

Communication Networks 2



Signaling (Mobile)

Gusztáv Adamis

BME TMIT

2018

Channel Associated Signaling

- ❑ Originally: analogue systems
 - or in the voice channel itself – in-band signaling
 - or in a signaling channel associated to the voice line – out-of-band signaling
- ❑ Later: digital
 - Signaling bits in a signaling channel associated to the voice line (PCM signaling channel) – out-of-band signaling

Channel Associated Signaling

□ Advantages:

- simple
- relation between signal and voice channel is obvious

□ Disadvantages:

- limited signaling transfer capability
- signal transfer is not protected
- different signaling for different services

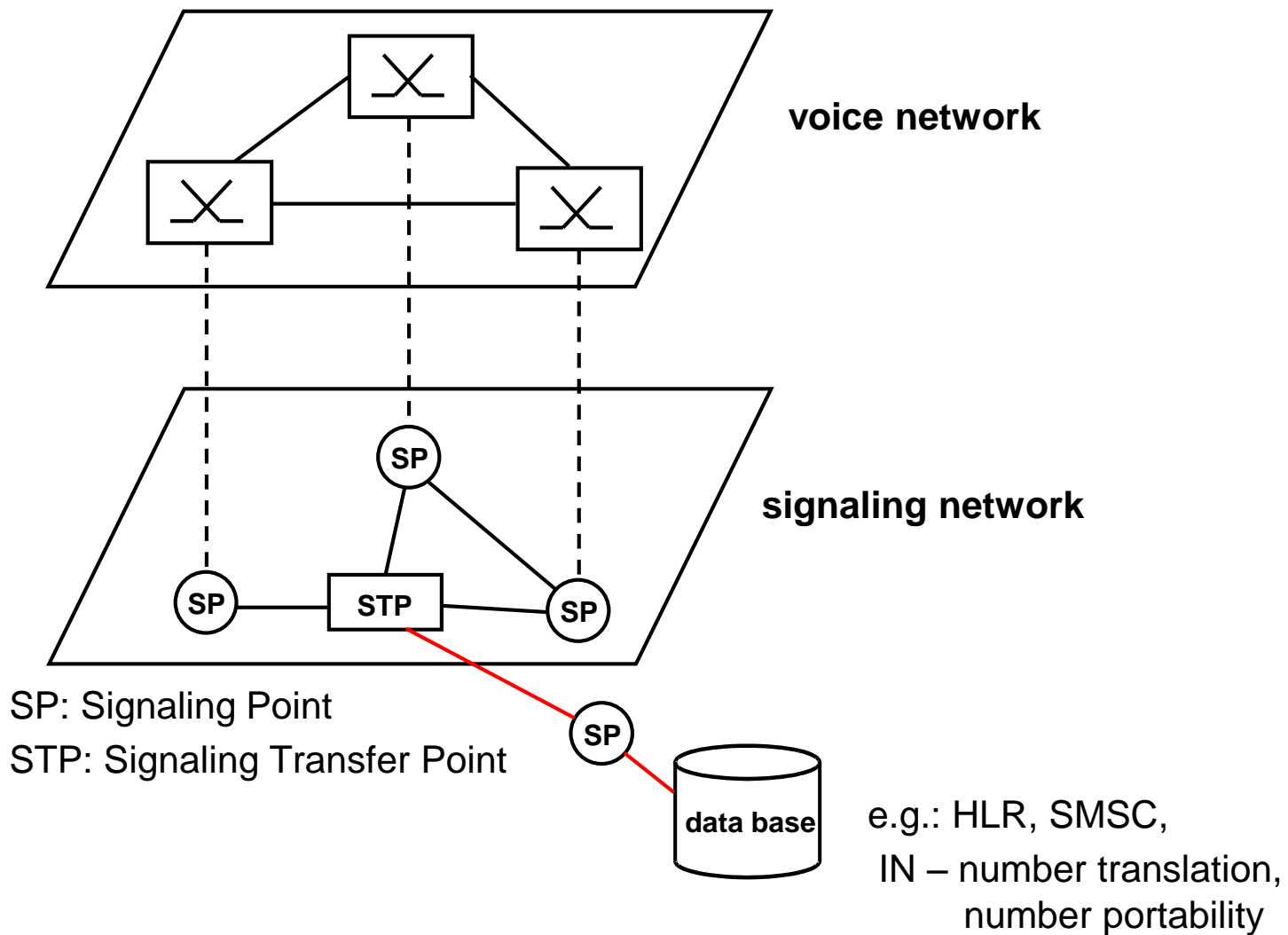
□ No non-call-related signal

Common Channel Signaling Systems

- ❑ Digital signals on a dedicated signaling channel that is independent from the voice channel
- ❑ Idea: not to occupy a voice channel for several, short (~100 byte) signals
- ❑ Advantages:
 - better utilisation of voice circuits
 - more complicated signals: lot of services can be controlled
 - signal transfer can be protected more than voice transfer
 - internal (e.g. management) messages possible
 - non-voice-related (e.g. data base query) signals possible (!!!!!)
- ❑ Disadvantages:
 - separated signaling network → plus cost
 - more complicated functioning of switches, etc.
 - voice path to be established separately – may be checked (call continuity control)
- ❑ More advantages...

Common Channel Signaling Systems

□ Separate signaling network



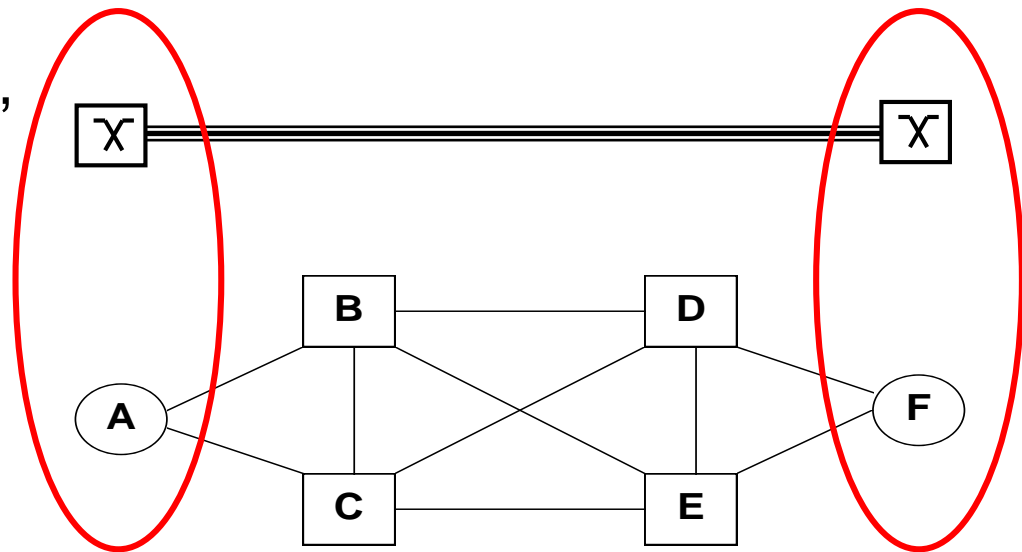
Connection Types

□ Associated connection

- Same path for link and circuit
 - different, dedicated time slots
 - different, dedicated cables

