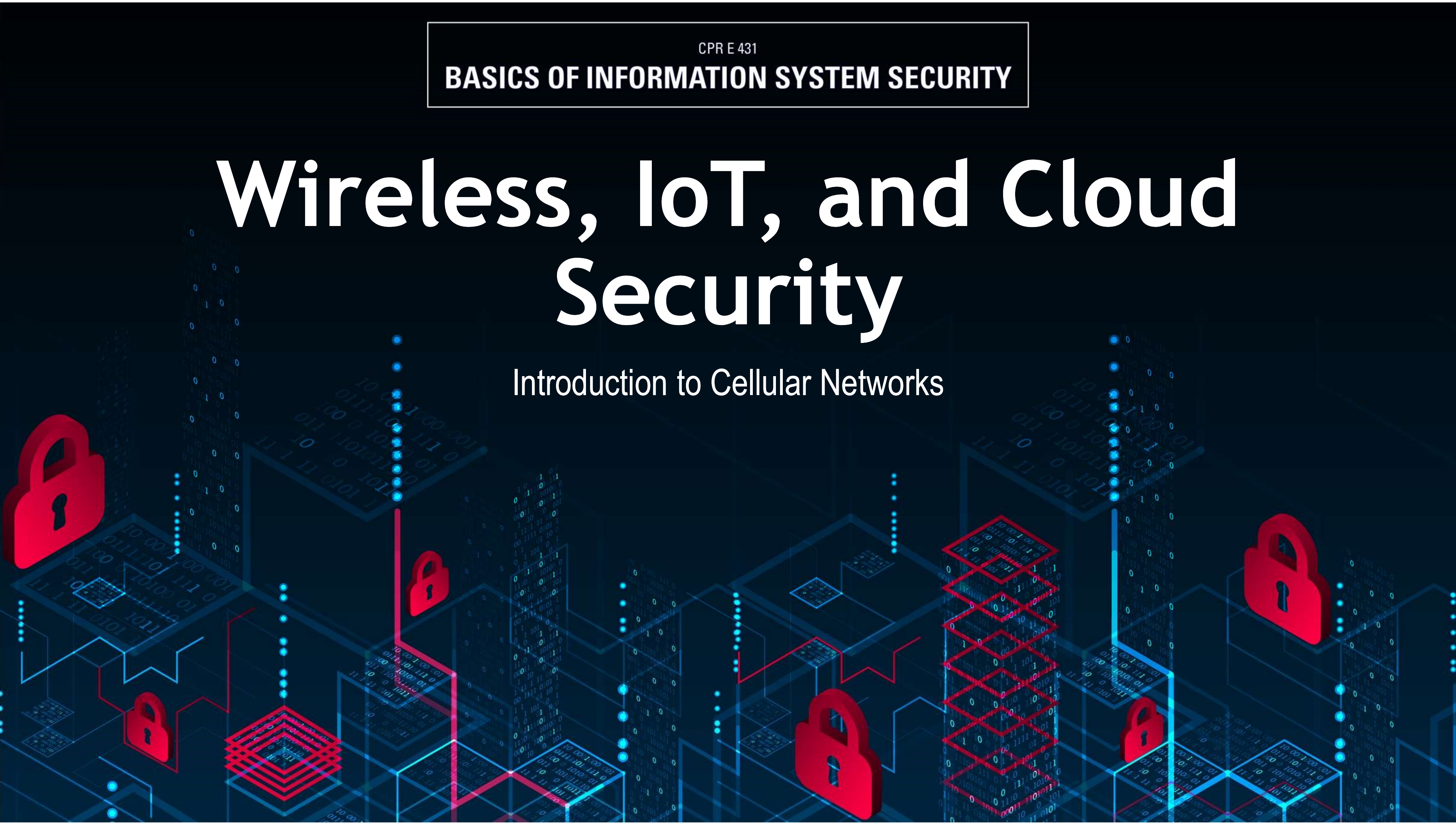
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

