Mobile Communications

Security in 3GPP Networks

Manuel P. Ricardo

Faculdade de Engenharia da Universidade do Porto

- *How is authentication and ciphering handled in GSM?*
- *How is authentication and ciphering handled in UMTS?*

GSM

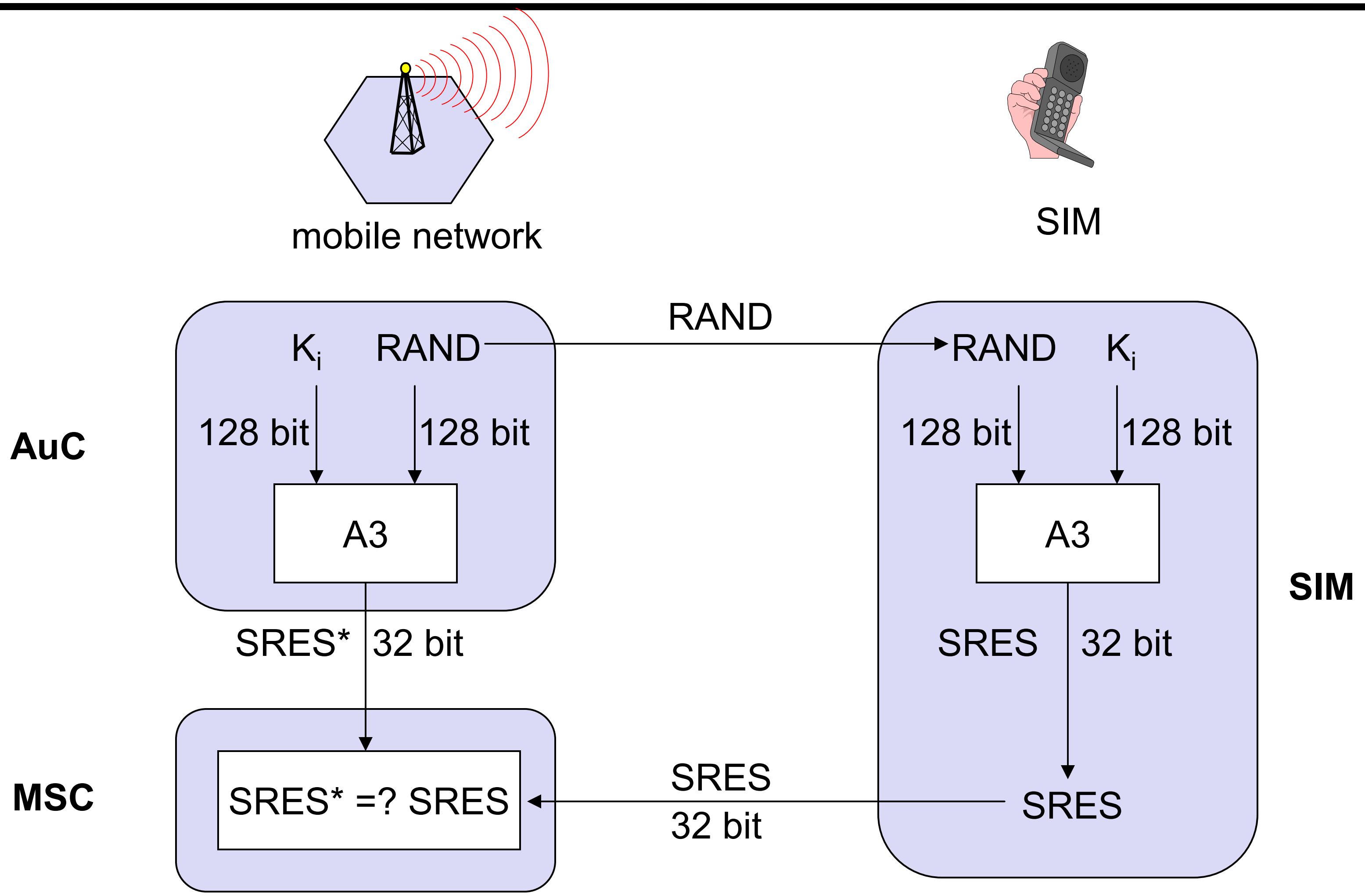
Security in GSM

- Security services
  - access control/authentication
    - user ➔ SIM (Subscriber Identity Module): secret PIN (Personal Identification Number)
    - SIM ➔ network: challenge - response method

