SIM/USIM cards

Samia Bouzefrane

samia.bouzefrane@cnam.fr

CEDRIC Lab

CNAM

http://cedric.cnam.fr/~bouzefra

Agenda

- Introduction to GSM network
- Introduction to SIM cards
- SIM card services
- Security
- File systems of SIM cards

Introduction to GSM network

GSM

- Early 1980's, several cellular networks in Europe
- the systems are incompatible from one country to another
- Consequences : - mobile equipements are limited to the frontiers
  - limited market

-Creation of « Group Special Mobile » to:

- Increase the quality of service
- international support : roaming
- new functionalities
- provide terminals and services with low cost

GSM

- Standardization in 1982 : called « Group Special Mobile »

- Since 1989, the ETSI (European Telecommunications Standard Institute) provides the spécifications of GSM and of UMTS (*Universal Mobile Telecommunications System*, 3rd generation ntework).

  ETSI is at Sophia Antipolis (Nice, France).

- 1991 : becomes an international standard called « Global System for Mobile communications »

In Europe, the GSM standard uses frequency bandwidth of 900 MHz and 1800 MHz. In US, the bandwidth used is of 1900 MHz.

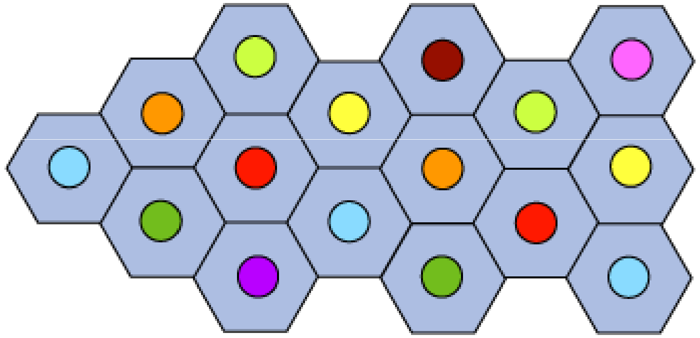
Tri-band: cell phones are usable in Europe and US (3 frequencies)
Bi-band : cell phones are usable only in Europe.

- The GSM standard allows a maximal rate of 9,6 kbps

  => transmission of voice, of data, text messages (**SMS**, *Short Message Service*) or multimedia messages (**MMS**, *Multimedia Message Service*).

Cell network principle

A cellular network is based on cells,
Each cell covers a geographical area.
A cell: hundred of meters (urban zone), thirty kms (rural zone).



Each cell has a central transmitter-receiver called *Base Transceiver Station*, **BTS**.
Over the radius of a cell is smaller, the available bandwidth is high.
Each cell is surrounded by six neighboring cells.
Adjacent cells can not use the same frequency.

Elements of the cellular network

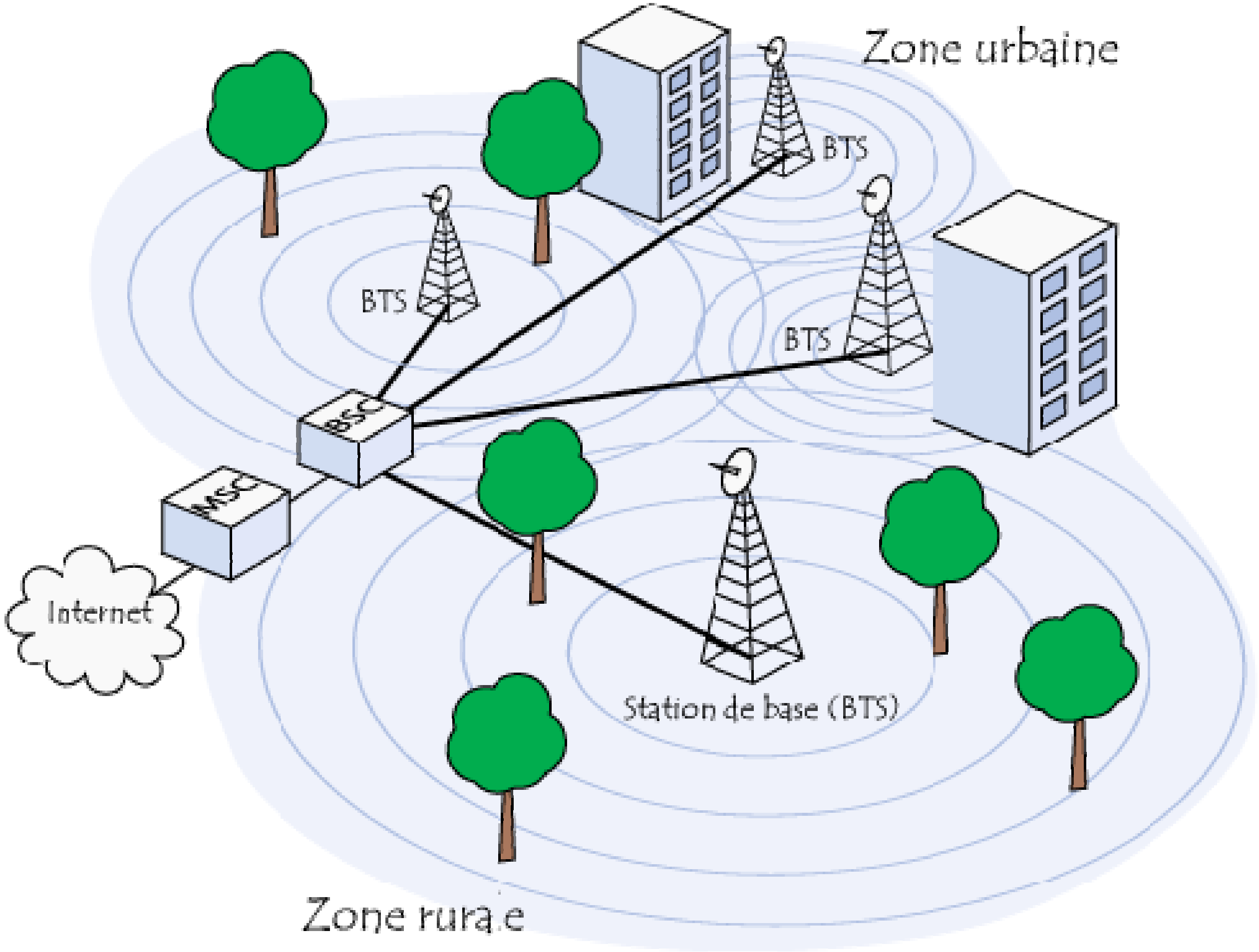
➢ **BSC**, *Base Station Controller*
that connects all the base stations.