Introduction to Cellular Networks

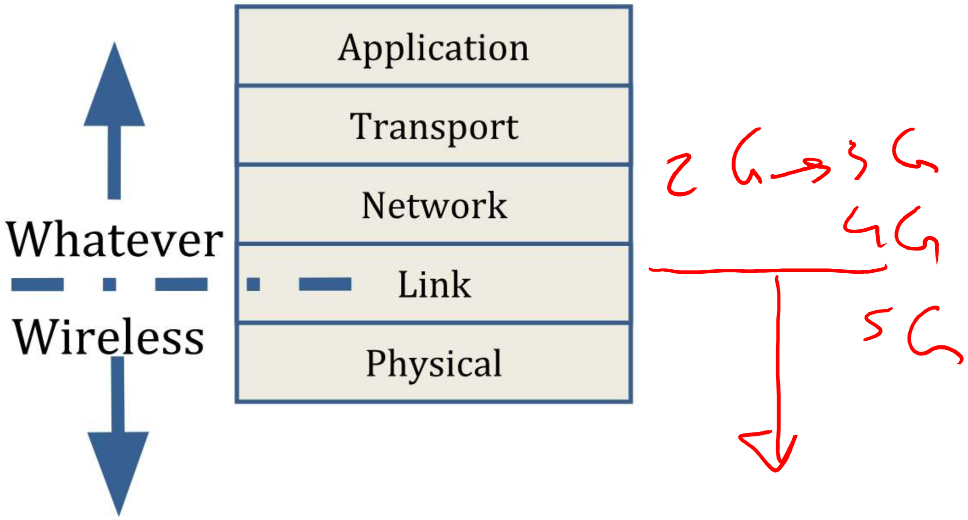


Video summary

- Layering in Wireless Networks
- What is IMTS? 3G?
- 3G Security Principles
- 3G Network Access Security
- 4G LTE Network

Layering in Wireless Networks

- Below a certain point, things can be designed for wireless communication
- Above that point, the medium doesn't matter…
  - Or does it?
  - Or should it?



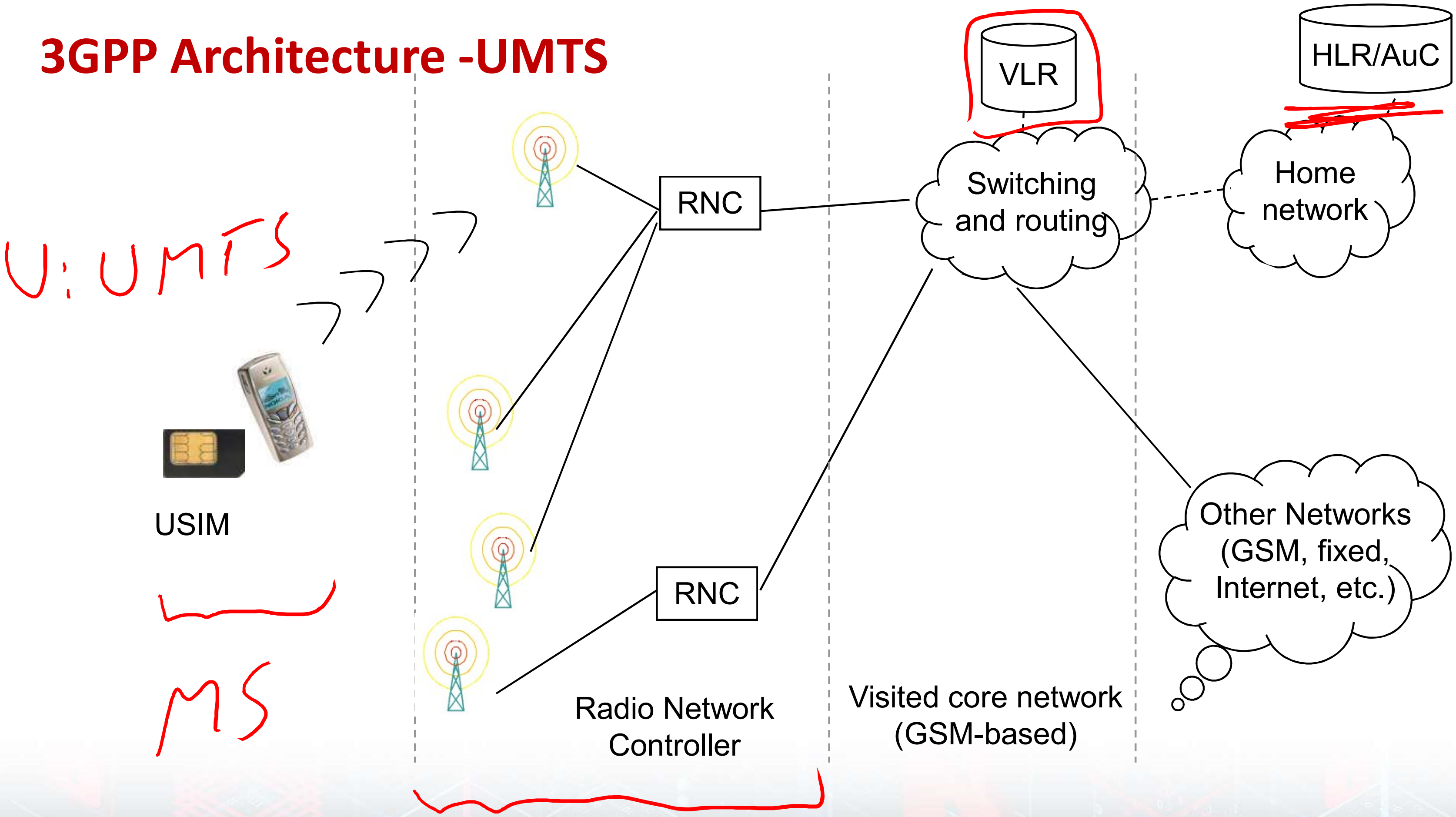
Universal Mobile Telecommunications Service (UMTS) 3G

