NOS8/ NOS-14: SIM encryption

Link: https://lcsnosim.atlassian.net/browse/NOS-14

Haddad Rafik: LCS-HR

GSM Authentication Algorithm **'COMP128'.**

- A3, The MS Authentication Algorithm
- A8, the Voice-Privacy Key Generation Algorithm
- A5/1, The Strong Over-the-Air Voice-Privacy Algorithm.

For the auth, SIM and GSM/UMTS:

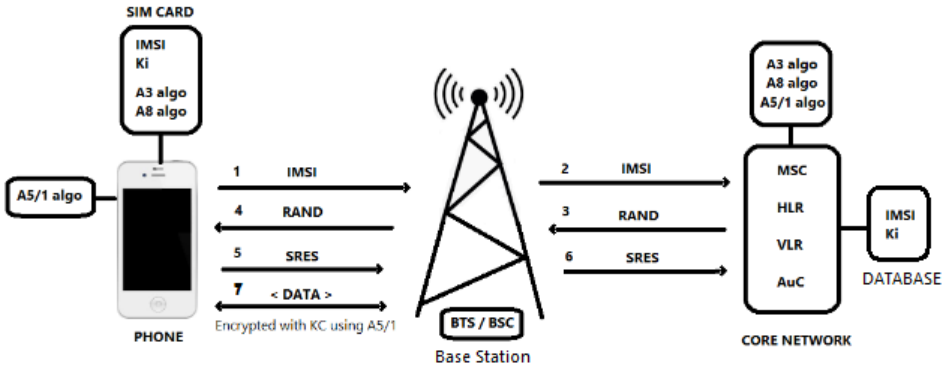
1. SIM Card Identification.
2. Registration Request.
3. BTS Identification.
4. Authentication.
5. Assigning Temporary Mobile Subscriber Identity (TMSI).
6. Connection Establishment.
7. Network Access.
8. Handover .
9. Control Channels

Data shared WITH SIM:

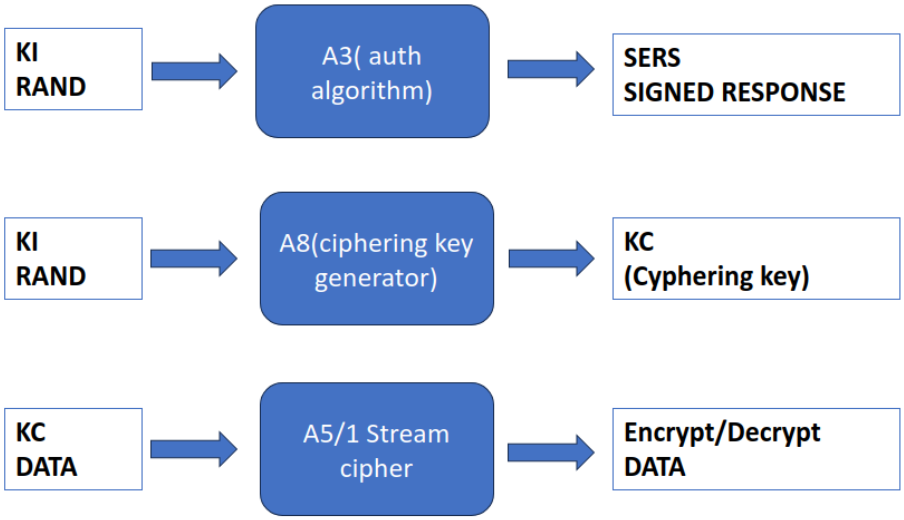
- **IMSI**: The international mobile subscriber identity (IMSI)
- **Kc**: A 64-bit ciphering key used to encrypt voice and data communication between the MS and BTS of GSM networks
- **K cGPRS:** A 64-bit ciphering key used to encrypt communication data between the MS and the SGSN of GPRS networks
- **CK**: A 128-bit ciphering key used to encrypt the communication between the MS and the RNC of UMTS
- **IK**: A 128-bit key to protect the integrity of the signaling data between the MS and the RNC of UMTS network.
- **TMSI** Time: This is a 1 byte value and represents the maximum time interval which the assigned TMSI can be used.
- **P-TMSI**: The packet TMSI (P-TMSI) is the complement of TMSI in the UTRAN/GERAN packet switching (PS) domain.
- **P-TMSI Signature value**: This is a signature used by the 3G network for verifying the validity of P-TMSI of MS. Its size is 3 bytes.
- **LAI**: The location area identity (LAI) is a 5 bytes unique identifier for each location area in the CS domain. It consists of MCC, MNC and the location area code (LAC). **RAI**: The Routing Area Identity for PS domains is analogous to the LAI for CS domains. RAI consists of LAI (which is 5 bytes) and a 1 byte Routing Area Code.
- **Cell Id**: This is the unique identity of the cell tower, where the MS is connected at the moment of data collection. Network type: This parameter indicates the mobile network technology, where the MS is connected, at the moment of data collection. It may have several values including GPRS, EDGE, UMTS, HSDPA, LTE, UNKNOWN, etc. Roaming: A 1-bit value that indicates whether MS is outside the coverage area of its home network.

