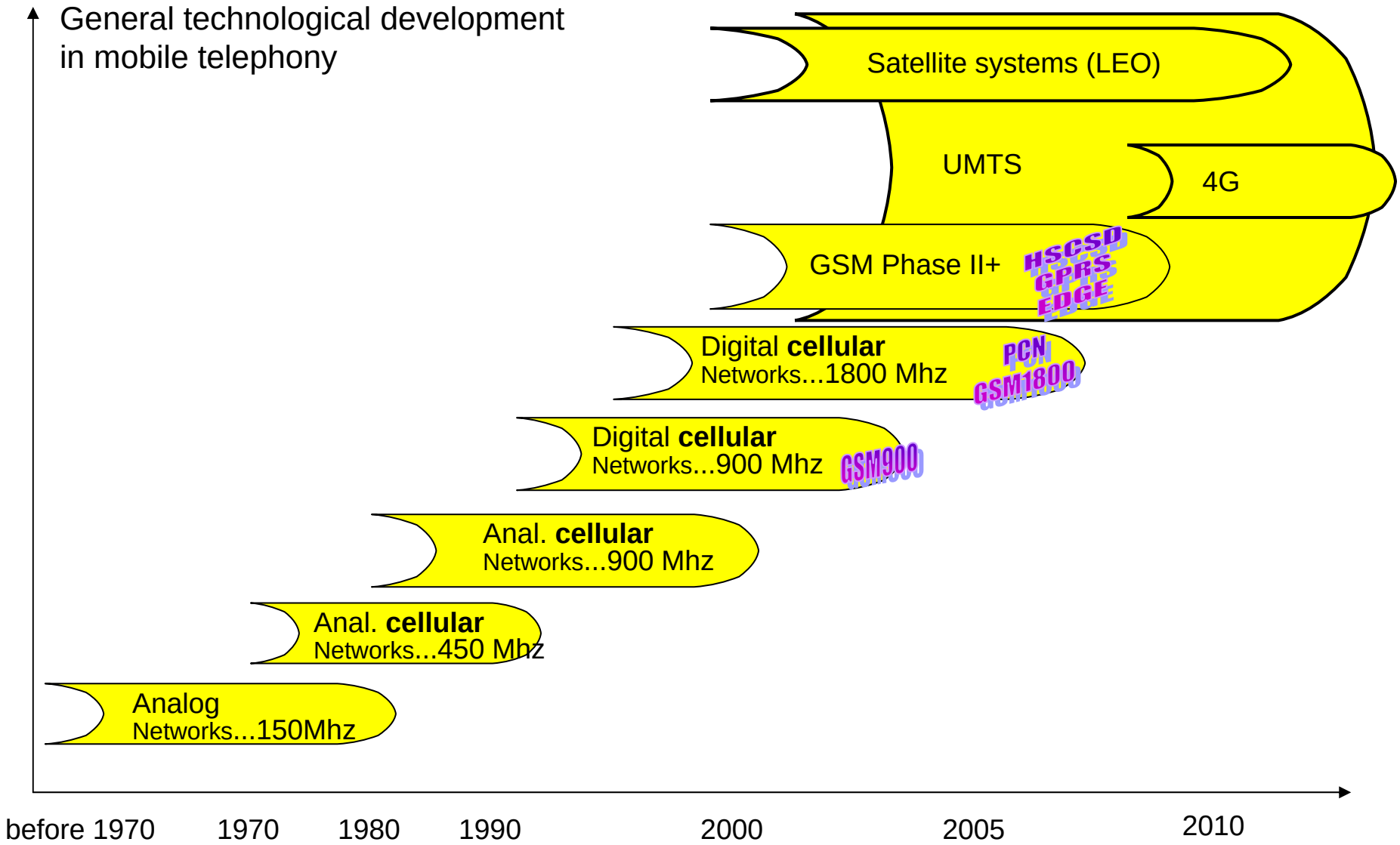
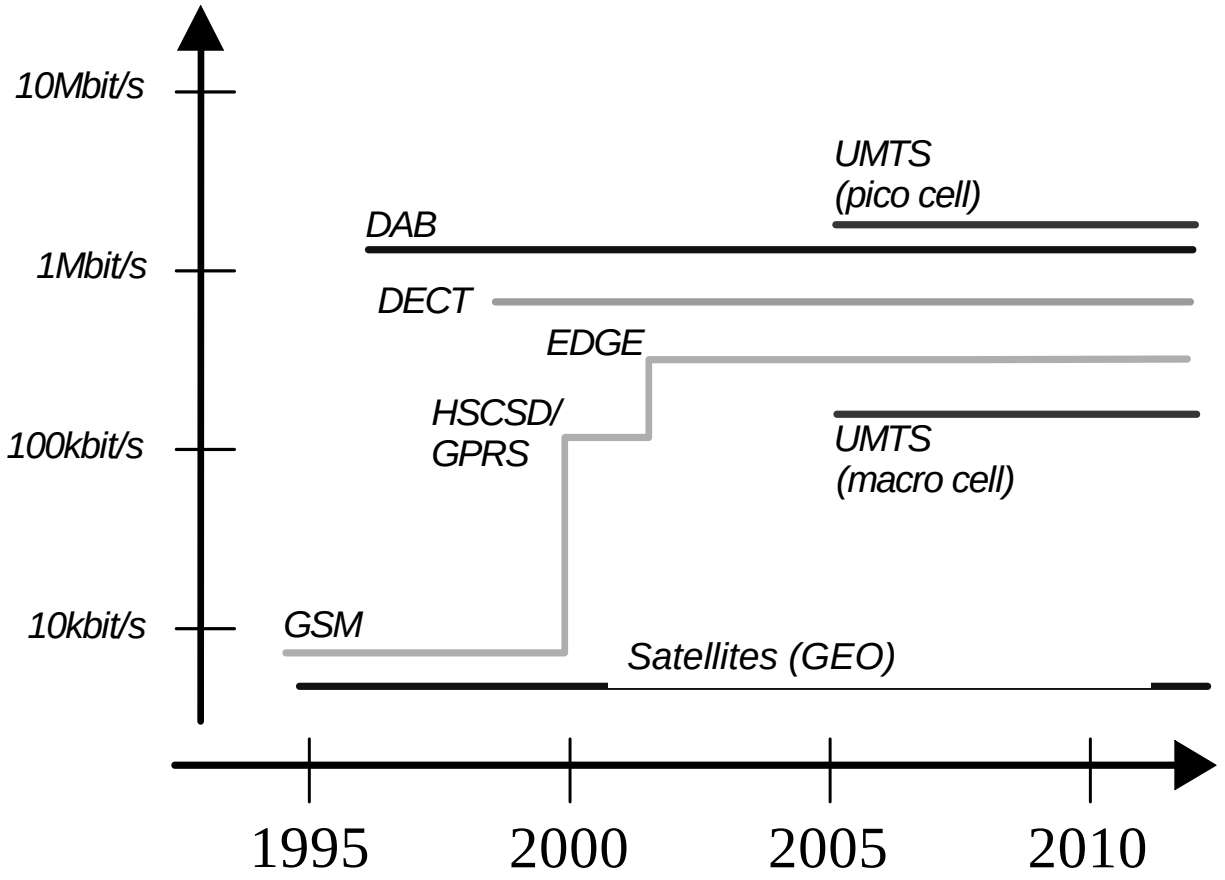
Mobile Radio Networks: Overview

