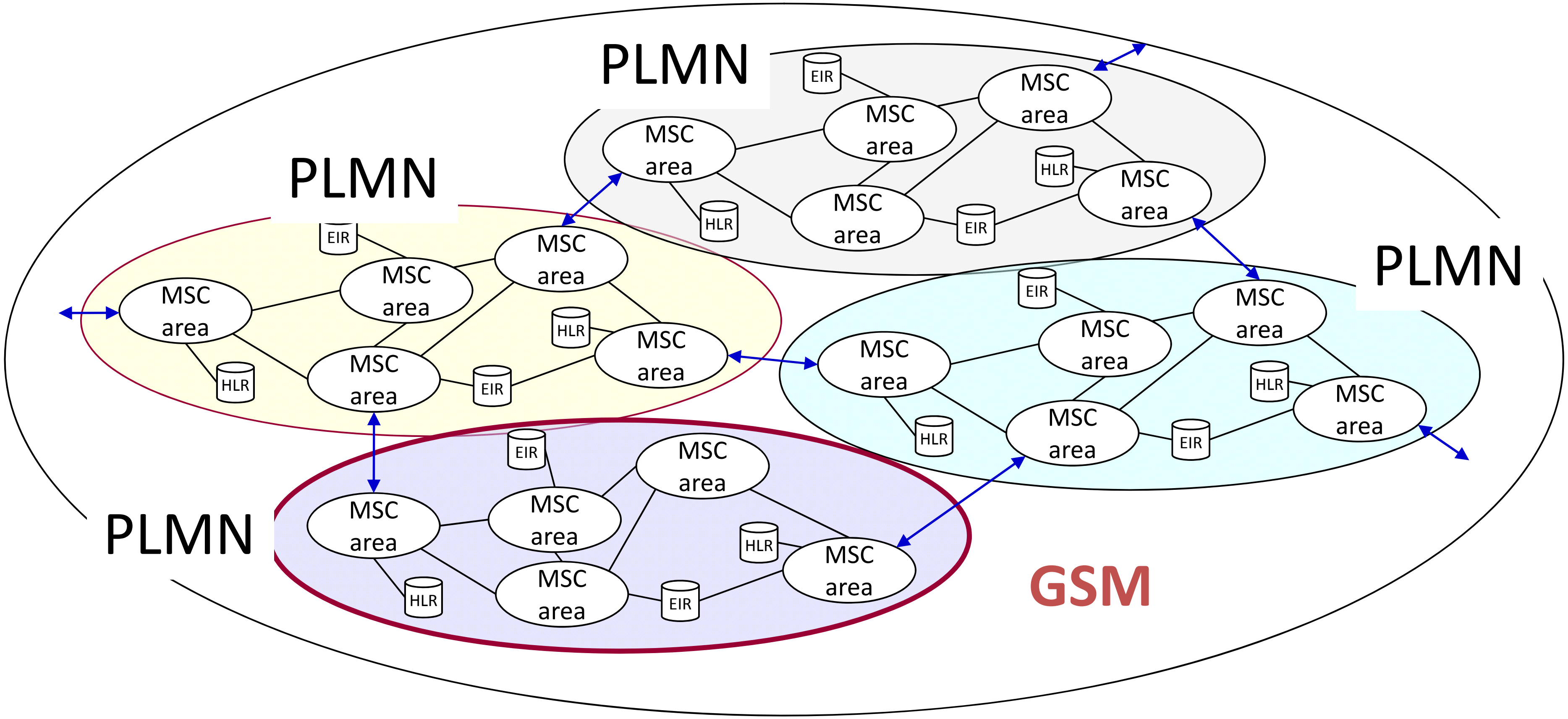
System Architecture
GSM as example

Dr. Hicham Aroudaki

Damascus, 18th December 2010

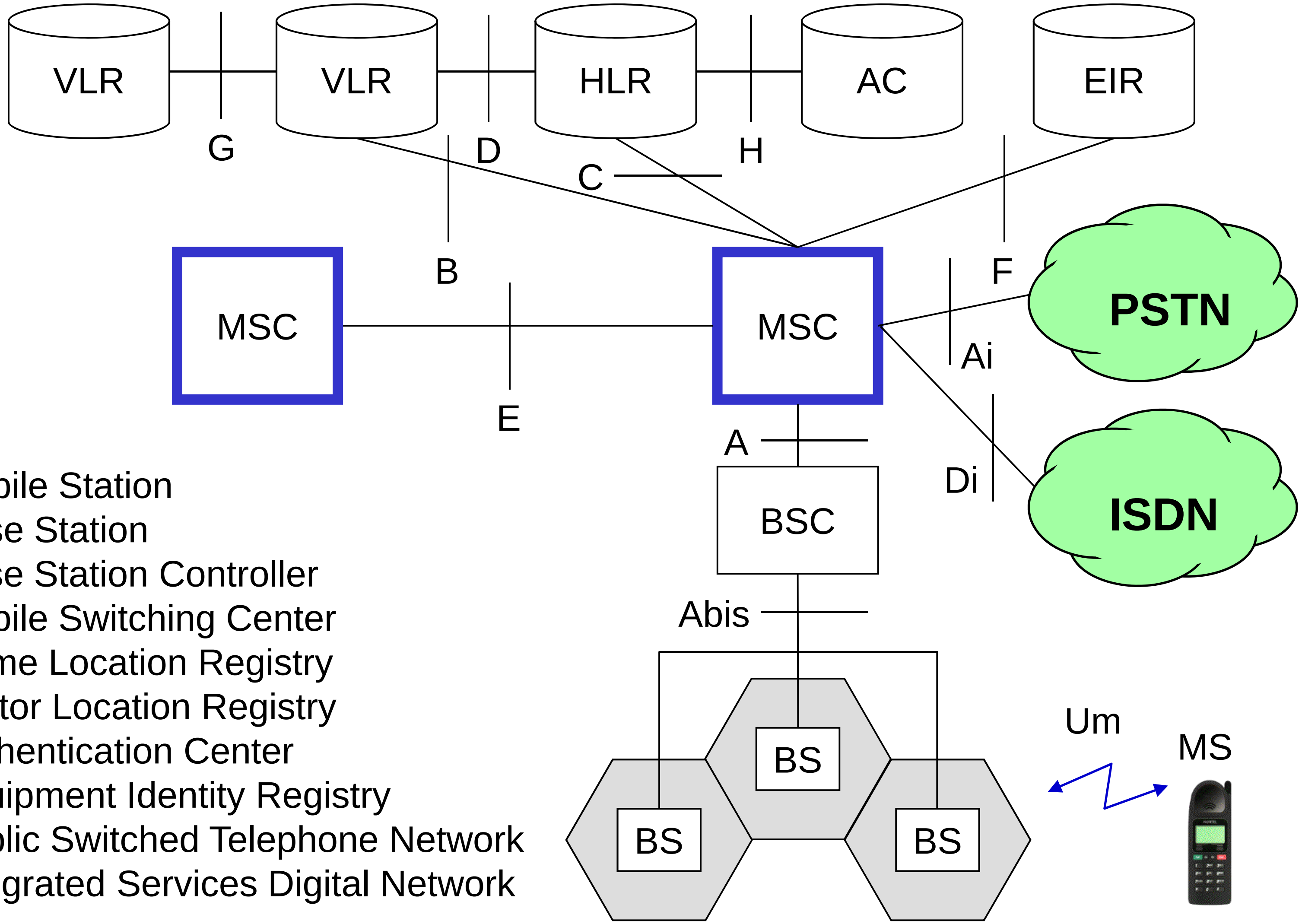
System Hierarchies

Overview of the GSM System



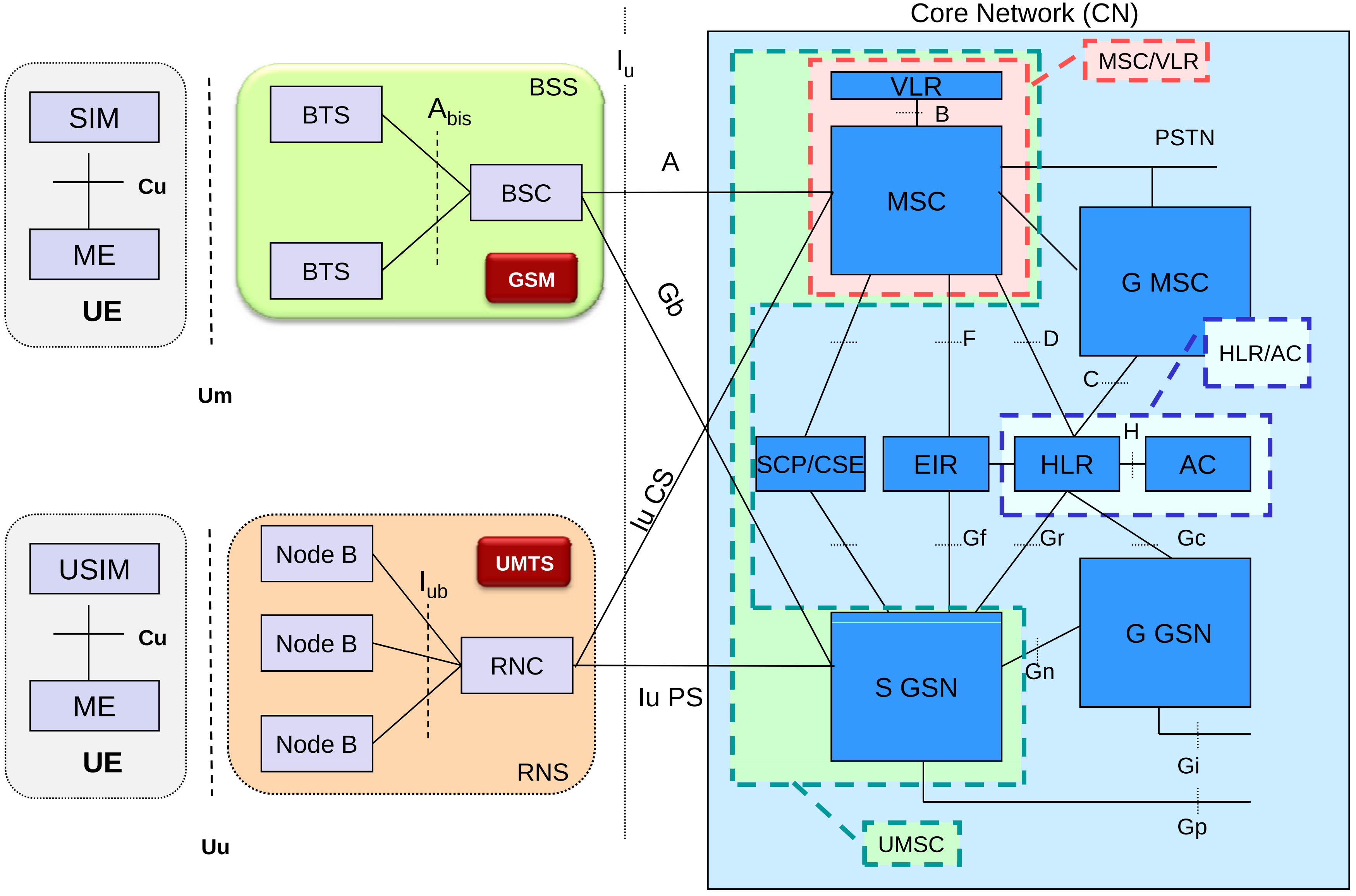
The GSM system is made up of sub-networks called: Public Land Mobile Network's (PLMN). Each member country has one or more PLMN depending on its size.

The GSM Network Model



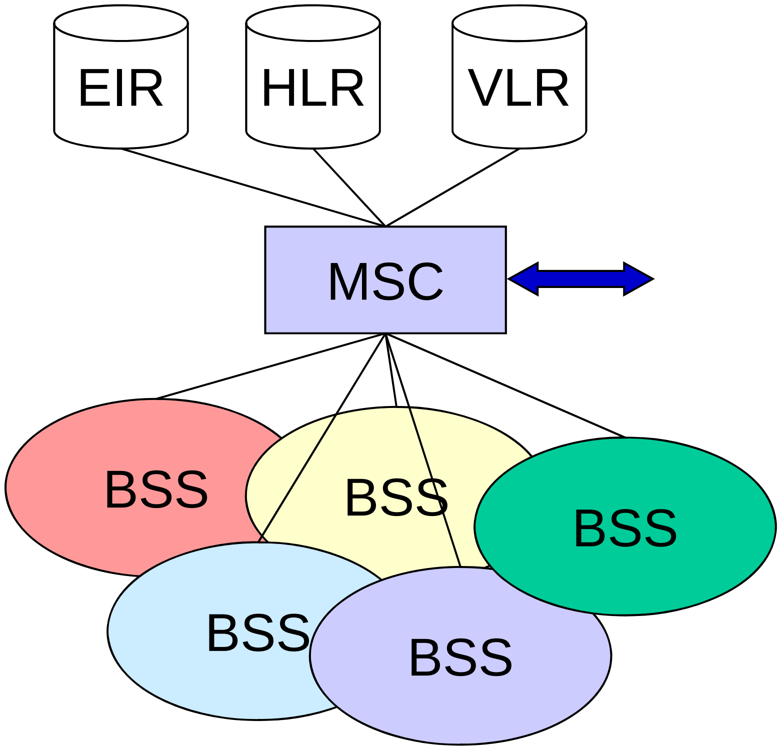
MS=	Mobile Station
BS =	Base Station
BSC =	Base Station Controller
MSC=	Mobile Switching Center
HLR=	Home Location Registry
VLR=	Visitor Location Registry
AC =	Authentication Center
EIR=	Equipment Identity Registry
PSTN=	Public Switched Telephone Network
ISDN=	Integrated Services Digital Network

Generic Network Model

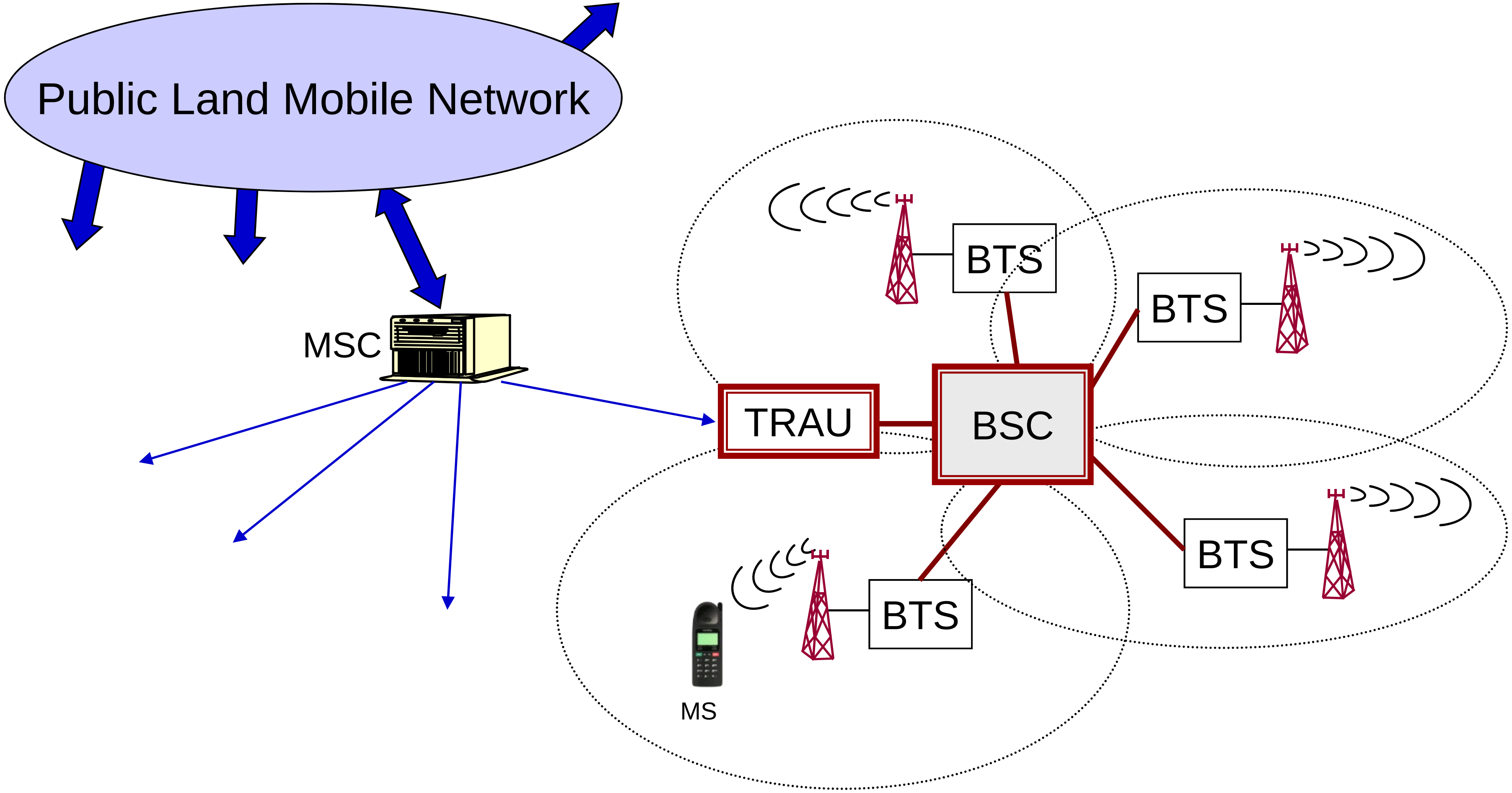


The MSC Area

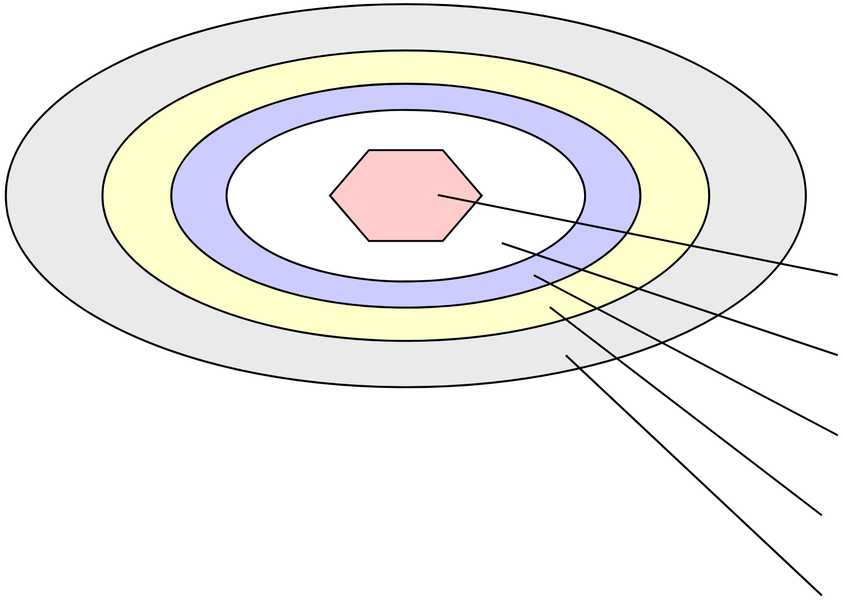
- The MSC area consists of one MSC and several BSS's
- The MSC provides the external interface, either directly or through a Gateway MSC
- Each MSC is connected to a Visitor Location Register (VLR)
- The MSC also has access to a Home Location Register (HLR) and Equipment Identification Register (EIR)



GSM MSC-BSC Hierarchy



Hierarchy of Areas



Cell

Location Area (locating & paging area)

MSC Service Area (area controlled by one MSC)

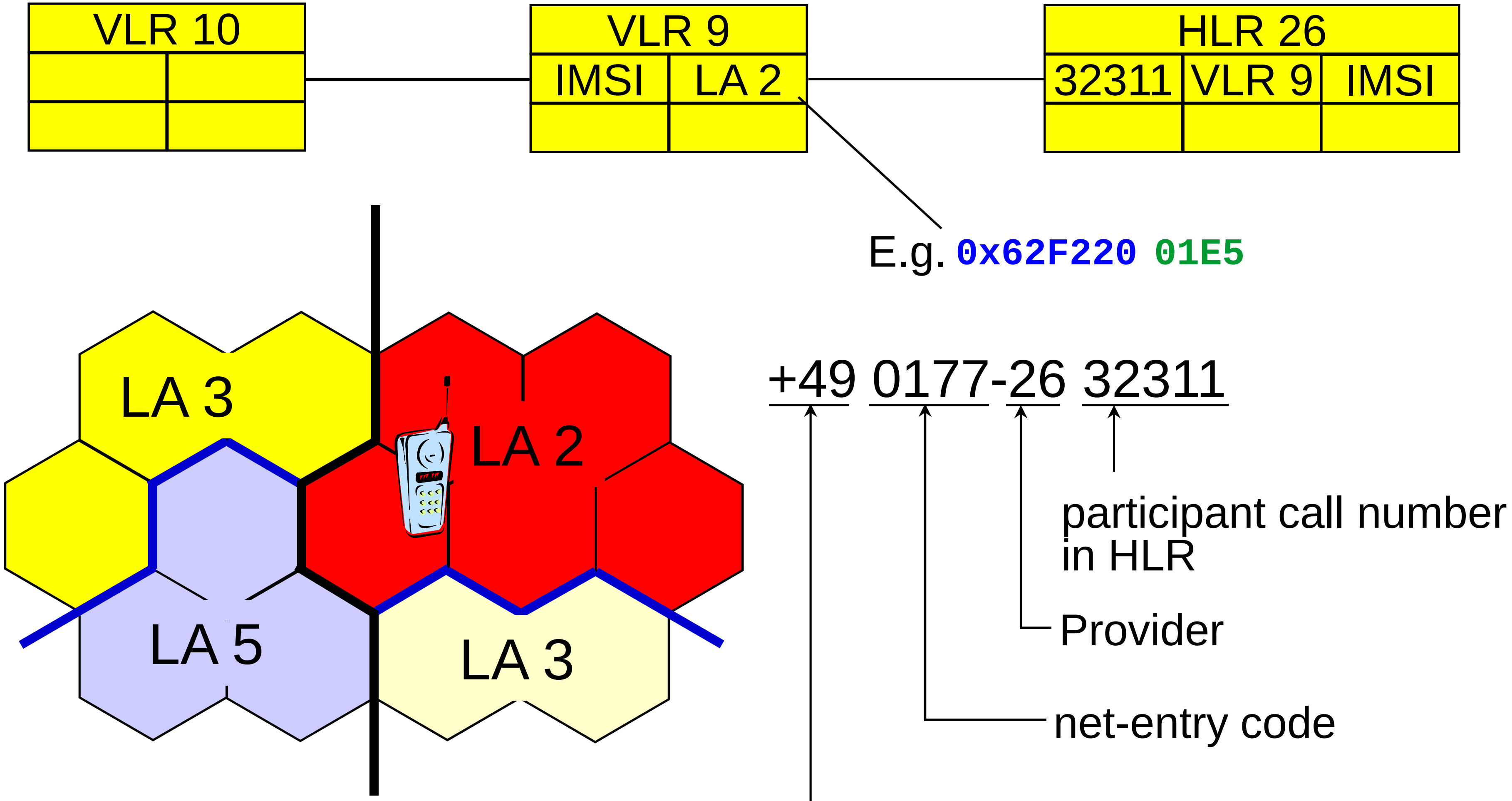
PLMN (one or more per country)

GSM Service Area (all member countries)

Location Area Identity (LAI)

3 digits	3 digits	2 Octet (max)
MCC	MNC	LAC
Mobile Country Code	Mobile Network Code	Location Area Code

