Protocol Technology

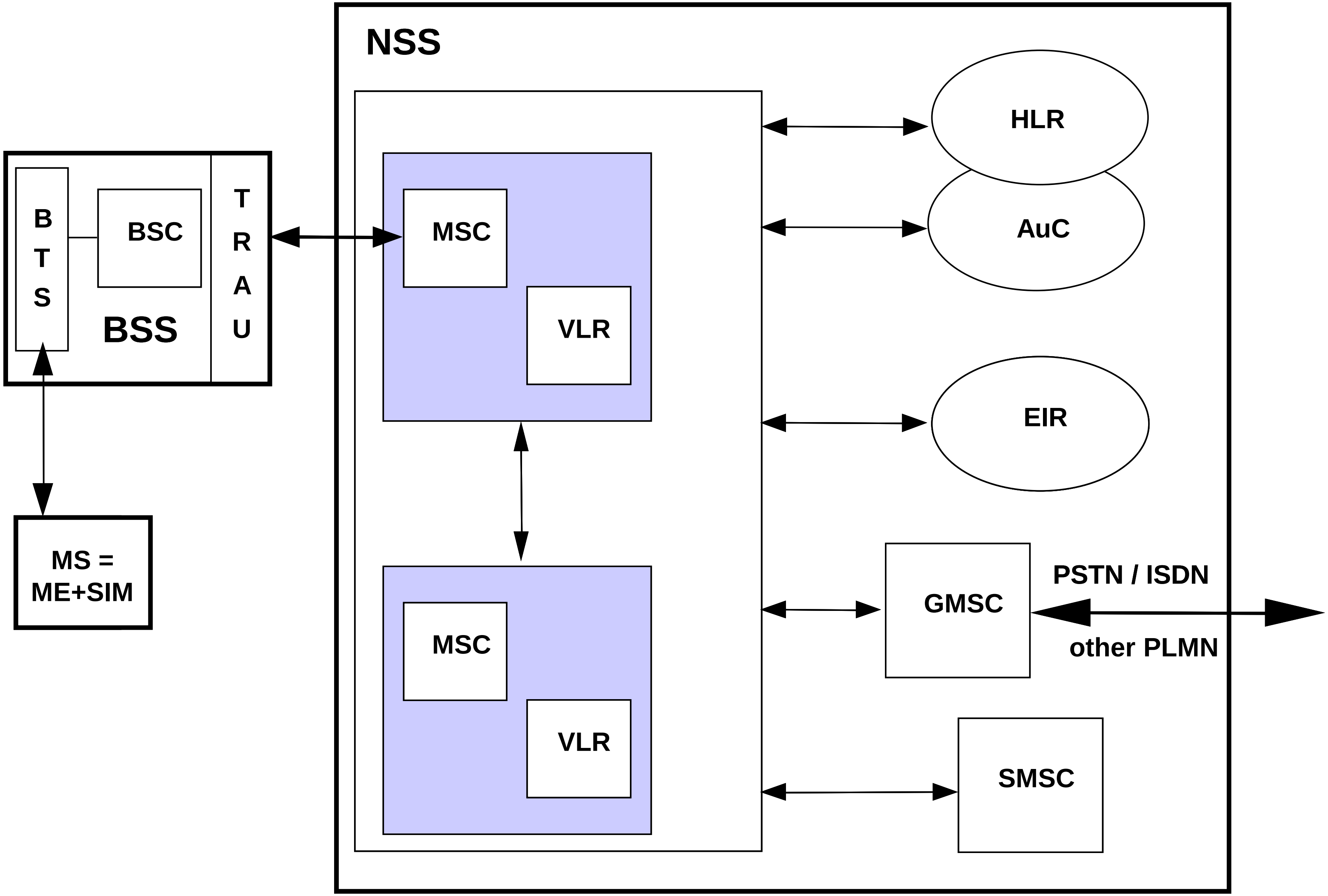
Mobile Networks, Protocols, Services

Gusztáv Adamis

BME TMIT

2016

Architecture of GSM networks



Base Station Subsystem (BSS)

- Base Transciever Station (BTS)
  - One or more elementary transmitter/receiver
  - Transcoder/Rate Adapter Unit, TRAU
    - FR, HR, EFR codec ⇔ 64 kbps PCM
      - Full Rate (13 kbps), Half Rate (5.6 kbps), Enhanced Full Rate (12.2 kbps, but better than FR)
    - Rate adaptation also at data transmission: 14.4 kbps ⇔ 64 kbps
- Base Station Controller (BSC)
  - Controls one or *more* BTSs
  - Radio channel assignment
  - Handover control

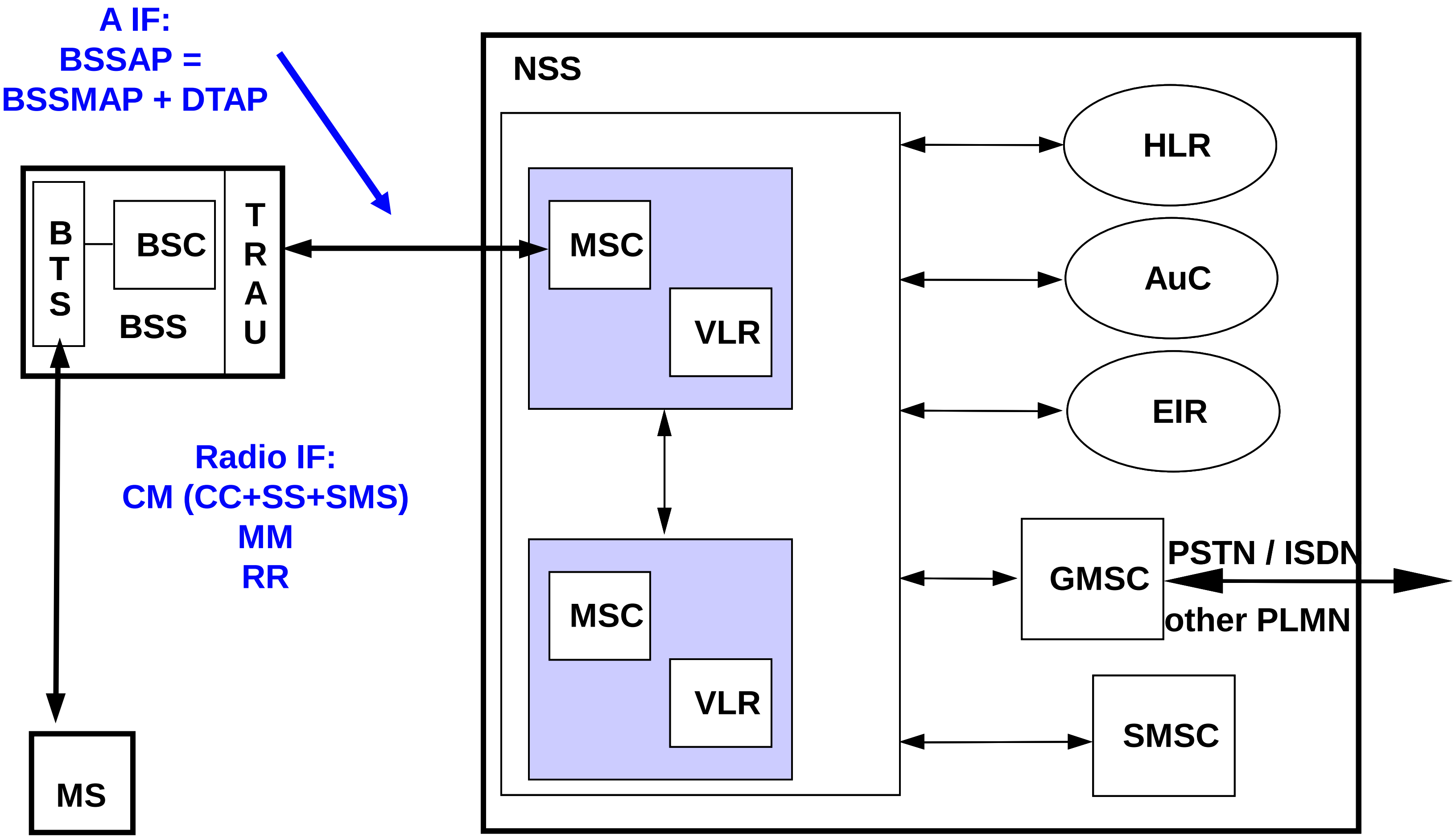
Network and Switching Subsystem

- Mobile Switching Centre (MSC)
  - a digital switch
  - with mobile specific extensions
    - authentication
    - location management (VLR)
    - inter-BSC handover
    - roaming
- Visitor Location Register (VLR)
  - Built in the MSC
  - Stores temporarily some parts of the HLR info about the currently served mobile stations
- Home Location Register (HLR)
  - subscriber data, subscription information (services), current location
  - one HLR in every network
- Authentication Centre (AuC)
  - Typically integrated with HLR
  - It verifies that the subscriber is the same in reality as he is proposed to be

GSM signalling

- Signalling of GSM is based on the ISDN signalling 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 signalling connection between different signalling networks
    - in case of roaming

Mobile Protocols

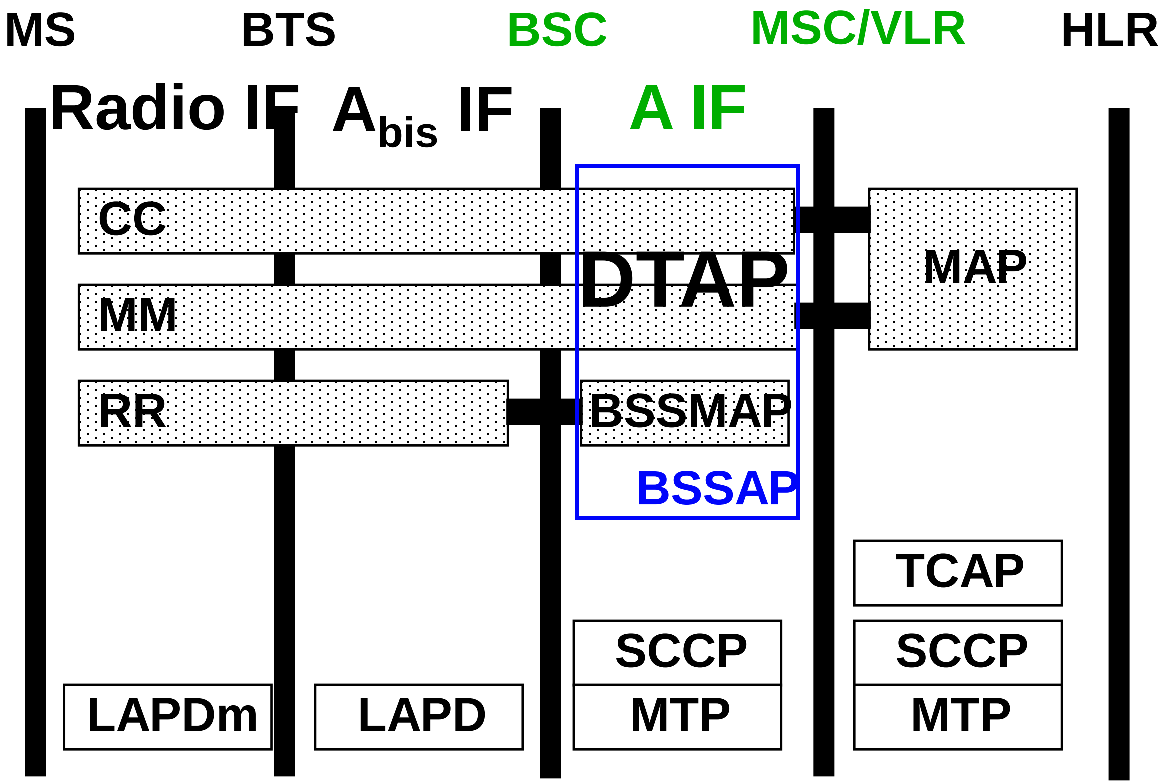


A IF:
BSSAP =
BSSMAP + DTAP

Radio IF:
CM (CC+SS+SMS)
MM
RR

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

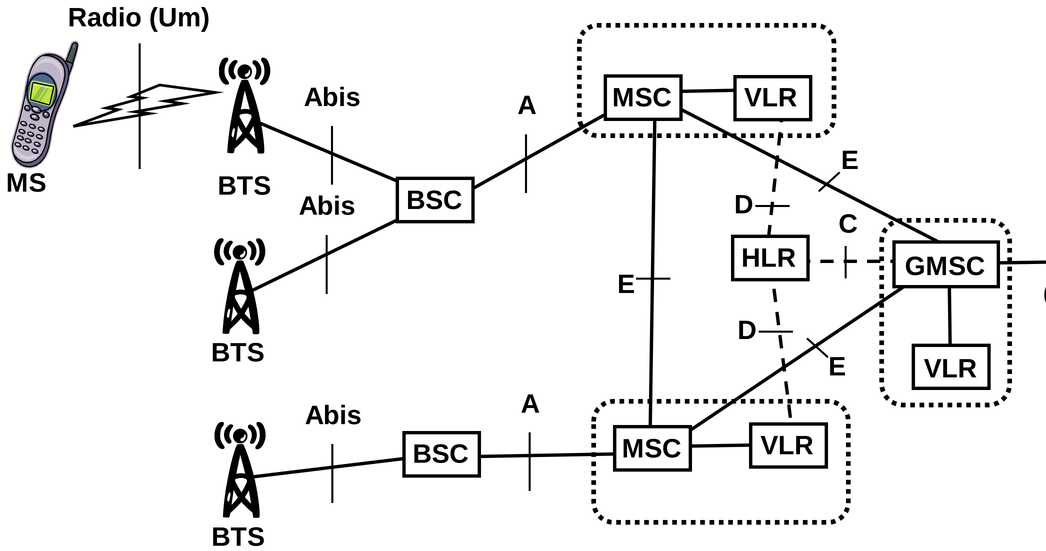
Mobile Protocols



BSSAP: Base Station Subsystem Application Part =
BSSMAP: Base Station Subsystem Management Application Part +
DTAP: Direct Transfer Application Part

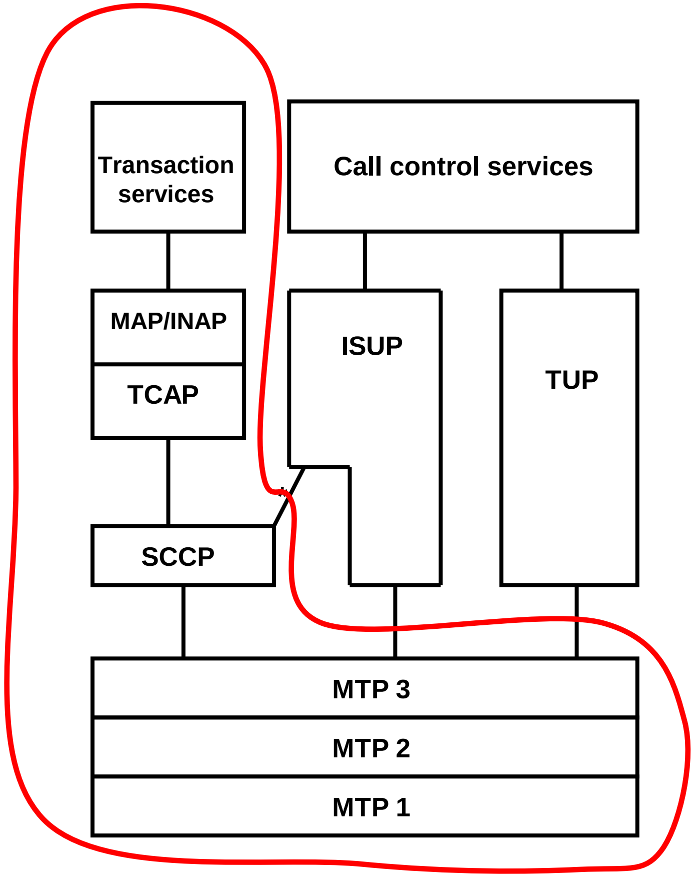
CC: Call Control MM: Mobility Management RR: Radio Resource Management

GSM interfaces in CS domain



to other (PSTN/ISDN/GSM) netwotks

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



MAP/INAP

- MAP: Mobile Application Part
- INAP: Intelligent Network Application Part
  - green/blue or premium rate number translation
  - number portability
  - etc.
- MAP: management of the communication between the network elements at C, D, E, F, G interfaces of GSM

Identifiers in GSM

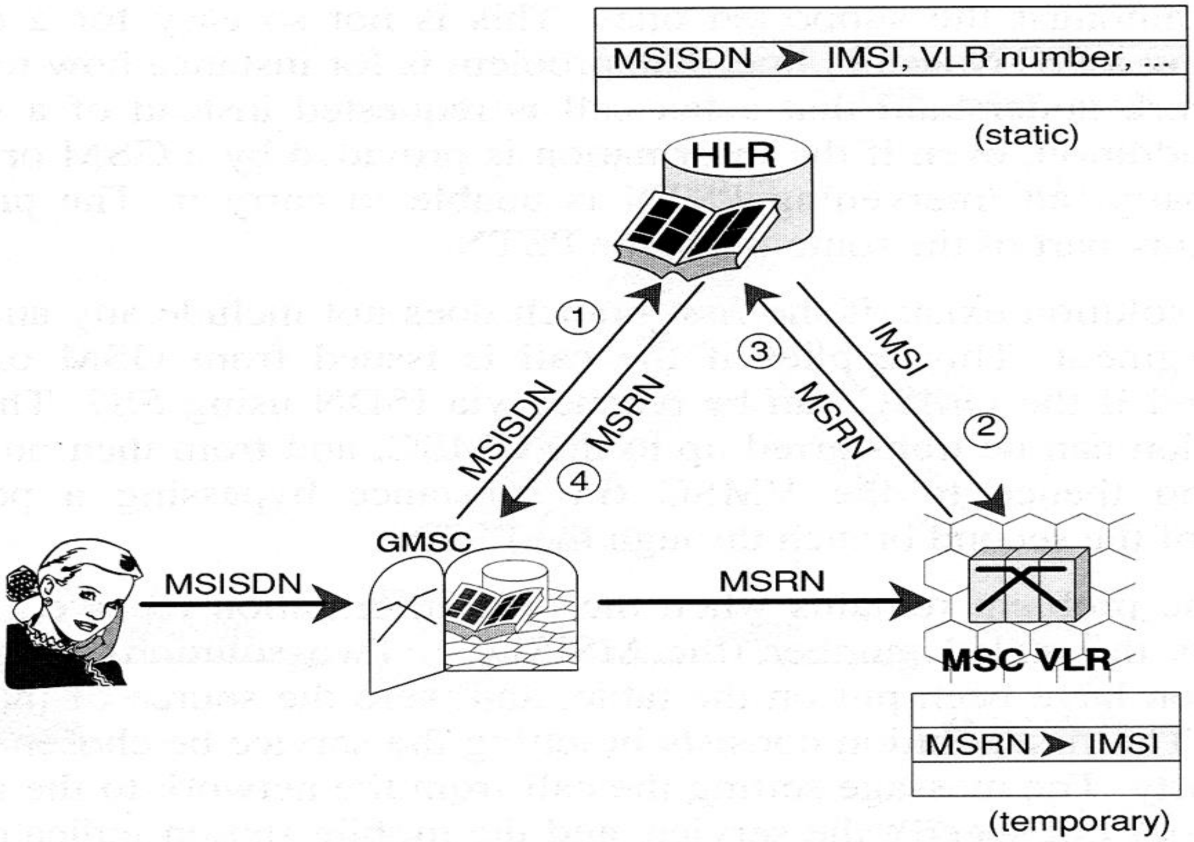
- MSISDN: Mobile Station ISDN Number
  - telephony number
  - unique worldwide
  - MSISDN = Country Code (Hungary: 36) + Network Identifier („area code”) (Hungary:20/30/70) + Subscriber Number
- IMSI: International Mobile Subscriber Identity,
  - in GSM network this identifies the subscribers
    - in 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

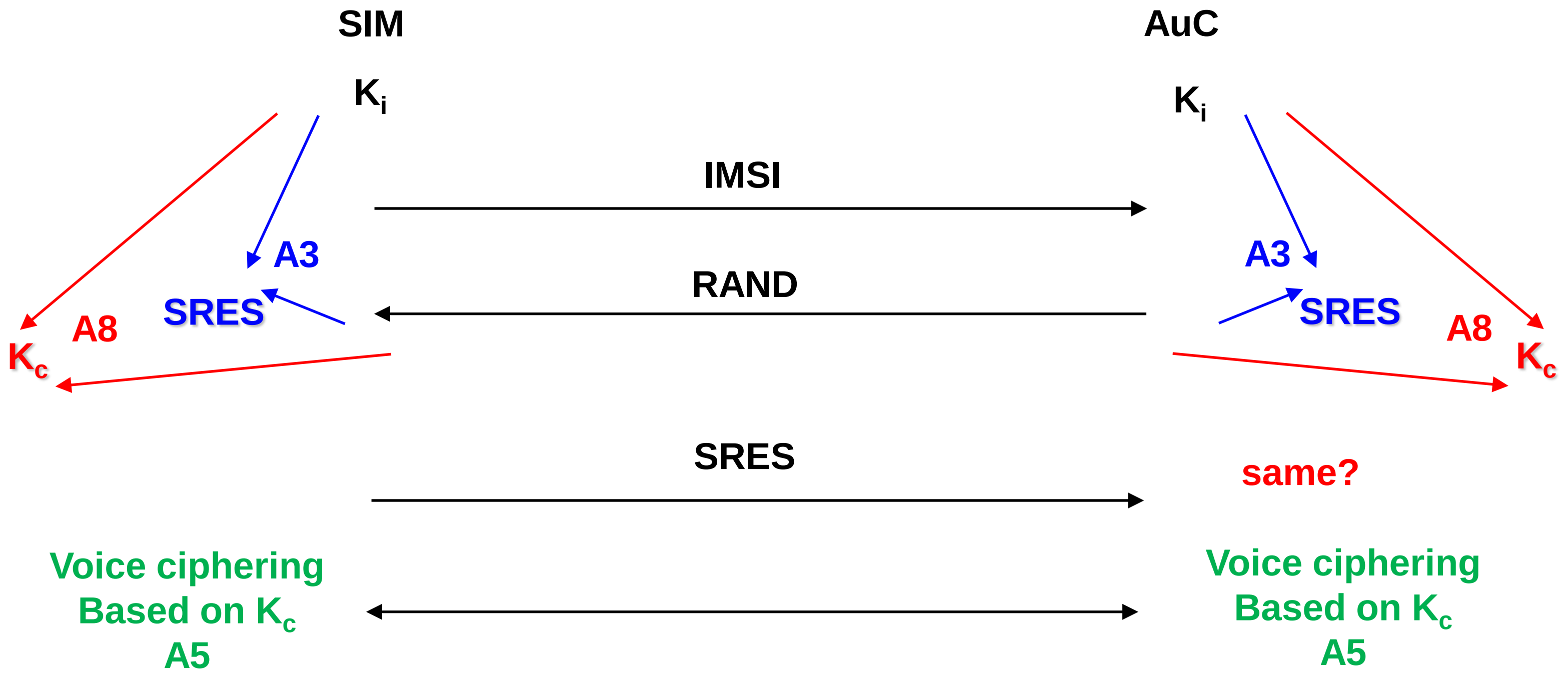
Authentication

- Problem: On the Radio Interface anyone can call in the name of anyone else by using a public identifier
  - And the cheated 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
  - Stores in Authentication Centre (AuC):
    - IMSI – K_i assignment

Authentication – theory

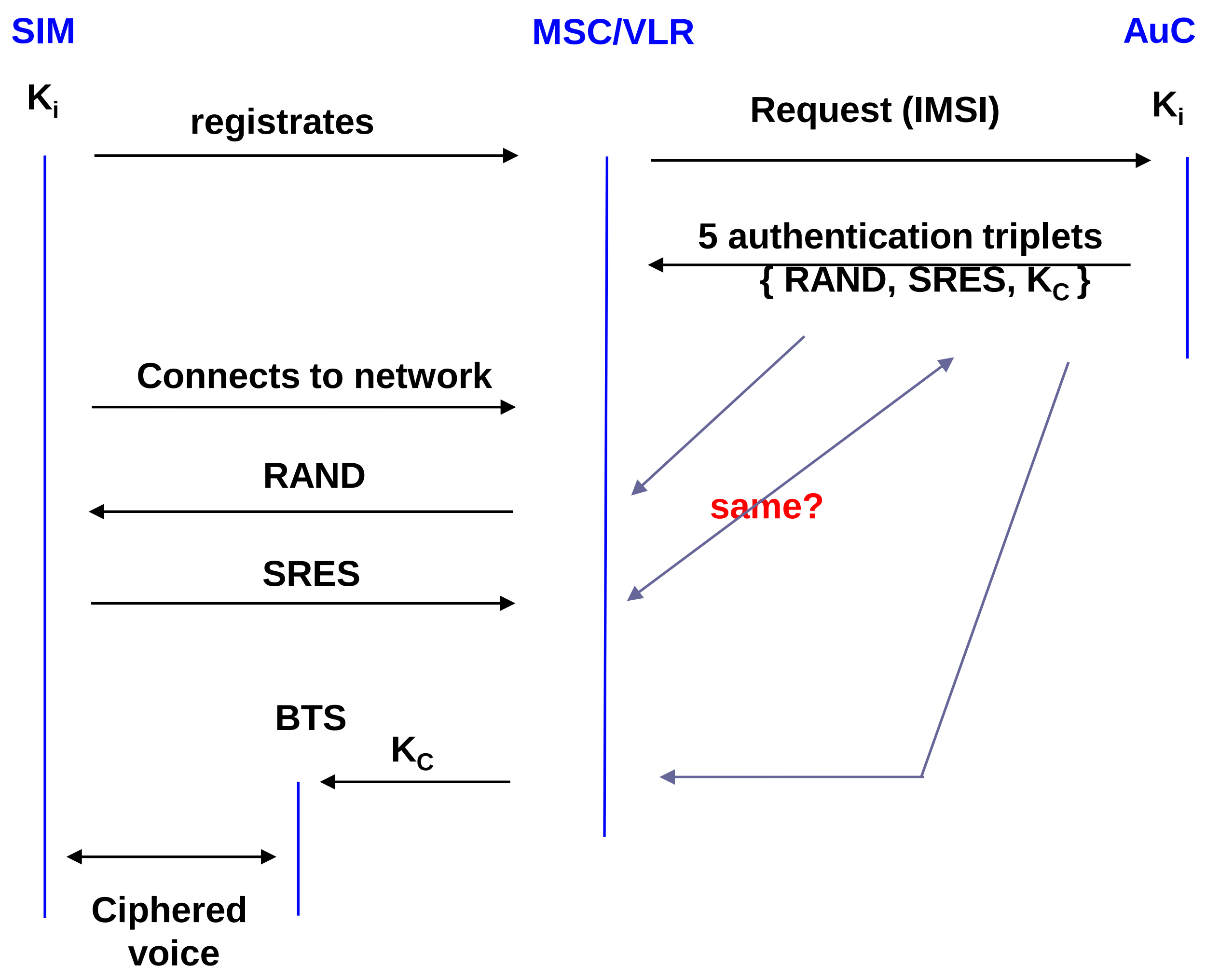


RAND: Random Number
SRES: Signed Result
Kc: Ciphering Key

REQUIRES TOO LARGE SIGNALLING TRAFFIC

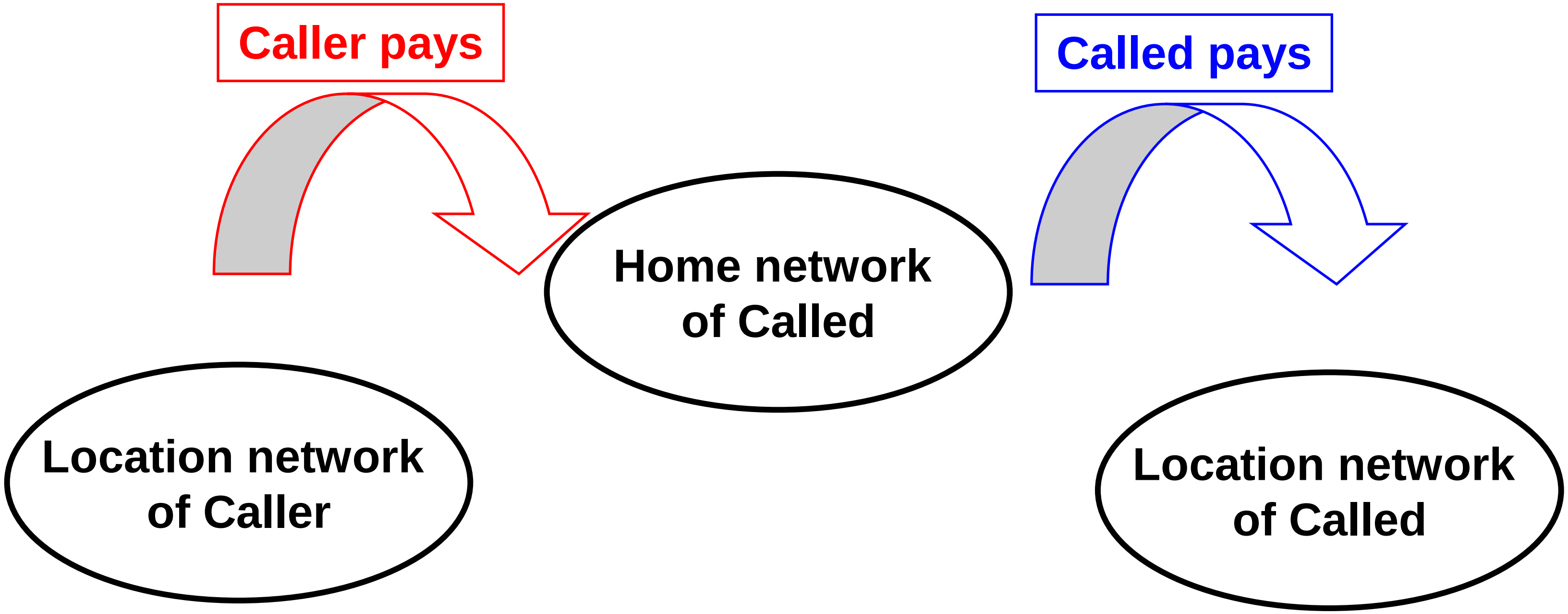
LET US INVOLVE THE SERVING MSC!

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



Caller pays

Called pays

Home network of Called

Location network of Caller

Location network of Called

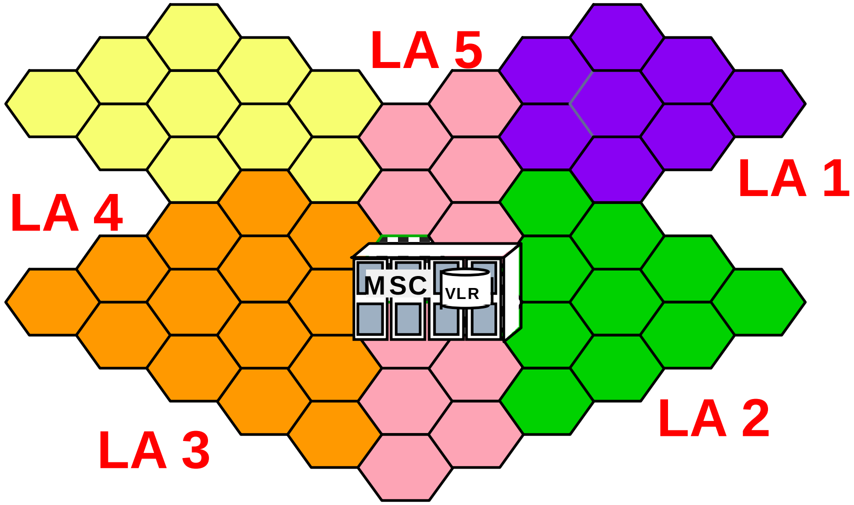
Usage of TMSI instead of IMSI

- 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

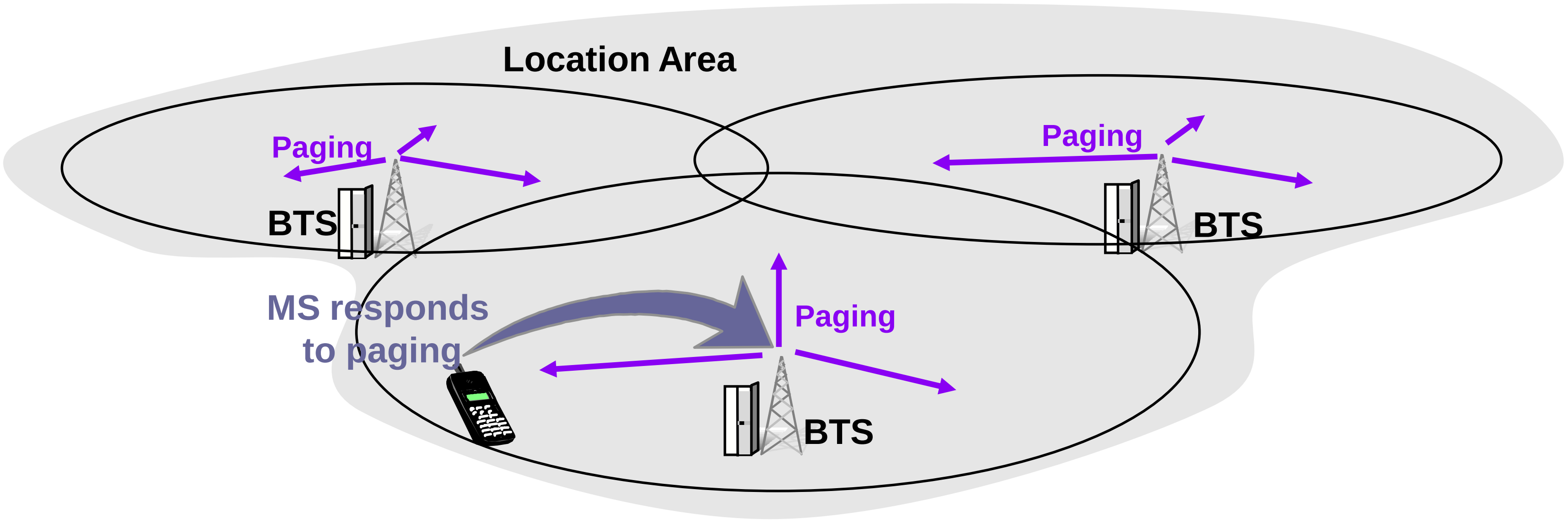
Mobility Management (MM)

- 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 signalling need
    - Additional network elements, processes
    - Still worth

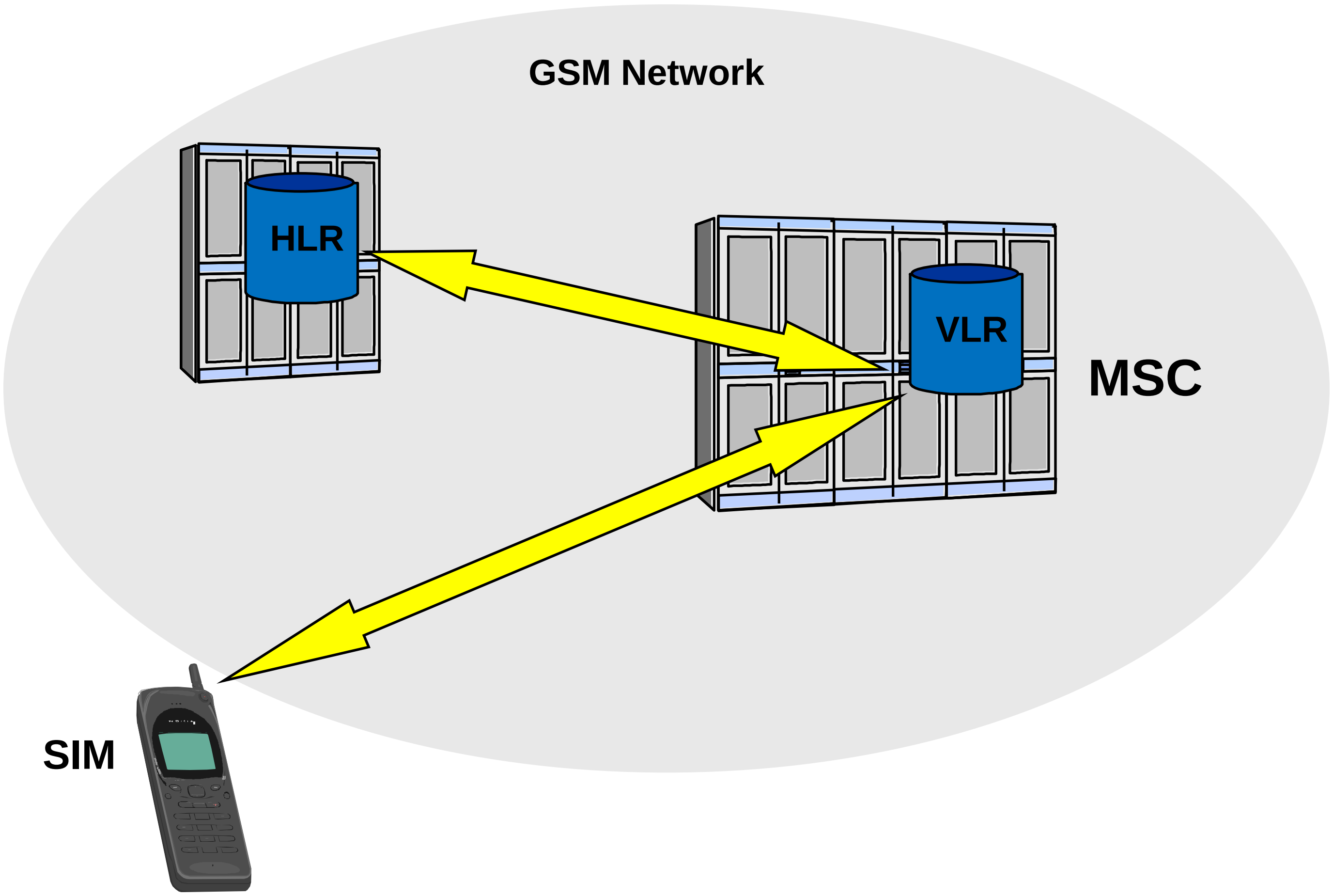
Location Areas



- 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



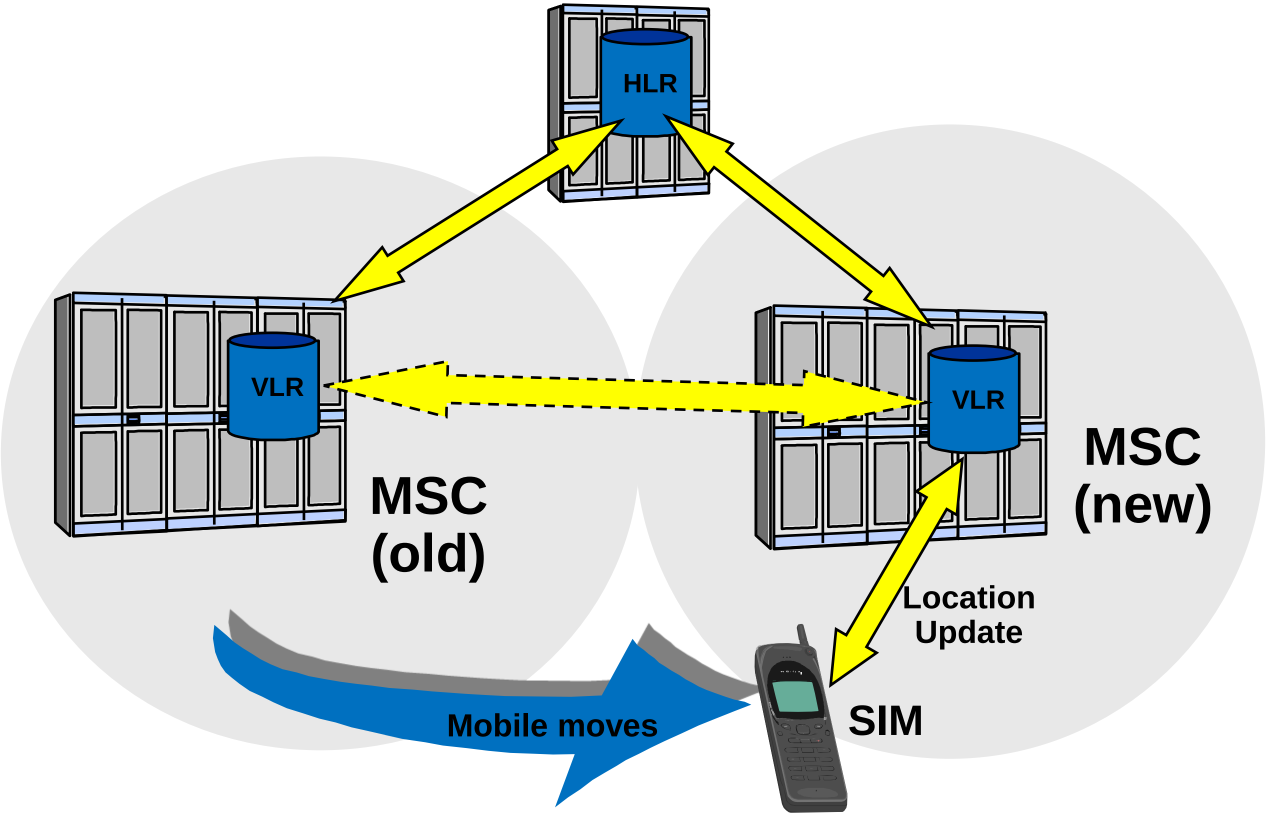
Databases involved in MM in a GSM Network



Location update

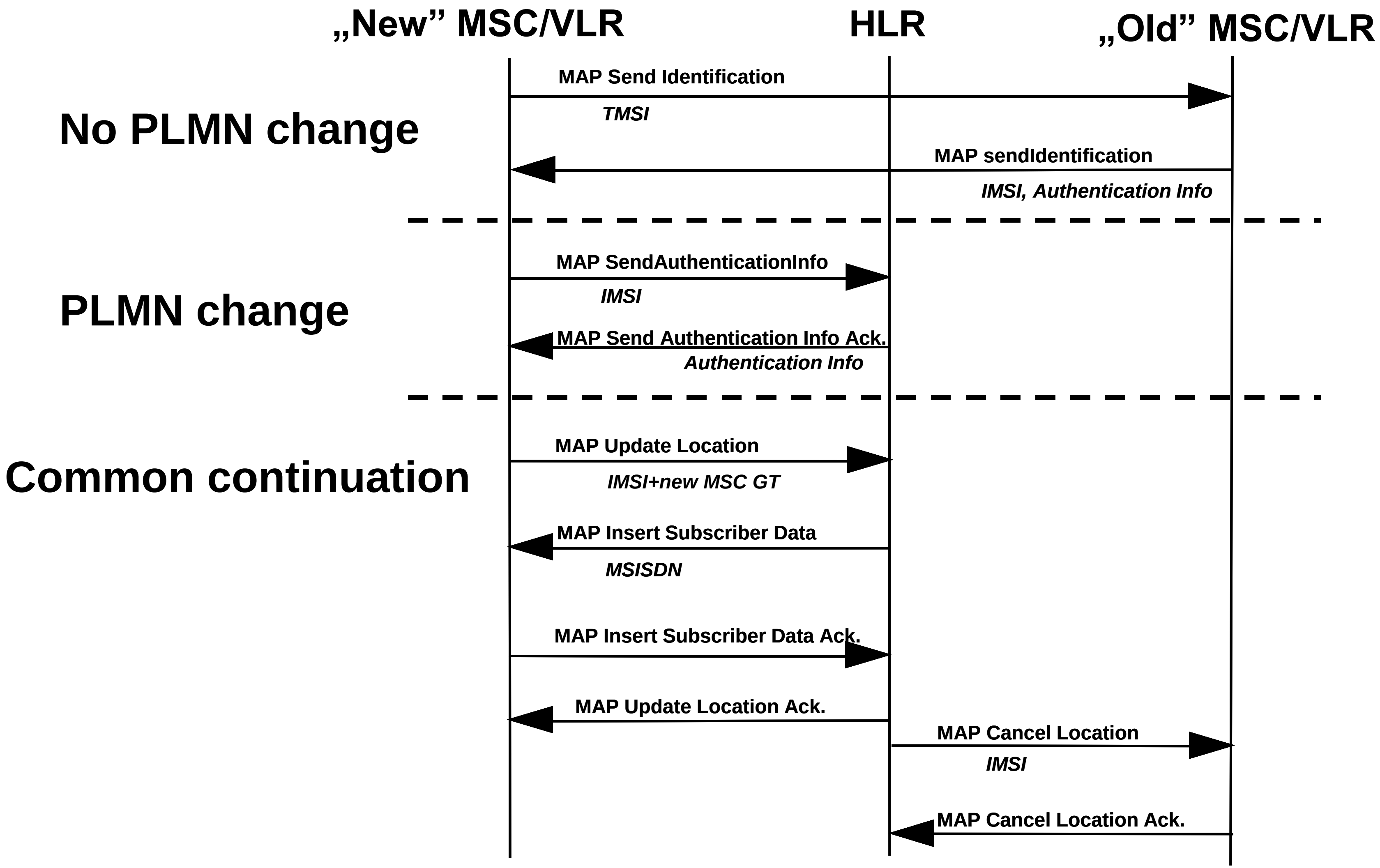
- The Mobile Station monitors the information broadcast by the network (BTS)
- The Mobile Station stores the current location area identity (LAI) in the SIM card
- The Mobile Station continues to monitor the broadcast information
- If the location area identity being broadcast by the network is other 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

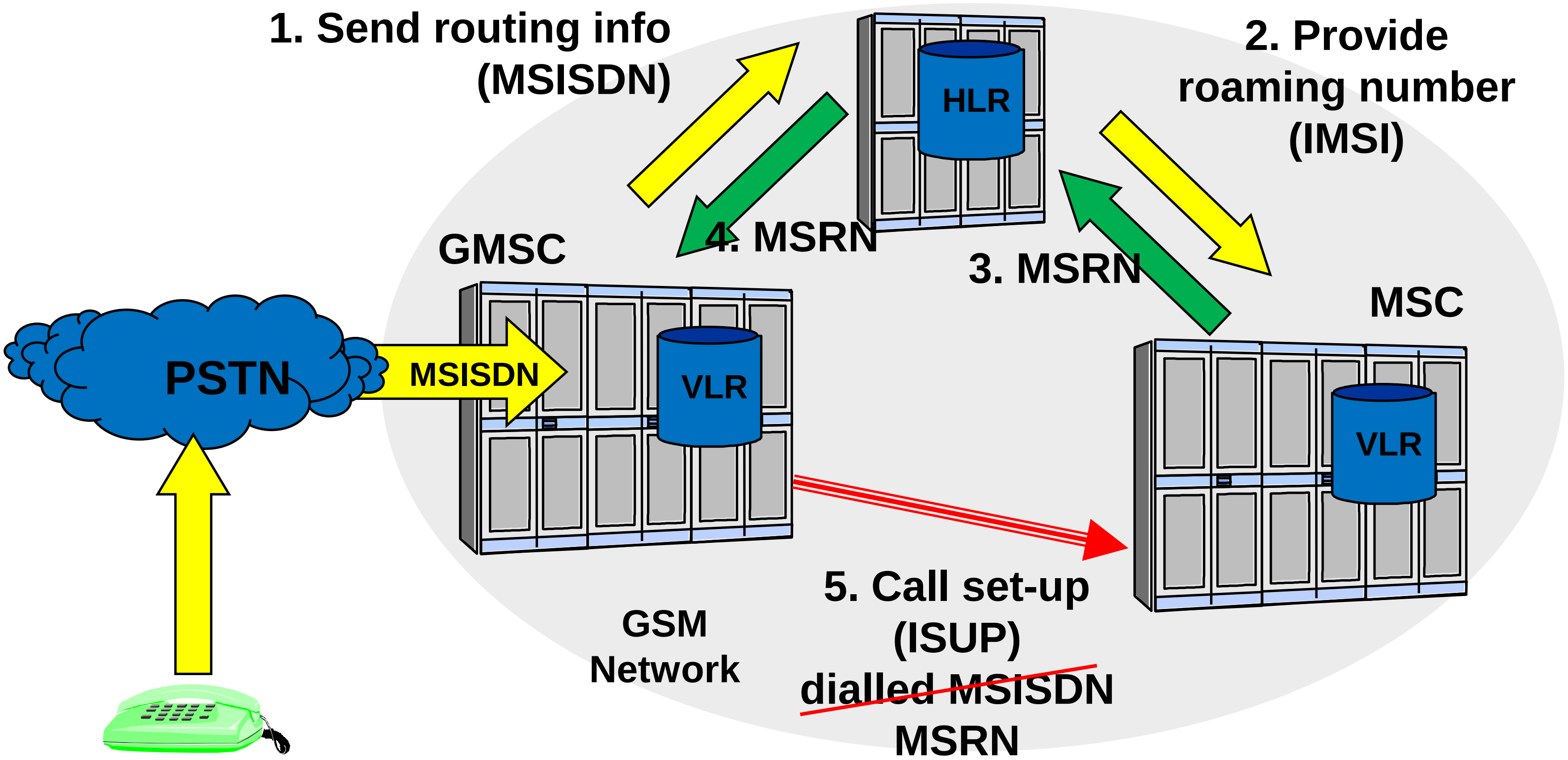


LU variants

- „Normal” (Generic LU)
- Periodic

- Switch on (IMSI Attach)
- Switch off (IMSI Detach)

Routing the call inside the GSM network



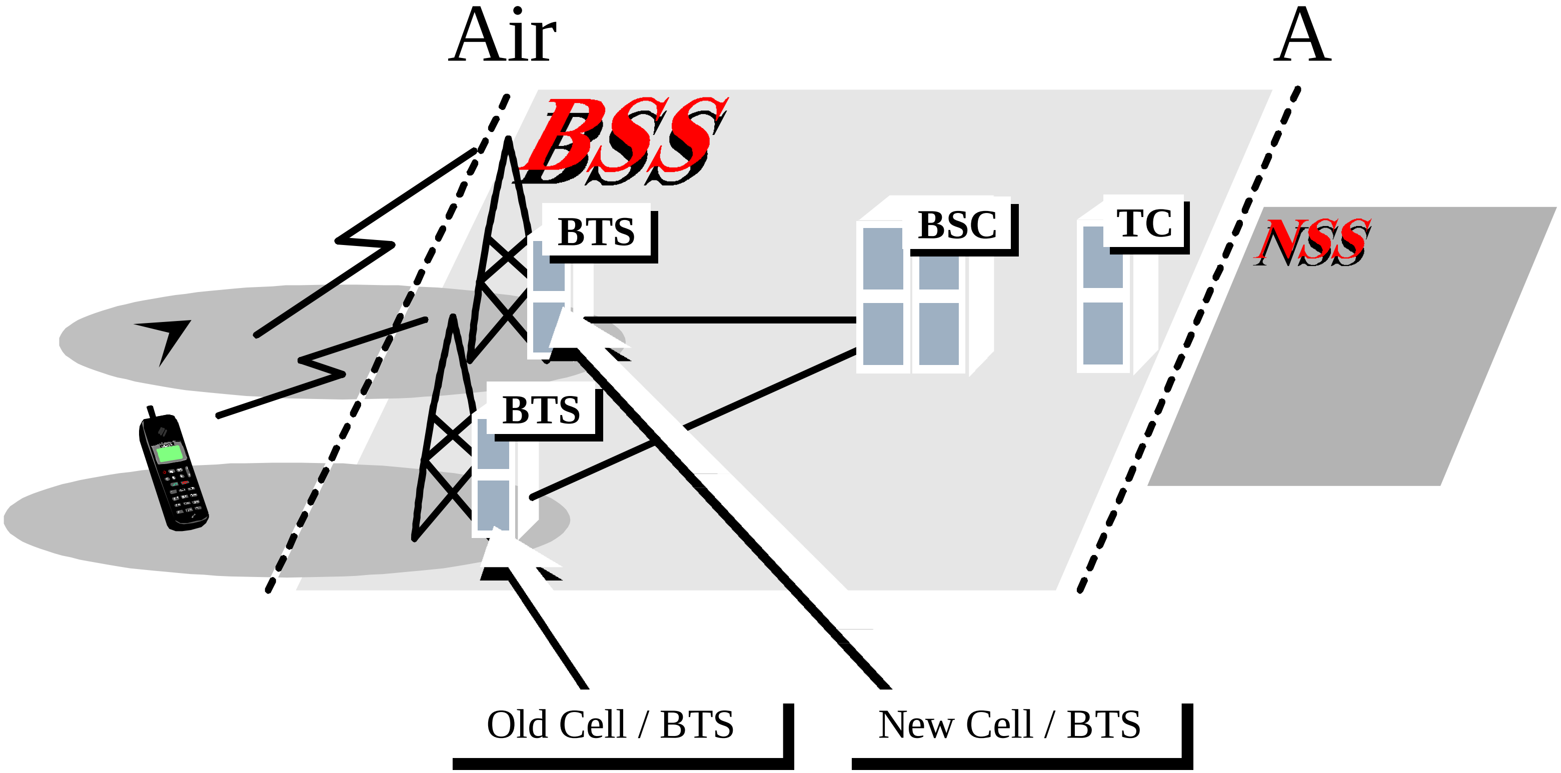
HLR and serving MSC (VMSC – Visited MSC) may be in different networks – SCCP Global Title

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

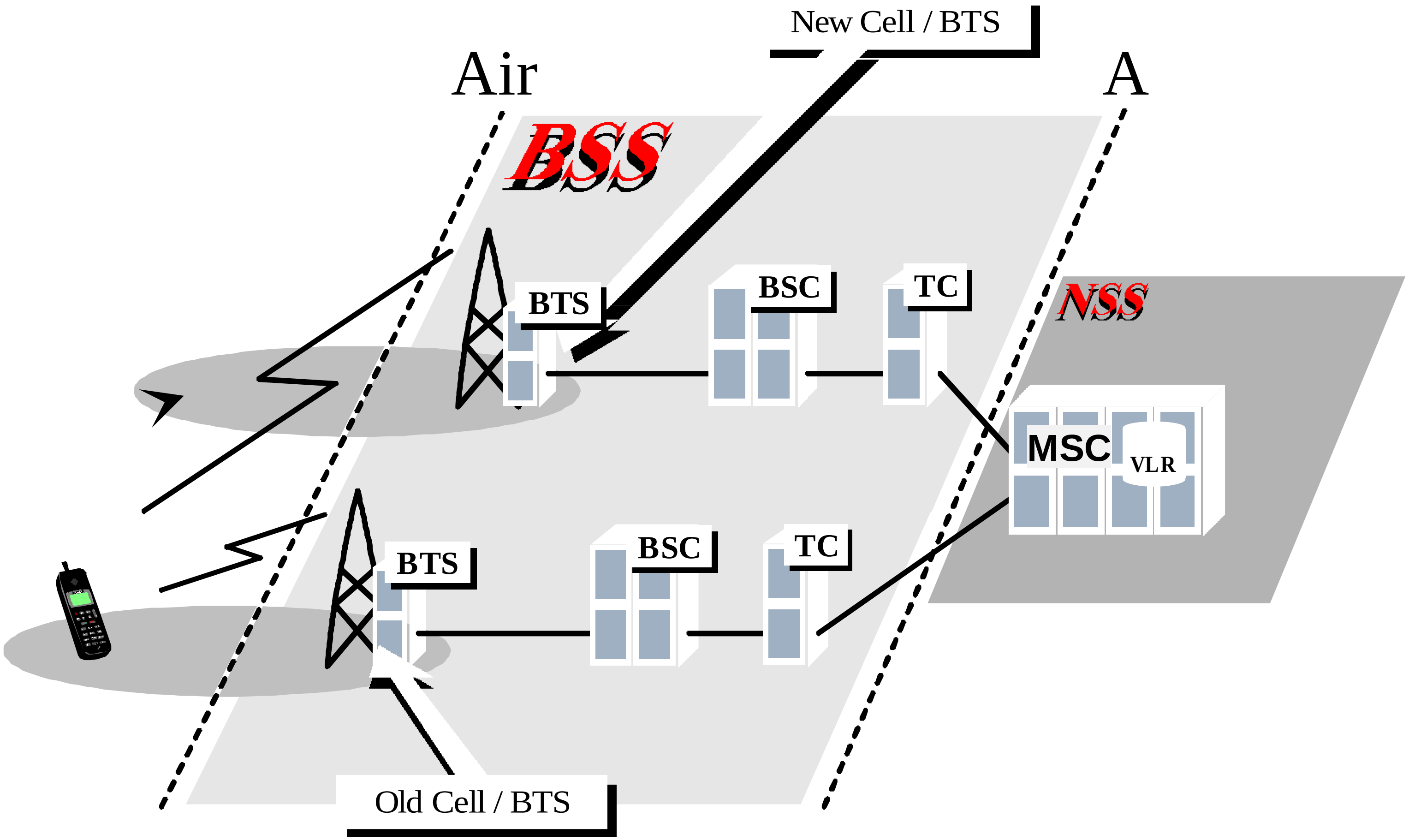
Handover (Handoff)

- Handover due to signal quality and strength
  - When a mobile subscriber is moving during a call, he may travel from one cell to another
  - Frequency resources of previous cells can not be used any more
  - The mobile station is handed over to the new cell
  - BSC controlling the current (new) cell makes the decision to perform a handover
  - There are 3 types of these handovers

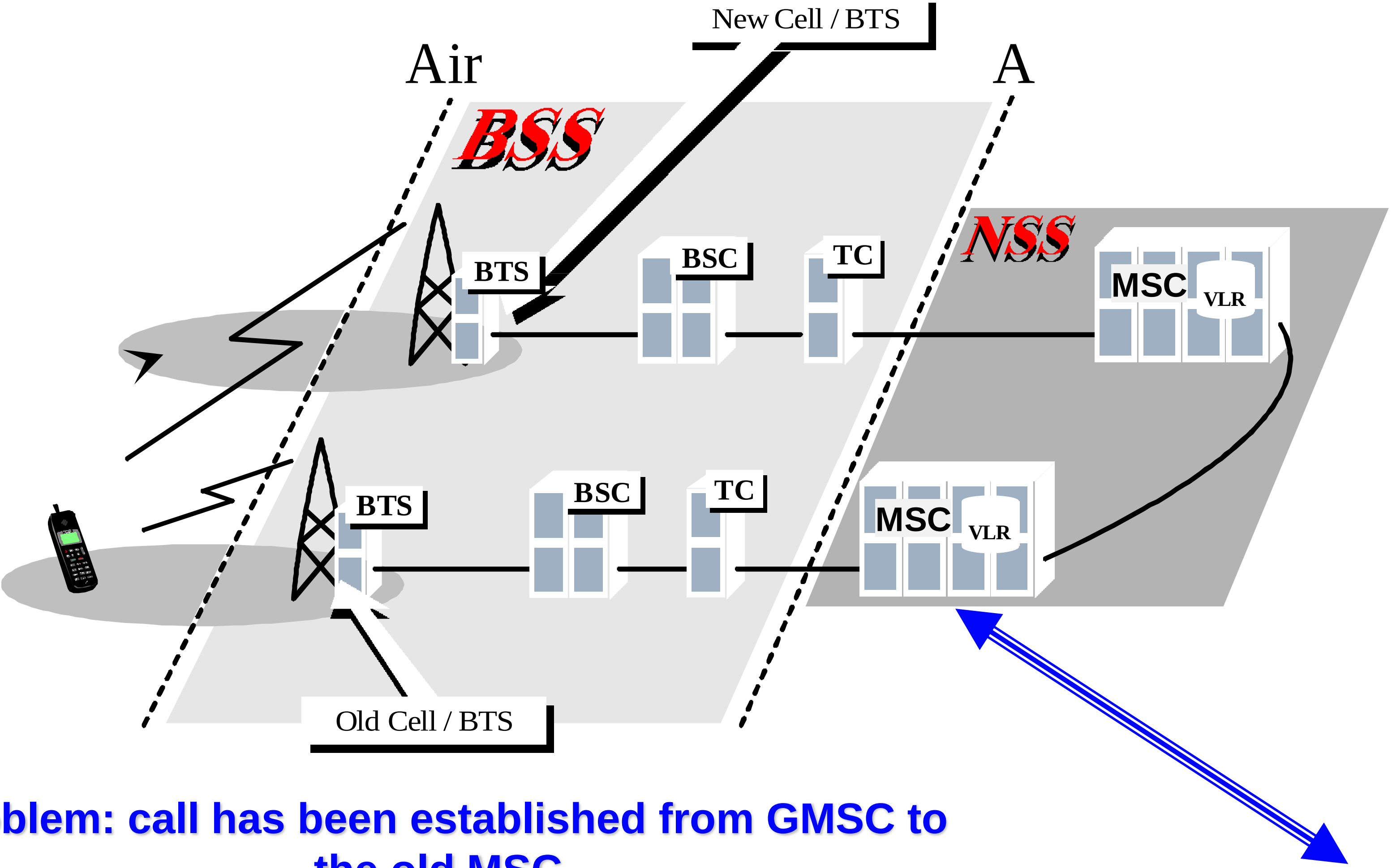
Intra BSS Handover



Inter BSS – Intra MSC Handover



Inter MSC Handover



Problem: call has been established from GMSC to the old MSC

How can we pass the call to the new MSC???

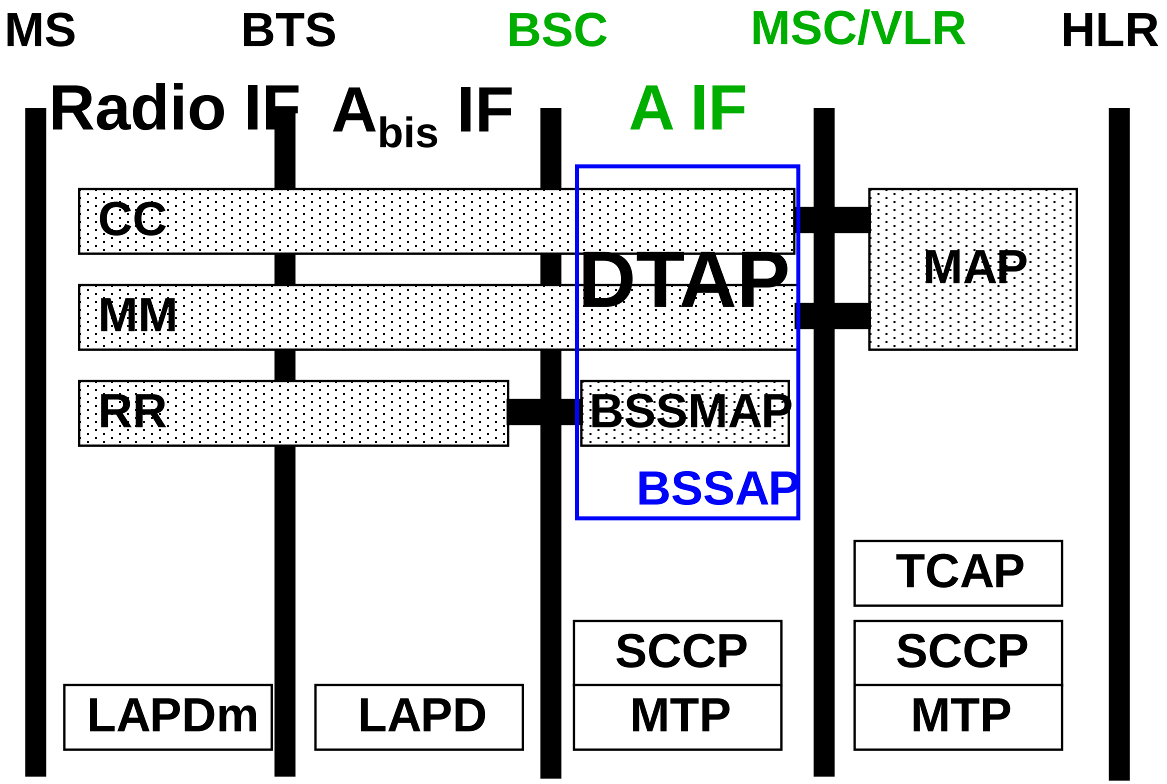
The HandOver Number (HON)

- The source MSC is known as **Anchor MSC**
- Call is routed from Source MSC to target MSC
- A routing number is needed to route a call from one MSC to another MSC
- Source MSC requests the target MSC for a **Handover Number (HON)**. Target MSC allocates one and gives it to the source MSC
- Format is the same as MSRN
  - **HON** = CC + NDC + SN
- Call control remains at anchor MSC even at subsequent handover(s)

GSM protocols

- Previously discussed: Protocos 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)

Mobile Protocols



BSSAP: Base Station Subsystem Application Part =

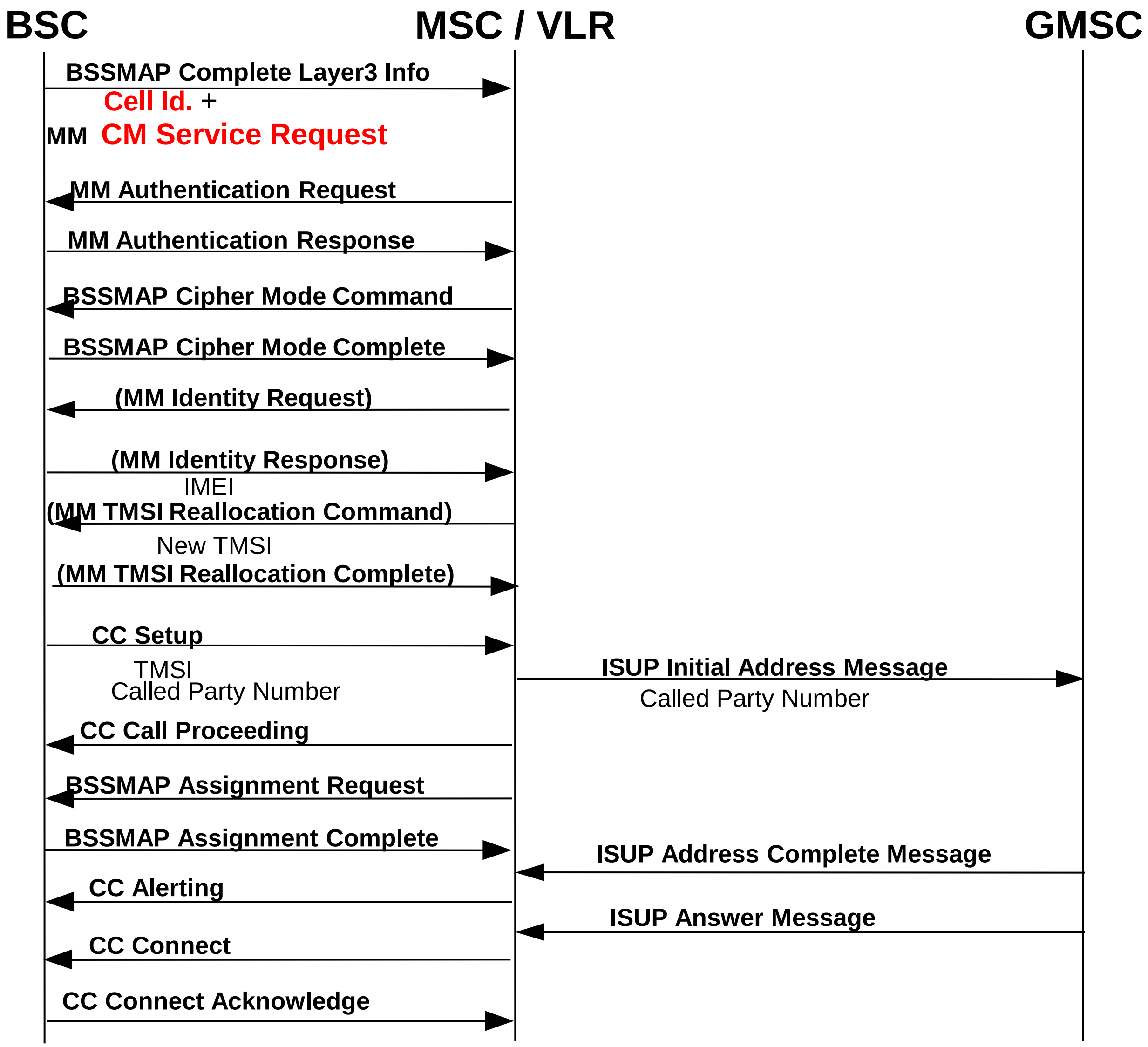
BSSMAP: Base Station Subsystem Management Application Part +

DTAP: Direct Transfer Application Part

CC: Call Control MM: Mobility Management RR: Radio Resource Management

Mobile Originated (MO) Call

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



BSC

MSC / VLR

GMSC

BSSMAP Complete Layer3 Info

Cell Id. +

MM CM Service Request

MM Authentication Request

MM Authentication Response

BSSMAP Cipher Mode Command

BSSMAP Cipher Mode Complete

(MM Identity Request)

(MM Identity Response)

IMEI

(MM TMSI Reallocation Command)

New TMSI

(MM TMSI Reallocation Complete)

CC Setup

TMSI

Called Party Number

ISUP Initial Address Message

Called Party Number

CC Call Proceeding

BSSMAP Assignment Request

BSSMAP Assignment Complete

ISUP Address Complete Message

CC Alerting

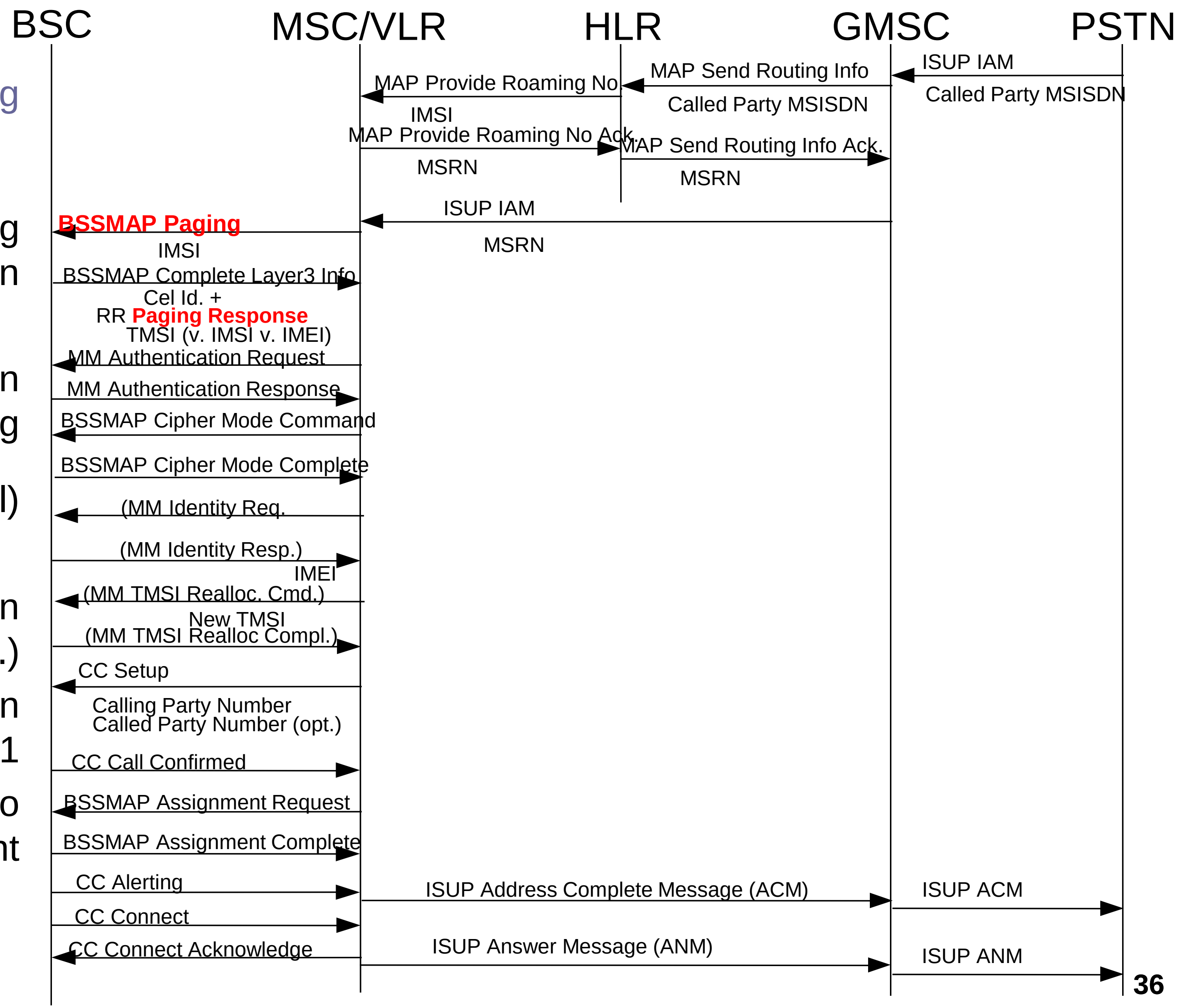
ISUP Answer Message

CC Connect

CC Connect Acknowledge

Mobile Terminated (MT) Call

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



BSC MSC/VLR HLR GMSC PSTN

ISUP IAM
Called Party MSISDN

MAP Send Routing Info
Called Party MSISDN

MAP Provide Roaming No
IMSI

MAP Provide Roaming No Ack.
MSRN

MAP Send Routing Info Ack.
MSRN

ISUP IAM
MSRN

BSSMAP Paging
IMSI

BSSMAP Complete Layer3 Info
Cel 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.)
IMEI

(MM TMSI Realloc. Cmd.)
New TMSI

(MM TMSI Realloc Compl.)

CC Setup
Calling Party Number
Called Party Number (opt.)

CC Call Confirmed

BSSMAP Assignment Request

BSSMAP Assignment Complete

CC Alerting

ISUP Address Complete Message (ACM)

ISUP ACM

CC Connect

ISUP Answer Message (ANM)

ISUP ANM

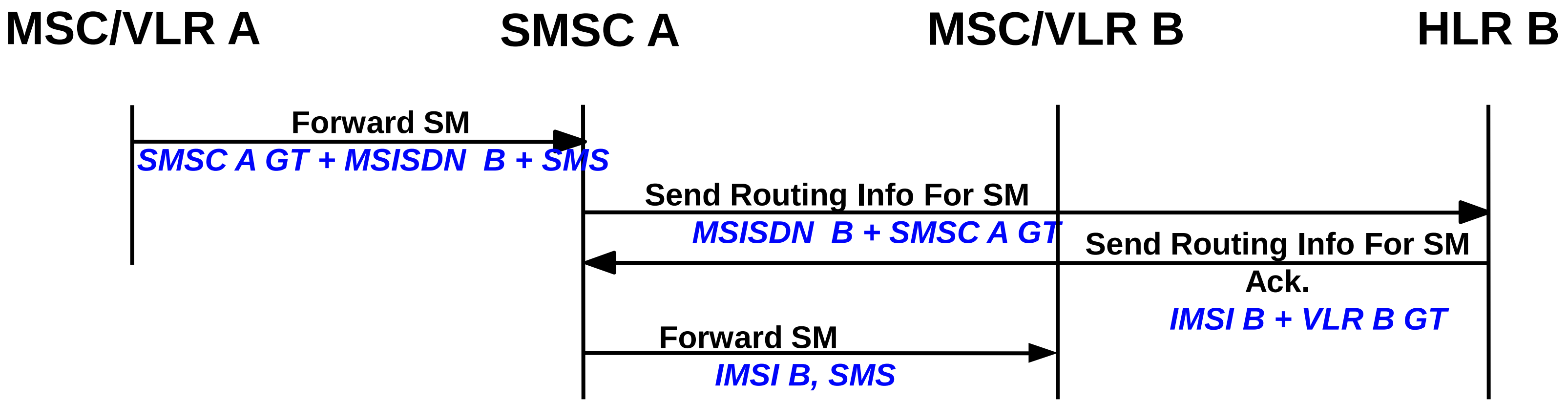
CC Connect Acknowledge

Short Message Service

- Signalling 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



MSC/VLR A

SMSC A

MSC/VLR B

HLR B

Forward SM
SMSC A GT + MSISDN B + SMS

Send Routing Info For SM
MSISDN B + SMSC A GT

Send Routing Info For SM Ack.
IMSI B + VLR B GT

Forward SM
IMSI B, SMS