      Ki - subscriber secret authentication key, stored in SIM
  - confidentiality

    voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - TMSI - Temporary Mobile Subscriber Identity
    - newly assigned at each new location update
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication (“secret”, open interface)
  - A5 for encryption (standardized)
  - A8 for encryption key generation (“secret”, open interface)

GSM - Authentication



mobile network

SIM

AuC

K_i RAND

128 bit 128 bit

A3

SRES* 32 bit

RAND

RAND K_i

128 bit 128 bit

A3

SRES 32 bit

SIM

MSC

SRES* =? SRES

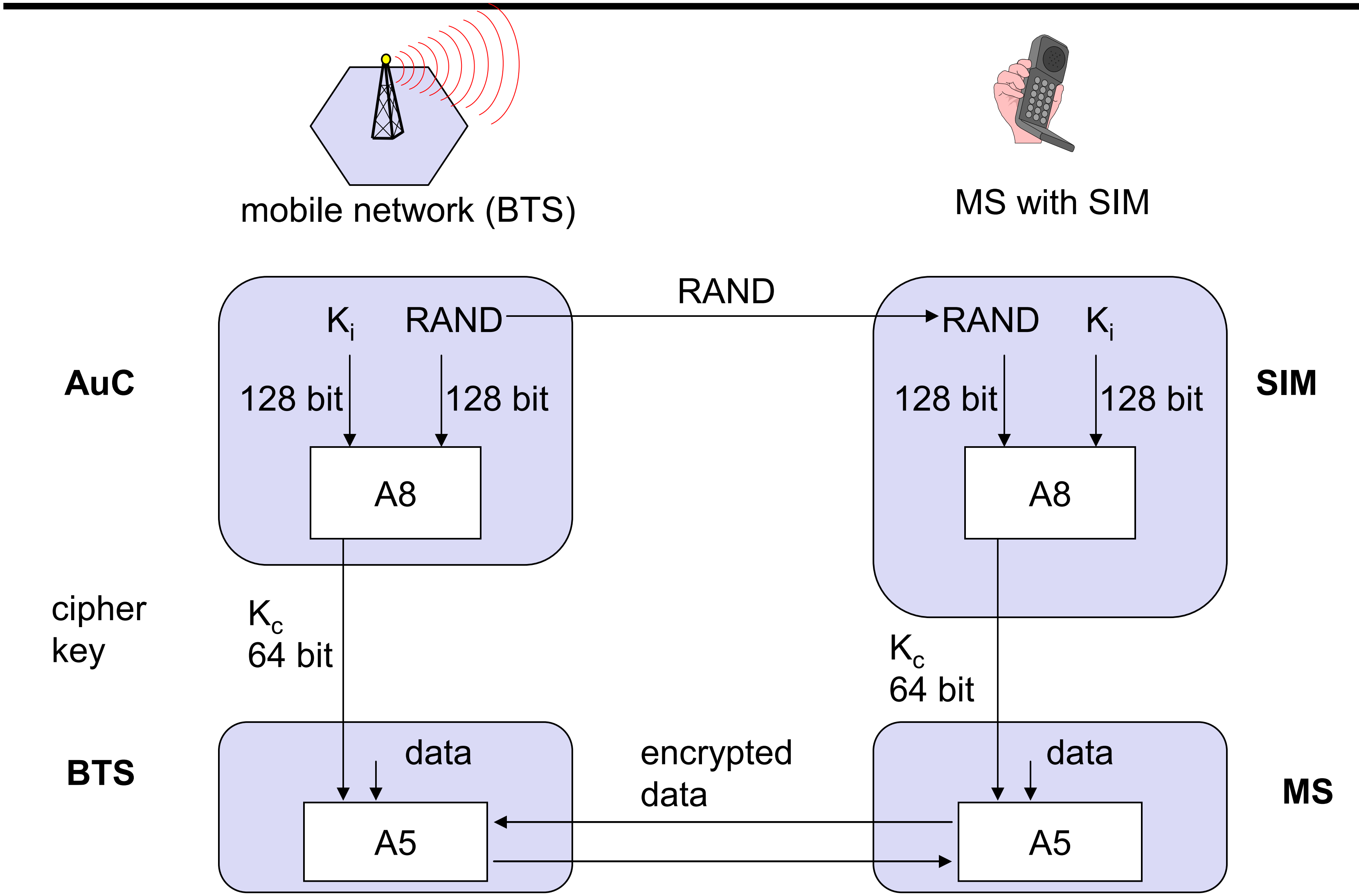
SRES

32 bit

SRES

K_i: individual subscriber authentication key SRES: signed response

GSM - Key Generation and Encryption



mobile network (BTS)

MS with SIM

AuC

K_i RAND

128 bit 128 bit

A8

RAND

RAND K_i

128 bit 128 bit

A8

SIM

cipher key

K_c 64 bit

K_c 64 bit

BTS

data

A5

encrypted data

data

A5

MS

3G

(3GPP TS 23.060, 3GPP TS 33.102)

