EEE-160016

SONARGAON UNIVERSITY

29/1, Kawran Bazar, Tejgaon, Dhaka.



Submitted By

Name	ID
Md. Murad Hossain	EEE1403003110

Supervisor

Md. Habibur Rahman

12.02.16

Coordinator & Lecturer

Department of Electrical and Electronics Engineering

SONARGAON UNIVERSITY

Candidates' Declaration

It is declared hereby that this thesis paper or any part of it has not been submitted to anywhere else for the award of any degree.



.....

Md. Murad Hossain (EEE1403003110)

SONARGAON UNIVERSITY



Certificate

This is to certify that the thesis entitled **A Study On Gsm Network Mangement System** have been carried out under my supervision

By

Md. Murad Hossain (EEE1403003110)

Supervisor

.....

Md. Habibur Rahman

Coordinator & Lecturer

Department of Electrical and Electronics Engineering

SONARGAON UNIVERSITY

Abstract

In high voltage ac system, the system voltage and frequency changes rapidly with the variation of load. The reactive power also changes with the variation of load which affects the system voltage therefore it is necessary to analyze the power system in order to determine system parameters and its variation under various load conditions In this thesis work, in order to get an idea about the power flow nature of the transmission system of Bangladesh, 42 buses are considered. The fast decoupled method is used for analyzing the power flow of 42 buses and later MATLAB coding is used for determining the buses having problem in reference system voltage. The proposed decoupled method is faster and easier than the conventional method. For reactive power compensation, the required capacitive or inductive bank is determined by using logical flow chart. The size of the reactor bank is calculated by conventional method and the thryristor based switching technique is used for connecting the reactor bank with the transmission line according to the system requirement. Since fast switching is required for maintaining the system voltage constant under various load conditions therefore Microcontroller is used for controlling the switching devices. The Microcontroller provides necessary gate pulses to the Triacs which perform the switching action for connecting either the capacitor or inductor bank with the system. The connected capacitor and inductor also acts as a harmonic suppressor in case of harmonic effect in the transmission line. The proposed method of power flow analysis and reactive power compensation can be applied in any complicated power system network.

Acknowledgement

It gives us a great pleasure to have the privilege of expressing our indebtedness and gratitude to our supervisor Md. Habibur Rahman, for his valuable guidance, his deep interest, advice and encouragement throughout the thesis work.

We also sincerely wish to acknowledge our gratitude to our faculty members of **Department of Electrical and Electronics Engineering Sonargaon University** for extending their help and assistance to work on this thesis.

Md. Murad Hossain (EEE1403003110)

CONTENT

CHAPTER

1 INTRODUCTION TO MOBILE TELECOMMUNIATION AND GSM 1

1.1 Mobile Telephony 1

1.2 History of wireless communication 1

1.3 Connection Types 2

1.3.1 Simplex connections 2

1.3.2 Duplex Connections 2

1.4 Single cell system 2

1.5 Innovations in Mobile Radio Communications 3

1.6 Cellular Mobile Radio Systems 3

1.7 First Generation (1G) cellular mobile radio systems 4

1.7.1 Limits of the first generation mobile radio systems 4

1.8 History of GSM 6

1.9 Second Generation (2G) cellular networks 8

1.10 2.5 Generation 9

1.11 3rd Generation 9

1.12 Adaptations of GSM 10

2 GSM ARCHITECTURE

2.1 Over view 12

2.1.1 The GSM-PLMN 12

2.1.2 Network Elements 13

2.1.3 Interfaces 15

2.2 Network Elements 16

2.2.1 The Mobile Station 16

2.2.2 The SIM Card 16

2.2.3 The Mobile Equipment 17

2.2.4 The Base Station Subsystem 18
2.2.4.1 Base Station Controller 19
2.2.4.2 Base Transceiver Station 20
2.2.4.3 Transcoding and Rate Adaptation Unit 21
2.3 The Network Switching Subsystem 22
2.3.1 Mobile Switching Center 23
2.3.2 Visitor Location Register 25
2.3.3 Home Location Register 26
2.3.4 Authentication center 28
2.3.5 Equipment Identity Register 28
2.4 Operation Sub-System 29

3 SPECIFICATIONS, PROCEDURES & SECURITY OF GSM NETWORK

3.1 GSM Specifications 30
3.1.1 GSM Subscriber Services 31
3.2 Codes & Identities 33
3.2.1 GSM Service Ares & Codes 33
3.2.1.1 International GSM Service Area 33
3.2.1.2 National GSM Service Area 34
3.2.1.3 PLMN Service Area 34
3.2.1.4 MSC/VLR Service Area 35
3.2.1.5 Location Area 35
3.2.1.6 BTS Service Area 35
3.2.1.7 Subscriber Identities 36
3.3 Security Features 36
3.3.1 Triples 38
3.3.2 Authentication 39
3.3.3 Ciphering 40
3.3.3.1 Ciphering process 41
3.3.4 TMSI Allocation 42
3.3.5 IMEI Check 43

3.4 Location Update 44
3.4.1 LUP without changing the MSC area 45
3.4.2 LUP with VLR Change 46
3.5 Radio Transmission 47
3.5.1 Transmission Problems 48
3.5.2 Solutions of transmission problems 48
3.6 Call Setup 49
3.6.1 Mobile Originating Call 49
3.6.2 Mobile Terminating Call 50
3.6.3 Mobile Mobile Call 51
3.6.4 Mobile Internal Call 51
3.6.5 Call from MS to PSTN 52
3.6.6 Call from PSTN to MS 53
3.7 Handover 54
3.7.1 Intra-Cell Handover 54
3.7.2 Intra-BSS Handover 54
3.7.3 Intra-MSC Handover 54
3.7.4 Inter-MSC Handover 55
3.7.5 Subsequent Handover 55
3.7.6 Handover Decision 55
3.7.7 Handover Example: Inter-MSC Handover 57
3.8 Emergency Call 58
3.8.1 MS Attached 59
3.8.2 MS Detached 60
61

4.1 Discretion **62**

4.2 Conclusion **63**
4.3 Reference Books & Links **64**
4.4 Glossary **65**

CHAPTER 1

Introduction to Mobile Telecommunications and GSM

1.1 MOBILE TELEPHONY

Mobile telecommunications is one of the fastest growing and most demanding of all telecommunications technologies. Currently, it represents an increasingly high percentage of all new telephone subscriptions worldwide. In many cases, cellular solutions successfully compete with traditional wire line networks and cordless telephones. In the future, cellular systems employing digital technology will become the universal method of telecommunication. [1]

1.2 HISTORY OF WIRELESS COMMUNICATION

"Mobile Communication" is much older than many people think. There have been diverse "acoustic and optic means of remote information transfer" in the most varied cultures and stages of civilization on all populated continents. The range of information transfer was very limited and the quality of the messages was affected by outer conditions such as the weather. In order to increase the range of information transfer in these times, transit stations were in part systematically constructed.

Beginnings of Electronic Communications

- Telegraph: S.F.B. Morse: 1843 First experimental telegraph line: Washington - Baltimore
- Telephone: Phillip Reis 1861: First speech transmission by cable / A. G. Bell: 1876 World Exhibition, Philadelphia

At first electronic communications was possible only via wire i.e. by means of fixed (immobile) connections, forerunners of today's Fixed Network Connections. Initially an operator ("switchboard girl") was needed to establish these fixed physical connections for the caller manually at the central office. The first automatic exchanges were first put into service in the mid-1920s. [3]

Radio Communications

Radio connections were first used for Wireless Communications in the late 19th century; information was sent via "ether".

1873: J.C. Maxwell - electromagnetic wave theory

1887: H. Hertz - experimental proof of the existence of electromagnetic waves

1895: A. Popow - first receiver with antenna for weather reports

1895: G. M. Marconi - first wireless transmission using spark inductor generated HF waves (Morse code)

1897: "Marconi Wireless Telegraphy Company" founded

1901: First transatlantic transmission (Marconi)

1903: "Deutschen Telefunken GmbH" founded by AEG and Siemens & Halske

1906: First speech & sound transmission (Lorenz AG / Deutsche Telefunken GmbH)

1909: First radio broadcast (New York, Caruso) [B2]

1.3 Connection Types:

There are two principles for radio connections:

1.3.1 Simplex Connection:

Simplex connections are a "one-way street" for communication in the form of (mostly fixed) transmitters and mobile receivers. This has been realized as e.g. (broadcast) radio and television. But simplex connections are also used for direct communication exchange i.e. two- way communication using stations which can be used both as a transmitter and a receiver (e.g. walkie-talkies). However the equipment (transmitting / receiving stations) cannot transmit and receive simultaneously. The call cycles or call intervals are determined by prior agreement or personal code words ("over"). [B2]

1.3.2 Duplex Connections:

Duplex connections signify two-way communication. Users can transmit and receive messages simultaneously. An example of an early duplex connection is radio telegraphy. [B2]

1.4 Single Cell Systems:

The first Mobile Telephone Service to offer duplex connections comparable to fixed network based telephone services started in 1946 as a car phone service in St. Louis, Missouri. Comparable mobile telephone services appeared in post-war Europe some years later.

Problems in early mobile (car) telephone services (late 1940s/early 1950s):

- An operator was needed to connect calls within the wireless network.

- The equipment required was extremely heavy, bulky (therefore only feasible as a car phone service) and expensive.
- The service range was limited to the area that could be covered by a single transmitting or receiving station (single cell system).

- The HF frequency range available was (is) very limited; it had to be (and still has to be) distributed among competitors (e.g. the military, radio, and television).

The result was limited capacity, rapid market saturation, high equipment costs and low service quality. [B2]

1.5 Innovations in Mobile Radio Communications:

Technical Innovations / Equipment

Fast development of new technologies such as semiconductor technology, diodes, transistors, integrated circuitry, microprocessors,...

- automatic switching
- reduction of hardware costs

reduction of size and weight of equipment (in the 1950s/1960s a car phone took up half of a car trunk; 1988: introduction of the mobile phone) but:

- very limited telephone network capacity.

During the 1970s large-scale integrated, electronic applications and the development of microprocessors made the configuration of more complex systems possible. One result of this was the development of single-cell transmitter systems with multiple receiving stations. This made it possible to extend the range of the supply area, i.e. the operational range of the subscriber because the mobile station's transmitter power limits the size of the cell in Single Cell Systems. However no increase in capacity resulted from this. [B2]

1.6 Cellular Mobile Radio Systems:

The breakthrough in capacity, which resulted in a significant increase in the number of subscribers, was achieved with the introduction of the Cellular Radio System in the late 1970s/early 1980s. The coverage of the supply area of a mobile communication operator involves many radio cells with cellular radio systems, in which the

aforementioned limitation of the available HF frequency range is neatly circumvented through the repeated use of the HF channels. [1]

1.7 First Generation (1G) Cellular Mobile Radio Systems:

Information transmission of first generation cellular mobile radio system takes place via analogue radio interface. These systems were tested in many countries in the end of the 70s.

In 1979, mobile services were introduced for commercial operation; in the USA, AMPS (Advanced Mobile Phone Service), and in Japan, NTT-MTS (Nippon Telegraph & Telephone Co.).

In the early 80s, the NMT (Nordic Mobile Telephone) was introduced in Scandinavia, in 1985 TACS (Total Access Communication System) was introduced in England and the C450 System in Germany. [B2]

Year	Standard	Mobile Telephone System	Technology	Primary Markets
1981	NMT 450	Nordic Mobile Telephony	Analogue	Europe, Middle East
1983	AMPS	Advanced Mobile Phone System	Analogue	North and South America
1985	TACS	Total Access Communication System	Analogue	Europe and China
1986	NMT 900	Nordic Mobile Telephony	Analogue	Europe, Middle East
1991	GSM	Global System for Mobile communication	Digital	World-wide
1991	D-AMPS	Digital-AMPS	Digital	North and South America
1992	GSM 1800	Global System for Mobile communication	Digital	Europe
1994	PDC	Personal Digital Cellular	Digital	Japan
1995	PCS 1900	Personal Communication Services	Digital	North America

Table 1.1: GSM Standards

1.7.1 Limits of the First Generation Mobile Radio Systems

1. **Capacity:** The capacities limits of analogue technology are reached quickly even with cellular networks. The demand increases with the offer and the sinking prices. A number of 850,000 subscribers, i.e. the maximum capacity of the analogue C-network, corresponds to less than 7 % of the mobile subscribers in 1998 (only 6 years after

introducing digital networks). The capacity of digital networks has not yet been exhausted.

2. **Quality:** A second problem was the often inadequate transmission quality of the analogue systems, which increased with the distance of the mobile subscriber. A detailed description and discussion of the problems regarding the transmission quality or the disadvantages of the analogue system in comparison to digital one can be found in the next chapter.

3. Incompatibility: One or more analogue networks on frequency bands 450/900 MHz existed in most European states in the late 1980s. Every one of these networks formed a mobile communication island since the individual standards of these networks were incompatible in most cases (or still are, as far as they still exist); they prevented mobile phone traffic across borders (International
Roaming). Europe thus looked liked a rag rug of incompatible systems.

The limits of existing analogue systems

1. Capacity: the number of potential mobile phone customers is larger than the expected capacity of analogue systems,
2. Quality: insufficient transmission quality with increasing distance between the mobile station and the base station,

3. Incompatibility: between different national standards,
were already recognized since the early 80s and were discussed on an international European level. The need to develop a new, standard cellular system for Europe was acknowledged.
The GSM Standard was developed for this purpose. [1]

1.8 HISTORY OF GSM:

This history of GSM is outlined in the following table:

Date	Activity
1982-1985	• Conference Europeenne des posteset Telecommunications (CEPT) began specifying a European digital telecommunications standard in the 900 Mhz frequency band. This standard later became known as Global System for Mobile communication (GSM).
1986	• Field test were held in Paris to select which digital transmission technology to use. The choice was Time Division Multiple Access (TDMA) or Frequency Division Multiple Access (FDMA).
1987	• A combination of TDMA and FDMA was selected as the transmission technology for GSM. • Operators from 12 countries signed a Memorandum of understanding committing themselves to introducing GSM by 1991.
1988	• CEPT began producing GSM specifications for a phased implementation. • Another five countries signed the MoU.
1889	• European Telecommunication Standards Institute (ETSI) took over responsibility for GSM specification.
1990	• Phase 1 specifications were frozen to allow manufactures to develop network equipment.
1991	• The GSM 1800 standard was released. • An addendum was added to the Mou allowing countries

	outside CEPT to sign.
1992	• Phase 1 specifications were completed. • First commercial Phase 1 GSM networks were launched. • The first international roaming agreement was established between Telecom Finland and Vodafone in UK.
1993	• Australia became the first non-European country to sign the MoU. • The MoU now had a total of 70 signatories. GSM networks were launched in Norway, Australia, Ireland, Hong Kong and Austria. • The number of GSM subscribers reached one million. • The first commercial DCS 1800 system was launched in the U.K
1994	• The MoU now had over 100 signatories covering 60 countries. • More GSM networks were launched. • The total number of GSM subscribers exceeded 3 million.
1995	• The specification for the personal communications services (PCS) was developed in the U.S.A. This version of GSM operates at 1900 Mhz. • GSM growth trends continued steadily through 1995, with the number of GSM subscribers increasing at the rate of 10,000 per day and rising. • In April 1995, there were 188 members of the MoU from 69 countries.
1996	• The first GSM 1900 systems became available. These comply with the PCS 1900 standard.

1998	• **At the beginning of 1998 the MoU has a total of 253 members in over 100 countries and there are over 70 million GSM subscribers world-wide. GSM subscribers account for 31% of the world's mobile market.**

Table 1.2: History of GSM System

1.9 Second Generation (2G) Cellular Networks:

In the 1990s, **'second generation'** (2G) mobile phone systems such as GSM, IS-136 ("TDMA"), iDEN and IS-95 ("CDMA") began to be introduced. In 1991 the first GSM network (Radiolinja) opened in Finland. 2G phone systems were characterized by digital circuit switched transmission and the introduction of advanced and fast phone-to-network signaling. In general the frequencies used by 2G systems in Europe were higher than those in America, though with some overlap. For example, the 900 MHz frequency range was used for both 1G and 2G systems in Europe, so the 1G systems were rapidly closed down to make space for the 2G systems. In America the IS-54 standard was deployed in the same band as AMPS and displaced some of the existing analog channels.

The second generation introduced a new variant to communication, as SMS text messaging became possible, initially on GSM networks and eventually on all digital networks. The first machine-generated SMS message was sent in the UK in 1991. The first person-to-person SMS text message was sent in Finland in 1993. Soon SMS became the communication method of preference for the youth. Today in many advanced markets the general public prefers sending text messages to placing voice calls.

2G also introduced the ability to access media content on mobile phones, when Radiolinja (now Elisa) in Finland introduced the downloadable ring tone as paid content. Finland was also the first country where advertising appeared on the mobile phone when a free daily news headline service on SMS text messaging was launched in 2000, sponsored by advertising. [B2]

1.10 2.5 Generation:

2.5G is a stepping stone between 2G and 3G cellular wireless technologies. The term "second and a half generation" is used to describe 2G-systems that have implemented a packet switched domain in addition to the circuit switched domain. It does not necessarily provide faster services because bundling of timeslots is used for circuit switched data services (HSCSD) as well.

2.5G provides some of the benefits of 3G (e.g. it is packet-switched) and can use some of the existing 2G infrastructure in GSM and CDMA networks. GPRS is a 2.5G technology used by GSM operators. Some protocols, such as EDGE for GSM and CDMA2000 1x-RTT for CDMA, can qualify as "3G" services (because they have a data rate of above 144 kbit/s), but are considered by most to be 2.5G services (or 2.75G which sounds even more sophisticated) because they are several times slower than "true" 3G services. [B2]

1.11 **3rd** Generation:

What is 3G? It's an International Telecommunication Union (ITU) standard for third generation mobile telephone systems under the International Mobile Telecommunications program, IMT-2000. Analog cellular was the first generation, digital PCS was the second. Along with W-CDMA, 3G was the big rage in the late 90's, with proponents announcing that it was the Killer Wireless Application because of its ability to simultaneously transfer voice data (the phone call) and other non-voice data such as music, photographs, video, email, instant messaging, and information downloads. 3G networks use a variety of wireless network technologies, including GSM, CDMA, TDMA, WCDMA, CDMA2000, UMTS and EDGE, and this leads to some confusion as well as a great deal of flexibility.

