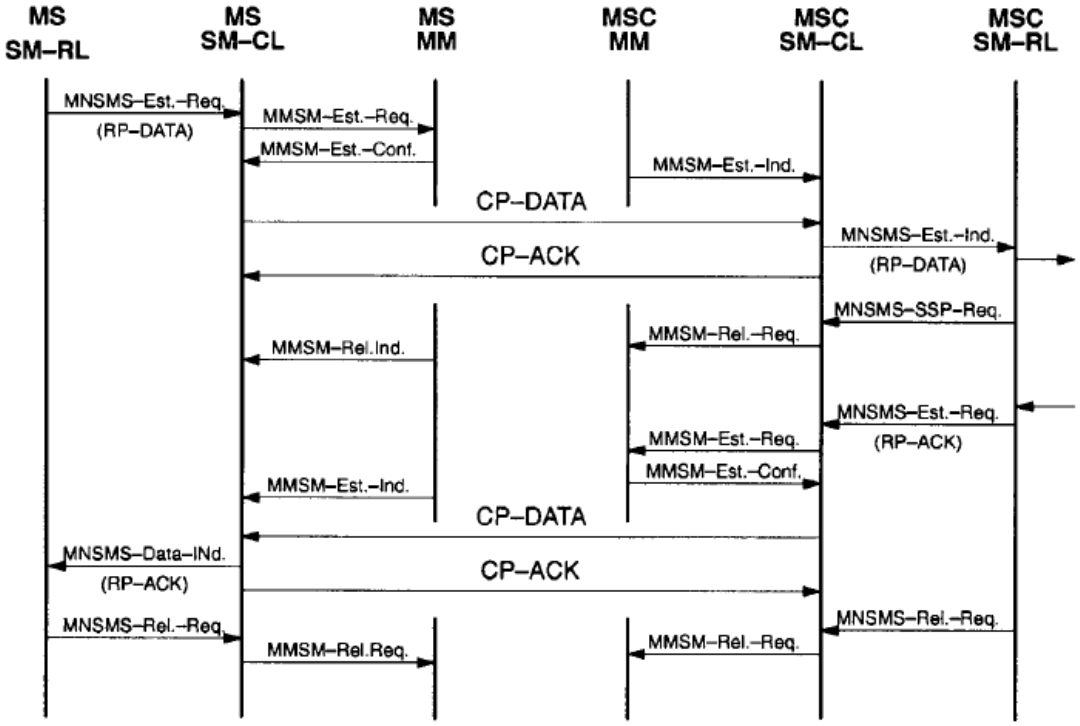
TUGAS TRANSLATE II (Mid-Term)
Mata Kuliah Sistem Komunikasi Nirkabel Generasi Baru

Indra Agustian, 06264

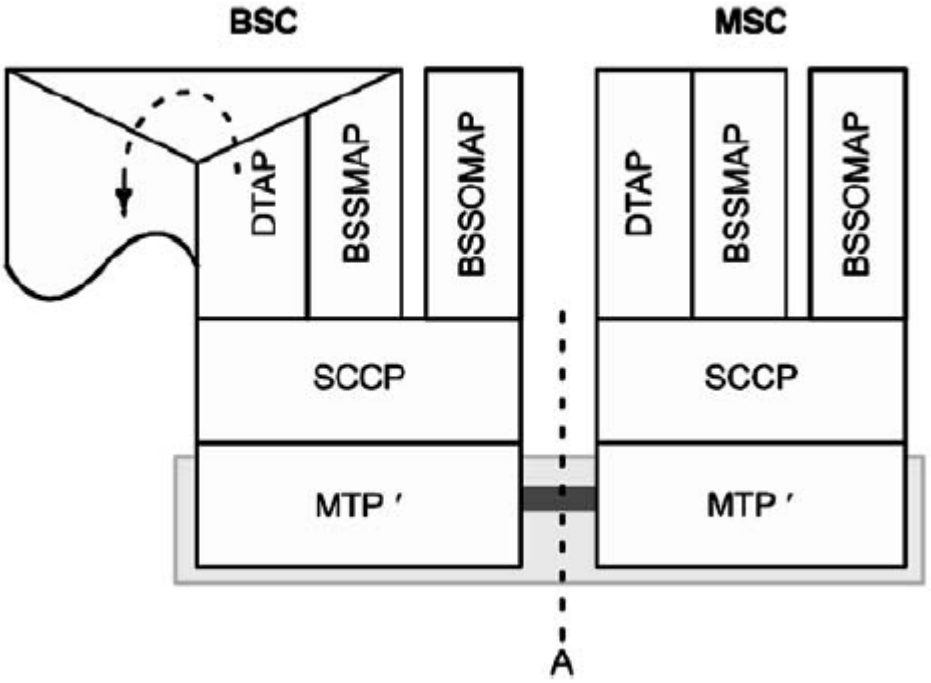
5.5. Pensinyalan Pada Antarmuka A dan Abis

Fungsi protokol yang menggunakan jasa SCCP didefinisikan pada antarmuka A, yaitu BSSAP, terbagi menjadi DTAP dan BSSMAP; lihat Gambar 5.37. Selain itu, diperkenalkan Base Station Sistem Operasi dan Pemeliharaan Bagian (BSSOMAP), yang diperlukan untuk transportasi manajemen jaringan informasi dari OMC melalui MSC ke BSC.

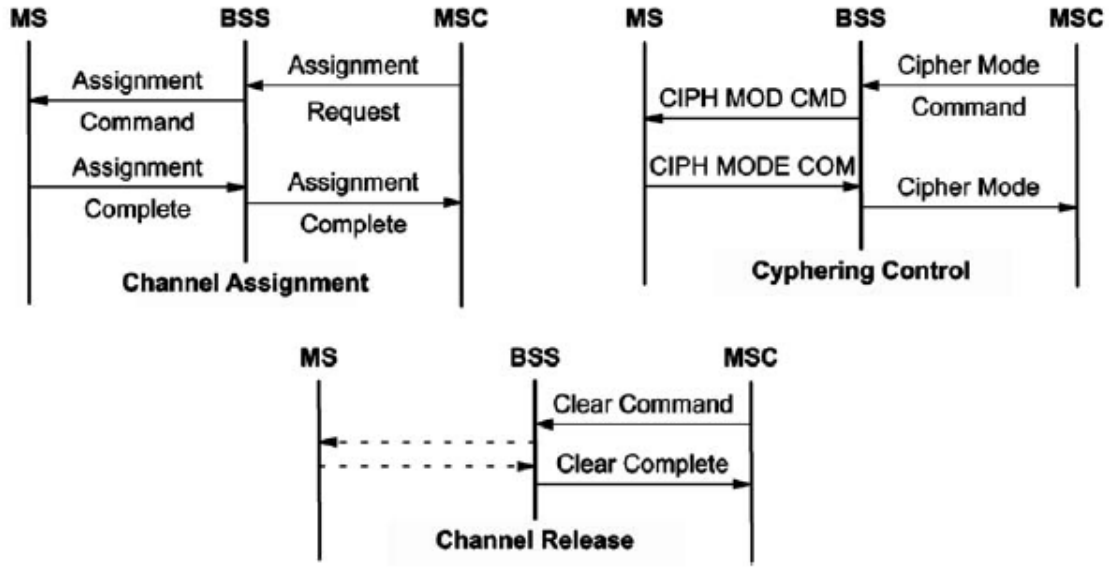
Pada antarmuka A, dapat dibedakan antara dua pensinyalan aliran pesan: yaitu antara MSC dan MS dan satu lagi antara MSC dan BSS. Pesan-pesan ke MS (CM, MM) diteruskan melalui BSS menggunakan Protokol DTAP bagian dari SS#7. BSC dan BTS tidak menafsirkannya. Bagian Protokol SCCP menyediakan layanan transfer "*connectionoriented*" dan "*connectionless*" untuk pensinyalan pesan. Untuk pesan DTAP, hanya diberikan layanan "*connectionoriented*". DTAP dari BSSAP menggunakan satu koneksi pensinyalan untuk setiap MS aktif dengan satu atau lebih transaksi per sambungan. Sebuah koneksi baru dibentuk setiap kali ketika pesan dari sebuah transaksi baru dengan MS harus ditransportasikan antara MSC dan BSS.



