GSM (Global System for Mobile Communication):

- GSM is the most successful digital mobile telecommunication system in the world today. It is used by over 800 million people in more than 190 countries.
- In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies.
- To avoid this situation for a second generation fully digital system, the **Group Special Mobile (GSM)** was founded in 1982.
- This system was soon named the **Global System for Mobile Communications (GSM).**

GSM Services:

- GSM permits the integration of different voice and data services and the interworking with existing networks.
- GSM has defined three different categories of services:

- A reference model for GSM services. A **mobile station MS** is connected to the **GSM public land mobile network (PLMN)** via the Um interface. (GSM-PLMN is the infrastructure needed for the GSM network.)
- This network is connected to transit networks, e.g., **integrated services digital network (ISDN)** or traditional **public switched telephone network (PSTN)**.

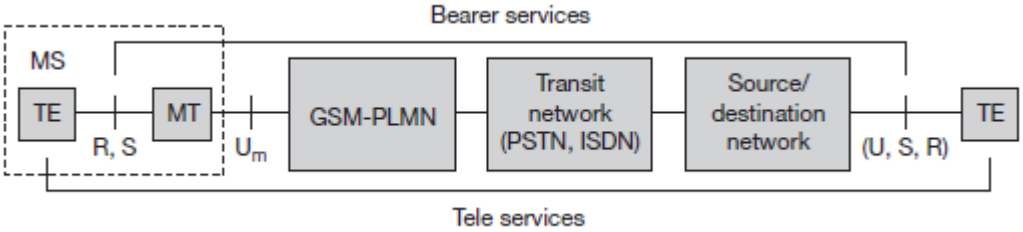


Fig: Bearer and tele services Reference model

Bearer services

- GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services.
- Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.
- **Transparent bearer services** only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur.

- The only mechanism to increase transmission quality is the use of **forward error correction (FEC)**.
- Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover.
- **Non-transparent bearer services** use protocols of layers two and three to implement error correction and flow control.
- These services use the transparent bearer services, adding a **radio link protocol (RLP)**. This protocol comprises mechanisms of **high-level data link control (HDLC)**.
- Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide.
- Data transmission can be full-duplex, synchronous with data rates of 1.2, 2.4, 4.8, and 9.6 Kbit/s or full-duplex, asynchronous from 300 to 9,600 bit/s.

Tele services

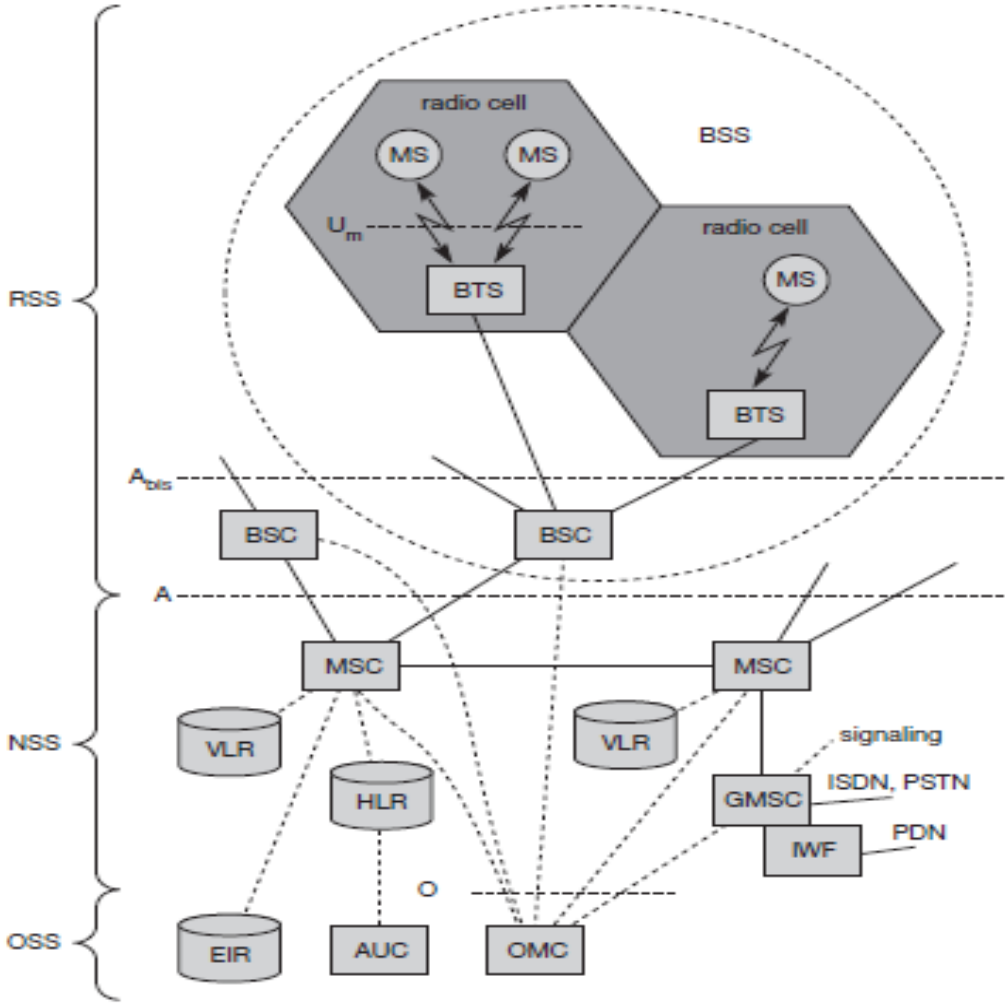
- GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN.
- However, as the main service is **telephony**, the primary goal of GSM was the provision of high-quality digital voice transmission, offering at least the typical bandwidth of 3.1 kHz of analog phone systems.
- Special codecs (coder/decoder) are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g., fax machines.
- Another service offered by GSM is the **emergency number**.
- A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters.
- The successor of SMS, the **enhanced message service (EMS)**, offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures, small images and ring tones in a standardized.
- EMS never really took off as the **multimedia message service (MMS)** was available.
- **MMS** offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc. and comes with mobile phones that integrate small cameras.

