INTRODUCTION TO GLOBAL SYSTEM FOR MOBILE COMMUNICATION - ARCHITECTURE & SECURITY

EEEN 464 – DIGITAL COMMUICATION

Friday, 13 March 2026

SECTION IN THE SYLLABUS

General architecture and interfaces of cellular system and the PSTN and Internet networks: BTS, MSC, Internetworking, user registers etc.

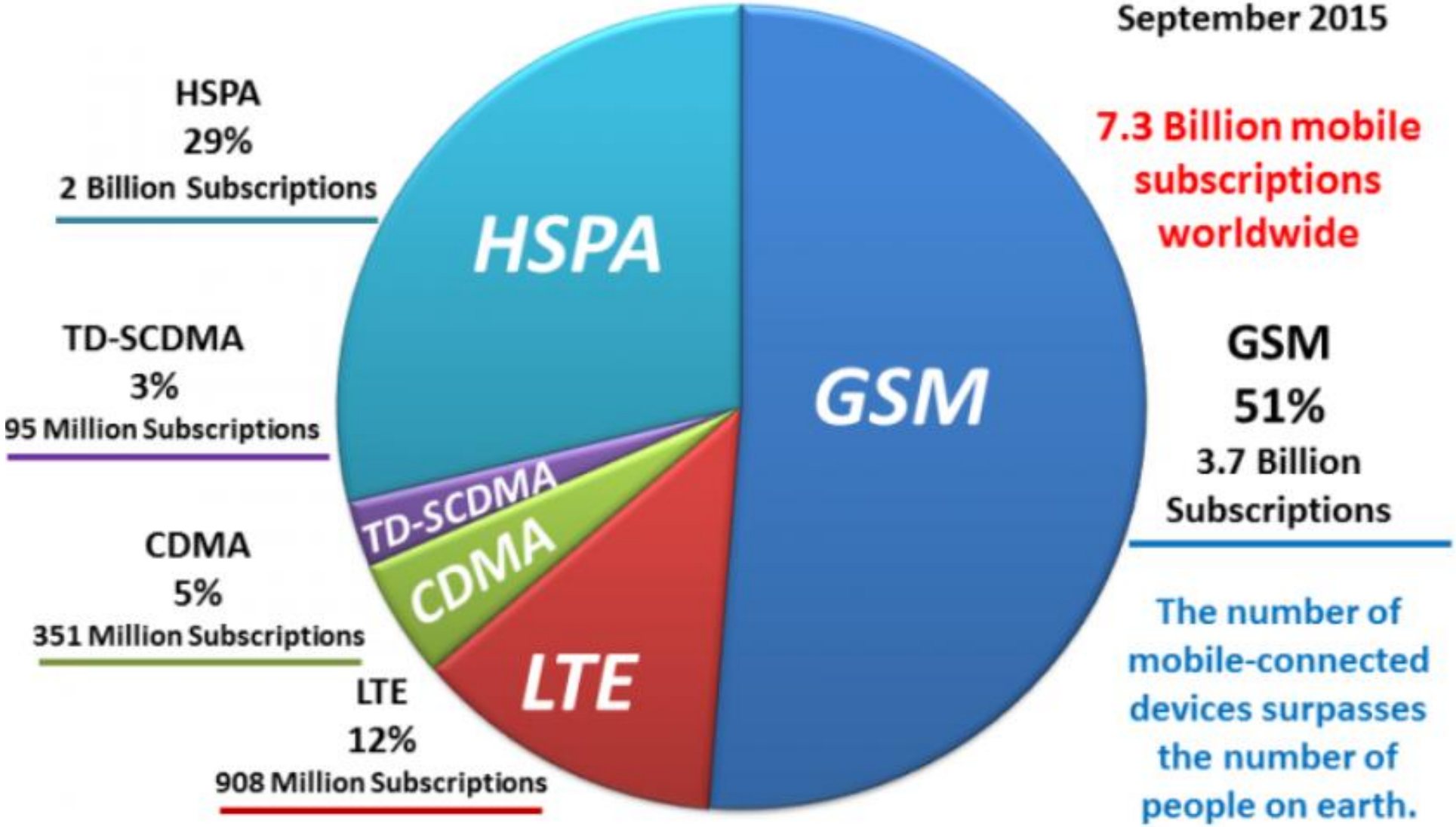
GROWTH OF GSM

1. Global System for Mobile Communications (GSM) was for along time the most popular mobile phone system in the world, accounting for 70% of the world's digital mobile phones.

2. By 2014, there were 3.7Billion GSM mobile phones in use in over 168 countries.

3. One of GSM's key strength is its international roaming capability, giving consumers a seamless service in over 168 countries.

GLOBILE MOBILE SUBSCRIBER & MAKET SHARE BY TECHNOLOGY - 2015



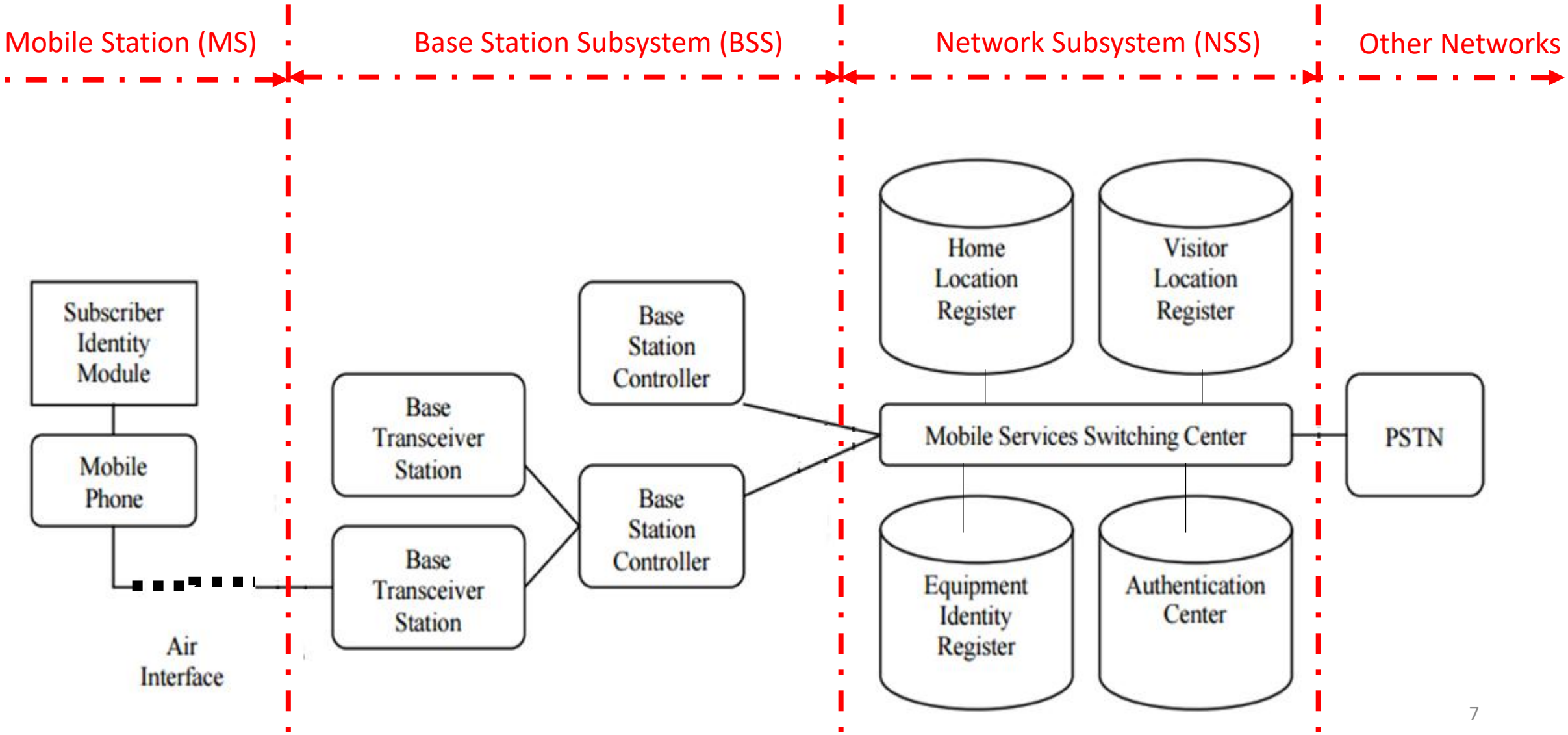
BRIEF HISTORY OF GSM

1. **1982:** The European Conference of Post and Telecommunications Administrations (CEPT) formed a group called Group Spéciale Mobile (GSM) to develop a pan-European cellular system to replace the many existing incompatible cellular systems.
2. **1987:** The GSM Memorandum of Understanding (MoU) by prospective telecommunication operators, agreeing to implement cellular networks, based on the GSM specifications.
3. **1991:** Group Spéciale Mobile (GSM) was renamed to Global System for Mobile Communications (GSM).
4. **1992:** The first commercial GSM service was launched.

