

Mobile Communications

GSM and voice service

2. GSM and voice services

2.1 The physical layer



2.2 Network architecture; functions and protocols

2.3 Services and Service enablers

2. GSM and voice services

2.2 Network architecture, functions and protocols

the GSM architecture
security algorithms
call set-up
handover
location updating
protocol stack

extensions:

E2.3 the synchronisation process

2

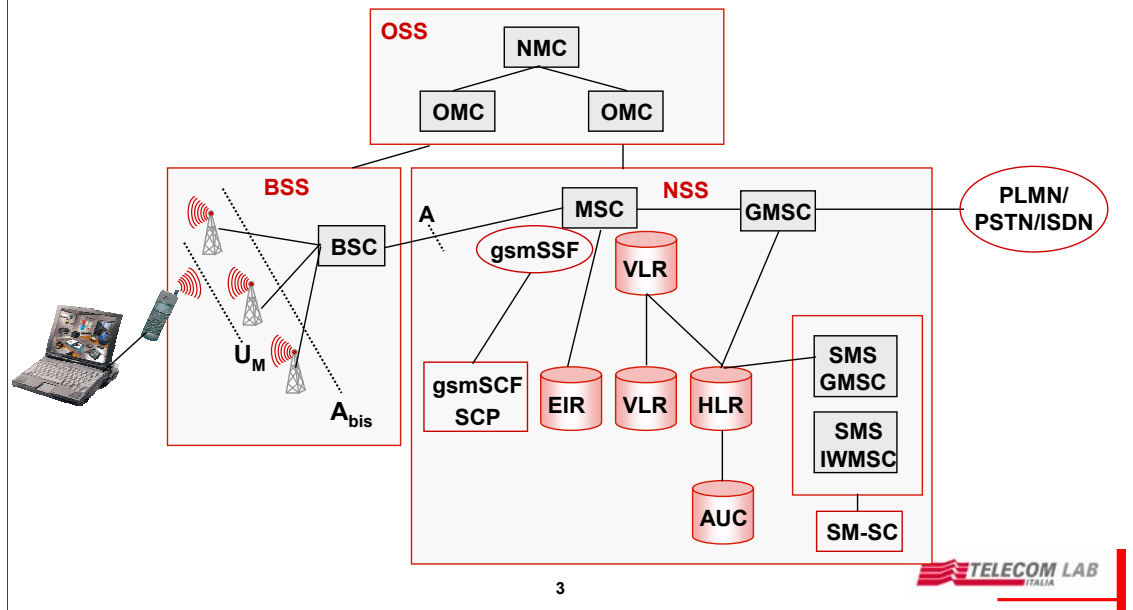
 TELECOM LAB
ITALIA

The chapter faces the main network *issues* arising in the GSM system

First of all the architecture, offering several interesting solutions, mostly in the hierarchical control and the re-use of ISDN protocols.

The major function driving the features of the system are described, including some protocol schemes and the most important exchanges of messages. They base on the physical structure considered in the previous section.

GSM network architecture

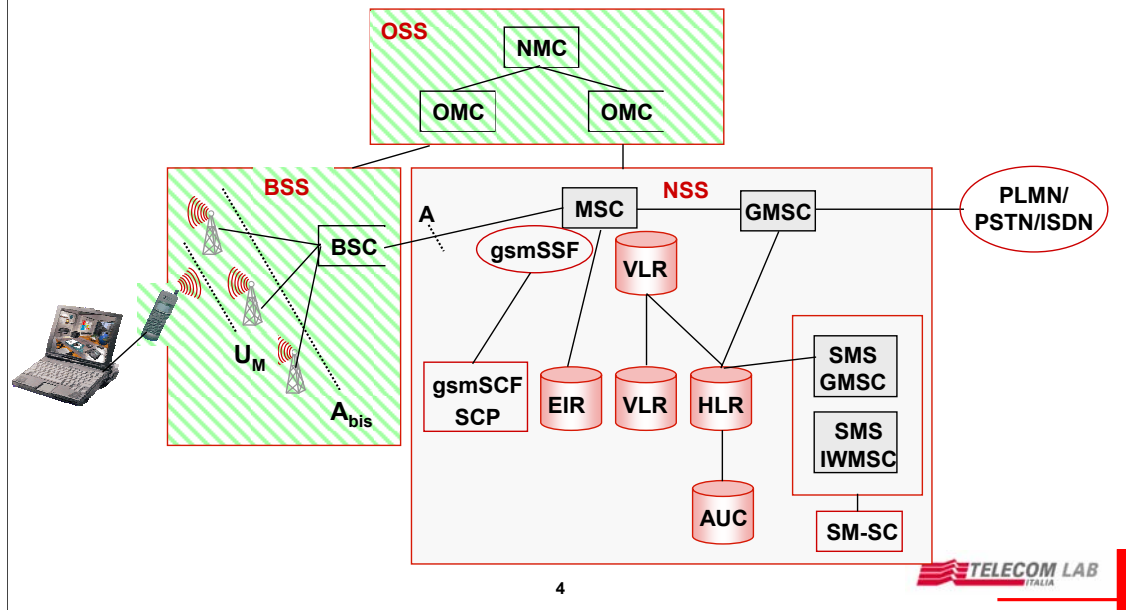


The GSM network entities shown in the figure may be grouped according to four levels:

- the intelligence level contains the Home Location Register (HLR) the Visitor Location Register (VLR) the Equipment Identity Register (EIR) and the Authentication Centre (AUC); HLR and VLR in particular contain: user service profiles, user data, charging files and manage the process of user location, and registration
- the switching level, where the Mobile Switching Centre (MSC) is implementing: call control, connection control, routing, network interconnection functions
- the radio resource control level, consisting of two entities, the Base Station Transceiver (BTS) and the Base Station Controller (BSC); the former performs all the layer 1 functions and the lower layer 2 functions; the latter is in charge of the radio resource control as well as of the upper layer 2 functions.
- the operations and maintenance level, represented by the Operations and Maintenance Centre (OMC).

The BSC controls several BTSs (depending on the BSC capacity). Typically, BSC is completely transparent to the functions tied to the call control. These functions are performed by the MSC.

GSM network architecture (II)



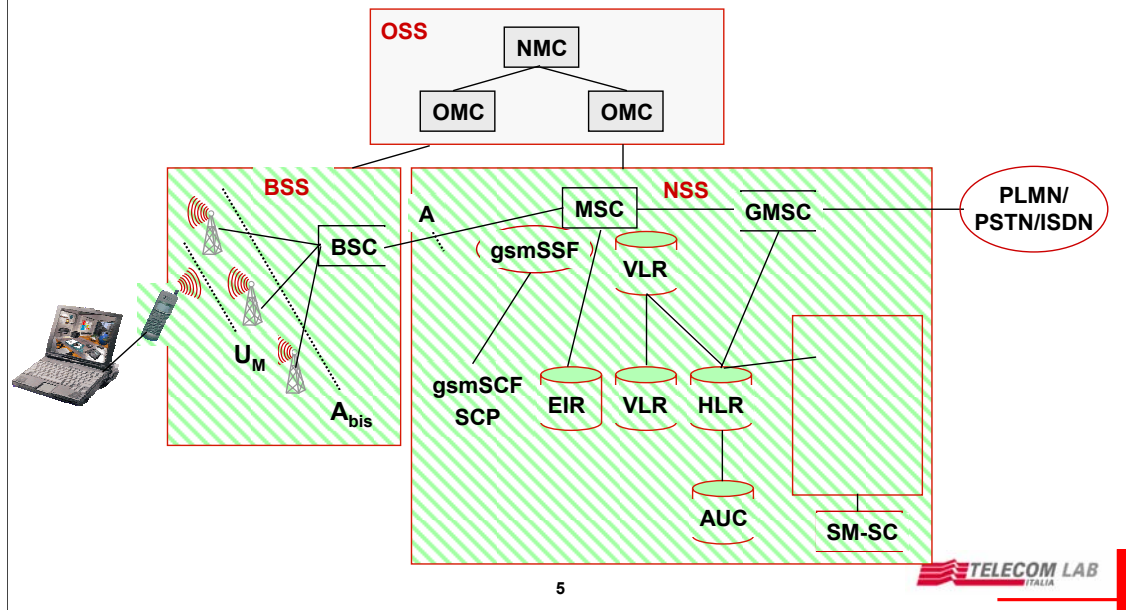
The *Network Sub System* (NSS) includes:

- the *Mobile Switching Centre* (MSC) containing the call control and the mobility control functions; a *Visitor Location Register* (VLR) is normally associated to the MSC. The area controlled by a MSC/VLR is named *MSC/VLR Service Area* and it is composed by one or several *Location Area*
- the *Gateway MSC* (GMSC) connects the network with other networks managed by other Operators.
- the *SMS-InterWorking MSC* (SMS-IWMSC) and the *SMS-Gateway* (MSC SMS-GMSC) are devoted to the *Short Message service*; they are connected to the *Short Message Service Centre* (SM-SC)

The data bases container in NSS are managing mobility and service control:

- the *Home Location Register* (HLR) contains permanently the user profiles and its location (if *Attached*) in terms of SS7 address of the MSC/VLR visited.
- the *Authentication Centre* (AuC) manages the user authentication parameters and the data ciphering (may be integrated with the HLR)
- the *Visitors Location Register* (VLR) contains a subset of the user data. In addition it contains the data necessary to manage the mobility in its *Location Area*.
- the *Equipment Identity Register* (EIR) contains information about every terminal (for instance the list of stolen terminals with related identification parameters)
- the *Service Control Point* (SCP) and the *Service Selection Point* (SSP) implement the Intelligent Network functions (may be integrated in the MSC/VLR).

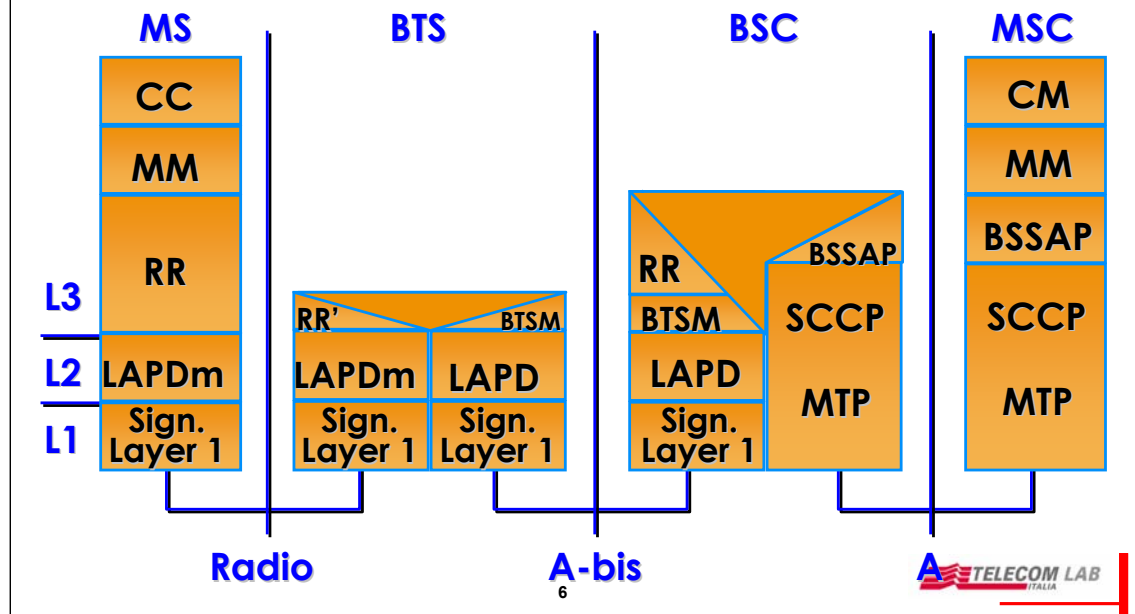
GSM network architecture (III)



The third portion of the GSM is the *Operations Sub-System* (OSS) composed by:

- *Operation and Maintenance Centre* (OMC) implementing all the management function in relation to the devices previously introduced. The OSSs often adopt proprietary solutions; they include the *billing* functions, collecting the *Call Detail Record* from the MSCs and GMSCs. They process these data for management and accounting purposes.
- *Network Management Centre* (NMC) managing the entire network.

GSM Interfaces and Signalling Protocols



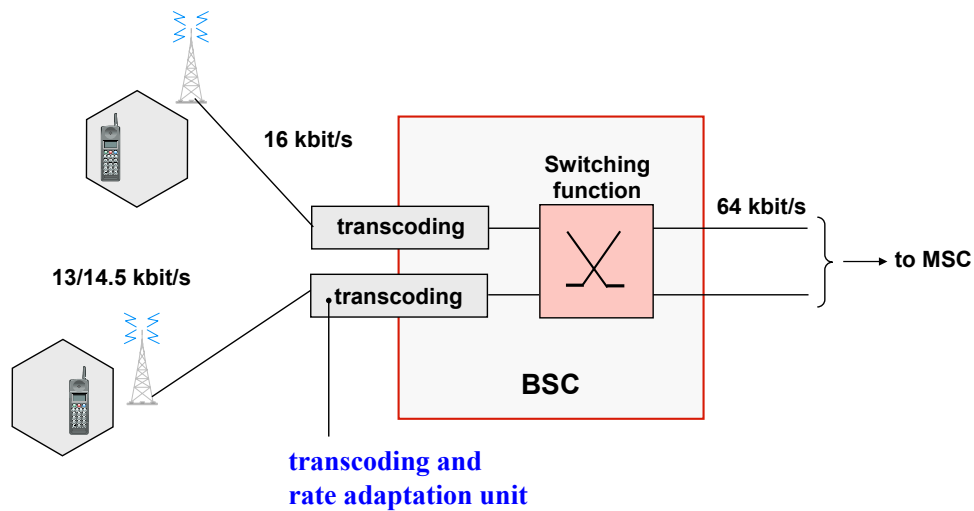
The main GSM interfaces. For the transport over the fixed segments, ISDN protocols are extensively utilised. TDM connections at 64 or 16 kbit/s are used. 64 kbit/s are used in the A interface; 16 kbit/s in the A-bis interface (this is the net *bit rate* without the radio-dependent redundancies).

More precisely, the net bit rates supplied by the radio interface are 13 e 14.5 kbit/s. The network adds to them some control information up to reach the above 16 kbit/s.

The A interface flows can then be multiplexed (4 flows at 16 kbit/s into a TDM flow at 64 kbit/s). This saves resources in the BSC-BTS link (the most capillary distributed in the network).

Flows at 64kbit/s are used towards the MSC: canonical ISDN switches are used from that level on.

Transcoding and switching functions in BSC



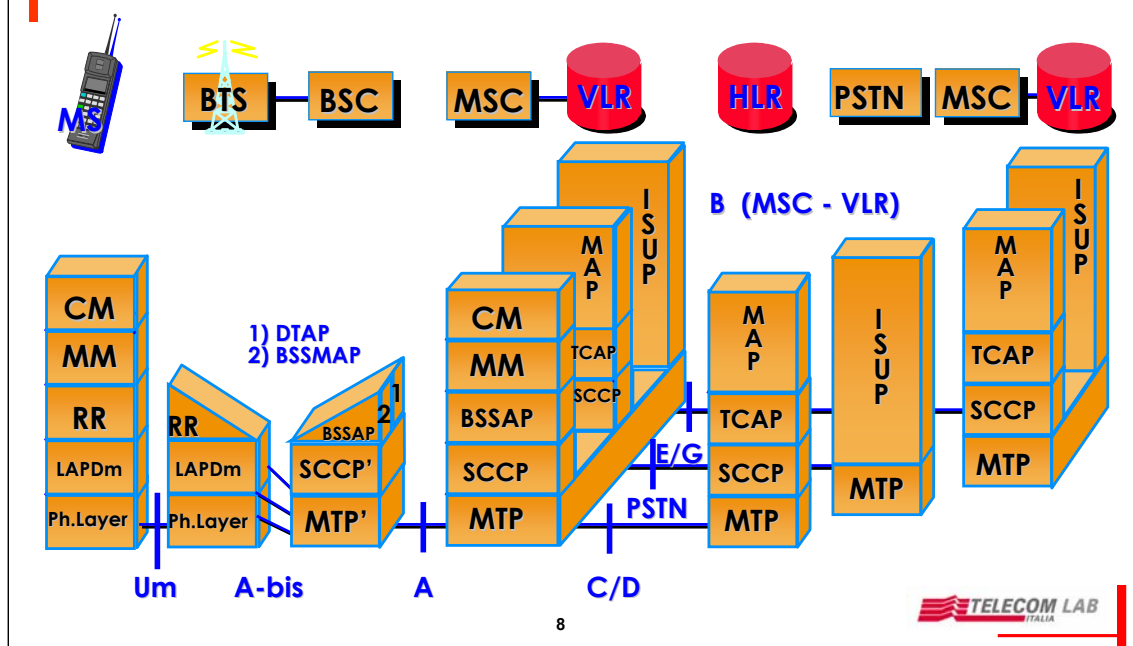
7

TELECOM LAB
ITALIA

A small remark on the previous statements.