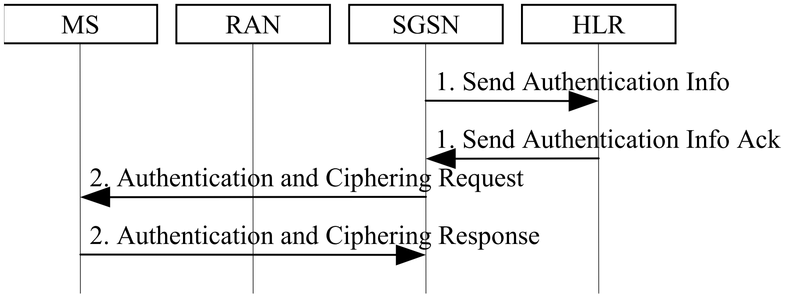
Security Function

- Authentication of the MS by the network
- Provides user identity confidentiality
  - temporary identification and ciphering
- Provides user data and signalling confidentiality
  - ciphering
- In UMTS (Iu mode)
  - authentication of the network by the MS
  - data integrity and origin authentication of signalling data

Authentication

- Two types of authentication
  - *UMTS authentication*
  - *GSM authentication*
  - Independent of the RAN modes
- GSM authentication
  - Based on SIM
  - Authentication of the MS by the network
  - Establishment of GSM ciphering key (Kc) between the SGSN and the MS
- UMTS authentication
  - Based on USIM
  - Requires authentication quintets
  - Implies mutual authentication
  - Agreement between SGSN and MS on
    ciphering key (CK) and integrity key (IK)

GSM Authentication


MS
RAN
SGSN
HLR
1. Send Authentication Info
1. Send Authentication Info Ack
2. Authentication and Ciphering Request
2. Authentication and Ciphering Response

1. SGSN requests Authentication-Info (IMSI); HLR responds
2. SGSN

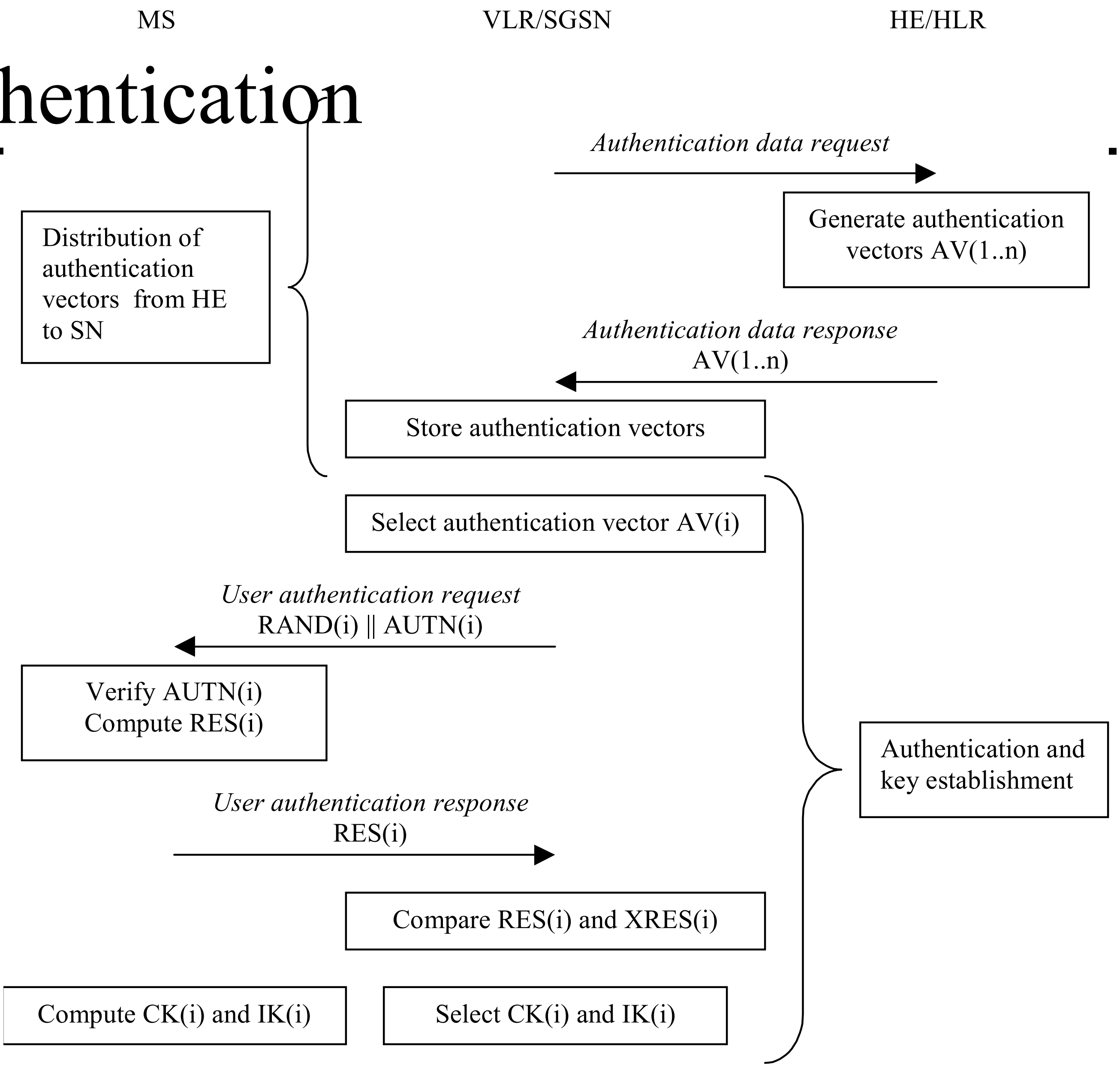
   sends Authentication-Ciphering(RAND, CKSN, Ciphering Algorithm);

   MS responds with Ciphering-Response (SRES)

   – A/Gb mode: MS starts ciphering after sending Response message

   – Iu mode: SGSN / MS shall generate CK and IK from the GSM Kc

UMTS Authentication



MS

VLR/SGSN

HE/HLR

Authentication data request

Generate authentication vectors AV(1..n)

Distribution of authentication vectors from HE to SN

Authentication data response
AV(1..n)

Store authentication vectors

Select authentication vector AV(i)

User authentication request
RAND(i) || AUTN(i)

Verify AUTN(i)
Compute RES(i)

Authentication and key establishment

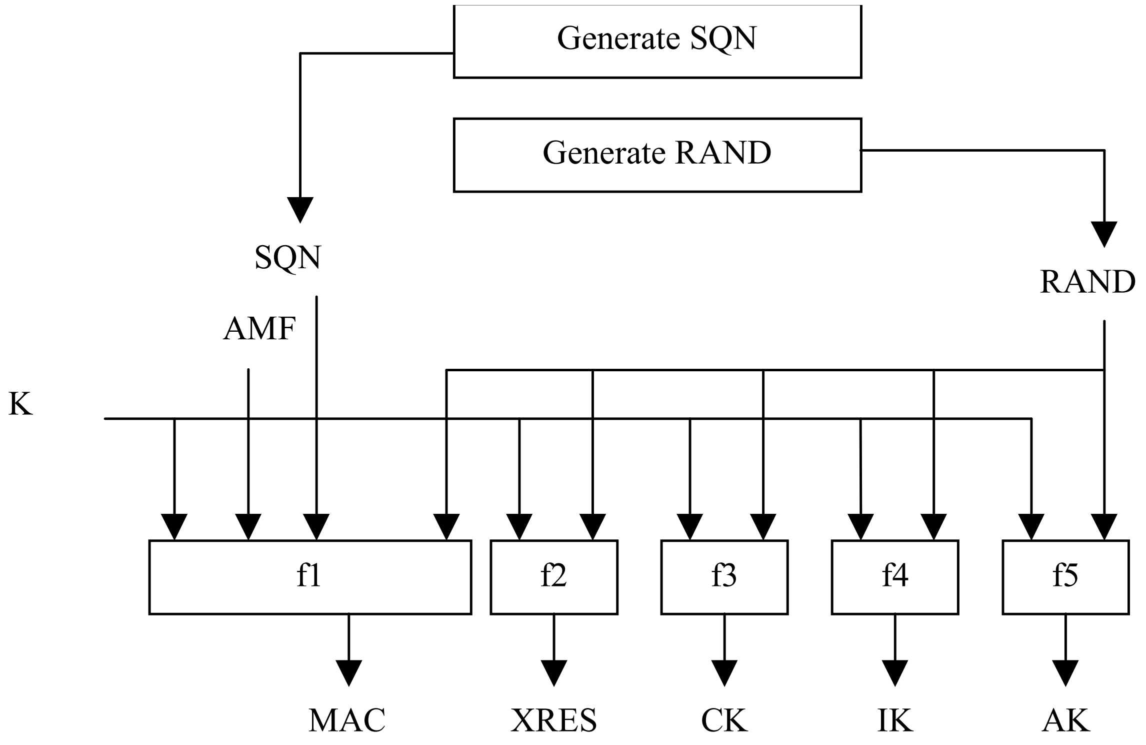
User authentication response
RES(i)

Compare RES(i) and XRES(i)

Compute CK(i) and IK(i)

Select CK(i) and IK(i)

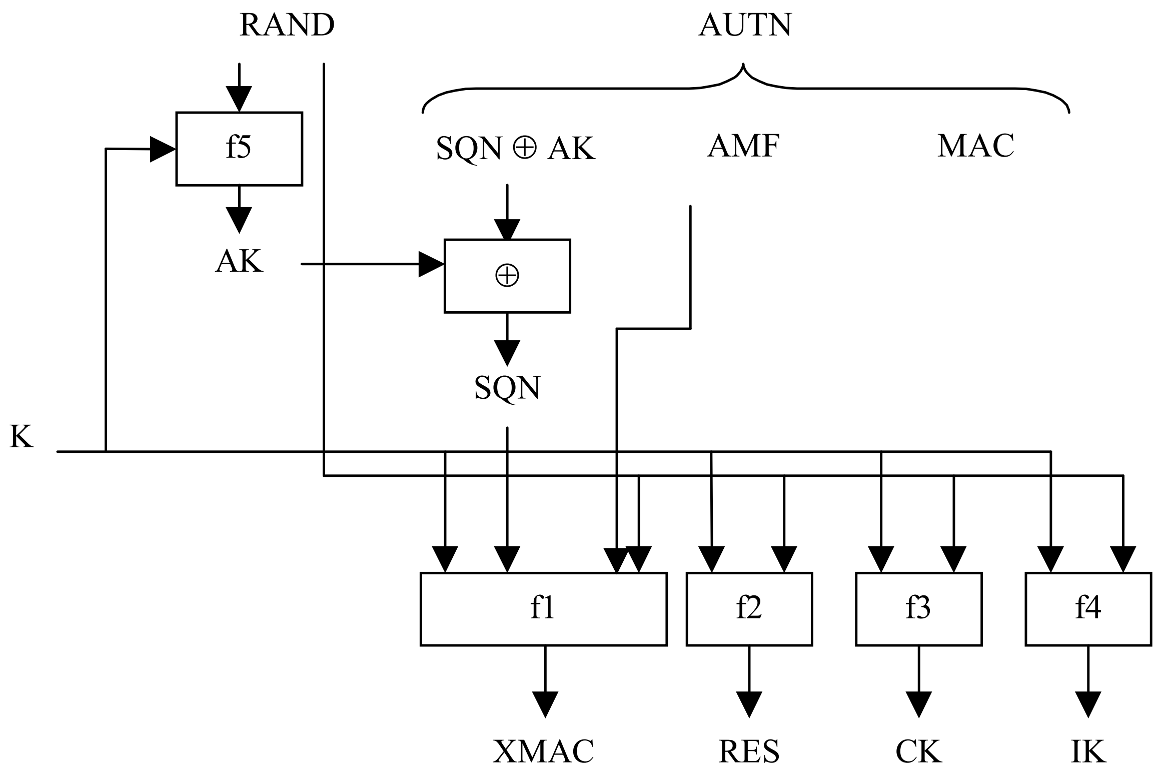
Generation of an Authentication Vector by HE/AuC



AUTN := SQN ⊕ AK || AMF || MAC

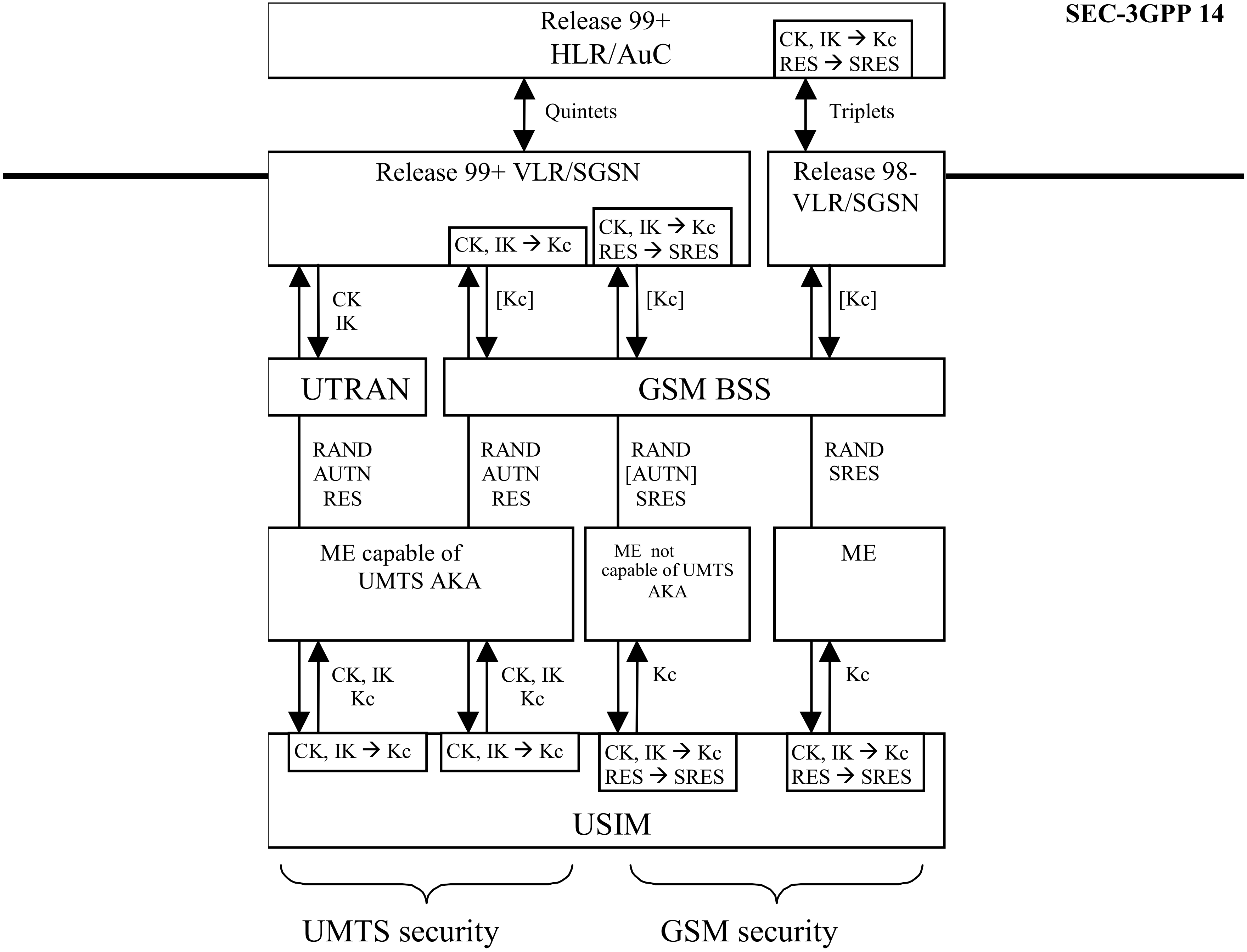
AV := RAND || XRES || CK || IK || AUTN

User authentication function in the USIM



Verify MAC = XMAC

Verify that SQN is in the correct range



Release 99+ HLR/AuC

CK, IK → Kc
RES → SRES

Quintets

Triplets

Release 99+ VLR/SGSN

CK, IK → Kc

CK, IK → Kc
RES → SRES

Release 98- VLR/SGSN

CK
IK

[Kc]

[Kc]

[Kc]

UTRAN

GSM BSS

RAND
AUTN
RES

RAND
AUTN
RES

RAND
[AUTN]
SRES

