# 2G & 3G Subscriber Security

## C1601

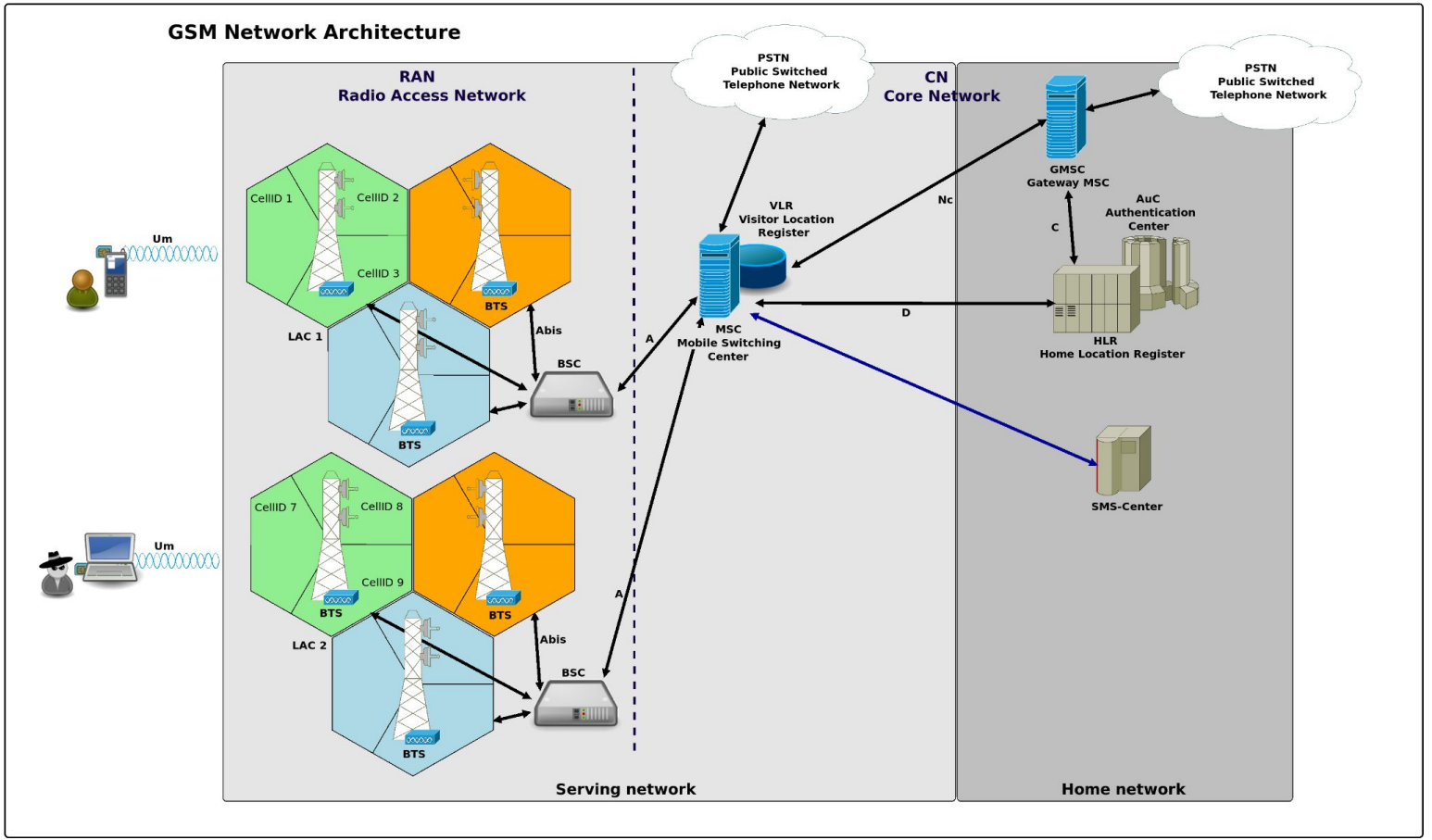
P1 Security Training

# Agenda

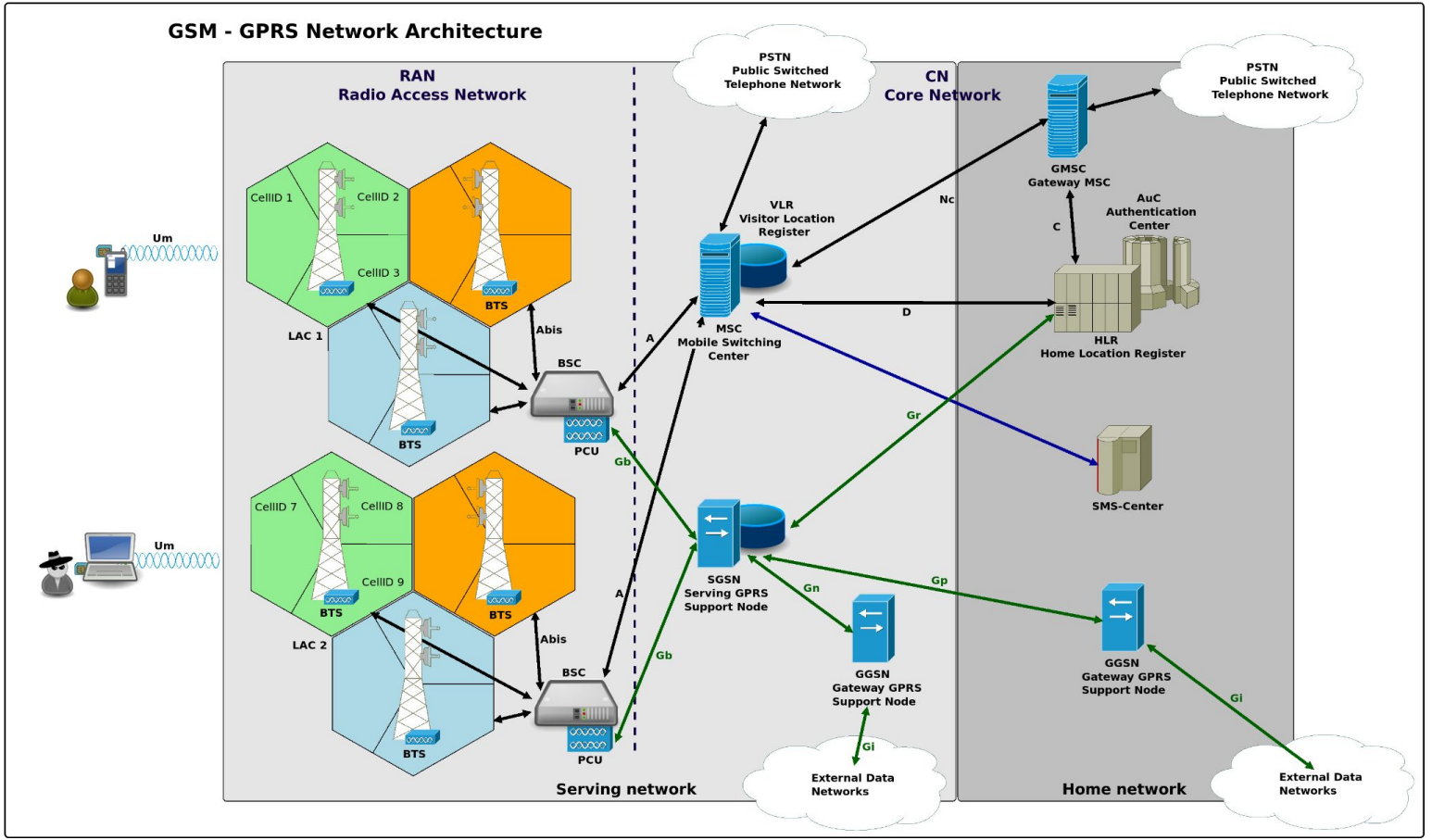
- 2G network architecture
- GSM and the CS domain
- GPRS, EDGE and the PS domain
- 2G network security
  - 2G subscriber authentication
  - GSM security activation
  - GPRS authentication and security activation
  - Temporary identifiers
- Attacks against 2G networks
- 3G network architecture
- 3G network security
  - 3G subscriber authentication
  - UMTS security activation
- Attacks against 3G networks
- Conclusion

# 2G network architecture

# GSM network architecture



# GSM - GPRS network architecture



# GSM and the CS domain

# Initial 2G network services

- **Initial technical specifications worked on at the end of the 80's**
  - Mostly by Germany, France and UK
- **Circuit-switched network**
  - Connect calls from / to mobile terminal
  - Interconnect with the fixed telephony infrastructure (PSTN)
- **Digital radio interface**
  - 200 kHz bandwidth per channel (or ARFCN: Absolute Radio Frequency Channel Number)
    - GMSK modulation
  - FDD: separated uplink and downlink bands
  - GSM 900 (45 MHz duplex spacing), GSM 1800 (95 MHz duplex spacing)
    - GSM 850 and 1900 in North America
  - TDMA (Time Division Multiple Access)
    - Subscribers multiplexed into different time-slots
- **SIM cards for handling subscriber's authentication**