KEY FEATURES OF GSM

1. **International Roaming** – using a single subscriber numbering systems worldwide (IMSDN).
2. **Superior speech quality** better than AMPS and DAMPS.
3. **High level of security** - user's information and communication are safe and secure
4. Universal and Inexpensive Mobile handsets
5. **Longer talk** time which gives doubled per battery life
6. Handles higher volume of calls at any one time compared to analogue networks
7. **Introduction of new services** call waiting, call forwarding, Short Message Service (SMS), GSM Packet Radio Service (GPRS)
8. **Digital compatibility** - easily interfaces with other digital networks i.e. Integrated Services Digital Network (ISDN)

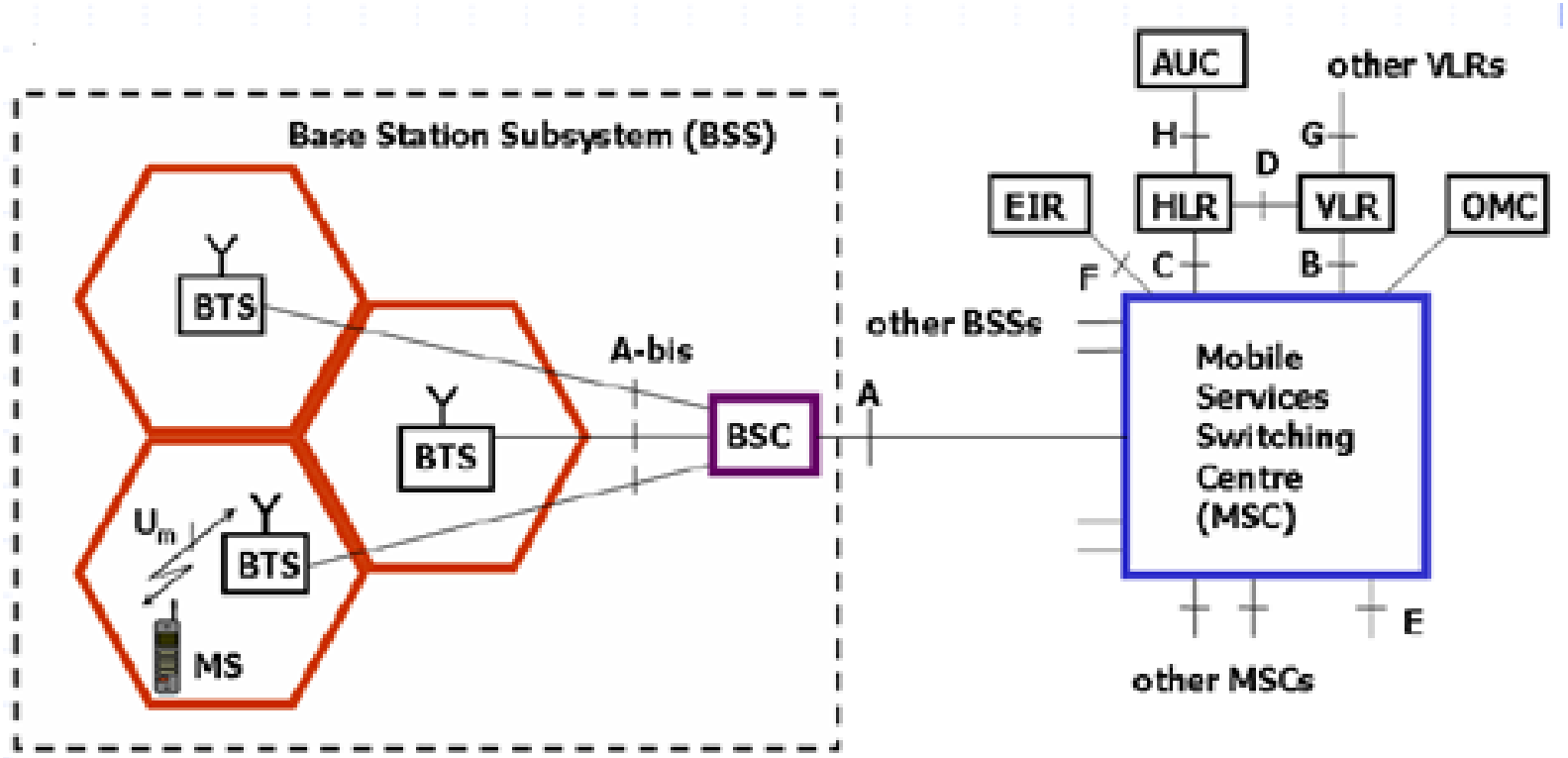
GSM ARCHITECTURE (1)



GSM ARCHITECTURE - INTERFACES

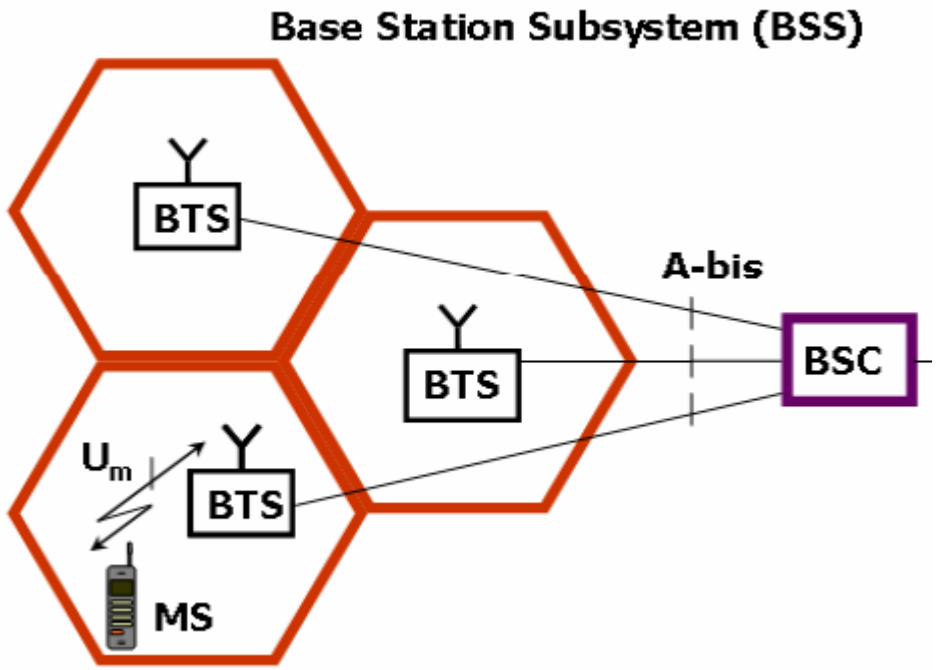
GSM has 9 physical and logical interfaces as follows:

1. **Um:** Connects the MS to the BTS
2. **A-bis:** Connects BTS to BSC
3. **A:** Connects BSC to MSC
4. **B:** Connects MSC to VLR
5. **C :** Connects MSC to HLR
6. **D:** Connects HLR to VLR
7. **E:** Connects MSC to other MSCs
8. **H:** Connects HLR to AUC
9. **G:** Connects VLR to other VLRs



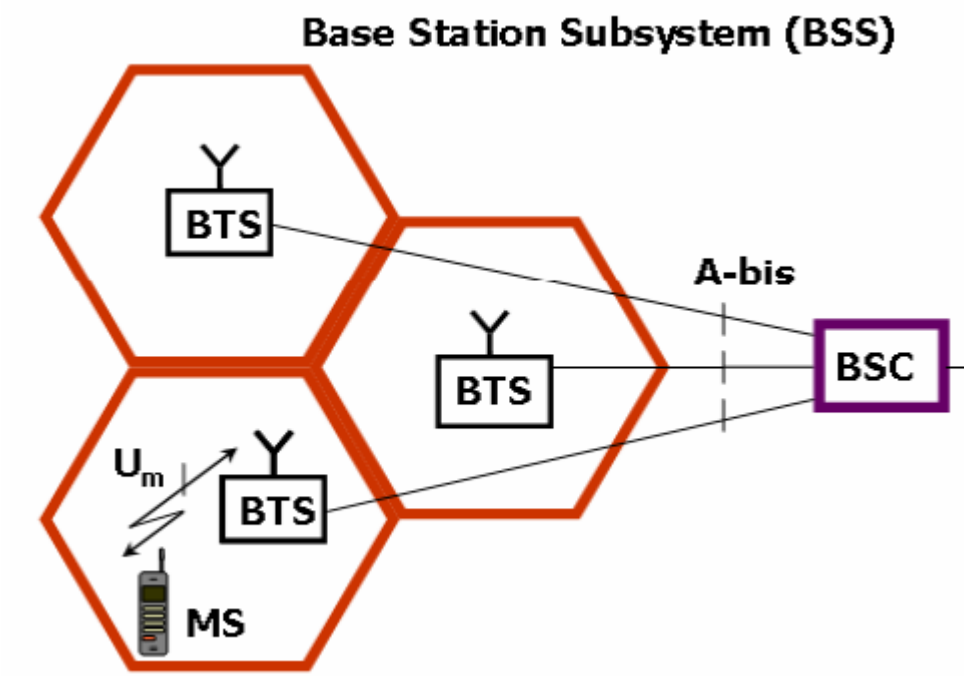
BASE TRANSCEIVER STATION (BTS)

1. The Base Transceiver Station (BTS) manages the radio interface to the mobile station by performing functions such as:
   a) communication set-up and monitoring
   b) Channel Encryption;
   c) hand-over functions
2. The BTS is a radio equipment serving each cell in the network.
3. A group of BTSs are controlled by a single BSC.