Development of Mobile Radio



Correspondent data rates



Frequency Assignment

Circuit Switched Radio Mobile Phones Cordless Phones Wireless LANs

380-400 453-457 450-470 **500Mhz** 864-868 885-887 890-915 930-932 935-960 **1GHz**

410-430 463-467 (nationally different)

1670-1675 1710-1785 1800-1805 1805-1880 1880-1900 *(1885-2025*

2110-2200)

WLAN

IEEE 802.11b Bluetooth

IEEE 802.11a: 5,15-5,25; 5,25-5,35; 5,725-5,825

HIPERLAN1 HIPERLAN2 HIPER-Link

2400-2483 2402-2480 5176-5270 *(ca.5200,5600)* *(ca.17000)*

2412-2472

HomeRF...(approx.2400)

TFTS - Terrestrial Flight Telephone System

Notes:

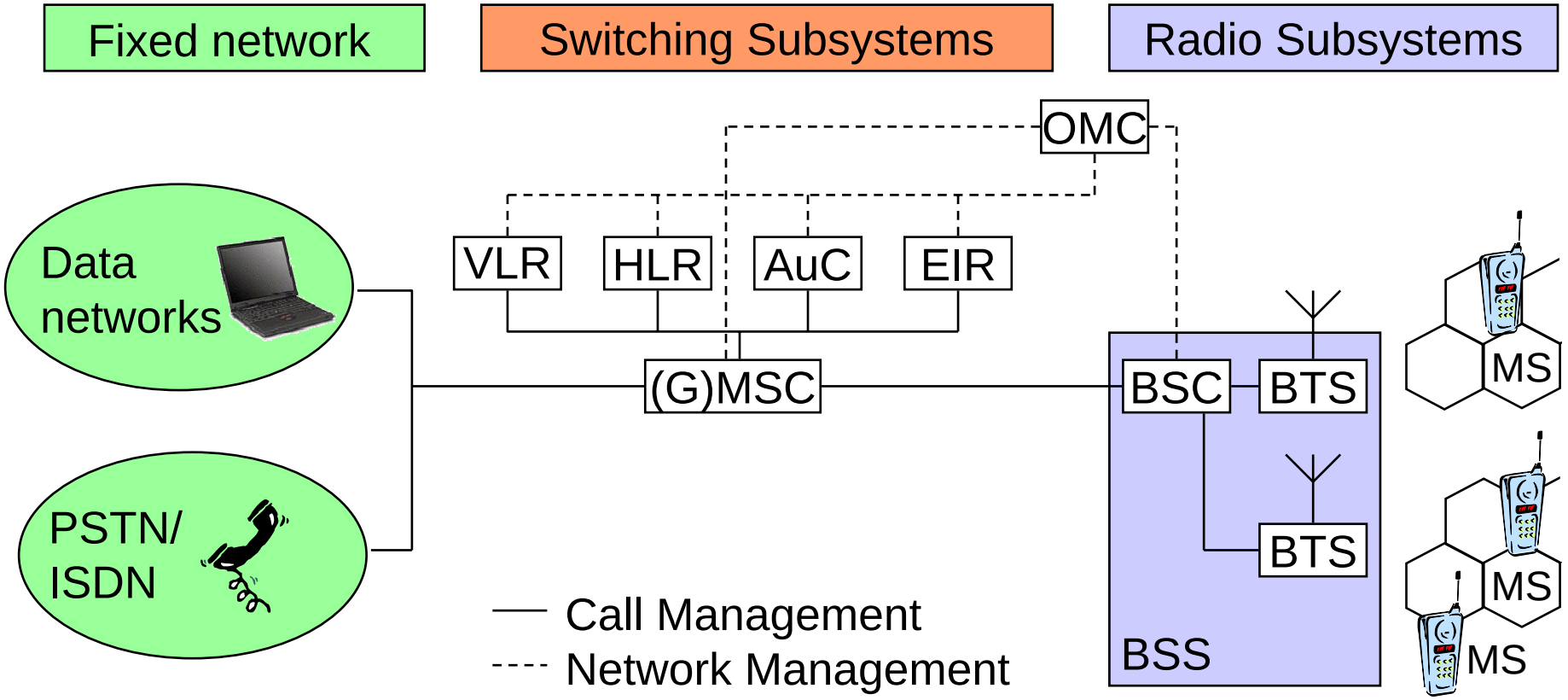
- 2,4 GHz license free, nationally different
- *() written : Prognoses!*
- today speech over license free frequencies up to 61Ghz -> interesting for high data rates

GSM: Global System for Mobile Communications

GSM: Properties

- cellular radio network (2nd Generation)
- digital transmission, data communication up to 9600 Bit/s
- Roaming (mobility between different network operators, international)
- good transmission quality (error detection and -correction)
- scalable (large number of participants possible)
- Security mechanisms (authentication, authorization, encryption)
- good resource use (frequency and time division multiplexing)
- integration within ISDN and fixed network
- standard (ETSI, European Telecommunications Standards Institute)

GSM: structure



AuC	Authentication Centre
BSS	Base Station Subsystem
BSC	Base Station Controller
BTS	Base Transceiver Station
EIR	Equipment Identity Register
HLR	Home Location Register
MS	Mobile Station
(G)MSC	(Gateway) Mobile Switching Centre
OMC	Operation and Maintenance Centre
PSTN	Public Switched Telephone Network
VLR	Visitor Location Register
ISDN	Integrated Services Digital Network

GSM: Structure

Operation and Maintenance Centre (OMC)

- logical, central structure with HLR, AuC und EIR

Authentication Centre (AuC)

- authentication, storage of symmetrical keys, generation of encryption keys

Equipment Identity Register (EIR)

- storage of device attributes of allowed, faulty and blocked devices (white, grey, black list)