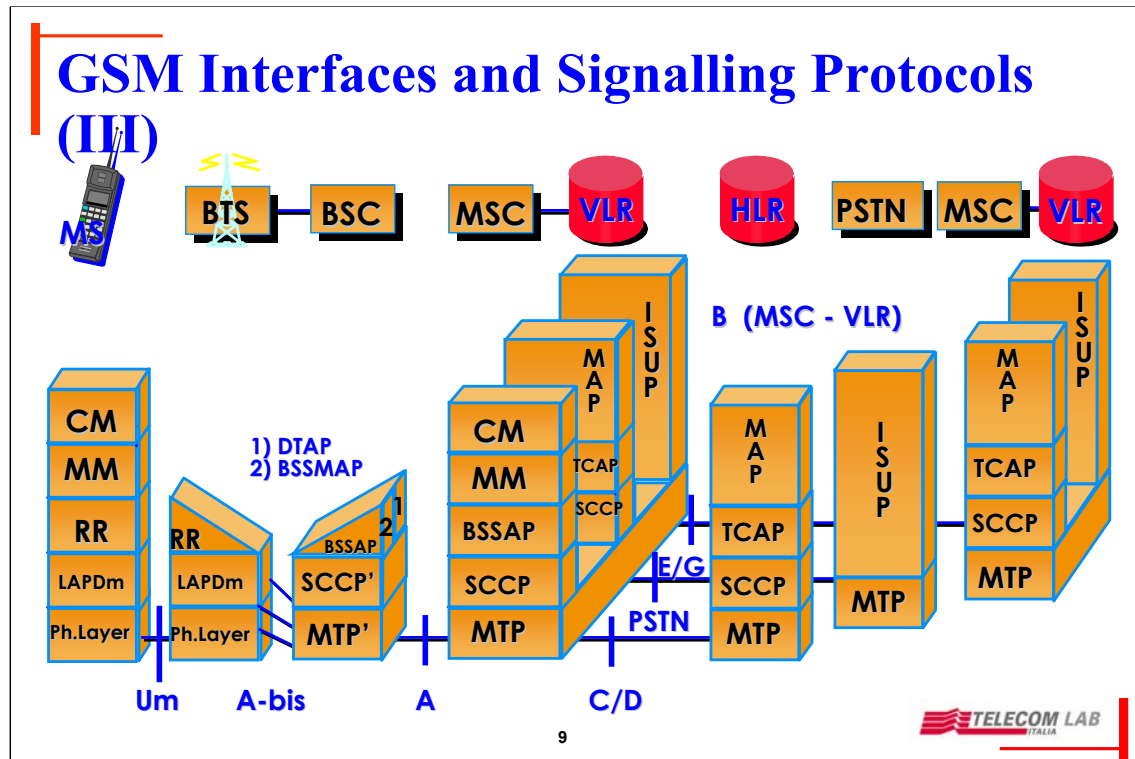
The *Transcoder and Rate Adaptor Unit* (TRAU) performs the flows conversion over the Abis interface (from 16 kbit/s to 64 kbit/s). These devices are normally contained in the BSC which is by turn asked to perform a switching function. The TRAU is then included in the switching matrix of the BSC, on the side of the Abis interface. A voice call arising between two GSM terminals has to pass through the MSC, hence undergoing a double voice encoding. This happens also when the two terminals roam under the same BSC or even the same BTS.

GSM Interfaces and Signalling Protocols (II)



As for the signalling protocols:

- the *Call Management* (CM) manages the *set up* and release of the calls, the *Mobility Management* (MM) the location updating procedures such as the *Attach* and the *Location Update*. These two protocols establish a direct relationship between MS and MSC/VLR; the related messages pass transparently the BSS device
- the *Radio Resource* (RR) protocol controls the assignment and release of the radio resources. The messages are exchanged between MS e BSS (BTS+BSC). For instance, during the call set-up, MS sends the request to the MSC, that requires the BSC to allocate the necessary radio resources. Levels CM, MM and RR form the layer 3 of the GSM protocol stack, not following strictly the OSI stack.
- the BSSAP protocol transports the messages between BSC and MSC. It is divided in two sub-protocols: the *Direct Transfer Application Part* (DTAP) and the *BSS Mobile Application Part* (BSSMAP). The former plays a pure transport role between MS and MSC; the latter controls the message exchange tied to the process managed through the BSC-MSC relationship. For instance, BSSMAP transports the messages tied to the handover procedure which involves BSC and MSC in an important segment of the overall procedure. The stack SCCP/MTP supports all the protocols defined between BSC and MSC.
- the protocol BTSM (previous figure) controls the messages between BTS and BSC, while the LAPDm protocol is a slight modification of the LAPD protocol, at the level of the *Data Link* (radio characteristics are affecting this level).

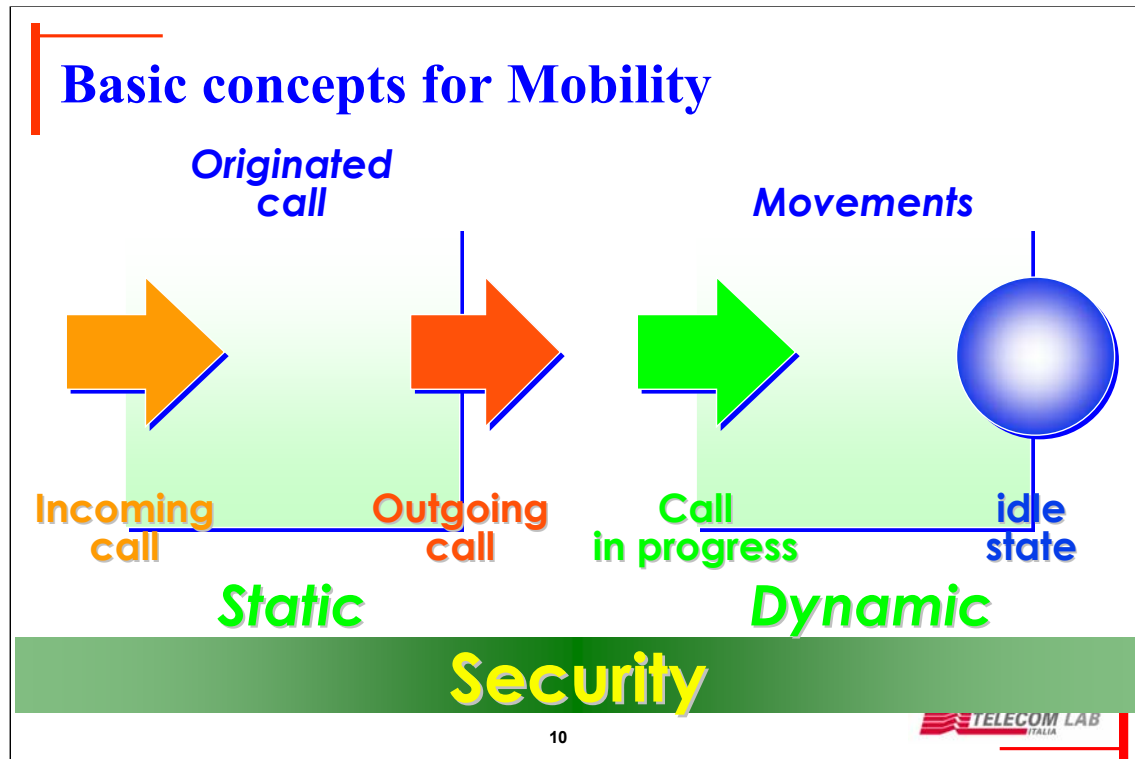


As for the protocols of the upper part of the network, it is apparent that *Mobile Application Part* (MAP) is the most important. It manages all the communication between the network nodes and the data bases. These relations are necessary for mobility and service control.