BASE STATION CONTROLER (BSC)

1. Base Station Controller (BSC) provides the control functions and physical links between the MSC and BTS.
2. It is a high-capacity switch that provides functions such as
   a) handover,
   b) cell configuration, and
   c) Control of radio frequency (RF) power levels in base transceiver stations.
3. A number of BSCs are served by an MSC.



POWER MANAGEMENT

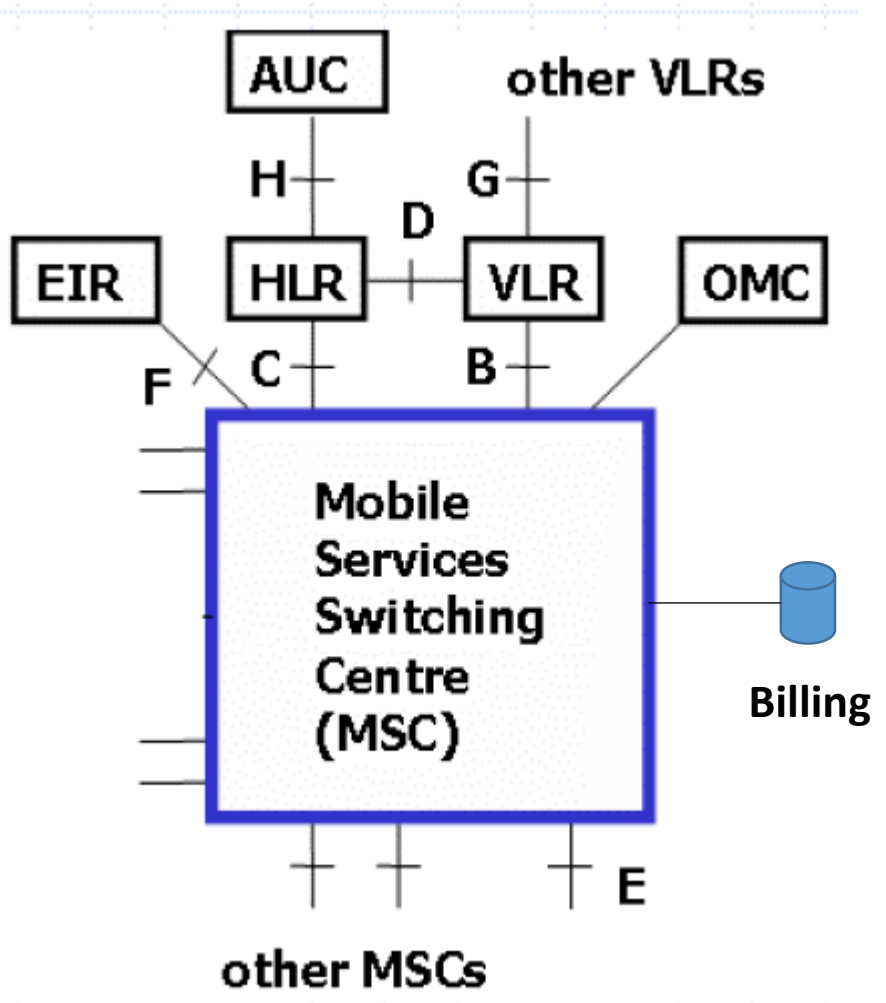
Power control and management is essential in all telecommunications installations because the public has to use telephone:

a) At times of emergency;
b) To report power outage;
c) Base stations are usually un-attended
d) Base stations are sometimes located in remote locations without reliable electricity supply
e) The mobile phone must conserve power to have longer intervals between charging.

MOBILE SWITCHING CENTRE

Functions of the MSC:

1. **Switching of voice and data traffic** including maintenance functions;
2. **Billing functions** required for the MSs located in an MSC area;
3. **Handover** functions;
4. **internetworking** functions to communicate with other networks such as PSTN and other GSM service providers.



SUBSCRIBER IDENTITY MODULE (SIM)

1. The **Subscriber Identity Module (SIM)** provides the mobile phone with a unique identity and store and process security information.
2. The SIM stores:
   a) Personal Identification Number (PIN)
   b) Personal phone numbers
   c) Short messages
   d) Logs of dialled, received and missed numbers
   e) Security related information:
      i. The A3 authentication algorithm,
      ii. The A8 ciphering key generating algorithm,
      iii. The authentication key (KI)
      iv. International Mobile Subscriber Identity (IMSI).

3. The mobile station stores the A5 ciphering algorithm.

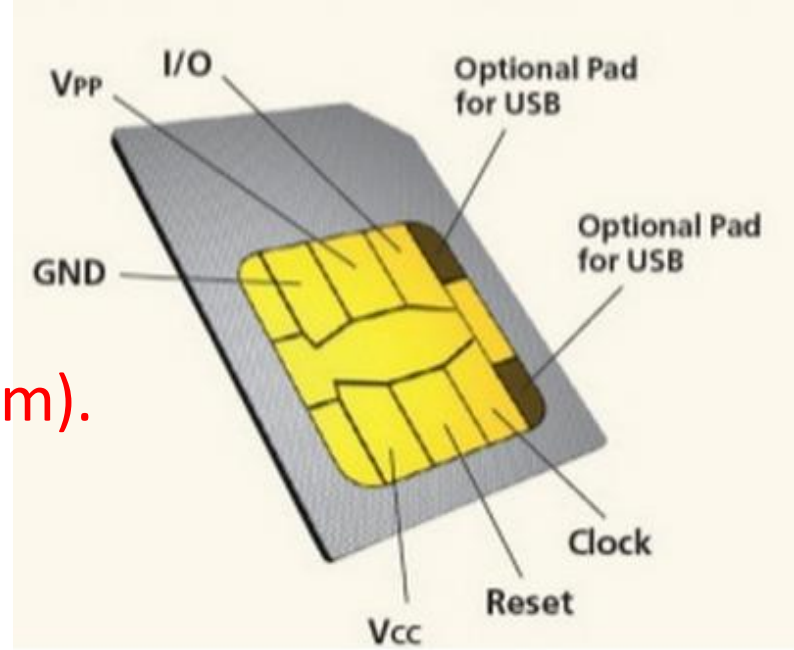
SIM CARD SIZES

A smart card comes in three physical sizes:

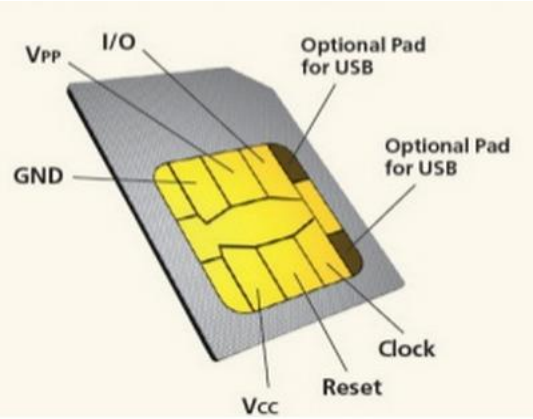
1. Credit-card sized

2. Standard 25x15mm

3. micro SIM format (12x15 mm).