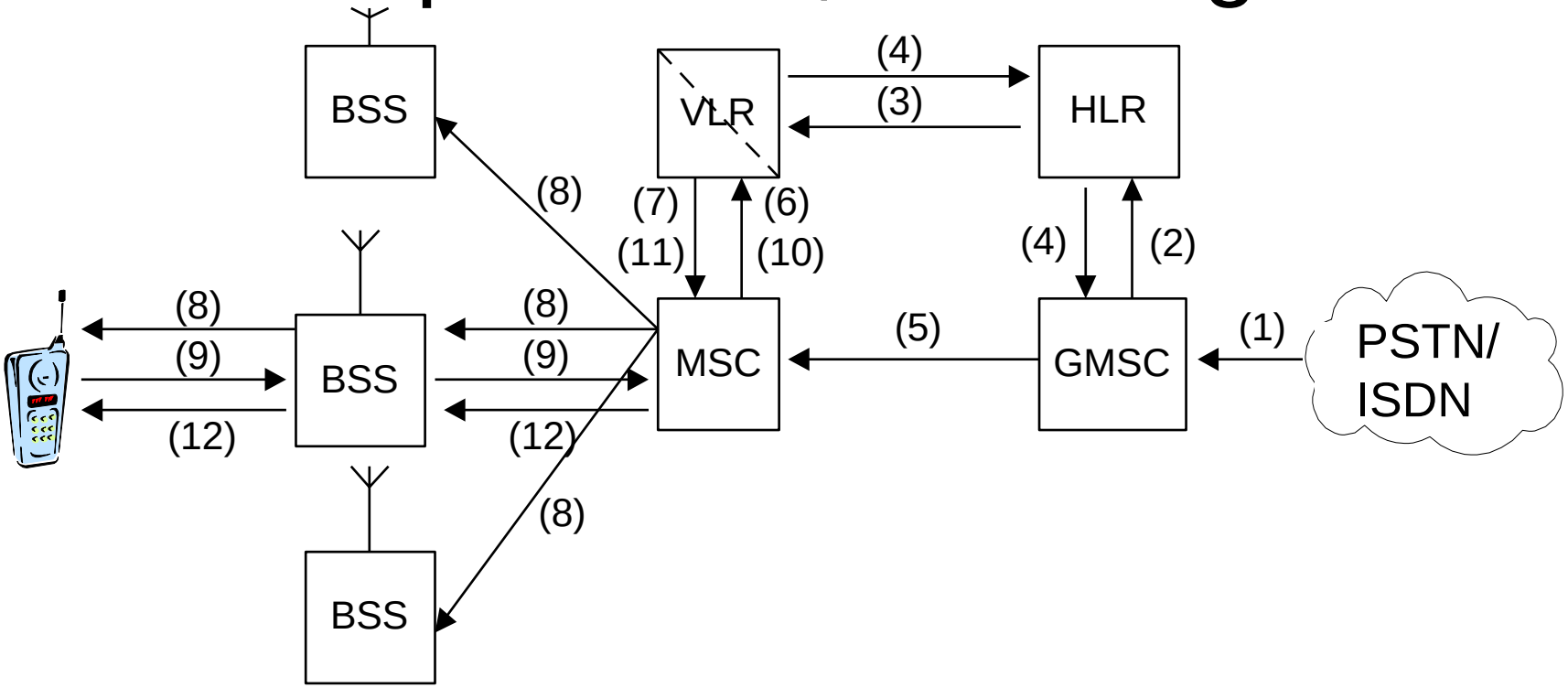
Mobile Switching Centre (MSC)

- networking centre, partially with gateways to other networks, assigned to one VLR each

Base Station Subsystem (BSS): technical radio centre

- **Base Station Controller (BSC)**: control centre
- **Base Transceiver Station (BTS)**: radio tower / antenna

GSM: protocols, incoming call



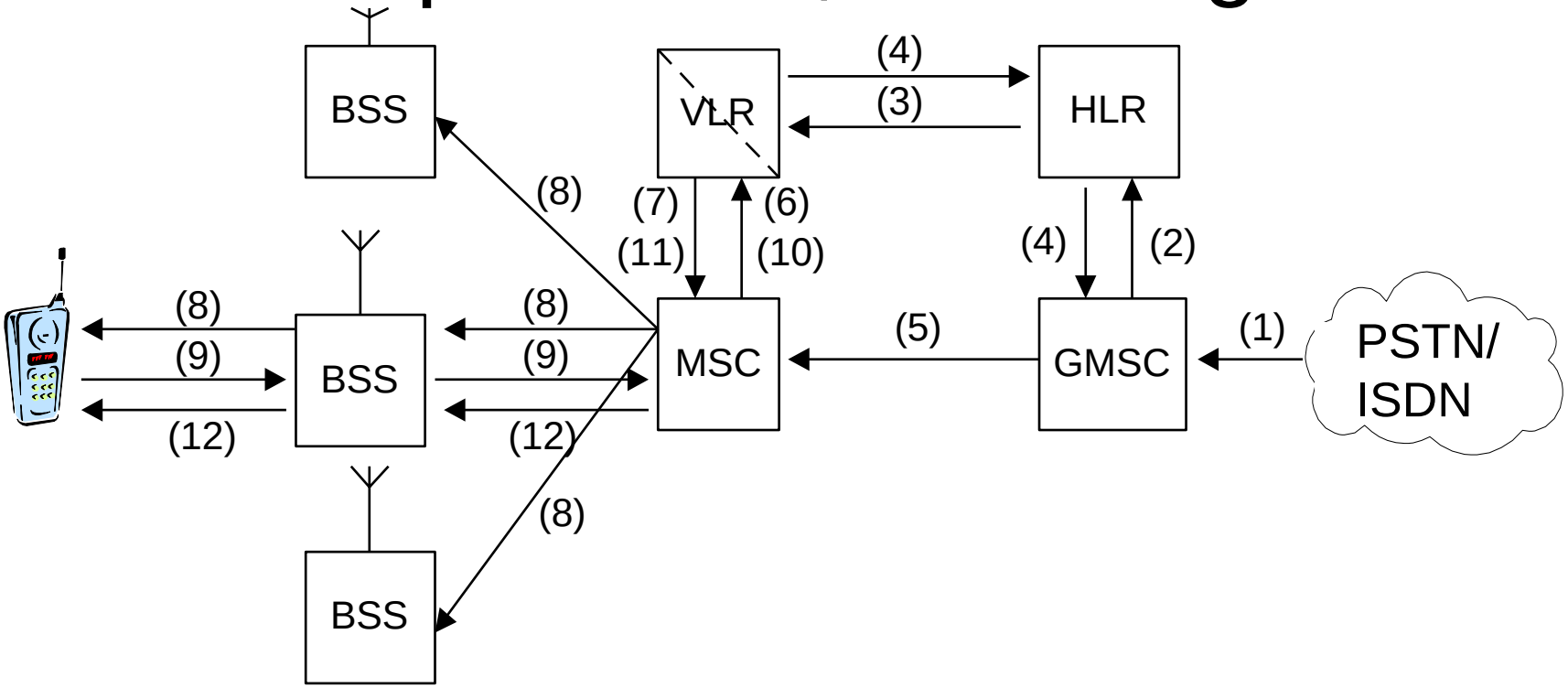
(1) Call from fixed network was switched via GMSC

(2) GMSC finds out HLR from phone number

(3) HLR checks whether participant is authorized for corresponding service and asks for MSRN at the responsible VLR