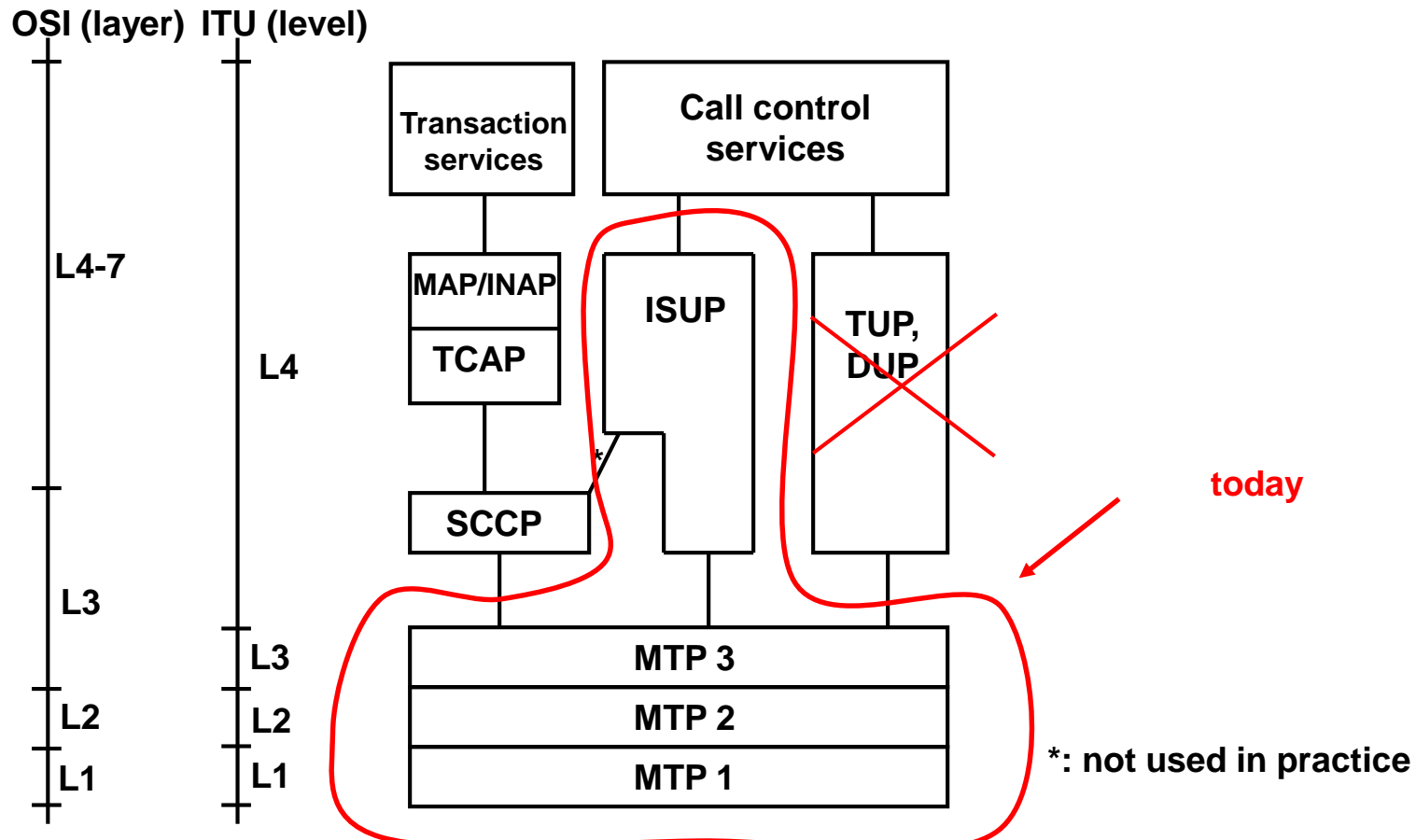
□ Quasi-associated connection

- Different paths
- “6 sub-network”



(CC)SS7

- „The” Common Channel Signaling System: SS7
- (CC)SS7 = (Common Channel) Signaling System No. 7,
- OSI-like architecture:

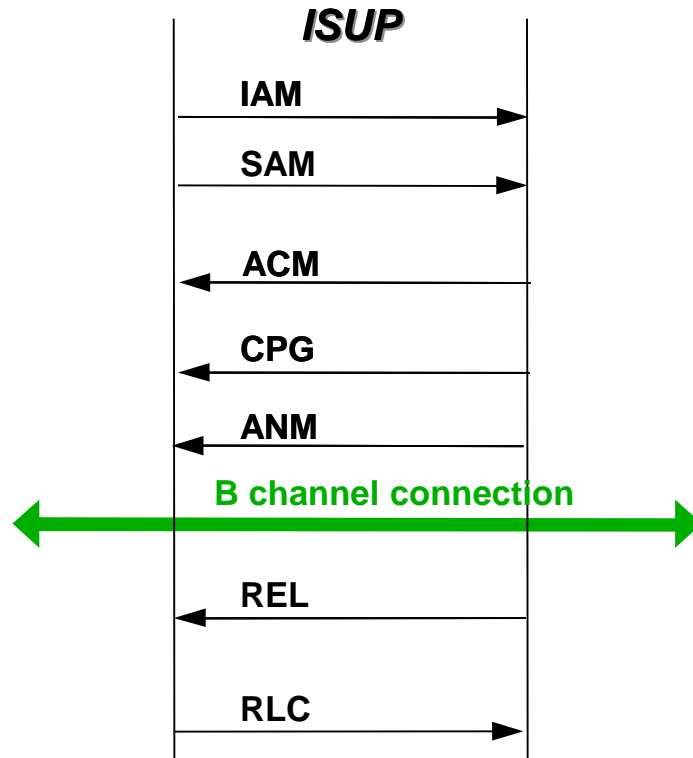


- MTP: Message Transfer Part
- MTP-1: physical level -- 64 kbps digital channel
- MTP-2: framing, error free transmission between neighbouring points
 - 3 types of signaling messages:
 - MSU, Message Signal Unit – carries signals from UPs (e.g. call control)
 - FISU, Fill-In Signal Unit
when no „useful” signal to be sent – empty signal to maintain synchronisation + acknowledgement
 - LSSU, Link Status Signal Unit – used to indicate the status of the link – processed by SNM

- MTP-3: message transfer between any two signaling points within a signaling network (national, national interconnecting, international networks)
 - two ends of every voice circuit are always in the same network
 - problem in GSM control: SCCP will be the solution
- + Signaling Network Management

- TUP, DUP: Telephony User Part, Data User Part
 - withdrawn → ISUP
- ISUP: ISDN User Part
 - call control/release messages with a lot of parameters
 - circuit supervision

ISUP call establishment/release



IAM: Initial Address Message,
SAM: Subsequent Address Message,
ACM: Address Complete

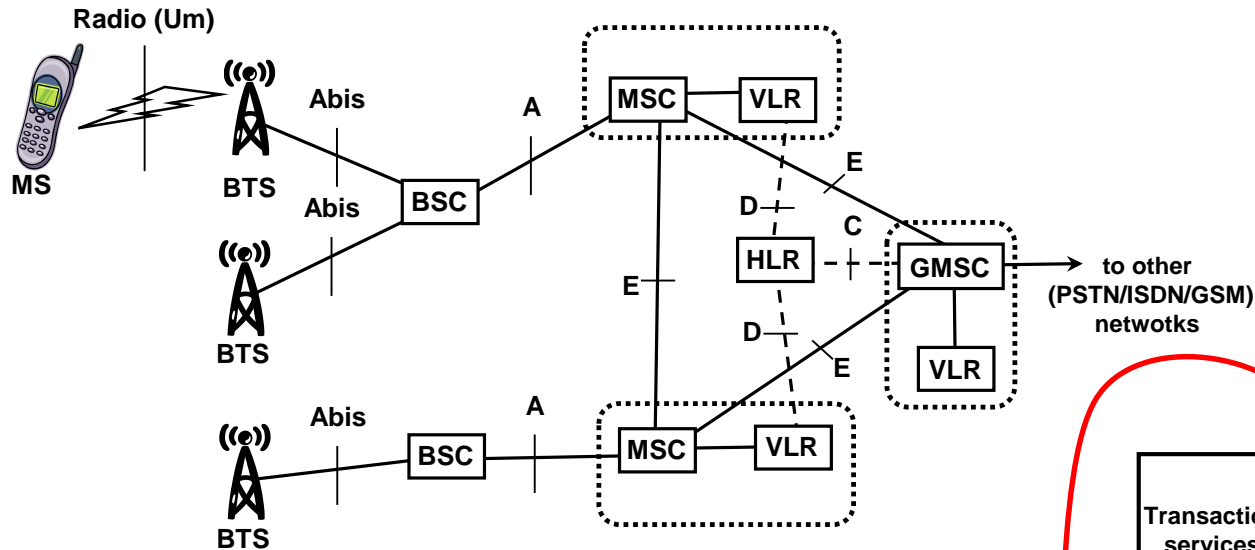
CPG: Call (in) Progress,
ANM: Answer Message
REL: Release
RLC: Release Complete