3G implementation was slower than initially anticipated, however, because of the cost of upgrading equipment and licensing fees for additional spectrum. The earlier, 2G networks didn't typically use the same frequencies as 3G (except in the United States), and licensing fees, particularly in Europe, were extremely expensive. Only Japan and South Korea were able to implement this technology quickly, largely because of the high level of government support for new infrastructure advances. In Japan, by the

end of 2006 the majority of customers was on 3G and upgrades to the next stage, 3.5G (with 3 Mbit/s data rates), was underway. Implementation in the rest of the world is coming along, but at a slightly slower pace. In December 2007, 190 3G networks were operating in 40 countries, with 200 million subscribers -- but that's still only around 7% of the 3 billion mobile phone subscriptions worldwide. [B4]

1.12 Adaptations of the GSM Standard

The GSM adaptations GSM900, GSM1800, GSM1900, GSM-R and GSM400 differ in the frequency ranges used and the resulting different technical implementations.

GSM900 (GSM, E-GSM)
Originally 2 x 25 MHz in the frequency range around 900 MHz (890 - 915; 935 - 960 MHz) were provided for mobile communication applications. In an extension of this range, called E-GSM (Extended GSM) these ranges will be increased to 2 x 35 MHz (880 - 915; 925 - 960 MHz) on a national level when further operation licenses expire.

GSM1800 (DCS1800)
As an adaptation of the GSM900 Standard the DCS1800 Standard (Digital Cellular System) was introduced in 1991. The DCS1800 was a British initiative with the intention of opening mobile communications to all sections of population as a "mass market", especially in urban areas. The GSM1800 has 2 x 75 MHz in the frequency range around 1800 MHz (1710 - 1785; 1805 - 1880 MHz). In 1997 the designation DCS1800 was changed to GSM1800 in order to clarify the common standard.

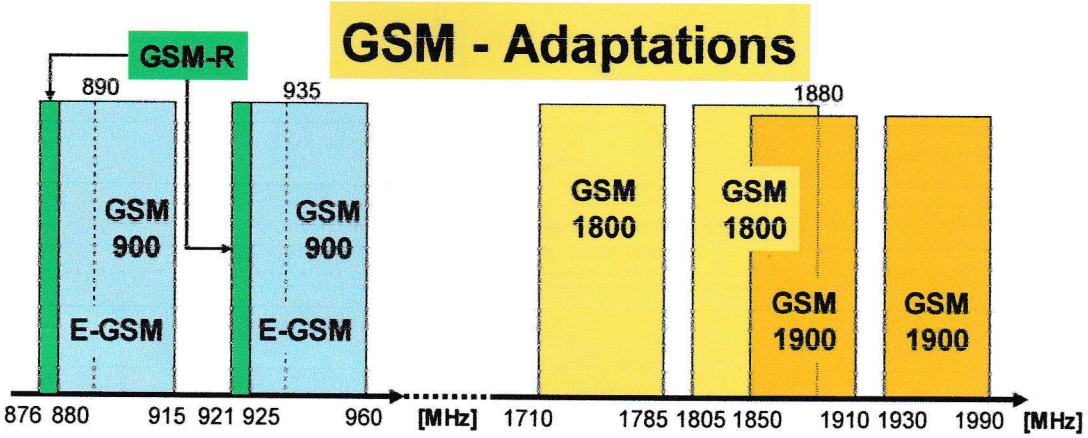
GSM1900 (PCS1900)
The PCS1900 Standard (Public Cellular System) is the American branch of the GSM Standard since 1995/96 in the frequency range around 1900 MHz. The frequency range available between 1850 - 1910; 1930 - 1990 MHz in the USA was split up in 1995 and auctioned off to different net-work operators. In 1997 the PCS1900 was renamed GSM1900 in order to clarify the common standard.

GSM-R (Railway)
For mobile communication of railway operators 2 x 4 MHz in the frequency range of

876 – 880 MHz & 921 – 925 MHz have been reserved.

GSM400

With Rel. '99 the frequency ranges between 450.4 – 457.6 MHz & 460.4 – 467.6 MHz respectively the ranges (of former 1G systems) between 478.8 – 486 MHz & 488.8 – 496 MHz are foreseen for GSM400. The GSM400 frequency range enables large area cells for rural environment. [B2]



	Frequency Range [MHZ]	Useable HF channels	Application Area
GSM400	450.4 – 457.6 / 460.4 – 467.6 478.8 – 486 / 488.8 - 496	35	rural environment
GSM900 E-GSM	890 - 915 / 935 - 960 880 - 915 / 925 - 960	124 174	Worldwide except America
GSM1800	1710 - 1785 / 1805 - 1880	374	Worldwide except America
GSM1900	1850 - 1910 /1930 - 1990	299	America
GSM-R	876 - 880 / 921 - 925	19	Railway systems

Fig. 15 (TM2100EU03TM_0001 Introduction, 31)

Fig 1.1: GSM Adaptations

CHAPTER 2
GSM ARCHITECTURE
GSM-PLMN

2.1 Overview:

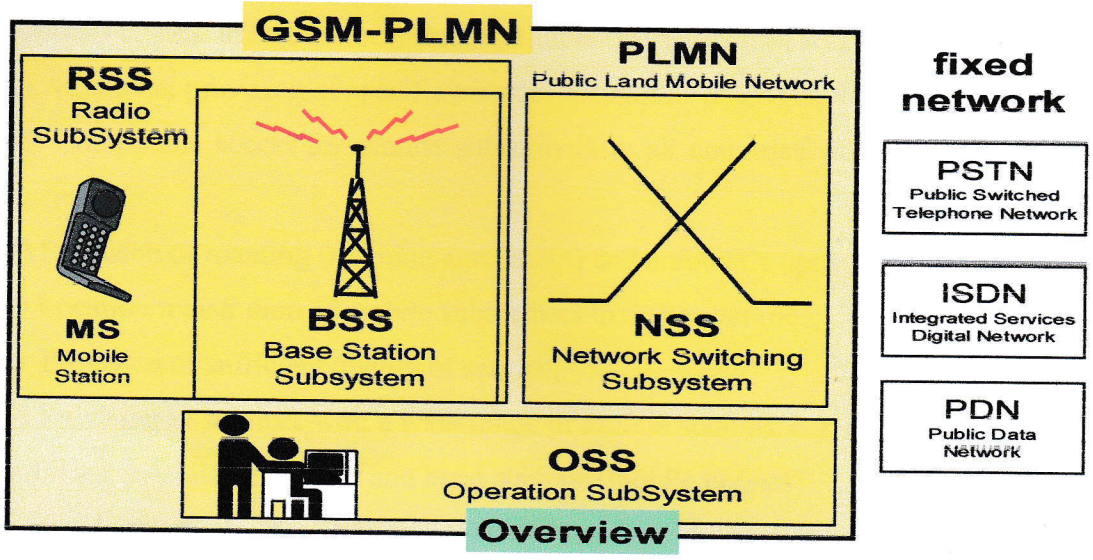


Fig 2.1: GSM PLMN: Subsystems

2.1.1 The GSM-PLMN

In the GSM System there must be a distinction between network operators, provider of Telecommunication services, supplier of terminal equipment and manufacturer of network components. Especially the sale of telecommunication services and terminal equipment differs from the conventional fixed network and mobile communication network of the first generation, in which state-owned network operators, service providers and equipment suppliers usually form a monopoly. In GSM the actual network operator often transfers services to private providers who supply the services to the mobile subscribers under different conditions. With the wide range of products there is also great competition in the field of mobile equipment as well as of mobile communication network components which should force further technical development and keep the prices down. [B2]

PLMN - Public Land Mobile Network

A PLMN is a terrestrial mobile communication network set up and run by public and private operators. It is used to provide public mobile communication services.

General Objectives of a GSM-PLMN (with respect to service aspects):

a) Provision of a wide range of speech and non-speech services and Compatibility to those services offered in fixed telecommunication networks such as PSTN, ISDN and PDN;

b) Additional provision of specific services for mobile access environment;

c) Compatible access for mobile subscribers in all countries where the GSM System is operated;

d) Provision of roaming (roaming agreement) and automatic updating;

e) Location registration of mobile subscribers in these countries;

f) Provision of sufficient quality of service;

g) Provision of services with a wide range of mobile stations, e.g. permanently in-stalled in vehicles, so-called portables and hand stations (mobile phones).

General Objectives of a GSM-PLMN (with respect to performance aspects):

a) Guarantee of a high spectrum efficiency;

b) Provision of a system concept which will lead to attractive costs regarding infra-structure and mobile equipment [B2]

A GSM-PLMN is subdivided into the following subsystems:

- Radio Subsystem RSS
- Network Switching Subsystem NSS
- Operation Subsystem OSS

2.1.2 Network Elements

The subsystems functions are grouped into functional units or network elements.

Functional units may be realized either as standalone Hardware HW units or associated with other GSM functional units in one HW unit.

The Radio Subsystem RSS consists of the Mobile Stations MS and the Base

Station Subsystem BSS, which is composed of the following functional units:

- Base Station Controller BSC

- Base Transceiver Station BTS
- Transcoding and Rate Adaption Unit TRAU

The Network Switching Subsystem NSS (Phase) consists of the following functional units:

- Mobile services Switching Center MSC
- Visitor Location Register VLR
- Home Location Register HLR
- Authentication Center AC
- Equipment Identity Register EIR.

The Operation Sub-System OSS consists of Operation & Maintenance Centers OMC; in the Siemens solution:

- Operation & Maintenance Center for the Base Station Subsystem OMC-B
- Operation & Maintenance Center for the Switching Subsystem OMC-S.

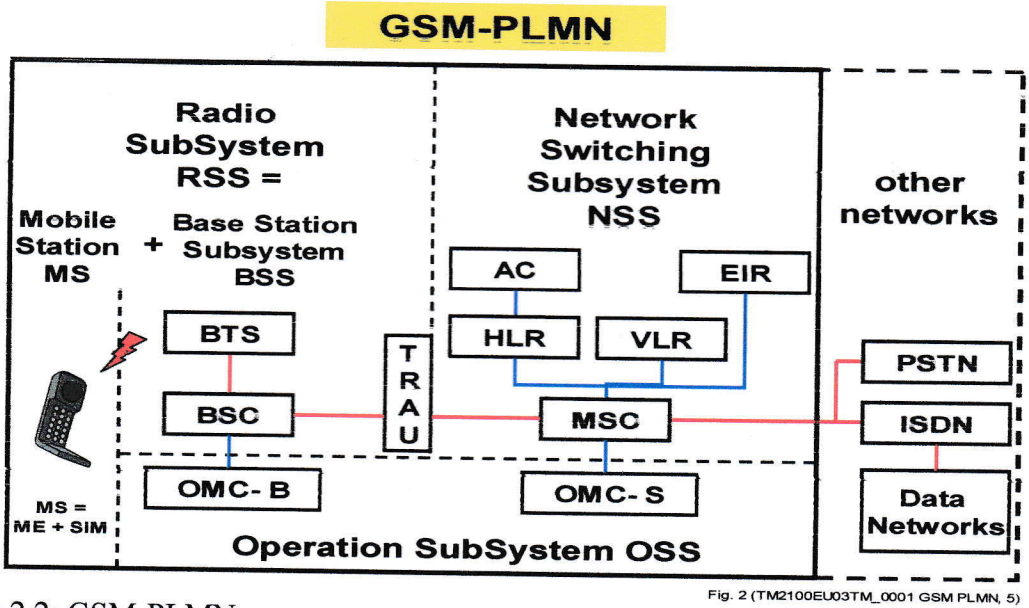


Fig 2.2: GSM-PLMN

2.1.3 Interfaces

The individual network elements are connected to each other for user data and/or signaling transfer. Some of the interfaces are specified by ETSI as open interfaces, allowing connecting equipment of different network manufacturer. Others are not specified or "weakly" specified, so that only proprietary solutions are possible. The following GSM Phase 1/2 interfaces are open interfaces:

Um: MS - BSS (Air interface)

- A: MSC - BSS (BSC)
- B: MSC - VLR
- C: MSC - HLR
- D: HLR – VLR
- E: MSC - MSC
- F: MSC - EIR
- G: VLR - VLR.

The following interfaces are proprietary solutions:
Asub: BSC - TRAU

- Abis: BSC - BTS
- T: BSC, BTS, TRAU - Local Maintenance Terminal LMT
- O: BSC - OMC-B
- HLR - AC (no name) [B2]

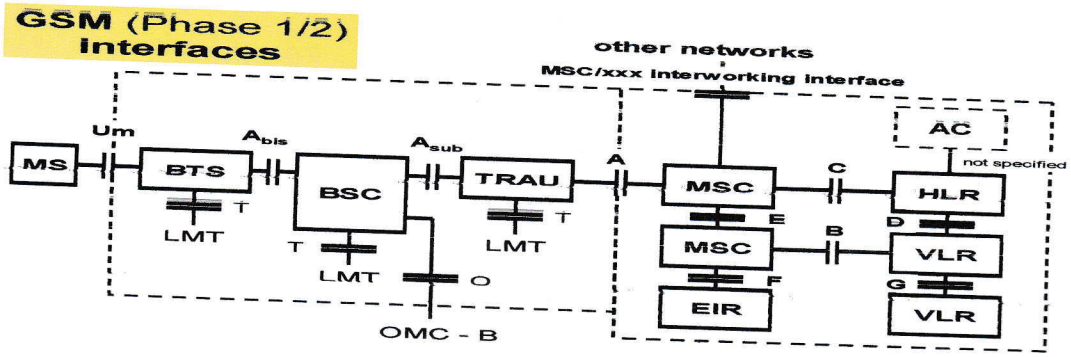


Fig 2.3: GSM Interfaces

Fig. 3 (TM2100EU03TM_0001 GSM PLMN, 7)

2.2 Network Elements:

2.2.1 The Mobile Station MS

The Mobile Stations represent the mobile network components. They consist of the Mobile Equipment ME and the Subscriber Identity Module SIM: MS = ME + SIM

2.2.2 The SIM card

The SIM consists of a microchip, which uses either a check card or a plate made of a synthetic material as a carrier. Without a SIM card, the use of an MS is normally not possible. An exception is the emergency call, which should always be possible with a functioning ME. The SIM card carries the subscriber-related information and codes, so that a GSM subscriber with a SIM card can use different ME. The main task of the SIM is the storage of data: permanent and temporary administrative data as well as data concerning security. Personal telephone lists may be stored and using the SIM toolkit with enhanced memory space, it is possible to enable applications such as
Mobile Banking, etc. [B2]
Important stored codes are e.g.:

- Personal Identity Number - PIN
- PIN Unblocking Key - PUK
- Mobile Station ISDN number - MSISDN
- International Mobile Subscriber Identity - IMSI
- Temporary Mobile Subscriber Identity - TMSI

Important data relating to security are, e.g.:

- the individual key - Ki
- the cipher key - Kc
- the algorithms for authorization and ciphering (A3, A8)

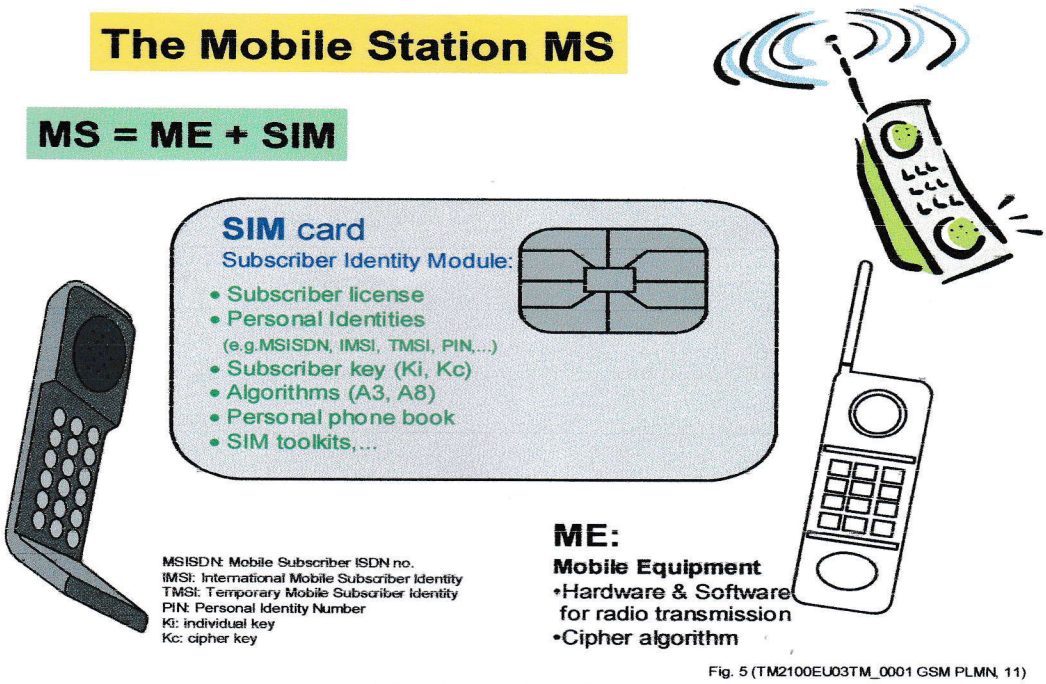


Fig 2.4: Mobile Station

2.2.3 The Mobile Equipment ME

The Mobile Equipment ME unites the tasks of many functional elements of the GSM-PLMN network.

