Cellular Mobile Networks - GSM
GSM Security Concept

Contents - GSM - GSM Security Concept

GSM Security Features Overview

- Access Control / Authentication
  - subscriber ⇔ SIM: Personal Identification Number (PIN)
    activation of the ME and getting access to personal data
  - SIM ⇔ network: via challenge-response method
    getting access to the network and network services
- Privacy (Encryption)
  - encryption at the air interface between MS and BTS
    encrypted transmission of voice and signaling data after successful authentication
- Anonymity (subscriber identity protection)
  - use of a temporary subscriber identity (TMSI)
    a new TMSI is assigned at every connection setup, location update or VLR change; usually the TMSI is encrypted before transmission
- ME Identity Check (optional)
  - IMEI verification through EIR query:
    identification of stolen, outdated and faulty MEs

Authentication & Encryption - Basic Concept

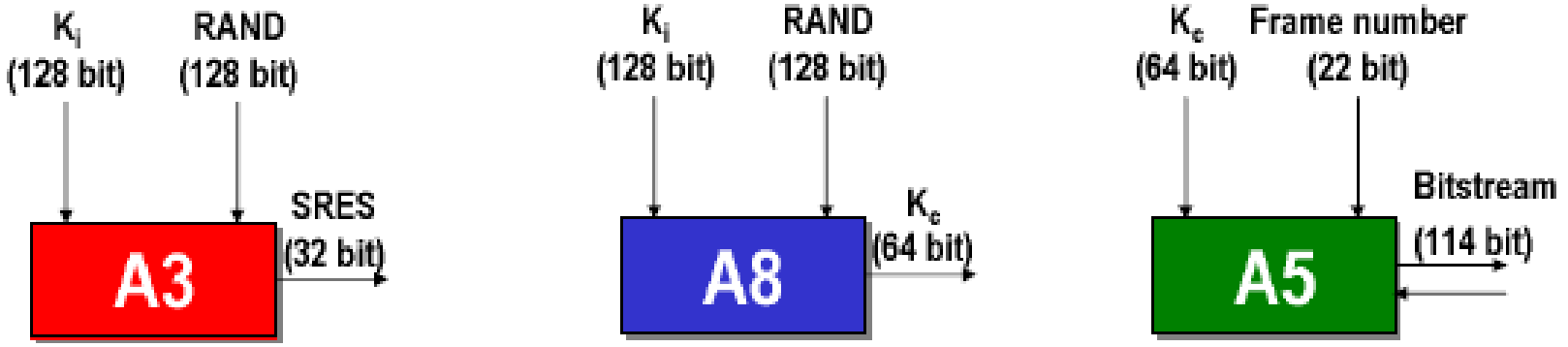
The GSM security concept for authentication and encryption comprises:

- the **IMSI**: stored in the SIM and in the AuC
- a set of crypto algorithms:
  - **A3, A8**: stored in the SIM and in the AuC
  - **A5**: stored in the ME and if necessary in the BTS
- two keys:
  - $\mathbf{K_i}$: (secret) subscriber specific key for authentication
    stored in the SIM (not readable) and in the AuC
  - $\mathbf{K_c}$: key for user data encryption on the air interface
    K_c is generated in the AuC and in the SIM with the algorithm A8
- random numbers **RAND**: generated in the AuC
- Signed Responses (**SRES**): generated in the AuC and in the SIM with the algorithm A3

Authentication & Encryption - Crypto Algorithms

In GSM 3 crypto algorithms are specified:

