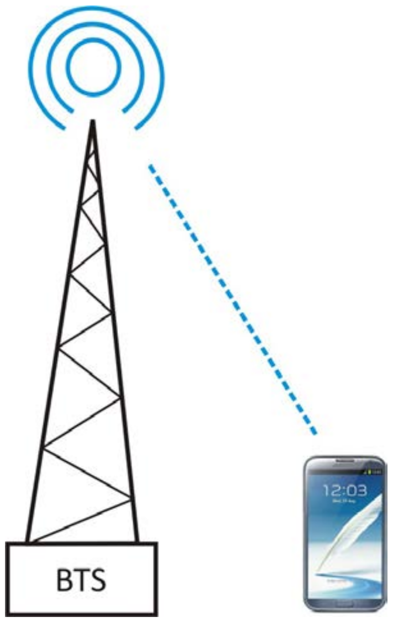
Security in Mobile System

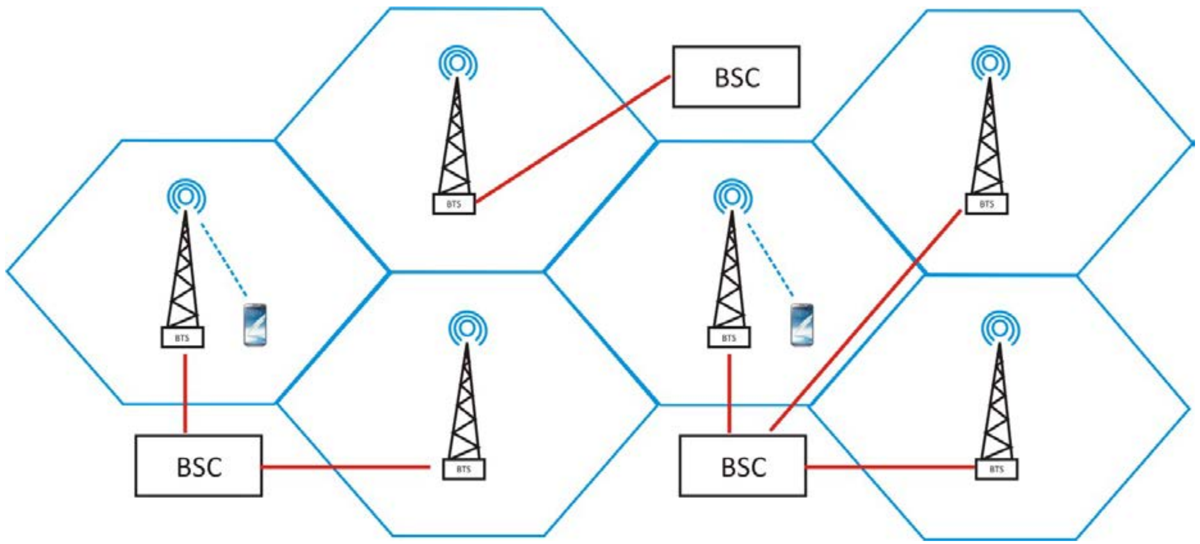
Prof. Dr. Eşref ADALI

www. Adalı.net

Elements of Mobile System

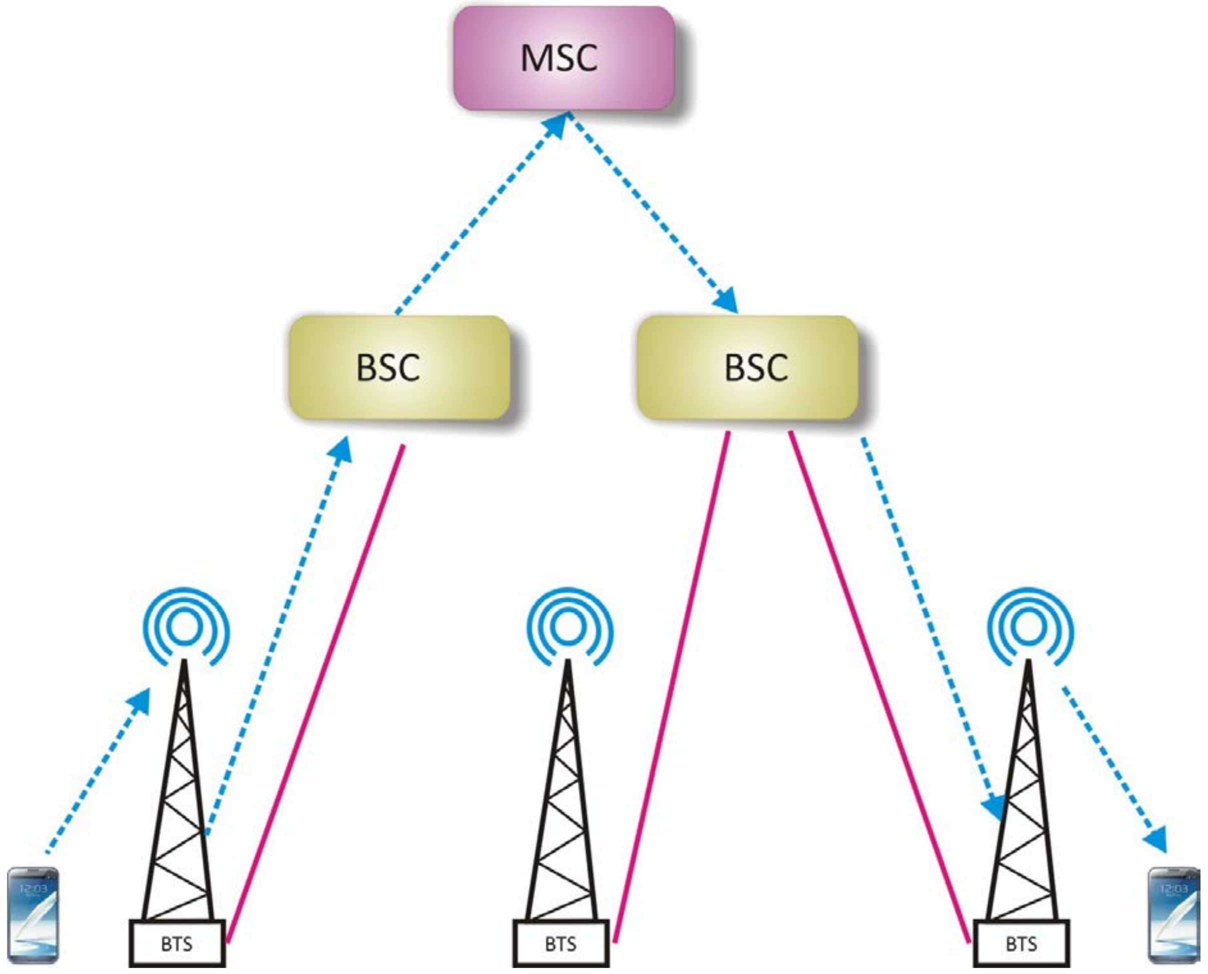
- MS : Mobile Station : Device have SIM card
- BTS : Base Transmitter Station : Base station that mobile device make connection
- BSC : Base Station Controller : Controller of base station
- MSC : Mobile Switch Center : Telephone switch for mobile devices
- HLR : Home Location Register : Database which consists of subscriber's information
  - ID : IMSI and MSISDN
  - Number
  - Current location





