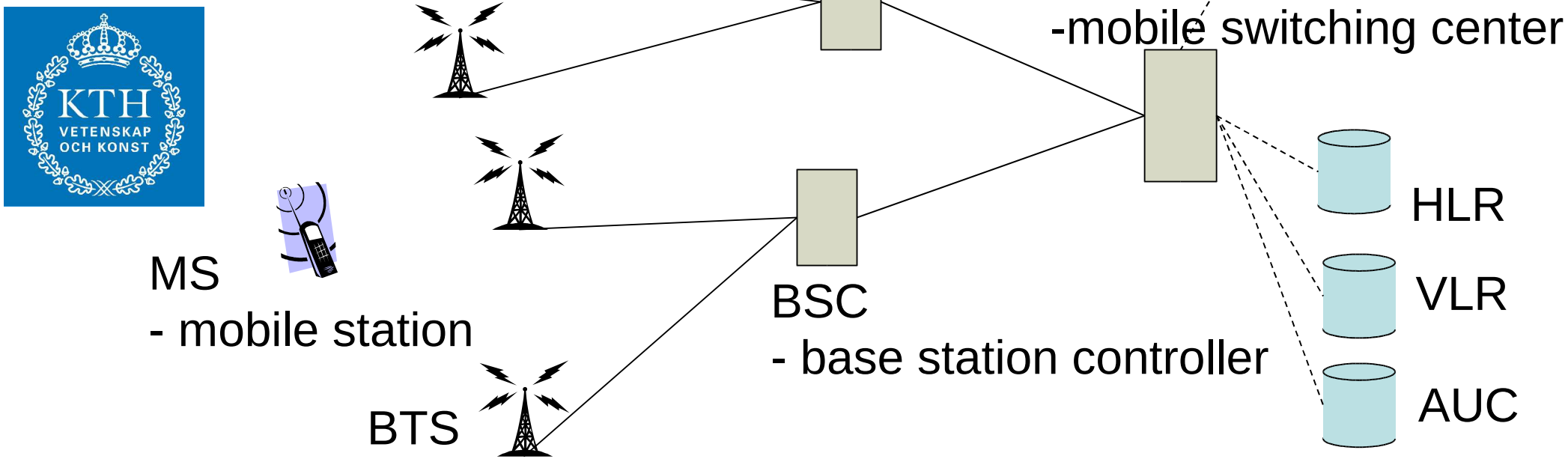
GSM Network and Services

Nodes and protocols

- or a lot of three letter acronyms

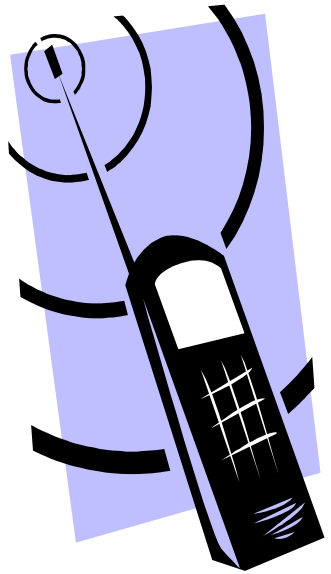
A GSM network



PLMN - public land mobile network

The mobile station

- Mobile station (MS) consist of
  - Mobile Equipment
  - Subscriber Identity Module (SIM)
- The operator owns the SIM
  - Subscriber identity
  - Secret keys for encryption
  - Allowed networks
  - User information
  - Operator specific applications



Mobile station addresses - IMSI

- IMSI - International Mobile Subscriber Identity
  - 240071234567890
    - Mobile Country Code (MCC), 3 digits ex 240
    - Mobile Network Code (MNC), 2 digits ex 07
    - Mobile Subscriber Id Number (MSIN), up to 10 digits
  - Identifies the SIM card

