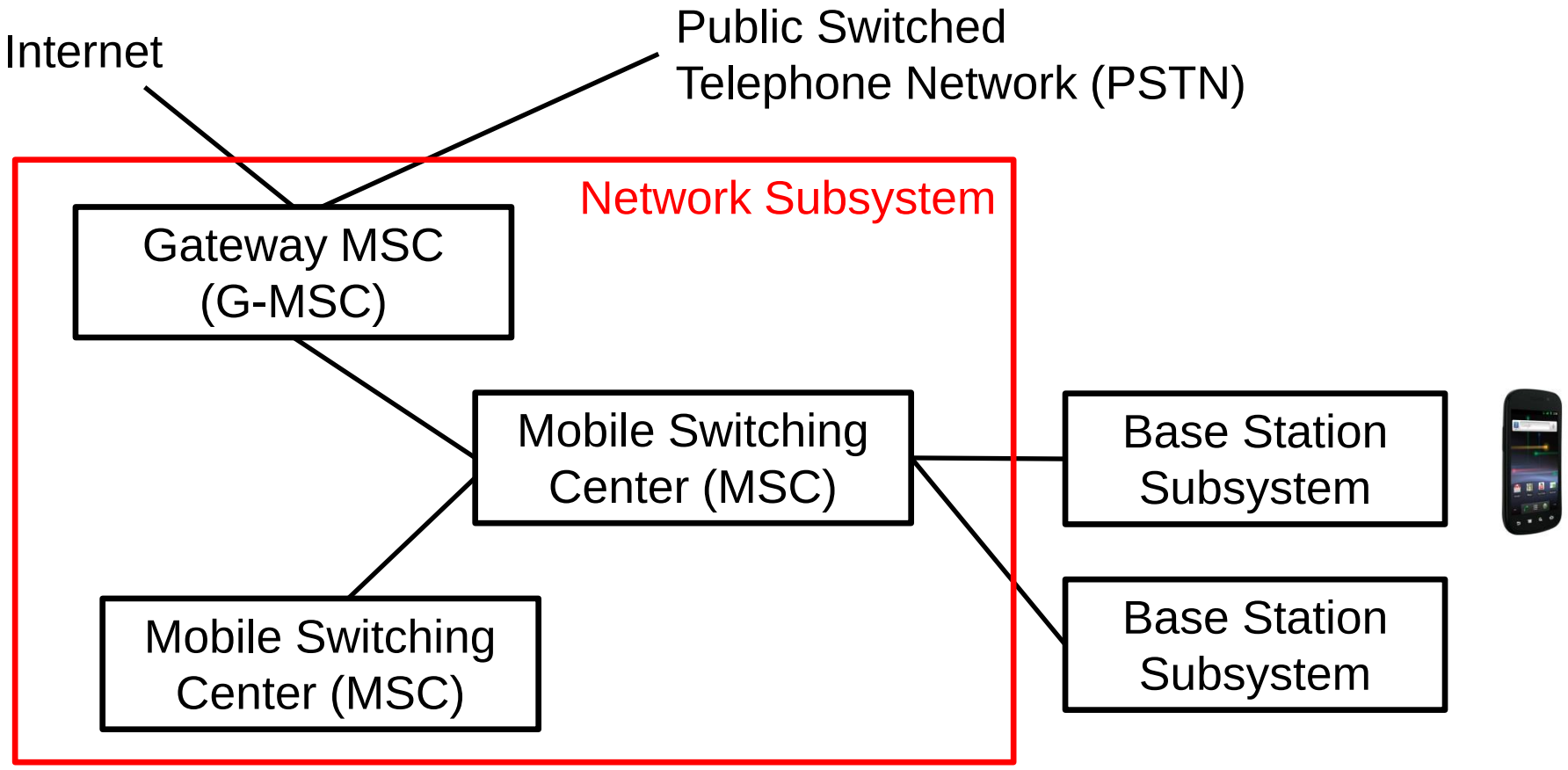
GSM Network

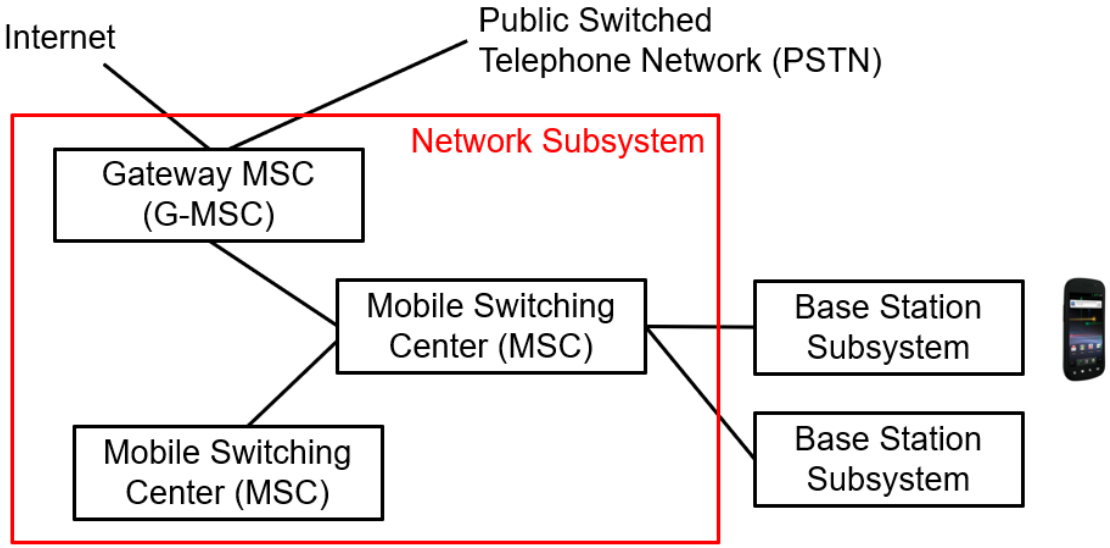
Network Subsystem



- Signaling with SS7 protocols running on top of MTP-3

Mobile Switching Center (MSC)

- MSC are responsible for switching phone calls between mobile stations or with fixed-line phones
  - G-MSC = MSC with gateway to PSTN or Internet
- A MSC is responsible for one or several BSS
- Since MS can roam freely between cells and even between operators, the MSC must keep track of the location of the MS (otherwise, calls to the MS can not be routed to the right BSS)



MSC

- An MSC has access to several databases:
  1. Equipment identity register (EIR): List of blocked, faulty, to-be-monitored devices.
     - Ideally, worldwide (not in practice)
  2. Home location register (HLR)
  3. Visitor location register (VLR)
  4. Authentication center

Home Location Register (HLR)

- HLR is the subscriber database of a GSM network
- Contains a record for each subscriber
- Each subscriber has a home area that is served by exactly one HLR
- A record contains for each SIM card:
  - International Mobile Subscriber Identity (IMSI) = Unique ID
  - One or more Mobile Subscriber International ISDN Numbers (MSISDN) = Phone numbers
  - Profile data (name, roaming limits etc.)
  - Temporary data
    - Mobile Subscriber Roaming Number
    - Current VLR and MSC address (next slide)
    - Authentication data, billing data