- *Intelligent Network Application Part* (INAP) and *Camel Application Part* (CAP) (not reported in the figure) perform the service control at the level of the Intelligent Network
- ISUP is and ISDN protocol utilised between switching nodes for the *set up*, the control and the release of the calls

The MAP protocol is split in different versions in function of the involved entities. In particular:

- MAP B between MSC and VLR: update of the terminal position, call *set up*, security and supplementary services procedures;
- MAP C between MSC and HLR: call routine and short message termination;
- MAP D between HLR and VLR: registration, update and cancellation of the terminal position;
- MAP E between MSC and MSC: *Handover Inter-MSC*;
- MAP F between MSC and EIR: control of the *International Mobile Equipment Identity* (IMEI) of the terminals;
- MAP G between VLR and VLR: *Location Update* and *Handover*, involving two MSC/VLR;
- MAP G between MSC and SMS Gateway for *short message* transmission.



Mobility and security mechanisms are applied to the various phases of a call as well as to the various mobile station states.

In the traffic origination phases (incoming and outgoing call) a static mobility concept is used in the sense that the mobile terminal location is identified and used for e.g. routing purposes.

More specifically, for an incoming call, two procedures are activated, namely the location of the MS and the paging procedure. For an outgoing call, the mobility mechanism is supplying the user profile data for the call management.

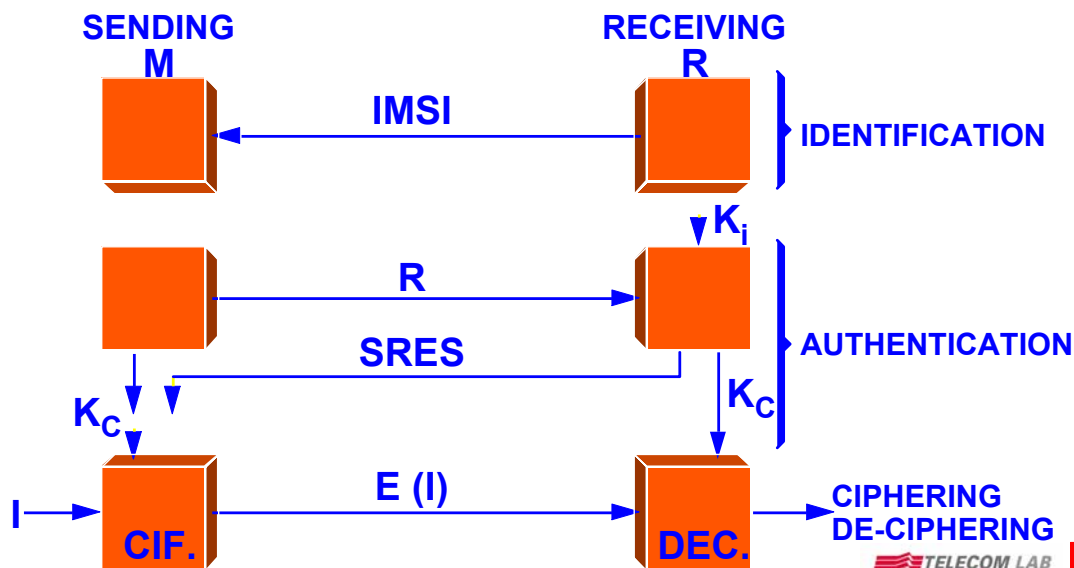
Dynamic mobility concepts are applied instead whenever the call is in progress and whenever the MS is in the idle state.

With a call in progress, mobility is managed through the handover process, ensuring the connection continuity.

In the idle state, the mobility processes are:

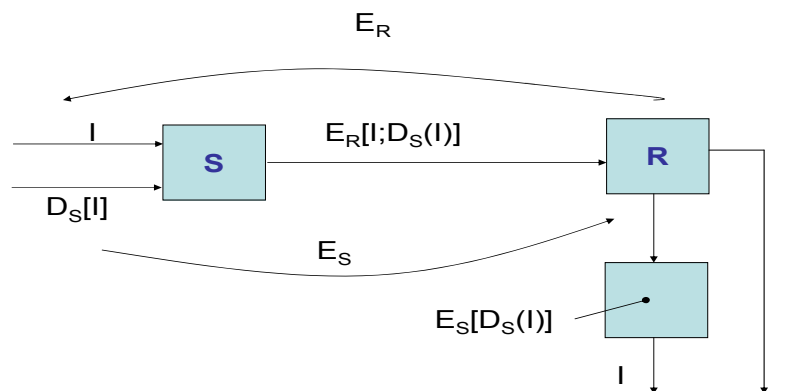
- cell selection (the MS is keeping track of its movements within the cells)
- location updating procedure (the MS is keeping track of its movements in the location areas). The location areas are those addressed by the network in order to locate the MS (i.e. the granularity according to which the network registers the movements MS is performing in its idle state).

GSM security procedure (secret key)



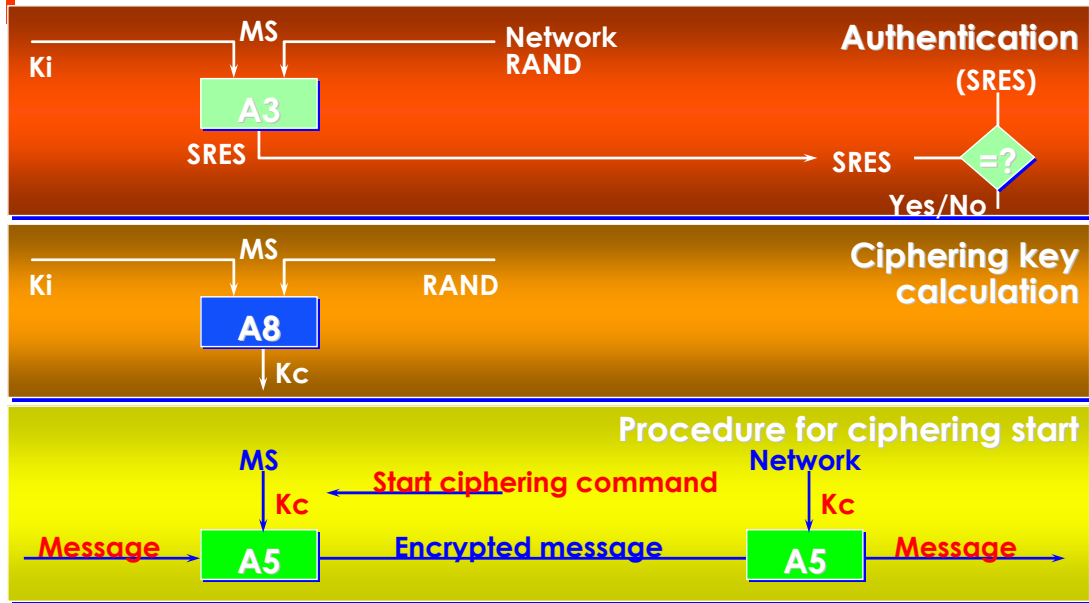
The figure sketches the security procedures adopted in the GSM.

The identification phase takes place through the exchange of the *International Mobile Station Identity* (IMSI) between MS and the network. The network knows the secret key k_i associated to that IMSI (the same association is known to the *Subscriber Identity Module* (SIM)).



The figure describes the public key ciphering mechanism. It allows the electronic signature of the information I sent by making use of the public key E_r , known by the sending party.

Security algorithms (secret key)



12

TELECOM LAB
ITALIA

The security procedures used in the GSM system are summarised in this figure.

The identification (not represented) takes place by exchanging the International Mobile Station Identity (IMSI) between the MS and the network. The network now knows the IMSI of the MS and the associated key K_i .

The network generates a random number $RAND$ towards the MS. MS applies algorithm A3 to k_i and $RAND$ and sends the result SRES to the network. The latter can perform the same operation performed by MS, hence it can verify the coincidence of the SRES calculated by both parties. In case of coincident results, the authentication is completed.

In the subsequent phase, algorithm A8 is used with $RAND$ and k_i to generate the ciphering key k_c . k_c is used with algorithm A5 on both sides to cipher and de-cipher the entire data flow transmitted on the air.

Note that parameters $RAND$ and SRES are sent on the air. However, even if received by a third party, it is almost impossible to recover through them the k_i , since the algorithm A3 is very difficult to invert.