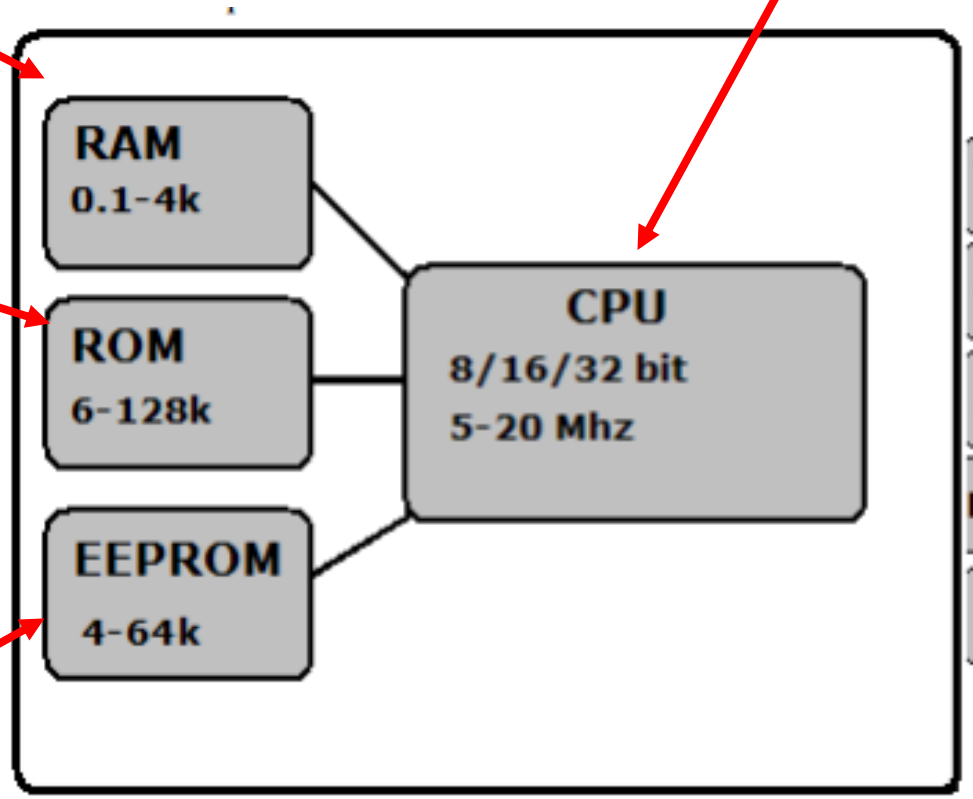


COMPONENTS OF A SIM CARD



CPU: Older models were 8-bit e.g. Motorola 6805 or Intel 8051. Today the norm is 16-bit. Java Card 3 based generation use 32-bit RISC processors.

RAM: Size ranges from few hundred bytes to several megabytes



ROM: Contains the smart cards core operating system and support libraries. Sizes ranges from 6 -300 kbytes.

EEPROM: Stores the card's file system. Typically sizes are from 4 - 64k

VCC - 1.8v, 3v, 5v

Clock: 5-20 Mhz.

Resets card and initiates the ATR (Answer-On-Reset) protocol

Input/Output: Serial half-duplex 9.6 - 115kbps

BASE STATION SUBSYSTEM (BSS)

The Base Station Subsystem (BSS) connects the user on a mobile phone with other landline or mobile users. It consists of the:

1. **The Base Transceiver Station (BTS)** is responsible for managing the air interface to the mobile station.
2. **The Base Station Controller (BSC):** is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manage radio frequencies allocated for the calls through the BTS.

NETWORK SUBSYSTEM (NSS)

NSS is a complete exchange, with the following functions

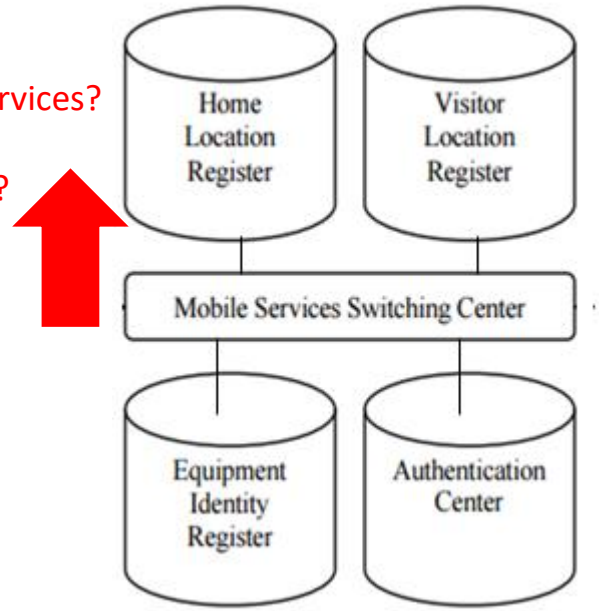
1. Co-ordinating setting up calls to and from GSM users,
2. Routing calls from a fixed network to the GSM system,
3. Interconnecting the cellular network with the Public Switched Telephone Network (PSTN).

THE HOME LOCATION REGISTER (HLR)

The Home Location Register (HLR) stores information of all subscribers belonging to an area served by a MSC. It stores

1. IMSI,
2. Services subscribed by the user,
3. Subscriber's number from a public network,
4. MS location
5. Encryption Key, K_I and some other temporary data.

- Valid User?
- Entitled to which Services?
- Number?
- Location-Which cell?
- Encryption Key?



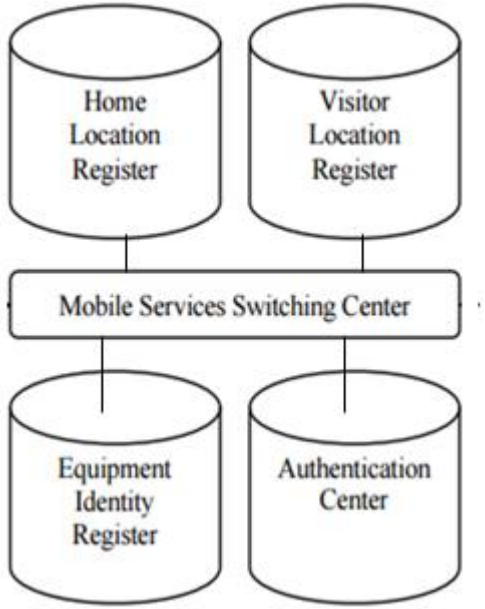
THE VISITOR LOCATION REGISTER (VLR)

a) **The Visitor Location Register (VLR)** contains relevant information for all mobiles currently served by a Mobile Switching Centre(MSC).

b) The data stored in the VLR is also stored in the HLR.

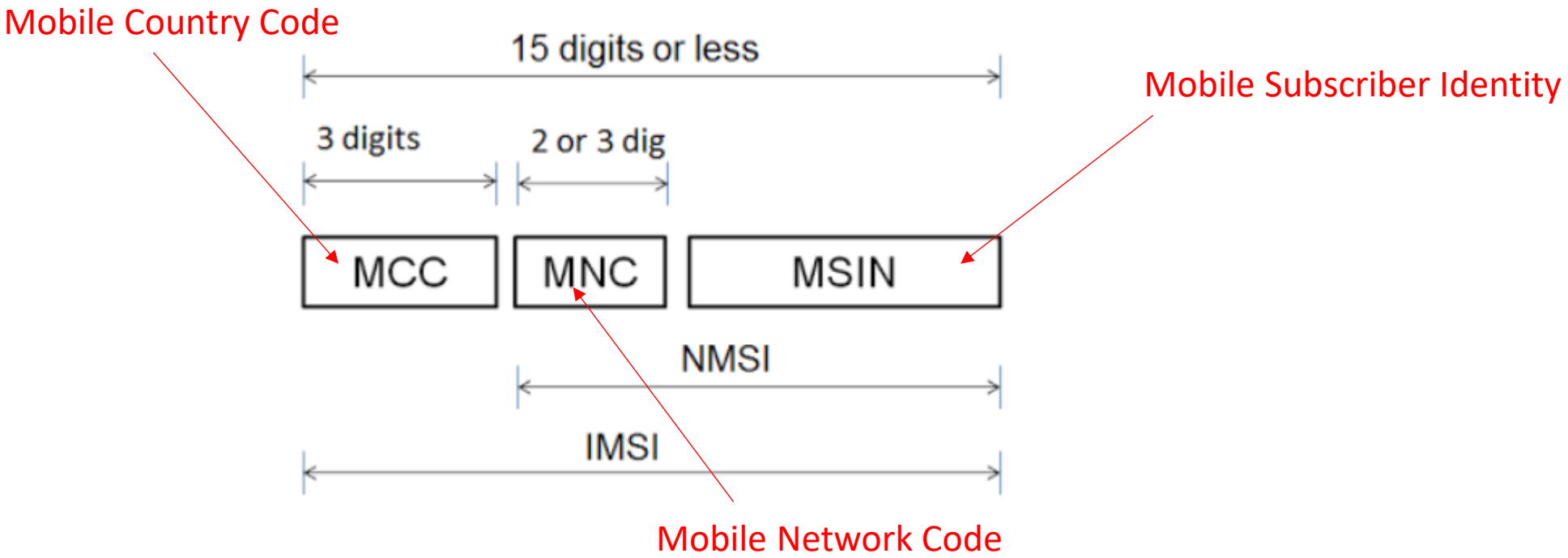
c) In addition, it also stores **the Temporary Mobile Subscriber Identity (TMSI),** which is used for limited intervals to prevent the transmission of the IMSI via the air interface.

d) The VLR supports the MSC during call establishment and authentication.



MOBILE SUBSCRIBER IDENTITIES (1) - IMSI

International Mobile Subscriber Identity (IMSI) is a unique identity allocated to each mobile subscriber in every GSM or UMTS system.



MOBILE SUBSRIBER IDENTITIES (1) - TMSI

1. **Temporary Mobile Subscriber Identity (TMSI)** is generated by the VLR and is used during paging instead of IMSI to protect subscriber from being identified and also make life more difficult to radio interface eavesdroppers.