UMTS is a 3G broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps).

3.5

UMTS specifies a complete network system, which includes the radio access network (UMTS Terrestrial Radio Access Network, or UTRAN), the core network and the authentication of users via SIM cards.

3GPP Architecture -UMTS



3G Security Principles

- Reuse of 2G (GSM) Security principales:
  - Removable hardware security module, SIM based Authentication
    - In GSM: SIM card
    - In 3GPP: USIM (User Services Identity Module)
  - Radio interface encryption
  - Protection of the identity of the end user (especially on the radio interface)

3GPP Security Principles (Cont.)

- Correction of the weaknesses of 2G:
  - 1 Possible attacks from a fake base station ➔ Mutual Authentication
  - 2 Data integrity not provided ➔Integrity protection of signalling message
  - Weak encryption (short key) ➔ Use of stronger encryption
  - Assurance that authentication information and keys are not being re-used ➔key freshness

Network Access Security

- **User identity confidentiality**
  - User identity confidentiality (GSM)
  - User location confidentiality
  - User intractability

- **Entity authentication**
  - User authentication (GSM)
  - Network authentication

- **Confidentiality**
  - Cipher Alg. agreement →
  - Cipher key agreement
  - Confidentiality of user data

- **Data Integrity**
  - Integrity Alg. agreement
  - Integrity key agreement
  - Data integrity and origin authentication of signaling data