By using the data of the SIM card, the speech is digitalized, compressed, secured against loss of data (redundancy + interleaving), encrypted to prevent interception and modulated onto the Radio Frequency (RF) created by the mobile station. Directly after, the signal is amplified and transmitted. In the opposite direction, the process runs inversely, beginning with the reception of the radio frequency (RF). The MS represents the counterpart to BSC, MSC, HLR, VLR and EIR as regards signaling. As a whole, ME and SIM cards are almost a complete GSM system as regards their functionality. [B2]

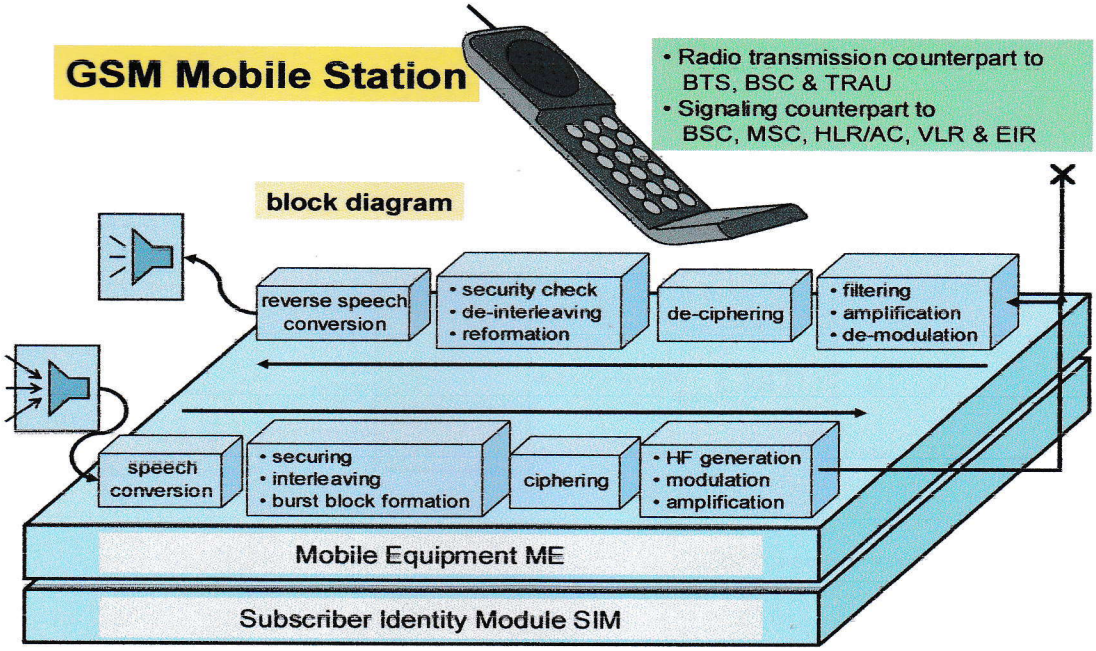


Fig 2.5: GSM Mobile station

2.2.4 The Base Station Subsystem BSS

The BSS consists of the following network elements:

1. BSC: Base Station Controller
2. BTS: Base Transceiver Station
3. TRAU: Transcoding and Rate Adaption Unit
4. LMT: Local Maintenance Terminal

The BSS architecture shall be selected to achieve maximum flexibility with regards to the various operator requirements. All BSS components can be installed in the same geographical location or in different locations where the transmission paths can be used via public networks. The ability of the BSC to manage several BTSs in different cell locations enables optimal adaptability to the traffic requirements in urban and rural areas. In terms of function, the main task of the BSC is the handling of the call connections (switching), sampling of operational/maintenance information of all BSS (BSC, BTSs and TRAUs), as well as their transfer to OMC-B. The BTS handles the radio specific aspects. [B2]

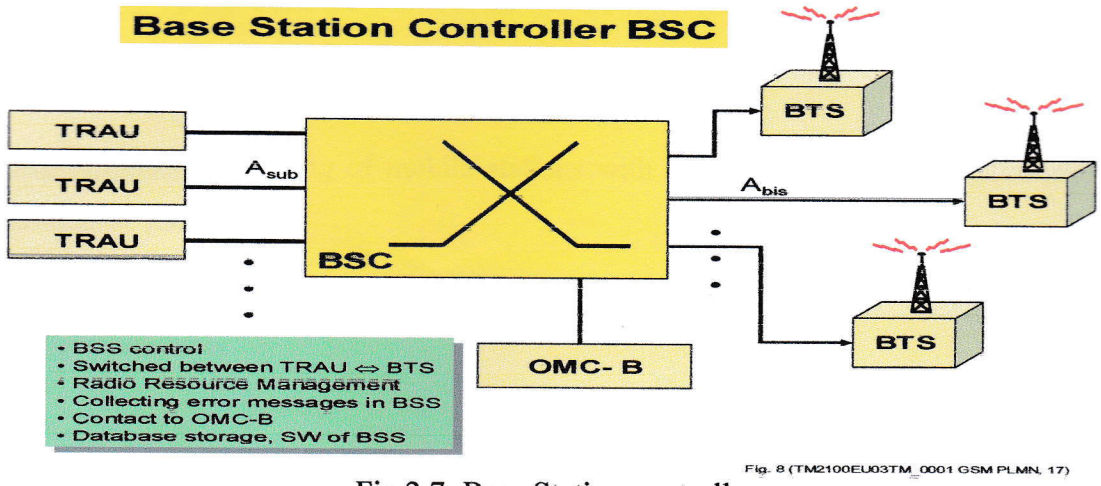


Fig 2.7: Base Station controller

2.2.4.2 Base Transceiver Station BTS

A BTS is the module which operates an individual cell and realizes the radio interface. A BTS encompasses all applications concerning radio transmission (sending, receiving), as well as the air interface specific signal processing. The BTS is connected via the Abis interface with the BSC and via Um interface to the MSs.

Functions:

Channel coding: To protect the transmission, incoming information is provided with parity check bits and redundancy (convolutional coding) and spread in time over several HF bursts (interleaving).

Ciphering: After channel coding, the transmission of message information and the subscriber data is coded to prevent illegal interception.

Burst block formation: The information is organized in blocks of a particular length (burst blocks). A so-called training sequence is added for synchronization and analysis of transmission quality.

Modulation: The carrier frequency is created in the 900/1800/1900 MHz range and the information is modulated upon this carrier.

Power Control PC: Control of the power level of the BTS and MS.

Timing Advance TA: Calculation of the distance of the MSs from the BTS; the MSs are informed of necessary transmission advance.

Frequency Hopping: a feature which enhances the reliability of information transfer

Synchronization: Providing of mobile stations with frequency and time synchronization information. [B2]

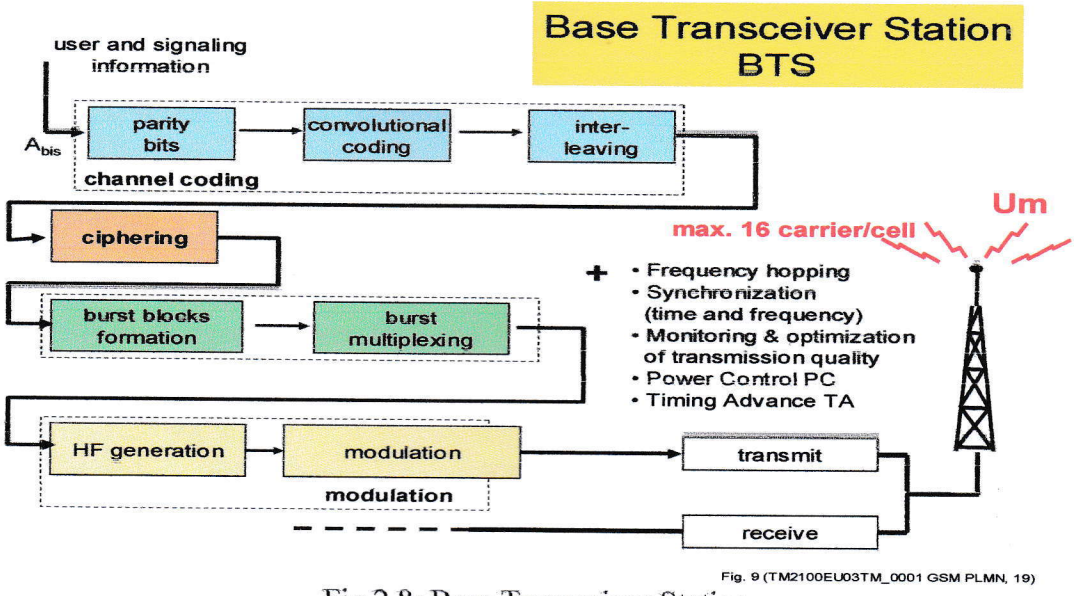


Fig 2.8: Base Transceiver Station

2.2.4.3 Transcoding and Rate Adaptation Unit TRAU

The TRAU is used for speech compression (Transcoding) and adaptation of data to the requirements of the air interface (Rate Adaptation). It lies between A and Asub interface.

Functions:

- Transcoding TC defines speech compression: compresses / decompresses the incoming speech data from 64 kbit/s to 13 kbit/s, 12.2 or 5.6 kbit/s (embedded in 16 or 8 kbit/s channels).

- Rate Adaptation RA filters out the useful data (0.3 – 9.6 kbit/s in Phase 1/2) coming from the MSC (64 kbit/s) signal and forms a 16 kbit/s signal toward the BSC

- The user data are sub-multiplexed into 16 kbit/s subslots on the Asub interface

Remarks:

- TC and RA are implemented as algorithms in the same hardware unit as the TRAU

(Siemens solution).

- The TRAU is logically allocated to the BSC. Consequently, it belongs to the Base Station Subsystem (BSS), but is generally installed at the MSC node in order to keep line costs to a minimum.

- In contrast to user information signaling information passes the TRAU transparently.
- The users information (data / speech) is embedded into 16 kbit/s channels. The additional space is filled with proprietary inband-signaling (i.e. information, which are directly exchanged between BTS and TRAU) [B2]

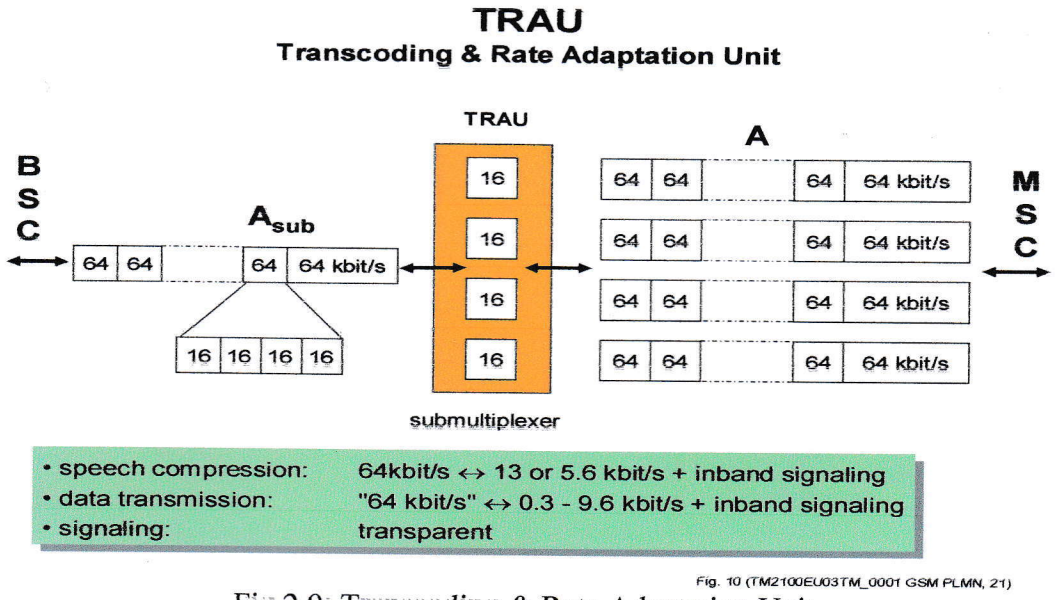


Fig 2.9: Transcoding & Rate Adaptation Unit

2.3 The Network Switching Subsystem NSS

The NSS comprises the following functional elements:

- MSC: Mobile services Switching Center
- VLR: Visitor Location Register
- HLR: Home Location Register
- AC: Authentication Center

- EIR: Equipment Identity Register

2.3.1 Mobile Switching Center MSC

The MSC is concerned with the central tasks of the NSS and covers the service areas of several BSSs. These tasks can be compared to those of an exchange in a fixed network. These tasks are supplemented by mobile specific tasks of the sub-scriber administration. The MSC handles connection tasks in the PLMN, i.e. set-up of circuit connections to the BSS, between each other and other networks (e.g. PSTN).

The MSC visited by a customer is described as a VMSC (Visited MSC). A MSC, which represents an interface to other networks, is called GMSC (Gateway MSC). MSCs connect the other networks with the Base Station Subsystem BSS, as well as the other NSS units with the BSS via the signaling highways. The MSC is a stored program controlled switching system for national and international GSM-PLMN applications. The MSC is a switching center that carries out all switching for the mobile stations which are actually located in the MSC area. Other functional units of the NSS (e.g. HLR, VLR, AC) can be associated to the MSC. [B2]

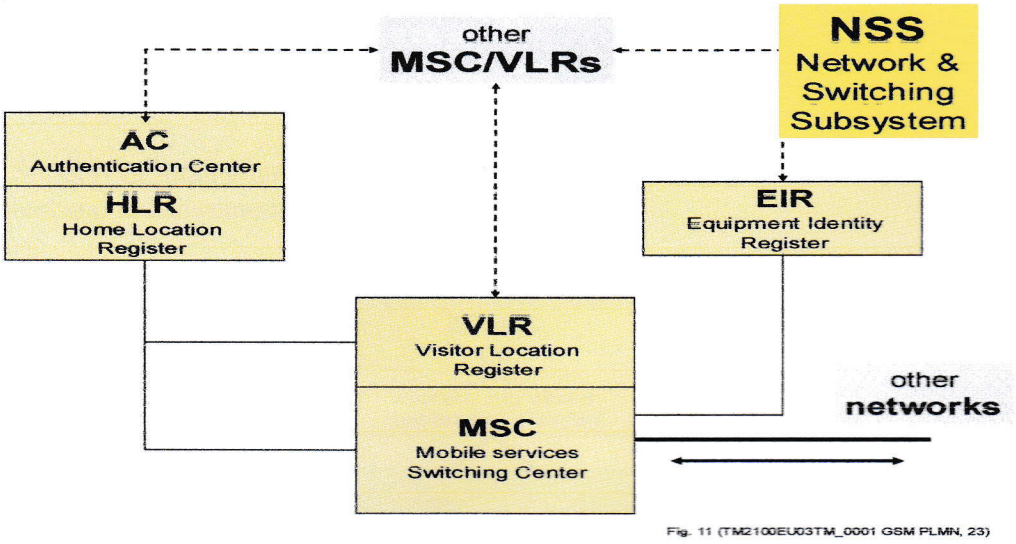


Fig 2.10: MSC/VLR

Overview of call processing functions

The MSC follows the functions of a fixed network exchange as regards its functionality. Consequently, varied proven call handling functions form the basis for mobile specific

supplementary services.

- Switching of user connections
- Routing functionality (path selection)
- Signaling with other MSCs and external network exchanges
- Evaluation of available signaling information for destination routing:
- Digit translation
- Legal interception
- Coping with abnormal signaling conditions, e.g. loss of signaling information
- Supplementary Service support
- Processing of transmission path attributes, e.g. echo compensation
- Call supervision
- Overload protection
- Control of priority calls, e.g. emergency call
- Charging
- Traffic measurement and traffic observation
- Support of maintenance and administration functions, e.g. connection cut off, trunk test and measurement [B2]

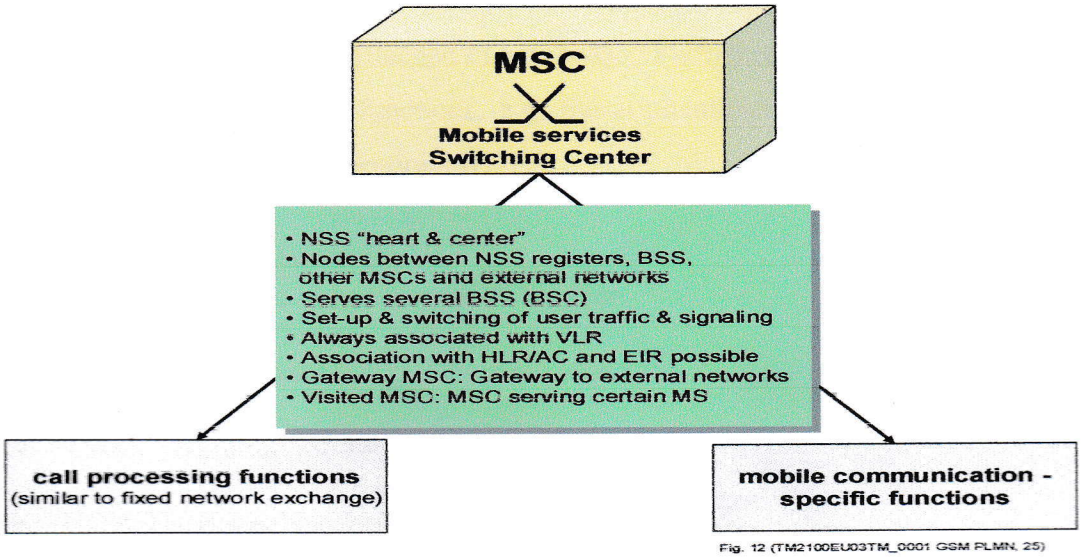


Fig 2.11: Mobile switching center

Mobile specific functions

Additional to normal fixed network exchanges, the MSC has many mobile specific functions due to the users mobility.

