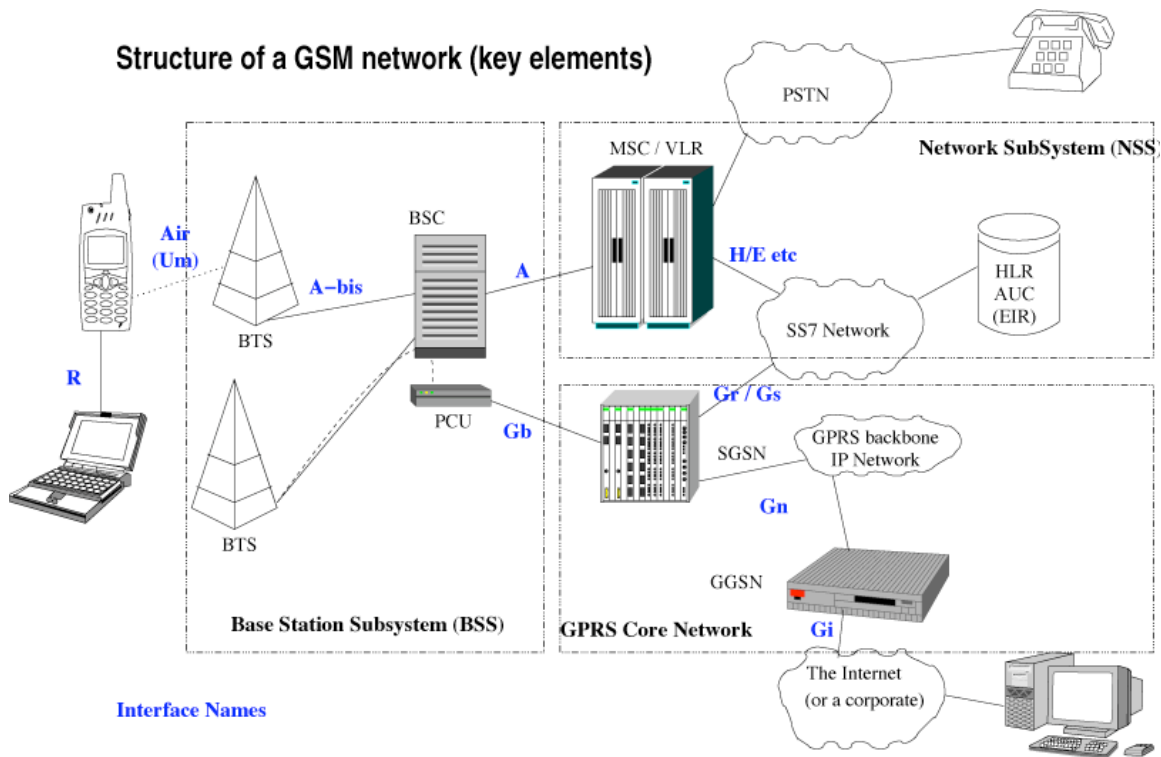


GSM Network Information/Subscriber identity/ GSM Security Information

The network behind the GSM system seen by the customer is large and complicated in order to provide all of the services which are required. It is divided into a number of sections and these are each covered in separate articles.

0. the **Base Station Subsystem** (the **base stations** and their controllers).
0. the **Network and Switching Subsystem** (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
0. the **GPRS Core Network** (the optional part which allows packet based Internet connections).
0. all of the elements in the system combine to produce many **GSM services** such as voice calls and **SMS**.



Subscriber identity module

One of the key features of GSM is the [Subscriber Identity Module \(SIM\)](#), commonly known as a SIM card. The SIM is a detachable [smart card](#) containing the user's subscription information and phonebook. This allows the user to retain his or her information after switching handsets.

Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as [SIM locking](#), and is illegal in some countries.

In the [United States](#), Europe and Australia, many operators lock the mobiles they sell. This is done because the price of the mobile phone is typically [subsidised](#) with revenue from subscriptions and operators want to try to avoid subsidising competitor's mobiles. A subscriber can usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or make use of ample software and websites available on the Internet to unlock the handset themselves. While most web sites offer the unlocking for a fee, some do it for free. The locking applies to the handset, identified by its [International Mobile Equipment Identity \(IMEI\)](#) number, not to the account (which is identified by the [SIM](#) card). It is always possible to switch to another (non-locked) handset.

Some providers will unlock the phone for free if the customer has held an account for a certain period. Third party unlocking services exist that are often quicker and lower cost than that of the operator. In most countries removing the lock is legal. Cingular provides free unlock services to its customer after 3 months of subscriptions.

In countries like India, Belgium, etc., all phones are sold unlocked. However, in Belgium, it is unlawful for operators there to offer any form of subsidy on the phone's price.

GSM security

GSM was designed with a moderate level of security. The system was designed to authenticate the subscriber using [shared-secret cryptography](#). Communications between the subscriber and the base station can be encrypted. The development of [UMTS](#) introduces an optional [USIM](#), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user - whereas GSM only authenticated the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

GSM uses several cryptographic algorithms for security. The [A5/1](#) and [A5/2 stream ciphers](#) are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. A large security advantage of GSM over earlier systems is that the Ki, the crypto variable stored on the [SIM](#) card that is the key to any GSM ciphering algorithm, is never sent over the air interface. Serious weaknesses have been found in both algorithms, and it is possible to break A5/2 in real-time in a [ciphertext-only attack](#). The system supports multiple algorithms so operators may replace that cipher with a stronger one.

Source:

<http://en.wikipedia.org/wiki/GSM>