2. Conventional networks
2.4 GSM (+ security principles of 3GPP)

Prof. JP Hubaux

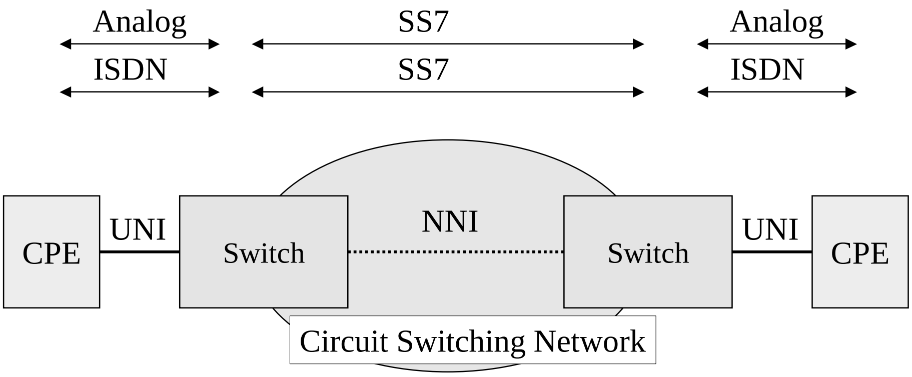
GSM: Global System for Mobile communications

- Objectives
  - Unique standard for European digital cellular networks
  - International roaming
  - Signal quality
  - Voice *and* data services
  - Standardization of the air *and* the network interfaces
  - Security
- Principles
  - Strong integration with the telephone network (PSTN)
  - Interfaces inspired by the Integrated Services Digital Network (ISDN)
  - Hence, supervision by means of Signaling System 7 (SS7)

Signaling System Number 7

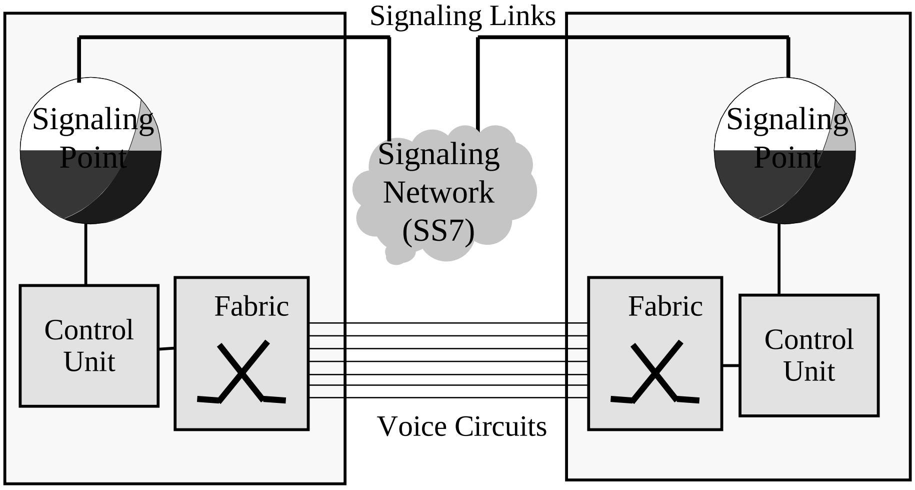
- Enhanced services requested by users require bidirectional signaling capabilities, flexibility of call setup and remote database access
- With SS7, a signaling channel conveys, by means of labeled messages, signaling information relating to **call processing** and to network management
- SS7 is the most important signaling system in the world: it supervises the PSTN, the cellular networks (GSM), and the Intelligent Network

SS7 in the PSTN



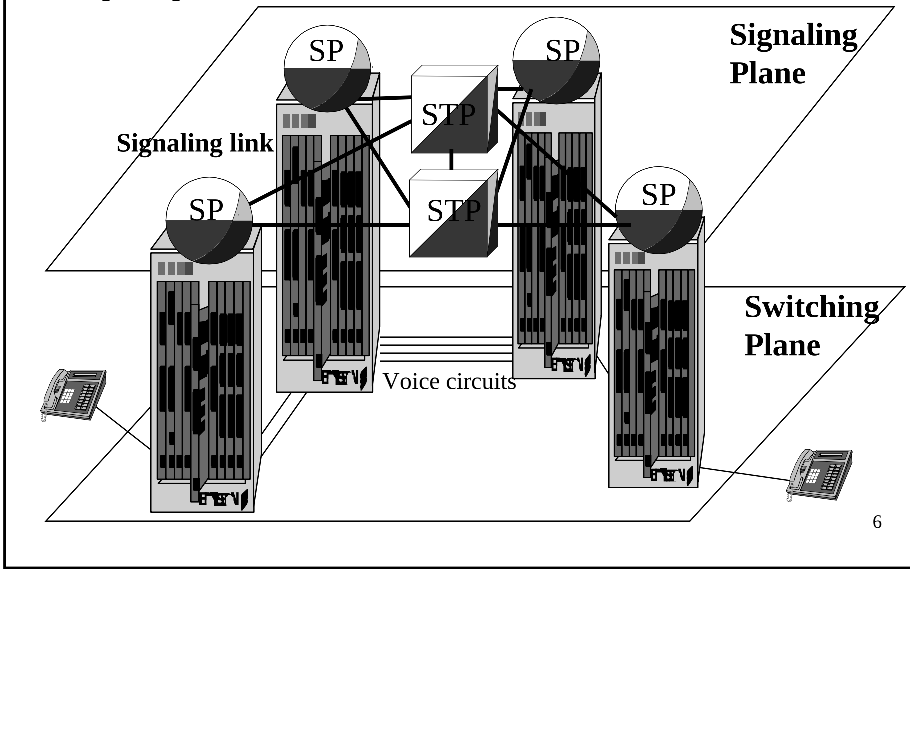
CPE: Customer Premises Equipment
UNI: User-Network Interface
NNI: Network-Network Interface
ISDN: Integrated Services Digital Network

Interface between the circuit switching network and the signaling network

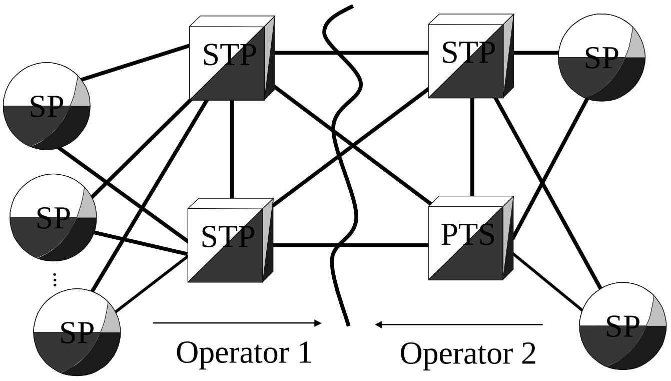


Signaling and Switching Planes

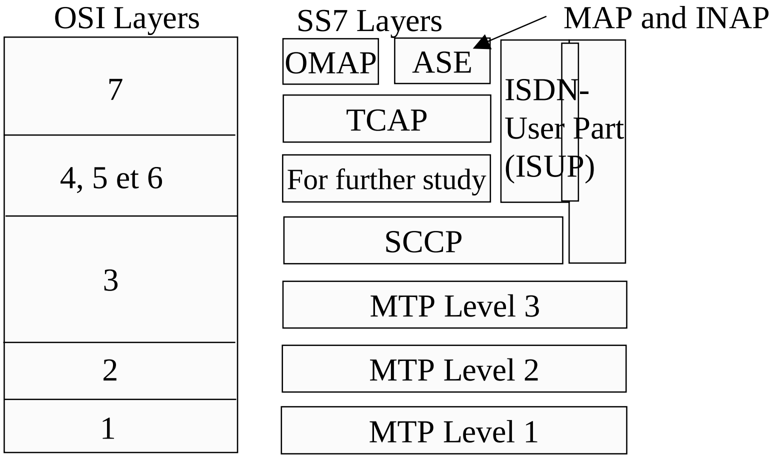
SP: Signaling Point
STP: Signaling Transfer Point



