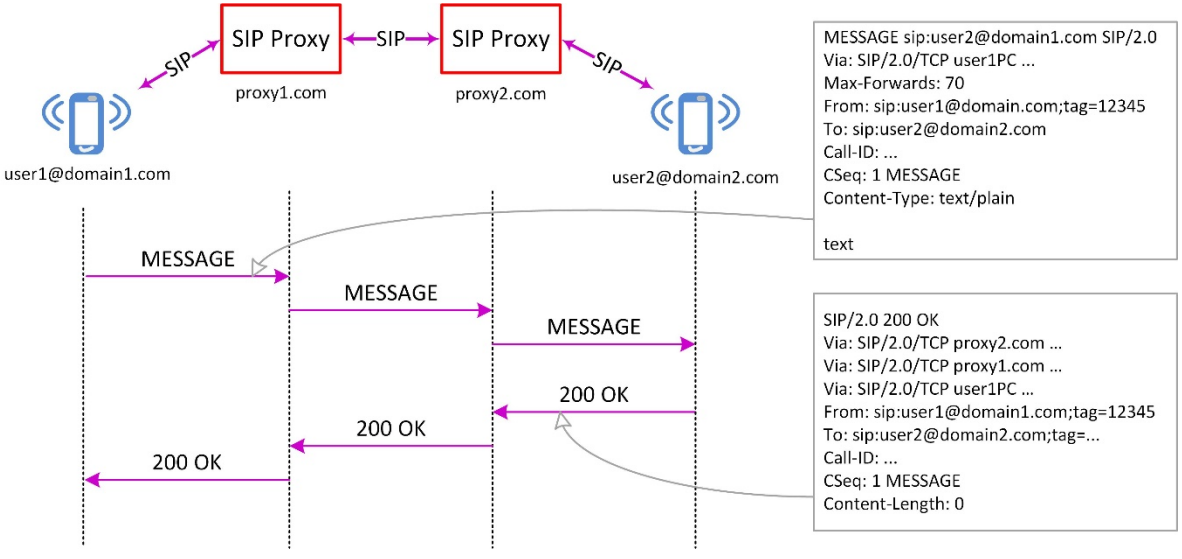
Zabezpečení nesmí sklouznout, jen k zabezpečení integrity. Velice důležité je rovněž šifrování zprávy. A to zejména v případě, že SDP zpráva obsahuje kryptografický materiál pro zabezpečení média (RTP).



11. Zasílání zpráv v LTE a IMS

SMS (*Short Message Service*) je neodmyslitelně spojené s GSM sítěmi. Jedná se o vyměňování krátkých textových zpráv, které si účastníci předávají přes servery nazývané SMS centrum. SMS centrum lze přirovnat k poštovnímu serveru (místo e-mailové adresy se používá telefonní číslo). SMS mají mnoho omezení. Kromě omezení délky je asi největším omezením, že byly urče-

- Využít referenční bod SGc, který propojuje MME a SMS bránu starších systémů. Předávání SMS mezi mobilním zařízení a MME zajišťuje stejný protokol, kterým se mobilní zařízení přihlašuje do LTE sítě (*Non Access Stratum*). Z MME pak SMS odejde rovnou do SMS centra. Vůbec se tedy nevyužívá IMS. Je tedy možné mít implementováno LTE bez VoLTE (tj. IMS) a z mobilního zařízení posílat klasické SMS.



obr. 11.1 SIP paging (převzato z RFC [75])

čeny pro anglické texty. Což bylo zlomeno tak, že můžeme zprávy psát i česky, ale azbukou nebo jinými písmy už v našem prostředí můžete mít problémy.

Zasílání zpráv je podporováno nezávisle na sobě jak LTE (tj. EPC), tak i IMS. Máme hned několik možností, jak zasílat krátké zprávy:

Vedle referenčního SGc existuje ještě referenční bod SBc, který propojuje MME a CBC *(Cell Broadcast Centre)* zajišťujících oběžníkových zpráv všem účastníkům v rámci buňky, resp. skupiny buněk (obdoba teletextu).

- Využít SIP komunikaci (SIP Paging), tj. využít IMS [74]. Protokol SIP má pro účely přenosu zpráv metodu MESSAGE. Jenže takto je možné poslat i zprávy, které nesplňují omezení na SMS, proto do záhlaví SIP zprávy nesoucí SMS vkládáme hlavičku „`Content-Type: application/vnd.3gpp.sms`“. Zpráva má pak specifický obsah, protože musí nést i informace ze záhlaví SMS zprávy. Předávání mezi IMS a SMS centem pak provádí aplikační funkce (AF) označovaná jako IP-SM-GW [74].
- Využít protokol MSRP (*Message Session Relay Protocol*) – kap. 12, který vytváří relaci pro přenos dat, která má jasný začátek a konec. Pro přenos používá protokol TCP.

11.1 SIP Paging (obecně)

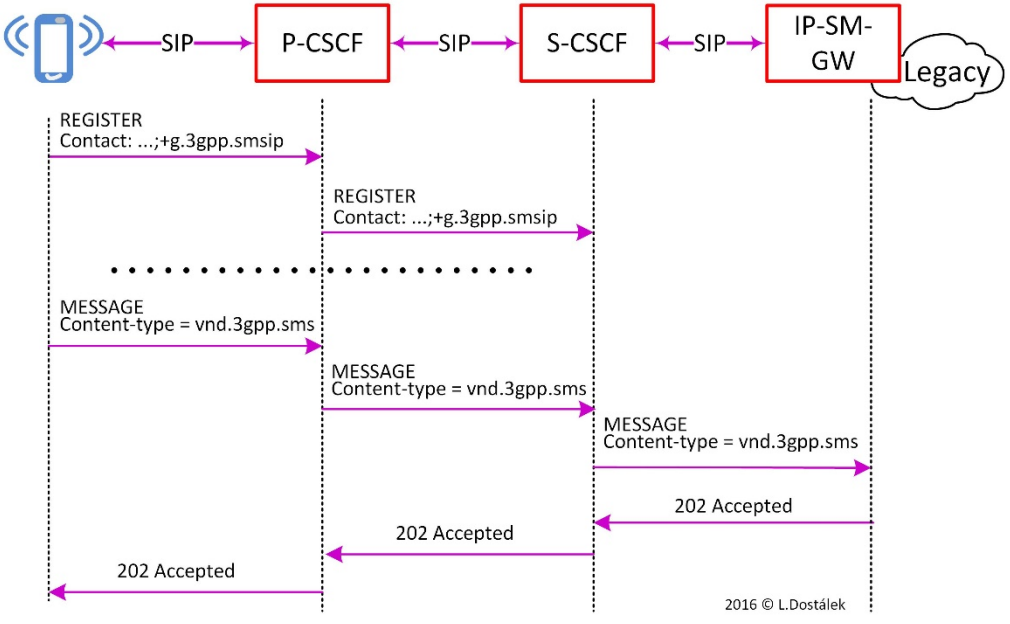
Protokol SIP má pro přenos zpráv metodu MESSAGE (obr. 11.1) [75]. Zpráva je přenášena v těle SIP zprávy, nevytváří se kanál pro přenos média (např. RTP). Zpráva je tak, přenášena přes všechny mezilehlé SIP entity.

11.2 SMS přes IP

SMS přes IP je aplikace obecného *SIP paging* pro SMS. Jak již bylo uvedeno, tak se SMS zprávou je třeba přenášet i její metadata (záhlaví SMS zprávy), aby mohla být interpretována jako SMS zpráva.

Komunikace se skládá z následujících kroků:

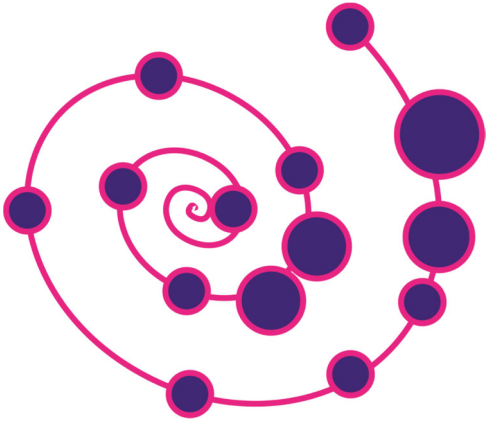
1. Při registraci účastníka do sítě protokolem SIP (metoda REGISTER), je třeba síti



obr. 11.2 SMS přes IP (případné potvrzení přijet SMS zprávy není zobrazeno)

sdělit, že účastníkovo zařízení má schopnost přijímat tradiční SMS přes IMS. To se provede přidáním řetězce „+g.3gpp.smsip“ do hlavičky Contact.

2. V okamžiku tvorby SMS zprávy v SIP protokolu se přidá do záhlaví hlavička „Content-type = vnd.3gpp.sms“. Takto vytvořená zpráva doputuje na IP-SM-GW, která ji transformuje do tvaru SMS zprávy (RP-DATA).
3. Volitelně může být nastaveno potvrzování přijatých SMS zpráv. To rovněž provede příslušnou SIP zprávou s metodou MESSAGE, která obsahuje pouze metadata SMS zprávy.

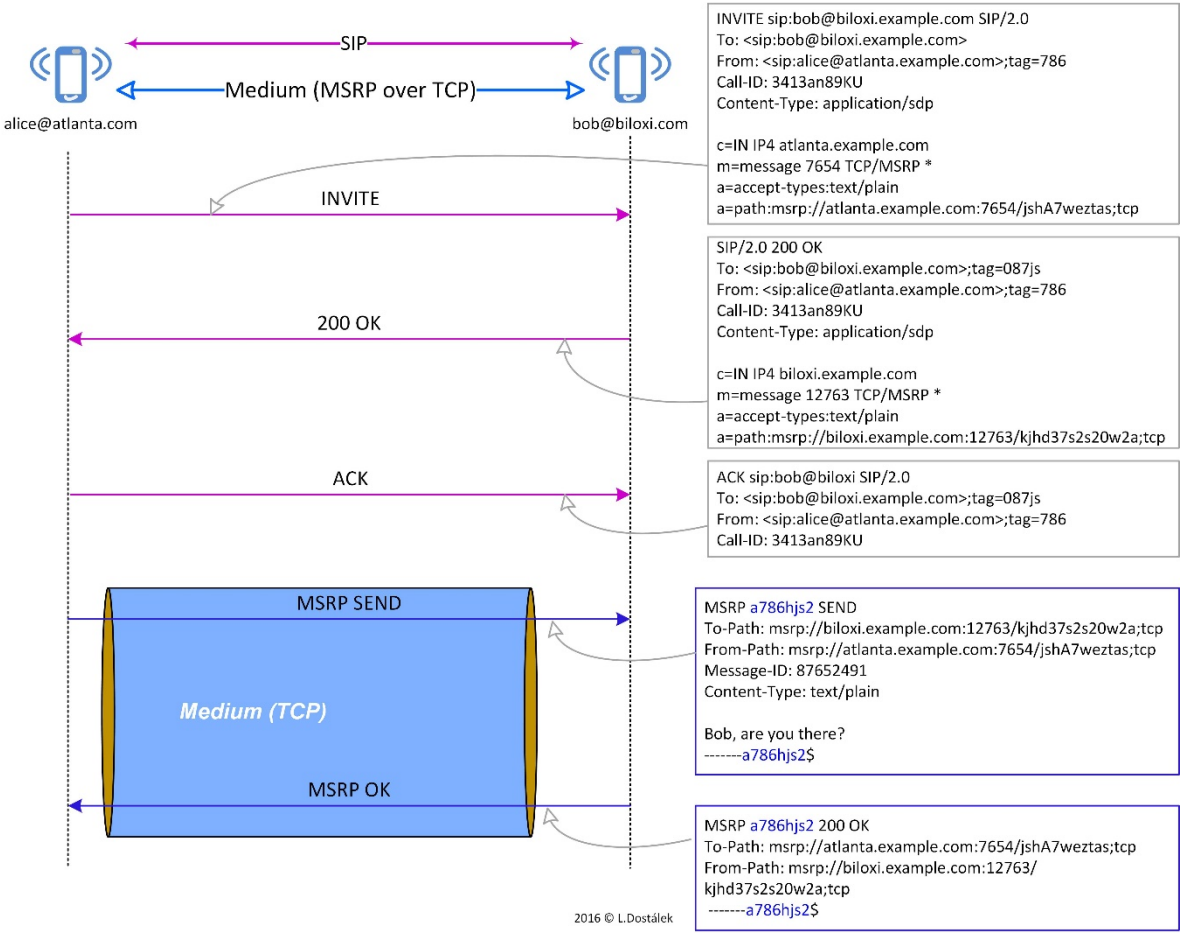


12. MSRP

Opravdové rychlé zasílání zpráv (*Instant Messaging*) mezi dvěma nebo vice účastníky umožňuje až protokol MSRP (*Message Session Relay Protocol*) [76]. MSRP umožňuje účastníky současně vytvořit např. hovornou relaci a během ní vytvořit další MSRP relaci pro rychlé zasílání zpráv. Účastníci tak mohou zároveň hovořit (multimediální relace) a zároveň si vyměňovat zprávy, posílat soubory atd.

MSRP je jistou modifikací protokolu SIP, rovněž metody (tab. 12.2) a hlavičky (tab. 12.3). MSRP používá mírně odlišnou terminologii pro své entity (tab. 12.1).

Protokol MSRP, na rozdíl od SIP pagging, vytváří relaci (*message session*) mezi účastníky přenosu. Předávané zprávy (ale např. i soubory



obr. 12.1 Příklad MSRP dialogu (převzato z [76])

[77]) nejsou přenášeny protokolem SIP, ale pomocí média. Na rozdíl od multimediálních relací se zde pro přenos méda nepoužívá protokol RTP, ale protokol TCP.

Protokol MSRP ale není úplně totožný s protokolem SIP – např. nekopíruje hlavičky To-path a From-Path z dotazu do odpovědi.

Protokol MSRP se zpravidla používá ve spojení s protokolem SIP (obr. 12.1).

tab. 12.1 Entity MSRP

ENTITA	**Význam**
MSRP uzel *(node)*	Entita, která má implementován protokol MSRP jako klient nebo jako relay.
MSRP klient	MSRP uzel, kterým je původcem nebo příjemcem MSRP zprávy.
MSRP relay	Mezilehlý MSRP uzel, který předává MSRP zprávy. Může vynucovat politiku předávání, může předávané zprávy fragmentovat a naopak sesazovat fragmentované části.

tab. 12.2 Metody protokolu MSRP

Metoda	**Standard**	
SEND	[76]	Metoda SEND se používá k odeslání zprávy nebo její části (*chunk*).
REPORT	[76]	Metoda REPORT hlásí status předchozí odeslané zprávy nebo její části. Metoda REPORT je podobná metodě SEND, ale nenese hlavičku Success-Report nebo Failure-Report. Naopak obsahuje hlavičku Status a Message-ID.
AUTH	[78]	Metoda AUTH se používá pro autentizaci účastníka, který je původcem zprávy s touto metodou. Účastník odešle zprávu s metodou AUTH zpravidla po obdržení chybové zprávy “401 Unauthorized”. Mechanismus autetnizace je shodný s autentizací protokolu HTTP a SIP (kap. 9). Komunikace je zpravidla následující: 1. Účastník obdrží “401 Unauthorized”, která obsahuje hlavičku „WWW-Authenticate“. 2. Účastník odešle zprávu s metodou AUTH s hlavičkou „Authorization“

3. V případě kladného výsledku, účastník obdrží zprávu „200 OK“ s hlavičkou „Authentication-Info“ a hlavičkou „Use-Path“.

tab. 12.3 Hlavičky protokolu MSRP

Header Field	**Standard**	
To-Path	[76]	Obsahuje MSRP URI příjemce zprávy. V případě, že mezi původcem a příjemce jsou relay, pak obsahuje seznam URI všech mezilehlých uzlů a příjemce v pořadí tak, jak jimi má procházet zpráva. Seznam musí být na jednom řádku.
From-Path	[76]	Obsahuje MSRP URI původce zprávy
Message-ID	[76]	Obsahuje jednoznačný identifikátor celé zprávy (nikoliv části zprávy)
Success-Report	[76]	Nabývá hodnoty „yes“. Tato hlavička pověřuje mezilehlý uzel (*relay*), aby po přijetí a předání zprávy vrátila kladné potvrzení (tj. s výsledkovým kódem 200).
Failure-Report	[76]	Nabývá hodnoty „yes“ nebo „partial“. Pověřuje mezilehlé uzly (relay), aby sledovali doručení zprávy, pokud nedojde do 30s, tak aby vrátily zprávu „408 Timeout error“.
Byte-Range	[76]	Indikuje část zprávy. Obsahuje, jaká část zprávy se přenáší.
Status	[76]	Obsahuje výsledkový (návratový kód). Výsledkové kódy jdou trojciferné: 200 – úspěch, 400 – nesrozumitelný příkaz atd.). Výsledkové kódy se používají ak v hlavičce Status, tak i v stavovém řádku odpovědi.
Expires	[78]	Indikuje, jak dlouho je požadavek platný. V případě metody AUTH indikuje, jak dlouho je nabízené URI platné.
Min-Expires	[78]	Indikuje, jak nejmenší dobu je server ochoten akceptovat v přijatých hlavičkách Expires.
Max-Expires	[78]	Indikuje, jakou nejdelší dobu je server ochoten akceptovat v přijatých hlavičkách Expires.
Use-Path	[78]	Obsahuje seznam URI poskytnutý MSPR relay v odpovědi na úspěšný požadavek AUTH. Účastník pak odpovídá metodou AUTH s hlavičkou „Authorization“ na některé z těchto URI.

WWW-Authenticate	[78]	Obsahuje autentizační výzvu, zpravidla pro autentizační metodu HTTP (viz kap. 9.5.2)
Authorization	[78]	Obsahuje autentizační odpověď.
Authentication-Info	[78]	Obsahuje autentizační informace.

12.1 SRP URI

MSRP URI se např. používá v SIP relaci pro odkaz ze SIP zprávy (resp. SDP zprávy) a MSRP relace (obr. 12.1). MSRP URI používá model “msrp”. Typické použití je ve tvaru

msrp://host:port/relace;tcp

Kde “relace” obsahuje identifikátor MSRP relace.

Protokol MSRP má registrovány porty 2855/tcp i 2566/udp, ale v MSRP URI se port uvádí vždy.

Schéma „msprs“ se používá v případě zabezpečení protokolem TLS [29].

12.2 Útoky

Útok	**Popis**
Muž uprostřed (Man in the middle)	Útočník může zachytit zprávu, pozměnit ji a unést spojení např. pomocí redirect serveru.
DoS/DDoS	Jelikož je zpravidla součástí dialogu protokol SIP, tak jsou zde možné všechny útoky proti SIP (kap. 9.9). Sám protokol MSRP používá jako transportní protokol TCP, takže případné DDoS útoky jsou podstatně náročnější (oproti protokolům využívající datagramové přenosy jako SIP).

13. H.248

Multimediální komunikace, nejenom v mobilních sítích, se skládá ze dvou částí (*plane*):

- *Control Plane* – tato část se zabývá vytvořením, správou a ukončením multimediální relace. Zde se používají např. protokoly SIP, SS7 (Signalizační systém č. 7) [62] apod.
- *Media Plane* – tato část řeší přenos multimediálních dat. Zde se používají např. protokoly RTP/RTCP, TDM apod.

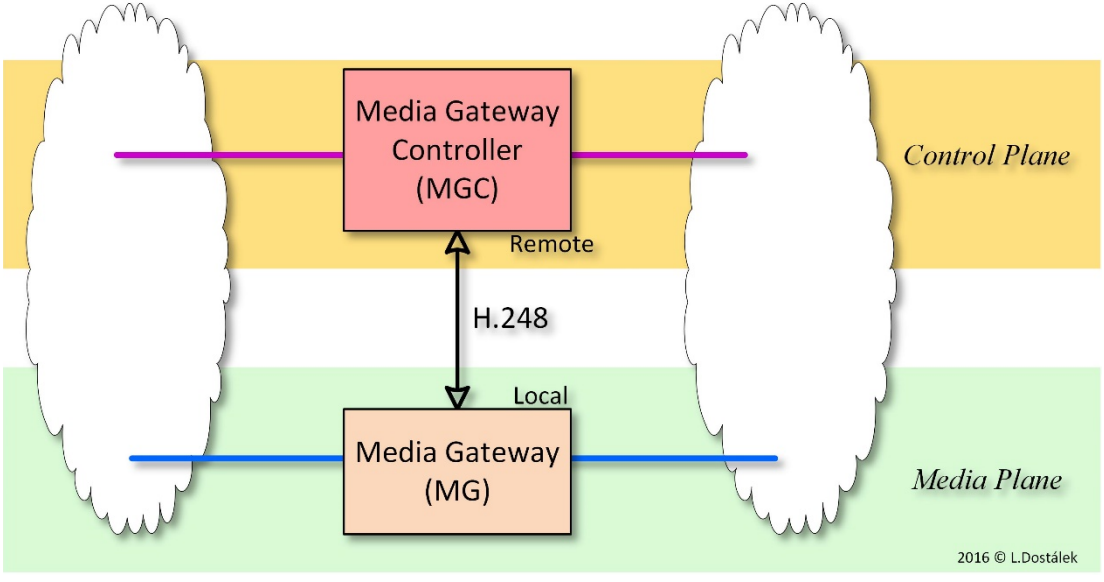
Každá z těchto částí je řešena samostatnou skupinou síťových protokolů. Na první pohled by se tak mohlo zdát, že jsou zcela nezávislé. Jen v aplikaci koncového účastníka (např. mobilní zařízení) se sejdou, aby společně poskytly kýženou službu koncovému účastníkovi.

Problém však nastává na hranici sítě. Např. na SBC (kap. 9.1), která multimediální relaci akceptuje, jakoby koncovým účastníkem, případně je transformuje a předává dále.

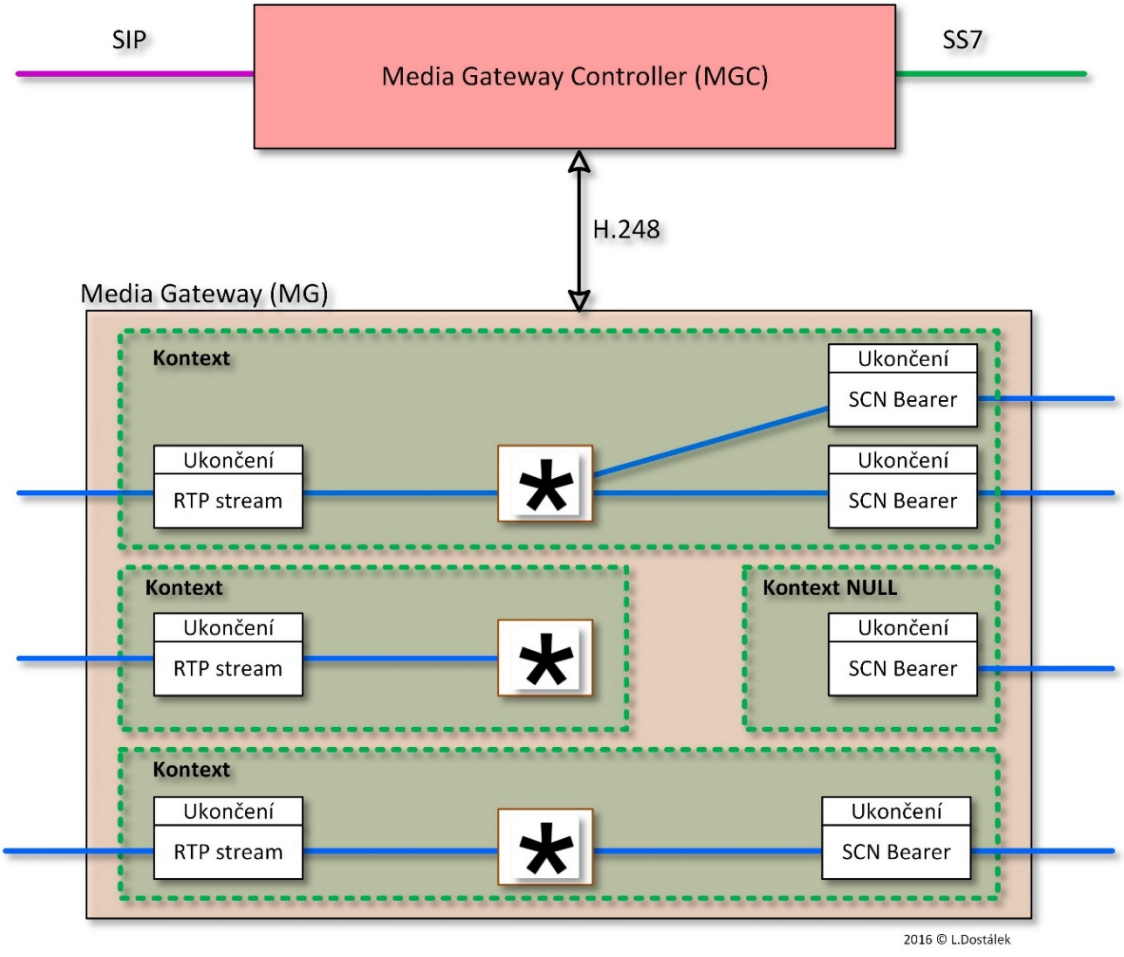
Na hranici sítě tak máme dvě brány (*gateway*):

- Pro *Control Plane,* používáme bránu označovanou jako MGC (*Media Gateway Controller*)
- Pro Media Plane, používáme bránu označovanou jako MG (*Media Gateway*)

Tyto dvě brány musí vzájemně koordinovat předávání komunikačního toku, např. protože metadata pro *Media Plane* se přenáší v *Control*



obr. 13.1 MGC a MG



obr. 13.2 Kontexty a ukončení

Plane, chyby vzniklé v *Media Plane,* je třeba signalizovat přes *Control Plane* atd. Pokud se jedná o transformaci z jedné rodiny protokolů do jiné (např. ze SIP/RTP do SS7/TDM[2]), pak je situace ještě komplikovanější.

Řešením je protokol H.248 [79], který zprostředkovává komunikaci mezi MGC a MG (obr. 13.1). Tento protokol mj. popisuje logické entity (objekty) v MG (*Media Gateway*), které mohou být řízeny MGC (*Media Gateway Controller*).

[2] Termín TDM *(Time Division Multiplexing)* se u nás používá místo anglického E-carrier. Jedná se o pevné okruhy využívající časové přepínání *(multiplexing)*. Např. linky E1, E2 apod.

13.1 Kontext

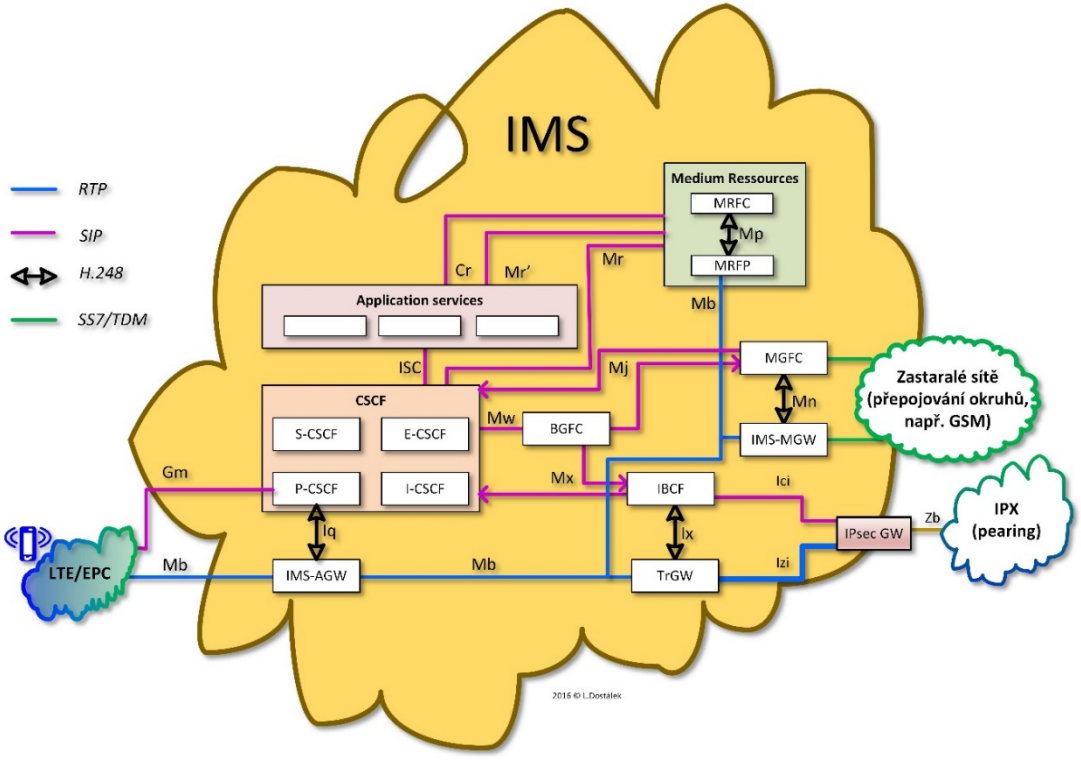
Kontext slouží k propojení jednotlivých ukončení (obr. 13.2). Kontext popisuje topologii předávání, mixování medií (pokud se propojuje více než dva toky) a další parametry propojení. Každé ukončení je přidáno právě do jednoho kontextu.

Máme ještě speciální kontext NULL neprovádí žádné propojení. Ukončení majícímu kontext NULL můžeme konfigurovat, měnit mu parametry a také můžeme na něm sledovat událostí.

Protokol H.248 se používá k vytváření kontextů a modifikování jeho parametrů tzv. příkazy. Maximální množství ukončení v kontextu je vlastností MG. Např. MG, které podporují jen komunikaci mezi dvěma účastníky, mohou umožňovat jen dvě ukončení v kontextu. Naopak MG, které podporují konference, musí umožňovat více ukončení v kontextu.

13.2 Ukončení

Ukončení (*Termination*) je logická entita MG (*Media Gateway*), která je buď původcem nebo



obr. 13.3 Referenční body H.248 v IMS

příjemcem datového nebo řídícího toku. Ukončení má celou řadu charakteristických vlastností. Charakteristické vlastnosti jsou specifikovány skupinu deskriptorů, které se používají v příkazech. Ukončení je identifikováno identifikátorem `TerminationID`, který přiřazuje MG v okamžiku jeho vytvoření.

Ukončení reprezentuje fyzickou entitu, která má různou dobu života. Např. RTP tok existuje pouze dočasně po dobu tohoto datového toku. Naopak TDM kanál bude nejspíše existovat permanentně po celou dobu existence brány.

Dočasná ukončení se vytváří příkazem `Add`, ruší příkazem `Subtract`. Fyzická ukončení se nepřidávají/ubírají příkazy `Add/Subtract`, ale nastaví se jim kontext na NULL.

Ephemeral terminations are created by means of an Add Command. They are destroyed by means of a Subtract Command. In contrast, when a physical termination is added to or subtracted from a context, it is taken from or to the NULL Context, respectively.

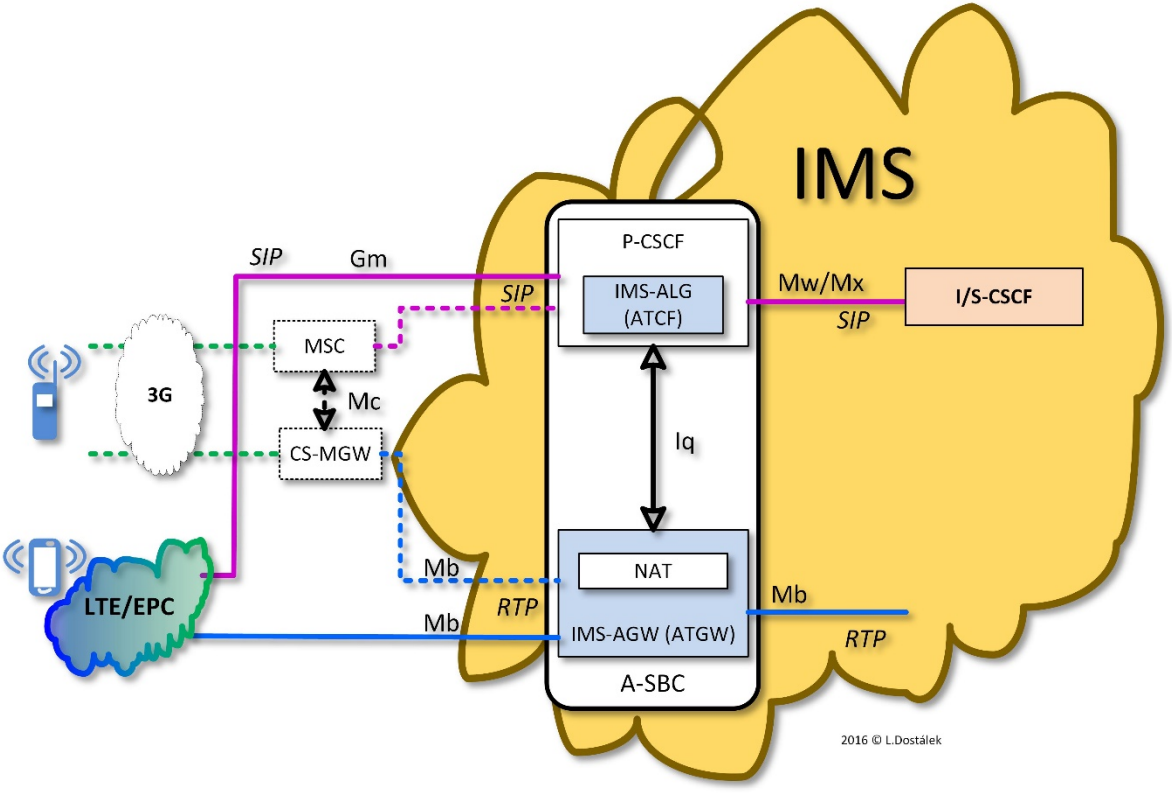
13.1 Příkazy

Protokol H.248 komunikuje pomocí tzv. příkazů. Příkazy slouží pro manipulaci s logickými entitami a vytvoření topologie propojení. Příkazem `Add` se obecně přidává ukončení do kontextu. Jestliže, MGC nespecifikuje existující kontext, do kterého se má přidat, tak MG automaticky vetvoří nový kontext. Ukončení se z kontextu odebírá příkazem `Subtract`. Dále ukončení může být převedeno do jiného kontextu příkazem `Move`. Přehled příkazů protokolu H.248 je uveden v tab. 13.1.

tab. 13.1 Přehled příkazů protokolu H.248

Příkaz	Význam
`Add`	Přidává ukončení do kontextu. Příkazem Add pro první ukončení se vytvoří kontext.
`Modify`	Modifikuje vlastnosti ukončení a událostí na něm.
`Subtract`	Odpojí ukončení z kontextu. Odpojením posledního ukončení se zruší kontext.
`Move`	Přesune ukončení z jednoho kontextu do druhého.
`AuditValue`	Příkaz vrací aktuální stav, události, signály a statistiky ukončení.
`AuditCapability`	Příkaz vrací možné hodnoty vlastností, událostí a signálů MG.
`Notify`	Pomocí tohoto příkazu MG informuje MGC o nastalých událostech na MG.

`ServiceChange`	Příkaz umožňuje MG sdělit MGC, že ukončení nebo skupina ukončení je mimo provoz, nebo že je naopak opět k dispozici. Naopak MGC může příkazem MG sdělit, aby vyřadila z provozu ukončení, nebo skupinu ukončení. Příkazem rovněž MG sděluje MGC svou dostupnost, svůj restart atp.



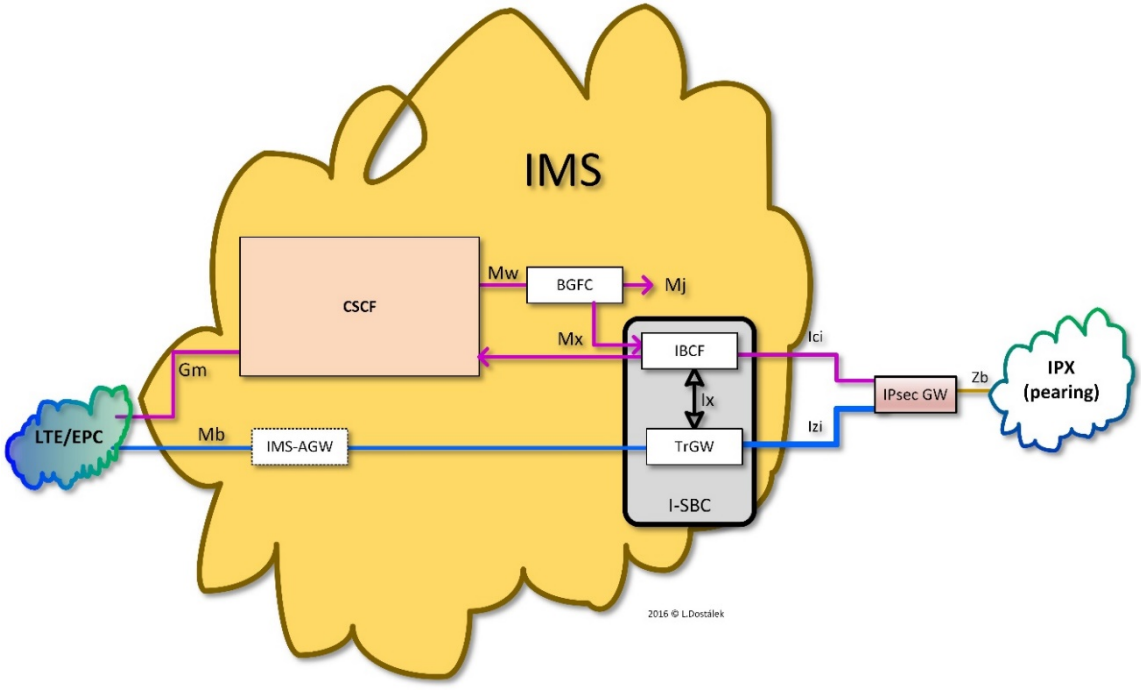
obr. 13.4 referenční body Iq a Mc

13.2 Referenční body IMS

Obrázek obr. 13.3 znázorňuje jednotlivé referenční body IMS, které využívají protokol H.248.

