

Introduction to the GSM standard

The **GSM** (*Global System for Mobile communications*) network is, at the start of the 21st century, the most commonly used mobile telephony standard in Europe. It is a so-called "second generation" (2G) standard because, unlike the first generation of portable telephones, communications occur in an entirely digital mode.

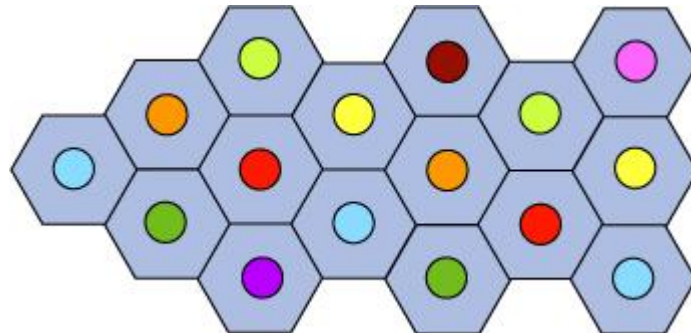
Called "Groupe Spécial Mobile" when first standardised in 1982, it became an international standard called "Global System for Mobile communications" in 1991.

In Europe, the GSM standard uses the 900 MHz and 1800 MHz frequency bands. In the United States, however, the frequency band used is the 1900 MHz band. For this reason, portable telephones that are able to operate in both Europe and the United States are called **tri-band** while those that operate only in Europe are called **bi-band**.

The GSM standard allows a maximum throughput of 9.6 kbps, which allows transmission of voice and low-volume digital data, for example text messages (**SMS**, for *Short Message Service*) or multimedia messages (**MMS**, for *Multimedia Message Service*).

The concept of cellular network

Mobile telephone networks are based on the concept of **cells**, circular zones that overlap to cover a geographical area.



Cellular networks are based on the use of a central transmitter-receiver in each cell, called a "**base station**" (or *Base Transceiver Station*, written **BTS**).

The smaller the radius of a cell, the higher the available bandwidth. So, in highly populated urban areas, there are cells with a radius of a few hundred metres, while huge cells of up to thirty kilometres provide coverage in rural areas.

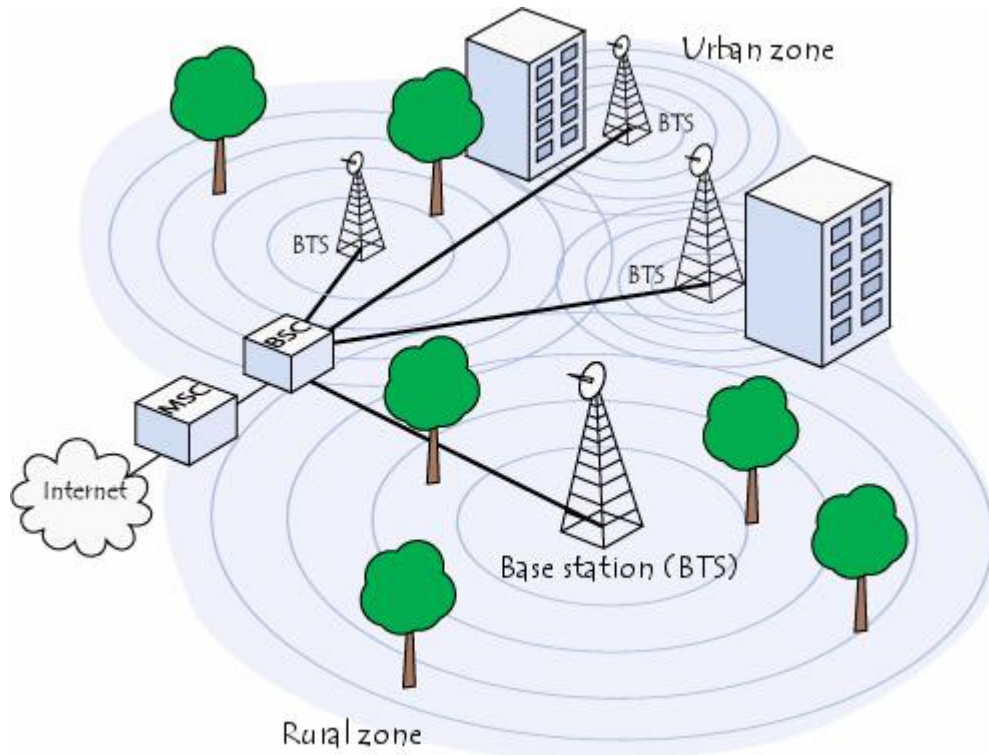
In a cellular network, each cell is surrounded by 6 neighbouring cells (which is why a cell is generally drawn as a hexagon). To avoid interference, adjacent cells cannot use the same frequency. In practice, two cells using the same frequency range must be separated by a distance of two to three times the diameter of the cell.

Architecture of the GSM network

In a GSM network, the user terminal is called a **mobile station**. A mobile station is made up of a **SIM** (*Subscriber Identity Module*) card allowing the user to be uniquely identified, and a mobile terminal, in other words the user device (normally a portable telephone).

The terminals (devices) are identified by a unique 15-digit identification number called **IMEI** (*International Mobile Equipment Identity*). Each SIM card also has a unique (and secret) identification number called **IMSI** (*International Mobile Subscriber Identity*). This code can be protected using a 4-digit key called a *PIN code*.

The SIM card therefore allows each user to be identified independently of the terminal used during communication with a base station. Communications between a mobile station and a base station occur via a radio link, generally called an **air interface** (or more rarely *Um interface*).



All the base stations of a cellular network are connected to a **base station controller** (written **BSC**), which is responsible for managing distribution of the resources. The system consisting of the base station controller and its connected base stations is called the **Base Station Subsystem (BSS)**.

Finally, the base station controllers are themselves physically connected to the **Mobile Switching Centre (MSC)**, managed by the telephone network operator, which connects them to the public telephone network and the Internet. The MSC belongs to a **Network Station Subsystem (NSS)**, which is responsible for managing user identities, their location and establishment of communications with other subscribers.

The MSC is generally connected to databases that provide additional functions:

- The **Home Location Register** (written **HLR**): a database containing information (geographic position, administrative information, etc.) on the subscribers registered in the area of the switch (MSC).
- The **Visitor Location Register** (written **VLR**): a database containing information on users other than the local subscribers. The VLR retrieves the data on a new user from the HLR of the user's subscriber zone. The data are maintained as long as the user is in the zone and are deleted when the user leaves or after a long period of inactivity (terminal off).
- The **Equipment Identify Register** (written **EIR**): a database listing the mobile terminals.

- The **Authentication Centre (AUC)**: responsible for verifying user identities.

The cellular network formed in this way is designed to support mobility via management of *handovers* (movements from one cell to another).

Finally, GSM networks support the concept of **roaming**: movement from one operator network to another.

SIM Card

A SIM card contains the following information:

- Subscriber telephone number (MSISDN)
- International subscriber number (**IMSI, international mobile subscriber identity**)
- **State of the SIM card**
- **Service code (operator)**
- **Authentication key**
- **PIN (*Personal Identification Code*)**
- **PUK (*Personal Unlock Code*)**