Example of Signaling Network



SS7 Architecture


OSI Layers

SS7 Layers

MAP and INAP

7

4, 5 et 6

3

2

1

OMAP

ASE

ISDN-User Part (ISUP)

TCAP

For further study

SCCP

MTP Level 3

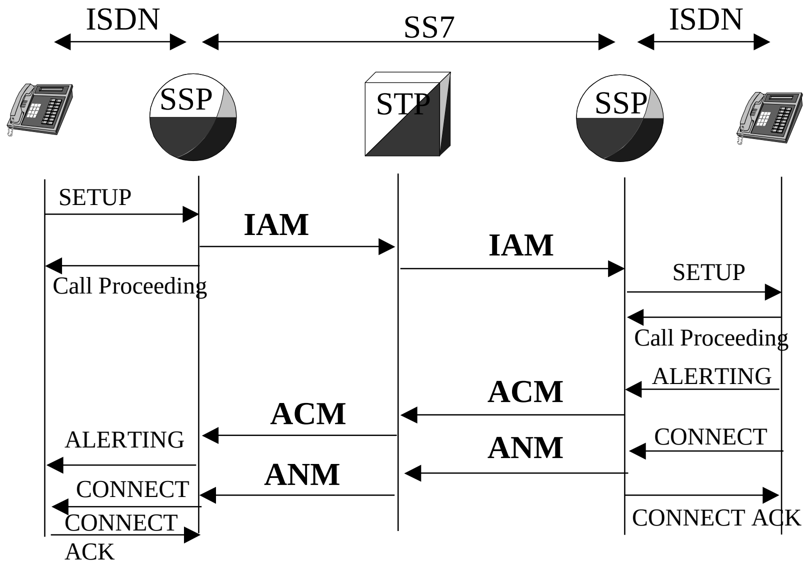
MTP Level 2

MTP Level 1

ASE: Application Service Element
INAP: Intelligent Network
Application Part
MAP: Mobile Application Part
MTP: Message Transfer Part

OMAP: Operations, Maintenance and Administration
Part
SCCP: Signaling Connection Control Part
TCAP: Transaction Capabilities Application Part

ISUP Call setup phase



ISDN

SS7

ISDN

SSP

STP

SSP

SETUP

IAM

IAM

Call Proceeding

SETUP

Call Proceeding

ALERTING

ACM

ACM

ALERTING

ANM

CONNECT

ANM

CONNECT

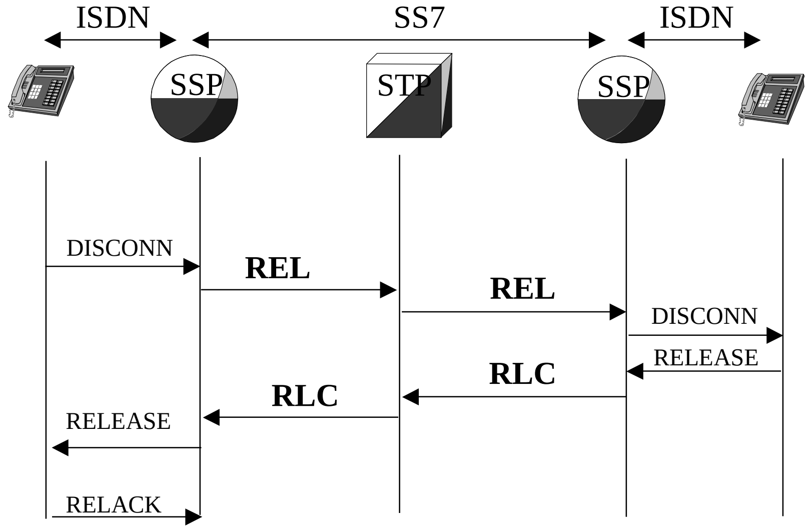
CONNECT ACK

CONNECT

ACK

IAM: Initial Message; ACM: Address Complete Message; ANM: Answer Message

ISUP Call Release phase



ISDN

SS7

ISDN

SSP

STP

SSP

DISCONN

REL

REL

DISCONN

RELEASE

RLC

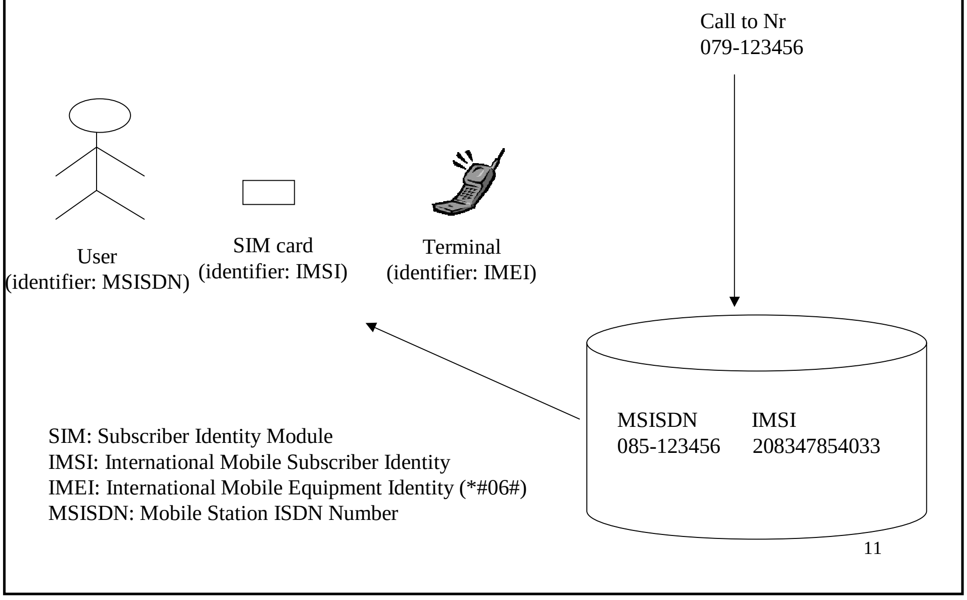
RLC

RELEASE

RELACK

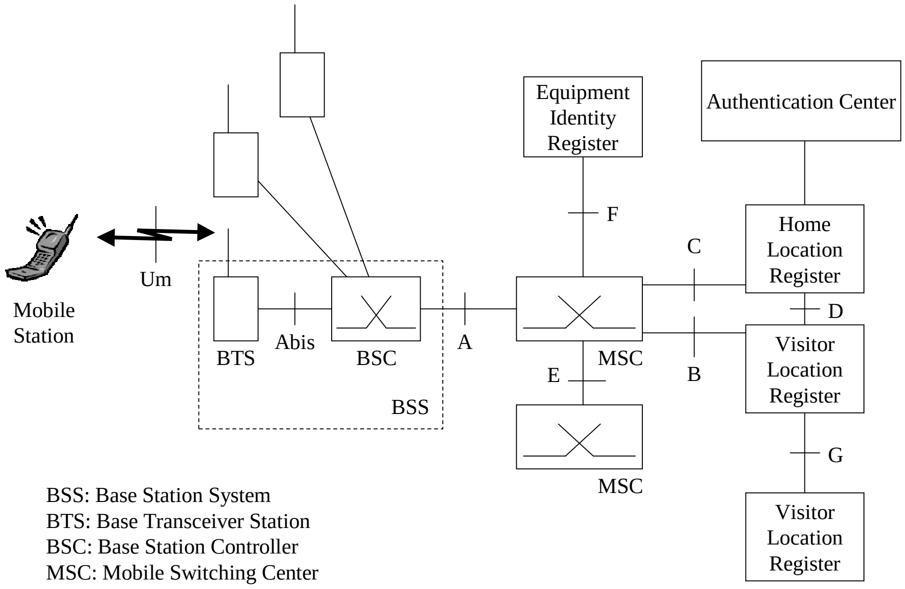
REL: Release   RLC: Release Complete

Addressing in GSM



SIM: Subscriber Identity Module
IMSI: International Mobile Subscriber Identity
IMEI: International Mobile Equipment Identity (*#06#)
MSISDN: Mobile Station ISDN Number