(4) MSRN will be returned to GMSC, can now contact responsible MSC

GSM: protocols, incoming call



(5) GMSC transmits call to current MSC

(6) ask for the state of the mobile station

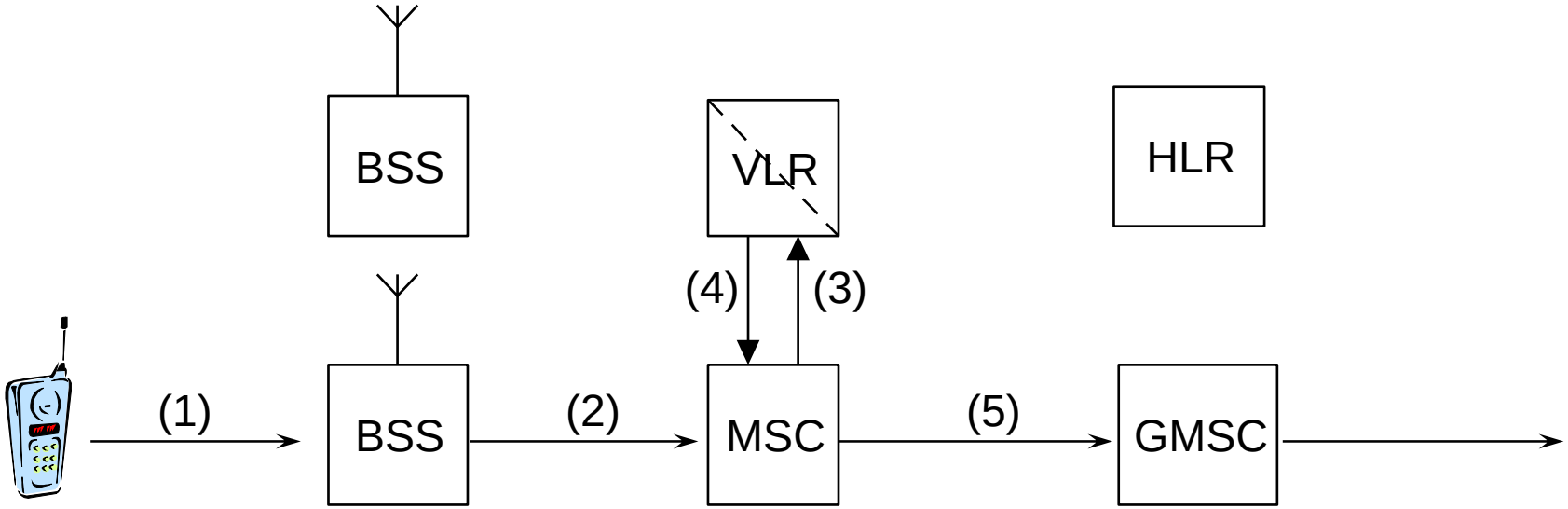
(7) Information whether end terminal is active

(8) Call to all cells of the Location Area (LA)

(9) Answer from end terminal

(10 - 12) security check and connection setup

GSM: protocols, outgoing call



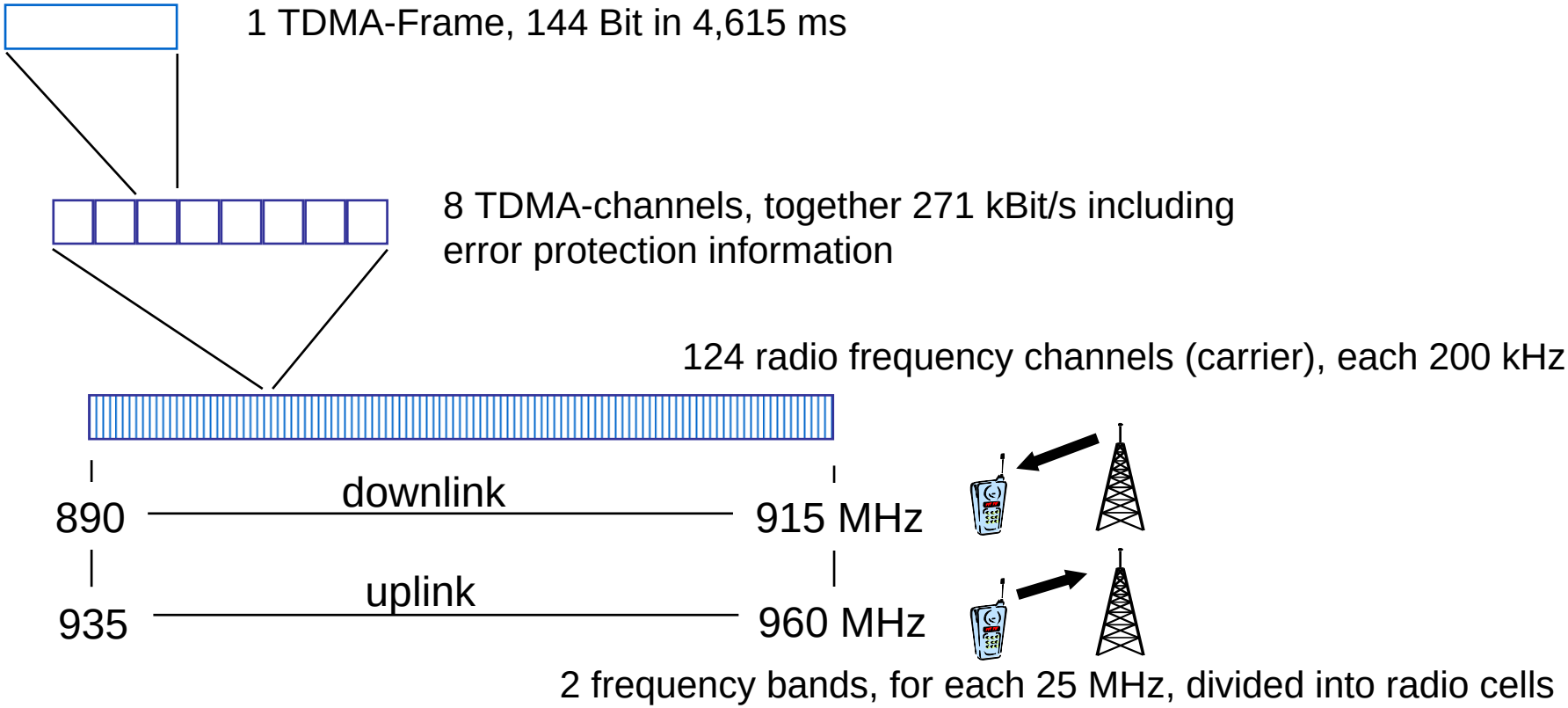
(1) Connection request

(2) Transfer by BSS

(3-4) Authorization control

(5) Switching of the call request to fixed network

Radio structure



- One or several carrier frequencies per BSC
- Physical channels defined by number and position of time slots

GSM: channel strucure

Traffic Channel

- speech- / data channel (13 kbit/s brutto; differential encoding)
- Half-rate traffic channel: for more efficient speech encoding with 7 kbit/s

Control Channel

- Signal information
- Monitoring of the BSCs for recognition of handover

Broadcast Control Channel

- BSC to MS (identity, frequency order etc.)