Localization of subscribers



VLR 10	

VLR 9	
IMSI	LA 2

HLR 26		
32311	VLR 9	IMSI

E.g. 0x62F220 01E5

+49 0177-26 32311

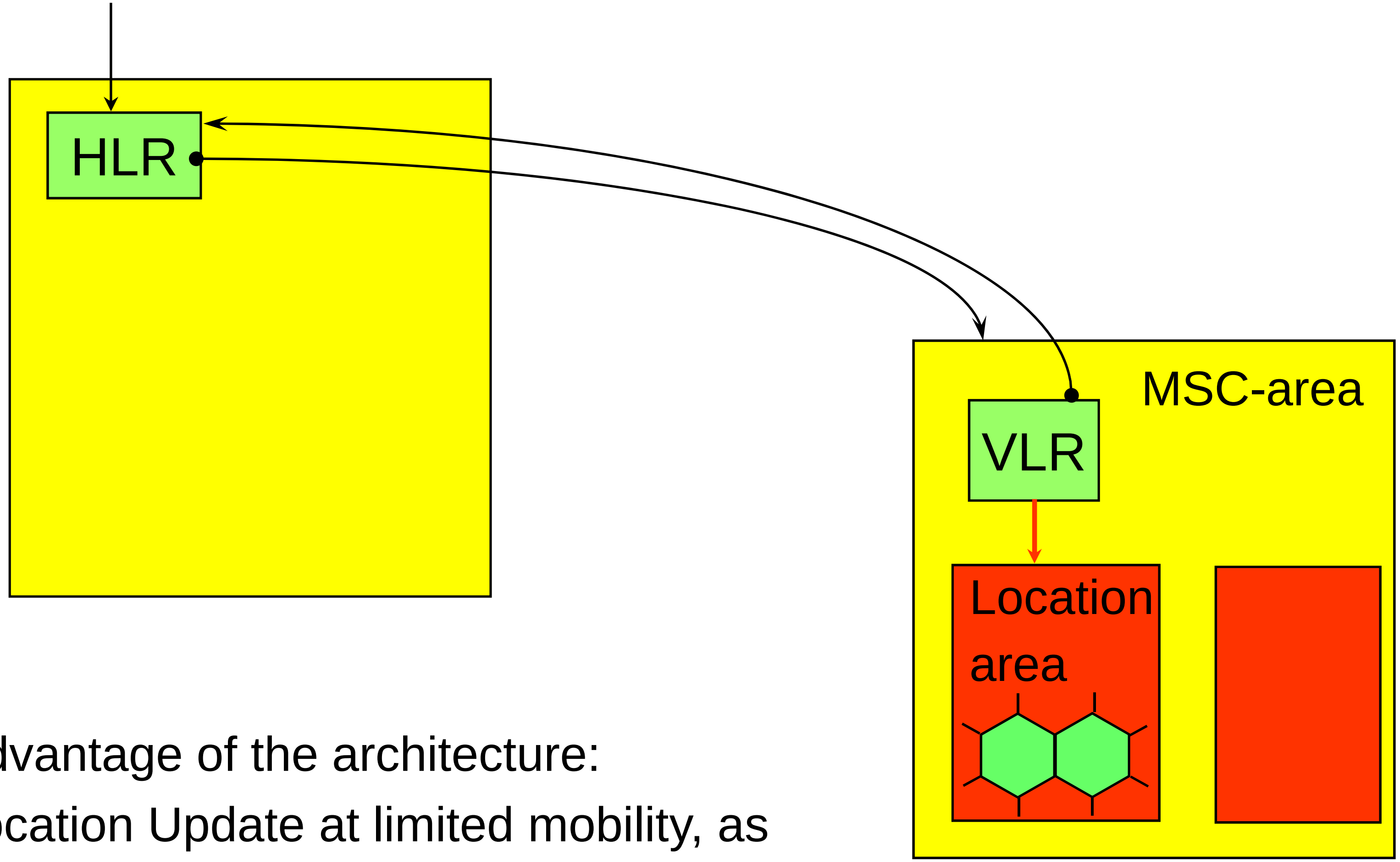
participant call number in HLR

Provider

net-entry code

country code number

Connection HLR, VLR

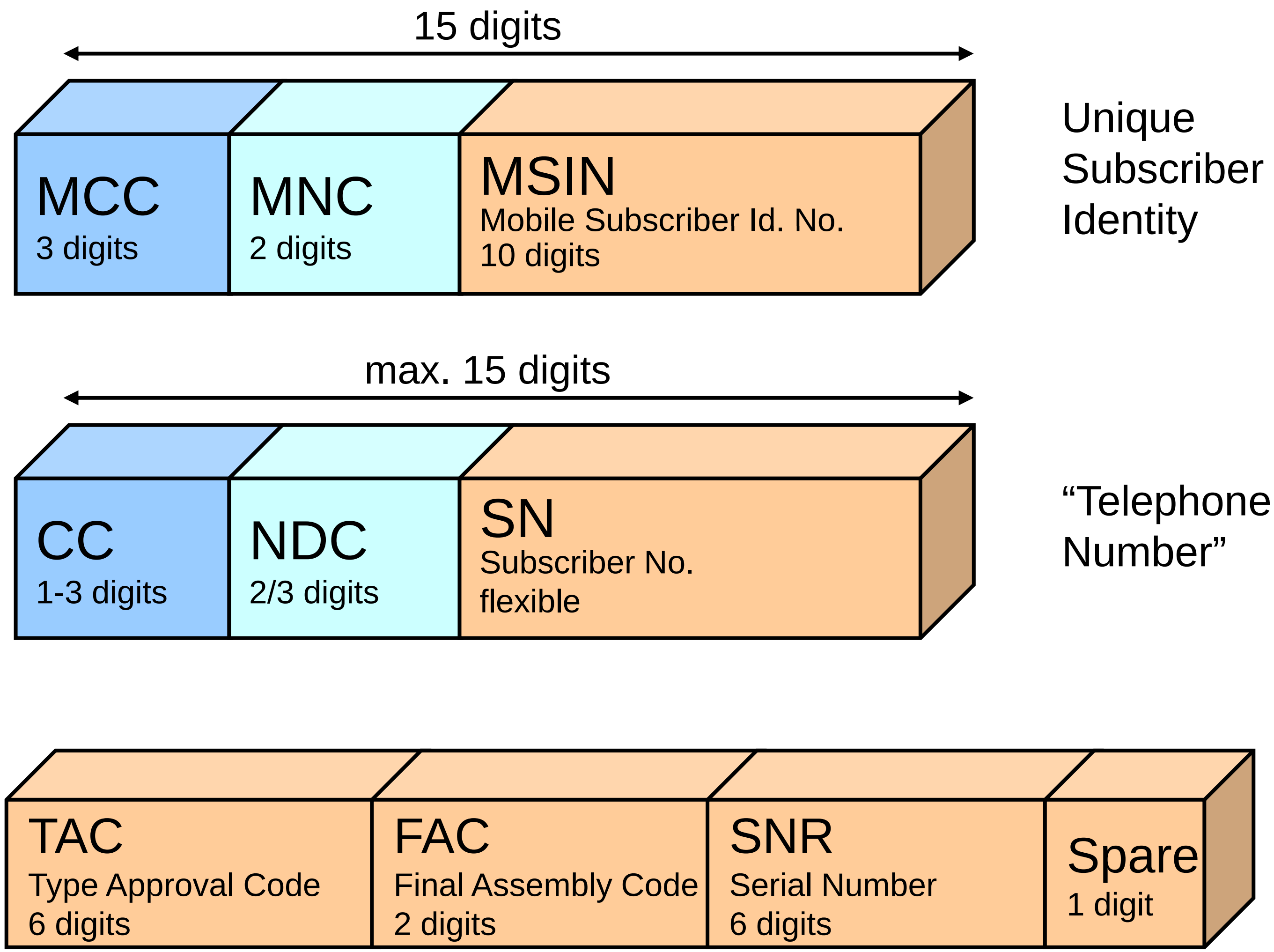


Advantage of the architecture:

Location Update at limited mobility, as a rule only at VLR, rarely at (perhaps far remote) HLR

GSM Identities

Subscriber Identity Numbers



IMSI
International Mobile Subscriber Identity

15 digits

MCC
3 digits

MNC
2 digits

MSIN
Mobile Subscriber Id. No.
10 digits

Unique Subscriber Identity

MSISDN
Mobile Subscriber ISDN Number

max. 15 digits

CC
1-3 digits

NDC
2/3 digits

SN
Subscriber No.
flexible

“Telephone Number”

IMEI
International Mobile station Equipment Identity

TAC
Type Approval Code
6 digits

FAC
Final Assembly Code
2 digits

SNR
Serial Number
6 digits

Spare
1 digit

GSM Identities

	IMSI			MS - ISDN		
Nature	International Mobile Subscriber Identity Conformity with E212			Mobile Station - Integrated Services Digital Network Nb Similar to ISDN, Conformity with E164/E213		
Format	Identify a PLMN worldwide		Identify the subscriber of a PLMN		National Significant Mobile Number	
	MCC	MNC	MSIN H1 H2 x x x .... x x x	CC	NDC	SN M1 M2 x x x x x x x x
Meaning	Mobile Country Code	Mobile Network Code	Mobile Subscriber Ident. Nb H1 H2 = Identity of HLR within the home PLMN	Country Code (where subscription has been made)	National Destination Code *	Mobile Subscriber (national definition) M1 M2 = nbr of logical HLR
Nb. digits	3	2	max 10	1 to 3	2 to 4	total max 15

* *This code does not identify a geographical area but an operator*

Temporary Mobile Subscriber Identity Number (TMSI)

- The TMSI can be allocated to the mobile subscriber in order to be used instead of his IMSI during all radio communications. The purpose is to keep subscriber information confidential on the air interface.
- “TMSI allocation” protects the subscribers identity in the initial access phase, where no ciphering is possible.
- The TMSI is relevant on the local MSC/VLR level only and is changed at certain events or time intervals. Each local operator can define its own TMSI structure.

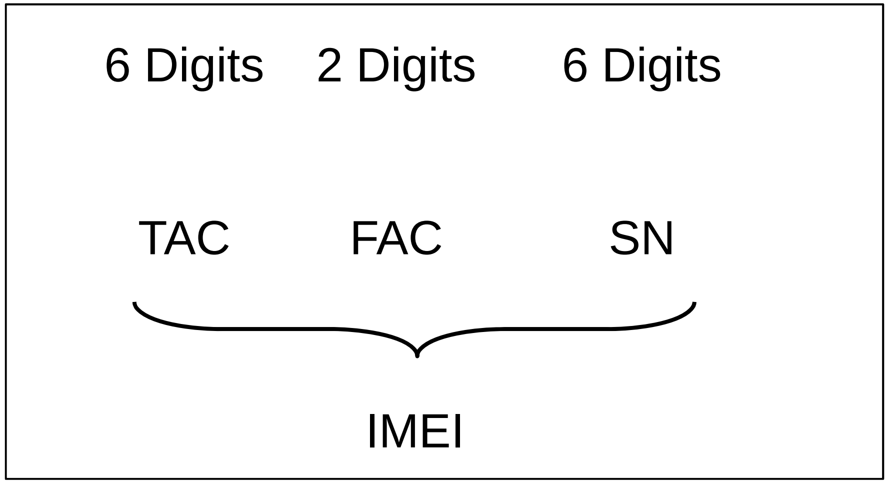
Mobile Station Roaming Number

- When a mobile terminating call is to be set-up, the HLR of the called subscriber requests the MSC/VLR to allocate an MSRN to the called subscriber.
- This MSRN is returned via the HLR to the GMSC.
- The GMSC routes the call to the MSC/VLR exchange where the called subscriber is currently registered.
- The routing is done using the MSRN. When the routing is completed, the MSRN is released.
- The interrogation call routing function (request for MSRN) is part of the MAP.
- All data exchanged between GMSC-HLR-MSC/VLR for the purpose of interrogation is sent over S7 signaling.
- The MSRN is built up like an MSISDN.

Mobile Station Roaming Number

- The MSRN format is the same as MSISDN, but it is temporary
- MSRN = CC + NDC + SN
  - CC = Country Code
  - NDC = National Destination Code
  - SN = Subscriber Number
- SN points to a database
  - in case of MSISDN located in the HLR
  - in case of MSRN stored temporarily in the VLR
- MSRN includes sufficient information to enable the GMSC to route the call to the target MSC

International Mobile Equipment Identity



6 Digits 2 Digits 6 Digits

TAC FAC SN

IMEI

TAC: Type Approval Code,
The first two digits are the code for the country approval
SN: Serial Number

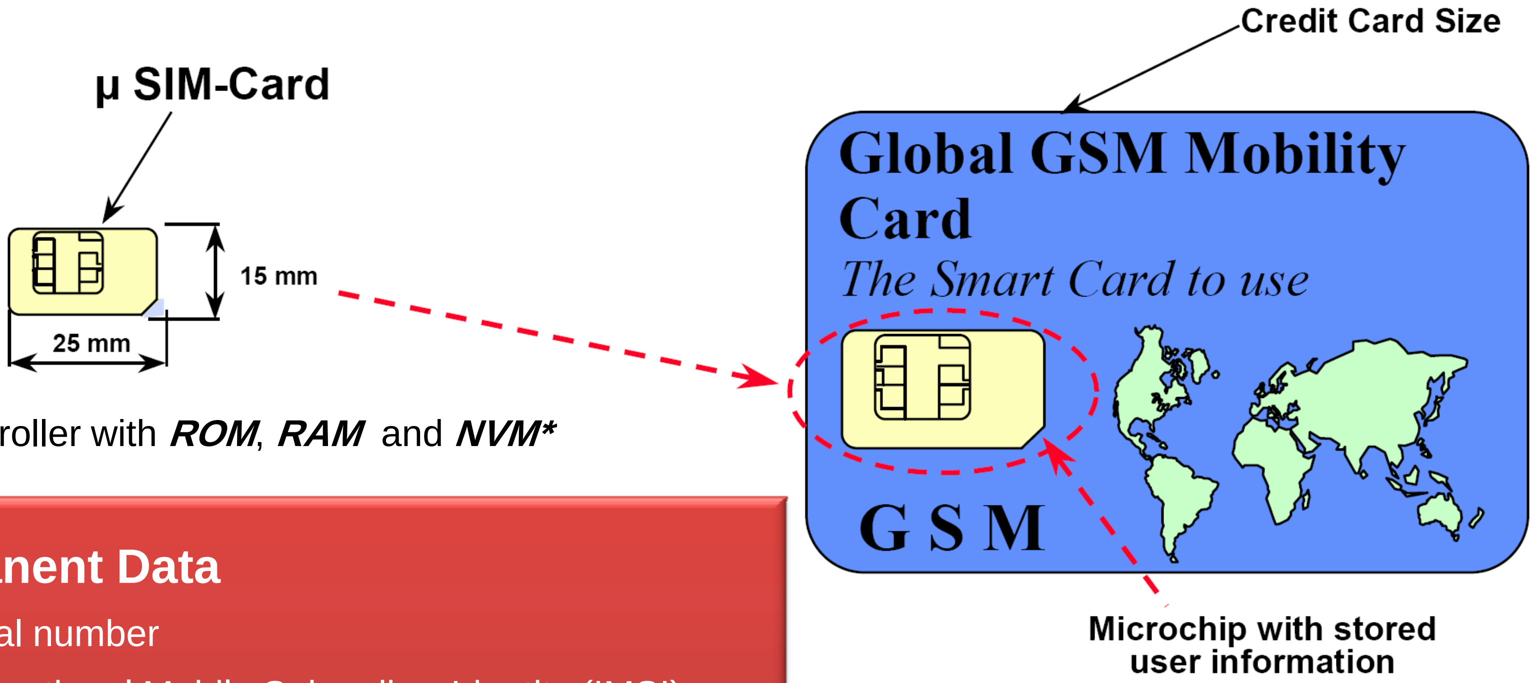
Final Assembly Codes (FAC)

01,02	AEG
07,40	Motorola
10,20	Nokia
30	Ericsson
40,41,44	Siemens
47	Optional International
51	Sony
51	Siemens
51	Ericsson
60	Alcatel
80	Philips
85	Panasonic

Network Elements

SIM Card

Data on the SIM



- µcontroller with ***ROM***, ***RAM*** and ***NVM****

Permanent Data

- Serial number
- International Mobile Subscriber Identity (IMSI)
- Security authentication and ciphering information
  - A3 and A8 algorithm
  - K_i, K_c
- Personal Identity Number (PIN)
- Personal Unblocking Number (PUK)

Removable Data

- Temporary Network information (LAI, TMSI)
- List of services subscribed by the user

**Non-Volatile Memory*

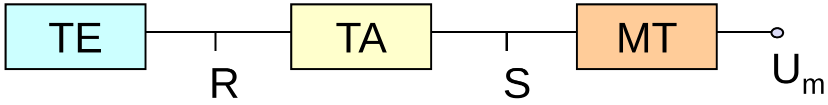
Stored before the SIM is sold

Mobile Station

Mobile station

- A Mobile Station (MS) is composed of a Mobile Termination (MT) and a Subscriber Module Identity (SIM) card.
- The SIM card stores information concerning the subscriber such as subscriber identity, services subscribed, parameters for security procedures and location information on the subscriber.
- The terminal can be used by any subscriber.
- The MT performs the following functions:
  - radio transmission termination;
  - radio transmission channel management;
  - terminal capabilities, including presentation of a man-machine interface to a user;
  - speech encoding/decoding;
  - error protection for all information sent across the radio path;
  - flow control of signaling and user data;
  - rate adaptation of user data between the radio channel rate and user rates;
  - multiple terminal support;
  - mobility management.

Mobile Station



Terminal Equipment

- It is an user terminal represented by one or more devices connected to a ME
  - data terminal
  - telex
  - fax machine
- Does not contain GSM specific functions
- TE can be classified based on the type of its interface
  - TE1 whether the interface is ISDN compliant
  - TE2 if the interface is not ISDN compliant (V.24/V.28, X.21, X.25, ...)

Terminal Adapter

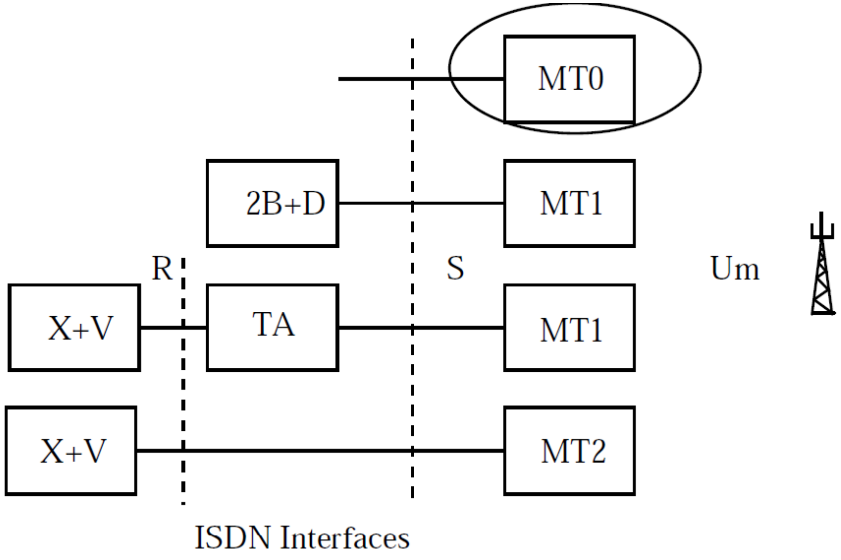
- It is used as a gateway between the TE and the ME
- It hides radio specific characteristics
- It is required when the external interface of the ME follows the ISDN standard and the TE presents a terminal-to-modem interface

Mobile Equipment (or MT)

- It carries out all functions related to
  - voice coding/decoding
  - channel coding
  - transmission over the radio interface
  - ciphering
  - management of the radio channel, the signalling, and the mobility

Mobile Termination

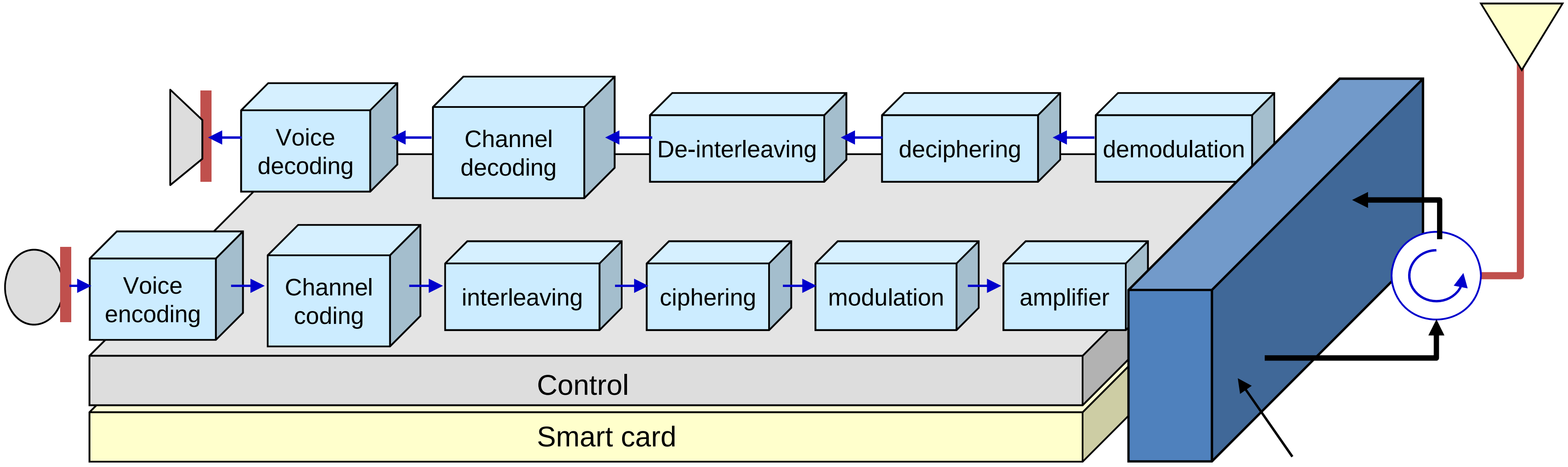
- There are three types of MT:
  - MT0 consists of the functions belonging to the functional group MT, with support of no terminal interfaces.
  - MT1 consists of the functions belonging to the functional group MT, and an interface with the GSM recommended subset of the ISDN user network interface recommendations.
  - MT2 consists of the functions belonging to the functional group MT, and with an interface that complies with the GSM recommended subset of the CCITT X or V series interface recommendations.



MT plus any TE (Terminal Equipment) or TE+TA (Terminal Adapter) will constitute the mobile station.

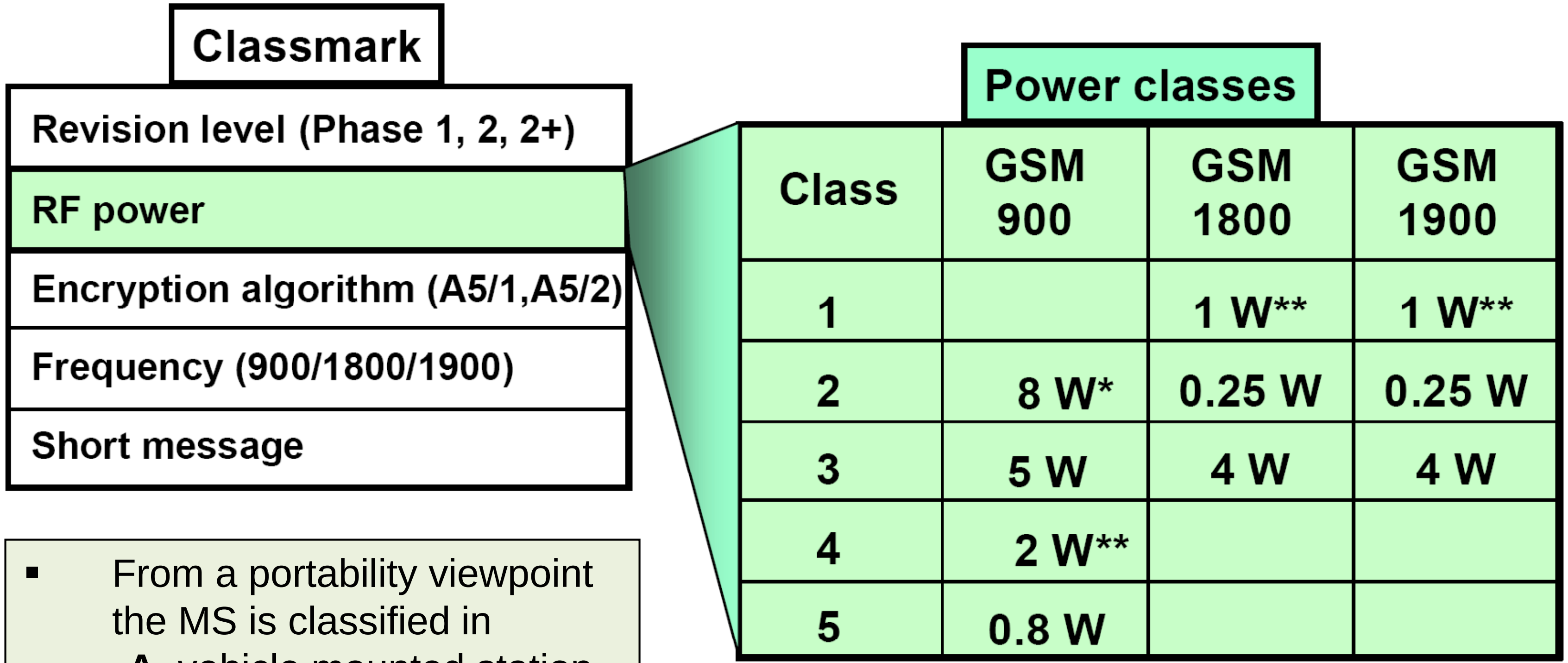
The Mobile Station

- The user identity is separate from the equipment identity.
- Different processing blocks are used to process the voice/data



Radio Transceiver

MS Classmark



Classmark

- Revision level (Phase 1, 2, 2+)
- RF power
- Encryption algorithm (A5/1,A5/2)
- Frequency (900/1800/1900)
- Short message

Power classes

Class	GSM 900	GSM 1800	GSM 1900
1		1 W**	1 W**
2	8 W*	0.25 W	0.25 W
3	5 W	4 W	4 W
4	2 W**		
5	0.8 W		

- From a portability viewpoint the MS is classified in
  A. vehicle mounted station
  B. portable station
  C. *hand-held station*

* Typical value for car mounted

** Typical value for handheld

BSS

Base Station Subsystem (BSS)

- BSS includes the network elements taking care of the radio cellular resources within the GSM network
- On one side, it is directly linked to the MSs through the radio interface (Air interface)
- On the other side it is interconnected with the switches of the NSS
  - its role consists in connecting MS and NSS and hence in connecting the caller to the other users
- It is controlled by the NMS (or OSS)

BSS Functions

- Radio path control
- Air and A interface signalling
- BTS and TC control through the BSC
- Hierarchical synchronisation
  - MSC synchronises BSCs and each BSC further synchronises the controlled BTSs
- Mobility management
  - different cases of handovers
- Speech transcoding
- Acquisition of statistical data