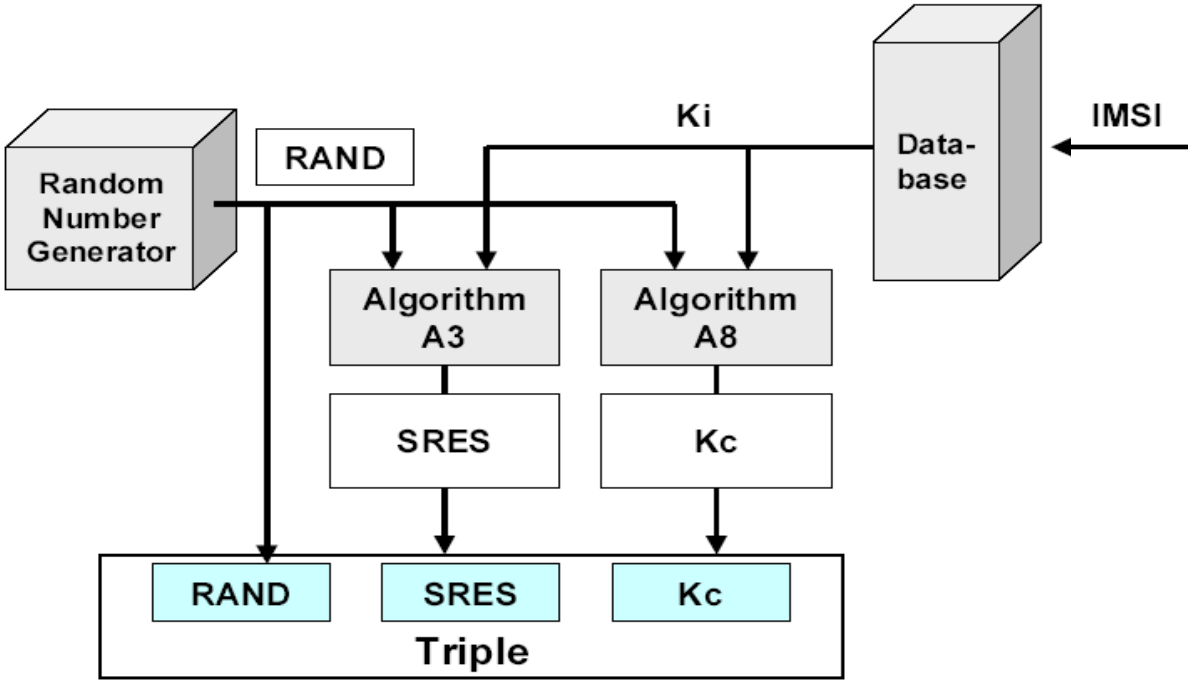
- **Algorithm A3** for authentication (confidential but open interface): generation of the response value SRES out of a random number (RAND) and the subscriber specific key K_i
- **Algorithm A5** for user data encryption (standardized): uses the key K_c (session key)
- **Algorithm A8** for key generation (confidential but open interface): generation of the key K_c (session key) which is used for symmetric encryption of user data; K_c is generated out of a random number (RAND) and the subscriber specific key K_i



Authentication & Encryption - Security Data

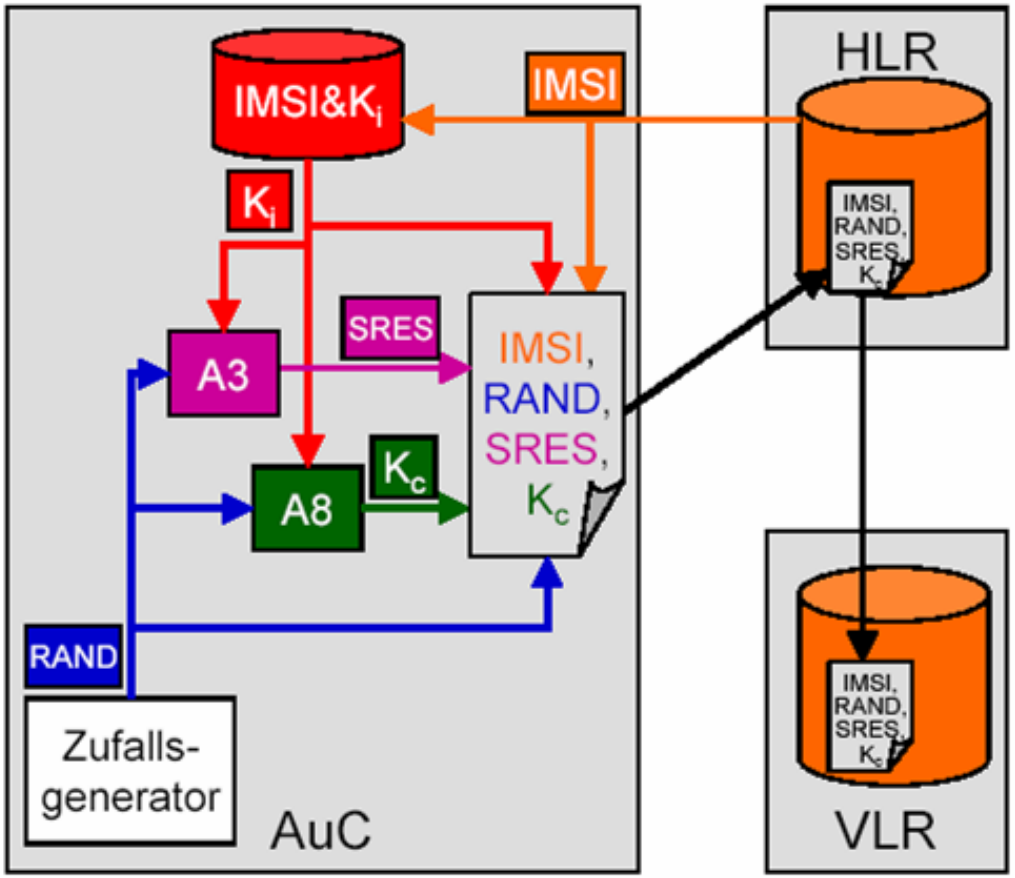
The subscriber specific security data ("Triples") RAND, SRES, K_c are required for authentication and encryption