Gambar 5.36 Pengiriman pesan singkat pada pesawat CM antara MS dan MSC.



Gambar 5.37 Protokol pada antarmuka A antara MSC dan BSS.



Gambar 5.38 Contoh prosedur BSSMAP

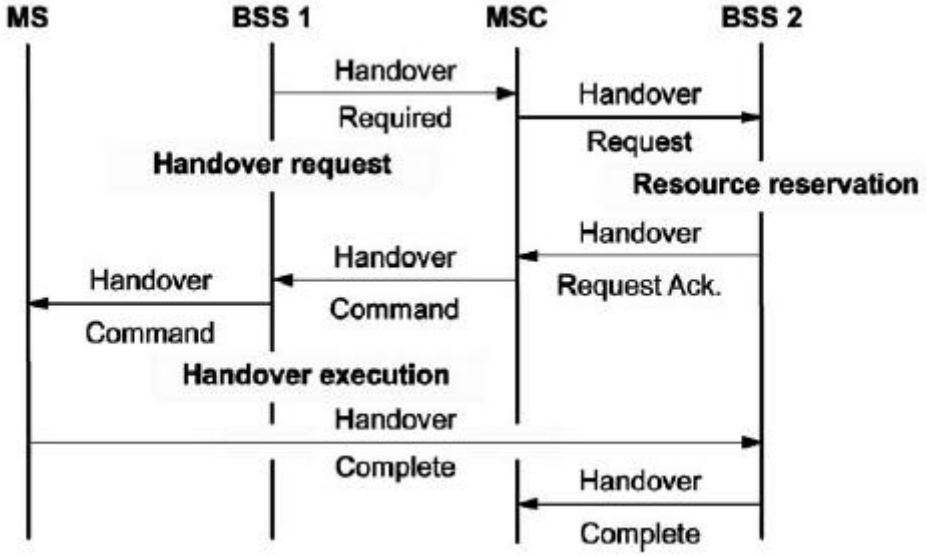
Dua hal dalam pengaturan koneksi SCCP yang baru dibedakan, pertama dalam hal update lokasi dan setup koneksi (keluar atau masuk), BSS meminta sambungan SCCP setelah permintaan saluran (burst akses di RACH) dari MS telah terpenuhi oleh SDCCH atau TCH dan setelah koneksi LAPDm telah diatur di SDCCH atau FACCH. Situasi kedua untuk mengatur koneksi SCCP, adalah serah terima(*handover*) ke BSS lain, dalam hal ini MSC memulai pengaturan sambungan. Sebagian besar pesan isyarat pada antarmuka udara (CM dan MM; Tabel 5.5 dan 5.6) dilewatkan secara transparan melalui BSS dan dikemas dalam DTAP-PDU pada antarmuka A, dengan pengecualian beberapa pesan RR.

BSSMAP mengimplementasikan dua macam lebih signaling prosedur antara MSC dan BSS: yang pertama menyangkut satu MS atau kanal fisik tunggal pada antarmuka udara,

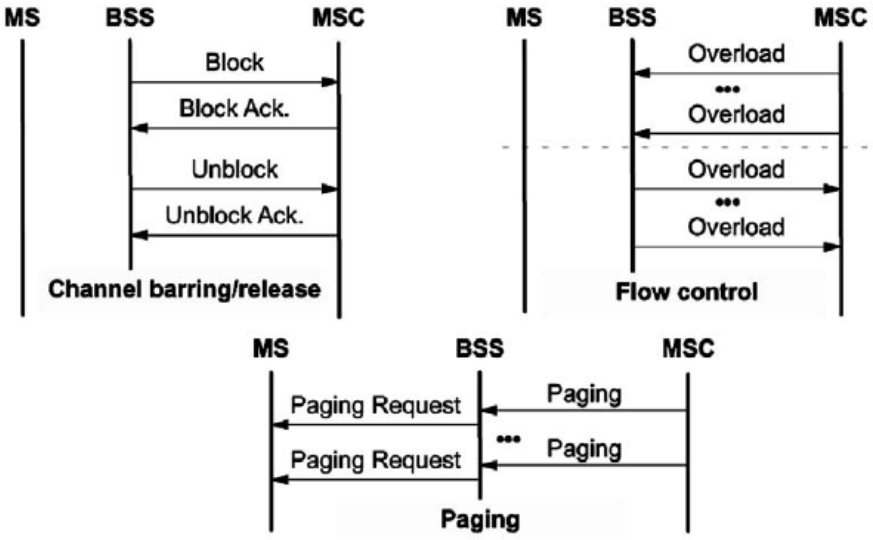
dan yang kedua adalah prosedur global untuk kontrol semua sumber daya dari BSS atau sel. Dalam kasus pertama, BSSMAP juga menggunakan layanan connection-oriented SCCP, sedangkan dalam kasus kedua, prosedur global dilakukan dengan layanan SCCP connectionless. Di antara prosedur BSSMAP untuk sumber daya tersendiri dari antarmuka udara merupakan fungsi manajemen sumber daya (saluran penempatan dan pelepasan, awal dari penyandian) dan kontrol handover(Gambar 5.38 dan 5.39).

Di antara prosedur global BSSMAP adalah paging, aliran kontrol untuk mencegah kelebihan beban prosesor protokol atau saluran CCCH, menutup dan membuka saluran, dan bagian pengendalian handover (Gambar 5.40).