GSM Architecture

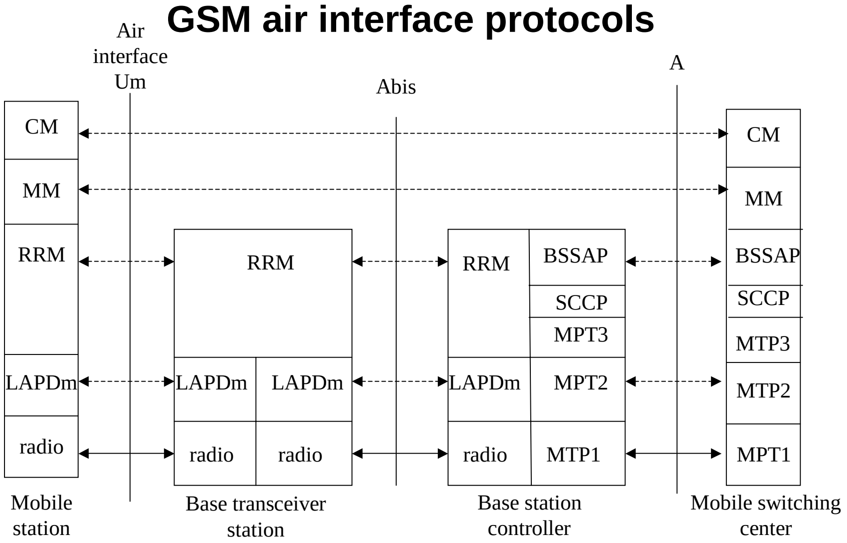


BSS: Base Station System
BTS: Base Transceiver Station
BSC: Base Station Controller
MSC: Mobile Switching Center

Functions of the MSC

- Paging
- Coordination of call set up from all MSs in its jurisdiction
- Dynamic allocation of resources
- Location registration
- Interworking function with different networks (e.g., PSTN)
- Handover management
- Billing for all subscribers based in its area
- Reallocation of frequencies to BTSs in its area to meet heavy demand
- Encryption
- Echo canceler operation control
- Signaling exchange between different interfaces
- Gateway to Short Message Service

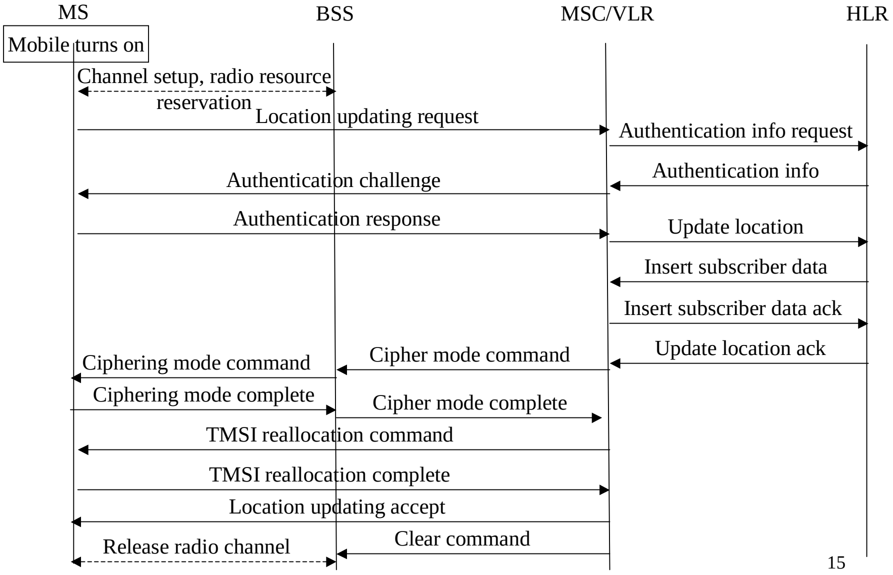
GSM air interface protocols



CM: call management
MM: mobility management
RRM: Radio resources management
(ISDN)
BSSAP: BSS Application Part

SCCP: Signal connection control part
MTP: message transfer part
LAPD: link access - protocol D channel