- they are usually generated in the AuC and forwarded to the HLR or VLR
- it is also possible to generate the security data in the VLR, but this is less secure as for that the key K_i has to be transmitted from the AuC to the VLR - therefore this method is only used in the home network



Authentication & Encryption - Security Data Distribution

Generation and distribution of security data:

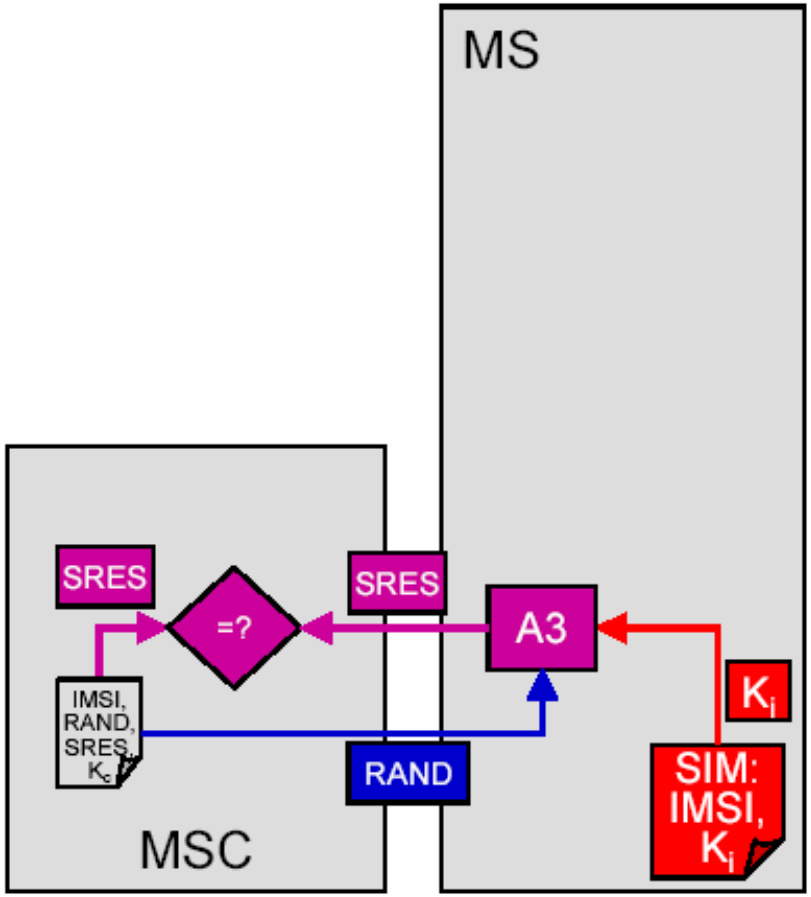


- on request of the HLR the AuC generates (several) security data triples
  - each triple is used only once
  - the triples can be generated in advance
  - K_i resides in the AuC only!
- the VLR requests a triple from the HLR, when the subscriber wants to establish a radio connection
- during a location area change the triples are transferred from the old to the new VLR
- alternatively K_i is transferred to the VLR and the triples are generated locally in the VLR (however this procedure is less secure)

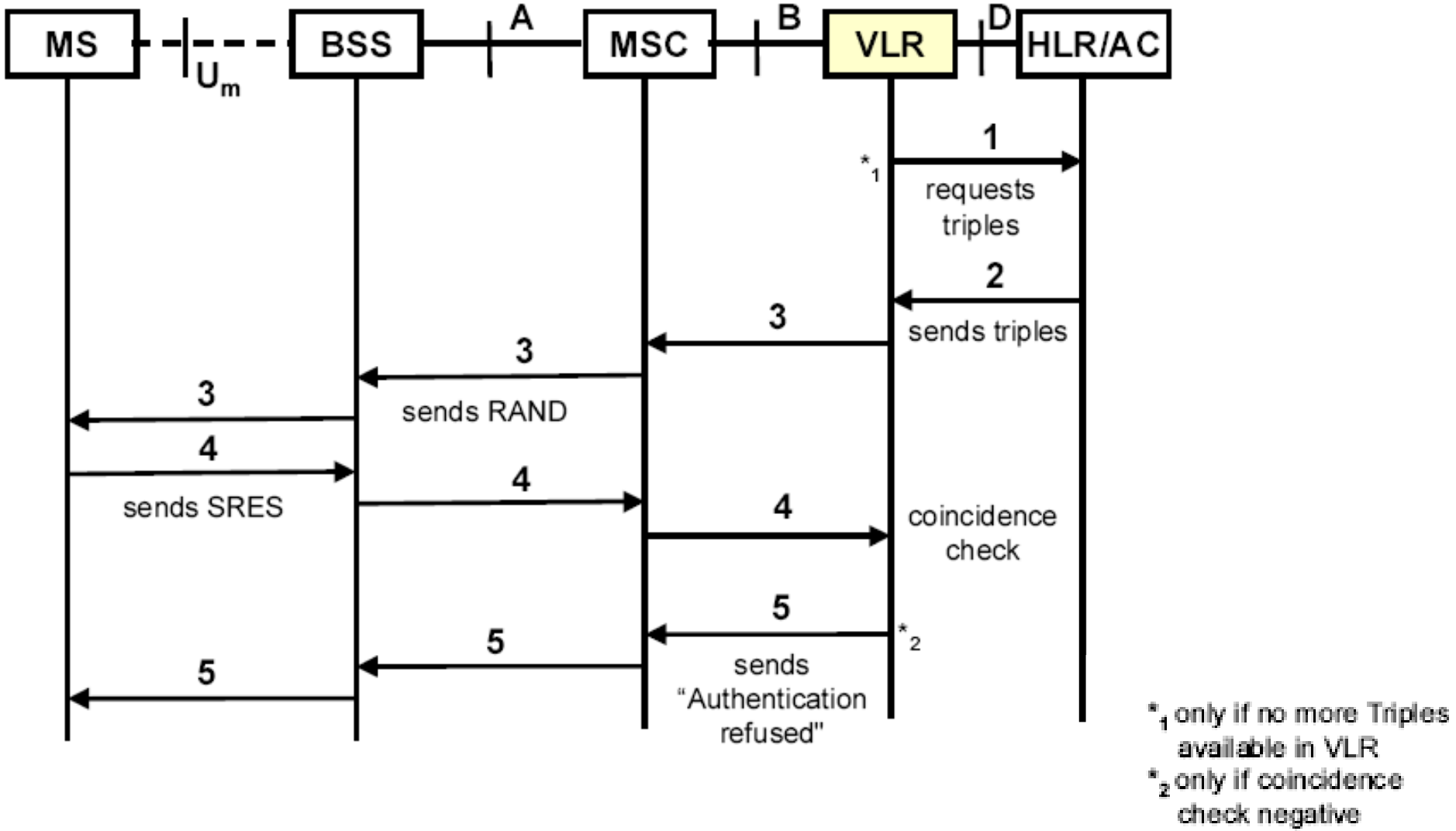
Authentication & Encryption - Subscriber Authentication