Lapisan transmisi pada antarmuka Abis diantara BTS dan BSC biasanya direalisasikan sebagai garis multiplexing primer dengan 2048 kbit/s (1544 kbit/s di Amerika Utara) atau 64 kbit/s. Ini mungkin termasuk satu koneksi fisik per BTS atau masing-masing satu untuk setiap koneksi antara modul / BCF TRX dan BTS (Gambar 5.5). Pada jalur digital ini, lalu lintas atau saluran isyarat adalah sebesar 16 atau 64 kbit/s. Protokol layer 2 pada antarmuka Abis adalah LAPDm yang memiliki Terminal Equipment Identifier (TEI) yang digunakan untuk mengatasi TRX dan / atau BCF dari BTS (Gambar 5.41).

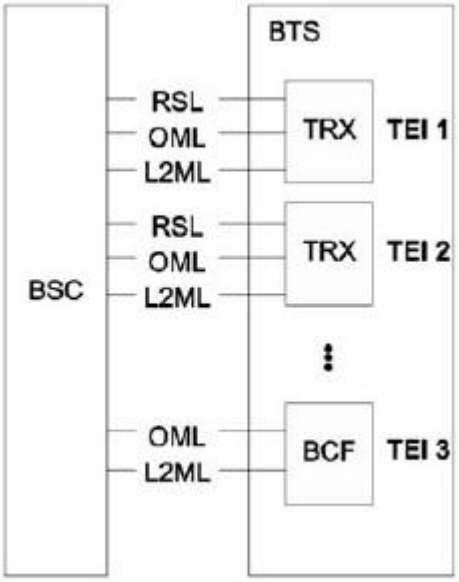


Gambar 5.39 Prosedur handover internal dedicated BSSMAP.

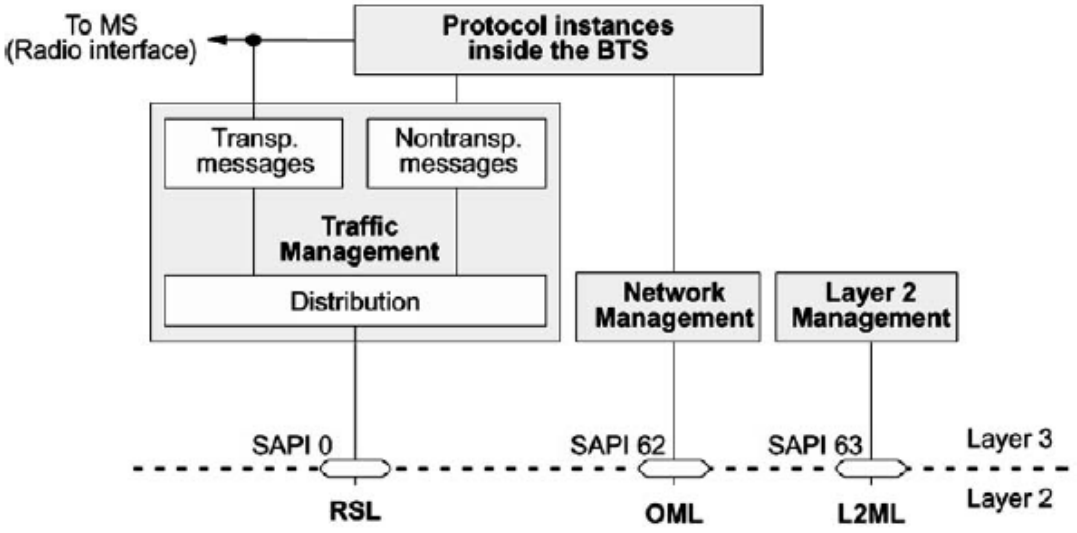


Gambar 5.40 Contoh prosedur BSSMAP global.

Beberapa sambungan LAPDm dibuat untuk setiap TEI: Radio Signaling Link (RSL), SAPI = 0; Operasi dan Pemeliharaan Link (Operation and Maintenance Link/OML), SAPI = 62; dan Layer 2 Link Manajemen (L2ML), SAPI = 63. Manajemen lalu lintas ditangani di RSL, operasi dan pemeliharaan pada OML, dan manajemen pesan-pesan dari layer 2 dikirim pada L2ML ke TRX atau BCF. RSL adalah yang paling penting dari ketiga link untuk kontrol sumber daya radio dan koneksi untuk komunikasi antara MS dan jaringan. Dua jenis pesan yang dibedakan pada link ini sinyal: pesan transparan dan nontransparan (Gambar 5.42). Sedangkan BTS melewati pada pesan transparan dari/ke entitas LAPDm dari MS tanpa menafsirkan atau mengubahnya, pesan nontransparan dipertukarkan antara BTS dan BSC.



Gambar 5.41 Loneksi logical pada Layer 2 antarmuka Abis.



Gambar 5.42 Protokol Layer 3 dari BTS pada antarmuka Abis (BTSM).

Selain itu, salah satu di antara empat kelompok membedakan pesan manajemen lalu lintas dari BTS.

Gambar 5.43 Transfer isyarat pesan transparan.

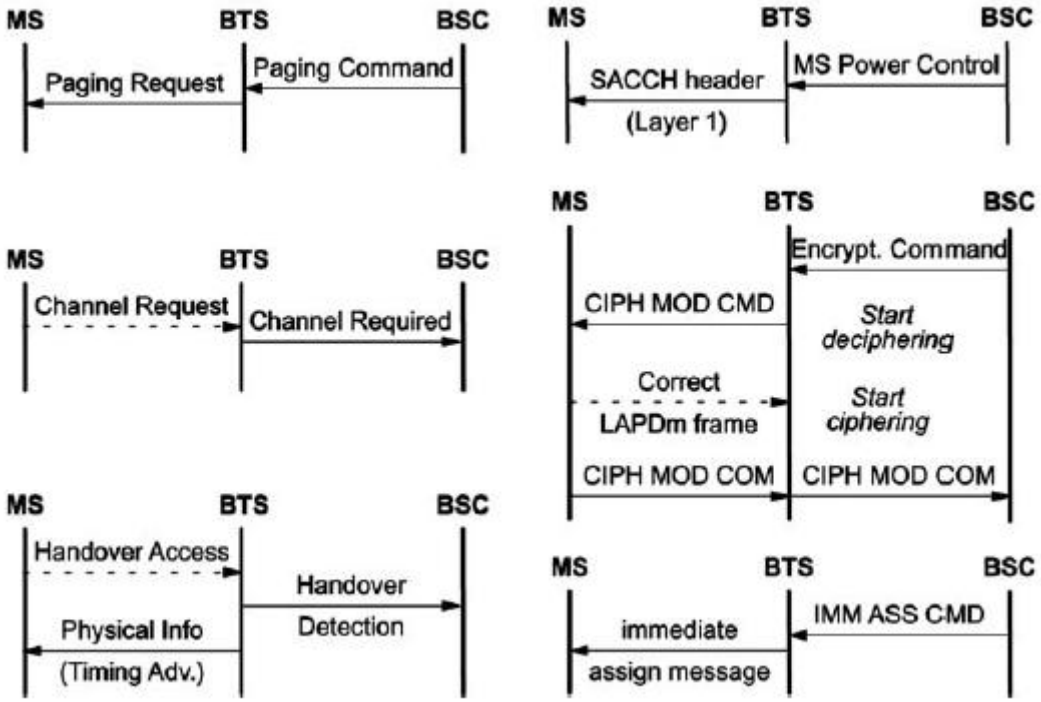
- Manajemen Layer Radio link: prosedur untuk membangun, memodifikasi dan melepaskan sambungan dari lapisan link (LAPDm) ke MS pada antarmuka udara Um.
- Manajemen saluran khusus: prosedur untuk memulai penyandian, pengalihan laporan pengukuran saluran dari MS, kontrol daya pemancar MS dan BTS, deteksi handover dan modifikasi saluran khusus dari BTS untuk MS tertentu yang kemudian dapat menerima saluran dalam pesan lain (menugaskan, perintah handover).
- Manajemen saluran umum : prosedur untuk mentransfer permintaan dari MS (diterima pada RACH), memulai panggilan paging, pengukuran dan transfer pengukuran beban lalu lintas CCCH, modifikasi informasi siaran BCCH, penugasan saluran ke MS (di AGCH) dan transmisi SMSCBs.
- Manajemen TRX : prosedur untuk transfer pengukuran saluran lalu lintas bebas dari TRX ke BSC atau untuk kontrol aliran. Dalam keadaan prosesor TRX kelebihan beban atau kelebihan pada downlink CCCH/ ACCH.