13.2.1 Iq a Mc

Referenční bod Iq [80] se používá mezi ALG (*IMS Application Level Gateway*) a IMS-AGW (*IMS Access Gateway*). Na obr. 13.4 je ještě čárkovaně



obr. 13.5 referenční bod Ix

vyznačeno možné připojení ze starších sítí 3G (referenční bod Mc).

Referenční bod Iq poskytuje mj. následující procedury:

- Převod IP adres (NAT/NAPT) v případě IPv4.
- Otevření/uzavření brány včetně filtrace IP adres a portů.
- Indikaci domény IP adres, ze které požadavek přichází.
- Vynucování předepsaných politik na příchozím síťovém provozu.
- Označování odchozích paketů QoS příznaky.
- Detekce ukončení spojení
- Obsluha protokolu RTCP
- Obsluha priority média (*Multimedia Priority Service*)
- Notifikace zahlcení sítě (*Explicit Congestion Notification support*)
- Volitelně může podporovat:
  - Konverzi kódování média (*Audio transcoding*)
  - Převod mezi IPv6 a IPv4.

- Převod mezi rodinou protokolů SIP/RTP a SS7/TDM

13.2.2 Ix

Referenční bod Ix [81] se používá (obr. 13.5) mezi IBCF (*Interconnection Border Control Function*) a TrGW (*Transition Gateway*), případně mezi CS-IBCF a CS-TrGW v případě přechodu do sítí na bázi přepínaných okruhů (CS).

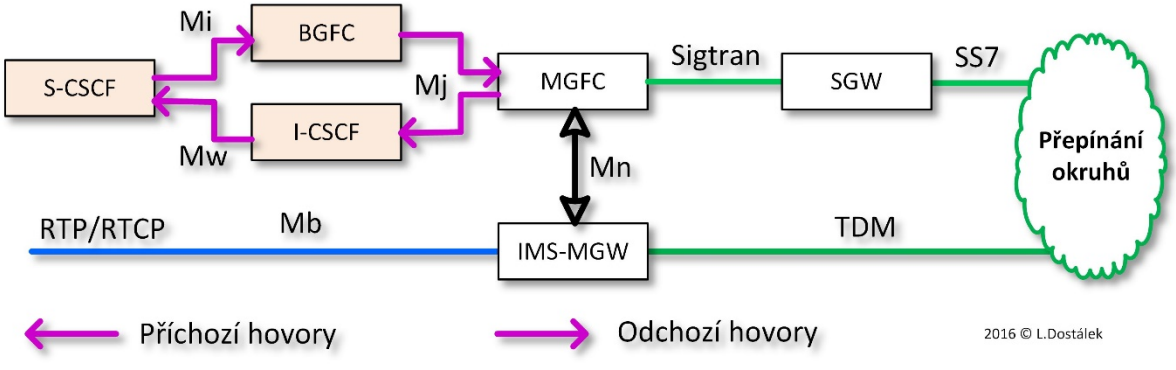
Referenční bod Ix poskytuje mj. následující procedury:

- Převod IP adres (NAT/NAPT) v případě IPv4.
- Otevření/uzavření brány včetně filtrace IP adres a portů.
- Indikaci domény IP adres, ze které požadavek přichází.
- Vynucování předepsaných politik na příchozím síťovém provozu.
- Označování odchozích paketů QoS příznaky.
- Obsluha ukončení spojení
- Obsluha protokolu RTCP
- Obsluha priority média (*Multimedia Priority Service*)
- Notifikace zahlcení sítě (*Explicit Congestion Notification support*)
- Volitelně může podporovat:
  - Konverzi kódování média (*Audio transcoding*)
  - Převod mezi IPv6 a IPv4.
  - Převod mezi rodinou protokolů SIP/RTP a SS7/TDM.

13.2.3 Mn

Referenční bod Mn [82] se používá mezi MGFC (*Media Gateway Control Function*) a IM-MGW (*IM Media Gateway)*. Jedná se rozhraní mezi IMS a sítěmi používajícími přepínané okruhy (ISUP, BICC a SIP-I).

Jestliže si účastník IMS sítě přepije propojit na TEL URI, které nepatří žádnému účastníkovi



obr. 13.6 Referenční bod Mn

místní (domovské) IMS sítě, pak požadavek předá na BGFC. Jestliže BGFC zjisti, že takovému požadavku neodpovídá žádné TEL URI v IMS, pak požadavek předá MGFC. MGFC ve spolupráci s IMS-MGW vytvoří spojení na E.164 telefonní číslo v telefonní síti (obr. 13.6).

V opačném směru, když účastník telefonní sítě vytočí číslo patřící účastníkovi IMS, tak jeho požadavek je předán na MGFC. MGFC ve spolupráci s IMS-MGW vytvoří spojení v IMS síti. Jelikož z externích sítí je viditelná pouze I-SCSF, tak příchozí požadavek je předáván skrze I-CSCF.

Referenční bod Mn provádí následující procedury:

- Vytváří/uvolňuje spojení mezi účastníkem IMS a účastníkem telefonní sítě (přepínané okruhy).
- Zajišťuje generování tónů.
- Zajišťuje generování zvukových zpráv, např. „Účastník, kterého voláte …“
- Obsluhuje DTMF tóny (*Dual-Tone Multi-Frequency*), tj. např. zadávání PIN na klávesnici telefonu pro Call-Centrum elektronického bankovnictví.
- Trans-kódování audia a videa, tj. převod z jednoho systému kódování do jiného systému.

13.2.4 Mp

Referenční bod Mp [83] popisuje funkční požadavky a informační tok mezi MRFC (*Multimedia Resource Function Controller*) a MRFP (*Multimedia Resource Function Processor*).

Umožňuje jak S-CSCF, tak i aplikačním funkcím (AF) využívat zdroje (nahrávky) dostupné přes MRFP (obr. 13.7).

Funkce MRFC jsou následující:

- Řídí datové toky zdrojů (nahrávek) uložených v MRFP.
- Interpretuje požadavky přicházející z AF a S-CSCF a převádí je na příkazy protokolu H.248.
- Generuje účtovací informace.
- Podporuje rozšíření řízení konferencí

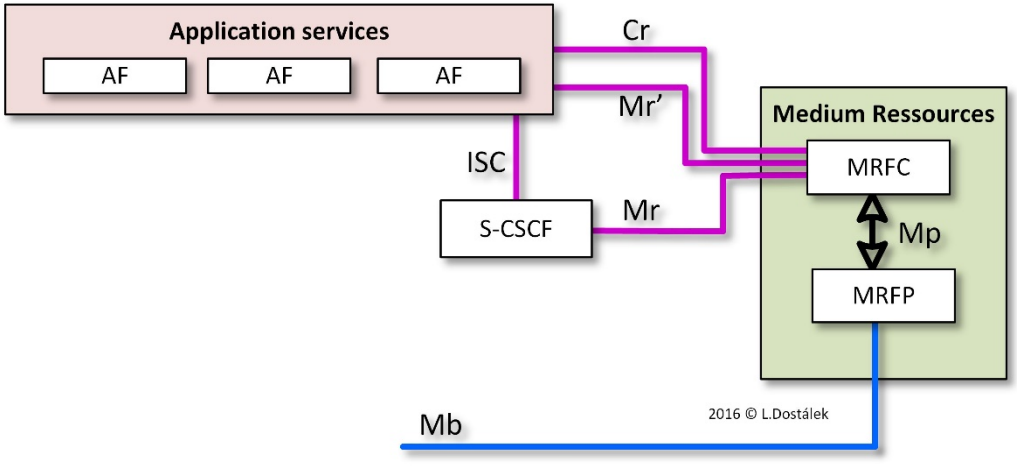
Funkce MRFP:

- Řízení datových nosičů přes referenční bod Mb.
- Poskytování zdrojů (nahrávek).
- Mixáž příchozích datových multimediálních toků.
- Zpracování datových toků (trnskódování, analýza toku atd.)
- Správa přístupových práv ke sdíleným zdrojům (nahrávkám) v případě konferencí.

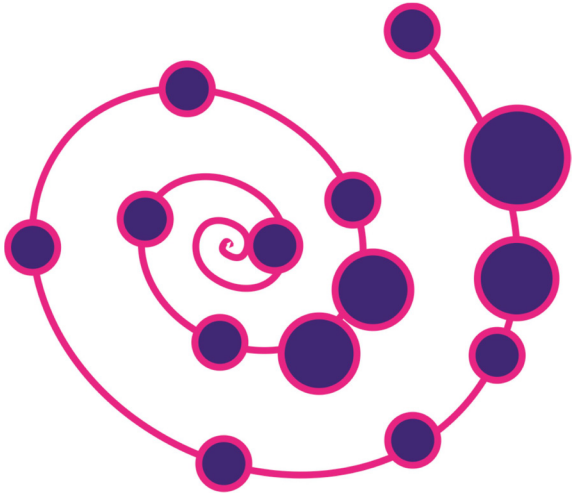
Referenční bod Mp zajišťuje následující procedury:

- Hraje tóny účastníkům a skupinám účastníků.
- Hraje hlasové zprávy typu: „Účastník, kterého voláte …“
- Generuje hlasový výstup z textového vstupu.

- Znamenává audio/video stram do soboru.
- Slučuje DTMF volby (*Dual-Tone Multi-Frequency*) do celku k dalšímu zpracování, tj. např. zadávání PIN na klávesnici telefonu pro Call-Centrum elektronického bankovnictví.
- Provádí automatizované rozpoznávání hlasu.
- Hraje synchronizované audio a video stramy.
- Zajišťuje podporu konferencí.
- Trans-kódování audia a videa, tj. převod z jednoho systému kódování do jiného systému



obr. 13.7 Referenční bod Mp



14. RTP/RTCP

RTP (*Real-time Transport Protocol*) [84] poskytuje přenosové služby pro aplikace, které vyžadují přenos dat v reálném čase. Např. audio, video, simulační data atp. Jako transportní protokol využívá nepotvrzované protokoly (např. UDP [25]), protože ztráta paketu je menším zlem než porušení režimu reálného času, které by bylo způsobeno dožádáním si ztraceného paketu. Např. pro telefonujícího účastníka je příjemnější, když je ztracený paket nahrazený umělým šumem, než kdyby se čekalo na opakování ztraceného paketu a následně se např. rychle informace přehrála. RTP proto jako transportní protokoly používá buď UDP [25] nebo nepotvrzovaný stream modernějšího protokolu SCTP (viz kap. 17).

Nutno ještě podotknout, že RTP přenáší data, aniž by věděl, co přenáší. Z tohoto důvodu se mezi RTP a aplikaci vkládá ještě další vrstva – tzv. kodek (*media codec* – vznikl jak zkratka z ***co**der-**dec**oder*). Kodek je obálka, která balí multimediální data do RTP streamu. Kodek řeší problémem jakým protokolem je multimediální informace digitalizována a jakým kmitočtem je vzorkována. Typ a parametry použitého kodeku jsou sdělovány protokolem SDP (viz kap. 10) a jsou přenášeny v těle SIP zprávy. Kodek je ve skutečnosti realizován programem, který kóduje/dekóduje audio/video do tzv. formátu (např. MP-3).

Z hlediska čistého síťového modelu TCP/IP je RTP aplikačním protokolem (leží nad vrstvou TCP, UDP, SCTP), ale z hlediska koncového účastníka je to „transportní" protokol, protože aplikace koncových účastníků vkládají data do obálky cocedu a ty se teprve vkládají do RTP.

14.1 RTP

RTP poskytuje transportní funkce aplikacím v reálném čase (audio, video, simulační data apod.). RTP podporuje jak IP adresy typu unicat, tak i multicast. Jako protokol nižší vrstvy RTP využívá buď UDP [25] nebo SCTP (viz kap. 17).

RTP zjišťuje pro podporu přepravy v reálném čase:

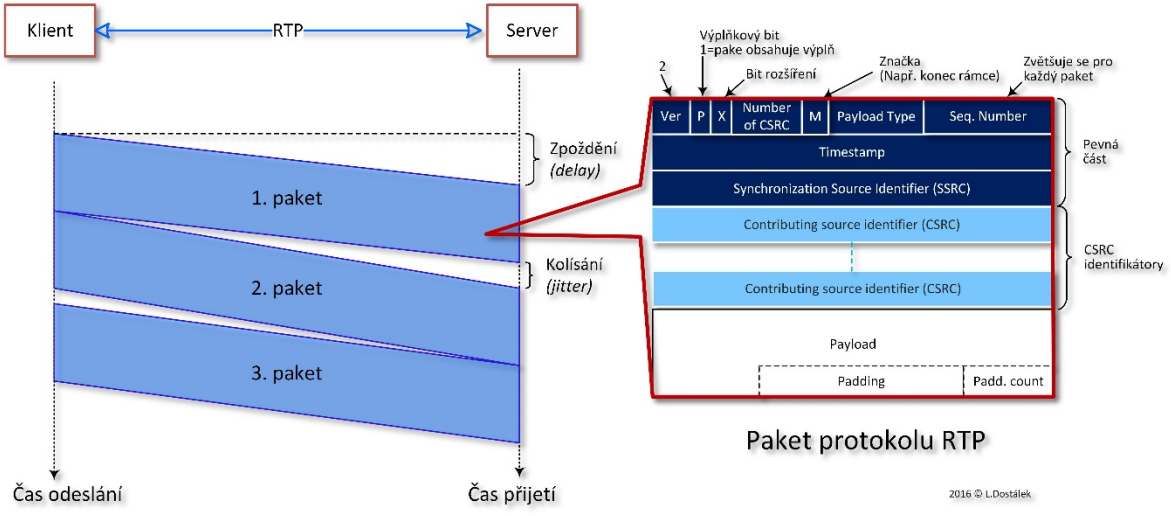
- Eliminaci rozptylu doručování paketů *(jitter elimination)* pomocí vyrovnávacích pamětí *(buffer)*.
- Synchronizaci audio/video stramů patřících téže multimediální relaci.
- Multipexování audio/video stramů do jednoho stramu.
- Převod z jednoho kódování stramu do jiného.

Terminologicky je tu trochu problém s pojmem relace (*session*). Z hlediska koncového účastníka se hovoří o tzv. multimediální relaci, kterou si můžeme přestavit třeba jako videokonferenci. Videokonference se pak skládá z audio RTP relace a video RTP relace. RTP relací tedy míníme množinu účastníků komunikujících protokolem RTP k konkrétním čase (více účastníků, protože se též může používat IP adresa typu multicast). V případě komunikace přes UDP je RTP relace určena množinou IP adres a UDP portů svých účastníků. Na druhou stranu účastník se může účastnit více relací současně.

V Čechách se někdy strana, která přispívá do relace svým multimediálním stramem označuje, jako vysílač a strana, který stream přijímá, se označuje jako přijímač. Strana, která jen přijímá, se pak označuje jako pasivní přijímač.

Na obr. 14.1 je zobrazena komunikace mezi klientem a serverem protokolu RTP. Dále je znázorněn i paket protokolu RTP, který obsahuje následující položky:

- Verze, která je vždy 2.
- Výplňkový bit (P) signalizuje, že RTP paket je na konci doplněn výplní. V případě, že bit P je nastaven, pak na konci TRP paketu je čítač *„Padding count“*, který obsahuje délku výplně (včetně čítače). Výplň je nutná např. v případě přenosu dat šifrovaných blokovou šifrou.
- Jestliže je nastaven bit rozšíření (X), pak záhlaví je následováno jedním rozšířením záhlaví.
- „*Number of CSRC*“ obsahuje počet CSRC identifikátorů, které následující za pevným záhlavím.
- Bit M se používá k označení události v přenášených datech. Např. označuje hranici multimediálního rámce.
- Typ přenášených dat (*Payload type* - PT) – viz tab. 14.1.
- „Sequence number“ pro každý přenášený RTP paket se zvyšuje o 1. Slouží pro detekci ztracených paketů.
- SSRC (*Synchronization source identifier*) – jednoznačně identifikuje zdroj multimediální relace. SSRC se generuje náhodně, ale



obr. 14.1 Komunikace v protokolu RTP, paket protokolu RTP

tak, aby bylo jedinečné v rámci RTP relace.

- CSRC (*Contributing source identifier*) – obsahuje SSRC stramů, které byly zkombinovány pomocí tzv. RTP mixeru. RTP mixer vloží seznam SSRC zdrojů, které zmixoval na počátek RTP paketu. Např. RTP mixer audio konference zmixoval audio stramy jednotlivých účastníků, kteří měli zapnutý mikrofon.

tab. 14.1 Typy přenášených dat v protokolu RTP [85]

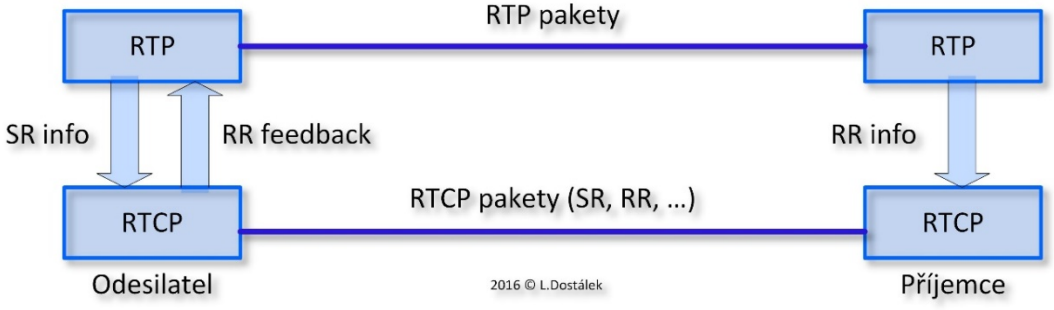
Payload Type	**Název (např. pro popis v SDP)**	**Audio/Video (A/V)**	**Vzorkovací kmitočet (Hz)**
0	PCMU	A	8000
3	GSM	A	8000
4	G723	A	8000
5	DVI4	A	8000
6	DVI4	A	16000
7	LPC	A	8000
8	PCMA	A	8000
9	G722	A	8000
10	L16 *(2 kanály)*	A	44100
11	L16 *(1 kanál)*	A	44100
12	QCELP	A	8000
13	CN	A	8000
14	MPA	A	90000
15	G728	A	8000
16	DVI4	A	11025
17	DVI4	A	22050
18	G729	A	8000

25	CelB	V	90000
26	JPEG	V	90000
28	nv	V	90000
31	H261	V	90000
32	MPV	V	90000
33	MP2T	AV	90000
34	H263	V	90000
96-127	Registrováno pro dynamické přidělování *Payload Type* [86]		

14.2 RTCP

Protokol RTP poskytuje aplikacím přenos paketů v reálném čase, ale nemá žádný mechanismus pro ošetřování chyb, řízení toku, řízení zahlcení, zpětnou vazbu o kvalitě přenosu, synchronizaci při doprovodu protokolu RTP musí podporovat i převody kódování a mixování.

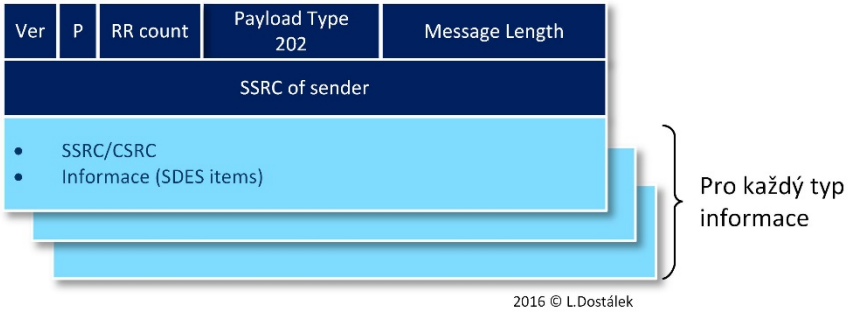
Z hlediska transportu je ale protokol RTCP nezávislý na protokolu RTP – používá např. svůj UDP port v případě UDP transportu. Protokol RTP zpravidla používá sudé porty protokolu UDP.



obr. 14.2 Protokol RTCP monitoruje protokol RTP

atp. Pro tyto účely slouží protokol RTCP (*Real-Time Control Protocol*) [84]. RTCP protokol doprovází RTP protokol, aby prováděl monitorování RTP stramu mezi koncovými entitami (*end-to-end monitoring*), a aby sledování QoS. RTCP RTCP pak používá nejbližší vyšší liché číslo pro číslo portu. IP adresy a čísla portů se zpravidla dohodnou protokolem SIP (resp. SDP).

RTCP periodický posílá své pakety všem účastníkům relace, přičemž používá stejné transportní



obr. 14.3 RTCP paket typu SDES

mechanismy, jako protokol RTP. Při kalkulaci zatížení sítě počítáme pro RTCP přibližně 5% ze zatížení kalkulovaného pro RTP. Naopak RTCP konfigurujeme tak, aby jeho tok odpovídal cca 5% toku RTP.

RTCP je zodpovědný za tři základní funkce:

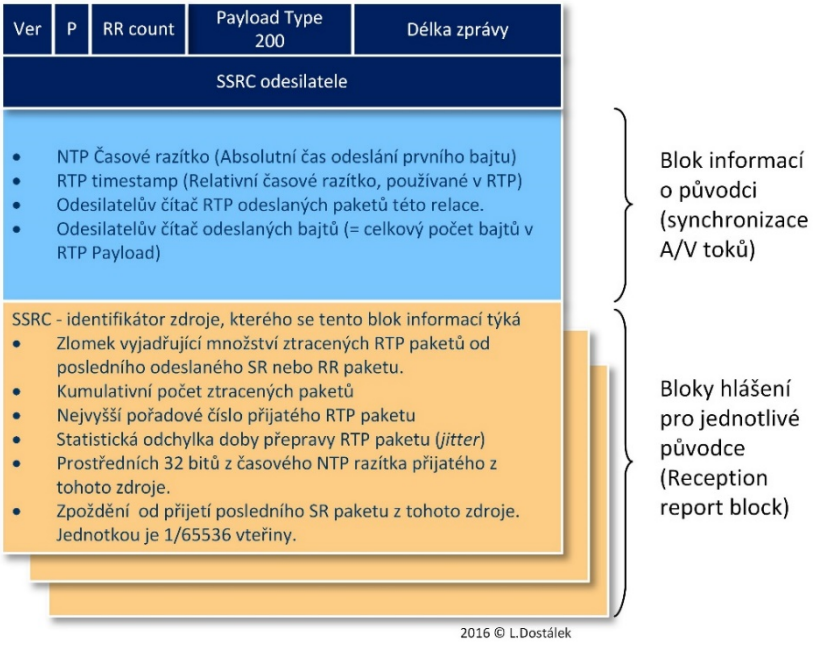
- Poskytnutí zpětné vazby zatížení sítě.
- Porovnávání a synchronizace různých stramů generovaných stejným původcem.(např. synchronizaci video a audio toku).
- Předání identity původce aplikaci, aby jej mohl zobrazit adresátům.

Protokol RTCP specifikuje jednotlivé své pakety (tab. 14.2). Na obr. 14.2 je vidět jak jsou při tomto monitorování jednotlivé pakety využívány: odesilatel odešle RTP paket a protokolu RTCP předá SR info (*Sender Info*: informace o odesilateli), které RTCP vloží do SR paketu a odešle. RTP příjemce vyhodnotí statistiky o příjmu a je protokolu RTCP jako RR info (*Receiver Info*: informace pro původce RTP streamu), který je odešle pomocí RR paketu. Původce příjme RR paket a informace předá formou RR feadbek původci RTP stramu.

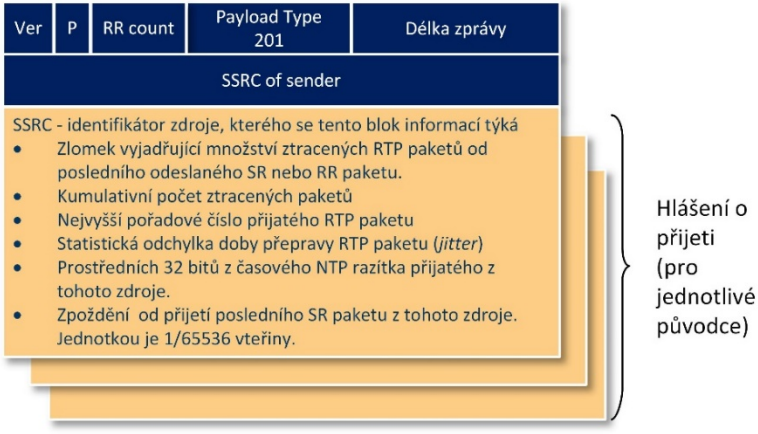
tab. 14.2 Typy paketů protokolu RTCP

Payload Type	Paket	Význam
200	SR	Pakety SR (*Sender report*) pravidelně odesílá entita, která jak přijímačem, tak vysílačem. Obsahuje jak informace o jim odesílaném

		streamu (Blok informací o původci na obr. 14.4), tak i případné informace přijímaných streamech (Blok hlášení pro původce). Časová razítka v Bloku informací o původci slouží např. pro synchronizaci streamů patřících téže relaci (např. synchronizaci audia a videa). Blok hlášení pro původce zase obsahuje statistiky o ztracených paketech a o rozptylu (kolísání) zpoždění (*jitter*). To je zase užitečné pro původce stramu, může např. na základě těchto statistik snížit kvalitu poskytovaného obsahu streamu, čímž pravděpodobně dosáhne nižší chybovosti.
201	RR	Paket RR (*Receiver Report*) používají pasivní přijímače. Je obdobou paket SR – pouze neobsahuje Blok informací o původci - obr. 14.5.
202	SDES	Pakety SDES (*Source Description*) posílá vysílač, aby propagoval informace o sobě (obr. 14.3). Přijímač pak tyto informace zobrazí účastníky. V paketu SDES má každý typ informace svůj typ položky. Máme následující typy informací: • CNAME – jméno ve tvaru NAI, tj. user@host. • NAME – jméno účastníka (původce streamu). • E-MAIL – e-mailová adresa. • PHONE – telefonní číslo. • LOC – geolokace. • TOOL – název aplikace generující stream. • NOTE – popis aktuálního stravu relace. • PRIV – aplikačně závislý typ. • END – konec seznamu informací.
203	BYE	Vysílač paketem BYE odesílá zprávu k ukončení streamu. Mixer ji v nezpěněném tvaru předává dále.
204	APP	Slouží pro zasílání zpráv, které nejsou definované ve standardu a umožňuje tak definici nových nebo experimentálních typů zpráv.
207	XR	Určen pro rozšíření RTCP.



obr. 14.4 RTCP paket typu SR



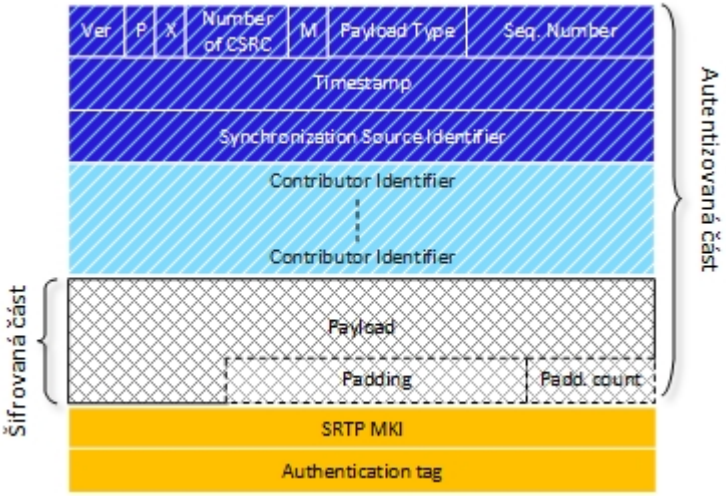
obr. 14.5 RTCP paket typu RR

14.3 SRTP

SRTP (*Secure Real-time Transport Protocol*) vytváří prostředí pro autentizaci a šifrování RTP. SRTP na straně vysílače zachycuje RTP pakety, zabezpečuje je, a posílá je dále jako SRTP pakety

- Klíče relace (*session keys*), které se přímo používají k zabezpečení RTP relací.

Příkladem ustanovení hlavního klíče je protokol SDES [70], který hlavní klíč přenáší ve zprávě



obr. 14.6 SRTP paket

(obr. 14.6). Na straně přijímače zase zachytává SRTP pakety, dešifruje je, ověří jejich autentizaci a předá je přijímači.

Každý SRTP stream musí na obou stranách udržovat příslušný kryptografický materiál a stavové informace. Hovoříme tak o tzv. kryptografickém kontextu SRTP streamu. Jelikož multimediální relace může mít více RTP streamů, tak SRTP používá dva typy kryptografických klíčů:

- Hlavní klíče (*master keys*), které se ustanovují mezi komunikujícími entitami a z nichž se odvozují klíče relací. Hlavní klíče se ustanovují mimo protokol ŚRTP.

protokolu SIP, resp. protokolu SDP v atributu “a=crypto:“ v nezabezpečeném tvaru (viz tab. 10.1). Existují sofistikovanější metody, např. [87] nebo starší [88].

SRTP paket je zabezpečeným RTP paketem s přidáním zápatí o dvou položkách: SRTP MKI a *Authentication Tag* (obr. 14.6). Přitom integrita je zabezpečována přes celý RTP paket, šifrování jen přes přenášená data (*payload*). Význam zbylých položek:

- MKI (*Master Key Identifier*) – identifikuje hlavní klíč (*master key*), který je použit pro odvození klíčů relacee.

- *Authentication Tag* – obsahuje autentizační data, která zabezpečují zejména pořadové číslo paketu a brání útoku zopakováním paketu (*replay attack*).

Je třeba si uvědomit, že SRTP MKI a *Authentication Tag* nejsou zabezpečeny.

14.4 SRTCP

SRTCP (*Secure RTCP*) poskytuje stejné zabezpečení pro RTCP, jak poskytuje SRTP pro RTP. Na rozdíl od SRTP obsahuje zápatí SRTCP navíc ještě položku SRTCP index, která obsahuje pořadové číslo SRTCP paketu.

14.5 Bezpečnost v 3GPP sítích

[89] definuje dva typy zabezpečení pro media plane:

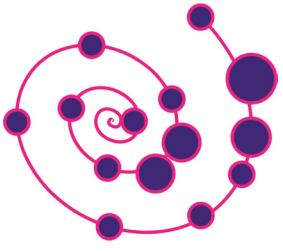
- e2ae (*End-to-access edge security*) – tímto termínem se míní zabezpečení media plane (RTP/RTCP) mezi mobilním zařízením a hranou sítě operátora (A-SBC).

- e2e (*End-to-end security*) - tímto termínem se míní zabezpečení media plane (RTP/RTCP) mezi koncovými účastníky (mobil – mobil).

Běžně se používá zabezpečení e2ae. Pro ustanovení hlavního klíče SRTP zabezpečení musí mobilní zařízení podporovat protokol SDES [70] a volitelně mohou podporovat protokol KMS (*Key Management Service*) [89].

14.6 Útoky na RTP

Útok	Popis	
Muž uprostřed	RTP Replay Attack	Běžící elace je zachycena útočníkem a pakety jsou zopakovány (musí být změněno alespoň pořadové číslo). Pro obranu se používá SRTP ve spojení se sledováním pořadového čísla skutečně přijatého paketu, tj. jestli pořadové číslo přijatého paketu je v souladu s očekávaným číslem paketu.
	RTP Injection	Během RTP relace útočník vloží (i třeba zaplaví) RTP relaci vlastními pakety.
	RTCP BYE	Útočník může do běžící relace vložit paket RTCP BYE, čímž relaci ukončí.
	Odposlechnutí relace	V případě, že relace není zabezpečena (SRTP/SRTCP), pak muž uprostřed může vcelku bez problému relaci odposlechnout. Např. programem wireshrk je možné relaci zaznamenat a uložit k pozdějšímu přehrání.
DoS, DDoS	RTP (UDP) packet flooding	Zahlcení (libovolnými) RTP pakety
RTP media spamming attack	Spam over telephony	Viz kap. 9.9



15. Photuris

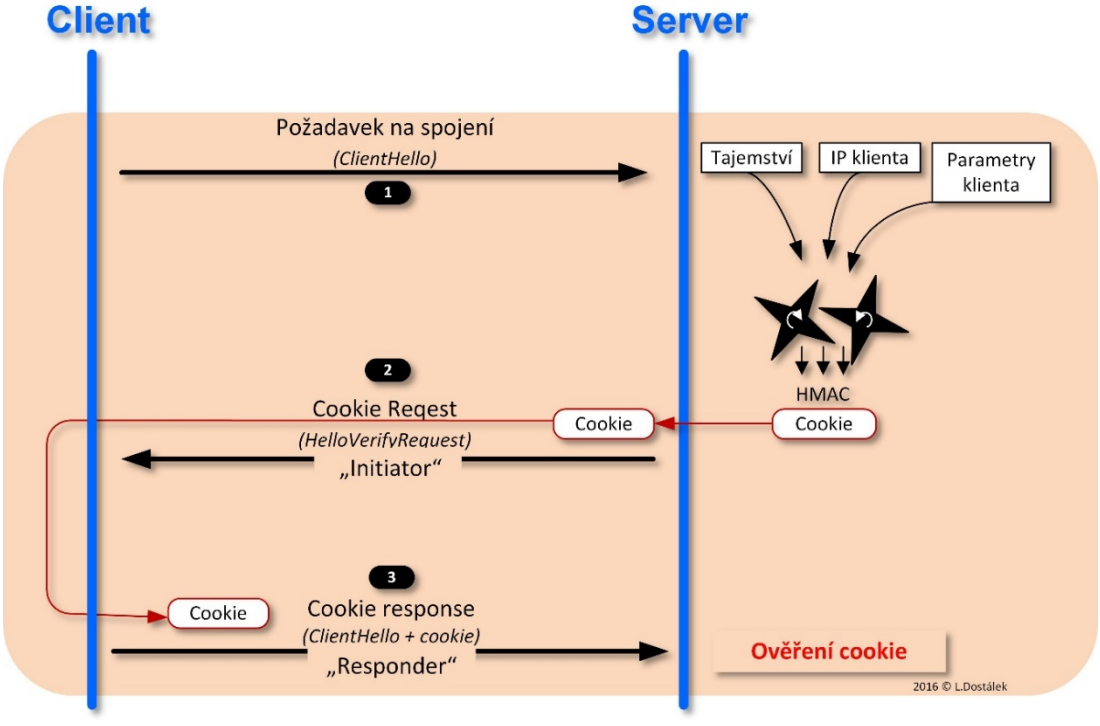
Photuris je latinský název rodu severoamerických světlušek, jejichž dospělé samičky napodobují světelné signály jiných druhů světlušek, aby přilákaly jejich samečky, a pak je sežraly.

Protokol Photuris [90] byl vtvořen pro dnes již zapomenutá zařízení. Zůstal z něj nápad na způsob obrny proti DoS (DDoS) útokům pomocí cookie, které mj. využívají protokoly DTLS (viz kap. 16) a SCTP (viz kap. 17).

Klasický útok na protokol TCP je *SYN flood attack*. Při tomto útoku útočník útočí na server TCP pakety s nastaveným příznakem SYN. Server okamžitě alokuje datové struktury pro navázání komunikace. Jestliže je paketů s nastaveným příznakem SYN velké množství, tak server může zkolabovat vyčerpáním alokovaných zdrojů.

V případě datagramových služeb je možnost útoku podstatně větší než v případě protokolu TCP. Bylo by tedy dobré útočníka nějak potrápit ještě před tím, než se alokují patřičné zdroje.

Protokol Photuris [90] přišel s řešením, že server vygeneruje cookie, které zašle klientovi, který musí svůj požadavek znovu zopakovat, ale se zkopírovanou cookie. Teprve pak je požadavek např. na zřízení relace akceptován.



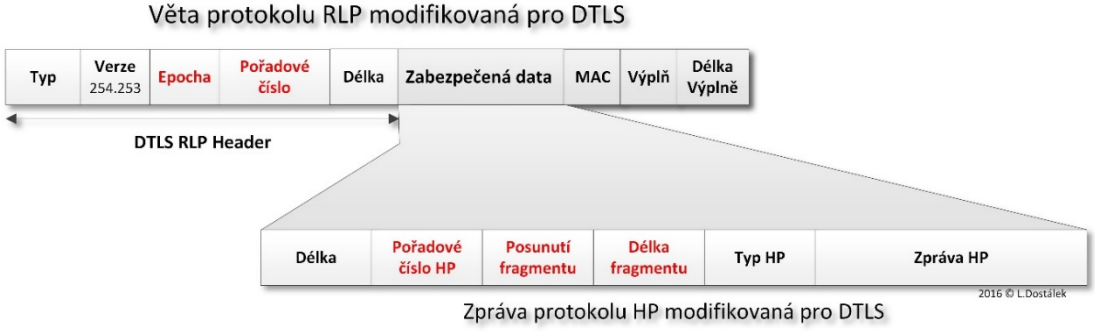
obr. 15.1 Mechanismus cookie (viz DTLS)

To je docela dobrá ochrana proti DoS útokům prováděným z neexistujících nebo falešných IP adres. Z existujících IP adres je možné správně odpovědět, ale vyžaduje to, aby útočník rozuměl danému protokolu.

Systém byl vylepšen tak, že se cookie negeneruje prostým generátorem náhodných čísel, ale server si nejprve vygeneruje tajemství. Vytvoří se struktura, která obsahuje IP adresu klienta a další parametry spojení s klientem. Z této struktury se spočte kryptografický kontrolní součtem MAC (*Message Authentication Code*). Ten se počítá z tajemství a předchozí části struktury např. protokolem HMAC [91]. Jelikož uvedený standard používá zastaralé algoritmy MD-5 a SHA-1, taka se v současné době spíše používá [22] byť se standardy odvolávají na [91].