# TDMA multiplexing (GSM and EDGE)



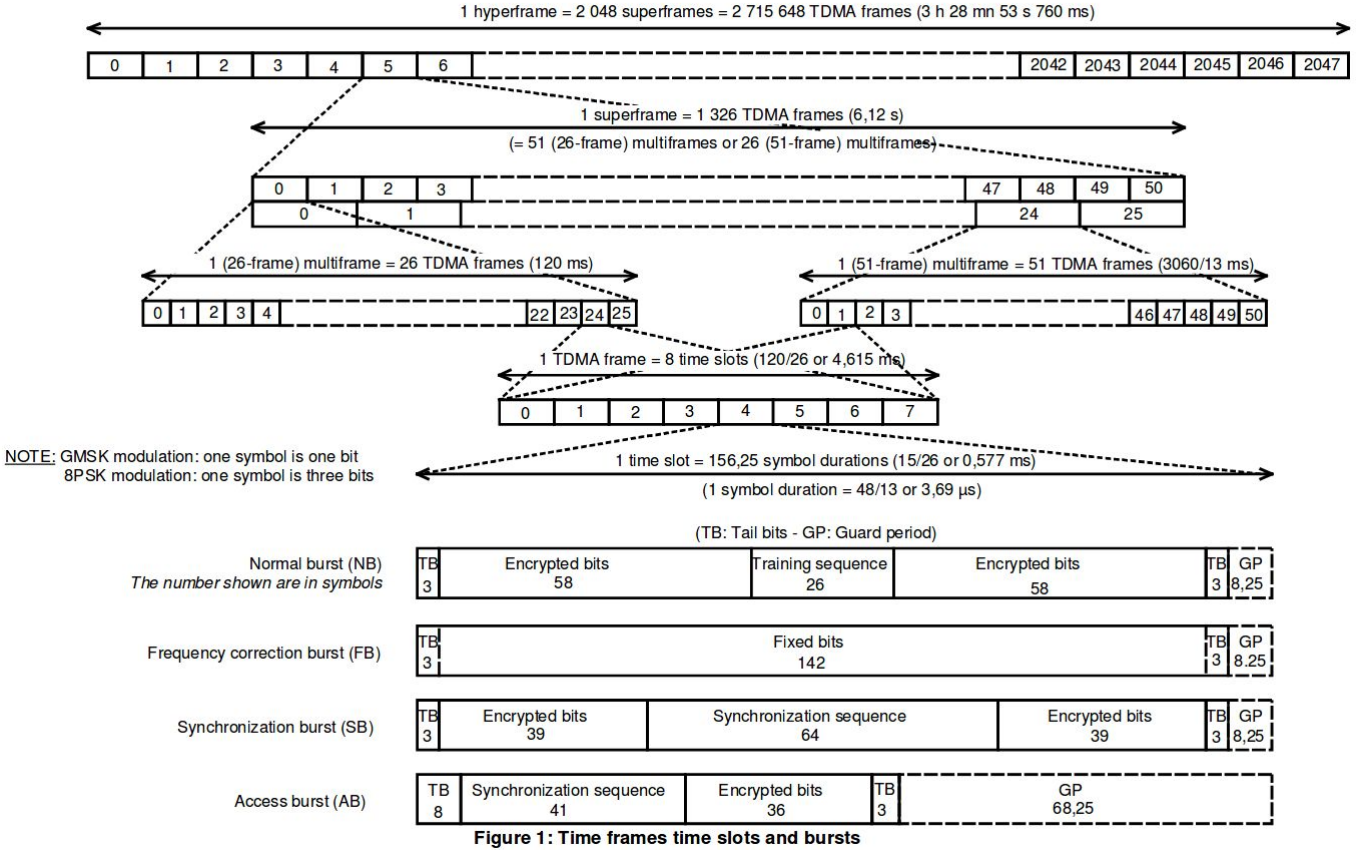



**Figure 1: Time frames time slots and bursts**

1 GSM timeslot
= 0,577 ms
= 156,25 GSM symbols
= 114 bits of information

8 time-slots per TDMA frame:
up to 8 subscribers multiplexed over a 200 kHz channel

# GSM channel types

- **Different types of GSM channels defined**
- **Downlink-only**
  - BCCH (Broadcast Control Channel), DL-only
    - broadcasts network settings and configuration (PLMN network codes, LAC, CellID, neighbouring cells...)
- **Downlink and Uplink**
  - CCCH (Common Control Channel)
    - Paging and channel assignment in the DL, RACH in the UL
  - SDCCH (Standalone Dedicated Control Channel)
    - Optionally with SACCH (Slow Associated Control Channel)
  - TCH (Traffic Channel)
    - TCH/F: Full-Rate, TCH/H: Half-Rate, supporting encoded voice
    - Optionally with FACCH (Fast Associated Control Channel) or SACCH
- **Channel hopping for frequency diversity**
- **See 3GPP TS 45.001**

# Circuit-Switched domain

- **Connect calls within / between Mobile Switching Centers**
- **Handle UE mobility**
  - Idle mobility: tracking inactive subscribers
    - At the LAC level within VLR
    - At the MSC/VLR level within HLR
  - Active mobility / handovers: support subscriber's mobility without interrupting on-going calls
    - change of BTS/BSC (handled within the MSC/VLR)
    - change of MSC/VLR (handled between MSCs/VLRs)
- **Authenticate subscribers, because MNOs**
  - want accurate billing
  - do not want to be frauded
- **Short Message Service**
  - enable exchange of short messages between subscribers, carried over the signaling

# GPRS, EDGE and the PS domain

# Introduction of GPRS

- **“General Packet Radio Service”**
- **Reuse the GSM air interface (Um) to enable connectivity to packet-based applications (e.g. the Internet)**
  - Define new TDMA channel types for packet service
    - 8 to 20 kbit/s per time-slot
    - Aggregate multiple slots to provide more bandwidth
  - Then enhance it with EDGE
    - 8-PSK modulation and more multiplexing: 8 to 60 kbit/s per time-slot, up-to 4 time-slots aggregated
- **New mobile core network equipments PS domain**
  - SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node)
  - UE connects to the PS domain in parallel to the CS domain
    - 2 distincts mobility and security contexts
    - GPRS adds RAC (Routing Area Code) in addition to GSM LAC

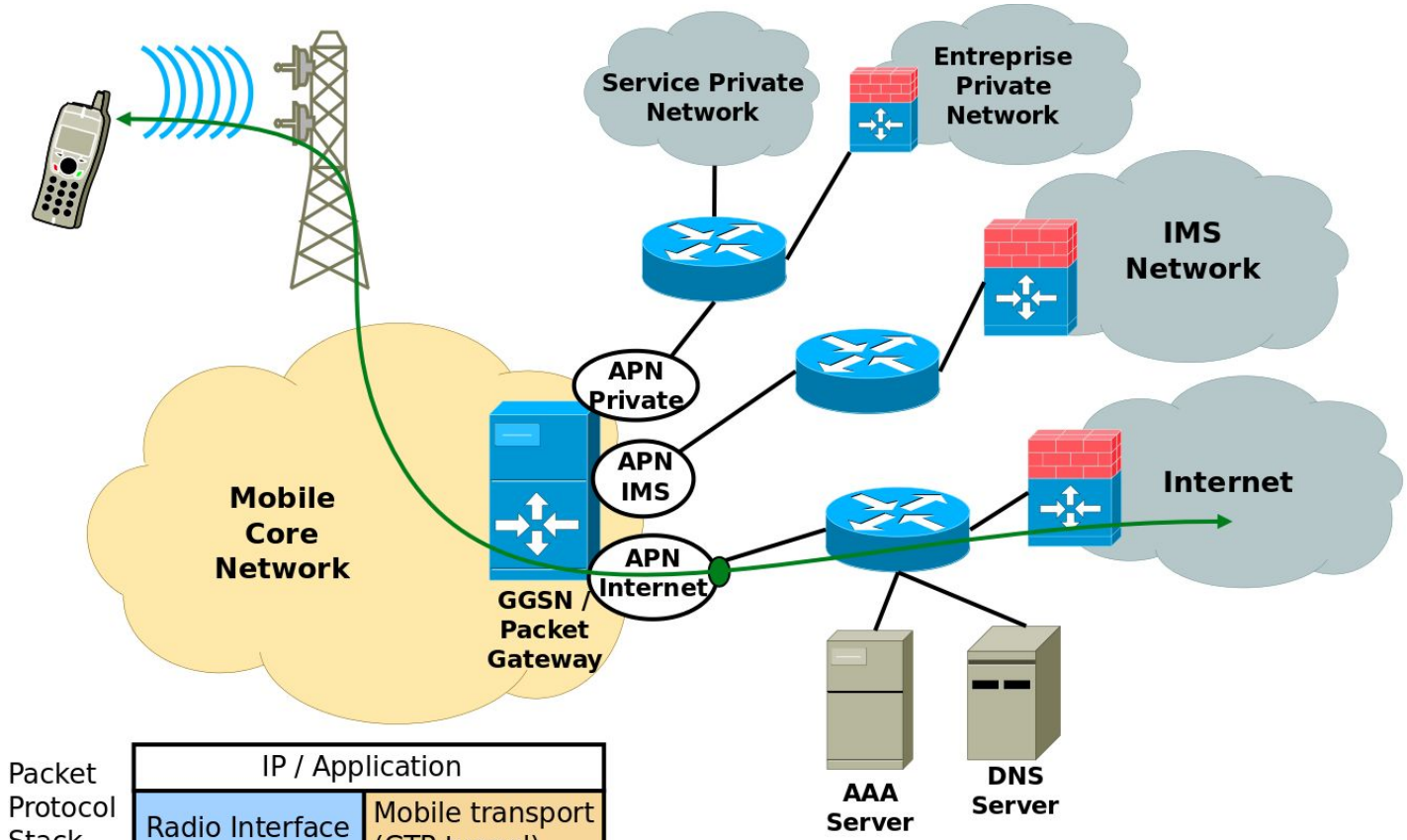
# GPRS services

- **Subscribers connect to APNs (Access Point Name)**
  - Corresponds to a *route* from a GGSN to a data network
  - Access to a given APN depends on the subscription (stored within the HLR)
    - And eventually a PAP or CHAP login / password

