Henri Haavisto

# TIETOTURVA MOBIILIVERKOISSA

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
2009

# TIIVISTELMÄ

TIETOTURVA MOBIILIVERKOISSA

Haavisto, Henri
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2009
Aromaa, Juha
UDK: 621.395
Sivumäärä: 37

Asiasanat: autentikointi, tietoturva, matkapuhelinjärjestelmät, UMTS

---

Tässä opinnäytetyössä tutustuttiin mobiiliverkoissa käytettäviin tietoturvaratkaisuihin. Työssä käsiteltiin tilaajan ja palvelun autentikointiin liittyvä teoria sekä GSM- että 3G-verkoissa ja todettiin GSM-verkon osalta toiminta Satakunnan ammattikorkeakoulun NGN-laboratorion matkapuhelinverkossa. Lisäksi tutkittiin, mitä muutoksia tietoturvaan SAMK:n verkkoon tehtävät 3G-päivitykset tuovat.

# ABSTRACT

SECURITY IN MOBILE NETWORKS

Haavisto, Henri
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme of Information Technology
May 2009
Aromaa, Juha
UDC: 621.395
Number of pages: 37

Key words: authentication, security, mobile networks, UMTS

---

The security solutions used in mobile networks were studied in this thesis. The theory of subscriber and service authentication in GSM and 3G networks was presented and investigated in the Satakunta University of Applied Sciences NGN laboratory network. The ongoing 3G updates of the network were also taken in consideration.

# SISÄLLYS

# LYHENTEET

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AAA | Authentication, Authorization and Accounting |
| AMF | Authentication Management Field |
| AVP | Attribute Value Pair |
| AuC | Authentication Centre |
| BSS | Base Station Subsystem |
| EIR | Equipment Identity Register |
| CHAP | Challenge-Handshake Authentication Protocol |
| COPS | Common Open Policy Service Protocol |
| DNS | Domain Name Service |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| HLR | Home Location Register |
| IANA | Internet Assigned Numbers Authority |
| IETF | Internet Engineering Task Force |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| ISDN | Integrated Services Digital Network |
| MD5 | Message-Digest algorithm 5 |
| MSC | Mobile Switching Centre |
| MSISDN | Mobile Station ISDN |
| NAS | Network Access Server |
| PAP | Password Authentication Protocol |
| PIN | Personal Indentity Code |
| PPP | Point-to-Point Protocol |
| QoS | Quality of Service |
| RADIUS | Remote Access Dial In User Service |
| RAN | Radio Access Network |
| RNC | Radio Network Controller |
| SGSN | Serving GPRS Support Node |
| SIM | Subscriber Identity Module |
| SN | Serving Network |
| SNMP | Simple Network Management Protocol |

| | |
|---|---|
| TCP | Transmission Control Protocol |
| TMSI | Temporary Mobile Subscriber Id |
| VLR | Visitor Location Register |
| UDP | User Datagram Protocol |
| UICC | Universal Integrated Circuit Card |
| USIM | Universal Subscriber Identity Module |

# 1 JOHDANTO

Tilaajien ja verkon keskusten välisellä todentamisella eli autentikoinnilla on mobiiliverkoissa hyvin keskeinen merkitys. Käyttäjille pitää pystyä takaamaan turvallinen pääsy verkon eri palveluihin ilman, että henkilökohtaiset tiedot joutuvat vääriin käsiin. Meneillään oleva siirtymävaihe 2G GSM-verkoista 3G-verkkoihin tuo omia haasteita ja muutoksia käytettyihin tietoturvaratkaisuihin. 3G tuo mukanaan uudet USIM-kortit, jotka tuovat käyttäjälle uusia palveluita ja mahdollisuuden hyödyntää 3G:n tietoturvamenetelmiä. Asioiden käsittely on erityisen ajankohtaista, koska Satakunnan ammattikorkeakoulussa 3G-päivitykset ovat parhaillaan menossa (Kevät/Kesä 2009).

# 2 AUTENTIKOINTI VERKOSSA

## 2.1 Tietoturva GSM

Käyttäjien yksityisyyden suojaaminen, autentikointi ja tiedon salaaminen ovat tärkeässä osassa GSM-verkoissa. GSM on mahdollistanut tehokkaiden algoritmien ja salauksien käytön. GSM-verkon tietoturvakysymykset voidaan jakaa neljään eri kohtaan:

- Tilaajan yksityisyyden suojaaminen
- Tilaajan autentikointi
- Merkinantotietojen suojaaminen
- Fyysisten linkkien tietoturva /2

### 2.1.1 Tilaajan yksityisyyden suojaaminen

Jokaisella puhelinlaitteella on sille ominainen IMEI-tunnus (International Mobile Equipment Identity), jonka avulla laite pystytään yksilöimään verkossa. Jos operaattorin verkossa on käytössä laiterekisteri EIR (Equipment Identity Register), pystytään esimerkiksi varastetun puhelimen käyttö estämään IMEI-tunnuksen avulla. /1

Tilaajalla voi olla useampia kansainvälisiä MSISDN (Mobile Station ISDN) puhelinnumeroita, joten tilaajan tunnistamiseksi verkossa on käytettävä IMSI-tunnusta (International Mobile Subscriber Identity). 15-merkkisen IMSI:n avulla pystytään yksilöimään tilaaja ja kohdistamaan esimerkiksi sille kuuluvat tietoliikennemaksut. /1

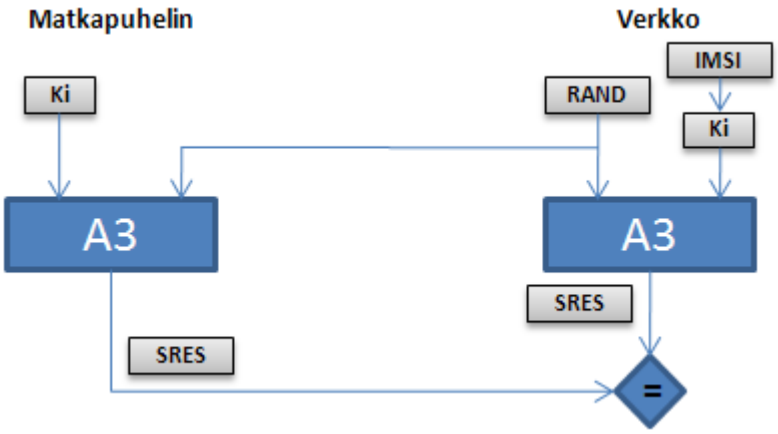
GSM-verkossa voidaan myös käyttää TMSI-tunnusta (Temporary Mobile Subscriber Identity). Se on vierailijarekisteri VLR:n antama uniikki tunnus, jonka avulla tilaaja on tunnistettavissa verkossa. Uusi tunnus annetaan aina kun tilaaja siirtyy sijaintialueelta toiselle, tällöin edellinen tunnus vapautuu muiden käyttöön. IMSI:n ja TMSI:n välinen yhteys on tallennettu VLR:ään. /2

### 2.1.2 Tilaajan autentikointi

SIM-kortti (Subscriber Identity Module) on älykortti, joka sisältää tilaajan tunnistetietoja ja autentikoinnin parametrejä. Käyttäjän on mahdollista tallentaa kortille puhelinnumeroita, tekstiviestejä ja esimerkiksi roaming-verkkojen tietoja. Kortti on yhteensopiva kaikkien GSM-puhelinten ja verkkojen kanssa (periaatetasolla), sen etuna on myöskin palveluiden helppo lisääminen ja poistaminen. Käyttäjän on mahdollista määrittää kortille nelinumeroinen PIN-koodi (Personal Indentity Code), jota kysytää aina kun puhelimeen kytketään virrat. Ilman koodin syöttämistä ainoastaan hätäpuhelut ovat mahdollisia. PIN -koodin syöttämistä voidaankin nimittää autentikoinnin ensimmäiseksi askeleeksi. /1

SIM-kortti sisältää tilaajan tunnistetietoja ja autentikoinnissa käytettäviä tunnistealgoritmeja kuten A3 ja A8. SIM-kortilla on myös kullekin tilaajalle määritelty tilaajakohtainen salausavain Ki. A5-algoritmi on tallennettu päätelaitteeseen ja tukiasemalaitteistoon. Kun tilaaja liitetään kotiverkkoon ensimmäistä kertaa, saa se Ki-avaimen, jota käytetään IMSI:n ohella käyttäjän tunnistuksessa. Kotiverkossa Ki on tallennettu todennuskeskukseen AuC (Authentication Centre). /1 /2