Summarising, the security mechanisms are based on the user identity authentication and the consequent assurance on:

- traffic confidentiality
- user data confidentiality.

GSM signalling channels

BCCH: Broadcast Control Channel

- point-to-multipoint unidirectional control channel
broadcasting system information to MS

CCCH: Common Control Channel

- up-link: RACH (Random Access CHannel)
- down-link: PCH (Paging Channel)
AGCH (Access Grant CHannel)

DCCH: Dedicated Control Channel

- point-to-point bidirectional control channel
- SACCH (Slow Associated Control CHannel)
- FACCH (Fast Associated Control CHannel)
- SDCCH (Stand Alone Dedicated Control CHannel)

13



In order to drive the various functions needed to manage connections and mobility, one (or more) slots of the TDMA frame are devoted to carry logical channels for signalling and control purposes (this has already been considered in the previous chapter).

- The BCCH carries in a point-to-multipoint manner all the system information needed to the mobile terminals roaming in that cell
- The CCCH on the up link carries the random access channel, accessed with contention by all the mobiles roaming in the cell; on the down link, two logical channels are time multiplexed on CCCH, namely:
 - the paging channel, addressing the mobile which is requested by an incoming call
 - the access grant, carrying the acknowledgements to the mobile access.
- The DCCH carries in both up and down links, control channels that are either signalling-dedicated or associated control channels; the former are carrying the call signalling in the phases when the traffic channel has not yet been activated for that call; the latter are active in conjunction with any channel activated (either signalling or traffic channel) and are basically devoted to transport measurement and handover-related information.
 - the SDCCH carries the signalling procedure outside the activation of a traffic channel
 - the SACCH and FACCH carry the control information associated to traffic (TCH) and signalling channels (SDCCH).

GSM network architecture and functions

call set-up sequence

TX /	RX PCH + BCCH paging system information
RACH random access	AGCH assignment of dedicated control channel
SDCCH + SACCH signalling procedure measurements	SDCCH + SACCH signalling procedure measurements
TCH + SACCH voice / data traffic or signalling procedure (FACCH) measurements	TCH + SACCH voice / data traffic or signalling procedure (FACCH) measurements

14



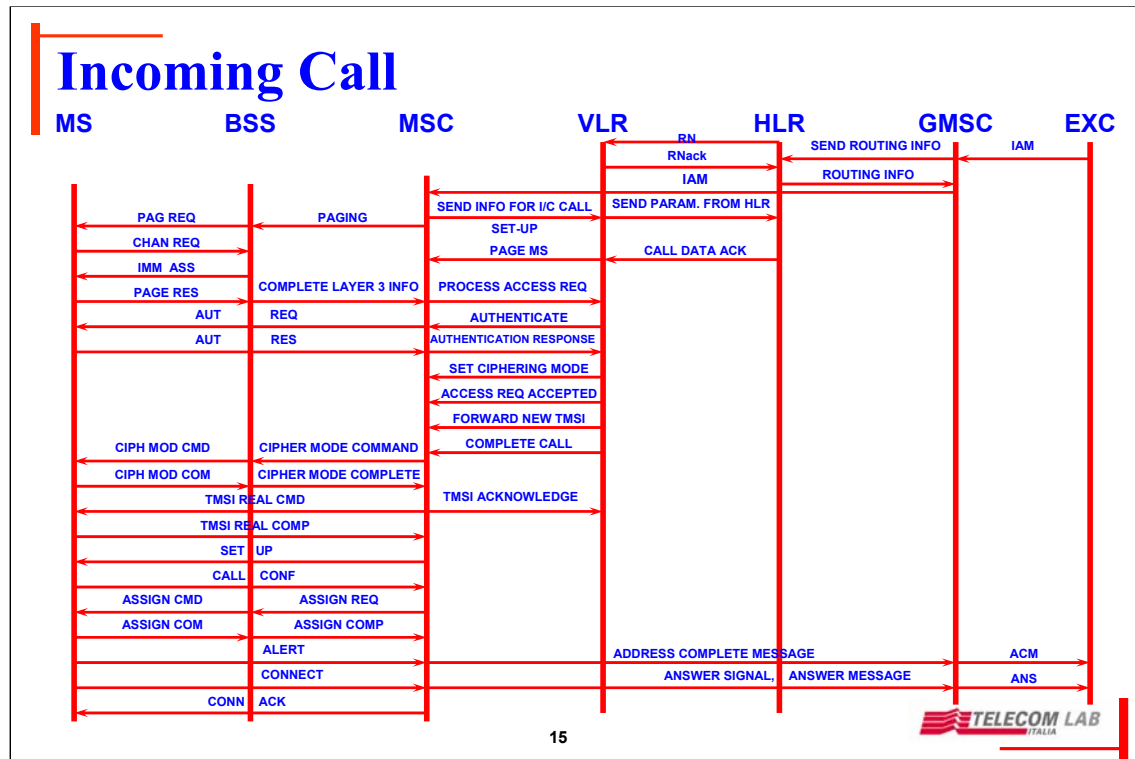
The channels previously introduced are here considered in the sequence they are used in a typical call set-up procedure. On the receiving side, the mobile station (MS) always receives the BCCH which is giving all the terminals roaming in that particular cell a number of system information, concerning the allocation of control channels (that can be used by the terminal itself) and some other data, identifying the actual cell characteristics and the characteristics of the neighbouring cells.

A generic call activated in the actual cell can be handed-over to a neighbour cell whenever the connection quality in the actual cell drops below a given threshold (this process will be explained later on).

Just looking at the BCCH, MS knows, among other information, the time location of the channel where it must watch for a possible paging sent by the network (a paging is generated whenever an incoming call is addressing that MS).

The RACH is accessed by MS to start a communication with the network (in our case the process of the call set-up). This channel is accessed with contention by the MSs roaming in the target cell. A retransmission protocol is solving possible collisions between two or more MSs accessing the same RACH at the same time. MS is implicitly informed about a collision or a biased transmission if the related acknowledgement is not received within a given time delay, so that it is able to plan a further transmission of the initial packet.

The successful reception of the initial packet is notified by the network through an acknowledgement sent over the AGCH, together with the assignment of a SDCCH to that communication.



The incoming call procedure is generated by an Initial Addressing Message (IAM) sent by the fixed network towards the Gateway MSC (GMSC). The HLR supplies the routing information to GMSC, which can send the IAM to the MSC controlling the addressed MS.

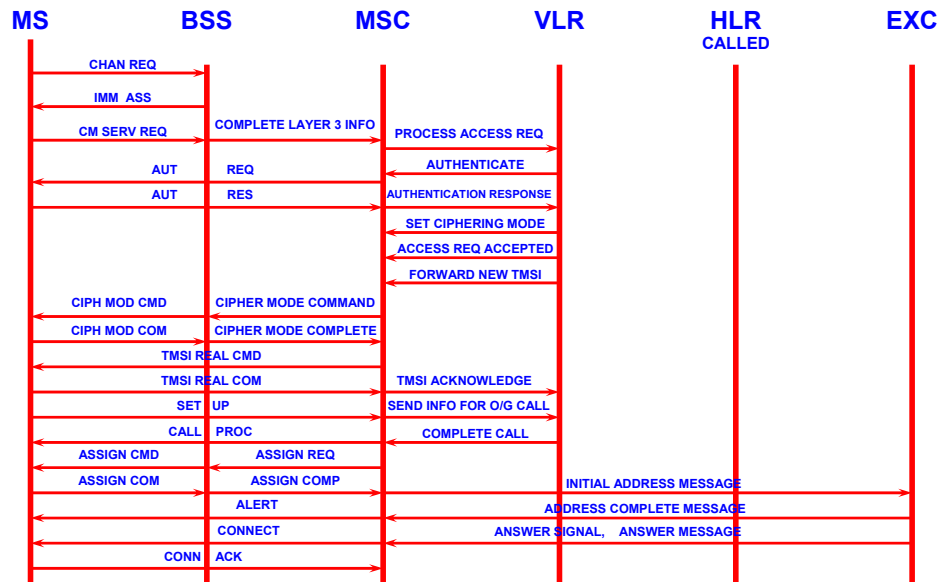
After the paging procedure is successfully completed, the MS is authenticated and the ciphering parameters are changed (the same happens during a location updating procedure).

Then the call is set-up between the MS and the MSC and an Address Complete Message (ACM) is sent to the generating Exchange which has initiated the procedure.