Subscriber authentication:

- the authentication takes place e.g.:
  - during an location update
  - during the connection setup
- authentication is performed via SRES which is calculated via A3 by using the security data (only once in time) and a random number (RAND) (challenge-response method)
  - thereby attacks through interception and repetition of data are avoided
- if the authentication fails the MS can only make emergency calls - all other functions are blocked



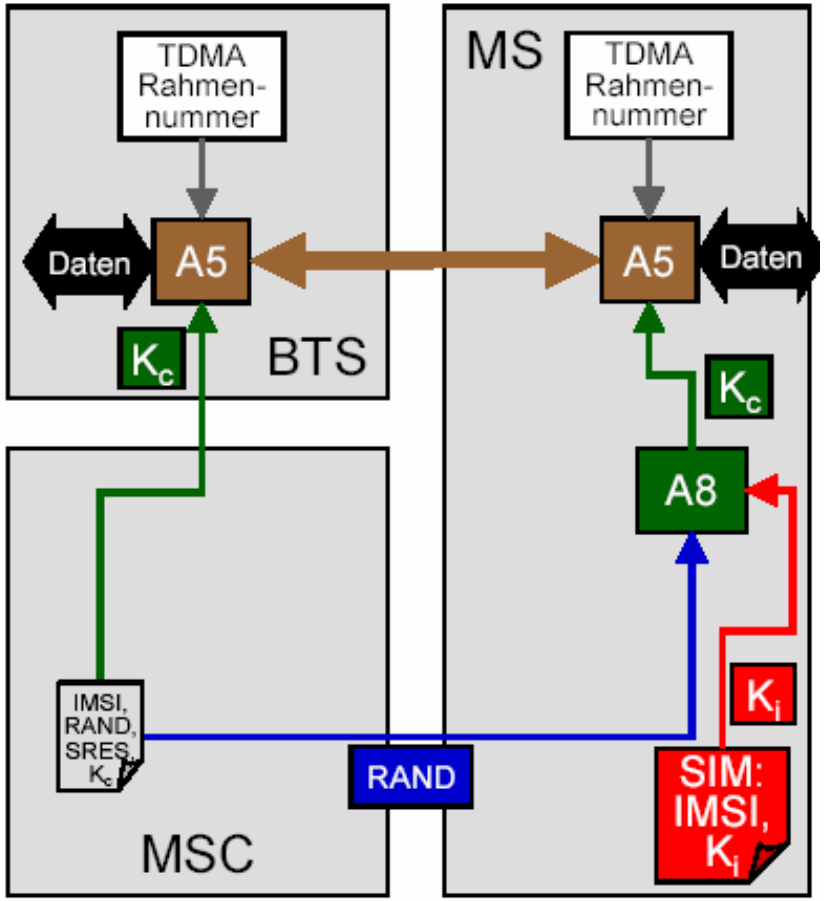
Authentication & Encryption - Subscriber Authentication



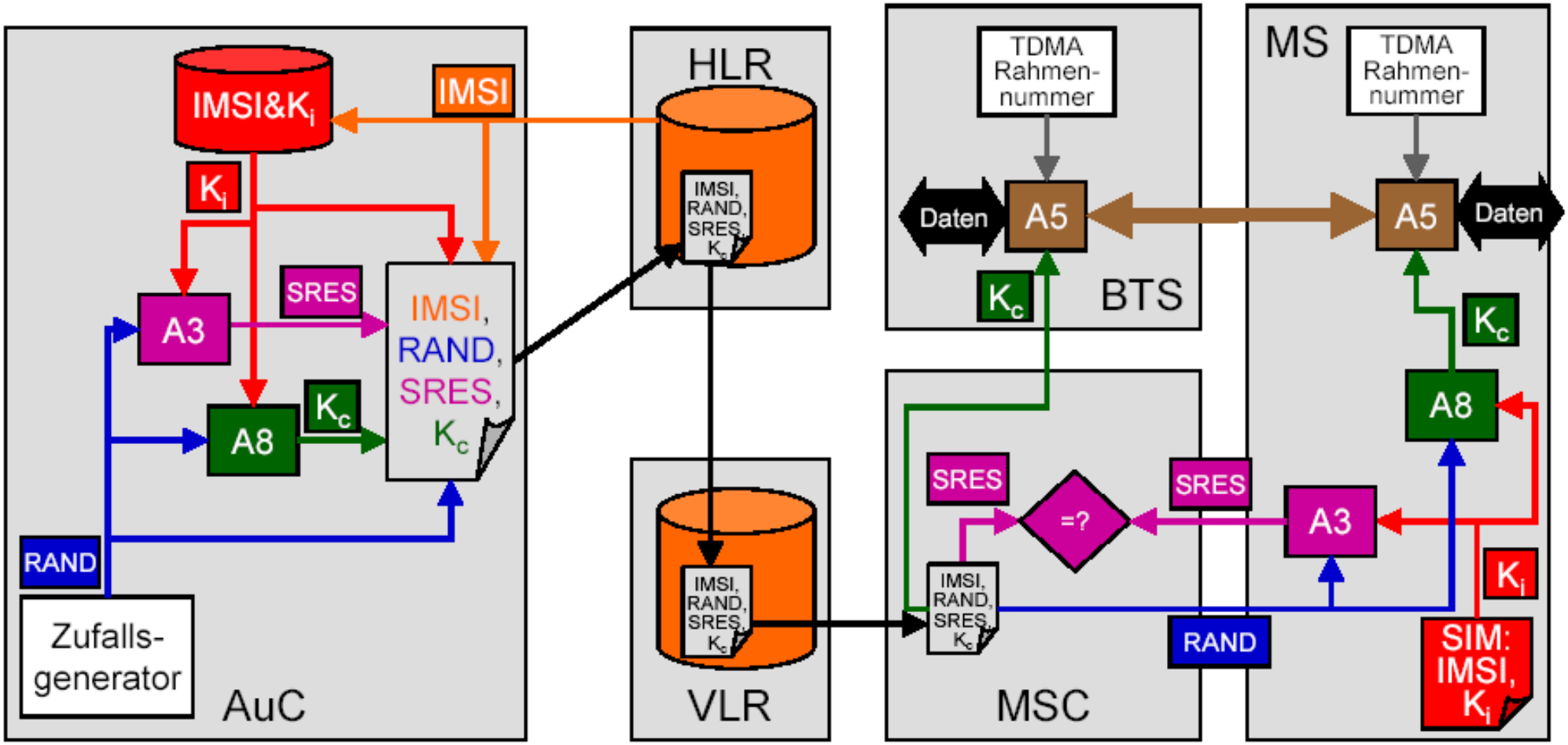
Authentication & Encryption - Encryption at the Air Interface

Encryption of user data:

- symmetric encryption
  - stream cipher with key K_c
  - only used for one “session”
- K_c is transferred from the MSC to the BTS
- the MS generates K_c out of RAND and K_i
- K_c is used for encrypting user and signaling data on the air interface between BTS and MS
- the encryption process is synchronized by using the frame number of the TDMA hyperframe