Mobile specific functions are for example:

- Signaling with BSC, MS & NSS databases (EIR, HLR, VLR)
- Processing of mobile-specific services
- Mobility Management, e.g. Paging, Inter-MSC Handover, Location Update.
- Overload handling, e.g. OACSU
- Interworking Function for data services
- Mobile specific Announcements

2.3.2 Visitor Location Register VLR

The Visitor Location Register VLR is responsible to aid the MSC with information on the subscriber, which are temporarily in the MSC service area. Therefore, in praxis it is always associated with an MSC. The VLR request the subscriber data of user with activated MS on the MSC service area from the HLR and stores them temporarily. Temporarily means as long as the subscriber is not registered in a new MSC/VLR, even if he deactivated the MS. Additional to the semi-permanent subscriber data received from the HLR the VLR stores temporary data, e.g. information on the subscribers current location (the Location Area), the state of activation (Attached / Detached),... Furthermore, the VLR is responsible for the initiation of security functions, e.g. the Authentication procedure, the start of ciphering and the TMSI re-allocation. [B2]

Examples of subscriber data in the VLR:

- MSISDN: Mobile Subscriber ISDN number
- IMSI: International Mobile Subscriber Identity
- TMSI: Temporary Mobile Subscriber Identity
- HON: Handover Number

- LMSI: Local Mobile Subscriber Identity
- MSRN: Mobile Station Roaming Number
- Triples (Authorization parameters)

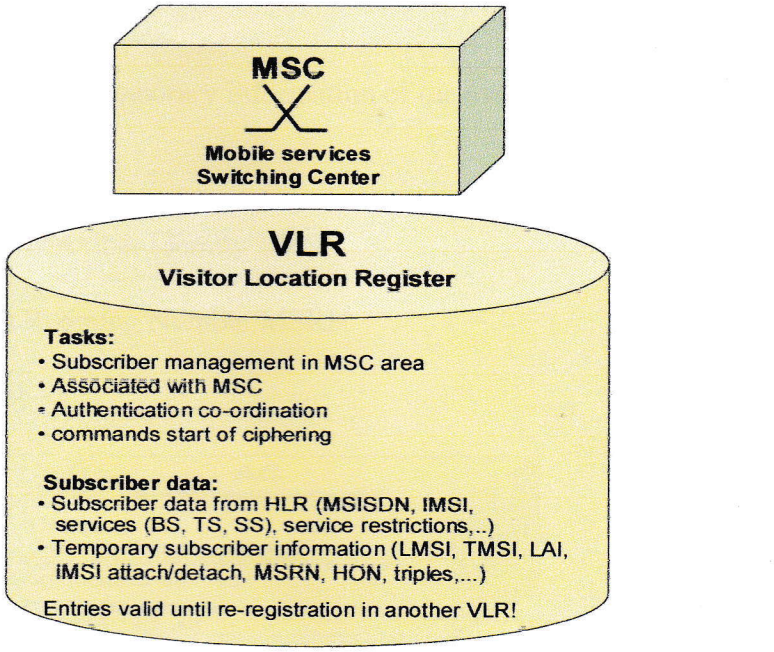


Fig 2.12: Visitor Location Register

2.3.3 Home Location Register HLR

The Home Location Register HLR is the main data base of the mobile subscriber. The subscription of a user / his subscription data is stored in one HLR only. There may be one or more HLRs in a GSM PLMN.

The HLR is always associated with an Authentication Center AC.

The HLR performs the following important tasks:

- It sends all necessary data to the VLR.
- It supports the call setup in case of Mobile Terminating Calls MTC by sending routing information to the Gateway MSC (Interrogation).
- It transmits the Triples from AC to VLR on request

An HLR contains different semi-permanent mobile subscriber data, e.g:
IMSI: International Mobile Subscriber Identity

- MSISDN: Mobile Station International ISDN number

- Bearer Services BS
- Tele Services TS
- Supplementary Services SS
- Restrictions

An HLR contains different temporary information of the mobile subscriber, e.g.:

- VLR address
- Local Mobile Subscriber Identity LMSI
- Mobile Station Roaming Number MSRN
- SMS flags [B2]

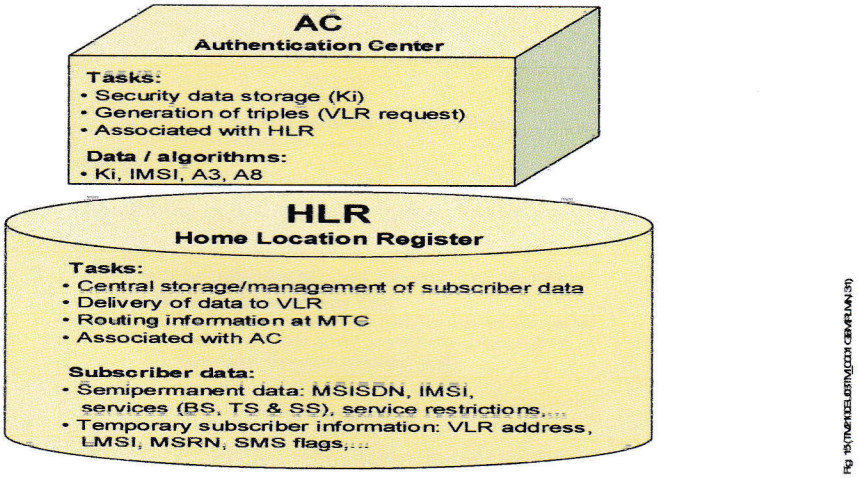


Fig 2.13: Home Location Register

2.3.4 Authentication Center AC

An Authentication Center AC contains all necessary means, keys and algorithms for the creation of security related authorization parameters, the so-called Triples. The Triples are created on VLR request and delivered via HLR to the VLR. An AC is always associated with an HLR.

Central information contained in the AC are:

- IMSI: International Mobile Subscriber Identity
- Ki: Individual Key (top secret mobile subscriber identity)
- Algorithms for authentication and encryption: A3, A8.

2.3.5 Equipment Identity Register EIR

The Equipment Identity Register EIR contains the Mobile Equipment identity: the International Mobile Equipment Identity IMEI. An IMEI clearly identifies a unique Mobile Equipment ME and contains information about the place of manufacture, device type and the serial number of the equipment. EIR are an optional feature in GSM. They have been defined by ETSI to enable theft prophylaxis. They carry out equipment identification functions: monitoring of stolen or

not allowed MEs. There are three validity lists in EIRs: "white", "gray" and "black" lists for valid, to be observed and to be blocked equipment. A Common EIR (CEIR) in Dublin (Ireland) enables the world-wide identification of stolen mobile equipment.

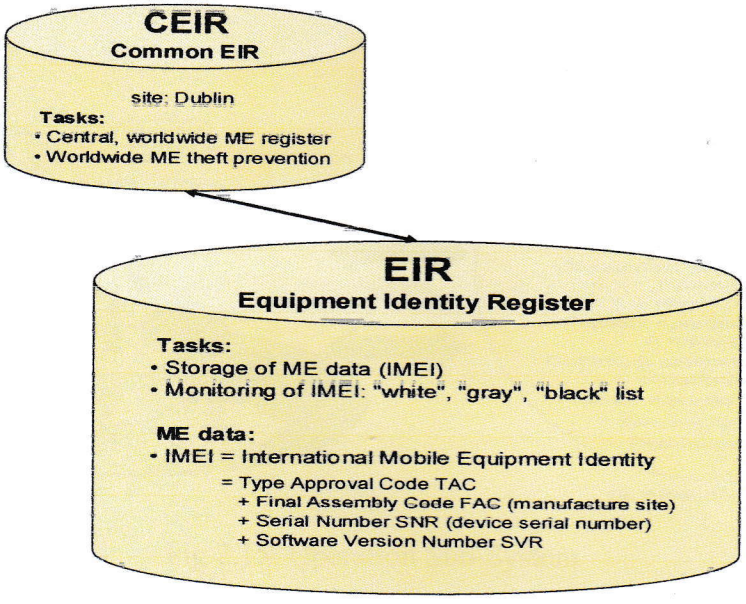


Fig. 18 (TME10EL03TM_0001 GSM PLMN 33)

Fig 2.14: Equipment Identity Register

2.4 Operation SubSystem OSS

The Operation SubSystem OSS undertakes operation and maintenance tasks. The functions of the network/ network elements may be centrally monitored and (remote) controlled by the OSS. The control/operation & maintenance locally at each Network Element NE (hardware implementation of functional elements) as local operation and maintenance is distinguished by the central, remote-controlled functionality of the OSS.

The functions of the OSS are performed by so-called Operation & Maintenance Centers OMC. Depending on the manufacturer, there is sometimes spatial separation between the operation & maintenance of BSS and NSS (Siemens: OMC-B and OMC-S).

Important functions of the OSS:

- Management and commercial operation (subscriber, mobile equipment, billing)

- Sampling of information on network loads (statistical survey) for network reorganization / optimization
- Security management
- Network configuration
- Remote operation of network elements
- Quality checks
- Preparation of maintenance work [B2]

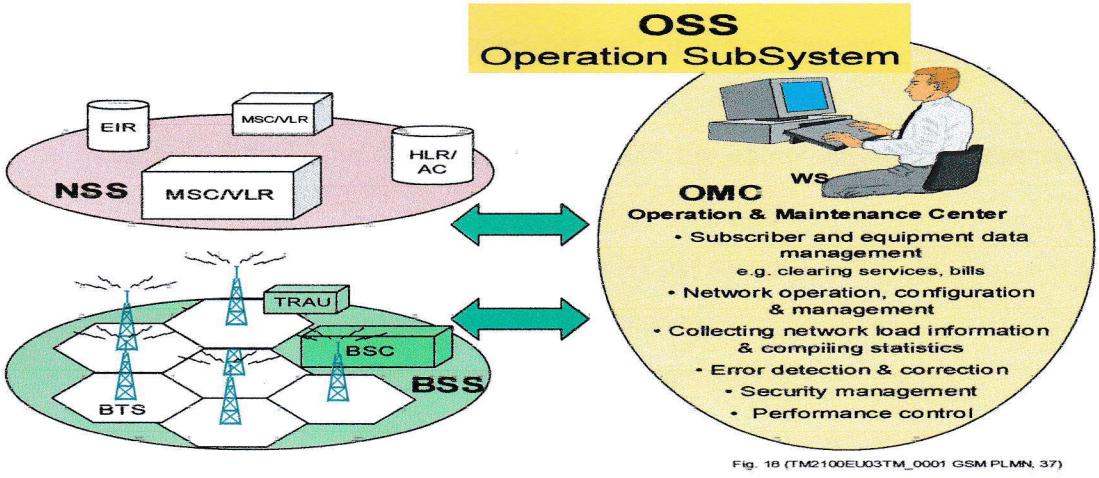


Fig 2.15: Operation Sub-System

CHAPTER 3

SPECIFICATIONS, PROCEDURES & SECURITY OF GSM NETWORK

3.1 GSM Specifications

Before looking at the GSM specifications, it is important to understand the following basic terms:

- bandwidth—the range of a channel's limits; the broader the bandwidth, the faster data can be sent
- bits per second (bps)—a single on-off pulse of data; eight bits are equivalent to one byte
- frequency—the number of cycles per unit of time; frequency is measured in hertz (Hz)
- kilo (k)—kilo is the designation for 1,000; the abbreviation kbps represents 1,000 bits per second
- megahertz (MHz)—1,000,000 hertz (cycles per second)
- milliseconds (ms)—one-thousandth of a second
- watt (W)—a measure of power of a transmitter [B2]

Specifications for different personal communication services (PCS) systems vary among the different PCS networks. Listed below is a description of the specifications and characteristics for GSM.

- frequency band—The frequency range specified for GSM is 1,850 to 1,990 MHz (mobile station to base station).
- duplex distance—The duplex distance is 80 MHz. Duplex distance is the distance between the uplink and downlink frequencies. A channel has two frequencies, 80 MHz apart.
- channel separation—The separation between adjacent carrier frequencies. In GSM, this is 200 kHz.
- modulation—Modulation is the process of sending a signal by changing the characteristics of a carrier frequency. This is done in GSM via Gaussian minimum shift keying (GMSK).

- transmission rate—GSM is a digital system with an over-the-air bit rate of 270 kbps.
- access method—GSM utilizes the time division multiple access (TDMA) concept. TDMA is a technique in which several different calls may share the same carrier. Each call is assigned a particular time slot.
- speech coder—GSM uses linear predictive coding (LPC). The purpose of LPC is to reduce the bit rate. The LPC provides parameters for a filter that mimics the vocal tract. The signal passes through this filter, leaving behind a residual signal. Speech is encoded at 13 kbps. [B2]

3.1.1 GSM Subscriber Services

There are two basic types of services offered through GSM: telephony (also referred to as teleservices) and data (also referred to as bearer services). Telephony services are mainly voice services that provide subscribers with the complete capability (including necessary terminal equipment) to communicate with other subscribers. Data services provide the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network. In addition to normal telephony and emergency calling, the following subscriber services are supported by GSM:

- dual-tone multifrequency (DTMF)—DTMF is a tone signaling scheme often used for various control purposes via the telephone network, such as remote control of an answering machine. GSM supports full-originating DTMF.
- short message services—A convenient facility of the GSM network is the short message service. A message consisting of a maximum of 160 alphanumeric characters can be sent to or from a mobile station. This service can be viewed as an advanced form of alphanumeric paging with a number of advantages. If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has reentered the coverage area of the network. This function ensures that the message will be received.
- cell broadcast—A variation of the short message service is the cell broadcast facility. A message of a maximum of 93 characters can be broadcast to all

mobile subscribers in a certain geographic area. Typical applications include traffic congestion warnings and reports on accidents.

- voice mail—This service is actually an answering machine within the network, which is controlled by the subscriber. Calls can be forwarded to the subscriber's voice-mail box and the subscriber checks for messages via a personal security code.
- fax mail—With this service, the subscriber can receive fax messages at any fax machine. The messages are stored in a service center from which they can be retrieved by the subscriber via a personal security code to the desired fax number. [B2]

GSM supports a comprehensive set of supplementary services that can complement and support both telephony and data services. Supplementary services are defined by GSM and are characterized as revenue-generating features. A partial listing of supplementary services follows.

- call forwarding—This service gives the subscriber the ability to forward incoming calls to another number if the called mobile unit is not reachable, if it is busy, if there is no reply, or if call forwarding is allowed unconditionally.
- barring of outgoing calls—This service makes it possible for a mobile subscriber to prevent all outgoing calls.
- barring of incoming calls—This function allows the subscriber to prevent incoming calls. The following two conditions for incoming call barring exist: baring of all incoming calls and barring of incoming calls when roaming outside the home PLMN.
- advice of charge (AoC)—The AoC service provides the mobile subscriber with an estimate of the call charges. There are two types of AoC information: one that provides the subscriber with an estimate of the bill and one that can be used for immediate charging purposes. AoC for data calls is provided on the basis of time measurements.
- call hold—This service enables the subscriber to interrupt an ongoing call and then subsequently reestablish the call. The call hold service is only applicable to normal telephony.

- call waiting—This service enables the mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call. Call waiting is applicable to all GSM telecommunications services using a circuit-switched connection.
- multiparty service—The multiparty service enables a mobile subscriber to establish a multiparty conversation—that is, a simultaneous conversation between three and six subscribers. This service is only applicable to normal telephony.
- calling line identification presentation/restriction—These services supply the called party with the integrated services digital network (ISDN) number of the calling party. The restriction service enables the calling party to restrict the presentation. The restriction overrides the presentation.
- closed user groups (CUGs)—CUGs are generally comparable to a PBX. They are a group of subscribers who are capable of only calling themselves and certain numbers. [B2]

3.2 Codes & Identities

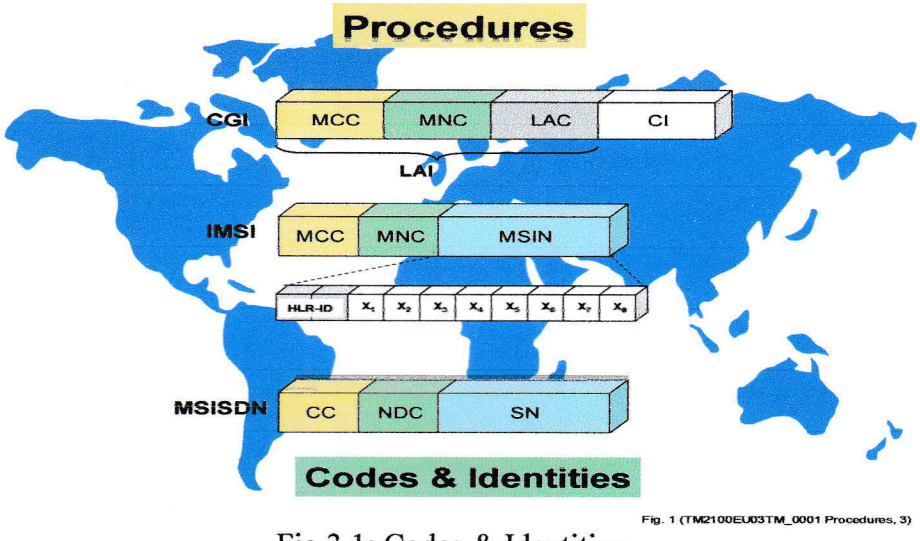


Fig 3.1: Codes & Identities

3.2.1 GSM Service Areas & Codes

The GSM system is hierarchically ordered into service areas. To identify and address a certain service areas codes are used.

3.2.1.1 International GSM Service Area

The international GSM service area is the sum of areas being served by GSM networks. A GSM subscriber may use all these GSM networks if his HPLMN has Roaming Agreements with the VPLMN and his ME supports the corresponding frequency range (GSM900 / GSM1800 / GSM1900).

3.2.1.2 National GSM Service Area

A national GSM service area contains one or more GSM-PLMN. The PLMN of different operators may supplement one another or overlap each other. The following codes are important to identify a national GSM service area:

Mobile Country Code MCC: The MCC consists of 3 digits; it is used e.g. for the International Mobile Subscriber Identity IMSI ,Location Area Identity LAI and Cell Global Identity CGI.

Country Code CC: The CC is the dialing code of the country in which the mobile subscriber is registered. The CC consists of 2 or 3 digits and is used e.g. in the Mobile Subscriber International ISDN number. [B2]

3.2.1.3 PLMN Service Area

A PLMN service area is administered by an operator. Several PLMN service areas can overlap within a country. Thus the individual PLMNs must have a clear identification:

- Mobile Network Code MNC: The MNC is the mobile specific PLMN identification; it consists of 2 digits. The MNC is used in IMSI, LAI, CGI.
- National Destination Code NDC: NDCs identify the dialing code of a PLMN; it consist of 3 digits. The NDC is used in MSISDN.
- Network Color Code NCC: The NCC is a PLMN discrimination code that is not unambiguous. It is used as short identity (length: 3 bits) of a particular PLMN in overlapping PLMN areas or in border regions; it is used e.g. in the Base Station Identity Code BSIC.