Autentikointi perustuu A3-algoritmin käyttöön sekä tilaajan että verkon päässä. Algoritmi laskee SRES-arvon (Signature Response) autentikointioavaimesta Ki ja verkon antamasta satunnaisluvusta RAND (lukuarvo väliltä 0..2^128-1). Matkapuhelinkeskus välittää SRES-arvon verkolle, joka vertaa sitä omaan arvoonsa. Arvojen ollessa erilaiset autentikointi epäonnistuu ja puhelu katkaistaan. Satunnaisluku RAND vaihtuu jokaisella autentikointikerralla, eikä sen arvoa voi etukäteen määritellä tai ennustaa. /2




Kuva 1. Todennus verkossa

Verkon ei tarvitse laskea RAND:ia ja SRES:iä jokaisella yhteydenotolla, vaan AUC voi laskea ne valmiiksi ja tallentaa kotirekisteri HLR:ään. Sieltä ne voidaan lähettää pyytävälle vierailijarekisterille VLR, jolloin tilaajan autentikointi pystytään suorittamaan. Toiminnon avulla saavutetaan parempi turvallisuus käyttäjän tietojen salaamisessa ja autentikointiavain Ki pystytään pitämään turvassa AUC:ssa. /2

## 2.2 Tietoturva 3G

3G-tietoturva rakentuu GSM-tietoturvan päälle ja se jatkaa hyväksihavaittujen ratkaisuiden kehittämistä. Tavoitteena on myös maksimoida GSM:n ja 3G:n välinen yhteensopivuus, jolloin esimerkiksi GSM-käyttäjällä on mahdollista vierailla 3G-verkossa ja saada silti GSM-tietoturvaratkaisut käyttöönsä. 3G:n tietoturva:

- Mahdollistaa käyttäjille turvallisen pääsyn 3G-palveluihin ja suojaa radiolinkeillä tapahtuvilta hyökkäyksiltä.
- Suojaa verkon solmujen välisen merkinantoinformaation siirron.
- Mahdollistaa päätelaitteen turvallisen käytön (USIM).
- Toteuttaa sovellusten turvallisen viestienvaihdon sekä käyttäjän että operaattorin päässä.
- Mahdollistaa käytössä olevien tietoturvaratkaisujen tarkkailemisen ja konfiguroimisen. /7

### 2.2.1 Tilaajan yksityisyyden suojaaminen

3G-verkoissa on mahdollistra käyttää päätelaitteissa USIM-kortteja (Universal Subscriber Identity Module). Pääero GSM:n SIM-korttiin on se, että USIM:n informaatio on luettavissa ja päivitettävissä radiotien kautta. Verkon tietoturvaa parantaa myös se, että USIM pystyy autentikoimaan tukiaseman, GSM-verkossa ainoastaan käyttäjä tunnistetaan. UICC (Universal Integrated Circuit Card) sisältää sekä SIM:n että USIM:n, joten korttia on mahdollista käyttää myös 2G GSM-verkoissa. /6

USIM sisältää tyypillisesti viidenlaista dataa, jotka ovat operaattori- ja käyttäjäkohtaisia:

- Hallinnollinen data sisältää kortin valmistajan ja operaattorin asettamia tietoja, kuten autentikoinnissa käytetyt avaimet ja IMSI.
- Verkon väliaikainen data koostuu esimerkiksi sijaintialueen tiedoista, TMSI:stä ja lasketuista turva-avaimista.
- Palveluun liittyvä data kertoo eri palveluiden käyttöoikeuden ja saatavuuden. Vaikka itse päätelaite tukisi palvelua saattaa käyttäjän USIM:stä kyseinen palvelu olla estetty. Mahdollisia palveluita voivat esimerkiksi olla palvelunumerot, estetyt numerot, puheluiden tiedot ja erilaiset raportit.
- Ohjelmat: USIM voi sisältää pieniä palvelukohtaisia ohjelmia, esimerkiksi erilaiset JAVA-ohjelmat.
- Henkilökohtainen data on käyttäjän tallentamaa tietoa, mm. yhteystiedot ja tekstiviestit.

USIM voi sisältää monta eri profiilia, joilla on eri tarkoituksensa. Profiilien perusteella määritellään käyttäjälle näkyvä informaatio. /6

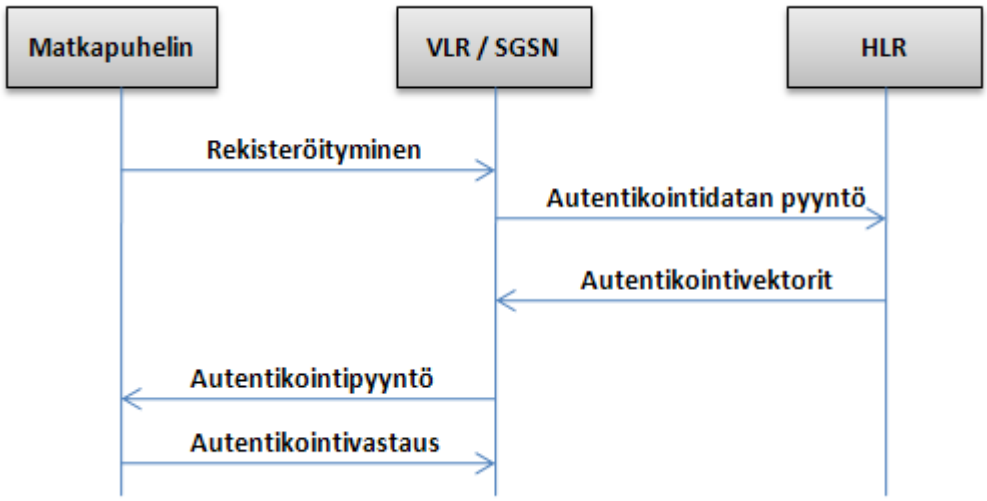
### 2.2.2 Autentikointi

3G autentikointiprosessissa on mukana kolme osapuolta, kotiverkko HLR, palveleva verkko SN (VLR, SGSN) ja päätelaitteen USIM. Autentikointi tapahtuu molemmissa suunnissa, SN (Serving Network) tarkastaa käyttäjän identiteetin, kun taas käyttäjä tarkastaa HLR:ltä, että SN on valtuutettu tekemään autentikointiopyyntöjä.

Järjestelmän avulla varmistuu, että käyttäjä on oikeassa verkossa kiinni, eikä esimerkiksi “valeverkossa”. Tämä kohentaa huomattavasti mobiiliverkon tietoturvaa. /6

Käyttäjän USIM:lle ja HLR:n tietokantaan on tallennettu 128-bittinen K-avain, joka on autentikoinnin yksi tärkeä osa. Jokaisen autentikointitapahtuman alussa luodaan myös väliaikaiset autentikointiavaimet. Käyttäjän tunnistaminen alkaa kun käyttäjän IMSI tai TMSI on siirretty SN:lle. SN lähettää tämän jälkeen “authentication data request”-pyynnön kotiverkon AuC:lle. AuC sisältää käyttäjien K-avaimet ja tiedon IMSI:stä, niiden avulle se pystyy luomaan käyttäjille autentikointivektorit. Ne lähetetään takaisin SN:lle “authentication data response”-sanomassa. Sanomien lähetys tapahtuu MAP-protokollan avulla. /6

SN lähettää päätelaitteelle “user authentication request”-sanoman, joka sisältää parametrit RAND ja AUTN. Niiden avulla päätelaitteen USIM suorittaa K-avaimen kanssa autentikointilaskelmat. Laskelmien avulla USIM pystyy varmistamaan, että AUTN on luotu AuC:ssa. Jos tilanne on tämä, lähetetään parametri RES SN:lle “user authentication response”-viestissä. SN vertailee RES ja autentikointivektorin XRES arvoja keskenään. Mikäli ne ovat samat, on autentikointitapahtuma onnistunut. Jos tarkistustulokset eivät ole samoja, täytyy autentikointi keskeyttää ja lähettää virheilmoitus. /6

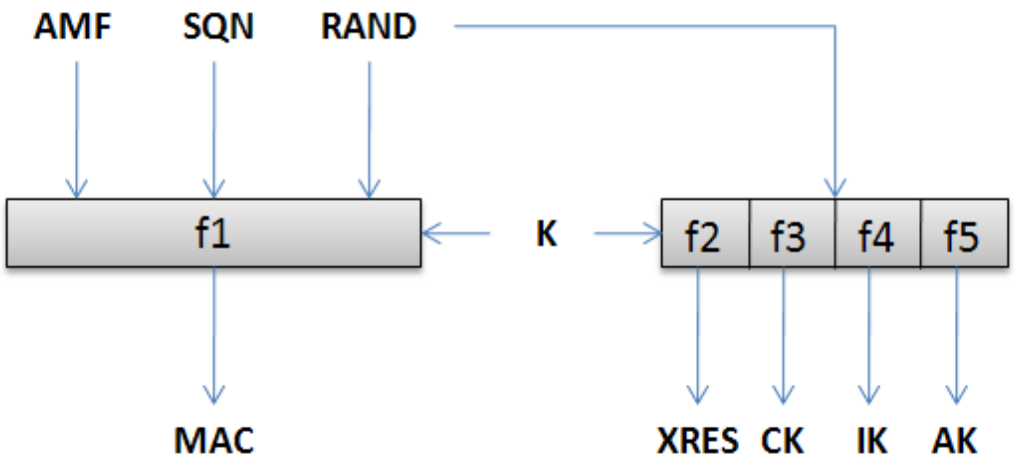



Kuva 2. Autentikointitapahtuman kulku.

