

BAB II

Sejarah, Struktur Wilayah, Arsitektur Wilayah, dan serta Aspek-Aspek Keamanan Pada System GSM

2.1 Sejarah GSM

Global system for Mobbile atau GSM adalah generasi kedua dari standar sistem sistem seluller yang tengah dikembangkan untuk mengatasi problem fragmentasi yang terjadi pada standar pertama di negara Eropa .GSM adalah sistem standar sellular pertama didunia yang menspesifikasikan digital modulation dan network level architectures and service. Sebelum muncul standar GSM ini negara-negara di Eropa menggunakan standar yang berbeda-beda , sehingga pada saat itu tidak memungkinkan seorang pelanggan menggunakan singele subscriber unit untuk menjangkau seluruh benua Eropa.

Pada awalnya sistem GSM ini dikembangkan untuk melayani sistem seluler pan-Eropa dan menjanjikan jangkauan network yang lebih luas seperti halnya penggunaan ISDN. Pada perkembangannya sistem GSM ini mengalami kemjuan pesat dan menjadi standar yang paling populer di seluruh dunia untuk sistem seluler.Bahkan pertumbuhannya diprediksikan akan mencapai 20 samapai 50 juta pelanggan pada tahun 2000.

Penggunaan alokasi frekuensi 900 MHz oleh GSM ini diambil berdasarkan rekomendasi GSM (Gropue special Mobile) cimitte yang merupakan salah satu grup kerja pada confe'rence Europe'ene Postes des Telecommunication

(CEPT). Namun pada akhirnya untuk alasan marketing GSM berubah namanya menjadi the Global System for Mobile Communication, sedangkan standar teknisnya diambil dari European Technical Standards Institute (ETSI)

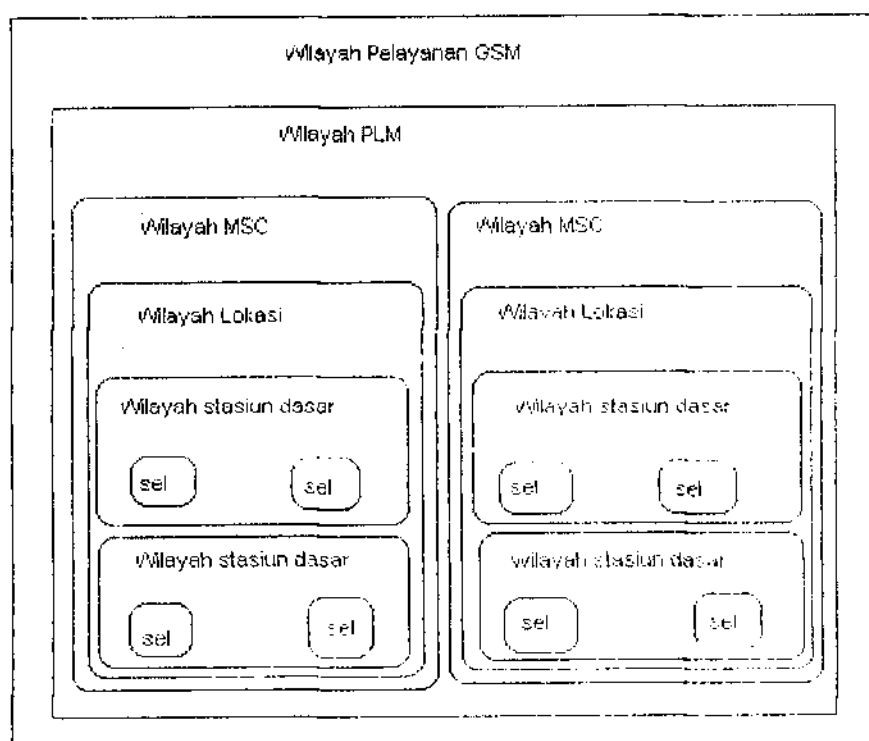
GSM pertama kali diperkenalkan di Eropa pada tahun 1991 kemudian pada akhir 1993, beberapa negara non Amerika seperti Amerika Selatan, Asia dan Australia mulai mengadopsi GSM yang akhirnya menghasilkan standar baru yang mirip yaitu DCS 1800, yang mendukung Personal Communication Service (PCS) pada frekuensi 1,8 Ghz sampai 2 Ghz.