- **Network encapsulates subscribers' data (e.g. IP packets) within the GTP protocol to the Gi interface**
  - GTP: GPRS Tunneling protocol (IP infrastructure / UDP / IP subscriber)

- **Subscriber connection can be routed locally (directly within the visited network), or home-routed (through the home network)**
  - Home-routing is often required by regulators due to law intercept requirements

# GPRS connectivity to APN

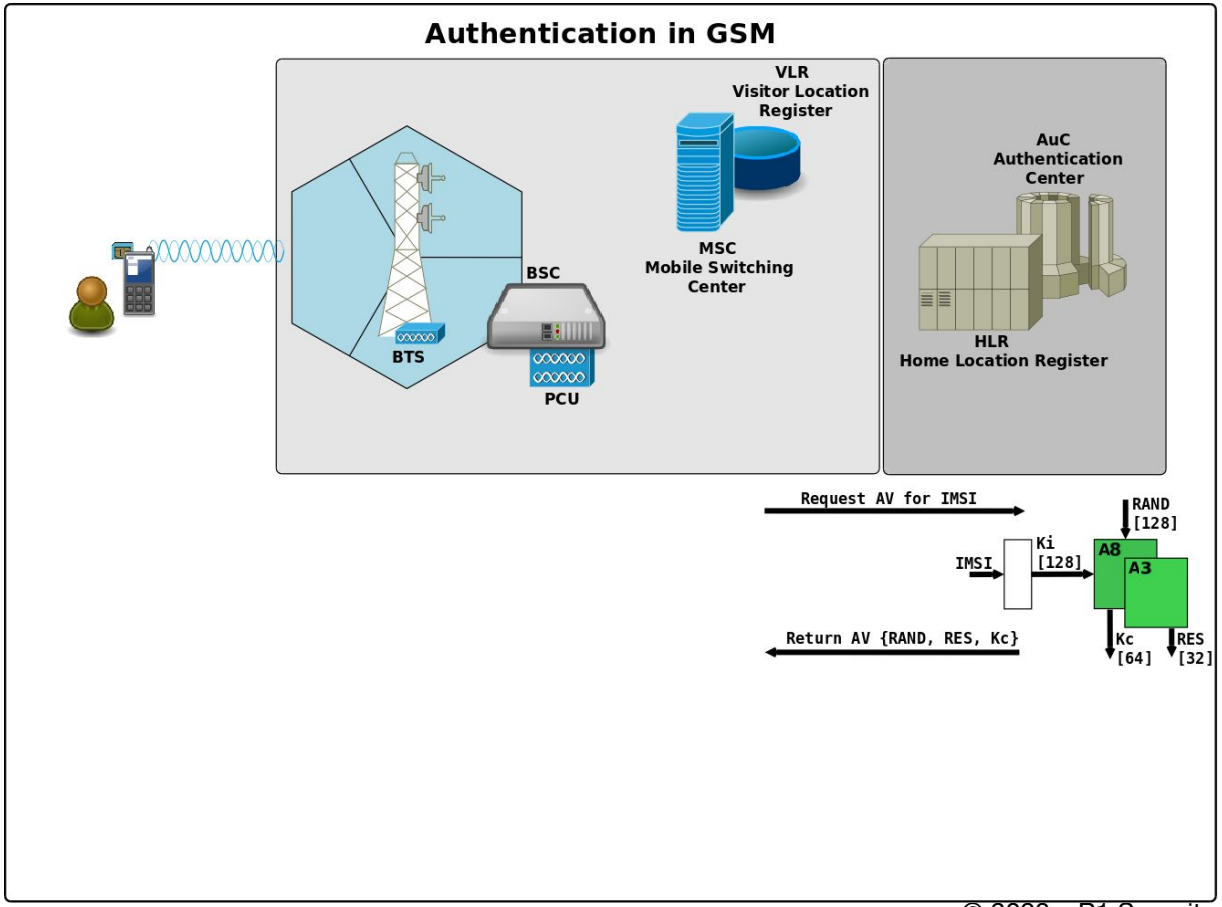


# 2G Network Security

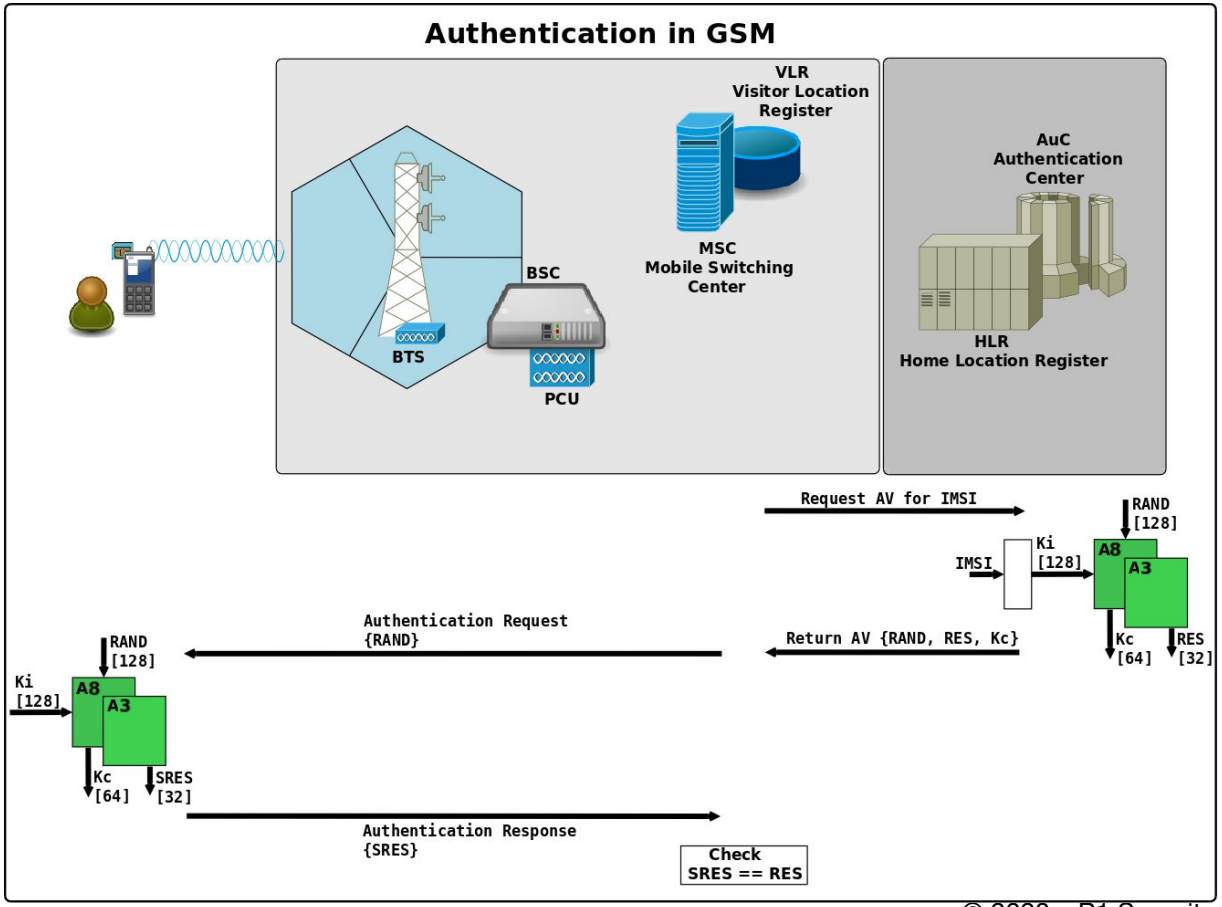
# 2G subscriber authentication

- **Based on a symmetric key Ki**
  - Shared between the AuC and the SIM card
  - 128 bit
- **Simple challenge (RAND) - response (RES) protocol**
  - Generate a shared session key Kc as side effect
- **Few variants of the cryptographic algorithm**
  - COMP-128-1: 56 bit Kc, algorithm broken and public tool to retrieve Ki from SIM
  - COMP-128-2: 56 bit Kc, fix cryptographic problem with the 1st version
  - COMP-128-3: 64 bit Kc
- **New algorithm adapted from the 3G authentication protocol**
  - Milenage-2G: AES-based, provided as a recommendation (and not a specification)
- **No authentication of the network to the subscriber**
  - Do not forget, this was the end of the 80's !