Base Transceiver Station

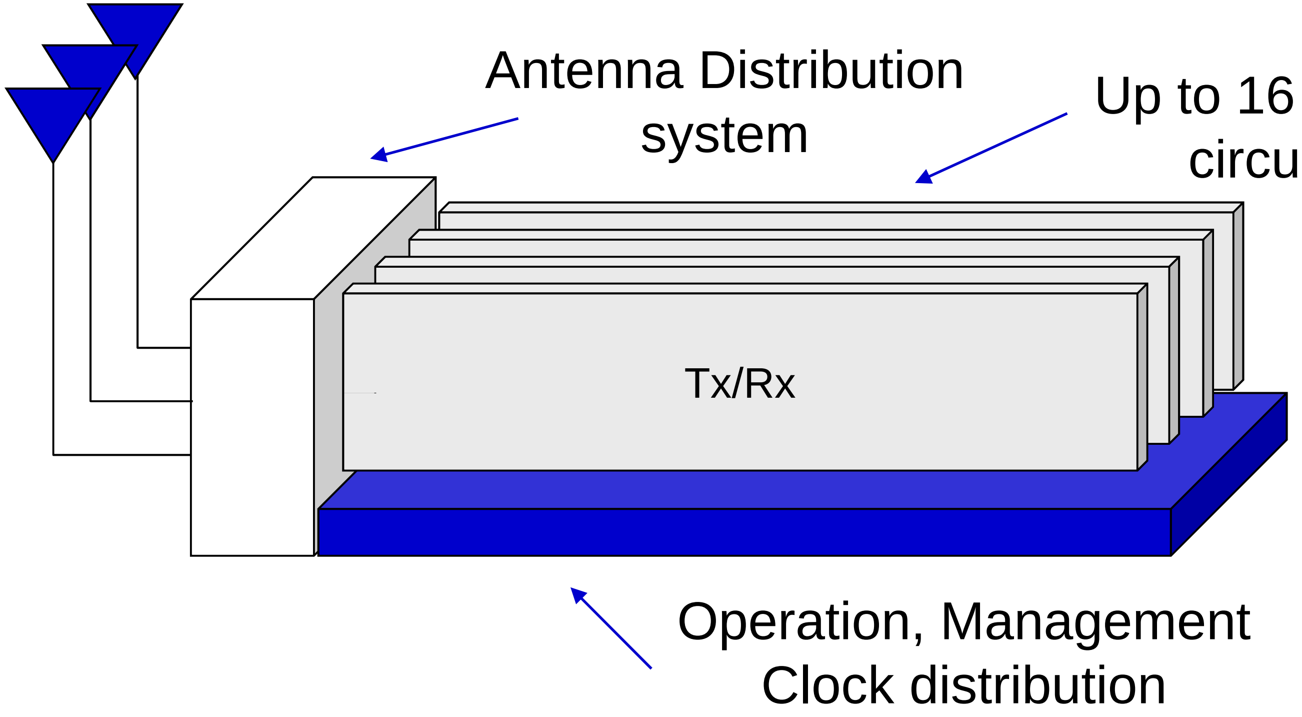
- BTS is a network element with transmission and reception devices (transceivers) to and from the MS, including
  - antennas
  - signal processing specific devices for the Air interface management
- It can be considered as a complex radio modem controlled by the BSC
- It is involved also in the transmission and reception with the BSC through the A-bis interface
- It has just executive functions (no management)

BTS Functions

- Broadcast/receive to/from the MS either signalling and traffic signals
- Perform source and channel coding
- Modulate/Demodulate signals to be broadcasted/received through the Air interface radio channel
- Multiplex the information to be transmitted over each carrier
- Measure the quality of the signalling and traffic signals in the downlink and uplink channels
- Transmit/receive signalling and traffic signals to/from the BSC through the A-bis interface

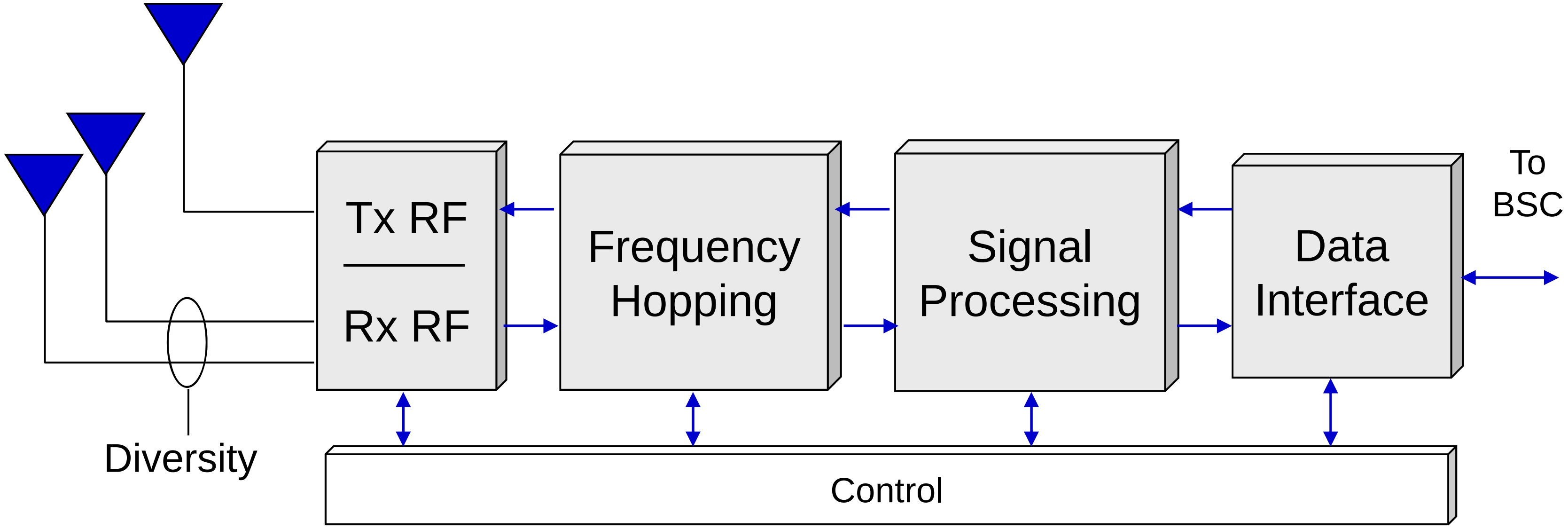
Base Transceiver Station

- Each BTS has several Transmit/Receive (Tx/Rx) units.
- The maximum number of Tx/Rx units per BTS is 16
- The BTS also has control circuits for operation, management and clock distribution

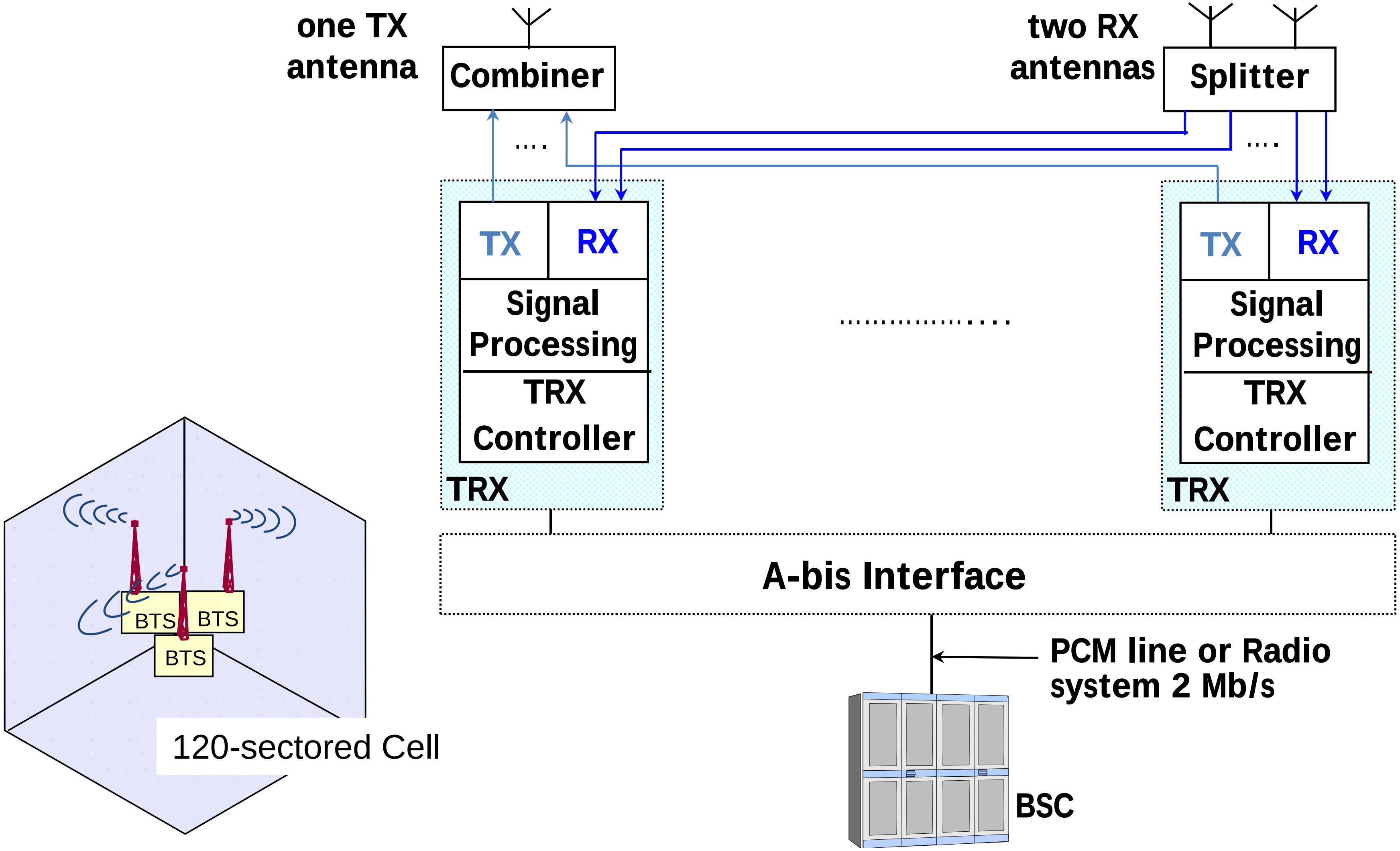

Antenna Distribution system
Up to 16 Tx/Rx circuits
Tx/Rx
Operation, Management Clock distribution

The Transmit/Receive Module

- The Tx/Rx unit consists of five sections:
  - Data interface unit to provide interface with the BSC
  - Baseband signal processing unit
  - Frequency Hopping and Radio frequency control module
  - Tx/Rx RF section
  - Control unit



BTS Scheme


one TX antenna
Combiner
two RX antennas
Splitter
....
....
TX
RX
Signal Processing
TRX Controller
TRX
....
TX
RX
Signal Processing
TRX Controller
TRX
A-bis Interface
PCM line or Radio system 2 Mb/s
BSC
BTS
BTS
BTS
120-sectored Cell

Base Station Controller

- The BSC is the central node within a BSS and co-ordinates the actions of Base Stations. The BSC controls a major part of the radio network
- BTS configuration: This involves the allocation of frequencies to channel combinations and power levels for each cell according to available equipment.
- Cell Description Data (e.g. cell identity, BCCH channel number, maximum and minimum output powers in the cell).
- Supervises the transmission network and the operation of each BTS

Base Station Controller Functions

- Control and supervise the BTSs
- Configure each cell with the allocation and the release of traffic and signalling channels
- Manage the paging operation
- Collect the signals quality measures acquired by the BTSs over the downlink and uplink channels
- Manage all the radio interfaces
- Manage the handover procedures
- Transcode and Sub-multiplex the bit stream
- Operate and sustain the whole BSS

Base Station Controller (BSC)

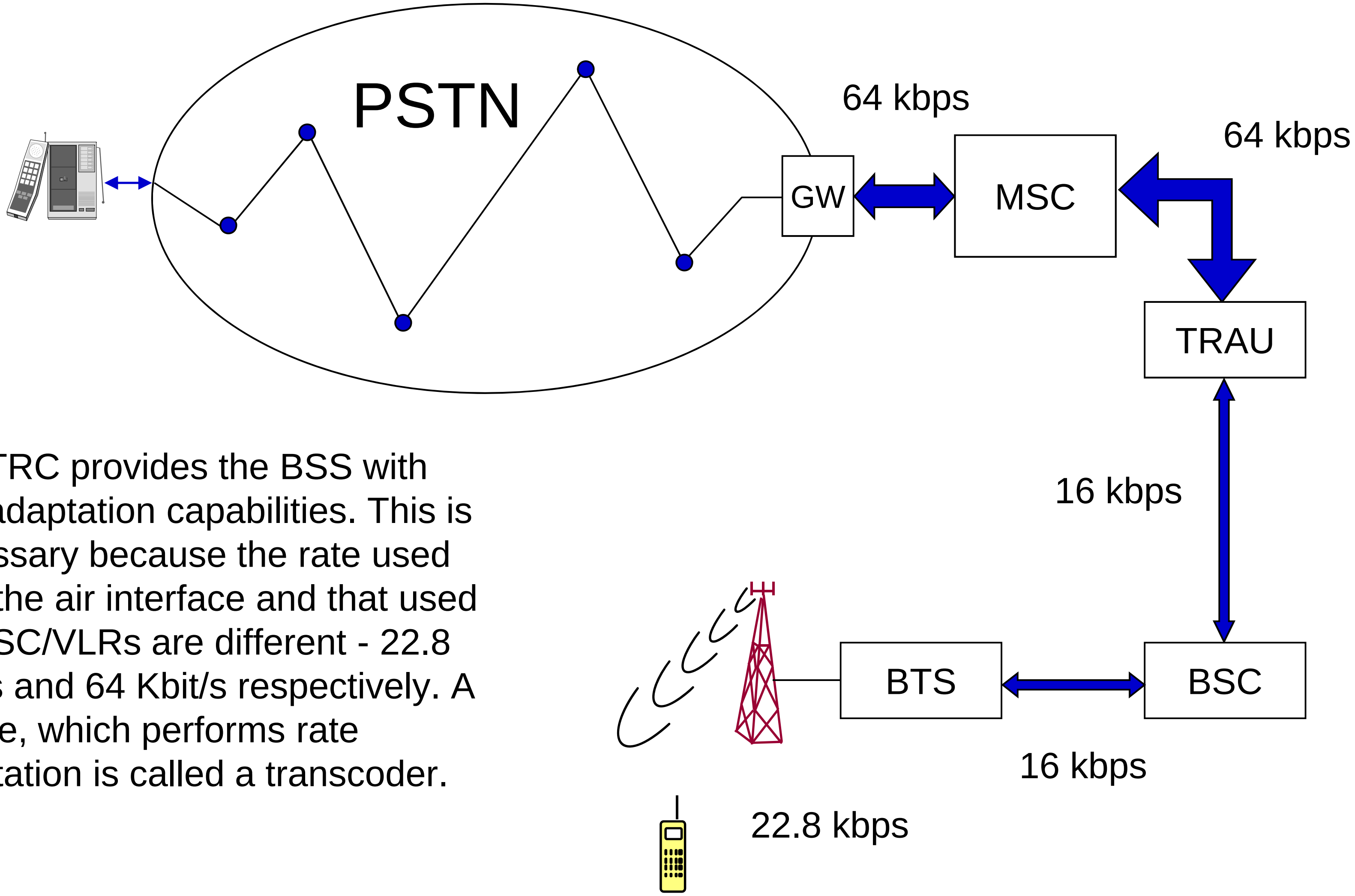
- Handling of MS connections :
  - During Call Set Up
    - Paging:
    - Signaling set-up
    - Assignment of traffic channel
  - During a Call:
    - Dynamic power control in MS and BTS
    - Locating
    - Handover
    - Frequency Hopping

BTS & BSC Functions

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

TRAU

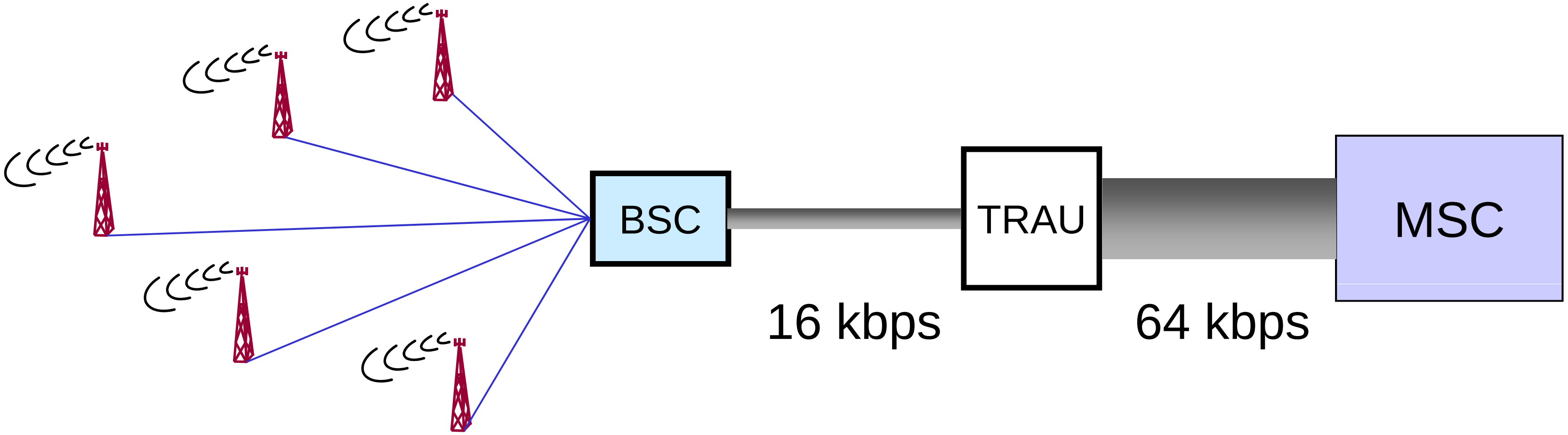
GSM Typical Voice Connection



The TRC provides the BSS with rate adaptation capabilities. This is necessary because the rate used over the air interface and that used by MSC/VLRs are different - 22.8 Kbit/s and 64 Kbit/s respectively. A device, which performs rate adaptation is called a transcoder.

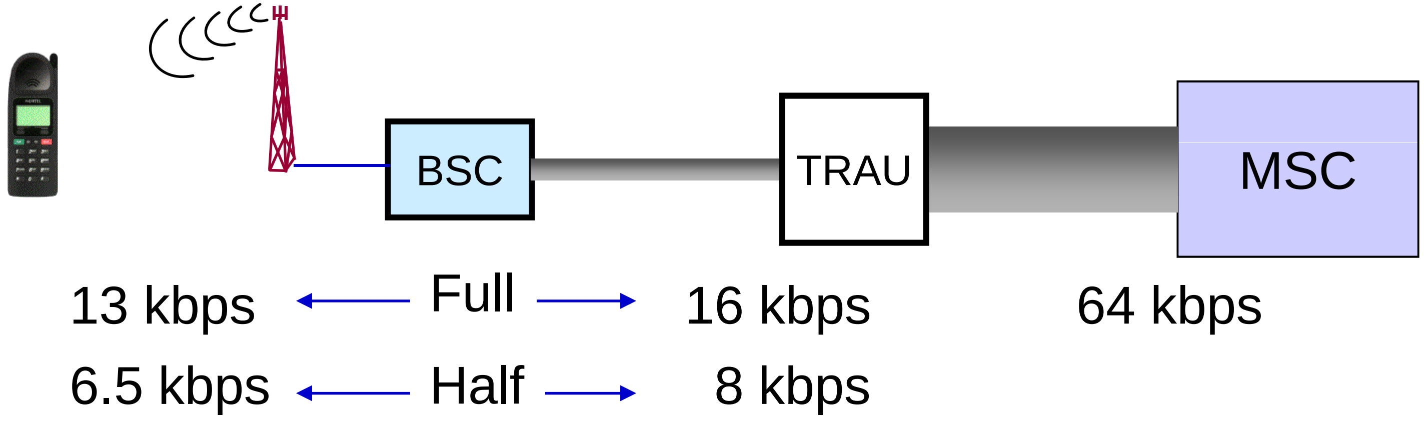
The TRAU Unit

- The Transcoding Rate and Adaptation Unit (TRAU) is typically located between the MSC and BSC.
- It could also be placed between the BSC and the BTS's
- It converts the 64 kbps PCM-speech into 16 kbps compressed speech [13 kbps speech + 3 kbps overhead]
- It uses speech vocoding technique.
- There is an equivalent unit in the Mobile Station (MS)



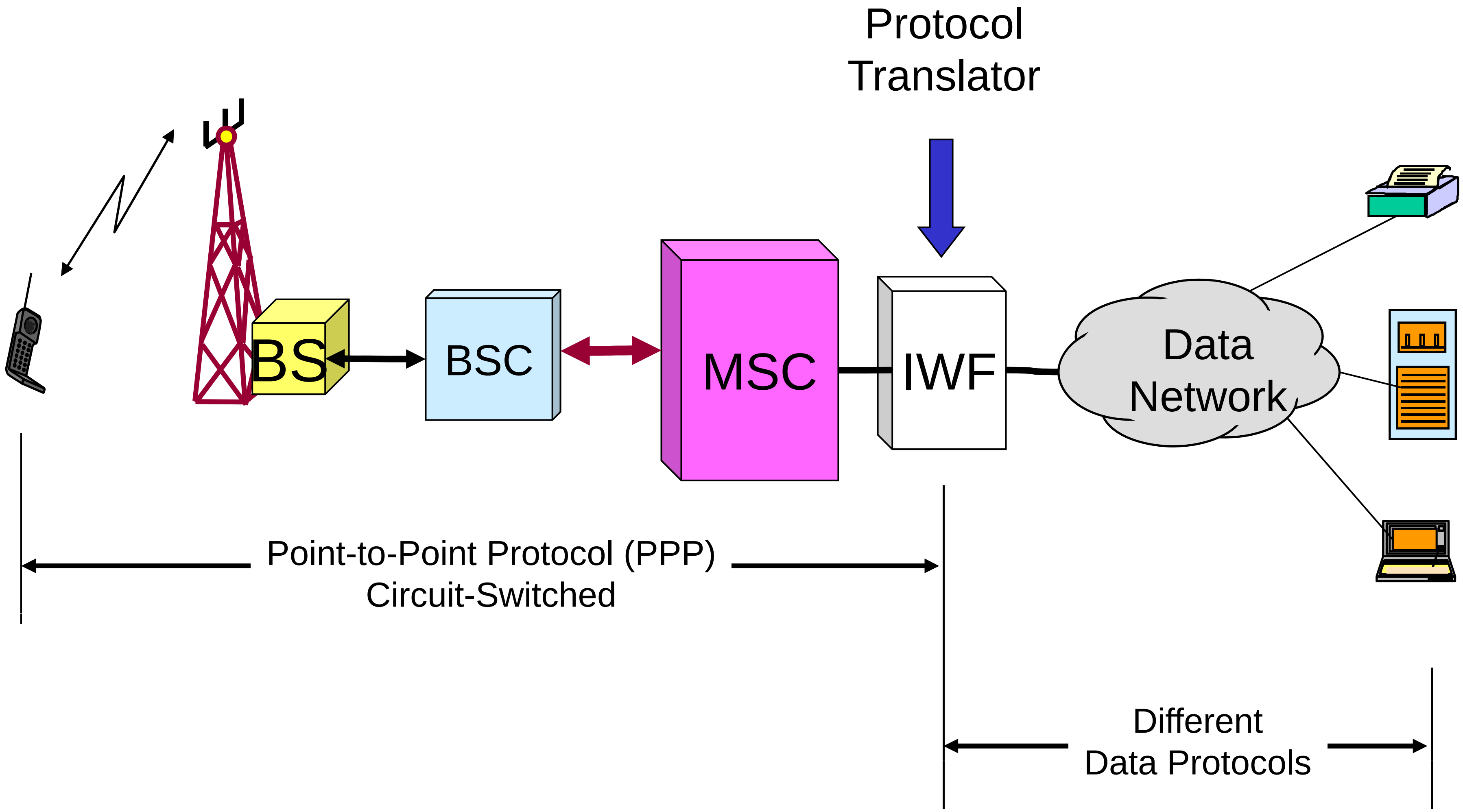
The TRAU Unit (cont.)

- The TRAU unit could be physically located with the MSC to save transmitting 64 kbps/speech connection
- If the connection is "data connection" (rather than speech), the unit is turned off
- In the MS, the same vocoding technique is used to convert analog signal into digital speech at 13 kbps (full rate)
- The unit could also operate at 6.5 kbps (half rate)



IWF

Inter-Working Facility (IWF)



NSS

NSS

- The Network and Switching Sub-system includes the main switching functions of the GSM network
- It directly interoperates with external networks (PSTN, ISDN, PSPDN)
- In the NSS, databases for the subscriber data and mobility management are installed
- A further function consists in managing the communication between the GSM subscriber and other telecommunication network users

NSS Functions

- Call control
  - identification of the subscriber
  - establishing a call and release of the connection after the call is over
- Mobility management
  - taking care of the location of the subscribers before, during and after a call
- Collecting the charging information about a call
  - number of the caller and of the called subscriber
  - length and type of the provided services
  - ….

NSS Functions

- Transfer the acquired charging information to the Billing centre
- Signalling with other networks and BSS through the different interfaces
- Subscriber data handling
  - Data storage permanently or temporarily in some databases

Mobile Switching Center (MSC)

- The primary node in a GSM network is the MSC. It is the node, which controls calls both to MS's and from MS's. The primary functions of an MSC include the following:
  - Switching and call routing to or from MS.
  - Charging.
  - Service provisioning.
  - Control of connected BSC's.
  - Direct access to Internet services.
  - Provides the gateway functionality to other networks.

MSC

- The MSC main scope consists in performing switching functions
- It co-ordinates the setting-up of the call to and from the GSM users located in the area of its competence
- It controls more BSCs
- MSC has interfaces with BSS on one side and with the external networks on the other side
  - the interface with external networks requires a gateway (GMSC) for adaptation

Gateway Mobile Switching Center (GMSC)

- Gateway functionality enables an MSC to interrogate a HLR in order to route a mobile terminating call. It is not used in calls from MS's to any terminal other than another MS.

- For example, if a person connected to the PSTN wants to make a call to a GSM mobile subscriber, then the PSTN exchange will access the GSM network by first connecting the call to a GMSC

Supporting Data Bases

Home Location Register (HLR)

- The HLR is a centralized network database that stores and manages all mobile subscriptions belonging to a specific operator.
- It acts as a permanent store for a person's subscription information until that subscription is cancelled.
- The primary functions of the HLR include:
  - Stores for each mobile subscriber:
    - Basic subscriber categories.
    - Supplementary services.
    - Current location.
    - Allowed/barred services.
    - Authentication data.
  - Subscription database management
  - Controls the routing of mobile terminated calls and SMS.