RAND
SRES

ME capable of UMTS AKA

ME not capable of UMTS AKA

ME

CK, IK
Kc

CK, IK
Kc

Kc

Kc

CK, IK → Kc

CK, IK → Kc

CK, IK → Kc
RES → SRES

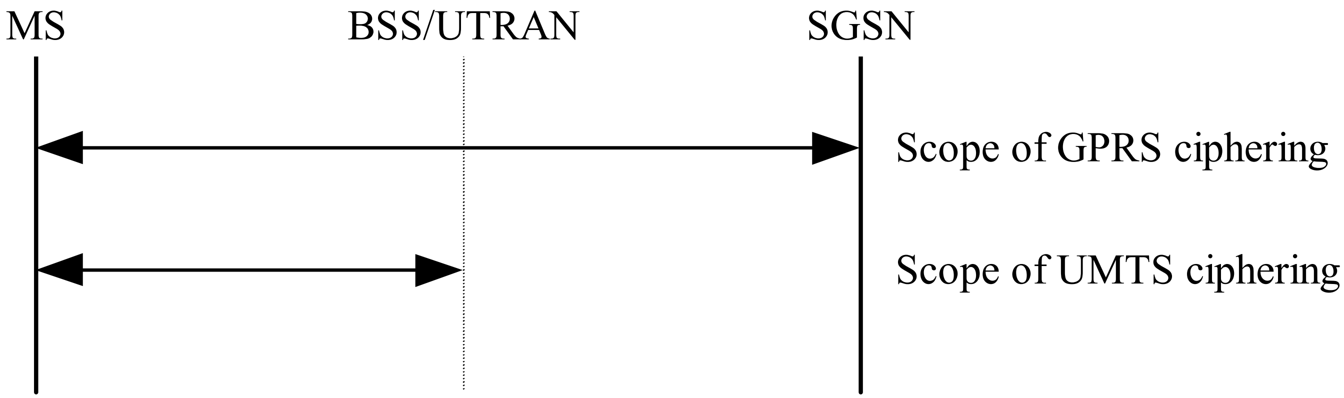
CK, IK → Kc
RES → SRES

USIM

UMTS security

GSM security

Scope of Ciphering



Ciphering Algorithm

- A/Gb mode: GPRS Encryption Algorithm (GEA)
  - Kc is an input to the algorithm
- Iu mode: UMTS Encryption Algorithm (UEA)
  - CK is an input to the algorithm.