Random Access Channel

- Control of channel entry with Aloha-procedure

Paging Channel

- signalize incoming calls

Databases

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

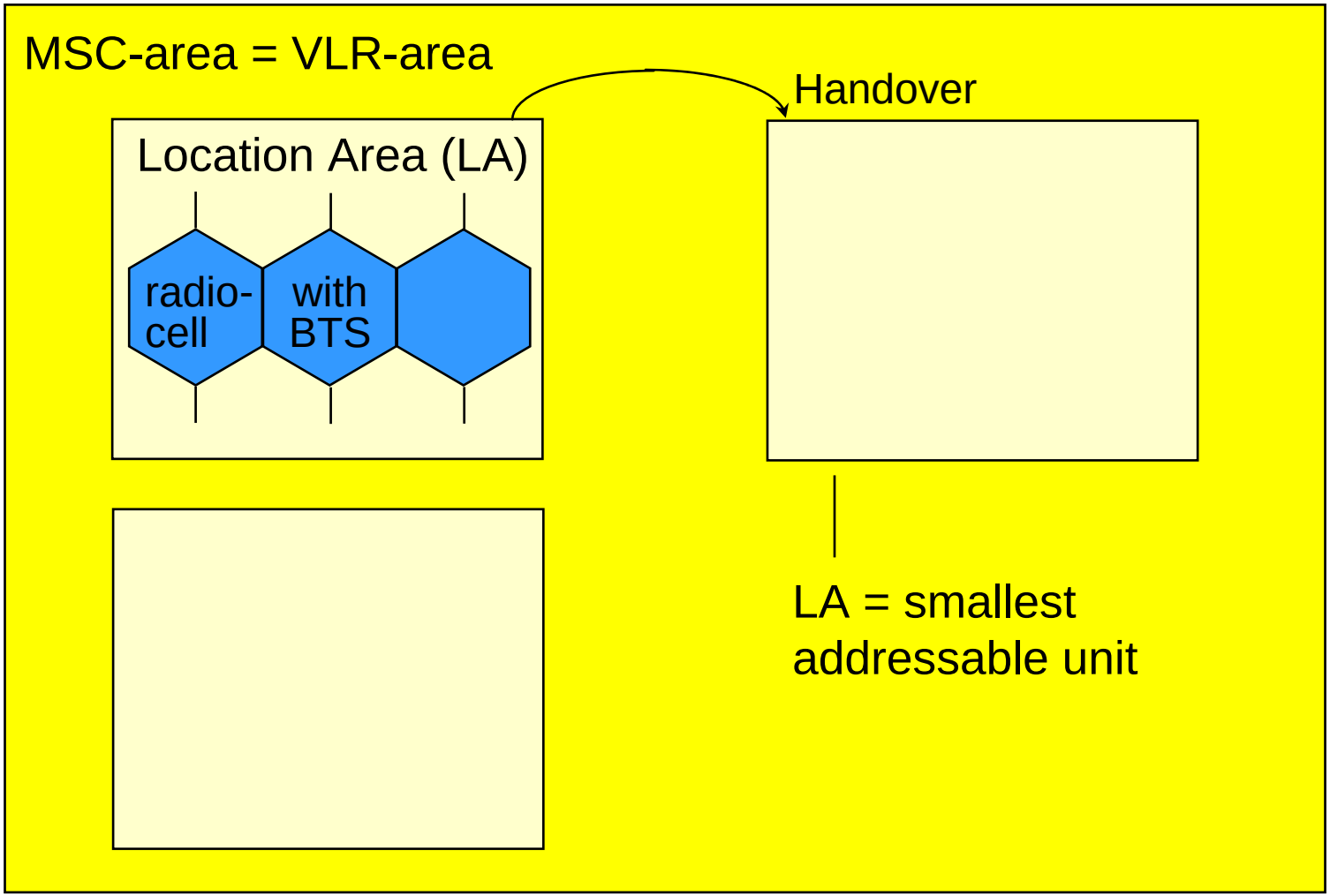
- Semi-permanent data:
  - Call number (Mobile Subscriber International ISDN Number) - MSISDN, e.g. +49/171/333 4444 (country, network, number)
  - identity (International Mobile Subscriber Identity) - IMSI: MCC = Mobile Country Code (262 for .de) + MNC = Mobile Network Code (01-D1, 02-Vodafone-D2, 03-eplus, 07-O2) + MSIN = Mobile Subscriber Identification Number
  - 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 AuC (RAND (128 Bit), SRES (128 Bit), K_C (64Bit))
  - billing data

Databases

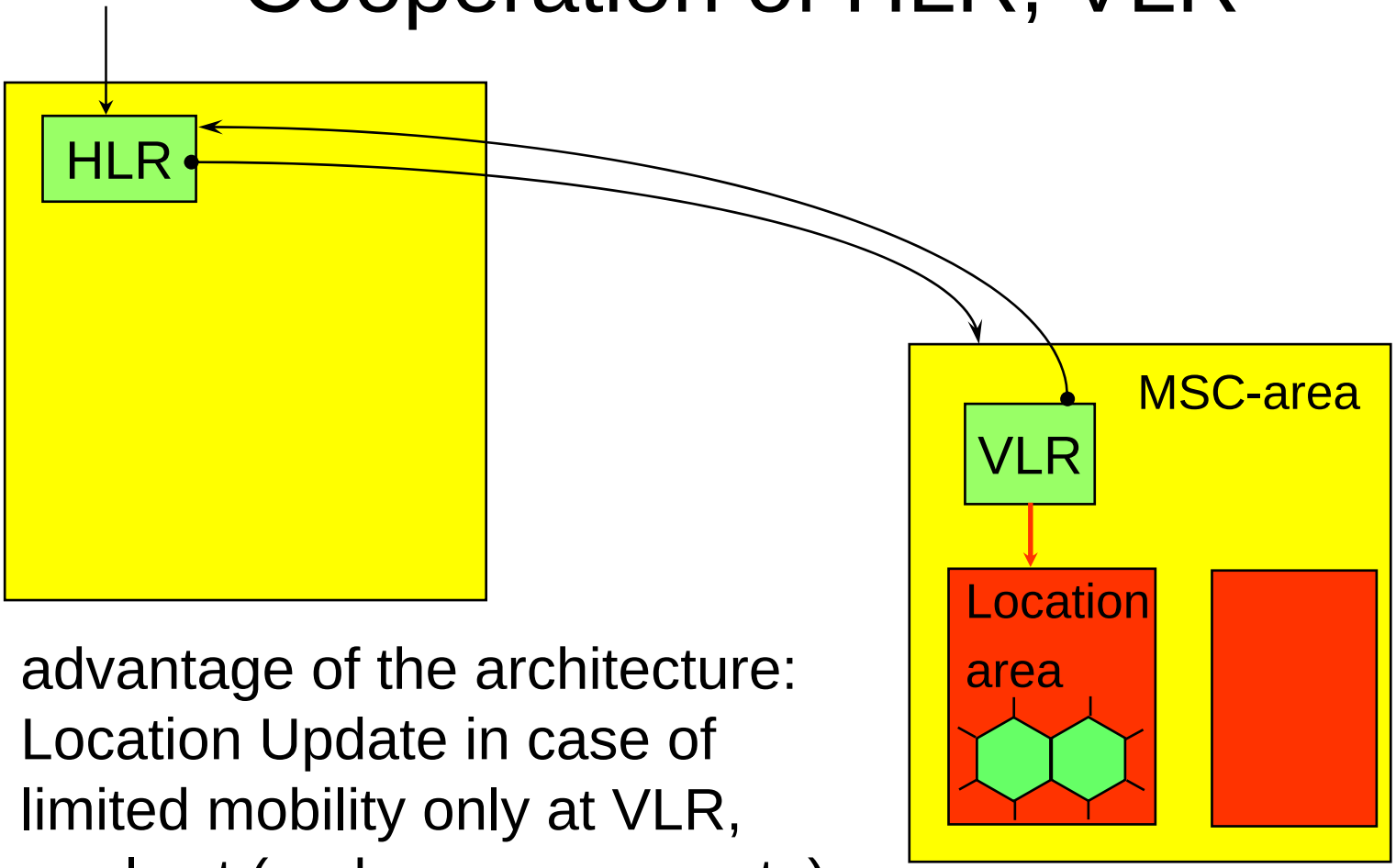
Visitor Location Register (VLR)

