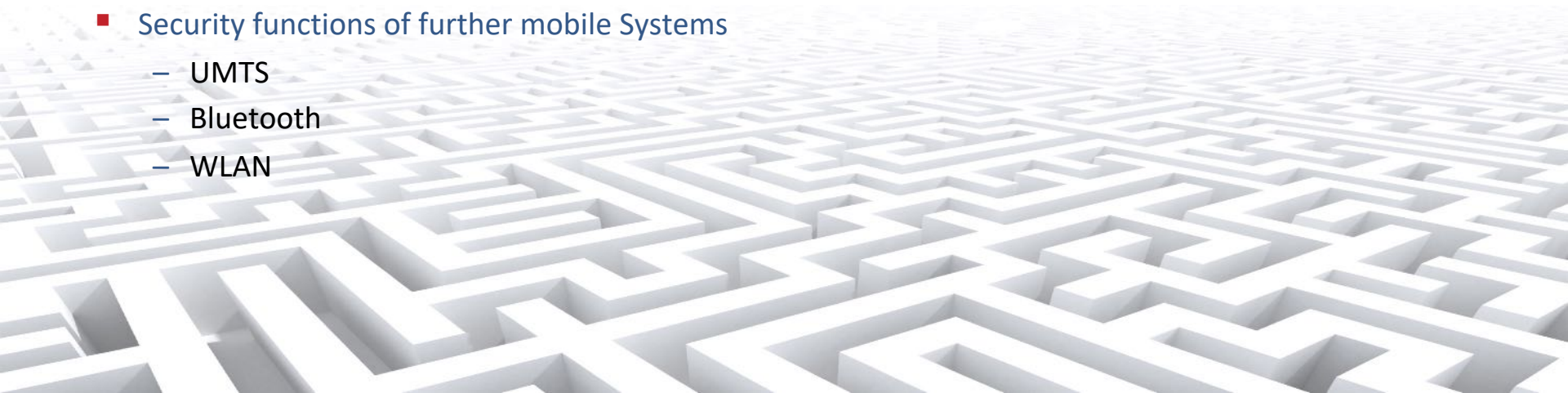
Mobile Security

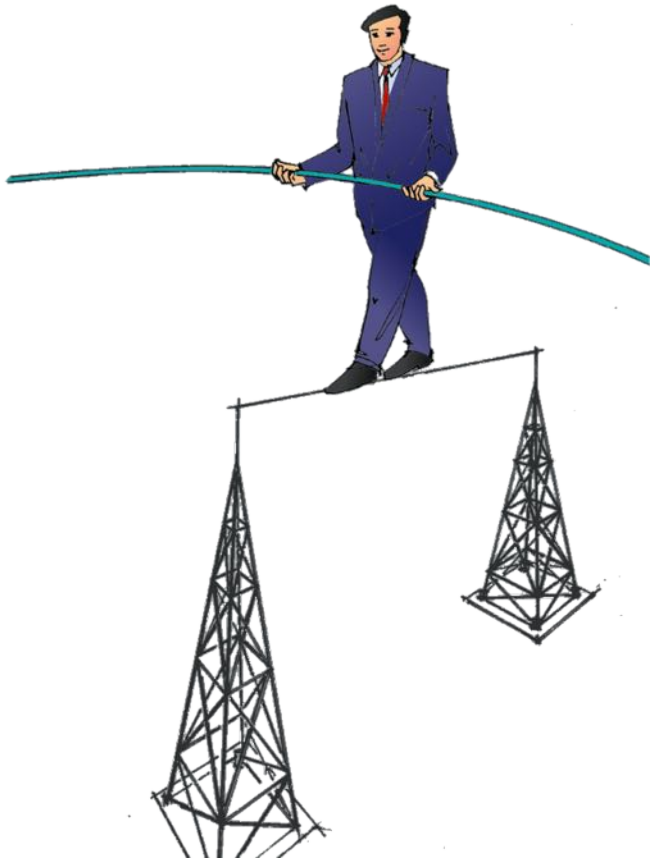
Contents

- Introduction
- Security functions of GSM
  - Basics and architecture of GSM
  - Security functions
  - Mobility management functions
  - Location based systems
  - Call management
- Security functions of further mobile Systems
  - UMTS
  - Bluetooth
  - WLAN



Mobile network communication vs. fixed networks

- Users are moving / roaming
- On air interface:
  - Limited bandwidth
  - Errors (bit failures, burst errors)
  - Communication breaks (lost connectivity)
- New threads
  - Sniffing / eavesdropping of wireless communication
  - Location finding (direction-finding, sense-finding)



Sensors make new Apps possible

- Sensors in mobile devices
  - GPS, Location
  - WiFi, NFC
  - Camera, Microphone
  - Motion Sensor (Gyro)
  - Compass
  - Temperature
  - Phonebook
  - Internal Storage
  - External Storage
  - Screen distance
  - Fingerprint Sensor
- Adapters for more sensors
  - Personal: heart rate monitors
  - Cars and Houses: CAN bus adapters, smart meter, heater, alarm system

http://blog.digifit.com/wp-content/uploads/2011/02/

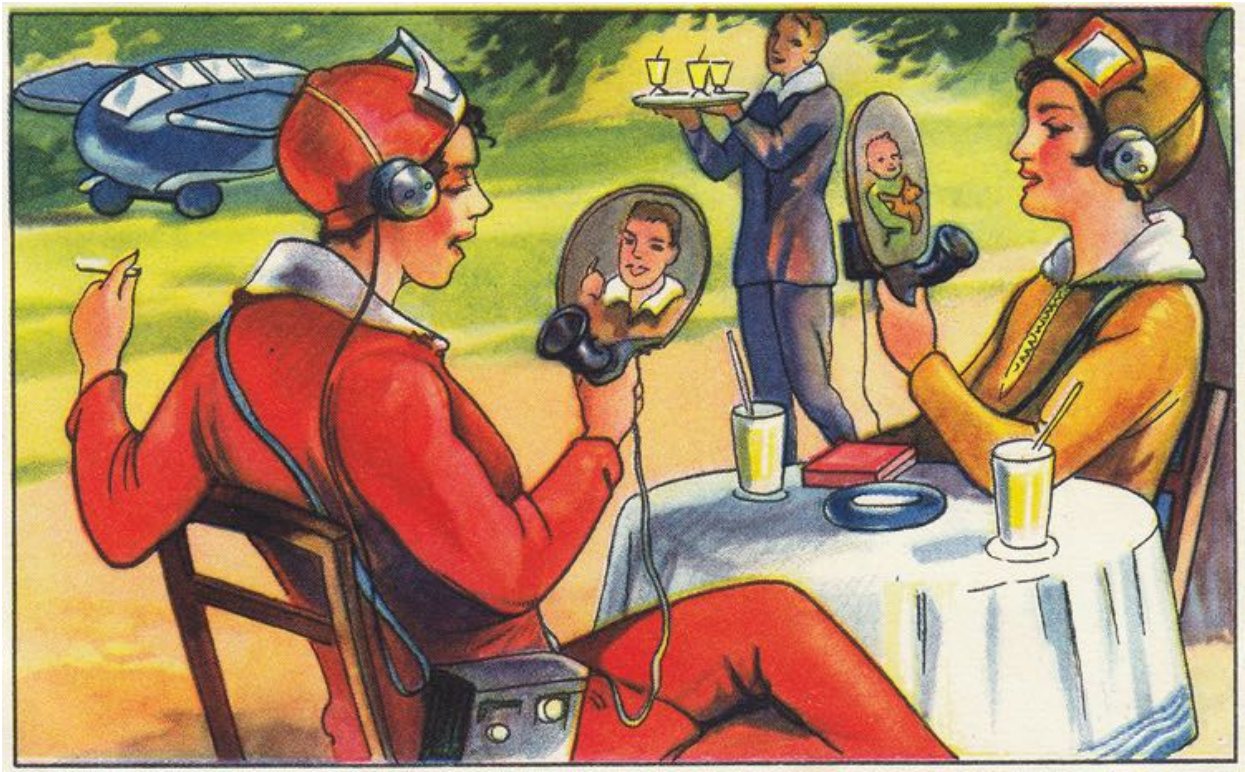
Sensors make new Apps possible

developer.android.com

Sensors in mobile devices	Explicit	Implicit permissions
– GPS, Location	x	
– WiFi, NFC	x	
– Camera, Microphone	x	
– Motion Sensor (Gyro)		x
– Compass		x
– Temperature		
– Phonebook	x	
– Internal Storage		x
– External Storage	x	
– Screen distance		x
– Fingerprint Sensor	x	

- All permissions to be found at
  - https://developer.android.com/reference/android/Manifest.permission.html

Echte Wagner Margarine, ca. 1930



Bildquellen: http://klausbuergle.de/sammelalben_zf.htm
https://monoskop.org/File:Echte_Wagner_Margarine_3_Serie_12_Zukunftsfantasien_Bild_4_c1930.jpg

Mobile communication – Classification

1. Types of Mobility

- Terminal Mobility:
  - Example: Mobile Phone
    - Wireless communication
    - Mobile device
- Personal Mobility:
  - Example: Public Terminals
    - Mobile user
    - Location-independent address
  - Special kind of personal mobility: Session Mobility:
    - Session Freezing and reactivation in other location and/or device

2. Wave lengths
   - Radio [waves] (f = 100 MHz up to several GHz)
   - Light [waves] (infrared)
   - Sonar [waves] (e.g. acoustic coupler)

3. Cell sizes
   - Pico cells d < 100 m
   - Micro cells d < 1 km
   - Macro cells d < 20 km
   - Hyper cells d < 60 km
   - Overlay cells d < 400 km

Further classifications
   - Point-to-point communication, Broadcast (paging services)
   - Analogue, Digital systems
   - Simplex, Duplex communication channels

Examples for mobile Systems

- Speech communication = mass market
  - 1. Generation: analogue: C-Netz, Cordless Telephone, AMPS
  - 2. Generation: digital: GSM, DCS-1800, DECT
  - 3. Generation: service integration: UMTS/IMT-2000/FPLMTS
  - 4. Generation: LTE

- Satellite services
  - Iridium, Inmarsat, Globalstar, Odyssey
  - GPS (Global Positioning System), Galileo (European satellite navigation system), GLONASS

- Internet (Mobile IP)

Security deficits of existing mobile networks

- Example of security demands: Cooke, Brewster (1992)
  - protection of user data
  - protection of signaling information, incl. location
  - user authentication, equipment verification
  - fraud prevention (correct billing)

- General security demands
  - Confidentiality
  - Integrity
  - Availability

- Mobile network cannot be considered trustworthy

Attacker model

The attacker model defines the maximum strength of an adversary regarding a specific security mechanism

- Aspects of an attacker model
  - Roles of attacker (Outsider or Insider, …)
    - combined roles also
  - Dissemination of attacker
    - Which stations or channels can be controlled?
  - Behavior of attacker
    - passive / active, observing / modificating
  - Computing power of attacker
    - unlimited: information theoretic
    - limited: complexity theoretic

Money

Time

Protection against an omnipotent attacker is impossible.

Attacker model (concrete)

- Outsiders
  - Passive attacks only (confidentiality)
- Insiders
  - Passive and active data modification attacks (integrity)
- Insiders and outsiders
  - Denial of Service attacks on air interface

- Mobile device
  - Trustwothy
- Network components
  - Safe against outsiders, but not against insiders
- Air interface
  - Location-finding (insiders and outsiders)

Global System for Mobile Communication (GSM)

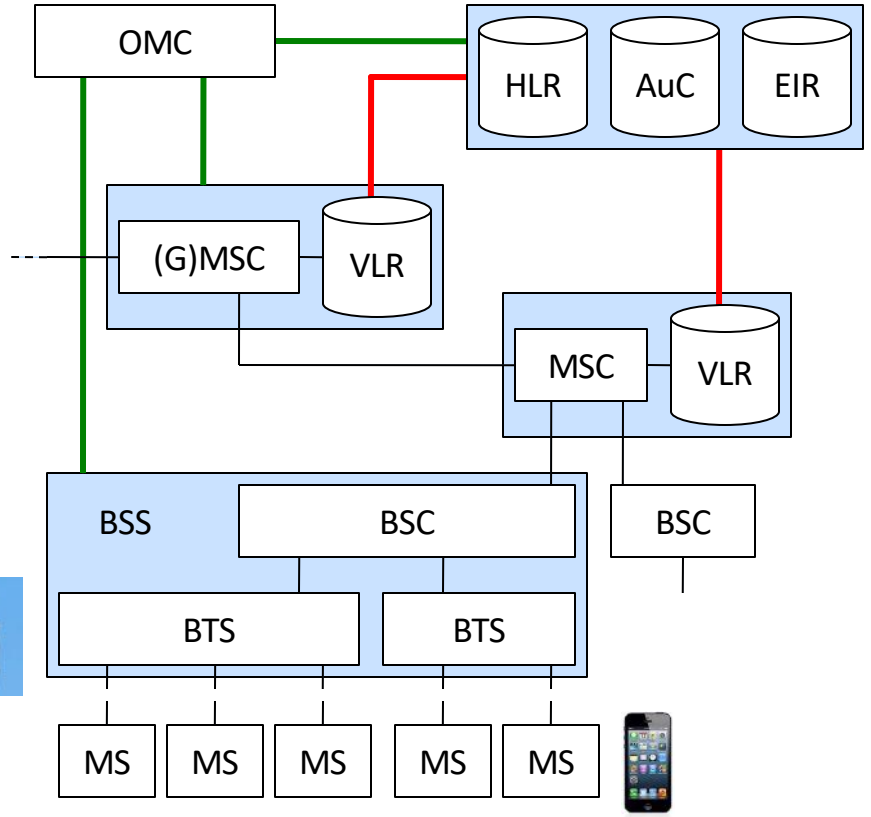
- Key features of Global System for Mobile Communication
  - Very high international mobility
  - Worldwide caller ID
  - High geographic coverage
  - High user capacity
  - High speech quality
  - Advanced error correction mechanisms
  - Advanced resource allocation strategies (e.g. FDMA, OACSU)
  - Priority emergency call service
  - Built-in Security functions
    1. Subscriber Identity Module (SIM, smart card)
    2. Authentication (Mobile station → network)
    3. Pseudonymization of users on the air interface
    4. Link encryption on the air interface

GSM Timeline:
1989 Group Spécial Mobile (ETSI)
1990 GSM Standard
1991 GSM Network in Operation
2000 Transition to 3rd Generation

Architecture of GSM

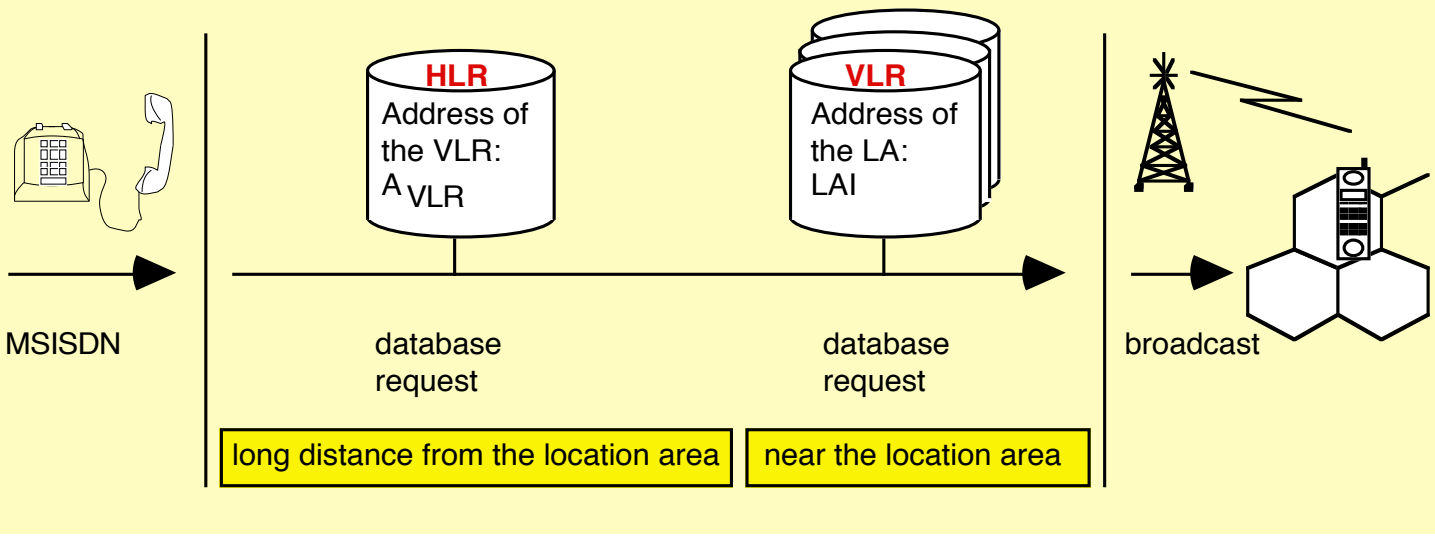
Network Management
Call Management
Database Management

OMC: Operation and Maintainance Center
HLR: Home Location Register
AuC: Authentication Center
EIR: Equipment Identity Register
MSC: Mobile Switching Center
GMSC: Gateway MSC to fixed network
VLR: Visitor Location Register
BSS: Base Station Subsystem
BSC: Base Station Controller
BTS: Base Transceiver Station
MS : Mobile Station
LA : Location Area



Location Management in GSM

- GSM (Global System for Mobile Communication)
  - Distributed storage at location registers
    - Home Location Register (HLR)
    - Visitor Location Register (VLR)
  - Network operator has global view on location information
- Tracking of mobile users is possible

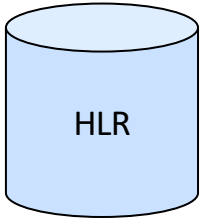


Security deficits of existing mobile networks

- Example of security demands: Cooke, Brewster, 1992
  - protection of user data
  - protection of signaling information, incl. location
  - user authentication, equipment verification
  - fraud prevention (correct billing)
- Security deficits of GSM (selection)
  - Only symmetric cryptography (algorithms no officially published)
  - Weak protection of locations (against outsiders)
  - No protection against insider attacks (location, message content)
  - No end-to-end services (authentication, encryption)
- Summary
  - GSM provides protection against external attacks only.
  - »…the designers of GSM did not aim at a level of security much higher than that of the fixed trunk network.« Mouly, Pautet, 1992

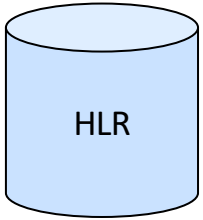
Data bases (registers) in GSM

- Home Location Register (HLR): Semi permanent data
  - IMSI (International Mobile Subscriber Identity): max. 15 numbers
    - Mobile Country Code (MCC, 262) +
      Mobile Network Code (MNC, 01/02) +
      Mobile Subscriber Identification Number (MSIN)
  - MSISDN (Mobile Subscriber International ISDN Number): 15 numbers
    - Country Code (CC, 49) +
      National Destination Code (NDC, 171/172) +
      HLR Number + Subscriber Number (SN)
    - Number porting: translation table
  - Subscriber data (name, address, account etc.)
  - Service profile (priorities, call forwarding, service restrictions, e.g. roaming restrictions)



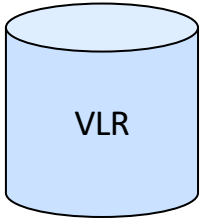
Data bases (registers) in GSM

- Home Location Register (HLR): Temporary data
  - VLR address, MSC address
  - MSRN (Mobile Subscriber Roaming Number)
    - CC + NDC + VLR number
      VLR number = MSC number + SN
  - Authentication Set, consists of several Authentication Triplets:
    - RAND (128 Bit),
    - SRES (32 Bit) ,
    - Kc (64 Bit)
  - Billing data later on transferred to Billing Centres



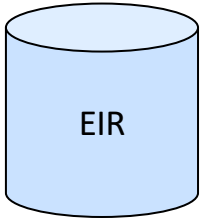
Data bases (registers) in GSM

- Visitor Location Register (VLR)
  - TMSI (Temporary Mobile Subscriber Identity)
  - LAI (Location Area Identification)
  - MSRN
  - IMSI, MSISDN
  - MSC-address, HLR-address
  - Copy of Service profile
  - Billing data later on transferred to Billing Centres



Data bases (registers) in GSM

- Equipment Identity Register (EIR)
  - IMEI (International Mobile Station Equipment Identity): 15 numbers = serial number of mobile station
    - white-lists (valid mobiles, shortened IMEI)
    - grey-lists (mobiles with failures are observed)
    - black-lists (blocked, stolen mobiles)
  - USSD (Unstructured Supplementary Service Data) code for showing IMEI: *#06#

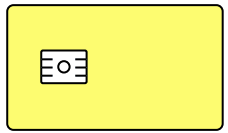


Security functions of GSM

- Overview
  1. Subscriber Identity Module (SIM, smart card)
     - Admission control and crypto algorithms
  2. Authentication (SIM $\rightarrow$ network)
     - Challenge-Response-Authentication (A3)
  3. Pseudonymization of users on the air interface
     - Temporary Mobile Subscriber Identity (TMSI)
  4. Link encryption on the air interface
     - Generation of session key: A8
     - Encryption: A5

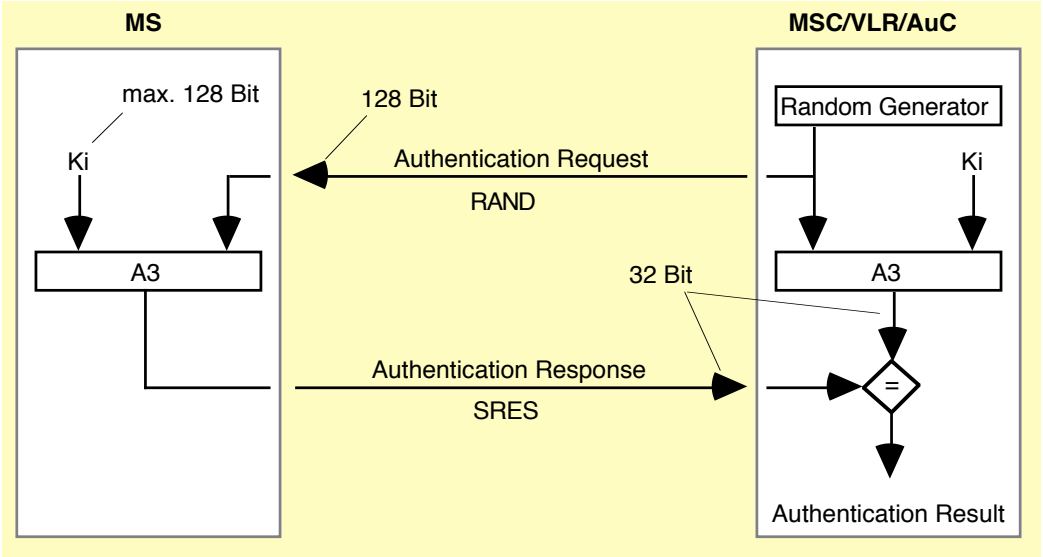
Subscriber Identity Module (SIM)

- Specialized smart card
  - Data stored on SIM:
    - IMSI (International Mobile Suscriber Identity)
    - individual symmetric key Ki (Shared Secret Key)
    - PIN (Personal Identification Number): admission control
    - TMSI (Temporary Mobile Subscriber Identity)
    - LAI (Location Area Identification)
  - Cryptographic algorithms:
    - A3: Challenge-Response-Authentication
    - A8: Session Key generation: Kc