GSM

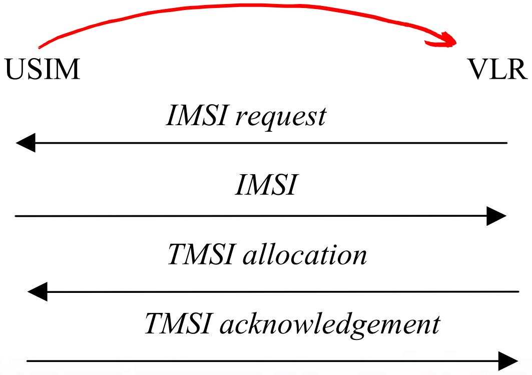
✗

User Identity Confidentiality

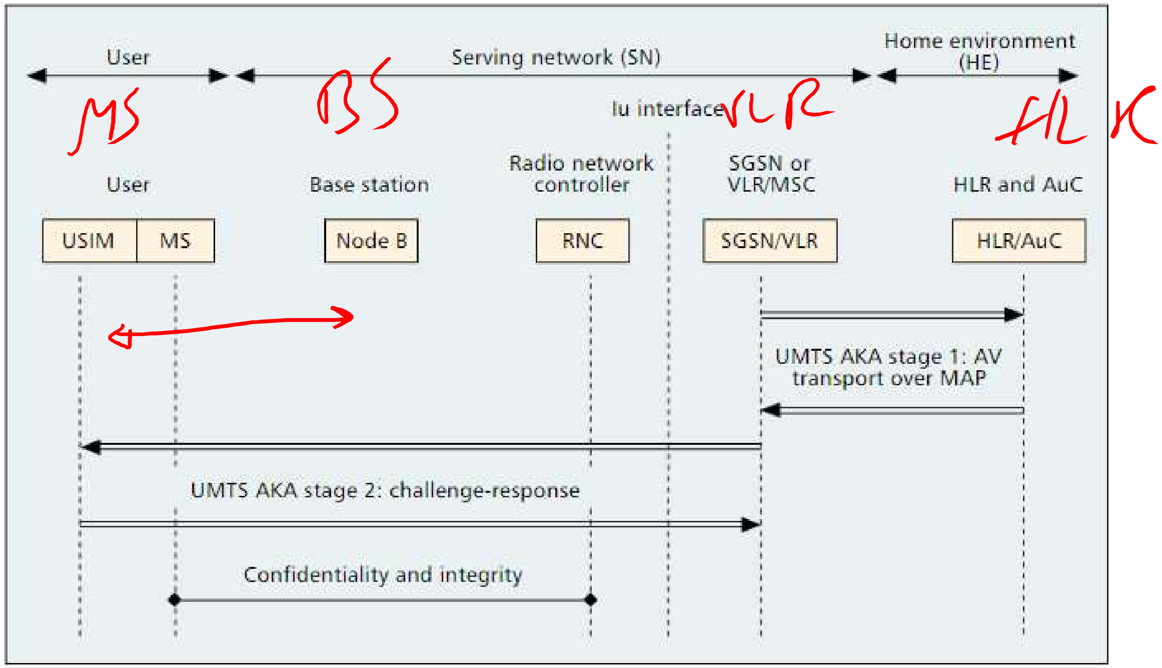
- Permanent user identity IMSI, user location, and user services cannot be determined by eavesdropping

- Achieved by use of temporary identity (TMSI) which is assigned by VLR

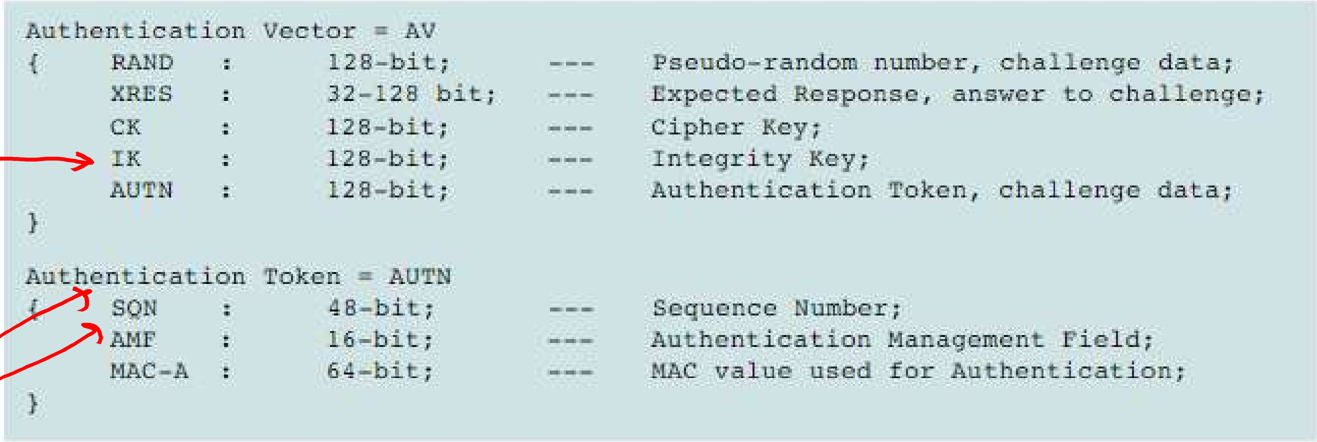
- IMSI is sent in clear text when establishing TMSI