Location updating



MS

BSS

MSC/VLR

HLR

Mobile turns on

Channel setup, radio resource reservation

Location updating request

Authentication info request

Authentication info

Authentication challenge

Authentication response

Update location

Insert subscriber data

Insert subscriber data ack

Update location ack

Cipher mode command

Ciphering mode command

Ciphering mode complete

Cipher mode complete

TMSI reallocation command

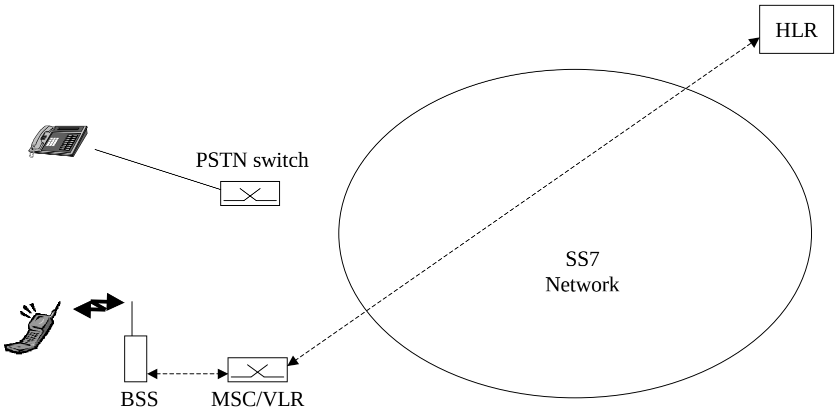
TMSI reallocation complete

Location updating accept

Clear command

Release radio channel

Role of SS7: location updating



HLR

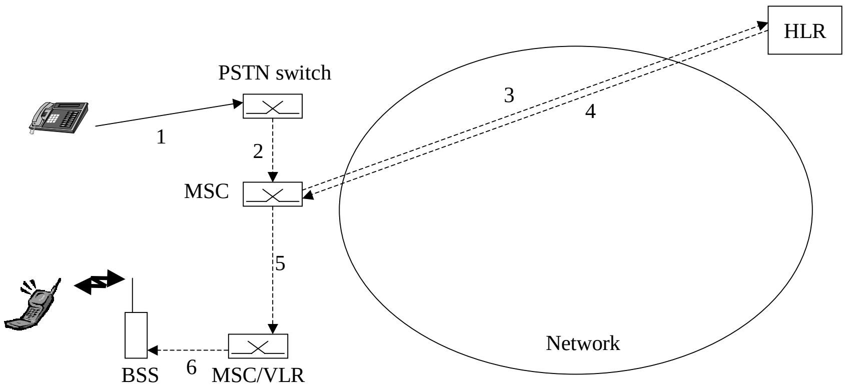
PSTN switch

SS7 Network

BSS

MSC/VLR

Role of SS7: call supervision



Data channels are setup after the messages shown
have been sent

↔ : messages conveyed by SS7

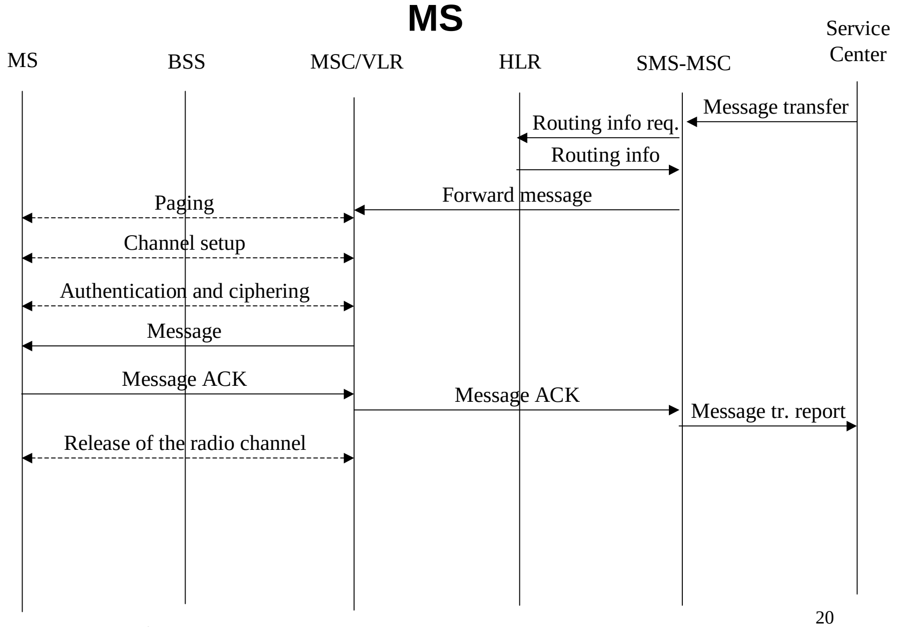
Billing Principles in GSM

- Basic principle: the calling party pays
- Exception: the calling party does not pay for extra charges induced by initiatives of the callee:
  - roaming
  - call forwarding

Data services of GSM

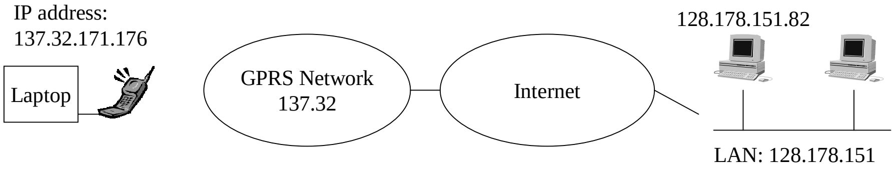
- Short Message Service (SMS)
  - Similar to advanced paging systems
  - Makes use of the control channel
- General Packet Radio Service (GPRS)
  - Aimed at interfacing the Internet (e.g., for Web browsing)
  - Rates up to 170kb/s
- High Speed Circuit-Switched Data (HSCSD)

Short Message Service: message sent to a MS

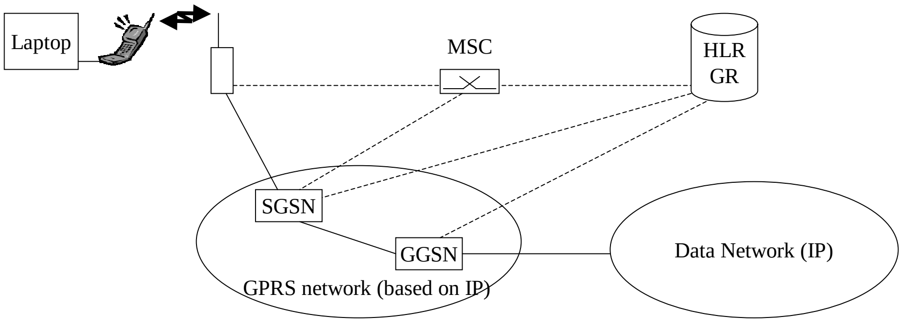


Assumption: before being paged, the terminal is idle

General Packet Radio Service



GPRS architecture

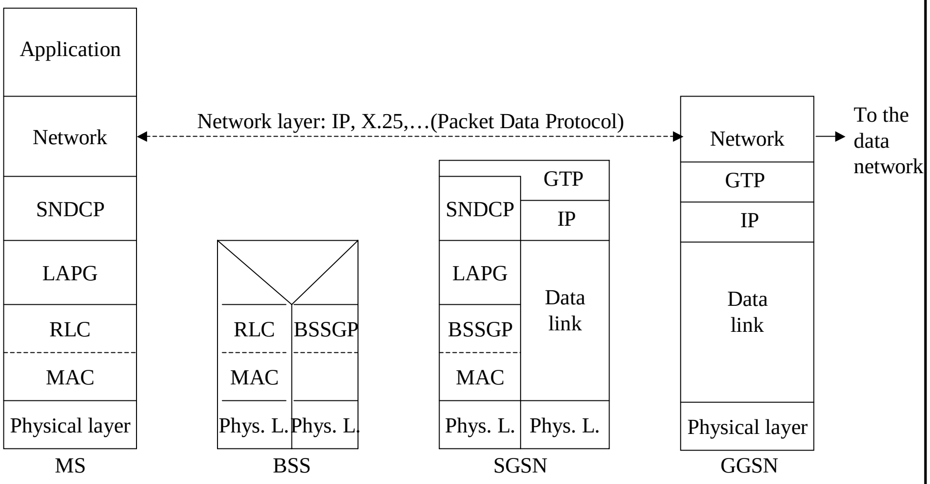


——— : signaling + data

- - - - - : signaling only

GR: GPRS Register: manages the association between the IP address and the IMSI
SGSN: Serving GPRS Support Node (router)
GGSN: Gateway GPRS Support Node (router)

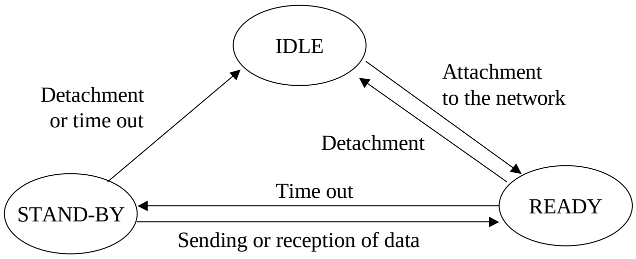
User plane protocols



RLC: Radio Link Control
BSSGP: BSS GPRS Protocol
GTP: GPRS Tunnel Protocol

SNDCP: Subnetwork Dependent Convergence Protocol
LAPG: Link Access Protocol on G channel

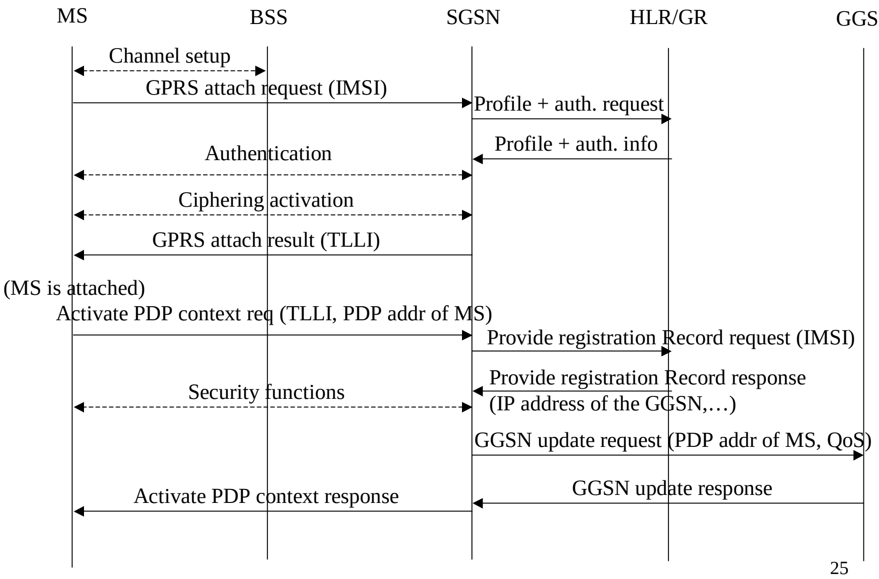
Mobility management



Idle: no active GPRS session
Ready: session established; ongoing data exchange; precise mobile location (which cell)
Stand-by: session established, with no ongoing data exchange; approximate mobile location, the mobile has to be tracked in its routing area

