Advanced Card Systems Ltd.
Card & Reader Technologies

Subscriber Identity Module (SIM)

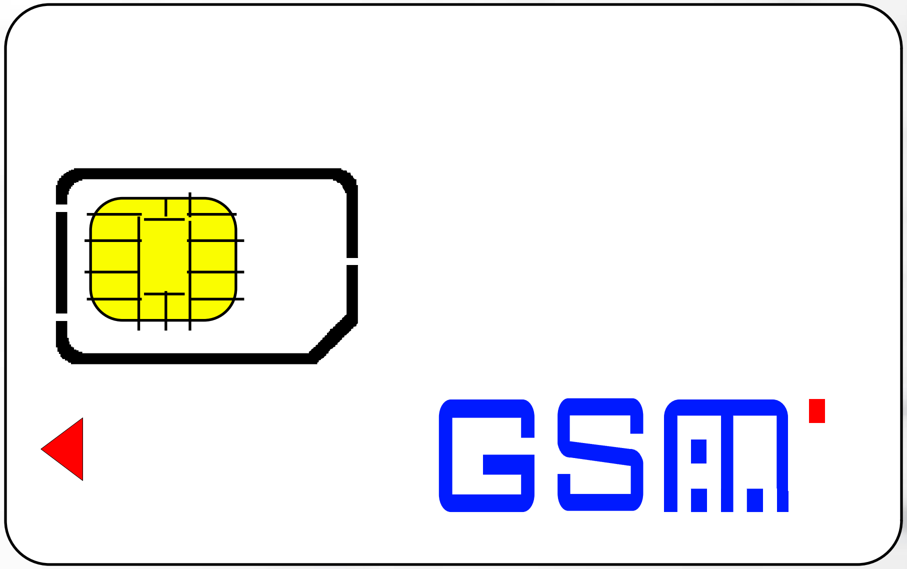
CARD & READER TECHNOLOGIES

SIM: Physical Characteristics

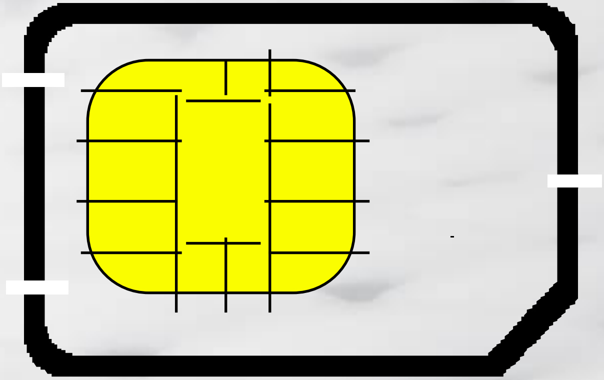
- ❑ Card Format
  - ISO 7816-1 format
  - Plug-in (GSM specific)
- ❑ Mechanical tolerance
  - Defined in ISO 7816-1 and 7816-2
- ❑ Thermal tolerance
  - Operation temp.: 25°C to +70°C
  - Occasional peaks max. temp.: +85°C

SIM

Recommendation 11.11 defines two GSM Card Dimensions



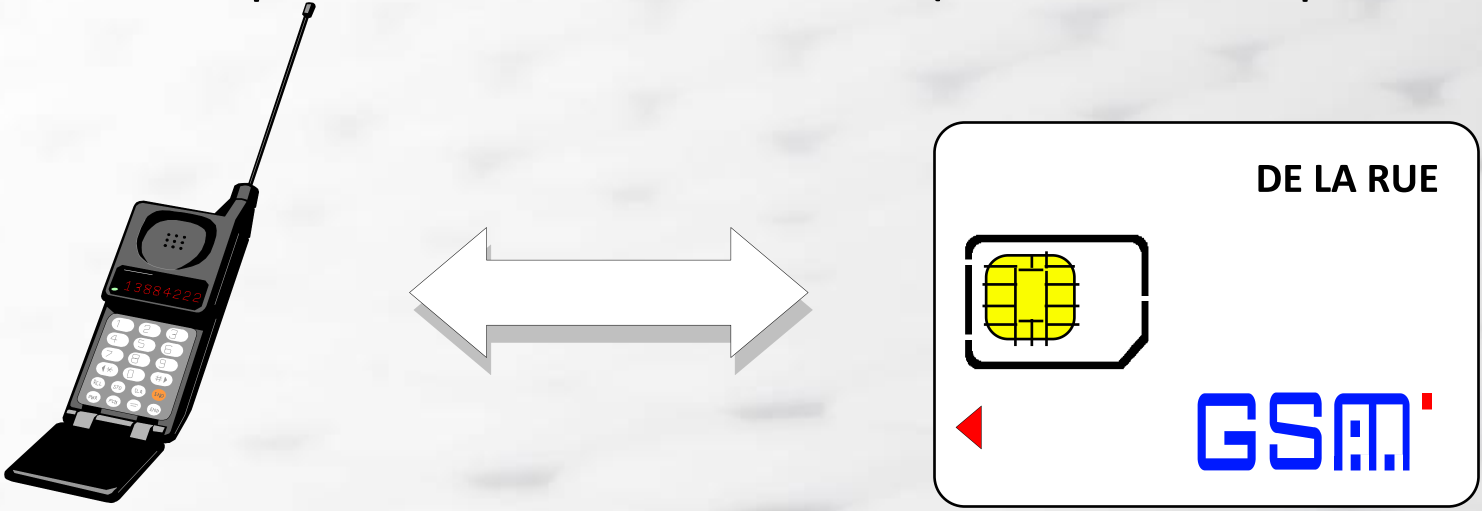
ISO dimension Card



Plug-in SIM

SIM: Mobile Equipment Interface

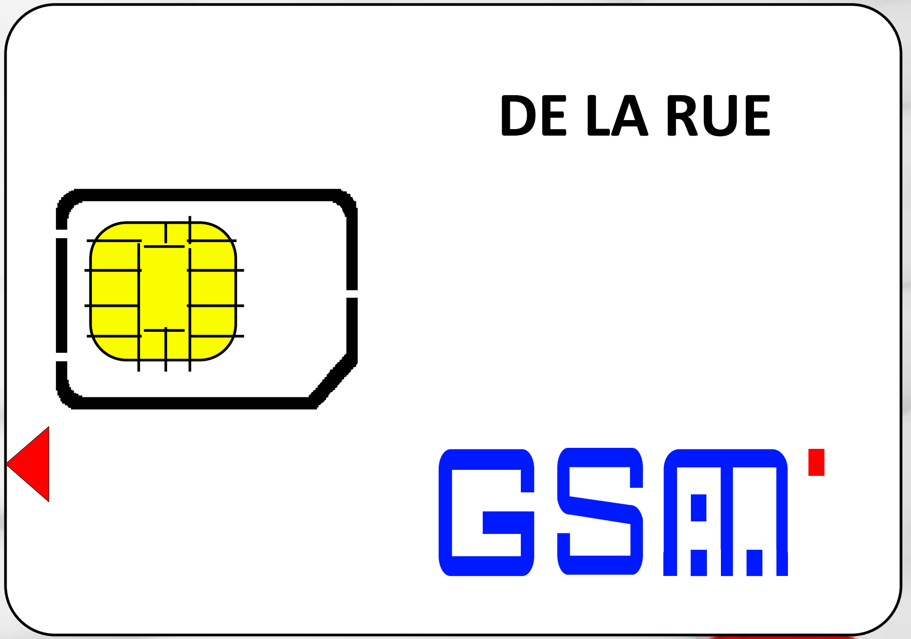
- Interface defined in GSM 11.11
  - Electrical Characteristics refers to ISO 7816-3
  - Communication Protocol is T=0 from ISO 7816-3
  - GSM Operational Instruction Set (ETSI/TE9 compatible)