Basic Access Security Services



UMTS Security Abbreviations

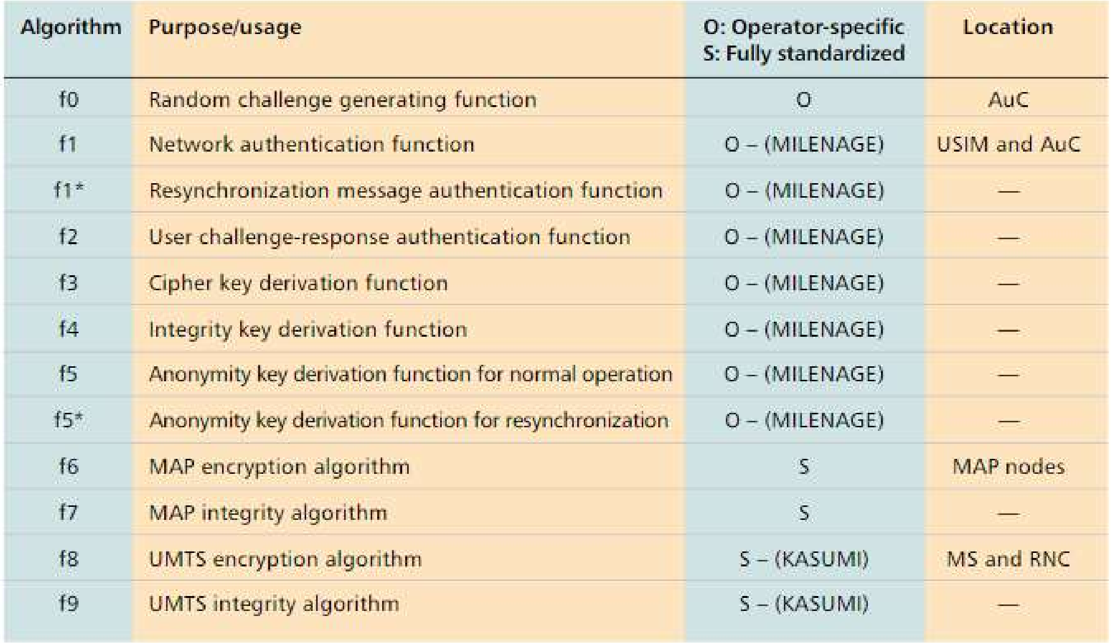


```
Authentication Vector = AV
{     RAND   :      128-bit;       ---    Pseudo-random number, challenge data;
      XRES   :      32-128 bit;    ---    Expected Response, answer to challenge;
      CK     :      128-bit;       ---    Cipher Key;
      IK     :      128-bit;       ---    Integrity Key;
      AUTN   :      128-bit;       ---    Authentication Token, challenge data;
}

Authentication Token = AUTN
{     SQN    :      48-bit;        ---    Sequence Number;
      AMF    :      16-bit;        ---    Authentication Management Field;
      MAC-A  :      64-bit;        ---    MAC value used for Authentication;
}
```