GSM signaling

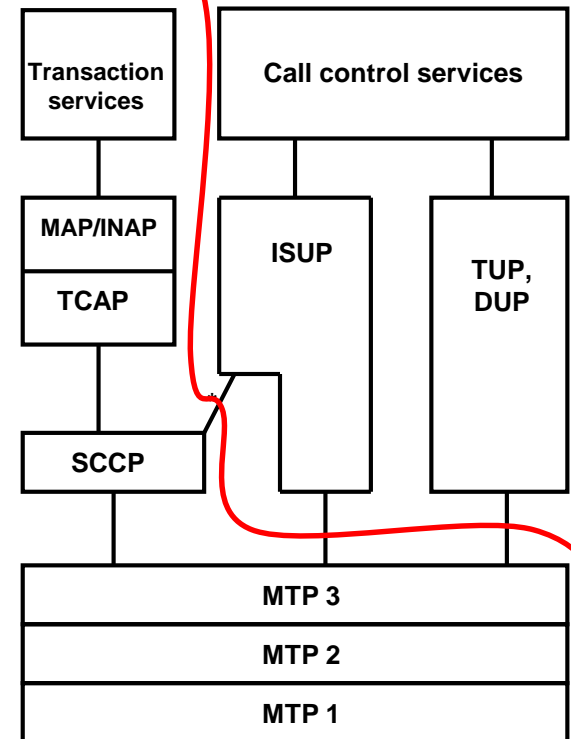


- Signaling of GSM is based on the ISDN signaling systems
 - SS7/DSS1
- But, because of mobility, roaming, radio access a lot of new problems to be solved, e.g.:
 - Authentication of subscribers, encryption of signals/voice transmission (ciphering)
 - Management of query/response transactions
 - e.g.: data base query between the MSC and HLR to learn the location of a called mobile subscriber
 - Establishment of a signaling connection between different signaling networks
 - in case of roaming

GSM interfaces in CS domain



- Continuous line: data (voice) + signaling
- Dashed line: only signaling
- On C, D, E, F & G interfaces: SCCP/TCAP/MAP protocols are used



SCCP

- SCCP: Signaling Connection Control Part
- Main problem: 14 bits long Point Codes used in MTP-3 are not suitable for every SP to have a globally unique address
 - not a problem in call control, because there trunk lines are to be controlled, and two ends of every trunk line belong always to the same network,
 - ISDN: if in a call more than one trunks are used: several, independent signaling connections
 - a signaling connection may be:
 - international
 - in between different operators of the same country (national interconnecting)
 - inside the network of an operator (national – for historical reasons)
 - But in GSM in case of roaming there is a need of a direct signal exchange between network elements of different operators, e.g.:
 - SMSC – MSC
 - HLR – MSC (VLR)

SCCP

- ❑ Solution: Global Titles (global, not SS7-related addresses)
 - Most typically: telephone number
 - A telephone number is assigned to every network element, that may be reached from an other network
- ❑ SCCP translates between the global (tel. number) and local (MTP-3 SPC) addresses
- ❑ 3 different services (SCCP „classes“):
 - connectionless, every signal sent independently (maybe on different route)
 - connectionless, every signal between two particular network elements sent always on the same route (sequence of signals is kept)
 - connection-oriented: connection establishment, usage, clearing phases
 - ❑ used at A interface in call control

- ❑ TCAP: Transaction Capabilities Application Part
 - SCCP provides only the transparent signal transfer
- ❑ TCAP supports the query-response data base transactions
 - e.g.: matches the response with the query
 - a transaction may contain several operations
 - management of operations within a transaction

MAP/INAP

- MAP: Mobile Application Part
- INAP: Intelligent Network Application Part
 - e.g.: green/blue or premium rate number translation
- MAP: management of the communication between the network elements

Identifiers in GSM

□ **MSISDN**: Mobile Station ISDN Number

- telephony number
- unique worldwide
- MSISDN = Country Code (Hungary: 36) + Network Identifier („area code”) (Hungary:20/30/70) + Subscriber Number

□ **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 so the IMSI must be changed

Identifiers in GSM

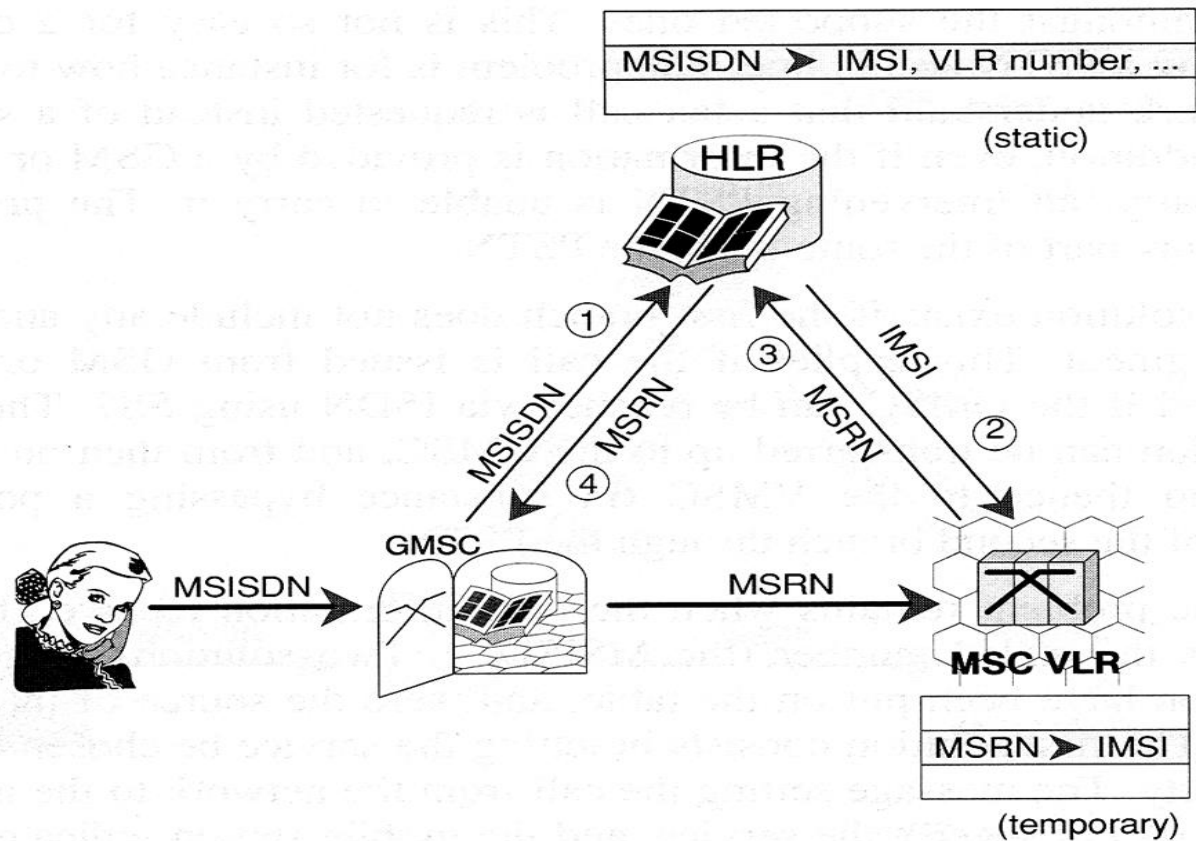
□ IMEI: International Mobile Equipment Identity

- identifier of the mobile terminal
- unique worldwide
- IMEI = <equipment type+producer id> (8 digits) + <serial number> (6 digits) + <control digit> (1 digit) (+<software version id> (1 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

Identifiers in GSM

□ MSRN: Mobile Station Roaming Number

- used when a MS is called
- assigned to MSC(VLR)



User Confidentiality

□ Authentication

- Verification of the identity of the subscriber

□ Ciphering

- Encryption of user speech and signal transmission in the Air interface

□ 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 in the air interface – TMSI

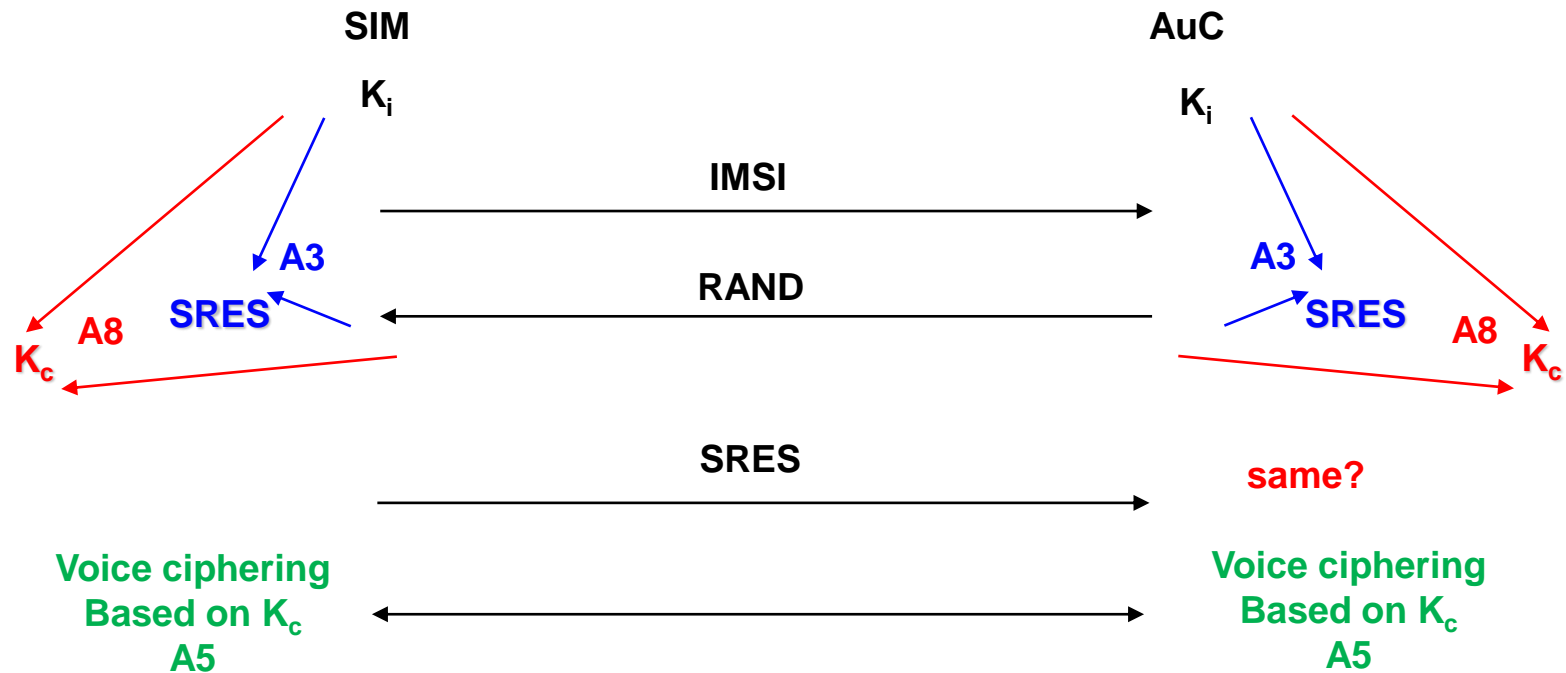
Authentication

- ❑ Problem: On the Radio Interface anyone can call in the name of anyone else by using a public identifier
 - And the cheater pays...
- ❑ Therefore the network must check the identity - authentication
- ❑ Private identifier needed
- ❑ But this must NEVER be transmitted through the radio interface
- ❑ But, then how ????

Authentication

- 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

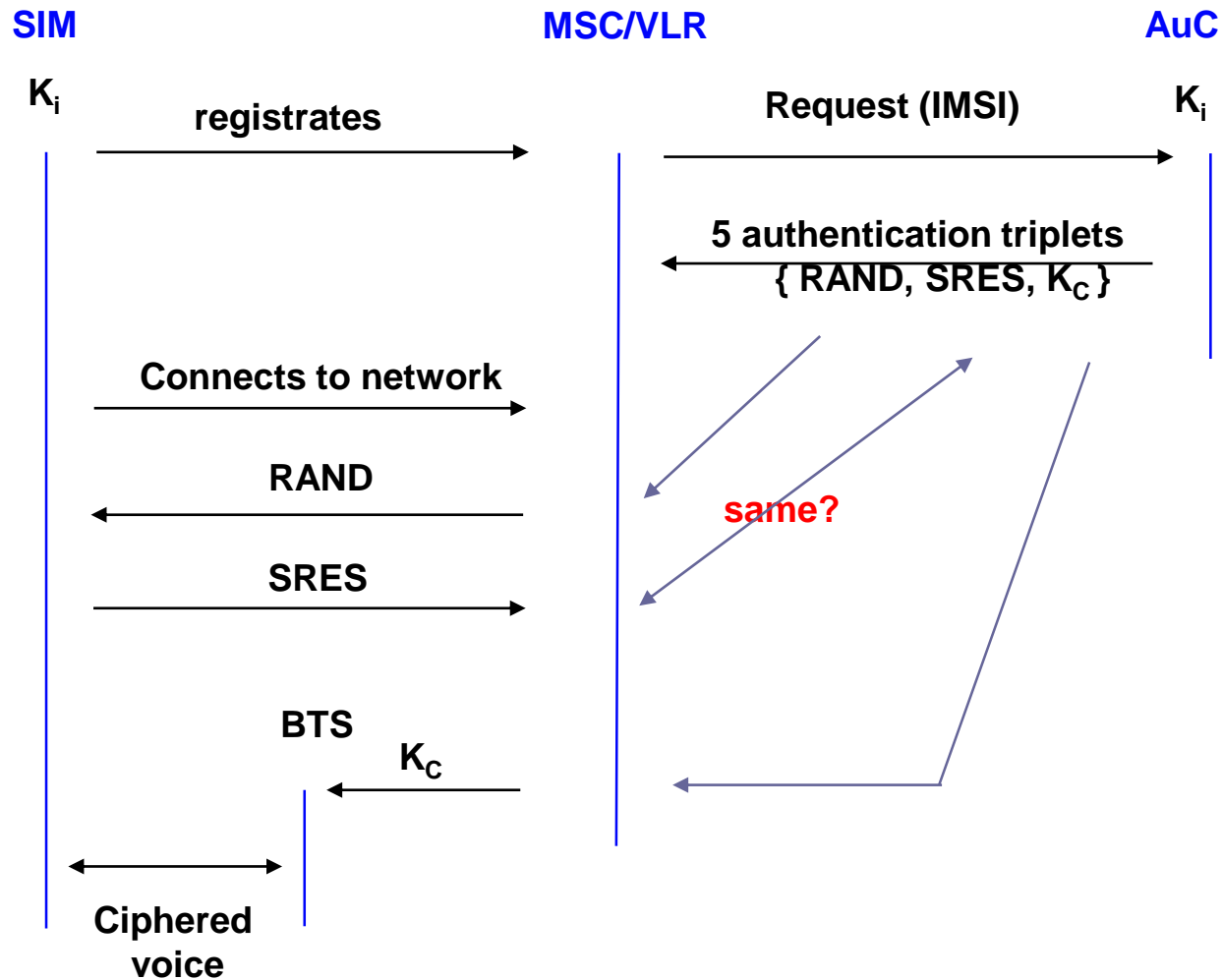
Authentication – theory



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

REQUIRES TOO LARGE Signaling TRAFFIC
LET US INVOLVE THE SERVING MSC!

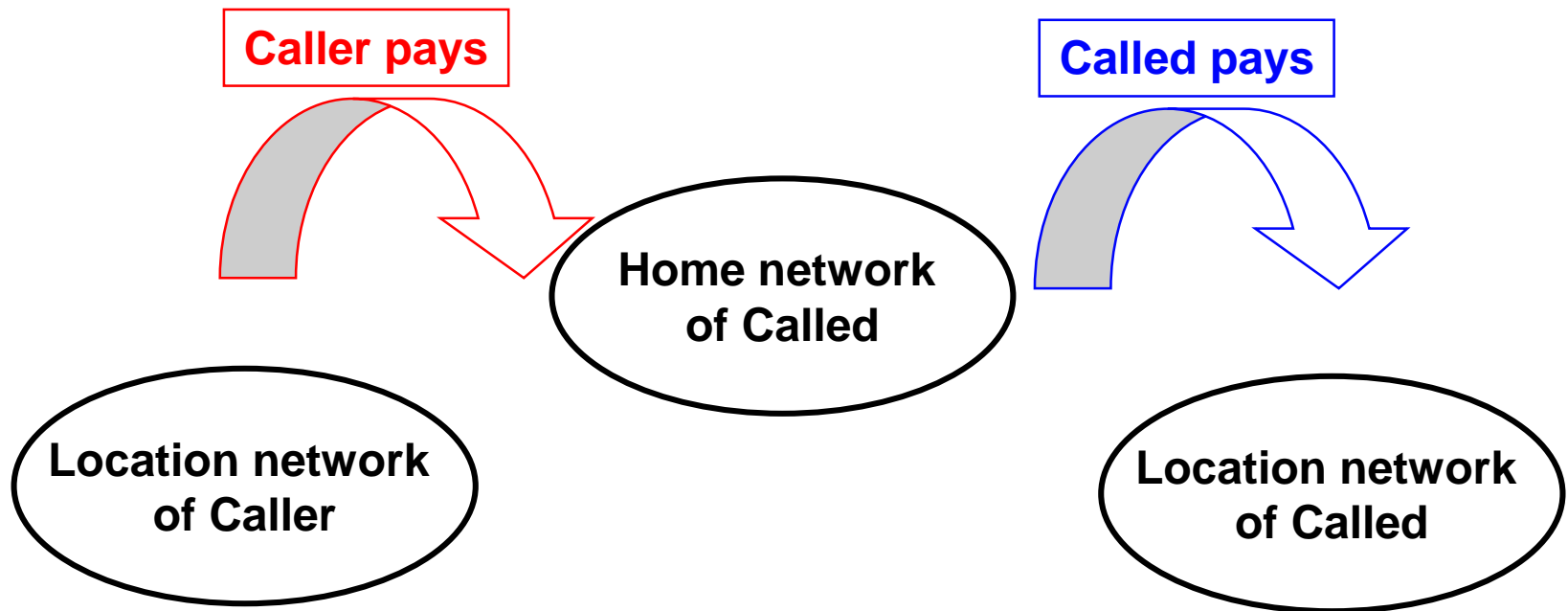
Authentication – practical implementation



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



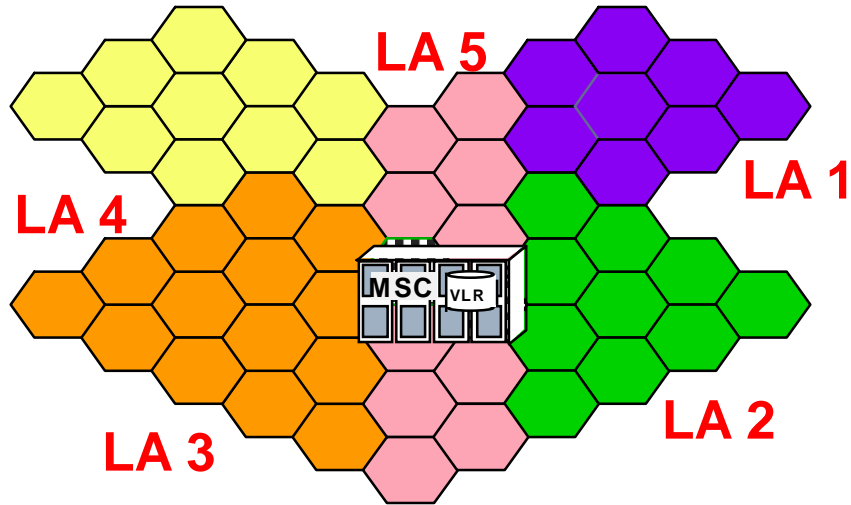
Usage of TMSI instead of IMSI

- ❑ Do not send „sensitive” identifier through radio IF
- ❑ At very first connection (LU): IMSI
- ❑ MSC gives a „random” identifier (this is the TMSI)
- ❑ At next connection – use TMSI instead of IMSI
- ❑ But how can the MSC whether the TMSI was assigned by itself or by an other MSC?
- ❑ MS sends not only the TMSI, but the LAI where it got the TMSI
- ❑ If LAI not own, MSC asks the „old” MSC

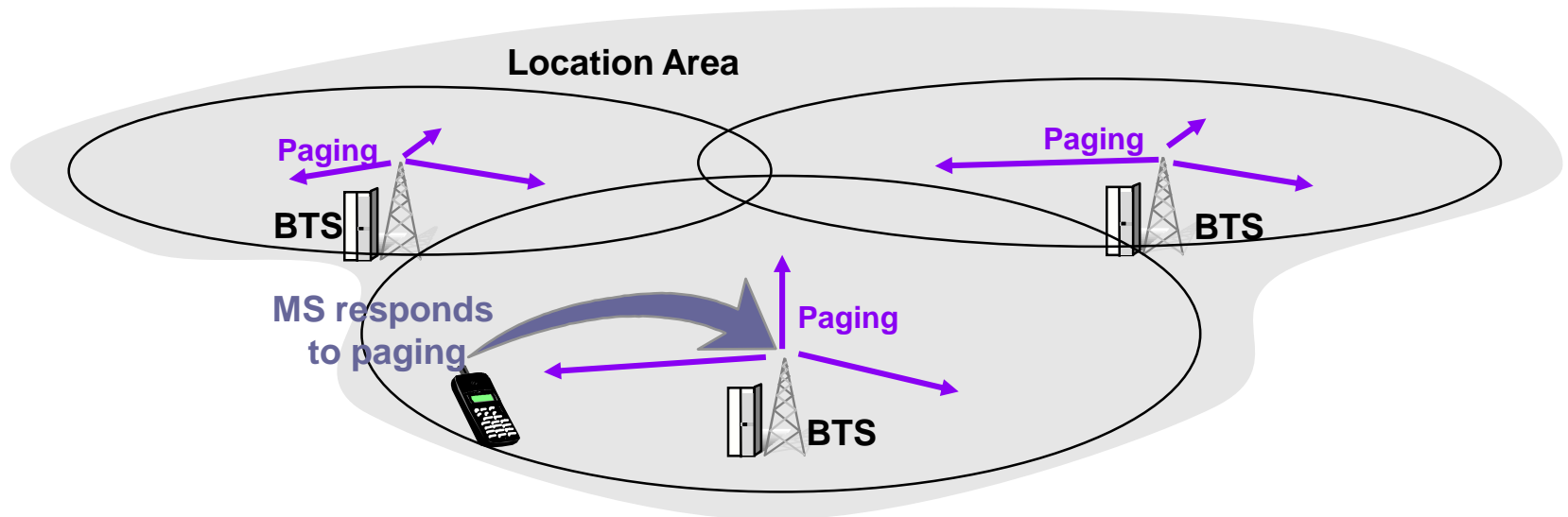
Mobility Management (MM)