2.2 Struktur Wilayah

Bagian terkecil dari wilayah pelayanan STB adalah sel. Beberapa buah sel menyusun sebuah wilayah yang disebut Wilayah Stasiun Dasar (Base Station Area), dimana merupakan bagian jaringan yang dapat dilingkupi oleh sebuah stasiun dasar. Setiap stasiun telepon bergerak (Mobile Station) yang berada dalam stasiun dasar, dapat dijangkau oleh peralatan radio dari stasiun dasar.

Wilayah yang lebih luas lagi disebut Wilayah Lokasi (Location Area). Selanjutnya satu atau beberapa wilayah lokasi membentuk sebuah wilayah yang disebut Wilayah MSC (Mobile Switching Centre/ Pusat Penyambungan Telepon Bergerak) atau wilayah VLR (Visitor Location Register / Register lokasi pengunjung) kesatuan beberapa wilayah MSC dalam suatu perencanaan penomoran bersama (misal kode tujuan nasional yang sama) dan rencana

pengrutean yang sama, menyusun sebuah wilayah yang disebut Wilayah PLMN (Public Land Mobile Network / Wilayah Jaringan Telepon Bergerak Untuk Umum), wilayah PLMN merupakan wilayah geografis dimana suatu PLMN menyediakan pelayanan Telekomunikasi. Beberapa PLMN membentuk suatu Wilayah Pelayanan (Service Area). Wilayah pelayanan dapat didefinisikan sebagai suatu wilayah dimana sebuah MS dapat dihubungi oleh pelanggan telepon tetap tanpa perlu mengetahui dimana MS tersebut berada. Suatu wilayah pelayanan dapat melingkupi sebuah negara, sebagian dari suatu negara atau beberapa negara. Gambar dibawah ini memperlihatkan Struktur Wilayah STB-GSM.



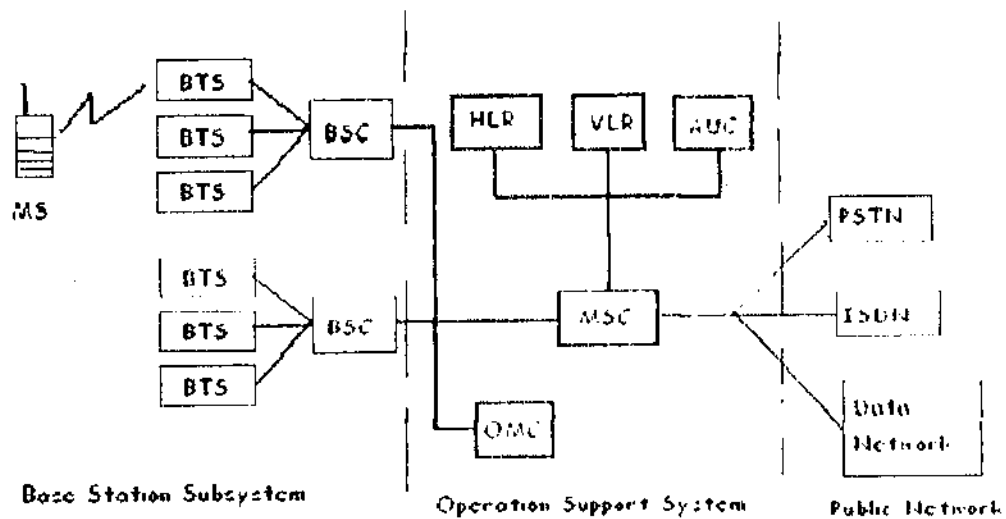
Gambar 2.1 Gambaran Struktur Wilayah STB-GSM