Autentikointivektoreitten luonti alkaa AuC:ssa sekvenssinumeron SQN valinnalla. Sekvenssinumero on kasvava luku, tällä varmistetaan, että sitä ei ole käytetty aikaisemmin. Ohessa luodaan myös 128-bittinen satunnaisluku RAND. Autentikointivektori lasketaan yksisuuntaisen funktion avulla. Yhteensä näitä funktioita tarvitaan viisi, f1, f2, f3, f4 ja f5. F1 eroaa muista sillä, että sen laskemiseen käytetään neljää eri parametria, pääavain K, RAND, SQN ja AMF (Authentication Management Field). Muissa vain K ja RAND. /6

Tuloksina saadaan:

- f1 -> MAC (Message Auth Code) 64-bittiä
- f2 -> XRES 32-128-bittiä
- f3 -> CK 128-bittiä
- f4 -> IK 128-bittiä
- f5 ->AK 64-bittiä




Kuva 3. Autentikointivektoreitten luonti.

Samankaltaiset autentikointimäärittelyt tehdään myös USIM:n puolella, kuitenkin hieman eri järjestyksessä. F5 on laskettava ensin f1:stä, koska sitä käytetään SQN:n piilottamisessa. Näin toimitessa mahdollinen hyökkääjä ei voi päästä käyttäjän identiteettiin käsiksi. /6

# 3 PALVELUN AUTENTIKOINTI

## 3.1 Remote Access Dial-In User Service (RADIUS)-protokolla

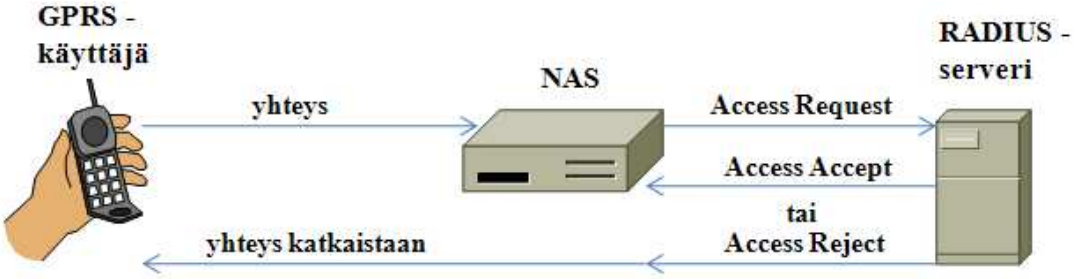
Huomattiin, että on käytännöllisempää keskittää käyttäjien / palveluiden autentikointi erillisille AAA-servereille (Autentication, Authorization, Accounting). Serverit käyttävät AAA-protokollia, joista käytetyin vielä nykypäivänä on RADIUS, joka on määritelty IETF:n (Internet Engineering Task Force) dokumentissa RF2865. RADIUS suunniteltiin alunperin sisäänsoittopalveluiden tunnistukseen ja se on käytössä lähinnä operaattoreiden sisäisissä verkoissa. /3

Ominaisuudet:

- Asiakas-serveri-malli. NAS ( Network Access Server) toimii RADIUKSEN asiakkaana, jolloin sen tehtävänä on käyttäjätietojen toimittaminen servereille ja toiminta saadun vastauksen mukaisesti. RADIUS-serverit vastaanottavat käyttäjän yhteyspyynnöt, autentikoivat käyttäjän ja palauttavat tarvittavat asetukset NAS:lle, jotta käyttäjän haluama palvelu pystytään toteuttamaan.
- Asiakkaiden ja serverien välisissä autentikointipyynnöissä käytetään shared secret-avainta, jota ei missään vaiheessa lähetetä verkon yli. Käyttäjien salasanat lähetetään kryptattuina, jolloin turvattomassakin verkossa niiden selvittäminen on lähes mahdotonta. Käytössä on MD5-message-digest-algoritmi, jolla salasanasta luodaan tiiviste.
- RADIUS tukee erilaisia tapoja ja mekanismeja käyttäjän autentikoinnin suorittamiseen. On mahdollista esimerkiksi käyttää PPP-, PAP- tai CHAP-protokollia. Käyttäjän tunnistus tapahtuu annetun käyttäjänimen ja salasanan perusteella. /4

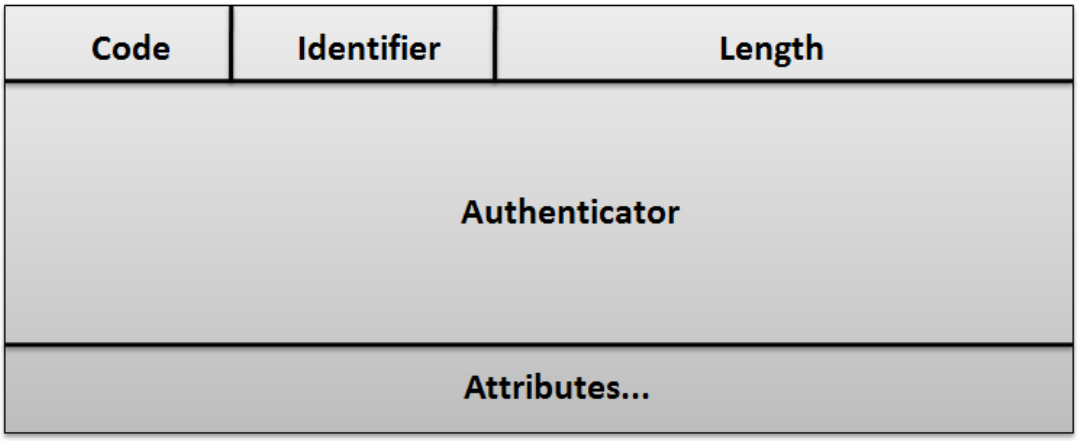
Sanomat:

- Access Request – NAS lähettää / välittää RADIUS serverille käyttäjän pyynnön saada käyttöoikeuden palveluun
- Access Challenge – Serveri kysyy NAS:lta tietoja tai haluaa käynnistää neuvottelun
- Access Accept – Serveri ilmoittaa NAS:lle pyynnön hyväksymisestä
- Access Reject – Serveri ilmoittaa NAS:lle pyynnön hylkäämisestä /3




Kuva 4. Yhteydenotto RADIUS-palveluun.

RADIUS-paketin muoto on yksinkertainen. Header (Otsikko) kenttään sisältyvät code, ID, length ja authenticator alikentät. Code kertoo minkätyyppisestä RADIUS – paketista on kyse, esimerkiksi 1 Access – Accept ja 2 Access – Reject. Oktetin mittaista ID-kenttää käytetään pyyntöjen tunnistukseen. Length-kenttä on kahden oktetin pituinen ja se kertoo koko lähetettävän viestin pituuden. Authenticator sisältää 16 oktettia tietoa, mm. serverin vastausten autentikointiin ja salasanan kryptaukseen liittyen. Otsikkokenttien jälkeen tulevat itse paketin sisältämät tiedot eli attribuutit. Attribuutteja voivat olla esimerkiksi käyttäjän salasanat ja käyttäjätunnukset. /3




Kuva 5. RADIUS-paketti.