Dengan cara ini, semua fungsi RR di BTS dapat dikendalikan. Mayoritas pesan RR (Tabel 5.4) disampaikan secara transparan dan tidak berakhir di BTS. Pesan ini diangkut antara BTS dan BSC (Gambar 5.43) dalam pesan khusus (DATA REQUEST/ INDIKASI) dikemas menjadi frame LAPDm (Layer 2 pada antarmuka radio).

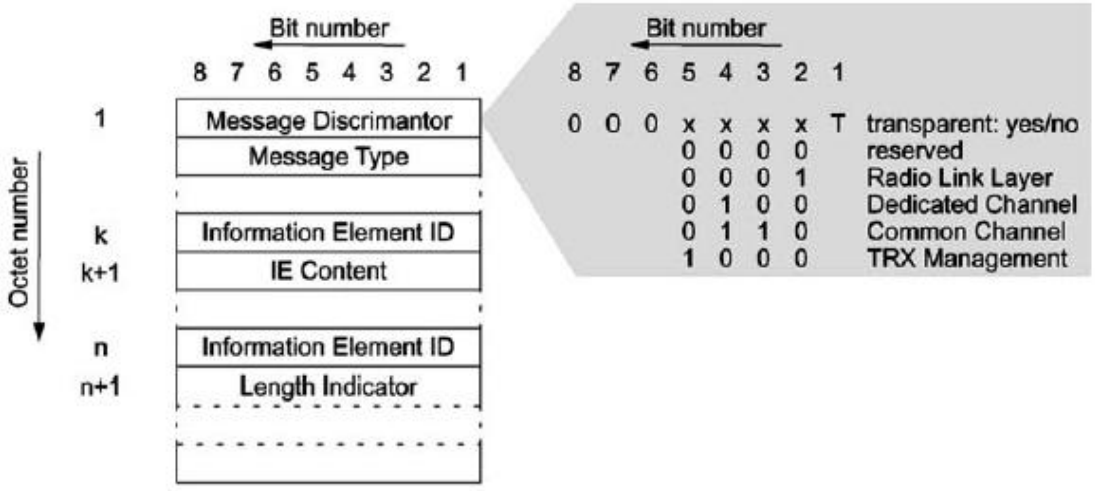
Semua pesan protokol yang diterima oleh BTS pada uplink dari MS dalam LAPDm I/ UI, kecuali untuk laporan pengukuran kanal dari MS, disampaikan sebagai pesan transparan dalam INDIKASI DATA.

Kecuali untuk LAPDm link protokol yang benar-benar diterapkan di BTS, ada beberapa fungsi yang juga ditangani oleh BTS, dan pesan terkait dari atau ke MS ditransformasi oleh BTS ke dalam pesan RR yang sesuai. Ini termasuk tugas saluran, penyandian, perakitan saluran pengukuran dari MS dan TRX dan mengalihkan mereka ke BSC (memungkinkan dengan pengolahan di BTS), perintah power control dari BTS untuk MS, dan permintaan saluran dari MS (di RACH) serta tugas saluran (Gambar 5.44). Dengan demikian, empat dari pesan RR pada arah downlink ke MS (Tabel 5.4) tidak dapat diperlakukan sebagai pesan transparan: Penyandian MODE COMMAND, PAGING REQUEST, SISTEM INFORMASI dan tiga pesan IMMEDIATE ASSIGN. Semua pesan RR lainnya ke MS dikirim transparan dalam PERMINTAAN DATA ke BTS.

Gambar 5.45 menunjukkan format pesan BTSM (Layer 3 antara BSC dan BTS). Transparan dan pesan nontransparan dibedakan antara dengan diskriminator pesan dalam oktet pertama. Untuk tujuan ini, T-bit (bit 1 dari oktet 1) diset ke 1 untuk pesan yang ditujukan agar BTS menanganinya secara transparan atau telah diakui sebagai pesan transparan.



Gambar 5.44 Contoh pensinyalan nontransparan antara BTS dan BSC.



Gambar 5.45 Format protokol pesan BTSM-RSL.

Bit 2 sampai 5 melayani untuk mengarahkan pesan ke salah satu dari empat kelompok didefinisikan pada RSL. Termasuk MT mendefinisikan pesan secara lengkap (Gambar 5.45). Sisa dari pesan BTSM berisi IEs wajib dan opsional yang memiliki panjang tetap, sebagian besar dua oktet atau yang mengandung indikator panjang tambahan dalam kasus panjang variabel.

5.6 Fungsi jaringan Keamanan-terkait: otentikasi dan enkripsi

Metode enkripsi untuk data pengguna dan untuk otentikasi pelanggan, seperti semua teknik untuk keamanan data dan perlindungan data, semakin penting pada sistem digital modern (Eberspächer, 1999). Oleh karena itu GSM diperkenalkan dengan algoritma yang

teknik enkripsi yang handal. Berbagai layanan dan fungsi yang berkaitan dengan keamanan dalam PLMN GSM dikategorikan dengan cara berikut:

- kerahasiaan identitas pelanggan;
- otentikasi identitas pelanggan;
- kerahasiaan elemen pensinyalan informasi;
- kerahasiaan data untuk koneksi fisik.

