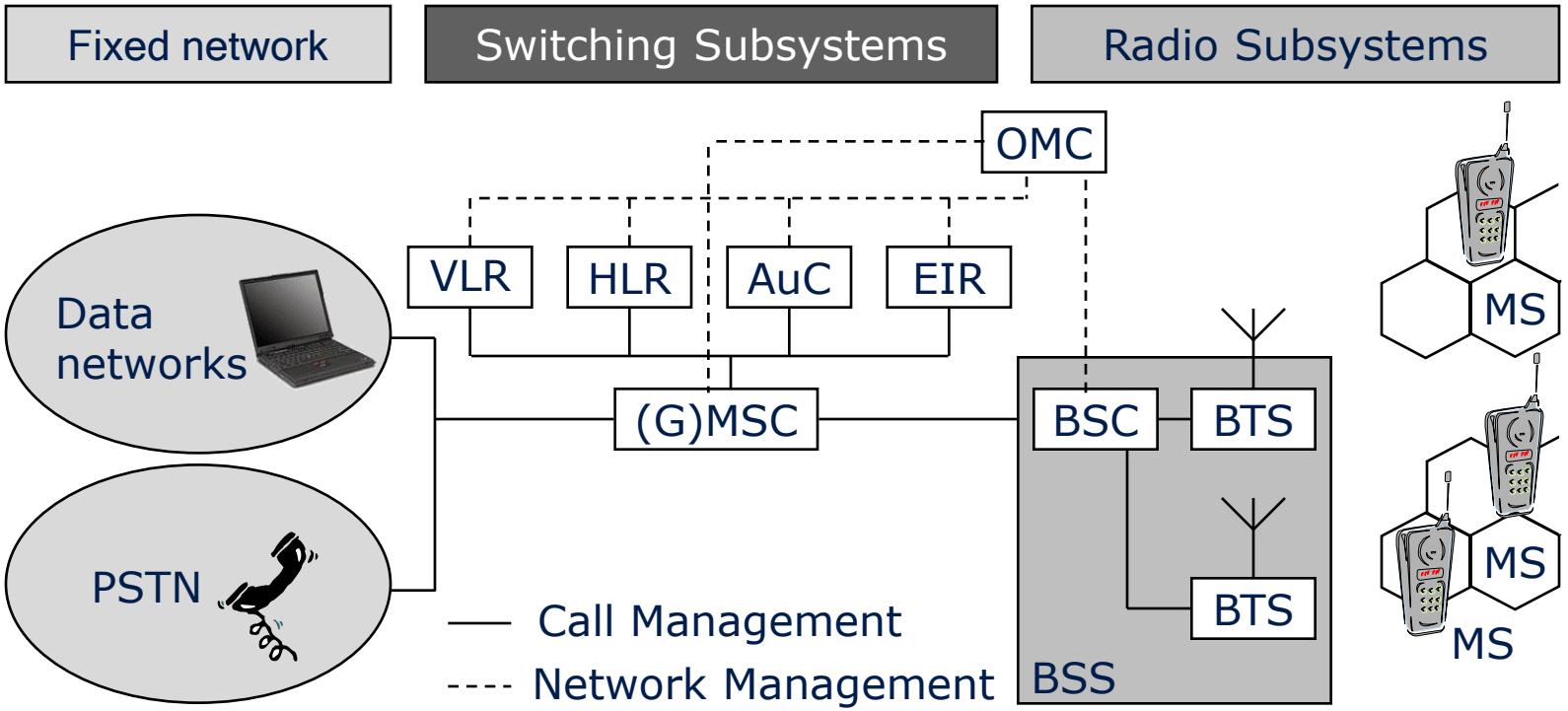
GSM: Properties

- cellular radio network (2nd Generation)
- digital transmission, integrated data communication
- roaming (mobility between different network operators)

- 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 multiplex)

- integration with fixed telephone network
- standard (ETSI, European Telecommunications Standards Institute)

GSM: Structure

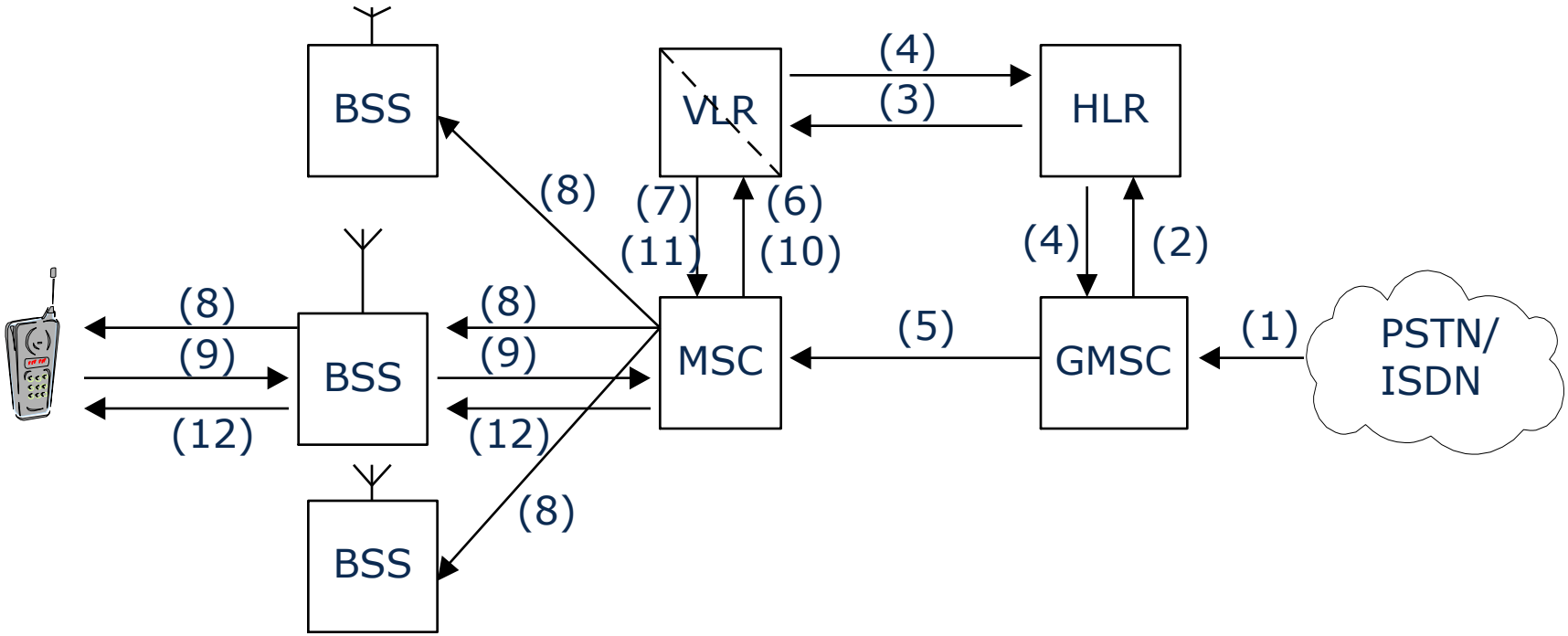


AuC	Authentication Center	MS	Mobile Station
BSS	Base Station Subsystem	(G)SMC	(Gateway) Mobile Switching Center
BSC	Base Station Controller	OMC	Operation and Maintenance Center
BTS	Base Transceiver Station	PSTN	Public Switched Telephone Network
EIR	Equipment Identity Register	VLR	Visitor Location Register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

GSM: Structure

- Operation and Maintenance Center (OMC)
- logical, central structure with HLR, AuC und EIR
- Authentication Center (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, gray, black list)
- Mobile Switching Center (MSC)
- networking center, partially with gateways to other networks, assigned to one VLR each
- Base Station Subsystem (BSS): technical radio center
- Base Station Controller (BSC): control center
- Base Transceiver Station (BTS): radio tower / antenna