RADIUS käyttää sanomien kuljetukseen UDP-protokollaa (User Datagram Protocol), joka on yhteydetön protokolla. Sen epäluotettavuudesta voi koitua ongelmia varsinkin RADIUKSEN tilastointiominaisuuksia käytettäessä. IETF onkin ilmoittanut, että nämä seikat on otettava tarkasti huomioon suunniteltaessa RADIUKSEN seuraajaa, jollaiseksi Diameter-ptorokollaa on kaavailtu. /3

## 3.2 Diameter-protokolla

IETF:n päättäessä RADIUKSEN kehittämisen vuonna 2000, piti löytää seuraava AAA-protokolla, jota lähdettäisiin kehittämään ja standardoimaan. Protokollalta odotettiin esimerkiksi seuraavia ominaisuuksia:

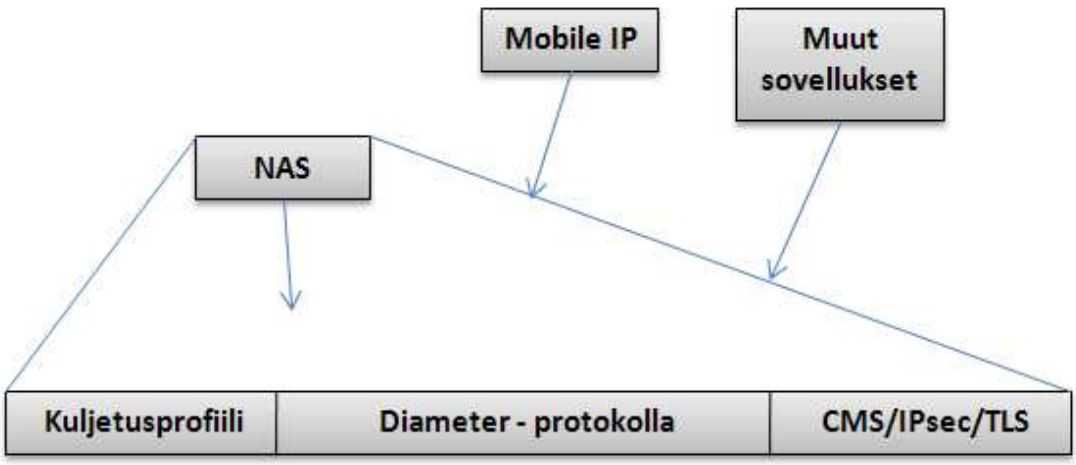
- Skaalautuvuus
- Client-server autentikointi
- Siirron turvallisuus, tietosuoja ja eheys
- Sekä IPv4- että IPv6-tuki
- Luotettava AAA-siirtomekanismi
- Kyky käsitellä palvelukohtaisia attribuutteja

Tarkasteltavana oli SNMP (Simple Network Management Protocol), RADIUS++, COPS (Common Open Policy Service Protocol) ja Diameter. SNMP:n käyttö hylättiin, koska sen autentikoinnin käsittely koettiin puutteelliseksi. RADIUS++ oli

työryhmän mielestä liian keskeneräinen, eikä se olisi ollut taaksepäin yhteensopiva RADIUKSEN kanssa. COPSia pidettiin kelvollisena AAA-protokollana, mutta sitä käytettiin jo QoS-protokollana (Quality of Service), joten sen monikäytöstä saattaisi aiheutua ongelmia palomuurien kanssa. Niinpä Diameter todettiin hieman paremmaksi juuri palomuuriystävällisyytensä takia ja sen ensimmäinen standardi julkaistiin syyskuussa 2003. 3GPP Release 6 tuki ainostaan RADIUKSEN käyttöä GGSN:ssä, Release 7 määritteli GGSN:n ja Diameterin välisen viestinkulun (TS 29.061). /3

### 3.2.1 Toiminta

Diameter-protokollaa käytetään sovellusten kautta, jollaisia ovat erilaiset palvelut, protokollat ja määritykset. Diameter-serverit, välityspalvelimet ja itse protokolla tarjoavat eri sovelluksille alustan, jolla ne pystyvät toimimaan. Diameterin spesifikaatiossa ei esimerkiksi ole ollenkaan määritelty autentikointiin liittyviä tietoja, vaan toiminta NAS:n kanssa on määritelty erillisessä NAS-sovelluksen spesifikaatiossa. Tärkeimpiä sovelluksia ovat PPP-yhteyksiä käyttävä NASREQ ja mobiiliverkkoihin suunniteltu Mobile IP. Diameter-kokonaisuus muodostaa kuvan kaltaisen pyramidirakenteen, jonka pohjalla perustana itse protokolla on. /3



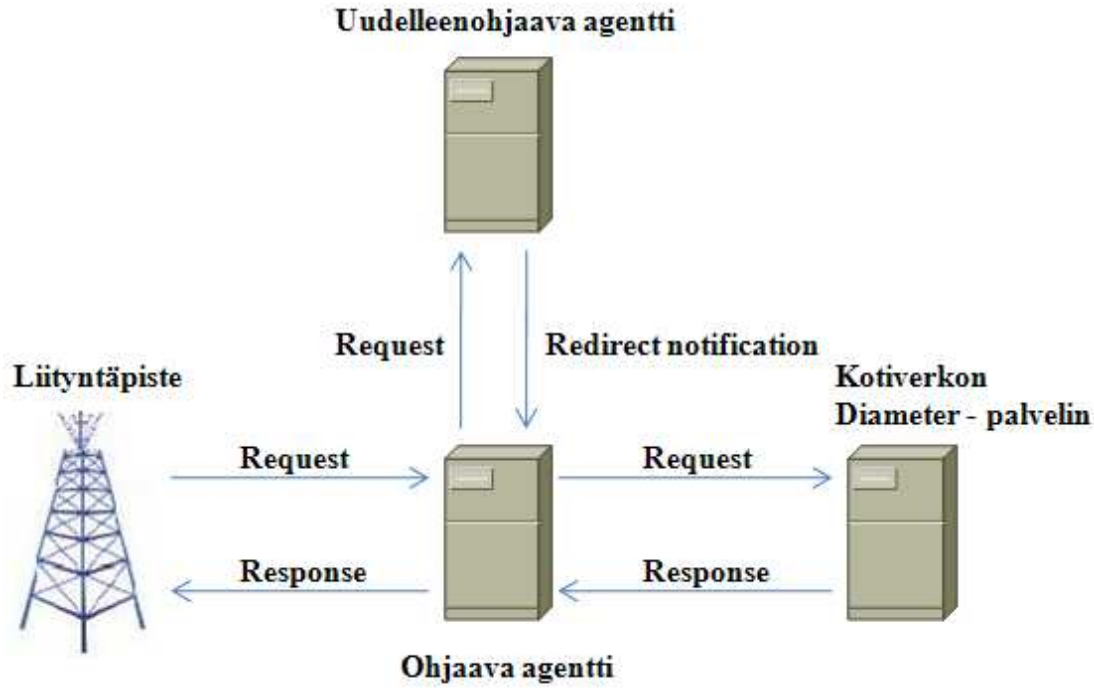

Kuva 6. Diameterin rakenne.

Diameterin tiedoissa on serverien ja asiakkaiden lisäksi määritelty käsite agentti. Agenteilla on eri tehtäviä, ne voivat esimerkiksi ohjata viestejä toiseen verkkoon ja

tehdä protokollamuunnoksia AAA-protokollien välillä. Jälkimmäisellä on erittäin suuri merkitys matkapuhelinverkoissa, tällöin eri palvelut eivät ole verkosta riippuvaisia, vaan omia palveluita pystytään käyttämään myös toisen palveluntarjoajan verkossa. Haut tehdään kuitenkin aina oman kotiverkon palvelimelta.

Agentit voivat toimia:

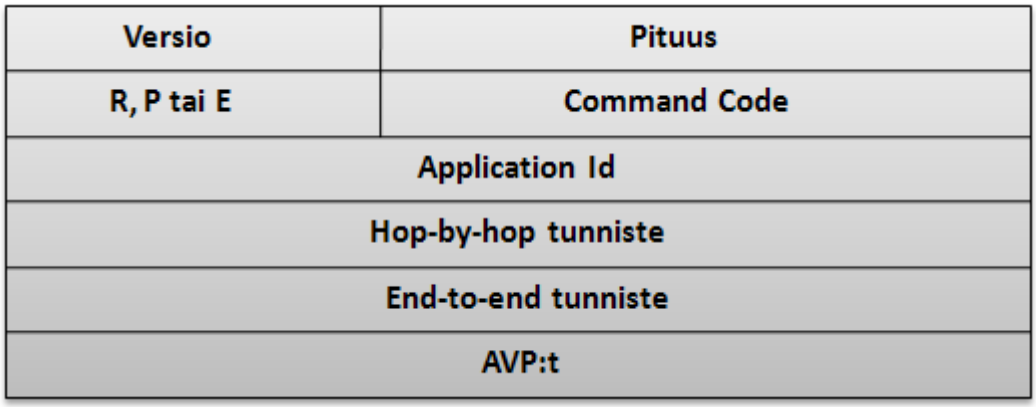
- Ohjaavina, jolloin ne ohjaavat saapuvat viestit oikeaan verkkoon.
- Uudelleenohjaavina, jolloin ne palauttavat kysyjälle viestin kohdeosoitteen.
- Välittävinä, kuten ohjaavat agentit, mutta niillä on mahdollisuus muokata viestin sisältöä.
- Muuntavina, eli mahdollistavat protokollamuunnokset Diameterin ja muiden AAA-protokollien välillä. /5




Kuva 7. Diameterin toiminta.