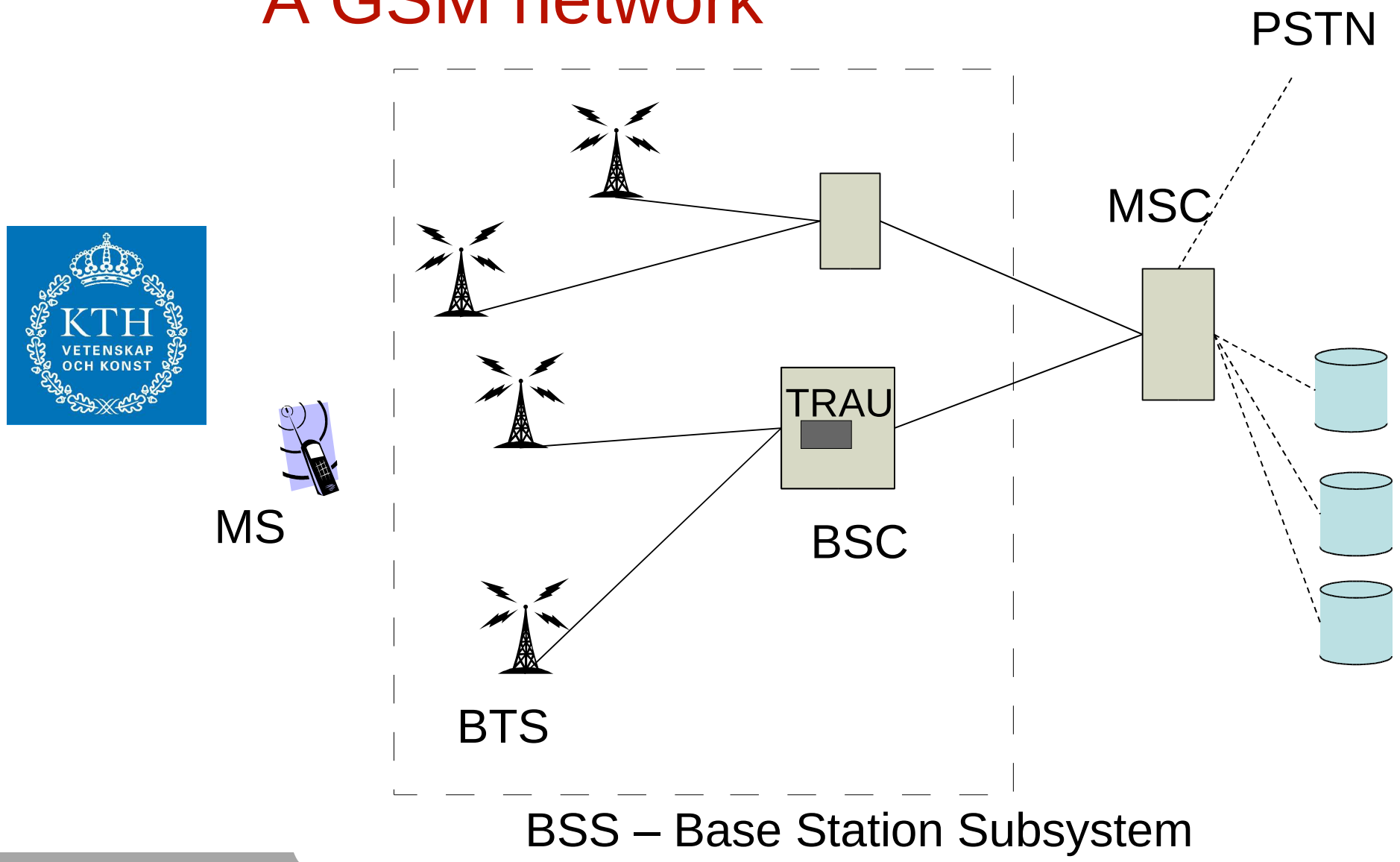
Mobile station addresses - IMEI

- IMEI – International Mobile Equipment Identity
  - fifteen digits written on the back of your mobile
  - has changes format in phase 2 and 2+
  - Type Allocation (8), Serial number (6), Check (1)
  - Used for stolen/malfunctioning terminals

Address of a user - MSISDN

- Mobile Subscriber ISDN Number - E.164
  - Integrated Services Digital Networks, the services of digital telephony networks
  - this is your phone number
- Structure
  - Country Code (CC), 1 – 3 digits (46 for Sweden)
  - National Destination Code (NDC), 2-3 digits (709 for Vodafone)
  - Subscriber Number (SN), max 10 digits (757812 for me)
- Mobile networks thus distinguish the address to *you* from the address to *the station*. This is something that PSTN also would benefit from.

A GSM network



BTS – Base Transceiver Station

- A BTS handles 2 to 6 transceivers connected to one to three antennas.
- Each transceiver handles a carrier.
- Antenna configuration
  - 1 omni-directional or sector
  - 2 to 3, each in a 180 or 120 degree sectors
- The transceivers of an antenna can be grouped in one or more cells covering the same area.
- Normally what you see is only the antenna, the actual BTS could be quite large.