# GSM subscriber authentication



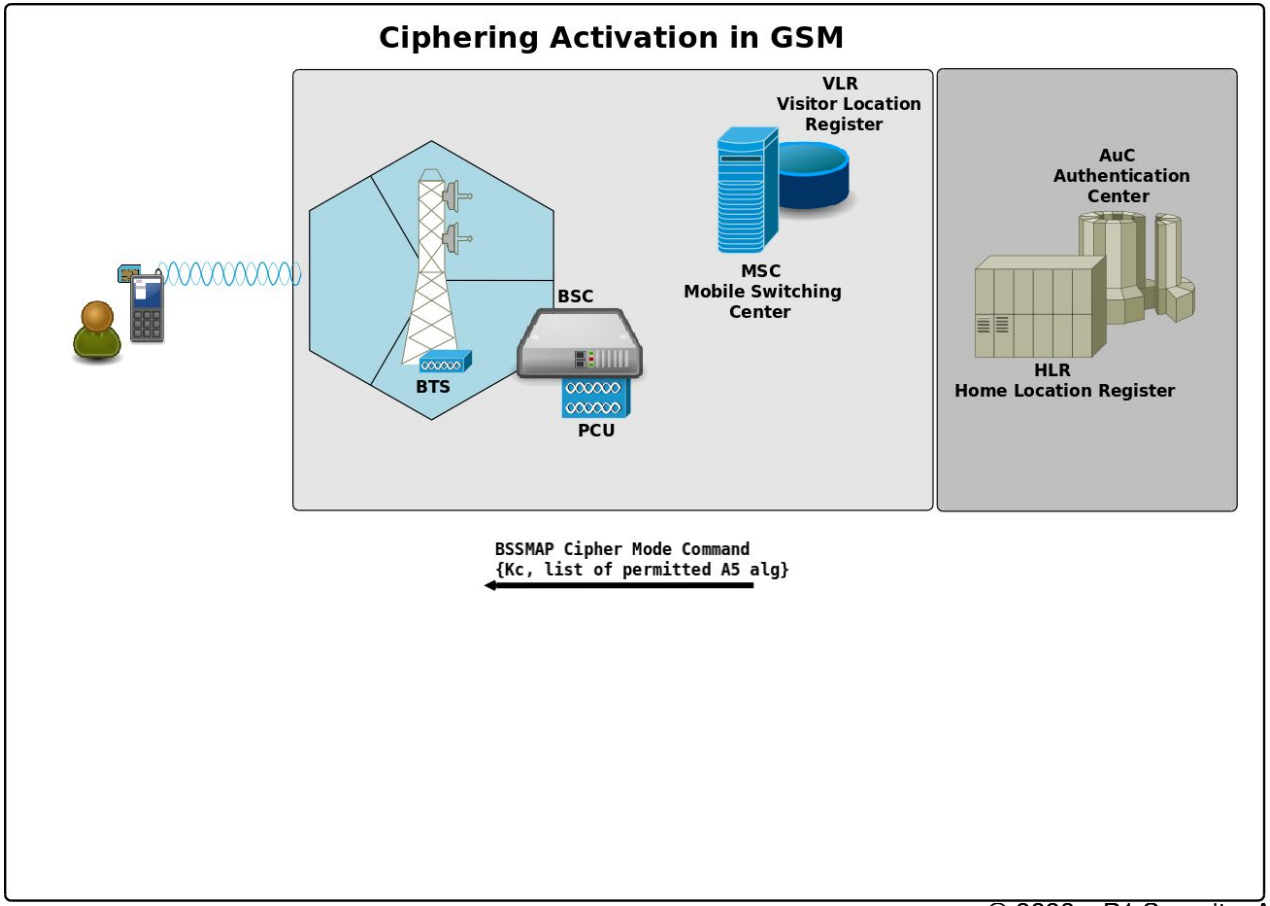
# GSM subscriber authentication (2)



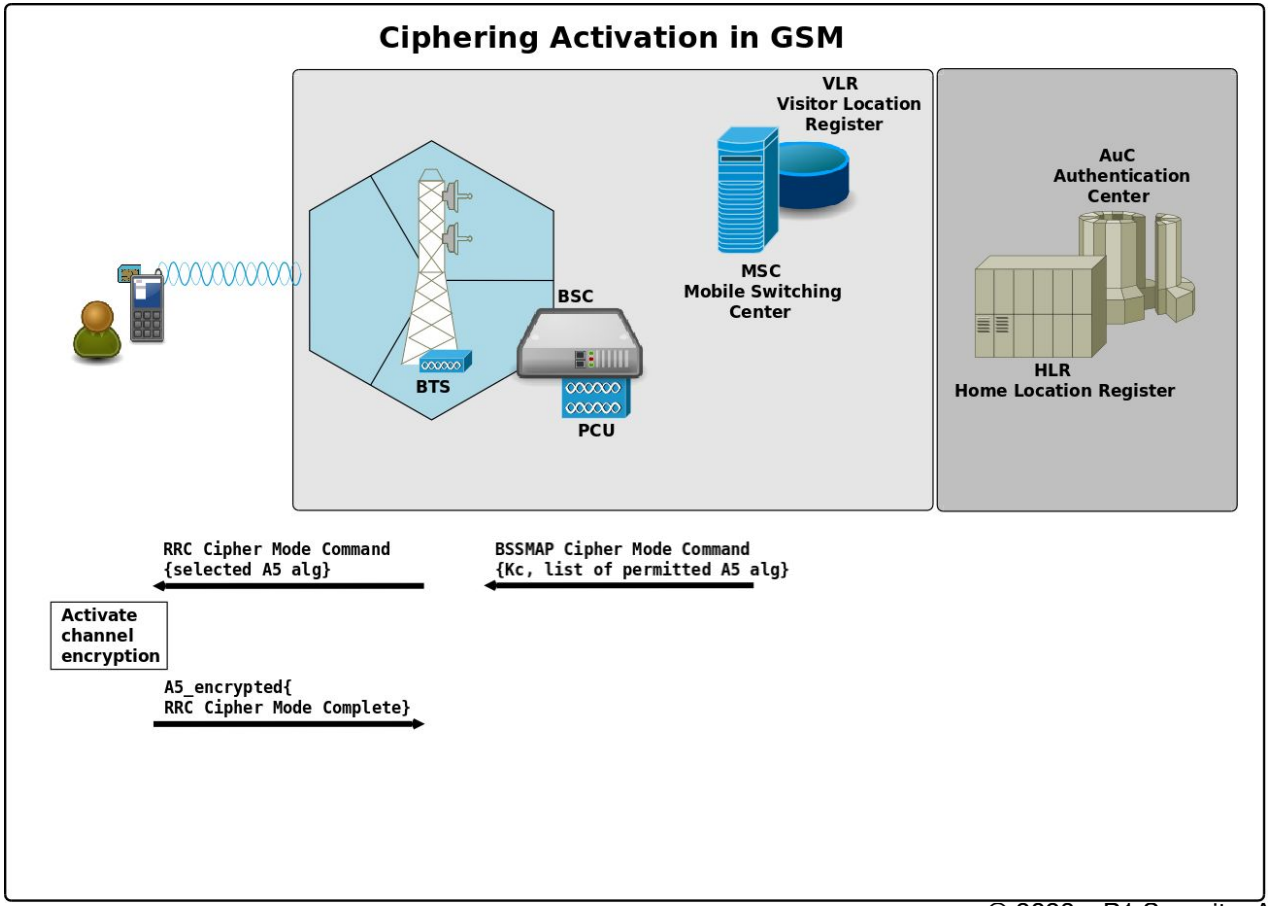
# Encryption of channels for CS services

- **GSM CS services are encrypted at a very low radio layer**
  - TCH and SDCCH radio burst between the UE and the BTS are encrypted
- **2 initial algorithms defined for encryption:**
  - Using a 64 bits symmetric key
  - A5/1: main GSM ciphering algorithm, stream-cipher, LFSR-based
    - Broken since the early 2000's, a public tool for cryptanalysis available since 2009
    - Still in use today
  - A5/2: "trapped" GSM ciphering algorithm, stream-cipher, LFSR-based
    - Broken since the early 2000's with a public tool for cryptanalysis straight
    - Not supported by handsets since 2007 / 2008.
- **New algorithms derived from the work done for UMTS security**
  - based on Kasumi, block-cipher
  - A5/3: 64 bit variant, today widely deployed and used
  - A5/4: 128 bit variant, rarely supported and not deployed at all
- **Encryption is not mandatory, but a MNO decision and configuration**
  - A5/0: actually no encryption