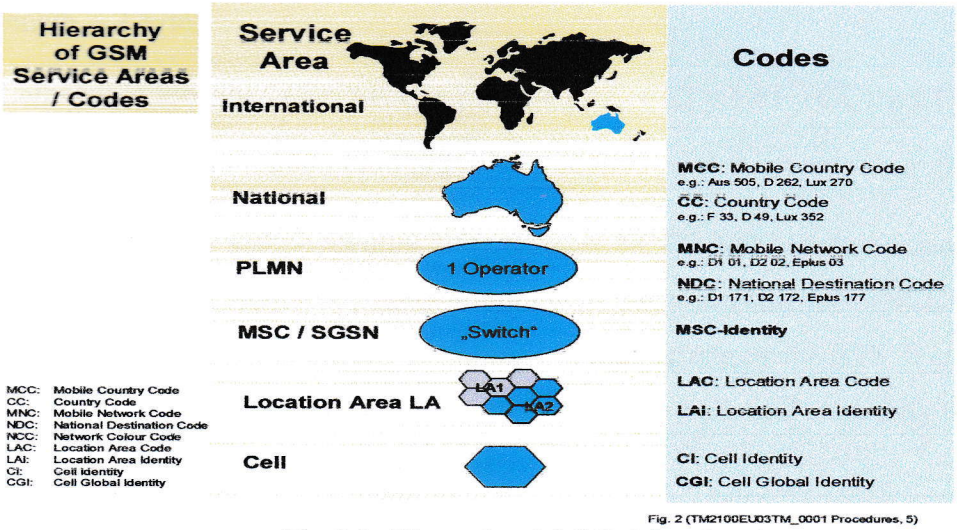


Fig 3.2: Hierarchy Of GSM Service Area

3.2.1.4 MSC/VLR Service Area

GSM-PLMN are subdivided into one or more MSC/VLR service areas. An attached mobile subscriber is registered in the VLR, which is associated to his Visited MSC. The MSC/VLR Id. is stored in the HLR, so that an MTC is possible.

3.2.1.5 Location Area LA

The LA is (in classical GSM) is stored as the most precise information of the (attached) subscribers current location. This information is stored in the VLR associated to the VMSC. If the MS turns from one LA to another, a Location Update Procedure is necessary. The size of a LA is configured by the operator according to the traffic or population density and the behavior of the mobile subscriber. A Location Area can encompass one or more radio cells that are controlled by one or more BSC, but never belong to different MSC areas. Location Area identities are:

- Location Area Code LAC: The LAC serves to identify a LA within a GSM-PLMN. The LAC length is 2 bytes.
- Location Area Identity LAI = MCC + MNC + LAC; the LAI serves as an unambiguous international identification of a location area. [B2]

3.2.1.6 BTS Service Area: the Cell

The cell is the smallest unit in the GSM-PLMN. A defined quality of the received signal must be guaranteed within a cell. If a MS leaves the range of a cell during a connection, a handover to the next cell is initiated. Cell identifications are:

Cell Identity CI: The CI allows identification of a cell within a location area. The CI

length is 2 bytes.

Cell Global Identity CGI = MCC + MNC + LAC + CI = LAI + CI; the CGI represents an international unambiguous identification of a cell.

Base Transceiver Station Identity Code BSIC = NCC + BCC (Base Station Color Code); The BSIC represents a non-unambiguous short identification (NCC: 3 bit; BCC: 3 bit) of a cell. The BSIC is emitted at a regular rate by the BTS. It enables the MS to differentiate between different surrounding cells and to identify the requested cell in a random access. [B2]

3.2.1.7 Subscriber Identities:

- International Mobile Subscriber Identity IMSI = MCC + MNC + MSIN (Mobile Subscriber Identification Number); IMSI length = 3 + 2 + 10 digits. The IMSI is the unique identity of a GSM subscriber. It is used for signaling and normally not known to the subscriber. Often die first two MSIN digits are taken to specify the users HLR in the PLMN (operator dependent).

- Mobile Subscriber ISDN number MSISDN = CC + NDC + SN. MSISDN length: 2 / 3 + 3 + max. 7 digits = max. 12 digits. The MSISDN is "the users telephone number". A user has one IMSI (with one contract), but he can have different MSISDN (e.g. for fax, phone,..).
- Temporary Mobile Subscriber Identity TMSI: The TMSI is generated by the VLR and temporarily allocated to one MS. It is only valid in this MSC/VLR service. When changing to a new MSC area, a new TMSI has to be allocated. The TMSI consists of a TMSI Code TIC with length 4 bytes. Often the TMSI is used together with the LAI. [B2]

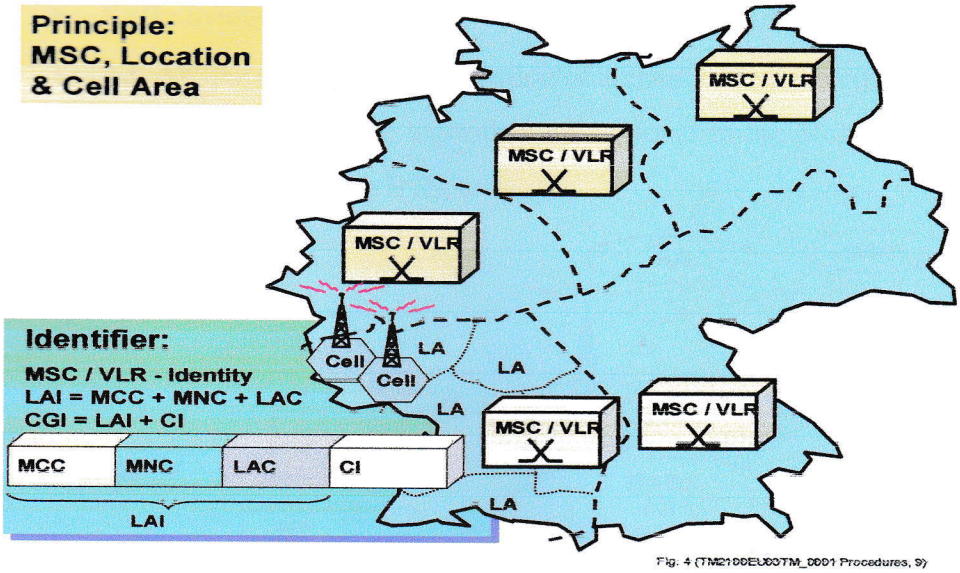


Fig 3.3: Principle of MSC, Location & Cell Area

GSM SECURITY FEATURES

3.3 Security Features:

In GSM the security of a mobile subscriber is ensured by several features.

- Authentication: protects the network operator and mobile subscriber against unauthorized network use.
- Ciphering: is used to prevent eavesdropping of radio communications.
- Temporary Mobile Subscriber Identity TMSI allocation: protects the subscriber's identity in the initial access phase, where no ciphering is possible.
- IMEI check: prevents the usage of stolen/non-authorized mobile equipment. [B2]

Security aspects are described in the GSM Recommendations:

- 02.09: "Security Aspects"
- 02.17: "Subscriber Identity Modules"
- 03.20: "Security Related Network Functions"
- 03.21: "Security Related Algorithm"

Prerequisites for Authentication and Ciphering

For authentication and ciphering, the Authentication Center AC and the SIM card are important; they store the following data:

- IMSI (International Mobile Subscriber Identity)

- Ki (Individual Key)
- A3, A8: Algorithms for the creation of authentication and ciphering parameters

Furthermore, for ciphering the algorithm A5 is stored in the Mobile Equipment. This algorithm can be found in the BTS, too.

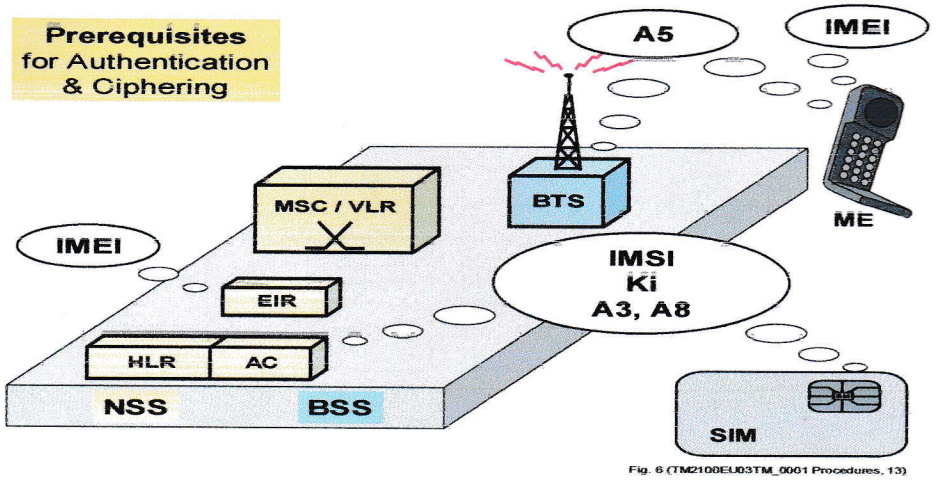


Fig 3.4: Prerequisites for Authentication & ciphering

3.3.1 Triples:

The triples are parameters, which are necessary for authentication and ciphering. They are produced in the Authentication Center AC and consist of:

- RAND (RANDom number)
- SRES (Signed RESponse): the reference value for the authentication
- Kc (Cipher Key): key necessary for ciphering.

The calculation of a triple in the AC occurs in the following manner:

- For the subscriber with a particular IMSI the reference value of authentication SRES is calculated by the algorithm A3 from the users individual key Ki and the random number RAND produced by a random number generator.
- The cipher key Kc is calculated by the algorithm A8 from the individual key Ki and the random number RAND.
- RAND, Kc and SRES make together a complete triple.

At the request of the VLR, several triples are generated for each mobile subscriber in the AC and transferred to the VLR via the HLR on request.

Remark: The individual key Ki is only stored in the AC and the SIM card. Different to the IMSI and the triples, it is never transmitted through the network. For all signaling procedures the users IMSI is used. [B2]

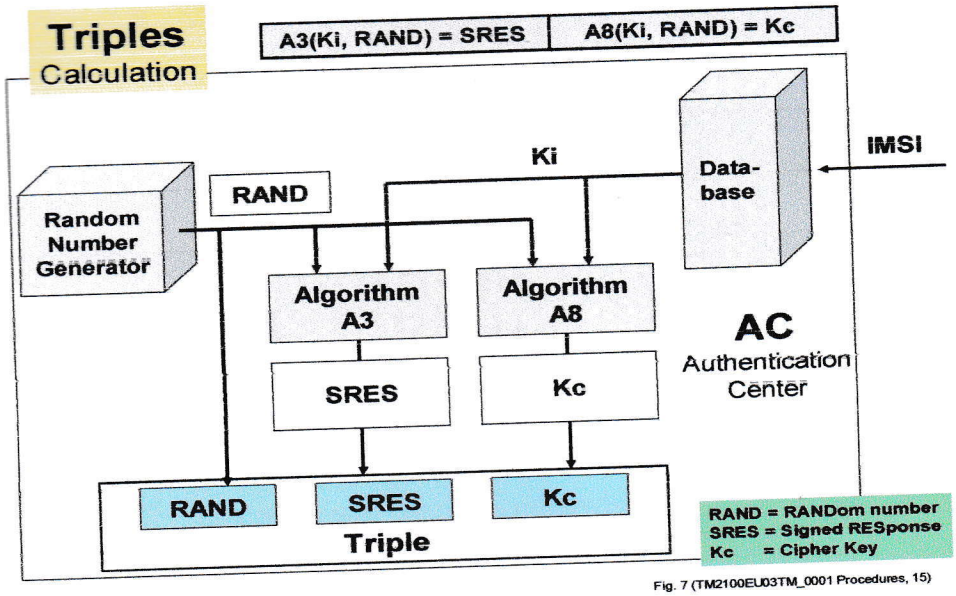


Fig 3.5: Triples Calculation

3.3.2 Authentication:

The authentication checks the real identity of a user, i.e. his authorization to take access to the network. Actually it is checked, whether the secret individual Key Ki stored on the SIM card is identically to the one stored for this user in the Authentication Center or not. The authentication procedure is or can be initiated by the VLR in the following cases:

- IMSI Attach
- Location Registration
- Location update with VLR change
- call setup (MOC, MTC)
- activation of connectionless supplementary services
- Short Message Service (SMS)

Authentication Procedure

1. The VLR recognizes the need for an authentication; in the case, that no

/ no more Triples are available in the VLR it requests a set of Triples from the HLR

2. The Triples are generated in the AC (see above) and sent via HLR to the VLR

3. The VLR sends the RAND to the MS; the SIM card calculates the SRES using Ki, A3 and RAND (see above)

4. The MS sends the SRES back to the VLR; the VLR compares the SRES in the Triple with the SRES calculated by the MS; if they coincide, the network access will be authorized and the general procedure will continue, otherwise

5. The access will be refused and the "Authentication Refused" message will be sent to the MS [B2]

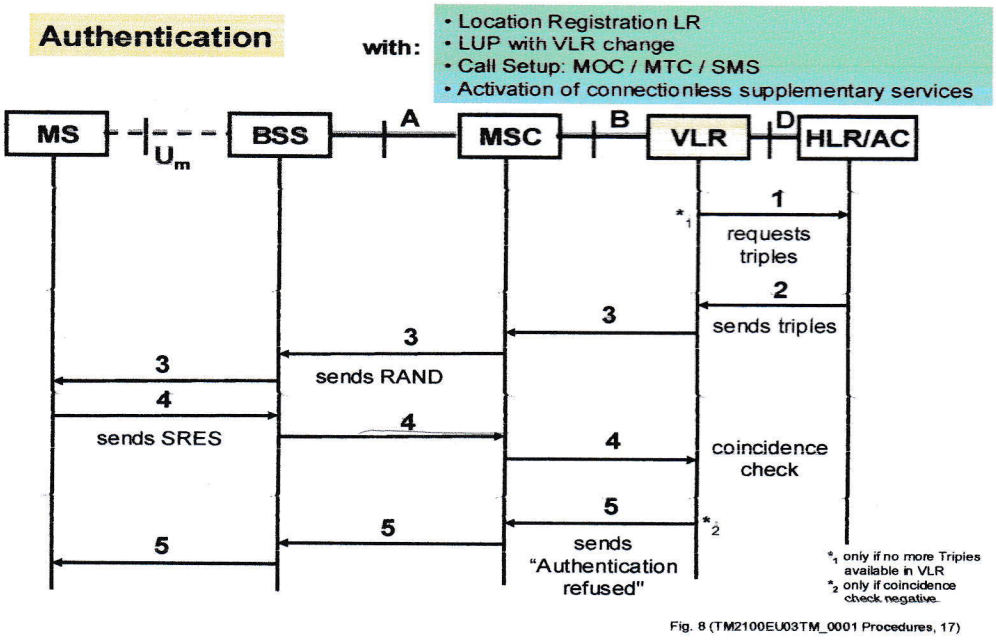


Fig 3.6: Authentication

3.3.3 Ciphering:

Ciphering regards the security aspects of the information exchange between the Mobile Station (MS) and the Base Station (BTS) on the air interface Um. User information

(speech/data) and signaling information are ciphered via air interface Um (UL & DL). An exception is given by the initial signaling, before the cipher command is sent from the network side. At initial signaling data exchange ciphering is not possible, because the users' identities are necessary prerequisite for the generation of ciphering parameters. The cipher command is given after transmission of the user identity (TMSI / IMSI) and the authentication procedure. Ciphering / Deciphering is carried out in the BTS and in the MS.

The GSM Recommendation (02.16) of Phase 2 states that up to 8 logically different encryption algorithms (incl. "no ciphering") should be used. The reason for this is the intention

- to assign different algorithms to different countries and
- to provide MS, which do not use the A5-1 algorithm, with the possibility of roaming in different GSM-PLMN networks.

Currently 3 algorithms are defined:

- A5-0: no ciphering for COCOM countries
- A5-1: "strict" cipher algorithm (originally MoU algorithm) for MoU-1 countries , A5-1comes from GB; due to military origin (NATO), high security arrangements are to be regarded
- A5-2: "simplified" cipher algorithm for MoU-2 countries (without COCOM countries); [B2]

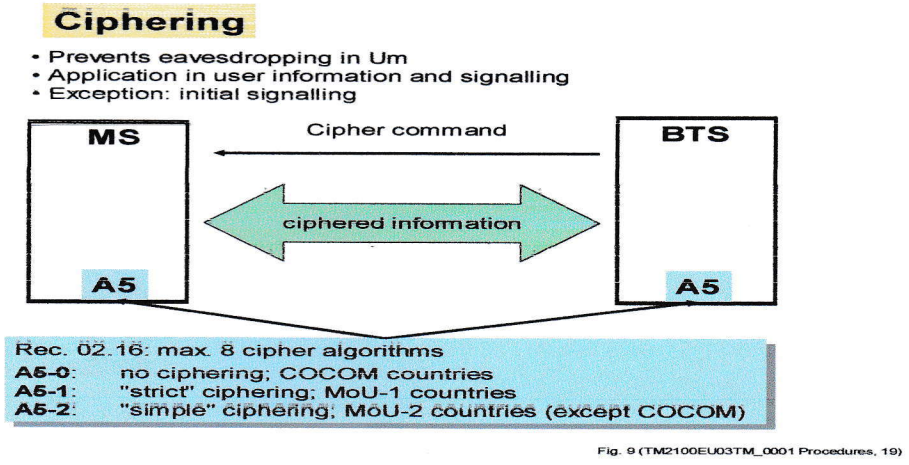


Fig 3.7: Ciphering

3.3.3.1 Ciphering process:

Transmitter/receiver must use the same cipher algorithms.

In order to handle ciphering individually for every user, the individual key Ki (stored

in the SIM card and the AC) is used.

The cipher key Kc is transmitted after ciphering from the VLR to the BTS. The MS is able to calculate Kc (after receiving RAND in the authentication procedure) by algorithm A8 from RAND and Ki.

A 114 bit long cipher sequence is calculated using the cipher algorithm A5, the cipher key Kc and the TDMA frame number (broadcasted cyclically by ever y BTS over the cell area).

The speech, data and signaling information are ciphered / deciphered in 114 bit long sequences being connected in a so-called "eXclusive OR" XOR operation.

Deciphering follows exactly the same scheme as ciphering, as the XOR operation yields the original values after double application of XOR (using the same cipher sequence).