Protokol DTLS používá tzv. bez stavové cookie, která obsahuje výsledek kryptografického kontrolního součtu. Protokol SCTP používá tzv. stavové cookie, kde cookie tvoří celá datová struktura včetně MAC. DTLS po odeslání stavové cookie de-alokuje všechny datové struktury, které vytvořil na příchozí požadavek a čeká, jestli dostane správnou odpověď (viz kap. 17.6). DTLS

Protokol TLS (*Transport Layer Security*) [29] je velice dobře prověřený protokol, jsou známy útoky na něj [92] atd. Má však jednu nevýhodu – zabezpečuje komunikaci přes TCP protokol. Tj. není určen pro zabezpečení datagramové komunikace. Tento problém řeší protokol DTLS (*Datagram Transport Layer Security*) [93], který modifikuje protokol TLS pro datagramové služby.



obr. 16.2 Věta protokolu RLP a zpráva HP, obě modifikovány pro DTLS (červeně jsou vyznačeny odlišnosti od TLS)

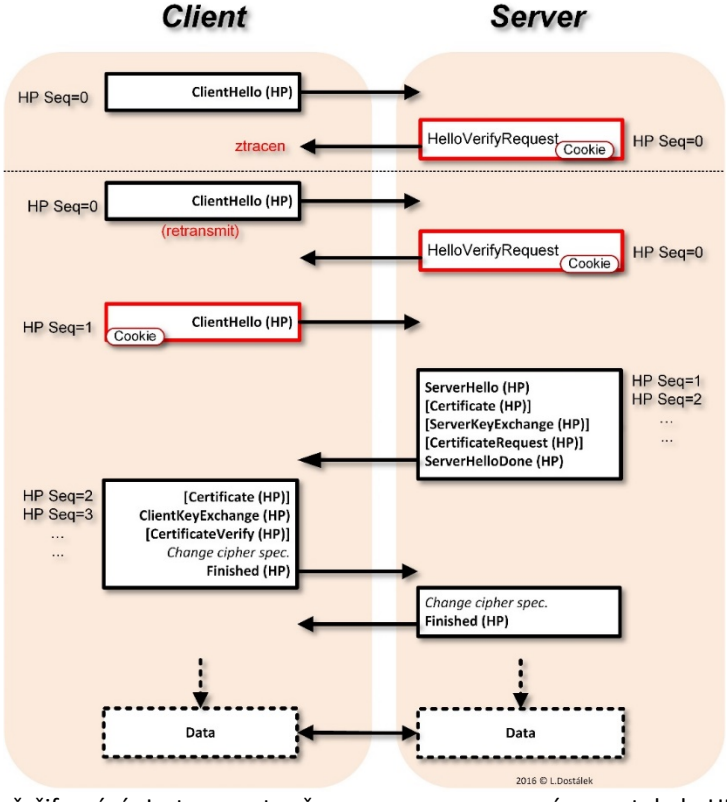
Cílem protokolu DTLS je minimalizovat změny protokolu TLS tak, aby byl uzpůsoben zabezpečení datagramových toků. Vše, co je možné ponechat z TLS, bylo ponecháno.

Hlavní rozdíly oproti TLS:

- Není možné používat proudové šifry (např. RC-4), protože při ztrátě paketu by nebylo možné následující pakety dešifrovat.
- TLS nepotřebuje číslovat pakety, protože TCP zajišťuje jejich plynulé předávání. V terminologii DTLS se říká, že RLP pakety jsou

v TLS implicitně číslovány. Jelikož to v případě datagramového toku neplatí (některé pakety se mohou ztratit), tak je třeba datagramy v toku explicitně číslovat. Čísluje se:

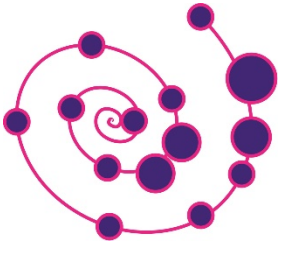
- Jednotlivé věty protokolu RLP (obr. 16.1) se číslují v položce Pořadové číslo. Položka Epocha se mění vždy změně šifrování. Je to z proto, že datagram obsahující změnu šifrování se může ztratit.
- Jednotlivé zprávy protokolu HP se rovněž explicitně číslují. To je také z důvodu, že datagram nesoucí zprávu protokolu HP se může ztratit. Při odeslání zprávy protokolu HP se aktivuje časový čítač, který měří čas došlé odpovědi, pokud odpověď včas nepřijde, tak se zpráva protokolu HP zopakuje. Zopakuje se se původním číslem zprávy protokolu HP. Na obr. 16.2



obr. 16.3 Dialog protokolu HP modifikovaný pro DTLS

se na počátku zpráva ClientHello včas nedočkala odpovědi, tak byla zopakována, ale se stejným číslem HP zprávy (HP seq).

- Zprávy protokolu HP mohou být fragmentovány, proto do záhlaví zprávy protokolu HP byly přidány položky Posunutí fragmentu a Délka fragmentu.
- Jako obrana proti DoS (DDoS) útokům byla zvolena bez stavová cookie. Přibyla tak nová zpráva HelloVerifyRequest, jejímž cílem je zaslat cookie. Klient začíná dialog zprávou Clienthello (obr. 16.2), která neobsahuje cookie, server odpoví zprávou HelloVerifyRequest s cookie. Klient přidá do původní zprávy ClientHello cookie a dialog protokolu HP běží již dálo, jako ho známe z TLS.



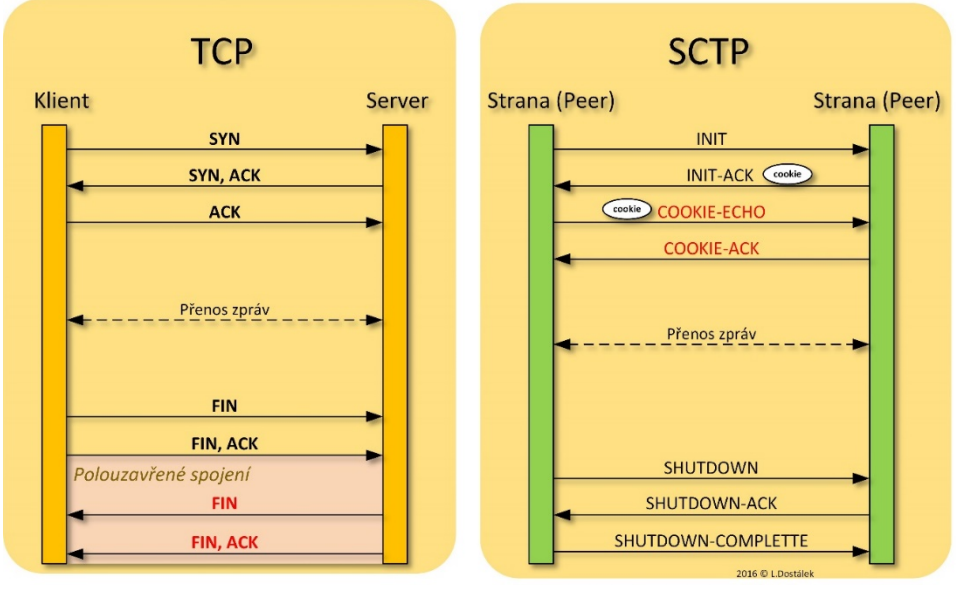
16. SCTP

Protokol SCTP (*Stream Control Transmission Protocol*) [94] je transportním protokolem v rodině protokolů TCP/IP. Od protokolů UDP [25] a TCP [26] se liší v mnoha ohledech. Zejména tím, že určen pro paralelní přenos několika nezávislých datových toků najednou. A také tím, že některé přenášené toky mohou být potvrzované (obdoba protokolu TCP) a jiné nepotvrzované (obdoba protokolu UDP).

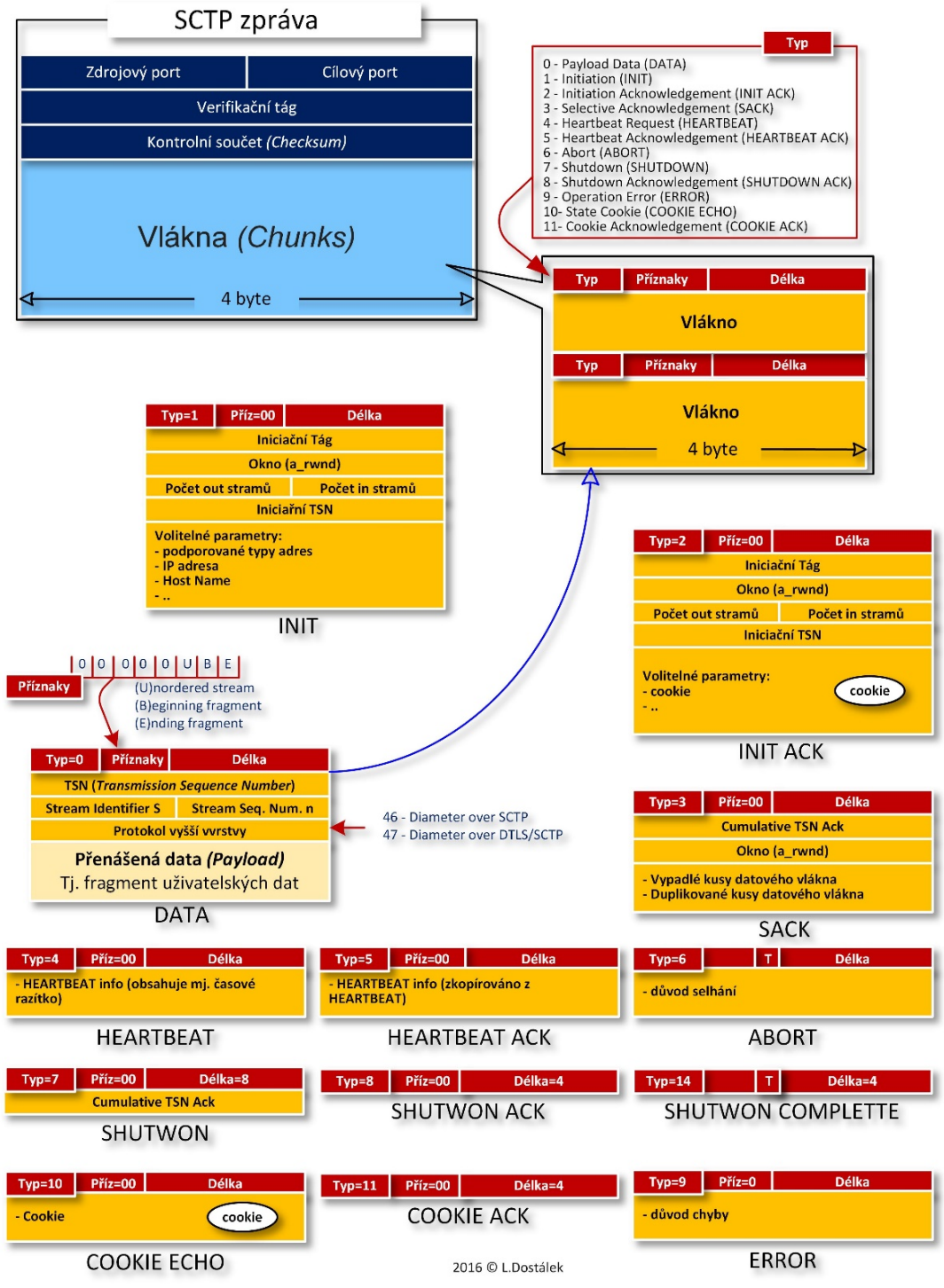
Zatímco protokoly UDP a TCP vytváření spojení typu klient/server, tak SCTP vytváří asociaci mezi dvěma stranami komunikace. Z (obr. 17.1) obrázku je patrné, že navázání spojení je v protokolu TCP pomocí "*three-way handshake*", kdežto asociace SCTP se provádí pomocí "*four-way handshake*". Čtyř paketová asociace je trochu dlouhá, tak poslední dva pakety už mohou nést data.

Vypadá to komplikovaně. Musíme ale vzít v úvahu, pro jaké aplikace protokol SCTP nasazujeme. V případě protokolu TCP koncový účastník i v jedné aplikaci často navazuje protokolem TCP velké množství spojení. Kdežto dva boxy se protokolem SCTP asociují i na značnou dobu, takže když zřízení asociace nějakou dobu potrvá, tak to není příliš na závadu. Protokol SCTP oceníme např. při spojení dvou boxů (např. entit EPC), kdy dojde k asociaci na dlouhou dobu.

Dále v SCTP nemáme žádnou obdobu polozavřeného (chcete-li polootevřeného) spojení. Asociaci ukončuje strana zprávu SHUTDOWN. Kromě toho je ještě možné asociaci abnormálně ukonči zprávou ABORT.



obr. 17.1 TCP spojení a SCTP asociace



obr. 17.2 Zprávy protokolu SCTP

16.1 Asociace

SCTP asociace probíhá v následujících krocích:

1. První strana zahajuje asociaci pomocí zprávy INIT.
2. Druhá strana:
    a. Přijme zprávu INIT.
    b. Pro komunikaci si mezitím vytvořila datovou strukturu TCB (*Transmission Control Block*), která obsahuje nutné informace pro komunikaci s první stranou.
    c. Vytvoří stavovou cookie (viz 17.6), do které z TCB přidá „nutné informace pro komunikaci s první stranou“.
    d. Potvrdí první straně komunikaci zprávou INIT-ACK do které přidá stavové cookie.
    e. Uvolní (de-alokuje) datovou strukturu TCB (obrana proti vyčerpání zdrojů DoS útokem).
3. První strana zkopíruje do své odpovědi COOKIE-ECHO přijaté cookie a vrátí druhé straně.
4. Druhá strana:
    a. Provede verifikaci stavové cookie:
        - Přepočte kryptografický kontrolní součet (MAC) na přijaté stavové cookie.
        - Porovná data (verifikační tág a porty) uvedené ve stavové cookie s aktuálními, jestliže jsou různá, ukončí asociaci.
        - Porovná časové razítko ze stavové cookie s aktuálním časem, jestliže je delší než doba přenosu, ukončí asociaci.
    b. Změní stav asociace na ESTABLISHED.
    c. První straně potvrdí asociaci zprávou COOKIE ACK.

SCTP asociace používá pro identifikaci svého toku mezi stranami identifikátor Verifikační tág (*Verification Tag*), který vyjadřuje, že konkrétní paket protokolu SCTP patří do konkrétní asociace. Každá strana má svůj vlastní verifikační tág.

Datové pakety se vkládají do SCTP zpráv typu DATA. Pro potvrzování přijatých datových paketů se používá zpráva SACK (*Selective Acknowledgement*). Zprávy typu SACK se posílají sousední straně k potvrzování přijatých datových

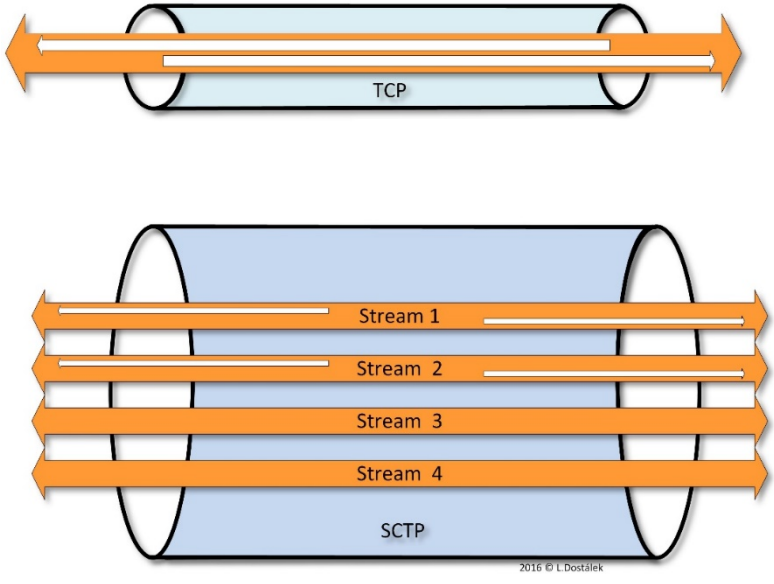
paketů. Dále zprávy typu SACK obsahují informace o nedoručných paketech a duplikovaných paketech.

16.2 Vlákno (*chunk*)

Tok paketů mezi SCTP stranami se skládá z jednotlivých vláken (*chunk*). Každé vlákno pak slouží pro přepravou jednoho aplikačního toku. Tj. více aplikačních toků (každý je reprezentován jedním vláknem) se mixuje do jednoho SCTP toku. Rozeznáváme vlákna potvrzovaná (obdoba protokolu TCP) a nepotvrzovaná (obdoba protokolu UDP).

Pro celý proud SCTP se číslují odeslané SCTP datové pakety pomocí čísla TSN (*Transmission Sequence Number*). Na rozdíl od protokolu TCP, kde se číslují jednotlivé odeslané bajty, tak zde se číslují jednotlivé SCTP pakety.

Aplikační tok vkládá aplikační pakety do konkrétního vlákna. Před odesláním SCTP se může aplikační paket ještě fragmentovat. Jednotlivé aplikační pakety jsou číslovány pomocí čísla SSN (*Stream Sequence Number*). První fragment aplikačního paketu označen příznakem „B“ a poslední fragment příznakem „E“.



obr. 17.3 SCTP Multi-straming

V rámci asociace se strany dohodnou na maximálním počtu vláken (*chunks*) v každém směru, a také na „okně přeplnění“ (*Congestion window* - cwnd), které sousedovi sděluje, kolik bajtů může odeslat před tím, než dostane potvrzení o jejich přijetí.

16.3 Multi- straming

O protokolu SCTP se říká, že je typu „*multi-straming*“. Označuje se tím fakt, že protokolem SCTP můžeme přenášet najednou několik aplikačních

toků – na rozdíl od protokolu TCP (obr. 17.3), který pro každý směr umožňuje jen jeden tok.

Na druhou stranu jeden aplikační tok je vždy přenášen jedním vláknem (*chunk*). Na úrovni protokolu SCTP tak nelze jeden aplikační tok přenášet více vlákny.

tzv. *Multi homing* (obr. 17.4). Jedno rozhraní je označeno jako primární a ostatní jako sekundární. Jestliže komunikace na primárním rozhraní selže, pak se použije sekundární rozhraní. Standard nepředepisuje rozložit komunikaci mezi sousedy přes všechna dostupná rozhraní

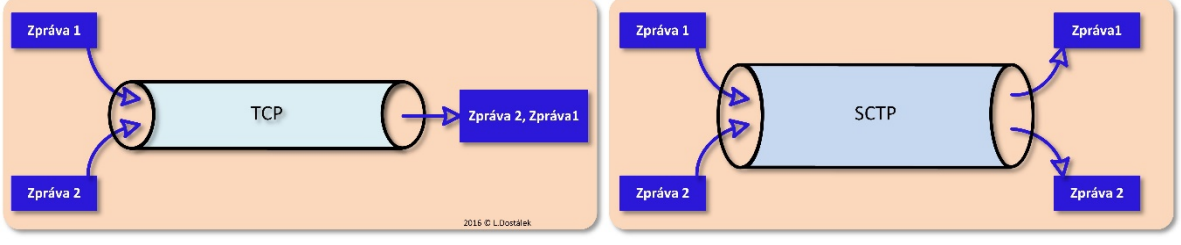
obr. 17.4 SCTP Multi-homing

Důležitou vlastností protokolu SCTP je, že pokud selže doručování jednoho vlákna (*chunk*), tak to nemá vliv na ostatní (paralelní) vlákna. (Pokud by se více aplikačních datových toků mixovalo do jednoho TCP spojení, pak pozastavení jednoho aplikačního toku by znamenalo pozastavení všech toků!)

16.4 Multi-homing

Pro dosažení vysoké spolehlivosti mohou mít strany v protokolu SCTP více síťových rozhraní – (*load balancing*), ale nevylučuje jej, ponechává to na implementaci.

Jestliže je ustanovena asociace mezi sousedy, pak všechna rozhraní jsou periodicky monitorována tak, že strana přes rozhraní odešle zprávu HEARBEAT a očekává odpověď (HEARBEAT-ACK). Počítá dobu, za kterou dostala odpověď (*Round Trip Time* - RTT), pokud přes sekundární rozhraní dostane odpověď rychleji, pak ho vymění s primárním rozhraním.



obr. 17.5 Oddělování zpráv

16.5 Zachování hranic zpráv

Jelikož protokol TCP má jen jeden tok (pro každý směr), tak pokud to protokolu TCP vložíme více zpráv najednou, tak na straně příjemce není mechanismus k oddělení těchto zpráv od sebe. V protokolu SCTP snadno můžeme jednotlivé příchozí zprávy oddělovat – viz obr. 17.5.

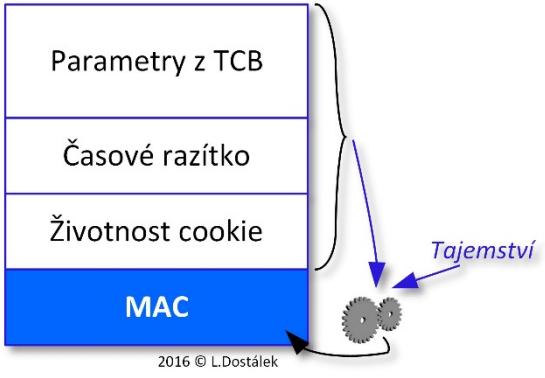
16.6 Ochrana proti DoS, Cookie

SCTP používá k ochraně proti DoS útokům stavové cookie (viz kap. 15). V rámci asociace, po přijetí zprávy INIT, generuje druhá strana zprávu INIT-ACK, do které přibaluje stavovou cookie. První strana pak stavovou cookie kopíruje do své odpovědi COOKIE-ECHO. Druhá strana verifikuje přijeté cookie. V případě, že verifikace proběhla úspěšně, pak stvrdí úspěšnou asociaci zprávou COOKIE-ACK.

Zbývá tedy popsat použité stavové cookie používaná protokolem SCTP (obr. 17.6). Druhá strana musí pro přijetí zprávy vytvořit datovou strukturu TCP (*Transmission Control Block*). Důležité údaje z TCB vloží do položky „Parametry z TCP“ struktury cookie (obr. 17.6). Přidá aktuální časové razítko a dobu, po kterou považuje cookie za platnou.

Datová struktura cooke se nakonec doplní ještě kryptografickým kontrolním součtem MAC (*Message Authentication Code*). Ten se počítá z tajemství a předchozí části struktury např. protokolem HMAC [91]. Jelikož uvedený standard používá zastaralé algoritmy MD-5 a SHA-1, taka se v současné době spíše používá [22] byť se standardy odvolávají na [91].

I když algoritmus HMAC slouží k autorizaci dat mezi entitami, tak v našem případě generuje i verifikuje cookie táž entita (druhá strana). Nemůžeme tedy hovořit o „sdíleném tajemství“, ale jen o „tajemství“. Nicméně to neznamená, že tajemství nemusí být generováno kvalitním generátorem náhodných čísel.



obr. 17.6 Stavová cookie používané SCTP

Jelikož první strana cookie pouze kopíruje, tj. bere ji jen jako řetězec bajtů, tak nemůže ověřit, jestli je správné. Nezbývá tedy jen apelovat na implementace, aby cookie opravdu kvalitně generovaly a ověřovaly (generování i verifikaci provádí táž entita).

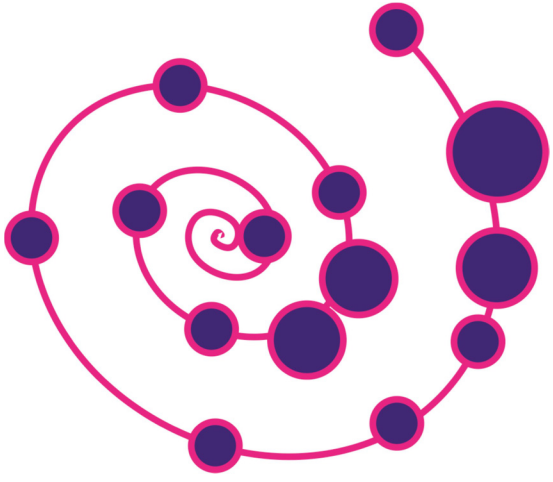
16.7 Autentizace vláken

Pro autentizaci vláken máme k dispozici standard [95], který je rozšířením SCTP. Tento standard předpokládá, že strany mají předem (jiným mechanismem) vyměněno hlavní sdílené tajemství. V rámci asociace si strany vymění náhodná čísla, algoritmus pro výpočet MAC a seznam vláken, která se mají autentizovat. Z vyměněných náhodných čísel a hlavního sdíleného tajemství se pak spočte sdílené tajemství, které bude následně použité pro autentizaci vláken.

SCTP paket se skládá z jednotlivých zpráv patřících vláknům. Zprávy vláken, které se neautentizují, se vloží na počátek SCTP paketu. Ze zbylých zpráv se spočte kryptografický kontrolní součet (MAC), který se vloží do speciální zprávy AUTH (*Authentication Chunk*). Ta se vloží do SCTP paketu za neautentizované zprávy. Nakonec se do SCTP paketu vloží autentizované zprávy, tj. ty ze kterých byl spočten MAC.

16.8 DTLS a SCTP

Pro zabezpečení aplikačních protokolů využívajících SCTP můžeme použít DTLS, jak je popsáno v [96]. Toto zabezpečení nikterak neomezuje aplikace ve využití protokolu SCTP. Příkazy DTLS (*Handshake protocol, ChangeCipherSpec, Alert*) se přenáší vláknem 0. [96] předepisuje, aby byla použita autentizace datových vláken (viz odstavec 17.7). Standard už neuvádí, jestli je možné nebo není využít sdílená tajemství, která byla ustanovena protokolem DTLS.



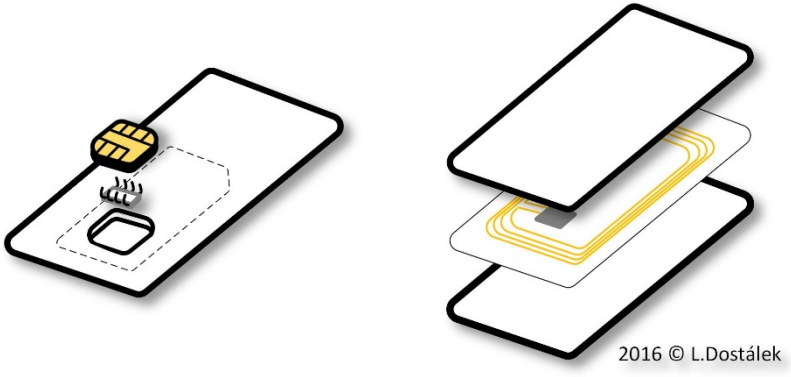
17. Čipové karty

Soukromé klíče, sídelná tajemství či jiný kryptografický materiál tvoří aktiva, která je třeba proti případným hrozbám chránit odpovídajícími opatřeními. Nejjednodušší metodou uložení aktiv je jejich uložení na lokální disk. Nevýhodou ale je, že data lokálního disku lze poměrně snadno zcizit. Nebezpečí ale např. spočívá v aplikacích typu „trojský kůň“, které mohou být schopny zjistit přístupové heslo k aktivu nebo přečíst přímo rozšifrovanou podobu aktiva ve chvíli, kdy je používáno v paměti počítače. Takové trojské koně mohou být staženy např. z internetu nebo získány elektronickou poštou. Jiným způsobem útoku je modifikace aktiva na lokálním disku a řada dalších.

Obdobným problémem je předání počítače (resp. mobilní zařízení) do opravy či přístup administrátorů na tato zařízení. Tady si může být uživatel jist, pouze pokud svá aktiva uloží mimo lokální (neodnímatelné) úložiště – např. na čipovou kartu – a při vydání zařízení z vlastních rukou, fyzicky vyjme tato aktiva ze zařízení.

Nejběžnějším typem ochrany osobních aktiv je jejich uložení do specializovaných hardwarových zařízení, někdy označovaných jako hardwarové klíče (čipové karty, autentizační kalkulátory, HSM apod.)

Autentizačními kalkulátory rozumíme samostatné technické zařízení přímo nepropojené s počítačem, které slouží pro generování jednorázových hesel pro autentizaci držitele kalkulátoru nebo autentizaci dat zasílaných držitelem kalkulátoru. Autentizační kalkulátory jsou tak elektronické pomůcky pro autentizaci klienta (případně pro autentizaci dat zadaných klientem).



obr. 18.1 Kontaktní a bezkontaktní čipová karta

Zatímco autentizační kalkulátory a čipové karty zpravidla slouží pro autentizaci konkrétního uživatele (člověka), tak tak HSM (*Host Security Module*, někdy též *Hardware Security Module*) slouží zejména pro ochranu aktiv serverů, které

často požadují paralelně vykonat velké množství kryptografických operací. HSM moduly jsou specializované zařízení (počítače), které zajišťují také oddělení rolí administrátorů těchto zařízení od rolí pracujících s kryptografickým materiálem, tj. tzv. *segregation of duty*.

Čipová karta *(Integrated Circuit Card - ICC*) je plastiková karta, která má ve svém těle vložen čip. Nejčastější technologii vložení čipu do karty je vyfrézování dutiny v těle karty a následné vlepení čipu s kontakty do této dutiny. V případě bezkontaktních čipových karet se se karta skládá ze dvou těl, mezi která se vloží velice tenký *inlay*, který obsahuje čip a po obvodu několik závitů tvořících anténu (obr. 18.1).

Čipová karta může obsahovat jak kontaktní část, tak i bezkontaktní část. Takové karty nazýváme buď hybridními, nebo duálními:

- Hybridní čipové karty obsahují dva na sobě nezávislé čipy (kontaktní a bezkontaktní).
- Duální čipové karty obsahují jeden čip, který má dva výstupy (kontaktní a bezkontaktní).

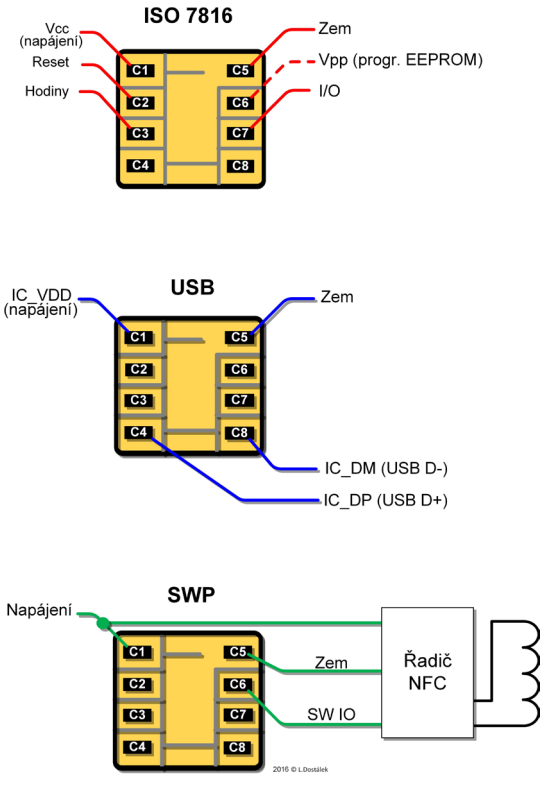
Pro komunikaci s terminálem (čtečkou) nepotřebují bezkontaktní čipové karty galvanický spoj, komunikují pomocí elektromagnetických vln. Napájení rovněž obstará čtečka (terminál) na bázi přenosu energie pomocí indukce. Kontaktní čipové karty mají na sobě kontakty, pomocí kterých se propojují se čtečkou. Napájení rovněž obdrží z terminálu (čtečky) pomocí kontaktů C1 a C5 (obr. 18.2).

V současné době se nejčastěji využívají následující standardy:

- ISO 14443 – standard pro bezkontaktní karty na frekvenci 13,56 MHz pracující přibližně do vzdálenosti 10 cm. Tento standard má historický základ ve firemním standardu firmy Philips Electronics pod označením MIFARE™. Hovorově se proto někdy o těchto čipových kartách stále někdy mluví jako o kartách MIFARE™.
- ISO 15693 – standard pro bezkontaktní karty na frekvenci 13,56 MHz pracující až do vzdálenosti 1-1,5 m.
- ISO 7816 – standard pro kontaktní karty. Nestandardizuje jen kontakty a jejich elektronické vlastnosti, ale i fyzické vlastnosti karet, datové příkazy, aplikační elementy atd. V těchto oblastech se často používá i pro bezkontaktní karty. Tento standard se skládá z následujících částí:
    - ISO 7816-1 specifikuje fyzikální charakteristiky karty (tepelnou odolnost, ohebnost karty, odolnost proti rentgenovému záření, UV záření, elektromagnetickému poli, minimální počet zasunutí karty do čtečky apod.).
    - ISO 7816-2 specifikuje umístění kontaktů na kartě, jejich rozměr a funkci.
    - ISO 7816-3 specifikuje elektrické signály a přenosové protokoly. Specifikuje dále zmíněné protokoly T=0, T=1, až T=15.
    - ISO 7816-4 specifikuje datové příkazy pro komunikaci s kartou, přístupové metody k datům na kartě, zabezpečení komunikace (*secure messaging*) mezi čtečkou a kartou atd.
    - ISO 7816-5 Registrace aplikací

- ISO 7816-6 Aplikační datové elementy
- ISO 7816-7 Příkazy jazyka *Structured Card Query Language* (SCQL)
- ISO 7816-8 Příkazy pro bezpečnostní operace
- ISO 7816-9 Příkazy pro správu karty
- ISO 7816-10 Elektronická signalizace pro synchronní karty
- ISO 7816-11 Osobní identifikace pomocí biometrických metod
- ISO 7816-12 Komunikace s kontaktní kartou s využitím USB
- ISO 7816-13: Příkazy aplikačního managementu muliti-aplikačního prostředí
- ISO 7816-15 Standardní aplikace pro uložení kryptografických informací

- ETSI *(European Telecommunications Standards Institute)* vydala celou řadu standardu pro čipové karty používané zejména v mobilních zařízeních označované jako UICC. Zkratkou UICC (*Universal Integrated Circuit Card*) se označují čipové katy používané v mobilních zařízeních, kde jsou využívané pro autentizaci (přihlášení) účastníka do sítě. Objevily se s 2G sítěmi. Umožnily oddělit mobilní zařízení od jeho autentizace. Účastník tak může vyjmout kartu ze zařízení a vložit ji do jiného zařízení a autentizovat se do sítě z nového zařízení aniž byla nutná asistence poskytovatele sítě. Tj. účastník si může svá osobní aktiva uložená na UICC ze zatížení vyjmout, pokud zařízení vydává ze své moci.
- GlobalPlatform je organizace, kterou založily společnosti zabývající se platebními kartami a mobilními komunikacemi, tj. business, který asi nejvíce využívá čipové karty. Specifikace GlobalPlatform se zabývají zejména správou obsahu karty, komunikací a bezpečností na úrovni aplikací. Specifikace pojmů jako TEE *(Trusted Execution Environment)* nebo SE *(Secure Element)* najdeme právě v jejích dokumentech.
- Mezinárodní organizace pro civilní letectví *(International Civil Aviation Organization - ICAO)* je mezivládní organizace přidružená



obr. 18.2 Kontakty čipové karty dle ISO 7816-2, USB a SWP (pokud vaše „SIMka" má jen 6 kontaktů, tak snadno pochopíte, které chybí)

k OSN, která se kromě civilního letectví zabývá i standardizací cestovních dokladů. Konkrétně její dokument 9303 specifikuje mj. elektronickou část cestovních dokladů. Cestovní doklady nemají tvar čipové karty, ale jejich inlay je „zataven“ buď v datové stránce, nebo v deskách cestovního pasu. Dokument 9303 využívá standard ISO 14443 pro radiovou komunikaci, standard ISO 7816 pro vyšší vrstvy, ale dokument 9303 už nemá žádnou souvislost např. se standardy GlobalPlatform. Dokument 9303 popisuje, jak budou v čipu uloženy základní identifikační údaje držitele a také určuje, jak budou uloženy jeho biometrické údaje a případně další údaje.

- Evropský výbor pro normalizaci (*Comité Européen de Normalisation – CEN*) vydal řadu standardů CEN/TS 15480, které specifikují tzv. Evropskou občanskou kartu (občanský průkaz). Standardy CEN/TS 15480 se odkazují i na dokument 9303. Uvedené normy CEN jsou přeložené do češtiny jako ČSN, ale jsou placené.

Standardy ICAO a CEN jsem uvedl proto, že čas od času někdo přijde s nápadem implementovat cestovní doklady nebo občanský průkaz v „mobilním telefonu“. Je vcelku zjevné, že technicky tomu v podstatě nic nebrání, ale problém je právní, protože mezi vlastníkem mobilního zařízení a držitelem cestovních dokumentů (resp. občanského průkazu) může být velký rozdíl, byť obojí se může nacházet ve stejné kapse kalhot. To už vůbec neuvažuji, že by byl občanský průkaz implementován v eSE *(Embedded Secure Element)* a já potřeboval dát mobil do opravy!

17.1 Kontakty čipové karty

Kontaktní čipové karty mají dle ISO 7816-2 osm kontaktů. Tento standard předepisuje osm plošek C1 až C8 o rozměru 2x1,7 mm, kde musí být umístěny kontakty (viz obr. obr. 18.2). Výrobci pak vytváří kontakty o trochu větším rozměru (zlaté plochy na obr. 18.2) tak, aby tvořily módní design karty.

Podle napájecího napětí (V_{CC}) dělí ETSI TS 102 221 [97] karty do následujících tříd:

- Třída A (V_{CC} mezi 4,5 a 5,5 V). Třída A nepředpokládá využití kontaktů C4 a C8.
- Třída B (V_{CC} mezi 2,7 a 3,3 V), pokud jsou využity kontakty C4 a C8 pro USB interface, pak se pro tyto kontakty použije napěťová třída Inter-Chip USB 3,0 V [98].
- Třída C (V_{CC} mezi 1,62 a 1,98 V) , pokud jsou využity kontakty C4 a C8 pro USB interface, pak se pro tyto kontakty použije napěťová třída Inter-Chip USB 1,8 [98].