Data stored in the HLR

Home Location Register (HLR), stores data of participants, which are reported in an HLR-area

- Semi-permanent data:
  - MSISDN
  - IMSI
  - Personal data (name, address, mode of payment)
  - Service profile (call transfer, Roaming-limits etc.)
- Temporary data:
  - MSRN (Mobile Subscriber Roaming Number) (country, net, MSC)
  - VLR-address, MSC-address
  - Authentication Sets of AC (RAND (128 Bit), SRES (128 Bit), K_C (64Bit))
  - charge data

HLR Functions

- HLR must recognise the VLR identification number for the MS location
- Update this field in its database
- Send the routing information (Mobile Station Roaming Number - MSRN) to the requesting GMSC
- Enable and disable the supplementary services
- Store and provide the authentication and ciphering triplets to the requesting VLR
- Manage the subscriber’s data
- Manage the user password for some supplementary services (e.g. “Call Barring”)

Visitor Location Register

- The role of a VLR in a GSM network is to act as a temporary storage location for subscription information for MSs, which are within a particular MSC service area.

- Thus, there is one VLR for each MSC service area. This means that the MSC does not have to contact the HLR (which may be located in another country) every time the subscriber uses a service or changes its status.

- VLR keeps location registrations and updates as long as subscriber is within its coverage area

- The VLR is always integrated with the MSC.

Data stored in the VLR

Visitor Location Register (VLR)

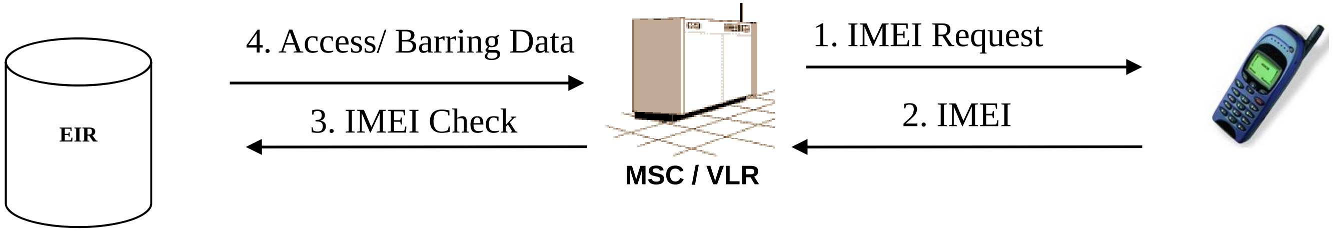
- local database of each MSC with following data:
  - IMSI, MSISDN
  - Service profile
  - Accounting information
  - TMSI (Temporary Mobile Subscriber Identity) - pseudonym for data security
  - MSRN
  - LAI (Location Area Identity)
  - MSC-address, HLR-address

VLR Functions

- For the visiting subscribers the VLR contains a copy of their subscriber data. This data is downloaded from the HLR during the Location Update procedure.
- The VLR is responsible for the MSRN number management for the visiting subscribers, during the Mobile Terminating Call Setup
- The VLR is responsible for the assignment of the TMSI (Temporary Mobile Station Identity) to the visiting subscribers
- To access the subscriber data the numbers IMSI, MSRN and the TMSI are used
- In many systems the MSC and VLR are always co-located within one hardware entity.

Equipment Identification Register (EIR)

- Because the subscriber and equipment are separate in GSM, it is necessary to have a separate authentication process for the MS equipment.
- The equipment identification procedure uses the identity of the equipment itself (IMEI) to ensure that the MS terminal equipment is valid.



Equipment Identification Register

- The Equipment Identification Register main goal consists in storing the International Mobile Equipment Identity (IMEI)
- EIR is a database installed in the NSS allowing at the GSM network to verify the authorisation of the active MEs
  - **White list**
    - include the IMEIs allocated to all approved MEs
  - **Grey list**
    - include IMEIs of faulty MEs, whose fault is not important enough to justify plain barring
    - include IMEIs of non homologated MEs (optional)
  - **Black list**
    - include the range of IMEIs related to stolen MEs and not authorised to access to the network

Authentication Center (AUC)

- To protect GSM systems, the following security functions have been defined:
  - Subscriber authentication: by performing authentication, the network ensures that no unauthorized users can access the network, including those that are attempting to impersonate others.
  - Radio information ciphering: the information sent between the network and a MS is ciphered. A MS can only decipher information intended for it.

Authentication Center (AUC)

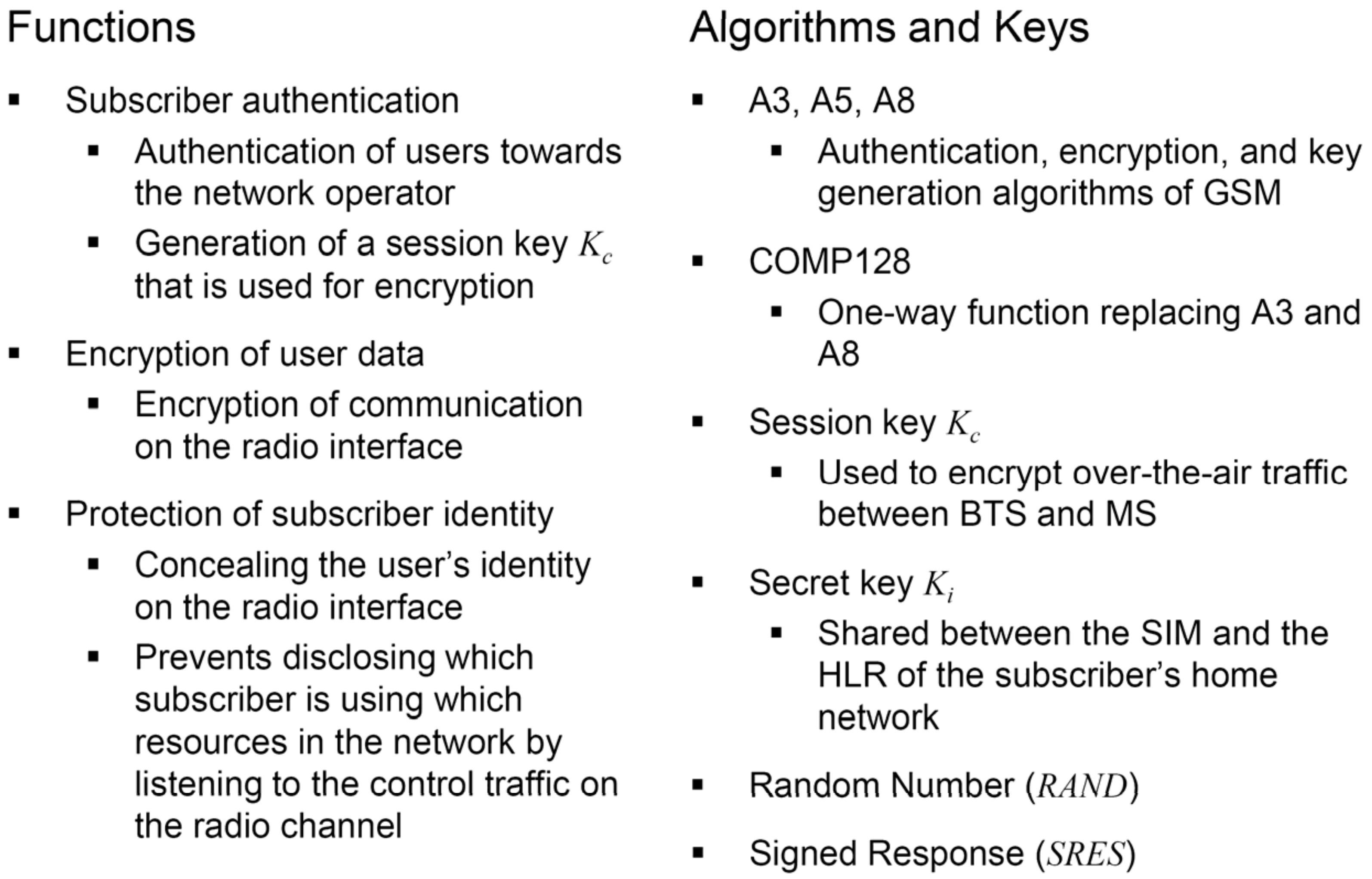
- The AC is a functional entity which is used for security related functions
- Management of the secret authentication key (Ki) per subscriber.
- Management of the authentication vectors RAND and SRES per call.
- Management of the encryption key Kc, used by the switching subsystem for signaling and user data security.
- For dynamic reasons, the AC is always co-located with the HLR within one hardware entity.

- A triplet consists of
  - RANDom number (RAND)
  - Signed RESponse (SRES)
  - ciphering key Kc

At the request of the VLR, several triples are generated for each mobile subscriber in the AC and transferred to the VLR via the HLR on request.
Remark: The individual key Ki is only stored in the AC and the SIM card. Different to the IMSI and the triples, it is never transmitted through the network. For all signaling procedures the users IMSI is used.

Encryption

Security Functions, Algorithms, and Keys



Functions

- Subscriber authentication
  - Authentication of users towards the network operator
  - Generation of a session key K_c that is used for encryption
- Encryption of user data
  - Encryption of communication on the radio interface
- Protection of subscriber identity
  - Concealing the user's identity on the radio interface
  - Prevents disclosing which subscriber is using which resources in the network by listening to the control traffic on the radio channel

Algorithms and Keys

- A3, A5, A8
  - Authentication, encryption, and key generation algorithms of GSM
- COMP128
  - One-way function replacing A3 and A8
- Session key K_c
  - Used to encrypt over-the-air traffic between BTS and MS
- Secret key K_i
  - Shared between the SIM and the HLR of the subscriber's home network
- Random Number ($RAND$)
- Signed Response ($SRES$)

Cryptographic Algorithms

A3

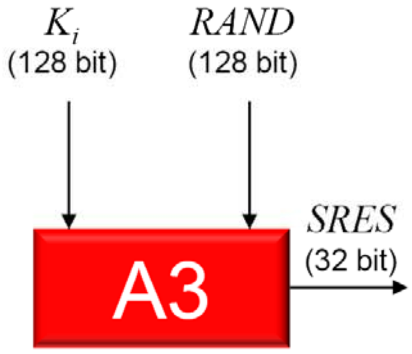
- Authentication algorithm
- Calculates $SRES$ based on the K_i key (stored on the SIM and in the HLR) and the $RAND$ sent by the MSC
- Not standardized; can be chosen independently by each operator

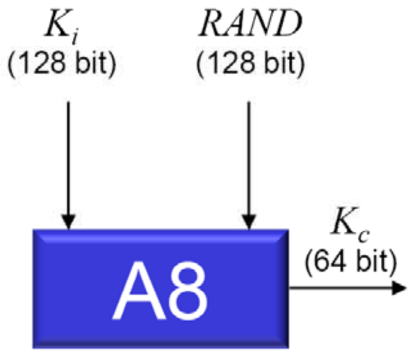
A8

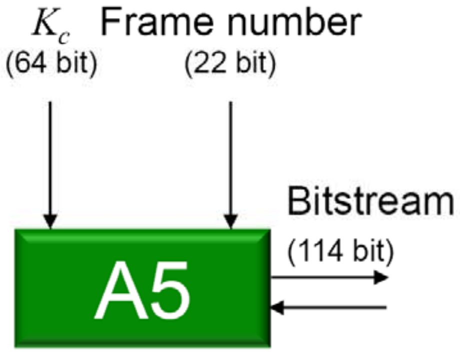
- Key generation algorithm needed to calculate the session key K_c
- Calculation of K_c depends on K_i and RAND
- Not standardized; can be chosen independently by each operator

A5

- Stream cipher used to encrypt over-the-air-transmissions
- Ciphering is based on K_c and the frame number
- Specified at international level to enable roaming

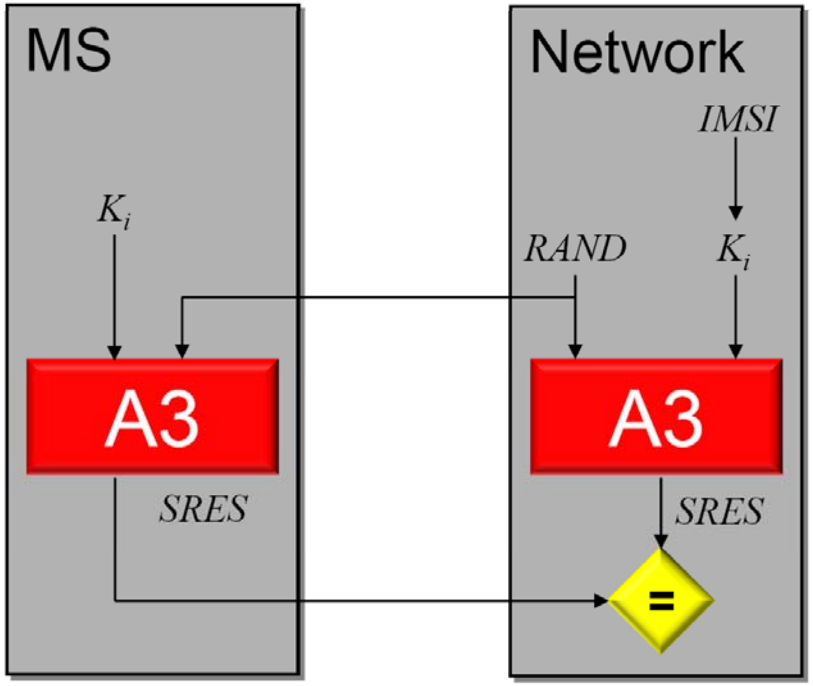






Subscriber Authentication

- Authentication is necessary during
  - Location registration
  - Location update with change of the VLR
  - Call setup
  - Sending a short message (SMS)
- **Challenge-response**: authentication technique where the subscriber is prompted (the challenge) to provide some private information (the response)
- Process of authentication is based on the algorithm A3, K_i and $RAND$
- Challenge: $RAND$
- Response: $SRES$
- K_i is stored on the SIM (terminal side) and in the AUC (network side) and is used to calculate $SRES$ based on A3

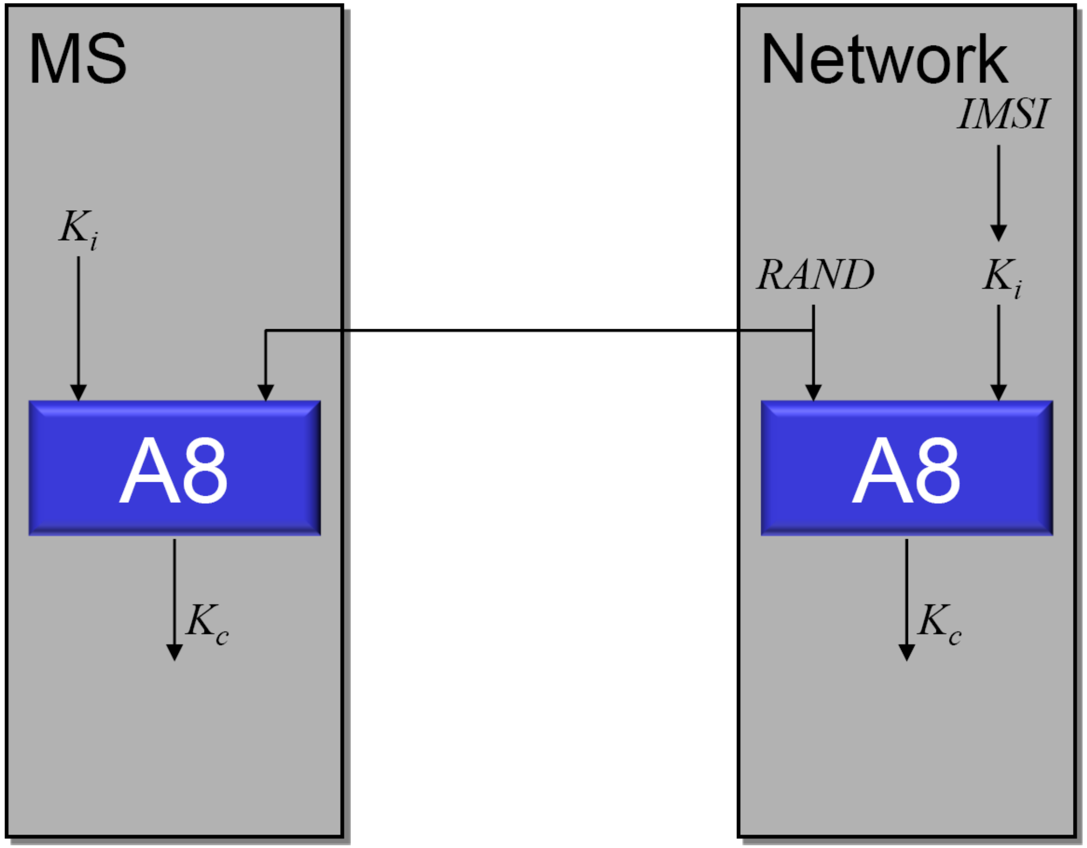


- Each execution of A3 is performed with a new value of $RAND$ (which cannot be predetermined)

➡ Recording the channel transmission and playing it back cannot be used to fake an identity

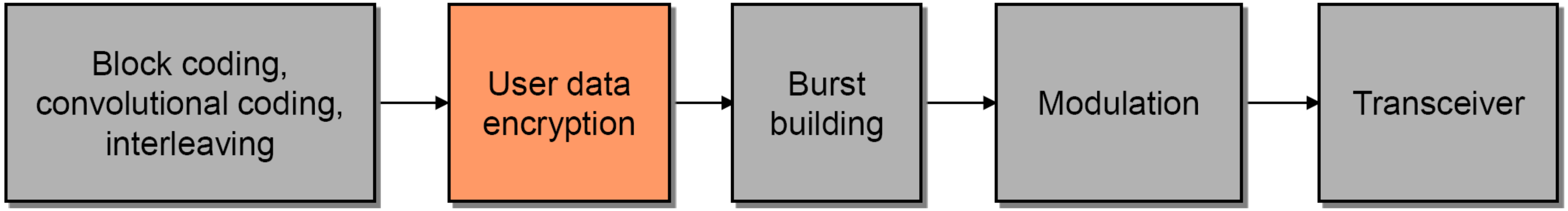
Generation of the Session Key Kc

- K_c is used in A5 for symmetric encryption of user and signaling data
- Generated at each side using the generator algorithm A8 and $RAND$
- At the network side, values for K_c are calculated simultaneously with $SRES$ (see subscriber authentication)
- For each session (call, SMS, location update,...) a new session key K_c needs to be generated



Symmetric Encryption of User and Signaling Data (1)

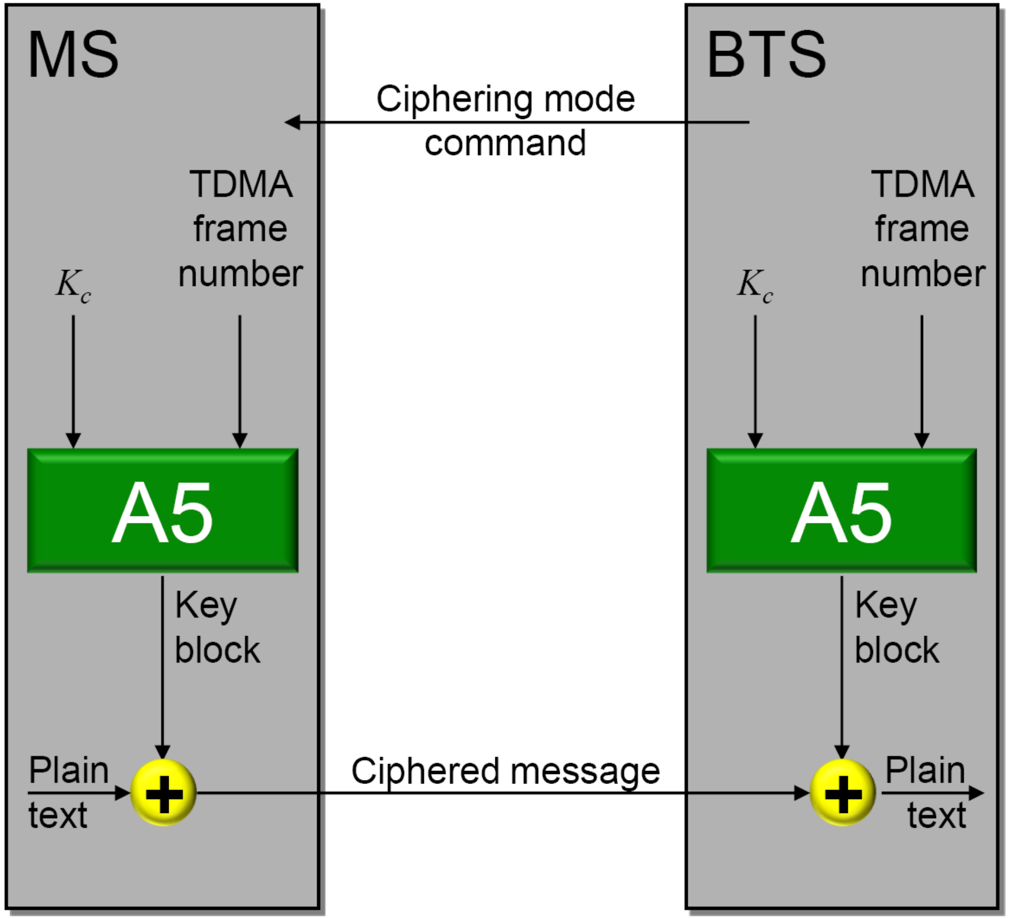
- Encryption of transmitted data is a special characteristic of GSM that distinguishes GSM from analogue cellular and ISDN networks
- Transmitting side: encryption after channel coding and interleaving
- Receiving side: decryption directly follows the demodulation of the data stream



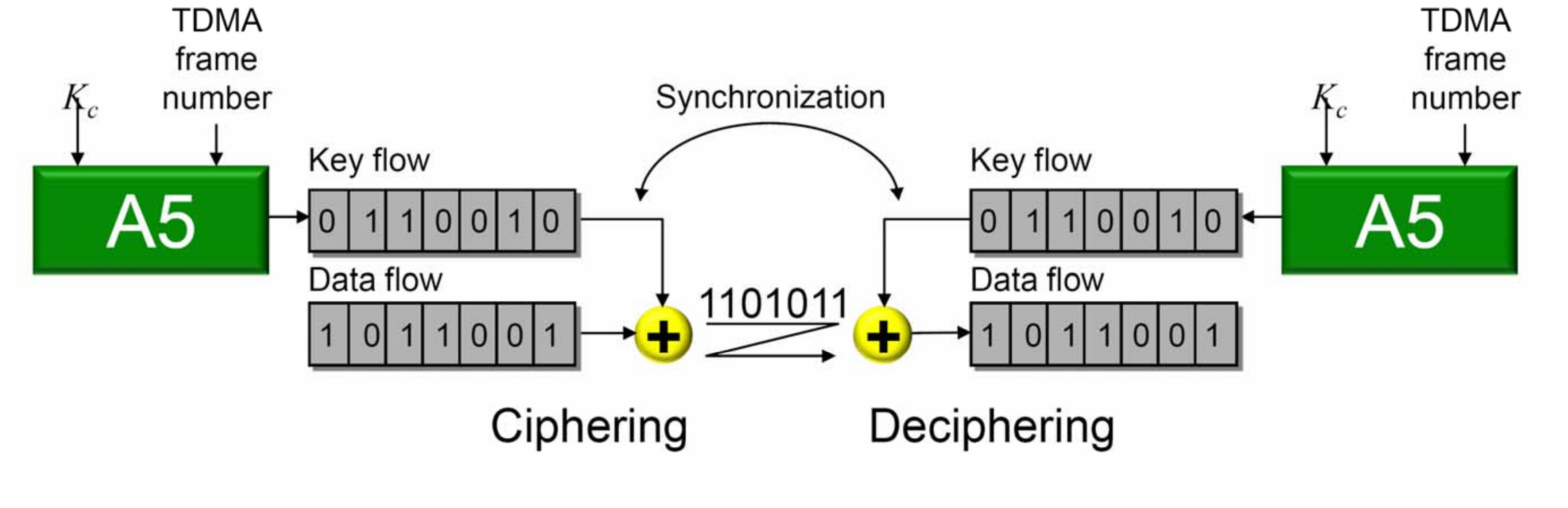
- **Block coding**: generates the parity bit for a block of data thus allowing the detection of errors in this block
- **Convolutional coding**: calculation of additional redundancy for error correction to correct errors caused by the radio channel
- **Interleaving**: distribution of code words by spreading in time and merging them across several bursts of transmission (achieves better error correction results)
- **Burst building**: each interleaving block (114 bit) is mapped onto a burst
- **Differential coding and modulation**: coding the bursts for transmission over the air interface

Symmetric Encryption of User and Signaling Data (2)

- Encryption of signaling and user data is performed at the mobile station as well as at the base station
- Symmetric encryption: ciphering and deciphering are performed with the same key K_c and the A5 algorithm
- Signaling and user data are encrypted together (TCH/SACCH/FACCH); for dedicated signaling channels (SDCCH) the same method is used as for traffic channels
- **Note**: encryption of user and control data is an optional feature of GSM and may be deactivated by the operator by suppressing the ciphering mode command



Symmetric Encryption of User and Signaling Data (3)



- **Stream Cipher**: Ciphering uses a bit stream which is added bitwise (EXCLUSIVE-OR) to the data to be ciphered
- Deciphering: EXCLUSIVE-OR operation on the enciphered data stream with the ciphering stream
- Synchronization between ciphering and deciphering is performed through the TDMA frame number
- TDMA frame number is related to the current TDMA frame within a hyperframe
- TDMA Frame number is broadcasted on the SCH and is thus available to all mobile stations currently in the cell

Protection of Subscriber Identity (1)