After this phase, the user data exchange (voice, data) can take place with all the security protections previously seen.

The figure is self-explanatory.

Outgoing Call



16

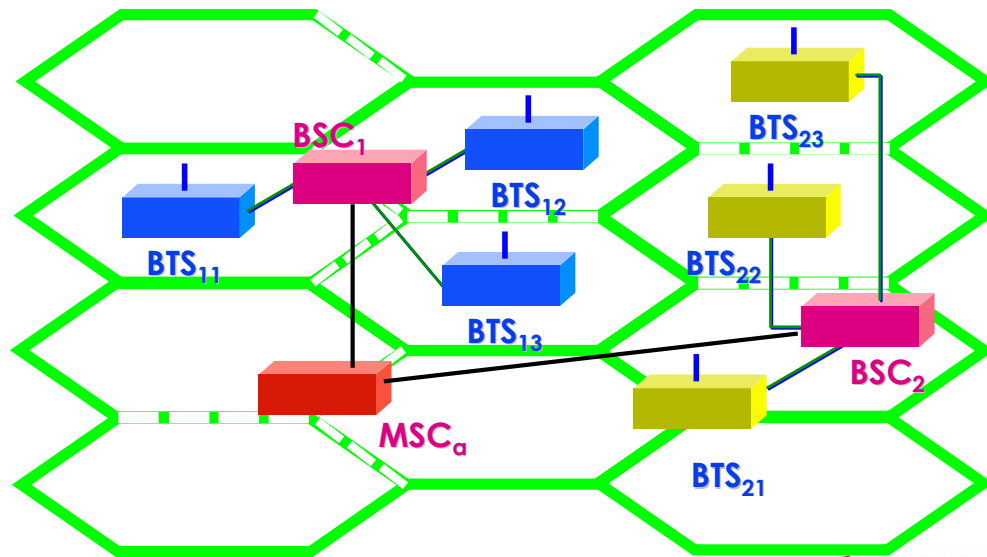
TELECOM LAB
ITALIA

For the outgoing call, the process is started by the MS through an autonomous access on the radio interface (RACH channel).

The subsequent process is similar to that described for the incoming call.

After the numbering of the called party has been sent to the MSC and a connection has been established between MS and the MSC, the latter sends the Initial Addressing Message (IAM) towards the fixed network exchange.

Handover - the role of topology



17

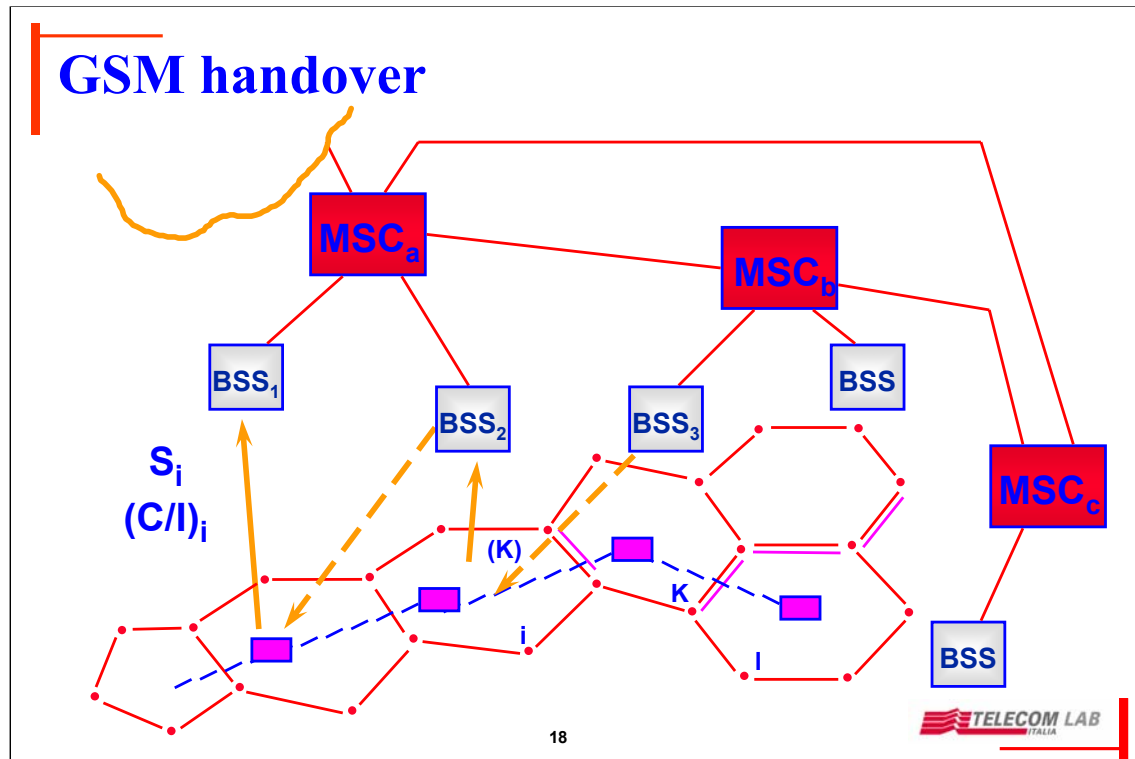
TELECOM LAB
ITALIA

The typical cellular network topology recalls a tree arrangement. This implies that the passage of the MS between contiguous cells triggers a sequence of actions that depend in general on the topological position of the involved BTSs. In case the passage happens when a call or, in general, a transaction is in progress between MS and the network, three cases of handover are envisaged, namely:

- intra BSS handover
- inter BSS, intra MSC handover
- inter BSS, inter MSC handover.

These different cases are to be considered separately, since their execution involves different network entities. and some examples are reported in the following. Handover is the procedure ensuring that the connection (or the transaction) continuity is maintained while MS is crossing the cell border. When this event takes place, some actions are to be performed in the network:

- the handover need is established on the basis of appropriate measurements reflecting both the quality of the actual connection (the one in progress in the hosting cell) and the potential feasibility of a new connection with an alternative cell (among those able to ensure a sufficient quality)
- in case the handover is decided (the network is taking this decision) the new target cell is chosen
- the new path is pre-disposed at both radio and network level; this implies that a bridge is identified in the network (the point where the old and new paths are converging)
- the handover is executed by activating the new path (the old one is then dropped).



The figure shows how the handover is executed in the GSM network. When a connection is in progress, the MS is evaluating continuously the intensity (S) and the quality (C/I) of the cells neighbouring the target cell. The measure is performed on the neighbour BCCHs whose allocation (carrier and time slot) is supplied to all the roaming MSs by the BCCH of the target cell.

The results of this evaluation are sent to the network by making use of the connection-associated channel SACCH.

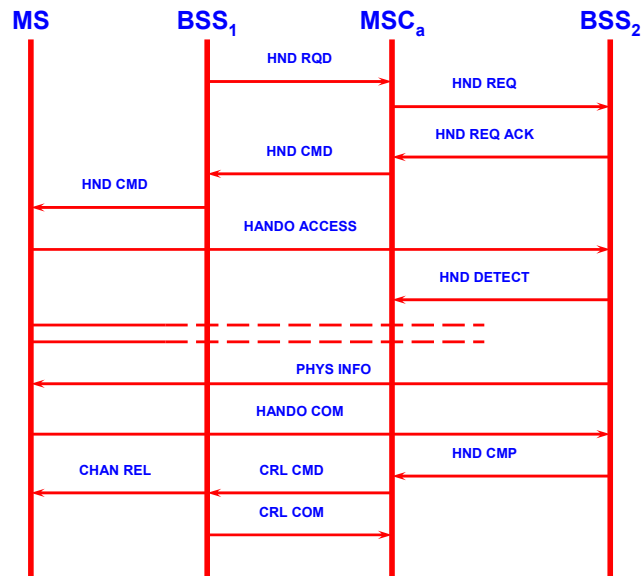
The network is able to perform the same kind of evaluation on the connection in progress. As soon as the estimate is detecting insufficient quality conditions for the connection in progress, the network activates an handover procedure towards the cell for which the best quality for that call is expected (other criteria can be adopted, based for instance on both the quality and the cells occupancy state).

The decision of starting an handover procedure gives rise to the real time exchange of the radio channel, in such a way that the connection continuity is ensured.