During a GPRS session (Ready or Stand-by states), the session itself is identified by a TLLI (Temporary Logical Link Identity)

Network attachment + context activation



MS

BSS

SGSN

HLR/GR

GGSN

Channel setup

GPRS attach request (IMSI)

Profile + auth. request

Profile + auth. info

Authentication

Ciphering activation

GPRS attach result (TLLI)

(MS is attached)

Activate PDP context req (TLLI, PDP addr of MS)

Provide registration Record request (IMSI)

Provide registration Record response
(IP address of the GGSN,…)

Security functions

GGSN update request (PDP addr of MS, QoS)

GGSN update response

Activate PDP context response

GSM Frequencies

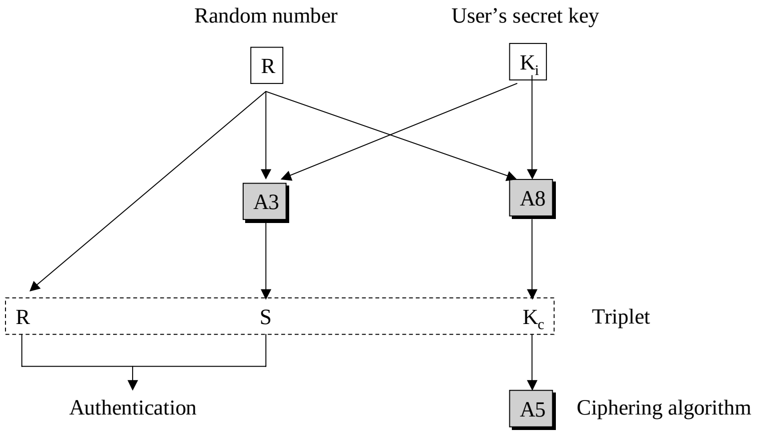
	GSM (Europe)	DCS (Europe)	GSM (USA)
Frequency band	890-915 MHz 935-960 MHz	1710-1785 MHz 1805-1880 MHz	1850-1910 MHz 1930-1990 MHz

DCS = Digital Cellular System: same principles as GSM, but at frequencies better suited for microcells

GSM Security:
The SIM card (Subscriber Identity Module)

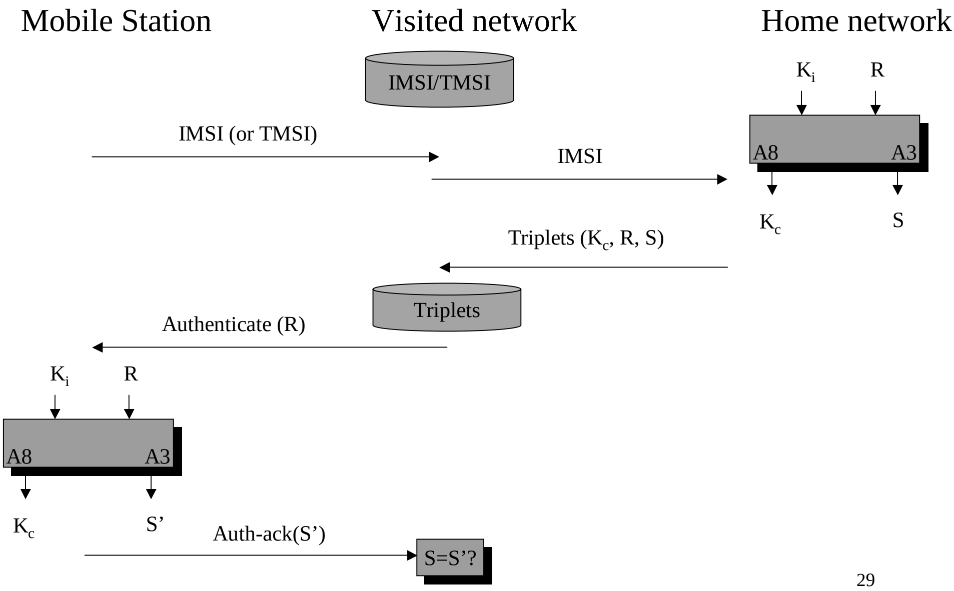
- Must be tamper-resistant
- Protected by a PIN code (checked locally by the SIM)
- Is removable from the terminal
- Contains all data specific to the end user which have to reside in the Mobile Station:
  - IMSI: International Mobile Subscriber Identity (permanent user's identity)
  - PIN
  - TMSI (Temporary Mobile Subscriber Identity)
  - K_i : User's secret key
  - K_c : Ciphering key
  - List of the last call attempts
  - List of preferred operators
  - Supplementary service data (abbreviated dialing, last short messages received,...)

Cryptographic algorithms of GSM



K_c: ciphering key
S : signed result
A3: subscriber authentication (operator-dependent algorithm)
A5: ciphering/deciphering (standardized algorithm)
A8: cipher generation (operator-dependent algorithm)

Authentication principle of GSM



Mobile Station

Visited network

Home network

IMSI/TMSI

K_i R

IMSI (or TMSI)

IMSI

A8 A3

K_c S

Triplets (K_c, R, S)

Triplets

Authenticate (R)

K_i R

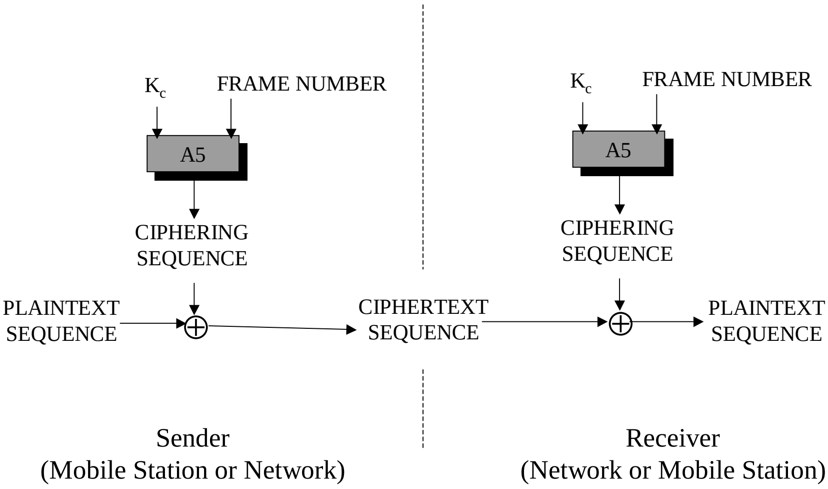
A8 A3

K_c S'

Auth-ack(S')

S=S'?