To start ciphering, the network sends a cipher start command, which has to be acknowledged by the MS (being the first ciphered information). [B2]

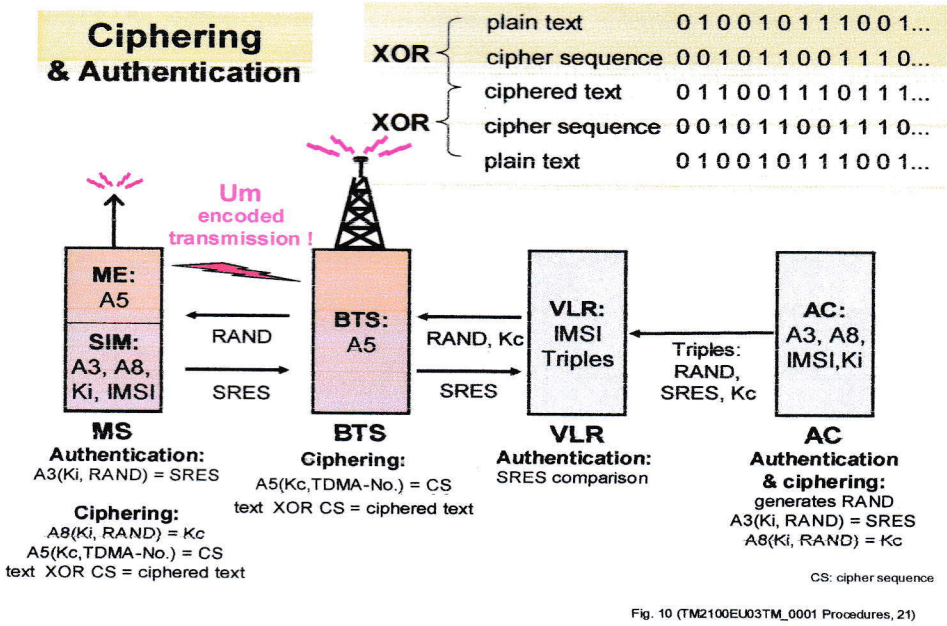


Fig 3.8: Ciphering & Authentication

3.3.4 TMSI Allocation:

Ciphering protects the user from being eavesdropped. However, the ciphering with Kc requires that the network is aware of the identity of the mobile subscriber with whom it is in contact. Thus, during the initial phase of communication setup, when the identity of the mobile subscriber is still unknown, the transmitted signaling information can not be ciphered. During this phase a third party may identify a subscriber and the desired service.

In order to protect the identity of the subscriber in this phase, a temporary identification of the subscriber is distributed: the Temporary Mobile Subscriber Identity TMSI.

The TMSI is used instead of the real user identity, the International Mobile Subscriber Identity IMSI. This TMSI is allocated by the VLR, which is associated to the VMSC. The MS usually identifies itself with the TMSI in the initial access phase to the VLR. The VLR uses this TMSI to re-identify the IMSI. This is only possible if the TMSI has been allocated by the same VLR. If not, the VLR has to request the VLR, which has allocated the TMSI to the MS, to deliver the IMSI. Therefore, the TMSI is in most cases transmitted together with the old LAI, which identifies uniquely a VLR. The request VLR - VLR is only possible, if both VLR belong to the same PLMN. Therefore, the IMSI has to be transmitted via Um at the first registration in a new PLMN and obviously at the very first usage of the SIM card (i.e. in the case of Location Registrations).

A new TMSI (TMSI re-allocation) can optionally be allocated to the MS after every authentication & cipher start (and the optional IMEI check). [B2]

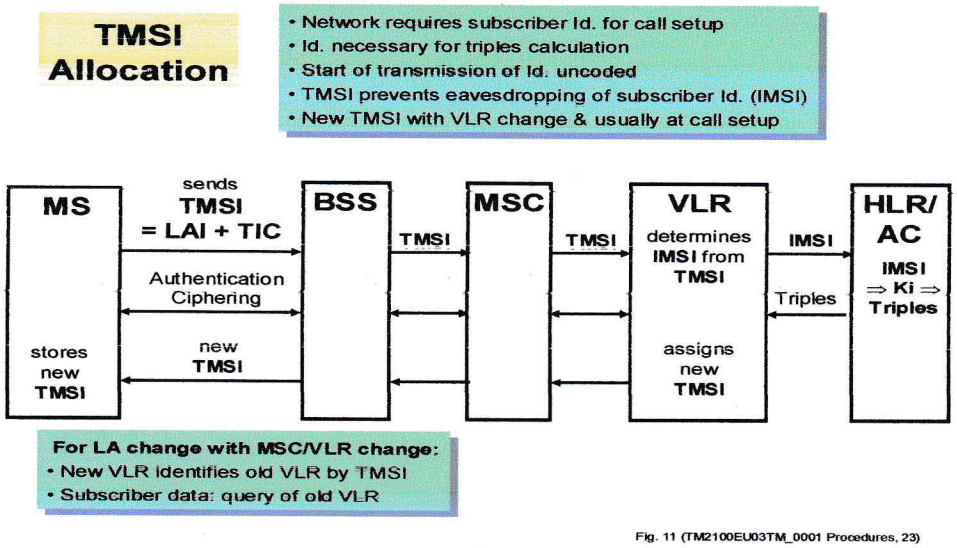


Fig 3.9: TMSI Allocation

3.3.5 IMEI Check:

In contrast to the other security mechanism authentication, ciphering and TMSI allocation, the check of the International Mobile Equipment Identity IMEI is optional. It depends on the operators decision whether a EIR is implemented and IMEI checks are done. IMEI check serves to identify stolen, expired or faulty mobile equipment. A

IMEI clearly identifies a particular mobile device and 3.3.5 IMEI Check:
contains information about the place of manufacture, type approval code and the serial number of the equipment.

The IMEI consists of: Type Approval Code TAC, Final Assembly Code FAC, Serial Number SNR and a Software Version Number SVN. If a IMEI check in the PLMN is intended, the Mobile Station MS will be requested to submit the IMEI during call setup after authentication and cipher command. The MS sends back its IMEI. The IMEI is routed to the EIR of the PLMN. A check occurs here to find out whether the IMEI is registered on the black or gray list, i.e. whether the MS is blocked from further use of the PLMN, or whether it has to be observed. [B2]

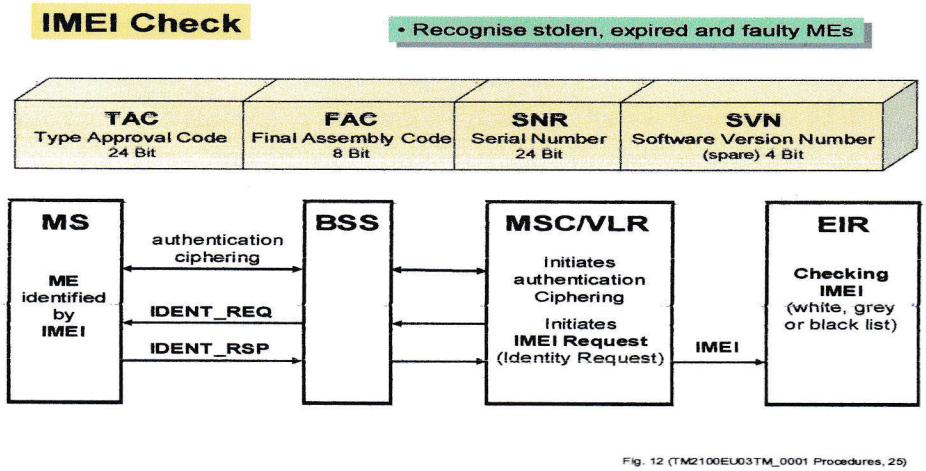


Fig 3.10: IMEI Check



Fig 3.11: Location Update

3.4 Location Registration / Location Update

Information of the current location of a mobile subscriber are necessary to built up a connection to the subscriber, i.e. to start a Mobile Terminating Call MTC. To keep track of the users current location the Location Registration / Update procedures are

used. Always the MS is responsible to initiate this Location Registration / Update procedures. It informs the network on its current Location Area. The Location Area information is stored in the currently responsible VLR. The identity of this VLR is stored in the users HLR.

If a MS is "new" in a PLMN a Location Registration is performed. "New" is defined as the very first usage of a SIM card or a first access after changing the PLMN.

In case of a Location Registration the network needs the IMSI of the MS, because either no TMSI has been allocated before to the MS (in case of first SIM usage) or it is impossible to regenerate the IMSI from the TMSI, because the new VLR is not able to get into contact with the old VLR (e.g. in case of PLMN changes). After Location Registration, in the following Location Updates are used to update the location information in the PLMN. In a Location Update only the TMSI is transmitted via Um.

There are three reasons to perform a Location Update Procedure LUP:

- Location Update with "IMSI Attach": If a MS is switched on / off, the network is informed about the change of the current MS state, i.e. whether to be reachable or not. Therefore, when being switched on / off, the MS performs an "IMSI Attach" / "IMSI Detach" procedure. The information whether the MS is Attached / Detached is stored in the VLR. If an "IMSI Attach is performed it is connected with a LUP.

- Normal Location Update: Normally a LUP is performed after the MS has recognized that it has crossed the boarder between two different Location Areas. The MS is able to recognize the LA change, because it always listens around to the broadcast information of all cells in its environment, which include the CGI (and so the LAI). If the LAI of the strongest cell changes, a LUP is performed.

- Periodical Location Update: A periodic LUP is initiated by a MS at regular intervals. If the VLR does not receive the LUP after a certain time, a "Mobile Station not reachable" flag is set. The LUP is not performed during the duration of a connection. In this case, the LUP is performed after call release. [B2]

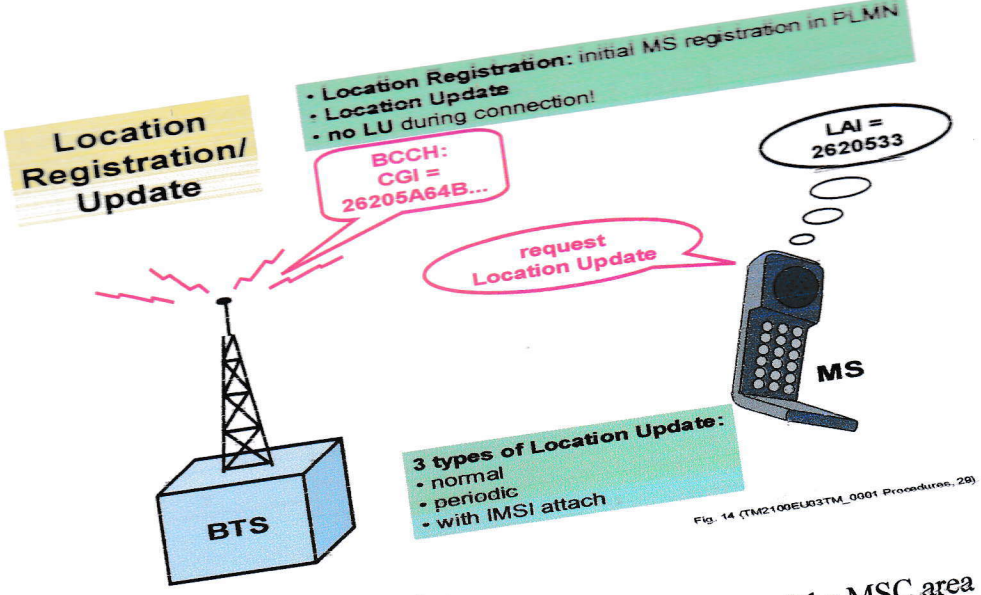


Fig 3.12: Location registration

3.4.1 Location Update Procedure LUP without change of the MSC area

1. The MS recognizes that the LAI has changed. It requests a LUP, identifying itself with the TMSI or IMSI. The request and the identity are forwarded to the VLR.
2. The VLR re-identifies the IMSI from the TMSI. If no / no more Triples are available in the VLR, it requests triples from the AC via the HLR.
3. The AC generates a set of Triples and delivers them via HLR to the VLR.
4. The VLR stores the Triples and initiates the Authentication, then gives the cipher start command and initiates an IMEI check (optional).
5. If the Authentication, cipher start and IMEI check are successful, the VLR needs for call setups the subscriber data. In case of a LR, they are have not been stored before in the VLR and so they have to be requested from the HLR. Together with this request, the VLR delivers its identity and the information, where this subscriber is stored in the VLR, i.e. the Local Mobile Subscriber Identity, to the VLR.
6. The HLR stores the VLR identity and LMSI and transmits the requested subscriber data to the VLR.
7. The VLR stores the subscriber data and assigns a TMSI (LR: mandatory) or a new TMSI (LUP: only with MSC/VLR change) to the MS. This TMSI is transmitted together with the VLRs acknowledgement, that the LUP has been successful, to the MS. There, the new TMSI and LAI are stored on the SIM card. [B2]

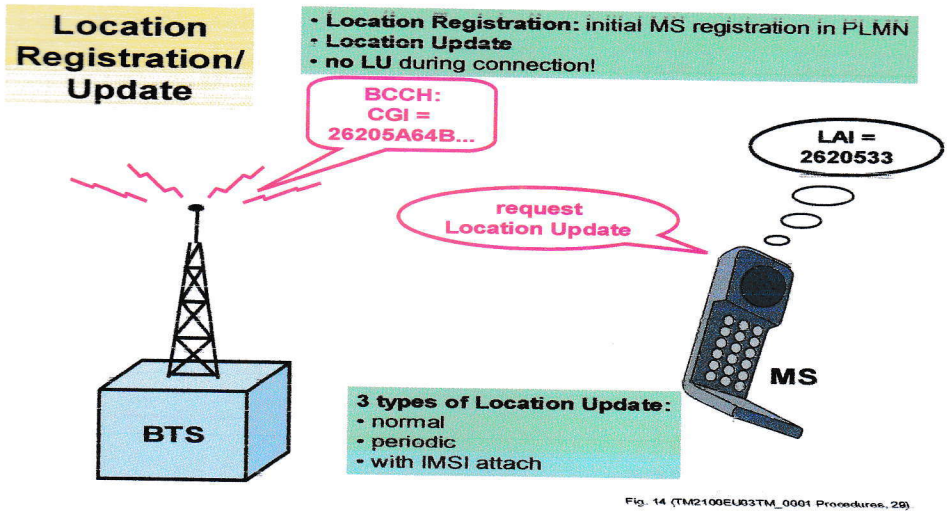


Fig 3.12: Location registration

3.4.1 Location Update Procedure LUP without change of the MSC area

1. The MS recognizes that the LAI has changed. It requests a LUP, identifying itself with the TMSI or IMSI. The request and the identity are forwarded to the VLR.
2. The VLR re-identifies the IMSI from the TMSI. If no / no more Triples are available in the VLR, it requests triples from the AC via the HLR.
3. The AC generates a set of Triples and delivers them via HLR to the VLR.
4. The VLR stores the Triples and initiates the Authentication, then gives the cipher start command and initiates an IMEI check (optional).
5. If the Authentication, cipher start and IMEI check are successful, the VLR needs for call setups the subscriber data. In case of a LR, they are have not been stored before in the VLR and so they have to be requested from the HLR. Together with this request, the VLR delivers its identity and the information, where this subscriber is stored in the VLR, i.e. the Local Mobile Subscriber Identity, to the VLR.
6. The HLR stores the VLR identity and LMSI and transmits the requested subscriber data to the VLR.
7. The VLR stores the subscriber data and assigns a TMSI (LR: mandatory) or a new TMSI (LUP: only with MSC/VLR change) to the MS. This TMSI is transmitted together with the VLRs acknowledgement, that the LUP has been successful, to the MS. There, the new TMSI and LAI are stored on the SIM card. [B2]

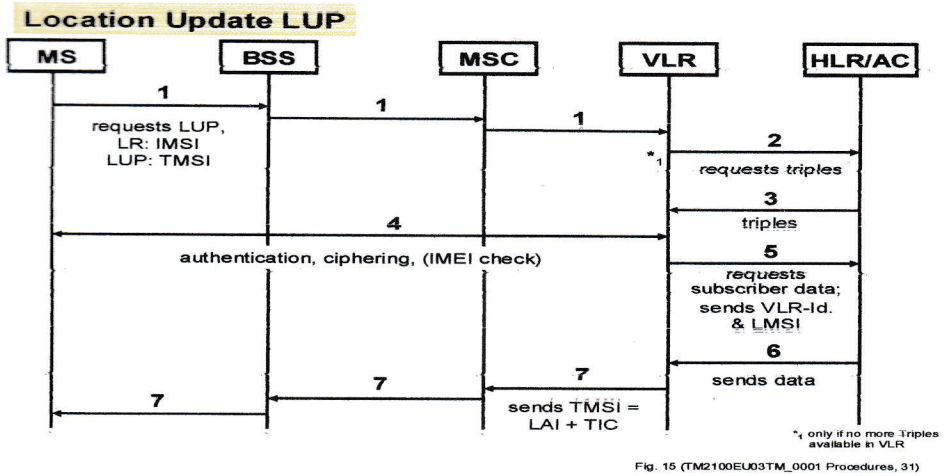


Fig 3.13: Location Update

3.4.2 Location Update Procedure LUP with VLR change

1. The MS recognizes that the LAI has changed. It requests a LUP, identifying itself with the TMSI. The request and the identity (TMSI in combination with the old LAI) are forwarded to the new VLR.

2. The new VLR receives the TMSI and LAI. It recognizes from the LAI, that the TMSI has been allocated by another VLR (old VLR). Thus, the VLR is not able to re-identify the IMSI from the TMSI and has no chance to request the subscriber data from the HLR. Therefore, the new VLR calculates the address of the old VLR from the LAI and transmits the TMSI to the old VLR and requests it to deliver the users IMSI. The old VLR delivers the IMSI and the remaining Triples to the new VLR. Remark: If this step 2 is not possible (e.g. line break between old and new VLR) the new VLR commands the MS to transmit the IMSI directly.

3. The new VLR uses the IMSI to calculate the users HLR. The new VLR transmit its identity and LMSI to the HLR and requests the HLR to deliver the subscriber data and, if necessary, a set of Triples.

4. The HLR stores the new VLRs identity and LMSI, confirms the information, supplies the subscriber data and, if necessary, the Triples.
5. The HLR informs the old VLR to erase the stored data set of this subscriber.
6. The VLR now starts authentication, ciphering and (optionally) IMEI check.