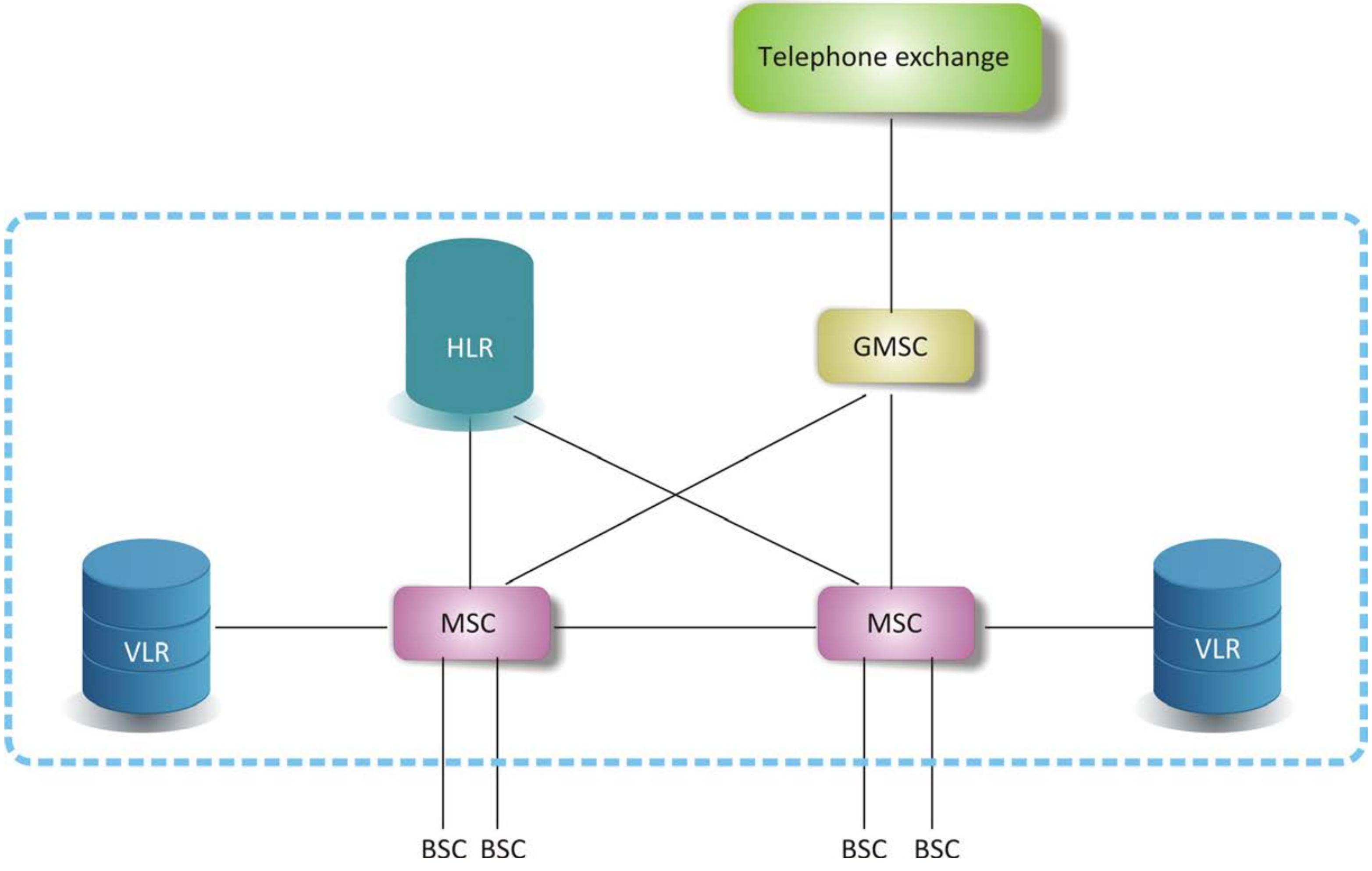
Connection of Mobile Devices

- VLR : Visitor Location Register : Database which consists of current and local information of subscriber
  - ID of local cell (LAI)
  - Temporary ID of subscriber (TMSI)
  - Mobile station roaming number (MSRN)
  - Condition of mobile device
- GNSC : Gateway MSC : Device which connects mobile switch and stationary switch.
- OMC : Operation and Management Center : Controller of wireless system
- AuC : Authentication Center : Authenticate the ID of mobile device



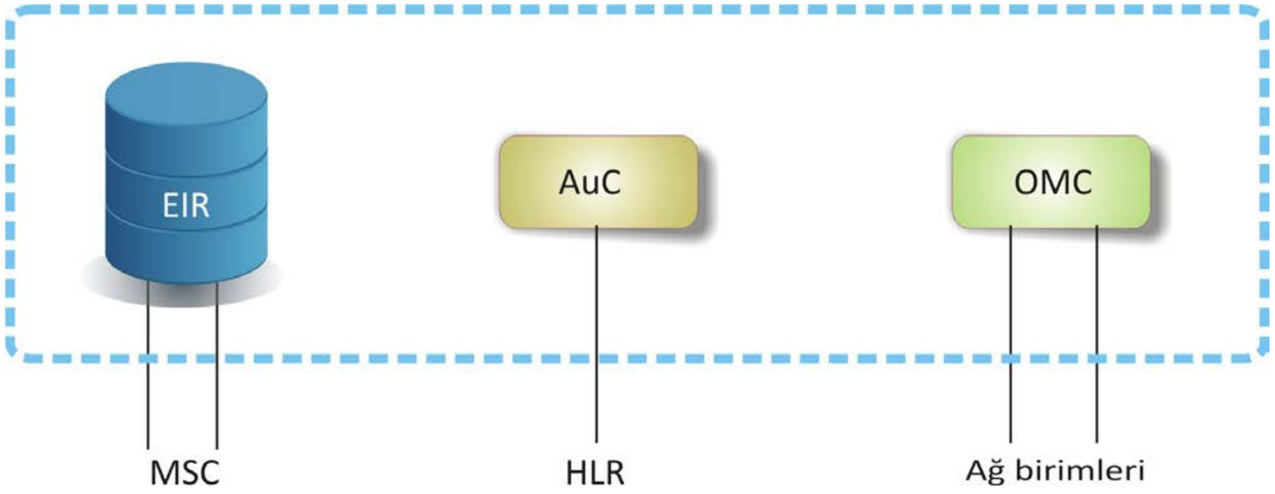
Structure of GSM Network - I

- AuC : Authentication Center : Authenticate the ID of mobile device
- Ki : Private key of subscriber
- A3 : Algorithm for authentication of subscriber
- A8 : Generate encryption key
- EIR : Equipment Identity Register : Register for subscriber:
  - White list
  - Black list
  - Gray list



Structure of GSM Network - II

- IMSI : International Mobile Subscriber Identity : IMSI consists of;
  - Mobile country code (MCC)
  - Mobile network code (MNC)
  - Telephone number of Subscriber (MSIN)
- TMSI : Temporary Mobile Subscriber Identity : Contains information in local database. Keeps IMSI and send TMSI
- MSRM : Mobile Station Roaming Number : Have the following information:
  - Visiting country code (VCC)
  - Visiting access code (VNDC)
  - Current location telephone exchange code
  - Temporary number of subscriber

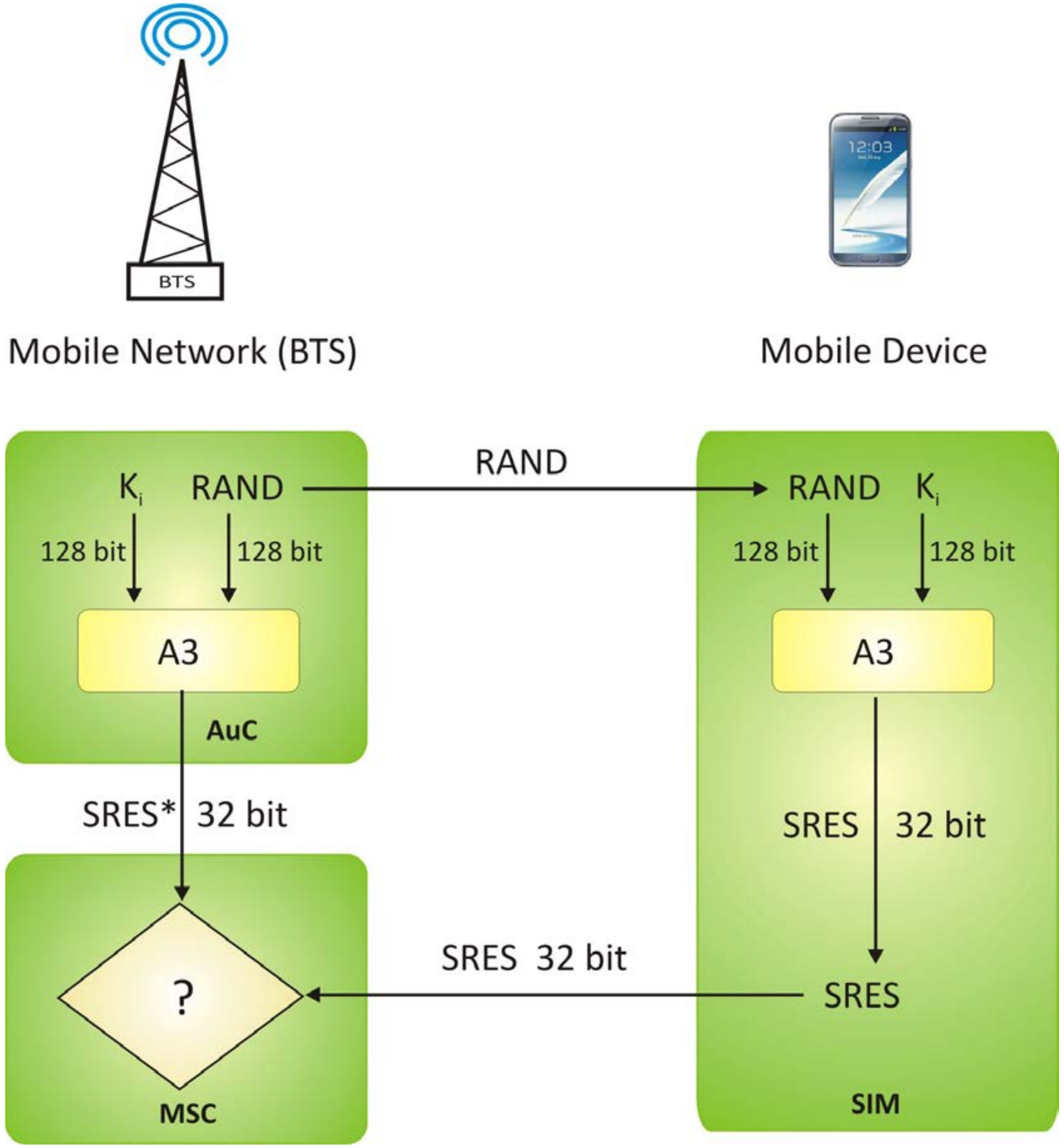


Security of GSM

Access security and Authentication

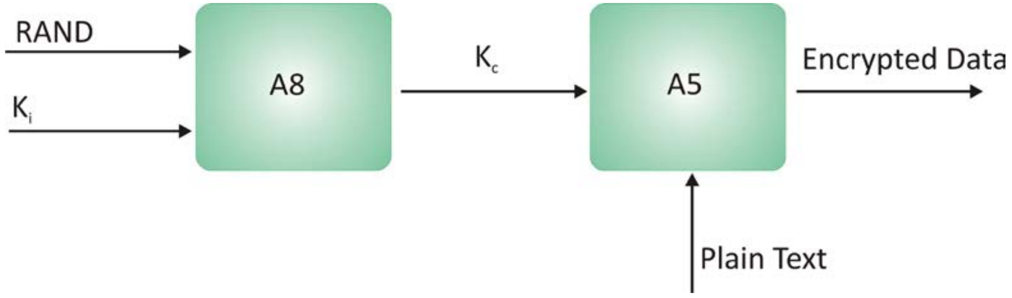
Confidentiality

Anonymity

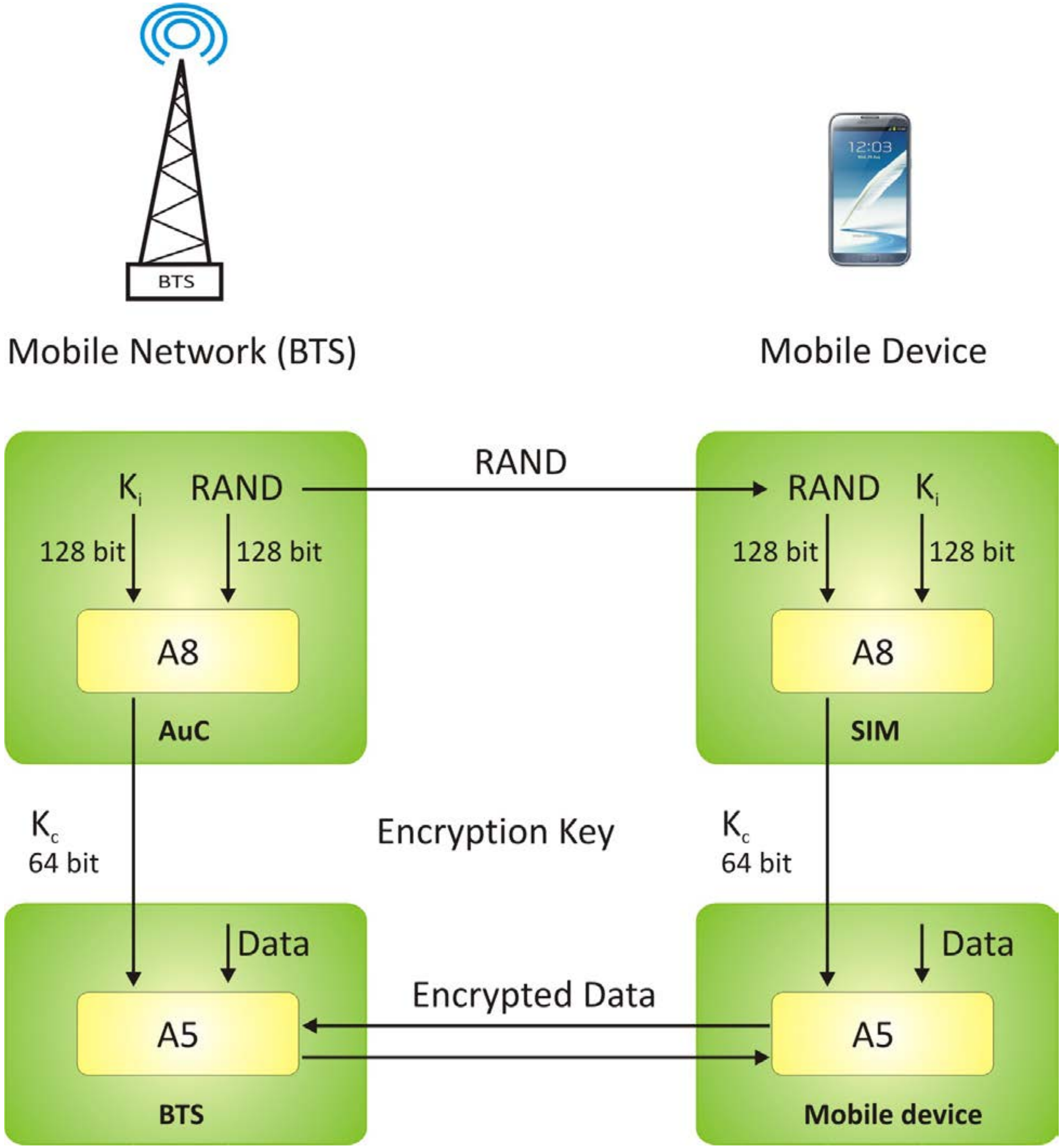


Authentication processes

Data Encryption Method



Encryption of data



BTS
Mobile Network (BTS)
Mobile Device
12:03
K_i
RAND
128 bit
128 bit
A8
AuC
RAND
RAND
K_i
128 bit
128 bit
A8
SIM
K_c
64 bit
Encryption Key
K_c
64 bit
Data
A5
BTS
Encrypted Data
Data
A5
Mobile device