Permanent Identifiers in GSM

- **IMSI**: International Mobile Subscriber Identity
  - in GSM network this identifies the subscribers
    - in data bases (HLR, VLR - index)
  - assigned to SIM cards
  - unique worldwide
  - IMSI = Mobile Country Code (Hungary: 216) + Mobile Network Code (Hungary: 01/30/70) + Mobile Subscriber Identifier (10 digits)
  - at operator change: MSISDN may be kept (number portability) but SIM card and therefore the IMSI must be changed

- **MSISDN**: Mobile Station ISDN Number
  - telephony number
  - unique worldwide
  - MSISDN = Country Code (Hungary: 36) + Network Identifier (“area code”) (Hungary: 20/30/70) + Subscriber Number
Permanent Identifiers in GSM

- **IMEI**: International Mobile Equipment Identity
  - identifier of the mobile equipment
  - unique worldwide
  - \( \text{IMEI} = \text{equipment type+producer id} \ (8 \text{ digits}) + \text{serial number} \ (6 \text{ digits}) + \text{control digit} \ (1 \text{ digit}) \ (+\text{software version id}) \ (1 \text{ digit}) \)
  - To query: \(*\#06\#
    - works on every GSM terminal
    - written under the battery, too
    - if they are different (or the latter is not present): the mobile is probably stolen!
      - exception: the SW version number is not always displayed by \(*\#06\#\) or it is not written under the battery
Temporary Identifiers in GSM

- **MSRN**: Mobile Station Roaming Number
  - used when a MS is called
  - assigned to MSC(VLR)
Temporary Identifiers in GSM

- **TMSI**: Temporary Mobile Subscriber Identity
  - used to hide IMSI on radio interface

- **LAI**: Location Area Identity
  - MCC+MNC+LAC
  - (Location Area Code)

- **GCI**: Global Cell Identity
  - LAI + CI (Cell Id)

  See User confidentiality chapter
User Confidentiality

- Authentication
  - Verification of the identity of the subscriber

- Ciphering
  - Encryption of user voice/data transmission and signal transmission in the Radio interface
    - To prevent interception

- IMEI check
  - Verification of the Mobile Equipment by checking the validity of the International Mobile Equipment Identity (IMEI)

- User Confidentiality
  - Tariff structure
    - called: right to hide location, not to be discovered even implicitly
    - caller: to know in advance how expensive the call will be
  - Avoidance of the broadcast of user’s IMSI on the Radio interface
    - TMSI
Authentication

- Problem: On the Radio Interface anyone can call in the name of anyone else by using a public identifier (IMSI, MSRN)
  - And the cheated pays…
- Therefore the network must check the identity of caller - authentication
- Private identifier needed
- But this must NEVER be transmitted through the radio interface
- But, then how ????
Authentication

- SIM card producer: Generates a 128 (in UMTS: 256) bit long private key (long enough) to each SIM card
  - $K_i$ – Individual Subscriber Key
  - Off-line presents (paper, CD, …) to the service provider buying the SIM
  - Stored in Authentication Centre (AuC):
    - IMSI – $K_i$ assignment
Authentication – theory

RAND: Random Number
SRES: Signed Result
Kc: Ciphering Key

REQUIRES TOO LARGE Signaling TRAFFIC
LET US INVOLVE THE SERVING MSC!
Authentication – practical implementation

SIM

\[ K_i \]

registrates

Connects to network

RAND

SRES

BTS

\[ K_C \]

Ciphered voice

MSC/VLR

Request (IMSI)

5 authentication triplets
\{ RAND, SRES, K_C \}

AuC

\[ K_i \]

same?
User Confidentiality – Tariff

- Tariff structure
  - called: right to hide location, not to be discovered even implicitly (through price of the call)
  - caller: to know in advance how expensive the call will be
Usage of TMSI instead of IMSI

- Do not send „sensitive” identifiers through radio IF
- At very first connection: IMSI
- MSC assigns a „random” identifier (this is the TMSI) to the mobile
- At next connection – mobile uses TMSI instead of IMSI
- But how can the MSC know, if the TMSI was assigned by itself or by another MSC?
- MS sends not only the TMSI, but the LAI where it received the TMSI
  - MSC queries the „old” MSC
  - See: Location Update
Mobility Management (MM)

- The network must know the location of a MS to be able to connect a call, or deliver an SMS to it
  - If the world were just one area
    - No need for location management
    - But Paging in every cell of the world 😞
  - Divide the world to smaller areas – to Page an MS only in a limited part of the world
    - Location Area – LA
    - Often LA = Area served by an MSC, but at heavy traffic areas it is divided logically into more LAs
  - But then the network must keep track the movement of MSs
    - Additional signaling need
    - Additional network elements, processes
    - Still worth
Location Areas

- Area served by an MSC/VLR can be divided into smaller units: **Location Area**
- The maximum size of LA can be one MSC area and the minimum size is one cell
- A subscriber can move within this area without having to make a normal location update
- Paging is done in all cells of the LA where the subscriber is currently located

A subscriber can move within this area without having to make a normal location update. Paging is done in all cells of the LA where the subscriber is currently located.
Databases involved in MM in a GSM Network

- HLR
- VLR
- MSC
- SIM

GSM Network
Location update

- The Mobile Station monitors the information broadcast by the network (BTS)
- The Mobile Station stores the current Location Area Identity (LAI) on the SIM card
- The Mobile Station continues to monitor the broadcast information
- If the Location Area Identity being broadcast by the network is other than the one stored in SIM, the Mobile Station starts the location update (LU) procedure
Elements Involved in a Location Update