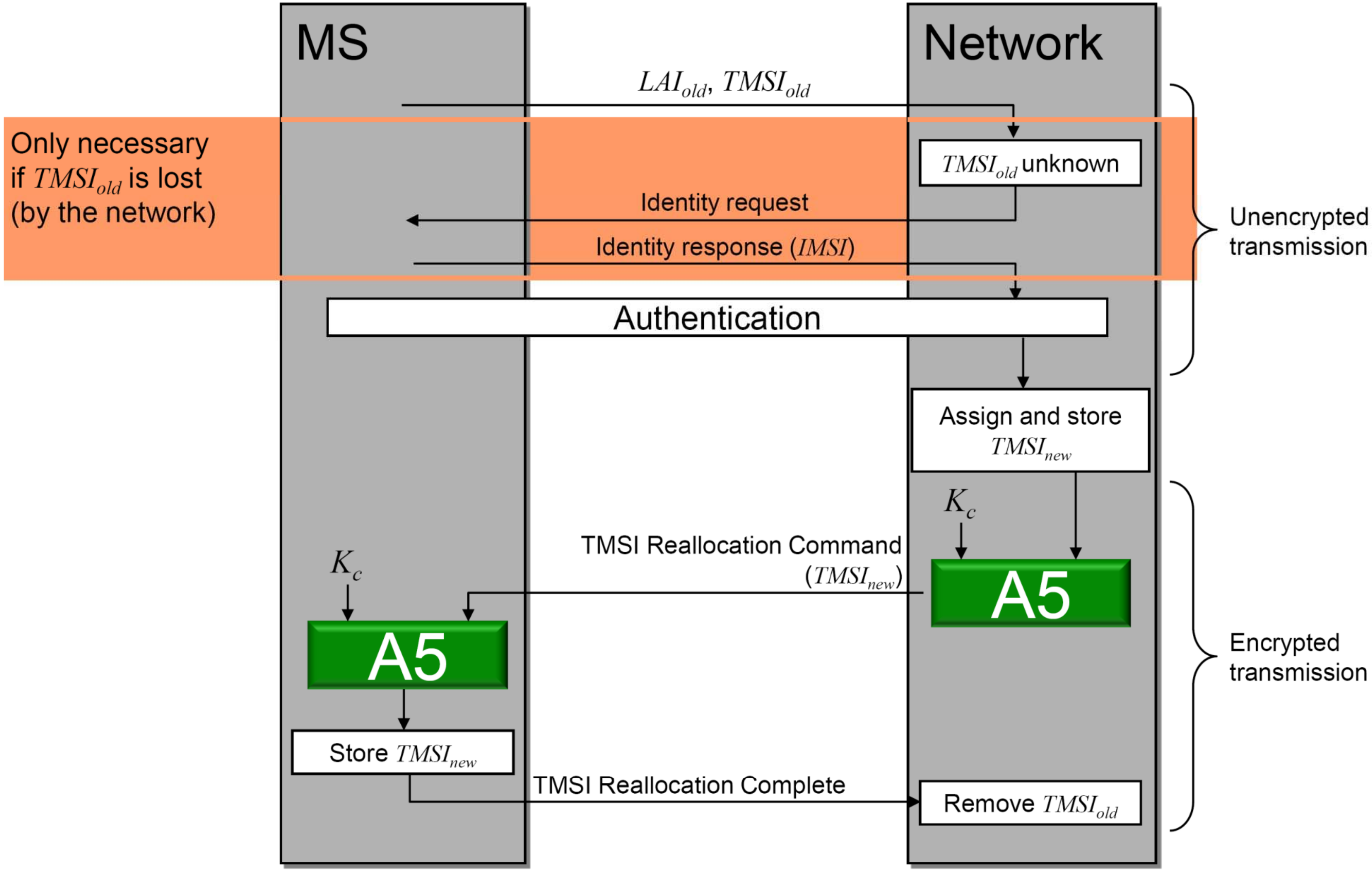
Purpose

- Prevents disclosing which subscriber is using which resources in the network
- Ensures the confidentiality of user data and signaling traffic
- Prevents localization and tracking of mobile stations by unauthorized entities

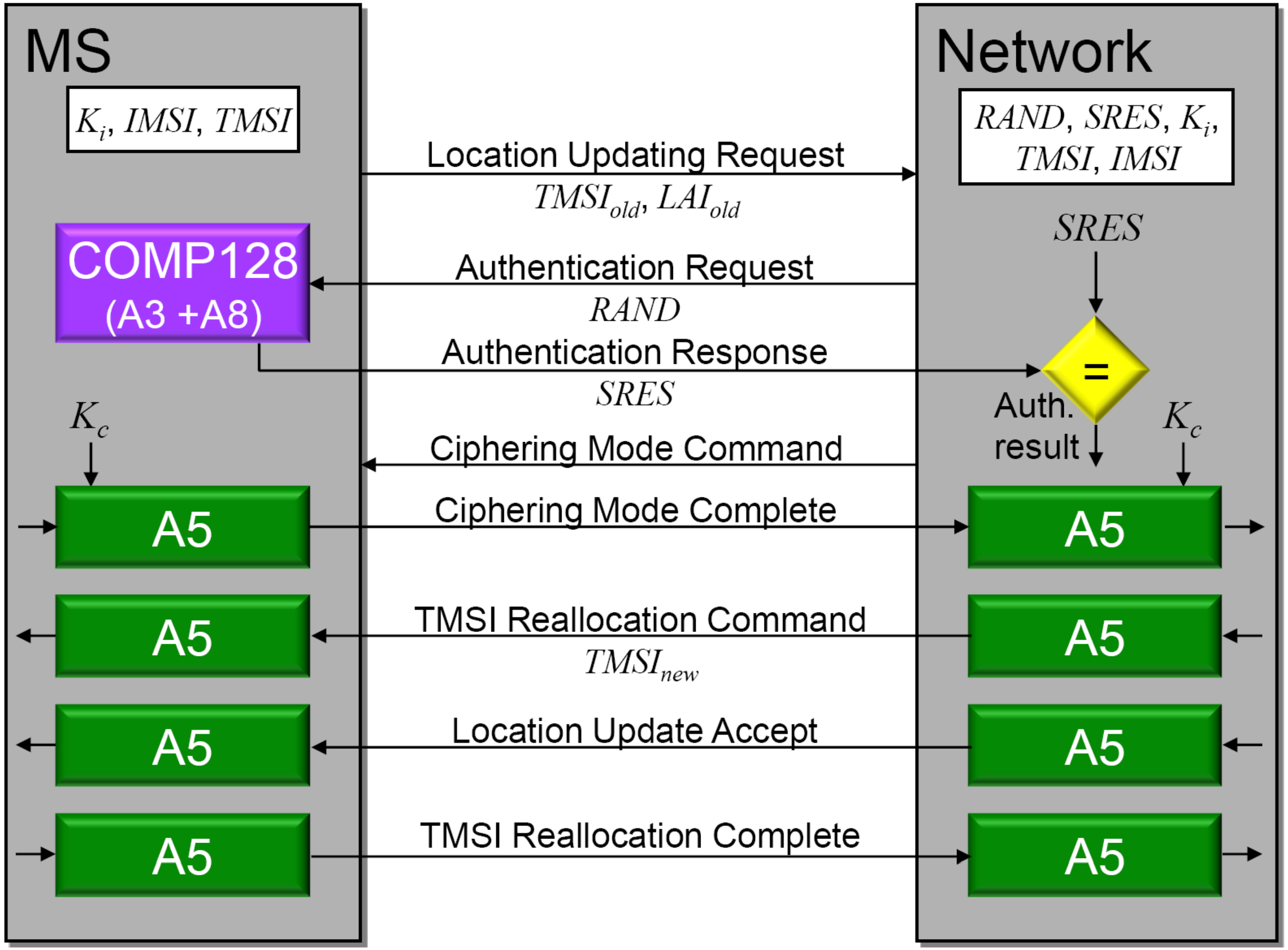
Realization

- It should be avoided to transmit the IMSI unencrypted
- Instead of the IMSI, the TMSI is used on the radio channel for identification purposes
- The TMSI is temporary and has only validity within the coverage area of the current VLR
- The subscriber can only be uniquely identified by using the TMSI in combination with the LAI
- Association between IMSI and TMSI is stored in the VLR
- Algorithm for generating the TMSI is determined by the network operator and is not subject to standardization
- Subscriber identity is protected against eavesdropping in two ways:
  - the temporary TMSI is used on the radio channel instead of the IMSI
  - each new TMSI is transmitted in encrypted form
- In case of database failures (loss of TMSI, TMSI unknown at VLR, etc.) the IMSI must be transmitted as clear text before encryption is turned on

Protection of Subscriber Identity (2)

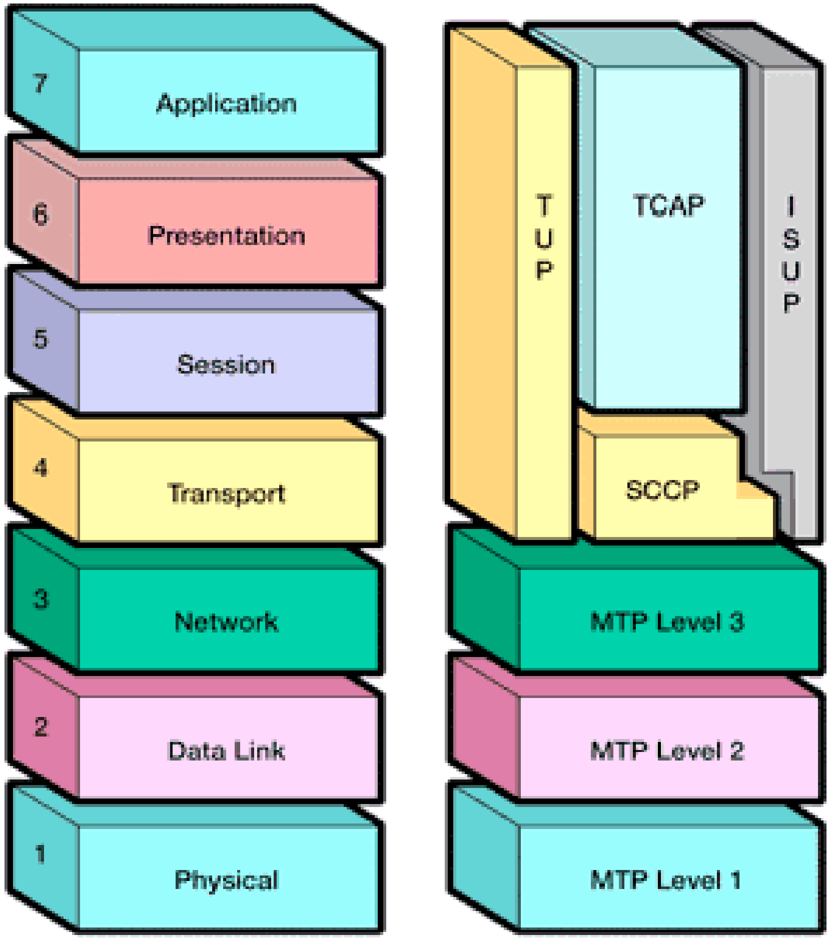

MS
Network
LAI_{old}, $TMSI_{old}$
Only necessary if $TMSI_{old}$ is lost (by the network)
$TMSI_{old}$ unknown
Identity request
Identity response ($IMSI$)
Unencrypted transmission
Authentication
Assign and store $TMSI_{new}$
K_c
A5
TMSI Reallocation Command ($TMSI_{new}$)
K_c
A5
Encrypted transmission
Store $TMSI_{new}$
TMSI Reallocation Complete
Remove $TMSI_{old}$

Interaction of GSM Security Mechanisms



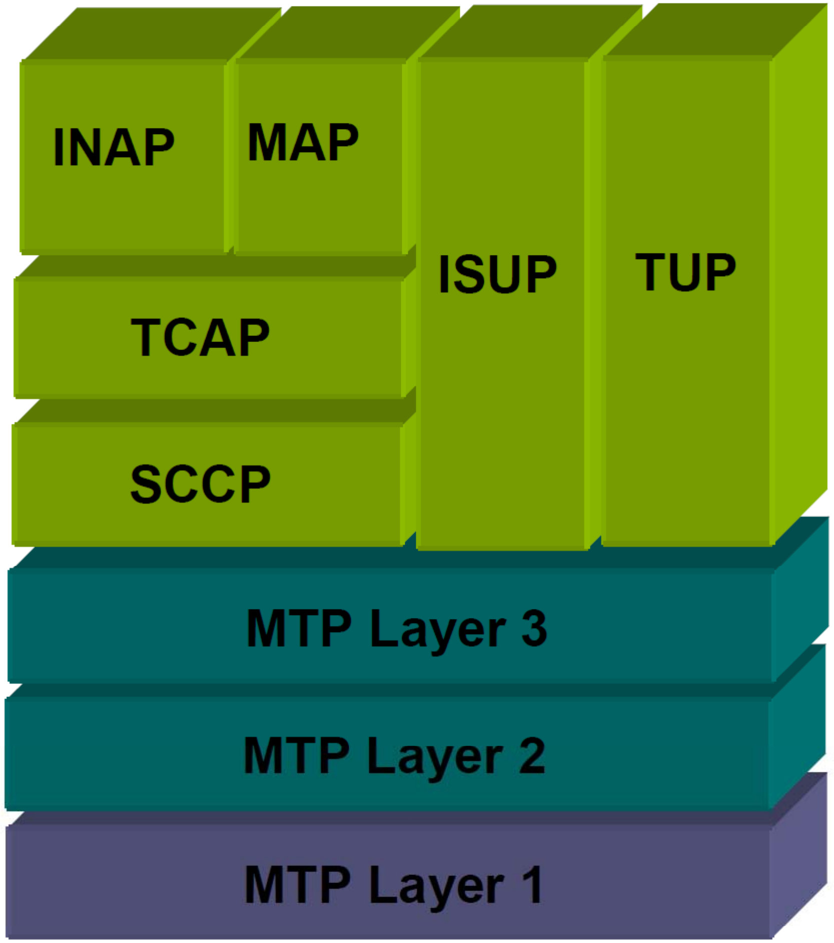
Call Flows

SS7 Protocol stack



SS7 network is an interconnected set of network elements that is used to exchange messages in support of telecommunications functions.

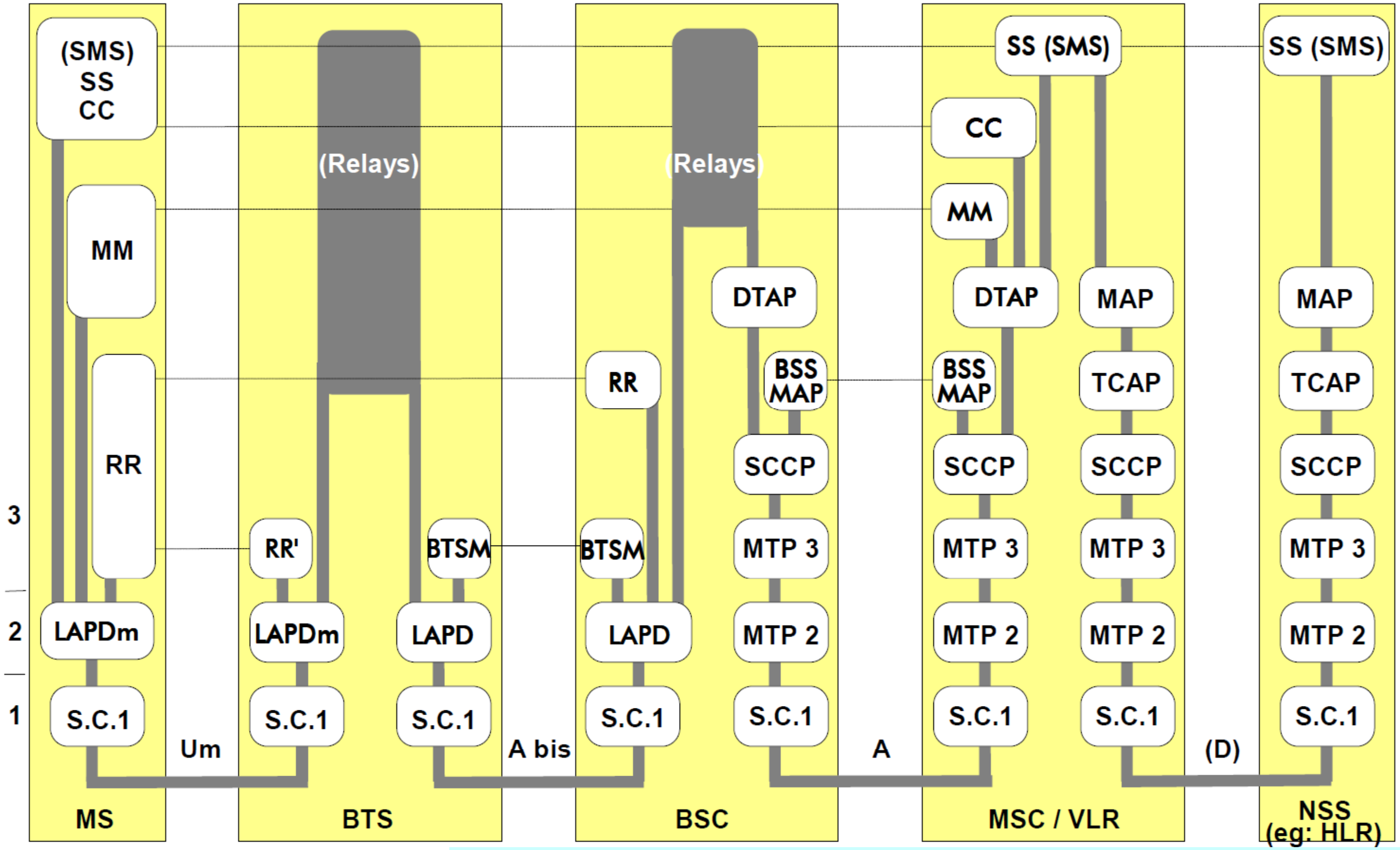
SS7 Protocol stack



Initial Address Message (IAM)

- Is an ISUP message
- The IAM is the first message sent to the next network node during call set-up. It is used for seizing a circuit and contains all information necessary for routing to the terminating network node.

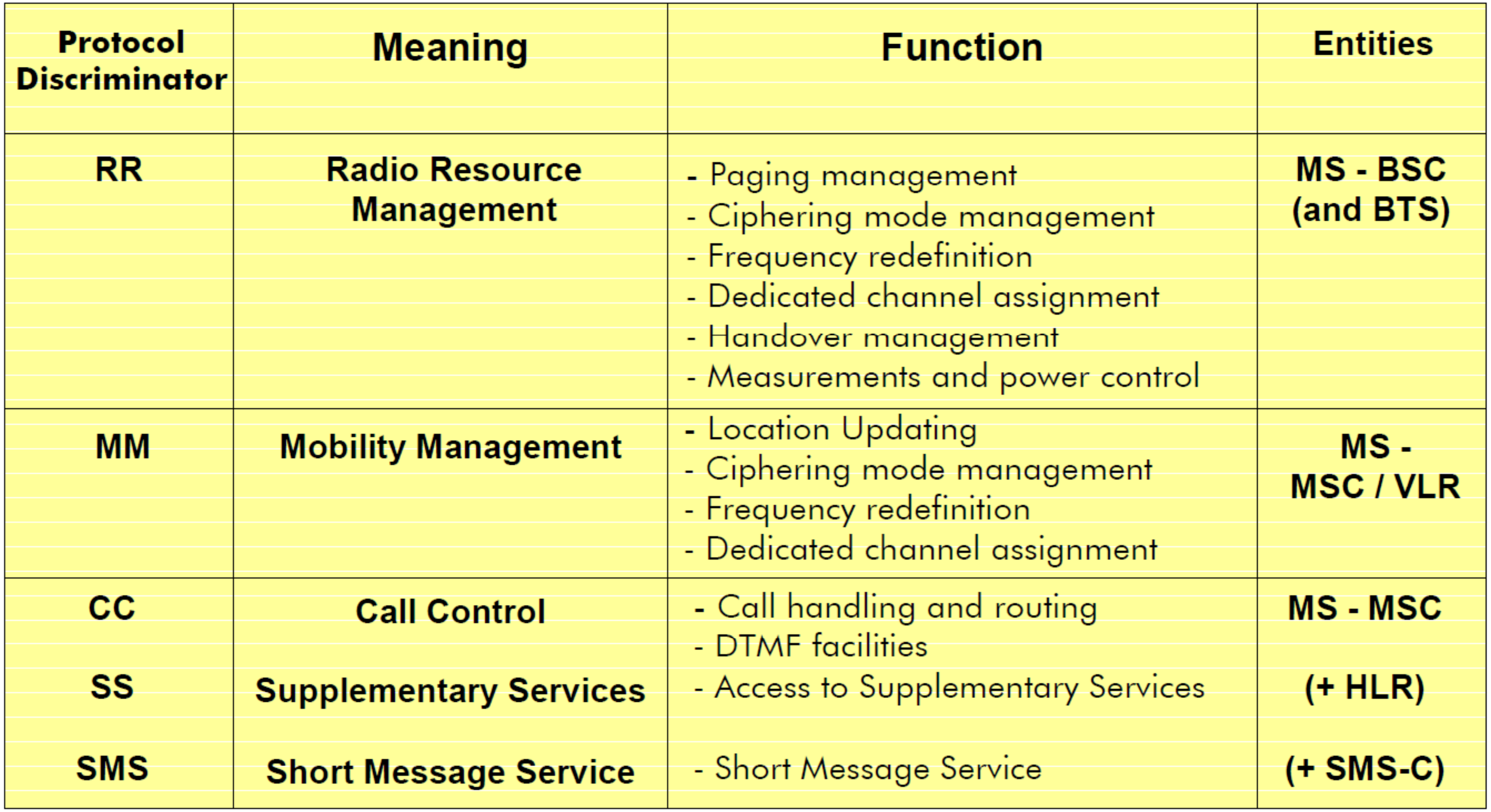
GSM protocol layers for signaling



- CC = Call Control
- SS = Supplementary Services
- SMS = Short Message Service
- MM = Mobility Management
- RR = Radio Resource
- BTSM = BTS Management

- DTAP = Direct Transfer Application Part
- BSSMAP = BSS Mobile Application Part
- MAP = Management Application Part
- SCCP = Signaling Connection Control Part (SS7)
- MTP = Message Transfer Part (SS7)
- TCAP = Transaction Capabilities Application Part (SS7)

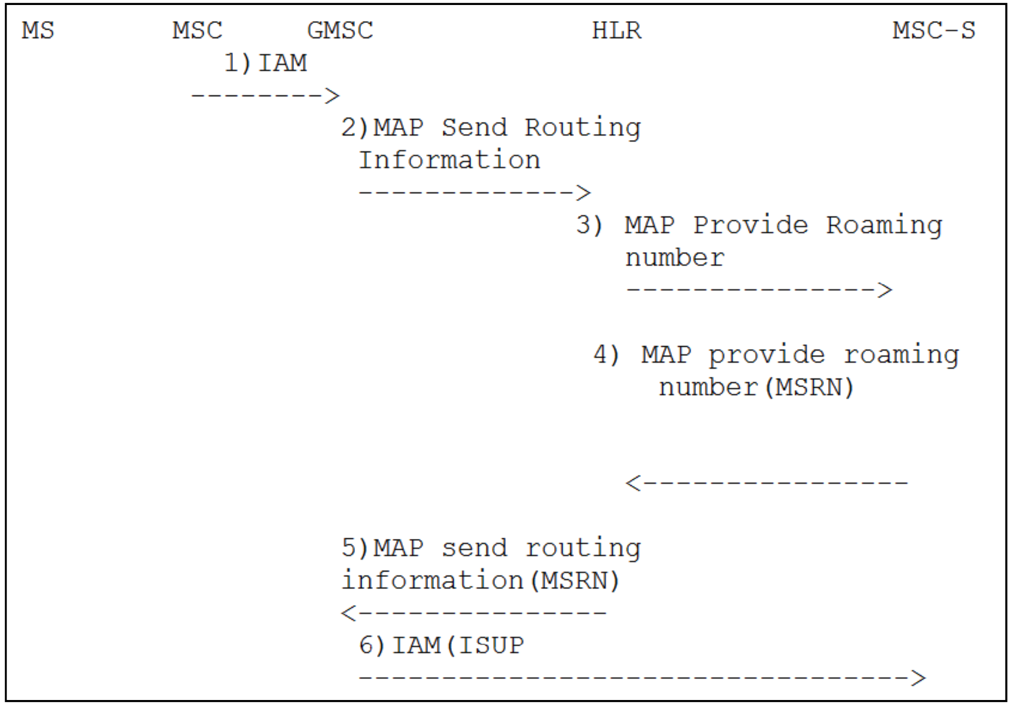
GSM protocol layers for signaling



Protocol Discriminator	Meaning	Function	Entities
RR	Radio Resource Management	- Paging management - Ciphering mode management - Frequency redefinition - Dedicated channel assignment - Handover management - Measurements and power control	MS - BSC (and BTS)
MM	Mobility Management	- Location Updating - Ciphering mode management - Frequency redefinition - Dedicated channel assignment	MS - MSC / VLR
CC	Call Control	- Call handling and routing - DTMF facilities	MS - MSC
SS	Supplementary Services	- Access to Supplementary Services	(+ HLR)
SMS	Short Message Service	- Short Message Service	(+ SMS-C)

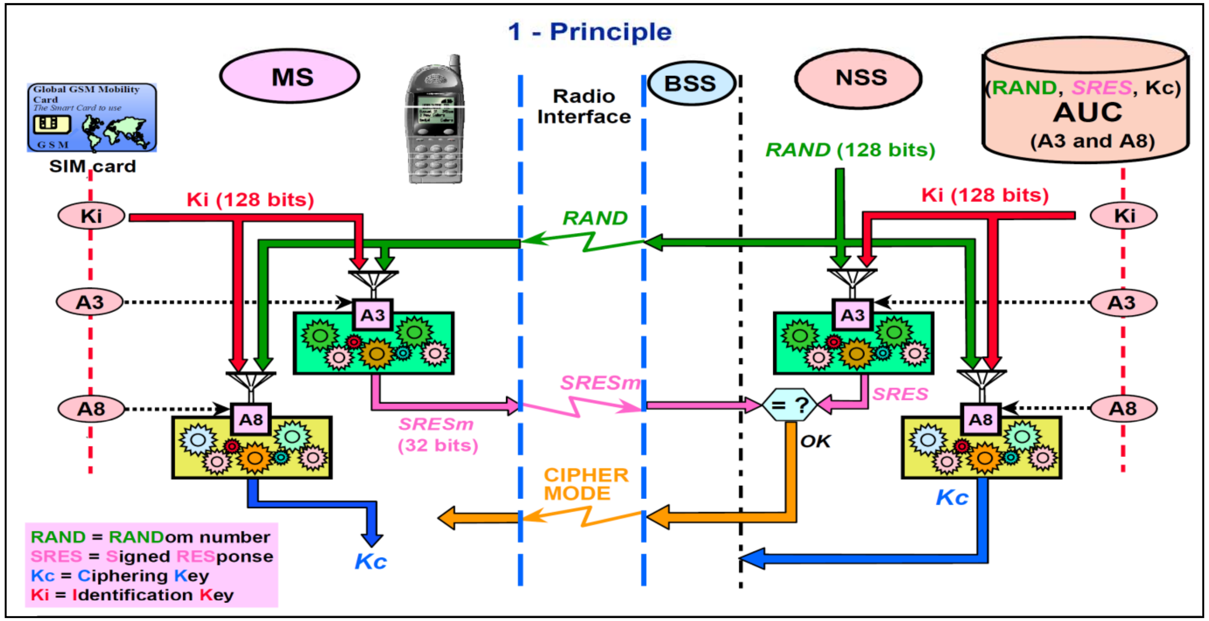
ISUP (IAM) & MAP (SRI) messages

- The MSC sends ISUP IAM to GMSC,
- GMSC analyses the dialled digits and figure out which HLR to query and sends "Send Routing Information".
- HLR always knows the exact location of mobile in the form of address of MSC/VLR.
- HLR sends "provide roaming number" asking MSRN(Mobile Station Routing Number).
- MSC-serving provides the MSRN in return message and HLR forwards it to GMSC which in turn sends IAM to MSC-S.