### 3.2.2 Diameter-paketti

Diameter-viesteissä kuljetetaan erilaisia sovellusten tai AAA-tietoja. Kuljetettavia tietoja kutsutaan attribuuteiksi, jotka ovat AVP-muodossa (Attribute Value Pair). Kuvassa Diameter-paketin otsikkokentän rakenne.




Kuva 8. Diameter-paketti.

- Version-kenttää kertoo Diameter protokollan version (1)
- Command flag-kenttä voi saada neljä eri arvoa. R (Request) kertoo, että viesti on pyyntö tai vastaus. P (Proxiable), viesti voidaan välittää, ohjata uudelleen tai se täytyy suorittaa paikallisesti. E (Error) kertoo viestissä olevasta virheestä. T voi kertoa viestin olevan uudelleenlähetetty esimerkiksi linjan häiriöiden takia.
- Command code-kenttä on oltava jokaisessa paketissa, se ilmoittaa vastaanottajalle mitä viestille on tehtävä. Command coden sisältö voi olla esimerkiksi “abort session request”.
- Application ID ilmaisee sovelluksen, johon viesti kuuluu.
- Hop by Hop-tunnistetta käytetään tunnistamaan pyynnöt ja vastaukset verkon eri hyppyjen välillä.
- End to End-tunnisteen avulla pystytään havaitsemaan duplikaattiviestit verkon eri päissä. /3

### 3.2.3 Diameter vs. RADIUS

Vaikka Diameter ja RADIUS ovat molemmat AAA-protokollia, on niiden perustoiminnallisuus jokseenkin erilainen. Diameterissä ei ole määritelty autentikointiin / tunnistamiseen käytettyjä parametrejä ollenkaan, vaan määritelty on ainoastaan käytettävien viestien muoto ja tapa, jolla ne lähetetään. Parametrit riippuvat käytettävästä sovelluksesta ja niitä hallinnoi IANA (Internet Assigned Numbers Authority). Esimerkiksi autentikoinnissa käytetty NAS on Diameterin päälle sijoittuva oma sovelluksensa. /5

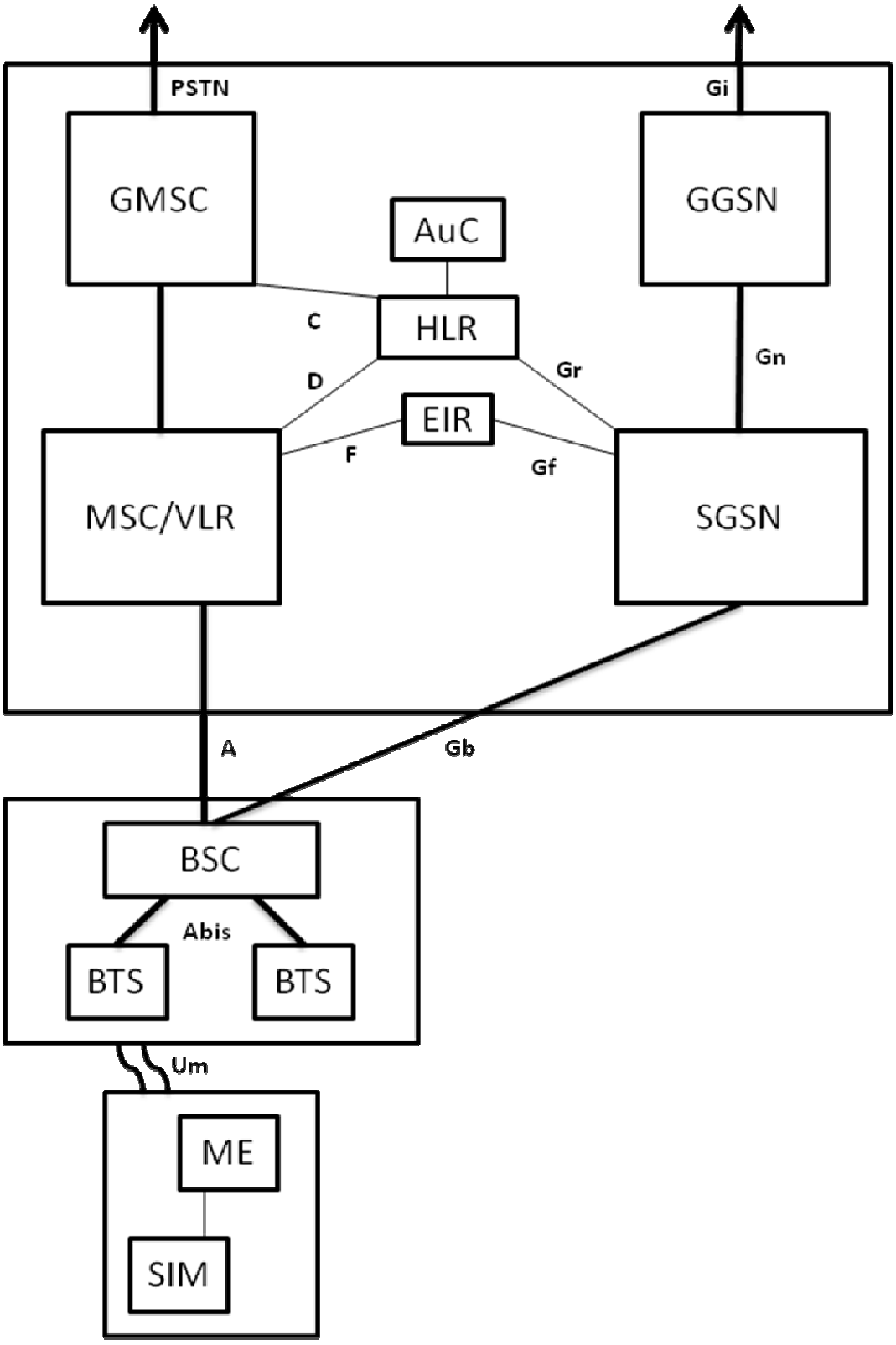
Esimerkkejä Diameterin hyödyistä RADIUKSEEN nähden:

- Helpompi palautuminen virheistä kuljetustilanteissa.
- Luotettavampi viestien kuljetus. RADIUKSESSA käytetty UDP-protokolla saattaa aiheuttaa pakettien häviämisiä, joista aiheutuu ongelmia. Diameterissä tuetut TCP ja SCTP eivät tällaista aiheuta.
- Serveri ja asiakas pystyvät neuvottelemaan paremmin halutuista palveluista ja attribuuteista Diameterissä. RADIUS ei myöskään tue virheilmoitusviestejä, joten virheiden käsittely on vajaavaista.
- RADIUKSESSA täytyy yleensä määritellä manuaalisesti servereiden ja asiakkaiden IP-osoitteet. Diameter pystyy dynaamisesti löytämään DNS:n kautta palveluiden eri osapuolet.
- Vaikka Diameterin ja RADIUKSEN viestityypit ovat erilaiset, on tehty määrittelyjä, joiden mukaan protokollia olisi mahdollista käyttää samassa verkossa. /3

# 4 TIETOTURVARATKAISUT JA NIIDEN KEHITYS SAMK-VERKOSSA

## 4.1 SAMK-verkko ennen 3G-päivityksiä

SAMK:n NGN-laboratorion verkko edustaa GSM Phase 2+ ja 3GPP Release 98-suositusten mukaista verkkoa, toisin sanoen kaikki laitteet ovat 2G-tasoisia. MSC:n, VLR:n ja HLR:n ohjelmistotaso Nokian terminologiassa on M10. GMSC ja radioverkon omistava MSC-keskukset ovat fyysisesti yksi ja sama keskus, josta voidaan kuitenkin erottaa kaksi erillistä loogista toimintoa. Myös SGSN ja GGSN ovat 2G tasoisia




Kuva 9. SAMK-verkko ennen 3G-päivitystä.