Ciphering in GSM



K_c FRAME NUMBER

A5

CIPHERING SEQUENCE

PLAINTEXT SEQUENCE

CIPHERTEXT SEQUENCE

K_c FRAME NUMBER

A5

CIPHERING SEQUENCE

PLAINTEXT SEQUENCE

Sender
(Mobile Station or Network)

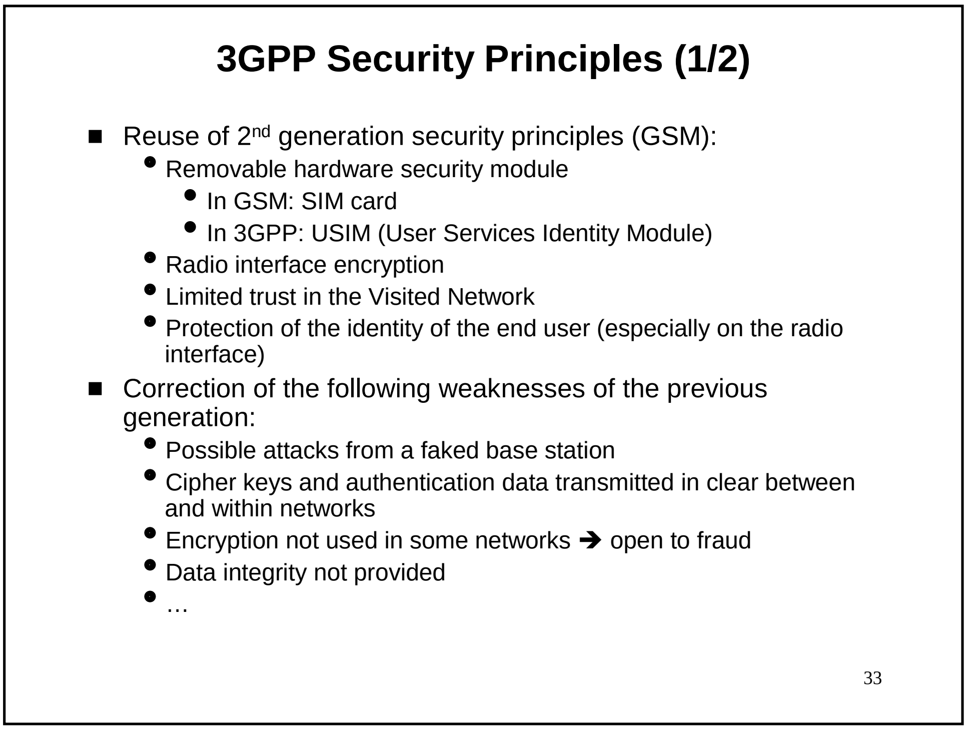
Receiver
(Network or Mobile Station)

Conclusion on GSM security

- Focused on the protection of the air interface
- No protection on the wired part of the network (neither for privacy nor for confidentiality)
- The visited network has access to all data (except the secret key of the end user)
- Generally robust, but a few successful attacks have been reported:
  - faked base stations
  - cloning of the SIM card

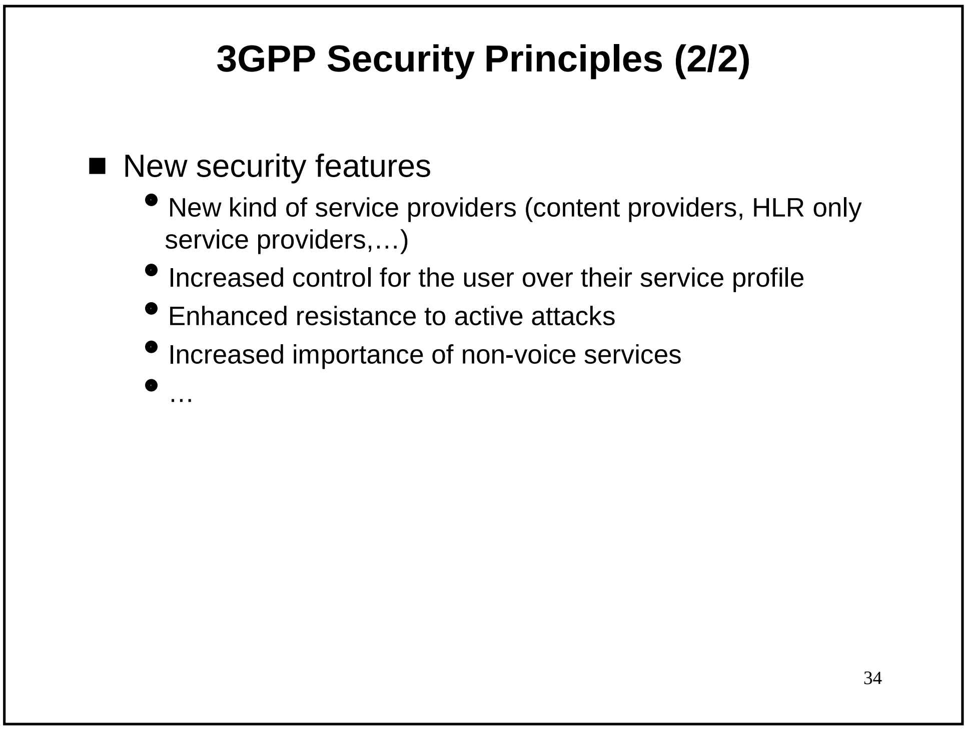
GSM today

- The common digital cellular technique deployed throughout Europe
- Probably the leading cellular technology worldwide
- Hundreds of millions of subscribers in more than 100 countries
- 7000+ pages of standards...



3GPP Security Principles (1/2)

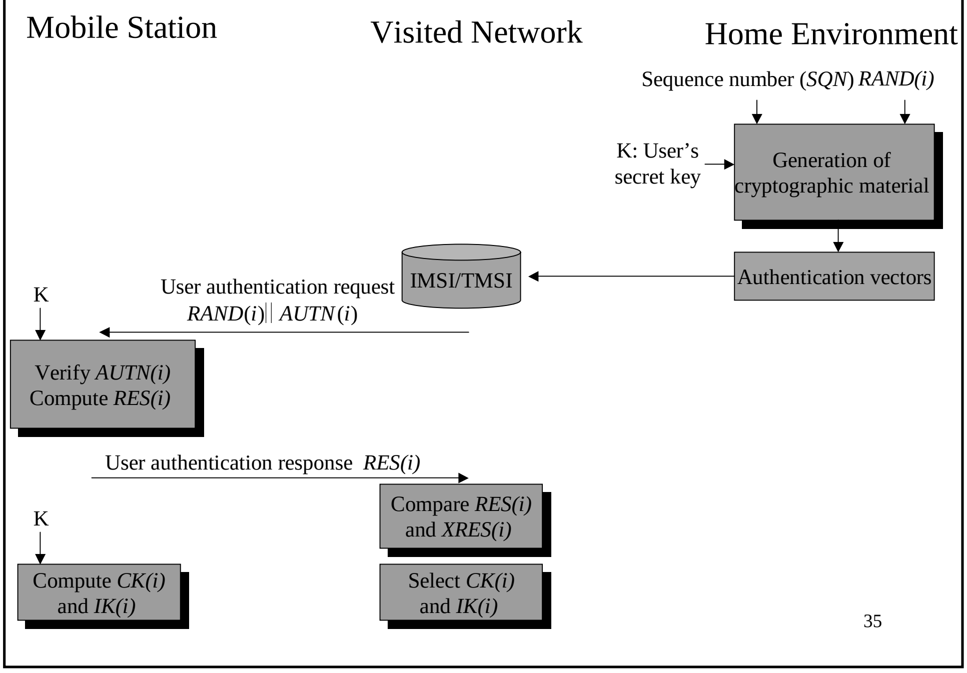
- Reuse of 2nd generation security principles (GSM):
  - Removable hardware security module
    - In GSM: SIM card
    - In 3GPP: USIM (User Services Identity Module)
  - Radio interface encryption
  - Limited trust in the Visited Network
  - Protection of the identity of the end user (especially on the radio interface)
- Correction of the following weaknesses of the previous generation:
  - Possible attacks from a faked base station
  - Cipher keys and authentication data transmitted in clear between and within networks
  - Encryption not used in some networks ➔ open to fraud
  - Data integrity not provided
  - …



3GPP Security Principles (2/2)