5.6.1 Perlindungan identitas pelanggan

Fungsi ini dimaksudkan untuk mencegah pengungkapan data pelanggan yang menggunakan jaringan, dengan mendengarkan lalu lintas sinyal pada saluran radio. Di satu sisi, harus menjamin kerahasiaan data pengguna dan lalu lintas sinyal, di sisi lain, juga harus mencegah lokalisasi dan pelacakan dari MS. Ini berarti di atas semua itu IMSI seharusnya tidak menular sebagai teks yang jelas, yaitu tidak terenkripsi.

Selain IMSI, salah satunya menggunakan TMSI pada saluran radio untuk identifikasi pelanggan. TMSI bersifat sementara dan hanya berlaku lokal, yang berarti bahwa pelanggan hanya dapat diidentifikasi secara unik oleh TMSI dan LAI. Hubungan antara IMSI dan TMSI disimpan di VLR.

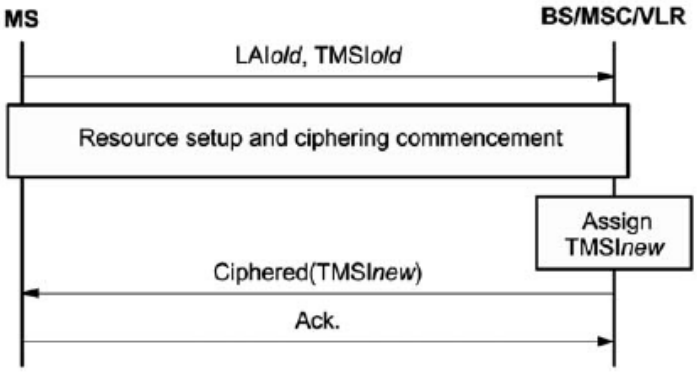
TMSI ini diterbitkan oleh VLR, paling akhir, saat MS berubah dari satu LA ke lainnya (lokasi updating). Ketika area lokasi baru dimasukkan, hal ini diperhatikan oleh MS (bagian 3.3.5) yang bertanggung jawab kepada VLR baru dengan LAI lama dan TMSI (LAIold dan TMSIold; Gambar 5.46). VLR kemudian mengeluarkan TMSI baru untuk MS. TMSI ini ditransmisikan dalam bentuk terenkripsi.

Identitas pelanggan dengan demikian dilindungi menghadapi *eavesdropping* dalam dua cara: pertama, TMSI yang digunakan pada saluran radio bukan IMSI, kedua, setiap TMSI baru ditransmisikan dalam bentuk terenkripsi.

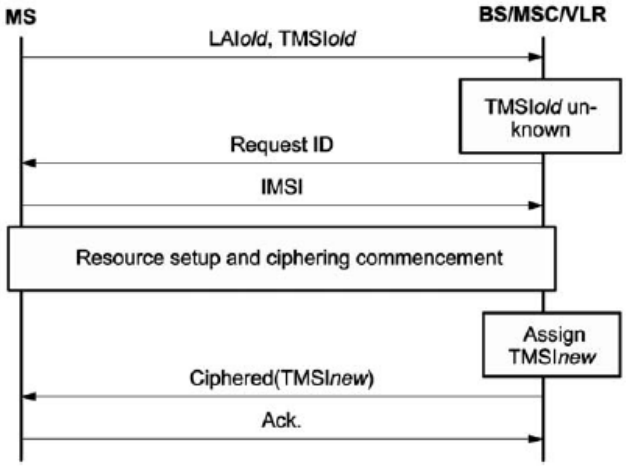
Dalam kasus kegagalan database, jika database VLR sebagian hilang atau tidak ada data pelanggan yang benar tersedia (kehilangan TMSI, TMSI diketahui di VLR, dll), standar GSM tersebut memberikan *acknowledgement* positif dari identitas pelanggan. Untuk itu identifikasi pelanggan, IMSI harus dikirimkan sebagai teks biasa (Gambar 5.47) sebelum enkripsi diaktifkan. Setelah IMSI diketahui, enkripsi dapat dimulai kembali dan TMSI baru dapat ditugaskan.

5.6.2 Verifikasi identitas pelanggan

Ketika pelanggan ditambahkan ke dalam jaringan utama untuk pertama kalinya, sebuah kunci otentikasi pelanggan (Ki) diberikan di samping IMSI untuk memungkinkan verifikasi identitas pelanggan (Juga dikenal sebagai otentikasi).



Gambar 5.46 Transmisi terenskripsi dari identitas pelanggan sementara.



Gambar 5.47 Penghapusan teks transmisi IMSI ketika TMSI tidak diketahui.

Semua fungsi keamanan didasarkan pada kerahasiaan kunci ini. Di sisi jaringan, Ki kunci disimpan dalam Authentication Center (AUC) PLMN utama. Di sisi pelanggan, akan disimpan pada kartu SIM pelanggan.

Proses otentikasi pelanggan didasarkan pada algoritma A3, yang dilakukan di sisi jaringan maupun di sisi pelanggan (Gambar 5.48). Algoritma ini menghitung secara independen pada kedua sisi (MS dan jaringan) *Signature Response* (SRES) dari Ki otentikasi kunci dan Nomor Random (RAND) yang ditawarkan oleh jaringan. MS mentransmisikan yang nilai SRES ke jaringan yang membandingkannya dengan nilai yang dihitung. Jika kedua nilai cocok, otentikasi berhasil. Setiap pelaksanaan A3 algoritma dilakukan dengan nilai baru dari RAND nomor acak yang tidak dapat ditentukan; dengan cara ini rekaman transmisi saluran dan bermain kembali tidak dapat digunakan untuk sebuah identitas palsu.

Gambar 5.48 Prinsip otentikasi pelanggan.

5.6.3 Pembangkit keamanan data

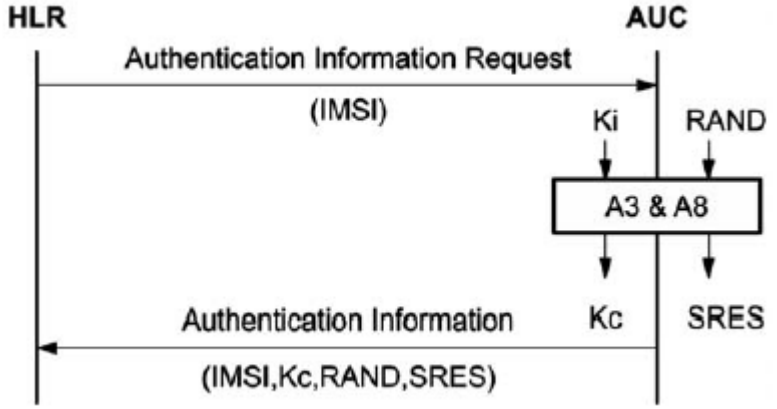
Di sisi jaringan, 2-tuple (RAND, SRES) tidak perlu dihitung setiap kali ketika otentikasi harus dilakukan. Sebaliknya AUC dapat menghitung satu set (RAND, SRES) 2-tuple di muka, simpan di dalam HLR, dan mengirimkannya pada permintaan ke VLR meminta. VLR menyimpan set (RAND [n], SRES [n]) dan menggunakan 2 baru-tuple dari ini ditetapkan untuk setiap prosedur otentikasi. Setiap 2-tuple hanya digunakan sekali, sehingga baru 2-tuple terus diminta dari HLR / AUC.