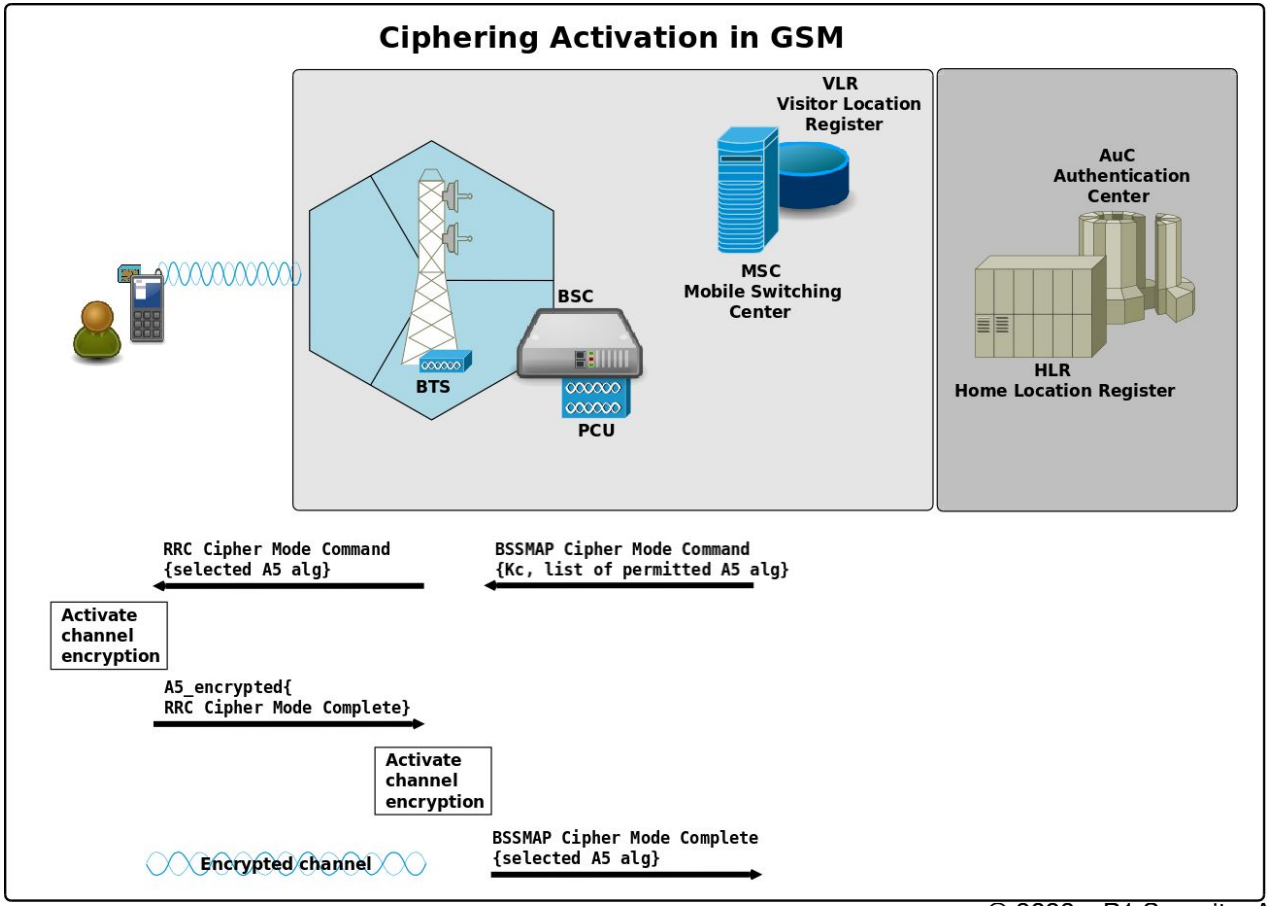
# GSM security activation



# GSM security activation (2)



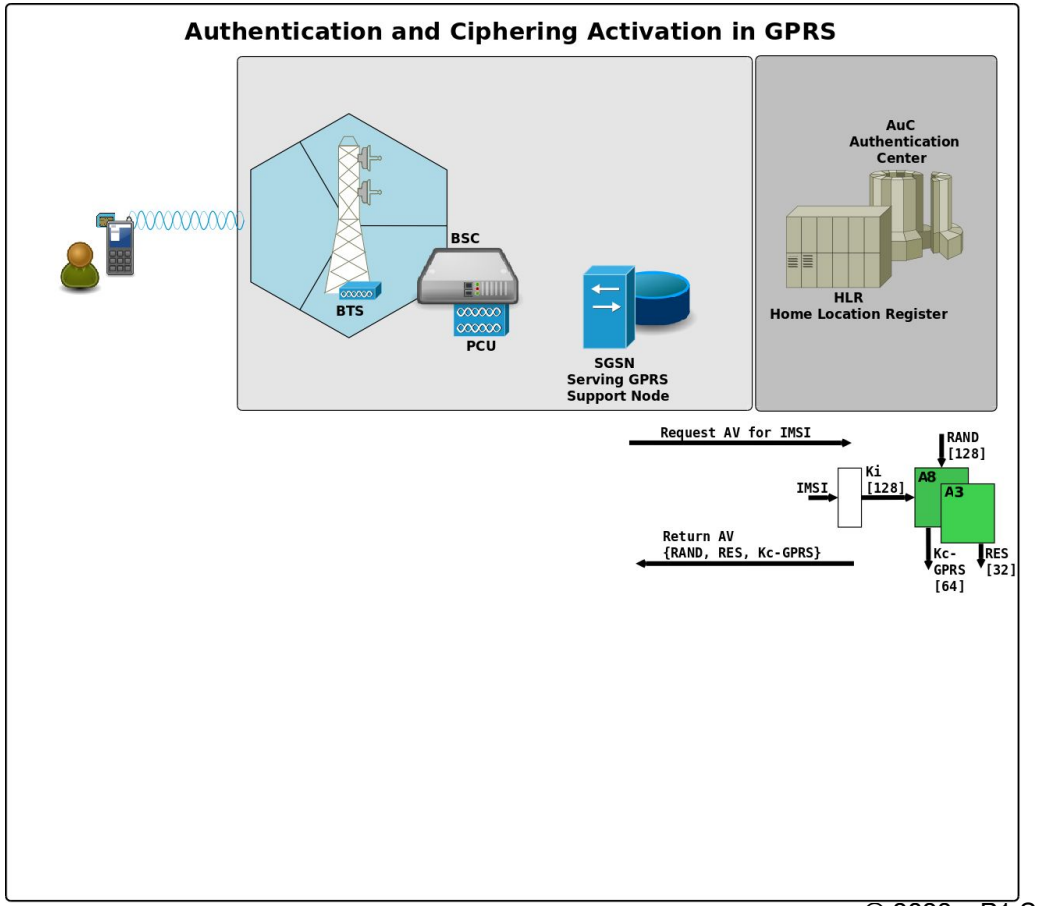
# GSM security activation (3)



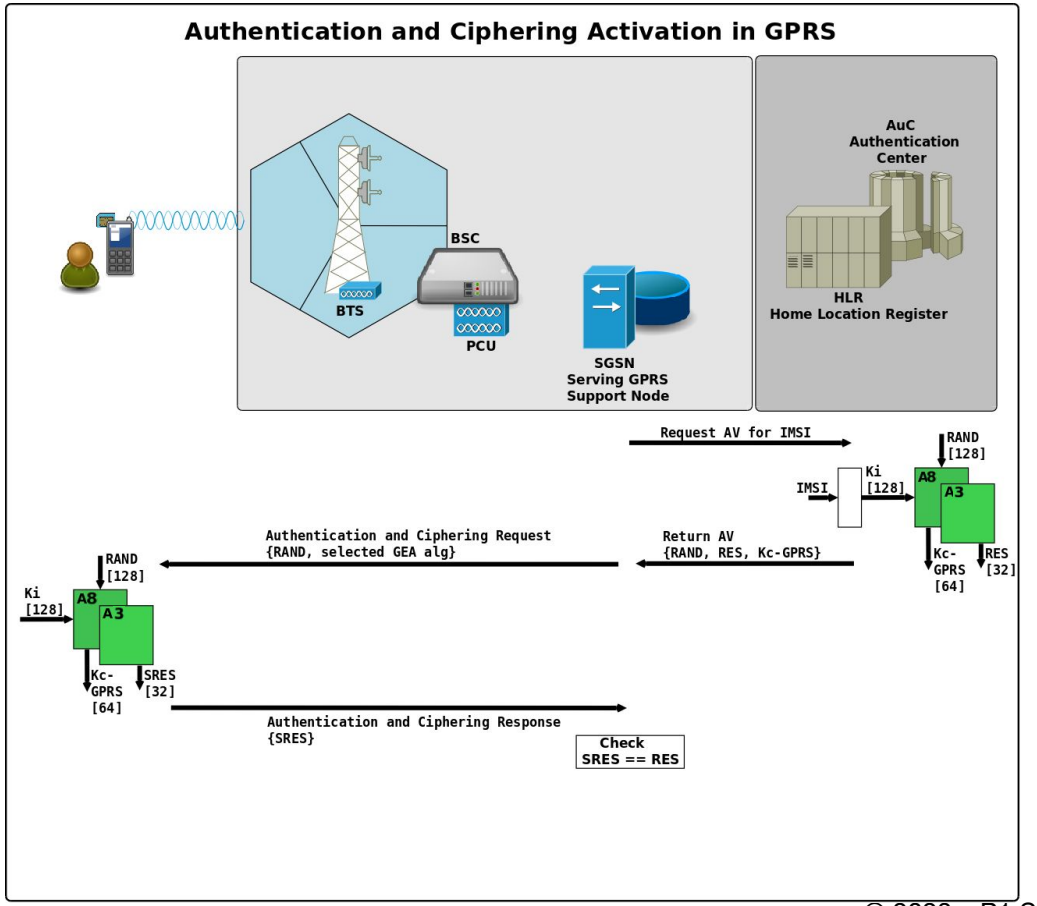
# Encryption of GPRS links

- **GPRS services encrypted at the logical link layer**
  - LLC link between the UE and the SGSN is encrypted
- **2 initial algorithms defined for encryption:**
  - Using a 64 bits symmetric key
  - GEA1: “trapped” GPRS ciphering algorithm, stream-cipher, LFSR-based
    - Known to be weak since 2011
    - “Officially” broken since 2021, public tools for cryptanalysis available
    - Little used today
  - GEA2: main GPRS ciphering algorithm, stream-cipher, LFSR-based
    - Not weakened like GEA1 ! May still be used in some networks
- **New algorithms derived from the work done for UMTS security**
  - based on Kasumi, block-cipher, used in a counter mode (mimicking a stream-cipher)
  - GEA3: 64 bit variant, widely deployed and used today
  - GEA4: 128 bit variant, rarely supported and deployed
- **Encryption is not mandatory, but a MNO decision and configuration**
  - GEA0: actually no encryption