GSM: Protocols, incoming call



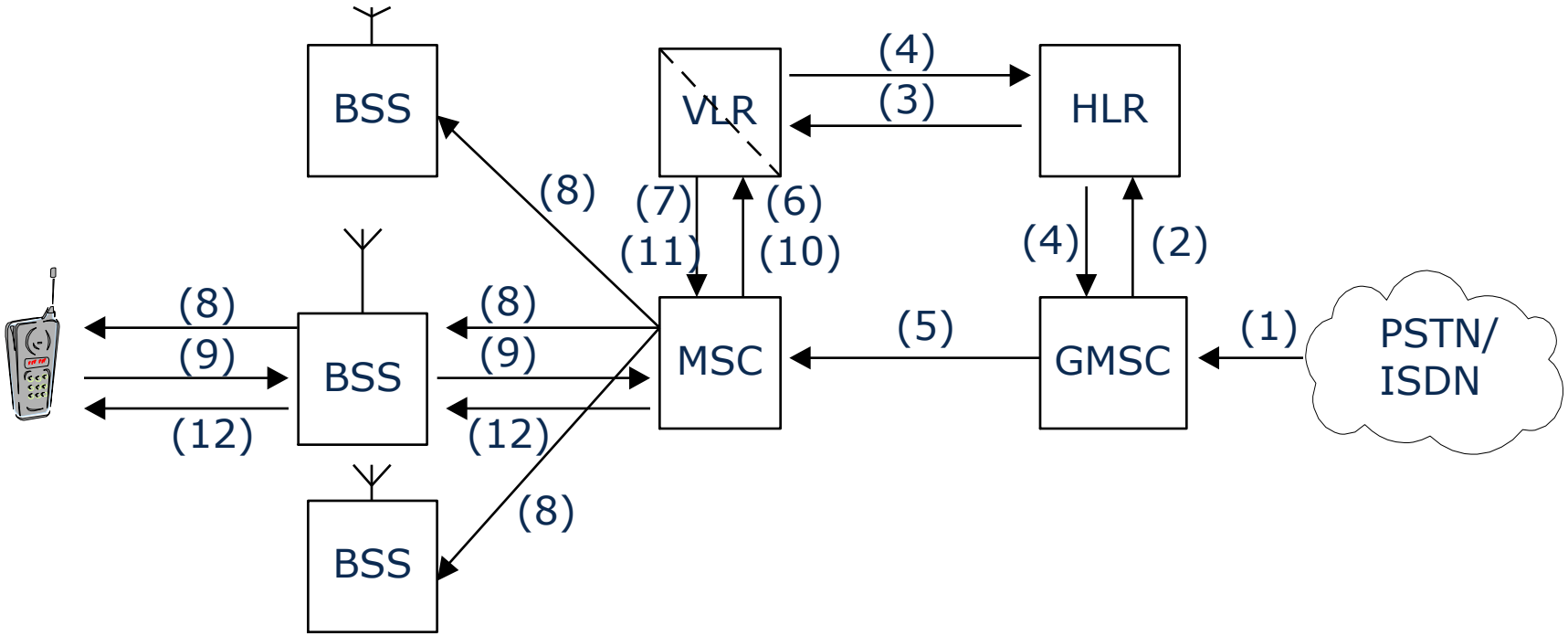
(1) Call from fixed network was switched via GMSC

(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

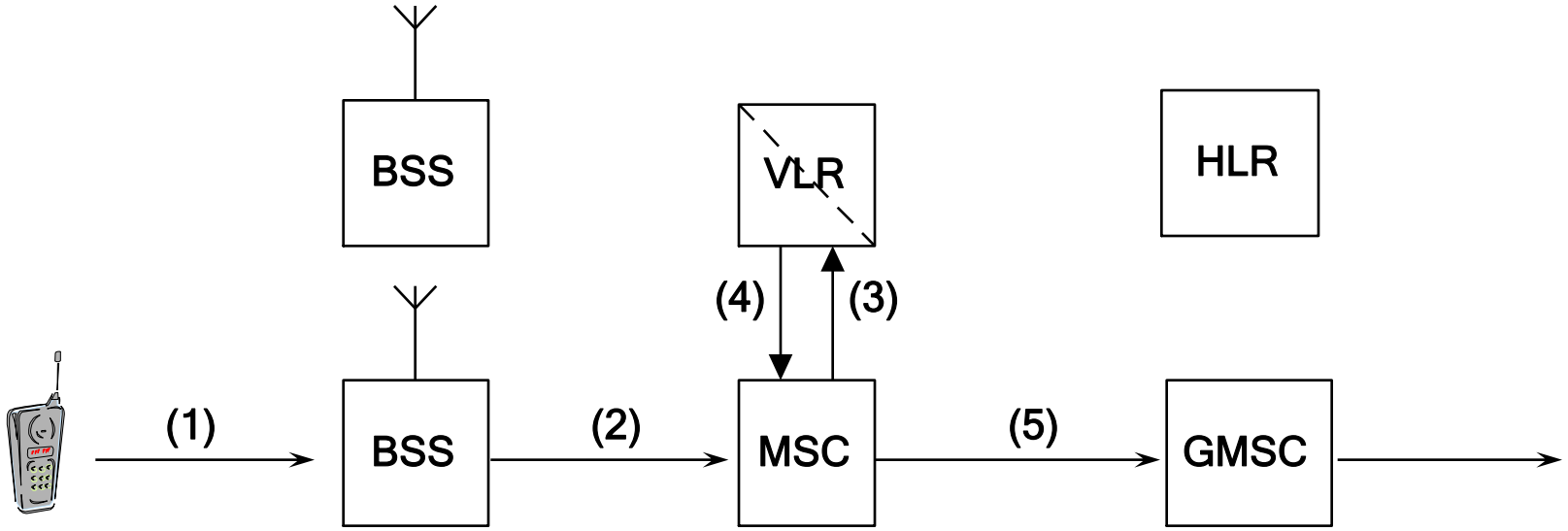
(4) MSRN will be returned to GMSC, can now contact responsible MSC

GSM: Protocols, incoming call



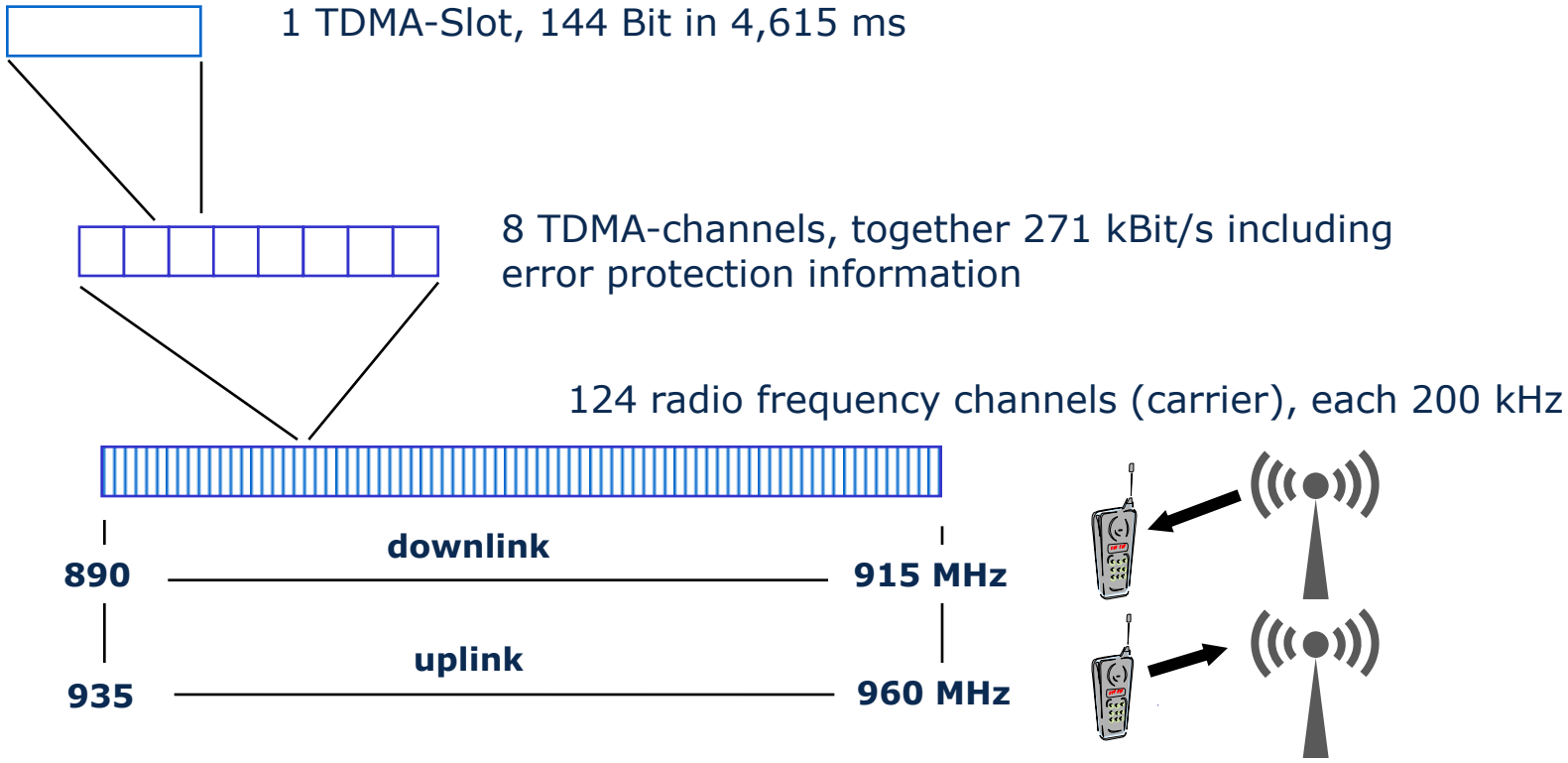
(5) GMSC transmits call to current MSC
(6) Ask for the state of the mobile station
(7) Information whether end terminal is active
(8) Call to all cells of the Location Area (LA)
(9) Answer from end terminal
(10 - 12) Security check and connection setup