BTS Identity Code - BSIC

- To be able to quickly tell the difference between base stations, or rather brodcasting channels operating in the same frequency, each base station is given a *color code*.
- The color code is not unique:
  - Network Color Code – NCC – 3 bits
  - BTS Color Code – BCC – 3 bits
- A PLMN has to internally assign BCC and agree with neighbouring PLMS on the NCC.

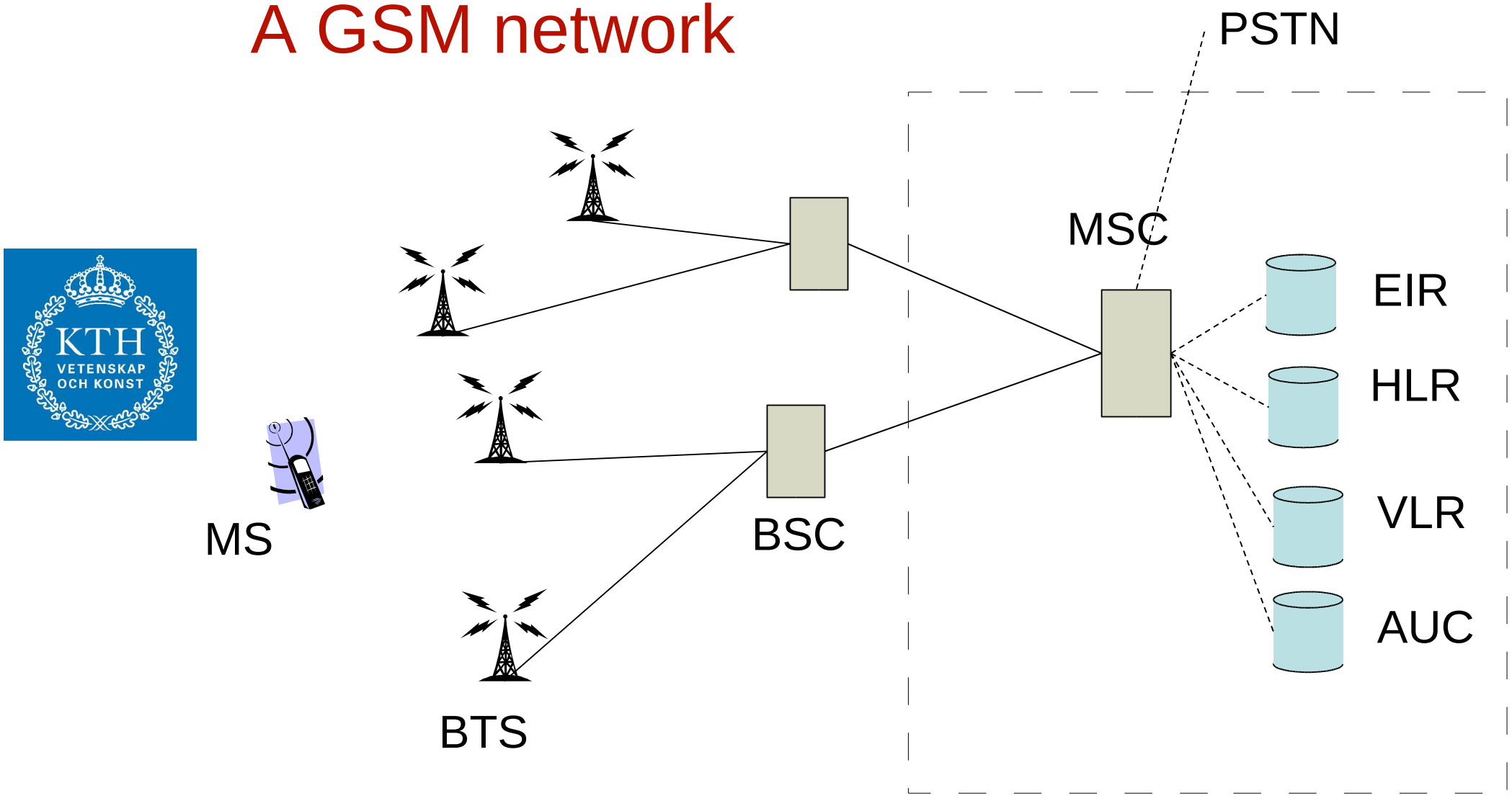
BSC – Base Station Controller

- The BSC handles everything that is related to the wireless network.
- An important role of the BSC is to configure the base stations, allocate resources to them and monitor their load.
- The functionality of the BSC could be distributed to the base stations but the base stations would be more complex and handover between base stations would be harder.