2.3 Arsitektur Jaringan GSM

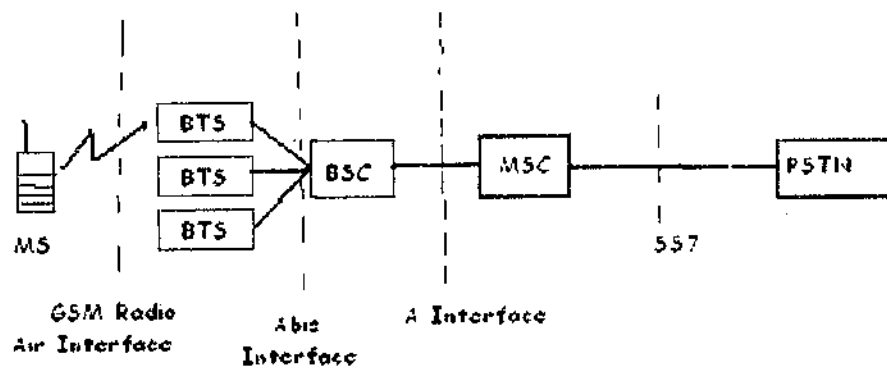
Secara keseluruhan system GSM dibagi menjadi dua sub-sistem, yaitu sub-sisitem radio dan sub-sistem jaringan (network). Gambar 2.2. menunjukkan suatu arsitektur jaringan dari sistem GSM, Gambar 2.3 variasi interfaces yang digunakan dalam GSM, dari gambar dapat dilihat bahwa interface yang menghubungkan BTS dengan BSC disebut sebagai *Abis Interface*. Interface ini membawa trafik dan data maintenance dan dispesifikasikan GSM untuk distandarisasi untuk seluruh vendor. BSC secara fisik terkoneksi dengan MSC via microwave / leased line dengan, sedangkan interface yang menghubungkan antara BSC dan MSC disebut sebagai *A interface*. Interface ini menggunakan SS7 protokol yang biasa dikenal sebagai *Signaling Correction Control Part*(SCCP) yang akan mendukung komunikasi antara BSS dengan MSC.

Secara umum NSS melakukan semua fungsi penyambungan yang diperlukan dalam suatu jaringan STB GSM tertentu, dengan jaringan STB GSM lain maupun dengan jaringan permanen (PSTN/ISDN), melakukan pengaturan kanal, kontrol panggilan, penggunaan data dan pensinyalan. NSS juga bertanggung jawab terhadap manajemen mobilitas seperti melakukan proses autentifikasi, pembaruan lokasi, handsover dan proses roaming. Terdapat lima fungsi-fungsi pokok dalam NSS yaitu: Mobile service Switching Centre (MSC) / Pusat Penyambungan Bergerak, Home Location Register (HLR) / Register

Lokasi Pengunjung, Authentication Centre (AUC)/ Pusat Autentifikasi, Equipment Identity Register (EIR) / Register Identitas Peralatan.



Gambar 2.2 Arsitektur Jaringan GSM



Gambar 2.3 variasi interface yang digunakan dalam GSM

MSC menyelenggarakan semua fungsi-fungsi switching yang diperlukan untuk MS yang berada pada MSC service area. MSC adalah jantung dari dari seluler radio system. Ia bertanggung jawab untuk routing, atau switching bagi semua panggilan dari originator ke destinator. Untuk itu MSC harus dapat berhubungan dengan PSTN, ke MSC pada GSM yang sama atau GSM network lainnya. MSC harus dapat berperan sebagai pengatur Managing panggilan-panggilan, akan bertanggung jawab untuk penyelenggaraan routing, control dan penentuan tujuanpanggilan collecting of charging dan accounting information. MSC harus dapat juga berperan sebagai fasilitas antar kerja (interworking) antara GSM network dengan public voice dan data network.