The important and **useful terminology:**

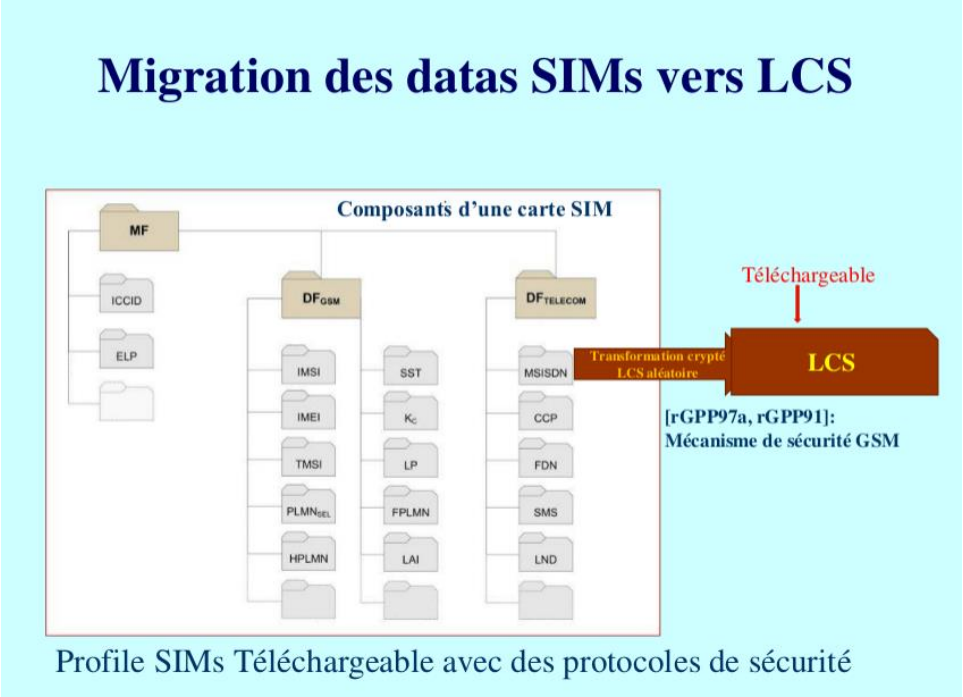
- **IMSI** international mobile subscriber identity (subscriber ID).
- **TMSI temporary IMSI (helps with privacy by obfuscating ISMI).**
- **Ki** 128-bit unique subscriber key (paired with IMSI).
- **RAND 128-bit random number (sent to MS by AuC to facilitate MS authentication challenge)**
- **SRES** challenge sent to MS (generated using RAND + Ki + A3 algorithm).
- **KC uniquely generated key (generated using RAND + Ki + A8 algorithm).**



1. Mobile station (MS) requests access to the network, MS sends its IMSI to the Network Subsystem (NSS) via the BSC / BTS.
2. The IMSI sent by the MS is forwarded to the MSC on the network, and the MSC passes that IMSI on to the HLR and requests authentication.
3. The HLR checks its database to make sure the IMSI belongs to the network.
   If valid, The HLR forwards the authentication request and IMSI to the Authentication Center (AuC).
   The AuC will access its database to search for the Ki that is paired with the given IMSI.
   The Auc will generate a 128-bit random number (RAND).
   The RAND and Ki will be passed into the A3 (authentication) algorithm, creating a 32-bit SRES (signed response) for the challenge-response method.
   The RAND is transmitted (via the BSC / BTS) to the mobile station (MS).
4. The RAND received by the MS, together with the SIM card-Ki are passed into the SIM card-A3 (authentication) algorithm, generating the phones SRES response.
5. The phones SRES response is transmitted (via the BSC / BTS) back to the AuC on the network.
6. The AuC compares the sent SRES with the received SRES for a match. If they match, then the authentication is successful. The subscriber (MS) joins the network.
7. The RAND, together with the SIM card-Ki are passed into the SIM card-A8 (ciphering key) algorithm, to produce a ciphering key (KC).
   The KC generated is used with the A5 (stream ciphering) algorithm to encipher or decipher the data.The A5 algorithm is stored in the phone's hardware and is responsible for encrypting and decrypting data on the fly.



Réf: https://www.blackhillsinfosec.com/gsm-traffic-and-encryption-a5-1-stream-cipher/
Test OSMO-SIM-AUTH: https://gitea.osmocom.org/sim-card/osmo-sim-auth



Interesting next step: **find the actual location of the SIM information in the mobile software section, GSM modem, antenna interface or other.**