7. The VLR allocates a new TMSI to the MS. [B2]

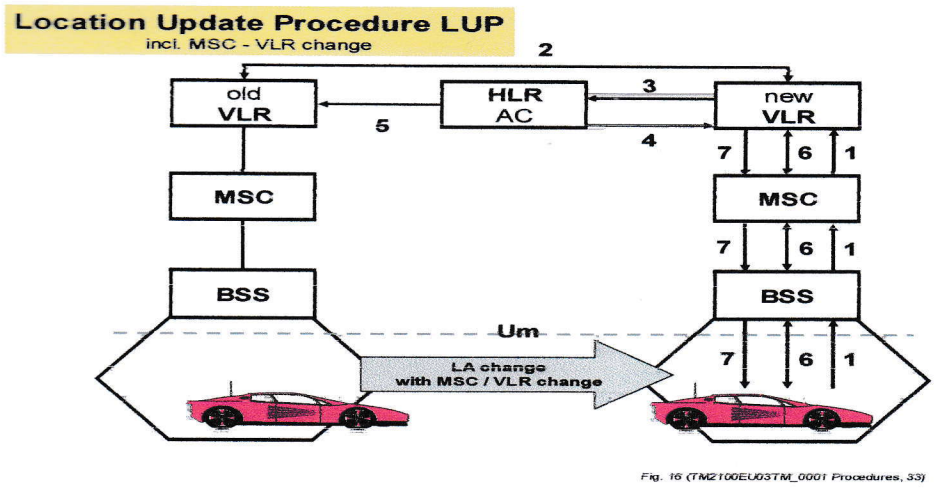


Fig 3.14: Location Update procedure

3.5 RADIO- TRANSMISSION

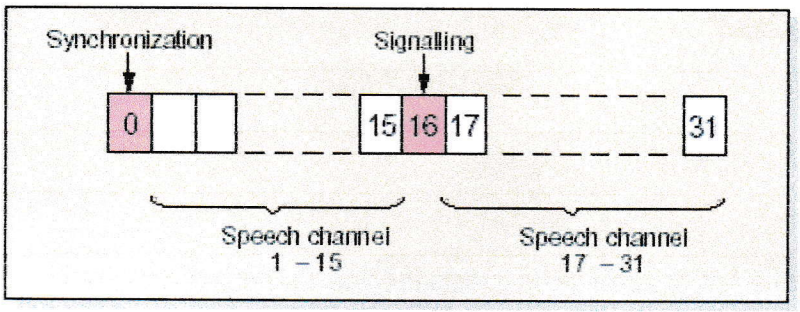
Analogue signals and digital transmission speech is an analogue, continuous wave, transform it in digital terms using Pulse Code Modulation PCM

Sampling:

Normal speech mainly contains frequency components lower than 3000 Hz. sampling theorem: the sampling frequency, fs,should therefore be at least 2 x 3 kHz = 6 kHz. Telecomm systems use 8 kHz

A digital link used to transmit these bits is called a PCM–link.

PSTN: sampling at 8 kHz and performing quantization and coding using 8 bits, produces a bit rate of 8000 x 8 = 64kbit/s.several channels are multiplexedonto the same link. by TDMA, Time Division Multiple Access, and means that several channels share the same link. Each channel uses a time slot. 32 channels are multiplexed onto one PCM–link The bit rate on such a link is 32 x 8 x 8000 = 2048 kbit/s.



The 32 channels are said to form a frame, Eight time slots will be used for each

frequency band.

– air interface

eight mobiles can use the same frequency band by using different time slots,

channel separation 200 kHz.

3.5.1 Transmission Problems

- Path loss
- Fading
- Rayleigh fading
- Time dispersion causes Inter Symbol Interference (ISI).
- Time alignment

3.5.2 Solution to Transmission Problem

- Interleaving
- Frequency hopping
- Antenna (or space) diversity
- The Equalizer
- Timing Advance [B2]

3.6 Call Setup:

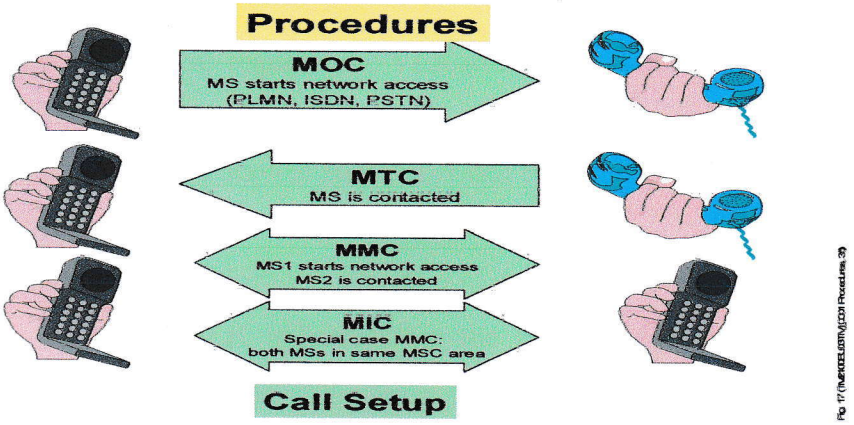


Fig 3.15: Call setup

Call Setup

- Different procedures are necessary depending on the initiating and terminating party:
- Mobile Originating Call MOC: Call setup, which are initiated by an MS
- Mobile Terminating Call MTC: Call setup, where an MS is the called party

- Mobile Mobile Call MMC: Call setup between two mobile subscribers; MMC thus consists of the execution of a MOC and a MTC one after the other.

- Mobile Internal Call MIC: a special case of MMC; both MSs are in the same MSC area, possibly even in the same cell.

- 3.6.1 Mobile Originating Call MOC
    - Channel Request: The MS requests for the allocation of a dedicated signaling
- channel to perform the call setup.
    - After allocation of a signaling channel the request for MOC call setup, included
- the TMSI (IMSI) and the last LAI, is forwarded to the VLR
    - The VLR requests the AC via HLR for Triples (if necessary).
    - The VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI
- Re-allocation (optional).
    - If all this procedures have been successful, MS sends the Setup information

    a. (number of requested subscriber and detailed service description) to the MSC.

    b. The MSC requests the VLR to check from the subscriber data whether the

    c. requested service an number can be handled (or if there are restrictions which do

    d. not allow further proceeding of the call setup)

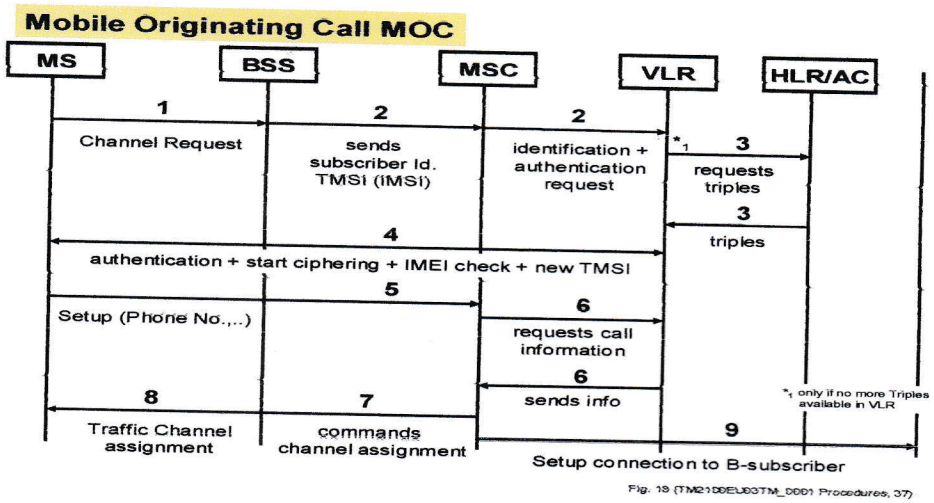
    e. If the VLR indicates that the call should be proceeded, the MSC commands the

    f. BSC to assign a Traffic Channel (i.e. resources for speech data transmission) to

    g. the MS

    h. 8. The BSC assigns a Traffic Channel TCH to the MS

    i. 9. The MSC sets up the connection to requested number (called party).



j.

k. Fig 3.16: Mobile Originating Call

l. 3.6.2 Mobile Terminating Call MTC

m. In the case of a MTC the mobile subscriber is the called party. The MTC call flow

n. differs in dependence on the initiating party. In this example the initiating party is

o. subscriber on an external network.

p. After analysis of the MSISDN (CC and NDC) a request to set up a call is

q. transmitted from an external exchange to the GMSC.

r. The GMSC identifies the users HLR from the MSISDN. It starts a so-called

s. Interrogation to the HLR to get information of the subscribers current location.

t. The HLR identifies the subscribers IMSI from the MSISDN and checks the

u. subscribers current location, i.e. the VLR address. The HLR informs the VLR

v. about the call and requests a Mobile Station Roaming Number MSRN (including

w. the VMSC address) from the VLR. The request to the VLR includes the LMSI,

x. which enables the fast access to the users data in the VLR.

y. 4. The VLR transmits the MSRN to the HLR, which forwards this number and the

z. IMSI to the GMSC. If the VLR has information, that the MS is Detached currently,

aa. the call is rejected / forwarded to the Mailbox.

bb. The GMSC uses the MSRN (including the VMSC address) and IMSI to get into

cc. contact with the VMSC. [B2]

dd. The VMSC requests information (LAI, TMSI) for call setup from its VLR

ee. The VLR sends these data.

ff. The VMSC uses the LAI to start the Paging procedure. Paging means to search

gg. to MS in the total Location Area (the precise cell is not known).

hh. The MS responses the Paging, i.e. from now on its cell is known.

ii. This topic includes: Authentication, cipher start, IMEI check and TMSI Re-

jj. allocation.

kk. The MSC transmits the Setup information to the MS, commands the BSC to

ll. allocate a Traffic Channel to the MS and switches through the connection.

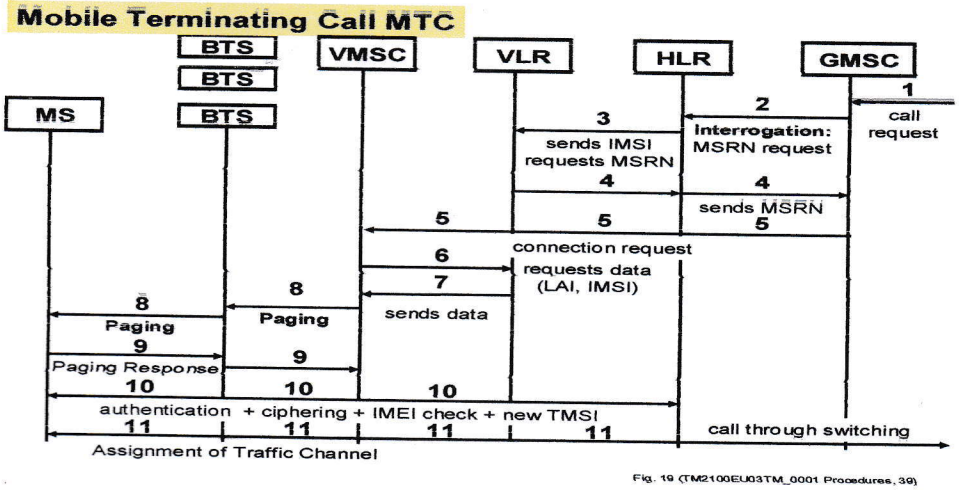


Fig. 19 (TM2100EU03TM_0001 Procedures, 39)

- Fig 3.17: Mobile Terminating Call

MMC and MIC are only special cases / combinations of the MOC and MTC.

3.6.3 Mobile Mobile Call MMC

The MMC is a call setup initiated by a MS and terminating at a MS. Thus, MOC and MTC are executed one after the other.

For the call setup of a MMC the same procedures are valid as in the case of MOC and MTC for the call setup between a mobile subscriber and a fixed subscriber. In the case of PLMN internal MMC, instead of inquiring the GMSC the VMSC of the calling party queries the HLR of the called party.

3.6.4 Mobile Internal Call MIC

A special case of the MMC is represented by the MIC. Here, both mobile subscribers are in the same MSC area or even in the same cell. No shortening of the procedure takes place here. MOC and MTC procedures are executed after each other, the only difference is that the MSC involved is VMSC for both, the calling and called party. [B2]

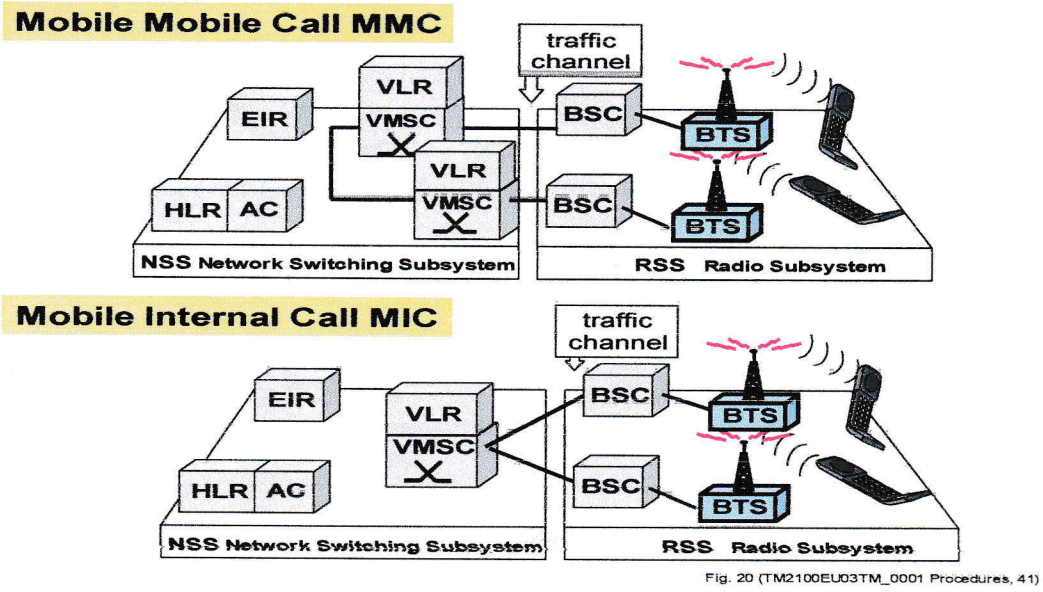
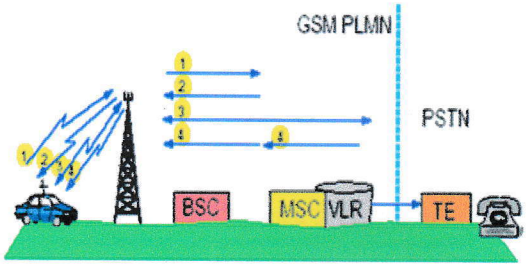


Fig 3.18: MMC & MIC

3.6.5 Call From MS To PSTN:

Call from MS to PSTN



1. MS uses RACH (Random Access channel) to ask for a signalling channel, SDCCH (Stand alone Dedicated Control channel).
2. BSC allocates a signalling channel, using AGCH (Access Grant channel).
3. MS sends a call set up request via SDCCH to the MSC/VLR. Over SDCCH all signalling preceding a call takes place. This includes marking the MS "busy" in MSC/VLR, authentication procedure, start ciphering equipment identification, sending the B-number (the number to the called subscriber, in this case a PSTN subscriber) and checking if the subscriber has the service "Barring of outgoing calls" activated.
4. MSC/VLR asks the BSC to allocate a free TCH (traffic channel). This is forwarded to the BTS and MS, which are told to activate the TCH.
5. MSC/VLR forwards the B-number to an exchange in the PSTN, which establishes a connection in PSTN to the B-subscriber.

B answers (hopefully), and the connection will be established.

Call From PSTN to MS

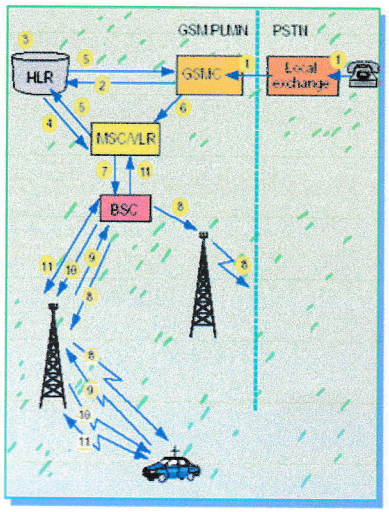


Fig 3.19: Call from PSTN to MS

3.6.6 Call from PSTN to MS

1. PSTN subscriber keys the MSISDN, (MS telephone number). MSISDN is analyzed in the local exchange in PSTN, which realizes that this is a call to a subscriber in a GSM network. A connection is set up to the GMSC

2. GMSC analyses MSISDN to find out in which HLR the MS is registered, and interrogates the HLR for information about how to route the call to the serving MSC/VLR.

3. HLR translates MSISDN into IMSI, and finds out which MSC/VLR is currently serving the MS. HLR also checks the service, "Call forwarding to C number". If the service is active the call is rerouted by the GMSC to that number, probably via PSTN.

4. HLR requests a roaming number, MSRN (Mobile Station Roaming Number), from the serving MSC/VLR. MSRN identifies the MSC/VLR.

5. MSC/VLR returns the MSRN via HLR to the GMSC.

6. GMSC reroutes the call to the MSC/VLR, directly or via the PSTN.

7. The MSC/VLR knows in which Location area, LA, the MS is. A Paging message is sent to the BSCs controlling the LA. (In CME 20 the information on which cells belong to which LA is stored in the BSC, but according to the GSM specification it can as well be stored in the MSC).

8. The BSCs distribute the Paging message to the BTSs in the wanted LA. The BTSs transmit the message over the air interface using PCH (Paging channel). To page the MS, IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity, valid only in the current MSC/VLR service area) is used.

9. When the MS detects the paging message it sends a request for a signalling channel, SDCCH.

10. BSC provides a SDCCH, using AGCH

11. SDCCH is used for the call set up procedures, as in the case for "Call from MS", and then a TCH is allocated. SDCCH is released.
    The mobile phone rings, and when the subscriber answers the connection is completed. [B2]

3.7 Handover:

In cellular telecommunications, the term handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to

another. In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service. Handover HO is a change of the physical channel during a current connection.
There are various types of handover:

3.7.1 Intra-Cell Handover: In the case of Intra-Cell Handover, a physical channel within a cell is changed. A reason for this may be interference in the frequency currently being used. Frequency and/or Time Slot can be changed. Therefore it differs from the feature "frequency hopping", in which the frequency is changed after a certain algorithm, but the time slot is never changed. Frequency hopping and Intra-Cell Handover exclude each other. The intra-cell handover is realized internally in the BSS, i.e. the BSC decides without MSC involvement. Only the message "handover performed" is sent to the MSC after the handover.