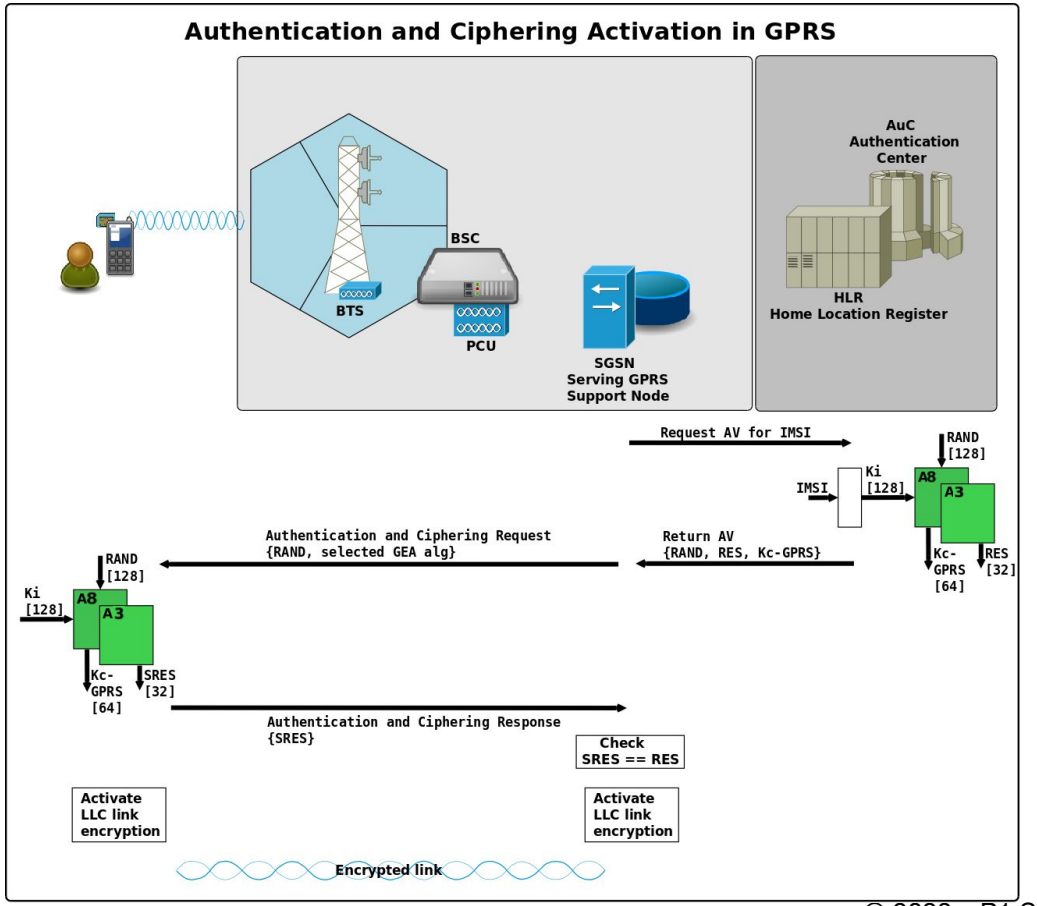
# GPRS authentication and security activation



# GPRS authentication and security activation (2)



# GPRS authentication and security activation (3)



# Temporary identifiers

- **As soon as GSM radio channel or GPRS link is encrypted, the network assigns a temporary identity to the subscriber**
  - TMSI assigned by the MSC/VLR
  - P-TMSI assigned by the SGSN
- **From here, the UE will use this temporary identity to identify itself to the network**
  - Specifically in signaling message, before activation of the ciphering
- **This prevents passive tracking of network subscribers through their IMSI**
- **It is renewed on a regular basis: e.g. every 2 to 4 hours**
  - Depends on the MNO configuration

# Attacks against 2G networks

# Tracking 2G subscribers

- **Passive tracking:**
  - IMSI is sometimes requested in clear-text
  - IMEI (in the CS domain) and IMEI-SV are also often requested in clear-text by MSC/VLR and SGSN
- **Semi-passive tracking:**
  - TMSI is often not renewed after each active connection
  - Enables the tracking of a given MSISDN, by correlating TMSI paged by the network after a few “silent” calls
- **Active tracking:**
  - IMSI-catcher: simply fakes a legitimate BTS and requests IMSI, IMEI and TMSI of all surrounding UEs
- **Open-source tools for 2G air interface monitoring**
  - osmocom-bb
  - gr-gsm

# Breaking 2G encryption

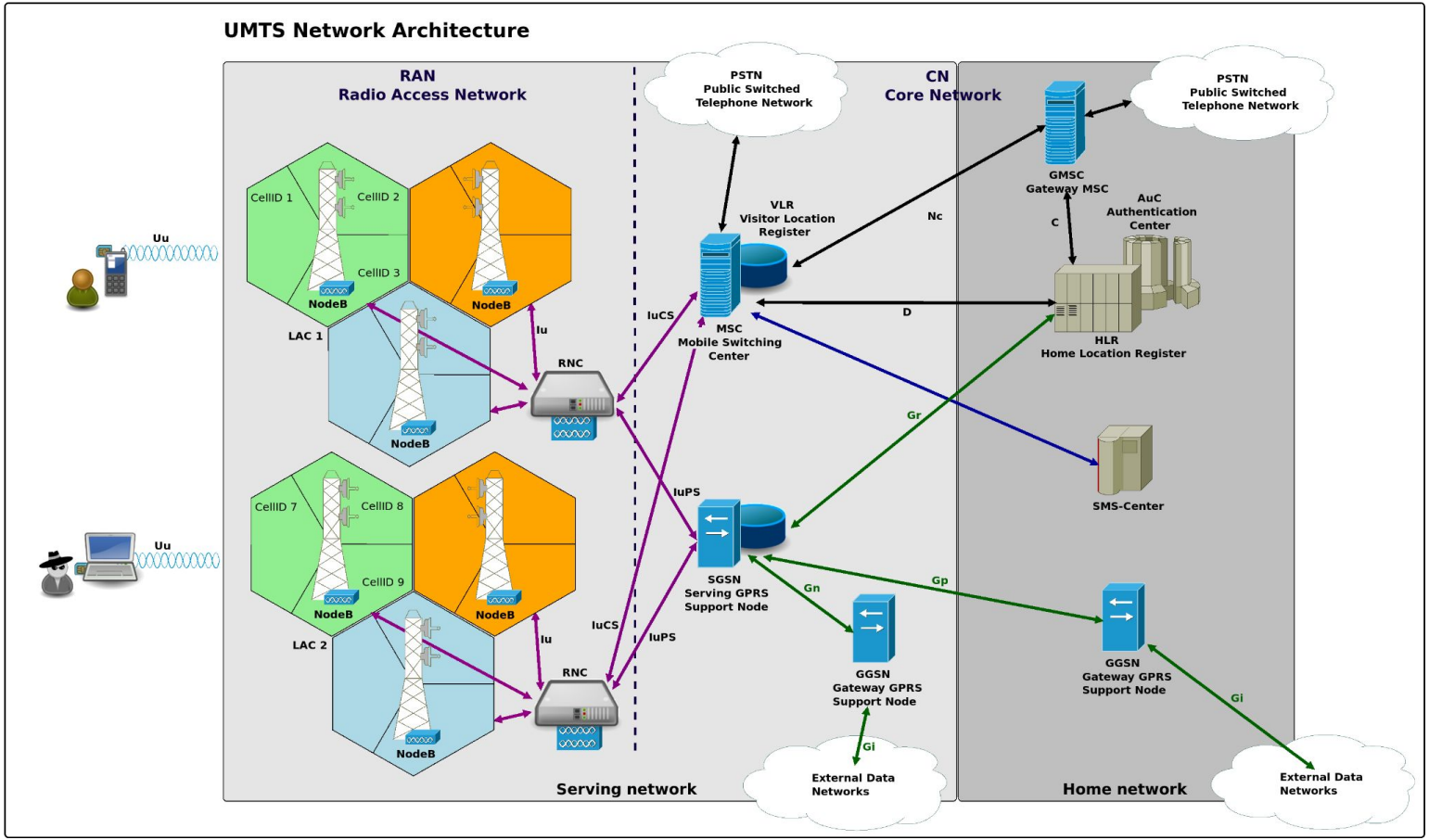
- **2G encryption is globally outdated**
  - 64 bit keys
  - Initial algorithms with LFSR design from the 80's
  - No support for 128 bit keys algorithms in recent handsets
- **Open-source tools exist to break A5/1 and A5/2 encryption**
  - A5/2: real-time cracking with no significant processing
  - A5/1: almost real-time cracking, using rainbow tables (~1.8TB) and a GPU
- **GSM encryption is badly designed**
  - Stream-cipher, many known plain-text (SI in SACCH frames, padding bits)
  - Error correction code encrypted
  - Presentation (from Blackberry at Defcon 2019) about cracking A5/3 with rainbow tables
- **GPRS encryption is also supposed to be badly designed**
  - GEA1 and GEA2 specifications was not public
  - Cryptanalysis from 2021: revealed GEA1 has intentional weakness and GEA2 is still weak
  - Open-source tools:
    - https://github.com/P1sec/gea-implementation
    - https://github.com/airbus-seclab/GEA1_break

# 2G security is outdated

- **No network-to-subscriber authentication**
  - Fake base-stations are straightforward
  - Capture surrounding subscribers of a given PLMN
    - Obtain their identification
    - Relay / intercept their GSM and GPRS traffic
    - Inject any signaling (SMS) and traffic (web pages, media files)
- **Many open-source software for 2G network emulation**
  - OpenBTS
  - YateBTS
  - Osmocom stack
- **No integrity-protection of the RRC / NAS signaling**
  - enables clever (less detectable) attacks, by e.g. modifying UE security capabilities