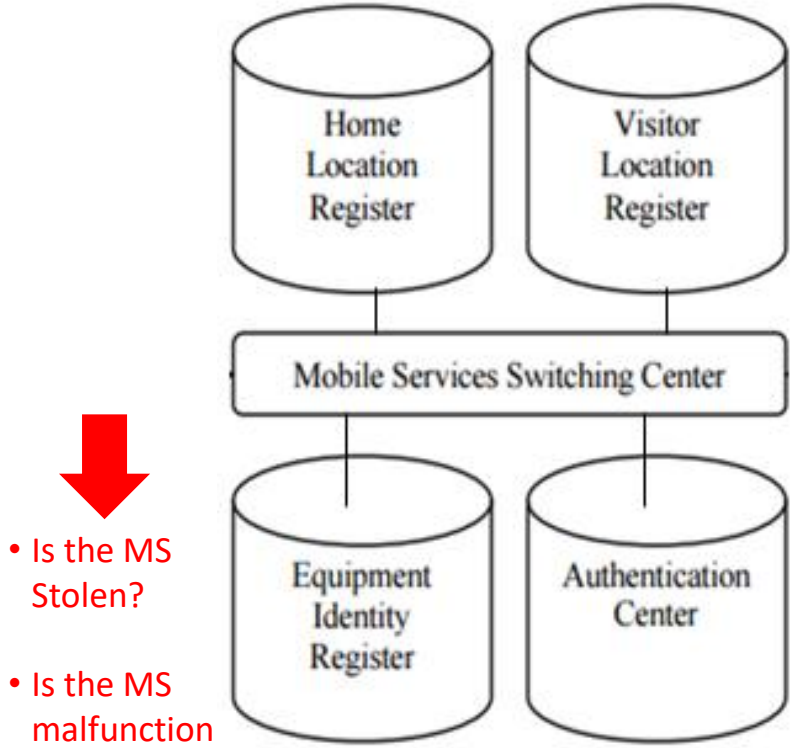
2. The TMSI consists of 4 octets since it is stored in the SIM, and SIM uses 4 octets.

3. TMSI is related to the time when it is created in order to avoid double allocation.

THE EQUIPMENT IDENTITY REGISTER (EIR)

1. The Equipment Identity Register (EIR) stores all the International Mobile Equipment Identities (IMEI) of mobile equipment and their rights on the network.
2. The EIR maintains three lists:
   a) **White list** are permitted on the network
   b) **Black list** are blocked from the network.
   c) **Gray list** consists of faulty equipment that may pose a problem on the network but are still permitted to participate on the network.
3. The IMEI reveals the serial number of the mobile station, manufacturer, type approval and country of production and can be accessed from any phone by entering:

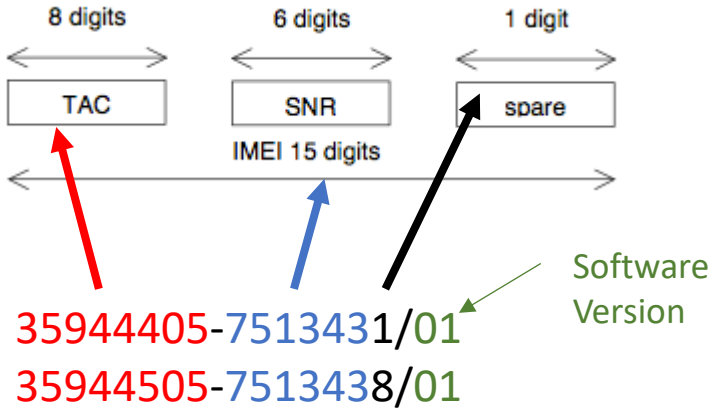
*#06#



COMPOSITION OF THE IMEI NUMBER

1. **Type Allocation Code (TAC).** 8 digits in length. Includes manufacturer ID and type of equipment;
2. **Serial Number (SNR)** is a 6 digit individual serial number uniquely identifying each equipment within the TAC.
3. **Spare digit:** Checksum of the entire string or Software version.

Additional TAGs
iPhone 5: 01-332700
Samsung Galaxy S2: 35-853704



SUMSUM SMART PHONE

WHAT IS THE PURPOSE OF IMEI?

1. Prevents subscribers masquerading
2. Enables law-enforcement agents to trace phone and hence individual movements
3. Used by law-enforcement agencies to track movements of people and for wiretapping of suspected criminals.
4. Enables operators to block certain terminal equipment for the purpose of:

   (i) Preventing theft

   (ii) Preventing malfunctioning equipment from using the network

THE AUTHENTICATION CENTER (AUC)

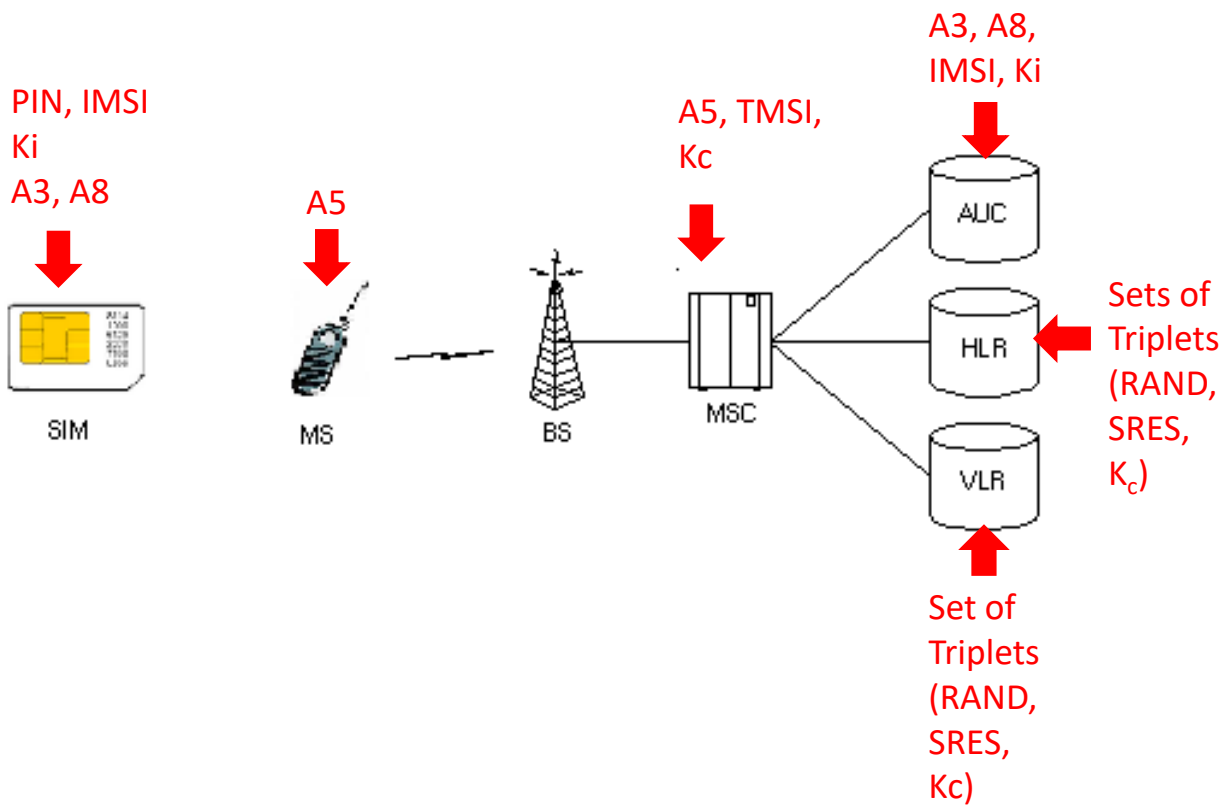
1. The Authentication Centre (AuC) is a database that keeps the following parameters:
   a) The K_I,
   b) The A3 authentication algorithm,
   c) The A5 ciphering algorithm
   d) The A8 ciphering key generating algorithm.