IMSI and MSISDN

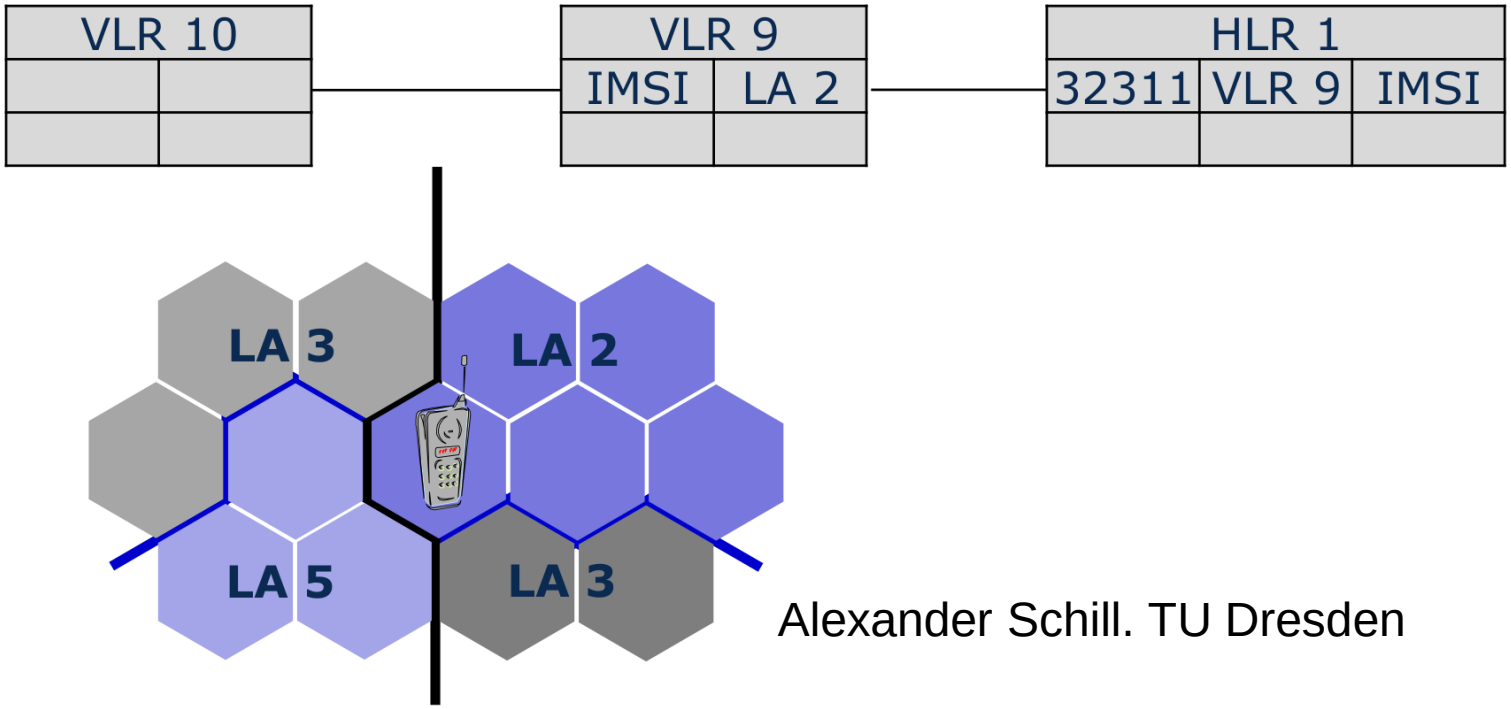
- IMSI = Country code + Network code + Subscriber ID
  - Example: 310150123456789

    Mobile Country Code 310 (USA)
    Mobile Network Code 150 (AT&T Mobility)
    Mobile Subscriber Identification Number 1234…
- IMSI is the key identifying the SIM card
  - Stored in the HLR and on the SIM card
  - MSISDN (phone numbers) not stored on SIM card!
- When the MS is switched on or enters a cell:
  1. MS sends IMSI to MSC
  2. MSC analyses the country code and network code
  3. MSC sends request to HLR to retrieve the record
- Advantages of separating IMSI and MSISDN: MSISDN can be changed afterwards

Visitor Location Register (VLR)

- Local database of an MSC (often built into MSC)
- Each base station served by exactly one VLR
- Contains information from HLR (or MS) when subscriber has roamed to VLR's service area
- Contains
  - Subscriber's ID number and phone number
  - Billing and accounting information
  - Roaming number: temporary phone number that can be used to find MS (includes MSC number)
  - HLR address
  - …