# 3G Network Architecture

# 3G Network Architecture



# Principles of UMTS

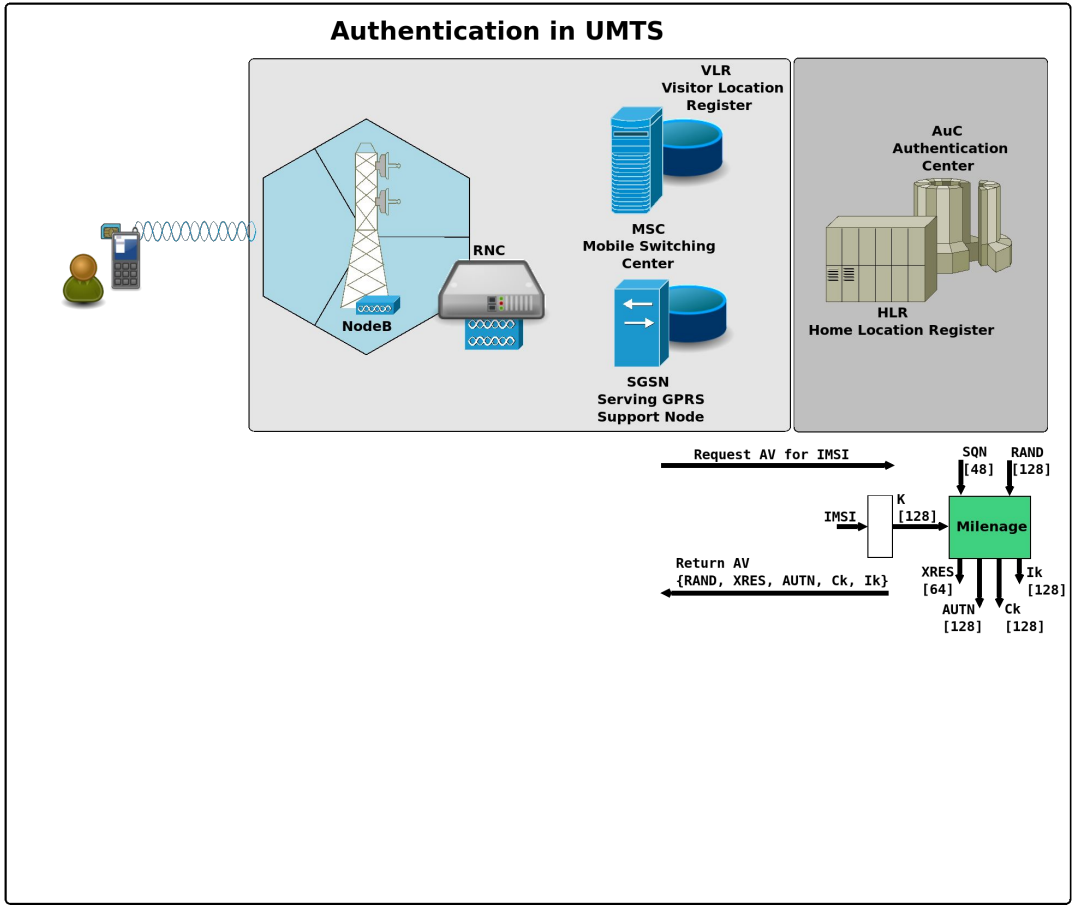
- **Entire rework of the radio interfaces and RAN equipments**
  - WCDMA for base-stations and subscribers multiplexing
  - 5 MHz bandwidth per channel
    - QPSK (UMTS), 16-QAM and 64-QAM (HSPA)
  - FDD mode: 2100 MHz downlink, 1900 MHz uplink
  - Rationalization of RAN interfaces and procedures
- **Reuse of the CS and PS core domains**
  - No new services compared to GSM / GPRS networks
  - Just an higher throughput for data connection and crystal-clear CS calls !
- **New security procedures**
  - New mutual authentication protocol: USIM application onto SIM card
  - Integrity-protection of the signaling

# 3G Network Security

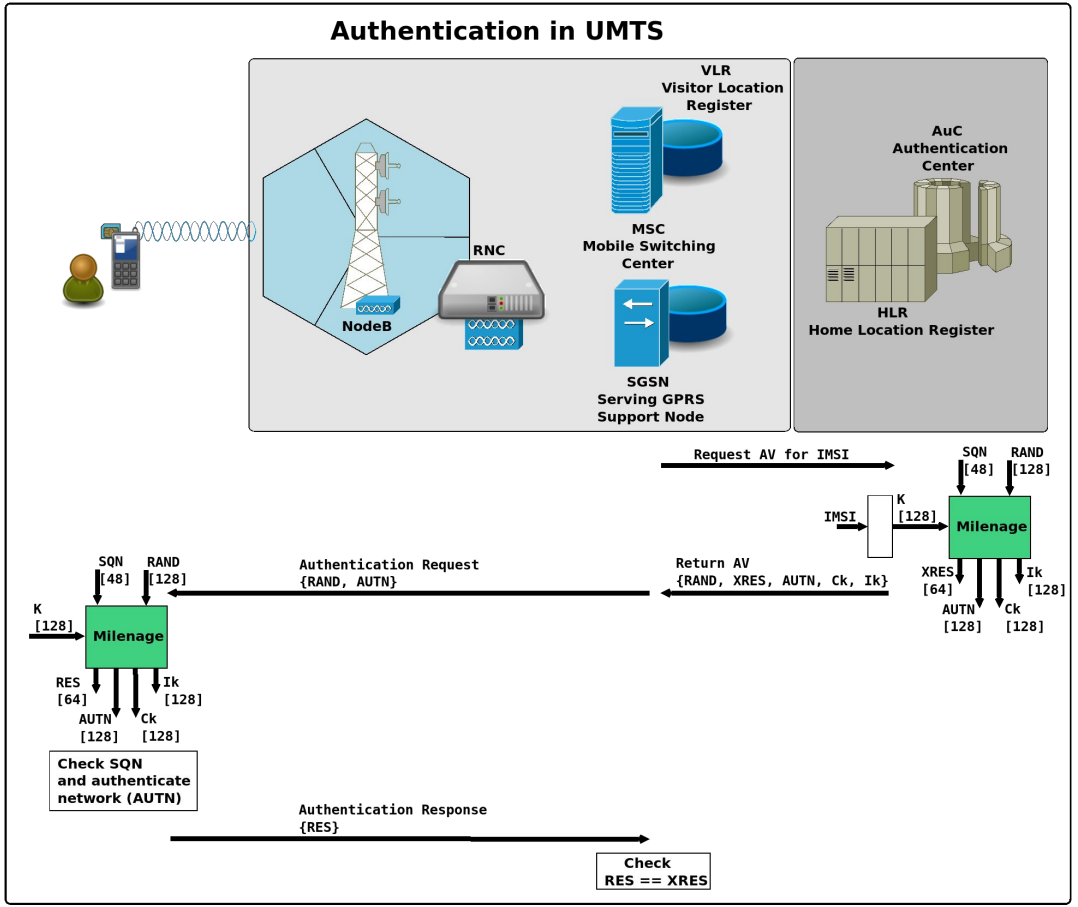
# 3G-AKA authentication properties

- **Mutual authentication**
  - Single challenge - response roundtrip
  - Anti-replay mechanism, based on a 48 bit counter SQN
  - Network-to-subscriber authentication based on a Message Authentication Code MAC-A,
    - using K, over {RAND, SQN, AMF}
  - Subscriber-to-network authentication based on a Message Authentication Code RES,
    - using K, over {RAND}
  - Two 128 bit keys {Ck, Ik} produced as side effect
    - To be used for ciphering and integrity-protection of the radio connection
- **Resynchronization procedure**
  - In case the SQN in the USIM shifted from the SQN in the AuC
  - USIM outputs its own SQN value, masked, to be processed by the AuC
- **Efficient implementation proposal**
  - Milenage: using AES as internal cryptographic function

# 3G subscriber authentication



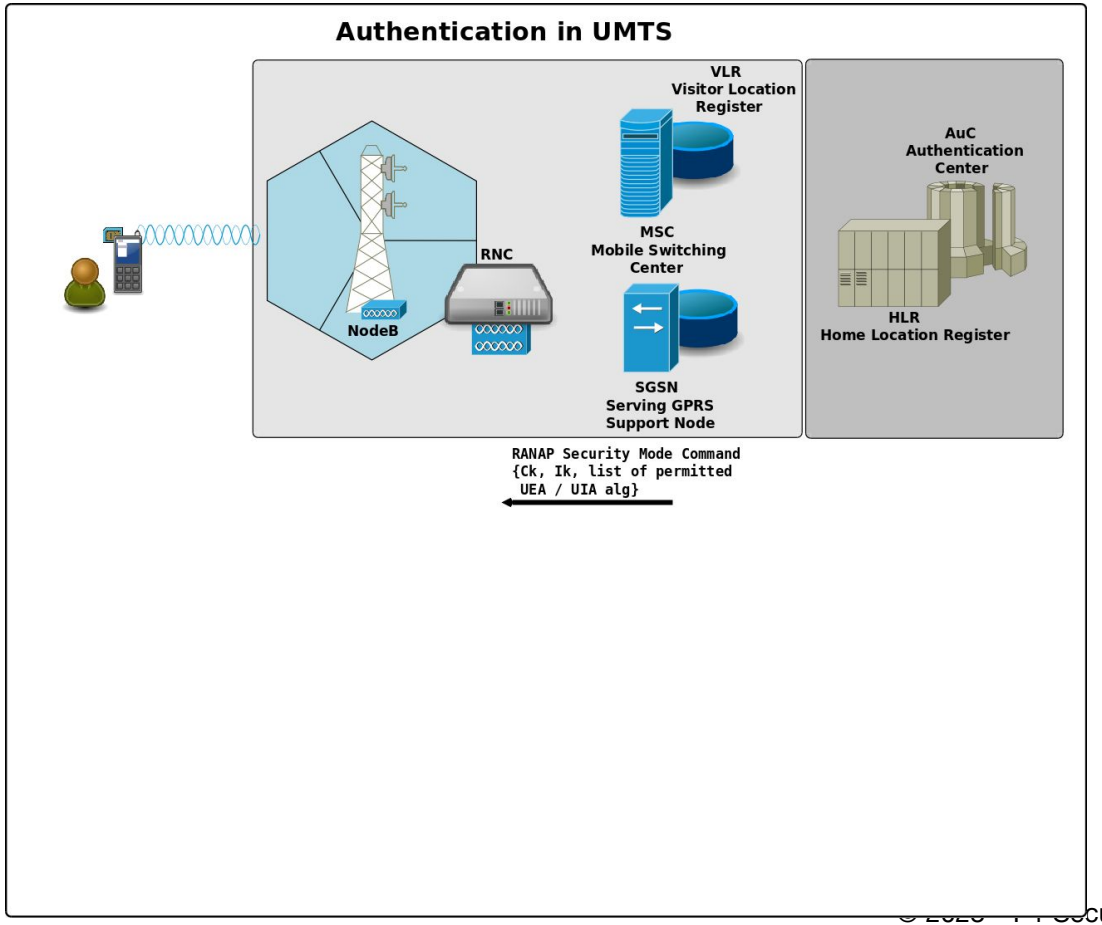
# 3G subscriber authentication (2)