1. „New” MSC/VLR acquires:
   - IMSI,
   - User Profile (MSISDN),
   - Authentication triplets

2. Inform HLR about new MSC area

3. Inform „Old” MSC/VLR that MS has moved – can clear
Location Update

**No PLMN change**

- „New” MSC/VLR:
  - MAP Send Identification
  - TMSI
- HLR:
  - MAP sendIdentification
  - IMSI, Authentication Info
- „Old” MSC/VLR:

**PLMN change**

- „New” MSC/VLR:
  - MAP Send Authentication Info
  - IMSI
  - MAP Send Authentication Info Ack.
- HLR:
  - Authentication Info
- „Old” MSC/VLR:

**Common continuation**

- „New” MSC/VLR:
  - MAP Update Location
  - IMSI+new MSC GT
  - MAP Insert Subscriber Data
  - MSISDN
  - MAP Insert Subscriber Data Ack.
  - MAP Update Location Ack.
- HLR:
  - MAP Cancel Location
  - IMSI
- „Old” MSC/VLR:
  - MAP Cancel Location Ack.
LU variants

- „Normal” (Generic LU)
- Periodic

- Switch on (IMSI Attach)
- Switch off (IMSI Detach)
Routing the call inside the GSM network

1. Send routing info (MSISDN)
2. Provide roaming number (IMSI)
3. MSRN
4. MSRN
5. Call set-up (ISUP) (dialled MSISDN)

- HLR and serving MSC (VMSC – Visited MSC) may be in different networks – SCCP Global Title
- GMSC and serving MSC (VMSC – Visited MSC) may be in different networks – (international) transit switches
GSM protocols

- Previously discussed: Protocols among MSC, VLR, HLR, EIR (C, D, E, F, G interfaces): SCCP/TCAP/MAP
- Let us have a look at the protocols between the MSC and MS (A, Abis, Um (radio) interfaces) -- simplified
  - Lower layers:
    - A interface: MTP + SCCP
    - Abis interface: LAPD (old friend...)
    - Radio (Um) interface: LAPDm: modified LAPD (optimized for radio channels – e.g. shorter messages, etc.)
  - Two special protocols above them:
    - MM – Mobility Management
    - CC – Call Control (~DSS1)
**GSM protocols**

**MS**  
BSC  
MSC  
HLR,…

**Radio IF**  
**A IF**

- Call Control
- Mobility Management

- SCCP
- MTP
- TCAP
- SCCP
- MTP

**NSS**

- MSC
- VLR
- GMSC
- SMSC
- HLR
- AuC
- EIR

**Radio IF:**  
- CC
- MM
- RR

**NSS:**  
- MTP + SCCP + TCAP + MAP (control)
- MTP + ISUP (call control)

**A IF:**  
- BSSAP = BSSMAP + DTAP
Mobile Originated (MO) Call

- Connection indication
- Authentication
- Ciphering
- IMEI check (optional)
- Call setup – as in DSS1
- The exception: radio channel assignment

<table>
<thead>
<tr>
<th>BSC</th>
<th>MSC / VLR</th>
<th>GMSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSMAP Complete Layer3 Info</td>
<td>ISUP Initial Address Message</td>
<td>Called Party Number</td>
</tr>
<tr>
<td>Cell Id. + MM CM Service Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM Authentication Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM Authentication Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSMAP Cipher Mode Command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSMAP Cipher Mode Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(MM Identity Request)</td>
<td>ISUP Address Complete Message</td>
<td></td>
</tr>
<tr>
<td>(MM Identity Response)</td>
<td>ISUP Answer Message</td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TMSI Called Party Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC Call Proceeding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSMAP Assignment Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSMAP Assignment Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC Alerting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC Connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC Connect Acknowledge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mobile Terminated (MT) Call

- MSRN acquiring
  - Paging
  - Conn. indication
- Authentication
  - Ciphering
- IMEI check (optional)
- Call setup – as in DSS1
- The exception: radio channel assignment

BSC → MSC/VLR → HLR → GMSC → PSTN

- BSSMAP Paging
- IMSI
- BSSMAP Complete Layer3 Info
- Cell Id. + RR
- Paging Response
- TMSI (v. IMSI v. IMEI)
- MM Authentication Request
- MM Authentication Response
- BSSMAP Cipher Mode Command
- BSSMAP Cipher Mode Complete
  - (MM Identity Req.)
  - (MM Identity Resp.)
- CC Setup
  - Calling Party Number
  - Called Party Number (opt.)
- CC Call Confirmed
- BSSMAP Assignment Request
- BSSMAP Assignment Complete
- CC Alerting
- CC Connect
- CC Connect Acknowledge
- ISUP Address Complete Message (ACM)
- ISUP ACM
- ISUP Answer Message (ANM)
- ISUP ANM

Called Party MSISDN

MSISDN

IMSI

MSRN

PSTN

GMSC

HLR

MSC/VLR

BSC
Short Message Service

- Signaling service, no voice lines involved
- Datagram service
  - Not requiring the end-to-end establishment of a traffic path between sender and receiver
  - Sender sends SM to SMSC of its home PLMN
  - SMSC delivers it to receiver
- Not guaranteed service
- Asymmetric: Mobile Originating Short Message transmission is considered as a different service from Mobile Terminating Short Message transmission
Successful SMS transmission

A: sender
B: receiver