GSM: Protocols, outgoing call



(1) Connection request
(via random access channel, possible collision handling)
(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 structure

Traffic Channel

- Full-rate codec (13 kbit/s; differential encoding)
- Half-rate codec: more efficient speech encoding at 7 kbit/s (two phone calls per time slot can be encoded)

Paging Channel

- Signalize incoming calls (BSC to MS)

(Broadcast) Control Channel

- Allocation of identity, frequency order etc. (BSC to MS)
- Monitoring of BSCs for recognition of handover

Random Access Channel

- Control of channel entry with Aloha-procedure for collision handling between competing participants (MS to BSC)

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-T-Mobile, 02-Vodafone, 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, network, MSC)
  - VLR-address, MSC-address
  - Authentication Sets of AuC (RAND (128 Bit), SRES (128 Bit), K_C (64Bit))
  - Billing data

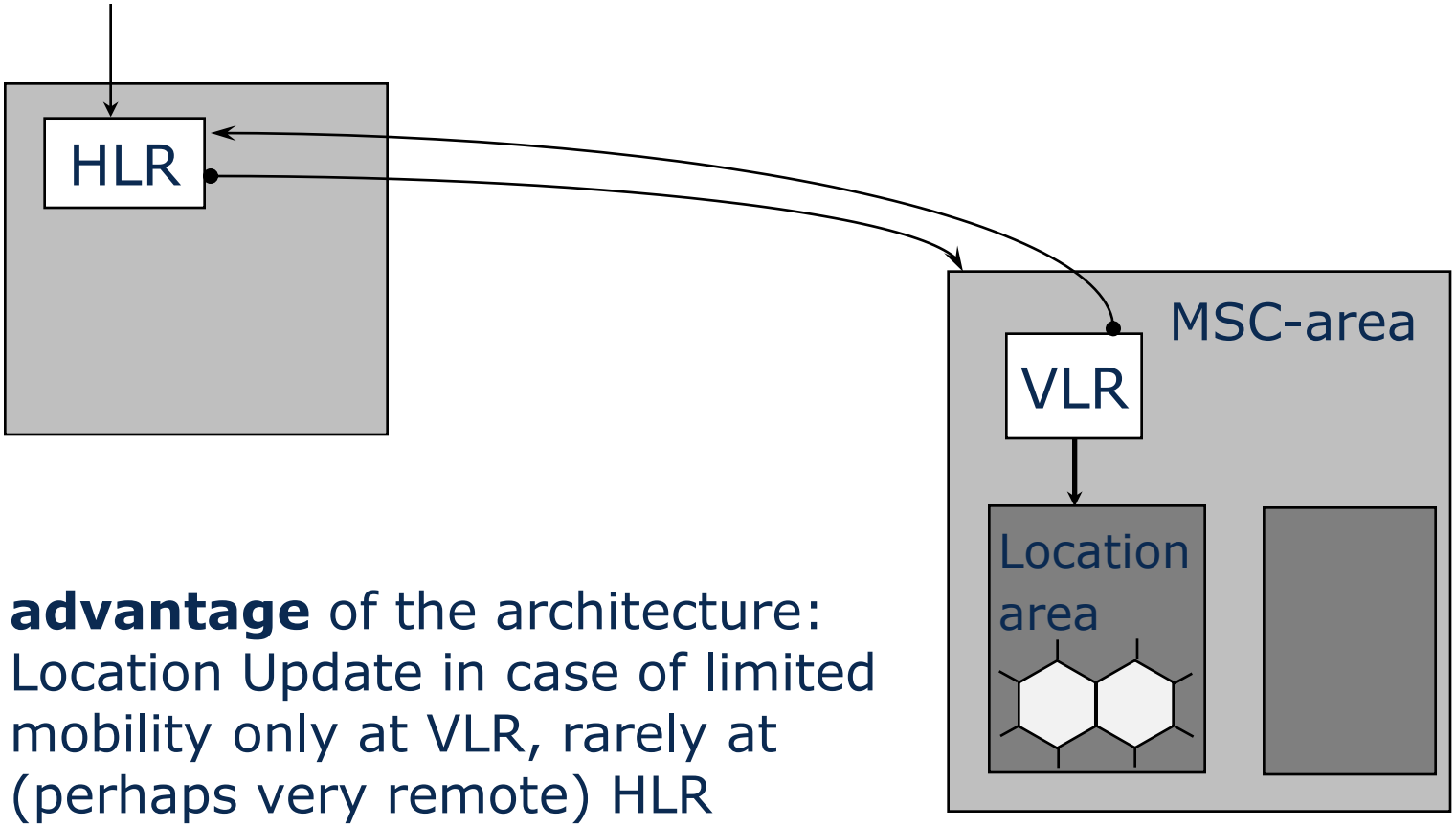
Databases

Visitor Location Register (VLR)

local database of each MSC with following data:

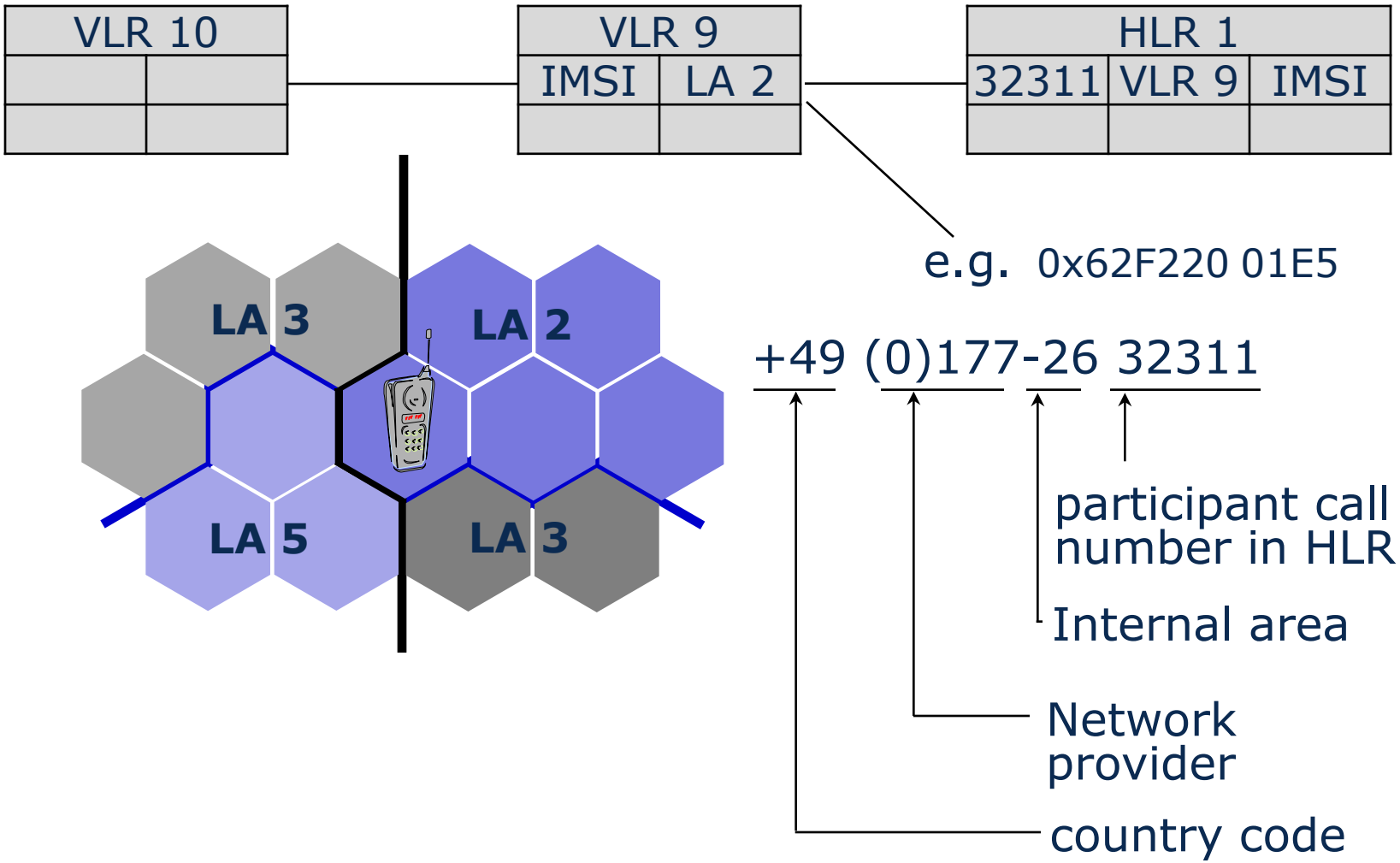
- IMSI, MSISDN
- Service profile
- Billing and accounting information
- TMSI (Temporary Mobile Subscriber Identity) - pseudonym for data security
- MSRN
- LAI (Location Area Identity)
- MSC-address, HLR-address