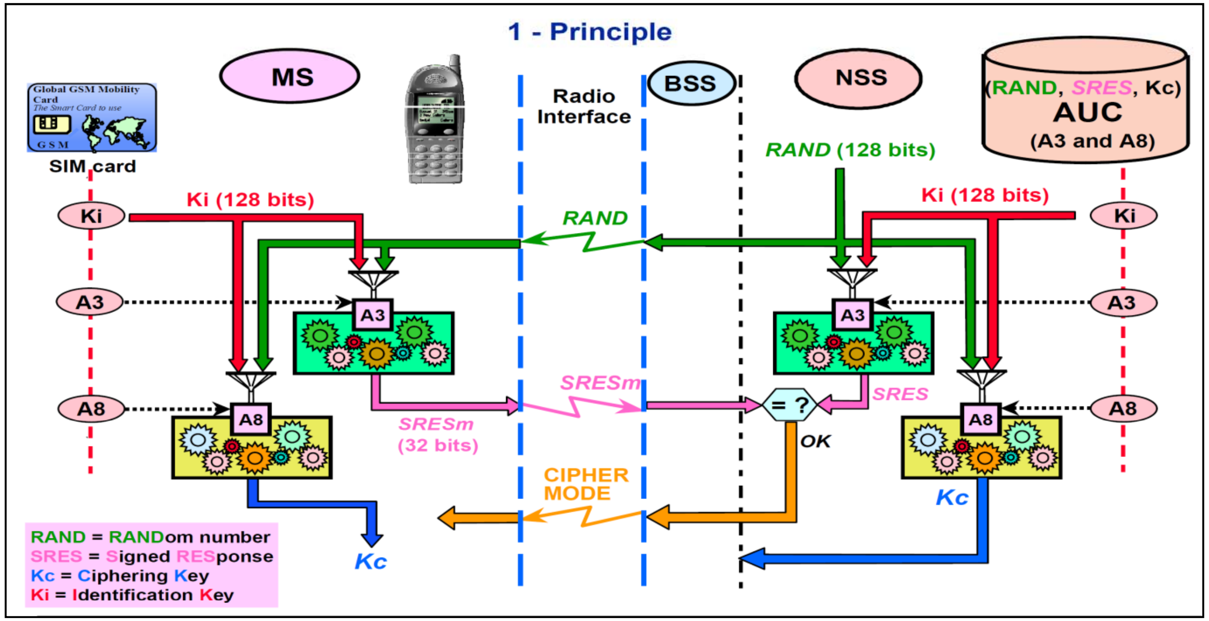
```
MS        MSC      GMSC                HLR                   MSC-S
              1)IAM
            -------->
                         2)MAP Send Routing
                          Information
                          ------------->
                                        3) MAP Provide Roaming
                                           number
                                           ---------------->

                                         4) MAP provide roaming
                                            number(MSRN)


                                           <-----------------

                         5)MAP send routing
                         information(MSRN)
                         <---------------
                          6)IAM(ISUP
                          ---------------------------------->
```

Authentication Purpose



- Authentication of the subscriber, to prevent access of unregistered users:
  - Authentication is performed by requiring from an algorithm A3 the correct answer to a random number input.
  - Eavesdropping recording of signaling is inefficient since there is never twice the same request.
  - **A3 algorithm is operator-dependent.**

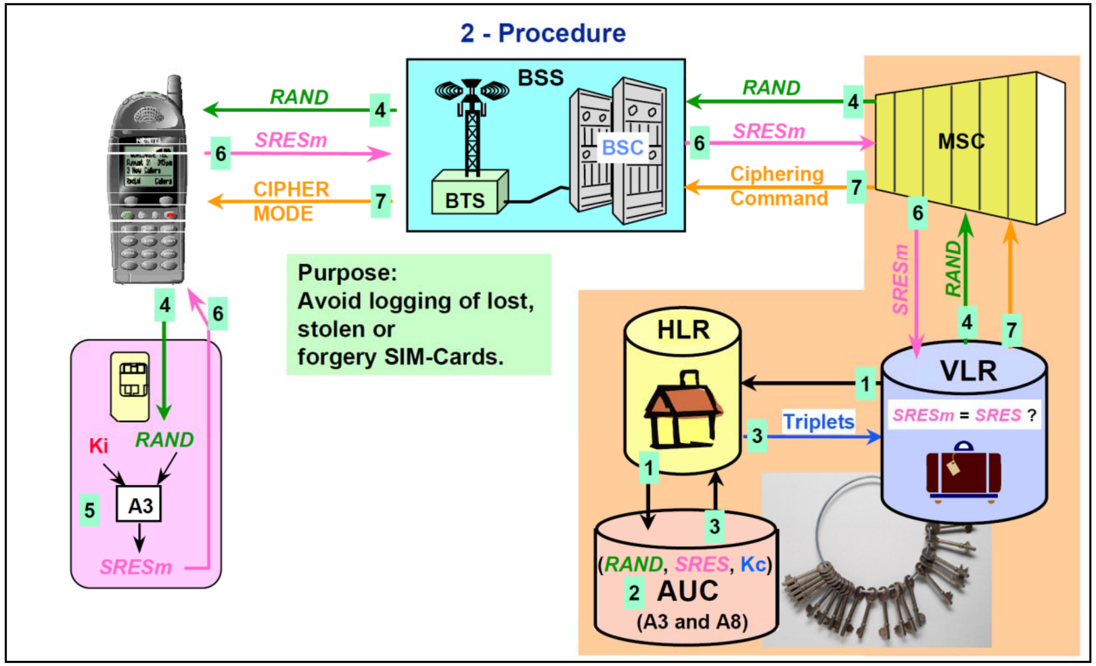
Authentication Principle



- The NSS transmits a non-predictable number RAND to the MS.
- The SIM card and the NSS compute the signature SRES, using algorithm A3, from the RAND and a secret key Ki.
- The MS transmits its signature SRESm to the NSS.
- The NSS tests the two SRES for validity.
- Each time authentication A3 algorithm runs, concurrently A8 algorithm is used to produce a ciphering key Kc.

Authentication Procedure

1. The VLR sends a MAP “Send Parameters” message to the HLR which relays this message to the AUC.
2. The AUC then generates some RAND numbers and applies algorithms A3 and A8 to provide the authenticated signature SRES and the cipher key Kc.
3. The AUC returns the triplets (RAND, SRES, Kc) to HLR which relays them to the VLR.



Purpose:
Avoid logging of lost, stolen or forgery SIM-Cards.

4. The VLR now sends a MAP “Authenticate” message to the MSC which in turn sends to the MS an AUTHENTICATION REQUEST message containing Rand; the Kc is also sent but stops at the BTS.
5. The SIM-Card calculates the required response SRESm, using RAND, algorithm A3 and authentication key Ki.
6. The MS returns SRESm to VLR in AUTHENTICATION RESPONSE.
7. VLR checks SRES = SRESm, then sends to the MSC a MM “Service accept” message; otherwise VLR denies access: the MS will receive an AUTHENTICATION REQUEST.

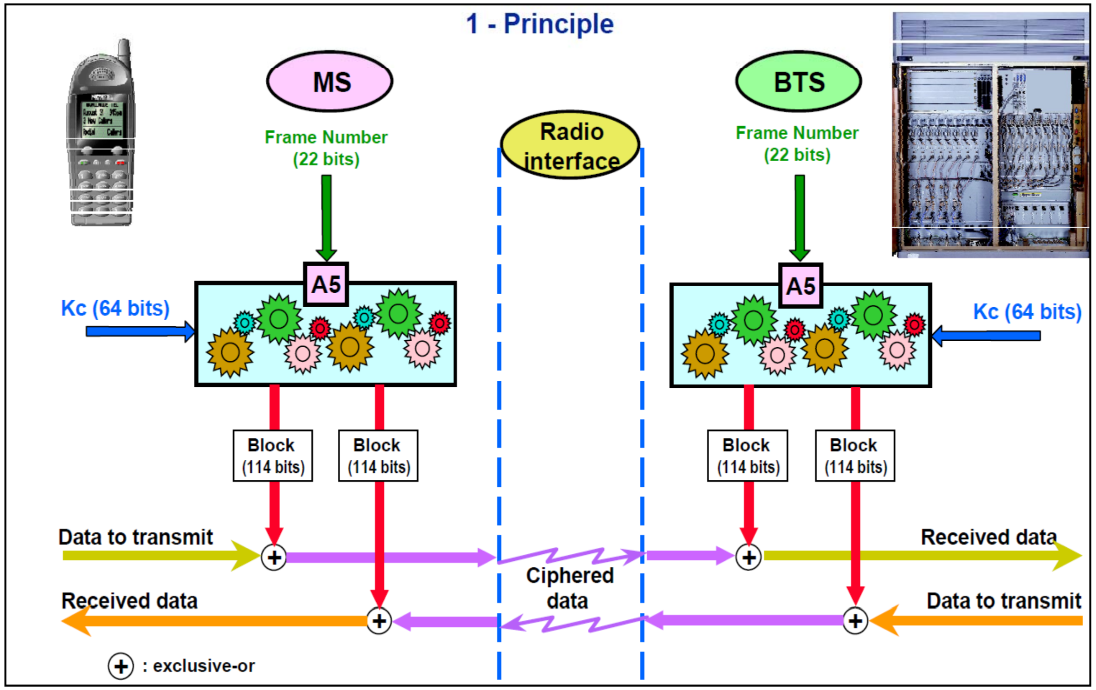
Ciphering
Principle

Radio path ciphering aims to prevent third party tapping (eavesdropping).

What is encrypted?:

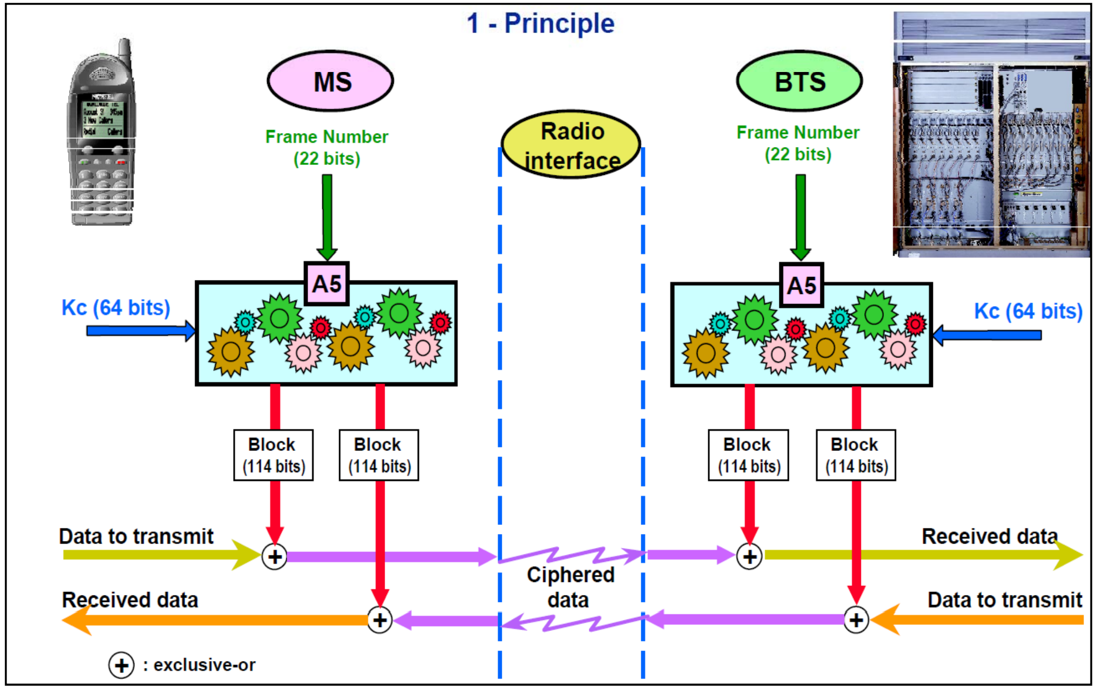
- Signaling (Subscriber Id.).
- Speech or data.

The encryption of signaling and user speech or data, is performed at the MS as well as at the BTS (symmetric encryption) using the same Kc and the A5 algorithm.



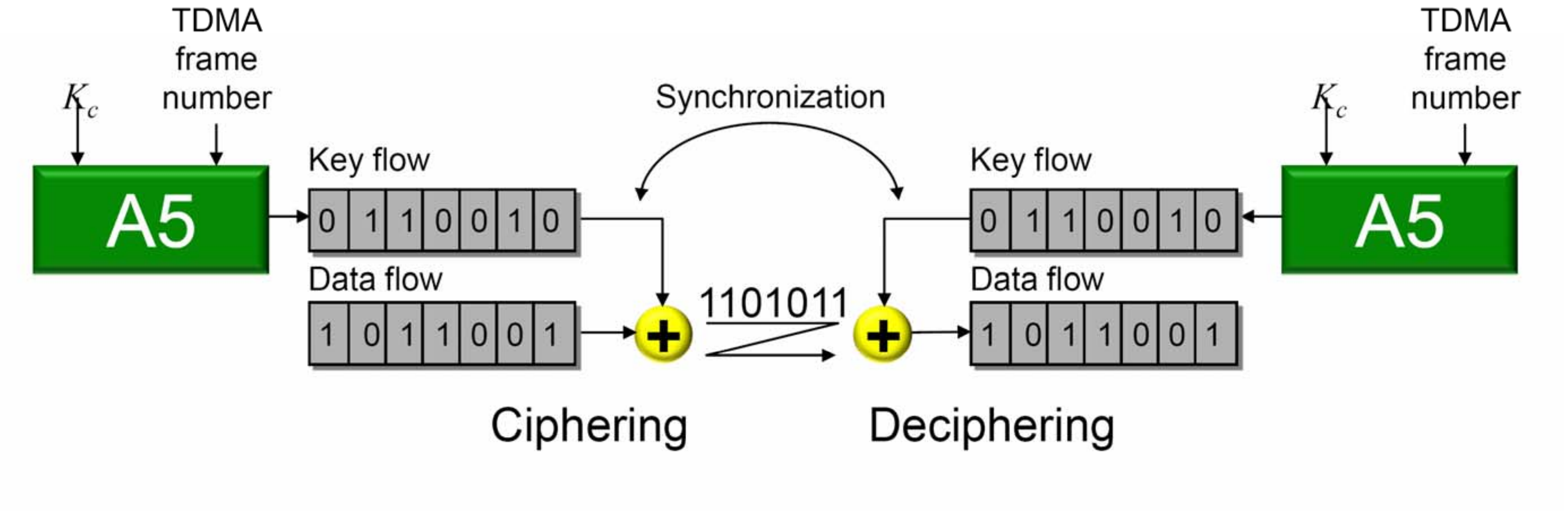
- Each time a Mobile Station is authenticated, this MS and the Network also compute the ciphering key Kc (algorithm A8) with the same inputs RAND and Ki as for the SRES (algorithm A3). The Frame Number FN of the current TDMA frame (within a hyperframe) is another input for the A5 besides the Kc.
- The output of Encryption algorithm A5 is a ciphering sequence of 114 bits. Exclusive OR operation is applied between data to be ciphered and the ciphering sequence in order to produce either ciphered or deciphered data.
- Algorithm A5 is not operator dependent to achieve international roaming between any
- Mobile Station and BSS infrastructure whatever the operator.Two types of ciphering

Ciphering
Principle



- Algorithm A5 is not operator dependent to achieve international roaming between any Mobile Station and BSS infrastructure whatever the operator.
- Three types of ciphering algorithms are available: A5/1, A5/2, and A5/3. But only one ciphering algorithm A5 is supported at a time in a BTS (for a certain call).
- The BSC checks the availability of the A5 algorithms in the MS. If the BSS does not support the same ciphering algorithm as the MS, the calls will be unencrypted.
- The ciphering BSS capability is an O&M parameter defined for all the BTS of the BSC.

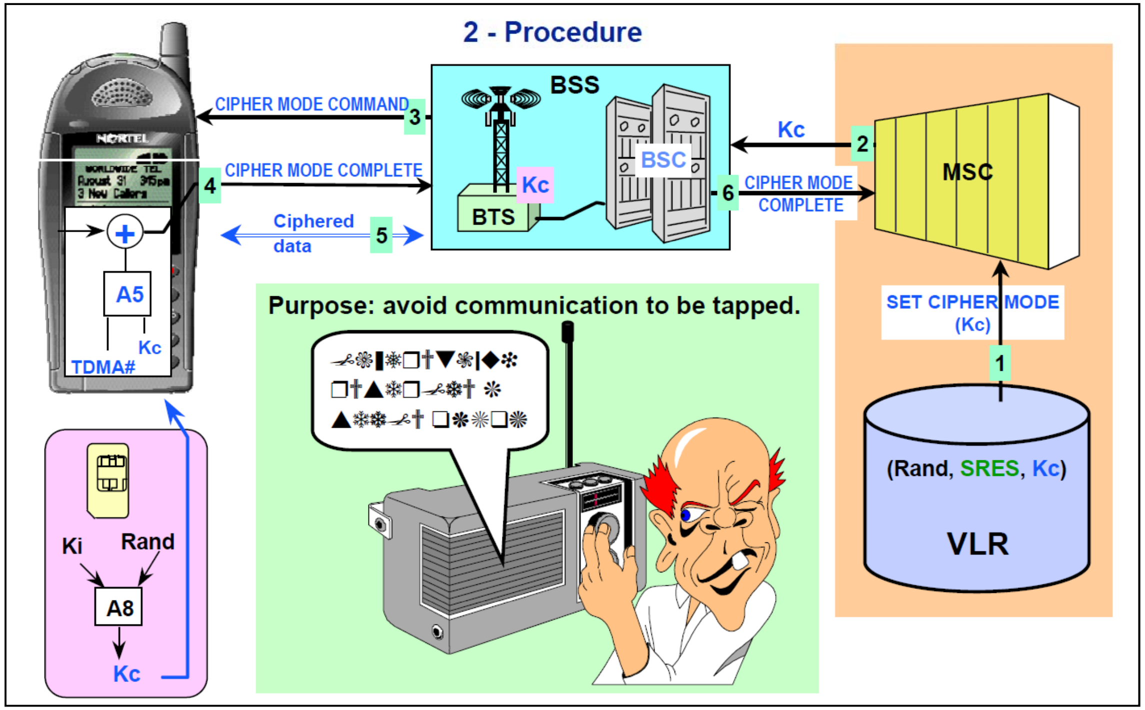
Ciphering
Principle



- **Stream Cipher**: Ciphering uses a bit stream which is added bitwise (EXCLUSIVE-OR) to the data to be ciphered
- Deciphering: EXCLUSIVE-OR operation on the enciphered data stream with the ciphering stream
- Synchronization between ciphering and deciphering is performed through the TDMA frame number
- TDMA frame number is related to the current TDMA frame within a hyperframe
- TDMA Frame number is broadcasted on the SCH and is thus available to all mobile stations currently in the cell

Ciphering
Procedure

1. Ciphering begins with the VLR sending the MSC a SET CIPHER MODE (MAP message) containing the value of Kc.
2. The MSC sends the ciphering key to the BSS (actually the BTS) in a CIPHER MODE COMMAND (BSSMAP message).
3. The BSS in turn sends an CIPHERING MODE COMMAND (RR message) to the MS.

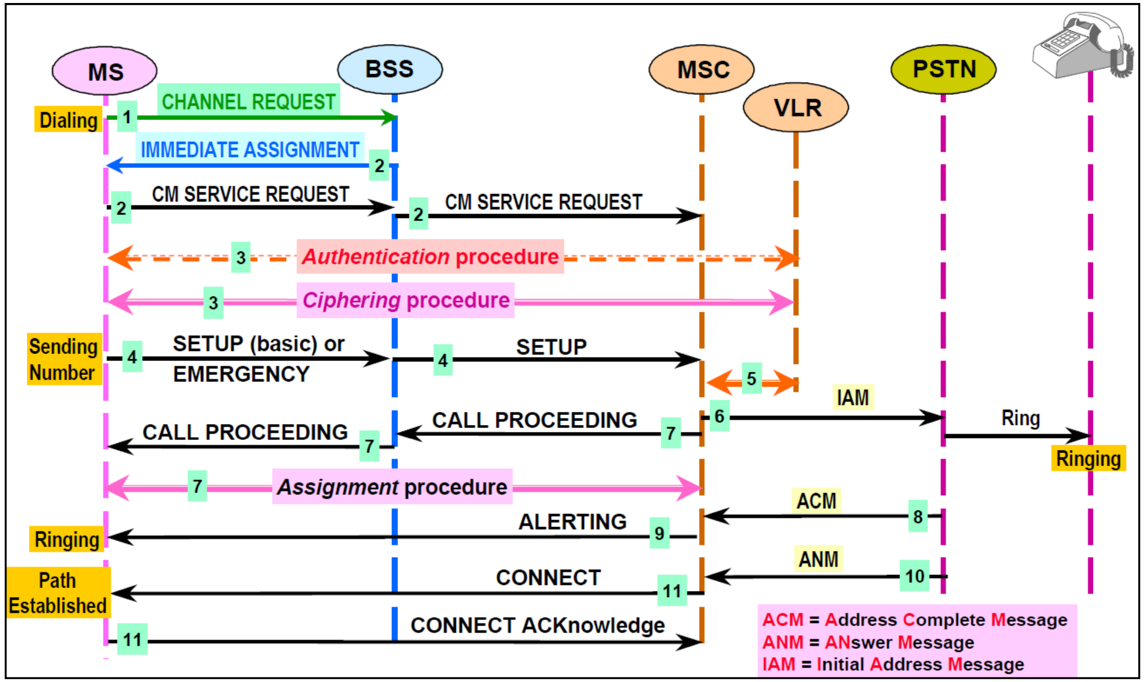


4. The MS switches to encrypted transmission and reception, then sends back to BSS an CIPHERING MODE COMPLETE (RR message).
5. After the BSS receives this message, it switches to encrypted transmission and reception for subsequent burst.
6. The BSS then sends a CIPHER MODE COMPLETE (BSSMAP message) to the MSC.

Ciphering is normally required for all user transactions over the RF link when the subscriber has been authenticated by the system. It is worth noting that this is an optional feature and it is dependent of the operator.

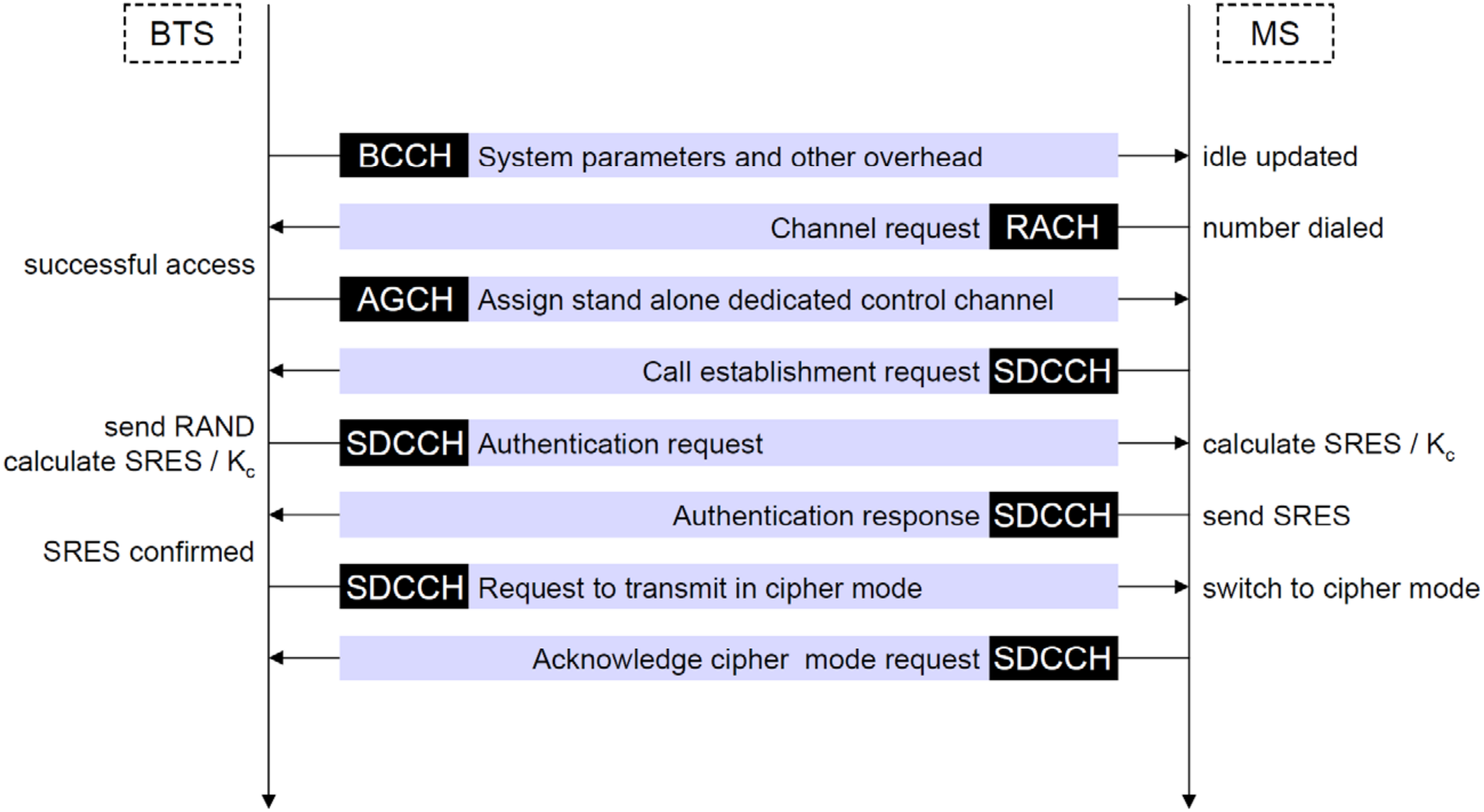
Mobile Originating Call

1. The MS originates the call by sending a CHANNEL REQUEST message (on RACH).
2. Immediate assignment: channel allocation with TCH / FACCH or SDCCH.
3. The VLR launches authentication (if required) and completes ciphering.
4. The MS initiates call establishment by sending a SETUP message (called party number) to the MSC.
5. The MSC in turn checks mobile subscriber capabilities with VLR for desired service.