Na obr. 18.2 je rovněž znázorněno zapojení kontaktů v případě rozhraní USB [98] a SWP [99]. Rozhraní IC_USB a SWP budou zmíněna později.

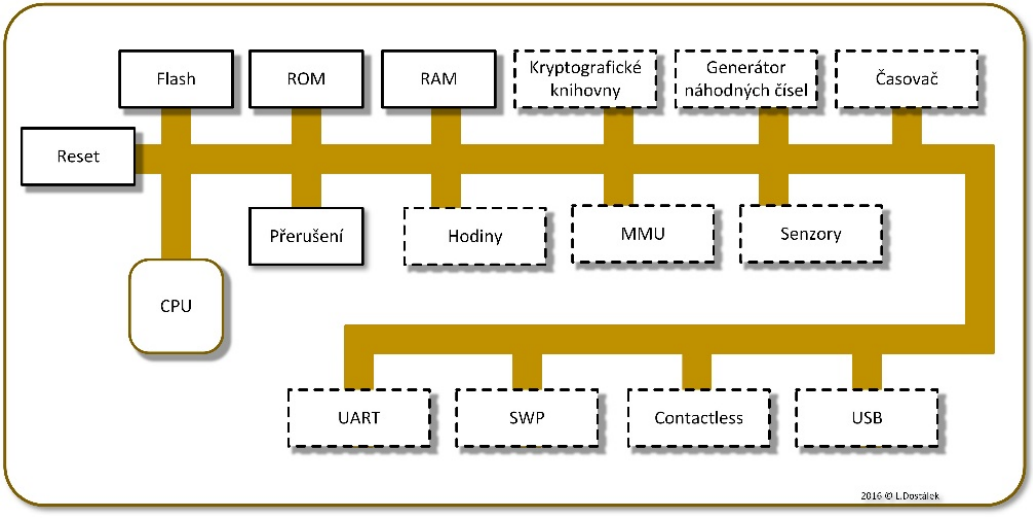
17.2 Logické schéma čipové karty

Nejjednodušší čipové karty byly osazeny pouze paměťovými registry, které je možné nastavovat, přičítat k nim, odečítat od nich apod. Na rozdíl od nich procesorové karty mají kromě paměti i jednočipový procesor schopný vykonávat příkazy. Procesor je řízen operačním systémem karty.

Procesorové čipové karty se mohou skládat z řady modulů (obr. 18.3). Vedle CPU, pak obsahují zejména paměť. V paměti ROM je zpravidla uložen operační systém, který se zavádí do RAM. Data se ukládají do souborových systémů realizovaných v paměti Flash (v minulosti se využívala i paměť EEPROM). V případě, že se čipová karta používá pro autentizaci či autorizaci, pak jsou též důležité kryptografické knihovny. Nejčastější kryptografické knihovny jsou pro algoritmy: DES/3DES, RSA a Eliptické křivky. Čipové karty pak obsahují jednu nebo více těchto knihoven.

- USB (ETSI TS 102 600 [98])
- Bezkontaktní (ISO 14443)
- SWP (ETSI TS 102 613 [99]) pro propojení s řadičem NFC.

Z hlediska spouštění aplikací v čipových kartách můžeme též karty dělit na statické s pevně nahranými aplikacemi (většina firemních operačních systémů jednotlivých výrobců karet) a dynamické, do kterých je možné vkládat nejen data, ale i spustitelný kód. Nejznámějšími technologiemi dynamických karet jsou systémy JavaCard™ či Multos™.

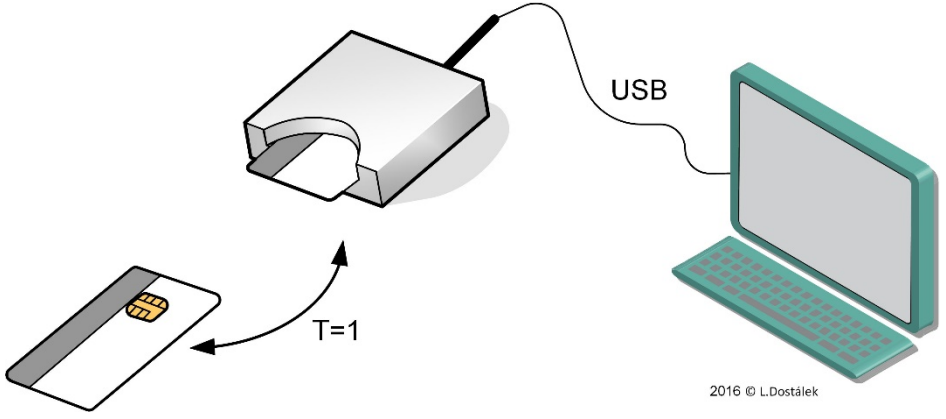


obr. 18.3 Blokové schéma čipové karty

Jak již bylo zmíněno, čipová karta může mít jeden nebo více vstupů/výstupů:

- Sériový vstup/výstup (I/O – ploška C7), k tomu slouží modul UART (*Universal Asynchronous Receiver Transmitter*). Je to jednodrátová obdoba, dnes již nepoužívaných COM portů osobních počítačů.

Pokud se v paměti karty spouští více aplikací, pak modul MMU (*Memory Management Unit*) monitoruje dodržování hranic jednotlivých aplikací v paměti. Před spuštěním každé aplikace jsou totiž stanoveny hranice oblasti paměti, kterou může aplikace využívat. Tuto hranici nelze za běhu aplikace změnit, tj. každá aplikace je zapouzdřená do své oblasti. Bariery na hranicích těchto oblastí se nazývají firewally.



obr. 18.4 Mezi kartou a čtečkou je jeden komunikační protokol (např. T=1) a mezi čtečkou a počítačem je druhý komunikační protokol (např. USB)

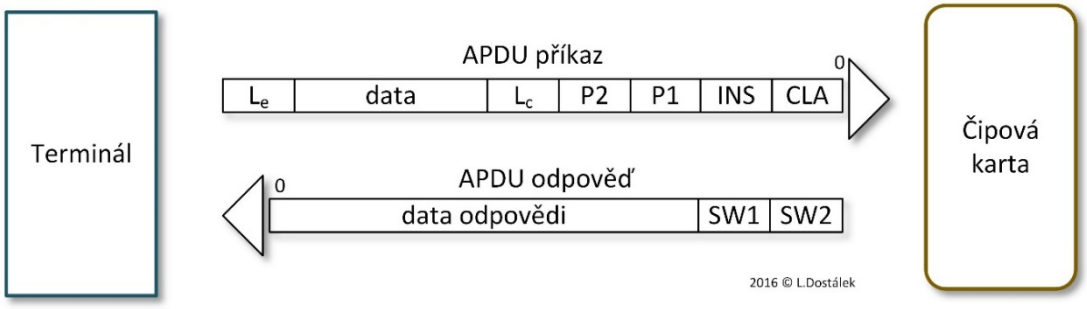
17.3 Terminály

Čtečka čipových karet se správně označuje jako terminál. Jedná se o zařízení, které zprostředkovává komunikaci s čipovou kartou. Terminál může být jako samostatné zařízení, nebo může být propojen např. s počítačem. Pro propojení terminálu s počítačem se často využívá jiný komunikační protokol než ten, který využívá terminál pro komunikaci s kartou. Např. na obr. 18.4 komunikace mezi kartou a čtečkou probíhá protokolem T=1, kdežto čtečka s počítačem komunikuje protokolem USB.

V případě vestavěného terminálu do zařízení se pak použije komunikace po interní sběrnici, např. I^2C, HCI, SPI apod.

Pro zajištění konverze komunikačních protokolů jsou čtečky často realizovány jednočipovým procesorem, což patřičně navyšuje cenu čteček. Nejčastějšími komunikačními protokoly mezi čtečkou a kartou na fyzické vrstvě jsou:

- **T=0** – jedná se o znakově orientovanou polo-duplexní sériovou výměnu dat mezi terminálem a kartou.
- **T=1** - jedná se rovněž o sériový protokol mezi terminálem a kartou, ale tentokrát blokově orientovaný, tj. mezi terminálem a kartou se přenáší data po celých blocích



obr. 18.5 Komunikace APDU příkazy

dat. Tento protokol zrychluje výslednou komunikaci s kartou, avšak karta musí disponovat větší RAM pro vyrovnávací paměti. Dnešní karty umí současně jak protokol T=0, tak i protokol T=1.

- **Bezkontaktní přenos,** někdy hovorově označovaný jako T=CL *(Contact Less)*.
- **USB,** někdy hovorově označovaný jako T=USB. Viz odstavec 18.6.

Velice důležitým parametrem čteček se stává signalizace vytažení karty z terminálu, který se ocení zejména v případě přihlašování k počítači (do Windows, k Linuxu apod.) pomocí čipové karty. V případě vysunutí karty z terminálu automaticky dojde k zablokování stanice. Bohužel mobilní zařízení tento test často nepoužívají.

V případě mobilních telefonů se zpravidla mobilní telefon chápe jako terminál. To pochopitelně neplatí pro NFC.

17.4 ATR

Čipová karta ISO 7816 po svém vložení do terminálu vrací tzv. ATR řetězec *(Answer To Reset)*. ATR je 2 až 33 B dlouhý řetězec, který nastaví již výrobce karty. Na základě ATR je často možné odlišit různé druhy karet, není to však pravidlem. Jestliže má operační systém pracovat s konkrétním typem karty, zpravidla to znamená, že pracuje s kartou o tom a tom ATR řetězci. U ISO 7816 karet se používá jako základní test jejich funkčnosti skutečnost, jestli po přivedení napájecího napětí vrací ATR.

ATR má interní strukturu, ze které lze vyčíst řadu vlastností karty: podporované komunikační (T=0, T=1 atd.), maximální doba čekání v protokolu T=0, maximální velikost bloku pro protokol T=1, maximální frekvenci hodin atd.

U bezkontaktních karet se používá termín ATS *(Answer To Select)*. Význam je obdobný jako ATR.

17.5 APDU

Protokoly na fyzické vrstvě řeší pouze fyzickou komunikaci mezi kartou a terminálem. Nad těmito protokoly se mezi aplikací v počítači/mobilu a kartou přenáší datové pakety nazývané APDU (*Application Protocol Data Unit*). Pomocí APDU se zasílají instrukce kartě, která vrací odpovědi. APDU je nízko úrovňové rozhraní, pomocí kterého již s kartou mohou komunikovat

specializované aplikace v počítači/mobilu, může probíhat personalizace karet apod.

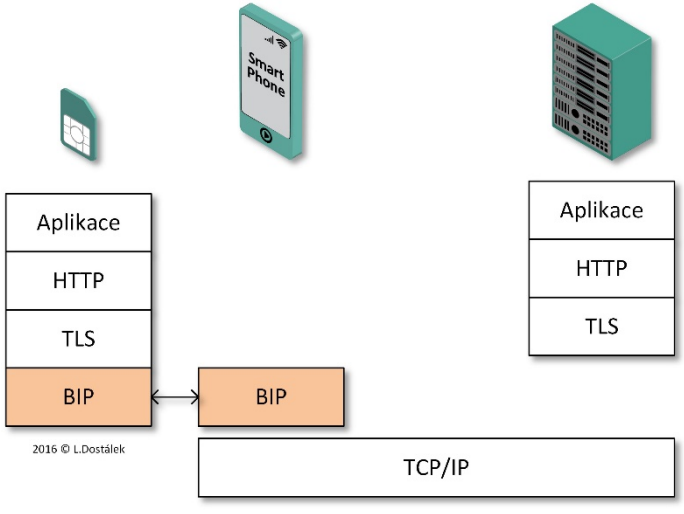
Komunikace APDU příkazy je znázorněna na obr. 18.5, význam jednotlivých polí:

- CLS - třída instrukce (0x80 - proprietární, 0x00 - standardní)
- INS - instrukce
- P1 - parametr 1
- P2 - parametr 2
- Lc - velikost dat (bajty) předávaných do karty v rámci příkazu
- Le - velikost dat očekávaných jako odpověď
- DATA IN - data vstupující do karty
- DATA OUT - data, která jsou výsledkem vykonání příkazu
- SW1,SW2 - návratový kód příkazu (OK nebo indikace chyby)

Příklad příkazu APDU (šestnáctkově): 00 A4 00 00 02 3F 00

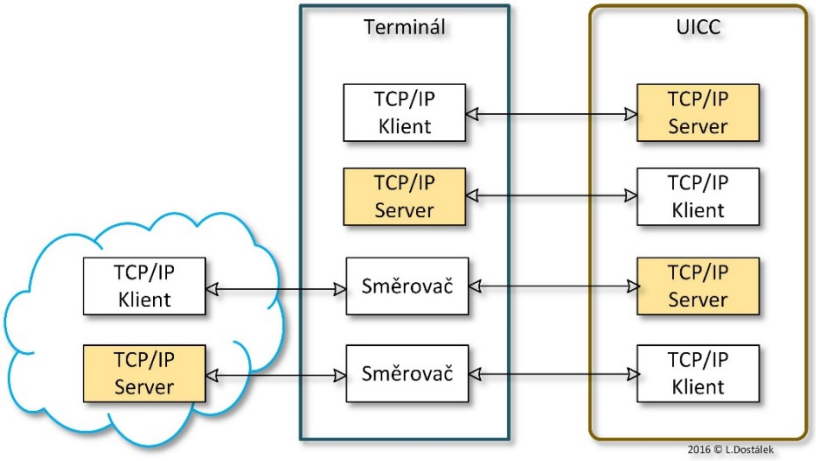
- 00 – třída instrukce (standardní instrukce)
- A4 – instrukce SELECT
- 00 00 – parametry P1 a P2
- 02 – do karty budou předávaný 2B
- 3F 00 – předávána data, konkrétně se jedná o identifikaci souboru, která je 3F00, tj. MF (*Master File*) - Jednalo se tedy o APDU příkaz SELECT MF.

Takto jednoduchá komunikace se používá v případě, že kartu využívá jen jedna aplikace. Dnešní karty podporují komunikaci s více aplikacemi. Pro každou takovou komunikaci se vytvoří mezi aplikací a kartou tzv. logický kanál. V APDU příkazu se pak musí vyjádřit číslo kanálu ke kterému APDU příkaz patří. K tomu se využívá pole CLS (třída instrukce) do které se kóduje číslo logického kanálu. Vždy máme k dispozici základní *(basic)* logický kanál číslo 0. Další logické kanály jsou podle ISO/IEC 7816-4 číslo-



obr. 18.6 Síťový model protokolu BIP

vány od 1 až teoreticky do 19. Tyto logické kanály se otevírají APDU příkazem MANAGE CHANNEL.



obr. 18.7 Architektura klient/server na čipové kartě

Velice důležité je, že pokud se zabezpečuje komunikace mezi kartou a terminálem, pak se zpravidla zabezpečuje na úrovni jednotlivých kanálů APDU příkazem MANAGE SECURE CHANNEL *(Application to Application Security)*. Je možný ale i případ, že se zabezpečuje celková komunikace mezi kartou a terminálem *(Platform to Platform)* – např. pokud karta neumožňuje zřizovat logické kanály, tj. podporuje pouze základní logický kanál 0.

17.6 USB

USB komunikaci mezi kartou a terminálem specifikuje ETSI TS 102 600 [98] (kontakty viz obr. 18.2). Tento standard využívá USB 2.0 s dodatkem *Inter-Chip USB supplement to the USB 2.0 Specification* [100] (dnes existuje i *Inter-Chip Supplement to the USB Revision 3.0 Specification*). Zkráceně se tento standard označuje jako IC USB (dále budu v této publikaci uvádět jen USB).

Při pohledu na obr. 18.2 snadno zjistíme, že kontakty pro USB nekolidují s kontakty ISO 7816. Existují terminály, které podporují USB i ISO 7816. Terminály podporující USB by měly podporovat i ISO 7816 komunikaci. Při zasunutí karty do terminálu pak dojde k volbě komunikačního protokolu. Příslušná procedura je popsána v [98].

USB komunikace mezi terminálem a kartou může být využita dvěma způsoby:

- Čipová karta se chová jako USB zařízení. V tomto případě není třeba používat APDU.
- USB se jen pro přenos APDU příkazů (tzv. APDU přes USB). Tato možnost je vhodná zejména pro již existující aplikace, které jsou postaveny na APDU.

17.7 SWP

SWP *(Single Wire Protocol)* specifikuje standard ETSI 102 613 [99]. Zapojení kontaktů je zobrazeno na obr. 18.2. Při pohledu na tento obrázek snadno zjistíme, že kontakty nekolidující s IC USB kontakty.

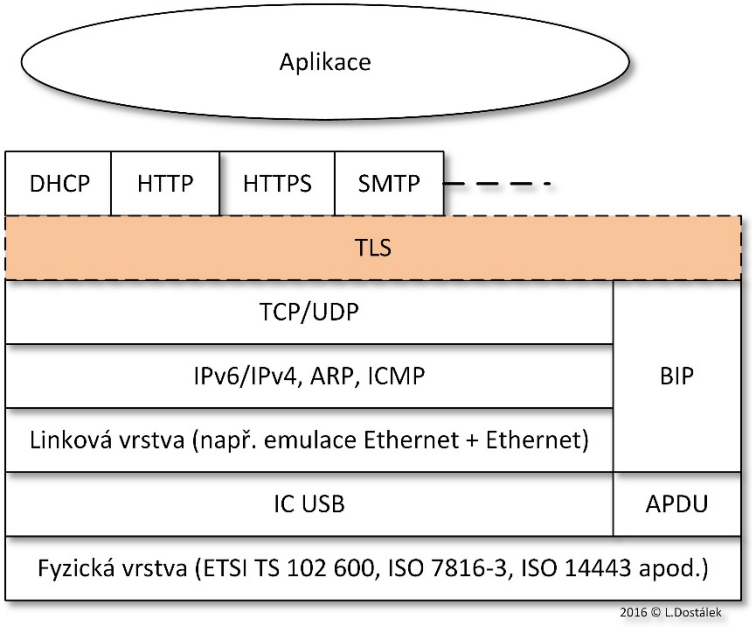
SWP je odvozen od dnes již historického protokolu HDLC *(High-Level Data Link Control).* SWP se využívá pro komunikaci mezi kartou *(secure element)* a řadičem NFC. Tyto dva hardwarové prvky jsou třeba např. pro aplikace emulující bezkontaktní platební karty pomocí mobilního zařízení.

Je třeba ještě dodat, že secure element pro NFC může být implementován i v mikro SD kartě nebo i vestavěn přímo na základní desce mobilního zařízení. V případě mikro SD karty se rovněž používá protokol SWP.

17.8 Emulace Ethernetu

Máme-li připojenou kartu s terminálem pomocí USB, pak emulace protokolu Ethernet přes USB je alternativou k používání APDU příkazů.

Protokol emulace protokolu Ethenrnet přes USB je specifikován v dokumentu *Universal Serial Bus Communications Class Subclass Specification for Ethernet Emulation Model Devices* [101]. Protokol emulace protokolu Ethenrnet přes USB je třeba k vyřešení problému, kterým je, že rámce USB jsou kratší než rámce protokolu



obr. 18.8 Síťový model čipové karty (TLS vrstva je volitelná)

Ethernet. Nezbývá než ethernetové rámce nakrouhat na menší části, které se doplní krátkým záhlavím emulačního protokolu a vloží do USB rámce. Záhlaví emulačního protokolu specifikuje, kterému rámci protokolu Etherent patří který USB rámec.

Máme-li mezi terminálem a kartou komunikaci protokolem Ethernet, pak dalším krokem je vložení IPv4 nebo IPv6 datagramů do těchto rámců. Terminál pak dokonce může pracovat jako směrovač *(router).* Následně může být implementován síťový model TCP/IP (obr. 18.8).

17.9 BIP

BIP *(Bearer Independent Protocol)* [102] je historickým mezičlánkem pro karty, které nemají implementované TCP/IP, ale mají implementovány nějaké aplikační funkce (např. webový server). TCP/UDP komunikace je pak zakončena na terminálu a mezi ním a kartou se pro přenos dat provádí pomocí APDU příkazů OPEN CHANNEL, CLOSE CHANNEL, SEND DATA, RECEIVE DATA a GET CHANNEL STATUS (obr. 18.6). Dalo by se říci, že TCP/IP rozhraní je z karty exportováno do terminálu.

17.10 Webový server

Máme-li na kartě TCP/IP, můžeme implementovat i webový server. Jak je znázorněno na obr. 18.7, tak z hlediska architektury klient/server jsou na čipové kartě přípustné všechny eventuality. Jako server si nyní představíme webový server.

Pro někoho může být překvapivé, že na čipové kartě muže být implementován webový server, který se často označuje zkratkou SCWS *(Smart Card Web Server).* Zajímavé je, že se může jednat i o HTTPS server, tj. server využívající zabezpečení TLS protokolem. Pro autentizaci s předem sdílenými klíči – tzv. TLS PSK, tj. *"Pre-Shared Key Ciphersuites for Transport Layer Security"* [103].

TLS relace může být zřízena nikoliv jen mezi terminálem a kartou, ale i mezi vzdálenou aplikací a kartou. Může být tak vytvořen bezpečný TLS kanál mezi kartou a vzdálenou aplikací. Toho lze využít např. pro vzdálený management karty (kap. 18.15).

17.11 Zabezpečení komunikace s čipovou kartou

ETSI TS 102 484 [104] rozlišuje 4 způsoby zabezpečení komunikace s čipovou kartou. Důležité rovněž je, mezi kterými entitami se zabezpečení realizuje:

- TLS zabezpečení mezi aplikací v čipové kartě a aplikací v terminálu nebo zařízení připojeném lokálně nebo přes IP protokol. Pro toto zabezpečení je nutné, aby čipová karta přímo podporovala IP protokol (např. přes USB) nebo aby alespoň podporovala BIP.
- IPsec mezi terminálem a čipovou kartou. Tato eventualita je možná jen v případě komunikace pomocí USB.
- Zabezpečení protokolu APDU *(Secured APDU)*. Tato možnost připadá do úvahy v případě ISO 7816 karet nebo karet podporujících IC USB v případě, že se jedná o

komunikaci APDU přes USB (nikoliv IP). Zde přichází do úvahy dva případy:

- Zabezpečení komunikace na úrovni logického kanálu, tj. zabezpečení komunikace mezi aplikacemi v terminálu a v čipové kartě *(Application to Application)*.
- Zabezpečení komunikace mezi kartou a terminálem *(Platform to Platform)*. Podpora tohoto typu zabezpečení je zpravidla signalizována v ATR.

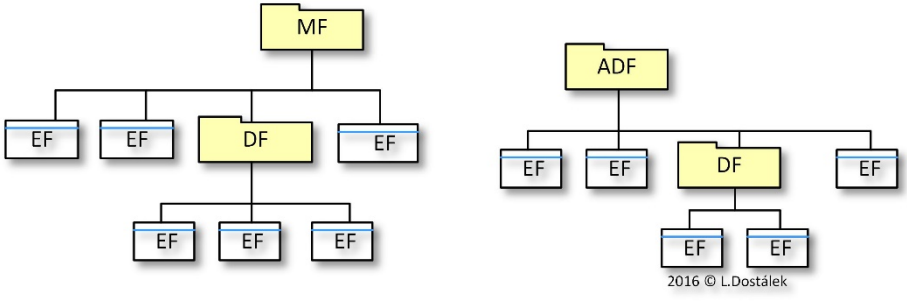
Při vytváření bezpečného kanálu pro zabezpečení protokolu APDU *(Secured APDU)* se nejprve vytvoří zabezpečený kanál, a pak se přenáší data. Při vytváření zabezpečeného kanálu zpravidla dochází i k autentizaci. Protokolů pro zabezpečení kanálu existuje celá řada. Od protokolů na bázi symetrické kryptografie, až pro protokoly na bázi asymetrické kryptografie.

17.12 Struktura dat uložených v kartě

Data uložená na čipové kartě jsou organizována do souborových systémů (obr. 18.9). Na kartě je vždy jeden kořenový adresář nazývaný MF (*Master File*), ve kterém mohou být podadresáře – DF (*Dedicated File*) nebo datové soubory EF (*Elementary File*). Původně už podadresáře nemohly obsahovat další podadresáře. Toto omezení padlo, avšak reálně nebývá vnoření hlubší než 3-4.

Kromě kořenového adresáře MF může být na kartě jeden nebo více ADF *(Application Dedicated File)*. Je to samostatná souborová struktura, která není zavěšena pod MF. ADF je zpravidla určen k uchovávání dat konkrétní aplikace.

EF se dělí na pracovní a interní. Pracovní EF jsou dostupné např. pomocí APDU příkazů i mimo čipovou kartu. Interní EF naopak takto dostupné nejsou (nejsou „viditelné“ mimo kartu). Do interních EF se ukládají např. soukromé klíče, tajné klíče, sdílená tajemství apod. Klasickým příkladem je čipová karta, která pomocí vlastní kryptografické knihovny sama generuje dvojici veřejný a soukromý klíč pro elektronický podpis.



obr. 18.9 Příklad struktury dat na čipové kartě

Soukromý klíč uloží do interního souboru a veřejný do pracovního souboru. Soukromý klíč pak nikdy nepouští kartu.
Konvence pro tvoru názvů souborů jsou uvedeny v tab. 18.1.

tab. 18.1 Názvy soborů na čipové kartě

Typ souboru	**Typ názvu souboru**	**Délka názvu souboru**
MF	FID *(file identifier)*	2B - hodnota vždy '3F 00'
DF	FID	2B
ADF	AID *(application identifier)*	1-16B, AID vznikne sřetězením RID *(Registered application provider Identifier)* a PIX *(Proprietary application Identifier eXtension).* Např.: • RID pro 3GPP je 'A000000087', pro Visa A000000003, pro Mastercard A000000004 atd.- • PIX pro USIM je '1002', pro ISIM je '1004', pro Visa Elektron 2010 atd.
EF	FID	2B
	SFI *(short file identifier)*	5 bitů

Se soubory je možné pracovat např. pomocí APDU příkazů. Soubor nejprve příkazem SELECT vybereme, pak příkazem READ BINARY (nebo READ RECORD) můžeme číst, příkazem UPDATE BINARY (resp. UPDATE RECORD) můžeme modifikovat atd. Zejména při personalizaci karet se provádí APDU příkazy CREATE a DELETE.

17.13 Personalizace a de-personalizace

Slovo personalizace se zde používá ve dvou významech:

- „Personalizace čipové karty" – jedná se o proces, který začíná ukončením výroby dávky čipových karet pro konkrétního zá-

kazníka (vydavatele).. Proces zpravidla postupuje v následujících krocích (operační systém se do karet zpravidla nahrává v rámci jejich výroby):

- Dávka karet a tzv. hlavní transportní klíč jsou předány odběrateli (vydavateli).
- Vyrobené karty jsou zpravidla identické až na číslo karty a tzv. transportní klíč. Tato dávka se v následujícím kroku personalizuje.
- Karty se personalizují zpravidla pomocí robotické linky, kdy kromě vnějšího potisku se rovněž personalizuje i obsah čipu. V čipu jsou vytvořeny souborové systémy, nahrány soubory a kryptografický materiál. Přístup do karty si robotická linka otevírá pomocí transportního klíče. Transportní klíč se zpravidla spočte (derivuje) jednocestnou funkcí z hlavního transportního klíče a čísla karty.
- Po otestování funkčnosti jsou personalizované karty připraveny k vydávání. Personalizace způsobí, že každá karta je jiná – je personalizovaná informacemi o/pro držitele karty.

- „Personalizace mobilního zařízení“ [105] je proces, jehož cílem je omezit krádeže mobilních zařízení. Při personalizaci mobilního zařízení se mobilní zařízení zamkne (přenese se identifikace USIM do mobilního zařízení), aby jej bylo možné používat jen s v něm vloženým USIM. Opačný proces, kdy se mobilní zařízení odemyká, se nazývá de-personalizace. Personalizaci (resp. de-personalizaci) je možné rovněž provádět přes OTA.

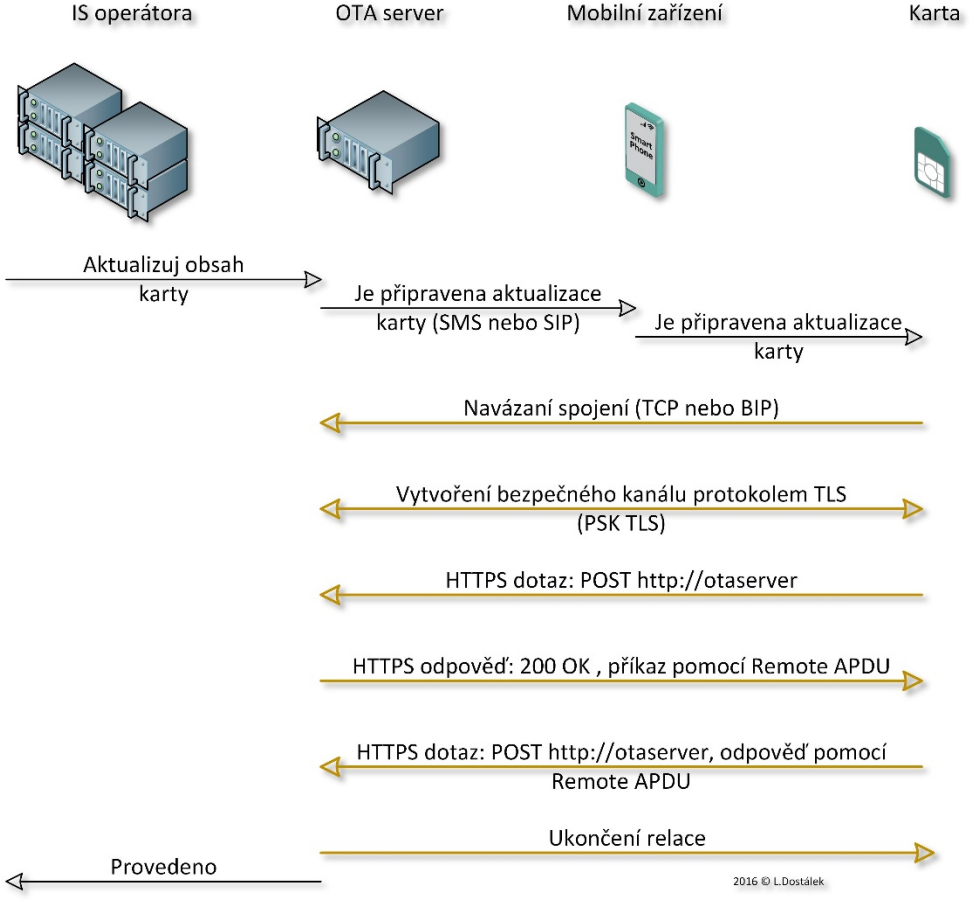
17.14 Řízení přístupu

Máme-li souborový systém, pak, v případě klasických operačních systémů, by následovala kapitola o správě uživatelů a řízení jejich přístupu k souborovému systému. V případě čipových karet je ale filosofie trochu jiná. Nepracuje se zde s uživateli, ale jen s autentizací. Tj. neptáme se, kdo se autentizuje, ale jaký způsob autentizace byl použit. Čipová karta vede seznam přístupových práv k adresářům a souborům, ve kterém je u souboru vyznačeno, jak k němu lze přistupovat za použití konkrétní autentizační metody. Soubory a podadresáře často mohou dědit přístupová práva po rodičích, pokud přístupová práva nejsou specifikována explicitně.

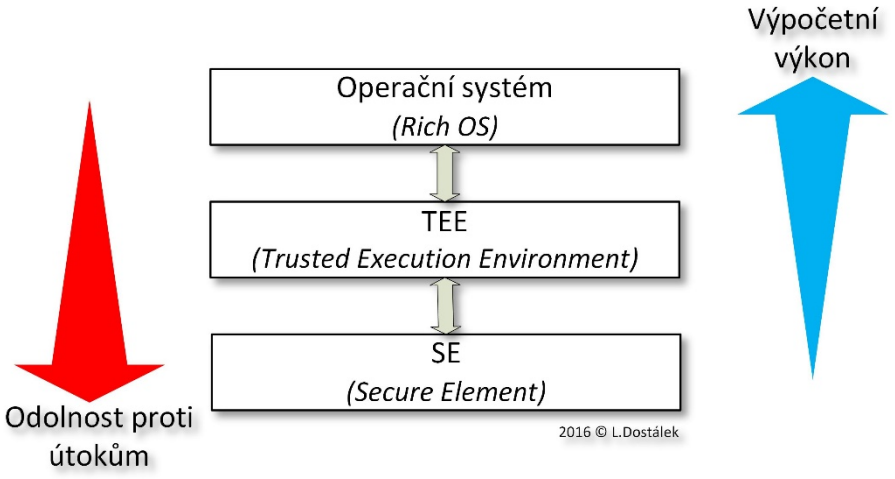
Některé soubory mohou být zcela veřejné, jiné pouze dostupné na základě autentizace. Klasickou autentizací je mechanismus PIN/PUK. Ta je určena pro autentizaci držitele karty. S kartou je však třeba pracovat i v jiných případech, např.:

- Na pobočce operátora, kdy je třeba na kartu nahrát aplikaci nebo obecně nějaká data. Pak je často držitel karty donekonečna vyzýván, aby zadával PIN ke kartě, aniž by věděl, co se s jeho kartou děje. Lepší variantou je, že aplikace s kartou sdílí sdílené tajemství, od kterého lze např. odvodit symetrické šifrovací klíče, na základě kterých dojde k autentizaci mezi kartou a aplikací a uživatel není obtěžován nesmyslným zadáváním PIN. V terminologii odstavce 18.11 se jedná o *Secured APDU*. Častěji se ale tato komunikace zabezpečeným kanálem s kartou označuje jako *Secure Messaging*.

- Při personalizaci karty, kdy personalizační robot (personalizační linka) nahrává na kartu základní struktury, ale často i kryptografický materiál (např. sdílená tajemství pro protokol AKA). Komunikace zde probíhá rovněž zabezpečeně, bezpečný kanál se otevírá mezi robotem a kartou na základě tzv. transportních klíčů, které do karty uložil výrobce karty a v rámci personalizace je bezpečné tyto klíče zlikvidovat. Jedná se tedy rovněž o *Secure Messaging*.
- Asi nejpraktičtější variantou je OTA *(Over The Air)* administrace čipové karty. Ta je možná zejména díky tomu, že zařízení je připojeno k síti, přes kterou může dojít k vzdálenému managementu karty, často aniž to držitel karty tuší.



obr. 18.10 Dialog OTA



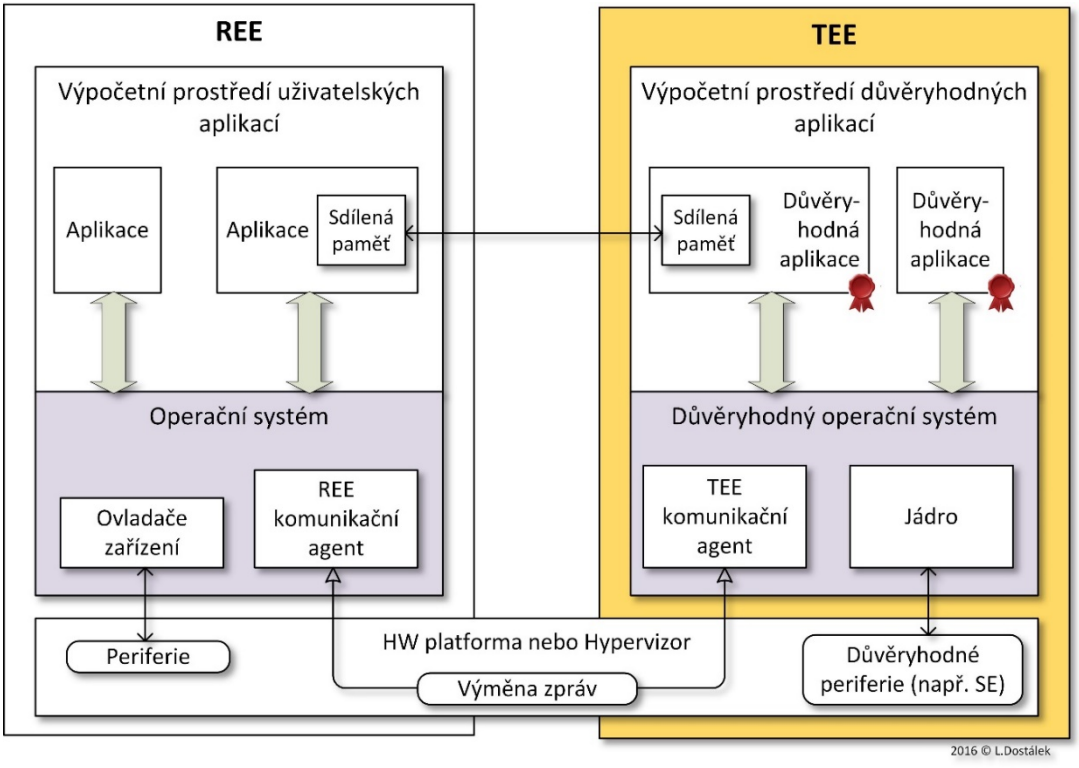
obr. 18.11 Operační systém, TEE a SE

17.15 OTA

OTA *(Over The Air)* je princip, jak vzdáleně spravovat čipovou kartu bez zásahu jejího držitele. Jelikož se jedná o velice praktickou věc, tak byla implementována už ve 2G sítích. V současné době nemáme jeden standard, jak OTA implementovat, ale máme několik standardů, které lze využít. Praktickým důsledkem je, že implementace OTA se liší u jednotlivých operátorů.