Localization

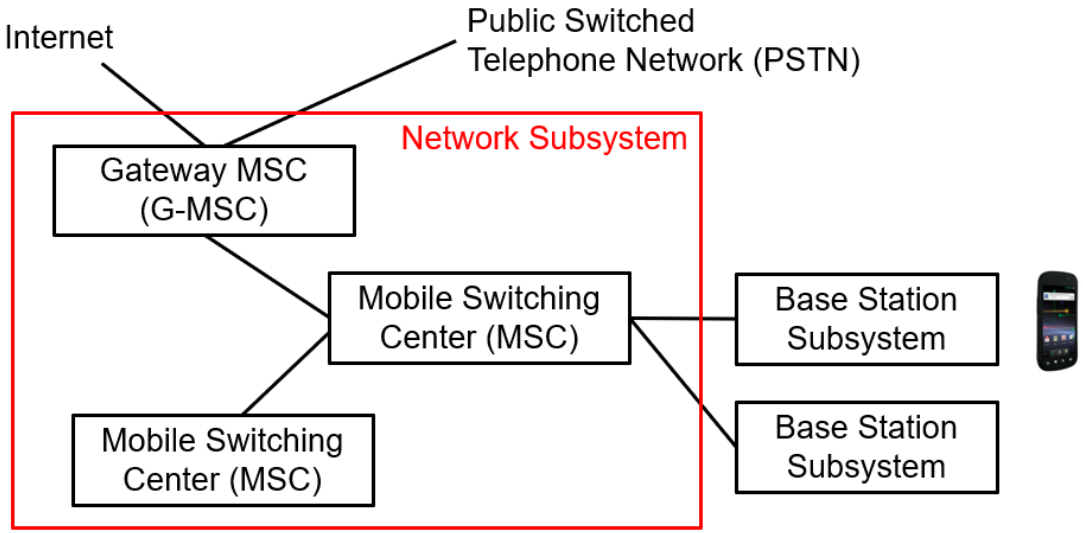


Alexander Schill. TU Dresden

- Service areas are divided into smaller location areas (LA)
- Small mobility of subscriber does not cause remote HLR update

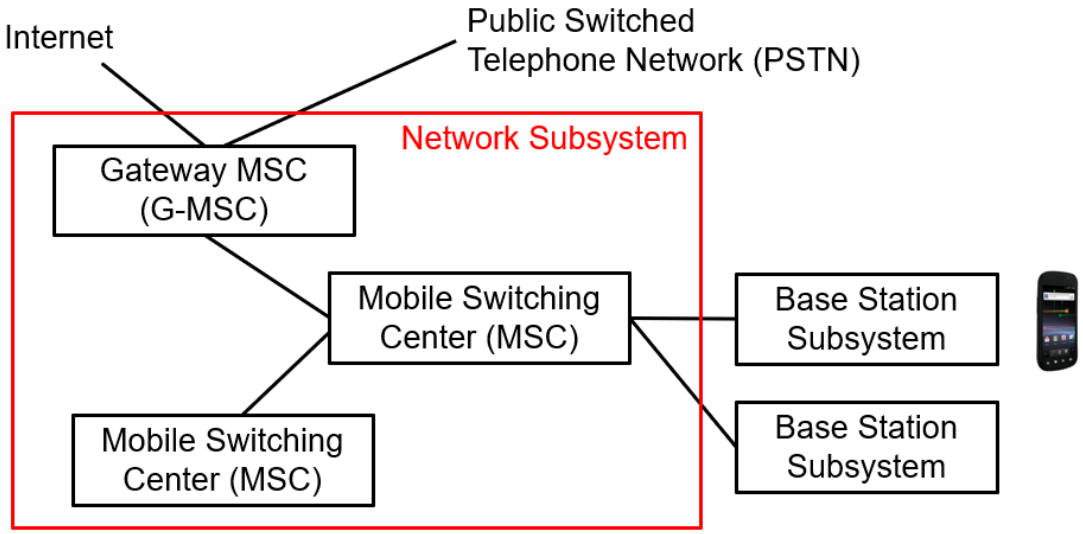
Call to MS

1. Call from fixed network switched to a G-MSC
2. G-MSC finds HLR from phone number
3. HLR checks participant profile and asks VLR for roaming number (assigned per call or registration)
4. G-MSC contacts current MSC
5. MSC asks VLR for state of MS (active?)
6. MSC sends call to all cells of Location Area
7. MS answers call
8. Security checks
   + connection setup



Call from MS

1. Connection request from MS to BSS
2. BSC forwards request to MSC
3. MSC and VLR perform authorization control
4. Switched to fixed network through G-MSC