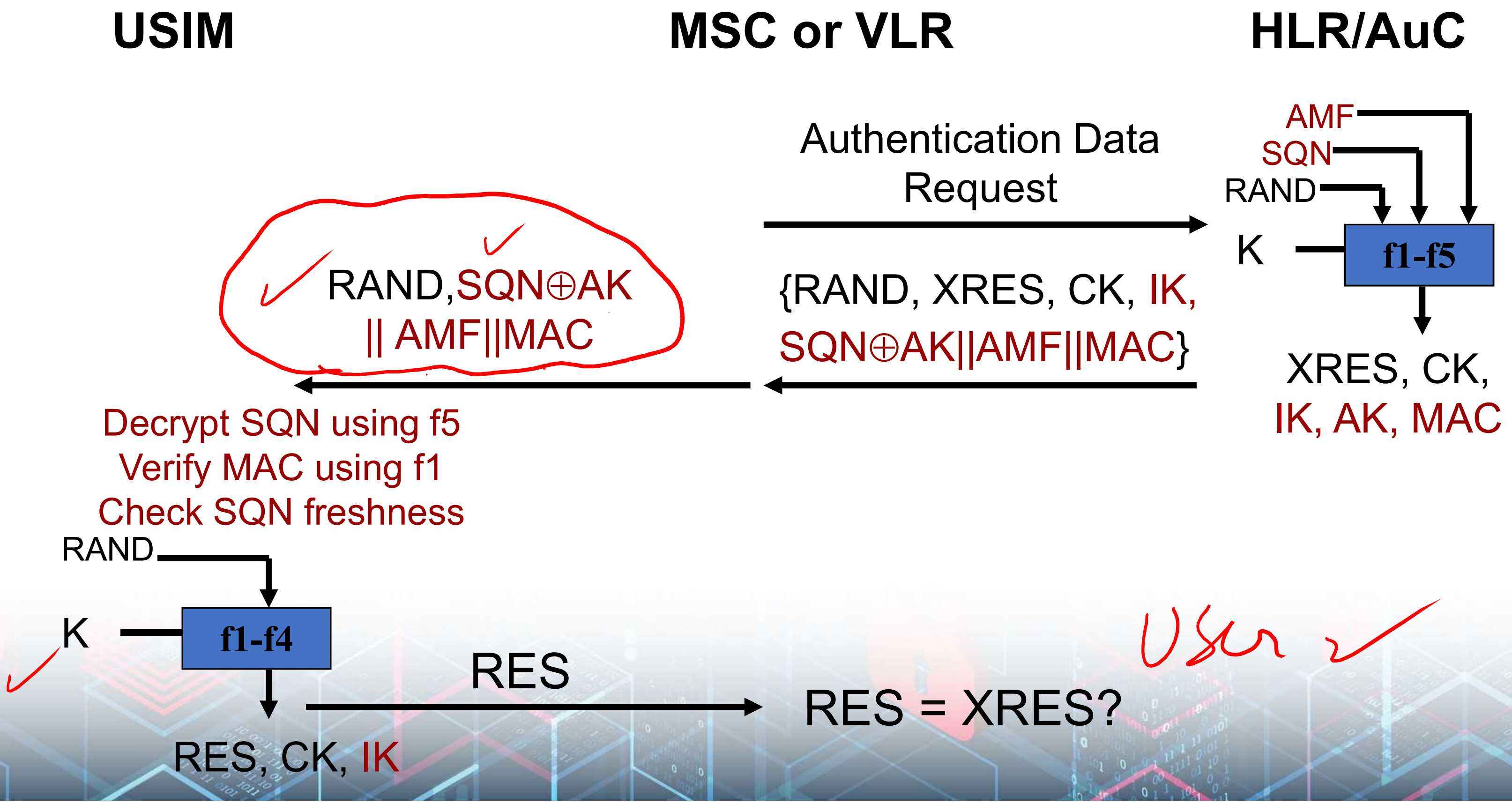
AK: Anonymity key

UMTS Security Algorithms



Algorithm	Purpose/usage	O: Operator-specific S: Fully standardized	Location
f0	Random challenge generating function	O	AuC
f1	Network authentication function	O – (MILENAGE)	USIM and AuC
f1*	Resynchronization message authentication function	O – (MILENAGE)	—
f2	User challenge-response authentication function	O – (MILENAGE)	—
f3	Cipher key derivation function	O – (MILENAGE)	—
f4	Integrity key derivation function	O – (MILENAGE)	—
f5	Anonymity key derivation function for normal operation	O – (MILENAGE)	—
f5*	Anonymity key derivation function for resynchronization	O – (MILENAGE)	—
f6	MAP encryption algorithm	S	MAP nodes
f7	MAP integrity algorithm	S	—
f8	UMTS encryption algorithm	S – (KASUMI)	MS and RNC
f9	UMTS integrity algorithm	S – (KASUMI)	—