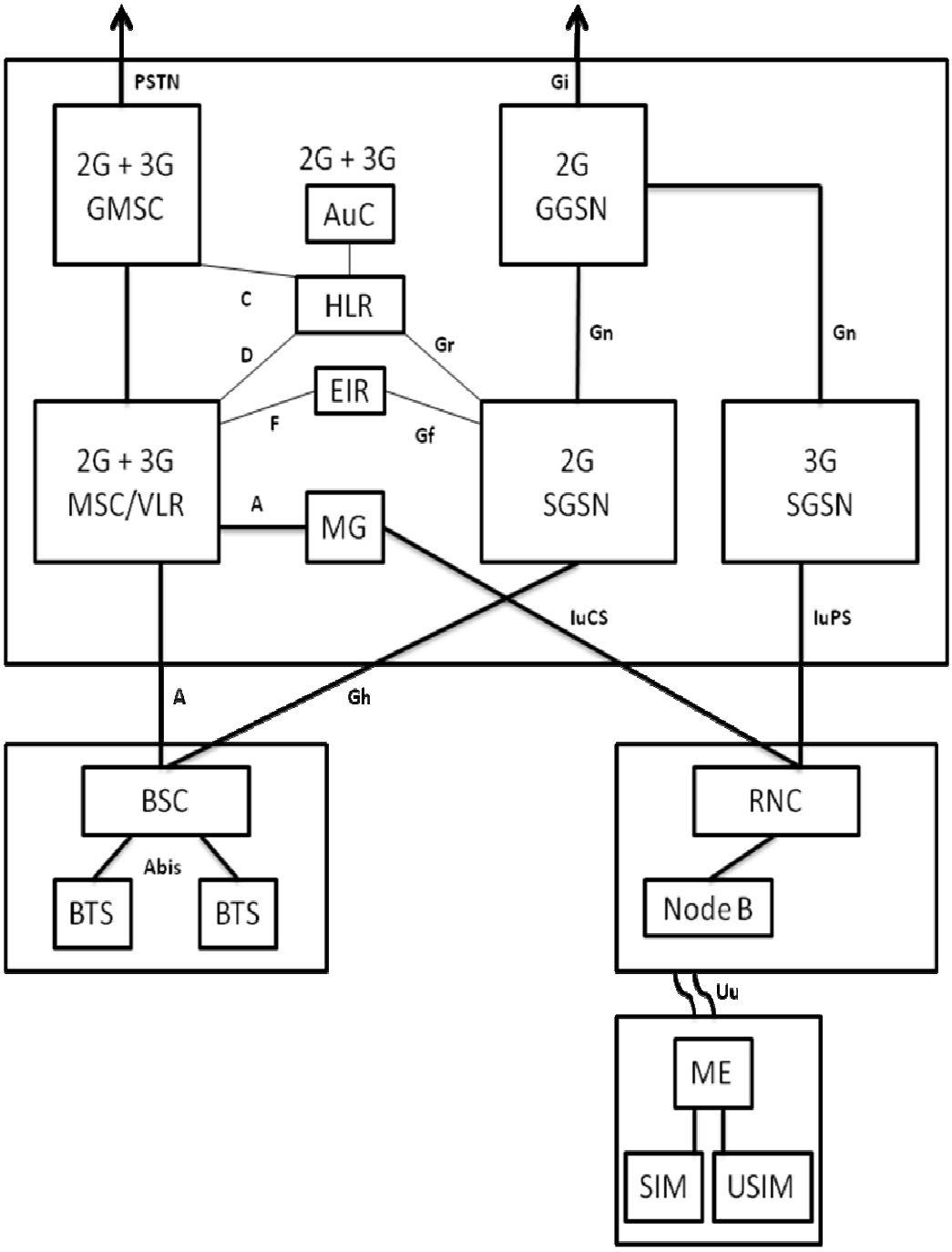
## 4.2 SAMK-verkko 3G-päivitysten jälkeen

SAMK:n verkkoa ollaan päivittämässä 3G-tasoiseksi kevään ja kesän 2009 aikana, tämä tarkoittaa, että MSC / VLR ja HLR päivitetään M13-ohjelmistotasoon, joka tukee 3GPP Release 99 mukaisia määrityksiä. Ohjelmiston päivityksen lisäksi on laitteistoa myös pitänyt päivittää. Muutoksen jälkeen MSC on ns. combi MSC, ts. siihen voidaan liittää sekä 2G BSS että 3G RAN.

Olevaa 2G SGSN:ää ei päivitetä, mutta se säilyy verkossa liittämään 2G BSS-pakettidomainiin. Sen rinnalle tulee uusi 3G SGSN (edustaa Release 99 tasoa), johon 3G RAN liitetään. Piirikytkentäisellä puolella tarvitaan interworking fuction-yksikkö, jona käytetään media gateway-laitetta liittämään 3G RAN MSC:hen.

GGSN-solmuna säilyy oleva 2G GGSN.

2G BSS rinnalle rakennetaan 3G UTRAN, joka koostuu yhdestä ohjaimesta RNC, sekä yhdestä tukiasemasta Node B. Myös nämä edustavat Release 99 tason määrityksiä.




Kuva 10. SAMK-verkko 3G-päivityksen jälkeen.

## 4.3 Muutokset tietoturvaan

3G-päivitykset tuovat SAMK-verkkoon lukuisia uusia ominaisuuksia. Tietoturvan kannalta keskeisimmät muutokset ovat:

Autentikointi

- Päivitetty HLR / AuC tukee jatkossa sekä GSM- että 3G-autentikointia. 3G-autentikointi toimii silloin kun käyttäjä on liittyneenä UTRAN radioverkkoon ja hänellä on käytössään USIM-kortti. Opinnäytetyössä oli tarkoitus todeta 3G-autentikointi käytännössä päivitetyssä verkossa. Tämä ei kuitenkaan ollut mahdollista verkon päivityksen viiveiden vuoksi.

Palvelun autentikointi

- Palvelun autentikoinnissa ei tapahdu muutosta. Mikäli GGSN päivitettäisiin 3GPP Release 7 mukaiseksi voitaisiin käyttää Diameter-protokollapohjaisia sovelluksia. GGSN:n päivitys on itsenäinen toimenpide ja riippumaton muista verkon solmuista, joten se on periaatteessa mahdollista tehdä myöhemmin milloin tahansa.

# 5 YHTEENVETO

Työssäni tutkin GSM- ja 3G-mobiiliverkoissa käytettäviä tietoturvamenteltemiä. Perehdyin erityisesti tilaajien yksityisyyden suojaamisessa käytettyihin ratkaisuihin ja verkon autentikointiin. Esittelin aiheeseen liittyvää teoriaa ja totesin autentikoinnin toimivuuden SAMK:n NGN-laboratorion verkossa.

Vertasin 2G- ja 3G-verkoissa käytettäviä tietoturvamenetelmiä ja totesin 3G:n käyttävän 2G-verkkoihin pohjautuvia ratkaisuja tuoden kuitenkin myös merkittävästi lisää uutta. Katson 3G-todennusmekanismien, erityisesti molemminpuolisen autentikoinnin lisäävän turvallisuutta siinä määrin, että operaattorien kannattaakin siirtyä mahdollisimman pian USIM-korttien käyttöön.

SAMK:n laboratorioverkon päivitys lisää mahdollisuutta perehtyä 3G-autentikointiin syvällisemmin ja mahdollistaa asioiden käytön opetuksessa. Tässä opinnäytetyössä en voinut päivitysten viivästymisten takia todeta 3G-autentikoinnin toimintaa käytännössä, joten se olisi todettava pikimmiten.

# LÄHTEET

1: Penttinen, J. 1999. GSM-tekniikka Järjestelmän toiminta, palvelut ja suunnittelu. Porvoo. WSOY

2: Eberspächer, J., Vögel, H. & Bettstetter, C. 2001. GSM Switching, Services and Protocols. Chichester England.. WILEY

3: Nakhjiri, Madjid & Nakhjiri Mahsa. 2006.AAA and Network Security for Mobile Access. Chichester England.. WILEY

4: Remote Authentication Dial In User Service (RADIUS) 2000. [Viitattu 15.4.2009.] http://tools.ietf.org/html/rfc2865

5: Keski-Kasari, Sami. Verkkopalveluiden autentikointi yhteisen käyttäjätietokannan avulla. [verkkodokumentti]. Tampere 2002 [viitattu 15.4.2009]. Diblomityö. Tampereen teknillinen korkeakoulu, Tietotekniikan osasto. Saatavissa: http://www.wirlab.net/pdf/di_tyo_samikk.pdf

6: Kaaranen, H., Ahtiainen, A., Laitinen, L., Naghian, S. & Niemi, V. 2001. UMTS NETWORKS Architecture, Mobility and Services. Chichester England. WILEY

7: GSM and UMTS Security [verkkodokumentti]. [Viitattu 17.5.2009]. Saatavissa: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html