2. AUC is responsible for creating the sets of triplets:
   a) Random numbers (RAND),
   b) Signed Response (SRES) and
   c) The Cipher key (K_C)

SECURITY MECHANISMS IN GSM

The security mechanisms of GSM are implemented in Mobile Station, SIM card and Network as follows:

1. **The Subscriber Identity Module (SIM)** contains
   a) Personal Identification Number (PIN)
   b) The International Mobile Subscriber Identity (IMSI)
   c) the Individual Subscriber Authentication Key (K_i),
   d) the Cipher Key Generating Algorithm (A8),
   e) the Authentication Algorithm (A3),
2. **The GSM handset (or MS)** contains
   a) Ciphering Algorithm (A5)
3. **The GSM network** contains
   a) Encryption algorithms (A3, A5, A8)
   b) IMSI,
   c) Temporary Mobile Subscriber Identity (TMSI)
   d) Location Area Identity (LAI),
   e) Individual subscriber authentication key (K_i)



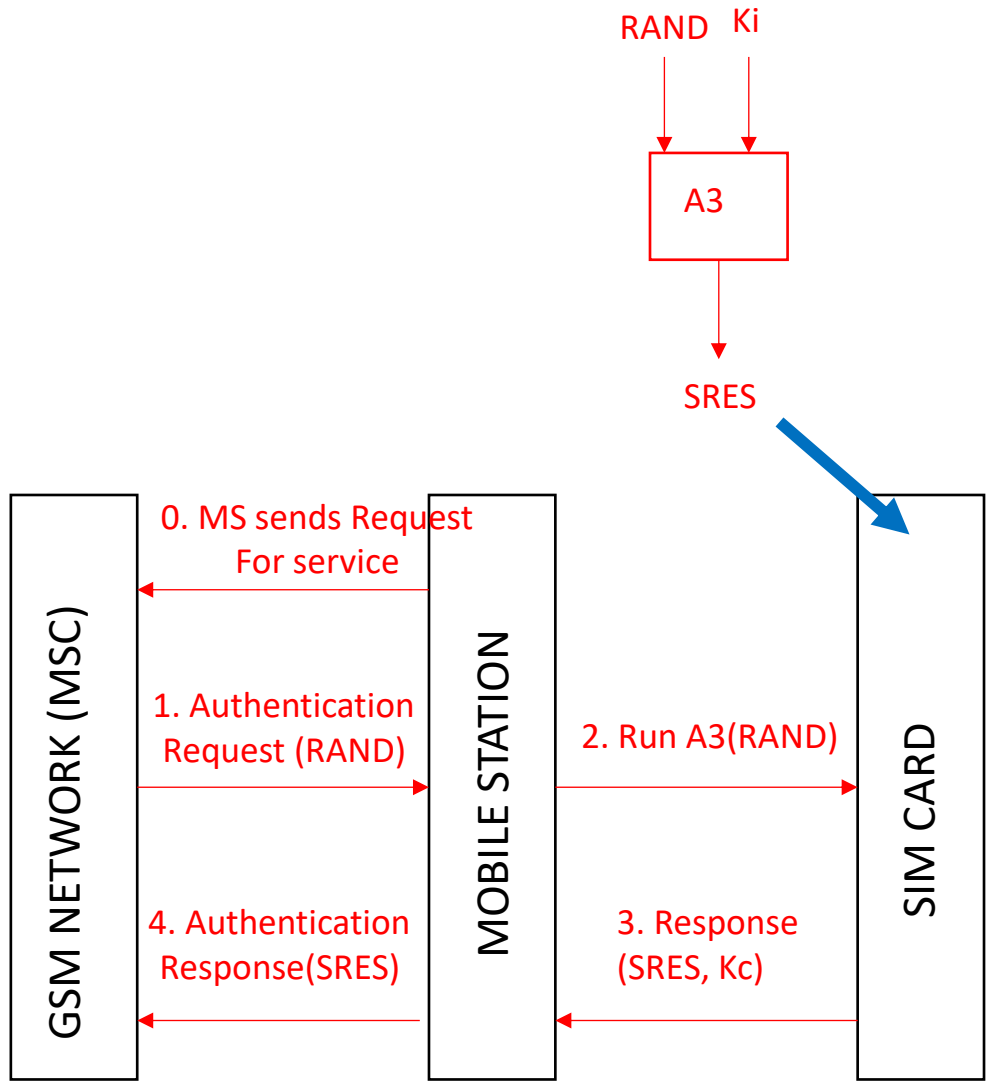
PURPOSE OF AUTHENTICATION

1. The GSM offers a mechanism for verifying the subscriber identity.
2. The purpose of authentication, is to **protect the network** against unauthorized use.

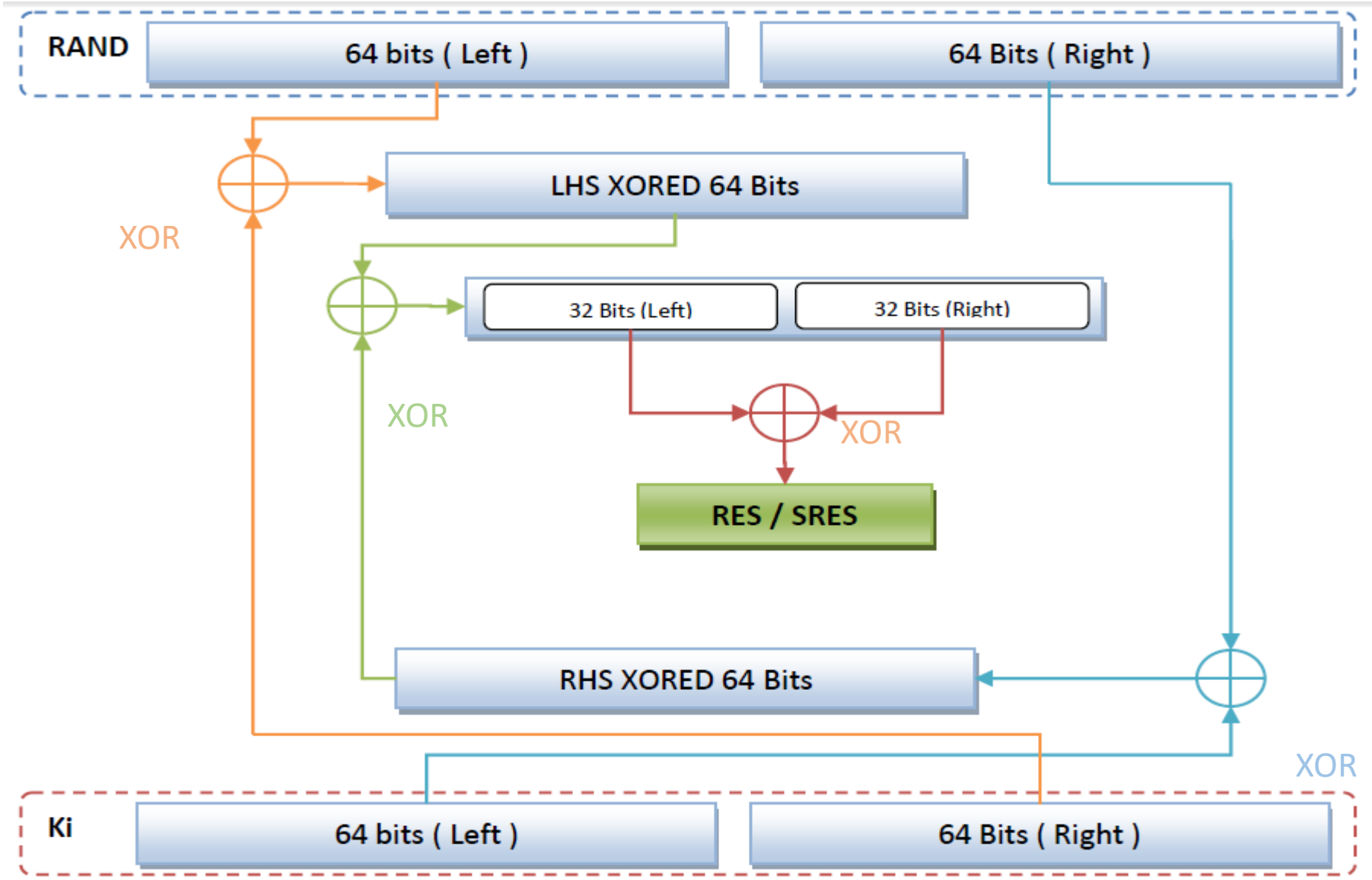
3. It also **protects GSM subscribers**, by making it practically impossible for intruders to impersonate authorized users- masquerading.

GSM AUTHENTICATION (GENERAL)

1. The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism.
2. **The aim** is to establish that the Ki stored in the AUC when first registering the subscriber is the same as that stored in the SIM card.
3. The process is as follows:
    1. A 128-bit random number (RAND) is generated by the AUC and sent to the MS.
    2. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (K_i).
    3. The SIM card responds with signed response (SRES) and Cypher Key (K_c)
    4. SRES is then transmitted to the network.
    5. Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.