- 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

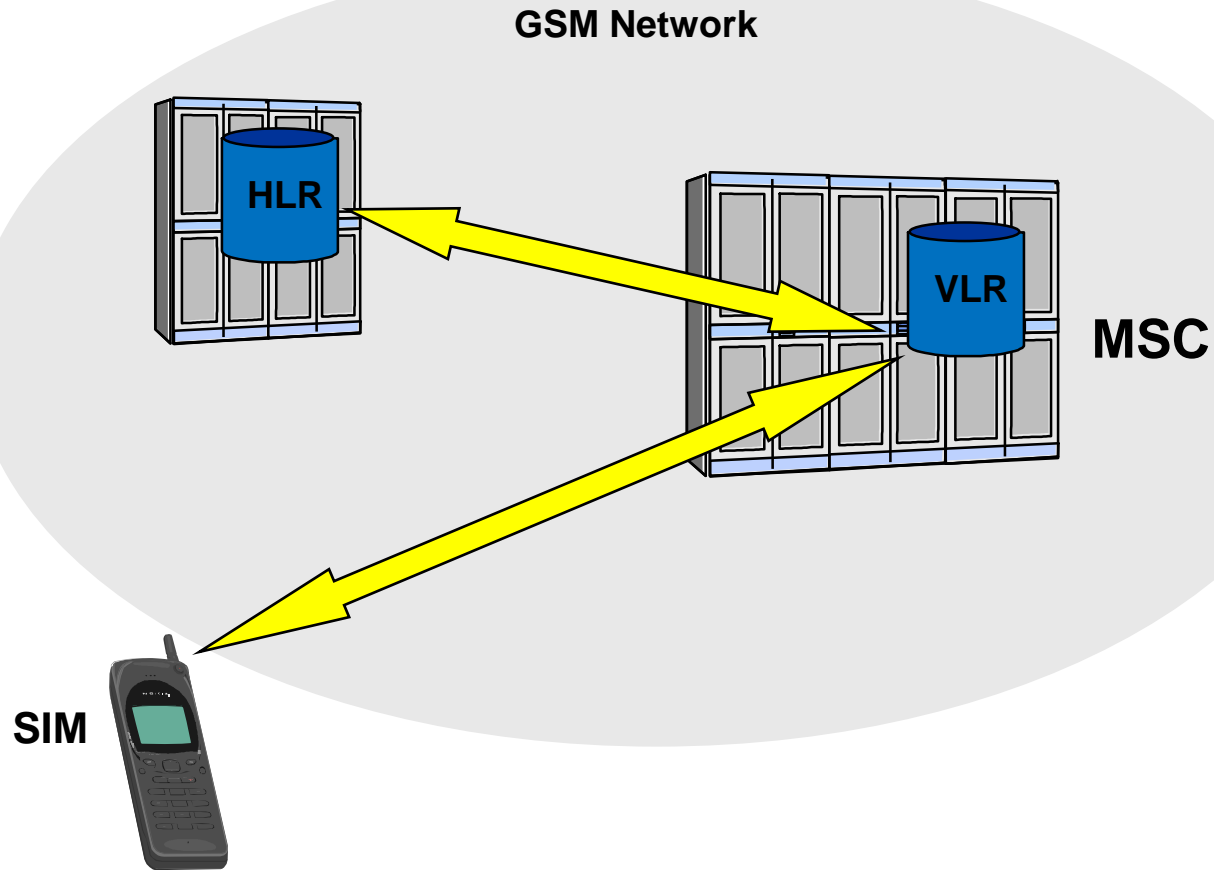
Location Areas



- 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



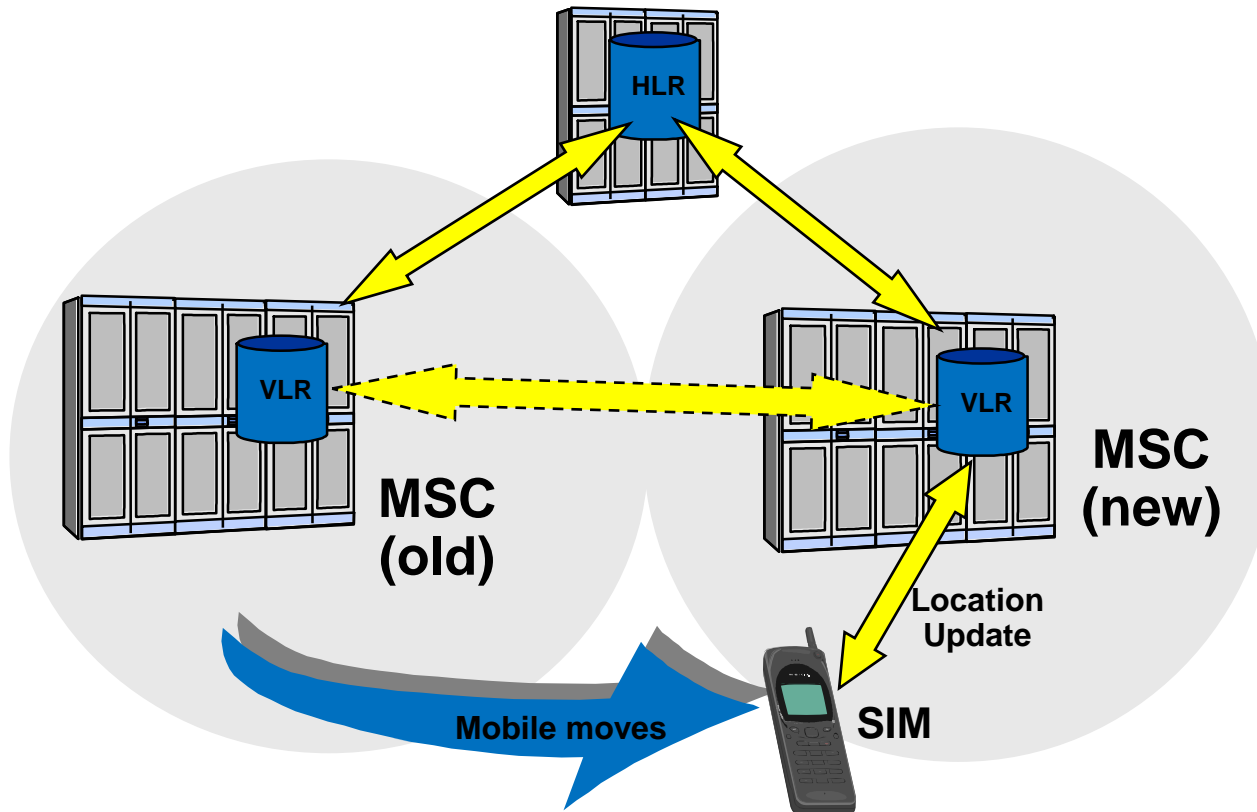
Databases involved in MM in a GSM Network



Location update

- ❑ The Mobile Station monitors the information broadcast by the network (BTS)
- ❑ The Mobile Station stores the current location area identity (LAI) in 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



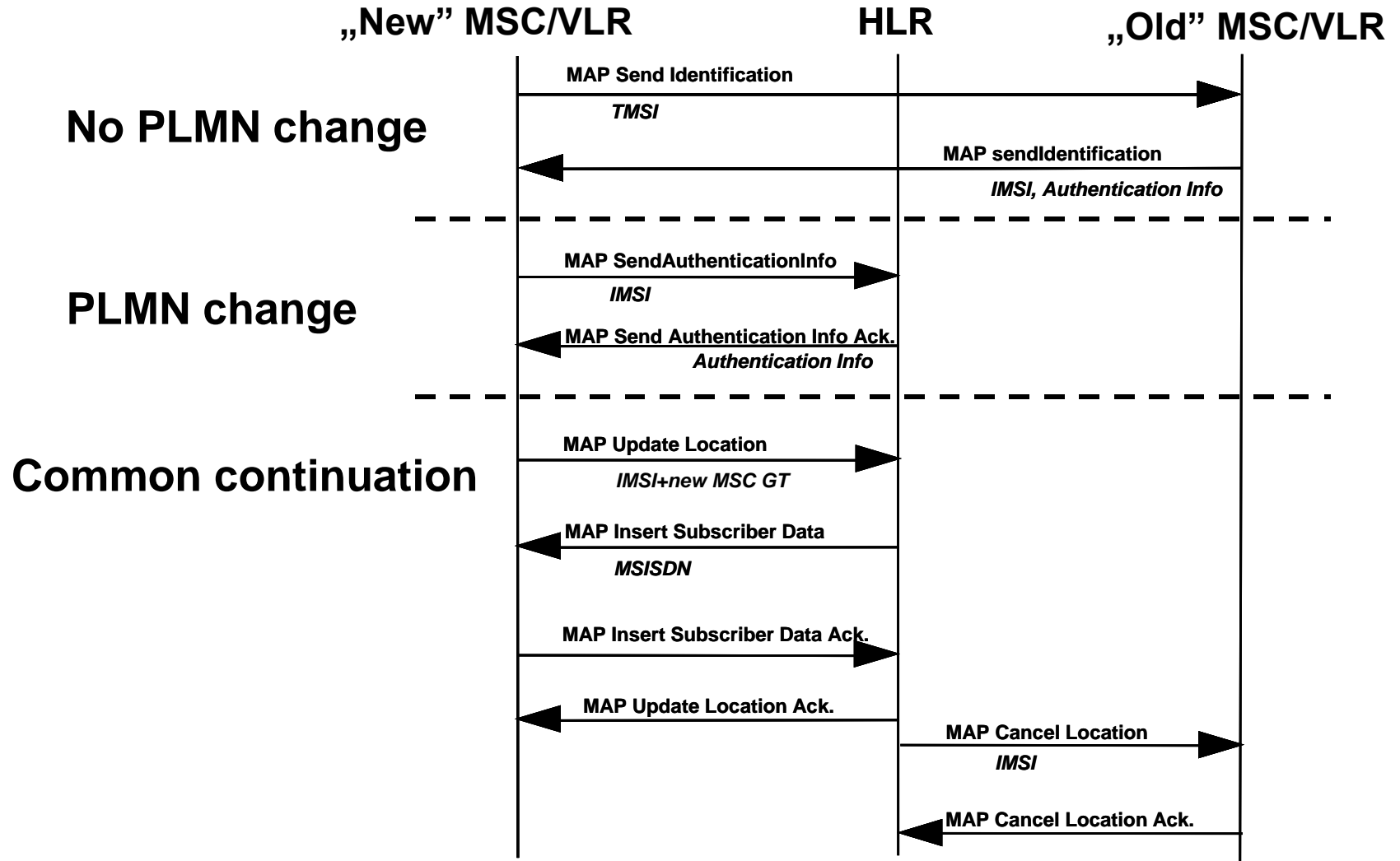
1. „New” MSC/VLR acquires:

- IMSI,
- User Profile (MSISDN),
- Authentication triplets

2. Inform HLR about new MSC area

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

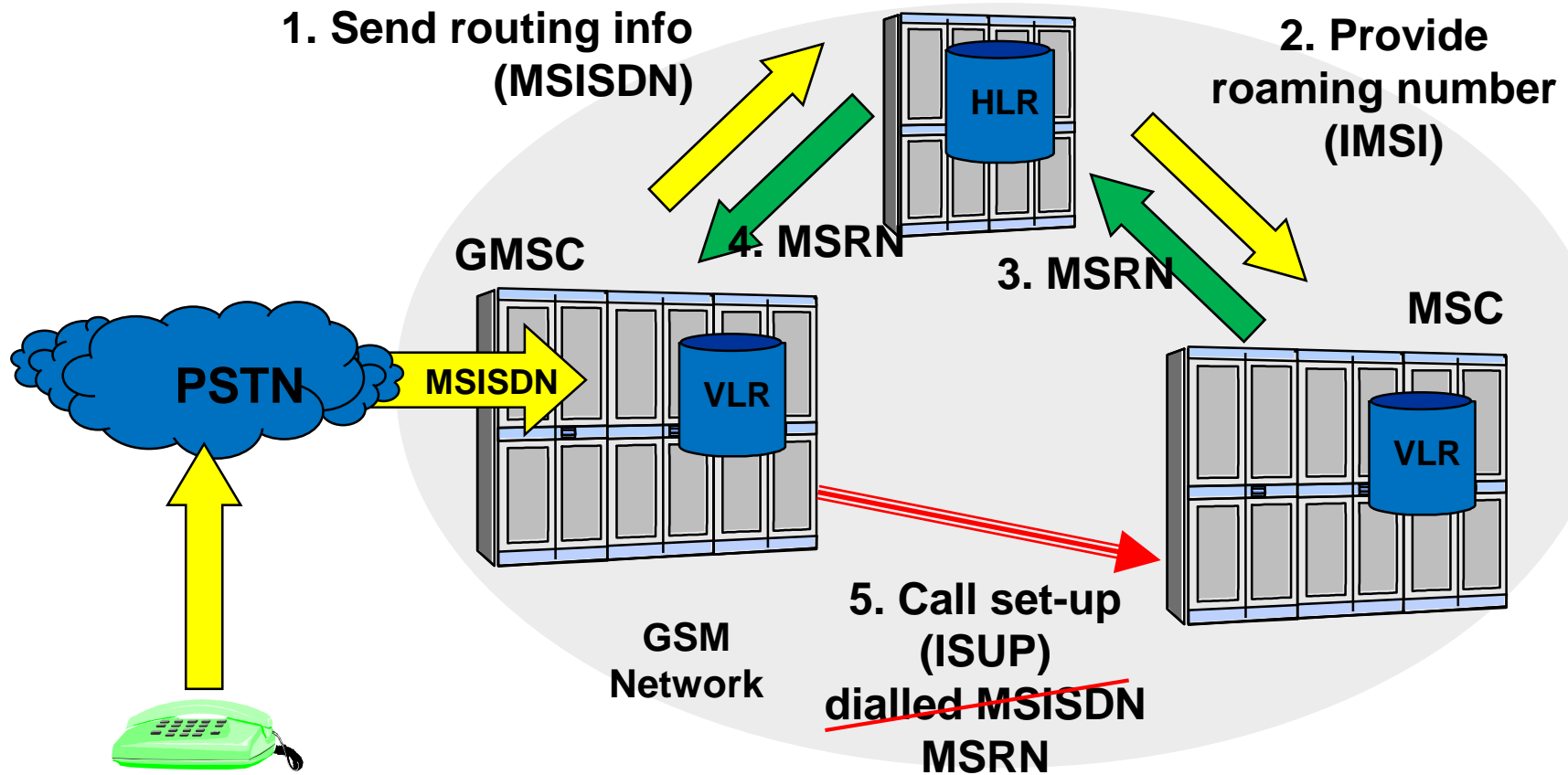
Location Update



LU variants

- „Normal” (Generic LU)
- Periodic
- Switch on (IMSI Attach)
- Switch off (IMSI Detach)

Routing the call inside the GSM network



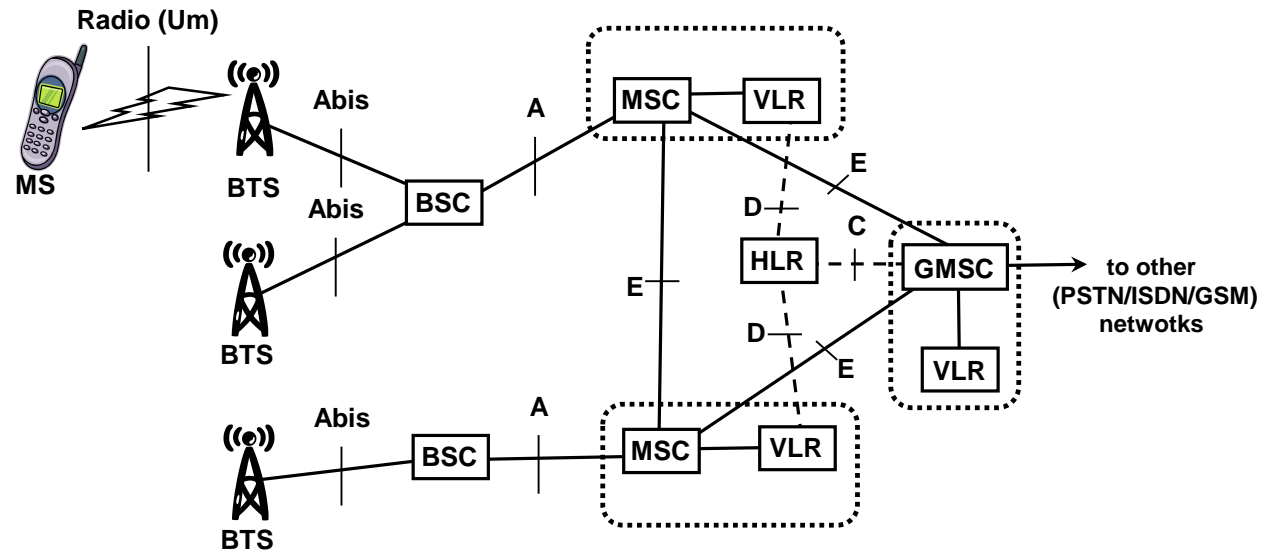
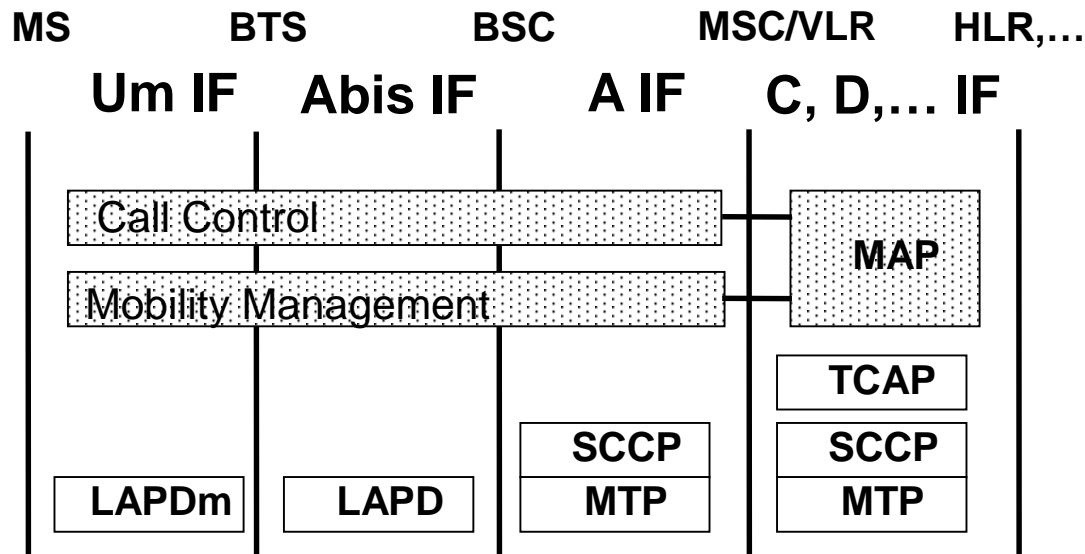
**HLR and serving MSC (VMSC – Visited MSC) may be in different networks –
SCCP Global Title**