HLR adalah data base yang utama yang digunakan untuk pengaturan pelanggan-pelanggan bergerak. GSM network mungkin memepunyai lebih dari satu HLR tergantung dari ukuran networknya sendiri. Dua macam data yang disimpan di HLR, yaitu: Subscriber informasi seperti data tentang Teleservices atau data tentang Bearer services, Supplementary services dan lain sebagainya. Pengguna-pengguna tersebut terdaftar pada HLR ini (Having their "home" in this HLR), dan Location Information, khusus untuk melayani permintaan dari VLR tentang alamat dari pelanggan yang dianggap baru. Pemberitahuan tentang lokasi

dari pelanggan ini digunakan untuk dapat menggerakkan panggilan –panggilan yang akan datang sehingga tepat alamatnya. Dua nomor-nomor identity dari tiap pelanggan bergerak disimpan pada HLR ini yaitu: International Mobile Subscriber Identity (IMSI) adalah nomor identity yang unik dari subscriber pada GSM network, dan Mobile Station ISDN Number (MSISDN) adalah nomor identity yang unik dari subscriber pada PSTN/ISDN numbering plan.

Setiap MSC mempunyai VLR sendiri yaitu data base yang berisi Dynamic Information dari seluruh MS yang sedang berada pada cakupan dari satu MSC. Bila ada roaming kepada MSC area yang baru maka VLR dari area yang baru tersebut akan menanyakan data-data tentang MS tersebut kepada HLRnya. Maka HLR akan mendaftarkan alamat yang baru ada pada VLR. Bila kemudian MS tersebut akan mengadakan hubungan maka VLR sudah mempunyai data-data lengkap untuk penyelenggaraan hubungan sehingga tidak perlu lagi menanyakan atau mengganggu HLR. VLR dapat disebut sebagai Distributed Replica dari HLR. VLR berisi data-data yang lebih lengkap (Exact Information) tentang lokasi dari MS yang berada pada MSC service area dan memuat data-data yang diperlukan MSC untuk melayani pelanggan yang berkunjung.

AuC dihubungkan dengan HLR. Fungsi dari AuC adalah untuk melayani HLR dengan menyampaikan authentication parameter dan ciphering keys didasarkan dari nomor-nomor pelanggan yang diberikan. Database AuC juga dilindungi terhadap mekanisme akses yang tidak berhak. Pada AuC terdapat kunci identitas untuk setiap pelanggan mobile yang terdaftar pada HLR. Dilakukan untuk menaikkan tingkat pengamanannya.

Ada perbedaan antara identitas dari peralatan (Physical Equipment Identity) Dari setiap MS dengan identitas pelanggan (Subscriber Identity). Setiap MS dikenal dengan dengan IMEI sedangkan pengguna sebagai pemegang SIM card dikenal dengan IMSI. Untuk menghindari penggunaan MS dari orang yang tidak diakui (Proven) maka EIR dihubungkan langsung dengan MSC. MSC akan menggunakan EIR untuk memeriksa keabsahan Validity dari MS yang sedang digunakan oleh pelanggan.

Fungsi utama dari Base Transceiver Station (BTS) adalah untuk melengkapi keperluan-keperluan base station radio pemancar dari penerima. BTS dapat terdiri dari hanya satu pemancar dan penerima. BTS dapat terdiri dari hanya satu pemancar dan penerima atau lebih tergantung dari kebutuhan kapasitas trafik. Cell site mungkin hanya Omnidirectional atau juga dirubah menjadi threedirectional cells. BTS mempunyai peralatan yang diperlukan untuk radio site covering untuk satu atau lebih jumlah cell. Interface yang digunakan antara BSC dan BTS adalah Abis interface sesuai dengan GSM technical Specifications.

Base station Subsystem adalah suatu peralatan yang meliputi pentransmisi dan pengendalian yang diperlukan untuk memastikan sambungan, dimana pelanggan mobil yang tersebar dan bergerak diantara sekian banyak sel dalam daerah cakupannya.

