Autentifikácia v mobilných sieťach

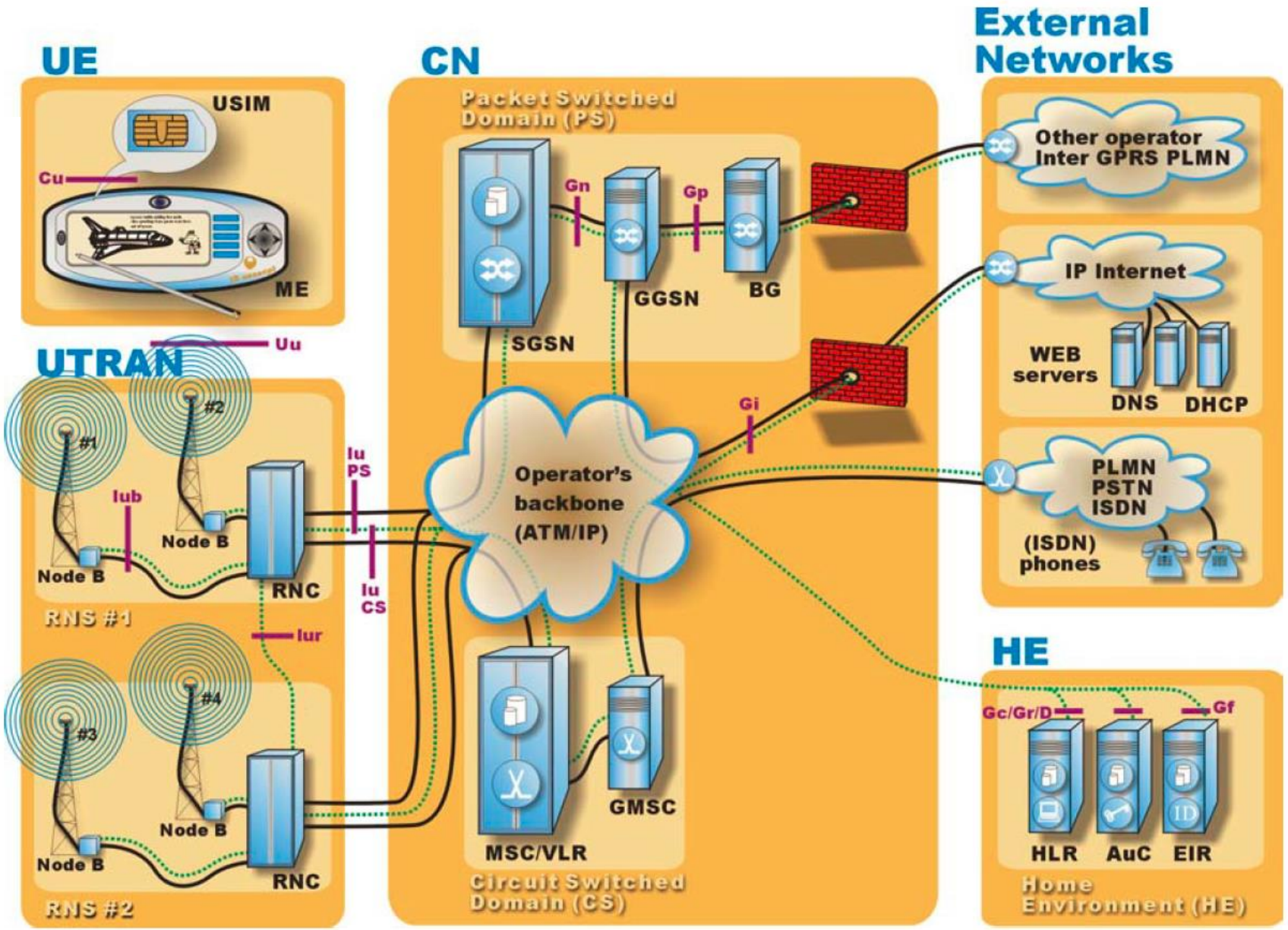
Bc. JÁN KOTRADY, UPJŠ 2016

Kľúčové slová

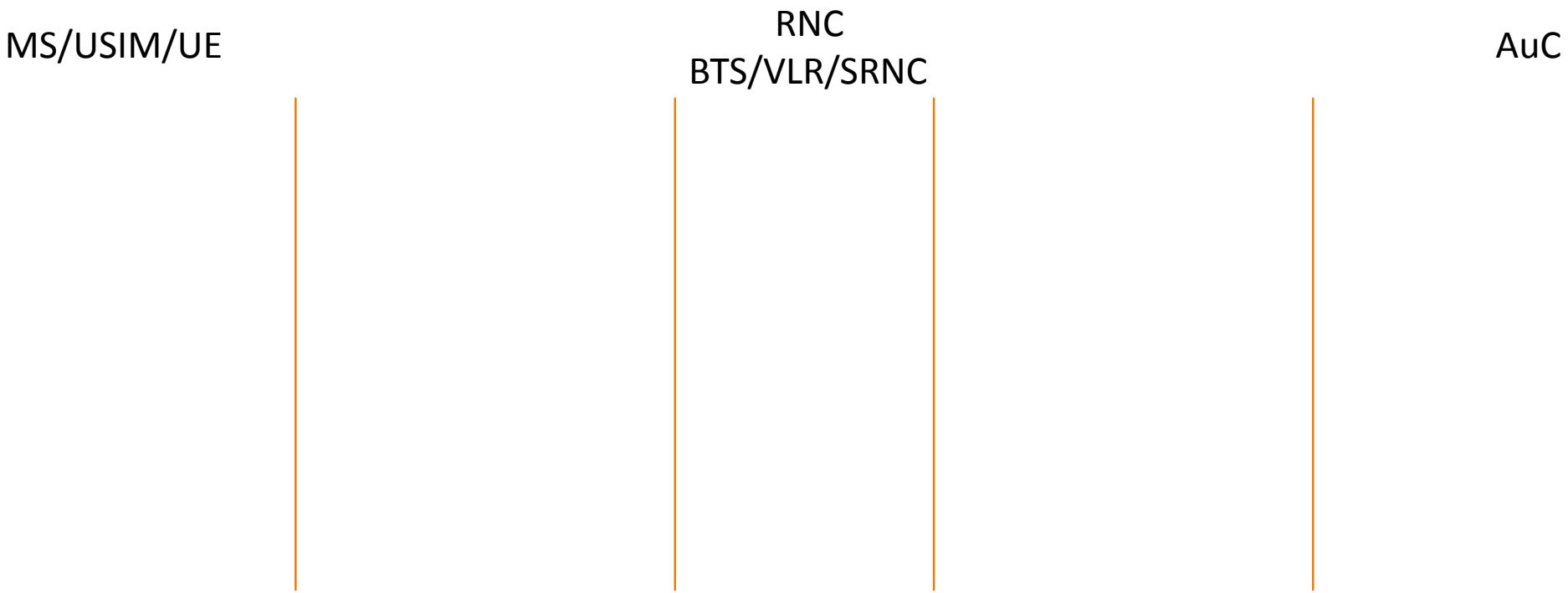
- Ki
- Kc
- RAND
- SRES (XRES)
- RES
- A3, A5
- IMSI – 15 čísel
- AUTN, MAC, SQN

Kľúčové slová

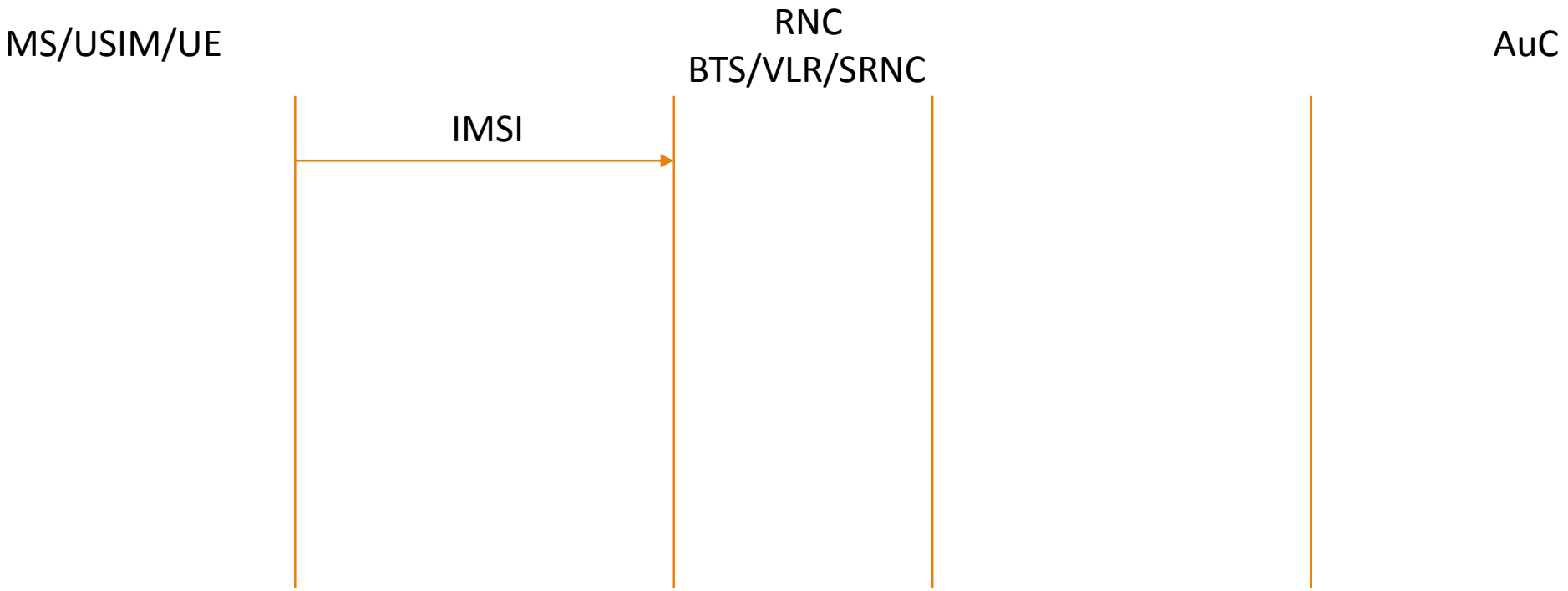
- USIM - Universal Subscriber Identity Module
- UE - User Equipment
- SRNC - Serving Radio Network Controller
- VLR - Visitor Location Register
- SQN - Sequence number
- AuC - Authentication Centre
- AUTN | S - Authentication token | Synchronization


UE
USIM
Cu
ME
Uu
UTRAN
#1
#2
Node B
Node B
Iub
RNC
RNS #1
Iur
#3
#4
Node B
Node B
RNC
RNS #2
Iu PS
Iu CS
CN
Packet Switched Domain (PS)
Gn
Gp
SGSN
GGSN
BG
Gi
Operator's backbone (ATM/IP)
MSC/VLR
GMSC
Circuit Switched Domain (CS)
External Networks
Other operator Inter GPRS PLMN
IP Internet
WEB servers
DNS
DHCP
PLMN
PSTN
ISDN
(ISDN) phones
HE
Gc/Gr/D
Gf
HLR
AuC
EIR
Home Environment (HE)

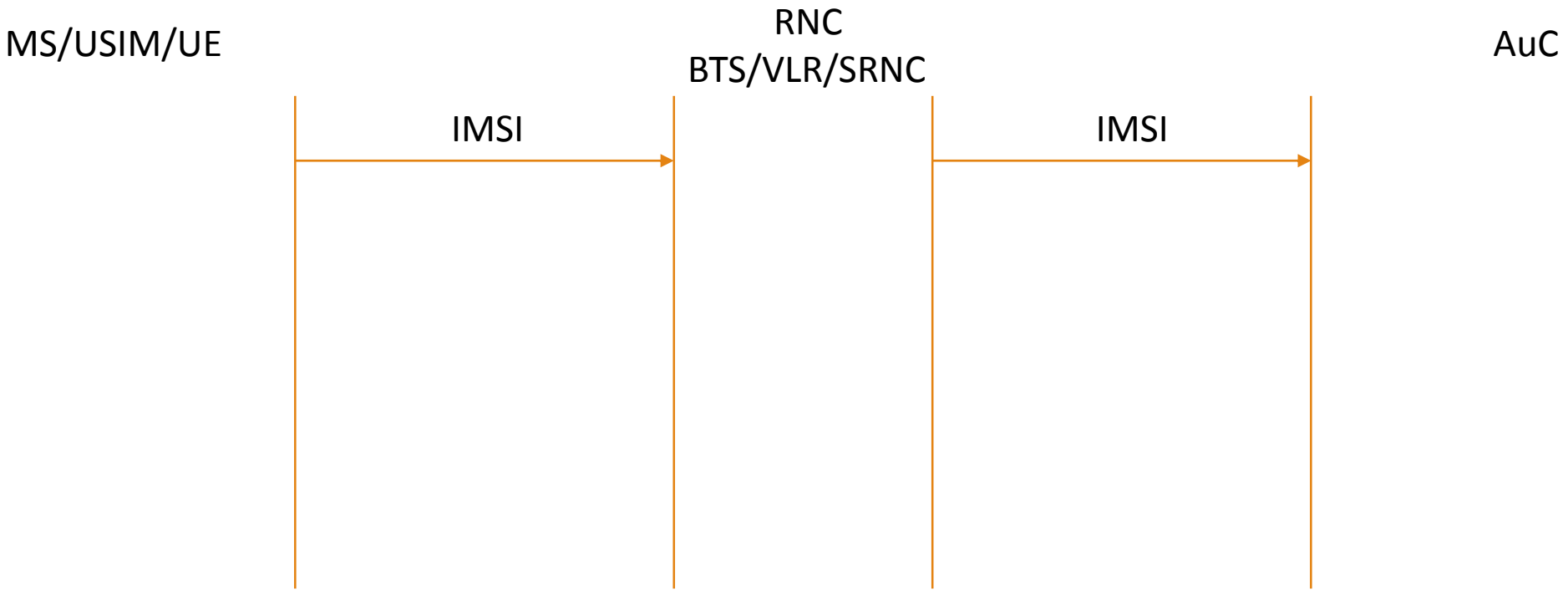
GSM autentifikácia



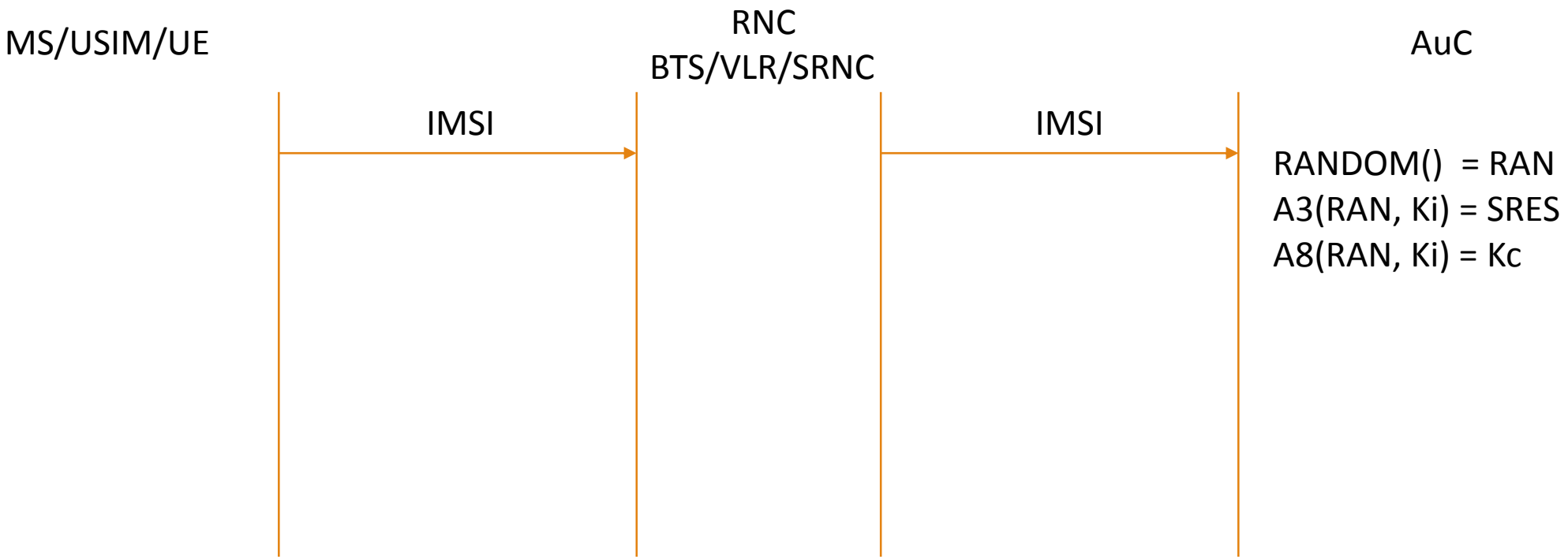
GSM autentifikácia



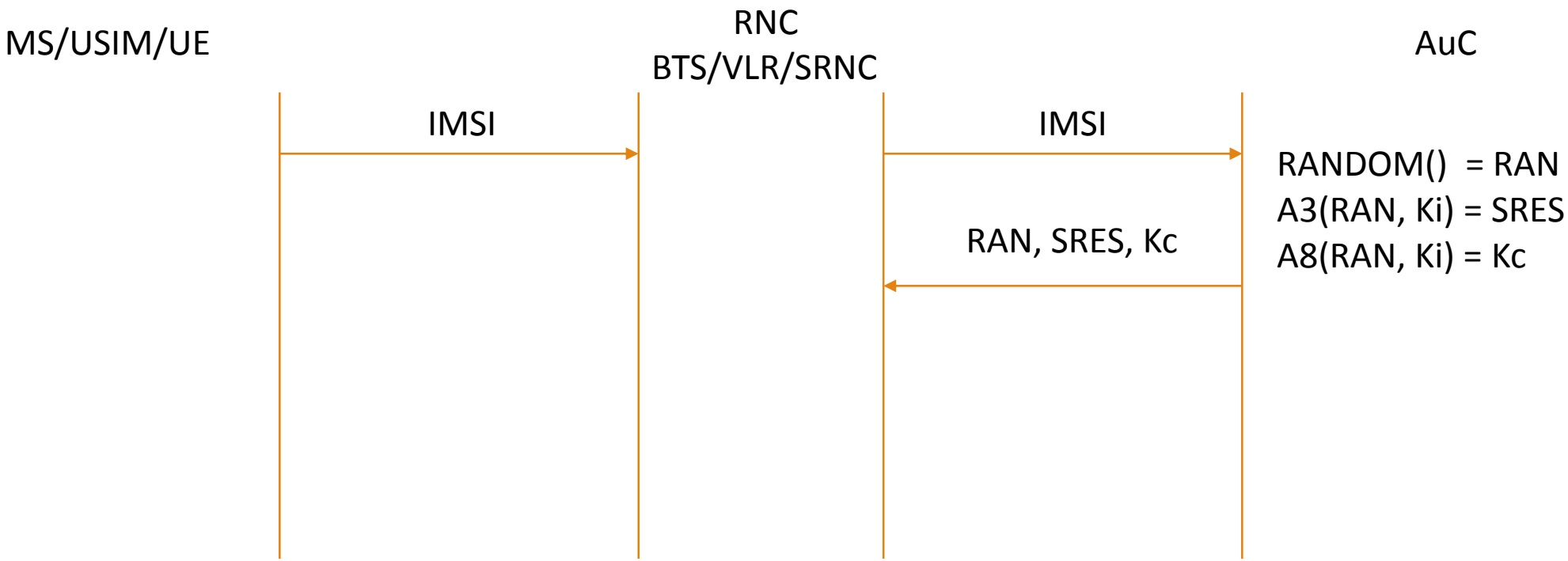
GSM autentifikácia



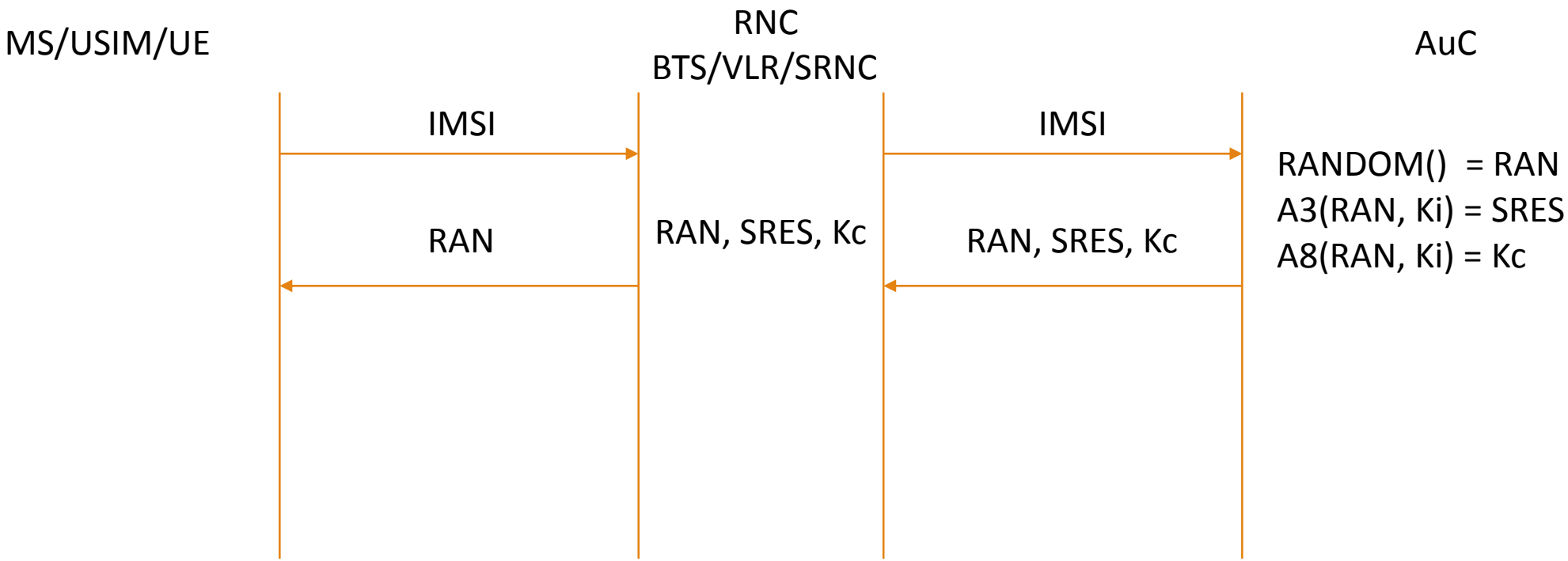
GSM autentifikácia



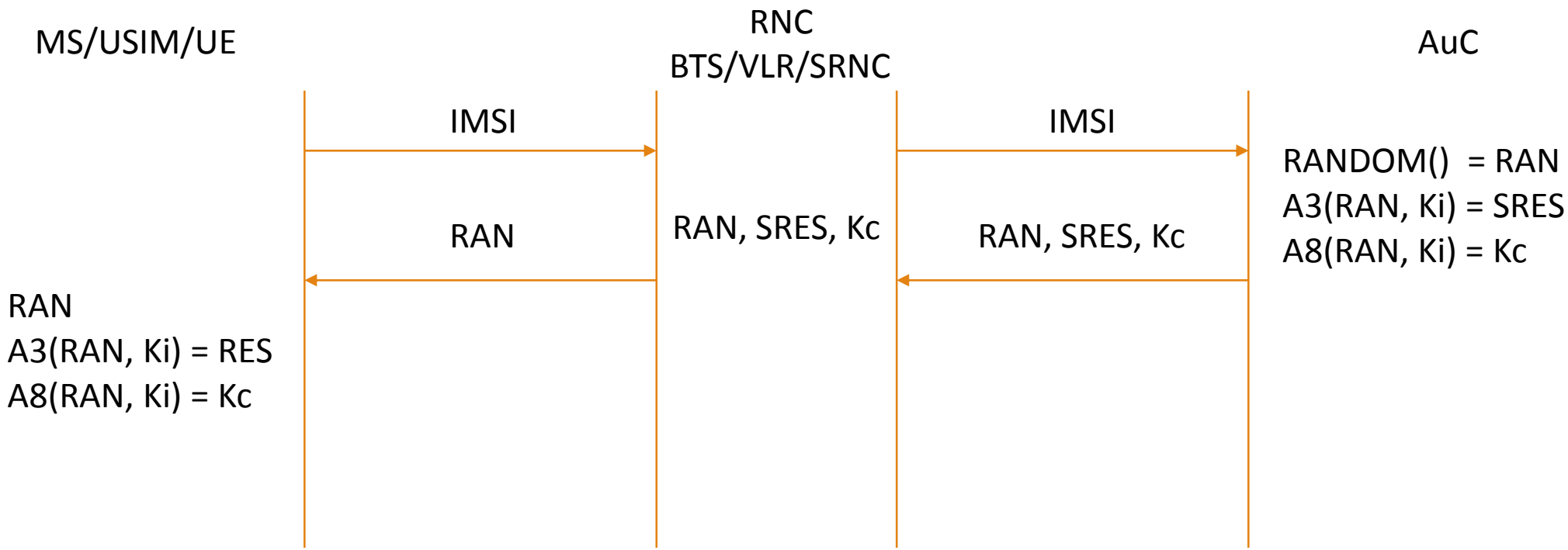
GSM autentifikácia



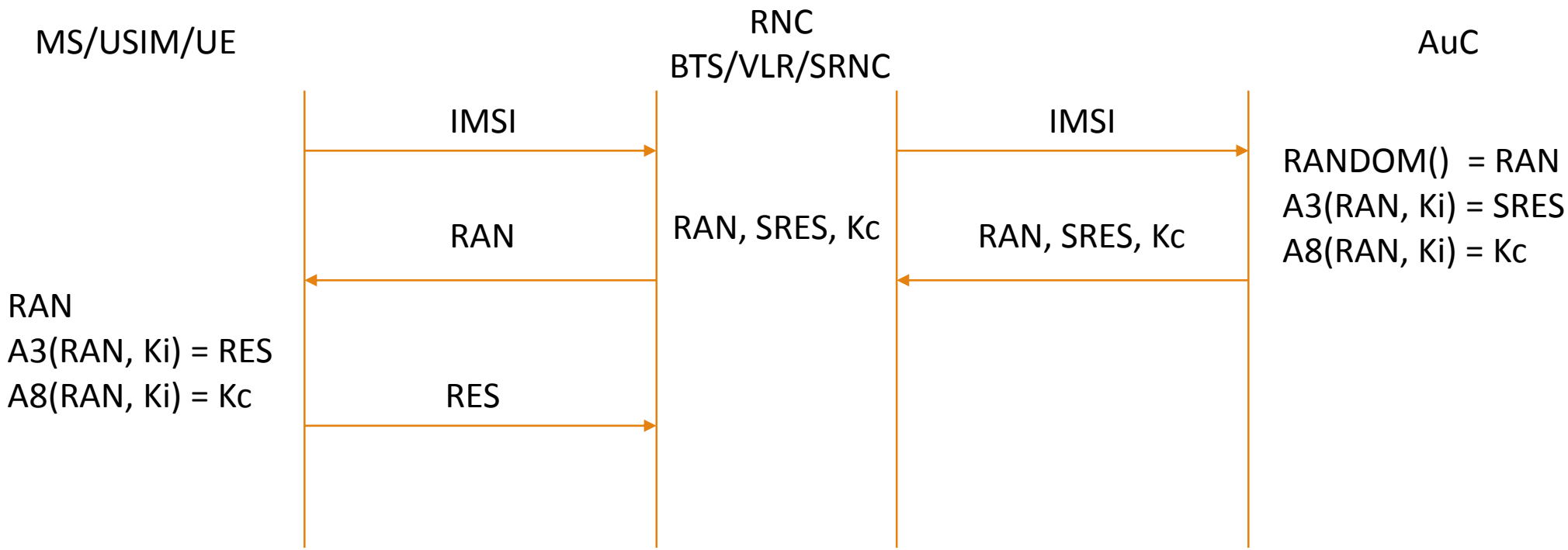
GSM autentifikácia



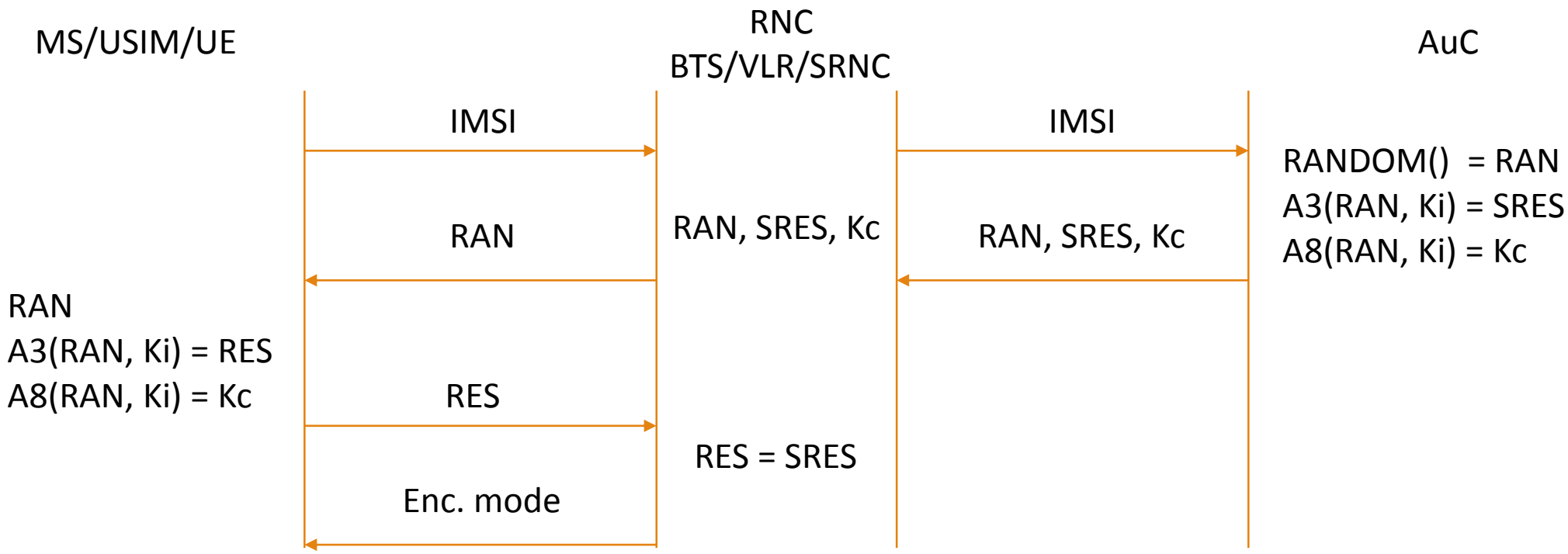
GSM autentifikácia



GSM autentifikácia



GSM autentifikácia



História chýb algoritmov

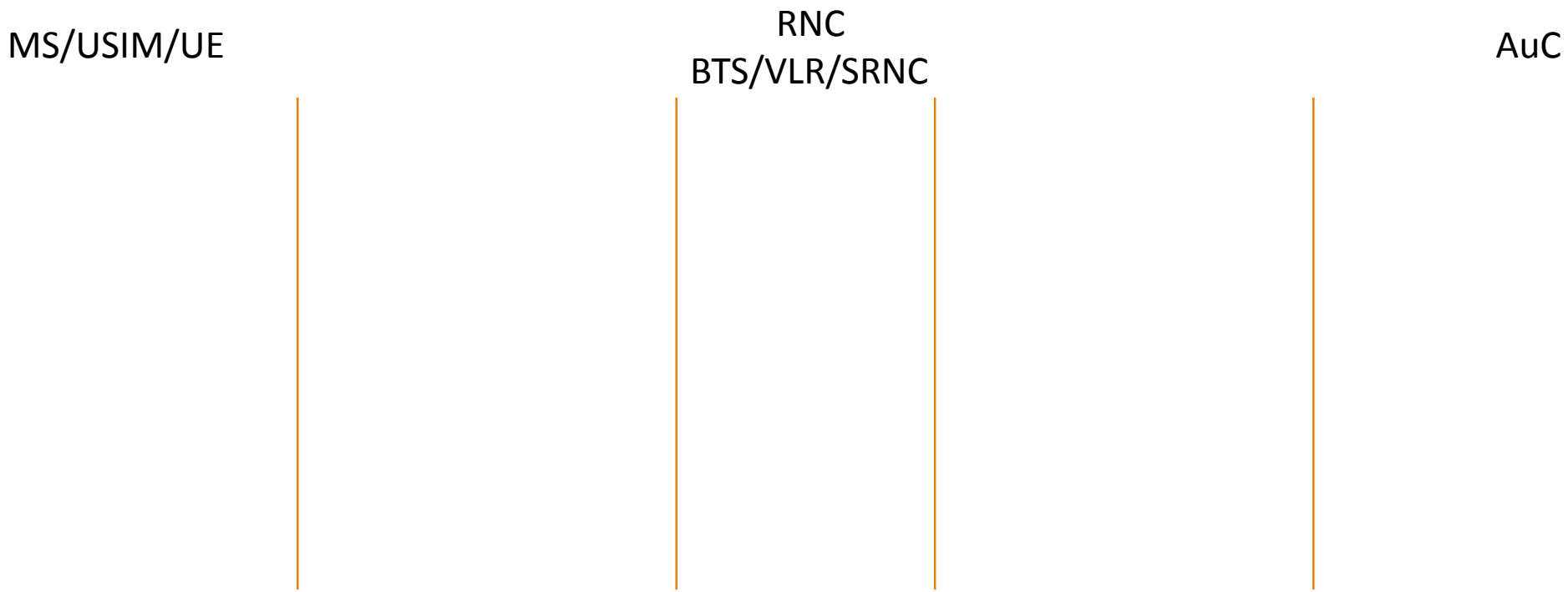
- 1991 – GSM implementácia
- Apríl 1998 - The Smartcard Developer Association (SDA) spolu s U.C. Berkeley researches prelomili COMP128 algoritmus uložený v SIM karte a úspešne získali Ki v priebehu pár hodín. Zistili, že Kc používa iba 54 bitov.
- August 1999: Slabá A5/2 bola prelomená použitím PC v priebehu pár sekúnd.
- December 1999: Alex Biryukov, Adi Shamir a David Wagner publikovali schému útoku na algoritmus A5/1. Pri získaní dvoch minút rozhovoru boli schopný prelomiť A5/1 algoritmus v priebehu 1 sekundy.
- Máj 2002: IBM Research group objavila nový spôsob rýchleho získavania Kc z COMP128 použitím útokov side channels.

3G a LTE

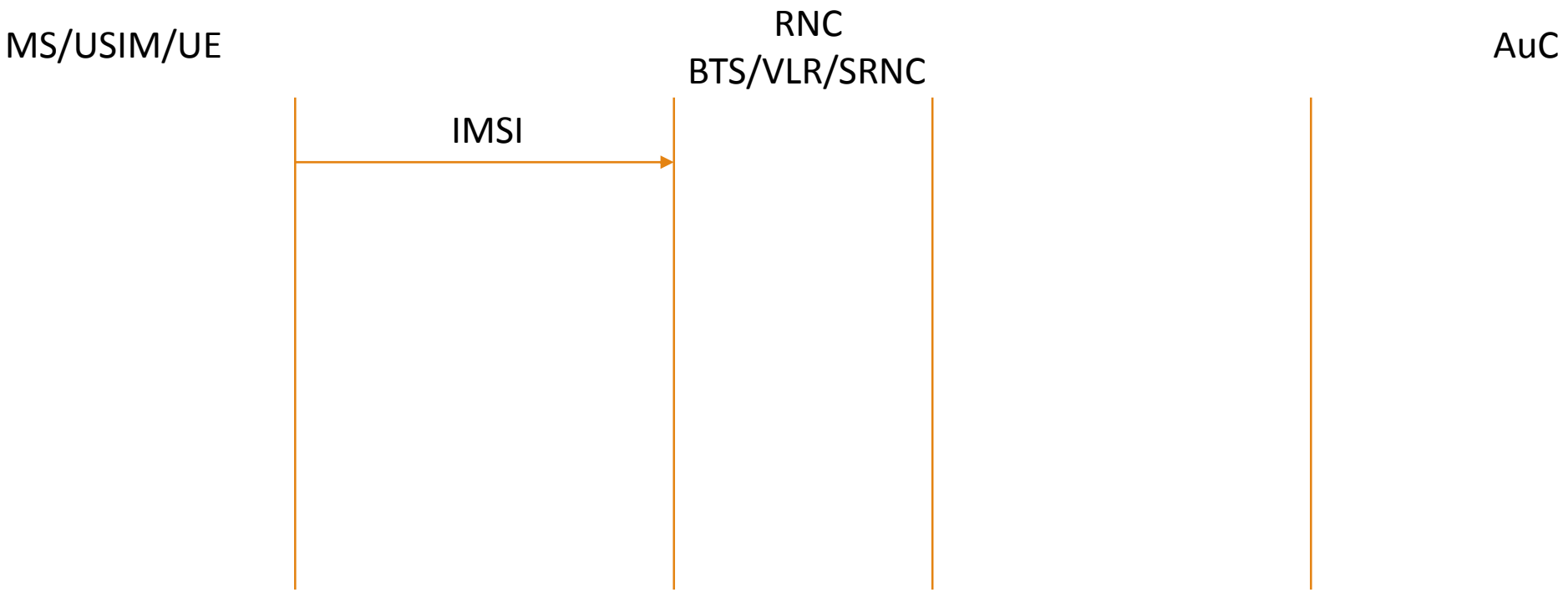
3G a LTE

Fukncia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	…	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na karte – zdieľaný	Žiadny	USIM, AuC		128

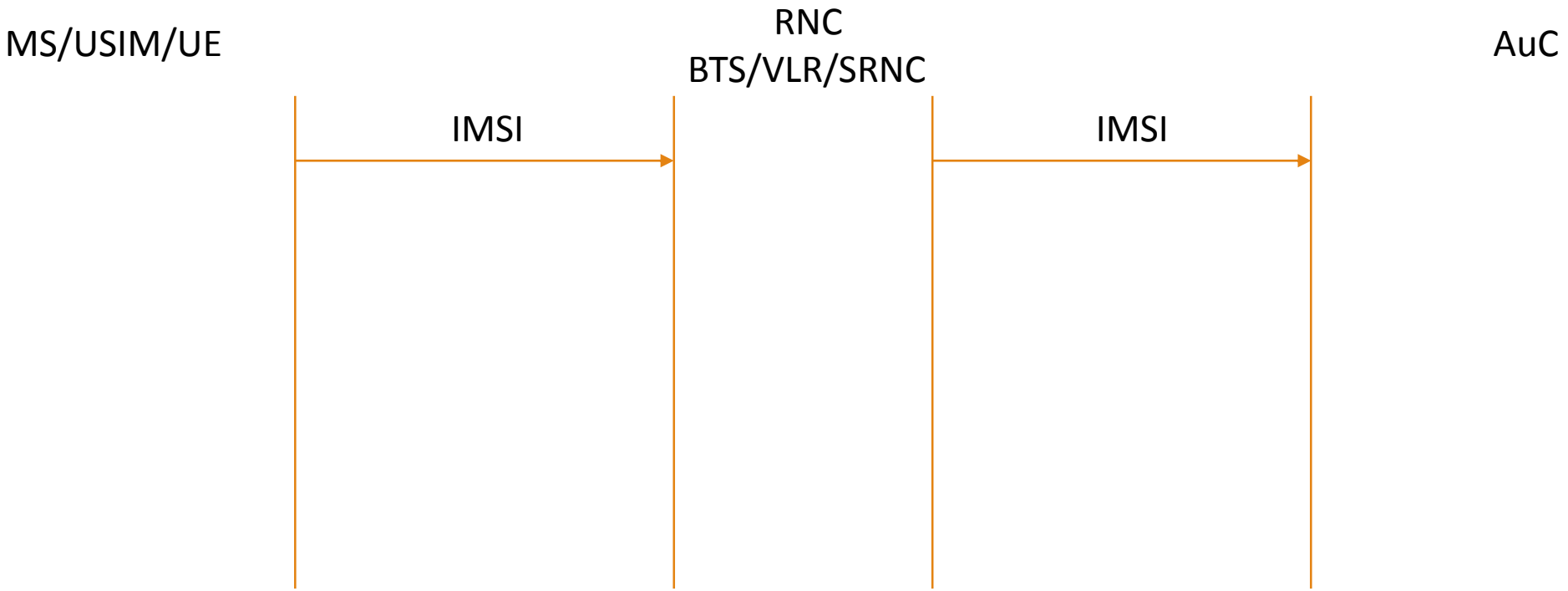
3G a LTE



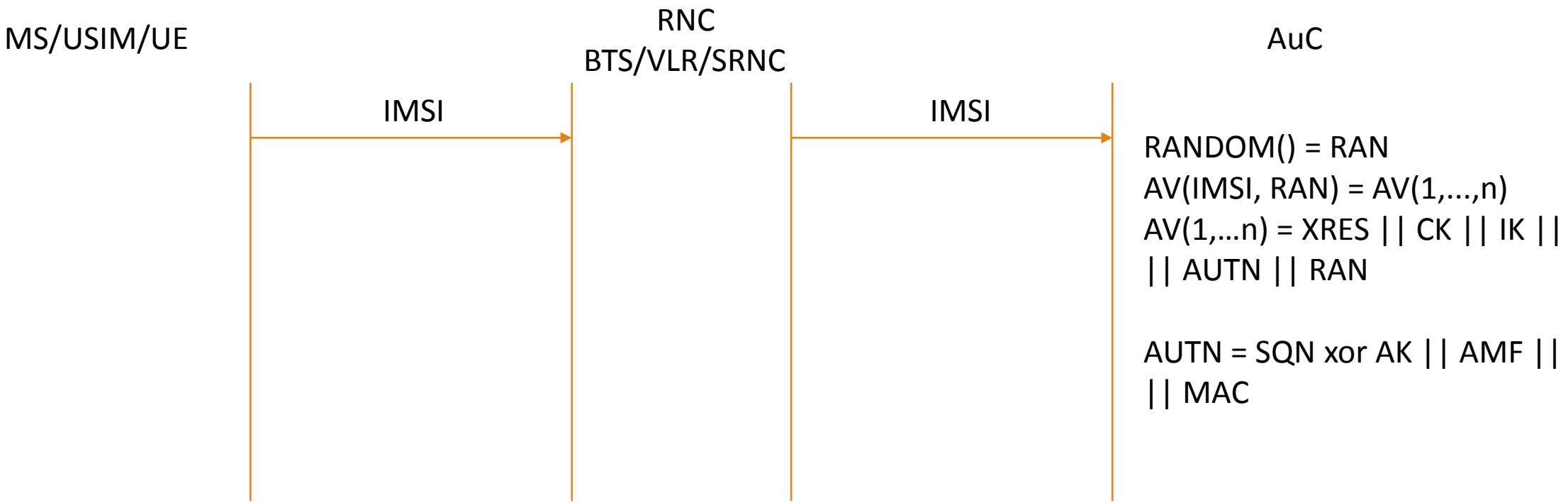
3G a LTE



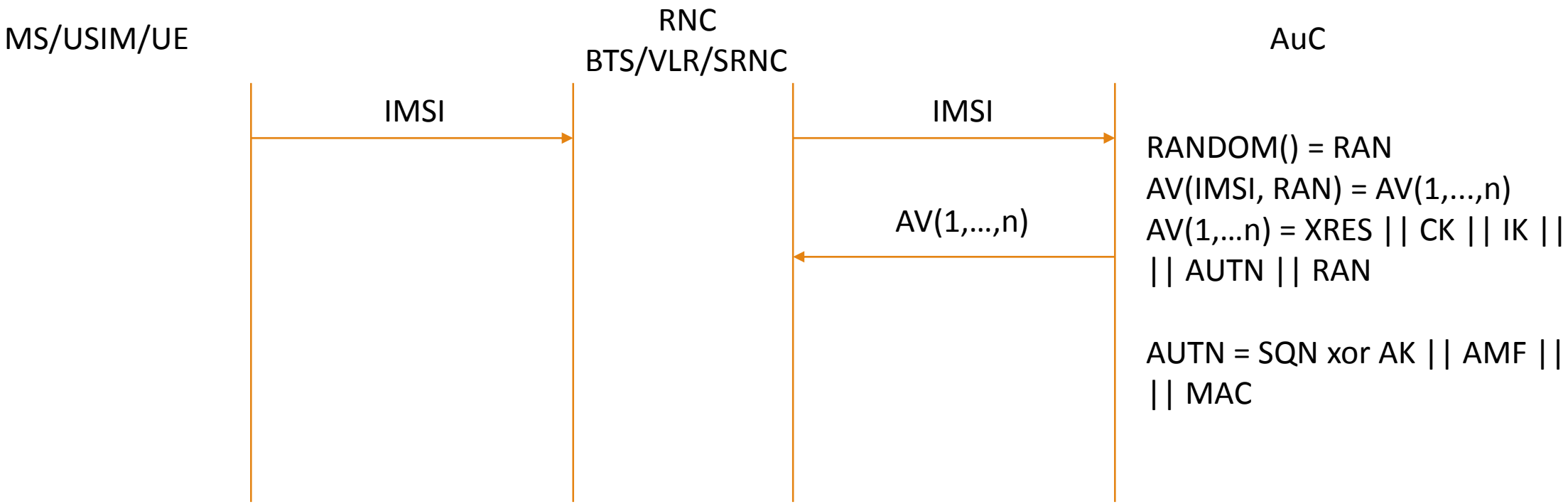
3G a LTE



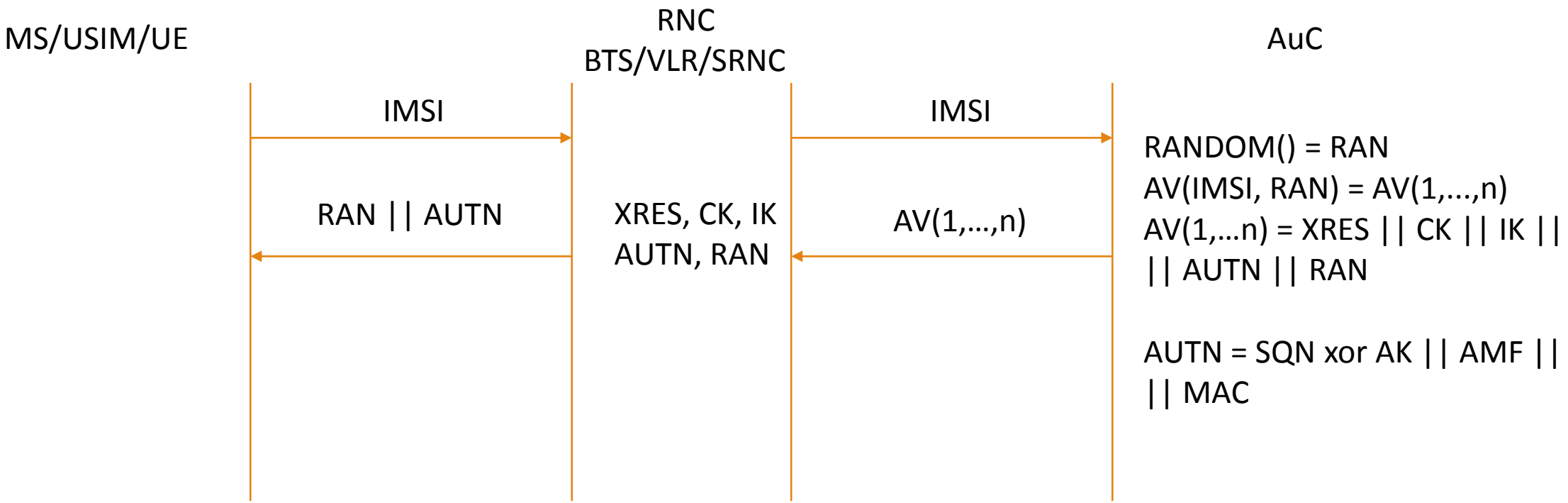
3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
AUTN = SQN xor AK || AMF ||
|| MAC

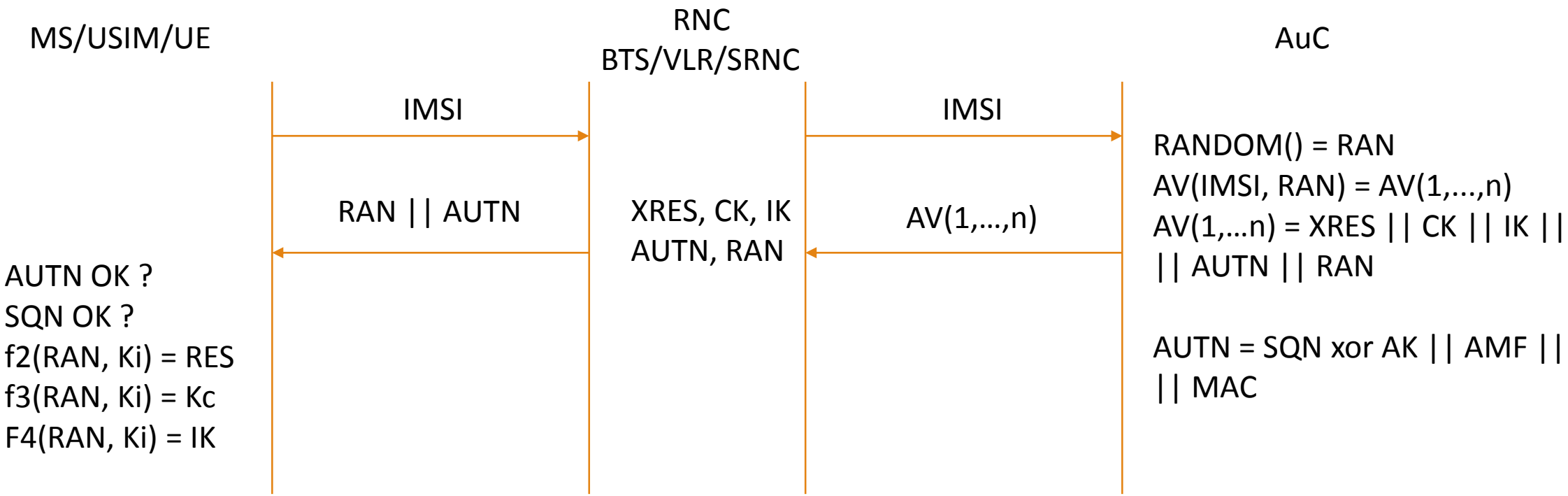
3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
AV(1,…,n)
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
AUTN = SQN xor AK || AMF ||
|| MAC

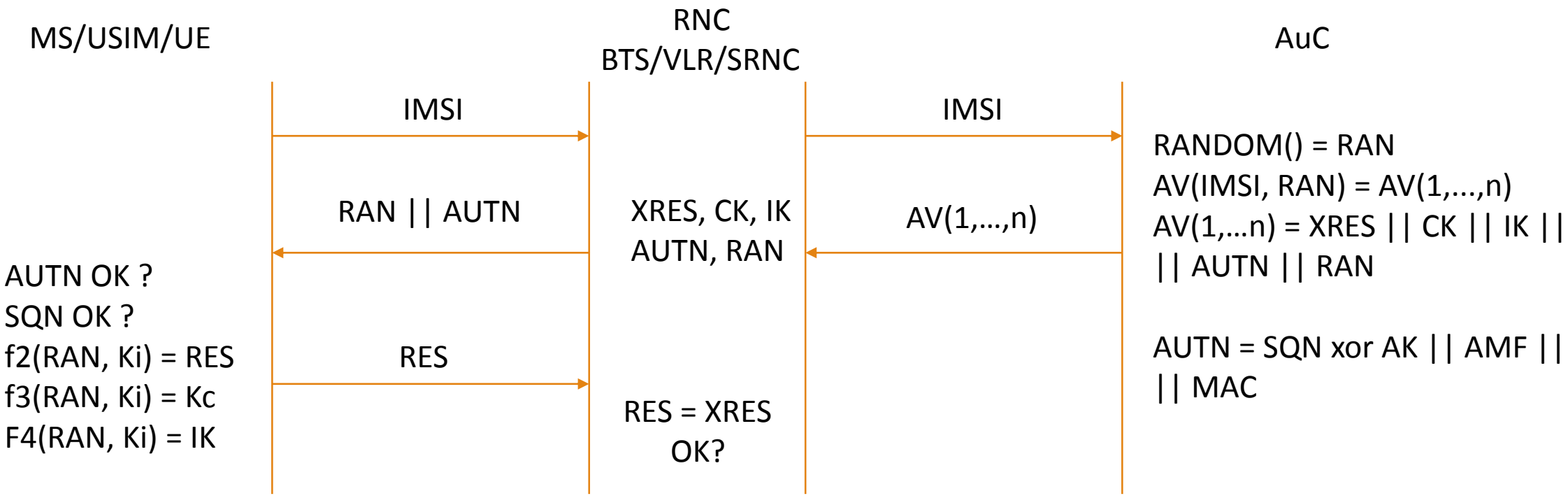
3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN = SQN xor AK || AMF ||
|| MAC

3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN OK ?
SQN OK ?
f2(RAN, Ki) = RES
f3(RAN, Ki) = Kc
F4(RAN, Ki) = IK
AUTN = SQN xor AK || AMF ||
|| MAC

3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN OK ?
SQN OK ?
f2(RAN, Ki) = RES
f3(RAN, Ki) = Kc
F4(RAN, Ki) = IK
RES
RES = XRES
OK?
AUTN = SQN xor AK || AMF ||
|| MAC

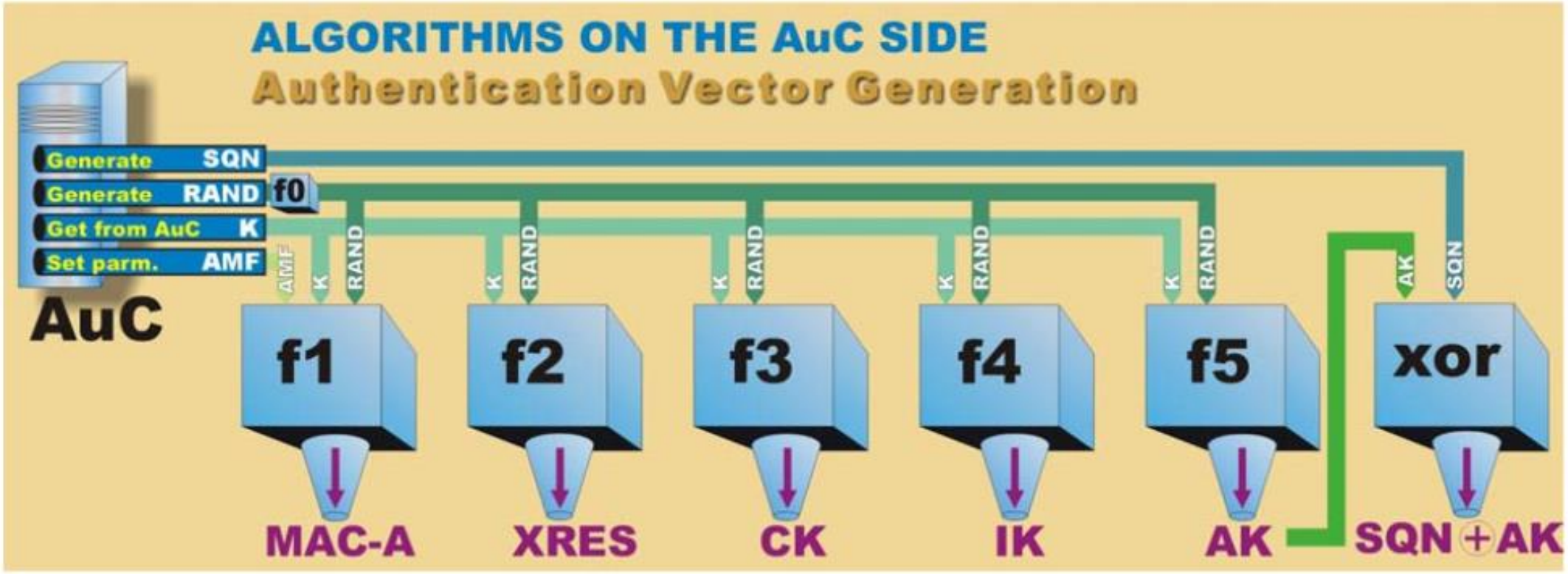
3G a LTE

Fukncia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	…	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na USIM – zdieľaný s AuC	Žiadny	USIM, AuC		128

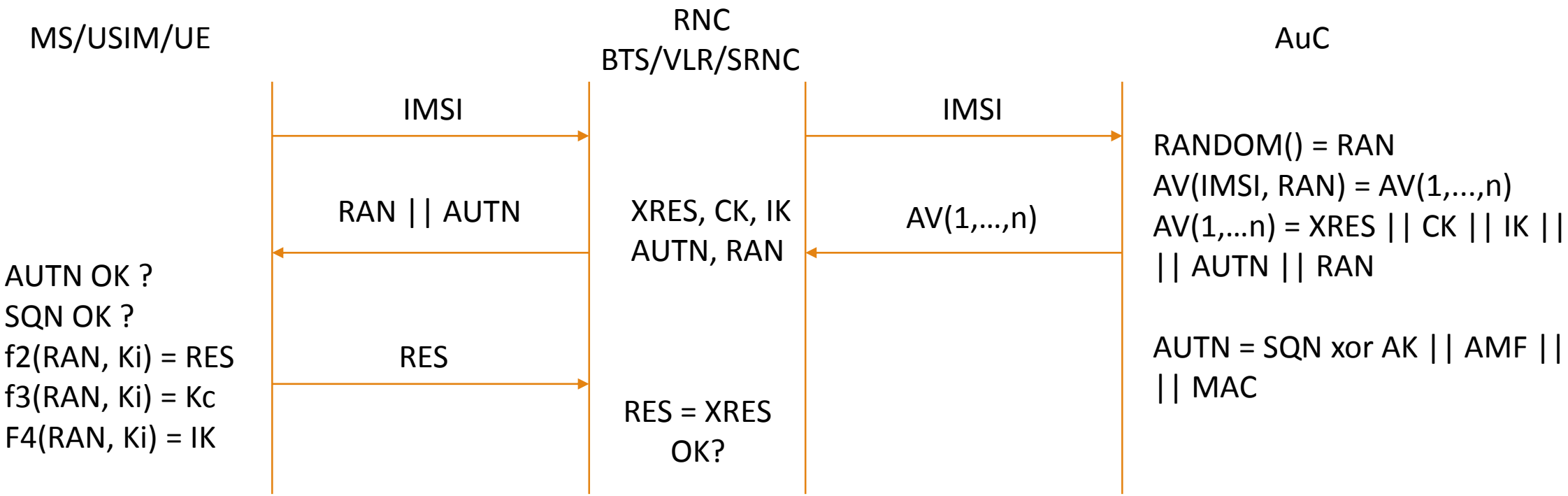
Algoritmy

- GSM:
  - ENC: A5/1 & A5/2
  - COMP128: A3 – 32 bit, A8 – 64 bit
    - Utajované
- 3G:
  - ENC: KASUMI (GEA0, GEA1) -> RNC CHOOSE ENC. -> MS
  - f9: Milenage
- 4G:
  - ENC: Snow 3G || AES 128b.
  - Možnosť dvojitého šifrovania

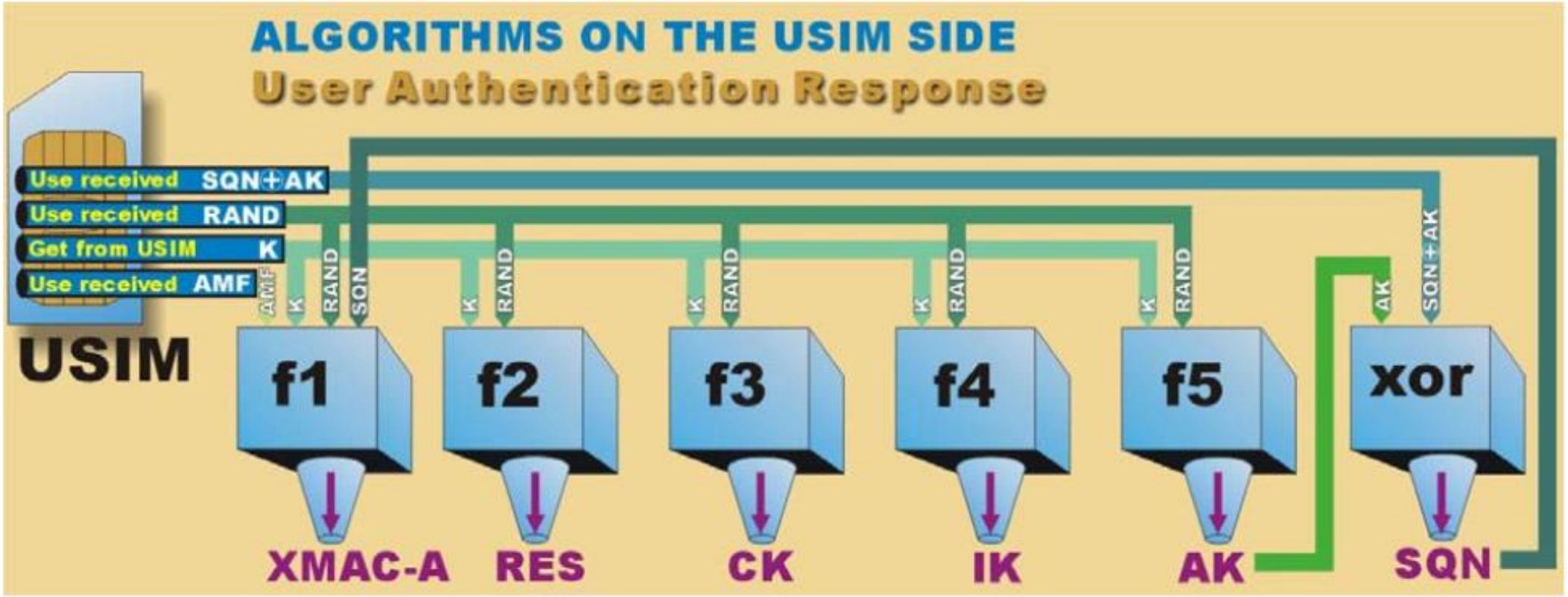
3G a LTE


ALGORITHMS ON THE AuC SIDE
Authentication Vector Generation
Generate SQN
Generate RAND
Get from AuC K
Set parm. AMF
AuC
f0
AMF
K
RAND
f1
f2
f3
f4
f5
xor
AK
SQN
MAC-A
XRES
CK
IK
AK
SQN + AK

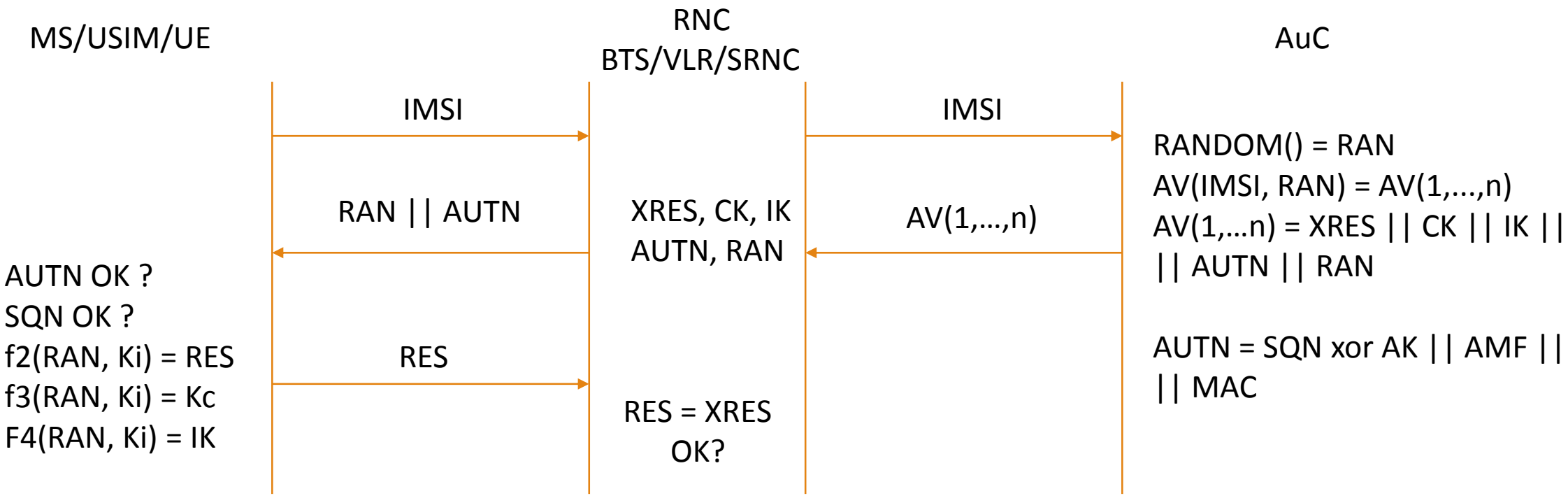
3G a LTE

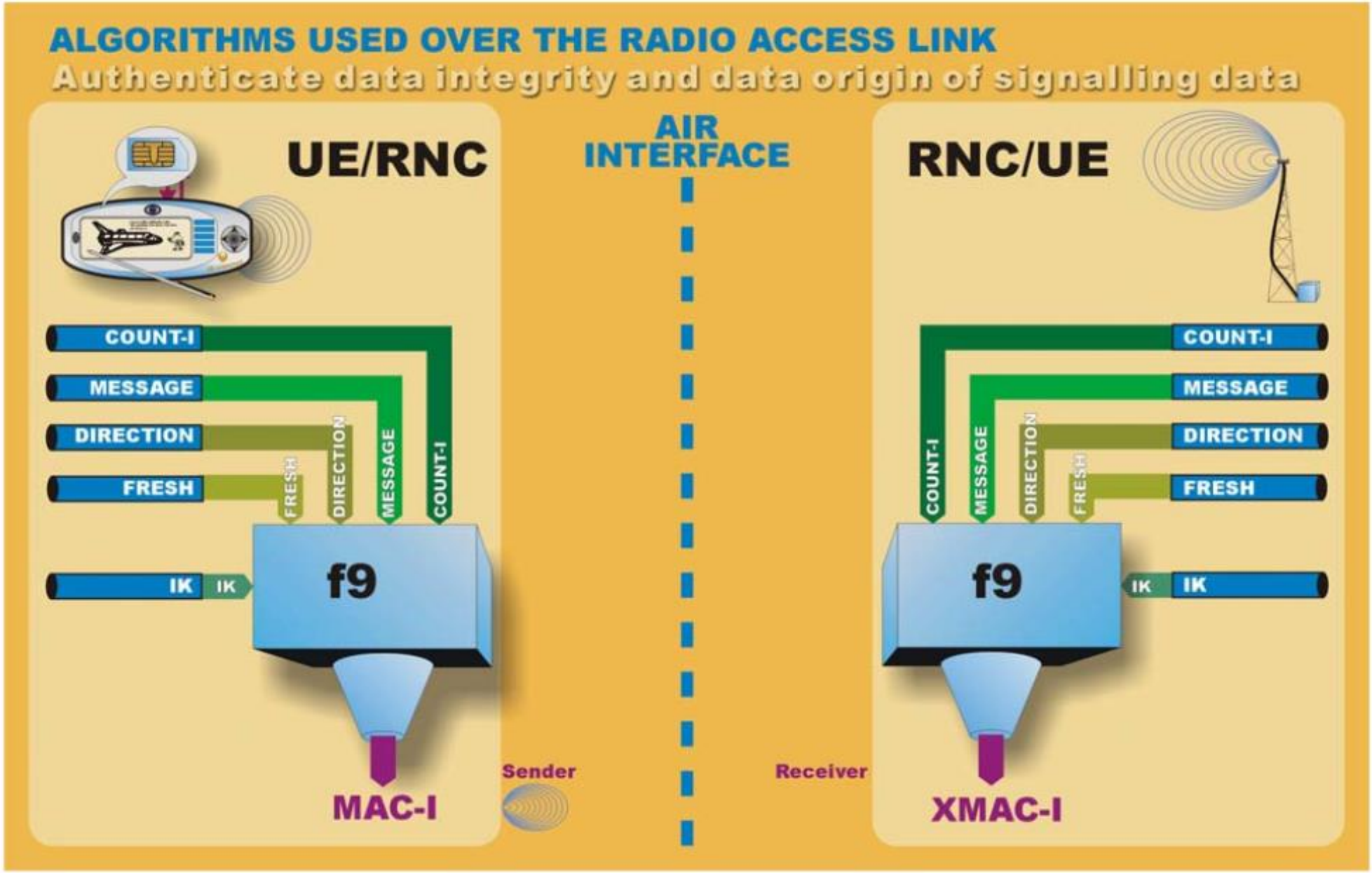

MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN OK ?
SQN OK ?
f2(RAN, Ki) = RES
f3(RAN, Ki) = Kc
F4(RAN, Ki) = IK
RES
RES = XRES
OK?
AUTN = SQN xor AK || AMF ||
|| MAC

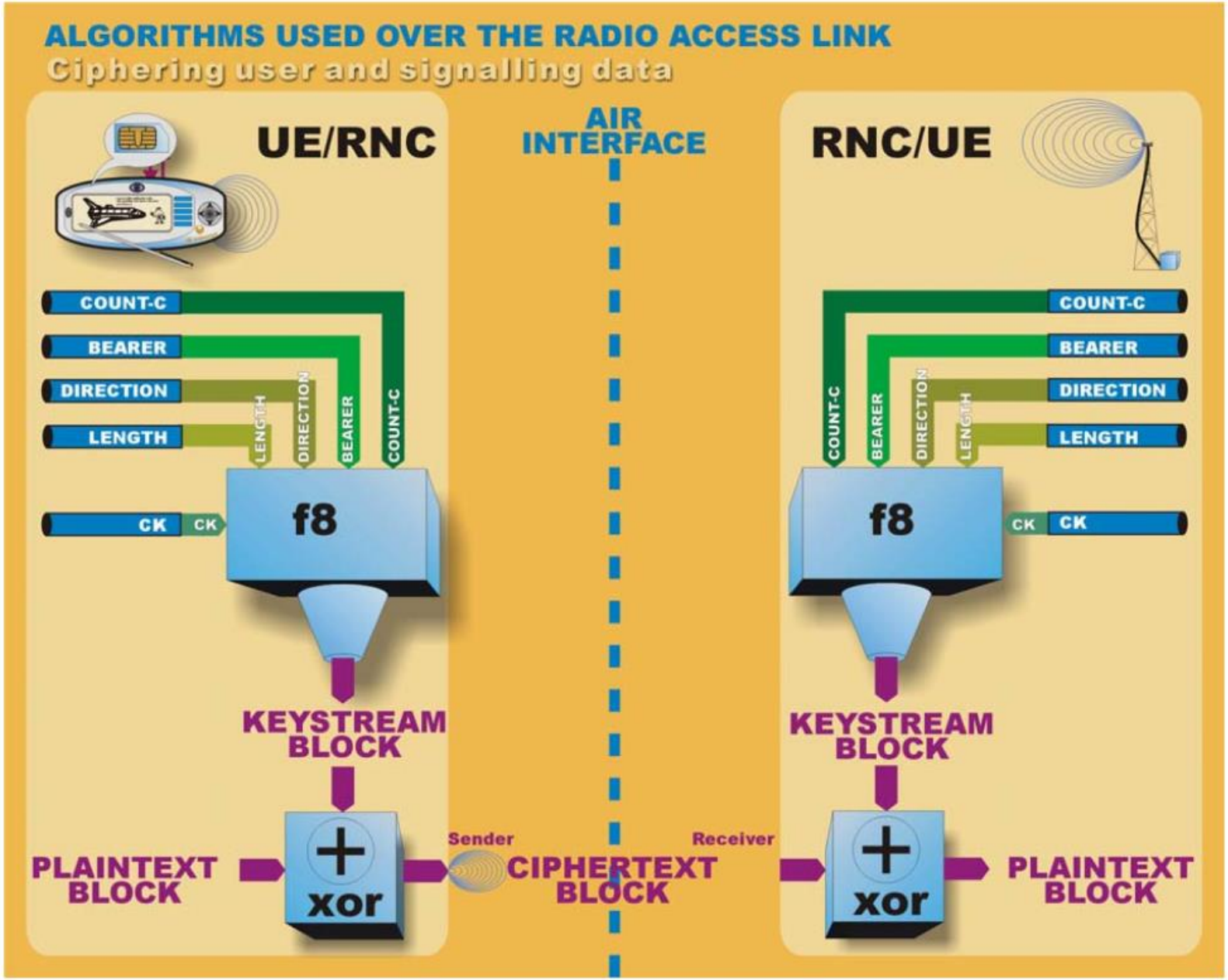
3G a LTE


ALGORITHMS ON THE USIM SIDE
User Authentication Response
Use received SQN⊕AK
Use received RAND
Get from USIM K
Use received AMF
USIM
AMF
K
RAND
SQN
f1
f2
f3
f4
f5
xor
AK
SQN⊕AK
XMAC-A
RES
CK
IK
AK
SQN

3G a LTE


MS/USIM/UE
RNC
BTS/VLR/SRNC
AuC
IMSI
IMSI
RANDOM() = RAN
AV(IMSI, RAN) = AV(1,...,n)
AV(1,…n) = XRES || CK || IK ||
|| AUTN || RAN
RAN || AUTN
XRES, CK, IK
AUTN, RAN
AV(1,…,n)
AUTN OK ?
SQN OK ?
f2(RAN, Ki) = RES
f3(RAN, Ki) = Kc
F4(RAN, Ki) = IK
RES
RES = XRES
OK?
AUTN = SQN xor AK || AMF ||
|| MAC


ALGORITHMS USED OVER THE RADIO ACCESS LINK
Authenticate data integrity and data origin of signalling data
UE/RNC
AIR INTERFACE
RNC/UE
COUNT-I
MESSAGE
DIRECTION
FRESH
IK
f9
MAC-I
Sender
Receiver
XMAC-I


ALGORITHMS USED OVER THE RADIO ACCESS LINK
Ciphering user and signalling data
UE/RNC
AIR INTERFACE
RNC/UE
COUNT-C
BEARER
DIRECTION
LENGTH
CK
f8
KEYSTREAM BLOCK
PLAINTEXT BLOCK
xor
Sender
CIPHERTEXT BLOCK
Receiver

Zdroje

https://brage.bibsys.no/xmlui/bitstream/handle/11250/137418/master_ikt_2001_dohmen.pdf?sequence=1

http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf

Pre 4G (LTE):

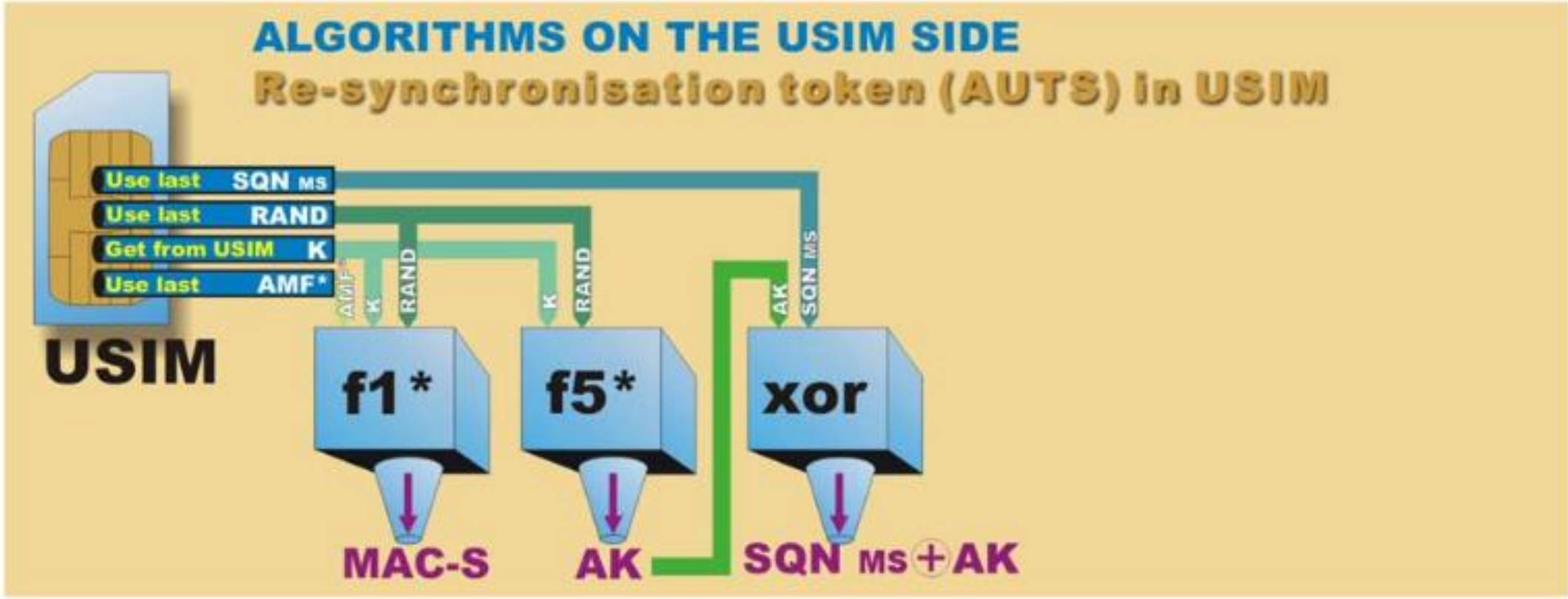
http://www.ijritcc.org/download/1430372773.pdf

Klonovanie (U)SIM kariet:

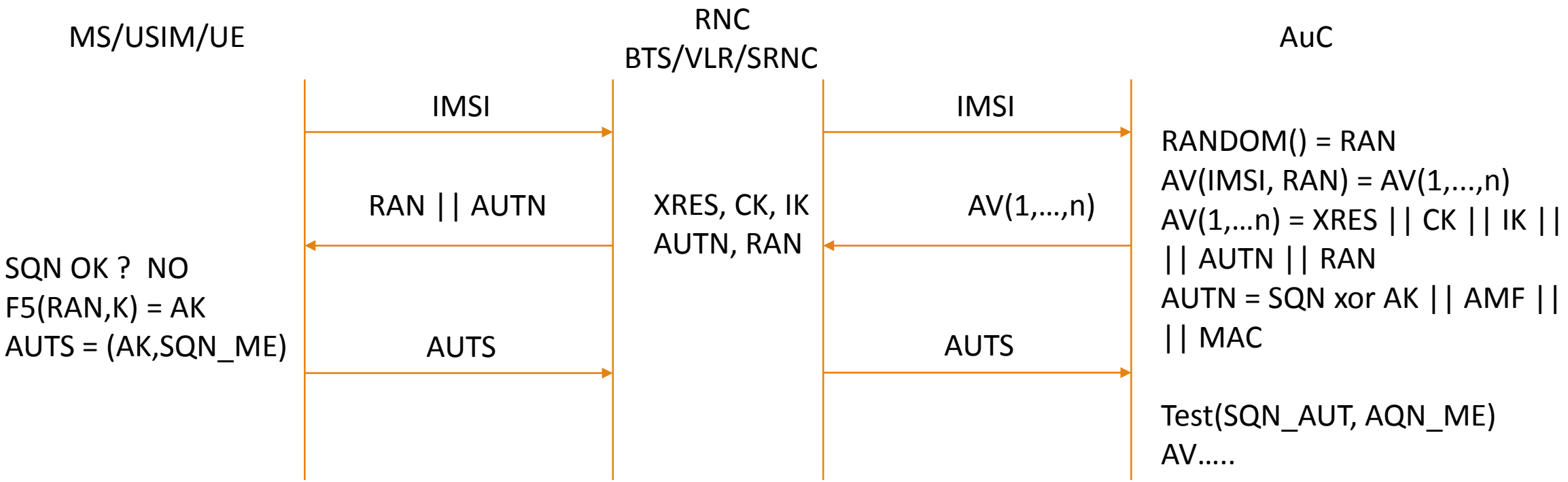
https://www.blackhat.com/docs/us-15/materials/us-15-Yu-Cloning-3G-4G-SIM-Cards-With-A-PC-And-An-Oscilloscope-Lessons-Learned-In-Physical-Security.pdf

Ďakujem za pozornosť.

Resynchronizácia



Resynchronizácia



Resynchronizácia