➢**BSS** *Base Station Subsystem*
Base station controller + base stations.

➢**MSC,** *Mobile Switching Center,*
managed by the telecom operator, links the station controllers to the Internet and to the telephone network.

➢**NSS,** *Network Station Subsystem* to which belongs the MSC,
In charge of managing the user identities, their location and establishing
of the communication with the other subscribers.

GSM Architecture



Involved Databases

- **HLR,** *Home Location Register*: the database of the subscribers linked to the MSC.
  It contains information (location, administrative information, etc.)

- **VLR,** *Visitor Location Register*: a database
  contains information on the local subscribers.
  The VLR retrieves data of new user from the HLR corresponding to its subscription area. The data is stored during the time of its presence in the area and are removed when he leaves or after a long period of inactivity (device off).

- **EIR,** *Equipement Identity Register* : a database of mobile equipments.

- **AuC**, *Autentication Center* : in charge of verifying the user identities (authentication).

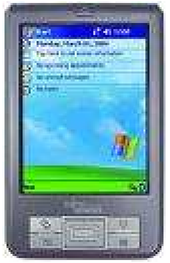
Mobility

➢The cellular network supports mobility by managing the handover, ie to pass from one cell to another.

➢GSM networks also support the concept of roaming ie the passage of a network operator to another.

Mobile stations

Mobile Station



➢**Mobile Station** : the terminal of the user

➢**Mobile Station** composed of:

- **SIM** (*Subscriber Identity Module*) card, to identify a unique user.
- a mobile equipment identified with a unique number of 15 digits called **IMEI** (*International Mobile Equipment Identity*).

➢Each SIM card owns a unique identity number (secret):**IMSI** (*International Mobile Subscriber Identity*), which can be protected with a key called 4-digit PIN.

➢Communication between a mobile station and a base station is done via a radio link, generally called *over the air*.

SIM card

- **Initially introduced in 1988**

- **10 billions of cards in 2011**

- **Functional role in the network:**

  - Contains details concerning the user subscription

  - Holds the secrets needed to prove the authenticity of the mobile and to quantify the exchange.

  - Loading new services.

SIM card: Mobility

- **Subscription details stored on the card:**

  - Unique identity of the subscriber (IMSI)
  - Telephone number of the subscriber (MSISDN)
  - Mobile equipment identity (IMEI)
  - Service Code (operator)

  and so on.

SIM card: Security Services

- The SIM card stores sensitive information:

Secret codes:

- User authentication: PIN (Personal Identification Code)
- Authentication of the operator: PUK (Personal Unlock Code)

Secret keys:

- For authentication of the SIM card by the network
- For encrypted communication

SIM Card: downloadable services

➢The SIM card is a runtime environment for trusted applications able to interact with the mobile:

* Display info on the mobile screen
* Collect information for the user
* Etc.

➢Able to interact with the network:

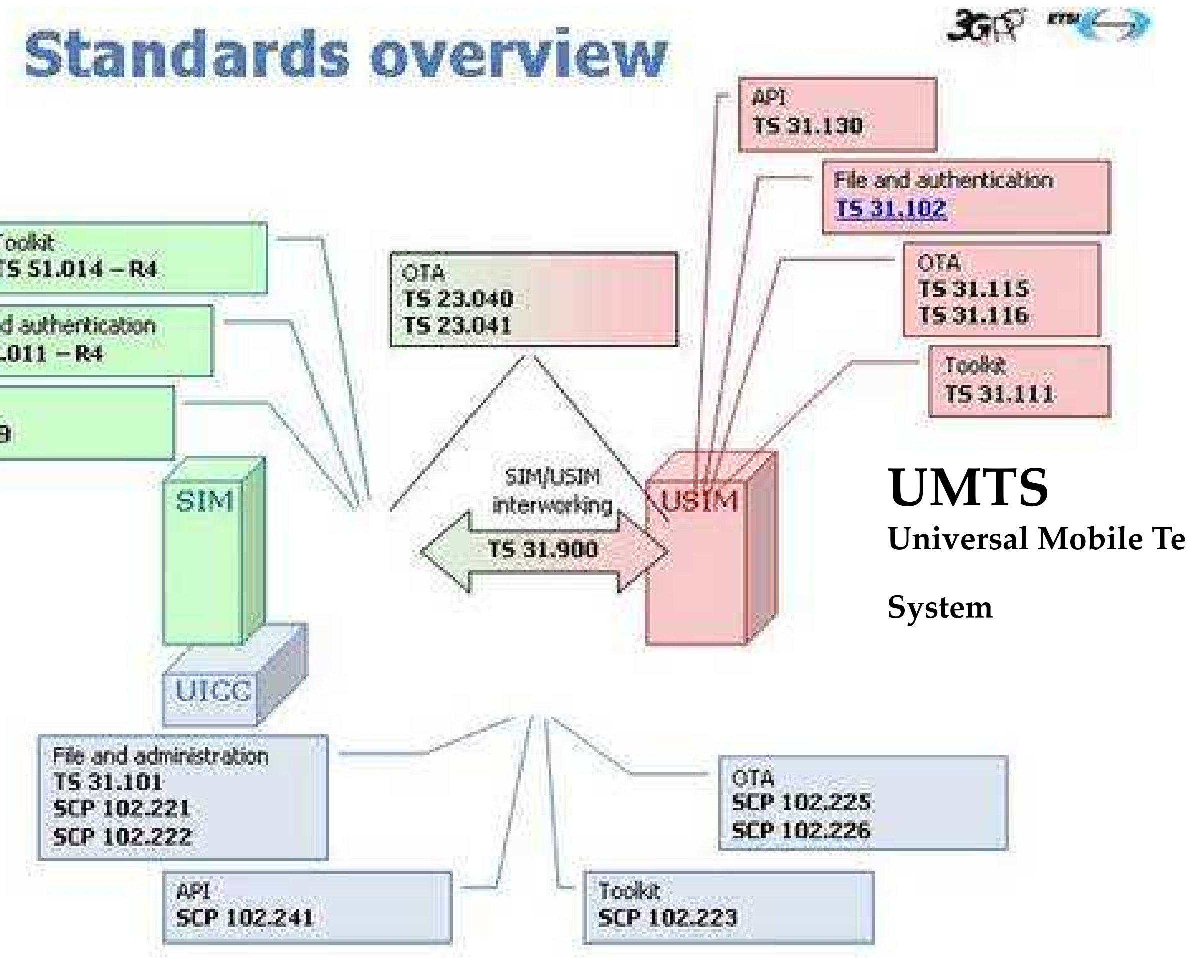
* Send and receive messages (SMS, GPRS, etc.).
* geolocalization

➢Able to interact with the system files from the SIM card

* Write / read files from the SIM

Standardization and security

The standards



GSM

UMTS

Universal Mobile Telecommunications System

UICC: Universal Integrated Circuit Card

ETSI standards

SIM

- ➢File management and Authentication : 3 GPP TS 51.011 (ETSI GSM 11.11)
- ➢SIM Toolkit Applet Management : 3 GPP TS 51.014 (ETSI GSM 11.14)
- ➢SIM API for Java Card : 3 GPP TS 43.019

USIM

- ➢File management and Authentication : 3 GPP TS 31.102
- ➢USIM Toolkit Applet Management : 3 GPP TS 31.111
- ➢USIM API for Java Card : 3 GPP TS 31.130

Protection methods proposed in GSM 02.09 / 1

1. **Protecting the identity of a subscriber:**
   The subscriber has an identifier (IMSI: International Mobile Subscriber Identity) to find the subscription settings in the HLR (Host Location Registe database of customer accounts.
   The network delivers a TMSI (Temporary Mobile Subscriber Identity) a temporary identity that changes with each call to ban traceability of communications.

2. The authentication of a subscriber:
Strong authentication is performed using the A3 algorithm associated with a 128-bit key Ki.

GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security Aspects".

Protection methods proposed in GSM 02.09/2

3. **The confidentiality of user data:**
In a cellular network, the information is transmitted by electromagnetic waves (Over The Air) between the mobile and base station (antenna).
Exchange between mobile and base station are encrypted using A5 algorithm that uses an encryption key Kc. Kc is updated each call (authentication) with the algorithm A8 key generation.
A3 and A8 are often confused (called A38 or A3A8).

4. The protection of certain information such as:

IMSI, the serial number of the phone, IMEI (International Mobile Equipment Identity).

Authentication in GSM network

There are 5 entities involved:

- SIM card

-Mobile

-VLR (*Visitor Location Register*)

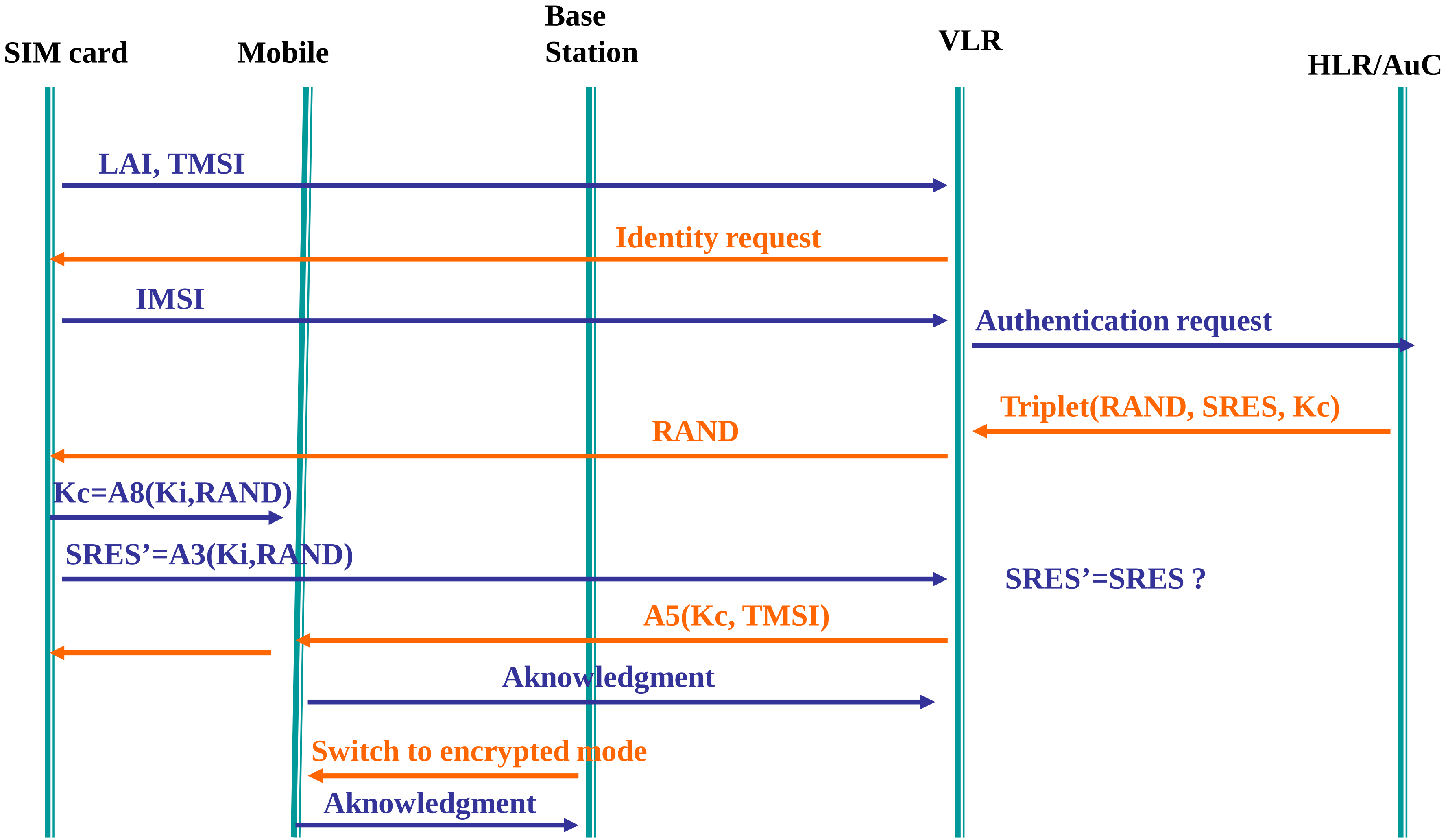
-HLR (*Host Location Register*) :

- AuC (*Authentication Center*).