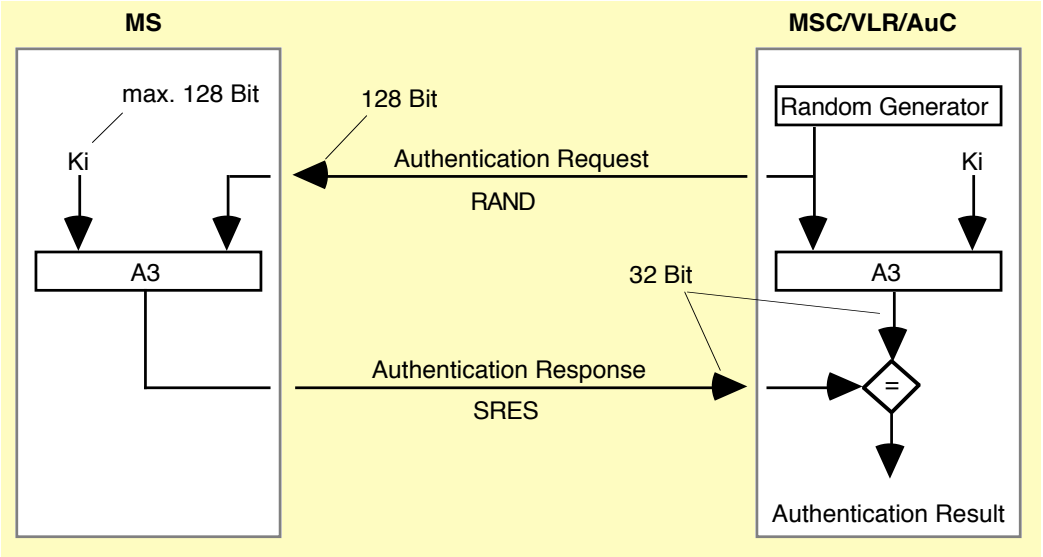
Challenge-Response-Authentication

- When initialized by the mobile network?
  - Location Registration
  - Location Update when changing the VLR
  - Call Setup (both directions)
  - Short Message Service



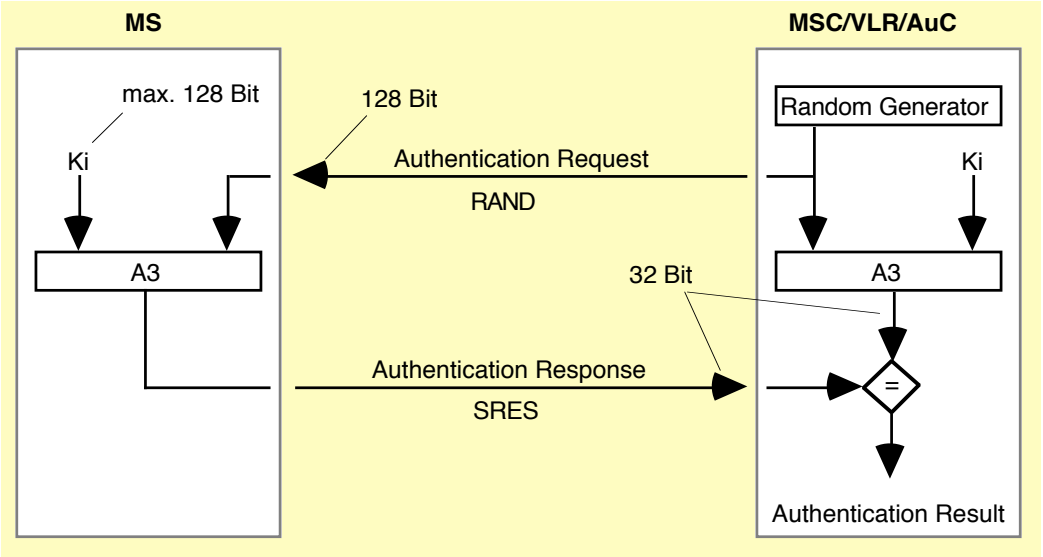
- Algorithm A3
  - Implemented on SIM card and in Authentication Center (AuC)
  - Cryptographic one way function A3:

    SRES' = A3(Ki, RAND) (Ki: individual user key)
  - Interfaces are standardized, cryptographic algorithm not



Challenge-Response-Authentication

- Specific algorithm can be selected by the network operator
  - Authentication data (RAND, SRES) are requested from AuC by the visited MSC
  - visited MSC: only compares SRES == SRES'
  - visited MSC has to trust home network operator



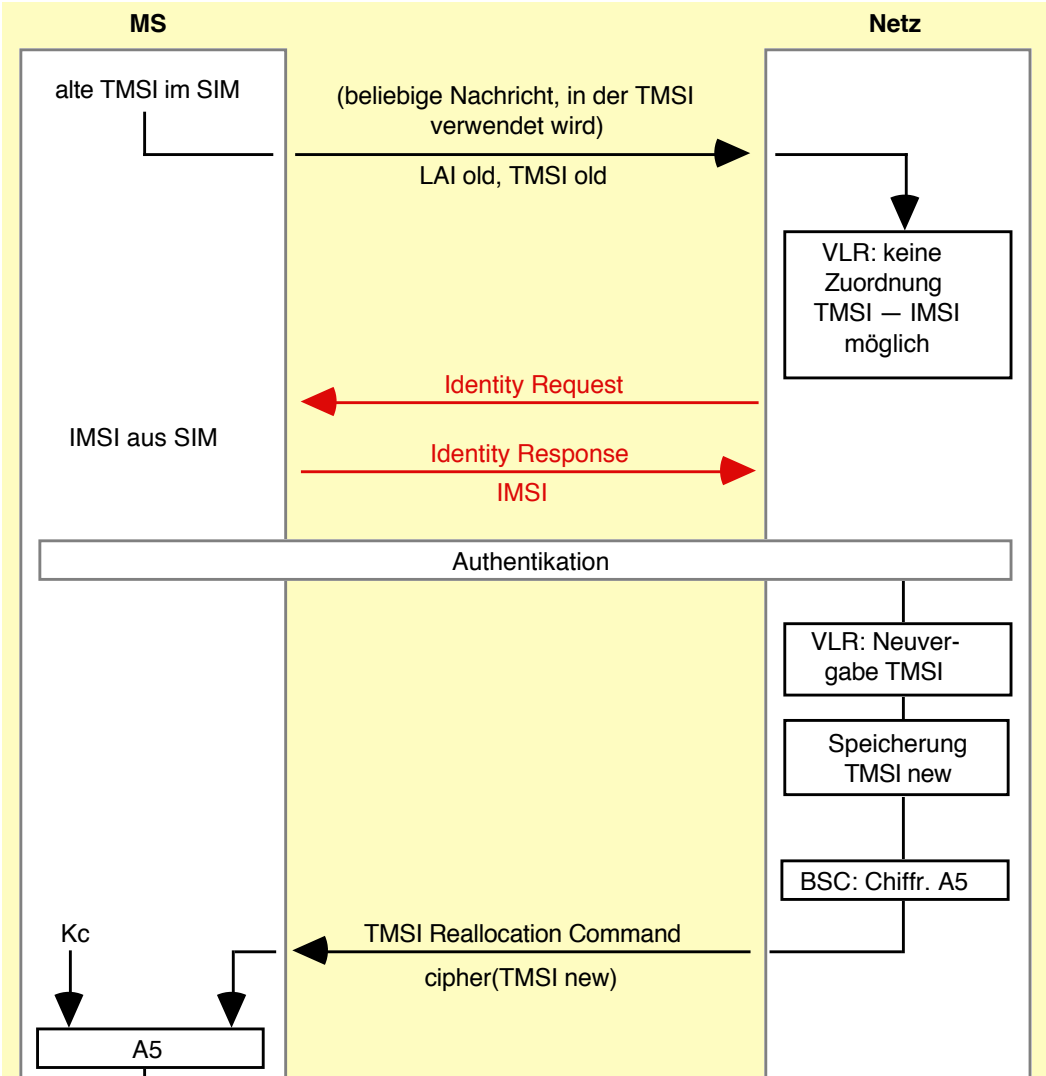
Pseudonymization on air interface

- TMSI (Temporary Mobile Subscriber Identity)
  - hides from traceability of mobile users by outsiders
  - on air interface: all (unencrypted) transactions from and to mobile user is addressed with TMSI
  - algorithm for TMSI generation is network individual (not standardized)

- Identity Request
  - first contact (home network)
  - after failure
    - IMSI is requested by serving network

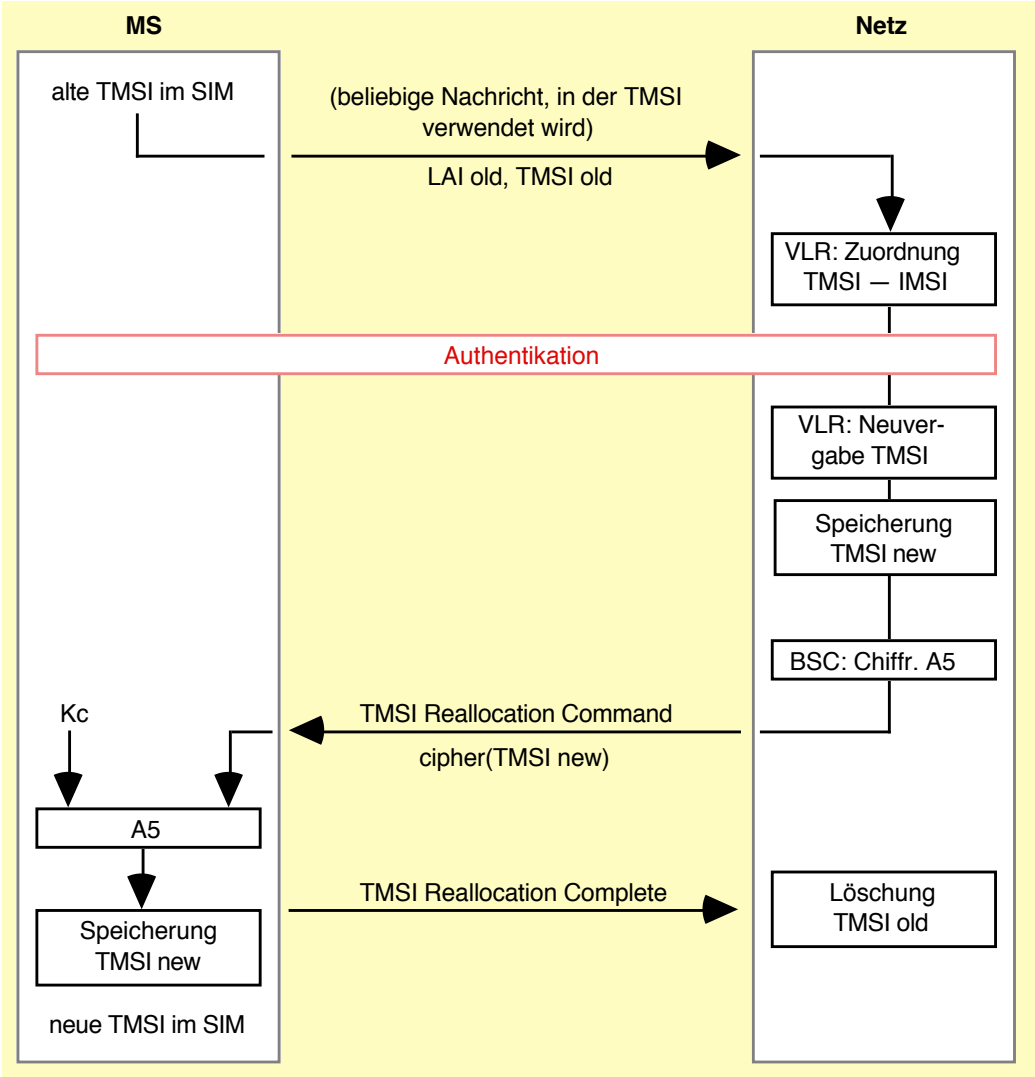
First contact
Failure

Identity Request



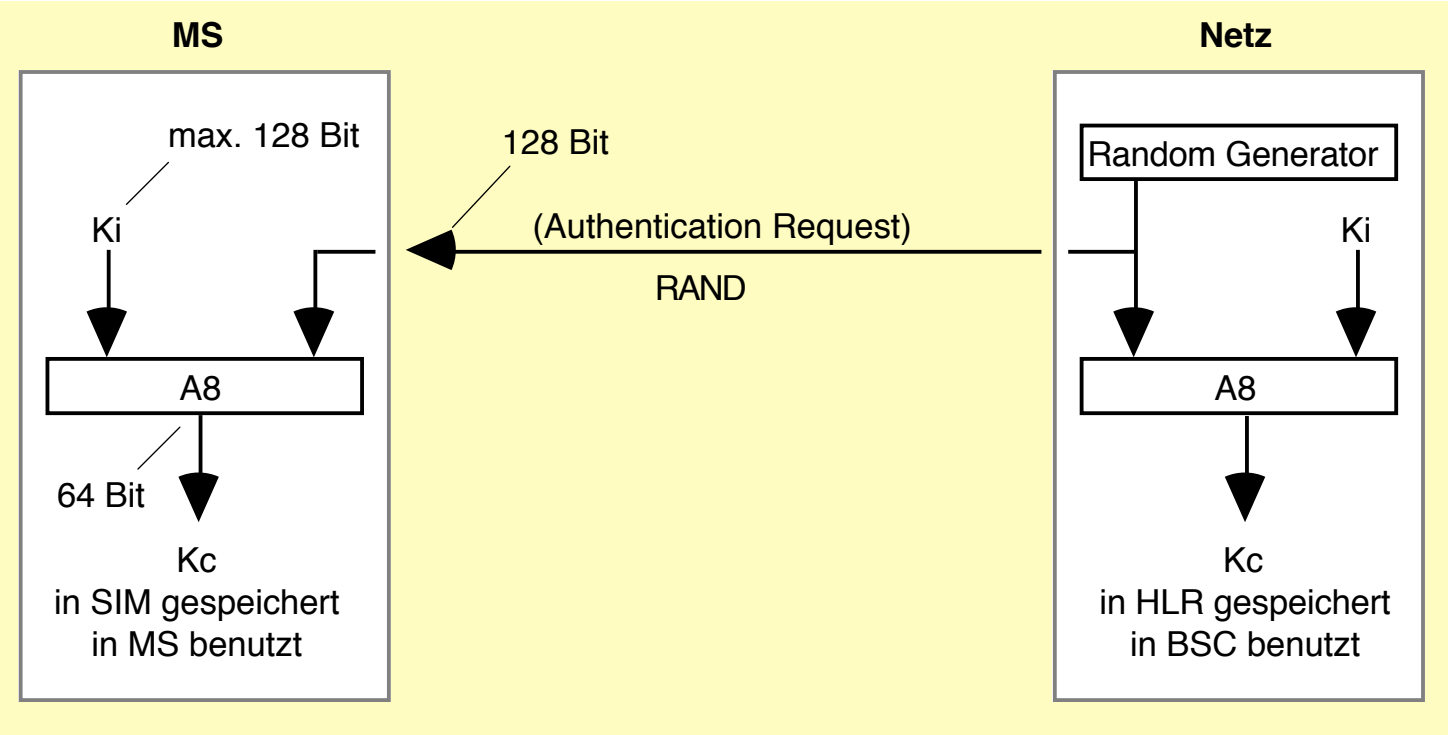
Normal case

TMSI used



Link encryption on air interface

- Session key generation: Algorithm A8

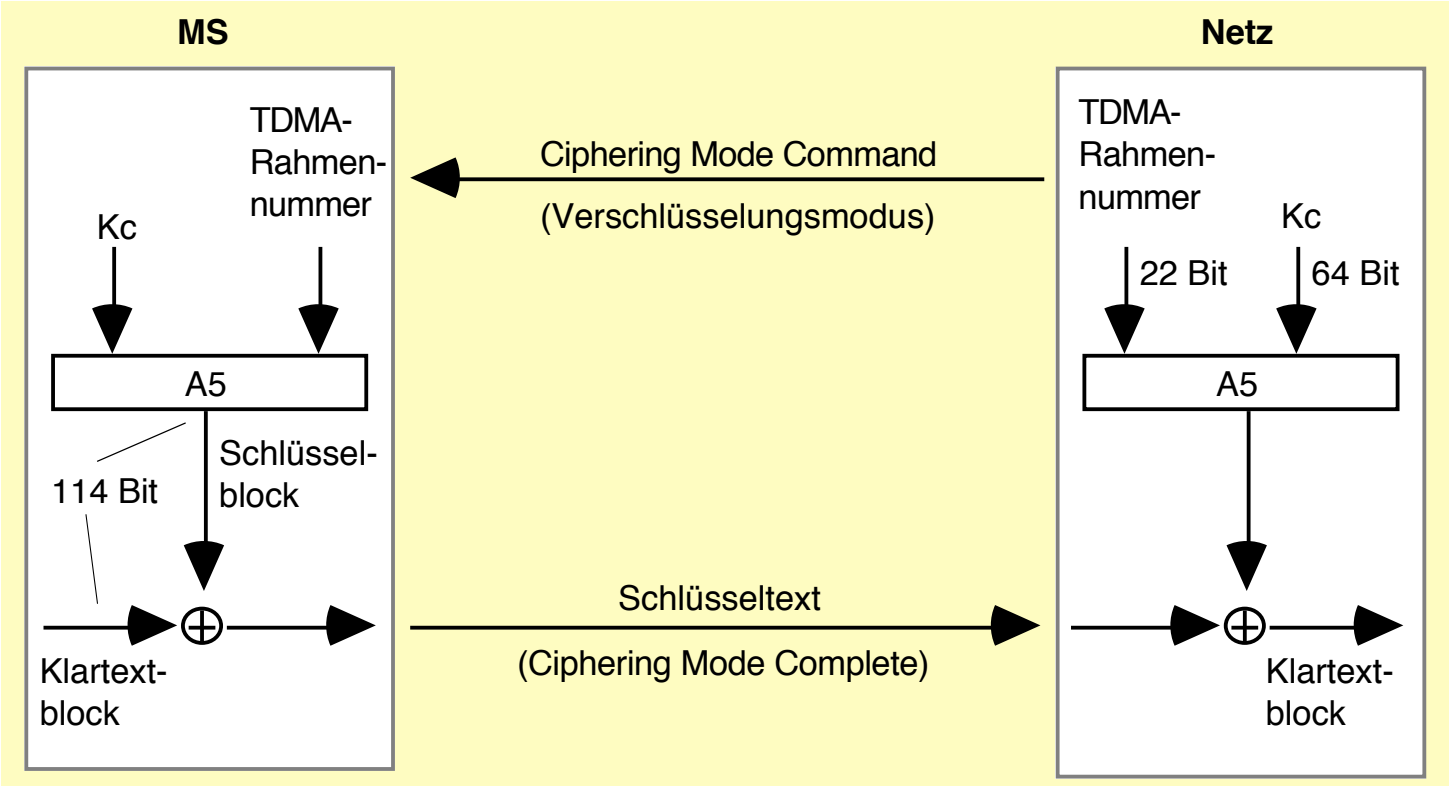


Link encryption on air interface

- Session key generation: Algorithm A8
  - implemented on SIM and in Authentication Centre (AuC)
  - cryptographic one-way function
  - interfaces are standardized
  - COMP128: well-known implementation of A3/A8

Link encryption on air interface

- Link encryption: Algorithm A5



Link encryption on air interface

- Link encryption: Algorithm A5
  - implemented in mobile station (not SIM!)
  - standardized algorithms:
    - A5 or A5/1
    - A5* or A5/2 »weak variant« of A5 — (deprecated)
    - [A5/3 based on KASUMI (UMTS) with length(Kc)=64 bit]
    - [A5/4 same as A5/3 with length(Kc)=128 bit]

- Security of A5/1 and A5/2
  - Cipher is based on non-linear shift registers
  - Algorithms considered insecure today
    - A5/1 broken by Nohl 2010
      - Attack uses ≈ 2 TByte of pre-calculated rainbow tables

- Ciphering Mode Command (GSM 04.08)

8	7	6	5	4	3	2	1	
TI flag	TI value			Protocol discriminator				octet 1
0	N(SD)	Message type						octet 2
Ciphering Mode Command								octet 3

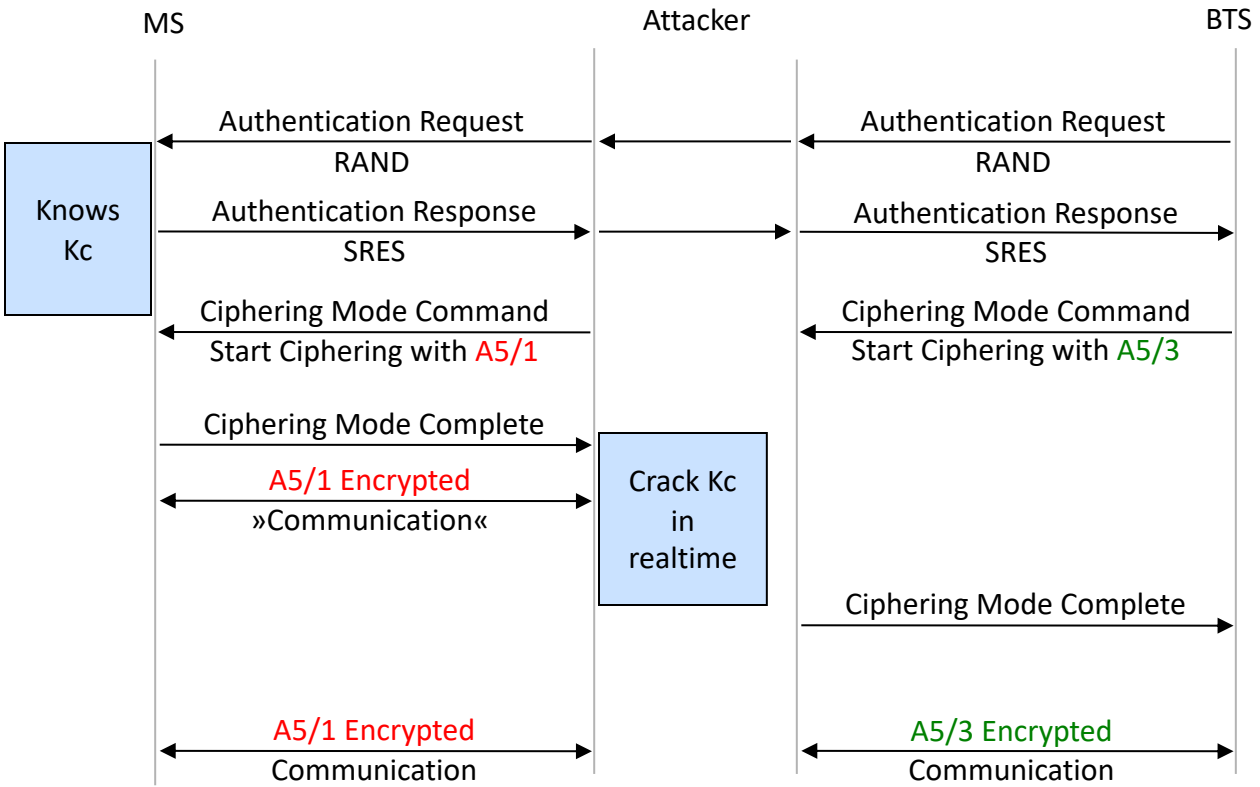
- Cipher mode setting information element