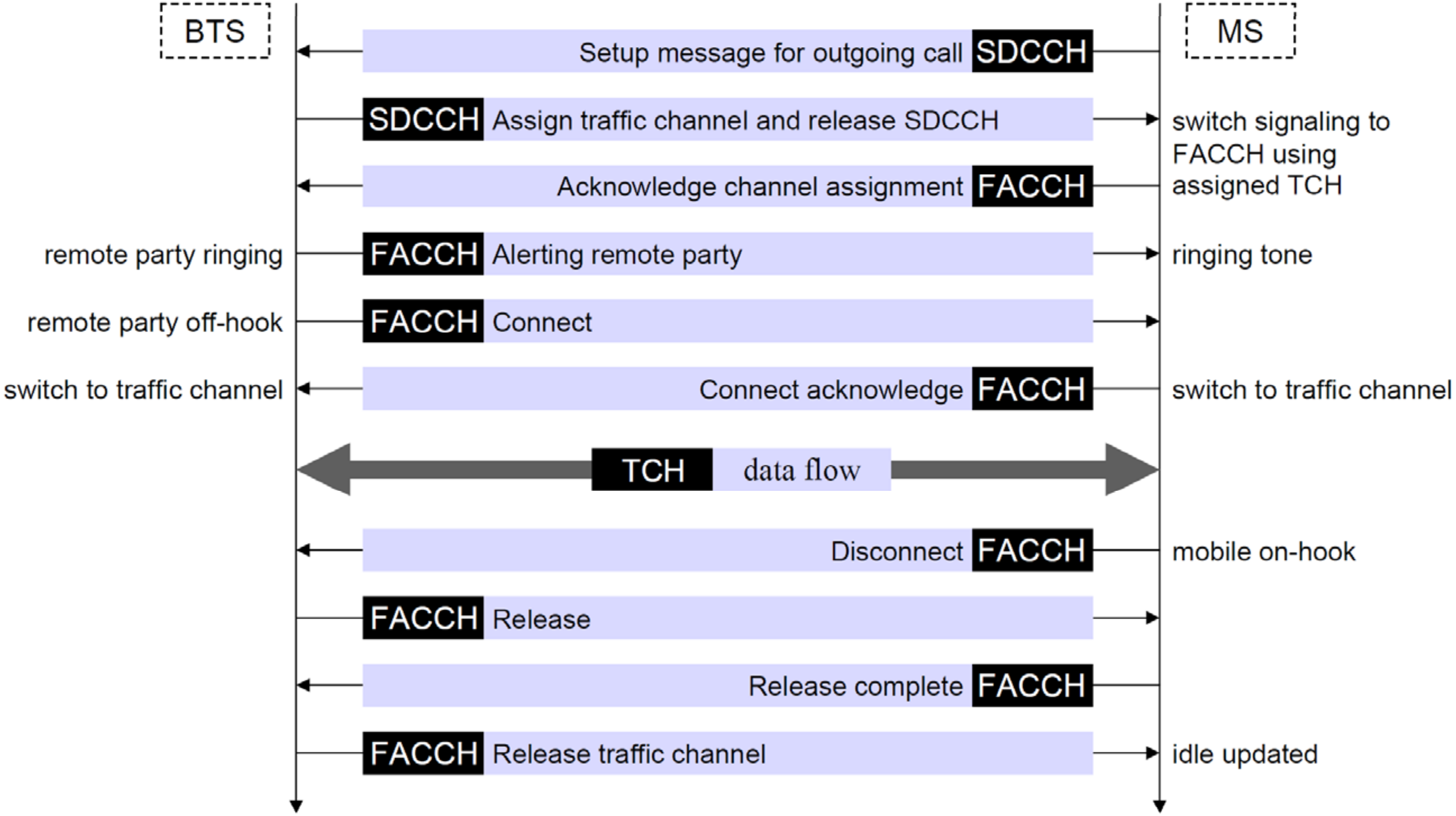


6. If it agrees, the MSC relays the called number over an ISUP Initial Address Message.
7. The MSC also sends a CALL PROCEEDING message to the MS (assigning TCH / FACCH EA in case of Early Assignment).
8. Recipient PSTN switch rings the land telephone and returns an ISUP Address Complete Message to the MSC.
9. Upon receiving this message, the MSC alerts the MS with an ALERTING message.
10. Called party goes off hook, thus PSTN sends to the MSC an ISUP ANswer Message. MSC then connects MS (assigning a TCH in case of OACSU).
11. Call is accepted (CONNECT/CONNECT ACK) and the conversation starts.

Mobile Originating Call
Channel activity at radio interface

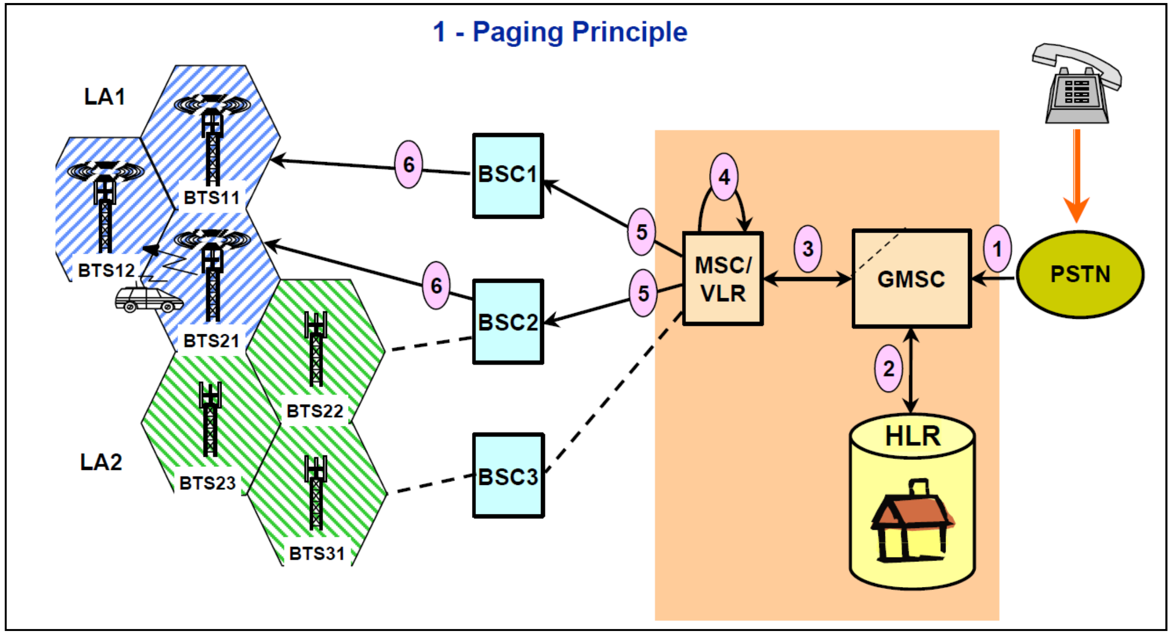


Mobile Originating Call
Channel activity at radio interface


BTS
MS
Setup message for outgoing call SDCCH
SDCCH Assign traffic channel and release SDCCH
switch signaling to FACCH using assigned TCH
Acknowledge channel assignment FACCH
remote party ringing
FACCH Alerting remote party
ringing tone
remote party off-hook
FACCH Connect
switch to traffic channel
Connect acknowledge FACCH
switch to traffic channel
TCH data flow
Disconnect FACCH
mobile on-hook
FACCH Release
Release complete FACCH
FACCH Release traffic channel
idle updated

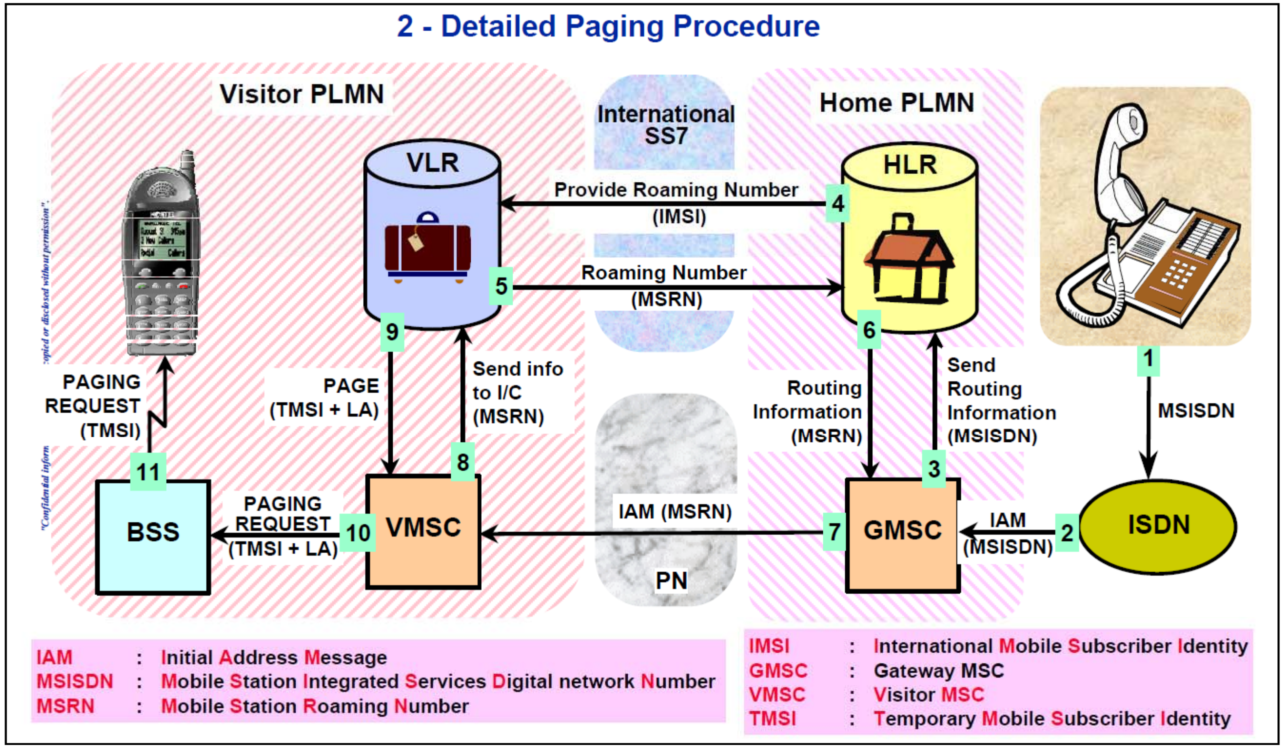
Mobile Terminated Call
Paging principle

- Main difference with MO Call procedure is the Paging of the Mobile Station.
- When the MS is in Idle mode, the network do not knows the cell but only the Location Area where the MS is located.
- Since RR sessions are only established at the initiative of the MS, the role of the Paging procedure is to trigger that operation.



1. A call from the fixed network (PSTN) is switched to the Gateway MSC (GMSC).
2. The GMSC reads in the HLR the identity of the MSC/VLR (or Visitor MSC) handling the Location Area of the Mobile Station.
3. The GMSC routes the call to the VMSC.
4. The VMSC reads the LA where the MS is located, into its VLR.
5. The VMSC sends instructions to one or several BSC (BSC1 and BSC2) to page the MS in the different cells of LA1.
6. BSC1 and BSC2 page the MS in the BTSs of the Location Area LA1. (BTS11, BTS12, BTS21).

Mobile Terminated Call
Paging procedure



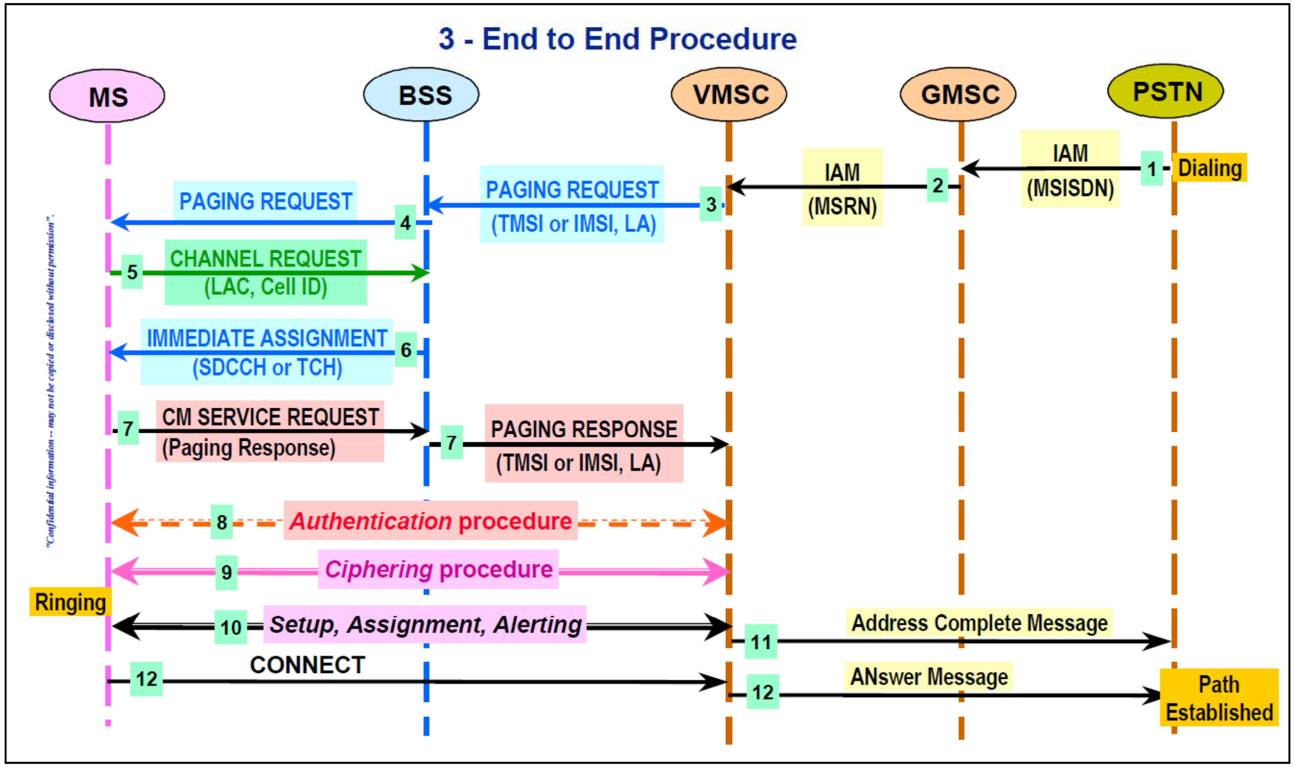
2 - Detailed Paging Procedure

IAM	:	Initial Address Message
MSISDN	:	Mobile Station Integrated Services Digital network Number
MSRN	:	Mobile Station Roaming Number

IMSI	:	International Mobile Subscriber Identity
GMSC	:	Gateway MSC
VMSC	:	Visitor MSC
TMSI	:	Temporary Mobile Subscriber Identity

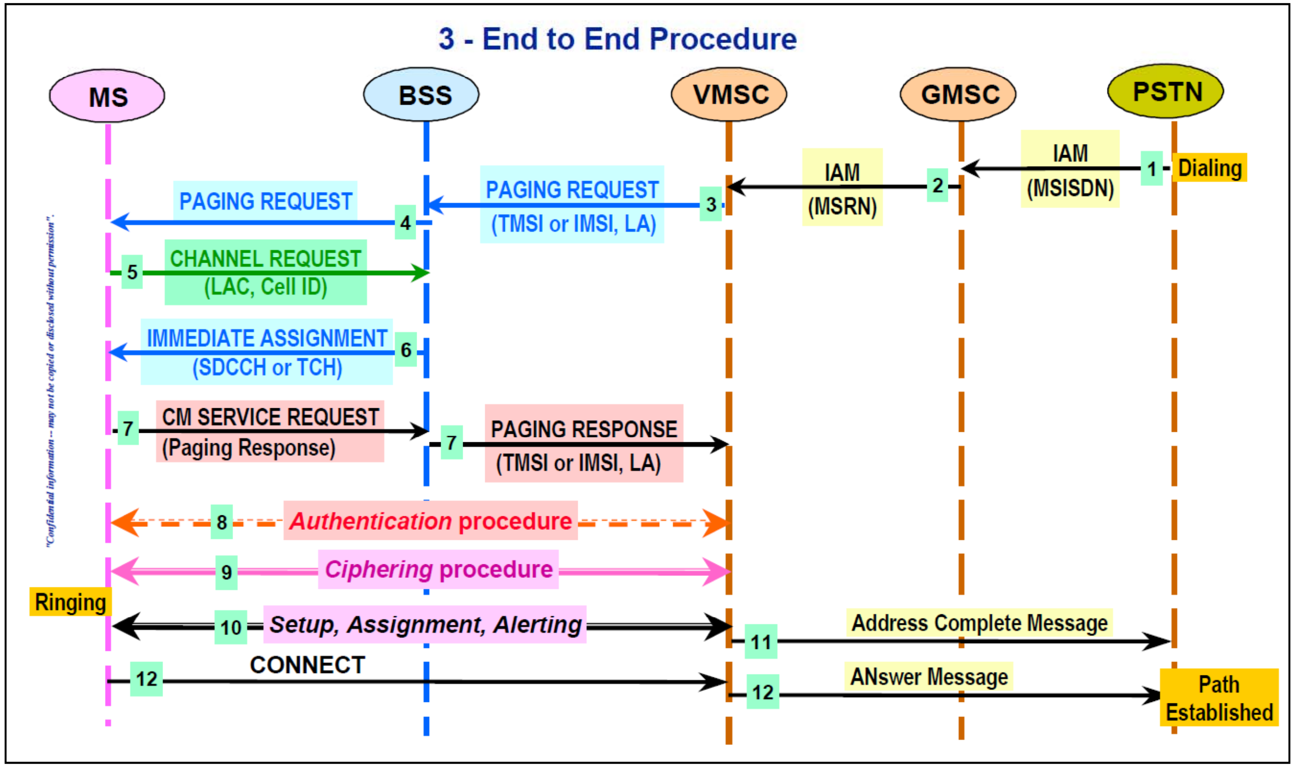
1. The caller subscriber access the ISDN by dialing the called MS-ISDN number.
2. Transmission of MS-ISDN number to GMSC through IAM (Initial Address Message).
3. Transmission of MS-ISDN number to HLR through SRI (Send Routing Information).
4. The HLR interrogates the VLR (Visitor MSC) that is currently serving the user.
5. The VLR returns a routing number (MSRN) to the HLR, which passes it back to the GMSC.
6. The MSRN is transmitted to GMSC (address of appropriate VMSC).

Mobile Terminated Call
End to End procedure



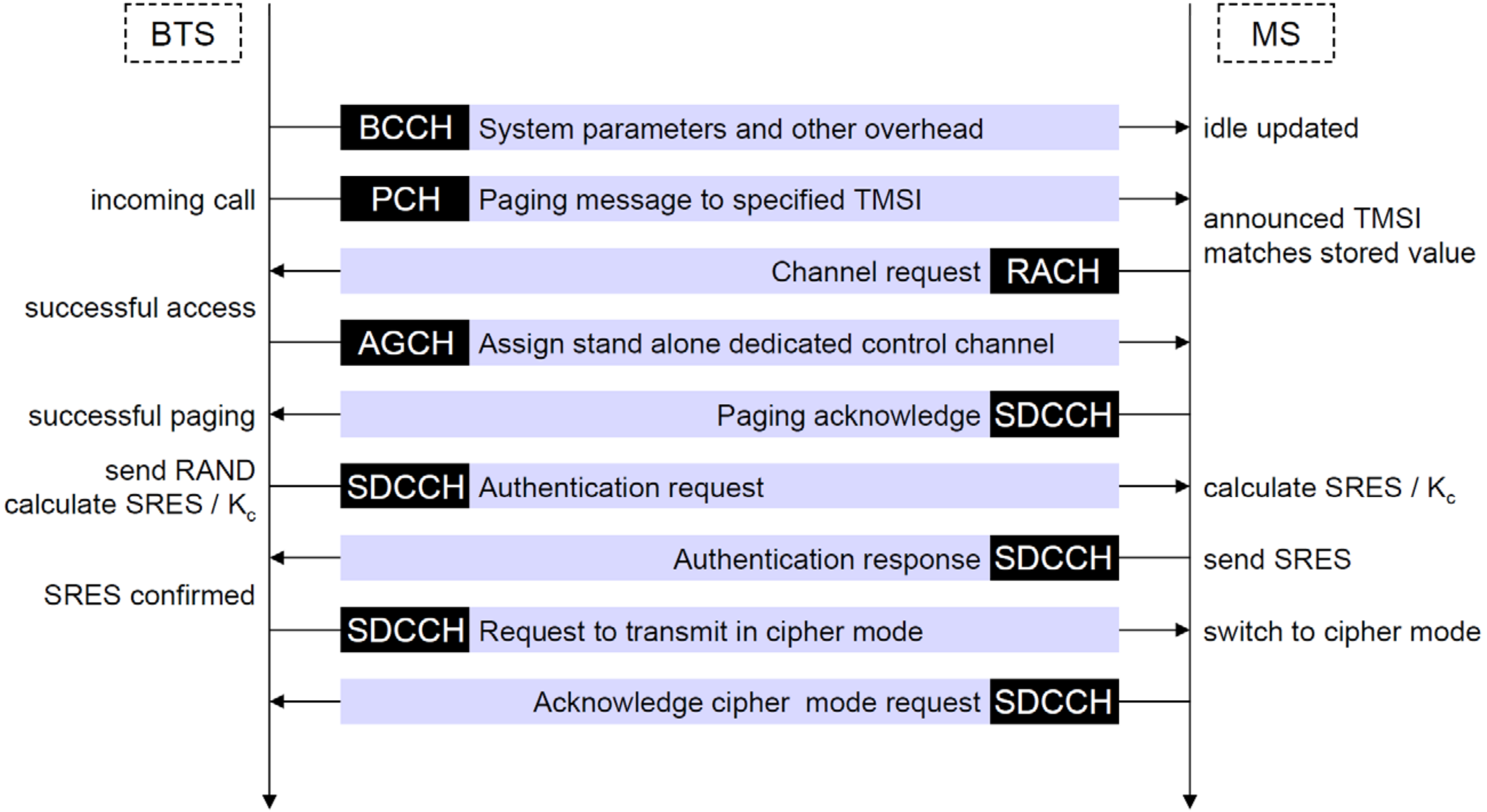
1. PSTN sends an IAM (with the MSISDN) to the GMSC.
2. GMSC sends an IAM (with the MSRN) to the VMSC.
3. The VMSC sends a PAGING REQUEST MM message to the BSS.
4. The BSS sends a PAGING REQUEST (with IMSI or TMSI) to the MS.
5. The MS must request a channel (CHANNEL REQUEST message with paging cause) over the RACH.
6. The BSS complies and assigns (on AGCH) a dedicated channel to the MS with IMMEDIATE ASSIGNMENT message.

Mobile Terminated Call
End to End procedure



7. The MS sends a PAGING RESPONSE to the VMSC via the BSS.
8. Authentication procedure (if required).
9. Ciphering procedure (if required).
10. Setup, Assignment, Alerting procedures (see MS Originating Call).
11. Alerting is sent to PSTN with an ACM (ISUP message).
12. CONNECT and ANM messages are sent to the PSTN: call is completed.