FLOW-CHART FOR THE GENERATION OF SRES

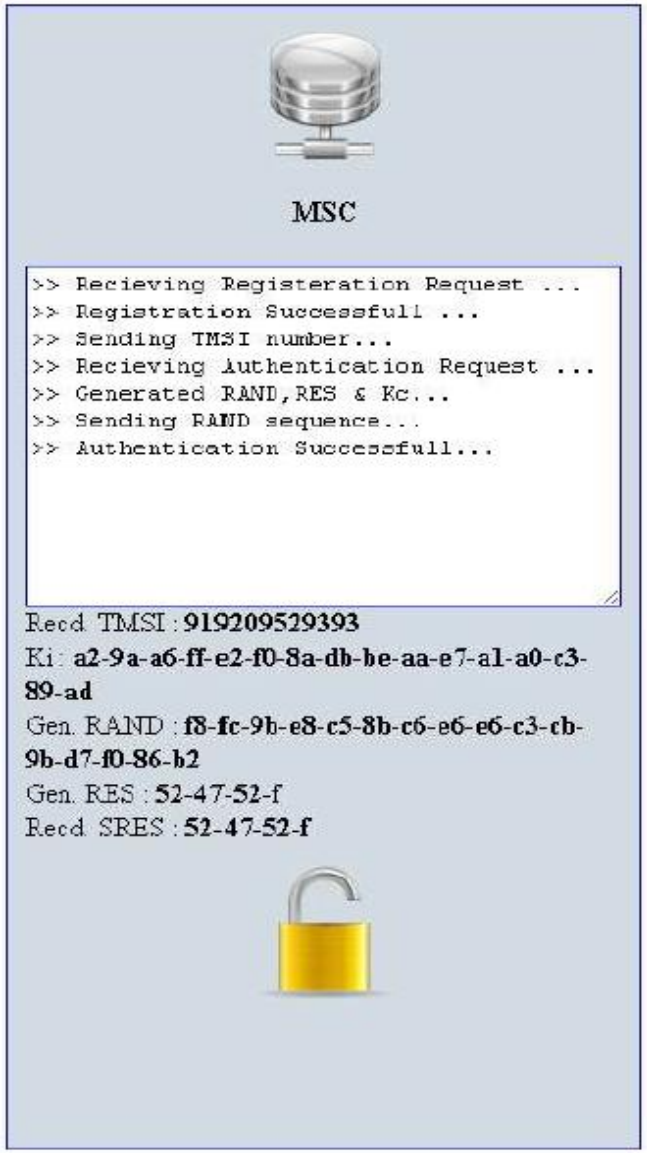


EXAMPLE OF AUTHENTICATION CODE

```
include_once('Database.class.php');
define("MSCTBL","msc");
$db = new Database('localhost', 'root', 'test123', 'mscsim');
    //connect to the server
    $db->connect();

if($_GET['action']=='register' && !empty($_POST['MSISDN']) &&
!empty($_POST['IMSI'])){
    $preMSISDN =
$ POST['MSISDN'][0].$ POST['MSISDN'][1].$ POST['MSISDN'][2].$ POST['MSISDN'][3]
;
    $data['TMSI'] = "91".$preMSISDN.rand('199999','999999');
    $sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` = '".$ POST['MSISDN']."'";
    $row = $db->query first($sql);
    if(empty($row)){
        $error_dat['status'] = "error";
        $error dat['reason'] = "Registration Failed...";
    }else{
        $db->query update(MSCTBL,$data," `MSISDN` = '".$ POST['MSISDN']."' ");
        $error_dat['regdata'] = $row;
        $error dat['regdata']['TMSI'] = $data['TMSI'];
        $error dat['status'] = "success";
        $error dat['reason'] = "Registration Complete...";
    }
    sleep(3);
    echo json_encode($error_dat);
}elseif($ GET['action']=='makesim' && !empty($ POST['MSISDN'])){
    $preMSISDN =
$ POST['MSISDN'][0].$ POST['MSISDN'][1].$ POST['MSISDN'][2].$ POST['MSISDN'][3]
;
```

MONITOERING THE AUTHENTICATION PROCESS



AUTHENTICATION OF ROAMING MOBILE STATION

Step1: MS enters a new visiting area and requests for service, an authentication request is sent to MSC first, where the request includes TMSI and LAI.

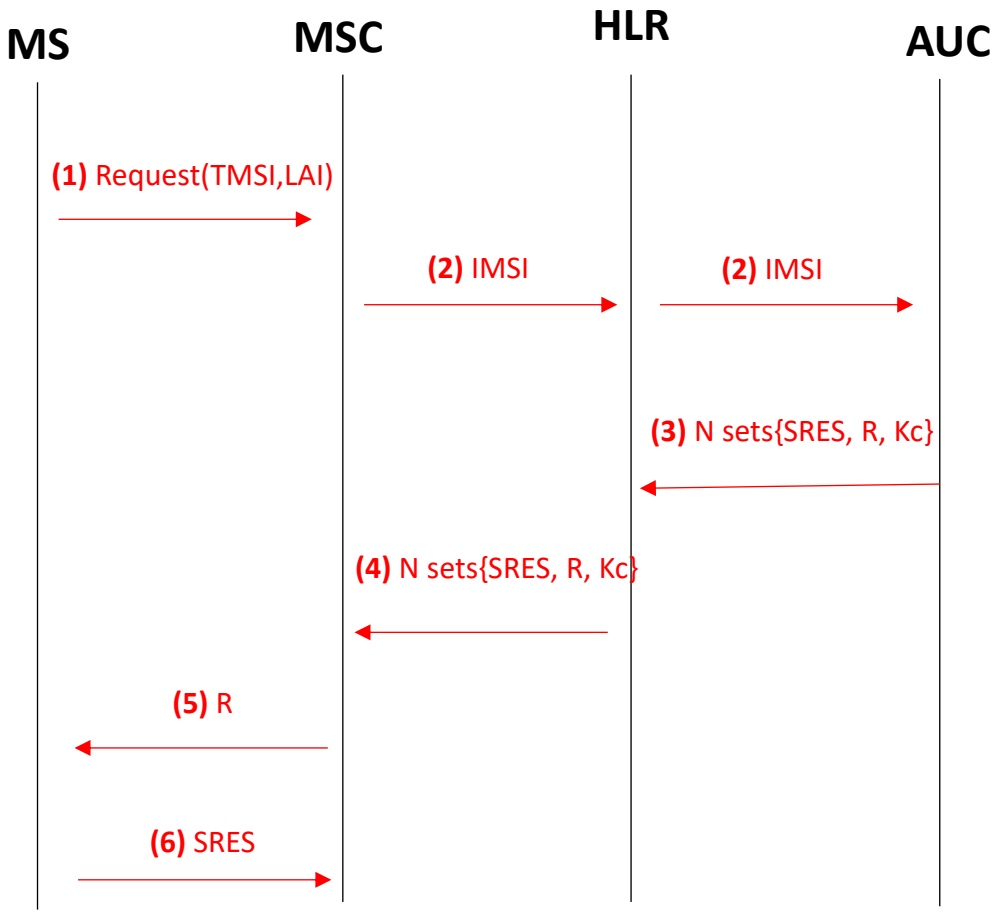
Step2: After receiving the request, the new MSC uses the received TMSI to get the IMSI from the old MSC and then sends IMSI to HLR and AUC.

Step3: The AUC generates n distinct sets of authenticating parameters {SRES, R, K_c} and sends them to HLR which transmits them to the MSC.

Step4: After receiving the sets of authenticating parameters, MSC keeps them in its own database and selects one set of them to authenticate the mobile station in subsequent calls and sends the selected R to MS.

Step5: Once MS receives R from MSC, it computes SRES = A3(R, K_i) and the temporary session key K_c = A8(R, K_i), respectively, where K_i is fetched from the SIM card. Then the SRES is sent back to MSC.

Step 6: Upon receiving SRES from MS, the MSC compares it with the corresponding SRES kept in its own database. If they are not the same, the authentication is failure and the MS is blocked from the network.



Authentication of a Roaming Phone

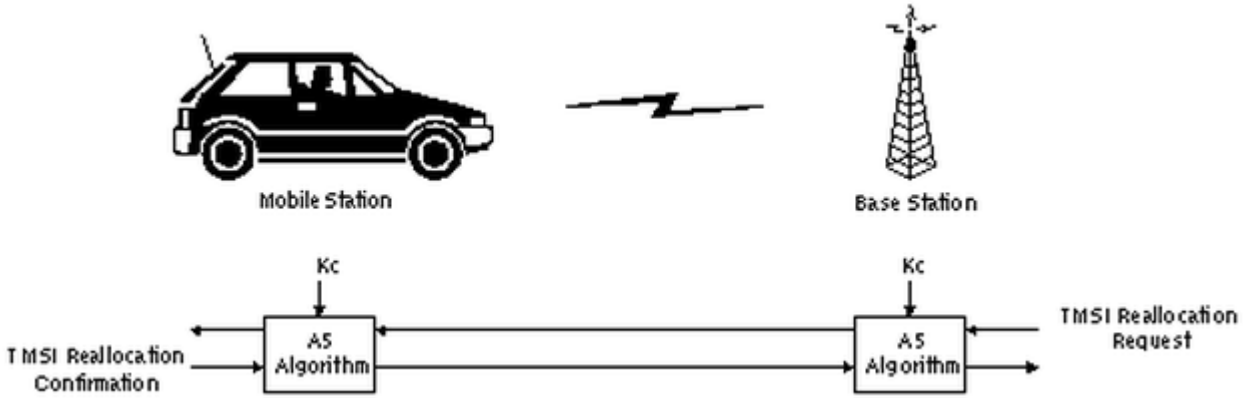
SUBSCRIBER IDENTITY CONFIDENTIALITY

1. **The Temporary Mobile Subscriber Identity (TMSI)** is used to ensure subscriber identity confidentiality.