Na obr. 18.10 je znázorněna komunikace dialogem OTA:

- Např. pracovník operátora provede změnu v uživatelském profilu klienta. To má za následek, že informační systém operátora vygeneruje požadavek na aktualizaci obsahu USIM klienta.
- Čipové kartě je notifikováno, že na OTA serveru operátora je připraven *Secure* APDU skript pro aktualizaci obsahu čipové karty. Tj. samotná aktualizace se vždy provádí z iniciativy karty, aby se vyhnulo situacím, kdy aktualizace by mohla být pro klienta nákladné, protože je např. v roomingu. Notifikace se provádí buď specializovanou SMS nebo pomocí SIP INVITE.
- Čipová karta naváže spojení s OTA serverem (jedná se webový server), spojení zabezpečí pomocí TLS PSK. Pokud karta přímo nepodporuje TCP/IP, pak se využije BIP.
- Pomocí HTTP metody POST se přenese Secure APDU skript, který karta následně vykoná. Secure APDU skript obsahuje jednotlivé APDU příkazy. APDU komunikace je postavena na odeslání APDU příkazu do karty a přijetí odpovědi. Pokud chceme odeslat blok příkazů (tj. skript), pak je třeba popsat jednotlivé příkazy. Tj. co je příkaz,



obr. 18.12 Příklad architektury karty podle GlobalPlatform – převzato z [136]

co parametry atd. K tomu se využije BER-kódování (známe jej např. z certifikátů veřejných klíčů). BER-kódování každou informaci kóduje do trojce: typ informace (*Type*), délka (*Length*) a hodnota (*Value*). V případě bloků APDU příkazů (tj. APDU skriptů) se říká, že jsou ve TLV formátu.

- Na závěr se ukončí spojení a IS operátora je notifikován výsledek operace.

17.16 Architektura karet podle GlobalPlatfom

Jedná se o architekturu z hlediska aplikací a komunikace mezi nimi. Z terminologického hlediska už nebudeme mluvit o čipové kartě, ale o SE *(Secure Element)*, který může být implementován jako čipová karta, mikro SD karta nebo může být implementován přímo na základní desce mobilního zařízení *(*tzv. *Embedded Secure Element – eSE)*. UICC od doby 3G sítí je zpravidla implementováno jako SE na čipové kartě.

GlobalPlatform rozděluje výpočetní systém mobilního zařízení do tří vrstev (obr. 18.11):

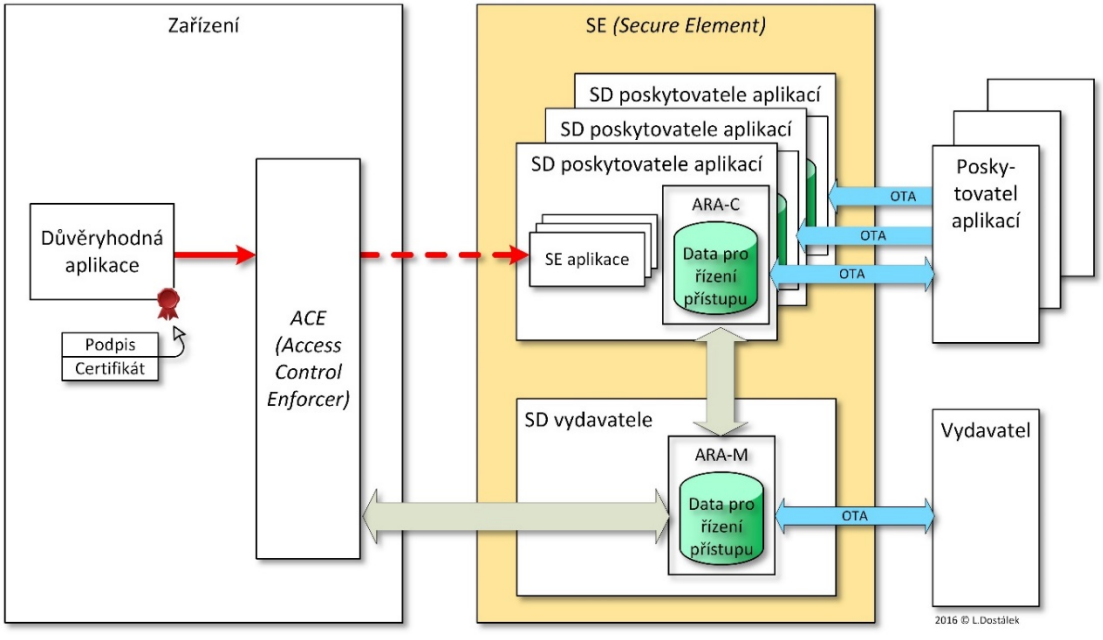
- Operační systém *(Rich OS)*, např. Android, Windows apod. Toto výpočetní prostředí se označuje jako REE *(Rich Execution Environment).*
- TEE *(Trusted Execution Environment)* - oddělené výpočetní, které běží vedle operačního systému a je od něj odděleno pomocí řízené komunikace.
- SE *(Secure Element)* – HW prostředek pro bezpečné ukládání kryptografického materiálu a dalších datových aktiv a provádění operací s ním.

Pod jedním operačním systémem může být implementováno více TEE. Rovněž SE může být více.

17.17 REE a TEE

Na obr. 18.12 je znázorněn jednoduchý příklad architektury REE a TEE. V prostředí TEE mohou být spouštěny pouze důvěryhodné aplikace. Jejich důvěryhodnost je stvrzena elektronickým podpisem, který se ověřuje pomocí certifikátu veřejného klíče vydaného důvěryhodným vydavatelem.

Komunikace mezi aplikacemi běžícími v REE a důvěryhodnými aplikacemi běžícími v TEE probíhá řízeně formou zpráv. Důvěryhodná aplikace



obr. 18.13 Komunikace s SE (SD = bezpečnostní doména)

má přístup do sdílené paměti aplikace běžící v REE.

Čipové karty (tj. SE) mohou být připojeny jako k TEE, tak ale i jako periferie k REE (viz kap. 18.18).

17.18 SE

SE je hardwarově realizované zařízení, které je „bezpečné“ proti útokům. Z hlediska bezpečnosti máme v SE následující typy bezpečnostních zón *(Security Domains)*:

- Zóna vydavatele karty *(Issuers' Security Domain)*, která povinně musí byt implementována v GlobalPlatform kartách.
- Zóny poskytovatelů aplikací *(Application Providers' Security Domain)*, kde každý z partnerů vydavatele karty má svou vlastní bezpečnostní zónu.
- Zóny poskytovatelů globálních služeb karty *(Controlling Authorities' Security Domains)*. Takovou aplikací je např. verifikace držitele karty (např. pomocí PIN).

Každá bezpečnostní zóna je zodpovědná za bezpečnostní zprávu svých aplikací a rovněž za příslušný kryptografický materiál. Tj. dochází k separaci bezpečnosti i kryptografického materiálu jednotlivých zón.

SE může být připojeno jak k TEE, tak i k REE. V případě připojení k REE (resp. k systému, který nehraje na REE a TEE) se vyžaduje komunikace pomocí bezpečného kanálu (SECURE CHANNEL). V následujícím textu nebudu proto používat ani termín TEE, ani REE, ale prostě jen zařízení.

Na obr. 18.13 je znázorněn příklad komunikace aplikace běžící v zařízení s aplikacemi v SE. Vydavatel karty má k dispozici management bezpečnostních domén, tj. může zřizovat, modifikovat a rušit bezpečnostní domény pro poskytovatele aplikací.

Vydaný SE podporuje tři typy komunikací [106]:

- Řízení přístupu aplikací.
- Přístup jednotlivých důvěryhodných aplikací běžících v zařízení k SE.
- Management karty přes OTA.

17.18.1 Řízení přístupu aplikací

V zařízení zajišťuje řízení přístupu k SE komponenta ACE (*Access Control Enforcer*). Pokud požaduje důvěryhodná aplikace přístup k SE, pak ACE si načte ze SE Data pro řízení přístupu. Data pro řízení přístupu obsahují přístupová pravidla pro přístup k ADF, která se skládají z heše z certifikátu veřejného klíče a vlastních pravidel. Pravidla mohou platit pro všechny ADF nebo jen pro některé ADF.

Data pro řízení přístupu poskytuje ACE aplet ARA *(Access Rule Application).* Jelikož v SD mohou být kromě bezpečnostní domény vydavatele i domény poskytovatelů aplikací, tak každá bezpečnostní doména má svůj aplet ARA. ARA aplet v bezpečnostní doméně vydavatele je master – označuje se jako ARA-M. Jednotlivý poskytovatelé aplikací pak mají aplet ARA-C (C od *Client*). ACE vždy komunikuje jen s ARA-M, který si vyžádá informace od jednotlivých klientů (ARA-C).

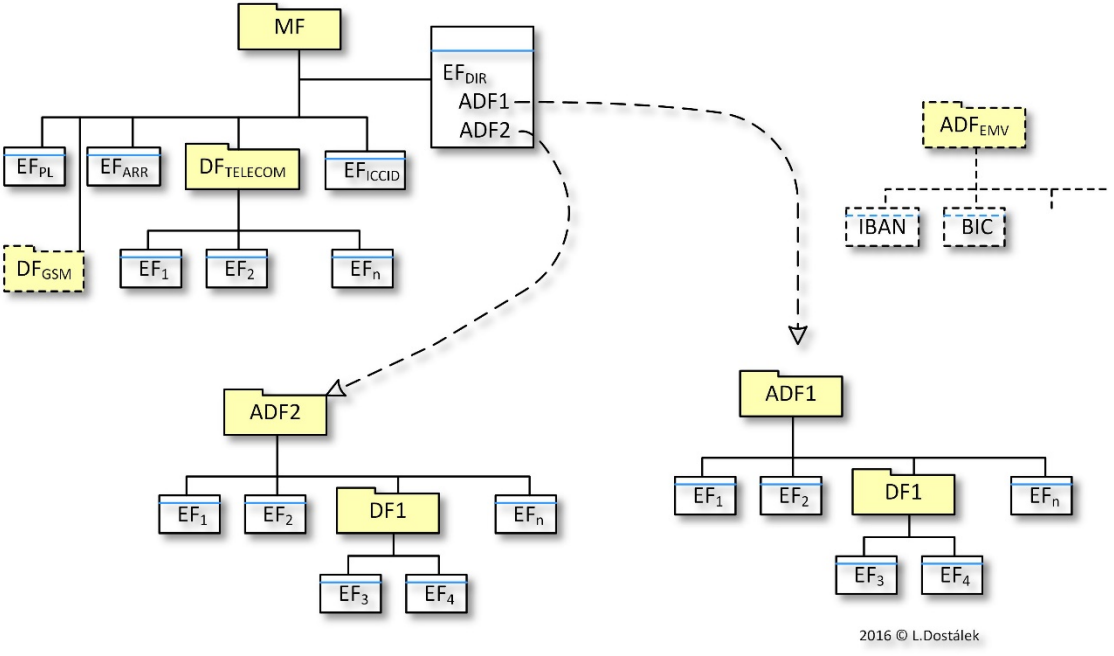
Pro úplnost jen dodám, že v datech pro řízení přístupu mohou být, kromě přístupových informací k jednotlivým ADF, také přístupové informace spojené s událostmi od NFC řadiče.

17.18.2 Přístup jednotlivých důvěryhodných aplikací

O přístupu jednotlivých aplikací k SE rozhoduje ACE, který má skrze ARA-M načteny přístupové informace pro jednotlivá ADF. Aplikace je elektronicky podepsána a je k dispozici i certifikát veřejného klíče, kterým se elektronický podpis ověřuje. Podle heše z certifikátu se naleznou příslušná přístupová pravidla. Podle těchto pravidel ACE buď aplikaci přístup umožní, nebo neumožní.

17.19 UICC

Zkratkou UICC se označují čipové karty pro mobilní zařízení. V poslední době jsou zpravidla realizovány jako SE *(Secure Element)*. UICC byly zavedeny ve 2G a dodnes s ohledem na zpětnou kompatibilitu obsahují i soubory pro podporu 2G. UICC obsahuje MF (kořenový adresář) ve kterém je kromě podpory 2G i EF_{DIR}, který obsahuje odkazy na ADF. Zejména na ADF obsahující



obr. 18.14 UICC (IBAN= International Bank Account Number, BIC= Bank Identifier Code)

strukturu USIM, případně na ADF obsahující struktury ISIM (muže jich být více).

UICC může obsahovat i další ADF, např. obsahující strukturu platební karty [107]. Ve struktuře USIM i ISIM nemusí být realizovány všechny teoreticky možné soubory. SimAliance vydala doporučení, ve kterém specifikovala dva profily pro nejběžněji vydávané karty: UICC1 a UICC2 (tab. 18.2).

tab. 18.2 Profily UICC1 a UICC2

Vlastnost	**UICC1** (doporučený)	**UICC2** (prémiový)
Autentizace do EPS (tj. LTE)	X	X
Autentizace do GSM	X	X
Autentizace do IMS	X	X
Podpora i-WLAN		X
Rozšíření USIM Toolkit	X	X
OTA administrace	X	X
GBA *(Generic bootstrapping architecture)*		X
EAP *(Extended Authentication Protocol)*	X	X
Podpora NFC		X
Podpora HeNB *(Femtocell) – viz kap. 4.1*	X	X
Optimalizace LTE roaming	X	X
Další vlastnosti	-	X

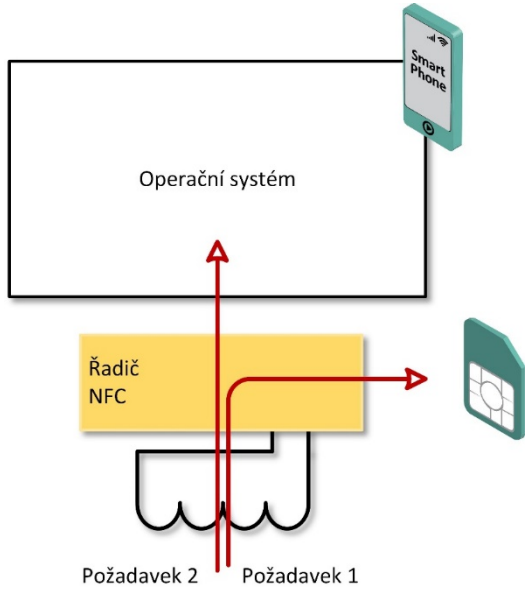
Na obr. 18.14 je znázorněna struktura karty. Důležité je ale si uvědomit, že se jedná pouze o strukturu pracovních souborů. Interní soubory zde zobrazeny nejsou. Interní soubory budou obsahovat zejména data pro zabezpečení karty a aplety. Zejména:

- Data pro management bezpečnostních zón (obr. 18.13)
- Pro management karty např. přes OTA.
- Přístupová práva (PIN/PUK, kryptografický materiál pro *Secure Messaging* atd.)

17.19.1 EAP

Dnes je již asi opuštěná představa, že by operátor mohl poskytovat kromě připojení pomocí LTE i konektivitu pomocí WiFi, přitom by mohla být využita stávající infrastruktura operátora (musely by být doinstalovány WiFi AP). Mluvilo se o tzv. i-WLAN (*Interconnect* WLAN). Vznikla k tomu celá řada norem popisující řadu referenčních bodů (zpravidla jejich název začíná písmenem W).

Pro autentizaci měl být využit protokol EAP *(Extended Authentication Protocol)* [108], který



obr. 18.15 Řadič NFC směruje příchozí požadavky

patří do rodiny protokolů PPP. Existují standardy EAP-AKA [109] a EAP-AKA' [110], které specifikují využití autentizačního mechanismu AKA pro autentizaci EAP. Zajímavé je, že i profile UICC1 (tab. 18.2) tento způsob autentizace podporuje. Je to tedy autentizační metoda, na kterou bychom neměli zapomínat. Možná, že by se dala zkombinovat i s OAuth 2.0 (kap. 20.3.3).

17.19.2 NFC

NFC *(Near Field Communications)* není předmětem této publikace, ale přece jenom považuji za nutné něco k NFC poznamenat. Nejprve je nutné ale sdělit, že si nesmíme NFC spojovat pouze s platebními kartami – jedná se o komunikační protokol pro bezkontaktní komunikaci na krátké vzdálenosti využívající mj. standard ISO 14443. Tj. může být např. implementován pomocí nejrůznějších samolepek na zboží, ale i např. na mobilním zařízení apod. Pochopitelně, že samolepka nebude obsahovat SE.

Přicházející požadavky do řadiče NFC směruje řadič NFC (obr. 18.15) do příslušné aplikace. Aplikací může být aplikace v SE, ale i např. v operačním systému mobilního zařízení. Směrování se provádí na základě identifikátoru aplikace AID. V případě, že je žádoucí události od řadiče NFC zpracovávat jak v SE, tak i v operačním systému, pak je třeba mít správně nastavenu směrovací tabulku NFC.

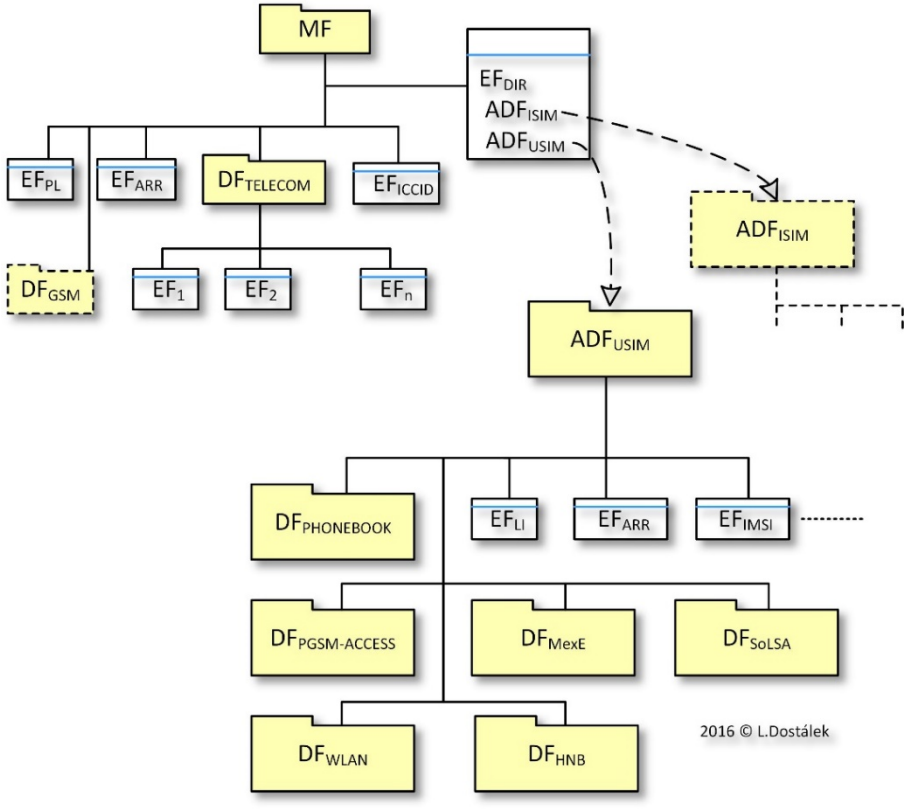
Pokud je zpracování události směrováno aplikaci o konkrétním AID v SE, pak aplet ARA zjišťuje, zdali v datech pro řízení přístupu je příslušných pravidlech uvedeno, že tato konkrétní aplikace (o konkrétním AID) má povoleno zpracovávat události od NFC řadiče.

Zajímavé je, že je možné, aby řadič NFC i SE byly v případě vypnutí mobilního zařízení napájeny z bezkontaktního terminálu, tj. NFC platební kartou emulovanou v mobilním zařízení pravděpodobně půjde platit, i když operační systém nepoběží (tj. zařízení bude „vypnuto").

17.20 USIM

Na obr. 18.16 je znázorněna struktura karty s ADF USIM. Důležité je ale si uvědomit, že se jedná pouze o strukturu pracovních souborů. Interní soubory zde zobrazeny nejsou. Interní soubory budou obsahovat zejména kryptografický materiál:

- Pro management karty např. přes OTA.



obr. 18.16 USIM

- Sdílená tajemství K.
- Přístupová práva (PIN/PUK, kryptografický materiál pro *Secure Messaging* atd.)
- Data pro řízení přístupu důvěryhodných aplikací.

Dále musí být na kartě uloženy applety.

Jak v ADF USIM, tak i v ADF ISIM je důležitý soubor EF_{UST} (v případě ISIM se jedná o soubor EF_{IST}), který obsahuje tzv. servisní tabulku. V servisní tabulce je vyznačeno, které služby jsou kartou podporovány. Služby jsou číslovány od nº1 dále (v tab. 18.3 pravý sloupec). Pokud příslušná služba podporována není, pak ani EF nesoucí data pro tuto službu na kartě být nemusí.

Autentizace účastníka do sítě se provádí APDU příkazem AUTHENTICATE. Tento příkaz lze provést v několika různých kontextech. Zejména:

- *„3G Security context“* – klasické využití AKA mechanismu:
  - Vstup: RAND, AUTN (AUTN = SQN ⊕ AK ‖ AMF ‖ MAC).

- Výstup: RES, CK, IK

- *„GBA security context (Bootstrapping Mode)“* – viz kap. 19.2.
  - Vstup: RAND, AUTN* (AUTN* = SQN ⊕ AK ‖ AMF ‖ MAC*, kde MAC* = MAC⊕ Trunc(SHA-1(IK)), ke Trunc je funkce, která vyřízne prvních 64 bitů)
  - Výstup: RES (GBA_U kryptografický materiál odvozený od IK a CK je uložen v interním souboru)
- *„GBA security context (NAF Derivation Mode)“* – viz kap. 19.2.
  - Vstup: NAF_ID, IMPI
  - Ks_NAF

tab. 18.3 Význam jednotlivých EF pod ADF USIM

Soubor (nezávazný název)	**Název EF**	**Význam**	**Služba**
EF_{LI}	'6F05'	Seznam uživatelem/operátorem preferovaných jazyků	
EF_{IMSI}	'6F07'	Obsahuje IMSI *(International Mobile Subscriber Identity)*	
EF_{Keys}	'6F08'	Obsahuje CK, IK a KSI (viz algoritmus AKA – kap. 6)	
EF_{KeysPS}	'6F09'	Obsahuje CK_{PS}, IK_{PS} a KSI_{PS} pro doménu PS *(Packet Switched)* - viz kap. 4.3	
$EF_{PLMNwAcT}$	'6F60'	Seznam uživatelem preferovaných mobilních sítí (PLMN) včetně jejich přístupové technologie (GSM, UTRAN, E-UTRAN, CDMA2000,…). Priorita sítě je dána pořadím PLMN v seznamu	nº20
EF_{HPPLMN}	'6F31'	Interval vyhledávání PLMN o vyšší prioritě	
EF_{ACMmax}	'6F37'	Maximální hodnota ACM *(Accumulated Call Meter)*. ACM obsahuje maximum kumulované hodnoty hovorových jednotek aktuálního volání a všech předešlých volání.	nº13
EF_{UST}	'6F38'	Servisní tabulka aplikace USIM	
EF_{ACM}	'6F39'	Aktuální hodnota ACM, viz EF_{ACMmax}	nº13

EF_{GID1}	'6F3E'	Identifikátor skupiny úrovně 1, může být použit pro identifikaci skupinu USIMů pro konkrétní aplikaci	nº17
EF_{GID2}	'6F3F'	Identifikátor skupiny úrovně 2, může být použit pro identifikaci skupinu USIMů pro konkrétní aplikaci	nº18
EF_{SPN}	'6F46'	Název poskytovatele v textové formě *(Service Provider Name)*	nº19
EF_{PUCT}	'6F41'	Cena za jednotku a tabulka měn *(Price per Unit and Currency Table)*	nº13
EF_{CBMI}	'6F45'	Identifikátor CBC, viz referenční bod SGc *(Cell Broadcast Message identifier selection)*	nº15
EF_{ACC}	'6F78'	Třída (priorita) přístupu účastníka k síti *(Access Control Class)*. Tříd je 15, z toho prvních 10 pro běžné uživatele. Ve zbytku mj. je: • 15 – údržba (zaměstnanci) mobilní sítě, • 14 – záchranná služba, • 13 - veřejné sítě (dodavatelé plynu, vody atp.), • 12 – bezpečnostní složky.	
EF_{FPLMN}	'6F7B'	Seznam mobilních sítí, ke kterým mobilní zařízení neposílá požadavek na připojení *(Forbidden PLMNs).*	
EF_{LOCI}	'6F7E'	Obsahuje následující lokalizační údaje: • *Temporary Mobile Subscriber Identity (TMSI);* • *Location Area Information (LAI);* • *Location update status.*	
EF_{AD}	'6FAD'	Obsahuje tzv. mód obsluhy v závislosti na typu USIM. Např. mód '04' *„cell testing"* je určen pro testování buňky před tím, než se základnová stanice uvede do komerčního provozu. Mód '00' je mód pro běžnou obsluhu atd.	
EF_{CBMID}	'6F48'	Obsahuje identifikátor typu zpráv, které mají být stahovány z CBC do USIM. Viz EF_{CBMI}	nº29
EF_{ECC}	'6FB7'	Obsahuje seznam nouzových volání	
EF_{CBMIR}	'6F50'	Obsahuje interval identifikátorů typu zpráv (CBC), které mají být akceptovány mobilním zařízením.	nº16

EF_{PSLOCI}	'6F73'	Obsahuje následující lokalizační údaje: • *Packet Temporary Mobile Subscriber Identity (P-TMSI);* • *Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);* • *Routing Area Information (RAI);* • *Routing Area update status*	
EF_{FDN}	'6F3B'	Obsahuje seznam čísel (nebo prefixů čísel) na které je možné volat. Konkrétně může se jednat o: • FDN *(Fixed Dialling Numbers)* – seznam čísel (resp. prefixů čísel) na které je možné volat • SSC (*Supplementary Service Control strings*) – řetězce identifikující doplňkové služby (viz kap. 4.8). Jedná se např. o rodičovskou ochranu dětí, aby jim bylo umožněno volat jen na konkrétní čísla (chráněno PIN2)	nº2 nebo nº89
EF_{SMS}	'6F3C'	SMS a jejich parametry	nº10
EF_{MSISDN}	'6F40'	Obsahuje MSISDN	nº21
EF_{SMSP}	'6F42'	Parametry SMS služby (adresa SMS centra, kódování dat atp.)	nº12
EF_{SMSS}	'6F43'	SMS status (např. příznak, že paměť pro SMS je vyčerpána)	nº10
EF_{SDN}	'6F49'	Obsahuje seznam kódů servisních služeb a doplňkových servisních služeb, na které je možné volat (viz kap. 4.8).	nº4 nebo nº89
EF_{EXT2}	'6F4B'	Obsahuje rozšiřující údaje k EF_{FDN}	nº3
EF_{EXT3}	'6F4C'	Obsahuje rozšiřující údaje k EF_{SDN}	nº5
EF_{SMSR}	'6F47'	Obsahuje status reporty (např. informace o doručení) SMS uložených v EF_{SMS}	nº11
EF_{ICI}	'6F80'	Obsahuje informace o příchozím hovoru (mj. telefonní číslo, datum a čas, délku hovoru, odkaz do adresáře atp.)	nº9
EF_{OCI}	'6F81'	Informace o odchozím hovoru, obdoba EF_{ICI} pro odchozí hovor	nº8
EF_{ICT}	'6F82'	Obsahuje časoměřič příchozího hovoru	nº9

EF_{OCT}	'6F83'	Obsahuje časoměřič odchozího hovoru	nº8
EF_{EXT5}	'6F4E'	Obsahuje rozšíření k souborům EF_{ICI}, EF_{OCI} a EF_{MSISDN}	nº44
EF_{CCP2}	'6F4F'	Umožňuje nastavit parametry sítě pro služby specifikované v EF_{FDN}, EF_{BDN}, EF_{MSISDN}, EF_{SDN}, EF_{ICI}, EF_{OCI}, EF_{MBDN} a EF_{CFIS}	nº14
EF_{eMLPP}	'6FB5'	eMLPP (*enhanced Multi Level Precedence and Pre-emption*) je vlastnost sítě, která umožňuje nastavit a řídit prioritu volání (např. volání dispečera železniční sítě). Tento EF obsahuje úroveň priority, která může být využita účastníkem.	nº24
EF_{AaeM}	'6FB6'	Pro každou úroveň priority eMLPP je v tomto souboru nastavena akce zpracování příchozího hovoru *(Automatic Answer for eMLPP Service)*	nº25
$EF_{Hiddenkey}$	'6FC3'	Obsahuje klíč, kterým se lze autentizovat k přístupu k položkám adresáře (tj. telefonní seznam), které jsou označeny jako skryté	
EF_{BDN}	'6F4D'	Seznam blokovaných doplňkových služeb (viz kap. 4.8).	nº6
EF_{EXT4}	'6F55'	Obsahuje rozšíření k EF_{BDN}	nº7
EF_{CMI}	'6F58'	Obsahuje rozšíření k EF_{BDN}	nº6
EF_{EST}	'6F56'	Obsahuje seznam povolených služeb, viz EF_{UST}	nº2, 6, 34 nebo 35
EF_{ACL}	'6F57'	Seznam povolených APN, viz obr. 4.6.	nº35
EF_{DCK}	'6F2C'	Obsahuje de-personalizační klíče pro OTA de-personalizaci	nº36
EF_{CNL}	'6F32'	Obsahuje seznam tzv. kooperujících mobilních sítí, který se při personalizaci mobilního zařízení nahraje do mobilního zařízení.	nº37
$EF_{START-HFN}$	'6F5B'	Pro zabezpečení komunikace mezi mobilním zařízením a základnovou stanicí se používají klíče IK a CK. IK a CK je třeba po čase obnovovat. Tento EF obsahuje aktuální množství dat,	

		která byla již používanými klíči IK a CK zabezpečena. Tato hodnota se označuje jako START (po dalším zapnutí mobilního zařízení).	
$EF_{THRESHOLD}$	'6F5C'	Pro zabezpečení komunikace mezi mobilním zařízením a základnovou stanicí se používají klíče IK a CK. IK a CK je třeba po čase obnovit. Tento EF obsahuje maximální množství dat (práh), kterým je možné těmito klíči zabezpečit.	
$EF_{HPLMNwAcT}$	'6F62'	Seznam domovských mobilních sítí (HPLMN) a jejich přístupových technologií. Priorita HPLMN je dána pořadím v seznamu.	nº43
EF_{NETPAR}	'6FC4'	Obsahuje informace o frekvencích používaných v buňce *(Network Parameters)*	
EF_{PNN}	'6FC5'	Obsahuje plné a krátké jméno mobilní sítě, ve které je registrován *(PLMN Network Name)*	nº45
EF_{OPL}	'6FC6'	Obsahuje prioritní seznam TAI - *Tracking Area Identity (Operator PLMN List)*	nº46
EF_{MBDN}	'6FC7'	Obsahuje telefonní číslo hlasové schránky, elektronické pošty a dalších služeb *(Mailbox Dialing Numbers)*	nº47
EF_{EXT6}	'6FC8'	Obsahuje rozšíření EF_{MBDN}	
EF_{MBI}	'6FC9'	Obsahuje texty k telefonním číslům hlasové schránky, elektronické pošty a dalších služeb *(Mailbox Identifier)*	nº47
EF_{MWIS}	'6FCA'	Obsahuje stavové informace k telefonním číslům hlasové schránky, elektronické pošty a dalších služeb – např. počet nepřečtených zpráv *(Message Waiting Indication Status)*	nº48
EF_{CFIS}	'6FCB'	Indikátor přesměrování hovorů *(Call Forwarding Indication Status)*	nº49
EF_{EXT7}	'6FCC'	Obsahuje rozšířeni EF_{CFIS}	
EF_{SPDI}	'6FCD'	Seznam poskytovatelů mobilních sítí *(Service Provider Display Information)*	nº51
EF_{MMSN}	’6FCE’	Nastavení notifikace MMS *(MMS Notification)*	nº52

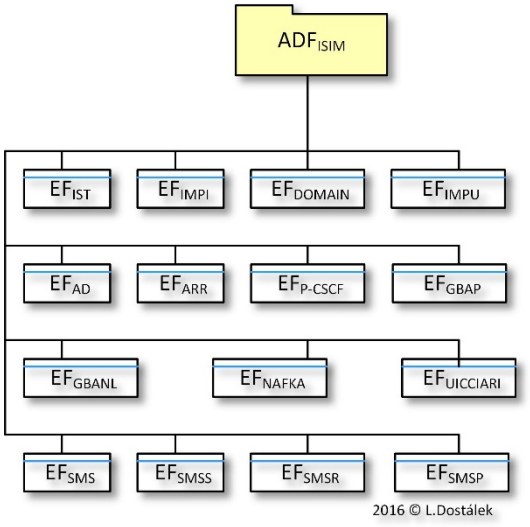
EF_{EXT8}	'6FCF'	Obsahuje rozšíření EF_{MMSN}	nº53
EF_{MMSICP}	'6FD0'	Obsahuje seznam síťových nastavení pro přenos MMS *(MMS Issuer Connectivity Parameters)*	nº52
EF_{MMSUP}	'6FD1'	Obsahuje uživatelské nastavení pro zpracování MMS *(MMS User Preferences)*	nº52
EF_{MMSUCP}	'6FD2'	Obsahuje uživatelem nastavených parametrů pro přenos MMS *(MMS User Connectivity Parameters)*	nº52 nebo nº55
EF_{NIA}	'6FD3'	Indikace zpráv doplňkových služeb (viz kap. 4.8).	nº56
EF_{VGCS}	'6FB1'	Obsahuje identifikátor hlasové konference, do které je účastník zapojen *(Voice Group Call Service)*	nº57
EF_{VGCSS}	'6FB2'	Status hlasové konference – např. aktivována, deaktivována *(Voice Group Call Service Status)*	nº57
EF_{VBS}	'6FB3'	Seznam lokálních vysílání do kterých s účastník přihlásil *(Voice Broadcast Service)* - zastaralé	nº58
EF_{VGCSCA}	'6FD4'	Šifrovací algoritmus hlasové konference *(Voice Group Call Service Ciphering Algorithm)*	nº64
EF_{VBSCA}	'6FD5'	Šifrovací algoritmy lokálních vysílání *(Voice Broadcast Service Ciphering Algorithm)*	nº65
EF_{MSK}	'6FD7'	Kryptografické klíče pro hlasové konference a lokální vysílání *(Multimedia Broadcast/Multicast Service Keys List)*	nº69
EF_{MUK}	'6FD8'	Uživatelské kryptografické klíče pro hlasové konference a lokální vysílání *(Multimedia Broadcast/Multicast User Keys List)*	nº69
EF_{GBANL}	'6FDA'	GBA: seznam NAF_ID a B-TID *(GBA NAF List)*	nº68
EF_{EHPLMN}	'6FD9'	Seznam ekvivalentních domácích mobilních sítí *(Equivalent HPLMN)*, který umožňuje poskytovat více kódů domácích mobilních sítí. Položky tohoto seznamu mohou nahrazovat i kódy mobilní sítě odvozený z IMSI.	nº71
$EF_{EHPLMNPI}$	'6FDB'	Názvy ekvivalentních domácích mobilních sítí *(Equivalent HPLMN Presentation Indication)*	nº71 a nº73

$EF_{LRPLMNSI}$	'6FDC'	Indikace poslední mobilní sítě ve které byl účastník registrován *(Last RPLMN Selection Indication)*	nº74
EF_{NAFKCA}	'6FDD'	GBA: *NAF Key Centre Address*	nº68 a nº76
EF_{SPNI}	'6FDE'	Odkazy na loga poskytovatelů *(Service Provider Name Icon)*	nº78
EF_{PNNI}	'6FDF'	Odkazy na loga sítí *(PLMN Network Name Icon)*	nº79
EF_{NCP-IP}	'6FE2'	Parametry pro IP konektivitu USIM *(Network Connectivity Parameters for USIM IP connections)*. Může obsahovat APN (viz obr. 4.6), uživatelské jméno, heslo, IPv6 prefix apod.	nº80
$EF_{EPSLOCI}$	'6FE3'	Obsahuje lokalizační údaje sítě LTE *(EPS location information)*: *- Globally Unique Temporary Identifier (GUTI);* *- Last visited registered Tracking Area Identity (TAI);* *- EPS update status.*	nº85
EF_{EPSNSC}	'6FE4'	*EPS NAS Security Context (K_{ASAME}, uplink count, downlink count atd.)*	nº85
EF_{UFC}	'6FE6'	Možnosti USIM *Application Toolkit (USAT Facility Control)*	
$EF_{NASCONFIG}$	'6FE8'	Konfigurační parametry protokolu NAS *(Non Access Stratum Configuration)*	nº96
$EF_{UICCIARI}$	'6FE7'	Seznam identifikátoru IARI *(IMS Application Reference Identifier)*, tj. identifikátorů IMS aplikací - používá se při SIP REGISTER	nº95
EF_{PWS}	'6FEC'	Konfigurační parametry pro veřejný poplachový systém *(Public Warning System)*	nº97

tab. 18.4 DF pod ADF USIM

$DF_{PHONEBOOK}$	'5F3A'	Tento DF je určen pro adresáře (telefonní seznamy). Může obsahovat globální adresář, i aplikační adresáře.	

$DF_{GSM-ACCESS}$	'5F3B'	Tento DF obsahuje informace pro USIM aplikace, které jsou schopny využívat přístup přes GSM síť.	nº27
DF_{MexE}	'5F3C'	Tento DF obsahuje data pro tzv. *Mobile Execution Environment* (MExE). Poté, co mobilní zařízení začaly využívat operační systémy, se toto prostředí opustilo.	nº41
DF_{WLAN}	'5F40'	Tento DF obsahuje EF pro WLAN, tj. mj.: • Dočasný identifikátor účastníka (pseudonym) • Preferovaná mobilní síť pro WLAN • Operátorem delfínová preferovaná mobilní síť pro WLAN • Seznam uživatelem preferovaných WLAN, tj. seznam WSID. • Operátorem definovaný seznam preferovaných WLAN, tj. seznam WSID. • Autentizační sekvence (zapamatovaná z předchozího přihlašování) • Seznam preferovaných WLAN domovské sítě • Poslední síť, ve které byl účastník registrován	nº59, nº60, nº61, nº62, nº63, nº66, nº81, nº82, nº83, nº84 nebo nº88
DF_{HNB}	'5F50'	Tento DF obsahuje data pro HeNB (viz kap. 4.1). Mj. obsahuje: • Název HeNB • Tzv. *Allowed CSG List* (CSG = *Closed Subscriber Group*), tj. seznam povolených účastníků ve Femtocell.	nº86 nebo nº90
DF_{SoLSA}	'4F30'	Operátor může definovat oblast jistého počtu buněk LSA *(Localized Service Area)* s konkrétními charakteristikami. Operátor v rámci LSA definuje charakteristiky této oblasti sítě. Tento DF obsahuje EF s definovanými charakteristikami LSA.	nº23



obr. 18.17 ISIM

17.21 ISIM

ADF ISIM není běžně na UICC, ale může tam jich být i více.