Ada dua system antenna yang digunakan pada suatu base station, yaitu : Sistem sel antenna omnidirectional, dimana pada system ini, antenna yang digunakan pada sel site adalah antenna omnidirectional (segala arah), sehingga daerah

liputannya melingkupi seluruh bagian sel, dan Sistem sel antena directional dimana suatu sel dibagi menjadi beberapa sector. Jumlah total kanal yang tersedia terbagi menjadi sejumlah grup sesuai dengan sektorisasi sel yang digunakan.

Untuk isitem 7 sel pada pola konfigurasinya, biasanya digunakan antena dengan sector 120^0 , sehingga dengan adanya 21 set kanal dapat ditempatkan 3 set pada setiap sel dari ke-7 dalam susunan pola. Pemakaian sector biasanya dilakukan didaerah yang padat penduduknya untuk memperbanyak sel dan pengulangan kanal frekuensi (frekwensi reuse). Biasanya digunakan antena dengan sector 120^0 .

BSC bertugas untuk melakukan pengendalian sejumlah BTS dan juga termasuk pemakaian sumber daya radio secara efisien. Adapun secara umum Base Station Controller mempunyai tugas : Mengawasi BTS dan mengendalikan BTS, menangani hubungan dengan Mobile Station, pengalokasian kanal dan Handover. BSC secara fisik dapat disambungkan langsung ke MSC, satu MSC dapat mengatur sampai lebih dari 1 BSC, BSC dapat dibagi menjadi 2 unit:

1. BSC Control Equipment (BCE)
2. Trascoding Control Equipment (TCE)

BSC mempunyai kemampuan untuk mengubah kecepatan transmisi yang berbeda dalam bentuk suara atau data pada bagian radio yang diperoleh dari tiap kanal trafik ke dalam bentuk yang telah distandarkan (64 Kbit/sec).

Mobile Station (MS) adalah peralatan yang dipergunakan oleh pelanggan untuk mengakses pelayanan PLMN GSM. MS didefinisikan oleh GSM sebagai

peralatan telepon bergerak (Mobile Equipment/ ME) ditambah dengan Modul Identitas Pelanggan (Subscriber Identity Modul / SIM). Kartu SIM berisi sebuah mikroprosesor dan sebuah EPROM, yang mengandung unsure-unsur informasi yang dibutuhkan oleh system untuk mengidentifikasi, mengautifikasi dan menalokasikan pelanggan telepon bergerak GSM. Sedangkan ME berisi sebuah pemancar dan penerima yang dikontrol oleh komputer, dan terhubung dengan sebuah telepon, FAX serta terminal komputer, dan sebuah pembaca kartu chip (Chipcard Reader). Setiap MS mempunyai nomor identity yang unik disebut International Mobile Equipment Identity (IMEI). Pada kartu SIM berisi nomor khusus dari pelanggan yang disebut International Mobile Subscriber Identity (IMSI). Untuk menambah tingkat kerahasiaan dari IMSI, maka IMSI umumnya tidak dipancarkan melalui radio, tetapi yang dipancarkan adalah Temporary Mobile Subscriber Identity (TMSI). TMSI adalah encryption Identity dari IMSI dengan cara perkalian antara IMSI dengan random encryption yang dikeluarkan oleh AuC.

OSS melakukan semua fungsi diperlukan untuk pengorasan yang memadai dari system jaringan, serta untuk mendapatkan informasi tentang unjuk kerja system. OSS akan bertanggungjawab atas pekerjaan-pekerjaan penting pada jaringan telepon bergerak seperti pelayanan pelanggan (customer care), tagihan (billing), keamanan (security), personalisasi kartu chip (chip card personalization). OSS memiliki fungsi – fungsi pokok sebagai pusat personalisasi untuk SIM (Personalisation Center for SIMs / PCS) yang melayani semua fungsi – fungsi yang berkaitan dengan administrasi dan kartu pengenalan pribadi yang dipergunakan pada jaringan GSM, seperti menerima permintaan dan

pemrosesan kartu SIM, pencetakan dan pengiriman huruf – huruf PIN / PUK dan sebagainya, dan system tagihan dan administrasi (Billing and Administration System / BAS) yang bertanggung jawab atas seluruh tugas OSS yang berkaitan dengan komponen komersial, yang mencakup pelayanan konsumen, administrasi SIM, tagihan dan faktur, manajemen dan kredit, koleksi pembayaran serta transaksi finansial.

