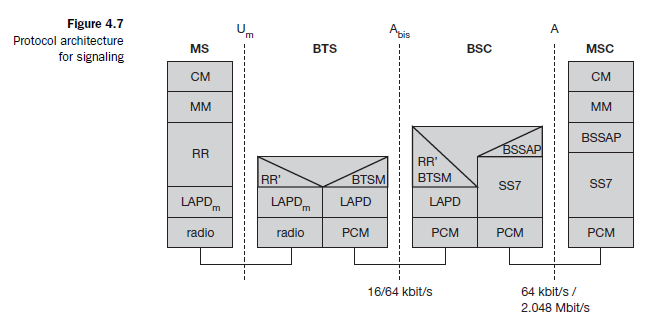
**Services of GSM – Refer Book**

**GSM security – Refer Book**

**GSM Architecture – Refer Book**

**Protocol Architecture of GSM:**

Figure 4.7 shows the protocol architecture of GSM with signaling protocols, interfaces, as well as the entities



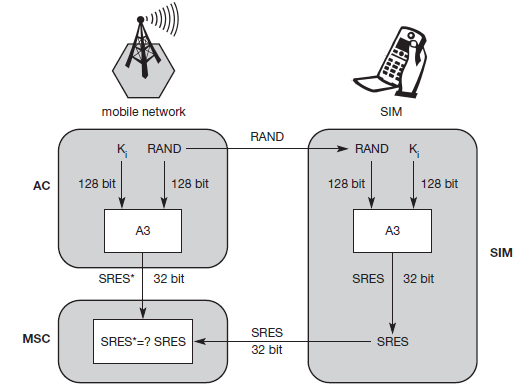
**GSM Security**

* GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS).
* The SIM stores personal, secret data and is protected with a PIN against unauthorized use.
* Three algorithms have been specified to provide security services in GSM.
* **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**.
* In the GSM standard only algorithm A5 was publicly available, whereas A3 and A8 were secret, but standardized with open interfaces.
* Both A3 and A8 are no longer secret, but were published on the internet in 1998.
* This demonstrates that security by obscurity does not really work.
* Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AuC and can be proprietary.
* Only A5 which is implemented in the devices has to be identical for all providers.

The security services offered by GSM are explained below:

**Authentication**

* Before a subscriber can use any service from the GSM network, he or she must be authenticated.
* Authentication is based on the SIM, which stores the **individual authentication key Ki**, the **user identification IMSI**, and the algorithm used for authentication **A3**.
* Authentication uses a challenge-response method: the access control AC generates a random number **RAND** as challenge, and the SIM within the MS answers with **SRES** as response(signed response).



**Figure shows subscriber authentication**

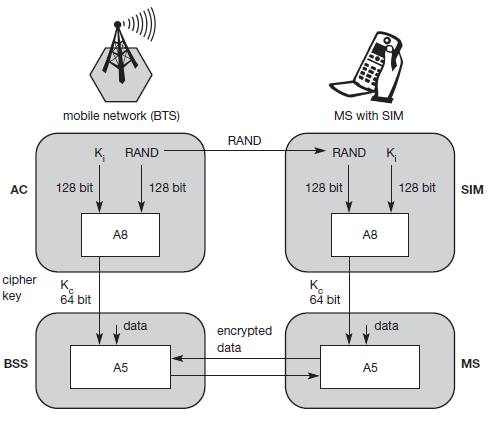
* The AuC performs the basic generation of random values RAND, signed responses SRES, and

cipher keys Kc for each IMSI, and then forwards this information to the HLR.

* The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR.
* For authentication, the VLR sends the random value RAND to the SIM.
* Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called A3.
* The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.

● **Confidentiality:** All user-related data is encrypted.

* After authentication, BTS and MS apply encryption to voice, data, and signaling.
* To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.
* After authentication, MS and BSS can start using encryption by applying the cipher key Kc (the precise location of security functions for encryption, BTS and/or BSC are vendor dependent).
* Kc is generated using the individual key Ki and a random value by applying the algorithm A8.
* Note that the SIM in the MS and the network both calculate the same Kc based on the random value RAND.
* The key Kc itself is not transmitted over the air interface.



* MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc.
* As Figure shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping.
* However, the publication of A3 and A8 on the internet showed that in certain implementations 10 of the 64 bits are always set to 0, so that the real length of the key is thus only 54 consequently, the encryption is much weaker.