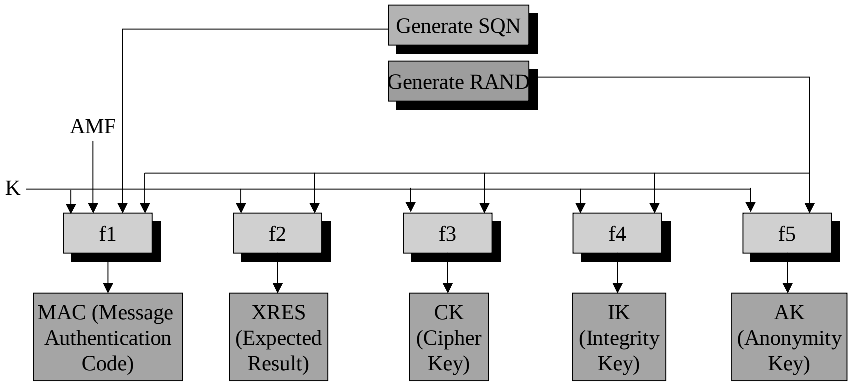
- New security features
  - New kind of service providers (content providers, HLR only service providers,…)
  - Increased control for the user over their service profile
  - Enhanced resistance to active attacks
  - Increased importance of non-voice services
  - …

Authentication in 3GPP



Mobile Station
Visited Network
Home Environment
Sequence number (*SQN*) *RAND(i)*
K: User's secret key
Generation of cryptographic material
Authentication vectors
IMSI/TMSI
User authentication request
RAND(*i*)|| *AUTN*(*i*)
K
Verify *AUTN(i)*
Compute *RES(i)*
User authentication response *RES(i)*
Compare *RES(i)* and *XRES(i)*
K
Compute *CK(i)* and *IK(i)*
Select *CK(i)* and *IK(i)*

Generation of the authentication vectors (by the Home Environment)

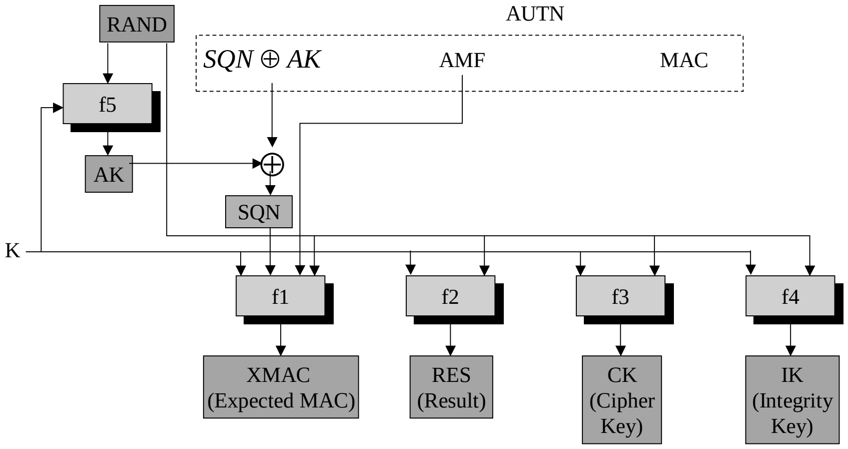


Authentication token: $AUTN := (SQN \oplus AK) \| AMF \| MAC$

Authentication vector: $AV := RAND \| XRES \| CK \| IK \| AUTN$

AMF: Authentication and Key Management Field

User Authentication Function in the USIM



AUTN

SQN ⊕ *AK* AMF MAC

RAND

f5

AK

SQN

K

f1 f2 f3 f4

XMAC (Expected MAC)

RES (Result)

CK (Cipher Key)

IK (Integrity Key)

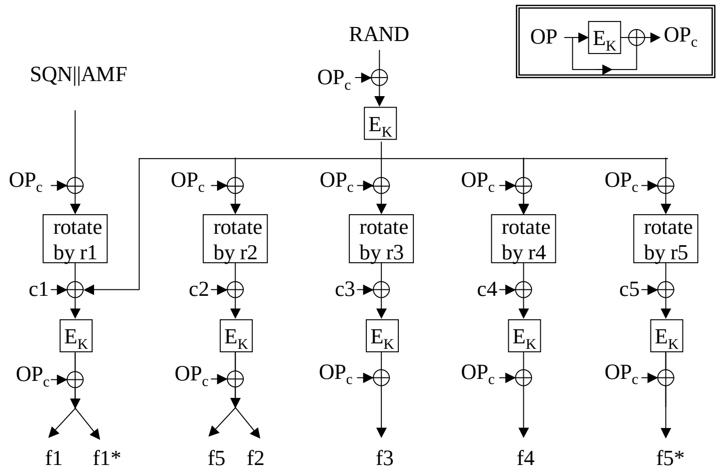
- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module

More about the authentication and key generation function

- In addition to f1, f2, f3, f4 and f5, two more functions are defined: f1* and f5*, used in case the authentication procedure gets desynchronized (detected by the range of SQN).
- f1, f1*, f2, f3, f4, f5 and f5* are operator-specific
- However, 3GPP provides a detailed example of algorithm set, called *MILENAGE*
- MILENAGE is based on the *Rijndael* block cipher
- In MILENAGE, the generation of all seven functions f1…f5* is based on the Rijndael algorithm

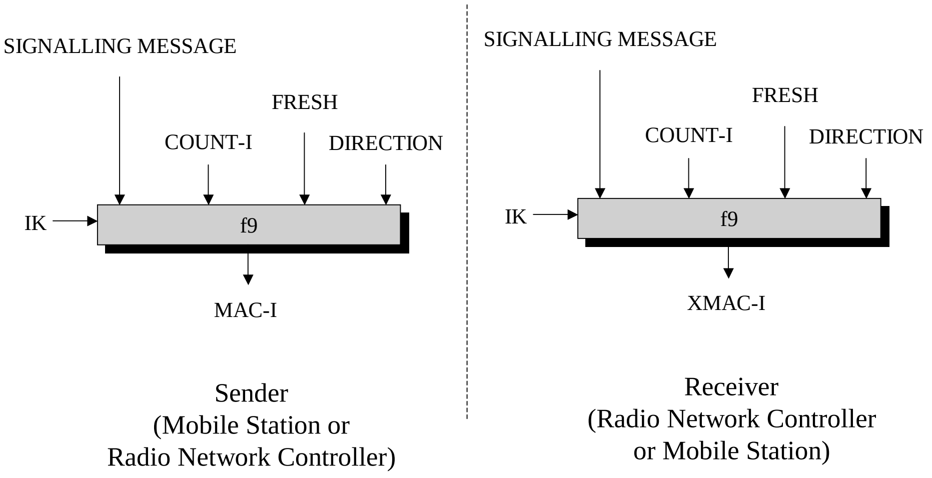
Authentication and key generation functions f1…f5*



OP: operator-specific parameter
r1,…, r5: fixed rotation constants
c1,…, c5: fixed addition constants

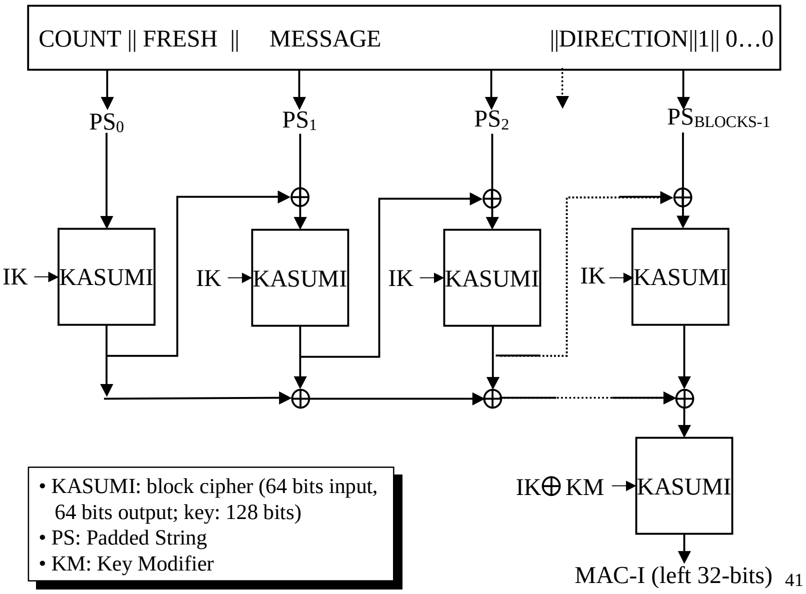
E_K : Rijndael block cipher with
128 bits text input and 128 bits key