3.7.2 Intra-BSS Handover: An Intra-BSS Handover is carried out between two cells of the same BSS. The procedure is decided and performed by the BSC (no MSC involvement). The MSC is informed only after the handover ("handover performed").

3.7.3 Intra-MSC Handover: An Intra-MSC handover is a handover between two BSSs of the same MSC. The MSC decides about this Handover and switches between the two BSCs.

3.7.4 Inter-MSC Handover: A Inter-MSC Handover include at least two MSCs. The MSC has to decide and to switch. Inter-MSC handovers are one of the most complicated GSM procedures, in particular in the case of MSCs made by different manufacturers. One has to distinguish between "Basic Inter-MSC Handover" and "Subsequent Inter-MSC Handover". Basic Inter-MSC Handover: If a MS changes for the first time from the area of an MSC (A) to the area of a MSC (B), this is described as Basic Handover.

3.7.5 Subsequent Handover: If the MS also leaves the MSC (B) area and moves into the area of a further MSC (C) or returns to the area of the old MSC (A), this follow-on handover is called Subsequent Inter-MSC Handover. The handover is controlled by the initial MSC, which is called MSC (A) = Anchor MSC. In a Subsequent Inter-MSC Handover with MSC (C) for a short time three MSCs are connected for one call. The connection MSC (A) - MSC (B) is released after successful set up of connection between MSC (A)and MSC (C). The Anchor MSC is responsible for billing. This is the

reason, why Inter-PLMN Handover, i.e. Handover between different PLMNs are normally not performed. [B2]

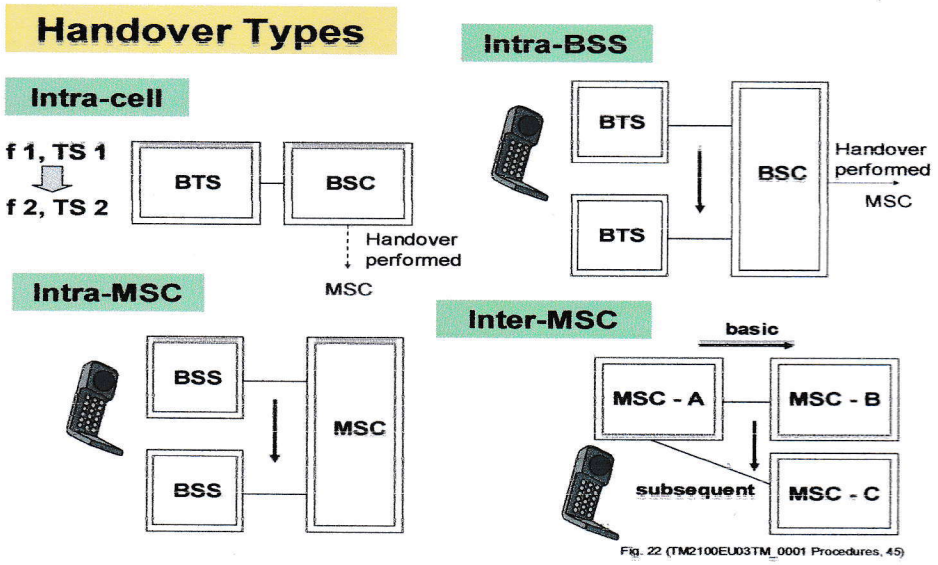


Fig 3.20: Handover Types

3.7.6 Handover Decision

The handover algorithm is based on periodically measurements of MS and BTS concerning the strength and quality of the received signals. The MS measures quality and strength of the connection and the strength of the serving BTS and that of the surrounding BTSs. The BTS measures quality and strength of the connection as well as the distance MS - BTS (Timing Advance TA).

The result of the MS measurements is transmitted to the BTS. The BTS adds its own measurements and transmits the data as "Measurement Report" to the BSC.

The BSC has to decide, whether a handover is necessary or not. The decision is determined by the comparison between the current measured values and the threshold values. If no threshold values are exceeded, the BSC analyses whether an other BTS as the current one would enable a better air interface quality. Different other aspects have to be taken into account, e.g. the current load of the cells. Furthermore, so-called "Ping-Pong Handover" should be prevented.

If an Inter-cell handover is initiated, the criterion of availability of surrounding cells is used to set up a list of suitable handover destinations in a declining order of priority. This list forms the basis for the final handover decision that is carried out by the BSC (in case of Intra-BSS Handover) or by the MSC (in case of Inter-BSC / -MSC Handover). [B2]

Handover criteria are e.g.:

Strength of the received signal (UL and DL)

Quality of the received signal (UL and DL)

Distance MS - BTS (Timing Advance, UL)

Signal strength of suitable surrounding cells (UL, BCCH)

Interference that decrease the signal quality (UL and DL)

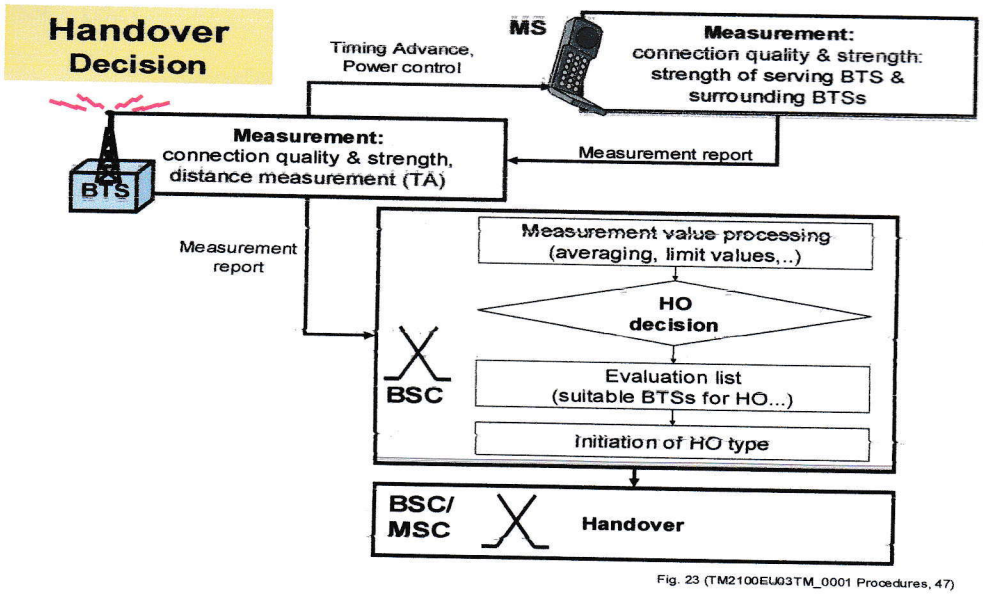


Fig 3.21: Handover Decision

3.7.7 Handover Example: (Basic) Inter-MSC Handover

1. During an existing connection, the MS permanently measures the quality and power level of the received information and measures the strength of its own and the surrounding BTS. Furthermore, the BTS measures the quality and strength of the connection and the Timing Advance. The results are as measurement report to the BSC. The BSC analyses the need for Handover. If an Handover is necessary, the BSC creates a list of preferable cells to which the Handover should be performed. If an Handover to a cell of another BSC / MSC is necessary, the information is forwarded to the MSC (A). In this example, a Handover from Cell A to Cell B is preferable. On basis of the BSC information, the MSC (A) decides to initiate a Basic Inter-MSC Handover to MSC (B), because Cell B is in the service area of MSC (B).

2. MSC (B) requests the BSC, which is responsible for Cell B to allocate resources for this connection and prepare network transmission capacities for the call. A

second connection is built up parallel to the existing connection. The DL information is split and delivered to both BTS.

3. MSC (A) gives command to the MS (via BSC) to change the physical channel. Changing the physical channel, the MS immediately is connected to Cell B.

4. The initial connection is released, the resources are set free for other connections. The users data are still transmitted via MSC (A); it is the Anchor-MSC. [B2]

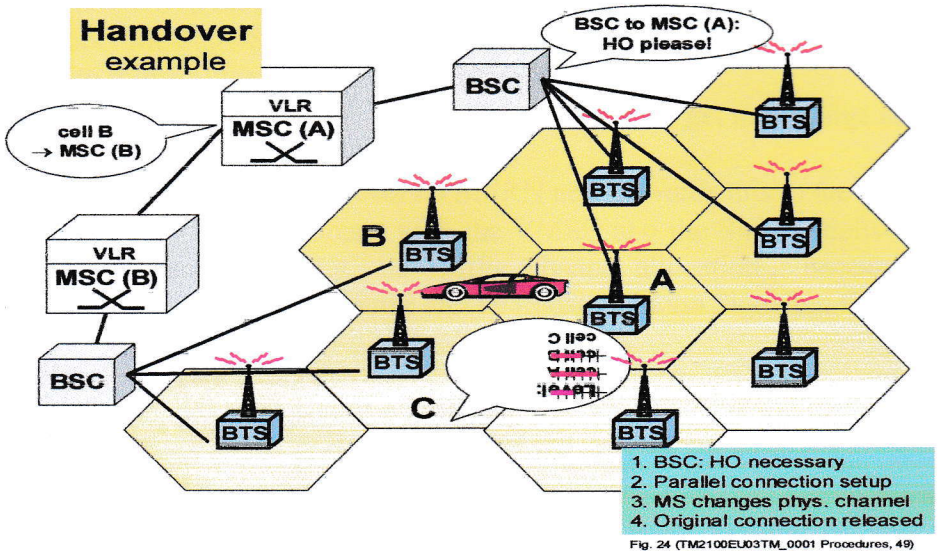


Fig 3.22: Inter MSC Handover

3.8 Emergency Call

The connection set up for the Tele Service "Emergency Call" is similar the that of the Mobile Originating Call MOC.

The mobile subscriber starts this service either by pressing a SOS key or by dialing an emergency service number (often: 112).

The setup follows the MOC signaling flow. Differences are:

- no Authentication is necessary
- no Ciphering will be used
- no IMEI check is performed
- no TMSI Re-allocation is performed

A short call setup is resulting in this lack of security features. Furthermore, the Emergency Call should always be possible with any MS, even without a valid SIM Card. Emergency calls are treated with precedence. This may also lead to the release of other existing connections.

The BSS always delivers the location of the emergency call to the MSC. Depending on this origin, the emergency connection is then transmitted from the MSC to the regionally responsible Emergency Call Center. The available location information can be delivered to the Emergency Call Center, too (operator dependent).

Short Message Service SMS transmission (MT-SMS)

3.8.1 MS attached (i.e. reachable):

- A Short Message Service Center SM-SC (out of the scope of the GSM Rec.) tries to transmit the SMS to the requested MS via GMSC.
- The GMSC performs an Interrogation to the HLR to get knowledge about the current VMSC.
- The HLR requests the VLR for an MSRN and forwards this to the GMSC.
- The GMSC gets into contact with the VMSC and the SMS is delivered to the MS. Different to the MOC, no Traffic Channel allocation is necessary in case of SMS transmission. The SMS can be transmitted via Signaling Channel.

3.8.2 MS Detached (not reachable):

- The SM-SC tries to transmit the SMS to the requested MS via GMSC.
- The GMSC performs an Interrogation to the HLR to get knowledge about the current VMSC.
- The HLR requests the VLR for an MSRN. This is not possible, because the subscriber is Detached and the VLR stores this information.
- In the following, a SMS flag is set in the VLR and in the HLR. Furthermore, the HLR stores the address of the SMS-SC.
- The HLR informs the GMSC that the SMS can not be delivered and the GMSC rejects the request of the SM-SC. The SMS is still stored in the SM-SC.
- If the MS is switched on again, an IMSI Attach procedure is performed to the VLR.
- Due to the SMS flags, the VLR informs the HLR, that the MS is reachable again.
- The HLR requests via GMSC the SM-SC to start the SMS transmission again. [B2]

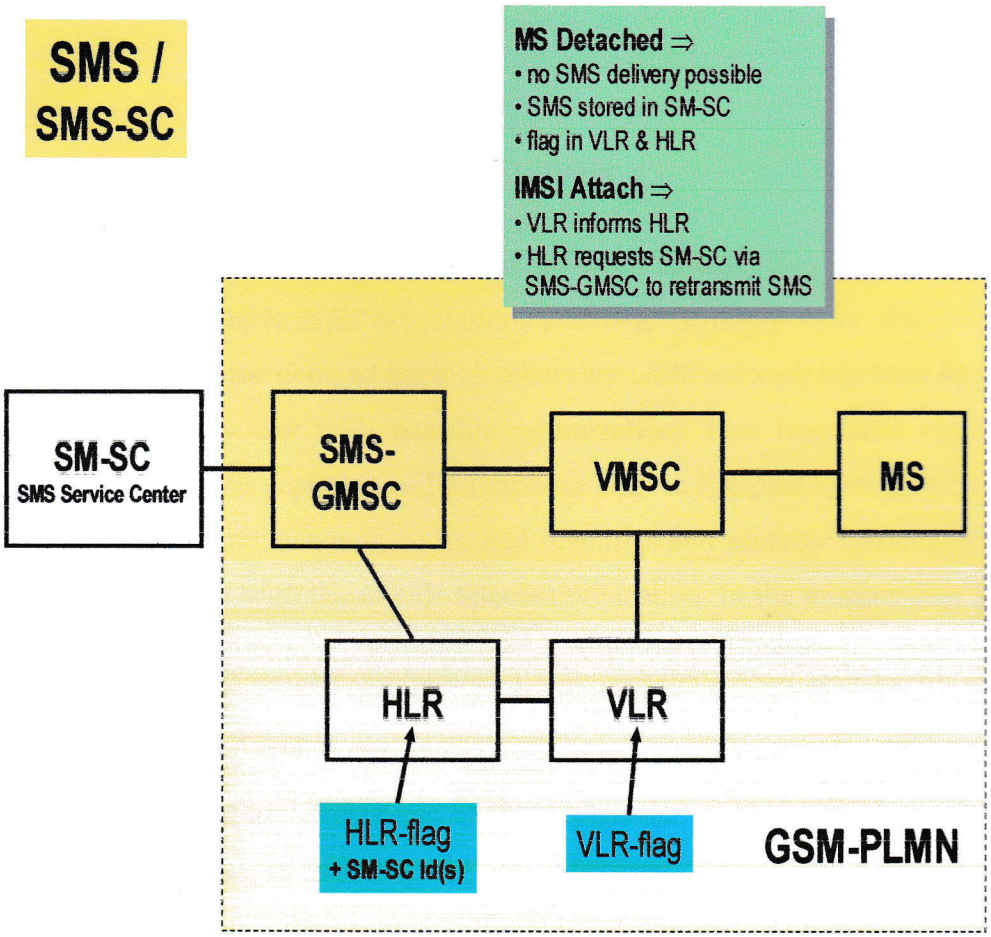


Fig. 26 (TM2100EU03TM_0001 Procedures, 53)

Fig 3.23: SMS/SMS-SC

CHAPTER 4

CONCLUSION

Cellular communication is something that provides reliable and highly accessible service. Subscribers have high expectations and react strongly when the service is unavailable. To meet the demand for high reliability GSM network has been upgraded progressively day by day with possible optimization. This Internship report has comprised with a detail depiction of IN functions and the Pre-paid system of IN. Also it includes the GSM architecture, codes and identities and security features. Uses of IN is not only limited with the mobile telecommunication. In the present time IN has been used in various fields like hospital, banks, different multinational companies and many others. Day by day we are discovering many things related with science and technologies, business to full fill the demands of our daily life. We always expect better. According to these circumstances IN has brought a tremendous change in the communication history of mankind and still it is trying to meet the demands of all users.

REFERENCES

BOOKS:

B1. GSM System Introduction *by Ericsson*

B2. Mobile Cellular Communication *by william cy lee*

B3. Simens Solutions (Manual)

B4. Training Modules of TMIB

B5. Wireless Communications Principles and Practice *by Theodore S. Rappaport*

LINKS:

1. www.google.com
2. www.gsmfavorites.com
3. www.robi.com.bd
4. www.ericsson.com
5. www.ice.org/online/tutorial/gsm

GLOSSARY

AMPS	Advanced mobile phone service
AOC	Advice of charge
AC	Authentication center
AIR	Account Information and Refill
BTS	Base transceiver station
CDMA	Code division multiple access
CI	Cell Identity
CGI	Cell Global Identity
CUG	Closed User Group
DTMF	Dual tone multifrequency
DAMPS	Digital advanced mobile phone service
DCS	Digital cellular system
EIR	Equipment Identity Register
E–TDMA	extended TDMA
ESN	Electronic serial number
FCC	Federal Communications Commission
FCCH	Frequency control channel
FDMA	Frequency division multiple access
FM	Frequency modulation
FRA	Fixed radio access
GSM	Global System for Mobile Communications
GMSK	Gaussian minimum shift keying
HLR	Home location Register
HO	Hand over
Hz	Hertz
kHz	kilohertz; thousands of hertz
IN	Intelligent Network
IVR	Interactive voice response
LA	Location Area
LAC	Location Area Code
LAI	Location Area Identity
LMSI	Local Mobile Subscriber Identity
MHz	Megahertz; millions of hertz
MM	Multi Mediation
MS or MSU	Mobile station unit
MSC	Mobile services switching center
MTSO	Mobile telephone switching office
MTX	Mobile telephone exchange
MINSAT	Mobile Intelligent Network Service Administration tools
MSRN	Mobile Station Roaming Number
MOC	Mobile Originating Call
MTC	Mobile Terminating Call
NADC	North American digital cellular
NAMPS	Narrowband advanced mobile phone service
OMC-B	Operation & Maintenance Center for Base Station Subsystem
OMC-S	Operation & Maintenance Center for the Switching Subsystem

OSS	Operation subsystem
PIN	Personal identity number
PUK	Pin unblocking number
PCS	Personal communications service;
PSTN	Public switched telephone network
RF	Radio frequency
SMAS	Service management application system
SIM	Subscriber identity module
SNSE	Supernode size enhanced
SSF	Service switching function
SCF	Service control function
SDF	Service data function
SRF	Service resource function
SMAS	Service management Application system
TS	Telecommunication Services
TMSI	Temporary mobile subscriber identity
TDMA	Time division multiple access
TRAU	Transcoding and Rate adaptation unit
UGW	USSD Gate Way
VS	Voucher Service
VLR	Visitor location Register