8	7	6	5	4	3	2	1
1	0	0	1	0	0	0	SC=0
	Ciph mode set IEI			Spare	Spare	Spare	SC=1

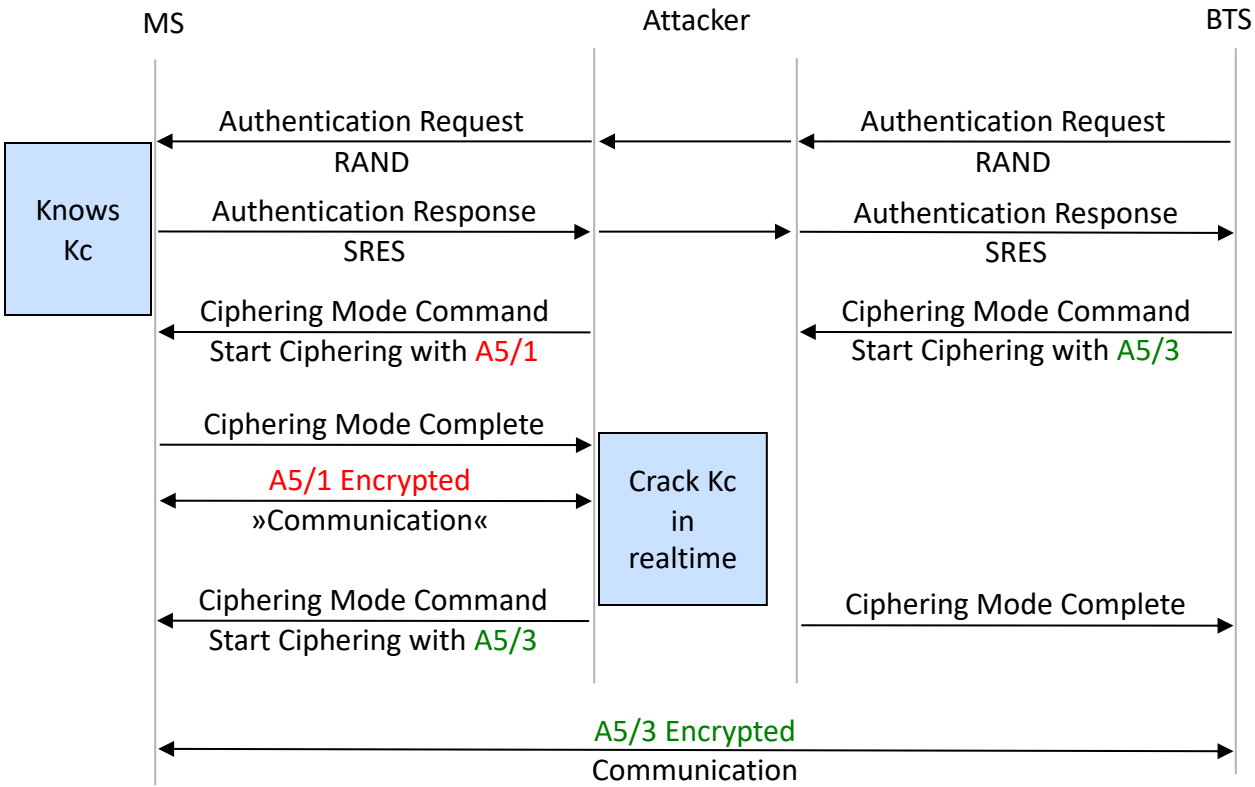
SC=0: No ciphering

SC=1: Start ciphering

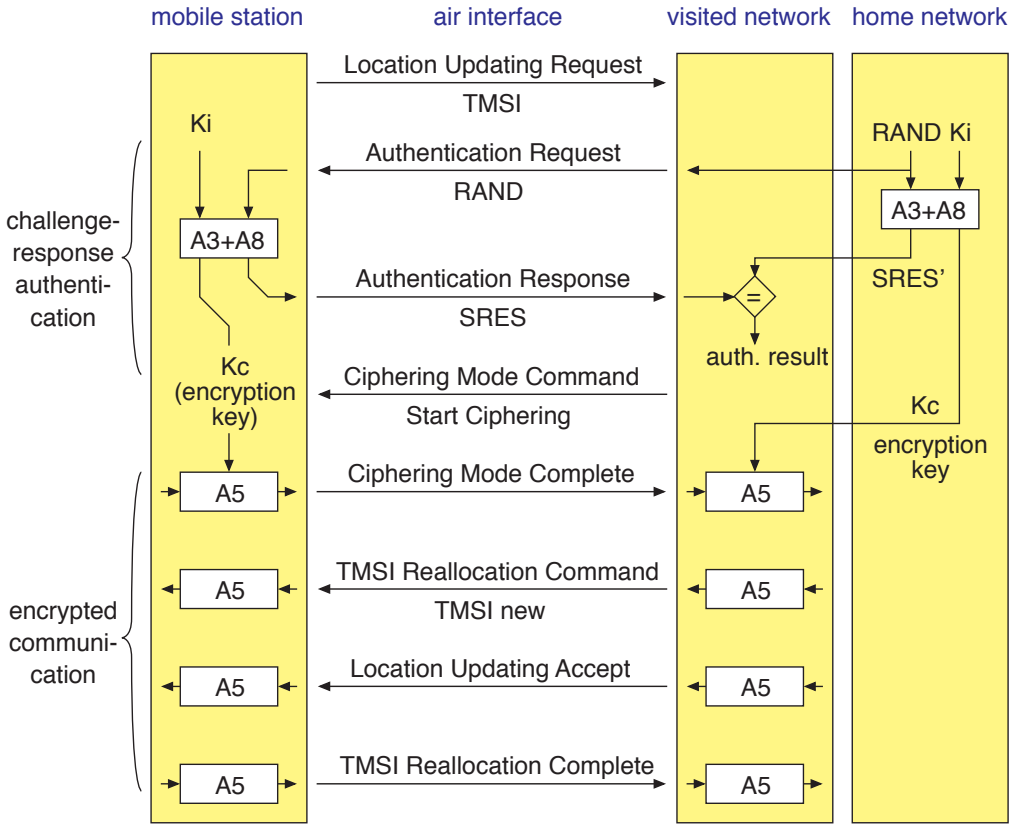
Active Man-in-the-Middle Attack on A5/3



Active Man-in-the-Middle Attack on A5/3 (Variation)



GSM security functions overview



Attacks – Telephone at the expense of others

- SIM cloning
  - Weakness of authentication algorithm
- Interception of authentication data
  - Eavesdropping of internal communication links
- IMSI catcher
  - Man-in-the-middle attack on the air interface

SIM cloning

- Scope
  - Telephone at the expense of others
  - Determine Ki in SIM card
- Attack 1
  - Marc Briceno (Smart Card Developers Association), Ian Goldberg and Dave Wagner (both University of California in Berkeley)
    - http://www.isaac.cs.berkeley.edu/isaac/gsm.html
  - Attack uses a weakness of algorithm COMP128, which implements A3/A8
  - SIM card (incl. PIN) must be under control of the attacker for at least 8-12 hours
  - Needs 2^{17} RAND values (≈ 150.000 calculations) to determine Ki (max. 128 bit)
  - 6,25 calculations per second only, due to slow serial interface of SIM card

SIM cloning

- Scope
  - Telephone at the expense of others
  - Determine Ki in SIM card

Source: http://www.ccc.de/gsm/

SIM cloning

- Scope
  - Telephone at the expense of others
  - Determine Ki in SIM card

- Attack 2
  - Side Channel Attack on SIM card
  - Measurement of chip power consumption during authentication reveals Ki
  - Attack on the implementation of COMP 128, not the algorithm itself
  - Very fast: 500-1000 random inputs used for practical attack

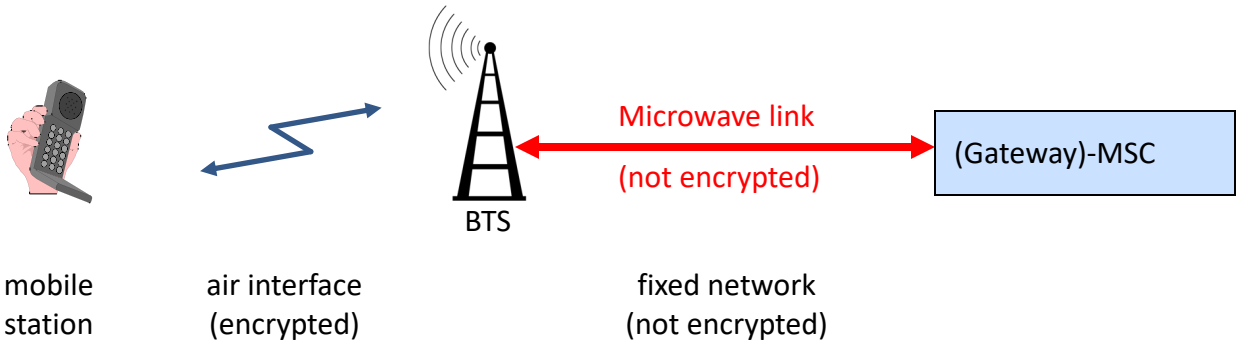
  - More reading:
    - Rao, Rohatgi, Scherzer, Tinguely: Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. Proc. 2002 IEEE Symposium on Security and Privacy, 2002

Interception of authentication data

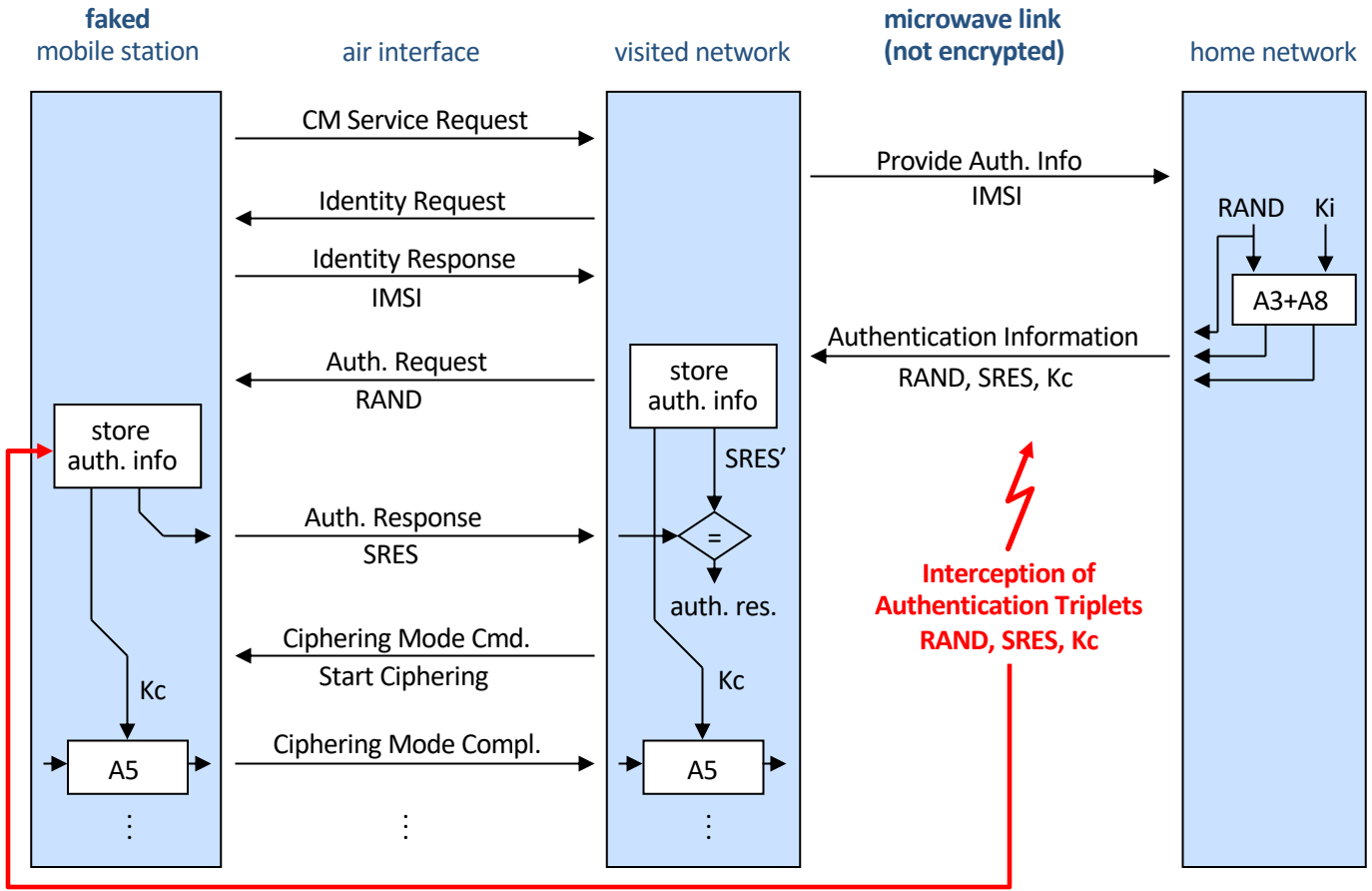
- Scope
  - Telephone at the expense of others
  - Described by Ross Anderson (University of Cambridge)
  - Eavesdropping of unencrypted internal transmission of authentication data (RAND, SRES, Kc) from AuC to visited MSC

- Weakness
  - GSM standard only describes interfaces between network components.
  - They forgot the demand for internal encryption.
  - Microwave links are widely used for internal linkage of network components.

No encryption of internal links



Interception of authentication data



IMSI-Catcher

- Scope
  - Identities of users of a certain radio cell
  - Eavesdropping of communications
  - (Telephone at the expense of others)
- Man-in-the-middle attack (Masquerade)

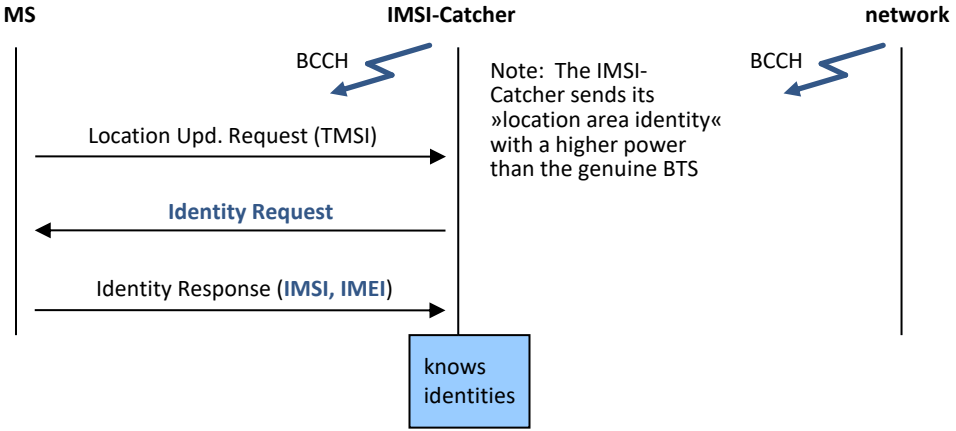
- Weakness
  - No protection against malicious or faked network components

- EP 1 051 053 B1
  - April 2000 by Rohde & Schwarz

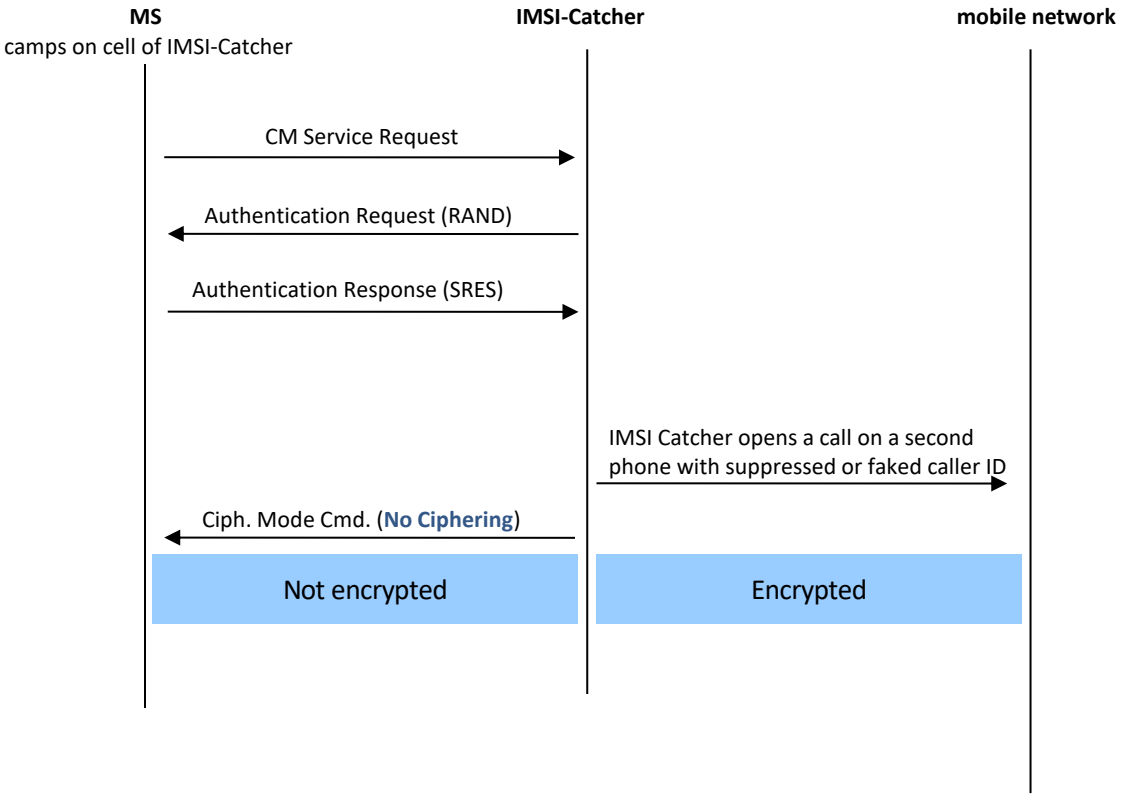
IMSI-Catcher

Pictures: Verfassungsschutz,
http://www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf
http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html

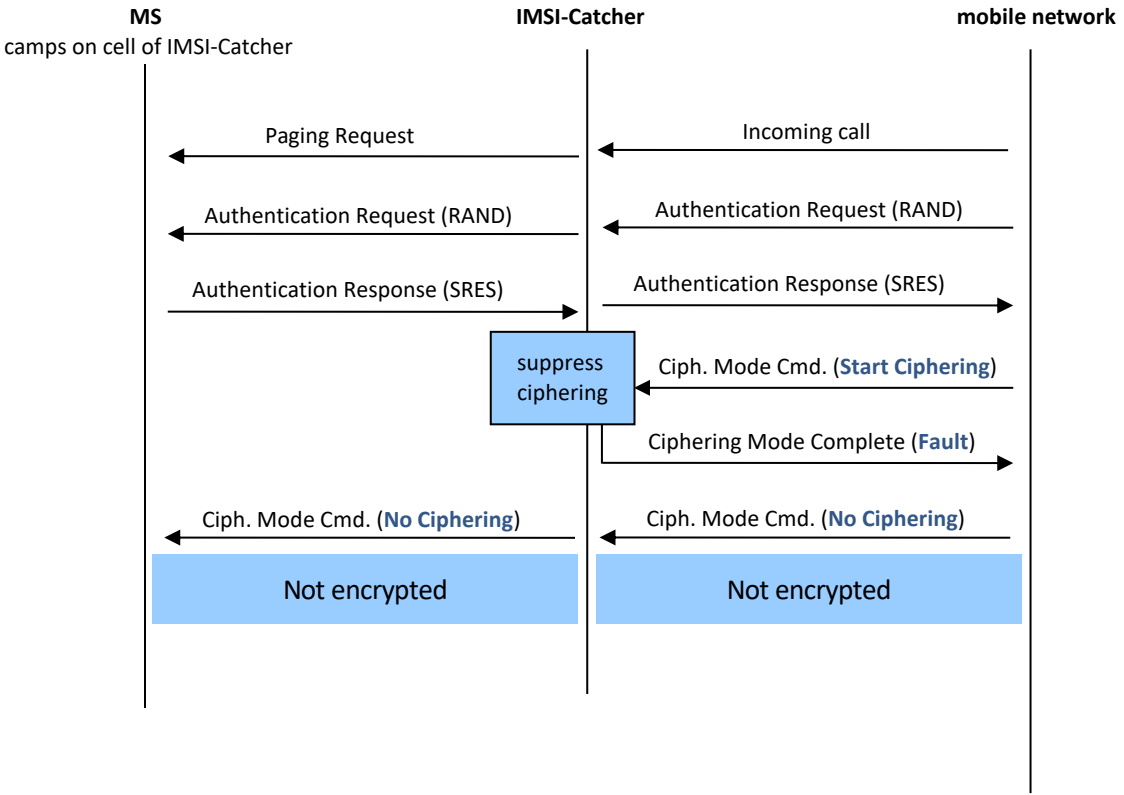
IMSI-Catcher: Getting IMSI and IMEI



IMSI-Catcher: Eavesdropping Mobile Originated Calls



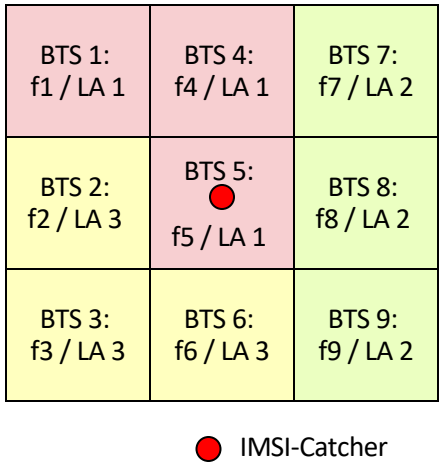
IMSI-Catcher: Eavesdropping Mobile Terminated Calls



IMSI-Catcher (1)

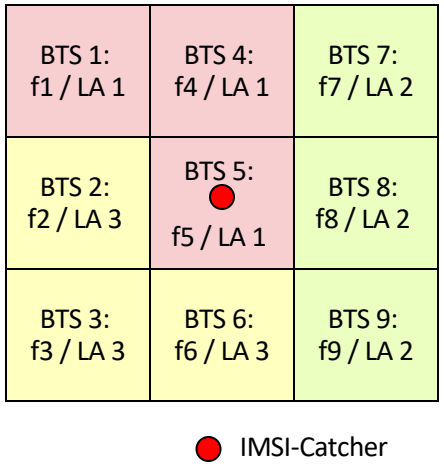
- All BTS' send a list of frequencies of BCCHs of their neighboring cells and the own LAI

- Examples:
  - BTS 7: f4, f5, f8; LA 2
  - BTS 8: f7, f4, f5, f6, f9; LA 2



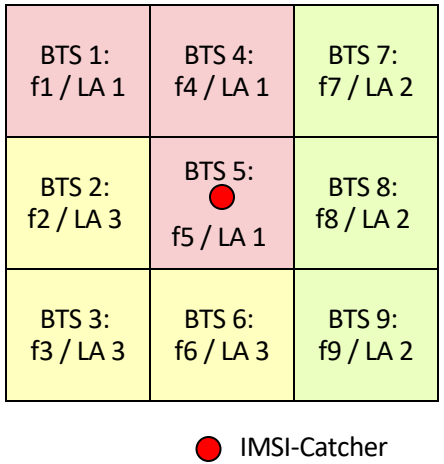
IMSI-Catcher (2)

- IMSI-Catcher
  - receive from BCCH of current cell (5)
    - BTS 5: f1, f2, f3, f4, f6, f7, f8, f9; LA 1
  - select any frequency (e.g. f4) and receives from BCCH on f4
    - BTS 4: f1, f2, f5, f8, f7; LA 1
  - choose any LAI which differs from actual LAIs in neighborhood (e.g. LA 9)
  - send on f4 with high power
    - IMSI-C.: f1, f2, f5, f8, f7; LA 9