# LIITTEET

1. Autentikointimäärittelyt SAMK – verkossa

Tulostukset ovat 3G-MSC:stä. Määritykset ovat osin keskeneräisiä.

```
MXO:; | Verkkokohtaiset parametrit

MSC       DX220-LAB                 1989-01-01  00:14:37

                                VLR PARAMETERS

TMSI:                          NOT USED
IMPLICIT IMSI DETACH:          NOT USED
AUTHENTICATION:                USED
AUTHENT RETRY:                 NOT USED
TMSI AUTHENT RETRY:            NOT USED
EMERGENCY CALL:       AUTHENT NOT USED          IMEI CHECKING NOT
USED
ALLOW CCBS WHEN UDUB:                                    NO
ALLOW CCBS WHEN CFB ACTIVE:                              NO
ALLOW LOCATION UPDATE WHILE SCP UNAVAILABLE:             YES
ALLOW GAPPING IN IN-MM:                                  NO
ALLOW SHORT MESSAGE TRANSFER WHILE SCP UNAVAILABLE:      YES
ALLOW GAPPING IN IN-SMS:                                 NO
NUMBER OF SIMULTANEOUS CALL TRANSFERS:
ALLOW CALL TRANSFER WHEN MAX EXCEEDED:                   NO
TRAFFIC TERMINATION ON TERM REQUEST:                     NOT USED
DEFAULT ACTION FOR CALL TRANSFER INVOCATIONS:            REPORT
------------------------------------------------------------------------
TIME LIMITS
  LOITERING:                          001 DAYS 00 HRS.
  IMPLICIT DEREGISTRATION:            012 HRS. 00 MIN.
```

```
  CALL WAITING:                          00 MIN. 50 SEC.
  INCOMING CALL COMPLETION RESPONSE:     04 MIN. 20 SEC.
-----------------------------------------------------------------
VLR CLEANING START TIME:         04:12
TRIPLETS:                        MIN=0
QUINTETS:                        MIN=2
CDR ON LOCATION UPDATE:          DISABLED
-----------------------------------------------------------------
VLR TRAFFIC CONTROL PRIORITIES
MOBILE ORIGINATED CALL             100
MOBILE TERMINATED CALL              95
MOBILE ORIGINATED SHORT MESSAGE     95
MOBILE TERMINATED SHORT MESSAGE    100
INTRA VLR LOCATION UPDATE           75
INTER VLR LOCATION UPDATE           50
PRIORITY MODE CPU LEVEL             85%
-----------------------------------------------------------------
SUPPORTED SUPPLEMENTARY SERVICES
  CALL FORWARDING:         CFU CFB CFNA CFNR
  CALL COMPLETION:         CW HOLD
  CHARGING:                AOCI AOCC
  CALL RESTRICTION:        BAOC BOIC BOIH
-----------------------------------------------------------------
SUPPORTED TELESERVICES
  SPEECH TRANSMISSION:     T11
  SHORT MESSAGE:           T21 T22
  FACSIMILE TRANSMISSION: T61 T62
-----------------------------------------------------------------
SUPPORTED BEARER SERVICES
  DATA C.D.A:              B11 B12 B13 B14 B15 B16
  DATA C.D.S:              B1A B1C B1D B1E
-----------------------------------------------------------------
PAGE AND SEARCH
  LIMIT FOR SIMULTANEOUS SEARCHES:  SEARCHES ARE NOT LIMITED
  NUMBER OF SEARCH REPETITIONS:     2
  SEARCH RESPONSE WAITING TIME:     3000 MSEC.
  TMSI PAGE REPETITION IN MT CALL:  NOT USED
  TMSI PAGE REPETITION IN MT SMS:   NOT USED
  TMSI PAGE REPETITION IN MT USSD:  NOT USED
  TMSI PAGE REPETITION IN MT LR:    NOT USED
-----------------------------------------------------------------
```

```
IMSI ANALYSIS FAILURE REJECT CAUSE CODE IN GSM NETWORK  : PLMN
------------------------------------------------------------------------
SUPER-CHARGER PARAMETERS

INFORM PREVIOUS NETWORK ENTITY       IFNOSI
HANDLING MTC FOR PASSIVE SUBS        REJECT
VLR UPDATE COUNTER                   000
WELCOME SM CRITERION                 00 DAYS 00 HRS.
------------------------------------------------------------------------
ADVANCED DB MANAGEMENT PARAMETERS
TARGET DB FILL RATIO                  95%
COMMAND EXECUTED

MXP:NAME=SAMKMSC:;  | Vierailijaryhmäkohtaiset parametrit

MSC       DX220-LAB                 1989-01-01  00:18:56

                                PLMN PARAMETERS

HOME PLMN SAMKMSC IN NATIVE COUNTRY
INDEX:          1
CIPHERING:      NOT USED
TRIPLET RE-USE: USED
EMLPP DEFAULT PRIORITY LEVEL: 4        SUPPORT OF EMLPP: YES
COUNTRY CODE LENGTH:    3
MSRN GROUP:                  00        BLACK LIST EFFECT:      ALLOW
MSRN LIFE TIME:              90 SEC.   GREY LIST EFFECT:       ALLOW
PNS TIME LIMIT:              20 SEC.   UNKNOWN IMEI EFFECT:    ALLOW
TRAFFIC TERMINATION ON CANCEL LOCATION: NOT USED
SUPPORTED CAMEL PHASE:                  NOT SUPPORTED
FRAUD OBSERVATION AND LIMITATION:       NOT USED
REGIONAL ROAMING:                       NOT ALLOWED
ZONE CODES:
ZONE CODES FROM HLR:                    USED
EXACT MS CATEGORY USAGE:                NOT ALLOWED
REJECT CAUSE FOR UDL REJECTION:         ROAM
SUPPORT OF BOR:                         NO
USAGE OF PLMN SPECIFIC SS 253:          NOT SUPPORTED
------------------------------------------------------------------------
ADVICE OF CHARGE PARAMETERS
```

```
  E1:    0,0            E2:    0,0             E3:     0,00
  E4:    0,0
  E7:    0,0
-------------------------------------------------------------------
A5 ALGORITHM PARAMETERS

  NONCIPHERED CONNECTION: ALLOWED
  A5/1: NOT ALLOWED     A5/2: NOT ALLOWED


-------------------------------------------------------------------
IMEI STATUS CHECK FROM EIR IN CASE OF...

  LOC UP:   NOT USED     PER UP:  NOT USED    IMSI ATTACH:  NOT USED
  MO CALL:  NOT USED     MO SMS:  NOT USED    SS OPER:      NOT USED
  MT CALL:  NOT USED     MT SMS:  NOT USED    MT USSD:      NOT USED
  MT LOC REQ: NOT USED
-------------------------------------------------------------------
USAGE FREQUENCY COUNTERS  (0 = NOT USED)

  TMSI ALLOCATION
    LOC UP NEW VIS:    0    LOC UP:     0          PER UP:        0
    IMSI ATTACH:       0    MO CALL:    0          MO SMS:        0
    MT CALL:           0    MT SMS:     0          MT LOC REQ:    0
    MT USSD:           0    SS OPER:    0

  AUTHENTICATION
    LOC UP NEW VIS:    0    LOC UP:     0          PER UP:        0
    IMSI ATTACH:       0    MO CALL:    0          MO SMS:        0
    MT CALL:           0    MT SMS:     0          MT LOC REQ:    0
    MT USSD:           0    SS OPER:    0

  IMEI CHECKING
    LOC UP NEW VIS:    0    LOC UP:     0          PER UP:        0
    IMSI ATTACH:       0    MO CALL:    0          MO SMS:        0
    MT CALL:           0    MT SMS:     0          MT LOC REQ:    0
    MT USSD:           0    SS OPER:    0
-------------------------------------------------------------------
EQUAL ACCESS

  DEFAULT PREFERRED INTEREXCHANGE CARRIER (PIC):  NOT USED
```

```
  DEFAULT PIC LOCK:   CARRIER ACCESS CODE (CAC) DIALLING IS ALLOWED
  PIC RELATION:       PLMN DEFAULT IS USED ALWAYS
  PIC LOCK RELATION:  PLMN DEFAULT IS USED ALWAYS
---------------------------------------------------------------------
INTELLIGENT NETWORK MOBILITY MANAGEMENT
  SCP ADDRESS:
  SERVICE KEY: N
---------------------------------------------------------------------
INTER-PLMN HANDOVER AGREEMENTS
  MOBILE COUNTRY CODE   MOBILE NETWORK CODE
---------------------------------------------------------------------
EQUIVALENT PLMNS
  MOBILE COUNTRY CODE   MOBILE NETWORK CODE
UMTS CIPHERING: NOT USED
---------------------------------------------------------------------
UMTS ENCRYPTION PARAMETERS
NONCIPHERED CONNECTION: ALLOWED
SUPPORTED ALGORITHMS: UEA1
---------------------------------------------------------------------
UMTS SECURITY PARAMETERS

SUPPORTED ALGORITHMS: UIA1
---------------------------------------------------------------------
TRACE ACTIVATION PARAMETER

  TRACE ACTIVATION FROM THIS PLMN: NOT ALLOWED
---------------------------------------------------------------------
LOCATION REQUEST

  MOBILE ORIGINATED:          SUPPORTED
  MOBILE TERMINATED:          SUPPORTED
  DEFERRED MOBILE TERMINATED: SUPPORTED
-------------------------------------------
SUPER-CHARGER PARAMETERS

PLMN UPDATE COUNTER                  000

COMMAND EXECUTED
```

2. Nethawk – analyysi autentikointitilanteesta

Nethawk – protokolla-analysaattorilla tehty jäljitys SAMK – verkossa D – rajapinnassa uuden tilaajan sijainninpäivityksen yhteydessä. Tulostuksesta ilmenee havainnollisesti, miten sijainninpäivityksen alussa VLR pyytää AuC:lta autentikointiparametreja (triplet). Samanaikaisesti olisi voitu monitoroida A – rajapintaa, josta olisi näkynyt MS:n haaste autentikointiin ja MS:n vaste. Tulosteesta voidaan kuitenkin päätellä, että autentikointi on tapahtunut onnistuneesti.

```
R1    R2
UDT - UNIT DATA
SCCP DPC
 - 80 (0050h)
SCCP OPC
 - 900 (0384h)
SCCP SLS
 - 0 (00h)
Message type
 - UDT Unitdata
Protocol Class
- 80h, connectionless, no special options
Called Party Address
- length 8 (08h)
- full GT configuration
- routing based on global title
- subsystem is HLR (MAP)
- translation type : 0 (00h)
- encoding : BCD, even number of digits
- numbering plan : ISDN/telephony (E.163, 164)
- nature of address : international number
- address signals : 358250
Calling Party Address
- length 9 (09h)
- full GT configuration
- routing based on global title
- subsystem is VLR (MAP)
- translation type : 0 (00h)
- encoding : BCD, odd number of digits
```

- numbering plan : ISDN/telephony (E.163, 164)
- nature of address : international number
- address signals : 3582384
SCCP User Data
- length 60 (3Ch)
- data:
62 3A 48 04 16 40 10 00 6B 1E 28 1C 06 07 00 11 86 05 01 01 01 A0 11
60 0F 80 02 07 80 A1 09 06 07
04 00 00 01 00 0E 02 6C 12 A1 10 02 01 00 02 01 38 04 08 42 14 15 11
11 01 30 F5
BEGIN
 OrigTransactionID:  16 40 10 00
 DialoguePortion
  External
   ObjectIdentifier: 0-0-17-773-1-1-1
   Single-ASN.1-Type
    DialogueRequest
     Protocol-Version:  00000111 10000000
     Application-Context-Name
      ObjectIdentifier: 0-4-0-0-1-0-14-2
      itu-t(0)  identified-organization(4)  etsi(0)  mobileDomain(0)
gsm-Network(1) map-ac(0) infoRet
rieval(14) version2(2)
 **ComponentPortion**
  **Invoke**
   **InvokedID:  00**
   **LocalOperationCode:  38**
   **Parameter: 4 (04h)   Length: 8 (08h)**
   **Tag: Universal, Primitive, value: 04h**
   **- length: 8 (08h)**
   **- data:  42 14 15 11 11 01 30 F5**
**SEND AUTHENTICATION INFO (ARGUMENT MSG) : 56 (38h)**

      PCM hlr    TS:1    Subch:0xFF    Type:hdlc            Id:203792
Time:2009.05.06 11:06:22.571705000
      VALID FRAME
      MSU
      - BSN: 14 (0Eh) BIB: 1   FSN: 11 (0Bh) FIB: 1
      - SCCP
      - network indicator: Reserved national

- data, length: 62 (3Eh)
UDT - UNIT DATA
SCCP DPC
 - 900 (0384h)
SCCP OPC
 - 80 (0050h)
SCCP SLS
 - 12 (0Ch)
Message type
 - UDT Unitdata
Protocol Class
- 80h, connectionless, no special options
Called Party Address
- length 9 (09h)
- full GT configuration
- routing based on global title
- subsystem is VLR (MAP)
- translation type : 0 (00h)
- encoding : BCD, odd number of digits
- numbering plan : ISDN/telephony (E.163, 164)
- nature of address : international number
- address signals : 3582384
Calling Party Address
- length 8 (08h)
- full GT configuration
- routing based on global title
- subsystem is HLR (MAP)
- translation type : 0 (00h)
- encoding : BCD, even number of digits
- numbering plan : ISDN/telephony (E.163, 164)
- nature of address : international number
- address signals : 358250
SCCP User Data
- length 215 (D7h)
- data:
64 81 D4 49 04 16 40 10 00 6B 2A 28 28 06 07 00 11 86 05 01 01 01 A0 1D 61 1B 80 02 07 80 A1 09 06
07 04 00 00 01 00 0E 02 A2 03 02 01 00 A3 05 A1 03 02 01 00 6C 81 9F A2 81 9C 02 01 00 30 81 96 02
01 38 30 81 90 30 22 04 10 B5 9F 4A 02 18 B1 47 1D FC 86 24 24 E0 AE 6A 08 04 04 10 3A EF A7 04 08

```
      BD 14 E2 B8 59 23 81 81 30 22 04 10 5E 1D 18 F6 20 32 E5 D2 BD
B3 CE C9 0B 6B 22 2E 04 04 FB B8 BD
      53 04 08 85 97 40 77 18 16 6B 6C 30 22 04 10 5F 48 3A 8A 94 DF
9F 38 B9 3A 89 9D 1D 4E 5A 46 04 04
      FA ED 9F 2F 04 08 31 7A 3A 9D 1C 9F 2C 38 30 22 04 10 05 54 78
41 B7 22 18 F7 EF FB E2 B5 79 27 FB
      2E 04 04 A0 F1 DD E4 04 08 12 87 BD 52 4A 5E 47 10
      END
       DestTransactionID:  16 40 10 00
       DialoguePortion
        External
         ObjectIdentifier: 0-0-17-773-1-1-1
         Single-ASN.1-Type
          DialogueResponse
           Protocol-Version:  00000111 10000000
           Application-Context-Name
            ObjectIdentifier: 0-4-0-0-1-0-14-2
            itu-t(0)       identified-organization(4)       etsi(0)
mobileDomain(0) gsm-Network(1) map-ac(0) infoRet
      rieval(14) version2(2)
            Result
            - Accepted (0)
            Result-Source-Diagnostic
             Dialogue-Service-User
             - Null (0)
       ComponentPortion
        ReturnResultLast
         InvokedID:  00
         Sequence
          LocalOperationCode:  38
          Parameter: 48 (30h)   Length: 144 (90h)
          Tag: Universal, Constructed, value: 10h
          - length: 144 (90h)
           Tag: Universal, Constructed, value: 10h
           - length: 34 (22h)
            Tag: Universal, Primitive, value: 04h
            - length: 16 (10h)
            - data:  B5 9F 4A 02 18 B1 47 1D FC 86 24 24 E0 AE 6A 08
            Tag: Universal, Primitive, value: 04h
            - length: 4 (04h)
            - data:  10 3A EF A7
```

**Tag: Universal, Primitive, value: 04h**
**- length: 8 (08h)**
**- data: BD 14 E2 B8 59 23 81 81**
**Tag: Universal, Constructed, value: 10h**
**- length: 34 (22h)**
**Tag: Universal, Primitive, value: 04h**
**- length: 16 (10h)**
**- data: 5E 1D 18 F6 20 32 E5 D2 BD B3 CE C9 0B 6B 22 2E**
**Tag: Universal, Primitive, value: 04h**
**- length: 4 (04h)**
**- data: FB B8 BD 53**
**Tag: Universal, Primitive, value: 04h**
**- length: 8 (08h)**
**- data: 85 97 40 77 18 16 6B 6C**
**Tag: Universal, Constructed, value: 10h**
**- length: 34 (22h)**
**Tag: Universal, Primitive, value: 04h**
**- length: 16 (10h)**
**- data: 5F 48 3A 8A 94 DF 9F 38 B9 3A 89 9D 1D 4E 5A 46**
**Tag: Universal, Primitive, value: 04h**
**- length: 4 (04h)**
**- data: FA ED 9F 2F**
**Tag: Universal, Primitive, value: 04h**
**- length: 8 (08h)**
**- data: 31 7A 3A 9D 1C 9F 2C 38**
**Tag: Universal, Constructed, value: 10h**
**- length: 34 (22h)**
**Tag: Universal, Primitive, value: 04h**
**- length: 16 (10h)**
**- data: 05 54 78 41 B7 22 18 F7 EF FB E2 B5 79 27 FB 2E**
**Tag: Universal, Primitive, value: 04h**
**- length: 4 (04h)**
**- data: A0 F1 DD E4**
**Tag: Universal, Primitive, value: 04h**
**- length: 8 (08h)**
**- data: 12 87 BD 52 4A 5E 47 10**

**SEND AUTHENTICATION INFO (RESULT MSG) : 56 (38h)**

value SendAuthenticationInfoRes ::=
{
extensionContainer