**GSM - Addresses and Identifiers**

GSM treats the users and the equipment in different ways. Phone numbers, subscribers, and equipment identifiers are some of the known ones. There are many other identifiers that have been well-defined, which are required for the subscriber’s mobility management and for addressing the remaining network elements. Vital addresses and identifiers that are used in GSM are addressed below.

## International Mobile Station Equipment Identity (IMEI)

The International Mobile Station Equipment Identity (IMEI) looks more like a serial number which distinctively identifies a mobile station internationally. This is allocated by the equipment manufacturer and registered by the network operator, who stores it in the Entrepreneurs-in-Residence (EIR). By means of IMEI, one recognizes obsolete, stolen, or non-functional equipment.

Following are the parts of IMEI:

* **Type Approval Code (TAC)** : 6 decimal places, centrally assigned.
* **Final Assembly Code (FAC)** : 6 decimal places, assigned by the manufacturer.
* **Serial Number (SNR)** : 6 decimal places, assigned by the manufacturer.
* **Spare (SP)** : 1 decimal place.

Thus, IMEI = TAC + FAC + SNR + SP. It uniquely characterizes a mobile station and gives clues about the manufacturer and the date of manufacturing.

## International Mobile Subscriber Identity (IMSI)

Every registered user has an original International Mobile Subscriber Identity (IMSI) with a valid IMEI stored in their Subscriber Identity Module (SIM).

IMSI comprises of the following parts:

* **Mobile Country Code (MCC)** : 3 decimal places, internationally standardized.
* **Mobile Network Code (MNC)** : 2 decimal places, for unique identification of mobile network within the country.
* **Mobile Subscriber Identification Number (MSIN)** : Maximum 10 decimal places, identification number of the subscriber in the home mobile network.

## Mobile Subscriber ISDN Number (MSISDN)

The authentic telephone number of a mobile station is the Mobile Subscriber ISDN Number (MSISDN). Based on the SIM, a mobile station can have many MSISDNs, as each subscriber is assigned with a separate MSISDN to their SIM respectively.

Listed below is the structure followed by MSISDN categories, as they are defined based on international ISDN number plan:

* **Country Code (CC)** : Up to 3 decimal places.
* **National Destination Code (NDC)** : Typically 2-3 decimal places.
* **Subscriber Number (SN)** : Maximum 10 decimal places.

## Mobile Station Roaming Number (MSRN)

Mobile Station Roaming Number (MSRN) is an interim location dependent ISDN number, assigned to a mobile station by a regionally responsible Visitor Location Register (VLA). Using MSRN, the incoming calls are channelled to the MS.

The MSRN has the same structure as the MSISDN.

* **Country Code (CC)** : of the visited network.
* **National Destination Code (NDC)** : of the visited network.
* **Subscriber Number (SN)** : in the current mobile network.

## Location Area Identity (LAI)

Within a PLMN, a Location Area identifies its own authentic Location Area Identity (LAI). The LAI hierarchy is based on international standard and structured in a unique format as mentioned below:

* **Country Code (CC)** : 3 decimal places.
* **Mobile Network Code (MNC)** : 2 decimal places.
* **Location Area Code (LAC)** : maximum 5 decimal places or maximum twice 8 bits coded in hexadecimal (LAC < FFFF).

## Temporary Mobile Subscriber Identity (TMSI)

Temporary Mobile Subscriber Identity (TMSI) can be assigned by the VLR, which is responsible for the current location of a subscriber. The TMSI needs to have only local significance in the area handled by the VLR. This is stored on the network side only in the VLR and is not passed to the Home Location Register (HLR).

Together with the current location area, the TMSI identifies a subscriber uniquely. It can contain up to 4 × 8 bits.

## Local Mobile Subscriber Identity (LMSI)

Each mobile station can be assigned with a Local Mobile Subscriber Identity (LMSI), which is an original key, by the VLR. This key can be used as the auxiliary searching key for each mobile station within its region. It can also help accelerate the database access. An LMSI is assigned if the mobile station is registered with the VLR and sent to the HLR. LMSI comprises of four octets (4x8 bits).

## Cell Identifier (CI)

Using a Cell Identifier (CI) (maximum 2 × 8) bits, the individual cells that are within an LA can be recognized. When the Global Cell Identity (LAI + CI) calls are combined, then it is uniquely defined.