Prosedur ini, yang memungkinkan data keamanan (Kc, RAND, SRES) dihitung dulu oleh AUC, memiliki keuntungan bahwa otentikasi kunci rahasia Ki pelanggan bisa disimpan

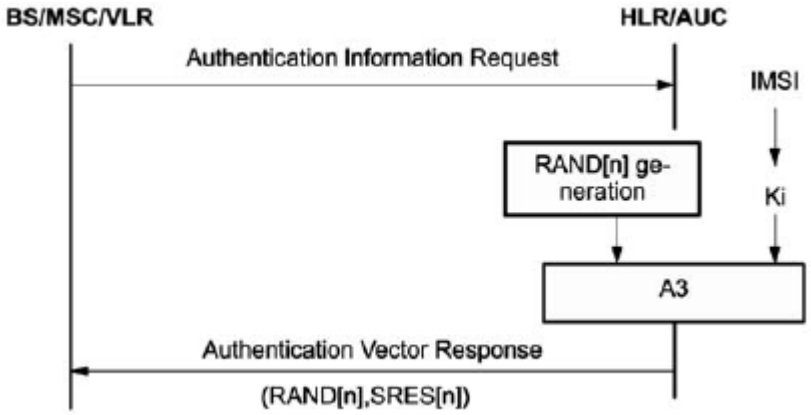
secara eksklusif dalam AUC, yang menjamin tingkat kerahasiaan yang lebih tinggi. Untuk sebuah varian yang agak kurang aman untuk memasok Ki yang sedang dibutuhkan oleh VLR lokal yang kemudian akan menghasilkan data keamanan lokal. Jika Ki kunci disimpan secara eksklusif di AUC, AUC telah menghasilkan satu set data keamanan untuk IMSI tertentu untuk permintaan HLR (Gambar 5.49): yang RAND adalah nomor acak yang dihasilkan dan SRES yang bersangkutan dihitung dengan A3 algoritma, sedangkan algoritma A8 menghasilkan kunci enkripsi Kc.

Himpunan keamanan data, 3-tuple yang terdiri dari Kc, RAND, dan SRES, dikirim ke HLR dan disimpan di sana. Dalam kebanyakan kasus, HLR menyimpan suplai data keamanan (misalnya 5), yang kemudian dapat dipancarkan ke VLR lokal, sehingga seseorang tidak harus menunggu AUC untuk menghasilkan dan mengirimkan kunci baru.

Ketika ada perubahan LA menjadi satu VLR baru, sejumlah set keamanan data dapat diteruskan ke VLR baru. Hal ini memastikan bahwa IMSI identitas pelanggan hanya sekali dipancarkan melalui udara, yaitu ketika TMSI belum diarahkan (melihat pendaftaran) atau ketika data tersebut telah hilang. Setelah itu TMSI (terenkripsi) dapat digunakan untuk berkomunikasi dengan MS. Jika IMSI disimpan di sisi jaringan saja di AUC, semua prosedur otentikasi dapat dilakukan dengan 2-tuple (RAND, SRES) yang belum dihitung oleh AUC.



Gambar 5.49 Pembangkitan satu set data keamanan untuk HLR.



Gambar 5.50 Keamanan otentikasi tingkat tinggi (tidak ada transmisi Ki).

Selain mengurangi beban pada VLR (tidak ada pelaksanaan algoritma A3), jenis identifikasi pelanggan (Gambar 5.50) memiliki keuntungan lain yaitu menjadi sangat aman,

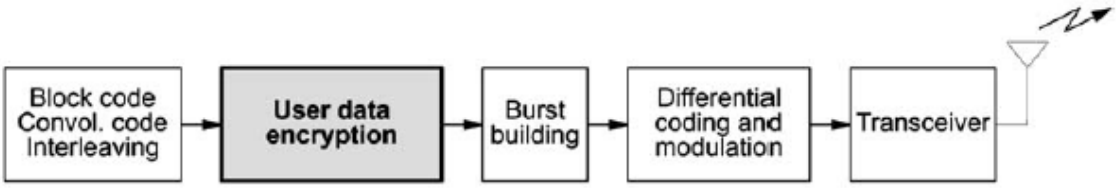
karena data rahasia, terutama Ki, tidak perlu ditransmisikan melalui udara . Ini harus digunakan, khususnya, ketika pelanggan tersebut roaming di jaringan operator luar.

Varian yang kurang aman (Gambar 5.51) hanya boleh digunakan dalam sebuah PLMN. Dalam hal ini, (keamanan-kritis) rahasia kunci Ki setiap kali dipancarkan dari HLR/AUC ke VLR, yang mengeksekusi A3 algoritma untuk otentikasi masing-masing.

5.6.4 Enkripsi Pensinyalan dan data payload

Enkripsi data yang ditransmisikan merupakan sebuah karakteristik khusus dari jaringan GSM yang membedakan layanan yang ditawarkan dari jaringan selular analog dan ISDN. enkripsi ini dilakukan di sisi pengirim setelah pengkodean kanal dan interleaving dan segera sebelum modulasi (Gambar 5,52). Pada sisi penerima, dekripsi langsung mengikuti demodulasi dari aliran data.

Gambar 5.51 Otentifikasi dengan tinkat keamana rendah (transmisi Ki untuk VLR).



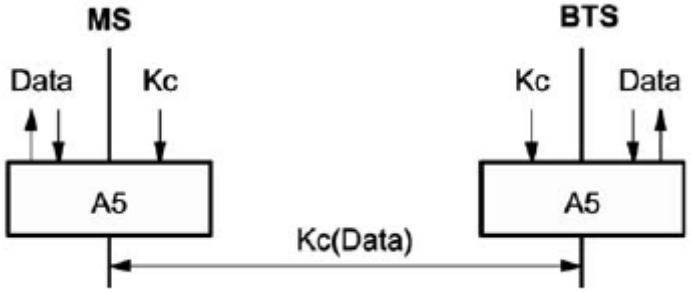
Gambar 5.52 Enkripsi data payload dalam rantai transportasi GSM.