It is shown in the figure how the handover can imply different routing configurations of the connection. Passing from the target cell to cell i , implies a re-routing completely managed by the common MSC_a (bridging point in MSC_a). The further passage to cell k , requires a re-routing involving two MSCs: MSC_a and MSC_b.

The call control is maintained in any case by MSC_a where the call has been originated and a double transit is avoided: a subsequent handover to cell l controlled by MSC_c, induces a call routing between MSC_c the original MSC_a. The previous MSC_a - MSC_b link is dropped.

Handover Intra-MSC



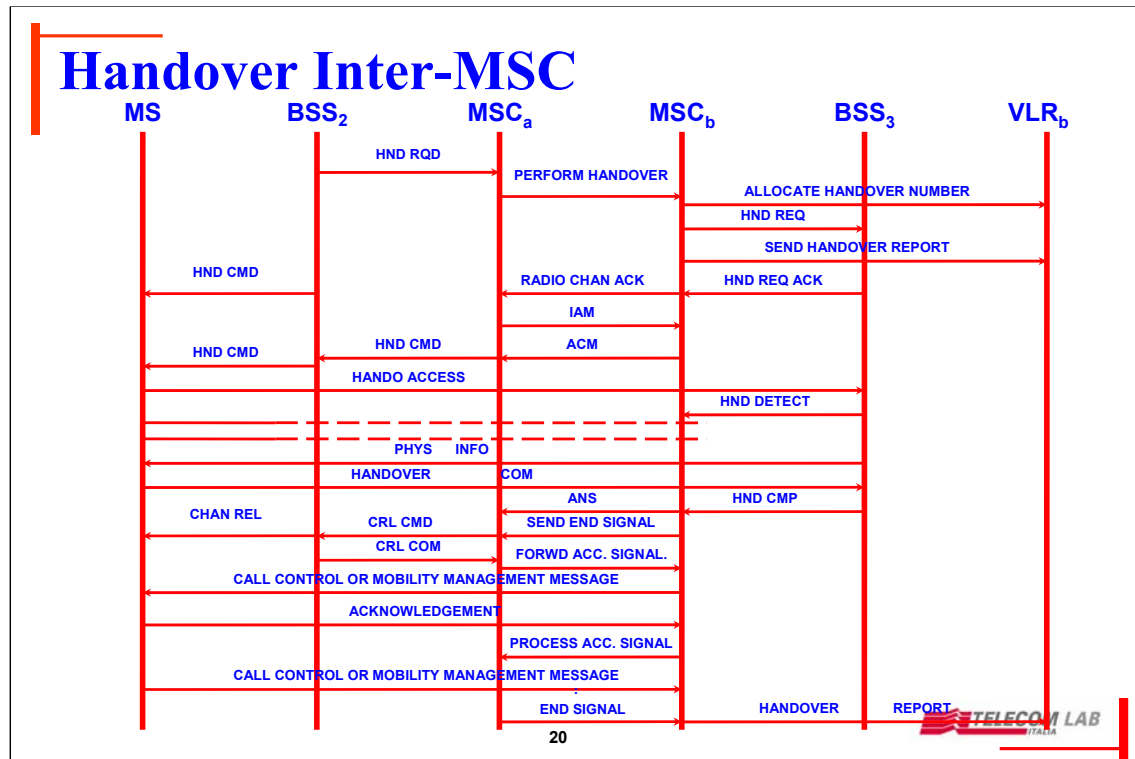
19

TELECOM LAB
ITALIA

With reference to the previous figure, this diagram describes an intra -MSCa handover, arising between BSS1 and BSS2.

The sequence is self-explanatory.

Note that the dropping of the old path (through BSS1) takes place after the success of the handover towards BSS2 has been guaranteed.



Still with reference to the previous figure, this diagram describes an inter-MSC handover, arising between BSS2 and BSS3 (controlled respectively by MSCa and MSCb).

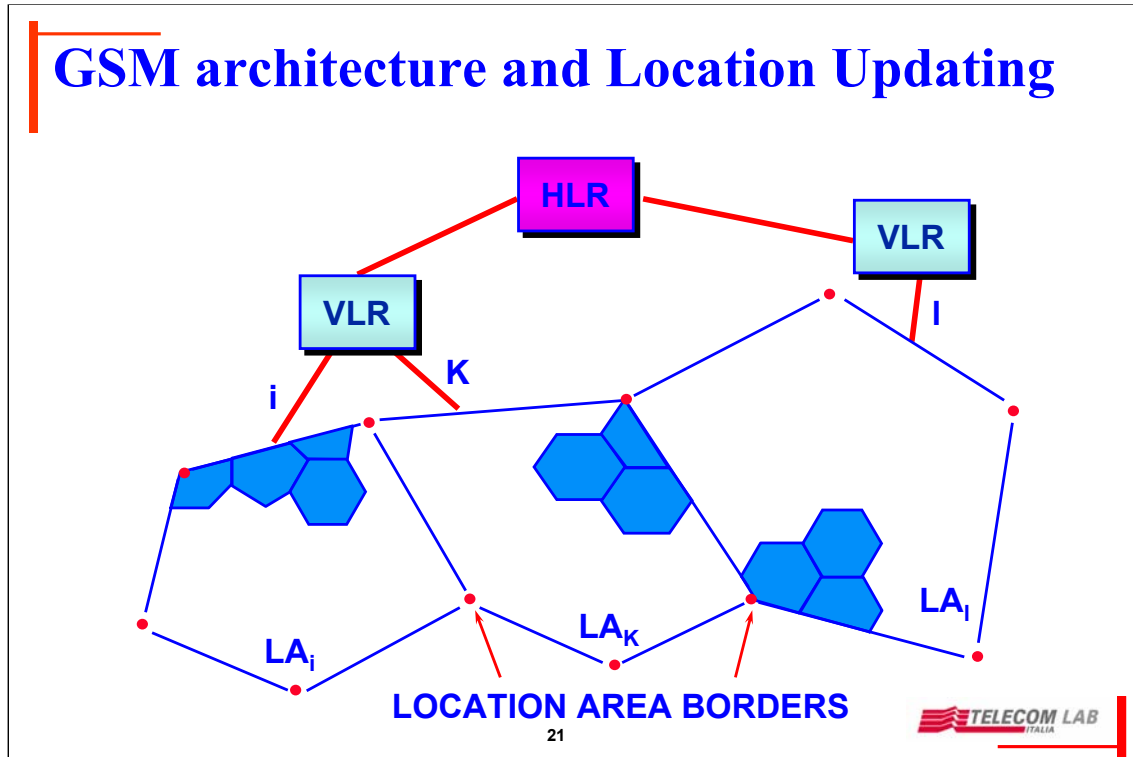
The sequence is self-explanatory.

Note that a link has to be set-up between the two MSCs in order to ensure the needed routing of the new path. The call control is maintained by MSCa as anticipated.

Also in this case, the dropping of the old path (through BSS2) takes place after the success of the handover towards BSS3 has been guaranteed.

The VLR is registering the handover number and the handover outcome. VLR is normally associated to the MSC.

GSM architecture and Location Updating



Location areas are groups of contiguous cells. The network recognises the mobile terminal location according to the location area (LA) granularity and, in conjunction with a LA change, moves the MS data from the old VLR to the new VLR where MS is located. The Home Location Register (HLR) is driving this deletion/registration process and, at the same time, it maintains a pointer to the VLR where MS is located (this is used to route properly the incoming calls). The location is updated whenever the order of a location area is crossed by MS.