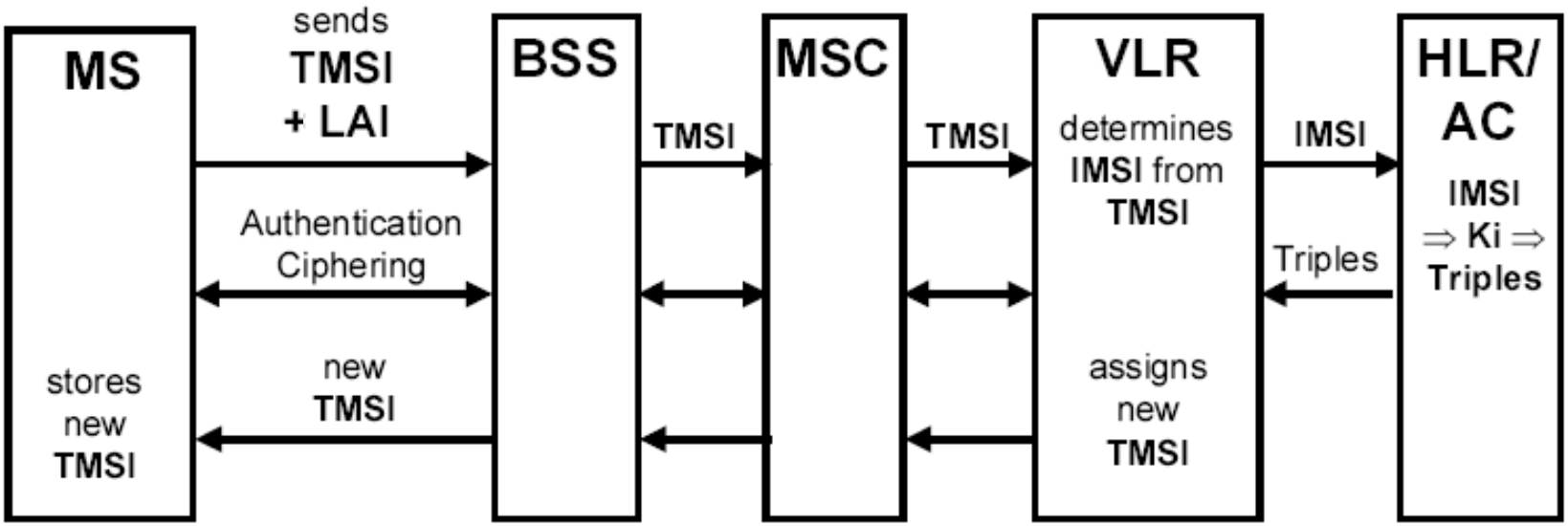
Authentication & Encryption - Summary



Subscriber Identity Protection via TMSI

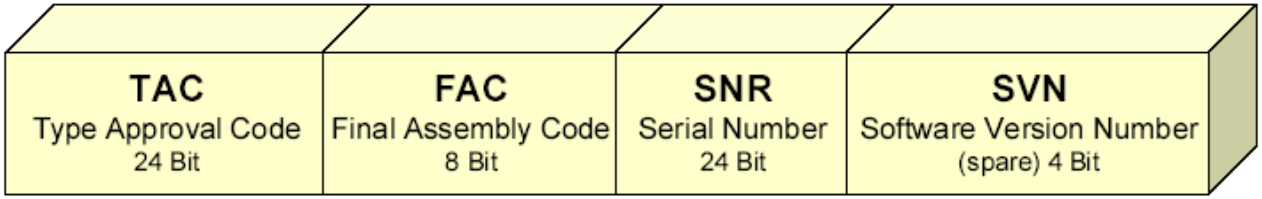
- To activate the encryption during connection setup the subscriber identity (IMSI) needs to be known by the network (required for the mapping subscriber ↔ security data (triples)); an unencrypted transmission of the IMSI over the air interface should be avoided - therefore the TMSI is transmitted instead of the IMSI
- The TMSI is assigned by the VLR that serves the location area in which the MS currently stays - only this VLR knows the mapping TMSI ↔ IMSI
- At a VLR change, the old VLR has to be queried to obtain the IMSI belonging to the TMSI (therefore the MS sends the TMSI and the LAI to the network)
- If the VLR doesn't know the TMSI (possible reasons: data base error, first registration at the PLMN, first use of a SIM) the IMSI has to be send by the MS
- The algorithm for TMSI generation is not standardized
- After activation of the user data encryption, also new TMSIs are encrypted

Subscriber Identity Protection via TMSI



ME Identity Check via IMEI

- The Equipment Identity Register (EIR) contains informations about MEs; MEs are uniquely identified by the so called "International Mobile Equipment Identity" (IMEI)
- IMEI structure:



  - SVN: Software Version Number
  - SNR: Serial Number
  - FAC: Final Assembly Code
  - TAC: Type Approval Code

ME Identity Check via IMEI

- The network (MSC/VLR) initiates the authentication of the ME (during the registration of the MS):
  - the IMEI is requested from the MS (IDENT_REQ)
  - the IMEI is checked by querying the EIR
  - the EIR stores the status of the ME: ME that are faulty, unapproved or registered as stolen can be blocked