Location Area: Concept



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

Localization with GSM



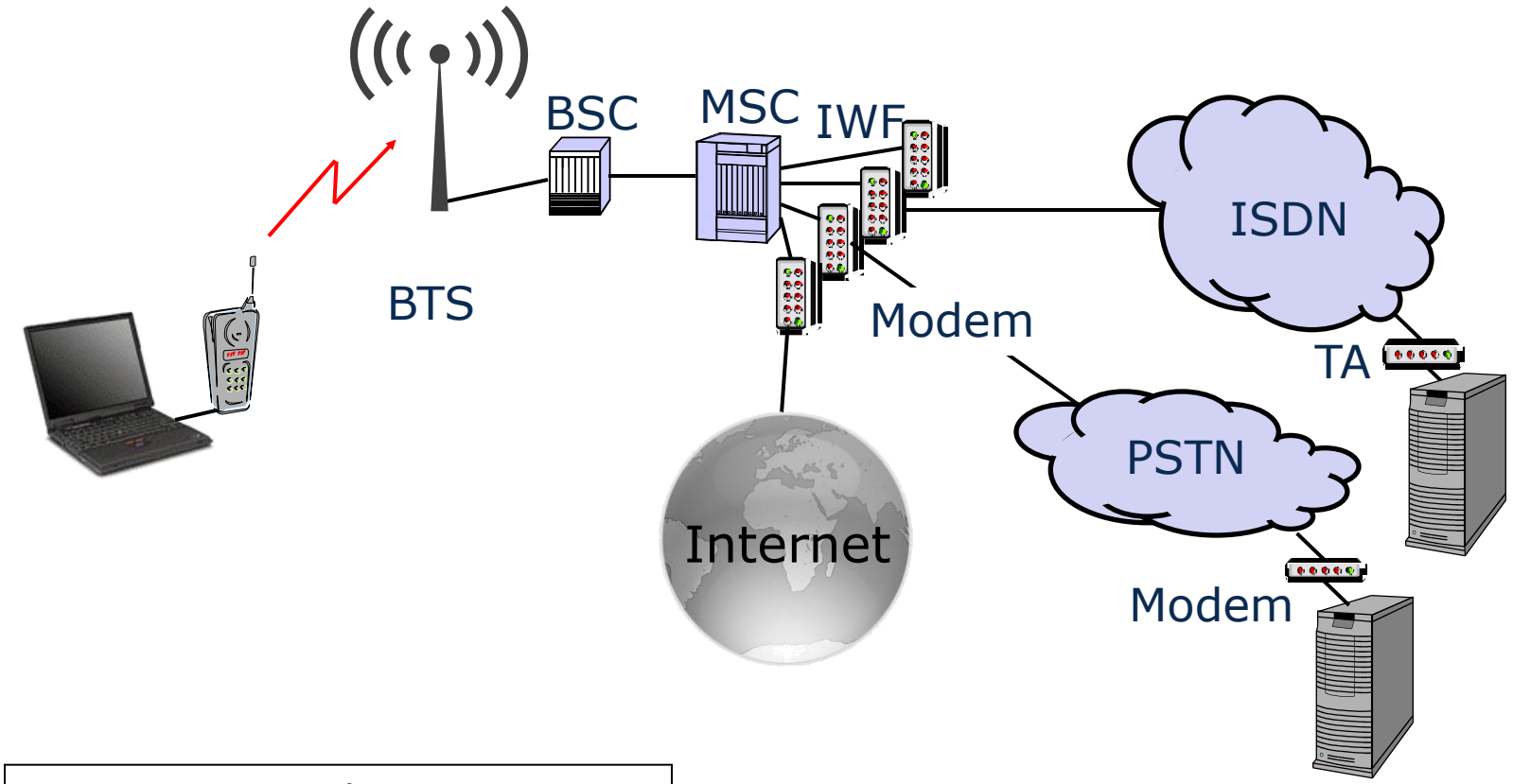
Data transmission

- Each GSM-channel configurable as data channel
- Kinds of channels:
  - non-transparent (repeat of faulty data frames; very low error rate, but also very low throughput below 10 kbit/s)
  - transparent (only very simple forward error correction; slightly higher data rate; error rate 10^{-3} up to 10^{-4})
  - in practice, only faster extensions like GPRS, UMTS and LTE are used (explained later)
  - Speech channels have higher priority than data channels

- 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 in one cell or location area, e.g. for location based services; further refinement: triangulation-based location check like in global positioning system (GPS)

Data transmission - structure

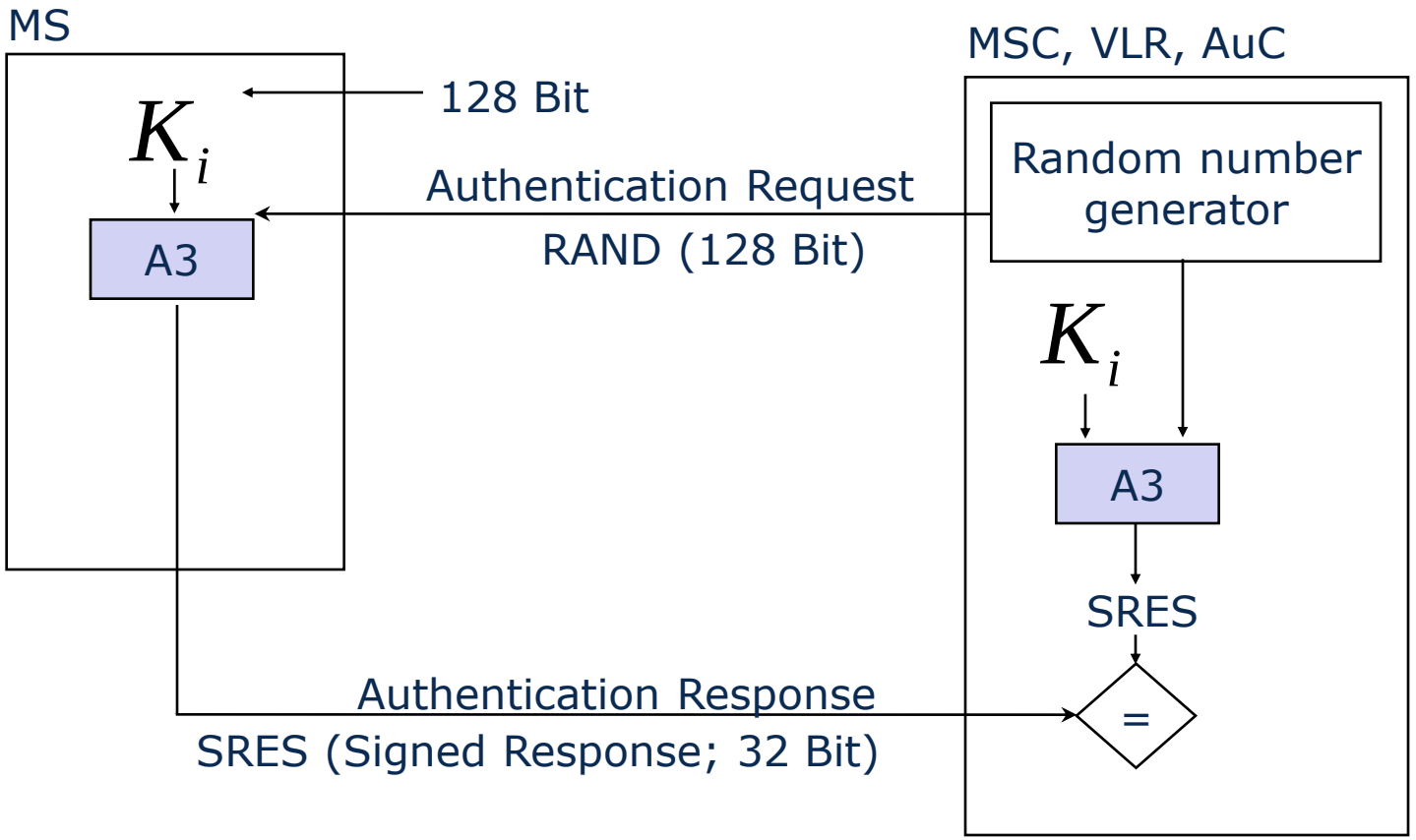


IWF - Inter Working Function
TA - Terminal Adapter

Security aspects: Subscriber Identity Module (SIM)

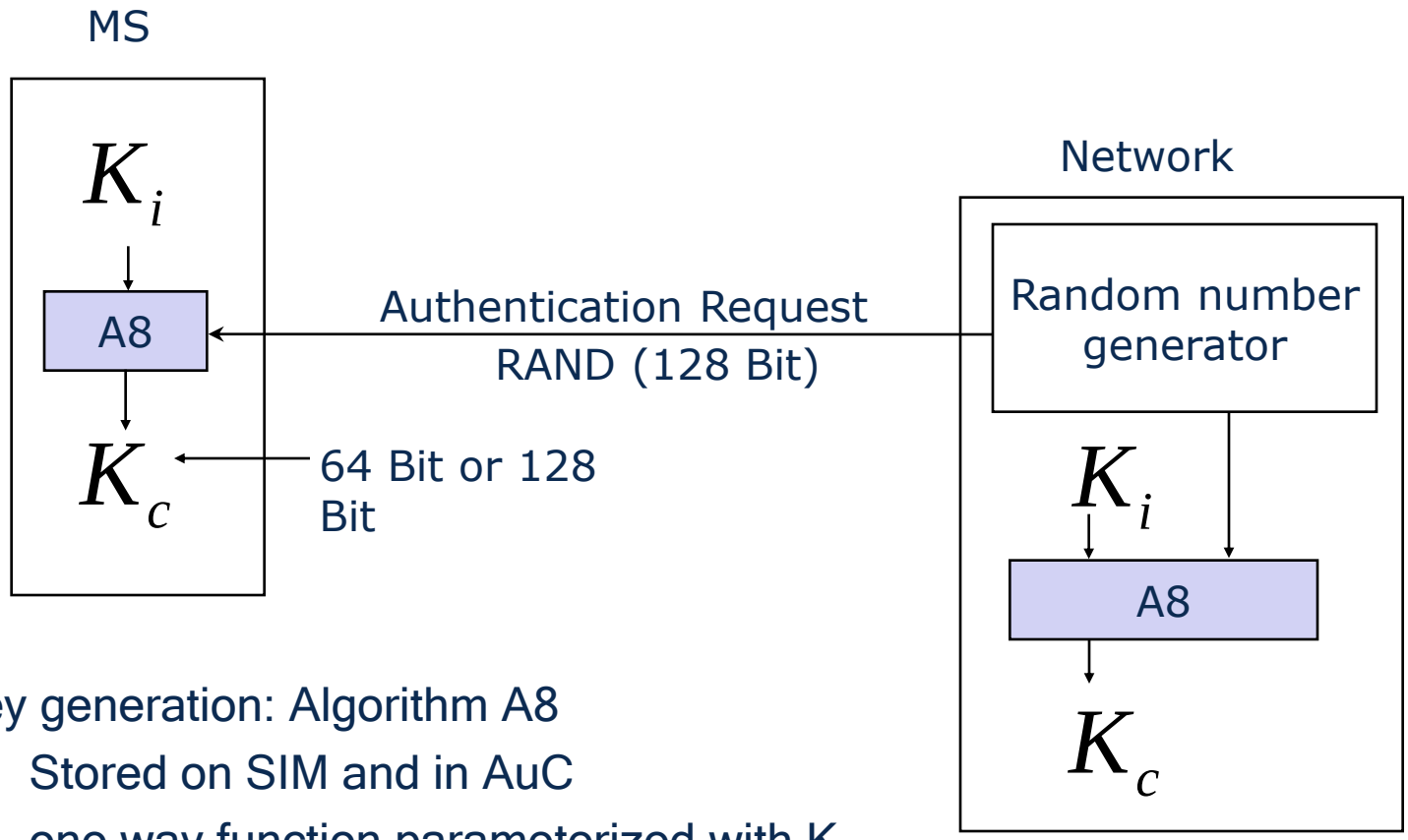
- Chip-card (Smart Cart) to personalize a mobile subscriber (MS):
- IMSI (International Mobile Subscriber Identity)
- symmetric key K_i of participant, stored also at AuC
- algorithm “A3” for Challenge-Response-Authentication
- algorithm “A8” for key generation of K_c for content data
- algorithm “A5” 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



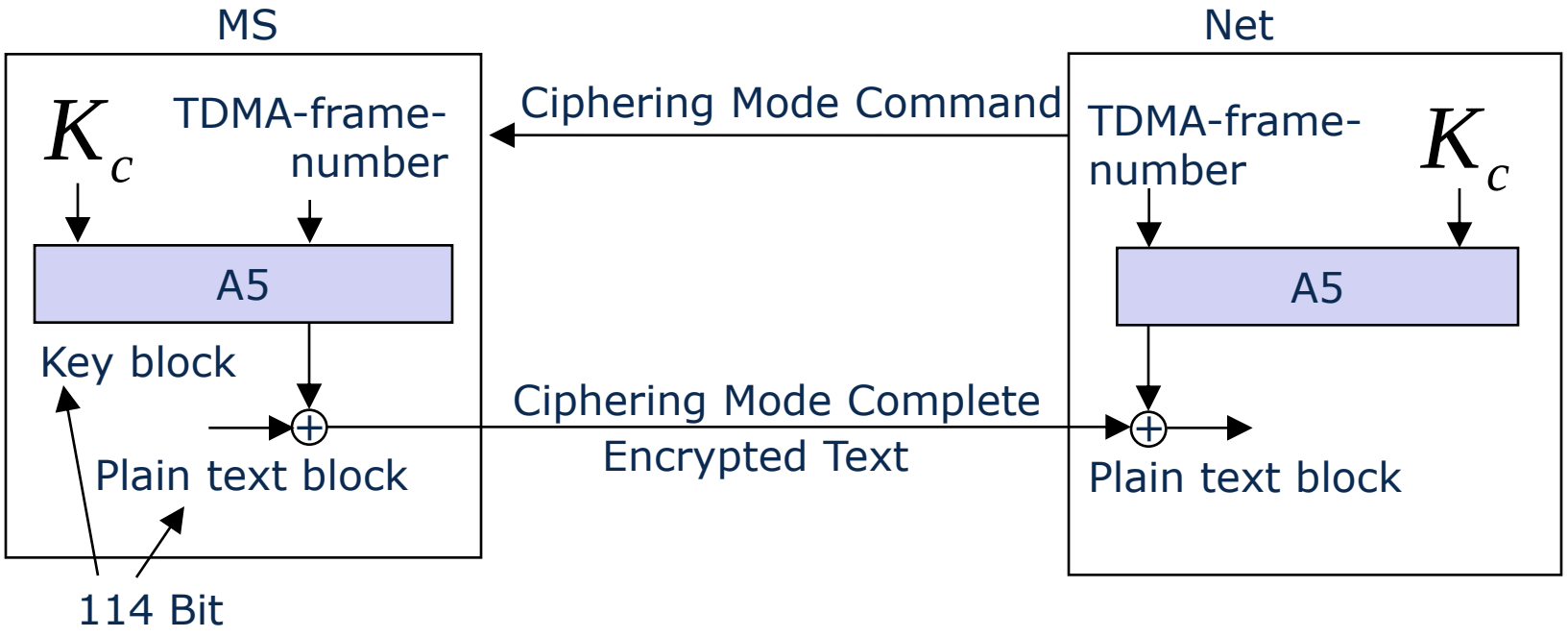
- Location Registration
- Location Update with VLR-change
- Call setup (in both directions)
- SMS (Short Message Service)

Security aspects: Session Key



- Key generation: Algorithm A8
  - Stored on SIM and in AuC
  - one way function parameterized with K_i
  - no global standard, can differ between countries
  - can be determined by network operator
  - Interfaces are standardized

Security aspects: Encryption



- Data encryption with algorithm A5:
  - stored in the Mobile Station
  - standardized in Europe and world wide
  - enhancement: A5/3 with improved security and 128 Bit key length