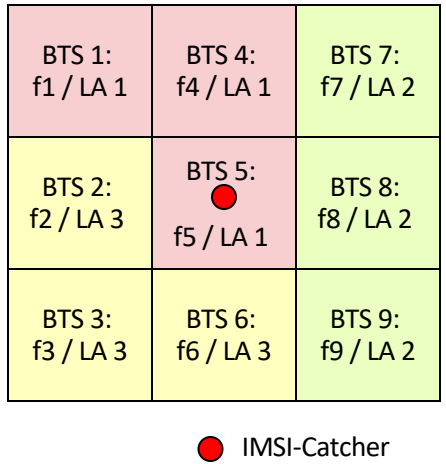
IMSI-Catcher (3)

- MS (camps on cell 5)
  - monitors BCCHs of cells 1-9
  - finds best signal on f4 (transmitted by IMSI-Catcher) and learns that cell belongs to a new LA
  - send a LUP request to IMSI-Catcher
- IMSI-Catcher
  - responds with a Identity Request
- MS
  - answers with IMSI and IMEI



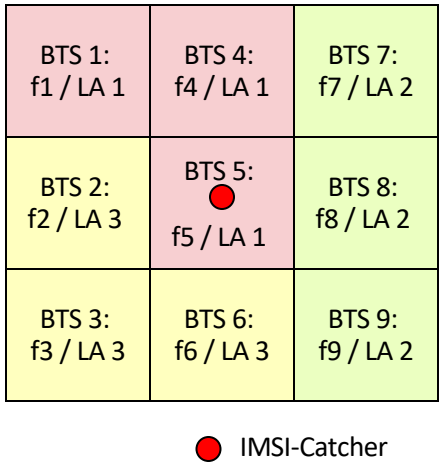
IMSI-Catcher (4)

- IMSI-Catcher
  - sends junk (non-decodable data) on Paging Channel (PCH) and
  - sends a frequency list of BTS which do not send the frequency of IMSI-Catcher (f4) in their frequency lists
    - IMSI-C.: f3, f6, f9; LA 9



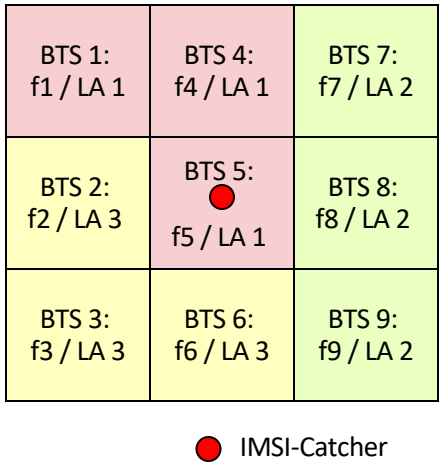
IMSI-Catcher (5)

- MS
  - receives junk on PCH and (according to GSM05.05) does a cell reselection:
  - MS monitors signal strengths of f3, f6, f9
  - changes to the best cell (LUP)



IMSI-Catcher (5)

- Result
  - MS is back in the network again
  - because BTS 3, 6 and 9 do not send f4 in their frequency lists, the MS does not recognize the powerful IMSI-Catcher signal again (and subsequently does not change back to it)



IMSI-Catcher detectors

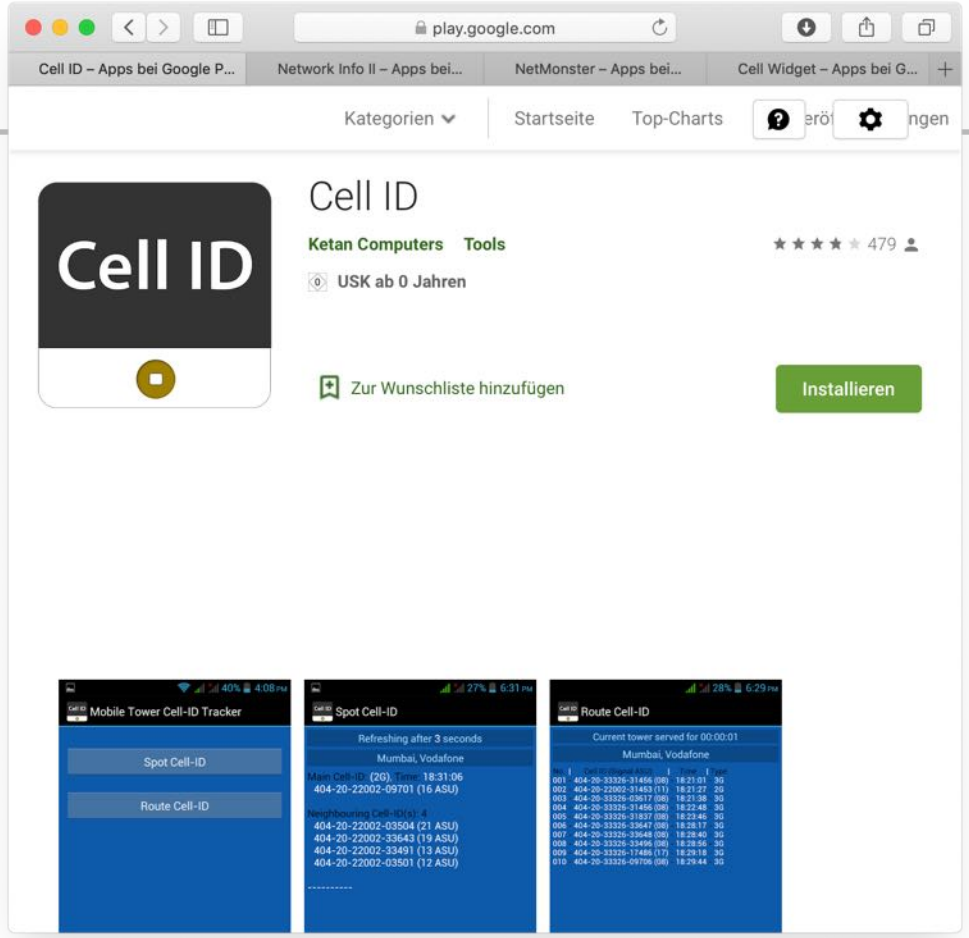
- AIMSICD
  - https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector
- SnoopSnitch
  - from SRLabs (Karsten Nohl)
- Darshak
  - TU Berlin
- GSMK CryptoPhone
  - special Smarthone
- IMSI-Catcher-Catcher (ICC)
  - SBA Research (Adrian Dabrowski)

Picture (ICC): heise.de

Sources: https://www.privacy-handbuch.de/handbuch_75.htm
http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html

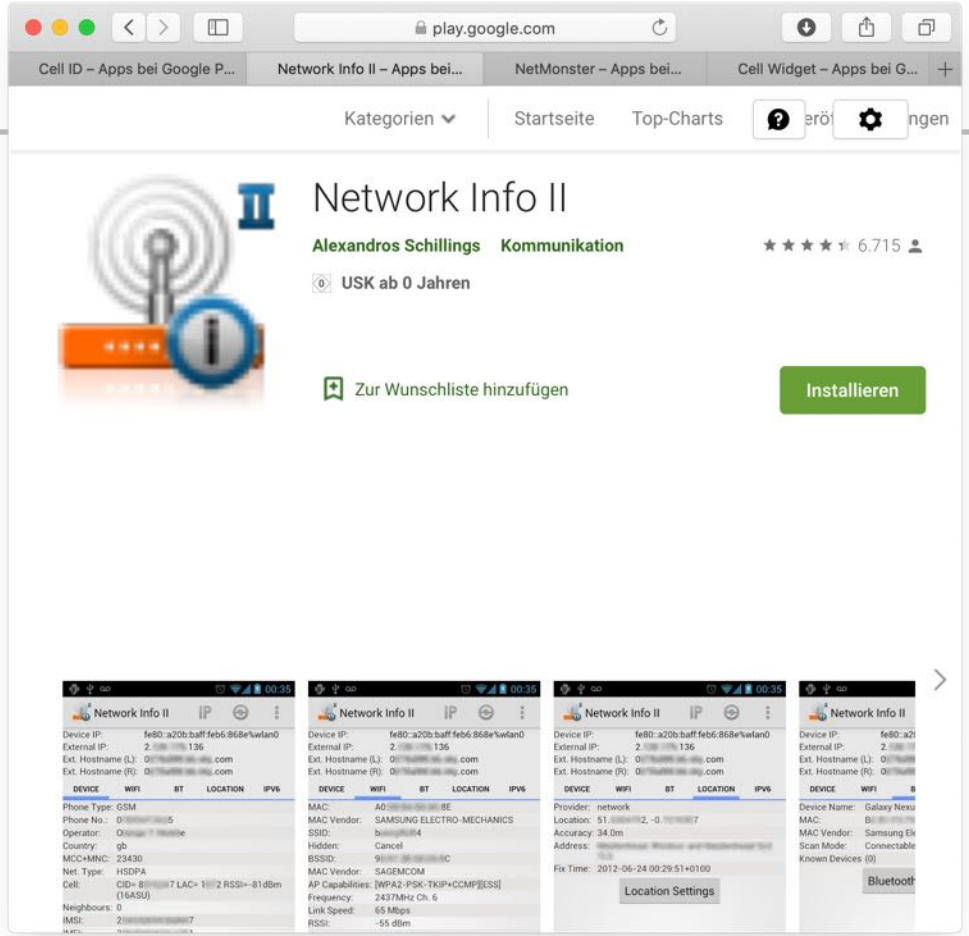
Example Apps for getting mobile network parameters

- Cell ID
- Network Info II
- Net Monster
- Cell Widget



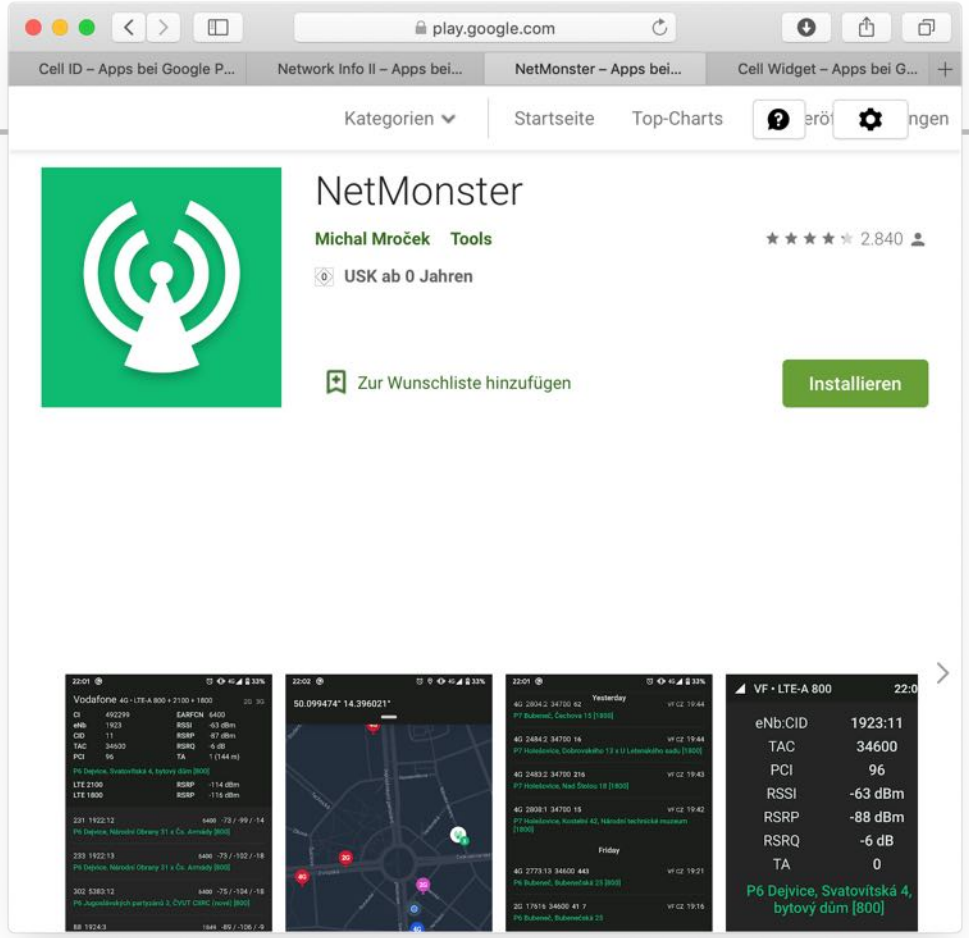
Example Apps for getting mobile network parameters

- Cell ID
- Network Info II
- Net Monster
- Cell Widget



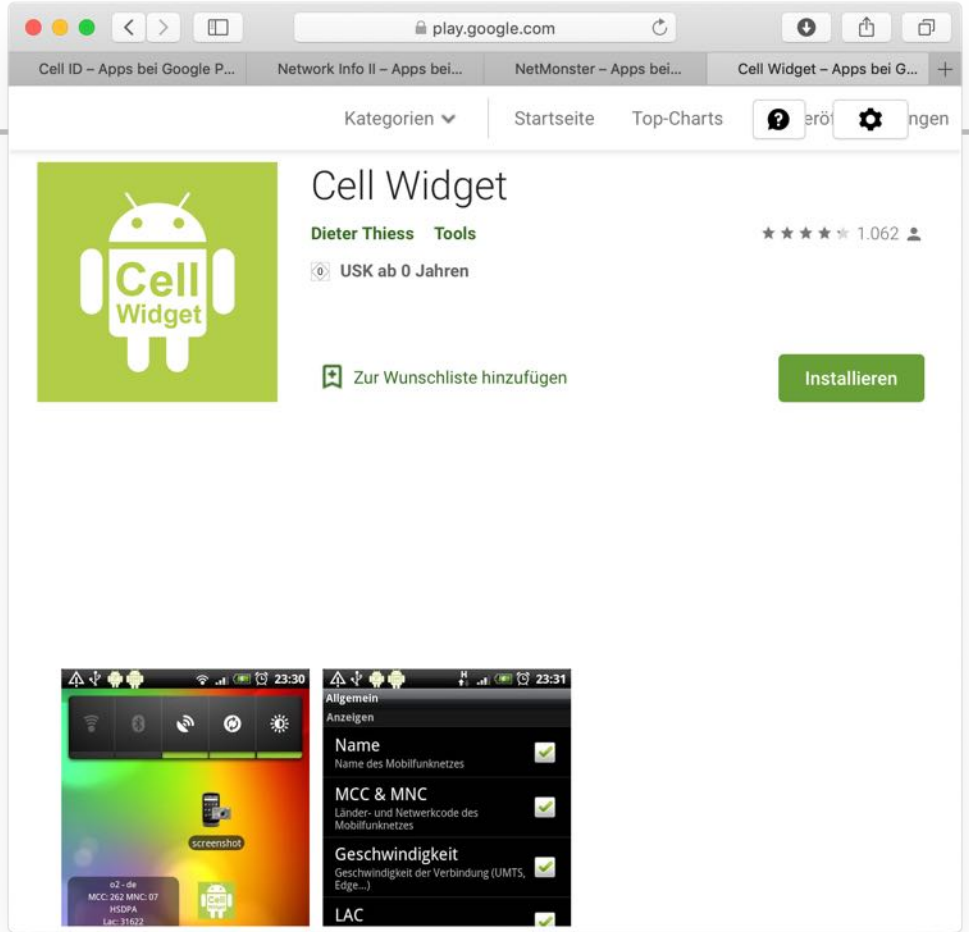
Example Apps for getting mobile network parameters

- Cell ID
- Network Info II
- Net Monster
- Cell Widget



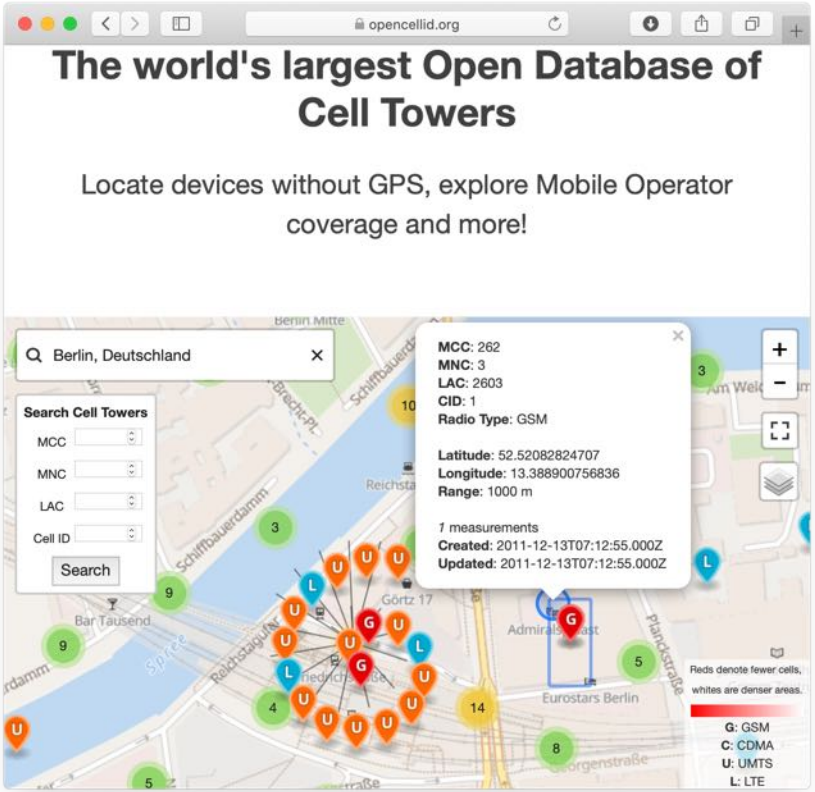
Example Apps for getting mobile network parameters

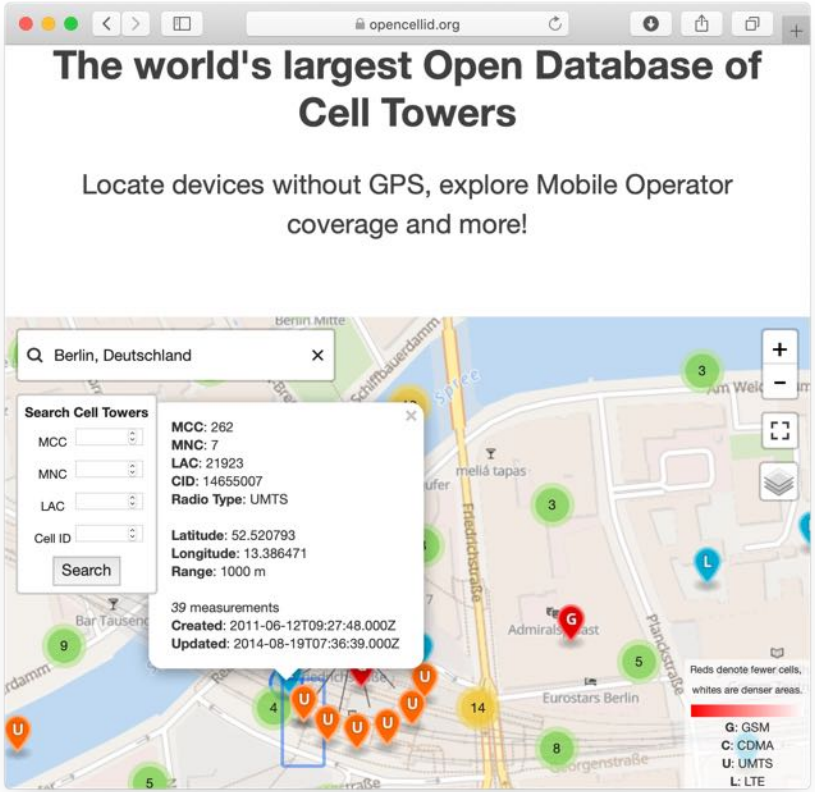
- Cell ID
- Network Info II
- Net Monster
- Cell Widget