Supplementary services

- In addition to tele and bearer services, GSM providers can offer **supplementary services**.
- Similar to ISDN networks, these services offer various enhancements for the standard telephony service, and may vary from provider to provider.
- Typical services are user **identification**, call **redirection**, or **forwarding** of ongoing calls. Standard ISDN features such as **closed user groups** and **multiparty** communication may be available.

GSM System Architecture:

- GSM architecture consists of mainly 3-parts.
  - **RSS:** Radio Subsystem
  - **NSS:** Network and Switching Subsystem
  - **OSS:** Operation Subsystem



RSS: Radio Subsystem:

- The **radio subsystem (RSS)** comprises all radio specific entities, i.e.,
  - **Mobile stations (MS)**
  - **Base station subsystem (BSS)**.
- the connection between the RSS and the NSS via the **A interface** (solid lines) and the connection to the OSS via the **O interface** (dashed lines).

●**Base station subsystem (BSS)**:

- A GSM network comprises many BSSs, each controlled by a base station controller (BSC).
- The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.

- **Base transceiver station (BTS)**:
  - A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission.
  - A BTS can form a radio cell or, using sectorized antennas, several and is connected to MS via the **Um interface** (ISDN U interface for mobile use), and to the BSC via the **Abis interface**.
  - The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) and will be discussed in more detail below.
  - The Abis interface consists of 16 or 64 kbit/s connections.
  - A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- **Base station controller (BSC)**:
  - The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS.
  - The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS)**:
  - The MS comprises all user equipment and software needed for communication with a GSM network.
  - MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM.
  - While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself.
  - Device-specific mechanisms, e.g., theft protection, use the device specific IMEI.
  - Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a **personal identity number (PIN)**, a **PIN unblocking key (PUK)**, an **authentication key Ki**, and the **international mobile subscriber identity (IMSI)**.
  - The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM.
  - The MS stores dynamic information while logged onto the GSM system, such as, e.g., the **cipher key Kc** and the location information consisting of a **temporary mobile subscriber identity (TMSI)** and the **location area identification (LAI)**.

NSS: Network and Switching Subsystem:

- The "heart" of the GSM system is formed by the **network and switching subsystem (NSS)**.
- The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries.

- The NSS consists of the following switches and databases:

Mobile services switching center (MSC):

- MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system.
- Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as **PSTN** and **ISDN**
- Using additional **interworking functions (IWF)**, an MSC can also connect to **public data networks (PDN)** such as X.25.
- MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs.
- The **standard signaling system No. 7 (SS7)** is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls).
- Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

Home location register (HLR):

- The HLR is the most important database in a GSM system as it stores all user-relevant information.
- This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**.
- Dynamic information is also needed, e.g., the current **location area (LA)** of the MS, the **mobile subscriber roaming number (MSRN)**, the current VLR and MSC.
- As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network.
- HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.

Visitor location register (VLR):

- The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address).
- If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR.
- This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information.
- The typical use of HLR and VLR for user localization will be described in section 4.1.5. Some VLRs in existence, are capable of managing up to one million customers.

OSS: Operation Subsystem:

- The third part of a GSM system, the **operation subsystem (OSS)**, contains the necessary functions for network operation and maintenance.
- The OSS possesses network entities of its own and accesses other entities via SS7.

- **Operation and maintenance center (OMC)**:
  - The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
  - OMCs use the concept of **telecommunication management network (TMN)** as standardized by the ITU-T.
- **Authentication center (AuC)**:
  - As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission.
  - The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.
- **Equipment identity register (EIR)**:
  - The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network.
  - As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices.
  - The blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible.
  - The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

Radio Interfaces:

- The network structure is defined within the GSM standards. Additionally, each interface between the different elements of the GSM network is also defined.

1. ***Um interface***:The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signaling, a modified version of the ISDN LAPD, known as LAPDm is used.
2. ***Abis interface***: This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardized. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS.
3. ***A interface*** : The A interface is used to provide communication between the BSS and the MSC. The interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipments being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface.