GSM Authentication

In terms of security, the main stuff that was introduced in GSM system was the
SIM - Subscriber Identity Module

SIM

- ✔ Subscriber information
- ✔ Information about user identification, cryptography, authentication and information to be used in roaming.
- ✔ Database to save identification code about the Mobile Station (MS)
- ✔ Key of Authentication (Ki = 128 bits)

HLR - Home Location Register

- ✔ Subscriber Identity
- ✔ Subscriber services
- ✔ Information about subscriber mobility
- ✔ Subscriber Authentication and Security information

VLR - Visitor Location Register

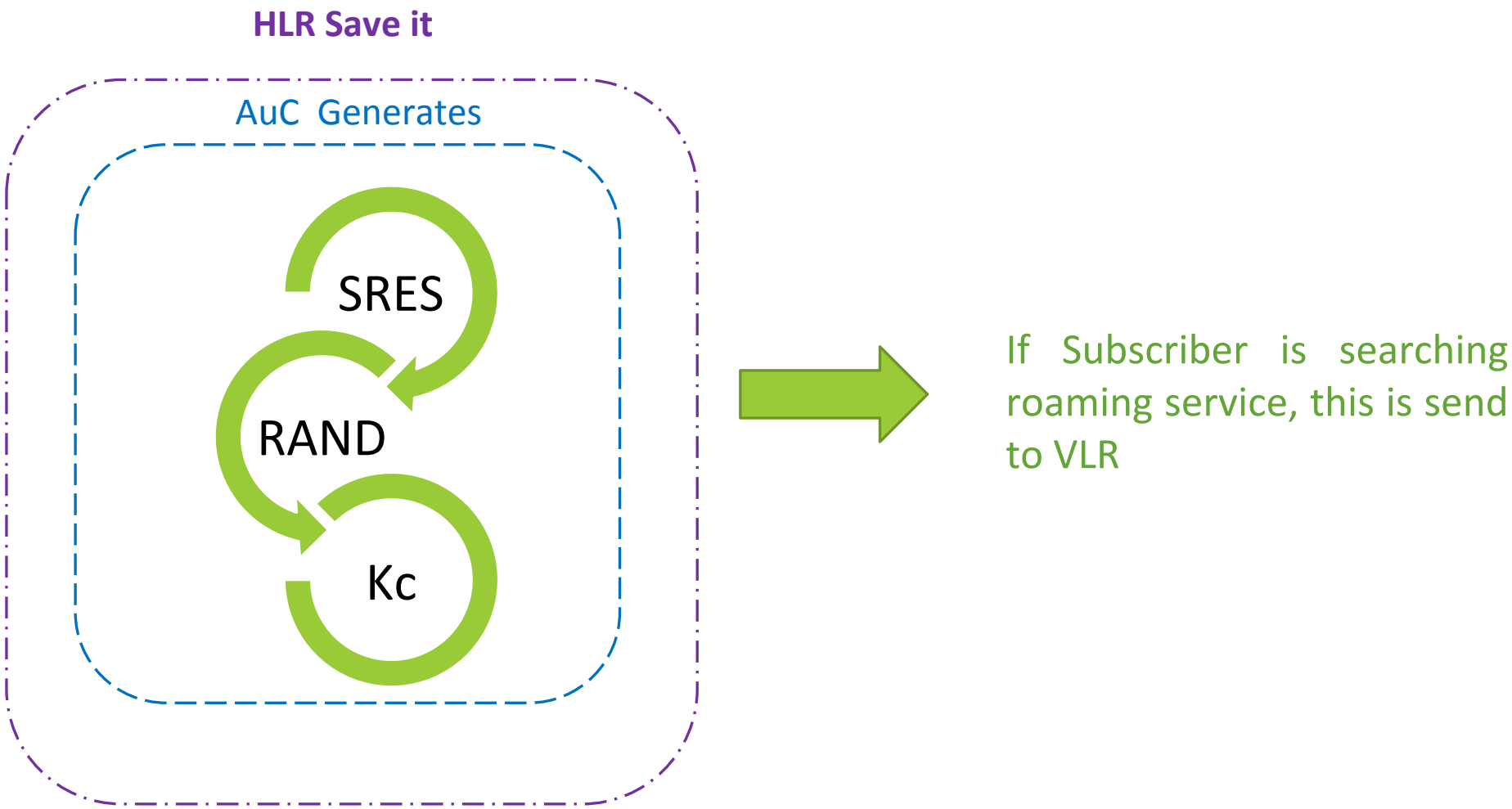
- ✔ Identity about Subscribers visitors
- ✔ As HLR, the VLR is kept in the system of service provider

AuC - Authentication Center

- ✔ Takes care of security for subscribers
- ✔ Is responsible for authenticating network users to prevent frauds such as Cloning
- ✔ Its authentication system is simple and effective, using keys and authentication algorithms

- ✔ Has a database with information about authentication and identity of each subscriber
  - **IMSI** (International Mobile Subscriber Identity) of subscribers
  - **Ki** (Keys of authentication)
  - **LAI** (Location Area Identifier)
  - **TMSI** (Temporary Mobile Subscriber Identity)

✔ The main point in this item is the **Ki**, to be stored into SIM and AuC, never is transmitted by network

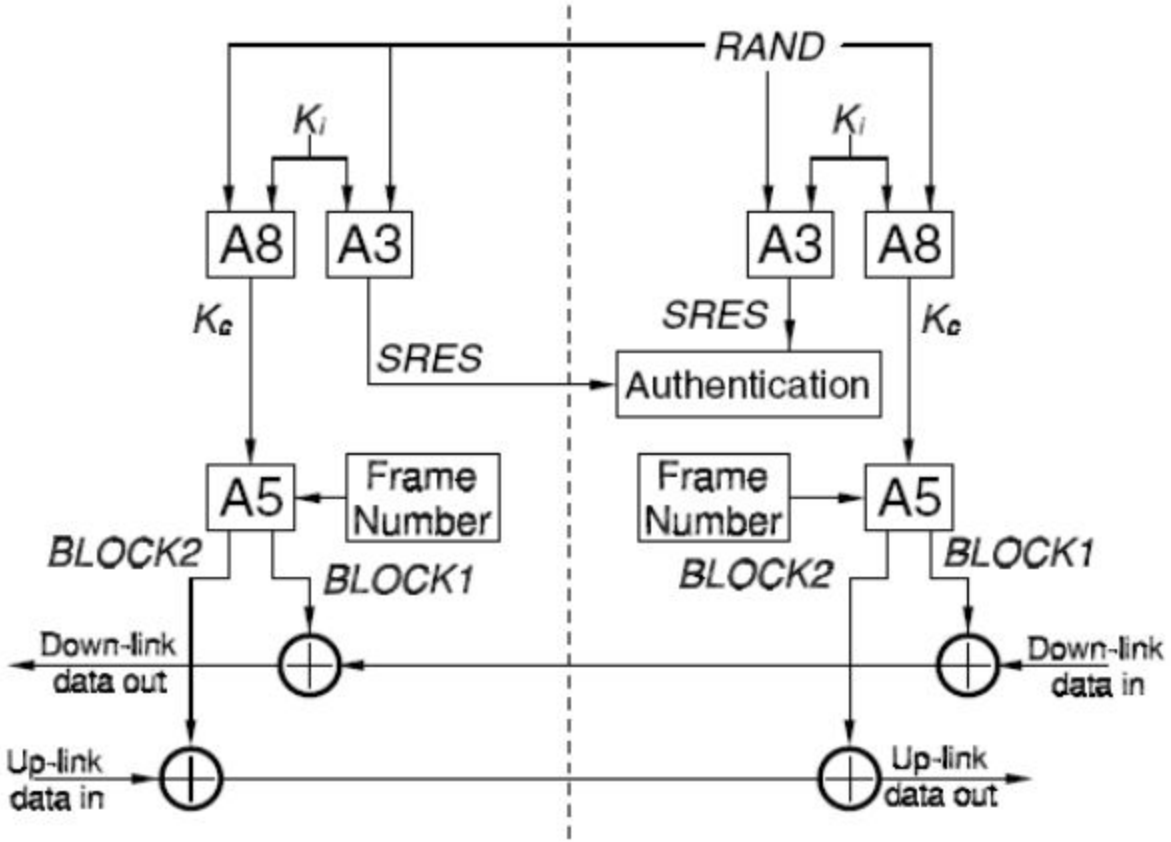


2G: Elements of Authentication Protocol

- RAND - Is a number with 128 bits
- SRES (Signed Response) - Is a number with 32 bits from A3 algorithm having RAND as input
- Kc - Is a key with 64 bits, used to encrypt and decrypt the data

  A8 algorithm generates it in AuC and in SIM, having RAND and Ki as input
- A5 algorithm – Is used to ensure encrypt and decrypt of information sent during a communication between MS and Base System Station

2G: Diagram of Authentication and Cryptography



GSM Network contains three main components

Mobile Station

- SIM

Base station subsystem (BSS)

- Connects the user on a mobile station to other mobile/landline users.

Network subsystem (NSS)

- Routing calls via the Base Station Controllers (BSCs) and Base Transceiver Stations (BTSs) to different mobile stations
- * AuC

The Main objective of GSM mobile communication is to make mobile phone system secure

✔ **SIM** – Subscriber Identity Module

- Secure that only licensed users can approach the network.
- The data transferred between the base station and mobile station across the air is **encrypted**.
- Key of Authentication (Ki = 128 bits)

- Mobile phones are inoperable without a SIM
- Duplicate SIMs are not allowed on the network
- Authentication of the registered subscribers only
- Subscriber identity protection