OpenCellID: shows locations of base stations

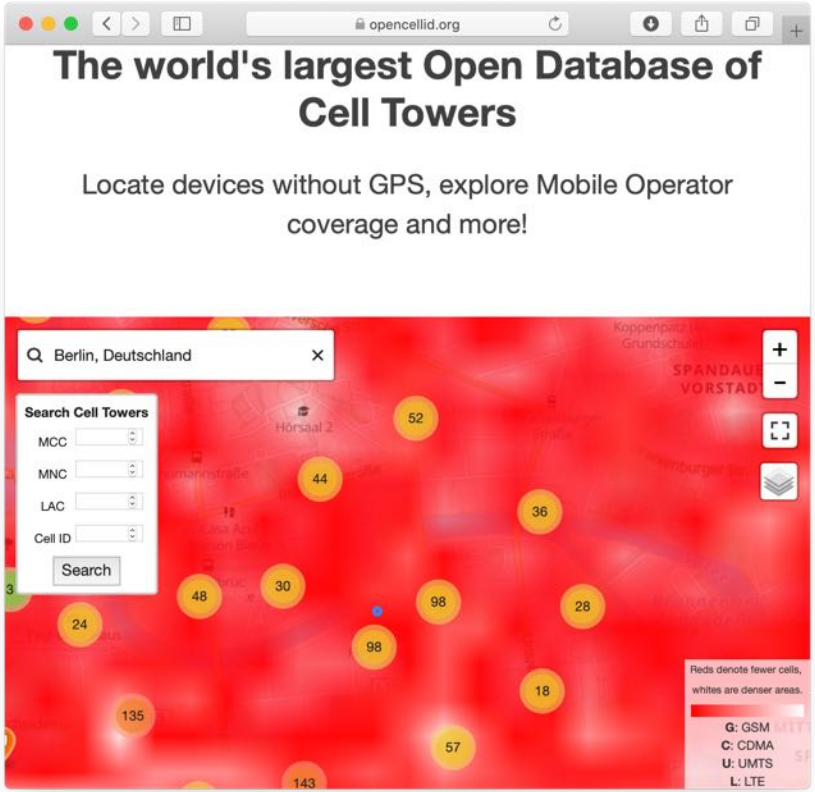
http://www.opencellid.org

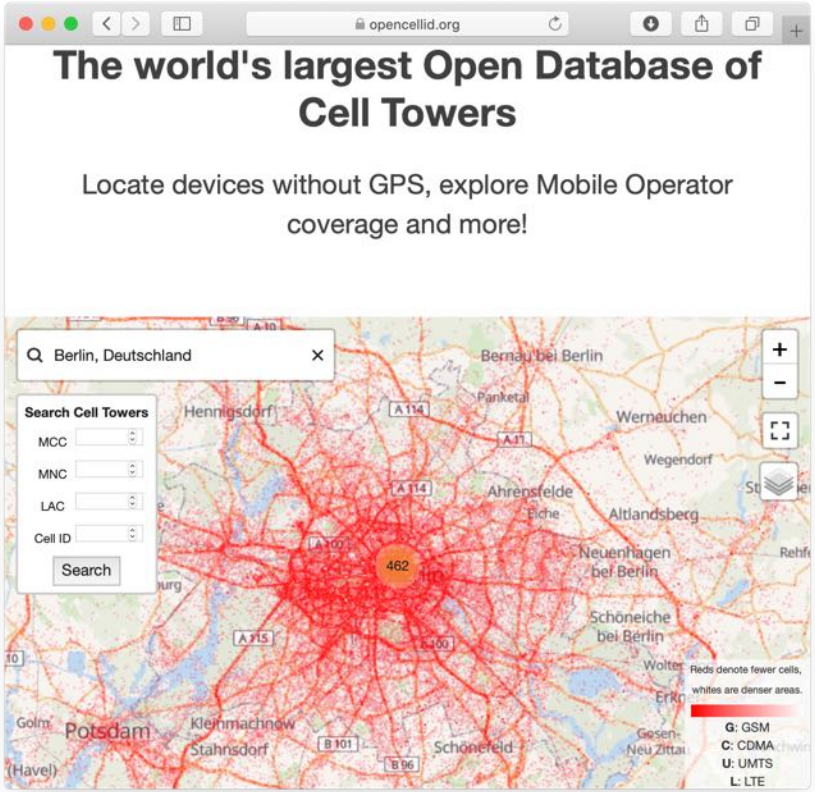




OpenCellID: shows radio coverage

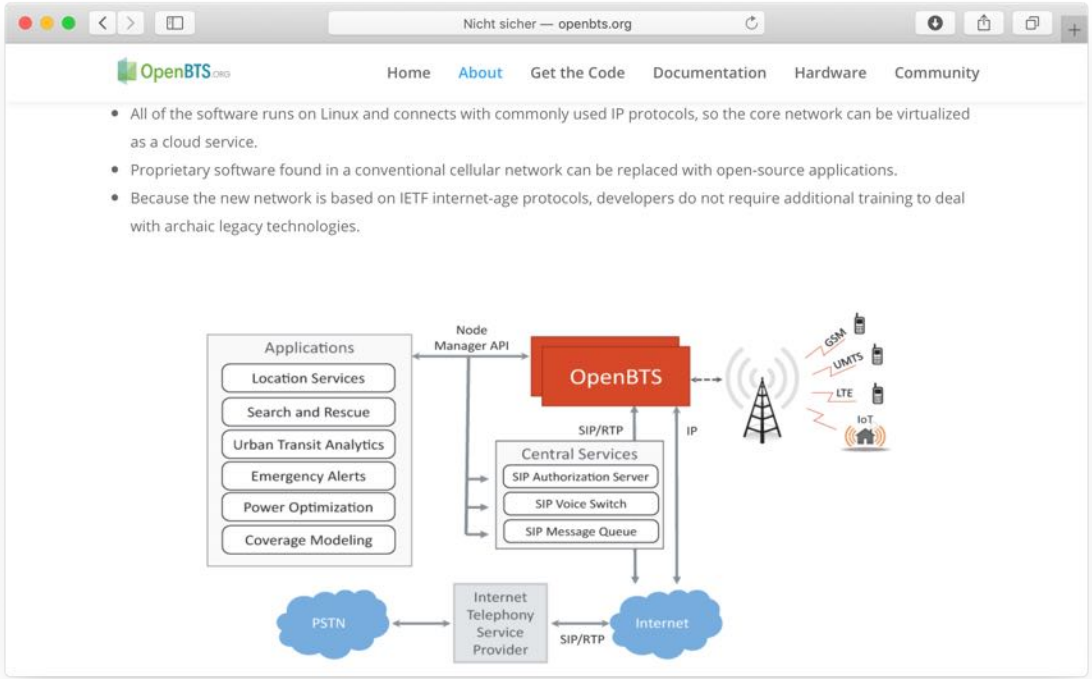
http://www.opencellid.org



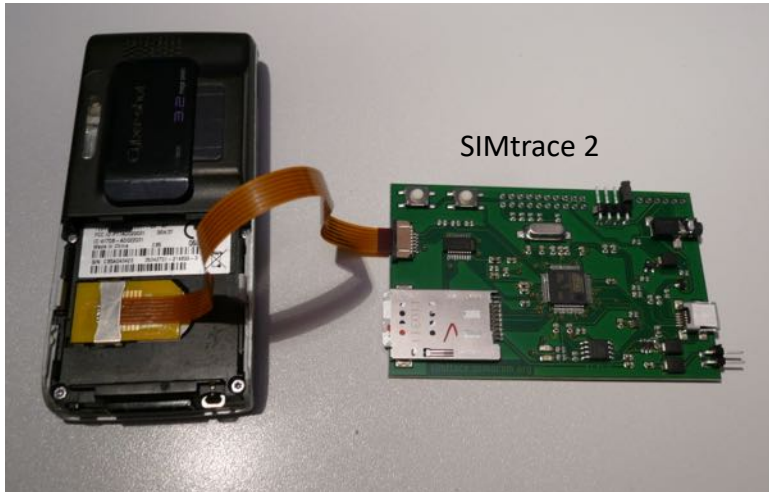


http://openbts.org

»OpenBTS.org is an open source software project dedicated to revolutionizing mobile networks by substituting legacy telco protocols and traditionally complex, proprietary hardware systems with Internet Protocol and a flexible software architecture. This architecture is open to innovation by anybody, allowing the development of new applications and services and dramatically simplifying the setting up and operation of a mobile network.«



- Osmocom SIMtrace 2
  - combination of software, firmware and hardware system
  - main purpose: sniff the communication between a phone and a SIM card
  - https://osmocom.org/projects/simtrace2/wiki



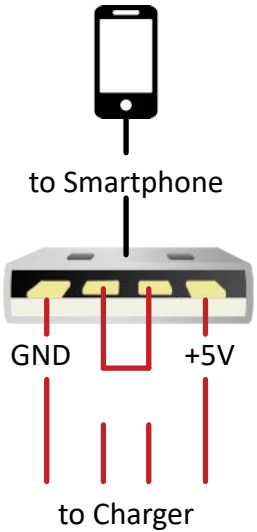
SIMtrace 2

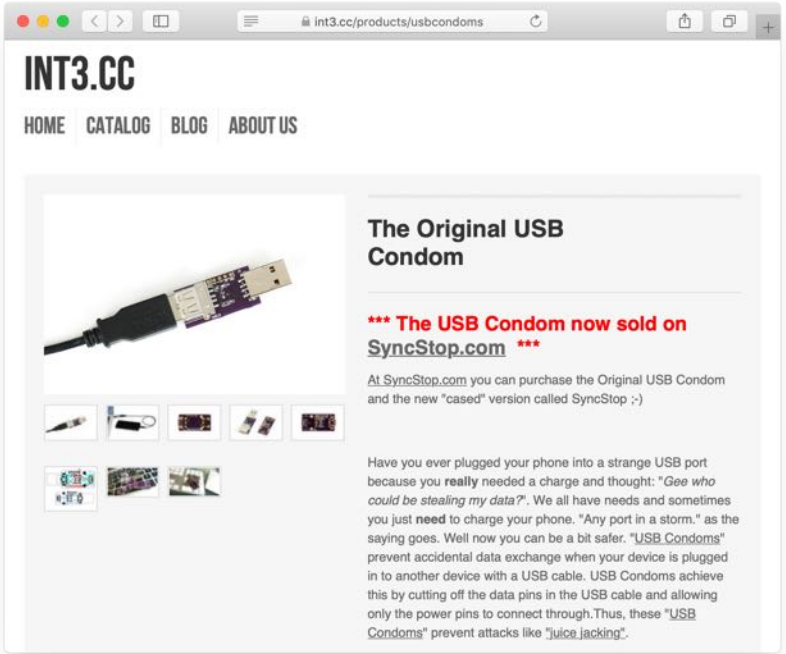
Turbo SIM: Earlier solution for sniffing communication between SIM and MS (introduced 2004, updated 2007)

https://arstechnica.com/gadgets/2007/08/turbo-sim-add-on-allows-full-iphone-unlocking/

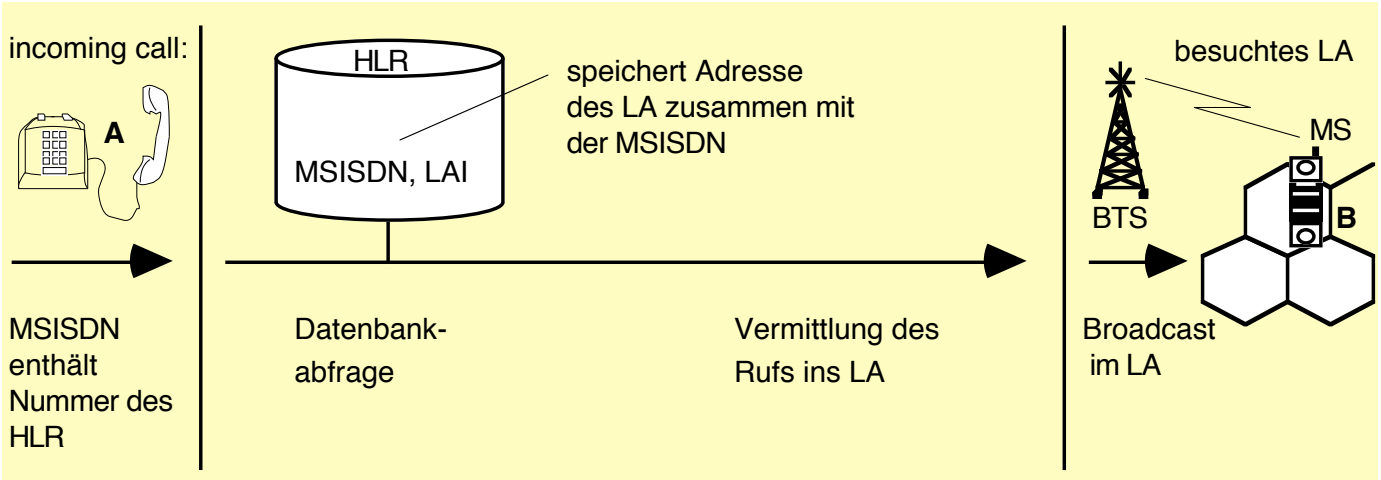
USB charging condom

- USB-A has 4 wires
- cut 2 inner data wires and short-circuit
- connect power wires only

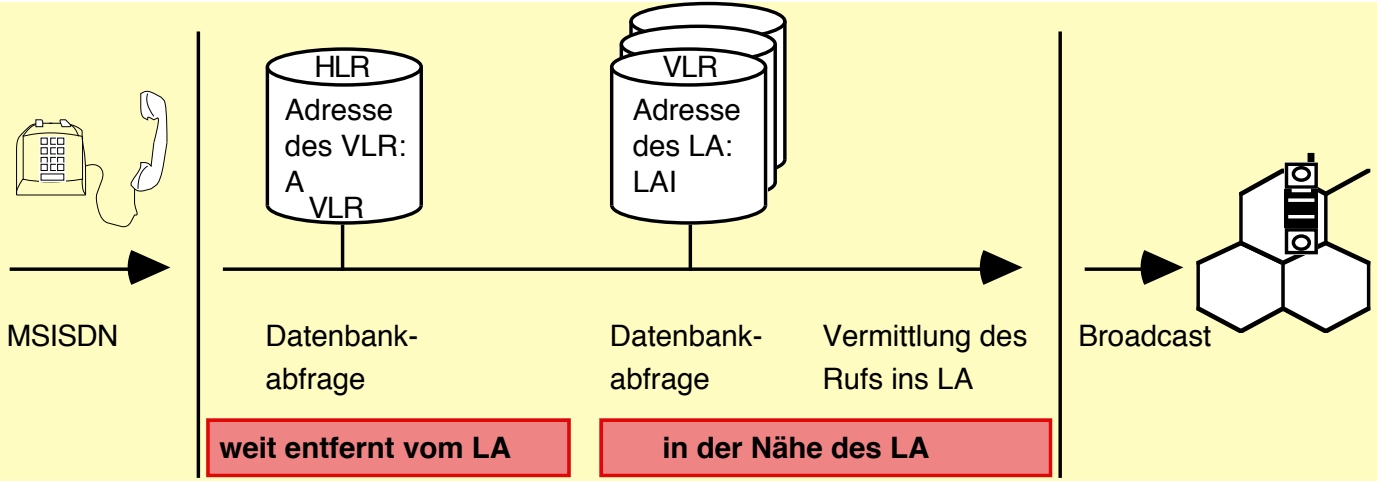




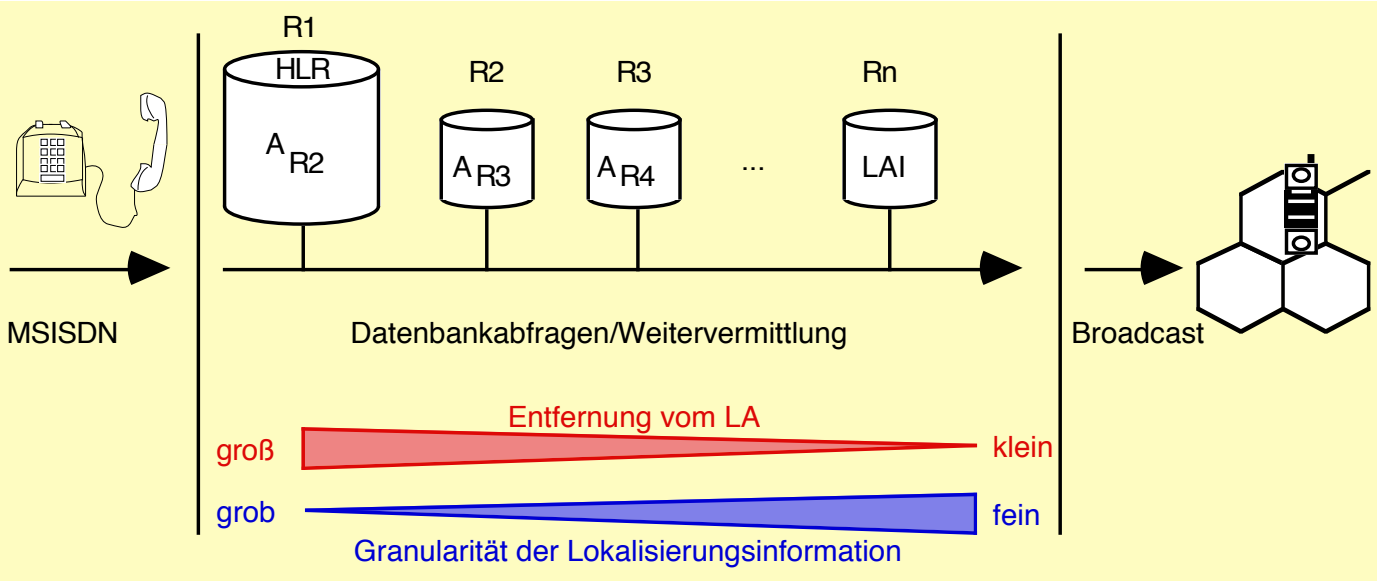
- Centralized approach
  - Change of Location Area (LA), i.e. Location Updating, needs communication with HLR (far away from LA)
  - Efficiency: Good at low Location Updating rates
- Used in Mobile IP
  - HLR = Home Agent



- 2-staged approach
  - Change of Location Area (LA) changes VLR entry
  - VLR serves geographically limited area (VLR-Area)
  - Rare changes of VLR-Area changes HLR entry
  - Reduced signaling costs in wide area network
  - Tradeoff: Delayed call setup (mobile terminated)



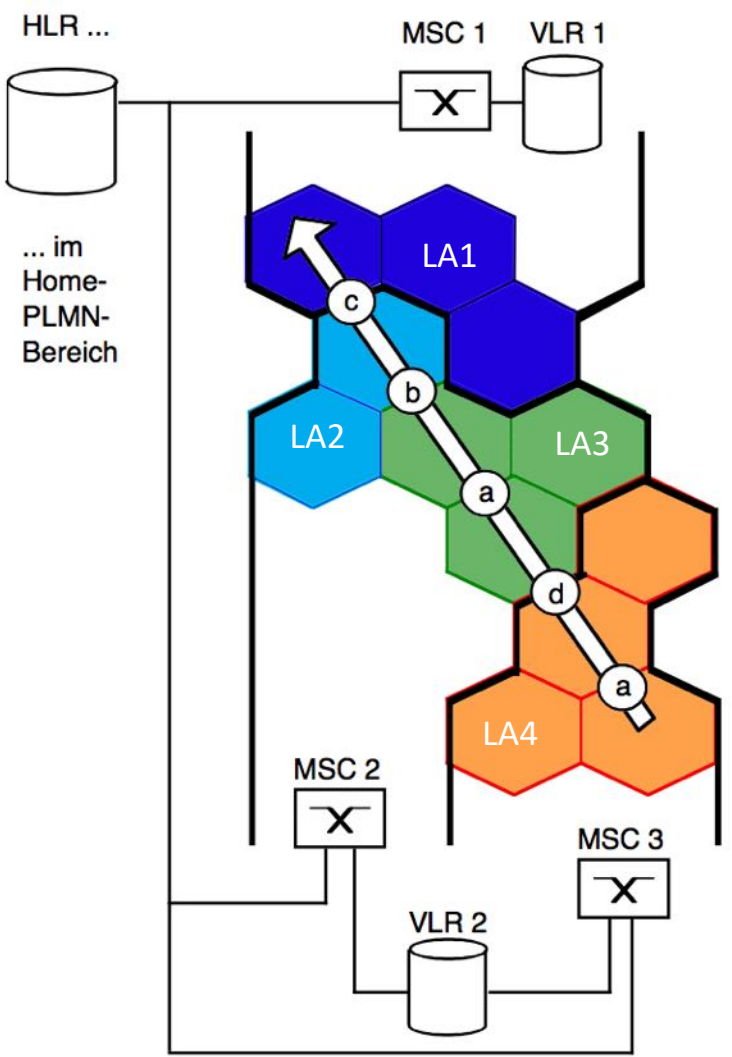
- Multi-staged storage
  - Many proposals for 3rd Generation Systems (UMTS), never realized in the field
  - Variations: Hierarchical storage, Forwarding strategies



Location Updating Situations

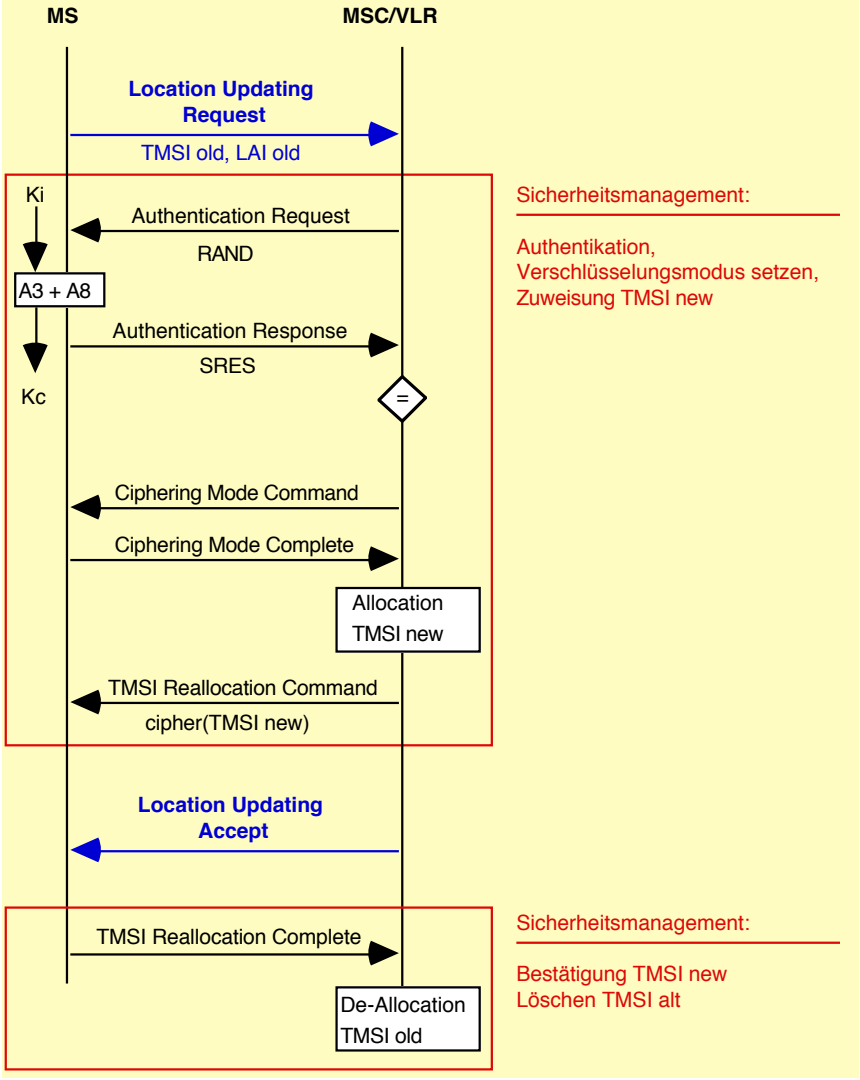
- Situations
  - a) Change of radio cell
  - b) Change of LA
  - c) Change of VLR/MSC area
  - d) Change of MSC area

  LA 1 (belongs to MSC 1 and VLR 1)
  LA 2 (belongs to MSC 2 and VLR 2)
  LA 3 (belongs to MSC 2 and VLR 2)
  LA 4 (belongs to MSC 3 and VLR 2)