2.4 Aspek-Aspek Keamanan Pada System GSM

System GSM yang menggunakan transmisi seperti halnya dengan STBS yang lain yang masih memungkinkan penyadapan pembicaraan oleh pihak ketiga sehingga mengganggu privasi pengguna peralatan komunikasi tersebut. Dalam system yang modern hal seperti tersebut di atas dapat lebih mudah diatasi.

Proteksi dalam system GSM dimulai dari pencegahan penggunaan perangkat oleh orang yang tidak mempunyai otorisasi, dengan demikian mekanisme otorisasi dinilai setiap kali perangkat akan mengakses system. Subscriber harus memberikan identitas kepada system sebelum proses membangun suatu hubungan dilakukan.

Untuk alasan privasi juga diterapkan mekanisme proteksi identitas subscriber pada radiopath. Pada subscriber diberikan identitas sementara yang hanya berlaku bagi area tertentu, dan apabila memasuki area lain akan diberikan identitas sementara yang baru. Dengan pemberian identitas tersebut tidak dimungkinkan untuk menjejak aktivitas suatu subscriber tertentu.

Hal lain yang memerlukan proteksi adalah hubungan signaling. Selain berlangsung antara subscriber dengan jaringan. System mengindikasikan prosedur "cipharing mode setting" yang berarti semua signaling ditransmisikan dalam modus proteksi, demikian halnya dengan user data yang ditransmisikan dan diterima oleh subscriber. Proteksi semacam ini merupakan salah satu fitur dalam system GSM.

Apabila keperluan sekuriti oleh semua network dan perangkat mobile, maka akan menghilangkan kemungkinan perpaduan pemakaian illegal pada system maupun perangkat subscriber.

Informasi pribadi (personal information mobile subscriber / PIMS) dan informasi lainnya, agar penggunaan system menjadi fleksibel dan efisien maka penyimpanan dilakukan pada unit khusus yaitu subscriber identity module (SIM).

2.4.1 Rekomendasi Mengenai Aspek Keamanan GSM

Dalam beberapa rekomendasi GSM, beberapa bagian menjelaskan mengenai aspek keamanan. Ada empat rekomendasi yang secara khusus membahas masalah keamanan dalam system GSM.

1. Rekomendasi GSM 02.09

"Security Aspect" berisi batasan mengenai fitur sekuriti yang disediakan dalam system GSM, suatu penjelasan kapan suatu fitur seharusnya digunakan dan serta implementasinya pada network

2. Rekomendasi GSM 03.02

"Security Related Network Function", berisi batasan mengenai fungsi network yang diperlukan dalam rangka menyediakan fitur seperti yang ditetapkan pada rekomendasi GSM 02.09

3. Rekomendasi GSM 03.21

"Security Related Algorithms" mengenai spesifikasi algoritma kriptologi yang diperlukan untuk mendapatkan fitur dan mekanisme security yang sangat bervariasi.

4. Rekomendasi GSM 02.17

"Subscriber Identity Modules" berupa penjelasan mengenai karakteristik dasar Modul.

2.4.2 Autentikasi

Untuk menghindari kesalahan dalam menggunakan identitas suatu subscriber yang sudah mempunyai otorisasi, dibuat suatu mekanisme autentifikasi. Setiap subscriber diberikan sebuah modul SIM (Subscriber Identity Module) yang berisi mengenai : IMSI (International Mobile Subscriber Identity), Ki (Individual Subscriber Authentication Key) dan A3 (Authentication Algorithm).

Apabila subscriber akan mengakses system, system akan memeriksa identitas tersebut di atas. Sistem mentransmisikan bilangan random (RAND) kepada subscriber. Subscriber kemudian memproses Signal Response (SRES) berdasarkan RAND, Ki dan algoritma A3. Subscriber kemudian mengirim SRES ke system, dan system lalu membandingkan dengan SRES system, apabila

sama maka proses autentikasi dinyatakan berhasil yang berarti dapat dilakukan proses selanjutnya.