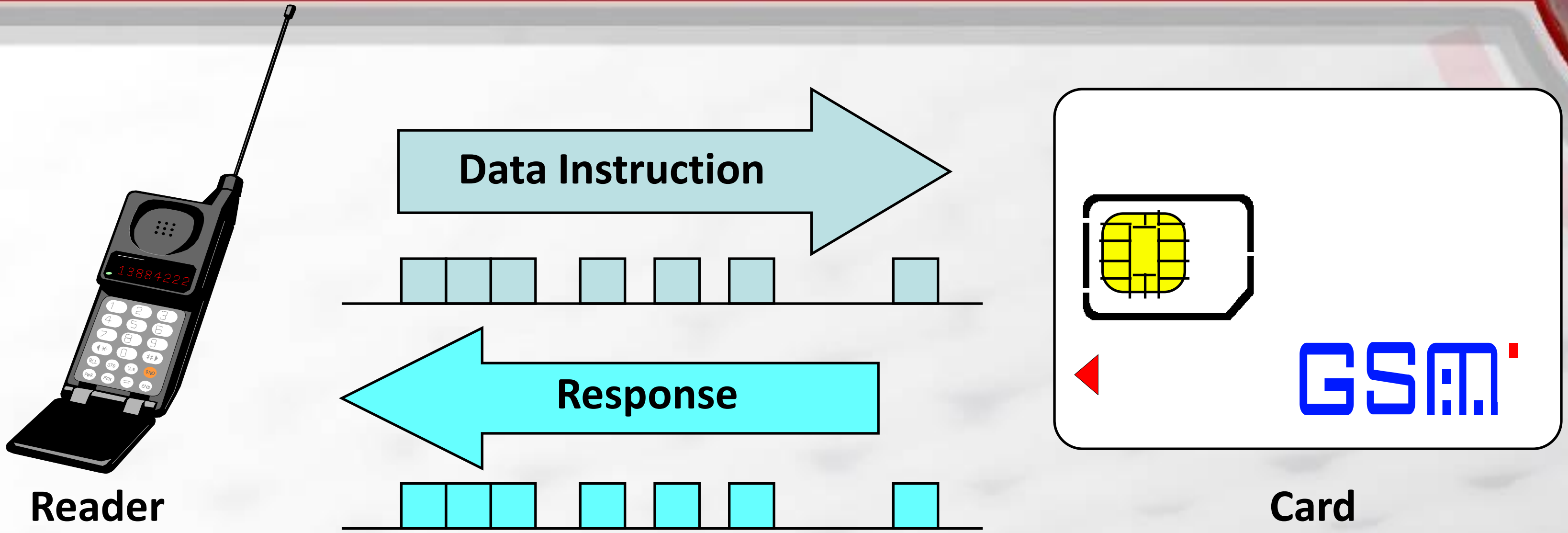
The Administrative Management of the SIM, including personalization and distribution, is not defined by GSM.

Summary: SIM Technical Description

- ❑ Memory Organization
- ❑ Data Organization
- ❑ Memory Management
- ❑ Security Management
- ❑ Commands



SIM: Instruction Format (ISO 7816-3 Protocol)



SENDING INSTRUCTION:

CLA: Instruction Class

‘A0’ is used in GSM application, all other values rejected by the Card.

INS: Instruction Code

P1, P2, P3: Instruction Parameters

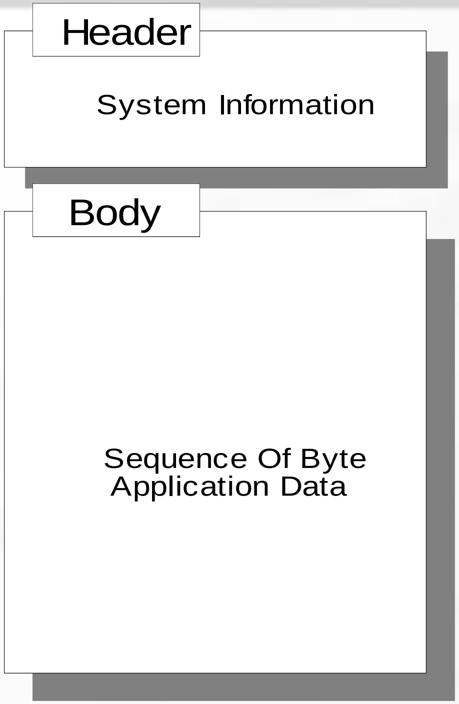
GSM SIM: GSM 11.11 Command Set

Commands	90 00	9F XX	92 0X	92 40	94 00	94 02	94 04	94 08	98 02	98 04	98 08	98 10	98 40	98 50	67 XX	6B XX	6D XX	6E XX
Select		*		*			*								*	*		*
Status	*			*											*	*		*
Update Binary	*		*	*	*			*		*		*			*	*		*
Update Record	*		*	*	*	*		*		*		*			*	*		*
Read Binary	*			*	*			*		*		*			*	*		*
Read Record	*			*	*	*		*		*		*			*	*		*
Seek	*	*		*	*		*	*		*		*			*	*		*
Increase		*	*	*	*			*		*		*		*	*	*		*
Verify CHV	*		*	*					*	*	*		*		*	*		*
Change CHV	*		*	*					*	*	*		*		*	*		*
Disable CHV	*		*	*					*	*	*		*		*	*		*
Enable CHV	*		*	*					*	*	*		*		*	*		*
Unblock CHV	*		*	*					*	*	*		*		*	*		*
Invalidate	*		*	*	*					*		*			*	*		*
Rehabilitate	*		*	*	*					*		*			*	*		*
Run GSM Algorithm		*		*				*		*					*	*		*
Sleep	*														*	*		*
Get Response	*			*											*	*		*

GSM SIM: Access Conditions

Access Condition	Meaning
0	Always / Free Access
1	CHV1(PIN1)
2	CHV2 (PIN2)
3	Reserve
4,5..E	ADM (GSM operator)
F	Never (impossible)

GSM SIM: File Type



Header

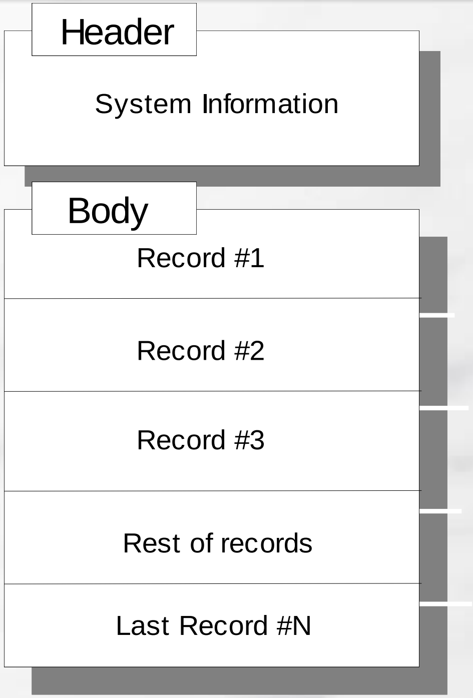
System Information

Body

Sequence Of Byte Application Data

Transparent File

File type 0



Header

System Information

Body

Record #1

Record #2

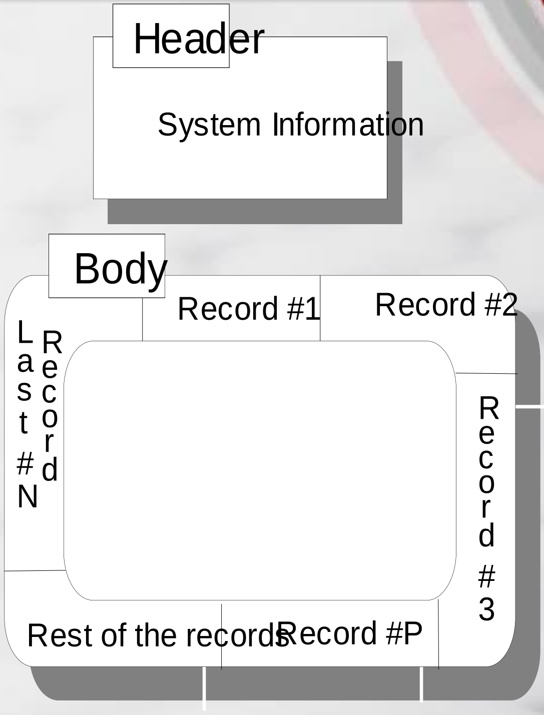
Record #3

Rest of records

Last Record #N

Linear File

File type 1



Header

System Information

Body

Record #1

Record #2

Record #3

Rest of the records

Record #P

Last Record #N

Cyclic File

File type 3

File Access Type

- **Read** - read (all EFs) or search a file (Linear)
- **Update** - update (all EFs)
- **Increase** - increase value in cyclic EF
- **Rehabitate** - reverse invalidated EF using Rehabitate command
- **Invalidate** - an invalidated EF (using Invalidate command) cannot be accessed
- Other types of access outside the GSM 11.11 specification
  - Delete, data-download, lock, etc.