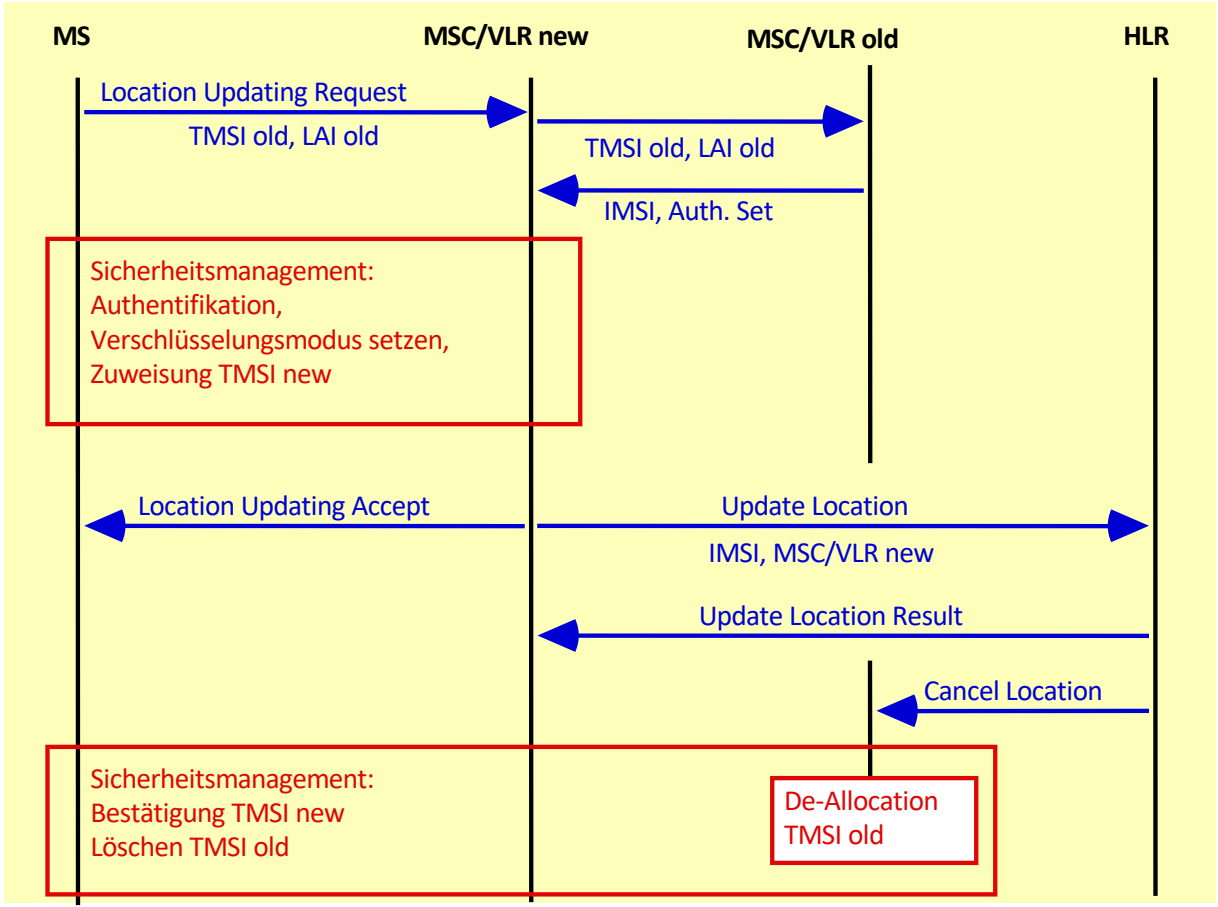


Location Updating: New LA

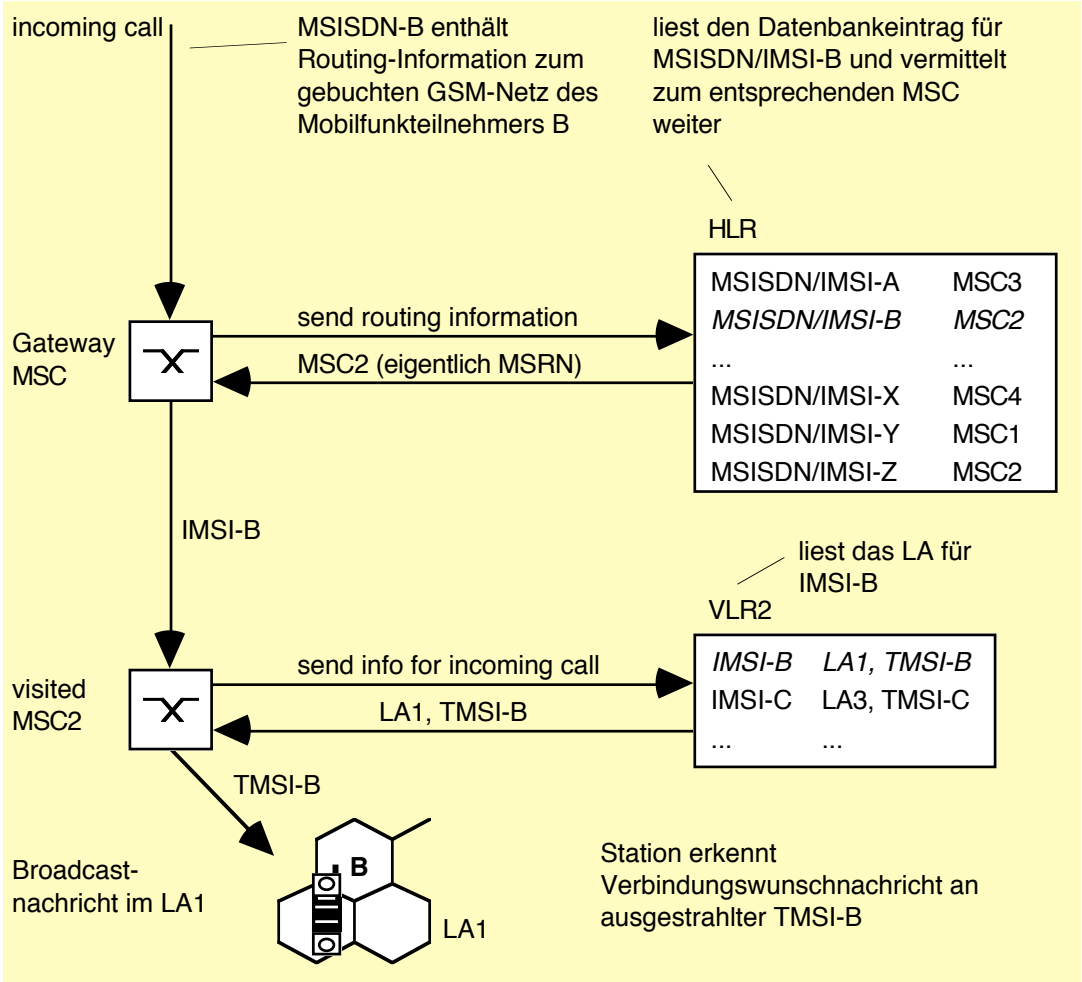
- New LA, old VLR (TMSI found)
  - Location Updating Request (TMSI, LAI)old
  - Security management
    - Authentication
    - Ciphering Mode
    - TMSI Reallocation
  - Location Updating Accept



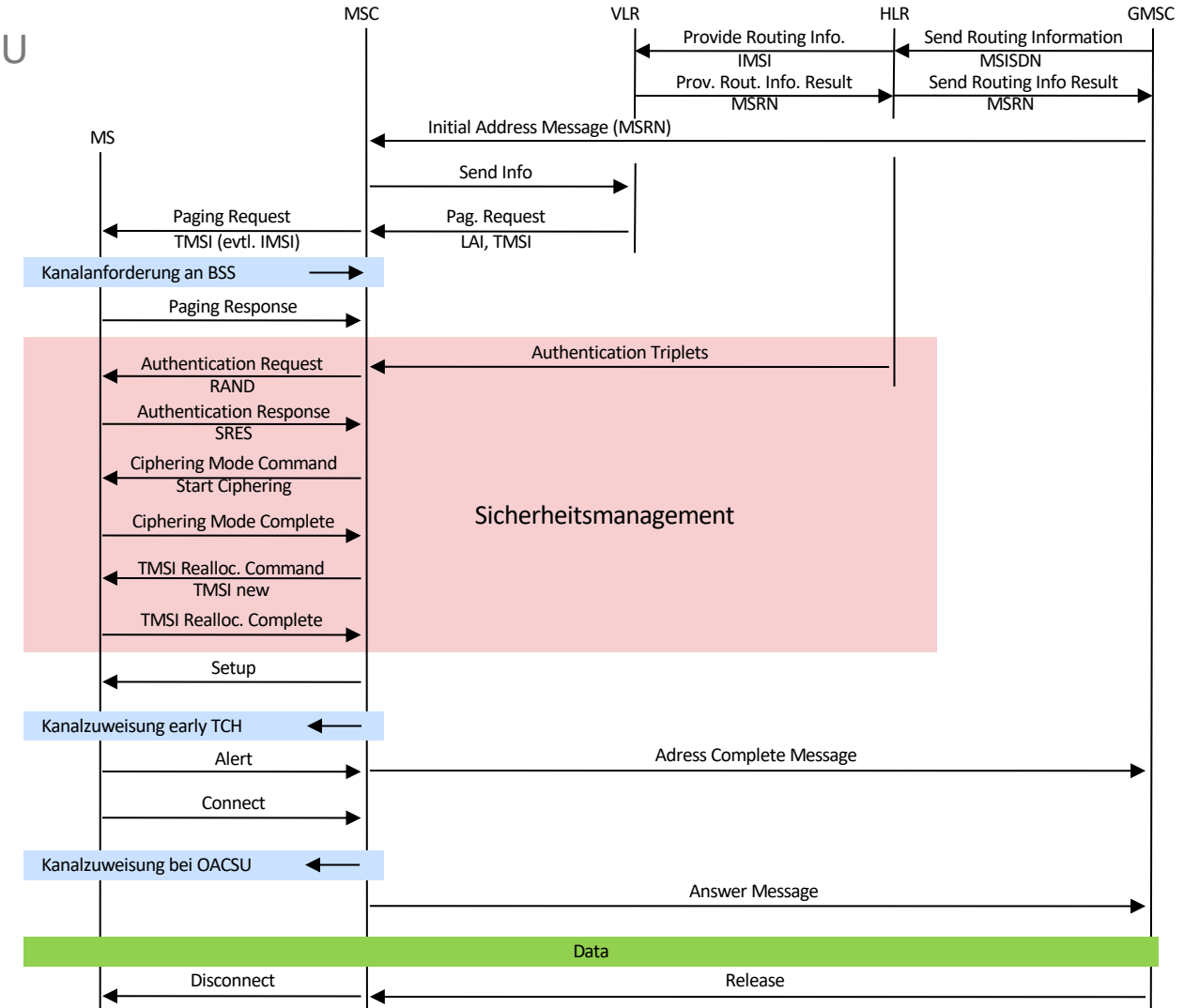
Location Updating: New VLR area



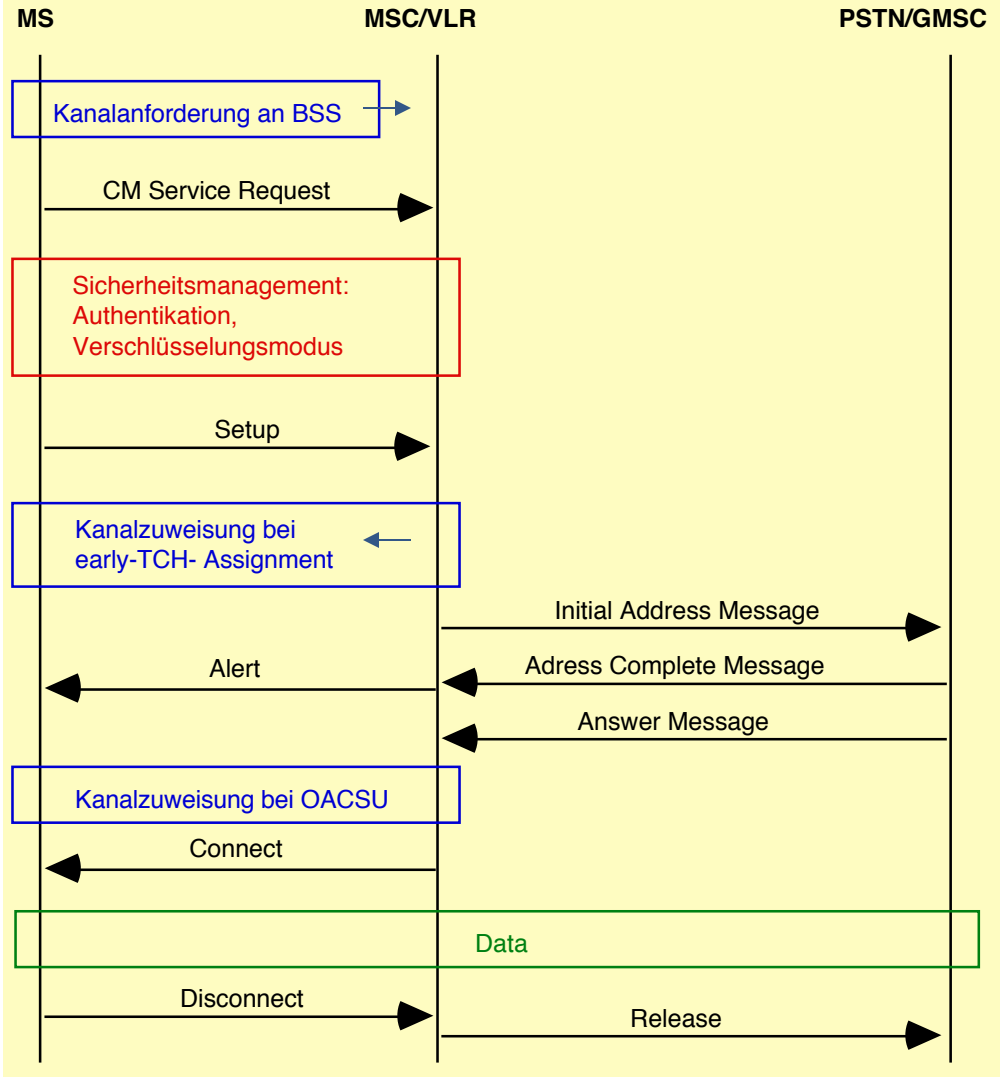
Mobile Terminated Call Setup (MTCSU)



MTCSU


MSC
VLR
HLR
GMSC
MS
Provide Routing Info.
IMSI
Send Routing Information
MSISDN
Prov. Rout. Info. Result
MSRN
Send Routing Info Result
MSRN
Initial Address Message (MSRN)
Send Info
Paging Request
TMSI (evtl. IMSI)
Pag. Request
LAI, TMSI
Kanalanforderung an BSS
Paging Response
Authentication Triplets
Authentication Request
RAND
Authentication Response
SRES
Ciphering Mode Command
Start Ciphering
Ciphering Mode Complete
TMSI Realloc. Command
TMSI new
TMSI Realloc. Complete
Sicherheitsmanagement
Setup
Kanalzuweisung early TCH
Alert
Adress Complete Message
Connect
Kanalzuweisung bei OACSU
Answer Message
Data
Disconnect
Release

Mobile Originated Call Setup

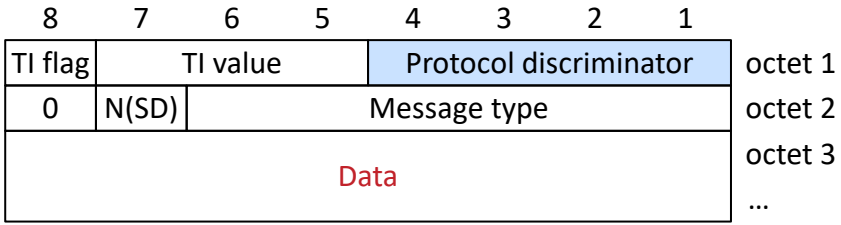


Message format GSM 04.08

- Protocol discriminator

4 3 2 1	bit number
0 0 1 1	call control, packet-mode, connection control and call related SS msgs
0 1 0 1	mobility management messages
0 1 1 0	radio resources management messages
1 0 0 1	short message service messages
1 0 1 1	non call related SS messages
1 1 1 1	reserved for tests procedures

All other values are reserved

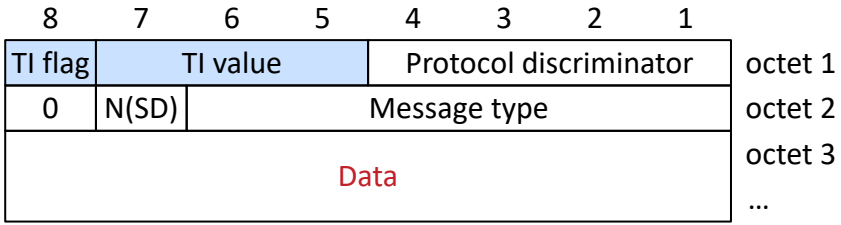


Message format GSM 04.08

- Transaction identifier (TI)
  - Used for distinction of parallel activities of MS
    - TI flag:

      0: message sent from the originated TI side

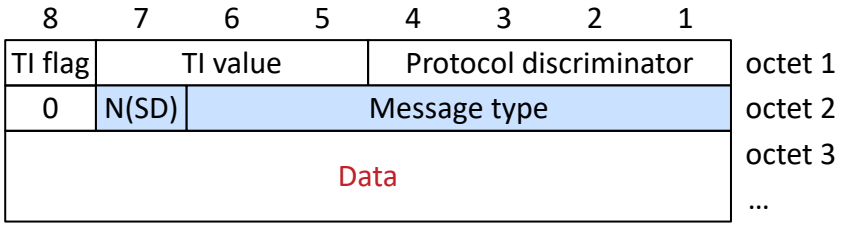
      1: message sent to the originated TI side
- TI value
  - Number 000…110 (bin: 0…6)
  - 111 reserved



Message format GSM 04.08

- 3 Classes:
  - Radio resources management
  - Mobility management
  - Call control

- N(SD)
  - Sequence number or Extension Bit



Message type (1)

- Radio resources management (1)

```
8 7 6 5 4 3 2 1            bit number
-----------------------------------------------------
0 0 1 1 1 – – – Channel establishment messages
          0 1 1            ADDITIONAL ASSIGNMENT
          1 1 1            IMMEDIATE ASSIGNMENT
          0 0 1            IMMEDIATE ASSIGNMENT EXTENDED
          0 1 0            IMMEDIATE ASSIGNMENT REJECT
0 0 1 1 0 – – – Ciphering messages
          1 0 1            CIPHERING MODE ASSIGNEMT
          0 1 0            CIPHERING MODE COMPLETE
0 0 1 0 1 – – – Handover messages
          1 1 0            ASSIGNEMT COMMAND
          0 0 0            ASSIGNEMT COMPLETE
          1 1 1            ASSIGNMENT FAILURE
          0 1 1            HANDOVER COMMAND
          1 0 0            HANDOVER COMPLETE
          0 0 0            HANDOVER FAILURE
          1 0 1            PHYSICAL INFORMATION
0 0 0 0 1 – – – Channel release messages
          1 0 1            CHANNEL RELEASE
          0 1 0            PARTIAL RELEASE
          1 1 1            PARTIAL RELEASE COMPLETE

                                                    ...
```

Message type (1)

- Radio resources management (2)

```
8 7 6 5 4 3 2 1           bit number
-----------------------------------------------------

...


0 0 1 0 0 – – – Paging messages
          0 0 1           PAGING REQUEST TYPE 1
          0 1 0           PAGING REQUEST TYPE 2
          1 0 0           PAGING REQUEST TYPE 3
          1 1 1           PAGING RESPONSE
0 0 0 1 1 – – – System information messages
          0 0 1           SYSTEM INFORMATION TYPE 1
          0 1 0           SYSTEM INFORMATION TYPE 2
          0 1 1           SYSTEM INFORMATION TYPE 3
          1 0 0           SYSTEM INFORMATION TYPE 4
          1 0 1           SYSTEM INFORMATION TYPE 5
          1 1 0           SYSTEM INFORMATION TYPE 6
0 0 0 1 0 – – – Miscellaneous messages
          0 0 0           CHANNEL MODE MODIFY
          0 1 0           RR-STATUS
          1 1 1           CHANNEL MODE MODIFY ACKNOWLEDGE
          1 0 0           FREQUENCY REDEFINITION
          1 0 1           MEASUREMENT REPORT
          1 1 0           CLASSMARK CHANGE
```

Message type (2)

- Mobility management
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent

```
8 7 6 5 4 3 2 1            bit number
-----------------------------------------
0 x 0 0 – – – – Registration messages
        0 0 0 1            IMSI DETACH INDICATION
        0 0 1 0            LOCATION UPDATING ACCEPT
        0 1 0 0            LOCATION UPDATING REJECT
        1 0 0 0            LOCATION UPDATING REQUEST
0 x 0 1 – – – – Security messages
        0 0 0 1            AUTHENTICATION REJECT
        0 0 1 0            AUTHENTICATION REQUEST
        0 1 0 0            AUTHENTICATION RESPONSE
        1 0 0 0            IDENTITY REQUEST
        1 0 0 1            IDENTITY RESPONSE
        1 0 1 0            TMSI REALLOCATION COMMAND
        1 0 1 1            TMSI REALLOCATION COMPLETE
0 x 1 0 – – – – Connection management messages
        0 0 0 1            CM SERVICE ACCEPT
        0 0 1 0            CM SERVICE REJECT
        0 1 0 0            CM SERVICE REQUEST
        1 0 0 0            CM REESTABLISHMENT REQUEST
0 x 1 1 – – – – Connection management messages
        0 0 0 1            MM STATUS
```

Message type (3)

- Call control (1)
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent
  - Nationally specific messages: next octets contain message

```
8 7 6 5 4 3 2 1            bit number
-----------------------------------------
0 x 0 0 0 0 0 0            Escape to nationally
                           specific message types
0 x 0 0 – – – - Call establishment messages
        0 0 0 1            ALERTING
        1 0 0 0            CALL CONFIRMED
        0 0 1 0            CALL PROCEEDING
        0 1 1 1            CONNECT
        1 1 1 1            CONNECT ACKNOWLEDGE
        1 1 1 0            EMERGENCY SETUP
        0 0 1 1            PROGRESS
        0 1 0 1            SETUP
0 x 0 1 – – – - Call information phase messages
        0 1 1 1            MODIFY
        1 1 1 1            MODIFY COMPLETE
        0 0 1 1            MODIFY REJECTED
        0 0 0 0            USER INFORMATION
...
```

Message type (3)

- Call control (2)
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent

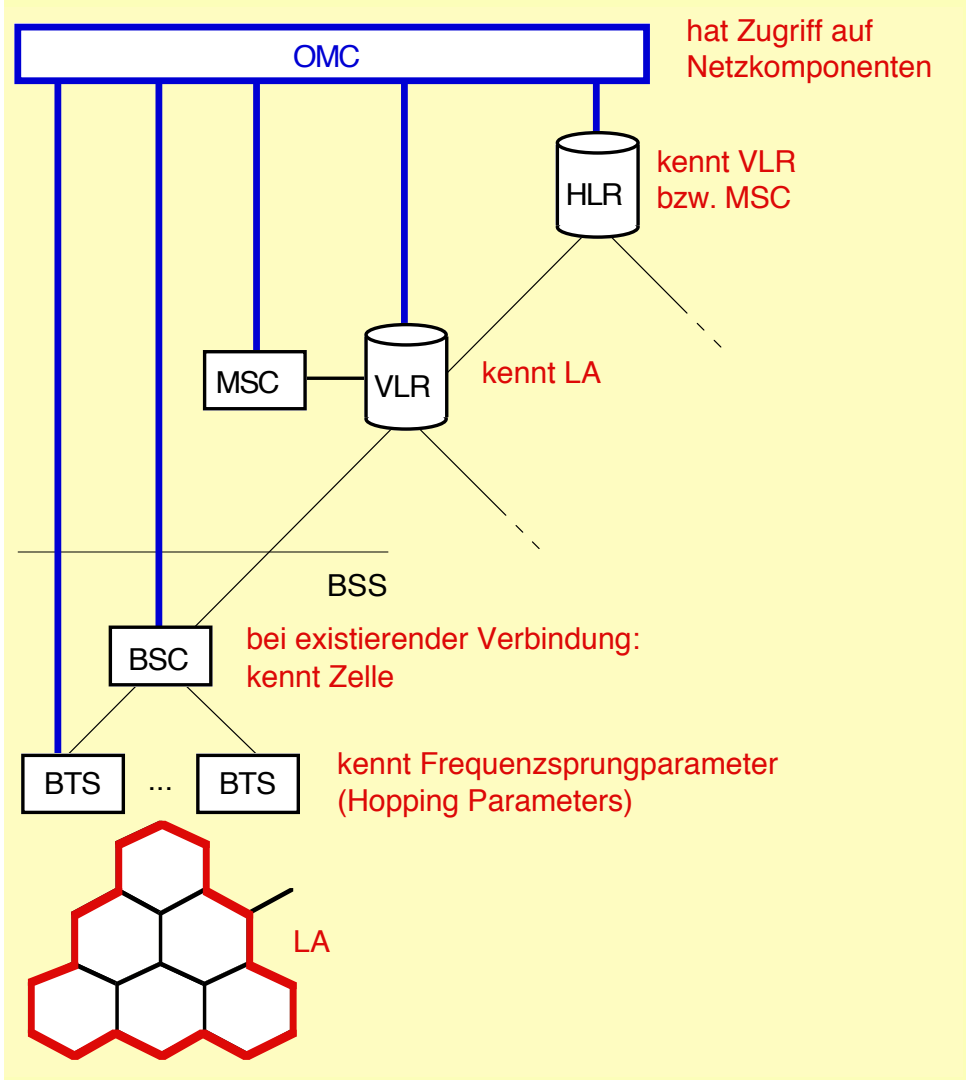
```
8 7 6 5 4 3 2 1           bit number
----------------------------------------

...

0 x 1 0 – – – – Call clearing messages
        0 1 0 1           DISCONNECT
        1 1 0 1           RELEASE
        1 0 1 0           RELEASE COMPLETE
0 x 1 1 – – – – Miscellaneous messages
        1 0 0 1           CONGESTION CONTROL
        1 1 1 0           NOTIFY
        1 1 0 1           STATUS
        0 1 0 0           STATUS ENQUIRY
        0 1 0 1           START DTMF
        0 0 0 1           STOP DTMF
        0 0 1 0           STOP DTMF
ACKNOWLEDGE
        0 1 1 0           START DTMF
ACKNOWLEDGE
        0 1 1 1           START DTMF REJECT
```