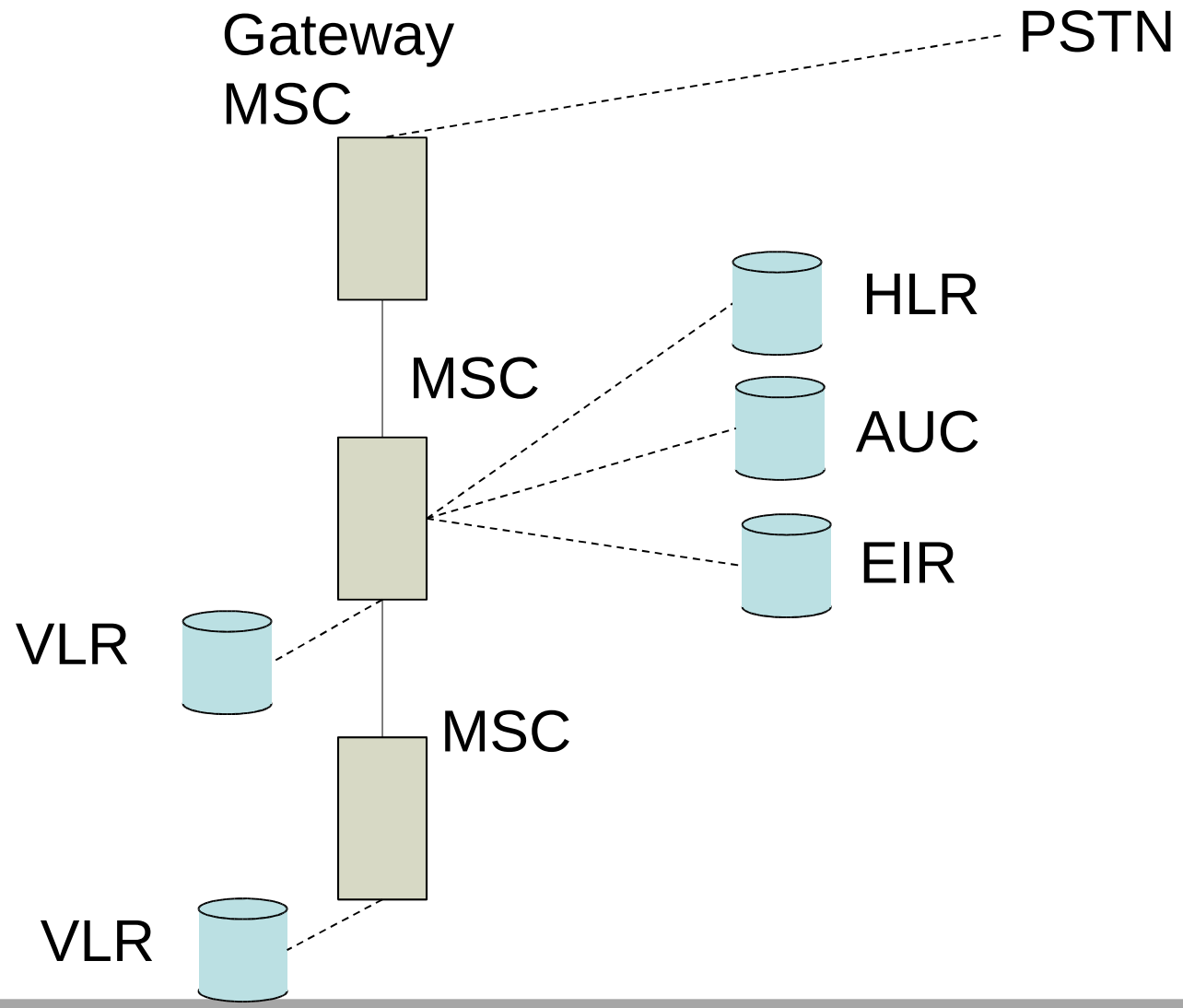
TRAU – transcoding and rate adapter unit

- The TRAU is often co-located with the BSC but could be a stand alone unit.
- Converts GSM coded voice (13/6.5 kbps) to regular ISDN code voice (64kbps).
- Why have a TRAU in the BSC and not in each BTS?
- Why have a TRAU at all?

