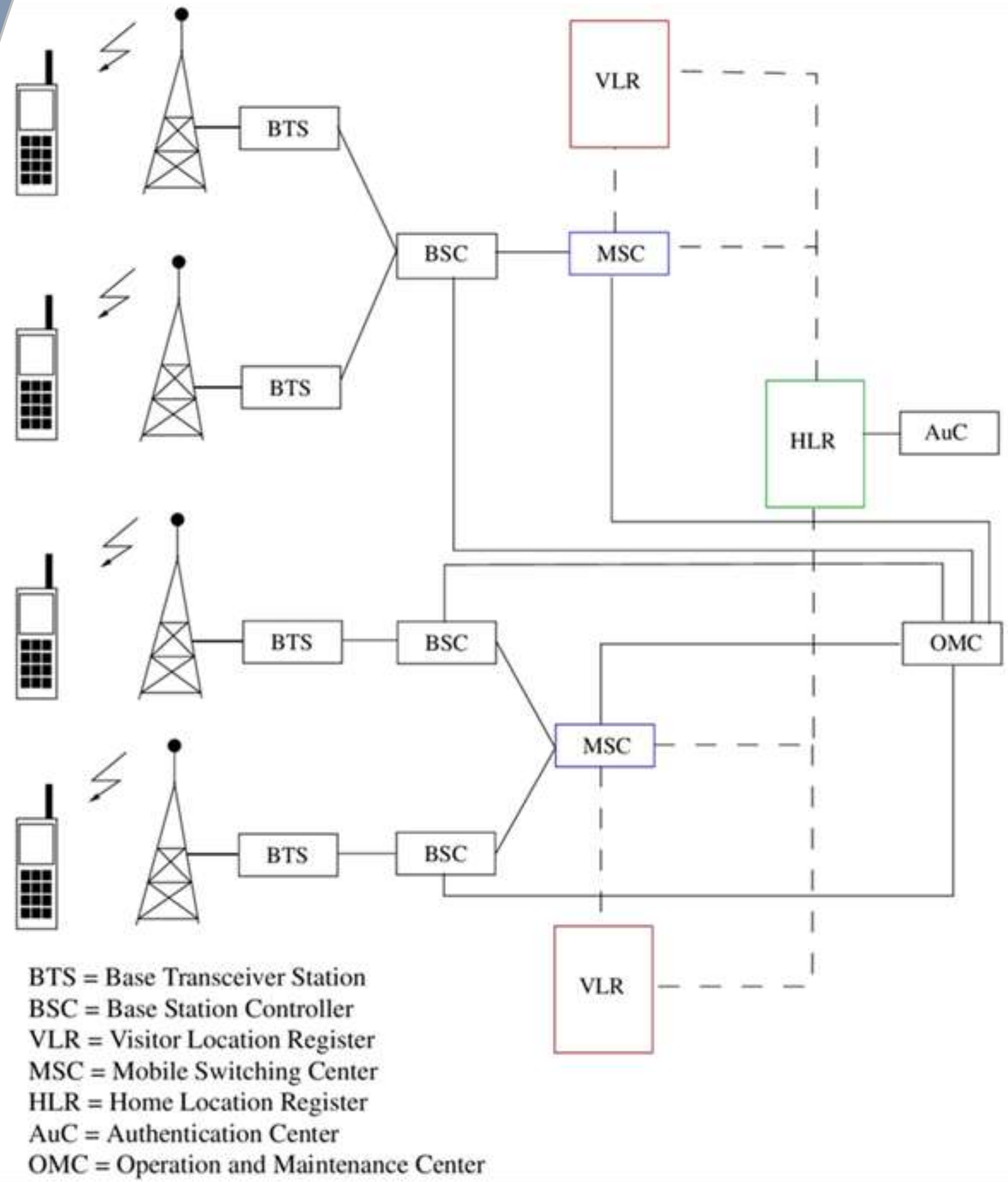
# GSM Security Features

By:

S. Anitha



BTS = Base Transceiver Station
BSC = Base Station Controller
VLR = Visitor Location Register
MSC = Mobile Switching Center
HLR = Home Location Register
AuC = Authentication Center
OMC = Operation and Maintenance Center

# GSM security features:

- The main goal for GSM is to secure the public switched telephone network(PSTN) and to prevent phone cloning.
- It was built to prevent air-interface communication because it allows a number of potential threats of eavesdropping the transmissions.
- It contain mainly three security aspects of GSM, there are
  - Subscriber identity authentication.
  - User and Signaling data confidentiality.
  - Subscriber identity confidentiality.
- The design of the authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel, because it along with subscriber authentication key(ki)
- The actual conversation are encrypted using a temporary, randomly generated ciphering key(kc).

- The Mobile station identifiers itself by means of the temporary mobile subscriber identity(TMSI), where is issued by the network and may be changed periodically for additional security.
- The security mechanisms GSM are implemented in three different system elements,
  - SIM
  - GSM headset or MS
  - The GSM network

**SIM** : Contains, individual subscriber authentication key, the ciphering key generating algorithms(A8), authentication algorithm(A3) as well as a personal identification number(PIN).

**GSM headset** : MS contains the ciphering algorithm(A5). All the algorithm(A8,A5 and A3) are present in the GSM network as well.