- 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

GSM: Location areas

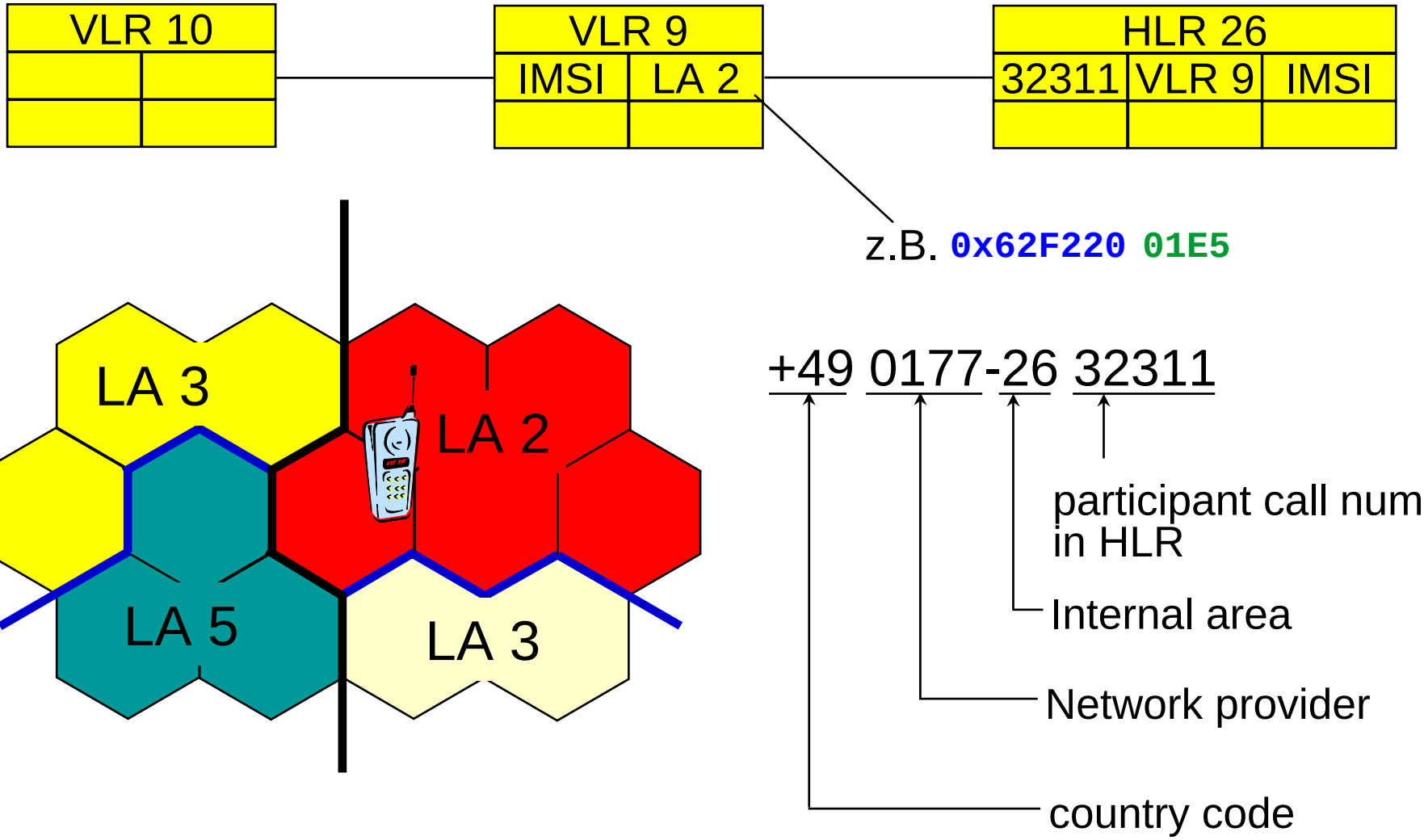


Cooperation of HLR, VLR



advantage of the architecture:
Location Update in case of limited mobility only at VLR, rarely at (perhaps very remote) HLR