A GSM network



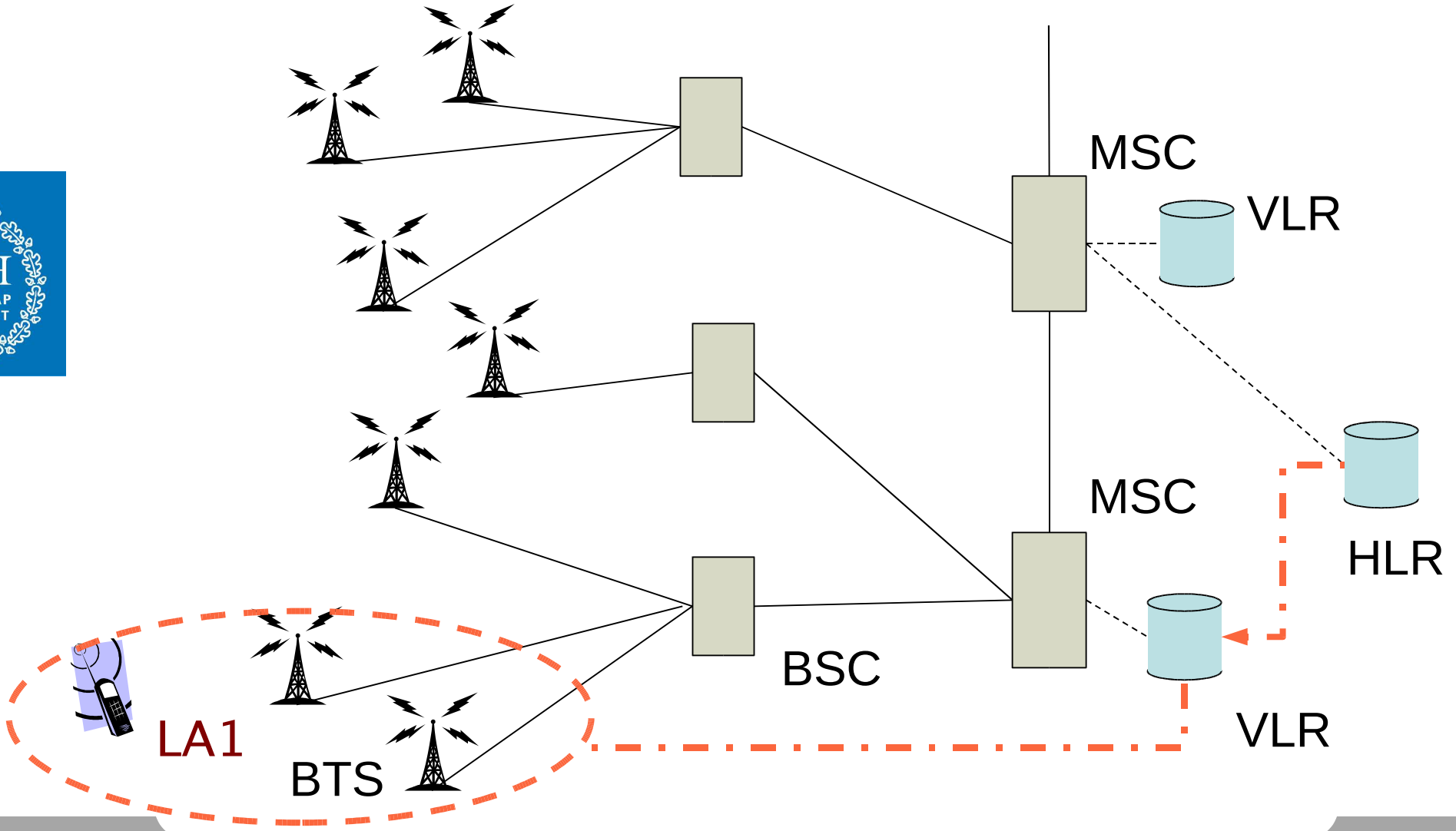
MSS – Mobile Switching Subsystem



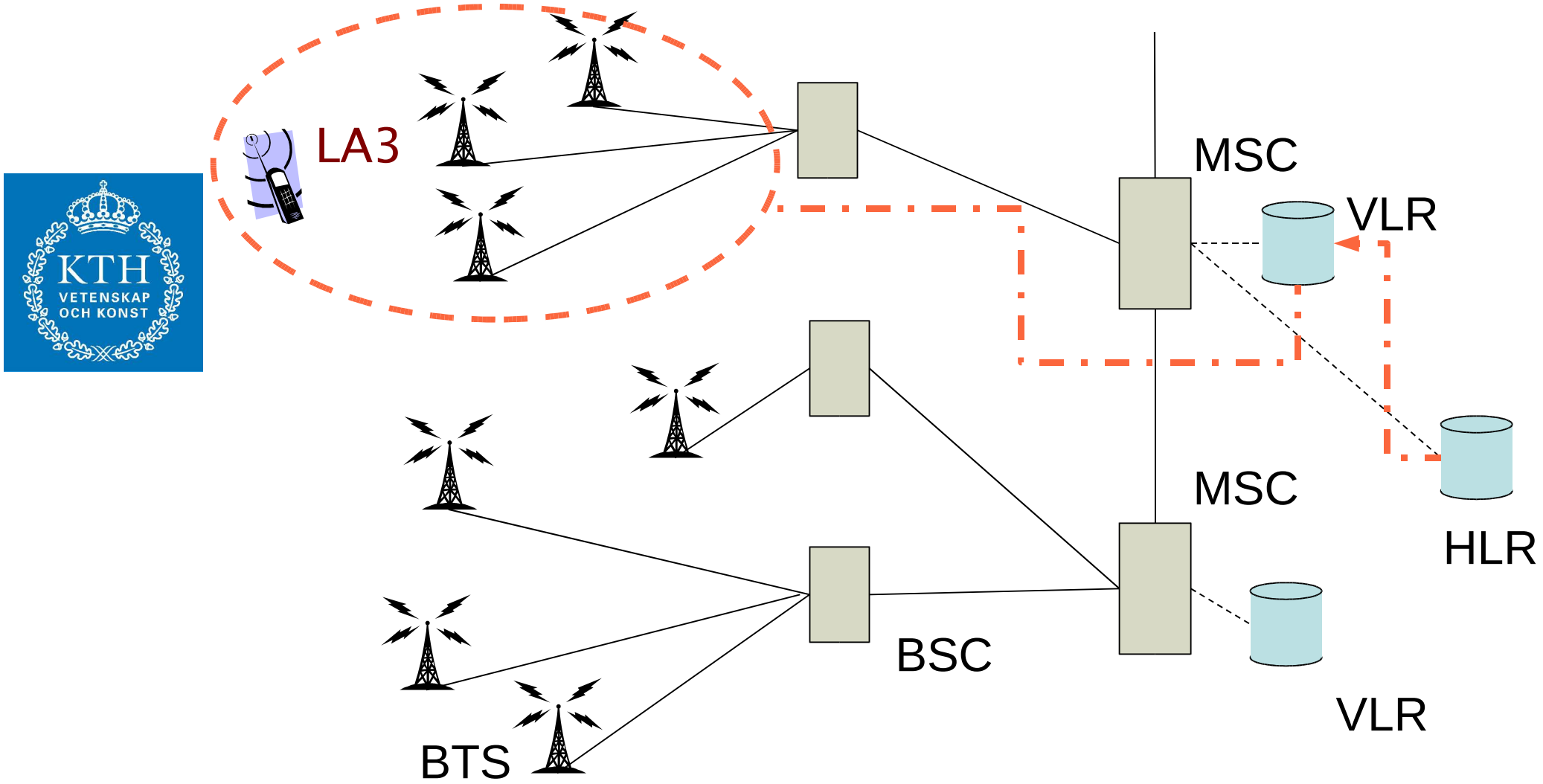
The databases

- HLR - Home Location register
  - maps phone numbers MSISDN, to subscribers IMSI
  - keeps the current VLR
- VLR - Visited Location Register
  - knows in which location area the subscriber can be found
- EIR - Equipment Identity Register
  - stolen phones (IMEI)
- Authentication Center
  - encryption keys for each SIM