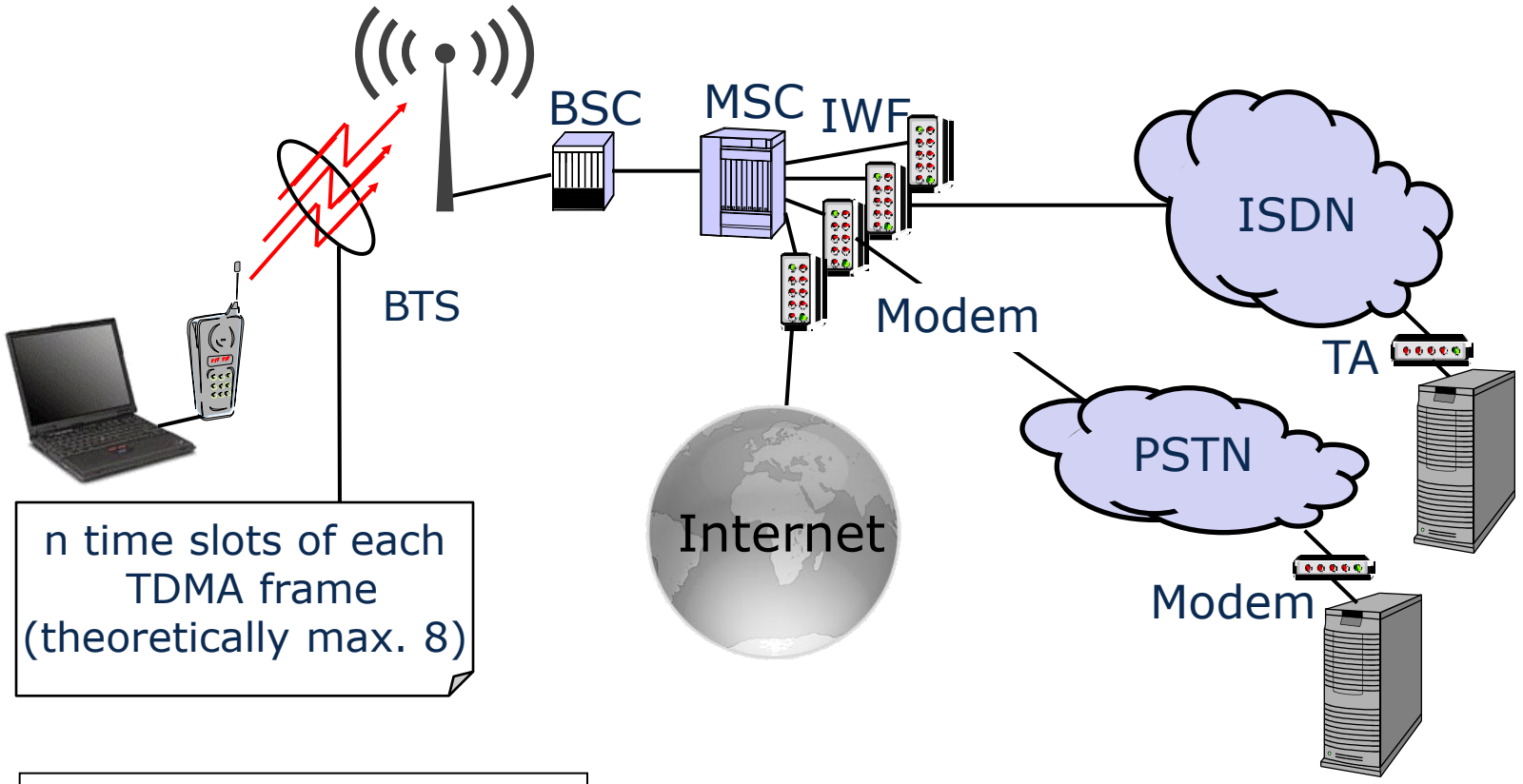
GSM-Security: assessment

- low key length K_i with max. 128 Bit (could be hacked by using Brute Force Attack in less than an hour using a regular computers as documented recently again)
- key generation and -administration not controlled by the participants (symmetric: network operator knows all keys)
- cryptographic methods secret, so they were not „well examined“ (but A5/3 and other enhancements open now)
- no mutual authentication; attacker can pretend a GSM-Net
- no end-to-end encryption or end-to-end authentication

HSCSD: High Speed Circuit Switched Data

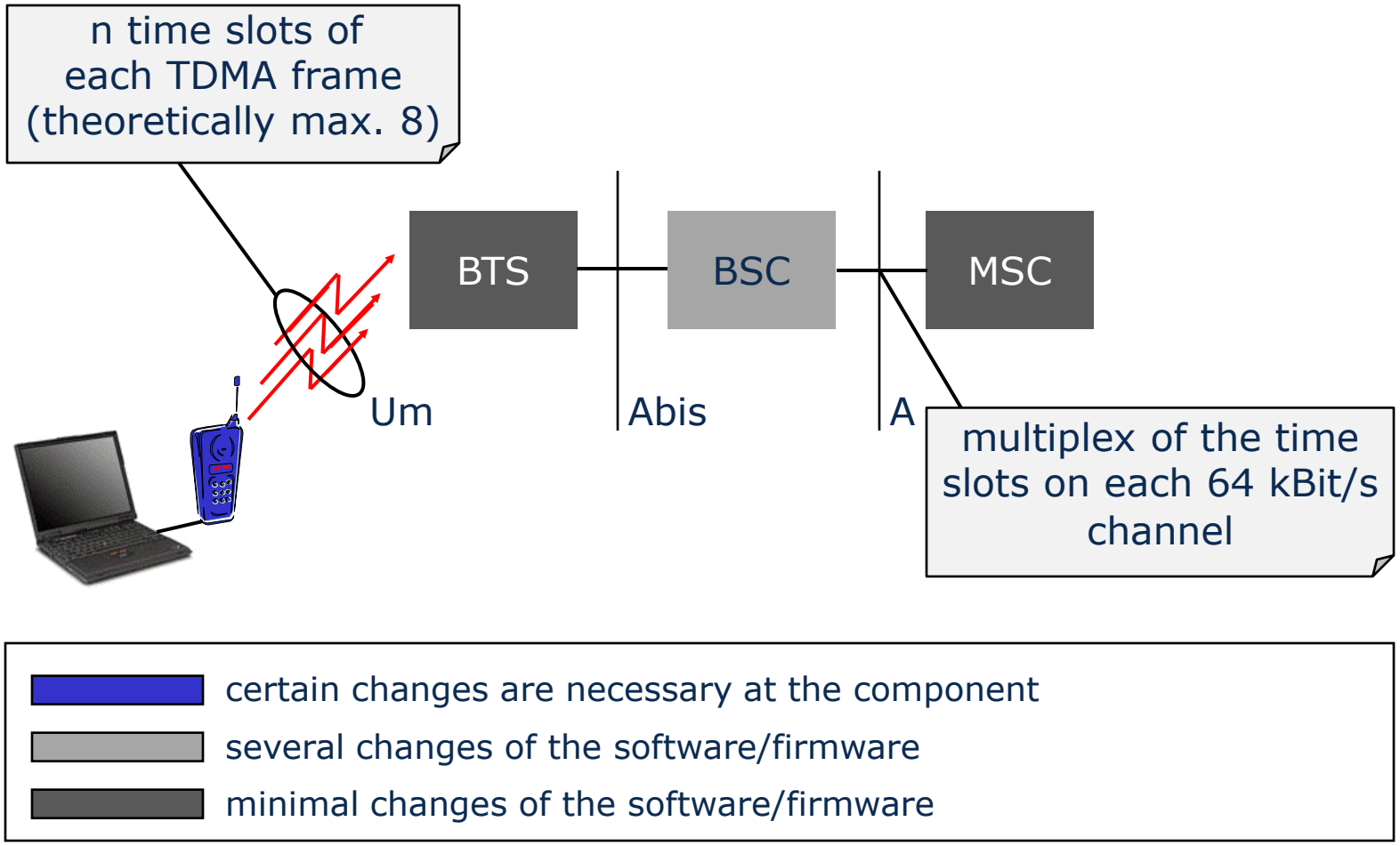
- GSM extension for higher data rates
- parallel usage of several time slots (TS) of one frequency on U_m (air interface)
- channel bundling with asymmetric transmission
  (1 TS Uplink / 3 TS or 4 TS Downlink)
- Data rates up to 4 * 14,4 kbit/s = 57,6 kbit/s
  (theoretically 8 time slots, but limited bundling in practice)