The standard 3GPP TS 43.020 identifies a cell and a set of cells thanks to LAI (*Location Area Identity*).

3GPP TS 43.020 – Technical Specification Group Services & System Aspects; Security Related Network Functions (Release 5, 2002).

Security Protocol of GSM/1



RAND : random number of 16 bytes
SRES (Signed RESponse) : SRES=A3(Ki, RAND)
Kc : key of encryption of the communications, Kc=A8(Ki, RAND).

Security Protocol of GSM/2

1. The subscriber has the values (LAI, TMSI) stored in the SIM module, following a previous call.
2. The mobile sends the VLR values (LAI, TMSI).
3. If the VLR fails to retrieve the IMSI, it sends an identification request to the mobile
4. The VLR retrieves the IMSI stored in the SIM card
5. The VLR sends to the HLR / AuC an authentication request
6. GSM AuC produces a triplet (RAND, SRES, Kc)
7. Upon receipt of the triplet, the VLR sends RAND to the mobile
8. The SIM calculates SRES = A3 (K_i, RAND) which is sent to the HLR.
9. The HLR compares SRES and SRES '=> authentication of the subscriber succeeds if SRES=SRES'.
10. The VLR chooses a new TMSI encrypted with A5 algorithm and K_c key and sends it to mobile.

The operations of encryption and decryption are applied to radio signals performed by the mobile (not the SIM card). From the base stations to the network cable operator, there is no guarantee of confidentiality.

Cryptographical algorithms

- The SIM card performs the calculation A3A8 in a safe space.

- In 1998, Mark Briceno, Ian Goldberg and David Wagner (Researchers at the University of Berkeley) broke A3A8 algorithm.

- While GSM recommends any algorithm, the operators use a secret Algo COMP128-1.

- These researchers have also broken the algorithm by finding the key Ki after approximately 500 000 tests. For this reason, the components that integrate COMP128-1 limited the number of calls to 100 000.

- SIM modules are now based on the COMP128-2 algorithm which is currently secret.

File systems

SIM card characteristics

In the 90’s:
SIM card : CPU (8 bits), RAM (128 bytes), ROM (7 Kb), EEPROM (3 Kb).

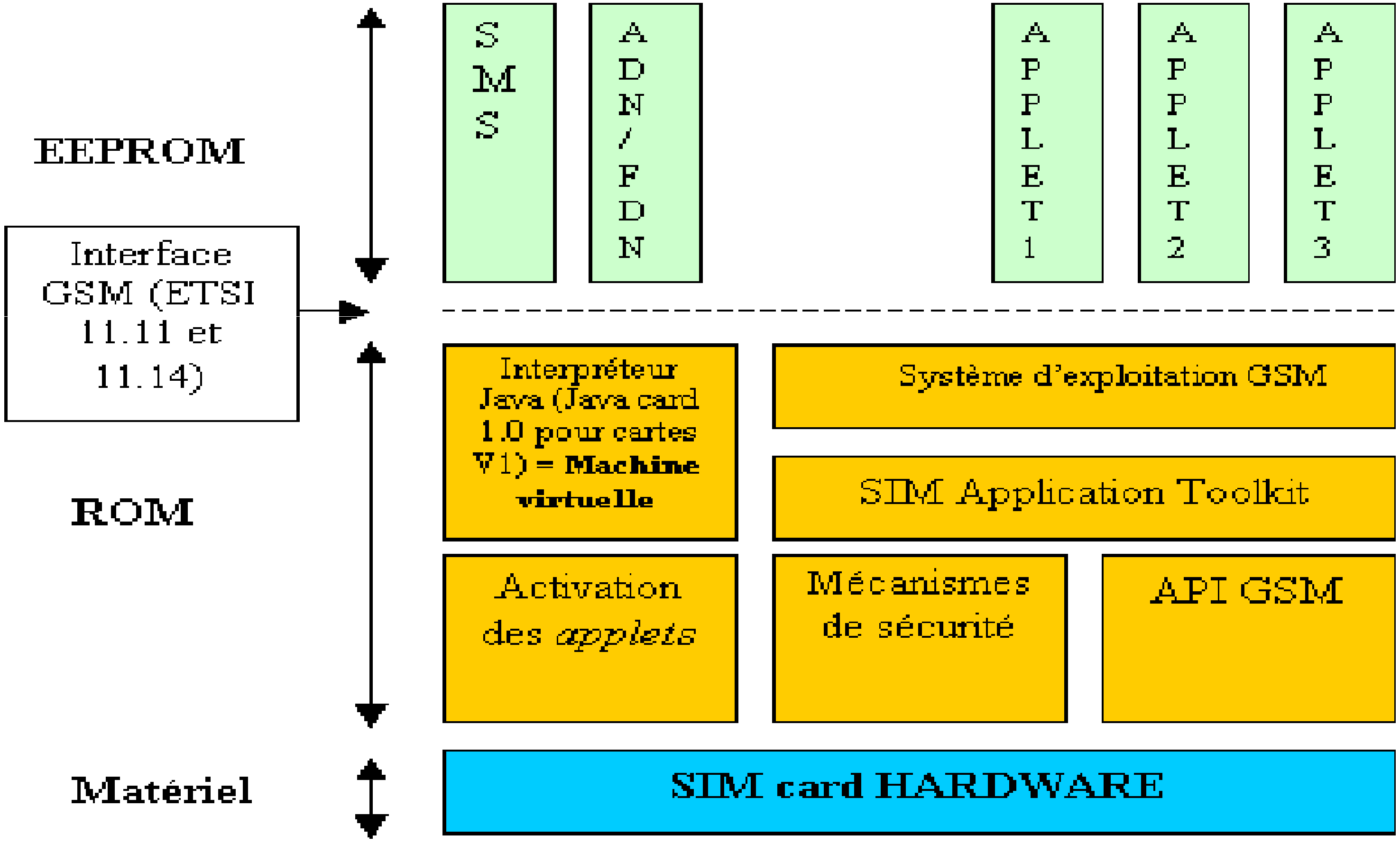
In 2011:
SIM card : CPU (32 bits), RAM (16 Kb), ROM (512 Kb), EEPROM/FLASH (512 Ko), a dedicated processor for crypto-calculations.

➢**ROM** (Read Only Memory) hosts the OS of the card, security mechanisms, API GSM.

➢**EEPROM** (Electrically Erasable Programmable Read Only Memory) contains directories as defined in GSM standard and applications.