Do IMS aplikací se lze přihlásit i pomocí USIM. Pokud se přihlašujeme do IMS pomocí USIM (bez ISIM), tak nám bude na čipové kartě chybět zejména veřejná identita (IMPU). Další nevýhodou je, že budeme používat stejné sdílené tajemství K jak pro přihlašování do EPS, tak i do IMS. To je nepříjemné zejména v případě, že EPS a IMS poskytují různí poskytovatelé.

Na obr. 18.17 je znázorněna struktura pracovních EF v ADF ISIM. Tabulka tab. 18.5 pak obsahuje popis jednotlivých EF. Je zde uvedena i servisní tabulka v EF_{IST}. Jelikož ADF ISIM má výrazněji jednodušší strukturu, tak bylo možné uvést celý obsah servisní tabulky.

Autentizace účastníka do sítě se provádí APDU příkazem AUTHENTICATE. Tento příkaz lze provést v několika různých kontextech. Zejména:

- „IMS AKA security context" – *obdoba „3G Security context"* – klasické využití AKA mechanismu:
  - Vstup: RAND, AUTN (AUTN = SQN ⊕ AK ‖ AMF ‖ MAC).
  - Výstup: RES, CK, IK
- *„GBA security context (Bootstrapping Mode)"* – viz kap. 19.2.

- Vstup: RAND, AUTN* (AUTN* = SQN ⊕ AK ‖ AMF ‖ MAC*, kde MAC* = MAC⊕ Trunc(SHA-1(IK)), ke Trunc je funkce, která vyřízne prvních 64 bitů)
- Výstup: RES (GBA_U kryptografický materiál odvozeny od IK a CK je uložen v interním souboru)

- *„GBA security context (NAF Derivation Mode)“* – viz kap. 19.2.
  - Vstup: NAF_ID
  - Ks_NAF

tab. 18.5 Význam jednotlivých EF pod ADF ISIM

EF_{IMPI}	'6F02'	IMPI *(IMS private user identity)*	
EF_{DOMAIN}	'6F03'	DNS doménové jméno domény domovské sítě *(Home Network Domain Name)*	
EF_{IMPU}	'6F04'	IMPU *(IMS public user identity)*	
EF_{AD}	'6FAD'	Obsahuje mód operací ISIM, např. normální (autentizace do IMS), terminál (komunikace s terminálem jako síťové zařízení) atp.	
EF_{ARR}	'6F06'	Obsahuje přístupová pravidla k EF pod ADF ISIM *(Access Rule Reference)*	
EF_{IST}	'6F07'	*ISIM Service Table:* *Service nº1: P-CSCF address* *Service nº2Generic Bootstrapping Architecture (GBA)* *Service nº3HTTP Digest* *Service nº4GBA-based Local Key Establishment Mechanism* *Service nº5Support of P-CSCF discovery for IMS Local Break Out* *Service nº6Short Message Storage (SMS)* *Service nº7Short Message Status Reports (SMSR)* *Service nº8Support for SM-over-IP including data download via SMS-PP* *Service nº9Communication Control for IMS by ISIM* *Service nº10Support of UICC access to IMS*	

$EF_{P\text{-}CSCF}$	'6F09'	Adresa P-CSCF	nº1 nebo nº5
EF_{GBABP}	'6FD5'	Parametry GBA: • RAND • B-TID • Doba platnosti kryptografického materiálu GBA_U	nº2
EF_{GBANL}	'6FD7'	Parametry GBA: seznam jednotlivých NAF-Id a B-TID	nº2
$EF_{NAF\text{-}KCA}$	'6FDD'	*NAF Key Centre Address*	nº2 a nº4
EF_{SMS}	'6F3C'	SMS a jejich parametry	nº6 a nº8
EF_{SMSS}	'6F43'	SMS status (např. příznak, že paměť pro SMS je vyčerpána)	nº6 a nº8
EF_{SMSR}	'6F47'	Obsahuje status reporty (např. informace o doručení) SMS uložených v EF_{SMS}	nº7 a nº8
EF_{SMSP}	'6F42'	Parametry SMS služby (adresa SMS centra, kódování dat atp.)	nº8
$EF_{UICCI\text{-}ARI}$	'6FE7'	Seznam identifikátoru IARI *(IMS Application Reference Identifier)*, tj. identifikátorů IMS aplikací - používá se při SIP REGISTER	nº10

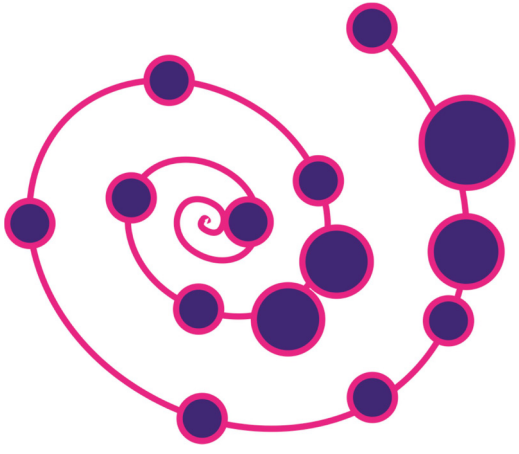
17.22 Embedded UICC, eSE

Stále více se hovoří o tom, že budoucností je eSE (resp. eUICC), tj. opuštění myšlenky o vyjmutelné čipové kartě s osobními aktivy držitele a umístění SE na základní desku mobilního zařízení. Argumentuje se tím, že stále více uživatelů si stejně svá aktiva (adresáře, archiv SMS zpráv apod.) ukládá do mobilního zařízení a nikoliv do UICC. Bohužel i já to dělal, a teď toho lituji.

Podle mého názoru je to omyl. Pokud si uložím osobní aktiva (včetně např. platebních karet) do mobilního zařízení, pak v případě opravy zařízení nebo prodeje zařízení mám oprávněné pochyby, jestli náhodou moje osobní aktiva nebudou novým majitelem zneužita. Vlastně upřednostňování eSE je návrat do 1G.

Tím ale nechci říci, že eSE by se neměly využívat, byly vyvinuty pro m2m nebo v2v komunikaci a pro tyto účely jsou naopak velice vhodné. Ne-

bude mi vadit, když vydavatelem eSE pro automobily bude výrobce automobilu, ale vadí mi, když to jsou téměř monopolní výrobci mobilních zařízení pro osobní používání.



18. Obecná autentizační architektura

IMS přináší do té doby nevídanou myšlenku, kterou je autentizace mobilního účastníka nejenom pro hlasové služby, ale pro webové služby. Původně to bylo myšleno tak, že účastník si bude přes web operátora objednávat/modifikovat operátorem poskytované služby – tzv. samoobsluha. Vznikl tak referenční bot Ut. Přes tento referenční bod může skrze protokoly HTTP/HTTPS spravovat poskytované služby jednak účastník (člověk), ale je to také možné automatizovat pomocí XCAP (*Configuration Access Protocol*) [111].

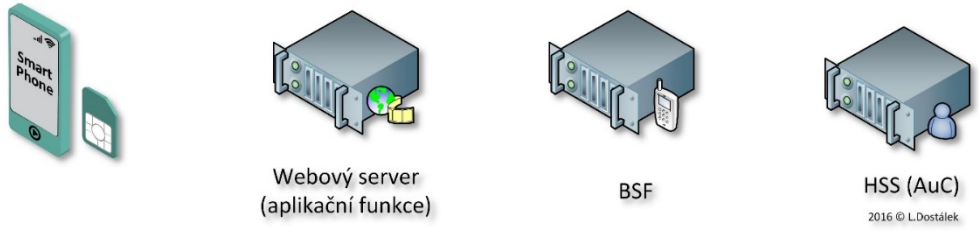
Později se tento mechanismus rozšířil i na obecné aplikace – vznikl referenční bod Ua.

Tento mechanismus se nazývá Obecná autentizační architektura (*Generic Authentication Architecture* - GAA). Cílem je poskytnout autentizaci na bázi mechanismu AKA zcela obecně. Např. pro již zmíněnou autentizaci na Web (tj. pro protokol HTTP), pro autentizaci terminálu vůči čipové kartě apod. Pro tyto účely je standardizována metoda GBA *(Generic Bootstrapping Architecture)* [21], která využívá sdílené tajemství K uložené buď na USIM kartě nebo na ISIM kartě (obě varianty jsou v podstatě rovnocenné).

Nadále nebudeme říkat webový server, ale obecněji Aplikační funkce - NAF. Představme si případ, kdy chceme využít autentizaci AKA pro přihlášení k NAF. Máme následující aktéry (obr. 19.1):

- Mobilní zařízení se sdíleným tajemstvím K na čipové kartě.
- NAF *(Network Application Function), např. zmíněný webový server.*
- BSF *(Bootstrapping Server Function)*
- HSS (resp. AuC), které rovněž má k dispozici sdílené tajemství K.

GBA nepředpokládá, že HSS by poskytovalo kryptografický materiál přímo NAF. Mezi NAF vkládá entitu BSF *(Bootstrapping Server Function)*, která provede autentizaci klienta za využití mechanismu AKA, tj. za využití kryptografického materiálu poskytnutého HSS formu autentizačního vektoru (AV). Následně pak BSF poskytne NAF kryptografický materiál odvozený od kryptografického materiálu získaného během autentizace. Myšlenka spočívá v tom, že jeden BSF může takto obsluhovat řadu NAF (tj. webových serverů).



obr. 19.1 Aktéři

18.1 Referenční body

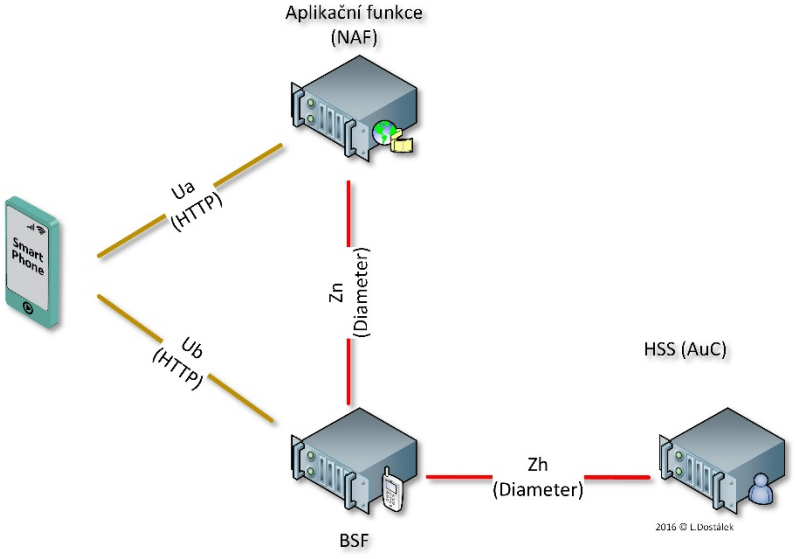
Na autentizační metodě GBA se podílí referenční body: Ua (resp. Ut), Ub , Zh a Zn (obr. 19.2).

18.1.1 Referenční bod Ub

Referenční bod Ub se nachází mezi mobilním zařízením a BSF, zajišťuje vzájemnou autentizaci mezi mobilním zařízením a BSF. Používá se zde autentizace HTTP Digest [9] s metodou AKA [6]. Takto získaný kryptografický materiál získá identifikátor B-TID *(Bootstrapping Transaction Identifier)*. B-TID se použije pro spárování kryptografického materiálu v mobilním zařízení a s kryptografickým materiálem v NAF.

18.1.2 Referenční bod Ua

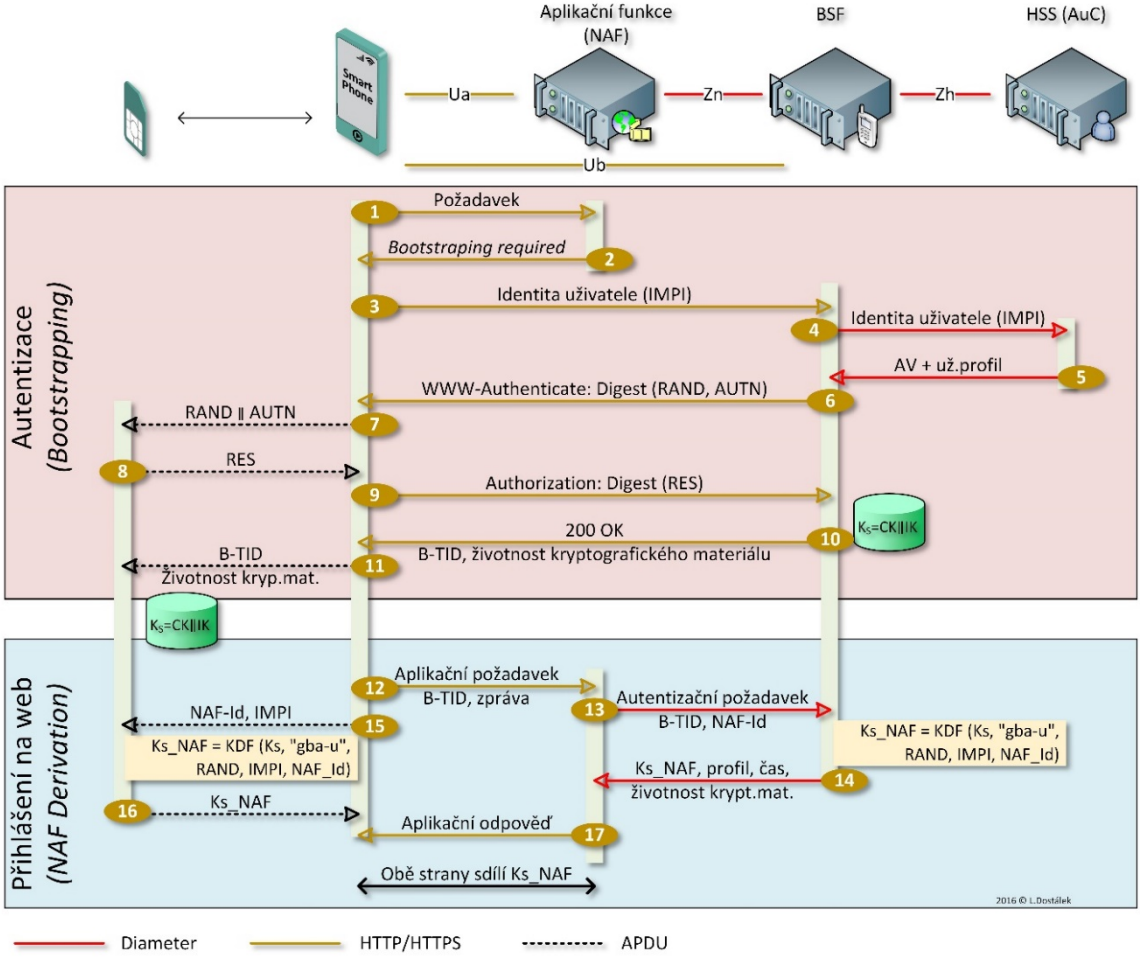
Referenční bod Ua je vlastní aplikační protokol zabezpečený kryptografickým materiálem získaným přes referenční bod Ub. Pro zabezpečení komunikace se využije kryptografický materiál identifikovaný identifikátorem B-TID.



obr. 19.2 Referenční body BSF

18.1.3 Referenční bod Zh

Referenční bod Zh umožňuje BSF získat autentizační informace a uživatelský profil z HSS.



obr. 19.3 Mechanismus GBA (KDF je obdobnou KDF z kap. 7.5)

18.1.4 Referenční bod Zn

Přes tento referenční bod BSF zasílá NAF kryptografický materiál pro zabezpečení komunikace skrze referenční bod Ua. Zasílaný kryptografický materiál má identifikátor B-TID.

18.2 Mechanismus GBA

Mechanismus GBA (obr. 19.3) se skládá ze dvou fází:

1. V první fázi (Autentizace) se uživatel autentizuje vůči BSF.

2. Ve druhé fázi (Přihlášení se na web) pak využívá výsledky této autentizace pro přihlášení k Aplikační funkci (NAF) a využití kryptografického materiálu pro zabezpečení komunikace. Druhá fáze se může opakovat pro další NAF.

18.2.1 První fáze (autentizace vůči BSF)

V zásadě máme dvě formy GBA:

- GBA_U, která ukládá Ks=CK‖IK do UICC interního souboru UICC. Tj. Ks nepouští UICC a derivování kryptografického materiálu Ks_NAF provádí UICC. Tj. jedná se o *„3G Security context“* (kap. 18.20, 1.1). Tento případ je znázorněn na obr. 19.3.
- GBA_ME *(GBA Mobile Equipment)*, kdy se využívá AKA mechanismus bez dodatečných požadavků na UICC. Tj. *„GBA security context (Bootstrapping Mode)“*. V tomto případě UICC vrátí nejenom RES, ale i CK a IK. Mobilní zařízení pak samo spočte a udržuje Ks=CK‖IK ze kterého derivuje následný kryptografický materiál Ks_NAF pro přihlášení se na web

V rámci autentizace klient kontaktuje NAF, který vrátí požadavek na autentizaci pomocí BSF (šipka 1 na obr. 19.3.). Klient se autentizuje vůči BSF (šipka 2), které si vyžádá z AuC autentizační vektor AV (4, 5). Vše postupně probíhá jako v případě popsaném u autentizace protokolu SIP. Výsledkem je, že klient (mobilní zařízení) i BSF získají Ks=CK‖IK. Navíc je tento kryptografický materiál označen indexem B-TID. B-TID generuje BSF a předá jej mobilnímu zařízení.

18.2.2 Druhá fáze (Přihlášení se na web)

Nejprve klient musí NAF sdělit, jaký kryptografický materiál chce využít (šipka 12 na obr. 19.3.). Využije ten, který má index B-TID. Tj. nejprve klient předá zvolený B-TID Aplikační funkci (NAF). NAF požádá BSF o kryptografický materiál o indexu B-TID. BSF nyní odvodí (derivuje) Ks_NAF, který předá NAF.

NAF nyní tento materiál použije k autentizaci a zabezpečení komunikace s klientem. Např. za využití TLS PSK, tj. *“Pre-Shared Key Ciphersuites for Transport Layer Security”* [103]. Je pochopitelně i možná autentizace za využití sdíleného tajemství Ks_NAF na úrovni protokolu HTTP.

18.3 Certifikační autorita

Standard [112] navrhuje jako NAF použít PKI portál, který klientovi vystaví certifikát. Následná autentizace pak může probíhat na základě tohoto certifikátu

18.4 Referenční bod Ut

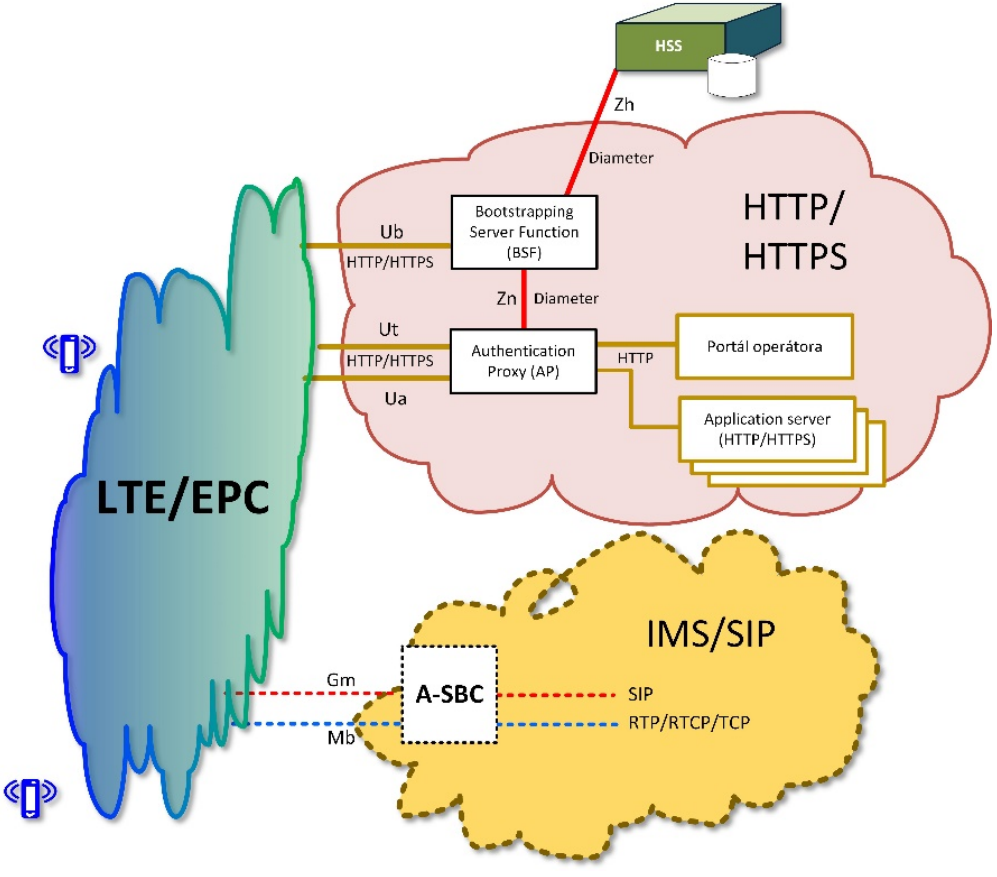
Z obr. 19.4 je tak vidět, že kromě přístupu do IMS může účastník přistupovat protokolem HTTP/HTTPS i na webové aplikace (tj. NAF). Přitom může využívat autentizaci mechanismem GBA (kap. 19.2) nebo pomocí certifikátu. Výhodou tohoto způsobu autentizace je, že účastník je dvou složkově autentizován pomocí USIM/ISIM.

Speciálně pro přístup účastníků na portál telekomunikačního operátora je zaveden referenční bod Ut, který je obdobou referenčního bodu Ua. Pomocí referenčního bodu Ut by si účastník mohl zjišťovat, nastavovat a konfigurovat své služby.

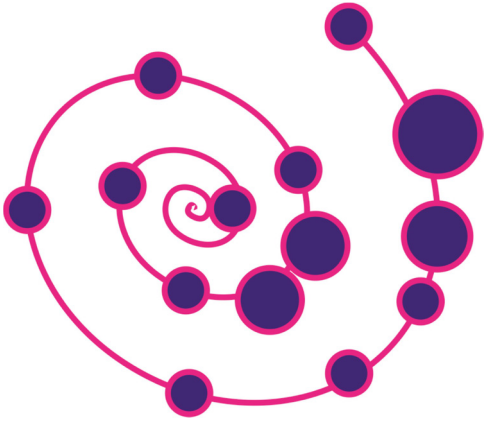
Na obr. 19.4 je znázorněno připojení referenčních bodu Ua a Ut skrze Autentizační proxy.

Jedná se o reverzní proxy, která je vyřizuje autentizační požadavky za servery, které jsou za ní skryté (viz kap. 8.11.10). Autentizace účastníka je buď certifikátem nebo pomocí GBA.

Základním předpokladem pro implementaci referenčního bodu Ut je mít na portále operátora implementován RBAC model [113] pro účastníky. Důvodem je skutečnost, že při ovládání poskytovaných služeb mohou mít zejména účastníci firemních zákazníků odlišné role. Tj. běžný zaměstnanec zákazníka by neměl mít roli objednávat si služby, tato role bude nastavena pouze smluvně ošetřené identitě.



obr. 19.4 Referenční body Ut, Ua a Ub.



19. Autentizace ještě obecněji

Autentizace je proces ověření identity subjektu. Tento proces provádí ověřovatel, který vydává záruku, že subjekt má deklarovanou identitu (obr. 20.1). Kvalita této záruky závisí na konkrétním procesu autentizace.

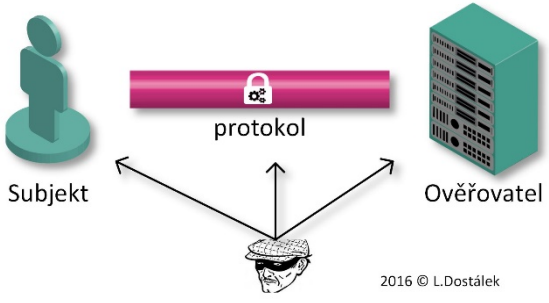
Rozlišujeme autentizaci entity a autentizaci zprávy. Rozdíl je v časovém hledisku. Autentizace zprávy (např. pomocí elektronického podpisu) nedává záruku o tom, kdy byla zpráva vytvořena[3]. Naopak autentizace entity zahrnuje doložení identity žadatele zpravidla prostřednictvím aktuální komunikace s ověřovatelem. Příkladem procesu autentizace je proces, kterým se uživatel pomocí uživatelského jména a hesla přihlašuje do aplikace.

Vedlejším efektem procesu autentizace může být skutečnost, že během autentizace entity bude rovněž vygenerován kryptografický materiál, který bude sloužit k zabezpečení následné komunikace.

19.1 Metody autentizace

Metody autentizace lze rozdělit do následujících kategorií:

1. Subjekt něco ví – např. autentizační faktory: heslo, soukromý nebo tajný klíč, sdílené tajemství atp.
2. Subjekt něco má – např. autentizační faktory: čipová karta, kalkulátor pro generování jednorázových hesel atp.
3. Subjekt něčím je – např. autentizační faktory: otisk prstů, dynamický biometrický podpis, tvar krevního řečiště ruky atp. V poslední době se pak hovoří i o tzv. digitální stopě.



obr. 20.1 Autetnizace

[3] V případě elektronického podpisu se tato informace dodatečně k elektronickému podpisu přikládá zpravidla formou časového razítka.

19.1.1 Kategorie „Něco ví“

Pro kategorii „něco ví“ Máme následující typy autentizačních metod:

- Autentizace na základě hesla.
- Autentizace pomocí dialogu.
- „Zero-knowledge“ autentizace.

Autentizace na základě hesla

Heslo je pro uživatele zapamatovatelný řetězec znaků, který je platný po jistou dobu. Obecně se autentizace heslem považuje za slabou. Existují ale i slabší autentizační metody, jako je např. autentizace na základě IP-adresy.

Vedle hesel máme jednorázová hesla, tj. hesla, která je možné použít pouze jednou. Pro vytváření jednorázových hesel existuje celá řada algoritmů. Od prostého seznamu jednorázových hesel, přes algoritmy založené na sdíleném tajemství mezi subjektem a ověřovatelem až např. po tzv. Lamportovo schéma [114]. Schémata pro generování jednorázových hesel už ale zpravidla řadíme do autentizace pomocí dialogu.

Autentizace pomocí dialogu

Dialog se může např. skládat za dvou kroků: výzvy a odpovědi. Výzva zpravidla obsahuje řetězec obsahující náhodné číslo, pořadové číslo autentizace, čas atd. V odpovědi pak nalezneme řetězec z výzvy, na který byla aplikována symetrická šifra, asymetrická šifra nebo jednocestná funkce. Aby autentizace mohla proběhnout, tak předem musí být mezi subjektem a ověřovatelem vyměněny tajné informace: např. kryptografické klíče, resp. sdílená tajemství. Tyto tajné informace se pak použijí např. jako šifrovací klíče, kterými se šifruje výzva. V případě jednocestné funkce se tajná informace sřetězí s výzvou před tím, než se na výzvu aplikuje jednocestná funkce.

Autentizace pomocí dialogu se někdy označuje jako silná (*strong*) v protikladu s autentizací heslem.

Autentizaci dialogem lze rozdělit do dvou skupin v závislosti na tom, zda na straně autentizovaného subjektu používají nebo nepoužívají datový nosič pro uložení dalšího kryptografického materiálu. Jako datový nosič se zpravidla používá čipová karta, proto v názvech schémat se často vyskytuje sousloví „čipová karta“, ale prakticky je tím míně v podstatě libovolný nosič dat.

V literatuře se tato schémata označují jako:

- Autentizace pomocí hesla „bez čipové karty“. Sem patří již zmíněné Lamportovo schéma [114], ale byla publikována i další schémata, např. [115]. Schémata z této skupiny schémat „bez čipové karty“ jsou dnes obecně brána jako slabá.
- Autentizace pomocí hesla „s čipovou kartou“. Místo sousloví „čipová karta“ budu raději používat termín „datový nosič“, aby nedošlo k záměně s čipovými kartami USIM/ISIM využívanými mobilními zařízeními.

Nadále se budu věnovat schématům „s čipovou kartou“ (resp. „s datovým nosičem“). Publikováno bylo několik schémat. U některých schémat po jejich publikaci následovalo publikování jejich slabin, zpravidla doplněných změnou schématu (resp. navržením schématu nového) tak, aby byla slabina odstraněna.

Autentizační schéma by mělo minimálně umožňovat:

- Oboustrannou autentizaci.
- Změnu hesla.
- Nastavení hesla v případě zapomenutí hesla.
- Odolnost schématu proti následujícím útokům:
  - Vylákání hesla.
  - Odposlechnutí hesla.
  - Uhodnutí hesla.
  - Útoky na synchronizaci času. Některé autentizační mechanismy využívají aktuální čas. Jelikož jsou známy útoky proti tomuto způsobu autentizace, vyžadujeme nezávislost na aktuálním čase.
  - Útoky na synchronizaci komunikace (např. na autentizační dialog). Subjekt ani ověřovatel nesmějí být desynchronizovány tak, aby si každý myslel, že používá jiné sdílené tajemství.

Těmto požadavkům vyhovuje řada autentizačních protokolů. Jak již bylo zmíněno, tak většinou po jejich publikaci následovalo publikování jejich slabin a návrh dalších protokolů odolných proti zjištěným slabinám. Výsledkem této diskuse jsou pak mj. dva protokoly:

- *Secure Hash-Based Password Authentication Protocol Using Smartcards* [116]. Protokol založený na hešovacích funkcích. Tomuto schématu předcházela publikovaná schémata, u kterých se ukázaly slabiny (např. [117] a [118]).
- *Robust Two-Factor Authentication and Key Agreement Preserving User Privacy* (Robustní dvou-faktorová autentizace) [119]. Jedná se o protokol založený na eliptických křivkách. Tomuto autentizačnímu schématu rovněž předcházela diskuse (viz např. [120]).

Robustní dvou-faktorová autentizace je novější schéma (2014). Toto schéma přišlo ještě s dalšími bezpečnostními požadavky:

- Odvolání datového nosiče („čipové karty“). Tj. v případě, ztráty čipové karty či zrušení platnosti čipové se musí útočníkovi zbránit zneužít čipovou kartu.
- Anonymita autentizovaného subjektu (User anonymity). Tj. třetí osoba sledující autentizační dialog nezjistí identitu subjektu.
- Nevystopovatelnost autentizovaného subjektu. Tj. třetí osoba sledující autentizační dialog nezjistí, kdy se jaký subjekt autentizuje.
- Generování kryptografického materiálu pro zabezpečení následné komunikace za podmínek:
  - *Session key agreement* – Během autentizace dojde k ustavování relace, kdy se obě strany dohodnou na kryptografických klíčích relace, které budou známy pouze subjektu a ověřovateli a budou využívány jen pod dobu relace.
  - *Perfect forward secrecy* - Útočník se nemůže dostat k datům relace, i když v budoucnu bude kompromitován

některý ze soukromých klíčů (subjektu nebo ověřovatele), kterými se provádí počáteční autentizace.

- *Forward and backward secrecy* - Vyzrazení klíče relace nepomůže k získání klíčů budoucích nebo minulých relací.
- *Key freshness* - Ani jedna ze stran nemůže předurčit sdílený klíč relace před zřízením relace.

Autentizace Zero Knowledge

Autentizace pomocí hesla nebo dialogu je založena na znalosti tajné informace (heslo, sdílené tajemství atp.). Jelikož tajnou informaci zná jen subjekt a ověřovatel, předpokládá se, že to je dostatečný důkaz o pravosti klienta. Slabinou těchto metod je skutečnost, že se tajná informace nějakým způsobem během autentizace poodhaluje, což může být příležitost pro útočníka.

Zero Knowledge schémata vycházejí z předpokladu, že subjekt má znalost nějakého složitého problému (je to jeho tajemství). Autentizace pak probíhá pomocí předvedení znalosti řešení tohoto složitého problému (např. NP problému). Výsledkem autentizace je pak jen jednobitová informace autentizován/neautentizován. To je sice z hlediska bezpečnosti velice zajímavé, protože se nepoodhaluje tajemství, ale tyto algoritmy negenerují kryptografický materiál pro zabezpečení následné komunikace.

19.1.2 Kategorie „Něco má“

Autentizační kategorie „Něco má“ může mít v reálném světě nejrůznější podoby – např. plastikový průkaz ke vstupu. V mobilních sítích to může být:

- Čipová karta nebo její obdoba. Tj. jednočipový počítač s uloženým kryptografickým materiálem sloužícím pro autentizaci osob (tj. zařízení pro uložení osobních autentizačních aktiv). Toto zařízení během autentizace elektronicky komunikuje s ověřovatelem. Přístup k osobním aktivům (kryptografickému materiálu) je zde chráněn:
  - Jedním nebo více PINy v případě přístupu osoby (držitele).
  - Mechanismem *Secure Messaging* v případě přístupu aplikací bez zásahu uživatele (držitele).
- Autentizační kalkulátor je rovněž jednočipový počítač s uloženým kryptografickým materiálem sloužícím pro autentizaci osob (tj. zařízení pro uložení osobních autentizačních aktiv), ale zpravidla elektronicky nekomunikuje s ověřovatelem, ale informaci zobrazí na displeji. Držitel pak informaci opíše a předá ověřovateli.
- HSM (*Host Security Module*, někdy též *Hardware Security Module*) je výkonný počítač sloužící pro uložení aktiv systému (např. serveru). Přímo elektronicky komunikuje se systémem.
- Mobilní telefon.

Toto dělení je dnes považováno za historické. Organizace GlobalPlatform abstrahovala od konkrétního fyzického provedení a definovala

tzv. Bezpečný prvek (*Secure Element* - SE) pro uchovávání osobních kryptografických aktiv [121] (viz kap. 18.18). Prakticky je míněn specializovaný jednočipový mikroprocesor určený pro bezpečné uchovávání kryptografických dat a bezpečné provádění operací s nimi. Uvedené operace se provádějí v tzv. *Trusted Execution Environment* (TEE – viz kap. 18.17) [122].

Bezpečný prvek (SE) může být realizován jako součást čipové karty (USIM, ISIM, SD atp.) nebo např. jako čip integrovaný na základní desce mobilního zařízení atp. Na bezpečný element se z hlediska bezpečnosti v podstatě díváme obdobně jako na HSM.

Závěrem lze tedy říci, že osobní autentizační aktiva mohou být uložena:

- Na datovém nosiči bez ochrany (resp. se slabou ochranou).
- V bezpečném prvku.
- V HSM modulu.

V případě porovnávání jednotlivých metod bereme v úvahu následující bezpečnostní vlastnosti (závisí též na konkrétní implementaci):

- Zařízení fyzicky uchovává kryptografický materiál (a aplikace jej využívá).
- Přístup ke kryptografickému materiálu pomocí hesla nebo PIN.
- Kryptografický materiál neopouští zařízení (je neexportovatelný).
- Zařízení je fyzicky chráněno proti neoprávněnému přístupu.

19.1.3 Kategorie „Něčím je“

Touto autentizační kategorií se zpravidla myslí autentizační faktory založené na biometrických vlastnostech subjektu, tj. ověření identity osoby na základě měřitelných fyziologických nebo behaviorálních charakteristik, jedinečných a relativně neměnných pro subjekt.

Konkrétní biometrická charakteristika se subjektu nejprve sejme a vytvoří se tzv. vzor. Autentizace pak probíhá na zjišťování korelace aktuálních charakteristik subjektu s charakteristikami uloženými ve vzoru. Vedle korelace se sledující další veličiny.

Základní nevýhodou biometrických charakteristik je, že je v případě zneužití nelze odvolat a následně změnit. Např. pokud útočník získá dynamický biometrický podpis subjektu, pak subjekt již nikdy nemůže dynamický biometrický podpis používat, aniž by nehrozilo jeho zneužití (lze např. ale podpis rozšířit o obrázek).

Digitální stopa (*Digital Footprint*) má obdobné vlastnosti jako biometrické charakteristiky. Jedná se zejména o sledování metadat, která používáme při komunikaci nebo která po sobě zanecháváme.

Součástí digitální stopy může být:

- IP adresa, resp. autonomní systém, ze kterého IP adresa je.
- Metadata aplikačního protokolu. V protokolu HTTP to může být např.: hlavička User-Agent, hlavičky Acceept*, navštívená URL, cookies atd.

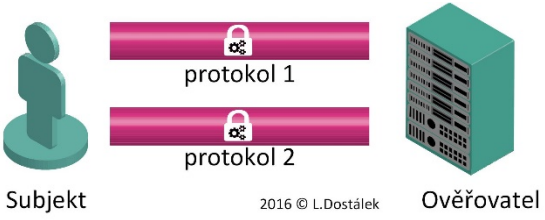
- Chování klienta v aplikaci (např. počet autentizací za den, obvyklá velikost transakcí atd.).
- Použité autentizační metody.
- Metadata přejatá z autentizace pomocí federaci identit.

Pokud si budeme tato metadata o subjektu (digitální stopu) ukládat, pak můžeme zjišťovat ko-

19.2 Více faktorová autentizace

Více faktorová autentizace[4] znamená, že pro autentizaci se použije dvou nebo více autentizačních faktorů (např. dva různé protokoly - obr. 20.2).