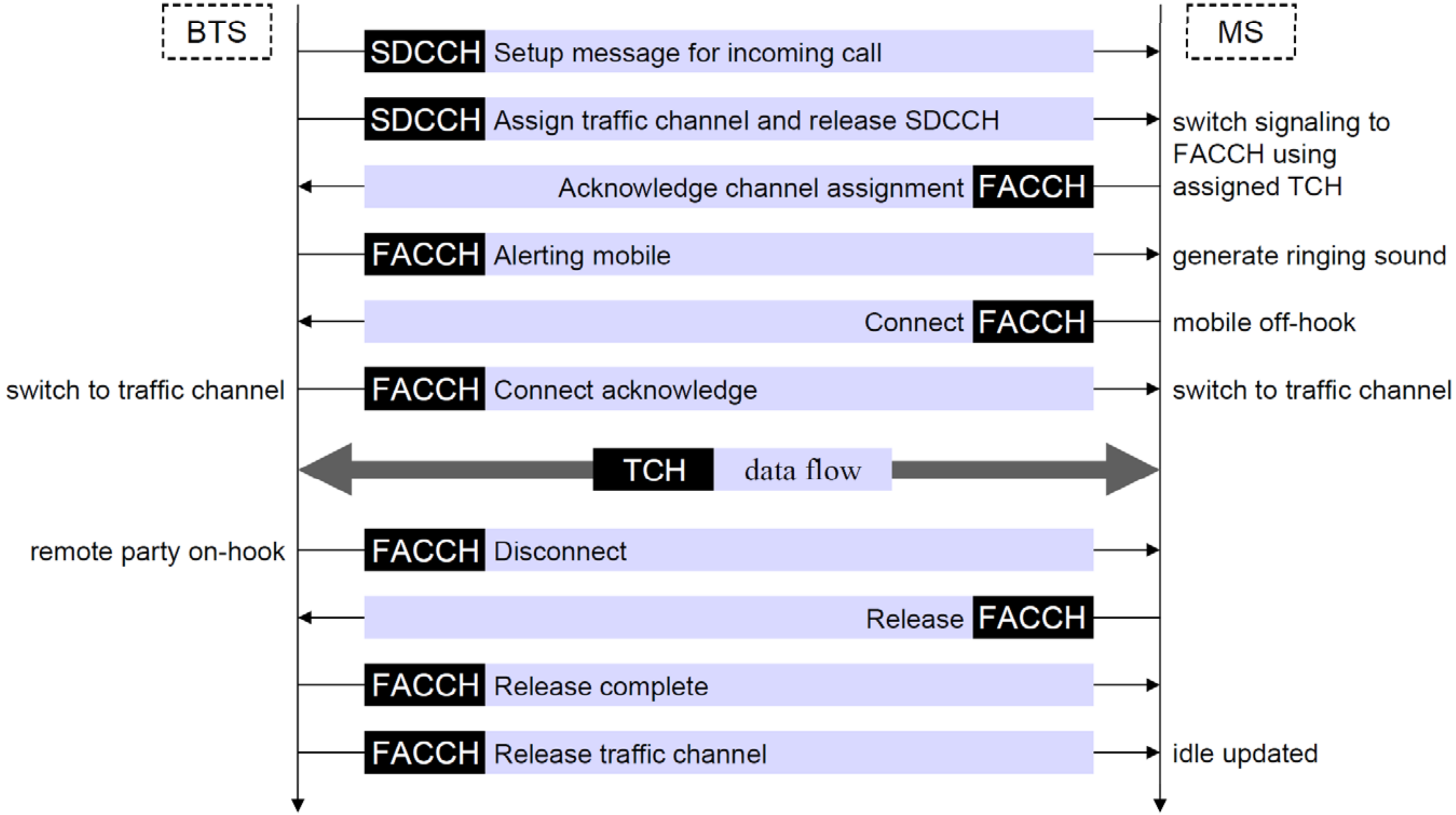
Mobile Terminated Call
Channel activity at radio interface



BTS
MS
BCCH System parameters and other overhead
idle updated
incoming call
PCH Paging message to specified TMSI
announced TMSI matches stored value
Channel request RACH
successful access
AGCH Assign stand alone dedicated control channel
successful paging
Paging acknowledge SDCCH
send RAND
calculate SRES / K_c
SDCCH Authentication request
calculate SRES / K_c
Authentication response SDCCH
send SRES
SRES confirmed
SDCCH Request to transmit in cipher mode
switch to cipher mode
Acknowledge cipher mode request SDCCH

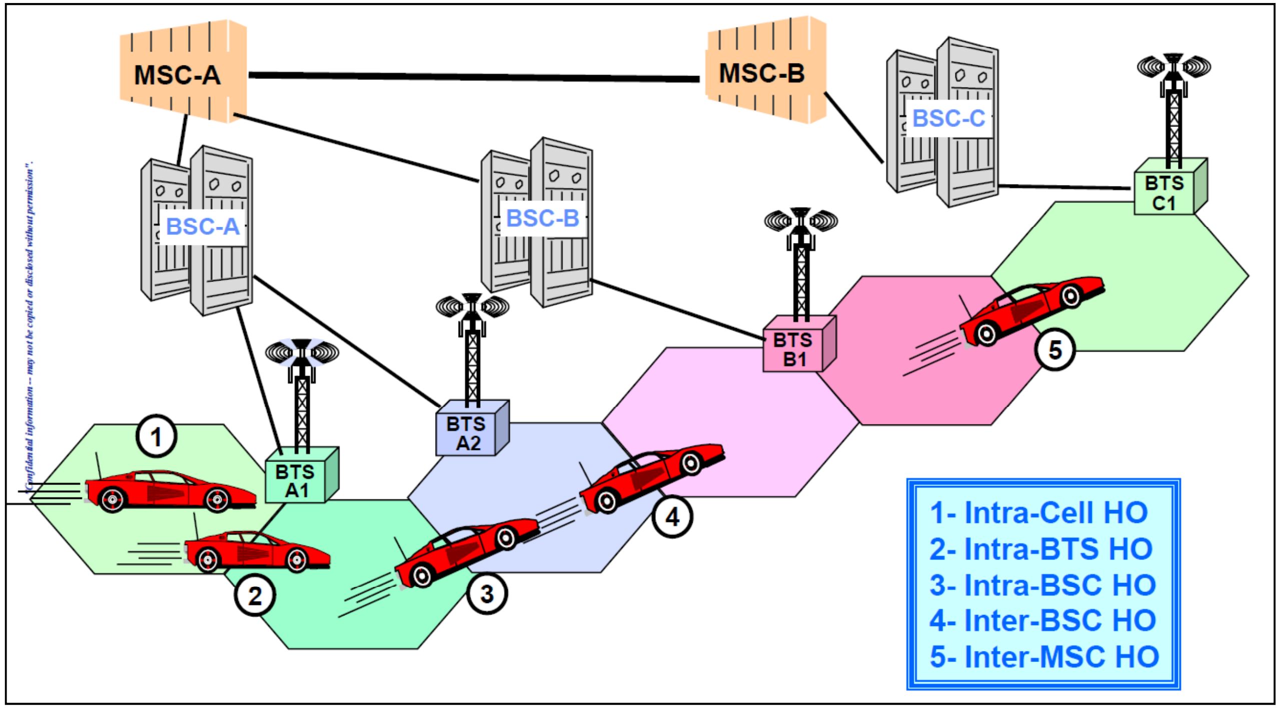
Mobile Terminated Call

Channel activity at radio interface


BTS
MS
SDCCH Setup message for incoming call
SDCCH Assign traffic channel and release SDCCH
switch signaling to FACCH using assigned TCH
Acknowledge channel assignment FACCH
FACCH Alerting mobile
generate ringing sound
Connect FACCH
mobile off-hook
switch to traffic channel
FACCH Connect acknowledge
switch to traffic channel
TCH data flow
remote party on-hook
FACCH Disconnect
Release FACCH
FACCH Release complete
FACCH Release traffic channel
idle updated

Handover types

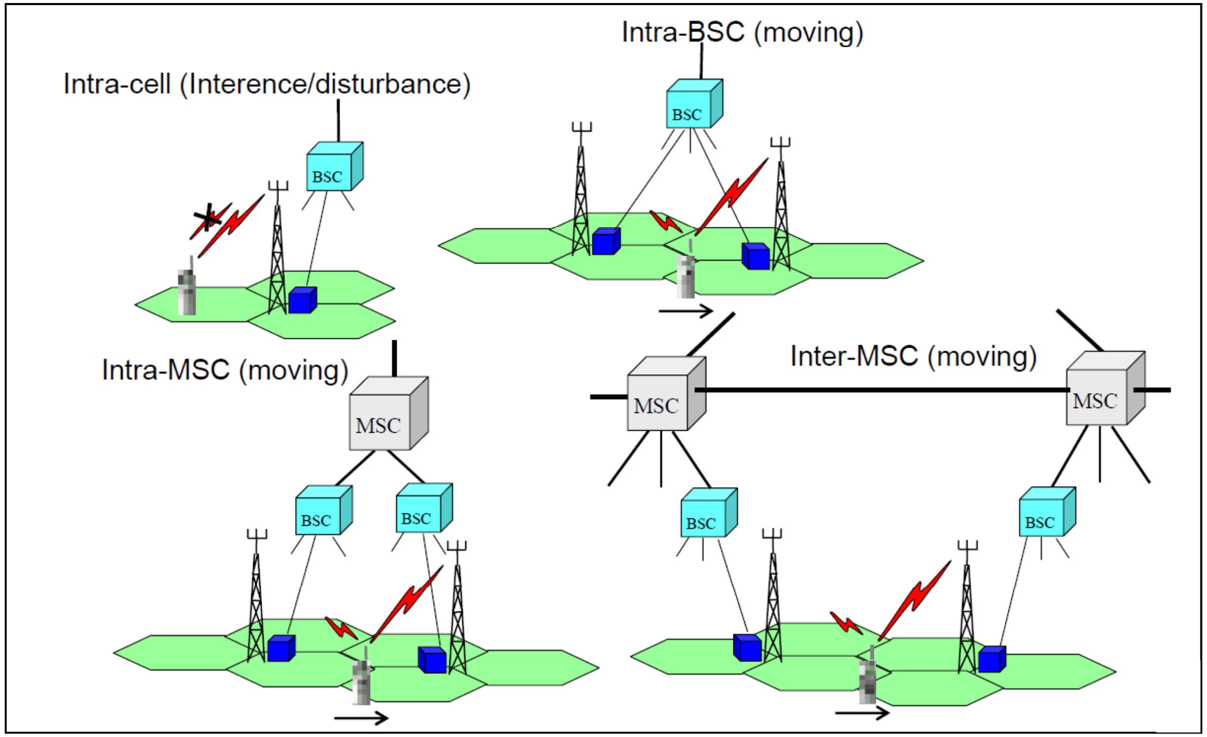
1. Intra-Cell Handover: MS is handed over to another channel on the same cell, under the same BTS.
2. Intra-BTS Handover: MS is handed over to another channel on a different cell, under the control of the same BTS.



3. Intra-BSC Handover: MS is handed over to another channel on a different cell, under the control of a different BTS of the same BSC.
4. Inter-BSC Handover: the MS is handed over to another channel on a different cell, under the control of a different BSC of the same MSC.
5. Inter-MSC Handover: the MS is handed over to another channel on different cell, under another MSC of the same PLMN.

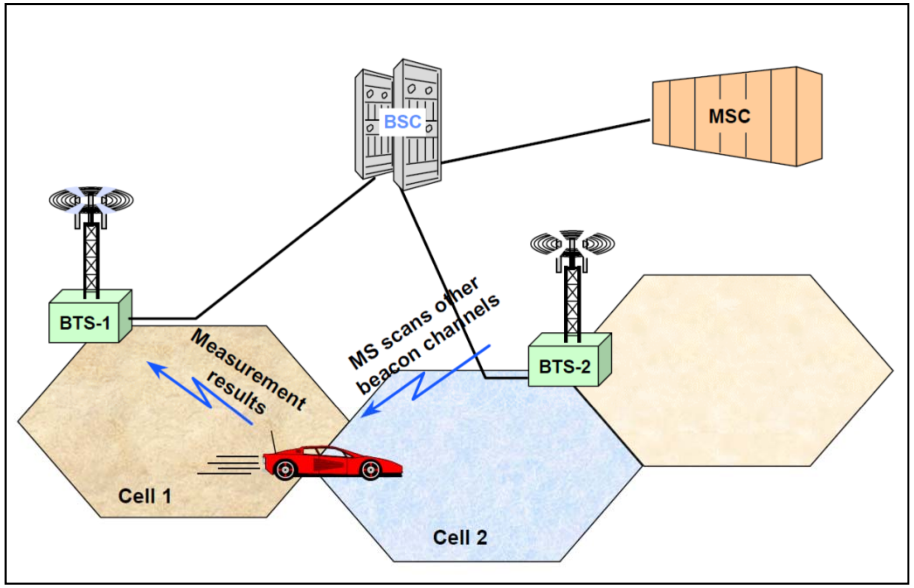
Handover types

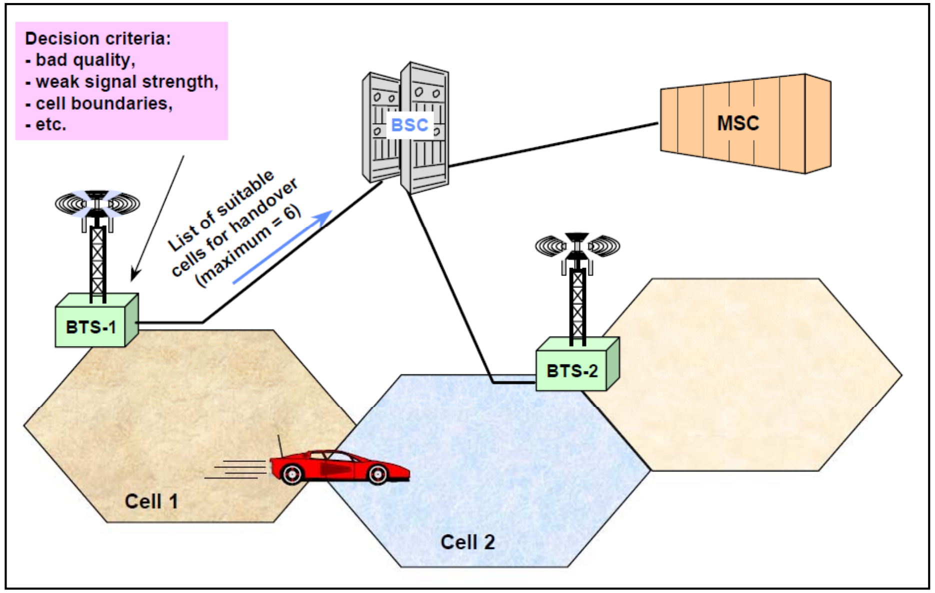
1. Intra-Cell Handover: MS is handed over to another channel on the same cell, under the same BTS.
2. Intra-BTS Handover: MS is handed over to another channel on a different cell, under the control of the same BTS.



3. Intra-BSC Handover: MS is handed over to another channel on a different cell, under the control of a different BTS of the same BSC.
4. Inter-BSC Handover: the MS is handed over to another channel on a different cell, under the control of a different BSC of the same MSC.
5. Inter-MSC Handover: the MS is handed over to another channel on different cell, under another MSC of the same PLMN.

Handover preparation




Decision criteria:
- bad quality,
- weak signal strength,
- cell boundaries,
- etc.

Procedure: Three steps:

- Handover decision (based on measurements results).
- Choice of the target cell.
- Handover execution.

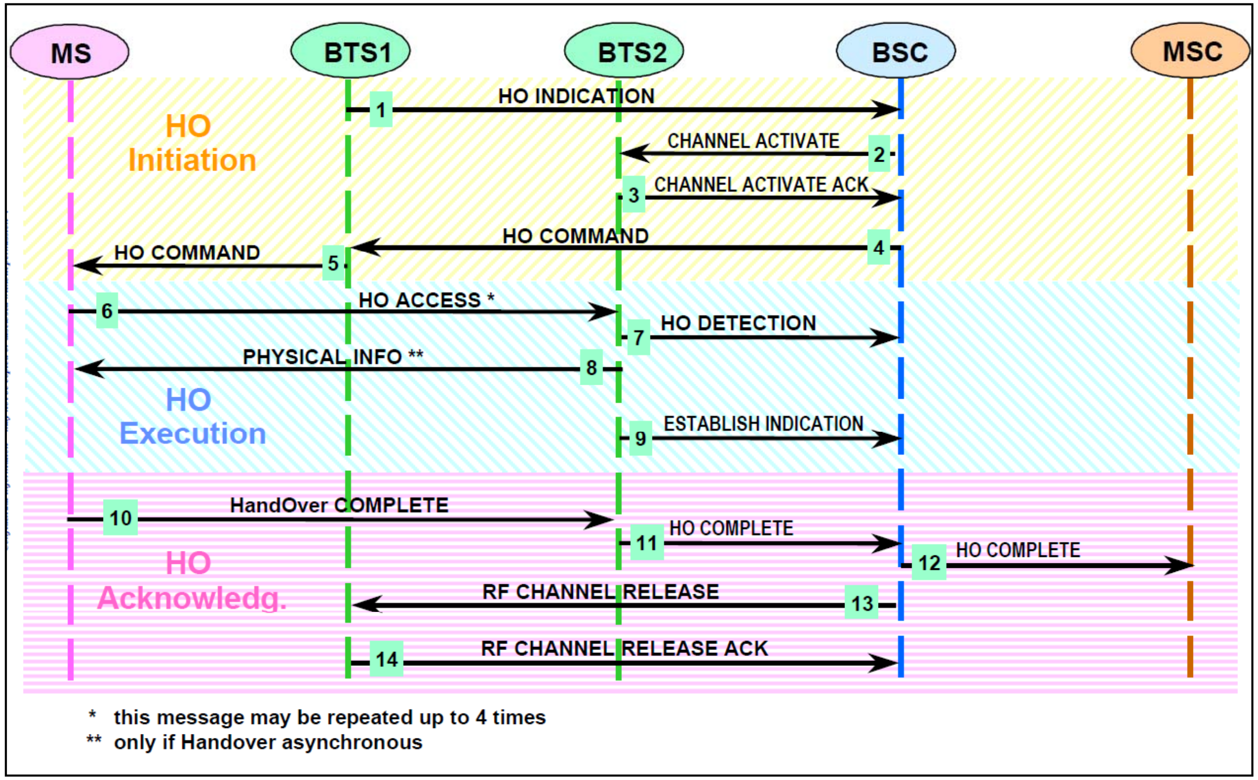
Handover topology

- Intra BTS (intra and inter cell).
- Inter BSC.
- Inter MSC including
- . . .

- Handover is initiated by the network based on radio subsystem criteria (RF level, quality, distance) as well as network directed criteria (current traffic loading per cell, maintenance requests, etc.).
- In order to determine if a handover is required, due to RF criteria, the MS takes radio measurements from neighboring cells; these measurements are reported to the serving cell on a regular basis.

Intra-BSC Handover

1. The BTS1 triggers HandOver by sending a HandOver INDICATION message to the BSC.
2. The BSC allocates if available a new channel from the BTS2.
3. The BTS2 establishes this channel, and responds to the BSC.

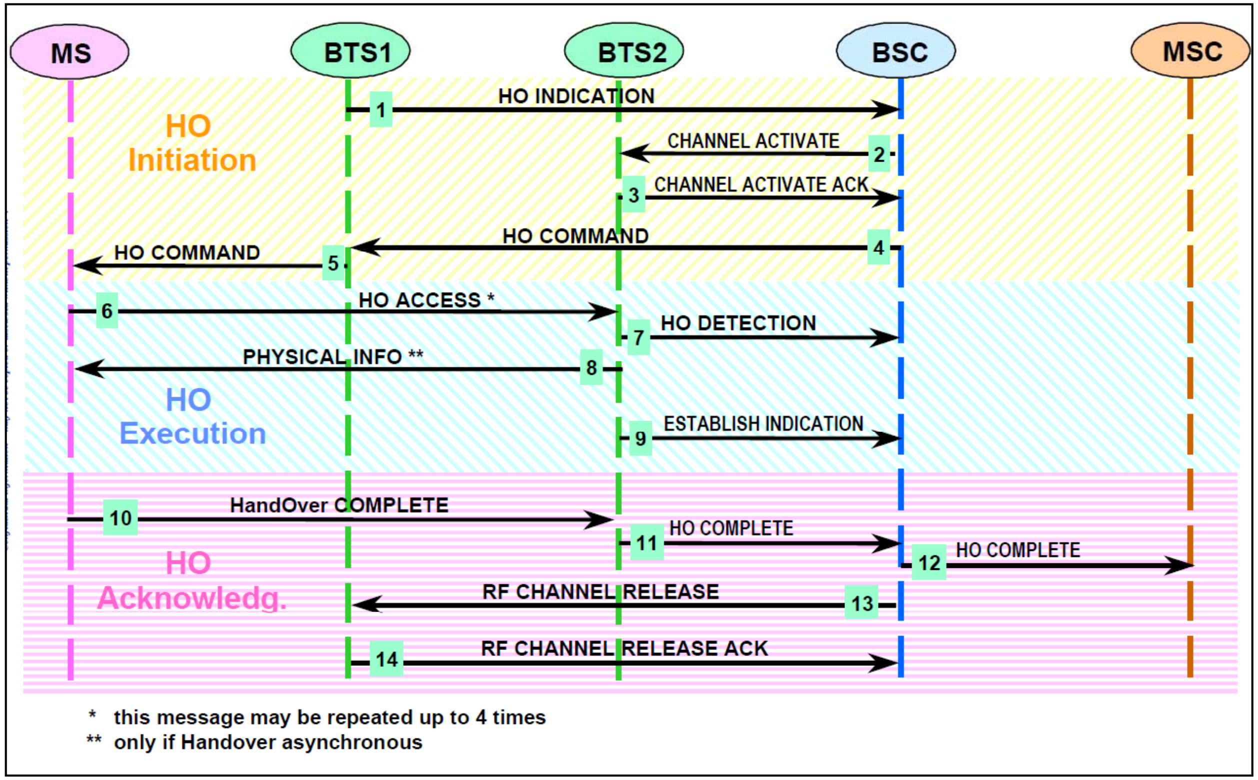


* this message may be repeated up to 4 times
** only if Handover asynchronous

4. 4/5- The BSC sends a HandOver COMMAND to the MS (on the FACCH) via the BTS1, assigning a new channel, its characteristics, the power level to use, the frequency hopping set, the Timing Advance TA if possible, and and whether to use synchronous or asynchronous HO.

Intra-BSC Handover

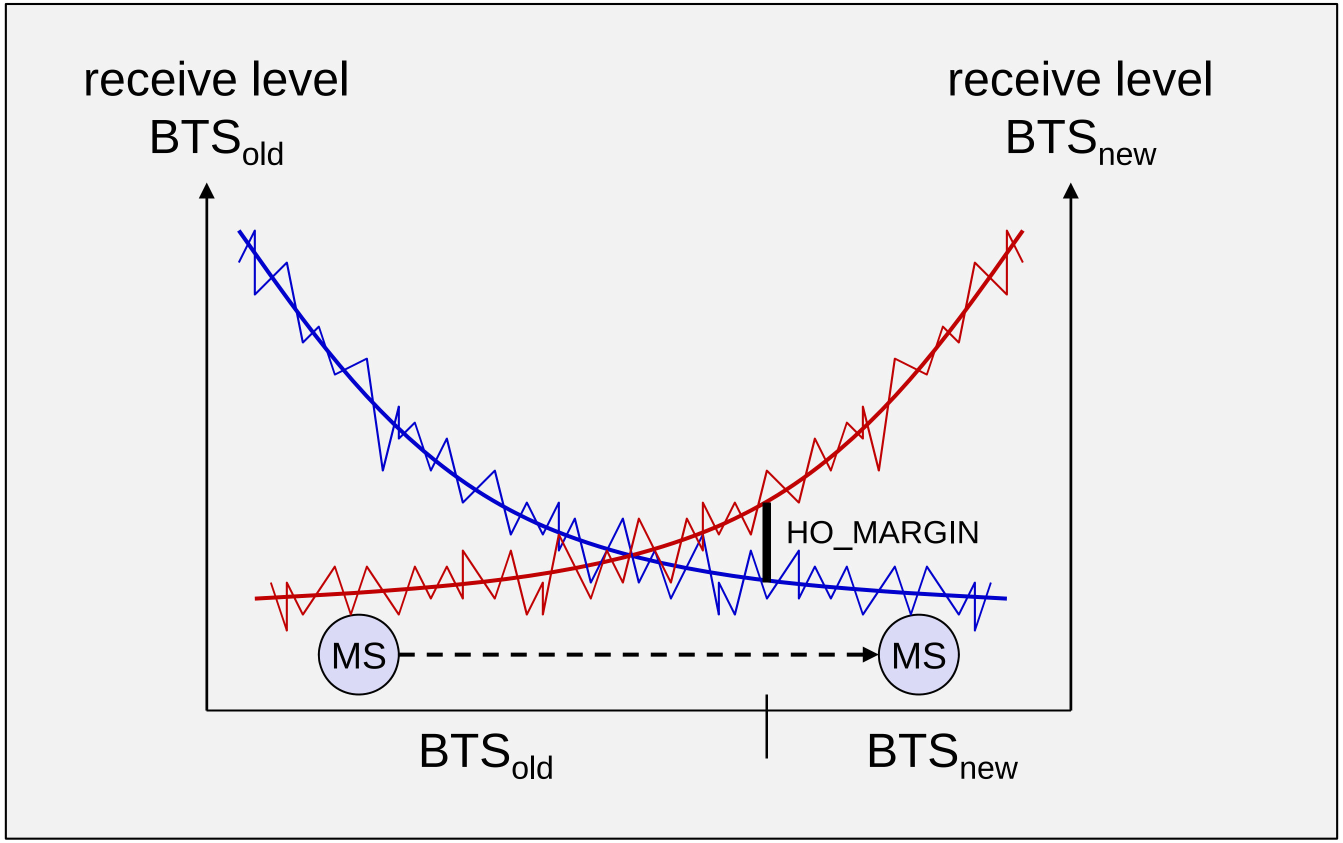
- 6a- In synchronous mode, MS sends to the BTS2 in successive multiframe slots (on the FACCH) four HandOver ACCESS messages. It then activates the new channel in both directions.
- 6b- In asynchronous mode, MS starts sending to the BTS2 a continuous stream of HandOver ACCESS messages, by sending access bursts on TCH until it receives the TA to apply.



* this message may be repeated up to 4 times
** only if Handover asynchronous

- 8- In asynchronous mode, MS receives the TA.
- 10/11- In both cases, MS replies with a HandOver COMPLETE message to the BSC over the new FACCH.
- 13/14- BSC in turn directs BTS1 to release the previous channel by sending a RF CHANNEL RELEASE message with ACKnowledgment from the BTS1.

Handover decision


receive level BTS$_{old}$
receive level BTS$_{new}$
HO_MARGIN
MS
MS
BTS$_{old}$
BTS$_{new}$