● **Anonymity:**

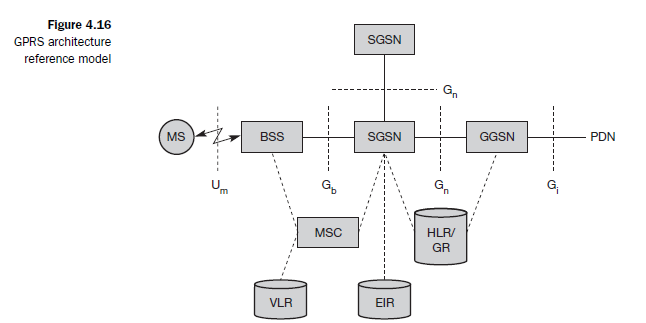
* A GSM network protects against someone tracking the location of a user or identifying calls made to (or from) the user by eavesdropping on the radio path.
* The anonymity of the subscriber on the radio access link in the GSM network is achieved by allocating Temporary Mobile subscriber identify (TMSIs) instead of permanent identities.
* This helps to protect against tracing a user’s location and obtaining information about a user’s calling pattern.

**GPRS**

* GPRS when integrated with GSM, significantly improves and simplifies internet access.
* It transfers data packet from GSM mobile stations to external packet data network (PDN).
* GSM uses a billing system based on the time(duration) of the connection, whereas GPRS uses a billing system based on the amount of transmitted data rather than the duration of the connection.
* So, users can remain continuously connected to the system, and yet get changed only for the amount of transmitted data.
* The main benefit for users of GPRS is the ‘always on’ characteristic – no connection has to be set up prior to data transfer.
* In GPRS no connection is setup prior to data transfer.

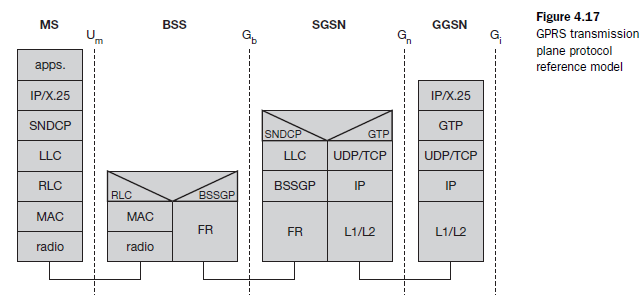
**GPRS Architecture:**

* The **GPRS architecture** introduces two new network elements, which are called **GPRS support nodes (GSN)** and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined (see Figure 4.16).
* The **gateway GPRS support node (GGSN)** is the interworking unit between the GPRS network and external **packet data networks (PDN)**. This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation.
* The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).



* The other new element is the **serving GPRS support node (SGSN)** which supports the MS via the Gb interface.
* The SGSN, for example, requests user addresses from the **GPRS register (GR)**, keeps track of the individual MSs’ location, is responsible for collecting billing information (e.g., counting bytes), and performs several security functions such as access control.
* The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC.
* The GR, which is typically a part of the HLR, stores all GPRS-relevant data. GGSNs and SGSNs can be compared with home and foreign agents, respectively, in a mobile IP network (
* As shown in Figure 4.16, packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS.
* The MSC, which is responsible for data transport in the traditional circuit-switched GSM, is only used for signaling in the GPRS scenario.
* Before sending any data over the GPRS network, an MS must attach to it, following the procedures of the **mobility management**.
* The attachment procedure includes assigning a temporal identifier, called a **temporary logical link identity (TLLI)**, and a **ciphering key sequence number (CKSN)** for data encryption.

**Figure 4.17 shows the protocol architecture of the transmission plane for GPRS.**



* All data within the GPRS backbone, i.e., between the GSNs, is transferred using the **GPRS tunnelling protocol (GTP)**.
* GTP can use two different transport protocols, either the reliable **TCP** (needed for reliable transfer of X.25 packets) or the non-reliable **UDP** (used for IP packets).
* The network protocol for the GPRS backbone is **IP** (using any lower layers). To adapt to the different characteristics of the underlying networks, the **subnetwork dependent convergence protocol (SNDCP)** is used between an SGSN and the MS.
* On top of SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa.
* To achieve a high reliability of packet transfer between SGSN and MS, a special LLC is used,

which comprises ARQ and FEC mechanisms for PTP (and later PTM) services.

* A **base station subsystem GPRS protocol (BSSGP)** is used to convey routing and QoS-related information between the BSS and SGSN.
* BSSGP does not perform error correction and works on top of a **frame relay (FR)** network.
* Finally, radio link dependent protocols are needed to transfer data over the Um interface.
* The **radio link protocol (RLC)** provides a reliable link, while the **MAC** controls access with signaling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels.
* The **radio interface** at Um needed for GPRS does not require fundamental changes compared to standard GSM (Brasche, 1997), (ETSI, 1998d).

-------------------------------------------------------------------------------------------------------------