Kunci Cipher (Kc) untuk enkripsi data pengguna dibangkitkan pada setiap sisi dengan menggunakan generator algoritma A8 dan angka random RAND dari proses otentikasi (Gambar 5,53). Kunci Kc ini kemudian digunakan dalam algoritma enkripsi A5 untuk enkripsi simetris data pengguna. Di sisi jaringan, nilai-nilai Kc dihitung dalam AUC/HLR bersamaan dengan nilai untuk SRES. Kunci Kc digabungkan dengan 2-tuple (RAND, SRES) untuk menghasilkan 3-tuple, yang disimpan di HLR/AUC dan diberikan sesuai permintaan, dalam hal identifikasi pelanggan Kunci Ki hanya diketahui bagian (HLR 5,6 .2). Dalam kasus VLR yang mempunyai akses ke Kunci Ki, VLR dapat menghitung Kc langsung.

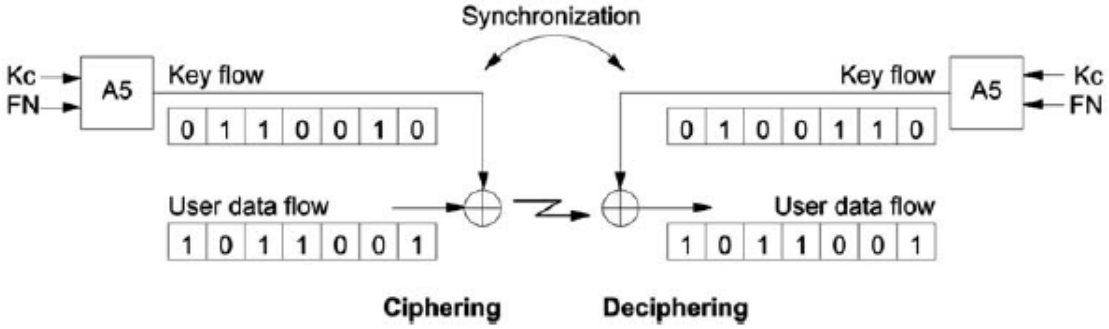
Enkripsi pensinyalan dan data pengguna dilakukan pada MS serta pada base station (Gambar 5.54). Ini adalah kasus enkripsi simetrik, yaitu penyandian dan pengartian dilakukan dengan kunci Kc yang sama dan algoritma A5. Berdasarkan Kunci Ki rahasia yang tersimpan dalam jaringan, kunci cipher Kc untuk koneksi atau transaksi sinyal bisa dihasilkan di kedua sisi, BTS dan MS dapat menguraikan data masing-masing. Pensinyalan dan data pengguna akan dienkripsi bersama (TCH / SACCH / FACCH), dan untuk sinyal saluran khusus (SDCCH) digunakan metode yang sama dengan yang digunakan untuk saluran lalu lintas.

Proses ini juga disebut stream cipher, yaitu Penyandian menggunakan aliran bit yang ditambahkan bitwise ke data yang akan enciphered (Gambar 5,55). Penguraian terdiri dari operasi EKSKLUSIF tambahan OR data stream enciphered dengan aliran Penyandian. Para FN dari frame TDMA yang sedang berlangsung dalam hyperframe (bagian 4.3.1) merupakan masukan untuk algoritma A5 selain kunci Kc, yang dibangkitkan lagi untuk setiap koneksi atau transaksi. Jumlah frame saat ini dipancarkan di SCH dan dengan demikian tersedia setiap waktu untuk semua stasiun mobile saat ini. Sinkronisasi antara Penyandian dan menguraikan proses demikian dilakukan melalui FN.

Gambar 5.53 Pembangkitan kunci cipher Kc.



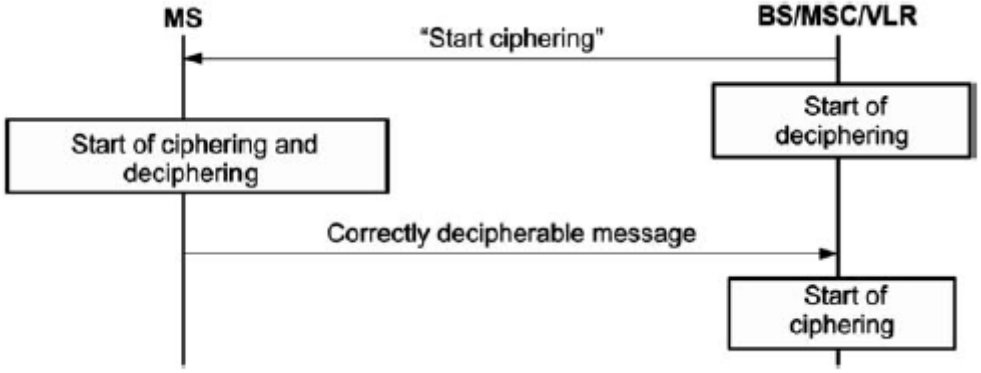
Gambar 5.54 Prinsip enkripsi simetris data pengguna.



Gambar 5.55 Penggabungan payload data stream dan stream penyandian.

Namun, permasalahan sinkronisasi pengaktifan mode penyandian harus diselesaikan terlebih dahulu: menguraikan mekanisme di satu sisi harus dimulai pada saat yang tepat. Proses ini dimulai di bawah kendali jaringan, segera setelah prosedur otentikasi selesai atau ketika kunci Kc telah diberikan ke base stasiun; Gambar 5.56. BTS, dipancarkan ke MS meminta untuk memulai proses penyandian, dan memulai proses mengartikan sendiri. MS

kemudian mulai penyandian dan mengartikan. Pesan ciphered pertama dari MS yang mencapai jaringan dan memecahkan dengan benar, mengarah ke awal dari proses penyandian di sisi jaringan.



Gambar 5.56 Start Sinkronisasi dari proses penyandian.

5.7 Pensinyalan pada antarmuka pengguna

Antar muka lain yang sering diabaikan namun demikian sangat penting dalam suatu sistem selular adalah antarmuka pengguna untuk peralatan MS. Man-Machine Interface (MMI) ini dapat direalisasikan secara bebas, dan oleh karenanya dilakukan dalam berbagai cara oleh para produsen perangkat mobile.

Untuk menjaga agar ada satu set fungsi kontrol layanan terstandarisasi meskipun banyak variasi yang dilakukan oleh produsen, maka diperkenalkan suatu perintah MMI.
Perintah-perintah MMI ini menetapkan prosedur-prosedur, terutama untuk kontrol pelayanan dasar dan SS. Prosedur kontrol ini dimasukkan di sekitar input string perintah dari token yang diukur dan diformat dengan tanda * dan #.
Untuk menghindari pengguna harus belajar dan menghafal sejumlah prosedur pengendalian layanan sebelum dapat menggunakan telepon selular, Disiapkan satu set kecil perintah dasar yang dibutuhkan untuk antarmuka MMI, ini adalah MMI umum paling dasar yang harus dipenuhi oleh semua MSS.