Přitom je důležité, aby byly použity dva odlišné autentizační faktory. Např. použití dvou hesel za



obr. 20.2 Více faktorová autentizace

relaci aktuálních metadat s uloženými. Situace zde není tak jednoznačná, protože subjekt může přistupovat z různých systémů či může cestovat. Subjekt si můžeme vytvořit více profilů subjektu (mobilní, osobní počítač atp.) – obdobně v případě otisků prstů může snímat otisky více prstů. Digitální stopa se v praxi hojně využívá např. v případě cílené reklamy.

Digitální stopa má oproti biometrickým charakteristikám výhodu v tom, že ji lze změnit. Nevýhoda spočívá v problému sporné legálnosti sledování osobních údajů.

sebou příliš kvalitu autentizace nezlepší. Autentizační faktory se mohou lišit:

- Různým kryptografickým materiálem.
- Různým autentizačním schématem.
- Různým komunikačním protokolem.
- Různým komunikačním kanálem.
- Různým ověřovatelem.

Důležité rovněž je, aby autentizační faktory byly provázané (nikoliv na sobě závislé!). Pokud nejsou, pak se útočníkovi ulehčuje práce, neboť útočník se nejprve může věnovat zlomení jednoho autentizačního faktoru a pak druhého. Ne však vždy toho lze prakticky dosáhnout. Např.

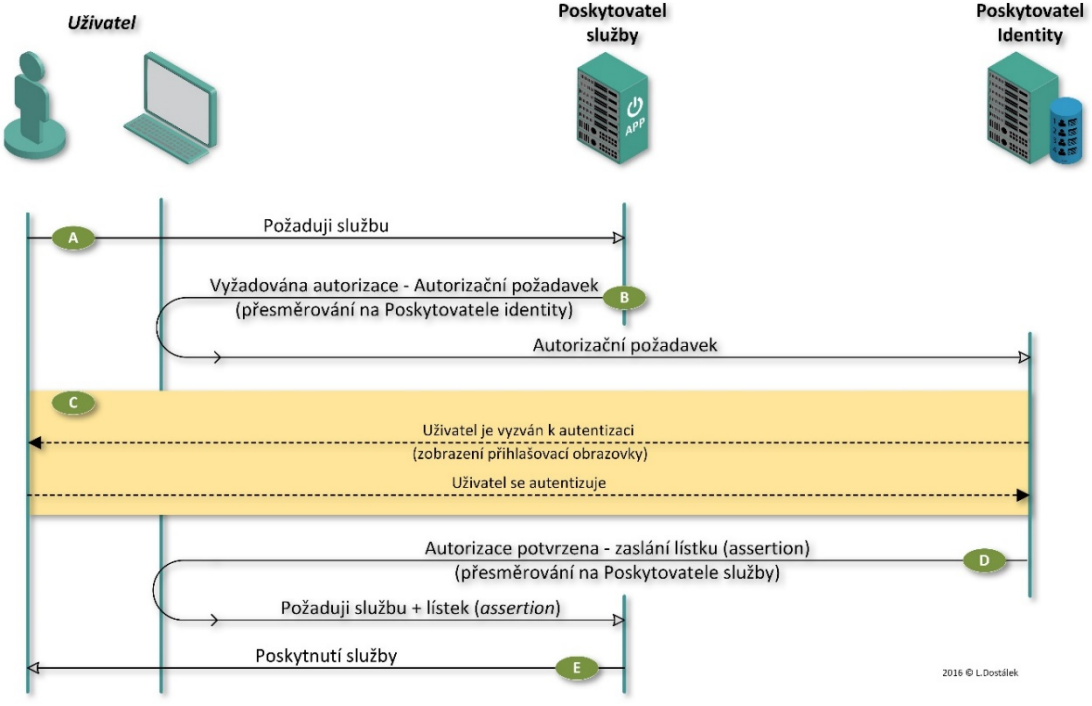
[4] Někdy se též používá termín vícesložková autentizace

pokud je již subjekt autentizován (např. si přinesl autentizace z aplikace Facebook) a ukáže se, že pro danou operaci je nutná silnější autentizace (např. čipovou kartou), pak se zpravidla re-autentizuje jen silnějším schématem (čipovou kartou), které je nezávislé na původní autentizaci. V tomuto případě autentizační metody nebyly provázány.

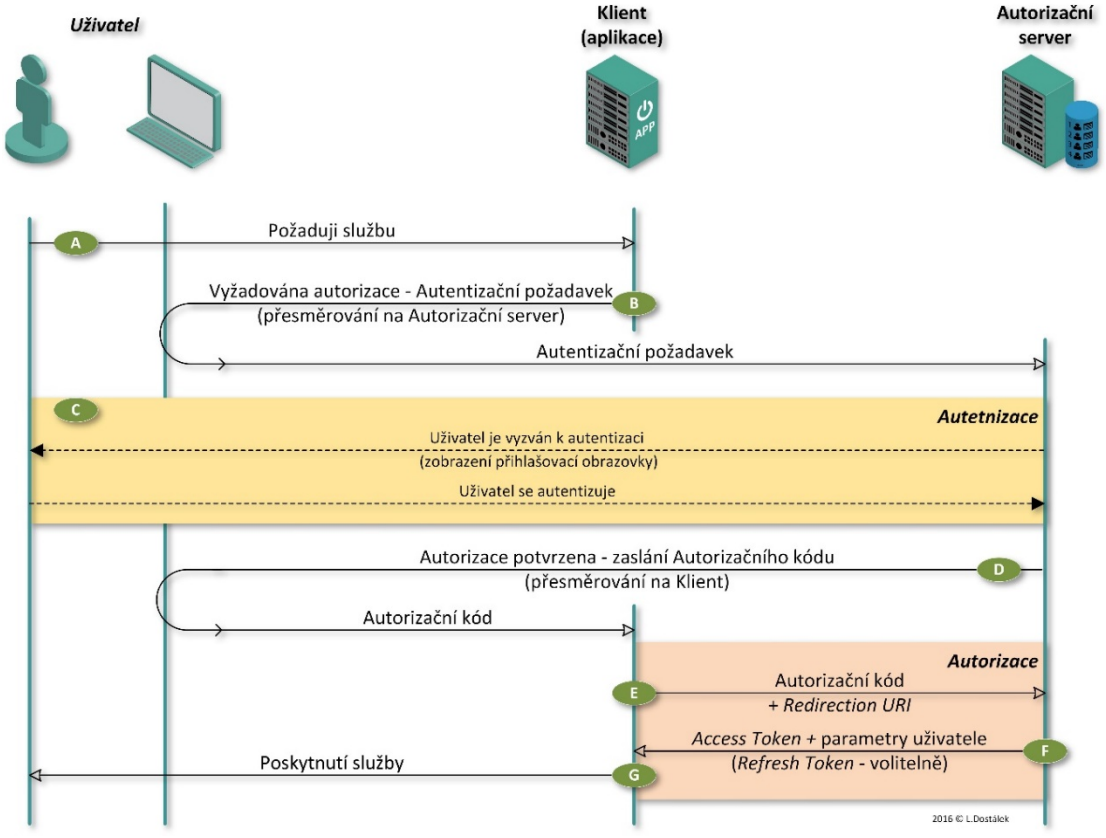
19.3 Federace identit

Byla-li identita ověřena jedním ověřovatelem, pak je otázkou, zda by i jiný ověřovatel mohl tomuto ověření věřit. Tj. zda by ověřovatel akceptoval ověření subjektu od jiného ověřovatele bez toho, aby sám provedl ověření.

Jedná se o standardní požadavek, který už řešil protokol Kerberos (založený na schématu Needham-Schroeder [123]). První verze protokolu Kerberos byla publikována v roce 1987 (aktuální verze [124]). Tento protokol používá pro subjekt termín principál, pro ověřovatel termín KDC (*Key Distribution Center*). KDC ověřuje identitu principálů v rámci své říše (*Realm*). Výsledkem ověření je systém lístků (*ticket*), pomocí kterých lze přistupovat ke službám v rámci říše.



obr. 20.3 SAML: Poskytovatel identity stvrzuje identitu uživatele poskytovateli služby



obr. 20.4 Příklad dialogu protokolu OAuth 2.0

Protokol Kerberos řeší i problém důvěry mezi říšemi, tj. řeší i problém jak se lístkem vydaným v jedné říši prokázat v jiné říši.

V současné době se, pro federaci identit (kromě protokolu Kerberos) používají zejména dva standardy:

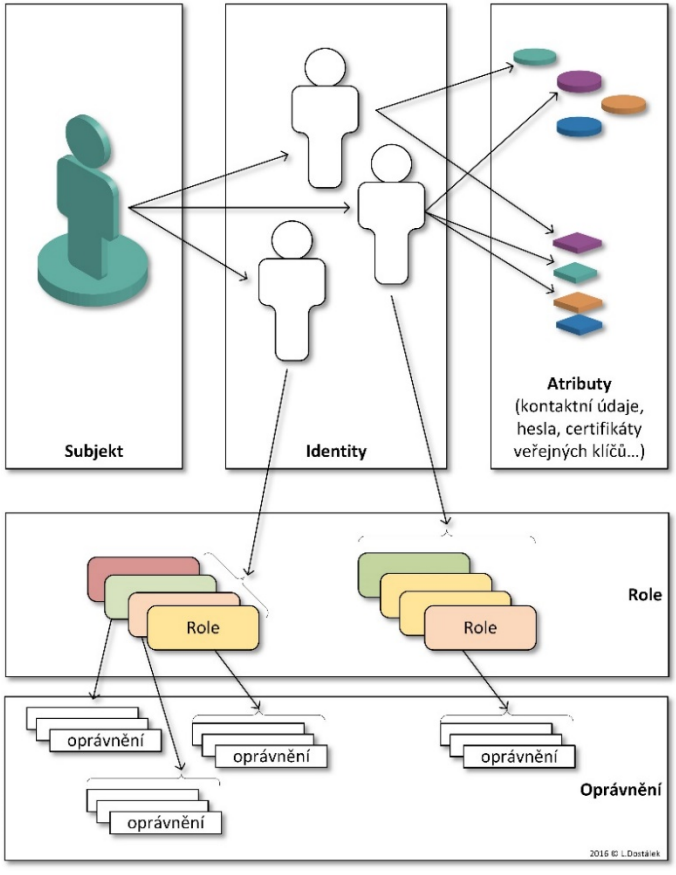
- *Security Assertion Markup Language* (SAML) [125] – nyní ve verzi 2.
- *Open Authentication* (OAuth) [126] [127] [128] – nyní ve verzi 2.

19.3.1 SAML

SAML (*Security Assertion Markup Language* [125]) řeší problém federace tak, že odděluje poskytovatele služby (tj. poskytovatele zdroje informace o kterou má subjekt zájem) a poskytovatele identity. Poskytovatel identity provádí autentizaci subjektu. Výsledkem autentizace je

vydání lístku[5] (*Assertion*), na základě kterého poskytovatel služby poskytne/neposkytne příslušný zdroj. Federace spočívá v tom, že Poskytovatel identit poskytuje lístky různým poskytovatelům služeb (obr. 20.3).

SAML sám je jen manipulační jazyk, který popisuje lístek (*Assertion*). Tj. jak samotná autentizace, tak mechanismus přesměrování[6] znázorněný na obr. 20.3 jsou mimo specifikaci tohoto standardu. Závisí na konkrétní implementaci.



obr. 20.5 RBAC model

[5] Někdy se též používají termíny oprávnění, tvrzení, token atp.

[6] Zpravidla se využívá mechanismus přesměrování protokolu HTTP

19.3.2 JWT

Manipulační jazyk SAML je velice obecný, ale díky své obecnosti je jednak složitý a jednak výsledný lístek příliš komplikovaný, což někdy vyvolávalo technické obtíže. Autentizační informace se proto dnes častěji nepopisují ve tvaru SAML, ale pomocí *JavaScript Object Notation* (JSON). Vznikl tak standard JSON Web Token (JWT) [129].

19.3.3 OAuth 2.0

Jak SAML, tak i JWT popisují jen lístek, který vydává poskytovatel identity subjektu, aby se jím prokázal poskytovateli služby. Protokol, kterým dojde k této komunikaci, je mimo tyto standardy (tj. není součástí těchto standardů).

OAuth 2.0 [126] [127] [128] je protokol, který tento problém řeší, tj. popisuje tuto komunikaci. OAuth 2.0 umožňuje obdobnou autentizaci jako na obr. 20.3. Umožňuje i jiné dialogy - na obr. 20.4 je příklad dialogu protokolu OAuth 2.0, kdy je rozdělen dialog do dvou fází:

1. Autentizace, jejíž výsledkem je získání Autorizačního kódu, který může být náhodný, a tak nezadat šanci útočníkovi útočícímu na uživatelův počítač zneužít lístek zaslaný Autorizačním serverem.
2. Autorizace, kdy Klient (aplikace) získá přístupový lístek s oprávněními poskytnout uživateli příslušnou službu. Lístek se zde nazývá *Access Token*. Klient může získat i tzv. *Refresh Token*, sloužící k obnovení lístku.

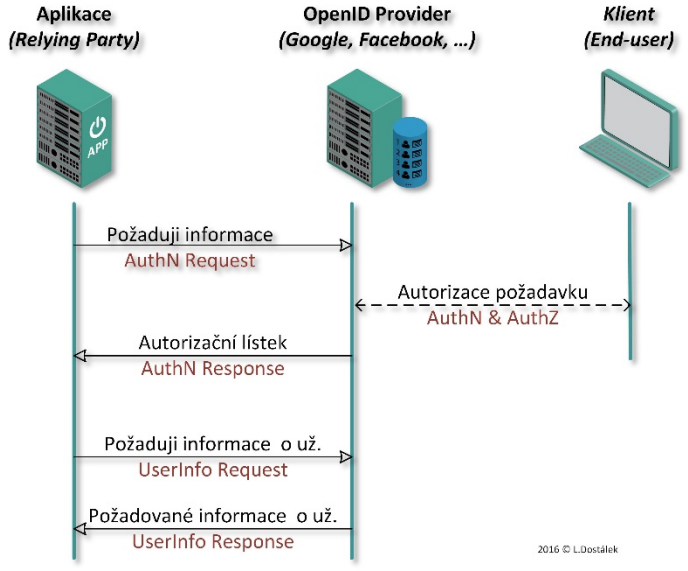
19.4 RBAC model

Role-Based Access Control (RBAC) model [113] předpokládá, že subjekt má v rámci nějaké oblasti/domény/říše (např. organizace) jednu nebo více identit (obr. 20.5). Každá jeho identita má konkrétní atributy (kontaktní údaje, hesla, certifikáty veřejných klíčů atp.). Důležité ale je, že konkrétní oprávnění pro přístup a práci s aktivy nejsou přímo vázaná na identitu, ale na role. Tj. identitám jsou přiřazeny role a teprve na role jsou navázána oprávnění. Při změně role, tak automaticky dojde ke změně oprávnění. Roli si můžeme představit např. jako pozici v organizaci (většinou v praxi jedné pozicí odpovídá více rolí). Role může být ale třeba občan při styku občana se státní mocí.

19.5 OpenID Connect

Informace o uživateli udržuje zpravidla ověřovatel. V případě, že využíváme federaci identit, pak je užitečné získat atributy ověřené identity od prvotního ověřovatele. OpenID Connect [130] je protokol, který umožňuje získání atributů identity od původního ověřovatele.

Přiklad (obr. 20.6): Pro ověření do aplikace budeme využívat přihlášení do systému Facebook (v systému Facebook máme odkaz do uvedené aplikace). V případě, že uživatel přejde na tento odkaz, díky federaci identit se akceptuje autentizace ze systému Facebook do uvedené



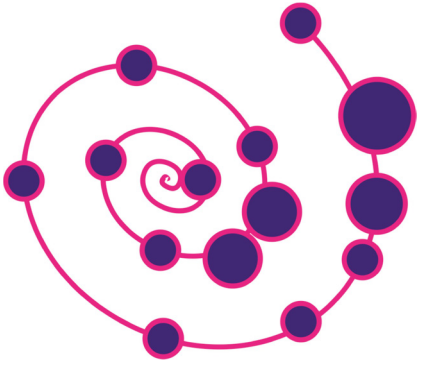
obr. 20.6 OpenID Connect

aplikace. Pro založení uživatele v aplikaci potřebujeme jeho atributy. Ty získáme přes protokol OpenID Connect.

19.6 Autorizace

Autentizace ověřila identitu subjektu. Nyní identita chce přistupovat ke konkrétním zdrojům (aktivům). Proces, který přiřadí práva autentizované identitě pro přístup ke zdrojům, se nazývá autorizace.

Z obr. 20.5 jakoby plynulo, že identita automaticky po autentizaci získá oprávnění sobě přiřazených rolí. Obecně tomu tak ale není. Proces autorizace totiž může být závislý na kvalitě (síle) použité autentizace. Identitě jsou pak přiřazeny jen ty role (z možných rolí, které mu mohou být přiřazeny), které odpovídají síle jim použité autentizační metody.



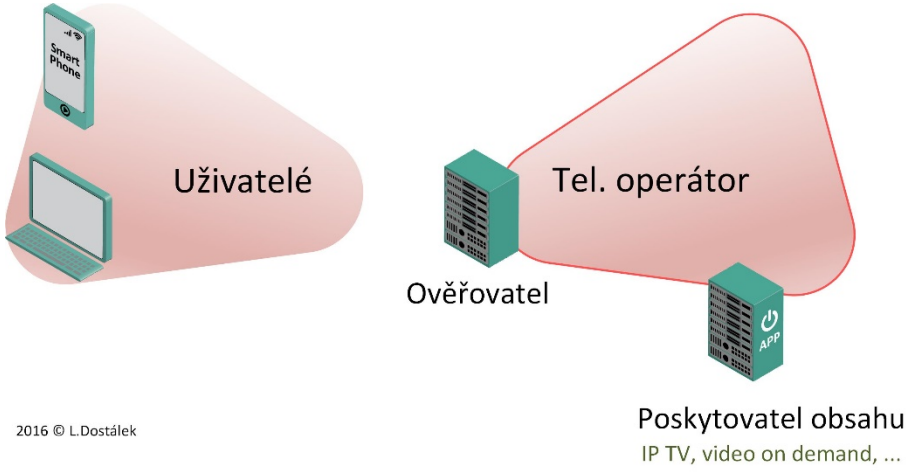
20. Problém autentizace v praxi

V současné době nasazovaný *Internet Multimedia Subsystem* (IMS) [131] bude služby telekomunikačních operátorů řešit jako aplikace (kap. 4.4). Aplikace budou zajišťovat nejen hlasovou komunikaci (obecně multimediální komunikaci), ale i další aplikační služby. Aplikační služby budou moci být poskytovány i třetími stranami. Příklady aplikačních služeb mohou být např. videokonference, ale např. i *video on demand* atp.

V případě poskytování aplikačních služeb se jedná o obdobnou situaci, která byla před lety na Internetu, kdy poskytování obsahu bylo v režii poskytovatelů připojení. Teprve v okamžiku, kdy obsah začaly poskytovat 3. strany (poskytovatelé obsahu), se Internet rozvinul do současných rozměrů.

Autentizace do aplikací třetích stran přitom může být v současné době řešena jednou z následujících možností:

- Autentizace si řeší sám poskytovatel služby (bez účasti operátora), např. pomocí jména a hesla.
- K autentizaci se využijí prostředky pro autentizaci účastníka mobilní sítě (tj. např. USIM). Jedná se sice o silnou autentizaci, ale ta je pod výhradní kontrolou operátora. Vlastník aplikace (3. strana) si může provádět správu svých uživatelů jen velice omezeně – nemá správu uživatelů zcela pod svou kontrolou.



Obr. 21.1 Poskytovatel obsahu využívá autentizaci operátora sítě

Motivací je snaha navrhnout autentizační algoritmy, které by využily silnou autentizaci účastníka mobilní sítě a přitom umožnily poskytovatelům obsahu mít správu svých uživatelů ve své moci.

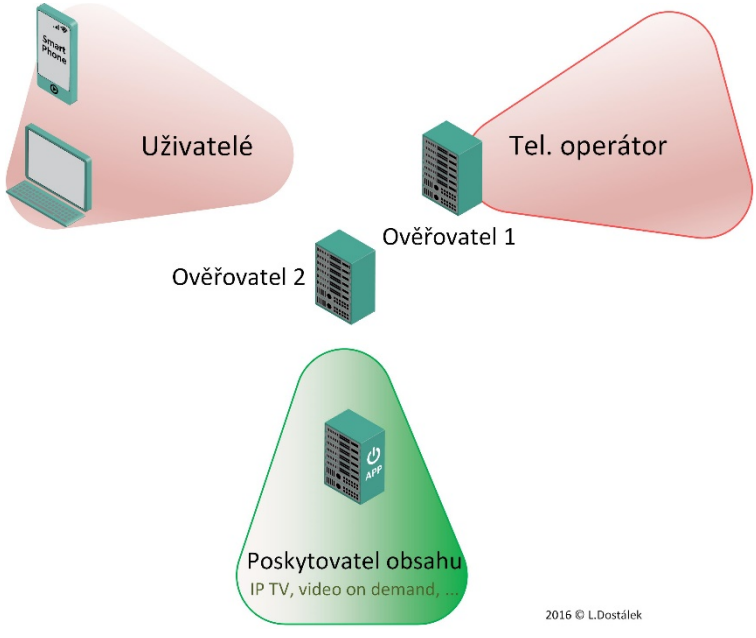
20.1 Druhý autentizační faktor

Je třeba rozvést termín „dvou (resp. více) faktorová“ autentizace (blíže viz kapitola 20.2). Jak AKA mechanismus, tak i sofistikovanější autentizace pomocí hesla (např. [118], [116], [119]) jsou dvou faktorovými autentizacemi:

- AKA mechanismus využívá USIM/ISIM čipovou kartu a PIN.
- Sofistikovanější autentizace pomocí hesla (např. [118], [116], [119]) využívají heslo a kryptografický materiál uložený na nějakém datovém nosiči (opět např. na čipové kartě).

Problémem ale je, že oba autentizační faktory jsou na straně aplikace (ověřovatele) v moci téže osoby. Což má následující nevýhody:

- V případě AKA autentizace je USIM/ISIM čipová karta poskytována telekomunikačním operátorem. Což je zase těžko přijatelné pro poskytovatele aplikací, protože správa jeho uživatelů je v moci telekomunikačního operátora.
- V případě sofistikovanější autentizace pomocí hesla (např. [118], [116], [119]) by z bezpečnostního hlediska nevadilo, že uživatel využívá heslo i např. čipovou kartu obdrženou od poskytovatele aplikace. Avšak z technického hlediska je problém, jak tuto aplikačně závislou čipovou kartu využívat uživatelovým zařízením.



obr. 21.2 Druhý autentizační faktor spravovaný poskytovatelem aplikace

Z praxe víme, že technické problémy spojené s takovou implementací často přinášejí uživatelům těžké problémy. Navíc každý poskytovatel aplikace by využíval jiné čipové karty.

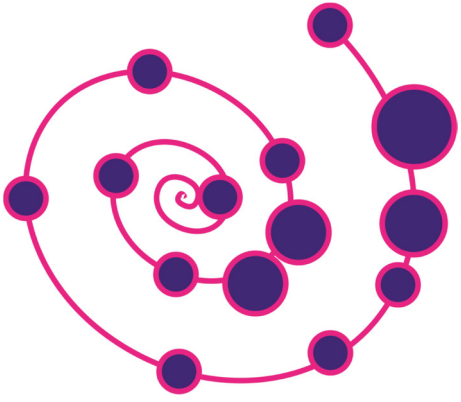
20.2 Cíl

Cílem je navrhnout takový autentizační algoritmus pro mobilní webové aplikace, který propojí AKA schéma se silnou autentizací heslem. Pokud možno takový, který umožní i autorizaci dat. Takovéto schéma bude užitečné zejména pro nové aplikace v nových mobilních sítích, kdy uživatel je neustále připojen k internetu (což vyplývá z podstaty těchto sítí). Následně by pak bylo vhodné, aby takto navržený mechanismus byl využitelný poskytovateli OpenID Connect (resp. OAuth 2.0).

Dalším důvodem k hledání nového algoritmu je již zmíněná skutečnost, že tajemství pro autentizaci AKA schématem spravuje operátor sítě. Pro nezávislé poskytovatele obsahu to znamená, že správa uživatelů je plně v moci telekomunikačního operátora (Obr. 21.1).

Cílem je, aby k autentizaci byl použit druhý autentizační faktor (např. druhý ověřovatel), který by si spravoval poskytovatel aplikace (obr. 21.2).

Kombinací AKA schématu a algoritmu silné autentizace heslem získáme více faktorovou autentizaci, která pevně spojí držitele USIM/ISIM s jeho heslem do aplikace. Heslo aplikace přitom bude ve správě poskytovatele aplikace. Této problematice jsem se věnoval v [132] [133].



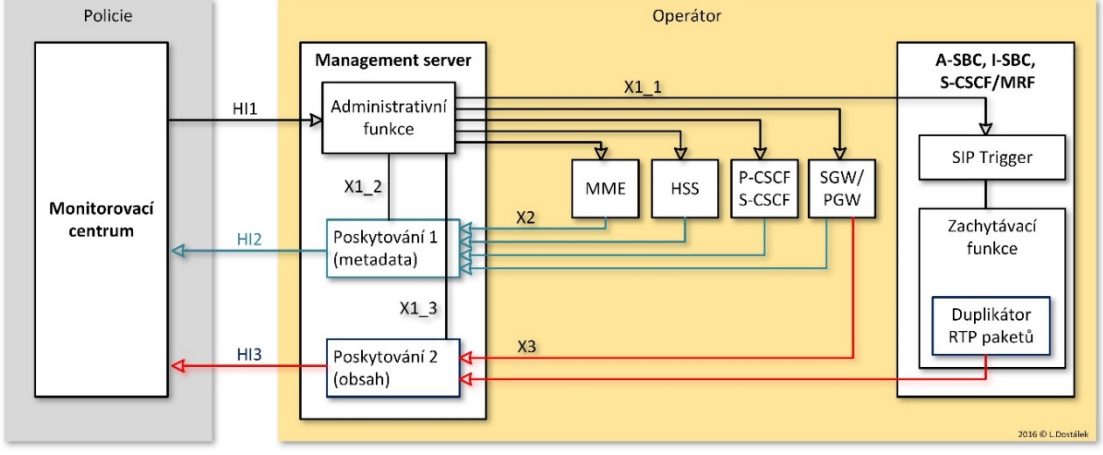
21. Poznámka k legálnímu odposlechu

IMS je navržen tak, aby komunikace byla zabezpečena mezi mobilním zařízením a hranou sítě, tj. v jádře sítě není komunikace zabezpečena, takže je ji je možné odposlouchávat.

Odposlech může být legální nebo nelegální. Nelegální odposlech může provést libovolný „muž uprostřed“, který se dostane k nešifrované komunikaci SIP/RTP[7]. Stačí k tomu např. obecně dostupný program Wireshark, který umí hovor nalézt a dokonce i uložit do souboru pro následné přehrání.

Legální odposlech je vymezen §§ 88 a 88a zákona 141/161 Sb., trestní řád. § 88 specifikuje, za jakých okolností se může provádět odposlech a § 88a pak specifikuje, za jakých okolností se mohou zjistit „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“.

Architektura legálního odposlechu [134] je zobrazena na obr. 22.1. Monitorovací centrum provozované např. policií nebo jinou agenturou komunikuje pomocí referenčních bodů HI1 až HI3 (*Handover Interface*) s operátorem. Operátor pro tyto účely provozuje Management server, který transformuje komunikaci z referenčních bodů HI1 až HI3 na interní referenční body X1 až X3 (nezaměňovat s referenčním bodem mezi



obr. 22.1 Architektura odposlechu

[7] Z obr. 9.13 plyne, že na nezabezpečenou komunikaci lze narazit na eNB a v jádru sítě. Tj. pro hackery budou jistě zajímavé zejména HeNB.

uzly eNB - obr. 4.4). Management server se skládá ze tří entit:

- Administrativní funkce – tato entita převádí požadavky Monitorovacího centra na jednotlivé dílčí požadavky.
- Poskytování 1 – tato entita poskytuje informace o telekomunikačním provozu a předává je Monitorovacímu centru.
- Poskytování 2 – tato entita poskytuje vlastní data a předává je Monitorovacímu centru.

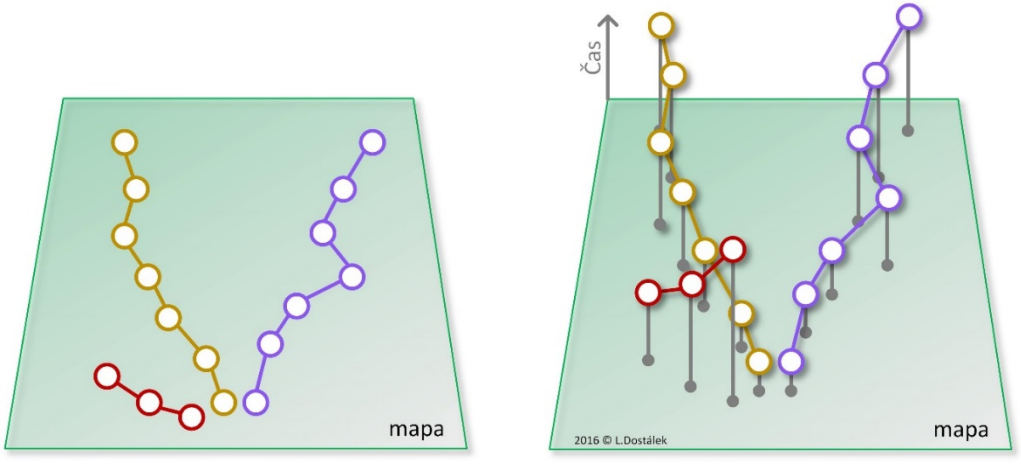
Referenčním bode HI1 Monitorovací centrum zadává požadavky, referenčním bodem HI2 získává požadované informace o telekomunikačním provozu a referenčním bodem HI3 pak získává data (médium), tj. např. obsah hovorů, IP provoz, SMS atp.

Uvnitř sítě operátora se referenční bod X1 rozpadá na tři typy komunikace:

- X1_1 – zadávání požadavků jednotlivým entitám sítě operátora.
- X1_2 – komunikace s entitou Poskytování 1.
- X1_3 – komunikace s entitou Poskytování 2.

Trochu komplikací je, odposlech VoLTE hovorů, protože pro duplikaci hovoru potřebujeme mít přístup jak k protokolu SIP, tak i k protokolu RTP. Když se nad tím zamyslíte, tak to lze provést na všech entitách, které používají referenční bod H.248. Na obr. 22.1 jsou tyto entity symbolicky označeny A-SBC, I-SBC a S-CSCF/MRF.

Zatímco zajistit klasický odposlech bude čím dál obtížnější, tak „údaje o telekomunikačním provozu“ budou stále pro vyšetřování důležité, byť třeba nebudou nakonec využity v řízení před soudem. Např. lokalizační údaje zakreslené do mapy (obr. 22.2 vlevo) nám zobrazí cesty, kudy se pohybovali jednotliví účastníci. Avšak pokud

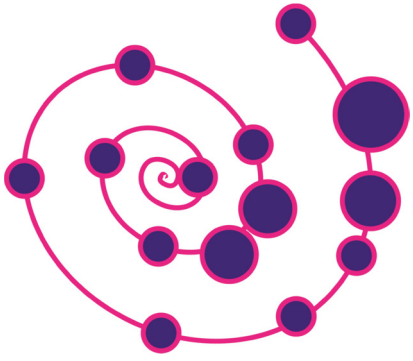


obr. 22.2 Lokalizační údaje zakreslené do mapy

nad mapu vztyčíme časovou osu a výsledek zobrazíme v 3D, pak je výsledek opravdu zajímavý (vpravo).

Obtížnost zajištění odposlechu bude dána několika faktory. Jednak nic nebrání, aby si účastníci nešifrovali RTP komunikaci (médium) mezi sebou navzájem. Jiným problémem je, že volající může volaného jen prozvonit, tím získá IP adresu jeho mobilu a následně s ním může navázat komunikaci např. přes Internet.

A navíc Google má stejně lokalizační údaje převážné části lidské populace, aby mohl vykreslovat provoz v Googlemaps ☺.



22. Citovaná literatura

[1] L. Dostálek a A. Kabelová, Velký průvodce TCP/IP a systémem DNS, Computer Press, páté vydání, 2008, p. 418.

[2] L. Dostálek, a kol. a kol., Velký průvodce protokoly TCP/IP - bezpečnost, Computer Press, 2001.

[3] L. Dostálek, M. Vohnoutová a M. Knotek, Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, Computer Press, druhé vydání, 2010.

[4] „Man-Machine Interface (MMI) of the User Equipment (UE),“ 3GPP TS 22.030, January 2016. [Online]. Available: http://www.3gpp.org.

[5] „IMS Roaming and Interworking Guidelines,“ GSM Association IR.65, February 2013. [Online]. Available: http://www.gsma.com.

[6] „3G security; Security architecture,“ 3GPP TS 33.102 , December 2014. [Online]. Available: http://www.3gpp.org.

[7] „3GPP System Architecture Evolution (SAE); Security architecture,“ 3GPP TS 33.401, December 2014. [Online]. Available: http://www.3gpp.org/.

[8] „3G security; Access security for IP-based services,“ 3GPP TS 33.203, December 2014. [Online]. Available: http://www.3gpp.org.

[9] A. Niemi, J. Arkko a V. Torvinen, „ Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA),“ IETF RFC 3310, September 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3310.txt.

[10] „3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General,“ 3GPP TS 35.205, September 2014. [Online]. Available: http://www.3gpp.org.

[11] „3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification,“ 3GPP TS 35.206, September 2014. [Online]. Available: http://www.3gpp.org.

[12] „Radio Resource Control (RRC); Protocol specification," 3GPP TS 25.331, January 2015. [Online]. Available: http://www.3gpp.org.

[13] „Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification," 3GPP TS 36.323, January 2015. [Online]. Available: http://www.3gpp.org/.

[14] „Radio Link Control (RLC) protocol specification," 3GPP TS 25.322, September 2014. [Online]. Available: http://www.3gpp.org/.

[15] „Medium Access Control (MAC) protocol specification," 3GPP TS 25.321, January 2015. [Online]. Available: http://www.3gpp.org/.

[16] G. Pelletier a K. Sandlund, „RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite," IETF RFC 5225, April 2008. [Online]. Available: https://tools.ietf.org/html/rfc5225.

[17] E. Soljanin, R. Liu a P. Spasojevic, „Hybrid ARQ with Random Transmission Assignments," *Advances in network information theory. Providence, Rhode Island: American Mathematical Society.,* Sv. %1 z %2 ISBN 0-8218-3467-3, p. pp. 321–334, 2004.

[18] „Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," 3GPP TS 24.301, December 2014. [Online]. Available: http://www.3gpp.org.

[19] „3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3," 3GPP TS 29.274, January 2015. [Online]. Available: http://www.3gpp.org.

[20] „General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)," 3GPP TS 29.281, January 2015. [Online]. Available: http://www.3gpp.org.

[21] „Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)," 3GPP TS 33.220, V 12.3.0, June 2014. [Online]. Available: http://www.3gpp.org.

[22] D. Eastlake a T. Hansen, „US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," IETF RFC 6234, May 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6234.txt.

[23] V. Fajardo, J. Arkko, J. Loughney a G. Zorn, „Diameter Base Protocol," IETF RFC 6733, October 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6733.txt.

[24] C. Rigney, S. Willens, A. Rubens a W. Simpson, „Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2865.txt.

[25] J. Postel, „User Datagram Protocol," IETF RFC 768, August 1980. [Online]. Available: http://www.rfc-editor.org/rfc/rfc768.txt.

[26] J. Postel, „Transmission Control Protocol," IETF STD 7, IETF RFC 793, September 1981. [Online]. Available: http://www.rfc-editor.org/rfc/rfc793.txt.

[27] H. Hakala, L. Mattila, J.-P. Koskinen, M. Stura a J. Loughney, „Diameter Credit-Control Application," IETF RFC 4006, August 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4006.txt.

[28] S. Kent a K. Seo, „Security Architecture for the Internet Protocol," IETF RFC 4301, December 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4301.txt.

[29] T. Dierks a E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.2," IETF RFC 5246, [Online]. Available: http://www.rfc-editor.org/info/rfc5246.

[30] „Authentication, Authorization, and Accounting (AAA) Parameters," IANA, [Online]. Available: http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml.

[31] „SMI Network Management Private Enterprise Codes," IANA, [Online]. Available: http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.

[32] „Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping," 3GPP TS 29.213, V13.0.0, December 2014. [Online]. Available: http://www.3gpp.org/.

[33] „LTE Roaming Guidelines, Version 9.0," GSM Association IR.88, Januar 2013. [Online]. Available: http://www.gsma.com/newsroom/wp-content/uploads/2013/04/IR.88-v9.0.pdf.

[34] „Numbering, addressing and identification," 3GPP TS 23.003, V 13.0.0, Januar 2015. [Online]. Available: http://www.3gpp.org/.

[35] „DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers," GSM Association IR.67, March 2010. [Online]. Available: http://www.gsma.com.

[36] M. Mealling, „ Dynamic Delegation Discovery System (DDDS), Part One: The Comprehensive DDDS," IETF RFC 3401, October 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3401.txt.

[37] M. Jones, J. Korhonen a L. Morand, „Diameter Straightforward-Naming Authority Pointer (S-NAPTR) Usage," IETF RFC 6408, November 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6408.txt.

[38] B. Aboba, M. Beadles, J. Arkko a P. Eronen, „The Network Access Identifier," IETF RFC 4282, December 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4282.txt.

[39] L. Daigle a A. Newton, „ Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),“ IETF RFC 3958, January 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3958.txt.

[40] G. Zorn, „Diameter Network Access Server Application,“ IETF RFC 7155, April 2014. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7155.txt.

[41] „Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol,“ 3GPP TS 29.272, V 13.0.3, January 2015. [Online]. Available: http://www.3gpp.org.

[42] „Policy and Charging Control (PCC) over S9 reference point; Stage 3,“ 3GPP TS 29.215, V 13.0.0, January 2015. [Online].