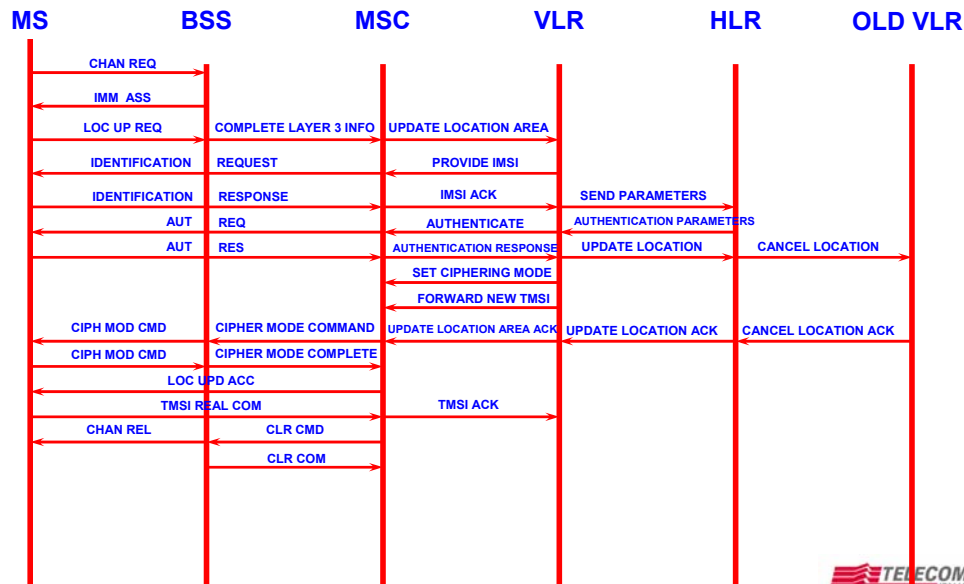
In systems like the GSM, a location area identifies also the set of cells where the paging is broadcast in case of incoming call (Paging Area - PA). The choice of the LA (and PA) size is a typical cellular network optimisation topic. The optimal solution derives from a trade-off between the traffic behaviour and the mobility level of the mobile user. A very high traffic activity associated to a low or vanishing mobility, would require small Location Areas. In fact this solution allows for a low radio resource usage to serve incoming calls (paging) and at the same time keeps limited the location updating load (again on the radio interface) thanks to the low user mobility level. Conversely, a very high mobility level associated with a low traffic activity, calls for bigger Location Areas.

The figure highlights the location updating process adopted for the GSM. The MS is in the idle state. In this condition, it is continuously tuned on the BCCH of the cell where it is roaming (cell selection procedure). Among other information, BCCH is broadcasting to the cell-roaming MSs, the LA identifier of the relevant cell. Accordingly, while changing cell (BCCH), the MS is able to verify if the new cell still belongs to the previous LA or, conversely, if it belongs to a new LA.

This mechanism ensures that MS is able to start a location updating procedure whenever a LA border is crossed.

The location updating procedure moves user's data from the old VLR to the new one (through the HLR). As a particular case, a single VLR can control more than one LA, but this does not modify the procedure described above.

Location Updating Procedure



22

TELECOM LAB
ITALIA

To perform the location updating procedure, MS needs a control channel, specifically an SDCCH channel. The latter is needed even if the entire procedure will not lead to any traffic channel (TCH) set-up. This is an example of *non-call related* procedure.

To be assigned an SDCCH, the MS starts with an access procedure (RACCH) which leads to the assignment of a control channel on which the location updating procedure can take place.

The sequence is self-explanatory.

Note that, in conjunction with the execution of the LU, an authentication procedure is performed by making use of the International Mobile Subscriber Identifier (IMSI). As a consequence, the ciphering parameters are changed. This procedure includes also the assignment of a new Temporary Mobile Subscriber Identifier (TMSI) to the MS.

After the above phase is completed, the update location command is sent to the HLR, which can delete the user data in the old VLR.

The control channel is then released.

SIM Card

Subscriber Identity Module



Contains:

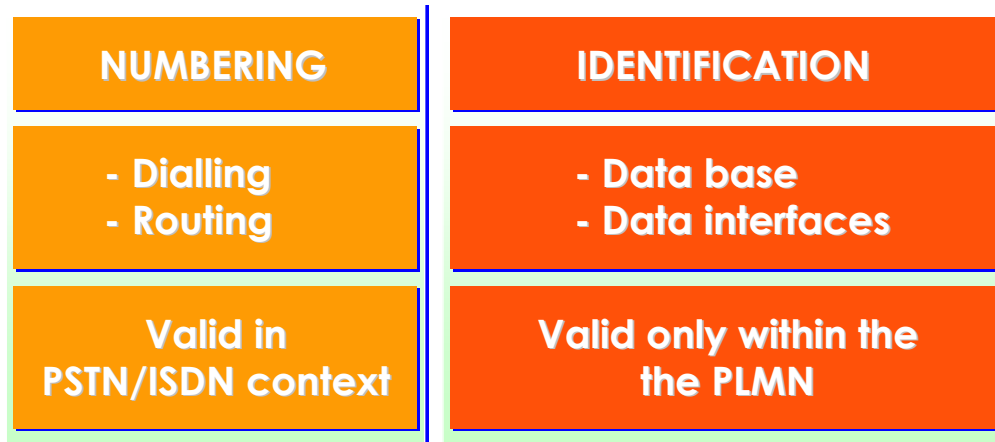
- **number and user identity**
- **authentication key**
- **authentication algorithm A3 and Kc generation (A8)**

23

 **TELECOM LAB**
ITALIA

The basic data for security are contained in the Subscriber Identity Module (SIM) which is a terminal - independent entity. It represents the true personalisation element which has characterised the GSM adventure with respect to all the other second generation systems. The SIM card is an autonomous component, with its own processing and memory capability.

Basic concepts for numbering and identification



24



The separation between *numbering* and *identification* schemes allows to separate specific mobile functions (mobility) from those driving the fixed network processes (routing)

The de-coupling between numbering and the identification levels gives flexibility to the numbering plan modifications and makes possible to associate more than one subscriber number (IMSI) to the same GSM user.

The *numbering* scheme adopted in the mobile network is consistent with the one adopted in the PSTN/ISDN context:

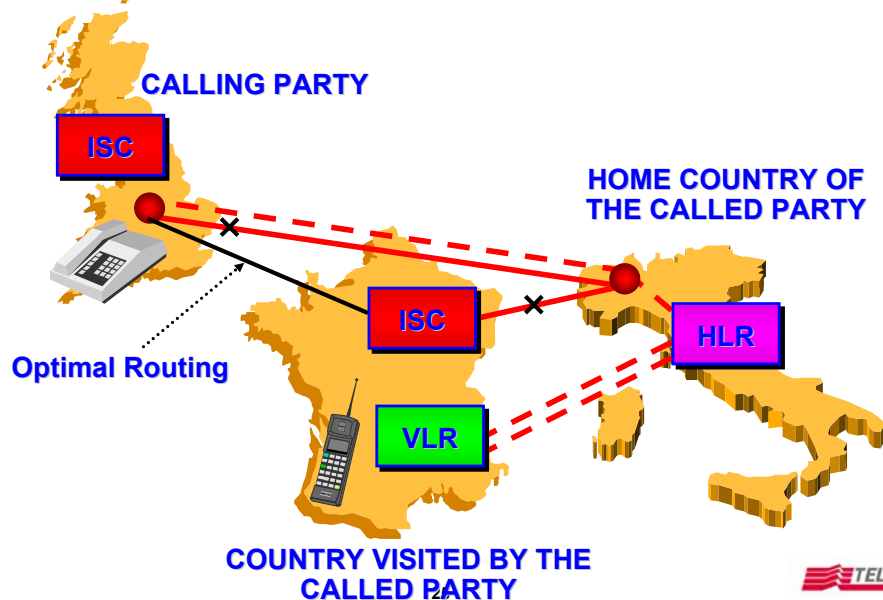
- user ISDN number (dialling, identification calling, called party)
- roaming number (routing towards the actual mobile location).

The *identification* of the mobile user is needed in function of the transactions arising with the data bases and through the data interfaces. The identification numbers are just valid in the Public Land Mobile Network (PLMN).

The main identification numbers are:

- International Mobile Subscriber Identity (IMSI) for the basic identification of the mobile subscriber
- Temporary Mobile Subscriber Identity (TMSI) for the temporary identification of the mobile subscriber; its definition comes from security and efficiency requirements
- International Mobile Equipment Identity (IMEI) for the international identification of the mobile terminal (control purposes).

International routing for a roaming subscriber



The international routing for a roaming subscriber (i.e. for a user located under a *foreign* network) is done through a query to the home HLR, which is continuously updated by the VLRs about the network LA where the user is roaming (the signalling process is represented with a dotted line).

The call routing is then performed by the International Switching Centres (ISCs) through the same path. This in general implies a non-optimal routing configuration and a waste of resources.

An optimised solution could be based on a direct call routing towards the ISC of the hosting country. Nevertheless, this solution requires some modifications to the ISUP protocol. In addition, it poses delicate charging splitting questions: if the optimal routing is implemented, the home network would not share any revenue, even if the relevant signalling links are heavily involved in the overall process.