Signalling integrity protection method



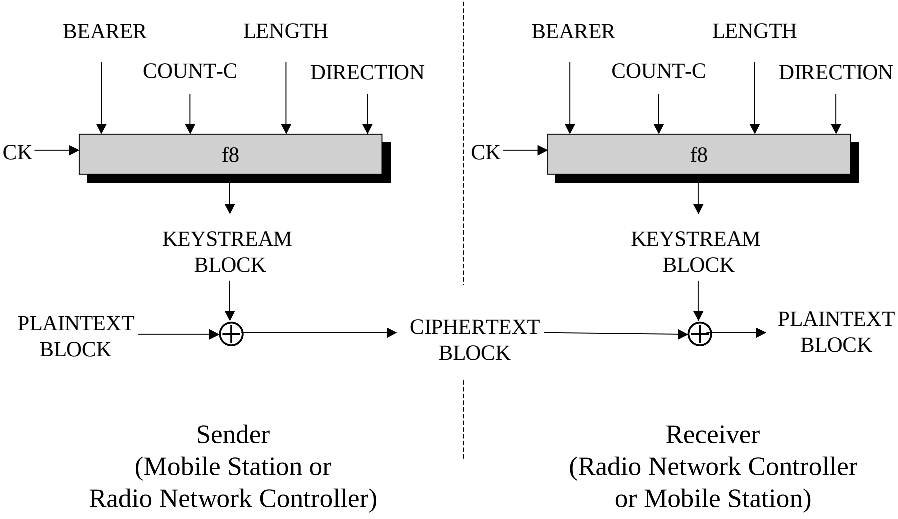
FRESH: random input

f9 integrity function



- KASUMI: block cipher (64 bits input, 64 bits output; key: 128 bits)
- PS: Padded String
- KM: Key Modifier

Ciphering method

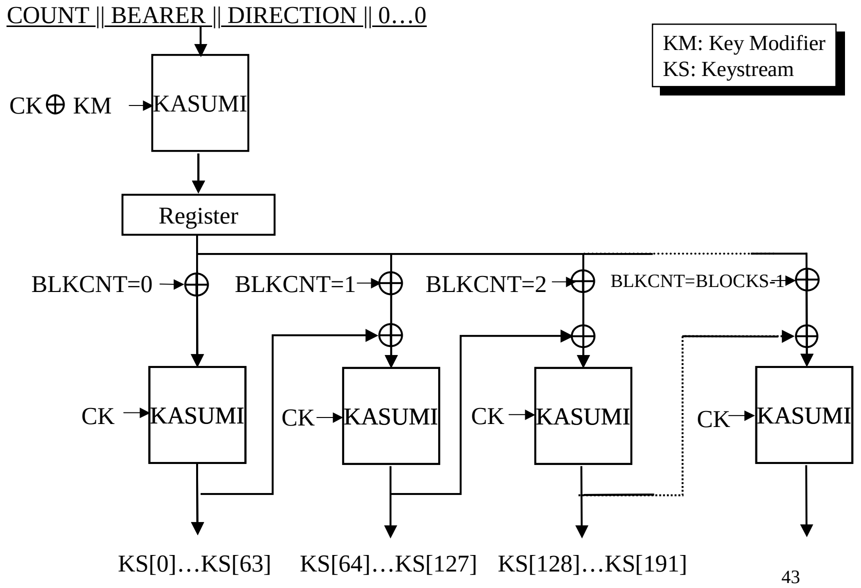


Sender
(Mobile Station or
Radio Network Controller)

Receiver
(Radio Network Controller
or Mobile Station)

BEARER: radio bearer identifier
COUNT-C: ciphering sequence counter

f8 keystream generator



KM: Key Modifier
KS: Keystream

Detail of Kasumi

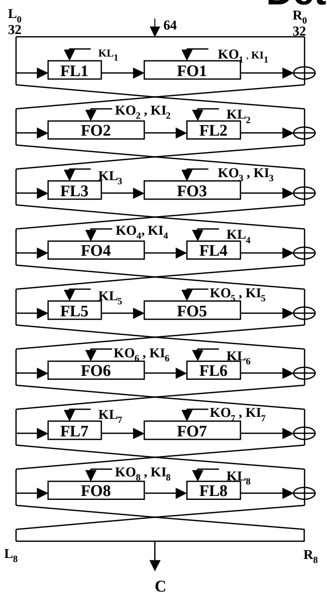


Fig. 1 **: KASUMI**

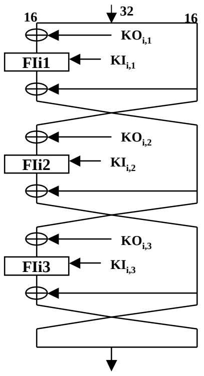


Fig. 2 **: FO Function**

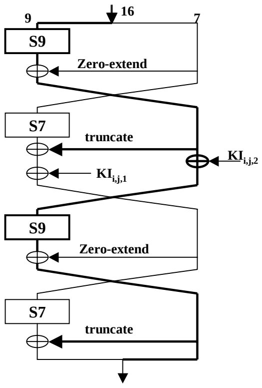


Fig. 3 **: FI Function**

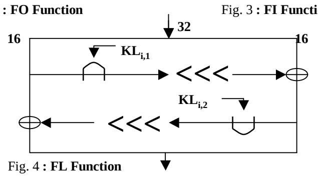


Fig. 4 **: FL Function**

KL$_i$, KO$_i$, KI$_i$: subkeys used at ith round
S7, S9: S-boxes

∩ Bitwise AND operation
∪ Bitwise OR operation
<<< One bit left rotation

Security: 3GPP vs Mobile IP

	3GPP	Mobile IP
Key management	Manual (K_{MH}) + roaming agreements	Manual or via the Internet Key Exchange (IKE)
Session key	Authentication vector	Registration key
Authentication	f1,…, f5* (e.g. MILENAGE)	AH
Data integrity	f9 (Kasumi)	AH
Confidentiality	f8 (Kasumi)	ESP
Location privacy ■ wrt correspondents ■ wrt foreign domain	 Yes No (it can require the IMSI)	 Yes (e.g., with rev. tunnelling) Partial
Protection of foreign domain against repudiation by user	No (cryptographic material provided in advance)	?
Lawful interception	Yes	-

Conclusion on 3GPP security

- Some improvement with respect to 2nd generation
  - Cryptographic algorithms are published
  - Integrity of the signalling messages is protected
- Quite conservative solution
- No real size experience so far
- Privacy/anonymity of the user not completely protected
- 2nd/3rd generation interoperation will be complicated and might open security breaches

References

On Signalling System 7

- Travis Russel, *Signaling System #7,* Second Edition, McGraw-Hill Telecommunications, 1998.
- Uyless Black, *ISDN and SS7,* Prentice Hall, 1997
- Abdi Modaressi and Ronald A. Skoog, *Signaling System N°7: A tutorial,* IEEE Communications Magazine, July 1990, pp 19-35.

■ On GSM

- D. Goodman: *Wireless Personal Communications Systems*
  Addison-Wesley, 1997
- S. Redl et al.: *GSM and Personal Communication Handbook*
  Artech House Publ, 1998
- A. Mehrotra: *GSM System Engineering* Artech House Publ, 1997

■ On GPRS

- R. Kalden et al.: *Wireless Interned Access Based on GPRS*
  IEEE Personal Communication Magazine, April 2000

■ On 3GPP

- 3rd Generation Partnership Project: http://www.3gpp.org