**GSM network :** The authentication center (AuC), part of the operation and maintenance subsystem (OMS) of this. This individual subscriber authentication key for each user are stored in the AuC, as well as A3 & A8 algorithm.

- Within the GSM network, the security information is distributed among the AuC, HLR, VLR.

- This AuC is responsible for generating the sets of triplets (RAND, SRES, authentication key) which is stored HLR and VLR for subsequent use in the authentication and encryption process.

**SUBSCRIBER IDENTITY AUTHENTICATION :**

- It is core of GSM security system.
- It is used to enable the fixed network to authenticate the identity of mobile subscriber and to establish and manage the encrypted keys needed to provide the confidentiality services.
- The service must be supported by all network and mobiles. Authentication is initiated by the fixed network and is based upon a simple challenge – response protocol.
- When a mobile station needed authenticate to a serving network one of the following situation may occur, there are described in cases,
- Case 1 : The visiting call belong to a network which the MS has not visiting in the (recent) past. It this case, it presents its IMSI to the serving network MSC finds out the visiting MS's home authentication vector, which is stored in the serving n/w VLR together with the IMSI of the MS.

- Case 2 : The visiting call is belong to the home network to which the MS belongs or to a n/w to which the MS has already authenticated in the(recent) past. If the authentication vector of the mobile station is still available in VLR and there are some triplets left unused, then the HLR of the visiting MS does not need to be contacted.
- In both cases, an unused random challenge RAND is sent to the MS. The MS compute a response SRES to RAND using a one-way function(A3) under control of a subscriber authentication key (Ki).
- The key K is unique to the subscriber and is shared only by the subscriber and authentication center (AuC), which serves the subscriber's home network.
- The value SRES computed by the MS is signaled to network, where it is computed with a precomputed value.
- If the two values of SRES argee the Mobile subscriber has been authenticated, and the call is allowed to proceed. If the value are different then access is denied.

- The A3 algorithm takes the random challenges RAND and the secret key K and generates SRES output. Both RAND and K are 128bits long and output SRES is 32bits long.
- The same mechanisms is also to establish a cipher key K for encrypting user and signaling data to the radio path. A8 algorithm generate the session key K from the RAND and secret key K.
- A8 algorithm takes these two 128 bits as a input and generates a 64 bits as output from them.

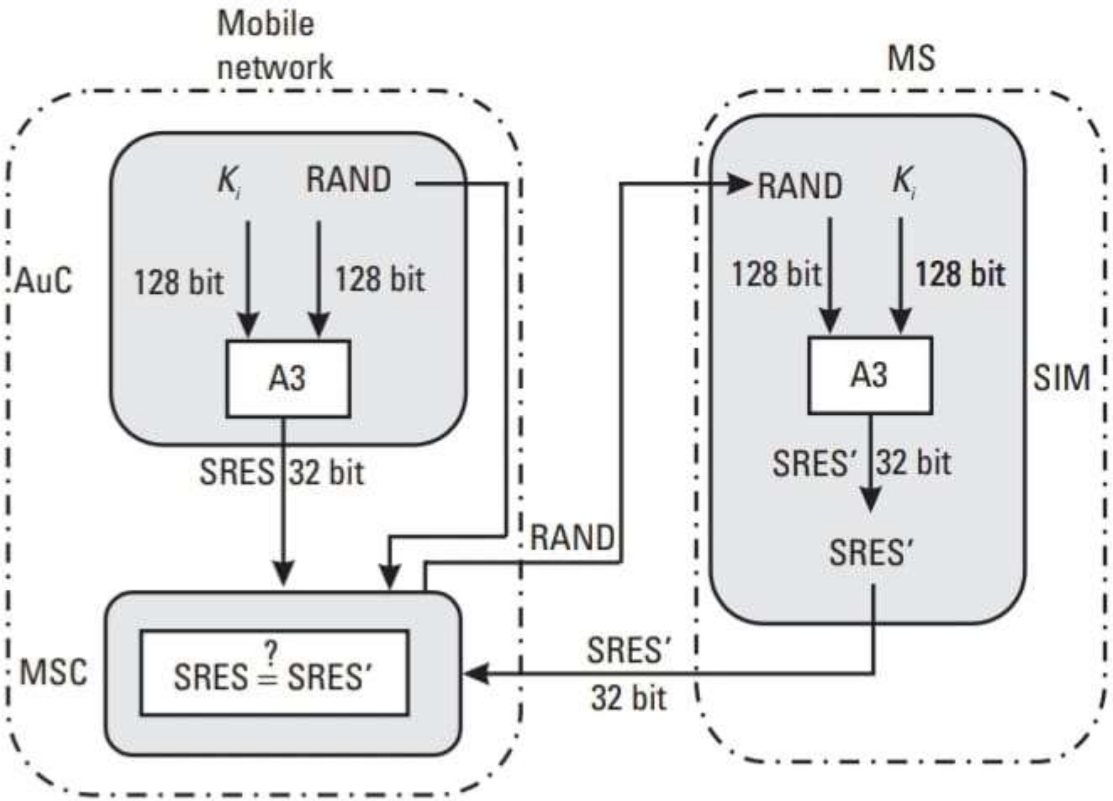


**Figure 5.3** GSM subscriber identity authentication scheme.