GSM: Commands and Files

Function	MF	DF	EF transparent	EF linear fixed	EF cyclic
SELECT	*	*	*	*	*
STATUS	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
INCREASE					*
INVALIDATE			*	*	*
REHABILITATE			*	*	*

Change CHV

CLA	INS	P1	P2	Lin	Data-in
A0	24	00	CHV#	10	old_CHV(8) new_CHV(8)

CHV# : 01 for CHV1; 02 for CHV2

*Note:

1. if CHV < 8 bytes, pad ‘FF’

2. CHV must not be blocked or disabled

Disable CHV

CLA	INS	P1	P2	Lin	Data-in
A0	26	00	01	08	CHV1

*Note:

1. if CHV1 < 8 bytes, pad ‘FF’

2. CHV1 must already be verified

3. CHV1 must not be blocked or already disabled

Enable CHV

CLA	INS	P1	P2	Lin	Data-in
A0	28	00	01	08	CHV1

*Note:

1. if CHV1 < 8 bytes, pad ‘FF’

2. CHV1 must already be disabled

3. CHV1 must not be blocked or already disabled

Get Response

CLA	INS	P1	P2	Lout	Data-out
A0	C0	00	00	LL	response_data

*Note:

1. Response data depends on preceding command:

   Run GSM Algo, Seek, Select, Increase returning 9F LL

2. Response data is lost if not immediately retrieved

3. Allowed as the first command after ATR

Increase

CLA	INS	P1	P2	Lin	Data-in
A0	32	00	00	03	increment_value

*Note:

1. Current EF selected must be cyclic EF

2. Current EF must not be invalidated

3. Increase access right must be achieved

4. Used to increment ACM EF

Invalidate

CLA	INS	P1	P2	Lin
A0	04	00	00	00

*Note:

1. Invalidate access right must be achieved

2. Current EF should exist and not already invalidated

3. Only Select and Rehabitate commands are allowed after an EF is invalidated

4. Used in ME to invalidate IMSI & ADN

Read Binary

CLA	INS	P1	P2	Lout	Data-out
A0	B0	Hi_offset	Lo_offset	Lout	data

*Note:

1. Last selected file must be a transparent file

2. Read access must be fulfilled

3. P1 P2 must be within EF boundary

4. P1 P2 + Lout must be < file size

Read Record

CLA	INS	P1	P2	Lout	Data-out
A0	B2	01=current	04	rec_length	data
		02-FF = rec#	04		
		xx	01=1st rec		
		xx	02=last rec		
		xx	03=previous		

*Note:

1. Last selected file must be a record file

2. Read access must be fulfilled

3. Lout must be record length

Rehabitate

CLA	INS	P1	P2	Lin
A0	44	00	00	00

***Note:**

1. A file must be selected

2. Selected file must already be invalidated

3. Rehabitate condition must be fulfilled

Run GSM Algorithm

CLA	INS	P1	P2	Lin	Data-in
A0	88	00	00	10	random#

*Note:

1.CHV1 must be disabled or verified

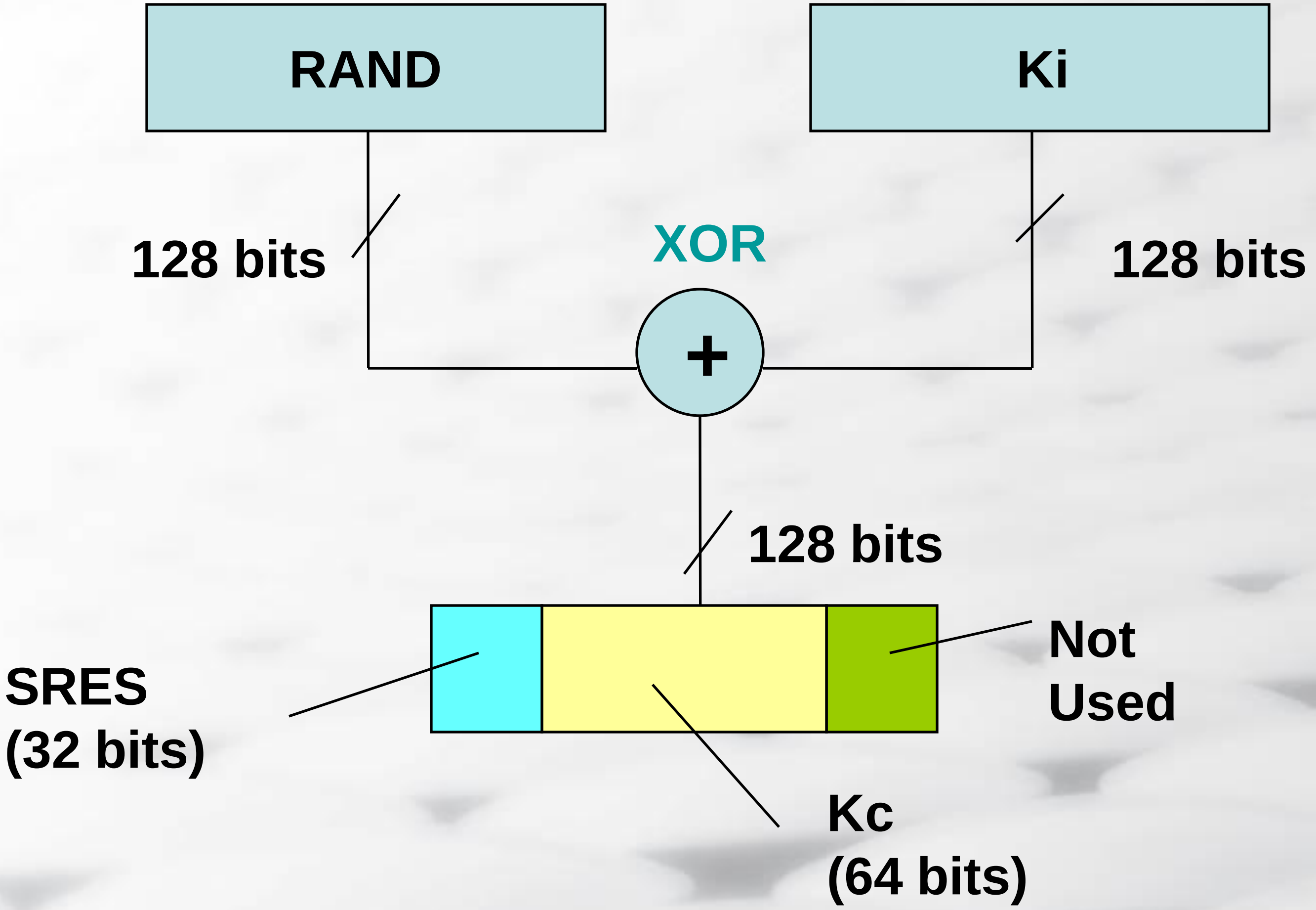
2.Current DF must be 7F20 or 7F21

3.Ki must be defined

4.12 bytes response = return cryptogram(4) + Kc(8), lost if Get Response is not issued as the subsequent command

Test Algorithm

The test algorithm employs bit-wise modulo 2 addition:



Seek

CLA	INS	P1	P2		Lin	Data-in
A0	A2	00	type | mode	Lin	pattern_to_seek	

t0 = from beginning forward

t1 = from end backward

t2 = from previous location, backward

t=0 (type 1), SW1 SW2 = 9000 if successful

t=1 (type 2), SW1 SW2 = 9F01 if successful, Get Response returns the current record

*Note:

1. Current EF must be linear or cyclic

2. Read access must be fulfilled

Select

CLA	INS	P1	P2	Lin	Data-in
A0	A4	00	00	02	DF ID / EF ID

*Note:

1. DF ID = 3F00, 7F10, 7F20 (or 7F21 phase 1 PCN)

Get Response returns free space in MF/DF, # child DF, #child EF, status of CHV, PUK1, CHV2, PUK2

2. Select EF Get Response returns EF type, size, access conditions and file status

Status

CLA	INS	P1	P2	Lout	Data-out
A0	F2	00	00	LL	data

*Note:

1.Used to retrieve the current context of the SIM

2.Return data becomes the same as Get Response after a Select command

3.If current file is MF/DF, returns free space in MF/DF, # child DF, #child EF, status of CHV, PUK1, CHV2, PUK2

4.If current file is EF, returns EF type, size, access conditions and file status

5.67 LL error code returns the correct length, LL

Unblock Code

CLA	INS	P1	P2	Lin	Data-in
A0	2C	00	CHV#	10	PUK(8) CHV(8)