➢**RAM** (Random Access Memory) allows computations.

SIM card structure



EEPROM

SMS

ADN/FDN

APPLET 1

APPLET 2

APPLET 3

Interface GSM (ETSI 11.11 et 11.14)

ROM

Interpréteur Java (Java card 1.0 pour cartes V1) = **Machine virtuelle**

Système d'exploitation GSM

SIM Application Toolkit

Activation des *applets*

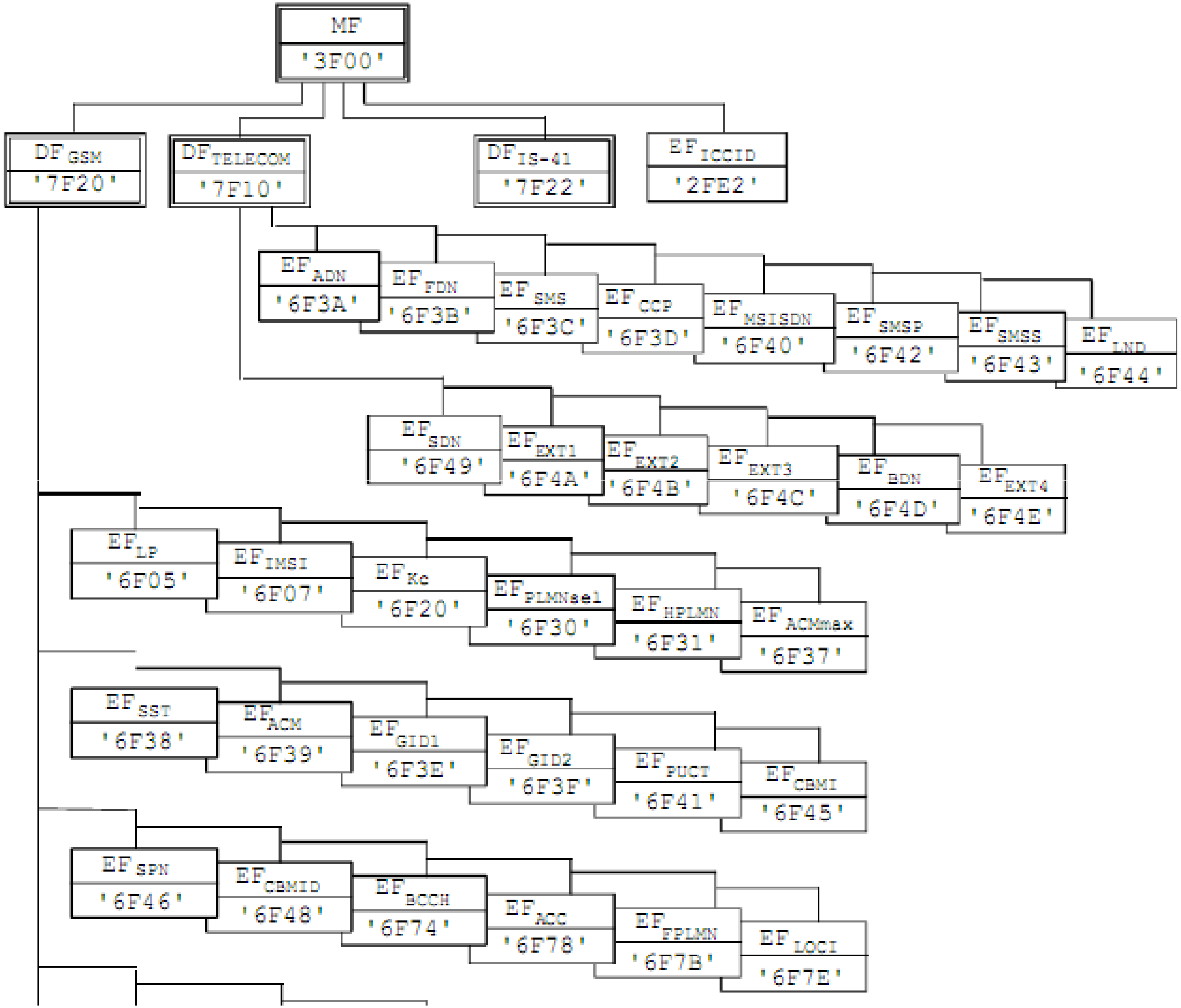
Mécanismes de sécurité

API GSM

Matériel

SIM card HARDWARE

File system according to 3GPP TS 51.011



MF '3F00'

DF$_{GSM}$ '7F20'

DF$_{TELECOM}$ '7F10'

DF$_{IS-41}$ '7F22'

EF$_{ICCID}$ '2FE2'

EF$_{ADN}$ '6F3A'

EF$_{FDN}$ '6F3B'

EF$_{SMS}$ '6F3C'

EF$_{CCP}$ '6F3D'

EF$_{MSISDN}$ '6F40'

EF$_{SMSP}$ '6F42'

EF$_{SMSS}$ '6F43'

EF$_{LND}$ '6F44'

EF$_{SDN}$ '6F49'

EF$_{EXT1}$ '6F4A'

EF$_{EXT2}$ '6F4B'

EF$_{EXT3}$ '6F4C'

EF$_{BDN}$ '6F4D'

EF$_{EXT4}$ '6F4E'

EF$_{LP}$ '6F05'

EF$_{IMSI}$ '6F07'

EF$_{Kc}$ '6F20'

EF$_{PLMNsel}$ '6F30'

EF$_{HPLMN}$ '6F31'

EF$_{ACMmax}$ '6F37'

EF$_{SST}$ '6F38'

EF$_{ACM}$ '6F39'

EF$_{GID1}$ '6F3E'

EF$_{GID2}$ '6F3F'

EF$_{PUCT}$ '6F41'

EF$_{CBMI}$ '6F45'

EF$_{SPN}$ '6F46'

EF$_{CBMID}$ '6F48'

EF$_{BCCH}$ '6F74'

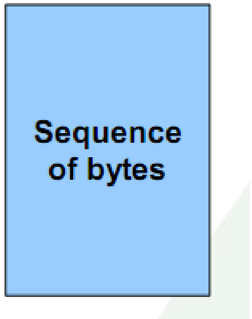
EF$_{ACC}$ '6F78'

EF$_{FPLMN}$ '6F7B'