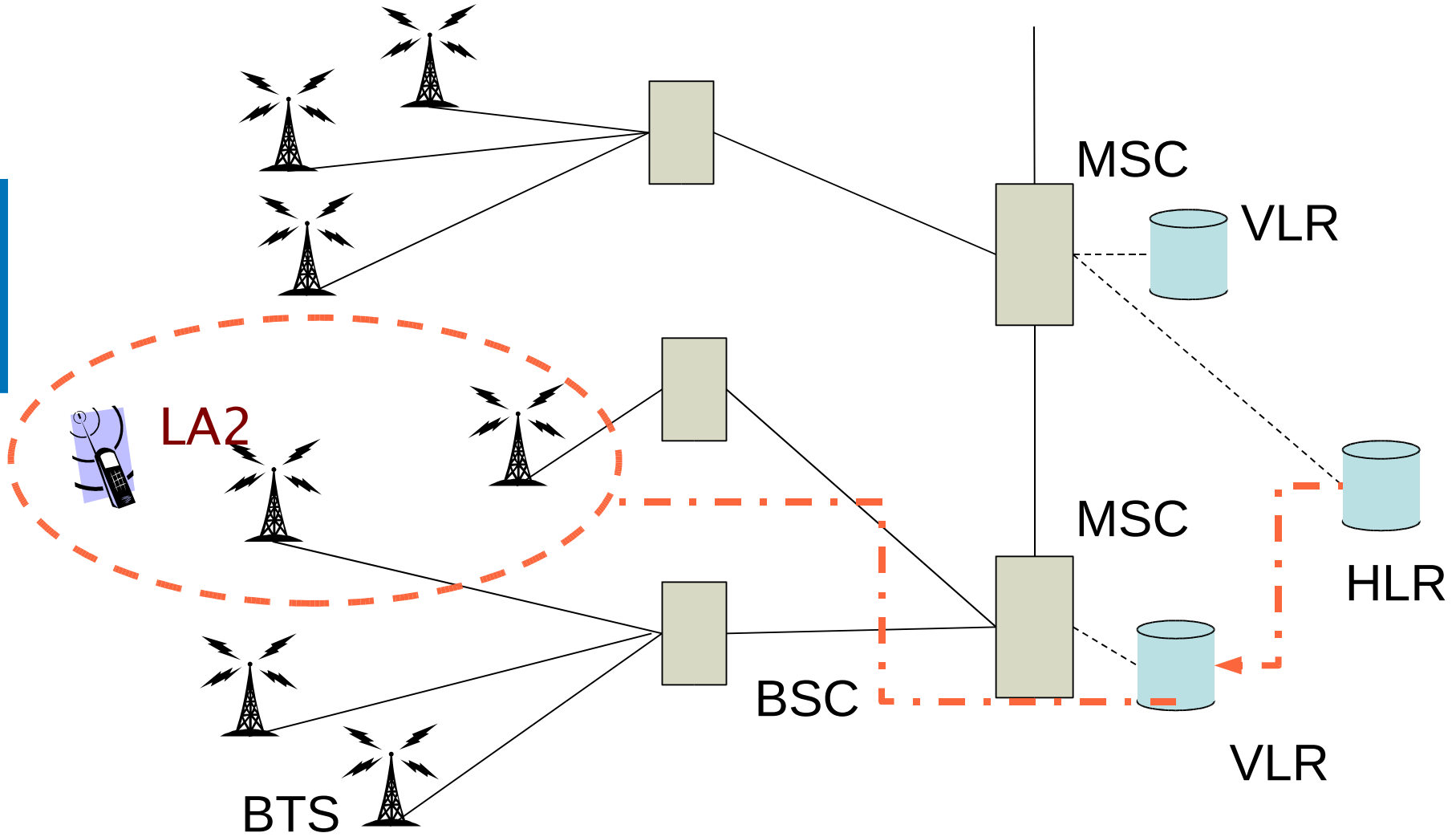
Location area



Location area



Location area



Location Area Identity

- MCC-MNC-LAC
  - Mobile Country Code, 3 digits
  - Mobile Network code, 2 digits
  - Location Area Code, 5 digits
- LAI is broadcasted by the BTS so a mobile station can determine if it has entered a new location area.
- If a new location area is entered the MSC is in formed and the VLR (and HLR) is updated.

Cell Identifier

- Each cell in a location area is allocated a Cell Identity, CI, constsing of 16 bits.
- The CI and LAI form a globaly unique identifier of a cell.