Sebaliknya apabila autentikasi dinyatakan tidak berhasil, hubungan diputus dengan indikasi pada subscriber (autentikasi tidak berhasil). Untuk alasan sekuriti, proses SRES dikaukan dengan SIM, dengan demikian tidak terdapat sandi rahasia lain yang diperlukan berada di luar SIM.

2.4.3 Signalling Data Confidentiality

A. Cipherring Key

Untuk melindungi elemen signaling yang sangat peka dalam transmisi maka dibuat suatu mekanisme proteksi. Semua pesan yang mengandung informasi yang peka harus ditransmisikan dalam modus proteksi.

Disamping disebutkan pada butir 4, pada SIM juga terdapat logaritma A8 untuk menghasilkan Ke (cipherring key). Setelah diterimanya RAND oleh subscriber, maka yang diproses tidaka hanya SRES, tapi juga Ke sebagai hasil dari RAND, Ki dan algoritma A8. $Ke = Ki (RAND)$. Ke tersebut tidak untuk ditransmisikan, karena baik subscriber maupun system memproses Ke tersebut. Untuk alasan keamanan, perhitungan KE dilakukan dengan SIM, sehingga tidak ada informasirahasia lain di luar SIM.

A.1. Chiphering Key Sequence Number

Bersamaan dengan pengiriman RAND, system juga mengirim chiphering key sequence number kepada subscriber. Angka tersebut dihubungkan dengan KE yang berlaku, dimaksudkan untuk pencegahan penggunaan angka yang salah. Angka yang dimasukkan oleh subscriber sebenarnya juga turut dikirim pada saat awaaal ke system. Beberapa system mengandalkan keabsahabn cipherring key sewuence number tersebut dalam menentukan keberhasilan autentikasi, juga ada yang mengandalkan cipherring key. Dalam beberapa kasus hal ini masih dianggap belum aman.

A.2. Cipherring Mode Setting

Apabila menurut prosedur suatu informasi yang peka harus ditransmisikan maka diberlakukan prosedur cipherring mode setting. System mengirimkan perintah untuk melakukan cipherring mode kepada subscriber. Setelah perintah tersebut diterima subscriber dapat memulai encipherring/decipherring dengan menggunakan perintah cipherring key yang tersedia. Alur proses encipherring/decipherring dilakukan bit demi bit dengan menggunakan algoritma A5 dan Kc.

B. Subscriber Identity Confidentiality

Untuk menghindari kemungkinan pihak ketiga mengali apakah suatu subscriber sedang mengadakan hubungan pada sisi subscriber sedang mengadakan hubungan pada sisi transmisi, maka dialokasikan

suatu temporary identity (identitas sementara). Identitas ini hanya bersifat local artinya hanya berlaku pada area yang bersangkutan.

Apabila subscriber tidak mempunyai TMSI (Temporary Mobile Subscriber Identity), maka identifikasi diambil dari IMSI (International Mobile Subscriber Identity). Setelah prosedur autentifikasi dan ciphering mode setting selesai, maka TMSI ditransmisikan ke subscriber dalam mode enciphered.

System mendapat informasi bahwa TMSI sudah diterima dengan benar, yang selanjutnya digunakan untuk membangun akses pada waktu yang lain ke system. Apabila TMSI ini digunakan pada area yang lain, maka TMSI harus disertai LAI (local area identity).

C. User Data Confidentiality

Setelah mode ciphering dimulai, enciphering/deciphering dari user data dilakukan sama halnya dengan proses pada signaling data confidentiality

D. Fitur Sekuriti Pada Prosedur Location Updating

Sebagai contoh dimisalkan suatu signaling dalam VLR dan suatu TMSI yang diberikan oleh lokasi sebelumnya masih digunakan. Subscriber dalam hal ini menentukan sendiri identitasnya dengan menggunakan TMSI dan LAI.