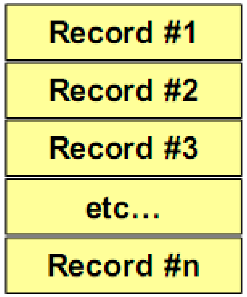
EF$_{LOCI}$ '6F7E'

File system of the SIM card

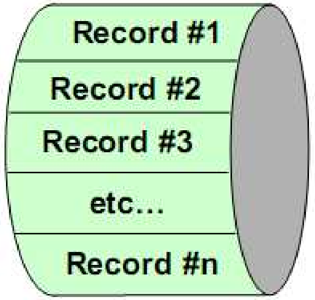
- ➢*Dedicated* **File**
- ➢*Elementary* **File**
  - ▪ Transparent file
  - ▪ Linear-fixed file
  - ▪ Cyclic file



Transparent



Linear Fixed



Cyclic

Directories and files

➢ **Root directory** : 3F 00

➢ **Principal sub-directories** : **GSM** (DF$_{GSM}$, 7F20) and **TELECOM** (DF$_{TELECOM}$, 7F10).

➢**1st byte:**

- '3F': Master File;
- '7F': 1st level Dedicated File;
- '5F': 2nd level Dedicated File;
- '2F': Elementary File under the Master File;
- '6F': Elementary File under a 1st level Dedicated File;
- '4F': Elementary File under 2nd level Dedicated File.

➢ After the reception of the ATR (*Answer To Reset*), the master file (MF) is selected automatically.

GSM directory

- File EF_{IMSI} (6F07) contains IMSI code.
- File EF_{LOCI} (6F 7E) contains : TMSI, LAI.
- EF_{LP} (Language preference)
- EF_{Kc} (Ciphering key Kc) contains Kc and the sequence number of the key.
- EF_{SST} (SIM service table) : is the list of available services.

  Service n°1 : CHV1 disable function
  Service n°2 : Abbreviated Dialling Numbers (ADN)
  Service n°3 : Fixed Dialling Numbers (FDN)
  Service n°4 : Short Message Storage (SMS)
  etc.
- EF_{ACM} (Accumulated call meter): contains the total number of units for the current cal and the preceding calls.
- EF_{MSISDN} (MSISDN): contains the phone number of the subscriber MSISDN.

TELECOM directory

➢**TELECOM directory has several files:**

- EF_{FDN} (6F3B) contains a phone book,
- EF_{SMS} (6F3C) contains a list of sent/received SMS,

etc.

These files are accessible in read/write and are protected by the PIN code of the user.

Access conditions to files

- **5 levels of priority :**

  ALWays (code 0) : the file is always accessible
  CHV1 (code 1) : file is protected by the PIN code of the user
  CHV2 (code 2) : file protected by the PIN code of the telecom operator
  ADM (codes de 4 to E) : file managed by the administrative authority
  NEVER (code F) : inaccessible file.

Level	Access conditions
0	ALWays
1	CHV1
2	CHV2
3	Réservé
4 à 14	ADM
15	NEver

Access conditions to files

ALWAYS : action executed without restriction ;

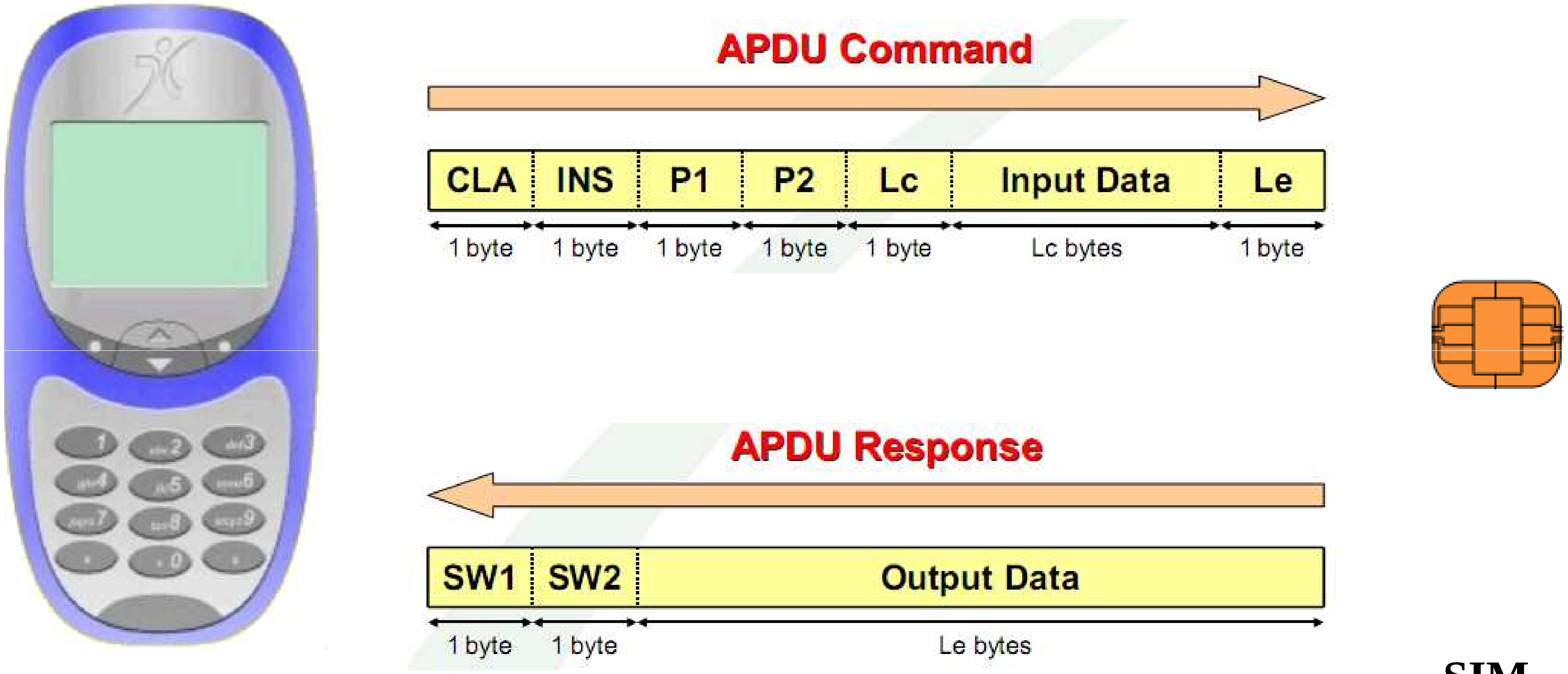
(**Card Holder Verification 1**) : the action is possible if the CHV1 has been presented to the SIM card successfully.