[43] „Policy and Charging Control (PCC); Reference points,“ 3GPP TS 29.212, V 13.0.0, January 2015. [Online]. Available: http://www.3gpp.org.

[44] „Policy and charging control over Rx reference point,“ 3GPP TS 29.214, V 13.0.0, January 2015. [Online]. Available: http://www.3gpp.org.

[45] „Telecommunication management; Charging management; Charging architecture and principles,“ 3GPP TS 32.240, V 12.6.0, December 2014. [Online].

[46] „Policy and charging control: Spending limit reporting over Sy reference point,“ 3GPP TS 29.219, V 13.0.0, January 2015. [Online]. Available: http://www.3gpp.org/.

[47] „IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents,“ 3GPP TS 29.228, V 12.4.0, January 2015. [Online]. Available: http://www.3gpp.org.

[48] „IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents,“ 3GPP TS 29.328, V 12.7.0, January 2015. [Online]. Available: http://www.3gpp.org.

[49] „Sh interface based on the Diameter protocol; Protocol details,“ 3GPP TS 29.329, V 12.5.0, January 2015. [Online]. Available: http://www.3gpp.org.

[50] „Generic Authentication Architecture (GAA); Support for subscriber certificates,“ 3GPP TS 33.221, V 12.0.0, September 2014. [Online]. Available: http://www.3gpp.org.

[51] „Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS),“ 3GPP TS 33.222, V 12.3.0, December 2013. [Online]. Available: http://www.3gpp.org.

[52] „Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function," 3GPP TS 33.223, V 12.0.0, December 2013. [Online]. Available: http://www.3gpp.org.

[53] „Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) push layer," 3GPP TS 33.224, V 12.0.0, September 2014. [Online]. Available: http://www.3gpp.org.

[54] „Short Message Service (SMS) capable Mobile Management Entities (MMEs) (Release 12)," 3GPP TS 29.338, V 12.5.0, December 2014. [Online]. Available: http://www.3gpp.org.

[55] „Telecommunication management; Charging management; Packet Switched (PS) domain charging," 3GPP TS 32.251, V 12.8.0, December 2014. [Online]. Available: http://www.3gpp.org.

[56] „Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging," 3GPP TS 32.260, V 13.0.0, December 2014. [Online]. Available: http://www.3gpp.org.

[57] „Telecommunication management; Charging management; Charging Data Record (CDR) transfer," 3GPP TS 32.295, V 12.2.0, December 2014. [Online]. Available: http://www.3gpp.org.

[58] „Telecommunication management; Charging management; Online Charging System (OCS): Applications and interfaces," 3GPP TS 32.296, V 12.3.0, December 2014. [Online]. Available: http://www.3gpp.org/.

[59] „Telecommunication management; Charging management; Diameter charging applications," 3GPP TS 32.299, V 12.7.0, December 2014. [Online]. Available: http://www.3gpp.org.

[60] „Cx and Dx interfaces based on the Diameter protocol; Protocol details," 3GPP TS 29.229, V 12.4.0, January 2015. [Online]. Available: http://www.3gpp.org/.

[61] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley a E. Schooler, „SIP: Session Initiation Protocol," IETF RFC 3261, June 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3261.txt.

[62] „Introduction to CCITT Signaling system No. 7," ITU-T Q.700, Mart 1993. [Online]. Available: http://www.itu.int.

[63] M. Handley, V. Jacobson a C. Perkins, „SDP: Session Description Protocol," IETF RFC 4566, July 2006. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4566.txt.

[64] H. Schulzrinne, C. U., A. Rao a R. Lanphier, „ Real Time Streaming Protocol (RTSP)," IETF RFC 2326, April 1998. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2326.txt.

[65] R. Fielding a J. Reschke, „Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing," IETF RFC 7230, June 2014. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7230.txt.

[66] N. Freed a N. Borenstein, „Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types," IETF RFC 2046, November 1996. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2046.txt.

[67] D. Mills, D. Mills, J. Martin, J. Burbank a W. Kasch, „Network Time Protocol Version 4: Protocol and Algorithms Specification," IETF RFC 5909, June 2010. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5905.txt.

[68] „Real-Time Transport Protocol (RTP) Parameters," IANA, [Online]. Available: http://www.iana.org/assignments/rtp-parameters/rtp-parameters.xhtml.

[69] M. Westerlund, „A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)," IETF RFC 3890, September 2004. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3890.txt.

[70] F. Andreasen, M. Baugher a D. Wing, „Session Description Protocol (SDP), Security Descriptions for Media Streams," IETF RFC 4568, July 2006. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4568.txt.

[71] M. Westerlund, I. Johansson, C. Perkins, P. O'Hanlon a K. Carlberg, „ Explicit Congestion Notification (ECN) for RTP over UDP," IETF RFC 6679, August 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6679.txt.

[72] „IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3," 3GPP TS 24.229, December 2014. [Online]. Available: http://www.3gpp.org/.

[73] B. Ramsdell a S. Turner, „Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," IETF RFC 5751, January 2010. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5751.txt.

[74] „Support of SMS over IP networks; Stage 3," 3GPP TS 24.341, December 2014. [Online]. Available: http://www.3gpp.org.

[75] B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema a D. Gurle, „Session Initiation Protocol (SIP) Extension for Instant Messaging," IETF RFC 3428, December 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3428.txt.

[76] B. Campbell, R. Mahy a C. Jennings, „The Message Session Relay Protocol (MSRP)," IETF RFC 4975, September 2007. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4975.txt.

[77] M. Garcia-Martin, M. Isomaki, G. Camarillo, S. Loreto a P. Kyzivat, „ A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer," IETF RFC 5547, May 2009. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5547.txt.

[78] C. Jennings, R. Mahy a A. B. Roach, „Relay Extensions for the Message Session Relay Protocol (MSRP)," IETF RFC 4976, September 2007. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4976.txt.

[79] „Infrastructure of audiovisual services – Communication procedures, Gateway control protocol: Version 3," ITU-T H.248.1, March 2013. [Online]. Available: Http://www.itu.int/rec/T-REC-H.248.1.

[80] „IMS Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW); Iq Interface; Stage 3," 3GPP TS 29.334, January 2015. [Online]. Available: http://www.3gpp.org.

[81] „Interconnection Border Control Functions (IBCF) - Transition Gateway (TrGW) interface, Ix interface; Stage 3," 3GPP TS 29.238, January 2015. [Online].

[82] „Media Gateway Controller (MGC) - Media Gateway (MGW) interface; Stage 3," 3GPP TS 29.232, January 2015. [Online]. Available: http://www.3gpp.org.

[83] „Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp interface: Procedures descriptions," 3GPP TS 23.333, January 2015. [Online]. Available: http://www.3gpp.org.

[84] H. Schulzrinne, H. Schulzrinne, R. Frederick a V. Jacobson, „RTP: A Transport Protocol for Real-Time Applications," IETF RFC 3550, July 2003. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3550.txt.

[85] „Real-Time Transport Protocol (RTP) Parameters," IANA, [Online]. Available: http://www.iana.org/assignments/rtp-parameters/rtp-parameters.xml.

[86] H. Schulzrinne a S. Casner, „RTP Profile for Audio and Video Conferences with Minimal Control," IETF RFC 3551, July 2003. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3551.txt.

[87] P. Zimmermann, A. Johnston a J. Callas, „ZRTP: Media Path Key Agreement for Unicast Secure RTP," IETF RFC 6189, April 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6189.txt.

[88] J. Arkko, E. Carrara, F. Lindholm, M. Naslund a K. Norrman, „MIKEY: Multimedia Internet KEYing," IETF RFC 3830, August 2004. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3830.txt.

[89] „IP Multimedia Subsystem (IMS) media plane security," 3GPP TS 33.228, September 2014. [Online]. Available: http://www.3gpp.org.

[90] P. Karn a W. Simpson, „Photuris: Session-Key Management Protocol," IETF RFC 2522, March 1999. [Online].

[91] H. Krawczyk, M. Bellare a R. Canetti, „HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, February 1997. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2104.txt.

[92] Y. Sheffer, R. Holz a P. Saint-Andre, „ Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)," IETF RFC 7457, February 2015. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7457.txt.

[93] E. Rescorla a N. Modadugu, „ Datagram Transport Layer Security Version 1.2," IETF RFC 6347, January 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6347.txt.

[94] R. Stewart, „Stream Control Transmission Protocol," IETF RFC 4960, September 2007. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4960.txt.

[95] M. Tuexen, R. Stewart, P. Lei a E. Rescorla, „Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)," IETF RFC 4895, August 2007. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4895.txt.

[96] M. Tuexen, R. Seggelmann a E. Rescorla, „Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)," IETF RFC 6083, January 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6083.txt.

[97] „Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 11)," ETSI TS 102 221, 11 2013. [Online]. Available: https://www.etsi.org/ .

[98] „Smart Cards;UICC-Terminal interface; Characteristics of the USB interface (Release 7)," ETSI TS 102 600, 4 2009. [Online]. Available: http://www.etsi.org.

[99] „Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7)," ETSI TS 102 613, 9 2008. [Online]. Available: http://www.etsi.org.

[100] „nter-Chip USB supplement to the USB 2.0 Specification, Inter-Chip USB supplement to the USB 2.0 Specification," USB Implementers Forum, Inc., USB Implementers Forum, Inc. 2006. [Online]. Available: http://www.usb.org/developers/docs/usb20_docs/.

[101] „Universal Serial Bus Communications Class Subclass Specification for Ethernet Emulation Model Devices," USB Implementers Forum, Inc., February 2005. [Online]. Available: http://www.usb.org.

[102] „Smart Cards; Card Application Toolkit (CAT) (Release 12),“ ETSI TS 102 223, 2014. [Online]. Available: http://www.etsi.org.

[103] P. Eronen a H. Tschofenig, „Pre-Shared Key Ciphersuites for Transport Layer Security (TLS),“ RFC 4279, December 2005. [Online].

[104] „Smart Cards; Secure channel between a UICC and an end-point terminal (Release 11),“ ETSI TS 102 484, 2012. [Online]. Available: http://www.etsi.org.

[105] „Technical Specification Group Services and System Aspects; Personalisation of Mobile Equipment (ME); Mobile functionality specification (Release 13),“ 3GPP TS 22.022, 2016. [Online]. Available: http://www.etsi.org.

[106] „Secure Element Access Control; Version 1.0,“ Global Platform, May 2012. [Online]. Available: http://www.globalplatform.org.

[107] „EMV, Integrated Circuit Card, Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal, Interface Requirements,“ EMVCo, LLC, November 2011. [Online]. Available: https://www.emvco.com.

[108] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson a H. Levkowetz, „ Extensible Authentication Protocol (EAP),“ IETF RFC 2284, June 2004. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3748.txt.

[109] J. Arkko a H. Haverinen, „Extensible Authentication Protocol Method for 3rd Generation, Authentication and Key Agreement (EAP-AKA),“ IETF RFC 4187, January 2006. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4187.txt.

[110] J. Arkko, V. Lehtovirta a P. Eronen, „Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'),“ IETF RFC 5448, May 2009. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5448.txt.

[111] „Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services,“ 3GPP TS 24.623, December 2014. [Online]. Available: http://www.3gpp.org.

[112] „Generic Authentication Architecture (GAA); Support for subscriber certificates,“ 3GPP TS 33.221, January 2016. [Online]. Available: http://www.3gpp.org.

[113] D. F. Ferraiolo a D. R. Kuhn, „Role-Based Access Controls,“ v *15th National Computer Security Conference*, Baltimore MD, 1992.

[114] L. Lamport, „Password Authentication with Insecure Communication,“ *Communications of the ACM,* sv. 24, č. 11, pp. 770-772, 1981.

[115] W. C. Ku, „A hash-based strong-password authentication, scheme without using smart card,“ *ACM Operating Systems Review, 38(1),* p. 29–34, 2004.

[116] H. Jung, H. S. Kim, B. Murgante, O. Gervasi a A. Iglesias, „Secure Hash-Based Password Authentication Protocol Using Smartcards,“ v *11th International Conference on Computational Science and Its Applications (ICCSA), PT V Book Series: Lecture Notes in Computer Science, Volume: 6786, Pages: 593-606*, 2011.

[117] M. Kim a C. K. Koc, „A secure hash-based strong-password authentication protocol using one-time public-key cryptography,“ *Journal of Computer and Systems Sciences International,* č. 45, p. 623–626, 2006.

[118] H. Jeong, D. Won a S. Kim, „Weaknesses and improvement of secure hash-based strong password authentication protocol,“ *Journal of Information Science and Engineering,* sv. 26, p. 1845–1858, 2010.

[119] Q. Jiang, J. Ma, G. Li a L. Yang, „ Robust Two-Factor Authentication and Key Agreement Preserving User Privacy,“ *IJ Network Security, 16(4),* pp. 321-332, 2014.

[120] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang a Z. Y. Feng, „Improvements of Juang's password authenticated key agreement scheme using smart cards,“ *IEEE Transactions on Industrial Electronics,* sv. 56, č. 6, pp. 2284-2291, 2009.

[121] „Secure Element Access Control,“ GlobalPlatform Device Technology, 2012. [Online]. Available: http://www.globalplatform.org.

[122] „TEE Protection Profile, Version 1.0,“ GlobalPlatform Device Committee, 2013. [Online]. Available: http://www.globalplatform.org/.

[123] R. M. Needham a M. D. Schroeder, „Using encryption for authentication in large networks of computers,“ *Communications of the ACM,* pp. 993-999, Volume 21 Issue 12, Dec. 1978 .

[124] C. Neuman, T. Yu, S. Harman a K. Raeburn, „The Kerberos Network Authentication Service (V5),“ IETF RFC 4120, July 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4120.txt.

[125] „Assertions and Protocols for the OASIS, Security Assertion Markup Language,“ OASIS, 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/.

[126] D. Hardt, „The OAuth 2.0 Authorization Framework,“ IETF RFC 6749, October 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt.

[127] M. Jones a D. Hardt, „The OAuth 2.0 Authorization Framework: Bearer Token Usage,“ IETF RFC 6750, October 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6750.txt.

[128] J. Richer, „ OAuth 2.0 Token Introspection," IETF RFC 7662, October 2015. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7662.txt.

[129] M. Jones, J. Bradley a N. Sakimura, „JSON Web Token (JWT)," IETF RFC 7519, May 2015. [Online]. Available: JSON Web Token (JWT).

[130] „OpenID Specifications," OpenID Foundation, 2015. [Online]. Available: http://openid.net/developers/specs/.

[131] „IP Multimedia Subsystem (IMS); Stage 2," 3GPP TS 23.228, September 2015. [Online]. Available: http://www.3gpp.org.

[132] L. Dostalek, „Authentication and authorization applications in 4G networks," v *Security and protection of information, ISSN 2336-5587, ISBN 978-80-7231-997-8*, Brno 2015, 2015.

[133] L. Dostalek a J. Ledvina, „Strong Authentication for Mobile Application," *International Conference of Applied Elecronics,* č. IEEE CFP1569A-PRT, pp. 23-26, September 2015.

[134] „Lawful interception architecture and functions," 3GPP TS 33.107, December 2015. [Online]. Available: http://www.3gpp.org.

[135] *Codes for the representation of currencies and funds,* International Standard ISO 4217, 2001.

[136] „TEE Protection Profile," GlobalPlatform Device Committee, August 2013. [Online]. Available: https://www.globalplatform.org/.

[137] D. Hardt, „The OAuth 2.0 Authorization Framework," IETF RFC 6749, October 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt.

[138] M. Jones a D. Hardt, „The OAuth 2.0 Authorization Framework: Bearer Token Usage," IETF RFC 6750, [Online]. Available: http://www.rfc-editor.org/rfc/rfc6750.txt.

[139] L. Adamec, „Testování biometrického systému založeného na dynamice podpisu," *Masarykova Univerzita Brno, Diplomová práce,* 2011.

23. Rejstřík

3

3GPP 16, 85

A

AAA 61
Access Point Name ..... *viz* APN
Access Rule Application ..... *viz* ARA
Access SBC ..... *viz* A-SBC
Access Server 61
Accounting 61
address-of-record ..... *viz* AOR
ADF 208
AF 172
AKA 31, 39, 97
ALG 169
AMF 40
AOR 128, 130, 131
APDU 208
  Secured 210
APN 24
Application Dedicated File ..... *viz* ADF
ARA 215
A-SBC 105, 132, 137, 156
ATR 203
ATS 203
AuC 39, 233
Autentizační centrum 39
Autetnizační server 97
Authentication 61
Authorization 61
AUTN 40

B

BBREF 92
Bearer 88, 137
Bearer Binding and Event Reporting Function 92
Bearer ID 58
Bearer Independent Protocol ..... *viz* BIP
BER-kódování 213
Bezpečnost
  end-to-access-edge 156
  end-to-end 156
  SDP 156
BGCF 27
BGFC 25, 172
Billing 83
BIP 207
BSF 97, 233
BTS 16
buňka 16

C

CBC 157
Cell Broadcast Centre
  CBC 157
CEN 200
CK 40, 41, 220
Comité Européen de Normalisation ..... *viz* CEN
Configuration Access Protocol ..... *viz* XCAP
Control Plane 23, 43, 165
Cookie 188
  Photuris 185
  stavová (SCTP) 194
CRM 12
C-RNTI 30

CSCF 27
CS-IBCF 171
CS-TrGW 171
Customer relationship management . *viz* CRM

Č

Čipové karty 197
bezkontaktní 198
duální 198
hybridní 198
inlay 198
terminál 198

D

Data Bearer 23
Data Radio Bearer 47
Datagram Transport Layer Security ... *viz* DTLS
Datový nosič 23, 137
DDoS 59
DEA 73
Dedicated Bearer 23
Default Bearer 23
De-personalizace 209
DF208
Diameter 61
agent 63
aplikace 68
Attribute-Value-Pair 65
Base Accounting 83
Base Accounting 62
Credit Control 85
Credit Control Application 62
Diameter Base Protocol 61
Diameter hub 72
Diameter Translation Agent 61
DNS směrování 77
Doména 74
Edge Agent 73
Hop-by-Hop Identifier 65
Peer Discovery 75
Proxy Agent 70
Realm 74
Realm Routing Table 70
Redirect Agent 71
Referenční body 3GPP 85
relace 64
Relay Agent 70
Routing Agent 72
Session-Identifier 64
Směrování 64, 76
Spojení 64
stavový agent 64
transakce 65
Translation Agent 71
DNS 141
ENUM 142
NAPTR 141
S-NAPTR 77, 78
Dokument 9303 200
DRA 72
DTLS 139, 186, 195
DTMF 172
Dual-Tone Multi-Frequency ..... *viz* DTMF

E

E.164 172
e2ae 183
e2e 183
EAP 217
EAP-AKA 218
EAP-AKA‘ 218
EATF 27
E-CGI 31
E-CSCF 27
EEA 57
EF
interní 208
pracovní 208
EIA 58
EIR 21, 91
eMLPP 223

EMM 52
eNB 16, 43
End-to-access edge security ..... *viz* e2ae
End-to-end security ..... *viz* e2e
EPC 21
EPS 20, 43, 217, 228
EPS Encryption Algorithm 57
EPS Integrity Algorithm 58
EPS Session Management 52
eSE 200, 213, 230
ESM 52
Ethernet
  emulace 206
ETSI 199
ETSI *(European Telecommunications Standards Institute)* 199
eUICC 230
Event Triggers 93
Evropská občanská karta 200

F

FDN 222
Femtocell 19, 217
Forward and backward secrecy 242
Funkce
  f1 až f5 40

G

GAA 233
GBA 96, 217, 233
Generic Authentication Architecture ... *viz* GAA
Generic Bootstrapping Architecture .... *viz* GBA
GGSN 21
GlobalPlatform 199
GSM 15, 16, 217
GSMA 16
GUMMEI 30
GUTI 30

H

H.248 165
  Kontext 167
  Ukončení (Termination) 167
hardwarové klíče 197
HCI 202
HeNB 19, 60, 217
HMAC 194
`HMAC-SHA-256` 57
HSM 197
HSS 12, 21, 24, 40, 43, 97, 132, 233
HTTP 149

Ch

Charging 23
Charging Control Information 93
Charging systems 20

I

I^2C 202
IANA 67, 85
IBCF 25, 27, 171
IC USB 205
ICAO 199
ICC 198
I-CSCF 27
IK 40, 41
IM Media Gateway ..... *viz* IM-MGW
IMEI 21, 91
  zobrazení 33
IMPI 28, 31
IMPU 28, 31, 228
IMS 21, 24, 217, 228
IMS Access Gateway ..... *viz* IMS-AGW
IMS Application Level Gateway ..... *viz* ALG
IMS-AGW 28
IMS-ALG 27
IMSI 22, 220
Inlay ..... *viz* Čipové karty

Instant Messaging 24, 101, 161
Integrated Circuit Card ..... *viz* ICC
Interconnection Border Control Function .... *viz* IBCF
International Civil Aviation Organization .... *viz* ICAO
Internet Message Format" 110
IPsec 19
IP-SM-GW 158
IPX 35
I-SBC 105
I-SCSF 172
ISIM 15, 32, 132
ITU 16
i-WLAN 217

J

JWT 248

K

K_{ASAME} 56
KDF 57
Key freshness 242

L

LAI 221
Local breakout 55
LTE 16, 20, 61, 217
LTE Advanced 17

M

MAC 46
MAC-A 40
Macro Cell 18
Man-Machine Interface ..... *viz* MMI
Master File ..... *viz* MF
Media Gateway ..... *viz* MG, *viz* MG
Media Gateway Control Function .... *viz* MGFC
Media Gateway Controller ..... *viz* MGC
Media Plane 23, 44, 165
Medium Access Control 46
MF 208
MG 104, 165
MGC 104, 165
MGCF 27
MGFC 25, 171
Micro Cell 18
MIFARE™ 198
MIME 149
Mixování medií
H.248 167
MKI 182
MME 21, 43
M-MGW 171
MMI 33
Modem 15
MRFC 172
MRFP 172
MSIN 28
MSISDN 222
MSRP 158, 161
MSRP URI 164
M-TMSI 30
Multimedia Resource Function Controller .. *viz* MRFC
Multimedia Resource Function Processor .. *viz* MRFP

N

NAF 233
NAI 74, 77
NAPTR 78
NAS 43, 52, 82
Network Access Identifier 74
NFC 203, 217, 218
Node B 16
Non Access Stratum 52, 157
Non-Access Stratum ..... *viz* NAS

O

OAuth 2.0 248
OAuth 2.0. 218
Občanský průkaz 200
OCS 98
Odposlech 255
Off-line Charging 62
Online Charging System 98
OpenID Connect 248
OSN 200
OTA 31, 211, 217

P

Packet Data Convergence Protocol 46
PCC 88, 94
PCEF 88
PCI 30
PCRF 22, 24, 43, 91
P-CSCF 24, 27, 37, 94, 132, 137, 146, 147
PDCP 45
Perfect forward secrecy 241
Personalizace 209
PGW 43
Philips Electronics 198
Photuris
  protokol 185
Point of Presence 61
Policy and Charging Control 88, 94
Policy and Charging Enforcement Function 88
Policy and Charging Rules Function 91
PoP 61
Presentity 129
Privátní identita účastníka 28
Protokol
  DTLS ..... *viz* DTLS
  RTP/RTCP ..... *viz* RTP
  S1AP 43
  SCTP ..... *viz* SCTP
  SWP 200
  TLS 186
P-TMSI 222
Push to talk over Cellular 34, 102

R

Radio Bearer 43, 47
Radio Link Control 46
Radio Resource Control 45
RADIUS 61, 71
RAI 222
RAND 40
RBAC 248
Real-time Transport Protocol ..... *viz* RTP
Referenční bod 15
  Cx 95
  Gm 140
  Gx 88
  Gxc 92
  Gxx 92
  Gy 99
  H.248 ..... 166, 256
  HI1 až HI3 255
  Iq 169
  Ix 171
  Mb 140
  Mc 169
  Mn 171
  Mp 172
  Rf 99
  Ro 99
  Rx 94
  S11 43
  S13 91
  S13' 91
  S1-C 43
  S1-MME 43
  S5/S8 43
  S6a 61, 89
  S6d 89
  SBc 157
  Sd 22, 91
  SGc 33, 157, 221

Sh 96
Sy 98
Ua 97, 234
Ub 97, 234
Un 19
Ut 97, 236
Uu 45
X1 až X3 255
X2 43
Zh 96, 234
Zn 96, 234
Relay Node 19
Remote Radio Head 19
RFC 16
Rich OS 214
RLC 46
Roaming 35
Roaming LTE 35
Home Routed 35
Local Break Out LTE 35
Roaming VoLTE 36
RRC 45
RTCP 178
end-to-end monitoring 178
RTP 101, 175
Contributing source identifier 177
jitter elimination 175
mixer 177
Synchronization source identifier 176
RTP/RTCP 165
RTS 149
Rychlé zasílání zpráv .... *viz Instant Messaging*

S

S/MIME 139, 156
SAML 246
SBC 24, 104, 165
S-CSCF 24, 27, 132, 172
SCTP
asociace 191
four-way handshake 189
chunk 192
Multi homing 193
multi-straming 192
Stream Sequence Number (SSN) 192
Transmission Sequence Number (TSN) .192
SCWS 207
SDES 182
sdílené tajemství K 31
Sdílené tajemství K 40
SDP 101, 149
SE 199, 213
Secure APDU 212
Secure Element ..... *viz* SE
Secure Messaging 210
Security Domain 215
Application Providers' 215
Issuers' 215
Security Domains
Controlling Authorities' 215
Security Gateway 19
SEG 28
Service Radio Bearer 47
Session Border Controller ..... *viz* SBC
Session control 24
Session Description Protocol .. *viz* SDP, *viz* SDP
Session Initiation Protocol ..... *viz* SIP
Session key agreement 241
SGSN 21
SGW 21, 43
Short Message Service ..... *viz* SMS
Signalizace sítě 23
Signalizační bouře 59
Signalling Radio Bearer 47
SIP 101, 149
Back-to-Back User Agent (B2BUA) 103
event 129
Event State Compositor (ESC) 103, 129
Gateway 103
Lokalizační databáze 131
Odchozí proxy ..... *viz Outboud proxy*
Outbound Proxy 103
Paging 158

Policy server ... 103
Proxy, *Proxy Server* ... 102
Redirect Server ... 103
Register ... 103
Registrátor ... 103
Relay ... 103
Server ... 102
Upsání se ... 138
User Agent (UA) ... 102
User Agent Client (UAC) ... 102
User Agent Server (UAS) ... 102
SIP URI ... 25, 28, 107, 141
Smart Card Web Server ... *viz* SCWC
SMS ... 157
brána ... 157
přes IP ... 158
SPI ... 202
SPIT ... 146
SQN ... 40
SRB1 ... 47
SRB2 ... 47
SRTCP ... 183
SRTP ... 32, 182
Authentication Tag ... 183
Key Management Service ... 183
master key ... 182
SSC ... 222
Standard
ISO 14443 ... 198, 218
ISO 15693 ... 198
ISO 7816 ... 198
S-TMSI ... 30
Stream Control Transmission Protocol ... *viz* SCTP
SWP ... *viz* Protokol SWP

T

T=0 ... 198
T=1 ... 198, 202
TACACS+ ... 71
TAI ... 31
TAU ... 52
TCP ... 61
TDF ... 91
TDM ... 165
TEE ... 199, 214
TEL URI ... 28, 107, 141, 171
TETRA ... 34
Tetrapol ... 34
TLS ... 139
TLS PSK ... 207, 236
TLV formát ... 213
TMSI ... 221
Toll fraud ... 146
Tracking Area ... 17
Tracking Area Update ... 52
Traffic Detection Function ... 91
Transition Gateway ... *viz* TrGW
TrGW ... 27, 171
Trojský kůň ... 197
Trusted Execution Environment ... *viz* TEE, *viz* TEE

U

UART ... 201
Účtování ... 62
UDP ... 61
UICC ... 31, 199
UICC1 ... 217
UICC2 ... 217
UMTS ... 16
Universal Integrated Circuit Card ... *viz* UICC
USB ... 200, 205
User Plane ... 23, 44
USIM ... 15, 22, 32, 132

V

Veřejná identita ... 28
VoIP ... 15
VoLTE ... 15, 24

W

Watcher 129
Wireshark 255

X

XCAP 233
XRES 40

Z

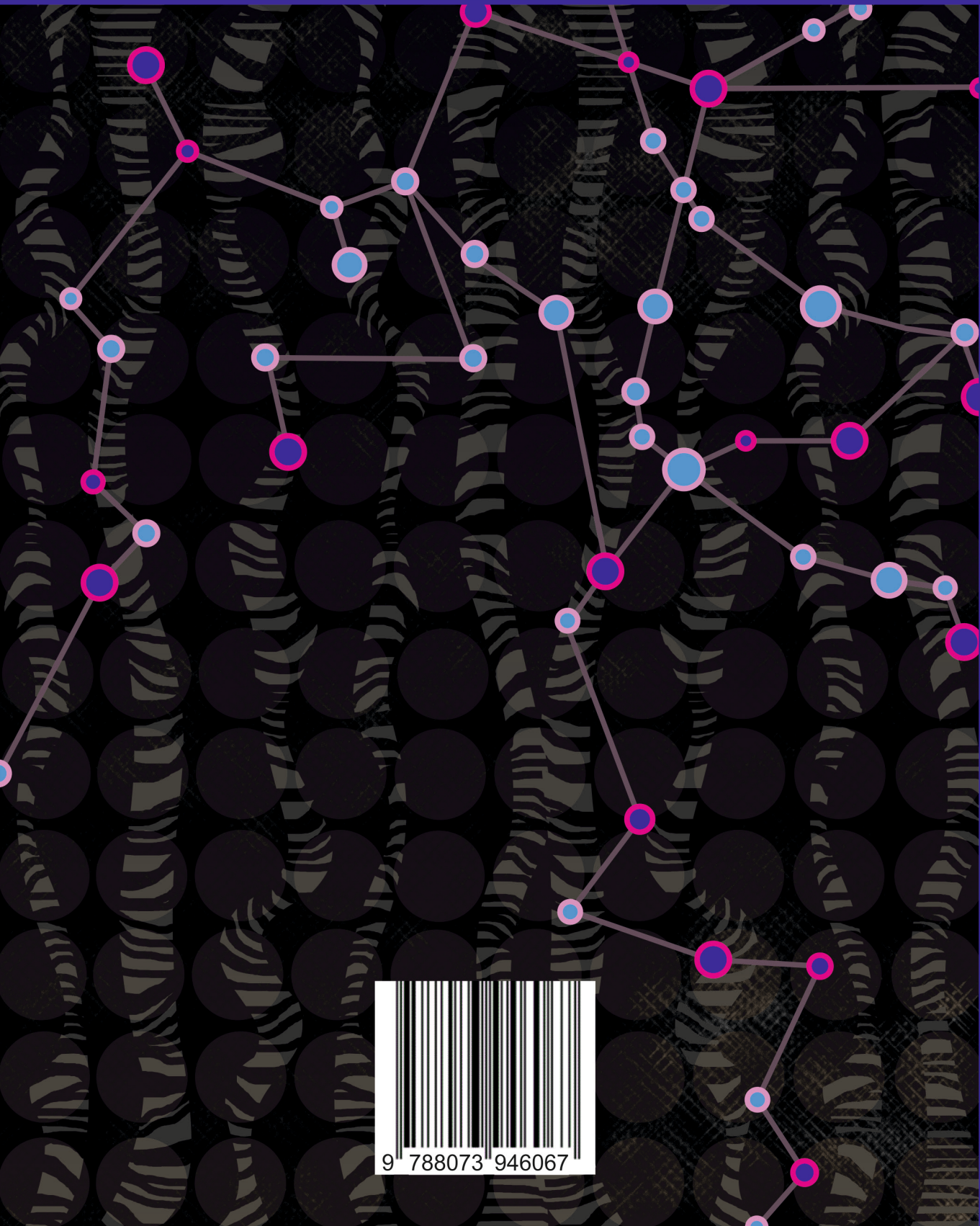
Základnové stanice 16
Zero Knowledge 242
Zmáčkni a mluv ..*viz Push to talk over Cellular*
zpoplatňovací systémy 20

24. Přehled zkratek

3GPP	*The 3rd Generation Partnership Project*
ACE	*Access Control Enforcer*
ADF	*Application Dedicated File*
AF	*Aplikační funkce*
AGW	*IMS Access Gateway*
AKA	*Authentication and Key Agreement*
ALG	*IMS Application Level Gateway*
AMF	*Authentication Management Field*
AOR	*Address-of-Record (SIP)*
APN	*Access Point Name*
ARA	*Access Rule Application*
AS	*Access Stratum*
A-SBC	*Access SBC*
ATR	*Answer To Reset*
ATS	*Answer To Select*
AuC	*Autentizační centrum*
AVP	*Attribute-Value-Pair*
B2BUA	*SIP Back-to-Back User Agent Client*
BBREF	*Bearer Binding and Event Reporting Function*
BGCF	*Breakout Gateway Control Function*
BSF	*Bootstrapping Server Function*
BTS	*Base Transceiver Station*
CBC	*Cell Broadcast Centre*
CEN	*Comité Européen de Normalisation*
CSCF	*Call Session Control Function*
CSRC	*Contributing source identifier (RTP)*
cwnd	*Congestion window (SCTP)*
DeNB	*Donor eNB*
DF	*Dedicated File*
DRA	*Diameter Routing Agent*
DTLS	*Datagram Transport Layer Security*
DTMF	*Dual-Tone Multi-Frequency*
e2ae	*End-to-access edge security*
e2e	*End-to-end security*
E-CSCF	*Emergency CSCF*
EEA	*EPS Encryption Algorithm*
EIA	*EPS Integrity Algorithm*
EIR	*Equipment Identity Register*
EMM	*EPS Mobility Management*
eNB	*evolved Node B (též E-UTRAN Node B)*
ENUM	*tElephone NUmber Mapping*
EPC	*Evolved Packet Core*
ESC	*SIP Event State Compositor*
eSE	*Embedded Secure Element*
ESM	*EPS Session Management*
ETSI	*European Telecommunications Standards Institute*
eUTRAN, E-UTRAN	*Evolved Universal Terrestrial Access Network (4G RAN)*
GAA	*Generic Authentication Architecture*
GBA	*Generic Bootstrapping Architecture*
GGSN	*Gateway GPRS Support Node*
GSM	*Groupe Spécial Mobile*
GSMA	*GSM Association*
GTP	*GPRS Tunnelling Protocol*
GTP-C	*GPRS Tunnelling Protocol for Control Plane*
GTP-U	*GPRS Tunnelling Protocol User Plane*

HeNB	*Home eNB*
HSS	*Home Subscriber Server*
IBCF	*Interconnection Border Control Function*
ICAO	*International Civil Aviation Organization*
ICC	*Integrated Circuit Card (čipová karta)*
I-CSCF	*Interconnect CSCF*
IMEI	*International Mobile Equipment Identity*
IM-MGW	*IM Media Gateway*
IMPI	*IP Multimedia Private Identity*
IMPU	*IP Multimedia Public Identity*
IMS	*Internet Multimedia Subsystem*
IMS-AGW	*IMS Access Gateway*
IMSI	*International Mobile Subscriber Identity*
IPX	*IP eXchange*
I-SBC	*Interconnect SBC*
ITU	*International Telecommunication Union*
LTE	*Long Term Evolution*
MAC	*Medium Access Control*
MF	*Master File*
MG	*Media Gateway (SBC)*
MGC	*Media Gateway Controller (SBC)*
MGFC	*Media Gateway Control Function*
MKI	*Master Key Identifier (SRTP)*
MME	*Mobility Management Entity*
MMI	*Man-Machine Interface*
MRFC	*Multimedia Resource Function Controller*
MRFP	*Multimedia Resource Function Processor*
MSIN	*Mobile Subscription Identification Number*
MSRP	*Message Session Relay Protocol*
NAF	*Network Application Function*
NAI	*Network Access Identifier*
NAPTR	*Name Authority Pointer*
NAS	*Non-Access Stratum*
NB	*Node B*
NFC	*Near Field Communications*
OCS	*Online Charging Systém*
OTA	*Over The Air*
PCC	*Policy and Charging Control*
PCRF	*Policy and Charging Rules Function*
P-CSCF	*Proxy CSCF*
PDCP	*Packet Data Convergence Protocol*
PGW	*PDN GW, Public Data Network Gateway*
RAN	*Radio Access Network*
RFC	*Requests for Comments*
RLC	*Radio Link Control*
RN	*Relay Node (Vykrývací základnová stanice)*
RRC	*Radio Resource Control*
RRH	*Remote Radio Head*
RTCP	*Real-Time Control Protocol*
RTS	*Real Time Streaming Protocol*
SBC	*Session Border Controller*
S-CSCF	*Serving CSCF*
SCTP	*Stream Control Transmission Protocol*
SCWS	*Smart Card Web Server*
SDP	*Session Description Protocol*
SE	*Secure Element*
SEG	*Security Gateway*

SGSN	*Serving GPRS Support Node*
SGW	*Serving Gateway*
SIP	*Session Initiation Protocol*
SMS	*Short Message Service*
SPIT	*Spam over IP telephone*
SRTCP	*Secure RTCP*
SRTP	*Secure Real-time Transport Protocol*
SSN	*Stream Sequence Number (SCTP)*
SSRC	*Synchronization source identifier (RTP)*
TAU	*Tracking Area Update*
TDF	*Traffic Detection Function*
TEE	*Trusted Execution Environment*
TETRA	*Terrestrial Trunked Radio*
TLS	*Transport Layer Security*
TrGW	*Transition Gateway*
TSN	*Transmission Sequence Number (SCTP)*
UA	*SIP User Agent*
UAC	*SIP User Agent Client*
UART	*Universal Asynchronous Receiver Transmitter*
UAS	*SIP User Agent Server*
UICC	*Universal Integrated Circuit Card*
UMTS	*Universal Mobile Telecommunication System*
UTRAN	*Universal Terrestrial Radio Access Network (3G RAN)*
VoIP	*Voice over IP*
VoLTE	*Voice over LTE*
XCAP	*Configuration Access Protocol*


9 788073 946067