HSCSD: structure

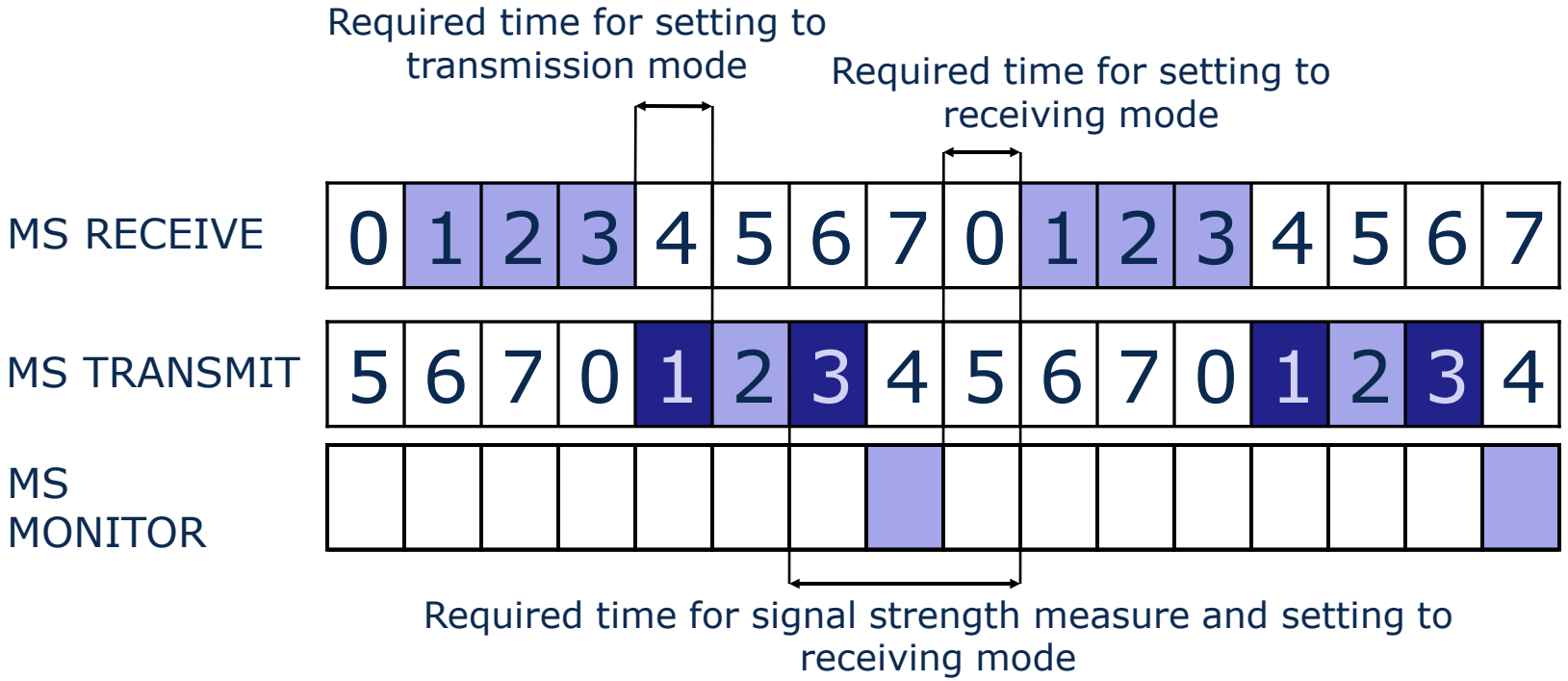


IWF - Inter Working Function
TA - Terminal Adapter

HSCSD: changes



HSCSD radio interface



- parallel usage of several time slots limited to one frequency, in half-duplex mode due to technical limitations of the end devices
- Cost factor limits number of used TS to (2+2) or (1+3, uplink, downlink); (1+4) with improved timing

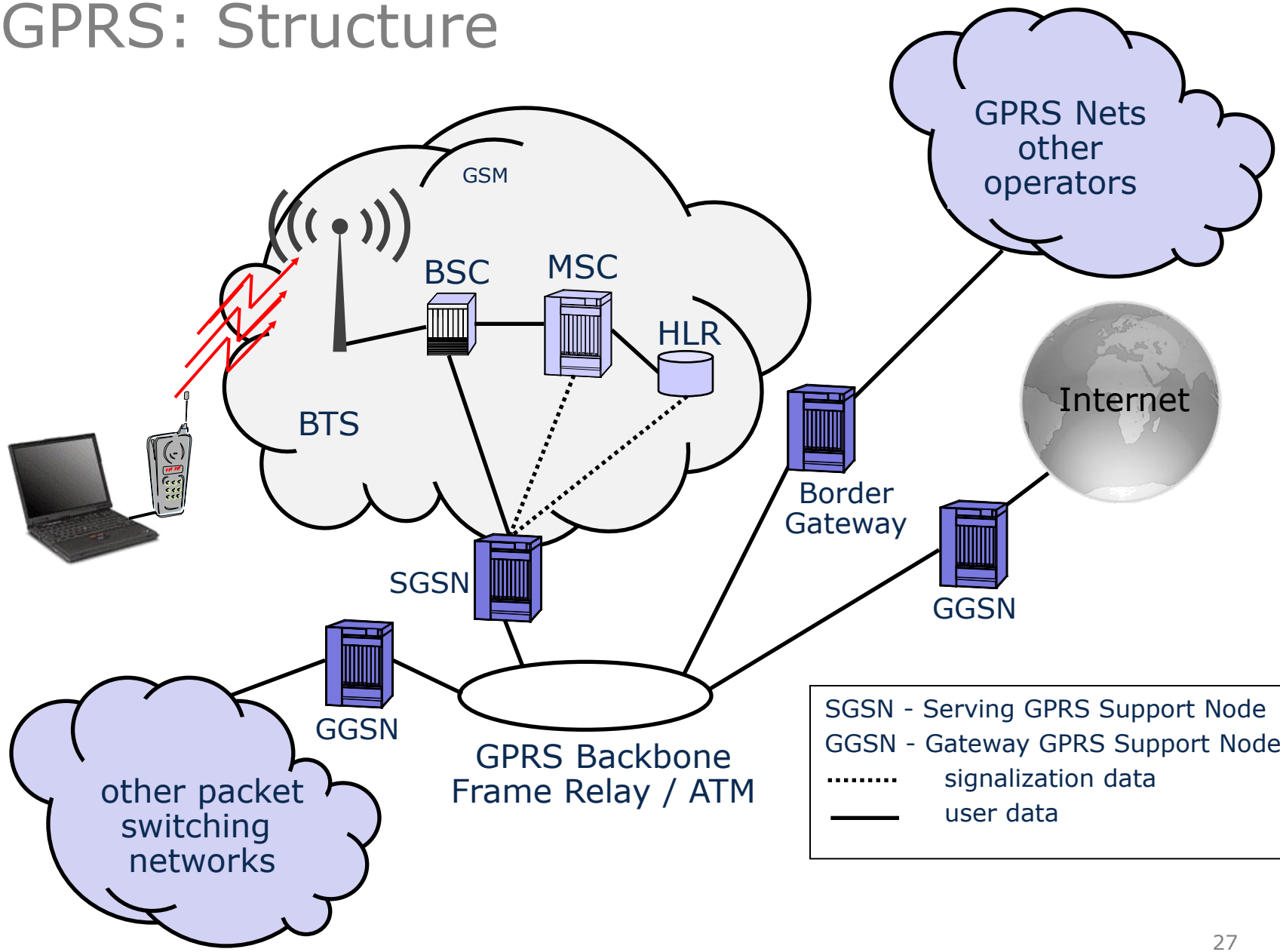
Assessment of HSCSD

+ existing network structure and accounting model maintained; only small changes were necessary
+ HSCSD is still circuit switched
  + has defined QoS-settings (data rate, delay)
  – one logical channel will be established on all interfaces for the time of the connection (inefficient)
  – badly suited for burst-like traffic (Internet) or Flat Rate billing (Logistics)
  – Only limited international acceptance (Roaming!)
- also uses more resources on the radio interface
  – problems with handover into a new cell