2. **TMSI** is sent to the MS after the authentication.

3. The mobile station responds by confirming reception of the TMSI.

4. The TMSI is valid in the location area in which it was issued.



TMSI Re-allocation Process

ENCRYPTION OF VOICE AND DATA

1. **Encryption** is used in the GSM air interface (Um Interface) to protect the confidentiality of data and signalling on the air interface.

2. Two algorithms are essentially involved in the encryption process; i.e

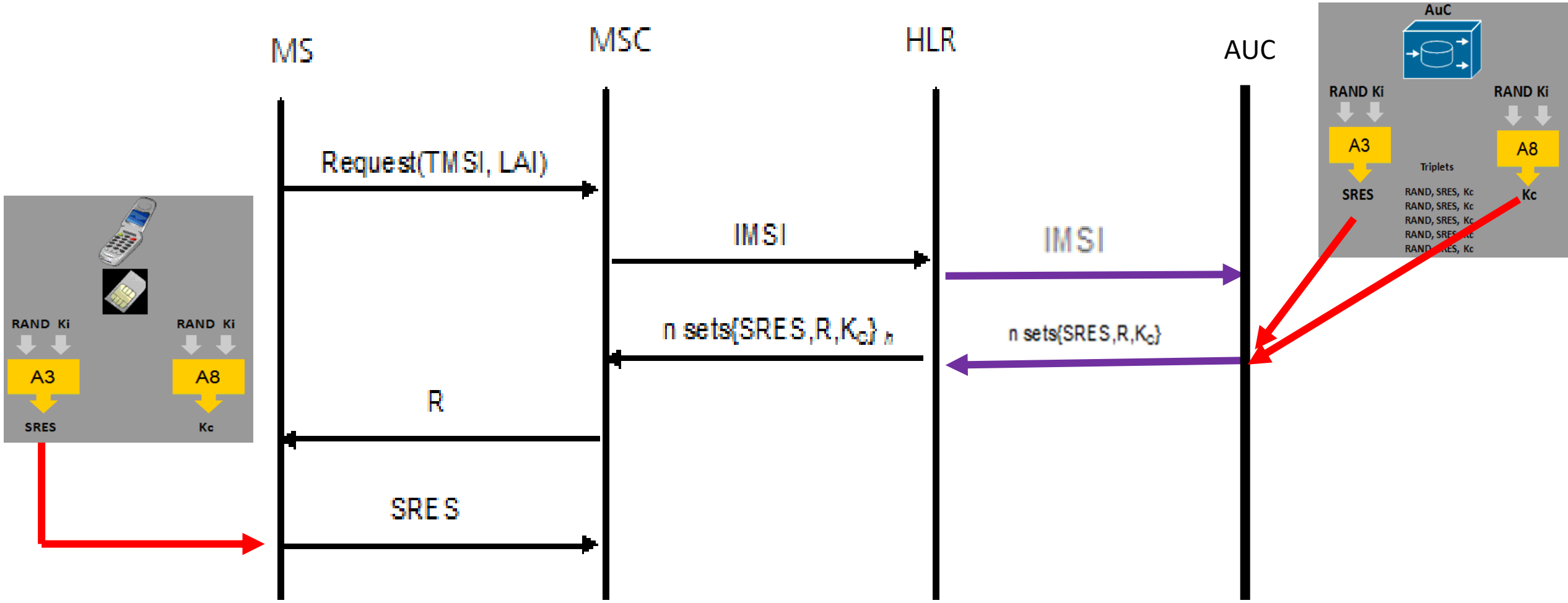
   a) The **ciphering algorithm (A5)** implemented in the MS and at the BTS.

   b) The **cipher key generation algorithm** (A8) implemented in the AuC and the SIM.

Telephone Eavesdropping

FLOW DIAGRAM OF THE GSM SECURITY PROCESS

1. After the user has been authenticated, the MS and the BTS can start using encryption by applying the cipher key Kc.
2. Kc is generated using the individual key K_i and a RAND by applying the A8 algorithm.
3. The SIM and the network both create the same value K_c based on the RAND.
4. The K_c itself is never transmitted over the air interface.

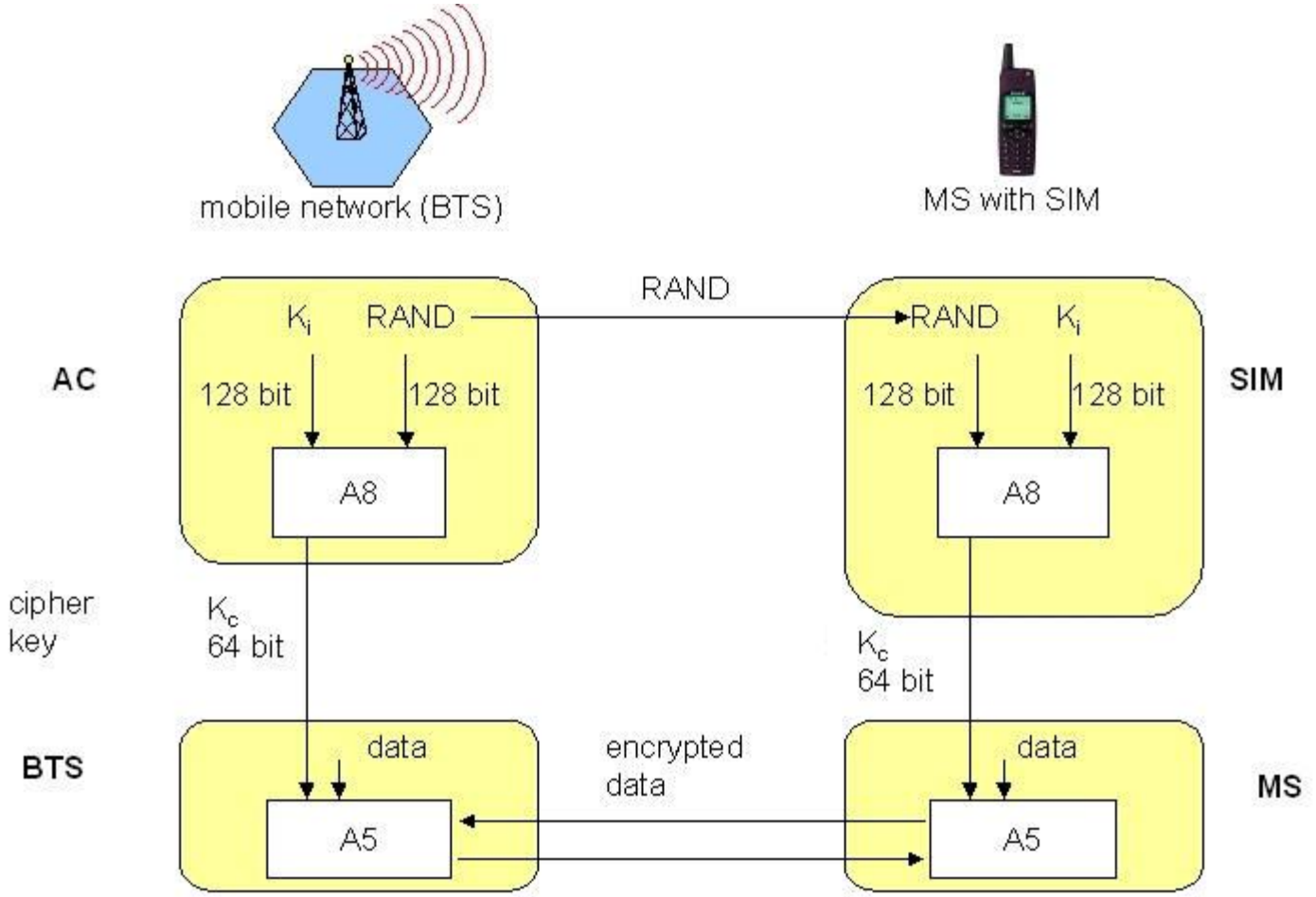


ENCRYPTION & DECRYPTION IN GSM NETWORKS

1. After authentication, the MSC passes the cypher key kc to the BTS.

2. The MS and the BTS can now encrypt and decrypt data using the A5 algorithm and the Kc.

3. Kc is a 64 bit key which is not very strong, but provides enough protection to stop simple eavesdropping.



WHERE DO YOU GET A3, A5, A8 SOFTWARE?

A variety of security algorithms are used to provide authentication, cipher key generation, integrity and radio link privacy to users on mobile networks. Details of the various algorithms and how they can be obtained are provided below.

3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3

July 2012: FINAL VERSIONS of the Algorithms 128-EEA3 & 128-EIA3 are now available for download following approval and publication by 3GPP. The algorithms themselves are identical to the draft versions published in January 2011, although some text in the documents has changed slightly. The documents have been included in the LTE standards following recommendations from 3GPP's Security Group.