Movement profiling in GSM

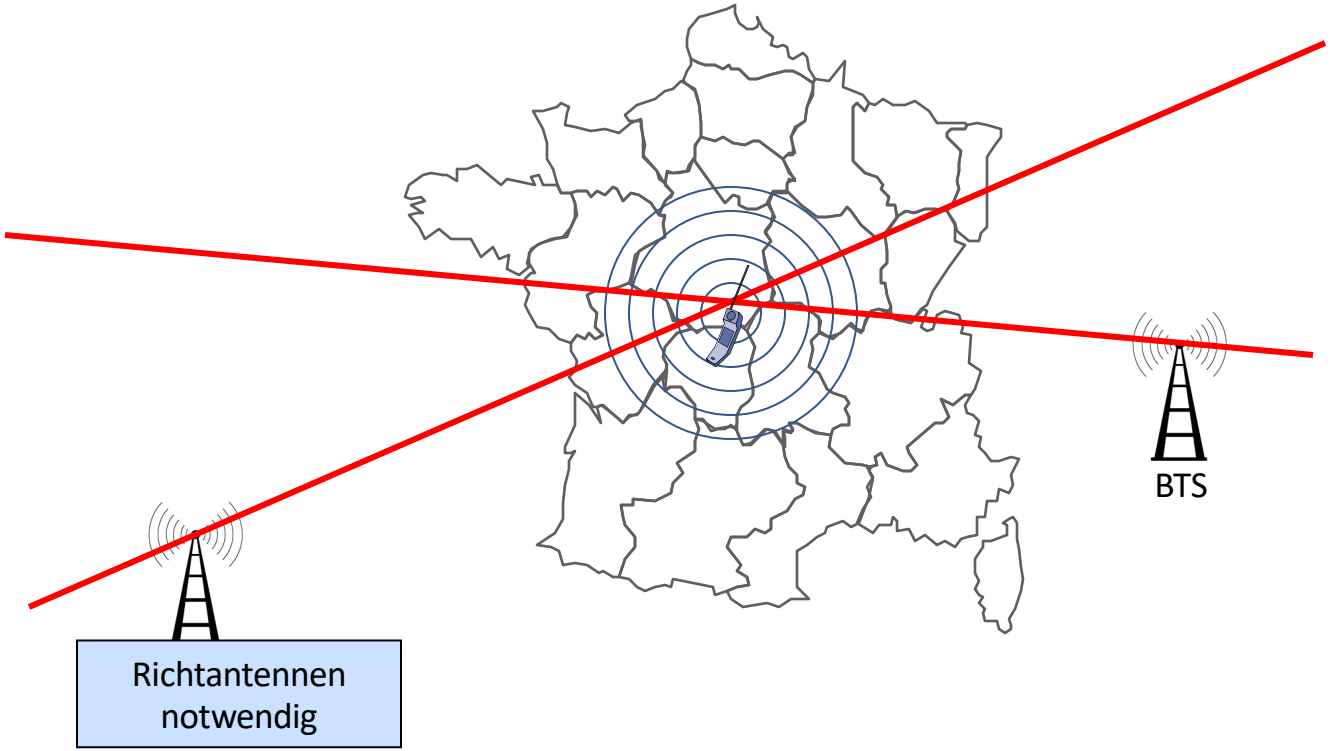
- Variants:
  - Access HLR and VLR data (insiders only)
  - Direction finding (*German:* »Peilung«)

- Protection:
  - Privacy protection of database entries
  - Direct Sequence Spread Spectrum

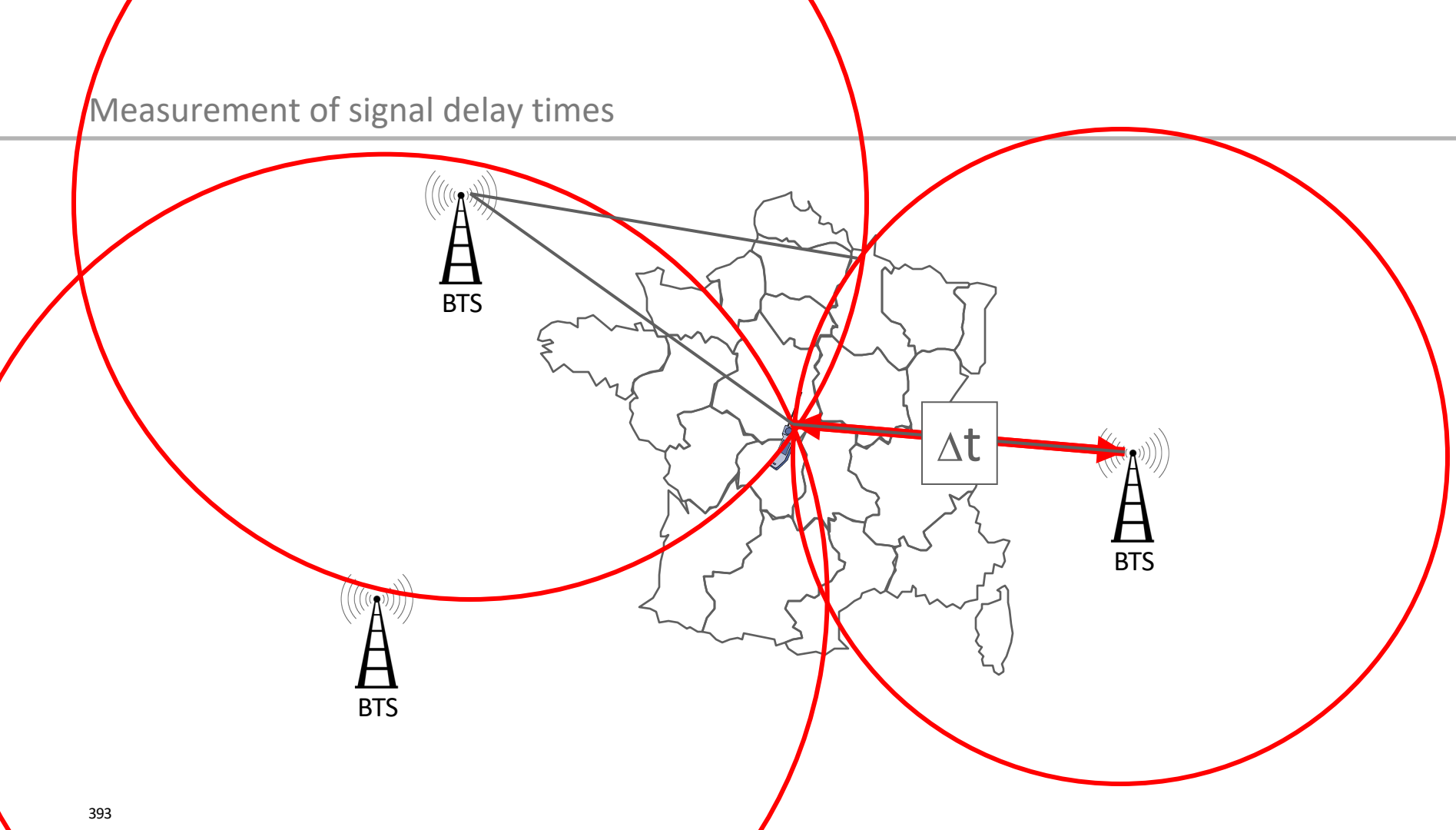
Access HLR and VLR data



Direction finding with directional antennas

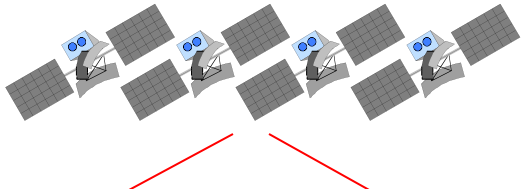


Measurement of signal delay times



- Terminal-based locating
  - Global Positioning System (GPS)
    - Accuracy: 10…100 m
    - Location time: up to 30 sec
  - Assisted-GPS (A-GPS)
    - GPS signals re-broadcasted by BTS
    - Increased location speed (and accuracy)
  - Observed Time Difference (OTD)
    - BTS1 … BTS3 send a location signal
    - Received after Δt_1, Δt_2 and Δt_3 by MS
    - If $\Delta t_i == \Delta t_j$ then OTD=0

Assisted-GPS (A-GPS)



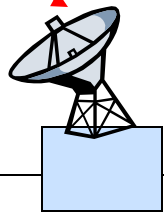
1. MS and A-GPS Server receive same satellite signals

3. Support information

5. Exact measure values

BTS

MSC



A-GPS Server

MS with simplified GPS receiver

4. Performs exact measure and transmits values to A-GPS server

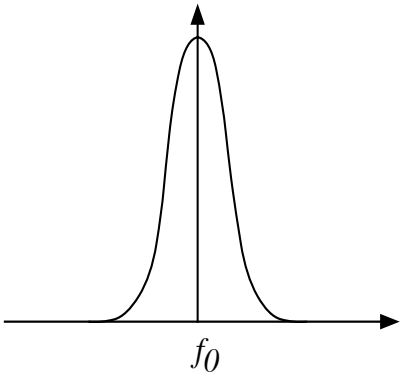
2. Calculates support information for fast localization (doppler shift, pseudo random noise phase)

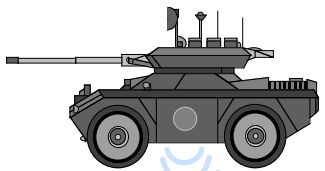
6. Calculates exact location

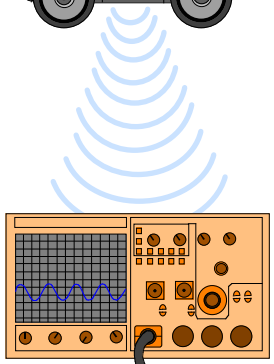
- Network-based locating
  - Time of Arrival (TOA)
    - Mobile station sends signal
    - BTS receive signal after Δt_i (i=1,2,3)
  - Cell of Origin (COO)
    - Cell-ID is associated with geographic location
    - Accuracy: 100 m … 35 km

Spread Spectrum Systems

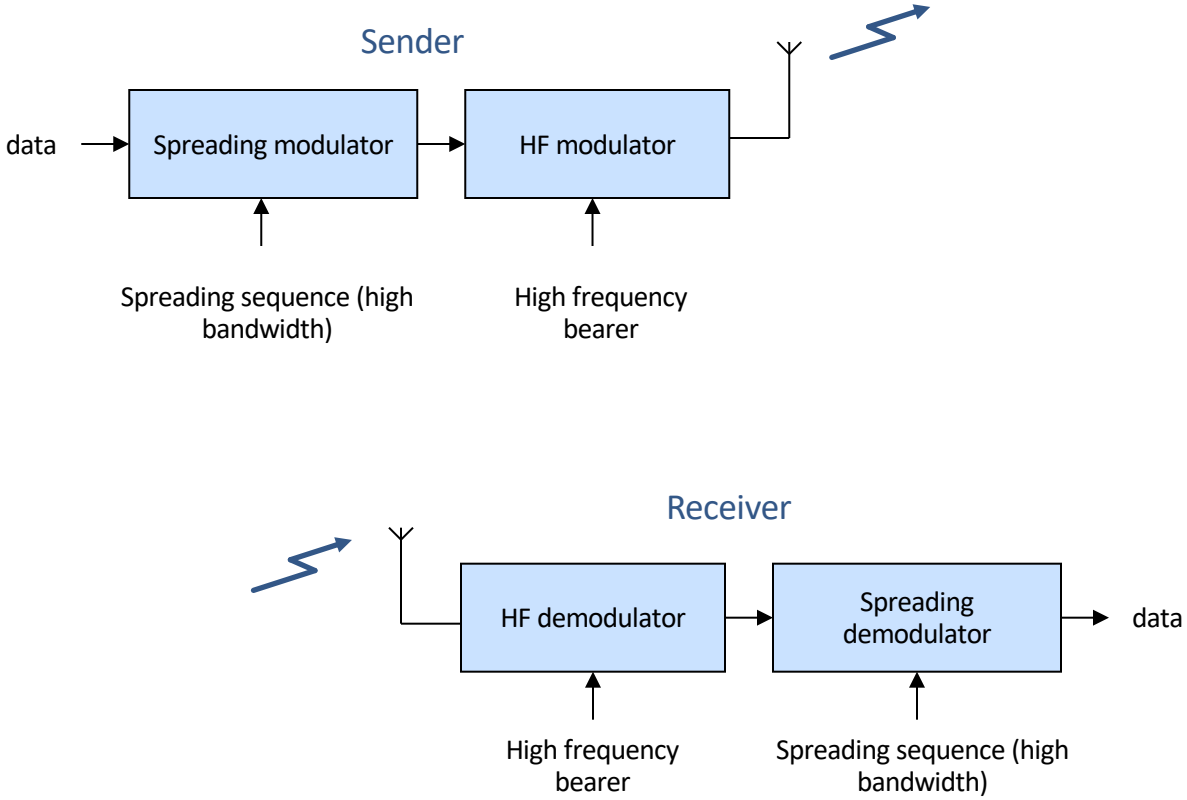
- Radio communication between military divisions
  - Sender sends on frequency f_0 with bandwidth B
- Problems:
  - Spectrum analyzer detects energy around f_0 and directional antennas locate source of signal
  - Jammer may interfere communication



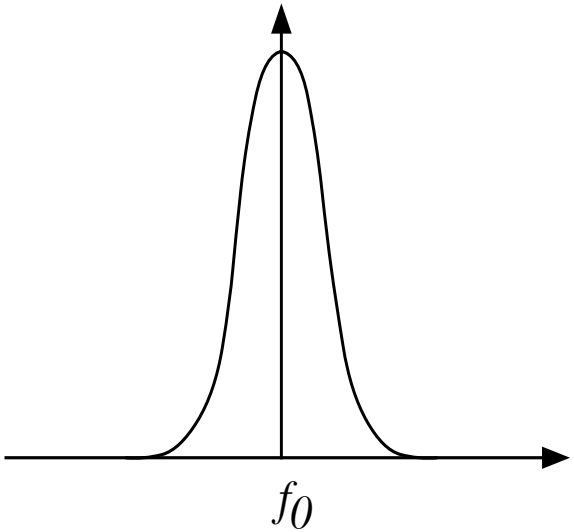




Transmision model Spread Spectrum Systems

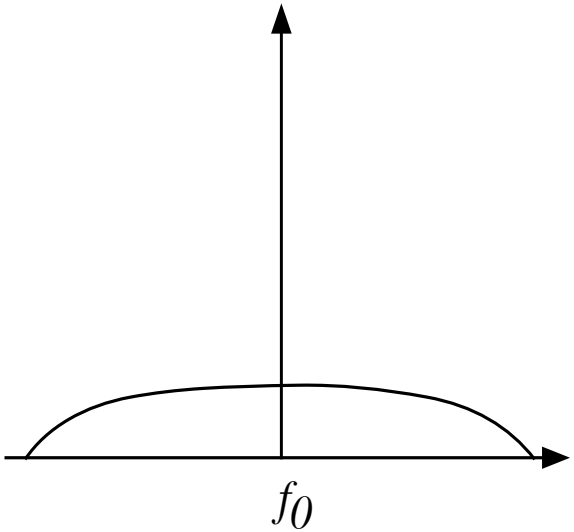


Spreading



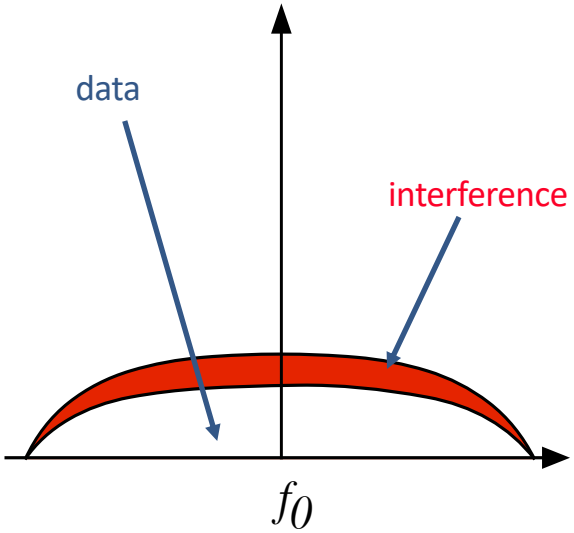
- Data is modulated with high-bandwidth spreading sequence:
  - Walsh functions (orthogonal codes)
  - Pseudo-Noise-Sequence (PN-Code)

Spreading



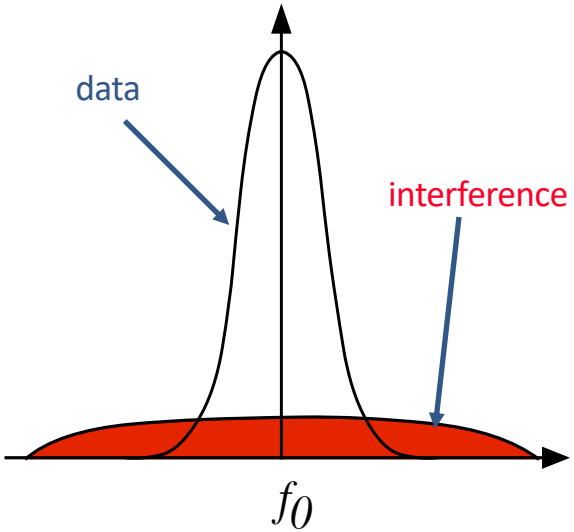
- Data is modulated with high-bandwidth spreading sequence:
  - Walsh functions (orthogonal codes)
  - Pseudo-Noise-Sequence (PN-Code)
- Spectral spreading of signal
- Dispersion of energy on a large frequency spectrum

De-Spreading



- Spread data interfered by (random) noise

De-Spreading



- Spread data interfered by (random) noise

- Spectral spreading of noise
- De-spreading of data

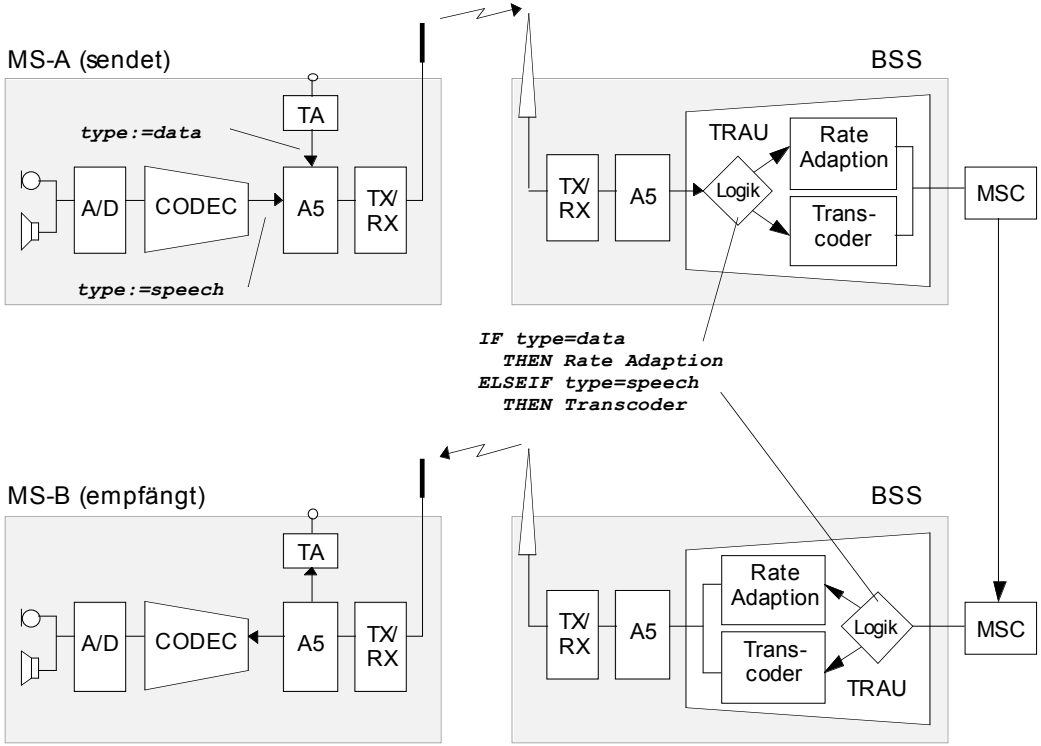
Missing end-to-end-Services in GSM

- Speech channels of GSM are not bit transparent channels
  - Lossy compression of speech channels

- Use data channel for additional end-to-end encryption
  - As an external add-on (e.g. GSM TopSec Med)
  - As integrated service (e.g. GSM TopSec GSM)

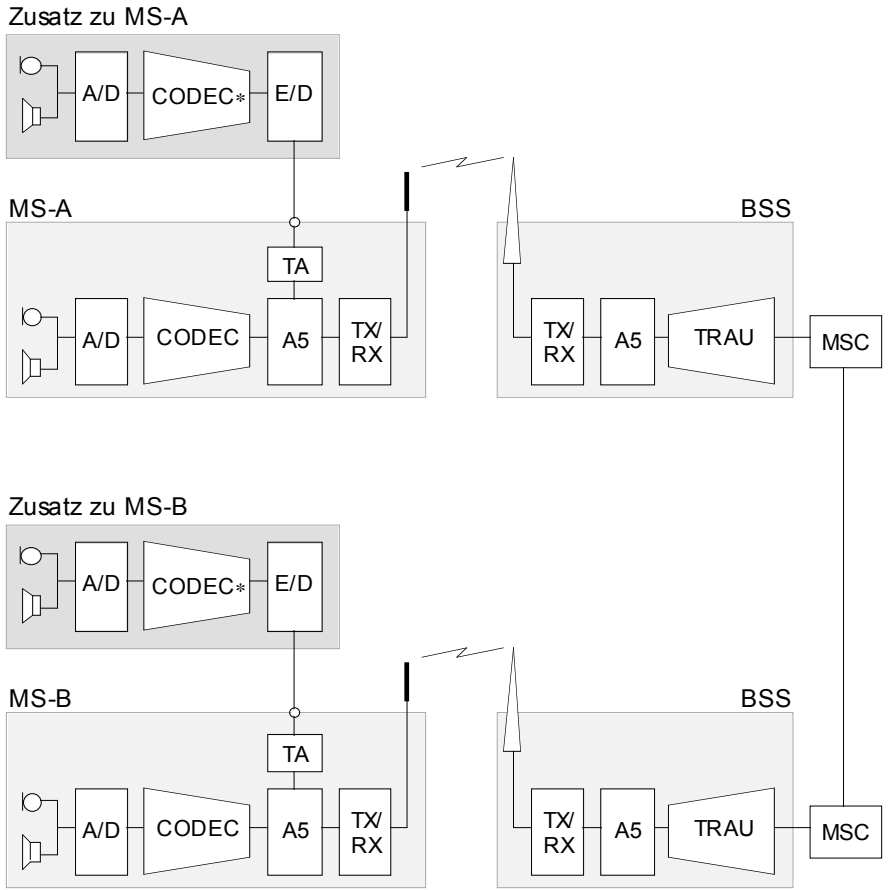
  - Both is not GSM standards conform add-on
  - Users need compatible devices or software on MS

Signaling of channel type (speech, data) in GSM



MS	Mobile Station	A5	GSM Link Encryption
BSS	Base Station Subsystem	TX/RX	Transmitter/Receiver
A/D	Analog-Digital-Converter	TRAU	Transcoder/Rate Adaption Unit
CODEC	Speech Coder/Decoder	MSC	Mobile Switching Centre
TA	Terminal Adaption		

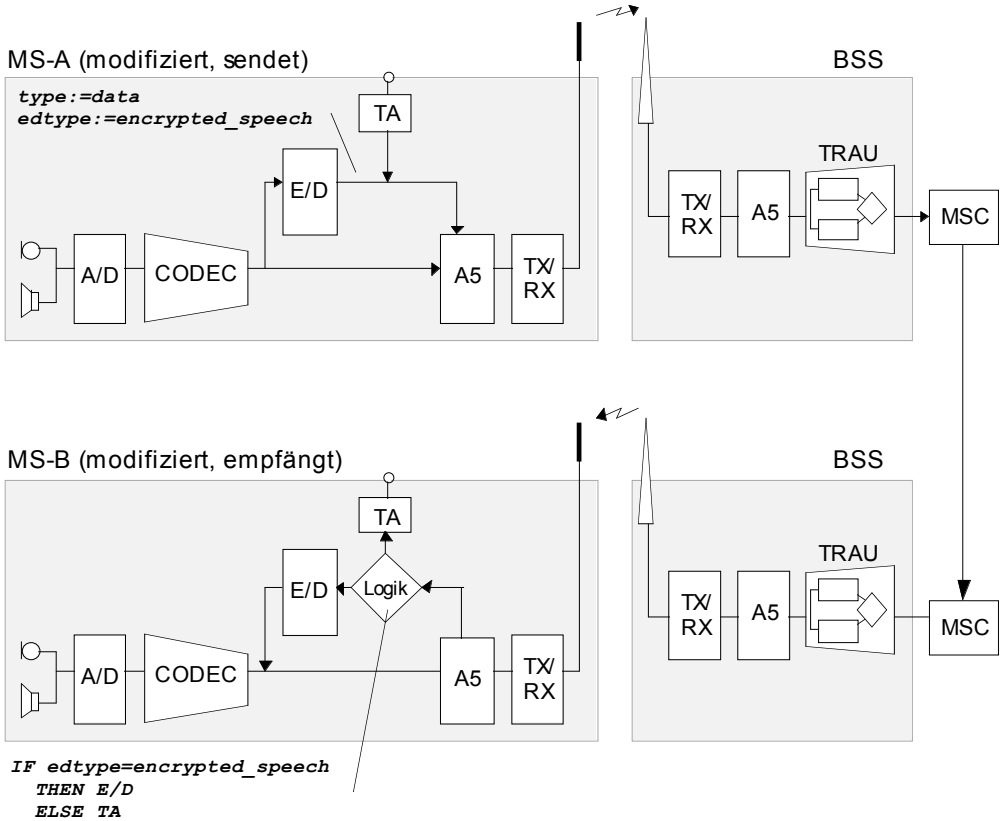
Bit transparent data channel for end-to-end speech encryption



Example:

TopSec MED
(Rohde&Schwarz):
external device bluetooth connected to mobile phone

Bit transparent data channel – internal use for end-to-end enc.