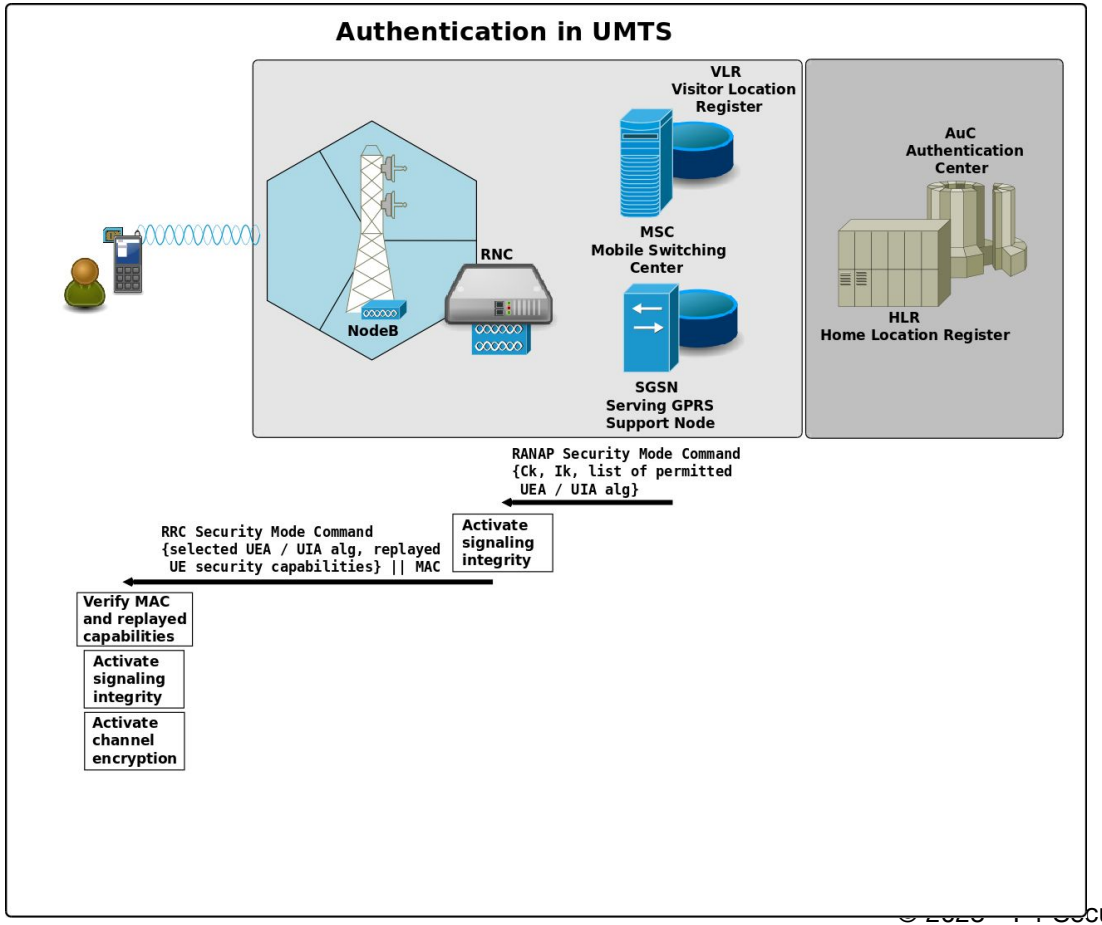
# Cryptographic protection of 3G connections

- **All CS and PS services are handled in a uniform way at the radio interface**
  - Parallel security contexts still exist
  - Protection of the radio interface between the UE and the RNC
- **Initial algorithms defined for UMTS**
  - Kasumi: 64 bit block-cipher with 128 bit key
  - UEA1: counter mode for encryption of both dedicated signaling and traffic channels with key Ck
  - UIA1: MAC mode for integrity protection for dedicated signaling channels with key Ik
- **Second algorithms developed in 2007**
  - SNOW-3G: stream-cipher with 128 bit key
  - Used as is for encryption (UEA2) and in a specific MAC mode for integrity-protection (UIA2)
  - Reused in LTE
- **Encryption is not mandatory, but a MNO decision and configuration**
  - UEA0: actually no encryption
- **Integrity-protection of the signaling mandatory in all cases !**
  - Except for emergency calls in LSM (Limited Service Mode)

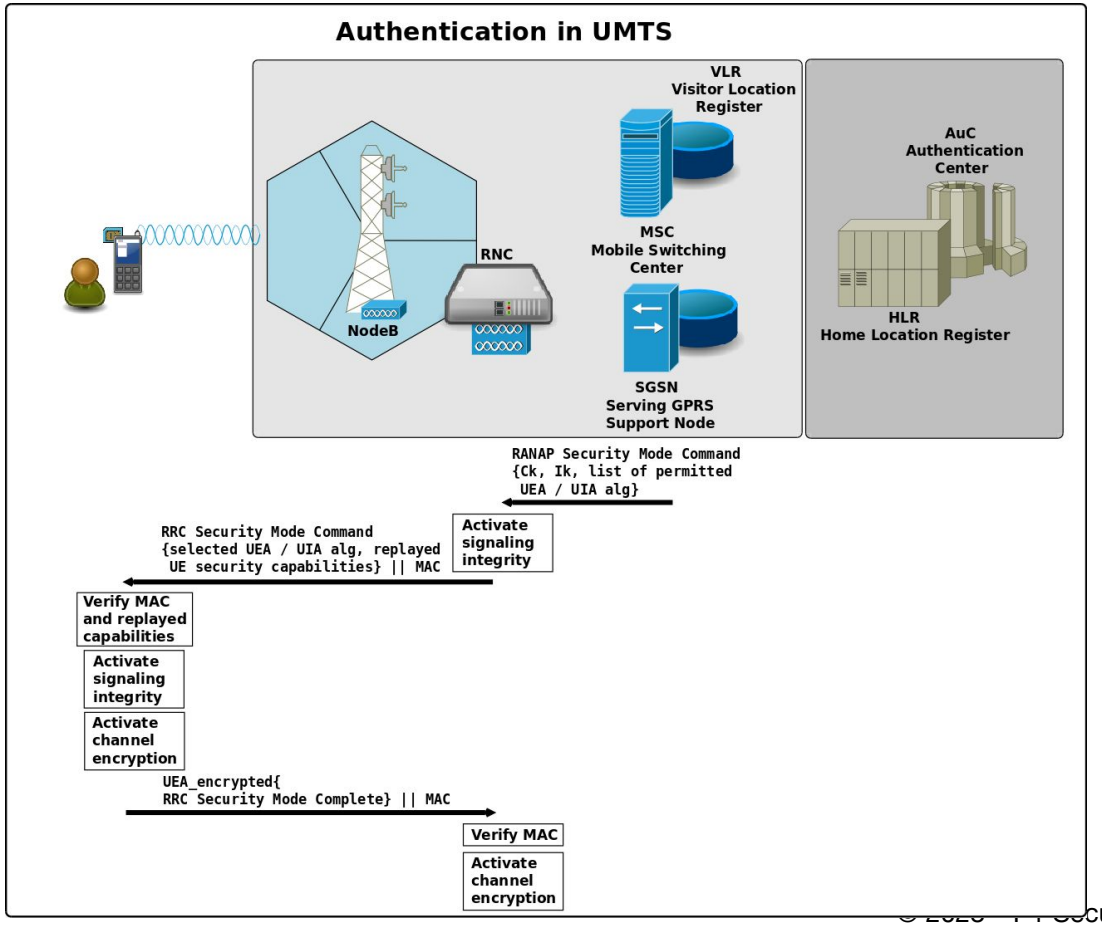
# UMTS security activation



# UMTS security activation (2)



# UMTS security activation (3)



# Attacks against 3G networks

# Not as many as in 2G, but still

- **Passive, semi-active tracking still possible on 3G**
  - However no open-source stack to do this
- **Push surrounding handsets to fallback to GSM / GPRS**
  - Jamming 3G frequencies (distincts from 2G)
  - Install a fake 3G base-station redirecting UE to a fake 2G base-station
  - OpenBTS-UMTS
    - Potentially catching IMSI, IMEI and TMSI too
- **Mutual authentication and integrity-protection of the signaling in 3G saves from traffic interception with a fake 3G base-station**
  - Attacker need a legitimate RNC from a MNO to access clear-text 3G traffic
  - Why not try a femtocell ?
- **If you have access to a roaming interconnect**
  - Attacker can obtain legitimate authentication vectors
  - Attacker's NodeB / RNC / femtocell setup becomes legitimate from the subscriber perspective

# Conclusion

# Conclusion

- **2G networks are largely insecure**
  - Many possible attacks
  - Many low cost equipments and open-source tools available

- **3G networks are more secure**
  - Most of the issues from 2G are addressed
  - Need to compromise legitimate femtocells, or access SS7 signalling, for intercepting 3G traffic
  - Protocol complexity leads to software bugs and potential vulnerable implementations
    - Both on handsets and network equipments
    - UE are multi-mode (support both 2G and 3G)

# Questions?

**Thank you for attention!**

**contact@p1sec.com**