Spesifikasi dari public MMI dasar ini, digarisbawahi pada fungsi-fungsi dasar yang harus dilaksanakan sebagai pensyaratan minimum MMI dari suatu MS. Hal ini mencakup pengaturan keyboard 12-tombol dengan angka 0 sampai 9 dan tombol untuk * dan # termasuk pula tombol SEND dan END, yang berfungsi untuk memulai panggilan yang diinginkan atau menerima/menolak panggilan. Beberapa urutan operasional dasar untuk membuat atau menerima panggilan juga termasuk dalam MMI ini. Persyaratan ini sangat umum sehingga mudah untuk dipenuhi oleh semua peralatan mobile. Perintah MMI untuk mengendalikan SS, penyelidikan dan konfigurasi parameter jauh lebih rumit. Dengan menggunakan set perintah MMI yang dibuat seragam untuk semua MS maka dimungkinkan untuk melakukan fungsi control yang sering tersembunyi pada menu user guidance peralatan yang spesifik. Namun untuk fungsional area tertentu, sebuah MS dapat dioperasikan dengan independen menurut pabrikannya. Jika seseorang memilih menu bimbingan pengguna (user guidance) yang terkadang sangat mudah dibandingkan mempelajari urutan kontrol untuk fungsi masing-masing. Urutan ini dipetakan ke masing-masing prosedur sinyal di dalam MS.

Tabel 5.8 Format input beberapa perintah MMI.

Function	MMI procedure
Activate	*nn(n)*Si#
Deactivate	#nn(n)*Si#
Status enquiry	*#nn(n)*Si#
Registration	**nn(n)*Si#
Delete	##nn(n)*Si#

Perintah MMI selalu dibangun menggunakan pola yang sama. Ada lima format dasar (Tabel 5.8), yang semua mulai dengan kombinasi dari token * dan #: aktivasi (*), penonaktifan (#), status penyelidikan (*#), pendaftaran (**) dan pembatalan (# #). Selain itu, perintah MMI harus berisi kode MMI pelayanan dari dua atau tiga token, yang akan memilih fungsi yang akan dilakukan. Dalam kasus tertentu, prosedur MMI membutuhkan argumen tambahan atau parameter, yang dipisahkan oleh *, sebagai Informasi Tambahan (Si). Perintah MMI selalu diakhiri dengan # dan mungkin juga memerlukan penekanan tombol SEND, jika perintah tersebut tidak dilaksanakan secara lokal dalam MS tetapi harus dikirimkan ke jaringan. Tabel 5.9 berisi beberapa contoh dasar dari perintah MMI, misalnya permintaan untuk IMEI dari MS (* # 06 #) atau perubahan PIN (** 04 old_PIN * * new_PIN * new_PIN #) yang digunakan untuk melindungi kartu SIM terhadap penyalahgunaan. Contoh ini juga menunjukkan bagaimana adanya informasi tambahan tertanam dalam perintah.

Tabel 5.9 Beberapa perintah.dasar MMI

Function	MMI procedure
Mobile phone IMEI enquiry	*#06#
Change password for call barring	**03*330*old_PWD*new_PWD*new_PWD#
Change PIN in SIM	**04*old_PIN*new_PIN*new_PIN#
Select SIM number storage	n(n)(n)#

Dengan adanya perintah MMI, juga memungkinkan untuk mengkonfigurasi dan menggunakan SS. Untuk tujuan ini, setiap SS dilengkapi dengan dua atau tiga digit kode layanan MMI untuk memilih SS tertentu (Tabel 5.10). Dalam beberapa kasus, informasi tambahan wajib ada untuk aktivasi layanan, misalnya ketika seseorang perlu target Tujuan Number (DN) untuk fungsi forwarding panggilan, atau Aktivasi Password (PW) untuk SS dari pembatasan panggilan masuk atau keluar (Sia pada Tabel 5.10).

Contoh dari pengalihan panggilan tanpa syarat (unconditional call forwarding) juga menggambarkan perbedaan antara pendaftaran dan aktivasi layanan. Dengan perintah call_number ** 21 * # maka fungsi pengalihan akan didaftarkan, nomor target dikonfigurasi, dan pengalihan tanpa syarat diaktifkan. Lebih lanjut, pengalihan tanpa syarat dapat dinonaktifkan setiap saat dengan # 21 # dan diaktifkan kembali dengan * 21 #. Nomor panggilan target ini akan tetap disimpan, kecuali dibatalkan dengan perintah # # 21 #. Setelah pembatalan, jika pengalihan panggilan diinginkan lagi, maka terlebih dahulu harus didaftarkan lagi menggunakan ** 21. . . perintah.

Tabel 5.10 kode layanan MMI untuk SS.

Abbreviation	Service	MMI code	Sia	Sib
	All call forwarding, only for (de)activation	2	–	–
	All conditional call forwarding (not CFU), only for (de)activation	4	–	–
CFU	Call forwarding unconditional	21	DN	BS
CFB	Call forwarding on mobile subscriber busy	67	DN	BS
CFNRy	Call forwarding on no reply	61	DN	BS
CFNRc	Call forwarding on mobile subscriber not reachable	62	DN	BS
	All call barring (only for deactivation)	330	PW	BS
BAOC	Barring of all outgoing calls	33	PW	BS
BOI	Barring of outgoing international calls	331	PW	BS
BOIC-exHC	Barring of outgoing international calls except those to home PLMN	332	PW	BS
BAIC	Barring of all incoming calls	35	PW	BS
BIC-Roam	Barring of incoming calls when roaming outside the home PLMN	351	PW	BS
CLIP	Calling line identification presentation	30	–	BS
CLIR	Calling line identification restriction	31	–	BS
CW	Call waiting	43	–	BS
COLP	Connected line identification presentation	76	–	BS
COLR	Connected line identification restriction	77	–	BS

Tabel 5.11 Kode MMI untuk pelayanan dasar.

Category	Service	MMI code BS
Telematic service	All telematic services	10
	Telephone	11
	All data services	12
	Facsimile	13
	Videotex	14
	Teletext	15
	SMS	16
	All data services except SMS	18
	All telematic services except SMS	19
Bearer service	All bearer services	20
	All asynchronous services	21
	All synchronous services	22
	All connection-oriented synchronous data services	24
	All connection-oriented asynchronous data services	25
	All packet-oriented synchronous data services	26
	All PAD-access services	27

Untuk beberapa layanan dasar, karakteristik-karateristiknya juga dapat diaktifkan secara selektif. Perintah MMI dapat berisi bidang parameter kedua dengan informasi tambahan (Sib, Tabel 5.10) yang sekali lagi dipisahkan dengan *. Bidang ini berisi kode layanan BS untuk layanan dasar dimana SS-nya efektif. Rangkuman kode MMI untuk pelayanan dasar diberikan dalam Tabel 5.11. Sebagai contoh, seseorang dapat membatasi panggilan masuk kecuali pesan singkat dengan perintah ** 35 * PW * 18 #, atau seseorang dapat meneruskan bila ada faks masuk ke nomor fax_number dengan perintah fax_number * ** 21 * 13 # (pelayanan jarak jauh lainnya tetap tidak terpengaruh).