CHV2 : the action is possible if the CHV1 has been presented to the SIM card with successfully.

ADM : the attribution of these levels are under the responsability of the appropriate administrative authority.

NEVER : the action cannot be executed.

APDU commands



APDU Command

CLA	INS	P1	P2	Lc	Input Data	Le
1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	1 byte

APDU Response

SW1	SW2	Output Data
1 byte	1 byte	Le bytes

SIM

Mobile

APDU commands

The standard 3GPP TS 11.11 (ex-GSM 11.11) defines 22 APDU commands gathered in 4 groups :

➢ **Six commands of file management**: SELECT, READ, WRITE

➢ **Five commands of PIN code management** : verification, modification, activation, deletion and unlocking with PUK code.

➢ **Execution of** A3A8 algorithm thanks to the command RUN GSM ALGORITHM.

➢ **Ten different commands**, some are related to SIM Tool Kit such that a program executed on a SIM card may access to the keyboard or the screen of the mobile, or communicate via SMS with outside.

APDU commands

COMMAND	INS	P1	P2	P3
SELECT STATUS	A4 F2	00 00	00 00	02 Lgth
READ BINARY UPDATE BINARY READ RECORD UPDATE RECORD SEEK INCREASE	B0 D6 B2 DC A2 32	Offset high Offset high Rec N° Rec N° 00 00	Offset low Offset low Mode Mode Type/mode 00	lgth lgth lgth lgth lgth 03
VERIFY CHV CHANGE CHV DISABLE CHV ENABLE CHV UNBLOCK CHV	20 24 26 28 2C	00 00 00 00 00	CHV N° CHV N° 01 01 Voir note	08 10 08 08 10
INVALIDATE REHABILITATE	04 44	00 00	00 00	00 00
RUN GSM ALGORITHM	88	00	00	10
SLEEP	FA	00	00	00
GET RESPONSE TERMINAL PROFILE ENVELOPE FETCH TERMINAL RESPONSE	C0 10 C2 12 14	00 00 00 00 00	00 00 00 00 00	Lgth Lgth Lgth Lgth Lgth

SELECT command

`A0 A4 00 00 02 XX XX` (XX XX : FID of the file/directory).

When selecting a directory, a response may include the following information:

- Memory size not used
- The FID of the selected directory
- The type of the directory (MF or not)
- presentation of the PIN code
- Number of the sub-directories

Reading files

➢Reading the IMSI

The file EF_{IMSI} (6F07) of the GSM directory is transparent, it contains the IMSI. The selection of the file returns the size of the file.

A0 B0 00 00 09 (READ BINARY 9 bytes, size of the IMSI).

➢Reading the TMSI and LAI

These parameters are read from the file EF_{LOCI} (6F 7E)

A0 B0 00 00 B (READ BINARY 11 bytes, 4 bytes for TSMI followed by 5 bytes for LAI, ..)

Authentification algorithm

- **Execution of the authentication algorithm**

UN-GSM-ALGORITHM executes the function A3A8 with as an argument The random number RAND of 16 bytes. The command returns the signature SRES (4 bytes) and the key Kc (8 bytes).

- **Update of file EF$_{Kc}$**

The file EF$_{Kc}$ is updated by the mobile thanks to the command UPDATE BINARY . Two values are stored in the file: the key and a validation byte(=00 if the key is valide else 07).

Reading the table of Services

The file EF$_{\text{SIM-Service-Table}}$ (6F 38) contains the list of the services provided by the SIMcard. Each service is associated to two bits (bit1 =1 if service is present, bit2 =1 if the service is active).

Example :
Service n°1 allows the desactivation of the PIN code of the user,
Service n°2 indicates the presence of a speed dial directory(fichier EF$_{\text{ADN}}$),
Service n°3 notifies the presence of an unabridged directory numbers (fichier EF$_{\text{FDN}}$),
Service n°4 indicates the presence of SMS file (fichier EF$_{\text{SMS}}$),
etc.

The files **EF$_{\text{ADN}}$, EF$_{\text{FDN}}$, EF$_{\text{SMS}}$** belong to the directory DF$_{\text{TELECOM}}$ (7F 10).

The files directory and SMS

- **SMS file:**
  - EF$_{SMS}$, has 6F 3C as FID,
  - a cyclic file,
  - read/write SMS withi n the SIM card.

- **A contact-list file ADN**
  –EF$_{ADN}$ has 6F 3A as FID,
  - is a contact list.

Cmd: A0 A4 00 00 02 6F 3A (SELECT EF-ADN)
Resp: 9F 0F (the cards wants to send 0F data)
Cmd : A0 C0 00 00 0F (GET RESPONSE 0F bytes)
Resp: 00 00 **1B 58** 6F 3A 00 11 00 22 01 02 01 **1C** 90 00.

File size : 1B 58 (7 000 bytes) and record size (1C : 28 bytes).
The number of records : 7000/28=250 bytes).

Each number contains a label with a size of 14 (28-14=14). The label has 0 in the most significant bit.

Operations on PIN codes

PIN coded on 8 bytes. The non significant bytes are coded with FF.

- **VERIFY CHV** : presenting PIN code

A0 20 00 P2 0B **PIN** (P2=01 for CHV1 : user PIN code, = 02 for CHV2).

- **DISABLE PIN** cancels the use of PIN code.

A0 26 00 01 08 **PIN**

- **ENABLE PIN** allows using the PIN code

A0 28 00 01 08 **PIN**

- **CHANGE CHV** allows the modifiction of PIN code

A0 24 00 01 10 **Ancien_PIN Nouveau_PIN**

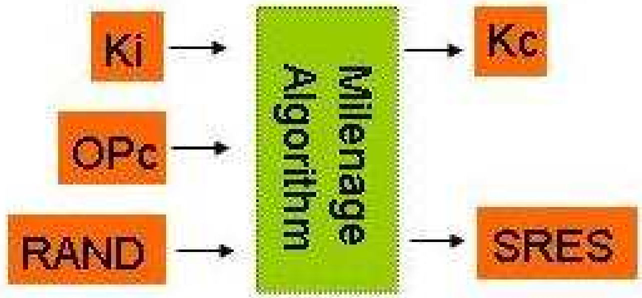
UNBLOCK CHV unlocks a blocked card after 3 three unsuccessful attempts
of the PIN code (CHV1).