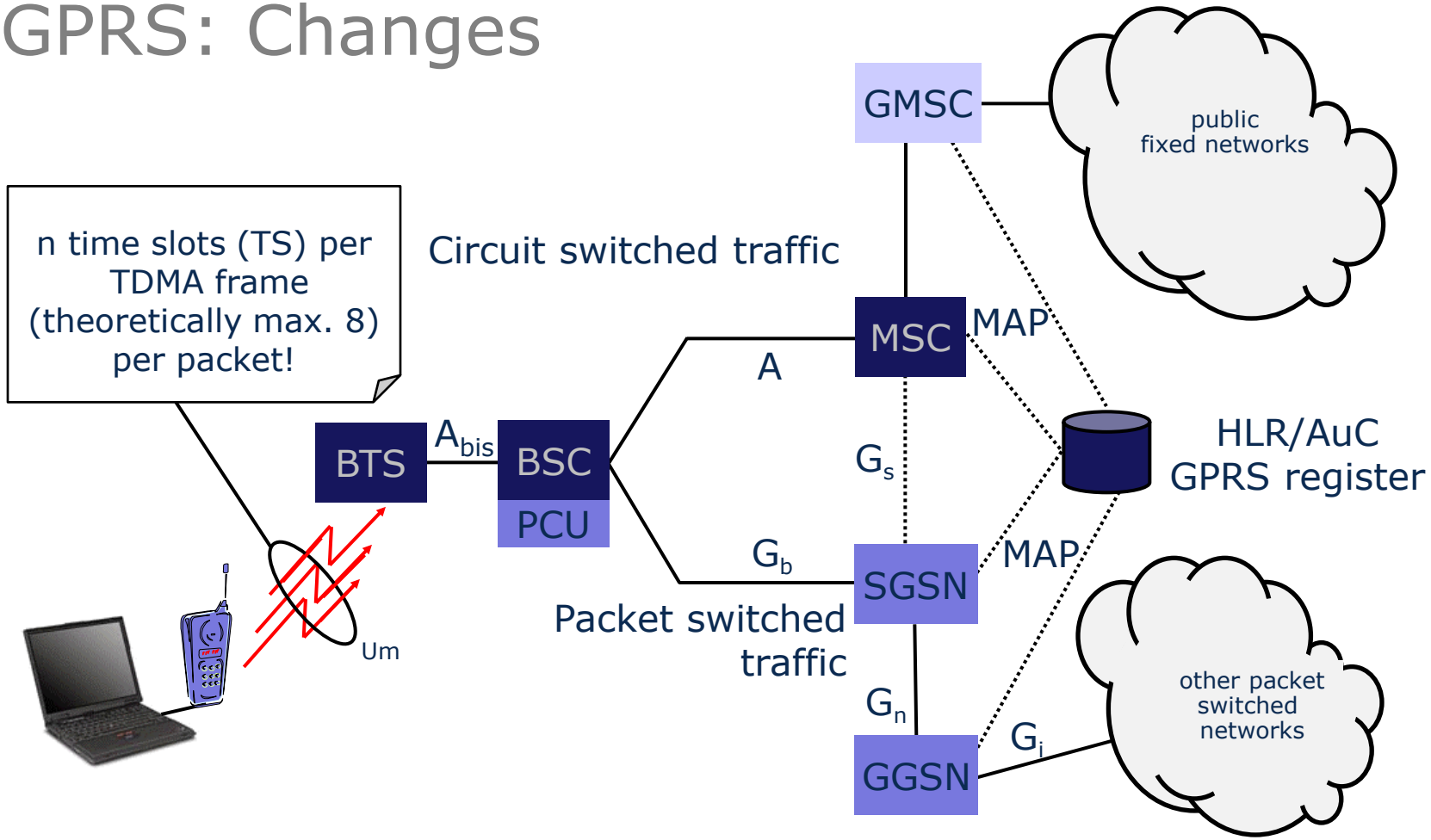
GPRS: General Packet Radio Service

- GSM extension based on packet switching service (end-to-end) and channel bundling based on multiple time slots
- Data rates up to 171,2 kbit/s (theoretical) – in practice however similar to HSCSD
- Effective and flexible administration of the radio interface; adaptive channel encoding
- Internetworking with IP networks standardized
- Dynamic sharing of resources with „classical“ GSM speech services
- Advantage: Billing and Accounting according to data volume

GPRS: Structure



GPRS: Changes



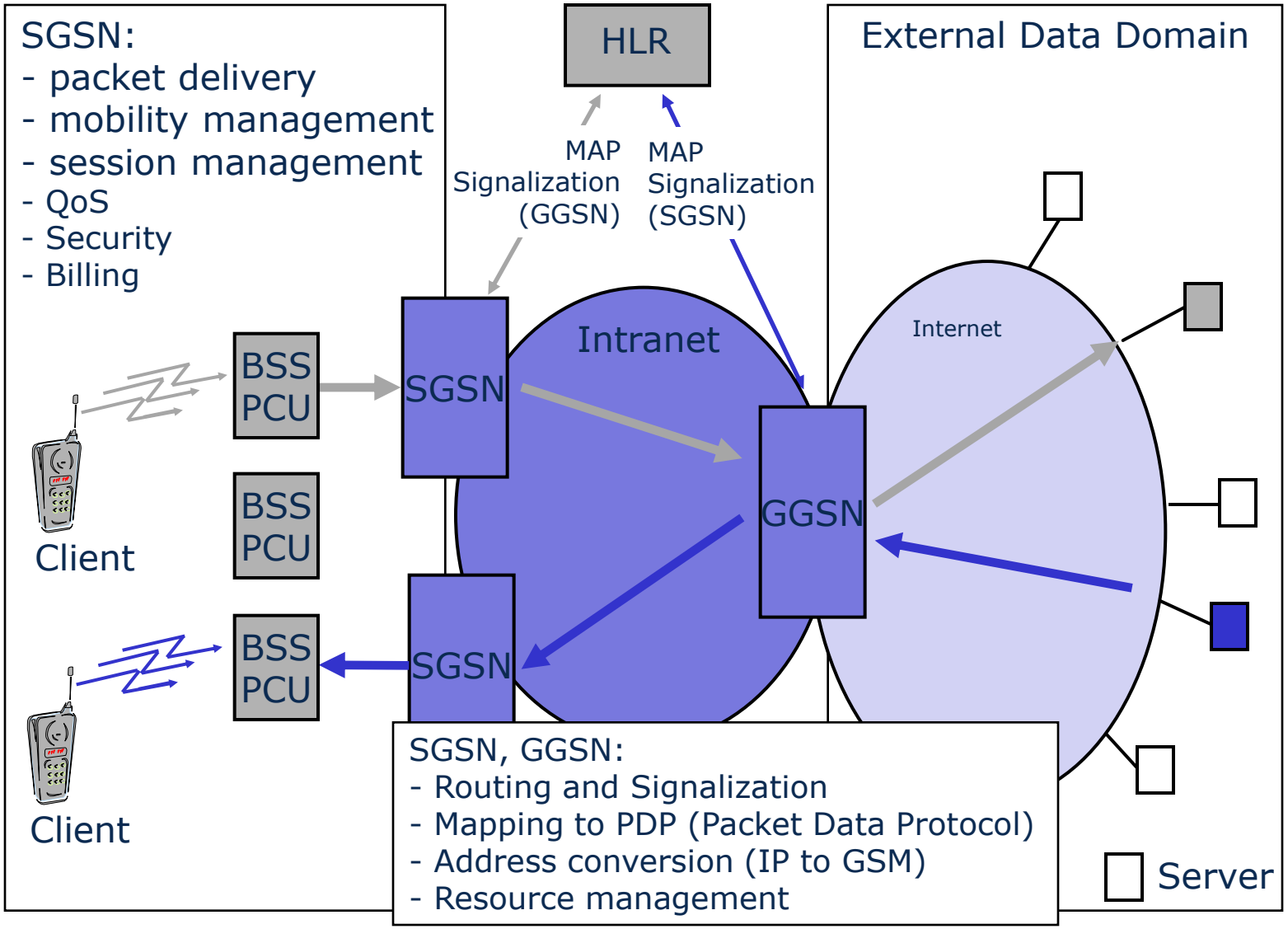
modified network components

new components or extensively modified components

Existing components

PCU - Packet Control Unit

Tasks: SGSN, GGSN



Quality of Service

- QoS profile agrees service parameters inside the whole network for the duration of PDP (Packet Data Protocol) context (session):
  - temporary address (IP) for mobile station
  - tunneling information, among others GGSN, which is used for access to corresponding packet switched network
  - type of the connection
  - QoS profile
- QoS profile commits:
  - precedence class, priority against other services (high, normal, low)
  - packet delay class, times valid for traffic inside the GPRS network
  - reliability class
  - peak throughput class
  - mean throughput class

Quality of Service: Examples

Packet delay classes

	Size: 128 octets		Size: 1024 octets	
Class	Mean Delay	95% Delay	Mean Delay	95% Delay
1 (predicitive)	< 0,5 s	< 1,5 s	< 2 s	< 7 s
2 (predicitive)	< 5 s	< 25 s	< 15 s	< 75 s
3 (predicitive)	< 50 s	< 250 s	< 75 s	< 375 s
4 (best effort)	Best effort			

Error classes

	Probability for			
Class	Lost packet	Duplicated p.	Out of Sequence p.	Corrupted p.
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

GPRS data rates

Coding	# of timeslots							
Scheme	1	2	3	4	5	6	7	8
CS-1	9,05	18,1	27,15	36,2	45,25	54,3	63,35	72,4
CS-2	13,4	26,8	40,2	53,6	67	80,4	93,8	107,2
CS-3	15,6	31,2	46,8	62,4	78	93,6	109,2	124,8
CS-4	21,4	42,8	64,2	85,6	107	128,4	149,8	171,2

(only CS-1 and CS-2 comprise reasonable error correction and are relevant in practice)

Assessment of GPRS

+ An up to four times higher data rate in comparison to ordinary GSM data services
+ better resource management through packet switched service
+ „always on” data service (email, etc.)
+ GPRS is a more suitable carrier for the mobile Internet

- IP-derivate, no true service guarantees (QoS)
- GPRS does not provide the data rates that advertising has sometimes promised, therefore most operators migrated to UMTS and LTE where possible, e.g. in urban areas

Some further readings

- ETSI standards (GSM etc.) in general:
  www.etsi.org
- GSM, HSCSD, GPRS: good overviews on
  www.wikipedia.org
- GPRS tutorial:
  www.telecomspace.com/datatech-gprs.html
- SMS tutorial:
  www.developershome.com/sms/