**GSM - Operations**

Once a Mobile Station initiates a call, a series of events takes place. Analyzing these events can give an insight into the operation of the GSM system.

## Mobile Phone to Public Switched Telephone Network (PSTN)

When a mobile subscriber makes a call to a PSTN telephone subscriber, the following sequence of events takes place:

* The MSC/VLR receives the message of a call request.
* The MSC/VLR checks if the mobile station is authorized to access the network. If so, the mobile station is activated. If the mobile station is not authorized, then the service will be denied.
* MSC/VLR analyzes the number and initiates a call setup with the PSTN.
* MSC/VLR asks the corresponding BSC to allocate a traffic channel (a radio channel and a time slot).
* The BSC allocates the traffic channel and passes the information to the mobile station.
* The called party answers the call and the conversation takes place.
* The mobile station keeps on taking measurements of the radio channels in the present cell and the neighbouring cells and passes the information to the BSC. The BSC decides if a handover is required. If so, a new traffic channel is allocated to the mobile station and the handover takes place. If handover is not required, the mobile station continues to transmit in the same frequency.

## PSTN to Mobile Phone

When a PSTN subscriber calls a mobile station, the following sequence of events takes place:

* The Gateway MSC receives the call and queries the HLR for the information needed to route the call to the serving MSC/VLR.
* The GMSC routes the call to the MSC/VLR.
* The MSC checks the VLR for the location area of the MS.
* The MSC contacts the MS via the BSC through a broadcast message, that is, through a paging request.
* The MS responds to the page request.
* The BSC allocates a traffic channel and sends a message to the MS to tune to the channel. The MS generates a ringing signal and, after the subscriber answers, the speech connection is established.
* Handover, if required, takes place, as discussed in the earlier case.

To transmit the speech over the radio channel in the stipulated time, the MS codes it at the rate of 13 Kbps. The BSC transcodes the speech to 64 Kbps and sends it over a land link or a radio link to the MSC. The MSC then forwards the speech data to the PSTN. In the reverse direction, the speech is received at 64 Kbps at the BSC and the BSC transcodes it to 13 Kbps for radio transmission.

GSM supports 9.6 Kbps data that can be channelled in one TDMA timeslot. To supply higher data rates, many enhancements were done to the GSM standards (GSM Phase 2 and GSM Phase 2+).

**GSM - Security and Encryption**

## Mobile Station Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

**GSM – Billing**

## Telephony Service

These services can be charged on per call basis. The call initiator has to pay the charges, and the incoming calls are nowadays free. A customer can be charged based on different parameters such as:

* International call or long distance call.
* Local call.
* Call made during peak hours.
* Call made during night time.
* Discounted call during weekends.
* Call per minute or per second.
* Many more other criteria can be designed by a service provider to charge their customers.

## SMS Service

Most of the service providers charge their customer's SMS services based on the number of text messages sent. There are other prime SMS services available where service providers charge more than normal SMS charge. These services are being availed in collaboration of Television Networks or Radio Networks to demand SMS from the audiences.

Most of the time, the charges are paid by the SMS sender but for some services like stocks and share prices, mobile banking facilities, and leisure booking services, etc. the recipient of the SMS has to pay for the service.

## GPRS Services

Using GPRS service, you can browse, play games on the Internet, and download movies. So a service provider will charge you based on the data uploaded as well as data downloaded on your mobile phone. These charges will be based on per Kilo Byte data downloaded/uploaded.

Additional parameter could be a QoS provided to you. If you want to watch a movie, then a low QoS may work because some data loss may be acceptable, but if you are downloading a zip file, then a single byte loss will corrupt your complete downloaded file.

Another parameter could be peak and off peak time to download a data file or to browse the Internet.

## Supplementary Services

Most of the supplementary services are being provided based on monthly rental or absolutely free. For example, call waiting, call forwarding, calling number identification, and call on hold are available at zero cost.

Call barring is a service, which service providers use just to recover their dues, etc., otherwise this service is not being used by any subscriber.

Call conferencing service is a form of simple telephone call where the customers are charged for multiple calls made at a time. No service provider charges extra charge for this service.

Closed User Group (CUG) is very popular and is mainly being used to give special discounts to the users if they are making calls to a particular defined group of subscribers.

Advice of Charge (AoC) can be charged based on number of queries made by a subscriber.