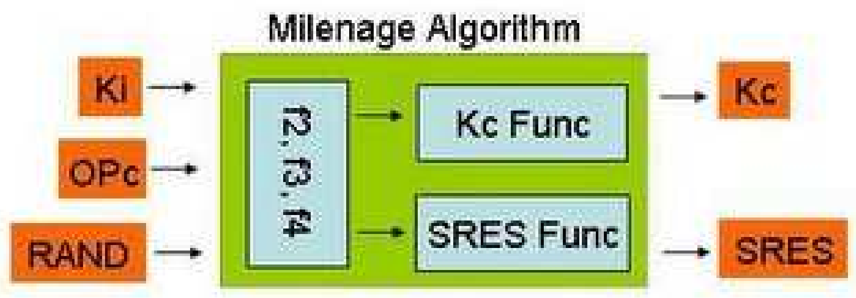
A0 2C 00 01 10 **PUK PIN** (**PUK** is a unique code of 8 bytes associated to the SIM card).

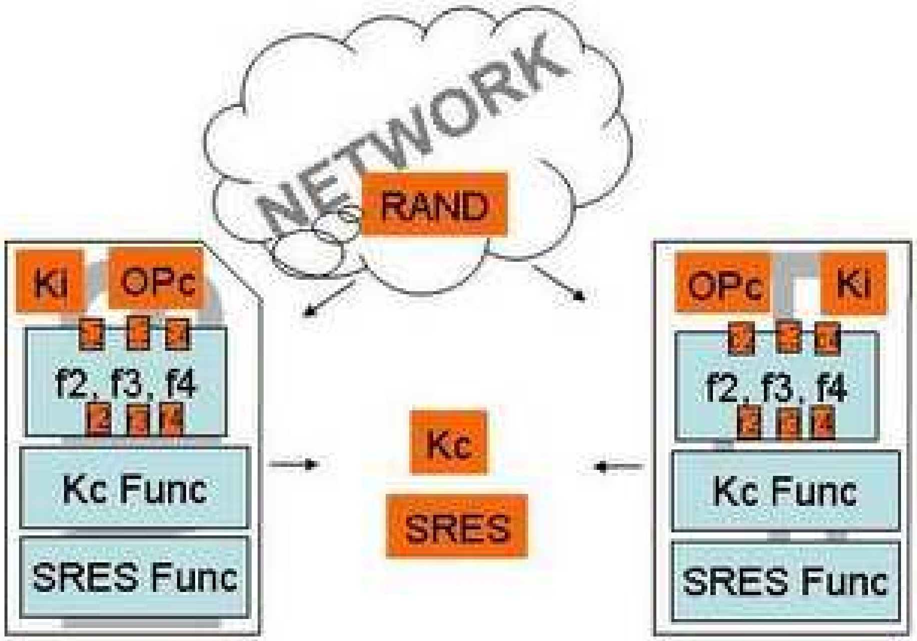
Comparison of the authentification SIM/USIM

GSM			UMTS		
Description	Bits	Alg	Description	Bits	Alg
Ki Subscriber authentication key	128		K Subscriber authentication key	128	
RAND random challenge	128		RAND random challenge	128	
XRES exepected result	32	A3	XRES expected result	32-128	f2
Kc cipher key	64 max	A8	Ck cipher key	128	f3
			IK integrity key	128	f4
			AK anonimity key	48	f5
			SQN sequence number	48	
			AMF authentication management field	16	
			MAC message auth. Code	64	f1
Example : algorithm COMP128-1			Example : algorithm Milenage		

« Milenage » Algorithm







SIM **ME**

SIM/USIM Comparison

Characteristics	SIM	USIM
Class used	CLA=’A0’	CLA=’00’
Root directory	MF (3F 00)	ADF USIM (7F FF)
Multiple channels support	No	Yes
Authentification command	RUN GSM ALGORITHM	AUTHENTICATE
Used with GSM	Yes	Yes
Used with 3G	Yes	Yes
SIM Toolkit	Yes	Yes
New standards	stopped	In progress
Versions	Release 1 à Release 4	Release 99 à Release 7

References

http://www.commentcamarche.net/contents/telephonie-mobile/gsm.php3

http://discobabu.blogspot.com/2006/02/gsm-milenage-implementing-it-at.html

Normes GSM : http://www.etsi.org

Article de Pascal Urien, « La carte SIM ou la sécurité du GSM par la pratique », Magazine MISC, hors Série « Cartes à puce », Nov. /Dec. 2008.

Article de Serge Chaumette et Jonathan Ouoba, « Java Card (U)SIM et Applications sécurisées sur téléphones mobiles », Magazine MISC, hors Série « Cartes à puce », Nov. /Dec. 2008.

Description des SMS : http://www.dreamfabric.com/sms/

Smart Card Handbook, Third Edition, Wolfgang Rankl and Wolfgang Effing, Giesecke & Devrient GmbH, Munich, Germany, Translated by Kenneth Cox, John Wiley & Sons, 2002.

Rapport de stage Niang Souleymane réalisé chez Trusted Logics, Master SEM, septembre 2008.

Keith E. Mayes and Konstantinos Markantonakis, Smart Cards, Tokens, Security and Applications, Springer, 2008, 392 pages.

3 GPP TS 11.14. Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipement interface (Release 1999).

3 GPP TS 11.11. Technical Specification Group Terminals Specification of the Subscriber Identity Module-ME interface (Release 1999).

3GPP TS 43.019 V6.0.0 (2004-12), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Terminals; Subscriber Identity Module Application Programming Interface, (SIM API) for Java Card™, Stage 2, (Release 6), http://www.3gpp.org

3GPP TS 51.014 V4.5.0 (2004-12), Technical Specification, 3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 4)

3GPP TS 51.011 V5.0.0 (2001-12), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, (Release 5)

ETSI SAGE Task Force for 3GPP, Authentication Function Algorithms, VERSION 1.0, Security Algorithms Group of Experts (SAGE); General Report on the Design, Specification and Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP, Authentication and Key Generation Functions, 2000 (http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_10/Docs/PDF/SP-000630.pdf).

3GPP TS 43.020 – Technical Specification Group Services & System Aspects; Security Related Network Functions (Release 5, 2002).

End