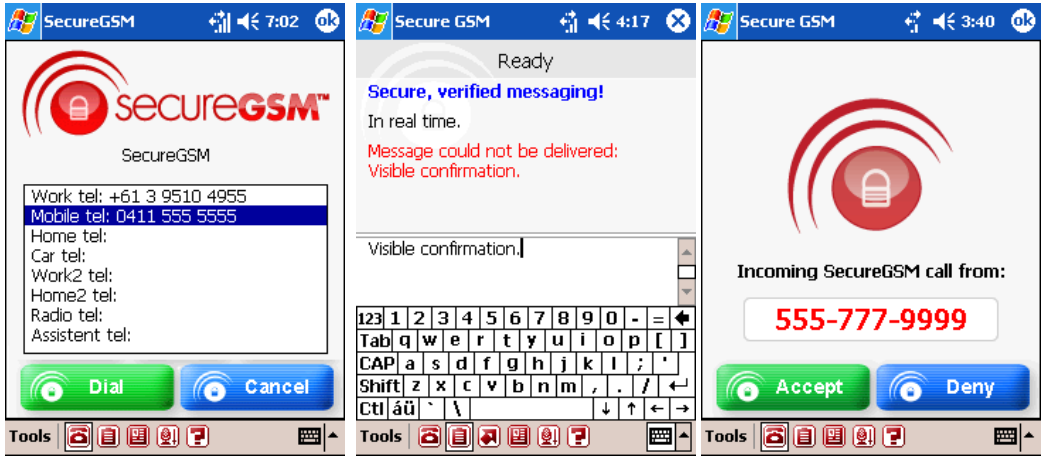


Example:

TopSec GSM
(Rohde&Schwarz): modified Siemens S35i with Crypto processor, 128 bit encryption

Software solutions for end-to-end encryption

- Historic example: SecureGSM · http://www.securegsm.com
  - For Windows Mobile Smartphones
  - Bit transparent data channel used
  - Asymmetric key agreement (»4Kbit«)
  - Triple encryption with AES, Serpent and Towfish with triple 256 bit session keys



Screenshots: http://www.securegsm.com

Summary of security problems in GSM

- Hard
  - Weak link encryption protects against outsiders only
  - No bit transparent speech channels –> no end-to-end encryption
  - Location finding for insiders possible
  - Mutual authentication is missing

- Further
  - Symmetric encryption
  - No anonymous network usage possible
  - Trust into accounting is necessary

Security functions of further mobile Systems

UMTS and LTE

Bluetooth security

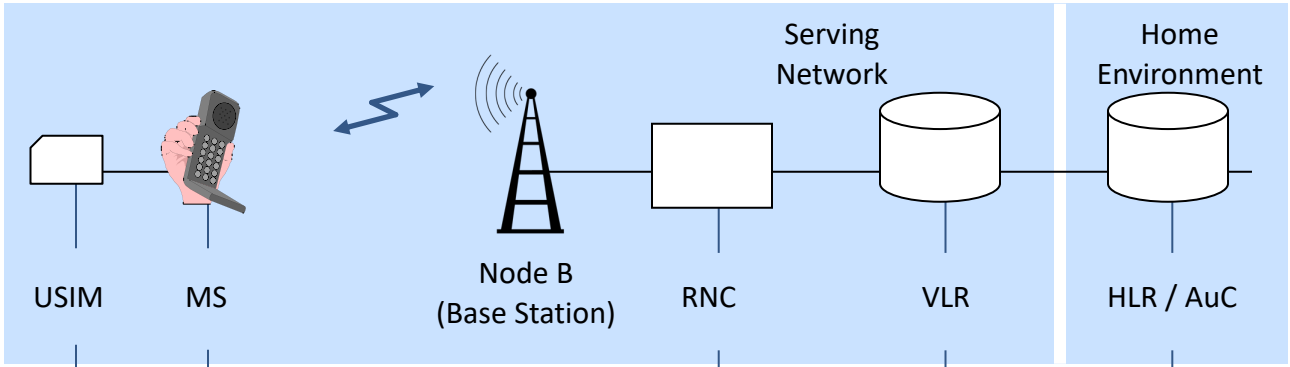
WiFi security

Universal mobile telecommunication system (UMTS)

- Security functions of UMTS –> inspired by GSM security functions
- From GSM
  - Subscriber identity confidentiality (TMSI)
  - Subscriber authentication
  - Radio interface encryption
  - SIM card (now called USIM)
  - Authentication of subscriber towards SIM by means of a PIN
  - Delegation of authentication to visited network
  - No need to adopt standardized authentication algorithms
- Additional UMTS security features
  - Enhanced UMTS authentication and key agreement mechanism
  - Integrity protection of signaling information (prevents false-base-station attacks)
  - New ciphering / key agreement / integrity protection algorithms

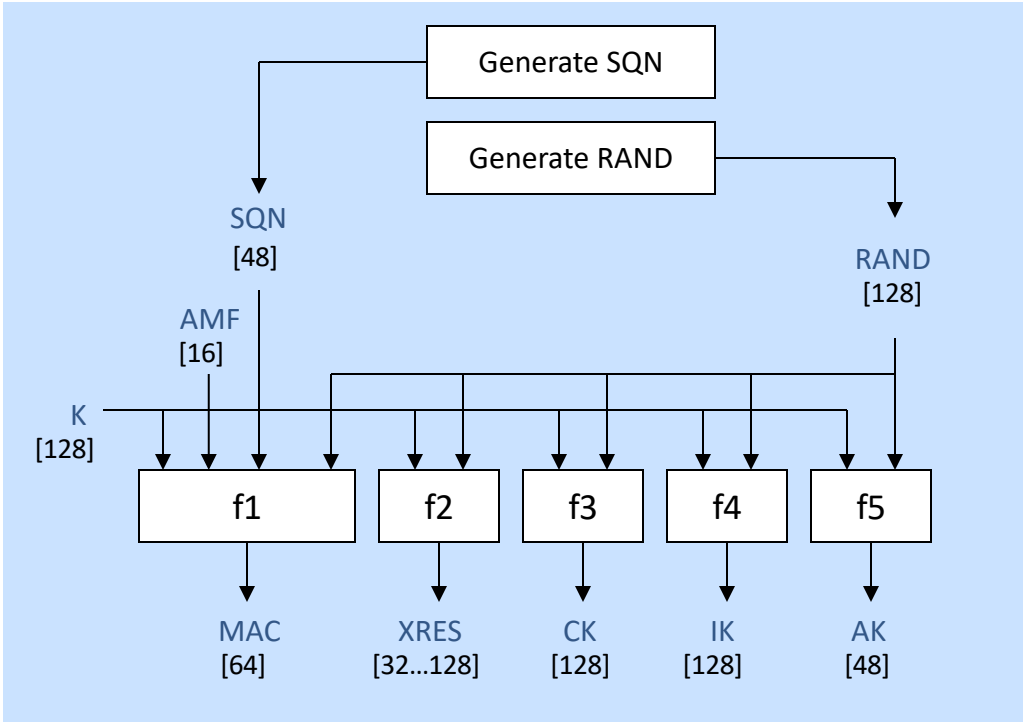
  … and a few minor features

UMTS Security Architecture



USIM	UMTS Subscriber Identity Module
MS	Mobile Station
RNC	Radio Network Controller
VLR	Visitor Location Reg.
HLR	Home Location Register
AuC	Authentication Centre

UMTS: Generation of authentication vectors (network side)



AUTN := SQN ⊕ AK || AMF || MAC

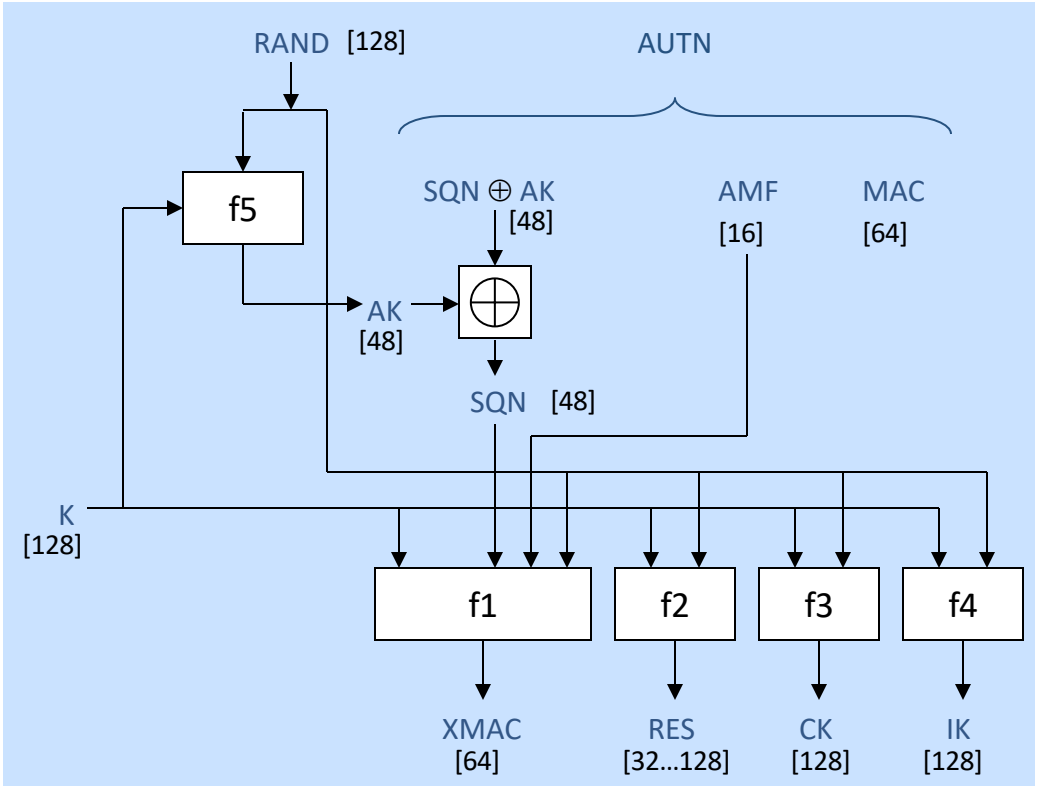
AV := RAND || XRES || CK || IK || AUTN

UMTS: Abbreviations

SQN	Sequence number
RAND	Random number
AMF	Authenticated Management Field
K	Secret Key
MAC	Message authentication code
XRES	Expected response
RES	Response
CK	Cipher key
IK	Integrity key
AK	Anonymity key
AUTN	Authentication token
AV	Authentication vector
[…]	# of bits

False-base-station attacks possible if attacker can eavesdrop AV on network internal communication lines

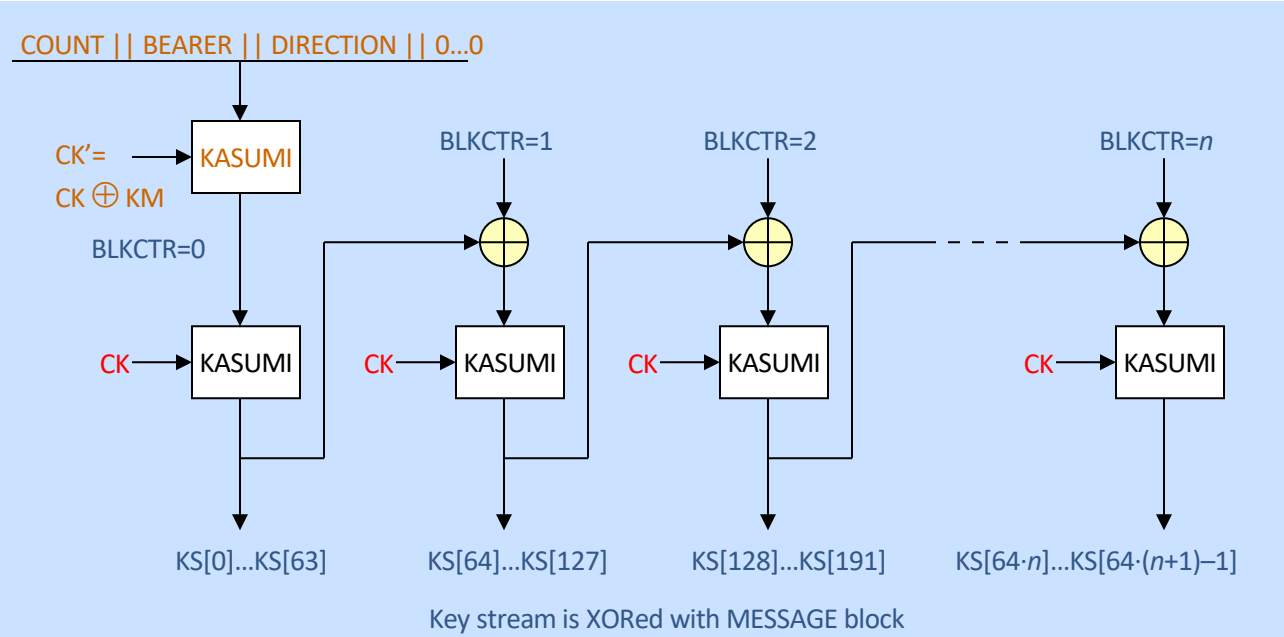
UMTS: Authentication function in the USIM (user side)



Verify MAC == XMAC, than verify that SQN is in the correct range

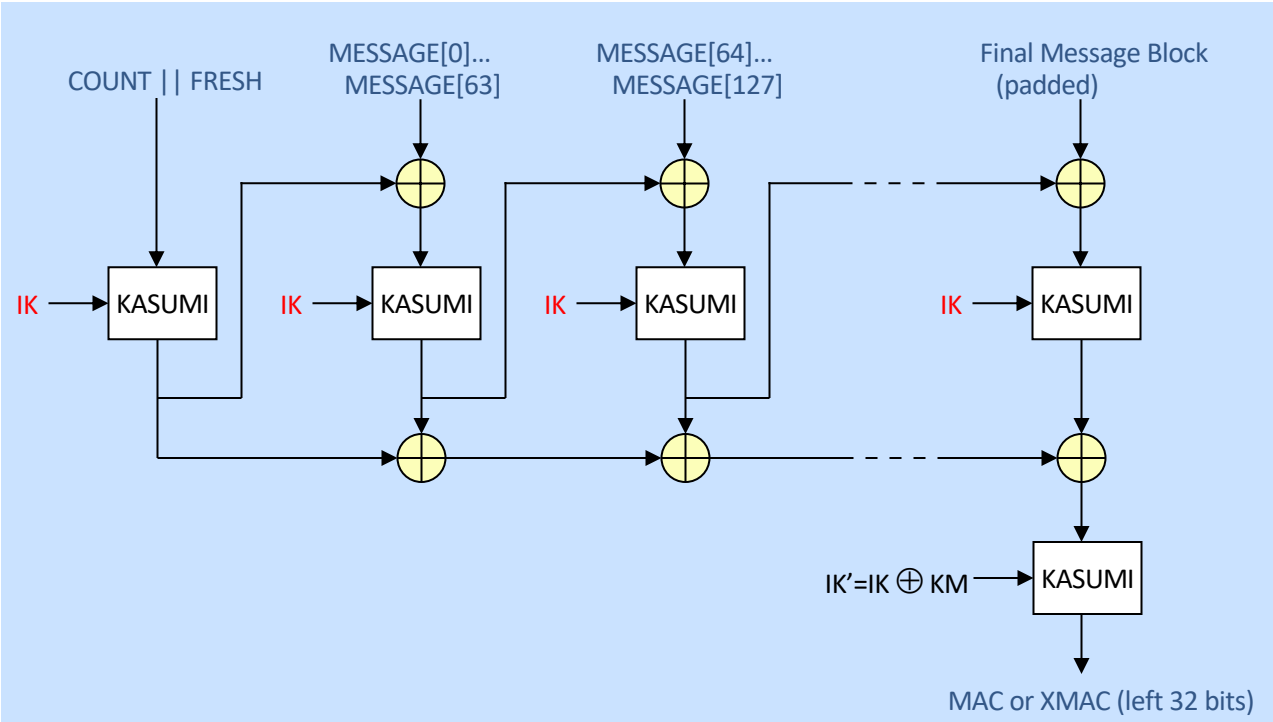
UMTS: Cipher algorithm f8

- Combination of Output Feedback mode (OFB) and counter mode
- First encryption under CK' prevents chosen plaintext attacks (initialization vector is encrypted, KM: key modifier)



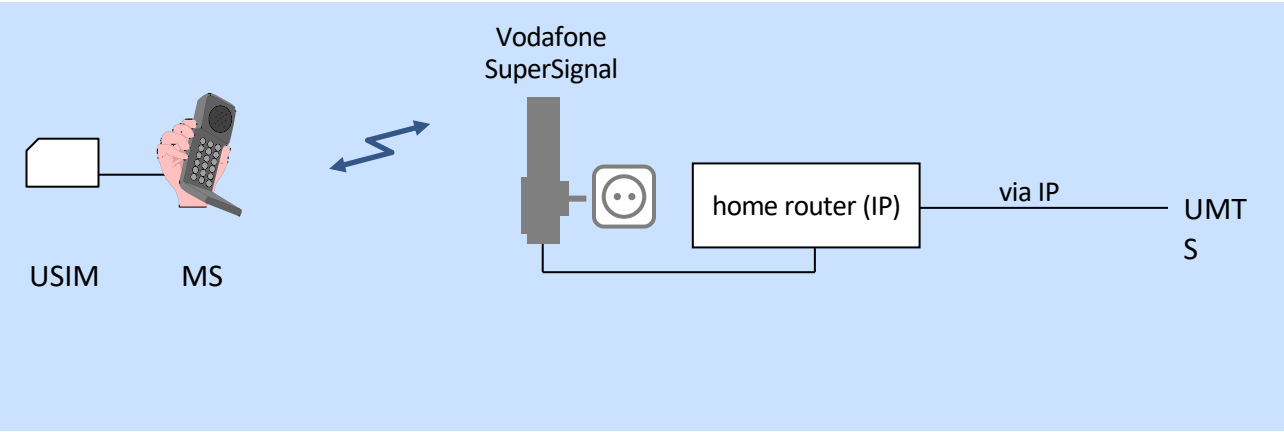
UMTS: Integrity algorithm f9: ISO/IEC 9797-1 (MAC algorithm 2)

- Sender and receiver use f9
- Receiver verifies MAC == XMAC



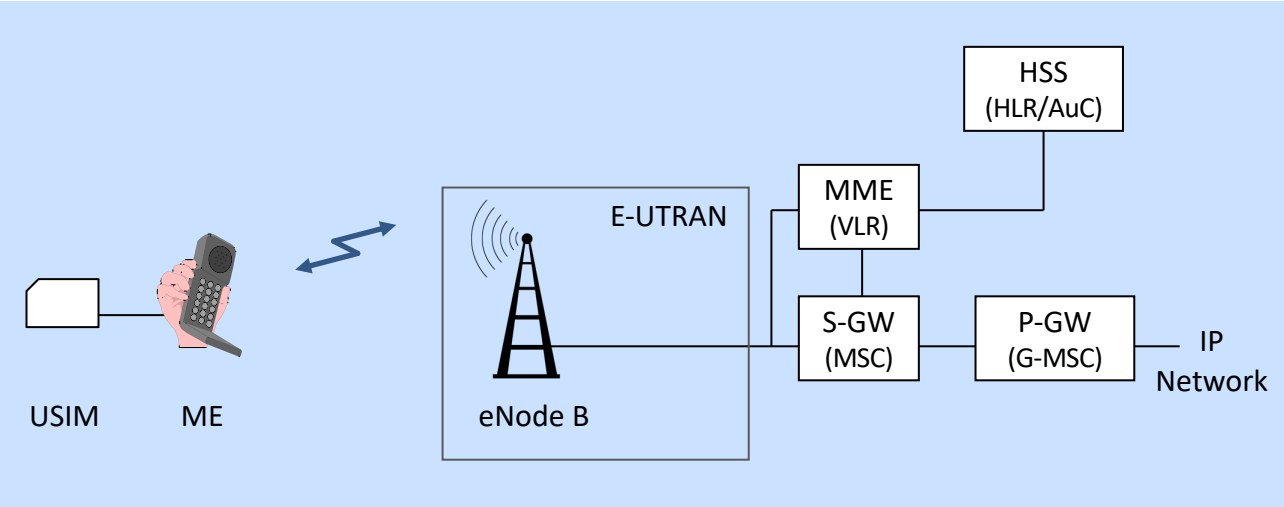
Own base station in UMTS

- Example: Vodafone SuperSignal
  - base station connected via IP with UMTS network
  - femto cell at home, not a repeater



Source: http://www.vodafone.de/business/hilfe-support/umts-basisstation-vodafone-supersignal.html

Long Term Evolution (LTE) Architecture



USIM	UMTS Subscriber Identity Module
ME	Mobile Equipment
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
MME	Mobility Management Entity
HSS	Home Subscriber Service
S-GW	Serving Gateway
P-GW	Packet Data Network Gateway
IP	Internet Protocol

Long Term Evolution (LTE)

- Characteristics
  - Traffic channels: Data services only, Speech is realized via Voice-over-IP
  - SMS is realized via signalling messages (similar to GSM)
- Security: inspired and closely related to UMTS
  - Individual symmetric key at USIM and HSS
  - Authentication vector
    - Calculated at USIM and HSS
    - Checked at MME
  - Pseudonymization on air interface:
    - Globally Unique Temporary Identity (GUTI)
  - Data encryption
    - Air interface: Advanced Encryption Standard (AES)
    - Network internal communication: IPSec

      -> False-base-station attacks: impossible