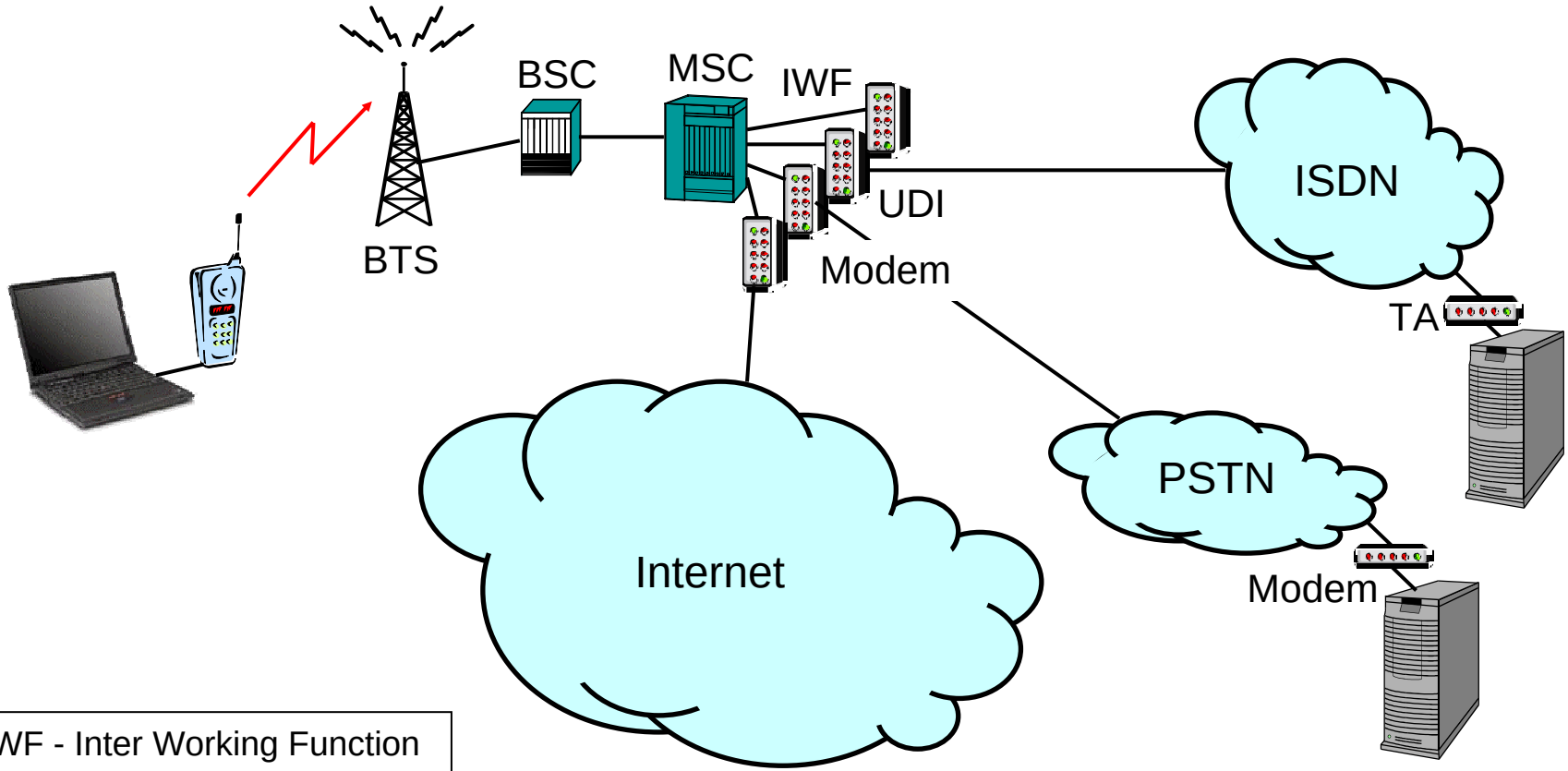
Localization at GSM



Data transmission

- each GSM-channel configurable as a data channel; similar structure like ISDN-B and -D-channels
- data rates up to 9600 bit/s
- delay approximately 200 ms
- speech channels have higher priority than data channels
- kinds of channels:
  - transparent (without error correction; however FEC; fixed data rate; error rate 10^{-3} up to 10^{-4})
  - non-transparent (repeat of faulty data frames; very low error rate, but also less throughput)
- Short-Message-Service (SMS)
  - connectionless transmission (up to 160 Byte) on signaling channel
- Cell Broadcast (CB)
  - connectionless transmission (up to 80 Byte) on signaling channel to all participants, e.g. for location based services

Data transmission - structure



IWF - Inter Working Function
UDI - Unspecified Digital
TA - Terminal Adapter

Security aspects: Subscriber Identity Module (SIM)

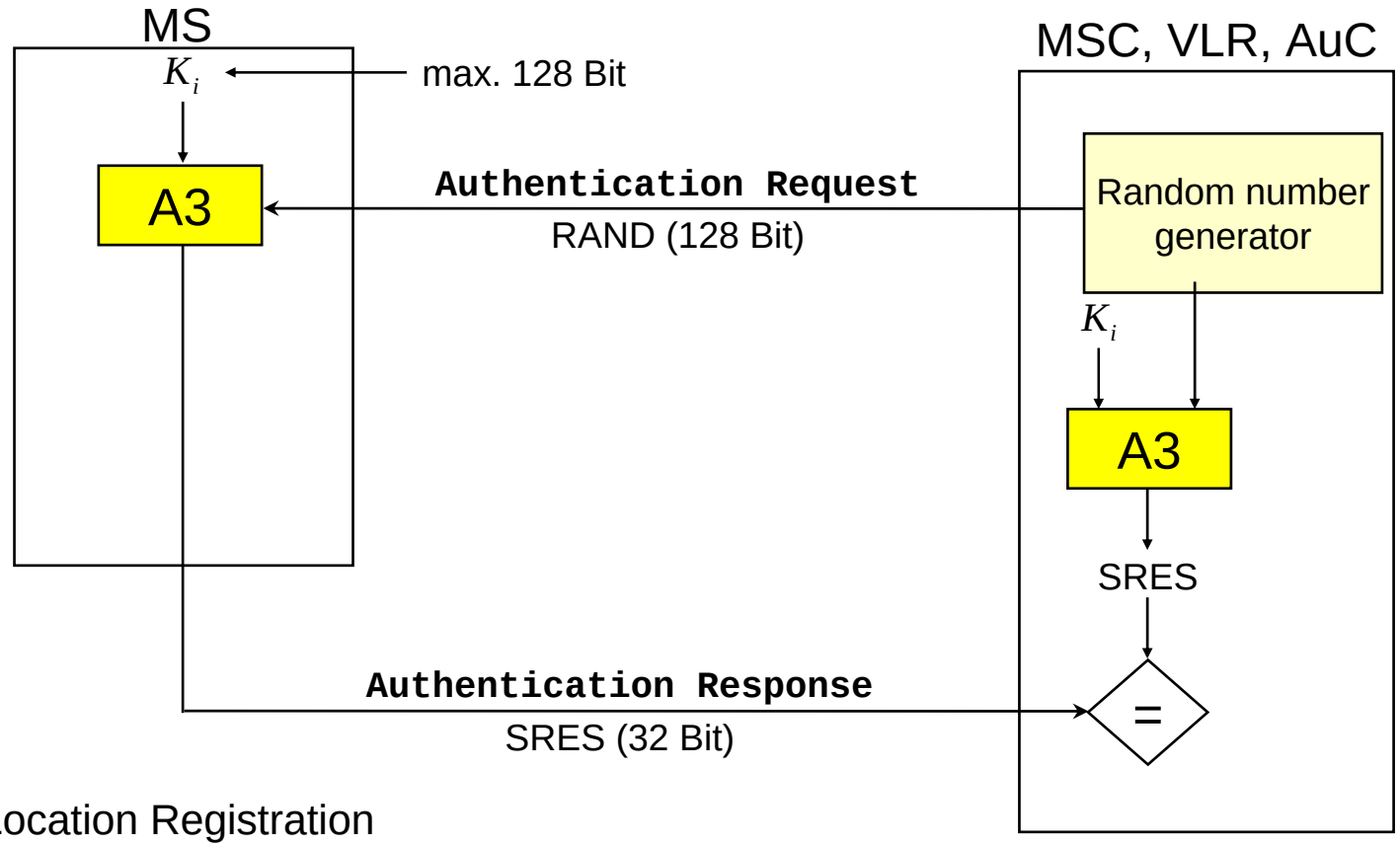
Chip-card (Smart Cart) to personalize a mobile subscriber (MS):

- IMSI (International Mobile Subscriber Identity)
- symmetric key K_i of participant, stored also at AuC
- algorithm “A3” for Challenge-Response-Authentication
- algorithm “A8” for key generation of K_c for content data
- algorithm “A5” for encryption
- PIN (Personal Identification Number) for access control

Temporary data:

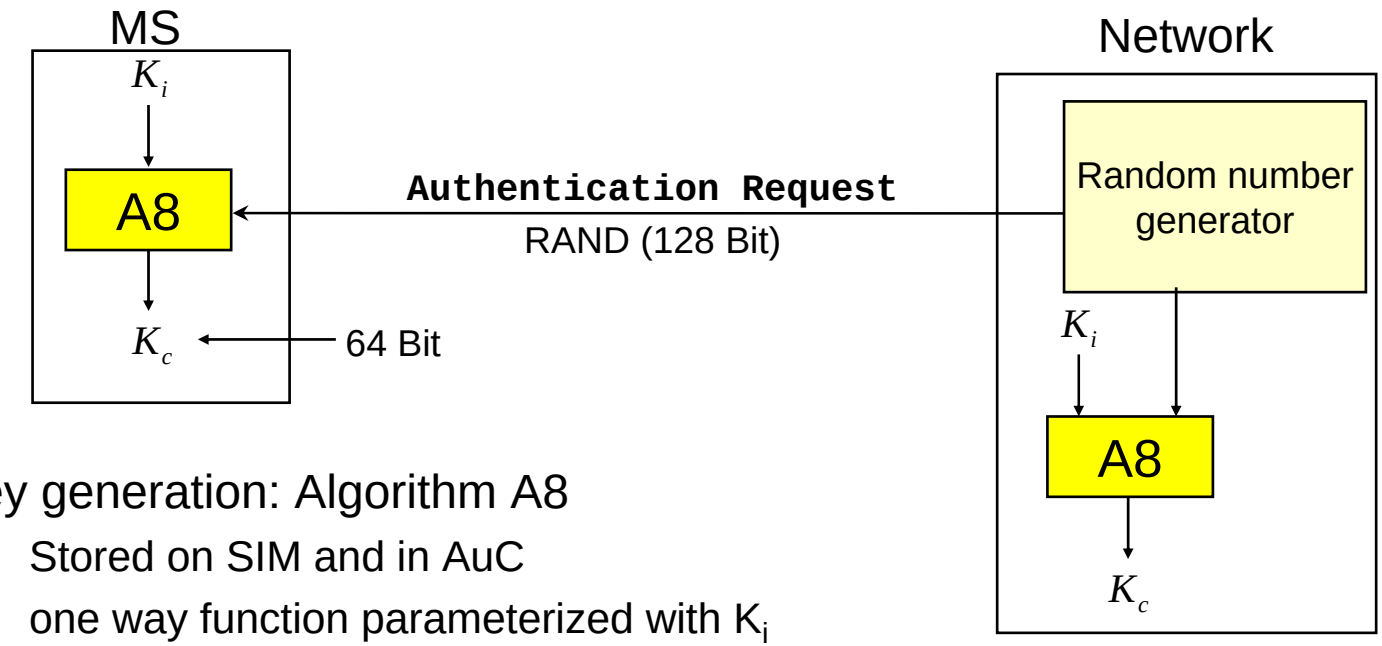
- TMSI (Temporary Mobile Subscriber Identity) - pseudonym
- LAI (Location Area Identification)
- Encryption key K_c

Security aspects: Authentication



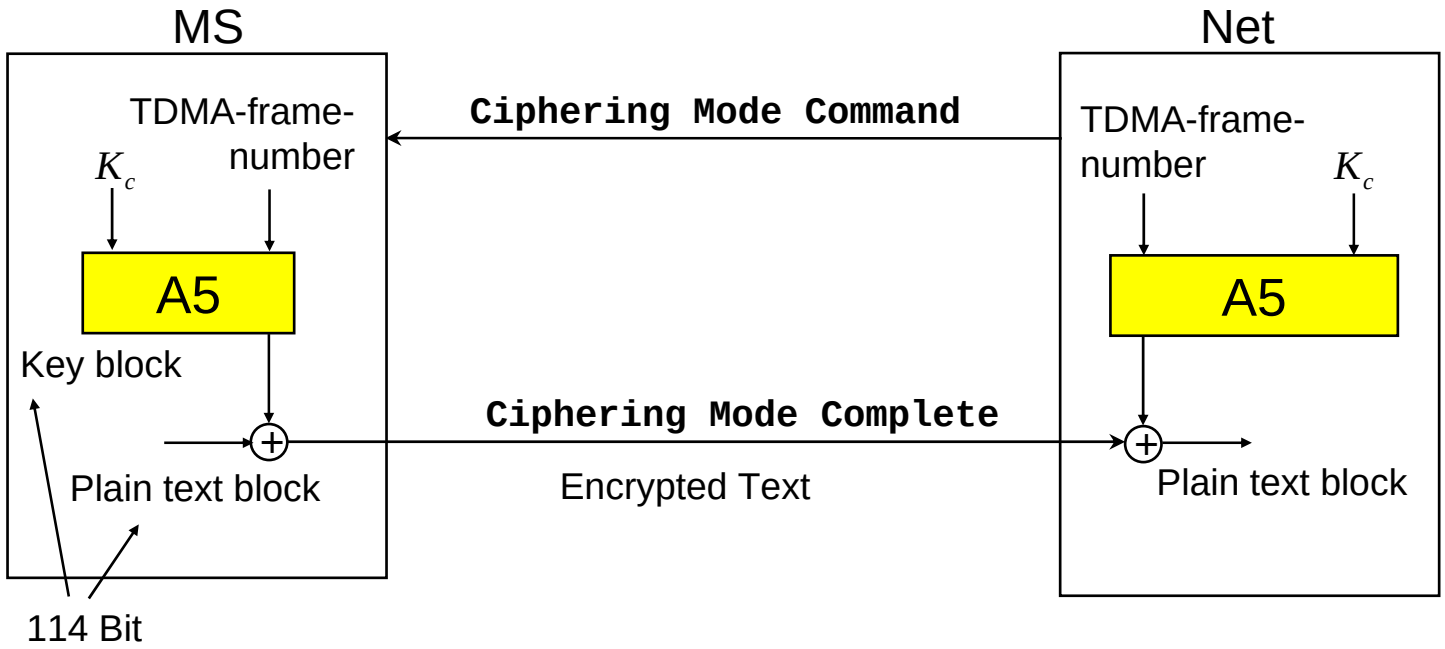
- Location Registration
- Location Update with VLR-change
- Call setup (in both directions)
- SMS (Short Message Service)

Security aspects: Session Key



- Key generation: Algorithm A8
  - Stored on SIM and in AuC
  - one way function parameterized with K_i
  - no (Europe, world wide) standard
  - can be determined by network operator
  - Interfaces are standardized

Security aspects: encryption at the Radio interface



- Data encryption through algorithm A5:
  - stored in the Mobile Station
  - standardized in Europe and world wide
  - weaker algorithm A5* or A5/2 for specific countries

GSM-Security: assessment

- cryptographic methods secret, so they are not „well examined“
- symmetric procedure
  - consequence: storage of secret user keys with network operators required
- low key length K_i with max. 128 Bit (could be hacked by using Brute Force Attack in 8-12 hours)
- no mutual authentication
  - consequence: Attacker can pretend a GSM-Net
- no end-to-end encryption
- no end-to-end authentication
- Key generation and -administration not controlled by the participants