**GMSC and serving MSC (VMSC – Visited MSC) may be in different networks –
(international) transit switches**

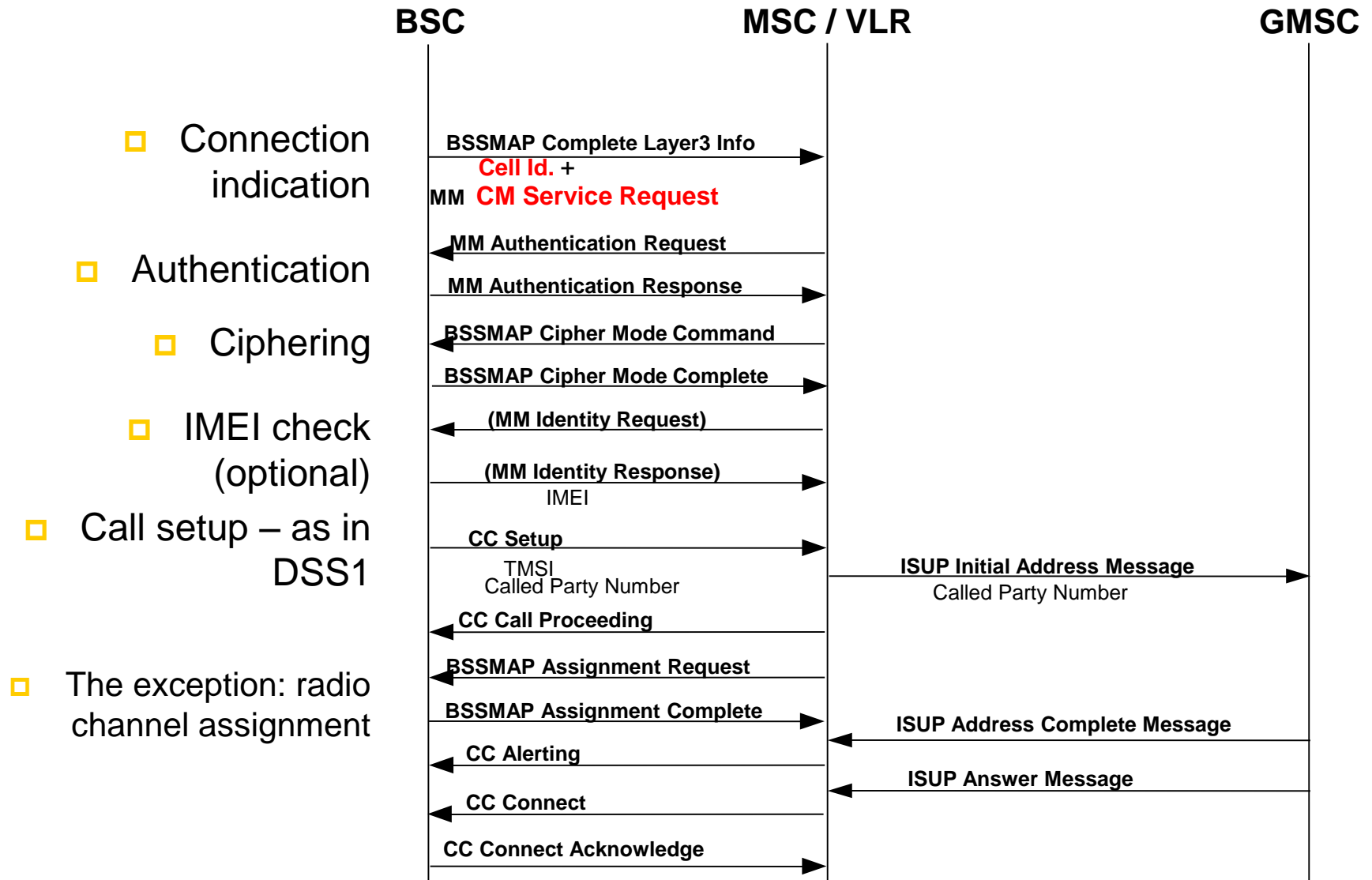
GSM protocols

- ❑ 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)

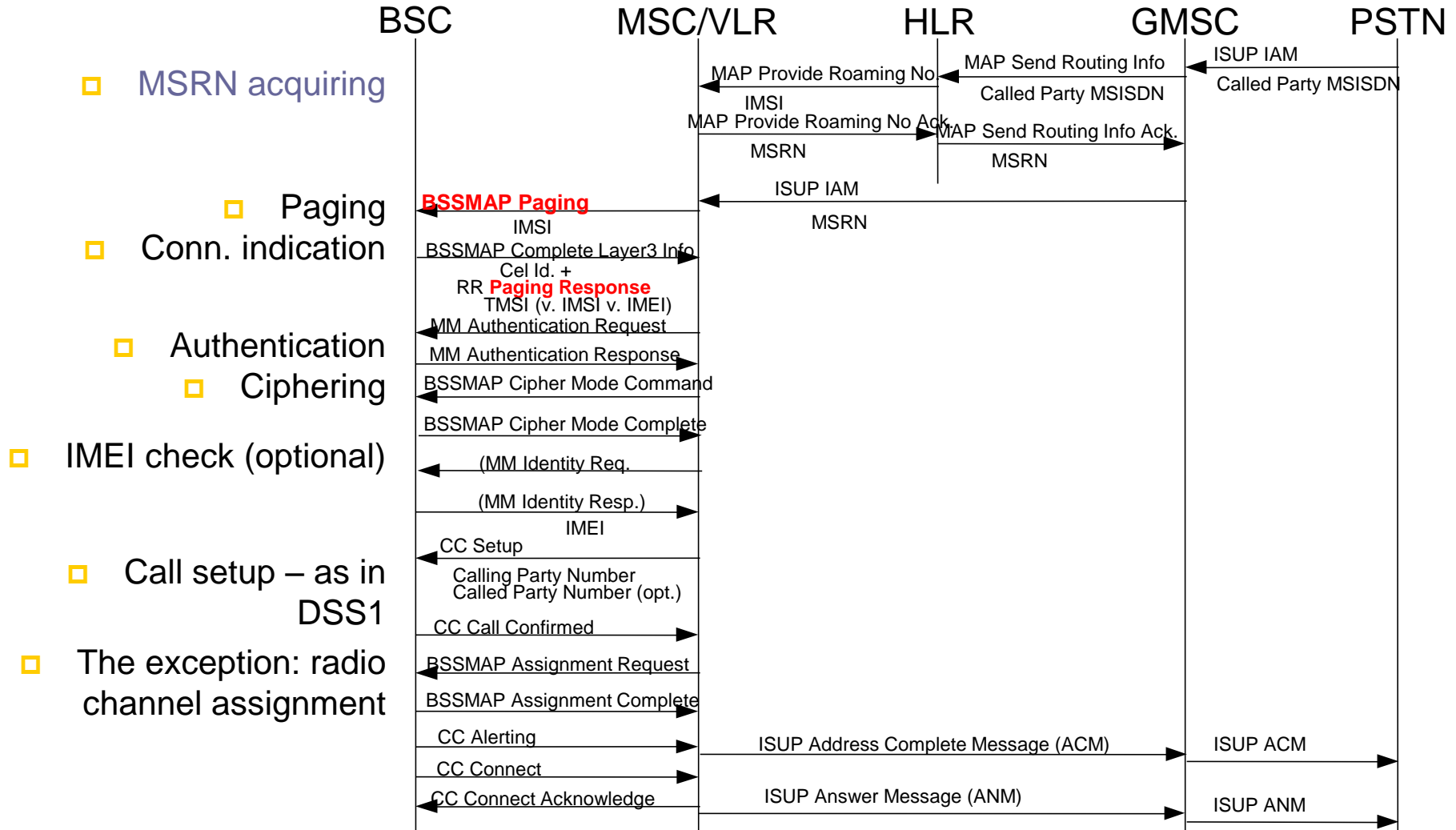
GSM protocols



Mobile Originated (MO) Call



Mobile Terminated (MT) Call



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