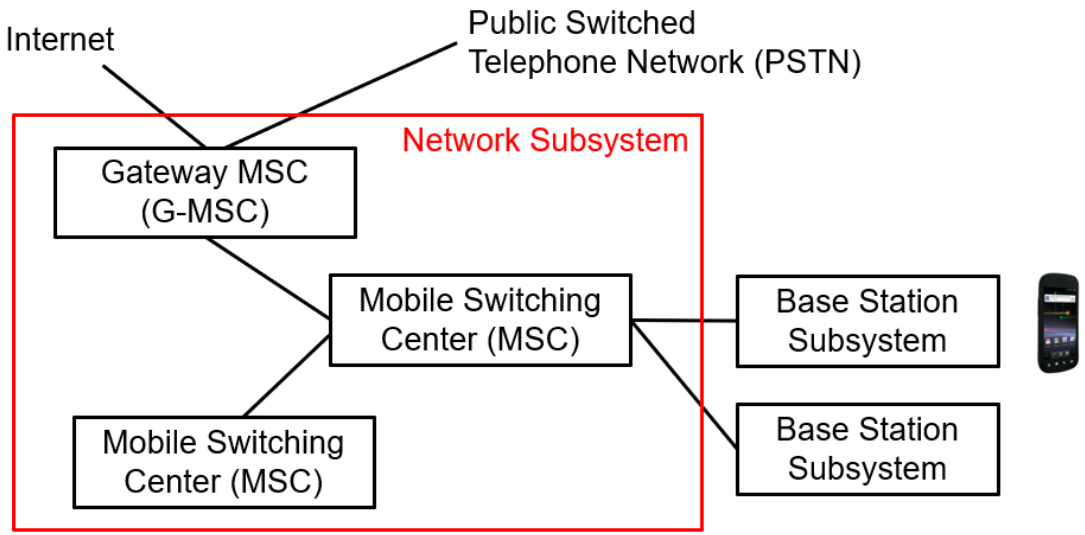
Handover

- MS can freely move
- BSC can decide to do a handover based on signal quality
  - BTS constantly measures signal quality and reports to BSC
  - MS also reports quality of signals it receives from other cells

- Three scenarios:
  - Intra-BSC handover: old and new cell connected to same BSC
  - Inter-BSC handover: old and new cell connected to different BSCs, but same MSC
  - Inter-MSC handover
- For MS, no difference between the three scenarios

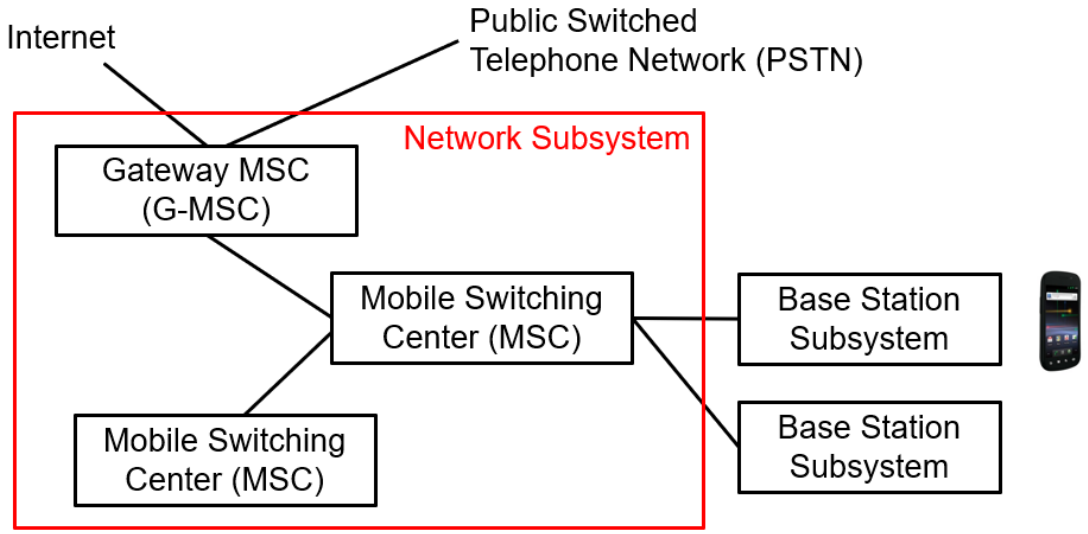
Intra-BSC handover

- Easy:
  1. BSC activates a TCH in new cell
  2. BSC informs MS via old cell to handover to new TCH
  3. Once MS and BTS have confirmed handover, BSC redirects voice data to new cell and deallocates old TCH