UMTS Authentication



USIM

MSC or VLR

HLR/AuC

Authentication Data Request

AMF

SQN

RAND

K

f1-f5

XRES, CK, IK, AK, MAC

{RAND, XRES, CK, IK, SQN⊕AK||AMF||MAC}

RAND,SQN⊕AK || AMF||MAC

Decrypt SQN using f5
Verify MAC using f1
Check SQN freshness

RAND

K

f1-f4

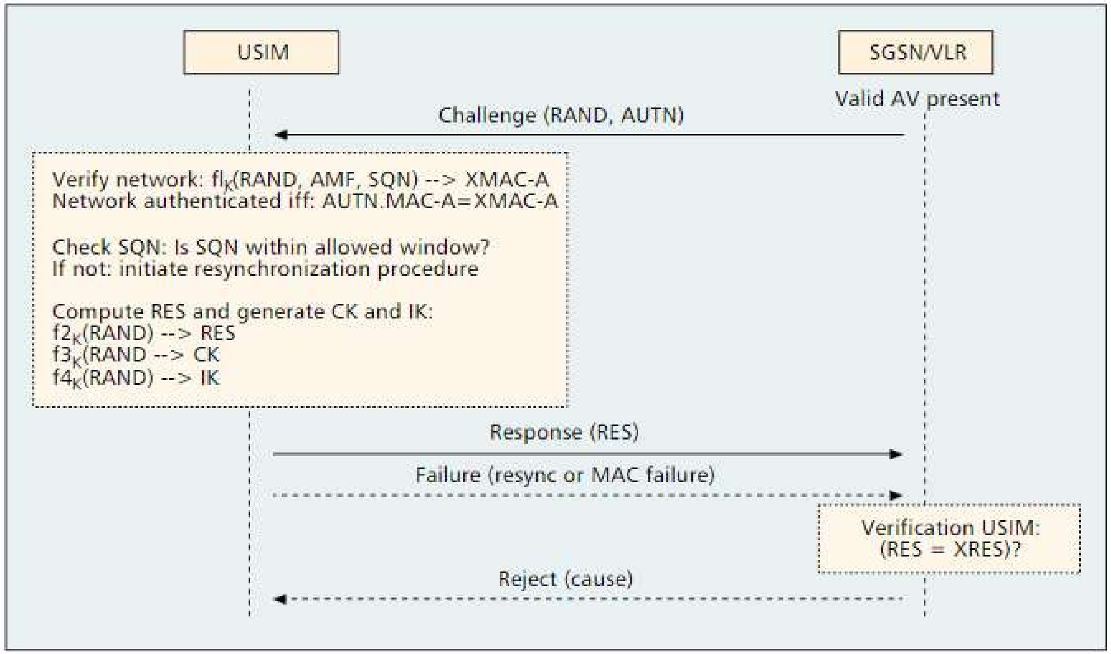
RES, CK, IK

RES

RES = XRES?

User ✓

UMTS Authentication



Verify network: fl_K(RAND, AMF, SQN) --> XMAC-A
Network authenticated iff: AUTN.MAC-A=XMAC-A

Check SQN: Is SQN within allowed window?
If not: initiate resynchronization procedure

Compute RES and generate CK and IK:
$f2_K$(RAND) --> RES
$f3_K$(RAND --> CK
$f4_K$(RAND) --> IK

Verification USIM:
(RES = XRES)?

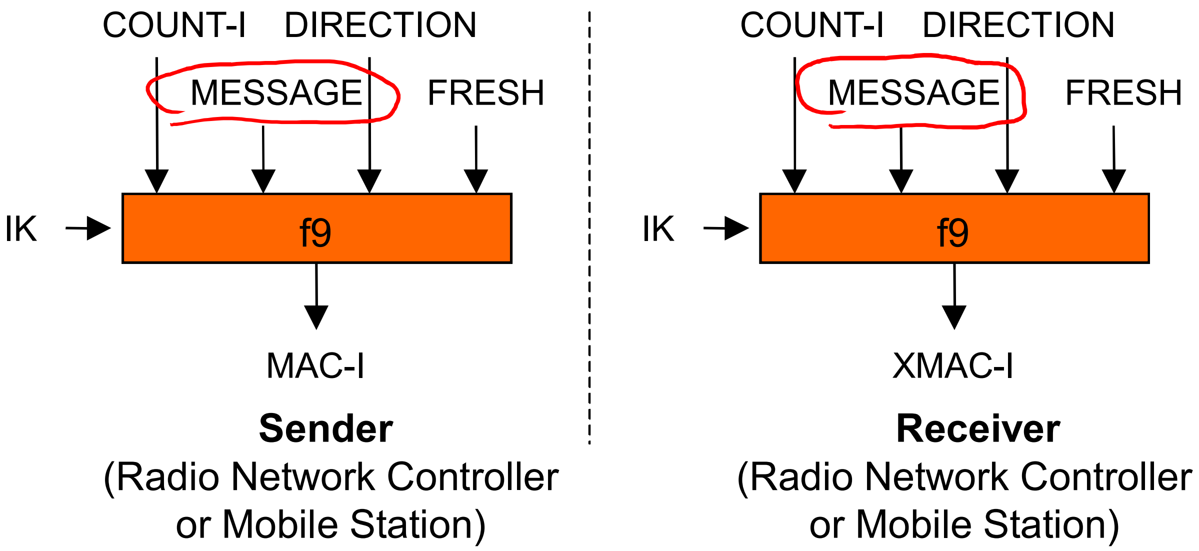
Mutual Authentication in 3G

- Subscriber can authenticate the network by the secret K using f1(K, SQN, AMF, RAND)

- SQN is introduced to prevent replay attacks

- Cipher Key and Integrity Key are generated after the authentication (Key Agreement)

Data Integrity in 3GPP



FRESH: Connection Nonce
COUNT-I: Integrity Sequence Number

Fresh: One value per user throughout the duration of a single connection. It is to protect the network against replay of signaling messages by the user.