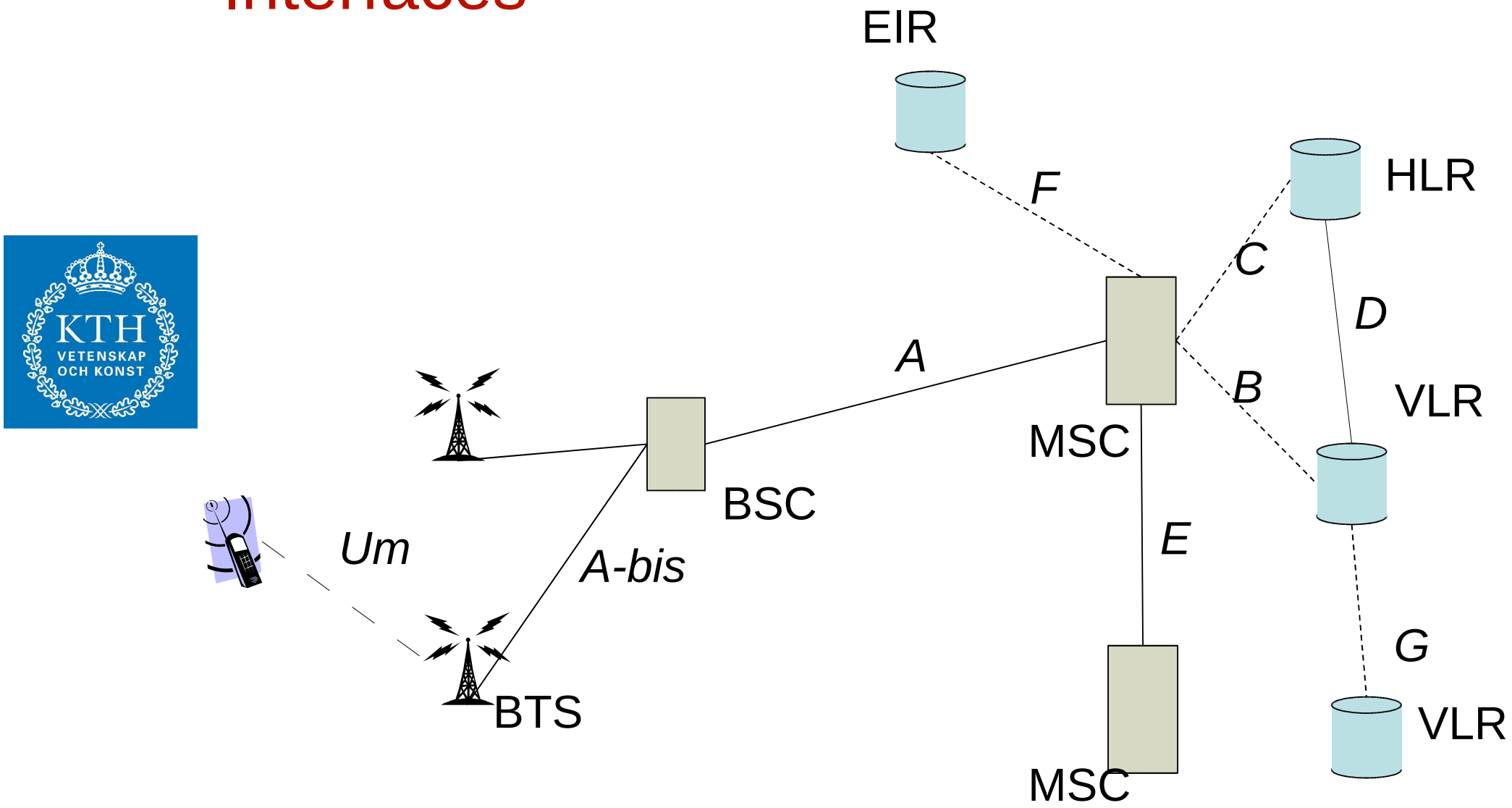
Authentication Center - AUC

- The AUC holds the secret key that is shared between the SIM and the network.
- The key never leaves the SIM nor the AUC.
- Network nodes can request the encryption of a set of challenges from the AUC. A challenge is then sent to the mobile station and if the respond matches the subscriber is authenticated.
- The authentication process also controls encryption for privacy.

Equipment Identity Register - EIR

- The EIR keeps a black list of stolen phones that should be barred from access.
- Stolen phones can be re-flashed with a new IMEI and thus avoid the EIR check.
- EIR can also block phones that are malfunctioning and disturb the network.

Interfaces



Signaling systems

- Mobile Switching Subsystem
  - The signaling in the MSS is buit on SS7.
  - Mobile Application Part – MAP is used between the MSC and databases.
  - BSSMAP is used between the MSC and BSC
- The Base Station Subsystem
  - uses LAPD, the signaling protocol of ISDN

Signaling

- The mobile Station commuincates with
  - The BTS for Radio Resources, RR
  - The BSC for Radio Resources, RR
  - The MSC for Call Control. CC, and Mobility Management, MM
- The BSC and BTS communicate using
  - BTS Management, BTSM
- The MSC and BSC communicate using
  - BSS MAP

Adding GPRS