E. Informasi Sekuriti Yang Tersimpan Dalam Sistem GSM

Informasi yang digunakan dalam system GSM adalah :

RAND	Bilangan acak yang digunakan untuk memastikan keabsahan subscriber
SRES	Sinyal sebagai respon bahwa RAND telah diterima
Ki	Authentication key untuk masing-masing subscriber digunakan dalam proses sinyal respon dan ciphering-key
Kc	Ciphering key digunakan untuk encipher/decipher signaling dan user data dalam transmisi.
A3	Authentication Algorithm, digunakan untuk menghitung sinyal respon dengan menggunakan Ki
A8	Algoritma bersama dengan menggunakan Ki untuk menghasilkan ciphering key (kc)
A5	Algoritma stream cipher digunakan untuk encipher/decipher dalam pentransmisian signaling dan user data
CKSN	Ciphering Key Sequence Number
TMSI	Temporary Mobile Station Identity

Sistem GSM yang memproses/menghendl informasi sekuriti :

Subscriber (tanpa SIM)	A5
Subscriber Identity Module	A3,A8,IMSI,Ki,TMSI/LAI,Kc/CKSN
Authentication Center	A3,A8,IMSI/Ki
Home Location Register	MSI/RAND/SRES/Kc
Visited Location Register	MSI/RAND/SRES/Kc,IMSI/TMSI/LAI/Kc
Mobile Swiching Center	A5,TMSI/IMSI/Kc

F. Perpindahan Informasi Sekuriti Antara HLR/VLR ke MSC dan Aspek Sekuriti yang Dilaksanakannya.

Subsistem yang paling bertanggungjawab terhadap aspek autentikasi adalah AuC (Authentication Center). AuC dapat saja merupakan system yang terpisah atau terintegrasi menjadi satu kesatuan dengan HLR. Bagaimana cara penanganan AuC dalam network tergantung dari masing-masing operator.

Tugas yang dilakukan oleh AuC adalah sebagai berikut :

- Menghasilkan Ki dan membandingkan dengan IMSI
- Menghasilkan beberapa RAND/SRES/Kc, untuk setiap IMSI yang selanjutnya disiapkan untuk demand yang ada di HLR

HLR menyimpan beberapa set RAND/SRES/Kc milik IMSI dan menerima yang baru dari AuC.

Apabila ada subscriber yang memasuki area suatu Visited Location Register (VLR), ada dua alternatif yang ada harus dipenuhi subscriber tersebut bagi VLR adalah :

- Subscriber memberikan identitas dengan menggunakan IMSI. VLR memerintahkan HLR untuk memberikan lima set RAND/SRES/Kc kepunyaan IMSI
- Subscriber memberikan identitas dengan menggunakan TMSI beserta LAI. VLR memerintahkan VLR sebelumnya untuk mengirimkan IMSI dan sisa RAND/SRES/Kc milik TMSI/LAI tersebut.

Apabila subscriber tidak lagi berada dalam suatu VLR kemudian setelah melakukan akses lain (tentu saja dengan autentikasi), VLR memerlukan beberapa set RAND/SRES/Kc tersebut bergantung pada permintaan di VLR. Semua prosedur ini ditetapkan dalam rekomendasi GSM 09.02, "Mobile Application Part".

G. Subscriber Identity Module (SIM)

Penerapan fitur sekuriti dalam system GSM mengakibatkan pengadaan peralatan khusus. Khususnya untuk masing-masing subscriber memerlukan proteksi ketat pada mekanisme autentikasi. SIM berisi informasi individual subscriber yang berupa unit yang dapat dilepas/dipasang. Penerapan SIM memungkinkan penggunaan perangkat sangat universal. Suatu subscriber dapat memakai SIM untuk mengakses jaringan GSM melalui perangkat mobitnya. Pada saat penyerahan perangkat, subscriber boleh menentukan apakah memerlukan personal identity number (PIN). PIN dapat mencegah penggunaan SIM yang tidak mempunyai otoritas.