Problems with 3G Security

- IMSI is sent in clear text when allocating TMSI to the user

- Hijacking outgoing/incoming calls in networks with disabled encryption is possible. The intruder poses as a man-in-the-middle and drops the user once the call is set-up

Long Term Evolution 4G

- Long Term Evolution (LTE)

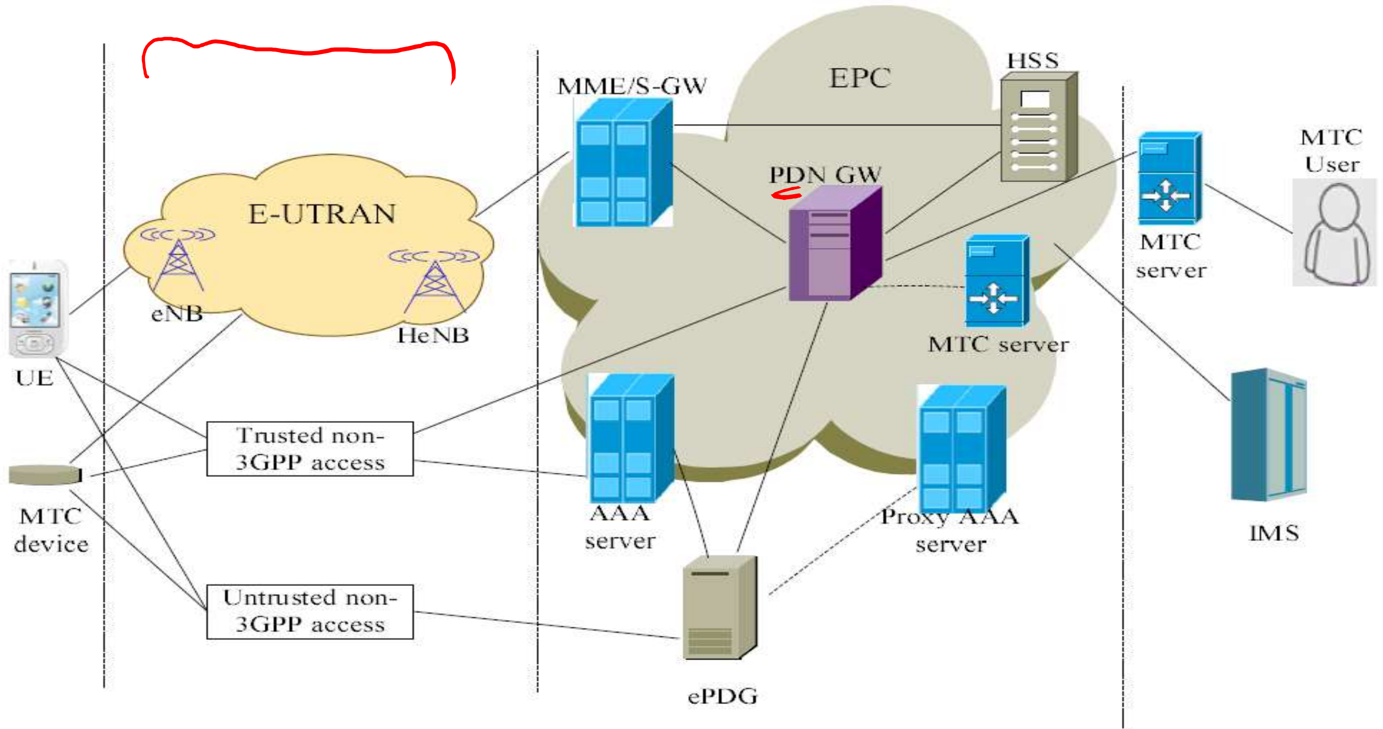
  - Long-Term Evolution (LTE) is an emerging radio access network technology standardized by 3GPP and it is evolving as an evolution of 3G.

  - It aims to provide seamless IP connectivity between user equipment (UE) and the packet data network (PDN) without any disruption to the end users' applications during mobility.

The Core Network

- EPC is responsible for the overall control of the establishment of the bearers and the UE
- The main logical nodes in the EPC:
  - ✓ Home Subscriber Server (HSS) holds HLR
    - users subscription data,
    - information about the PDNs,
    - dynamic information the identity of the MME
  - PDN Gateway (P-GW) is responsible for
    - IP address allocation for the UE,
    - filtering of downlink user IP packets into the different QoS-based bearers,
    - QoS enforcement for guaranteed bit rate bearers

Long Term Evolution



Video summary

- Layering in Wireless Networks
- What is IMTS? 3G?
- 3G Security Principles
- 3G Network Access Security
- 4G LTE Network