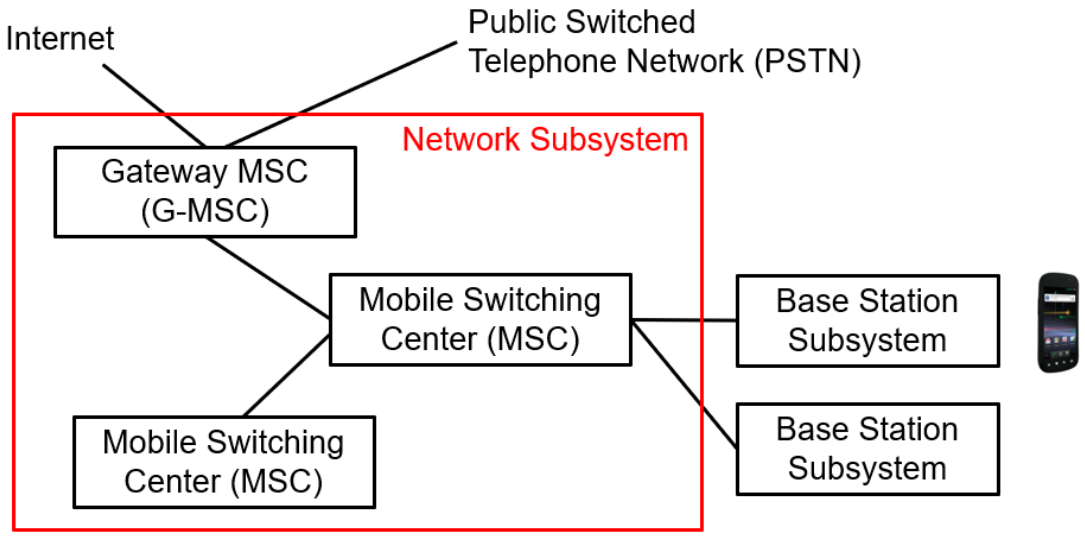
Inter-BSC handover

- Inter-BSC handover more complicated
  1. BSC of old cell asks MSC to initiate handover
  2. MSC asks BSC of new cell to prepare a TCH
  3. MSC notifies MS to handover
  4. Once MS and BSC have confirmed handover, MSC redirects voice data and tells old BSC to close old TCH



Handover: Scenarios (2)

- Inter-MSC
  1. Old MSC sends handover request to new MSC
  2. New MSC contacts new BSC to establish TCH
  3. Etc.
  4. Etc.



Security

- GSM security consists of
  - Authentication: MS is authenticated
  - Encryption: communication between MS and BTS is encrypted
- Keys of IMSI are stored in Authentication Center and in SIM card
- Algorithms implemented in the GSM network and on the SIM card

Authentication

- Symmetric key *Ki* (max. 128bit) for IMSI stored in SIM card and in Authentication Center
- MS authentication:
  1. Authentication Center generates
     - a 128bit random number RAND
     - a 32-bit signed response SRES = A3(Ki,RAND)
  2. MSC sends RAND to MS
  3. SIM card also computes SRES
  4. Response sent back to MSC
  5. MSC compares responses

Authentication (2)

- The A3 algorithm is not standardized
  - Different implementations exist
  - Network operator can choose their own implementation
  - Of course, MSC and the SIM card must know it.
- New RAND and SRES generated for each authentication
- For speed-up, several RAND/SRES computed in advance and buffered in MSC and VLR

Encryption: Session Key

- Data exchanges between MS and BTS are encrypted
- First step: Creation of a 64-bit session key *Kc*
  - Similar to authentication: Authentication center computes Kc = A8(Ki,RAND)
  - MSC sends RAND to MS, so MS can also compute Kc

- Session key can be changed, e.g., at regular intervals
- A8 often implemented together with A3 because of similarity

MSC and MS use *Kc* and *A5* algorithm to encrypt/decrypt data

Data Encryption

- A5 algorithm = set of algorithms A5/1,A5/2,… Operator chooses which one to use

- Input:
  - Kc
  - Current frame number N: different for every burst
- Output:
  - 114-bit sequence C = A5/*x*(Kc,N)
- Encryption:

  Encrypted burst = Original burst data XOR C

How good was the security in GSM?

Good:

- Keys and key generation inside SIM card, not by phone OS

Bad:

- Algorithms were secret and not publicly discussed. Hackers managed to reverse engineer and break them
- 128bit key length: Too short for modern computers
- Communication between BTS and BSC not encrypted
- MS is authenticated to network but not vice versa! Attacker can pretend to be network operator by installing a “fake” base station
- Symmetric keys: Network operator knows all keys
- No end-to-end authentication & encryption