CHV# : 00 = CHV1, 02 = CHV2

*Note:

1. PUK must not be blocked

2. PUK must be correct

Update Binary

CLA	INS	P1	P2	Lin	Data-in
A0	D6	Hi_offset	Lo_offset	Lin	data

*Note:

1. Last selected file must be a transparent file

2. Update access must be fulfilled

3. P1 P2 must be within EF boundary

4. P1 P2 + Lout must be < file size

Update Record

CLA	INS	P1	P2	Lin	Data-in
A0	DC	01=current	04	rec_length	data
		02-FF = rec#	04		
		xx	01=1st rec		
		xx	02=last rec		
		xx	03=previous		

*Note:

1. Last selected file must be a record file

2. Update access must be fulfilled

3. Lout must be record length

Verify CHV

CLA	INS	P1	P2	Lin	Data-in
A0	20	00	CHV# 08	CHV	

CHV# = 1 for CHV1

CHV# = 2 for CHV2

*Note:

1. If CHV1, it must not be disabled
2. CHV must not be blocked
3. CHV must be numeric,(eg. ‘30’ to ‘39’)
4. If CHV is < 8 bytes, pad with ‘FF’

SIM: Administrative Commands

- ❑ Administrative Commands refer to commands for personalizing the card
- ❑ SIM administrative commands are proprietary
- ❑ Most vendors follow ETSI TE9, but there is still no universal compatibility
- ❑ Perso System needs to cater to each card vendor of GSM, SIM & COS

*Note: The following commands illustrate the Administrative commands from De La Rue / Oberthur

Create Binary

CLA	INS	P1	P2	Lin	Data-in
A0	EA	00	00	Lin(<20)	EF content

*Note:

1. Current file must be transparent EF
2. Create access right must be achieved
3. EF must not be invalidated

Create File

Create File

Command description.

The CREATE FILE instruction allows the creation of a new Elementary File or a new directory under the Current Directory.
Sub-directories or EFs are added to the current directory until the maximum number of entries (given at its creation) is reached. In addition, the operating system verifies that the File Identifier is consistent with the file selection rules.
When creating a DF, the operating system checks if the maximum number of levels allowed is not exceeded.

At creation, the memory space (Max. number of entries for directory, Max. number of bytes for Transparent EFs, Max. number of records for Linear Fixed or Cyclic EFs) requested for the newly created file is allocated. When the memory space available in the card is insufficient, the creation fails.

Create File

The following table gives the memory size allocated depending on the File type:

File Type	Allocated Size
DF	(Max. number of entries) * 16
Transparent EF	Max. number of bytes
Linear Fixed EF	If lock record is available for this file: (Max. number of records) * (record length) +1) [1] If lock record is not available for this file : (Max. number of records)* (record length)
Cyclic EF	(Max. number of records) * (record length +1) [2]

When creating an DF, P1 and P2 must be equal to zero.
When creating an EF, 3 modes are available:

- **CREATE FILE Type 1**: the OS creates an already filled file (used length for transparent EFs or used number of records set to the maximum values).
- **CREATE FILE Type 2**: the OS creates an empty file (used length or used number of records set to zero).
- **CREATE FILE Type 3**: The OS creates an already filled file and initializes the first byte of each record to '00' value and the other bytes to 'FF'. This mode is specially designed for initialisation of EF_SMS at personalisation time.

Create File

The following table gives compatibility of creation mode against EF type:

	Transparent EF	Linear fixed EF	Cyclic EF
Type 1	√	√	√
Type 2	√	√	
Type 3		√	√

Table 1: Creation modes available.

The physical memory space for the created file is initialised by the filling pattern given in P1 command parameter. This is done whatever the mode used.

☞ **Note:** when the filling pattern matches the content of the EEPROM memory location, no writing occurs.

☞ **Note:** When a file has been successfully created, it is not automatically selected. So it is mandatory to use a SELECT instruction before working with the newly created file.

Prerequisites.

- The last selected File must be a Directory.
- The AC for the CREATE group must be fulfilled.
- The Directory should not be invalidated.

[1] The system area (one byte per record) which contains the locks, is allocated at the end of the file.

[1] The system area (one byte per record) which permits to determine the first record, is allocated at the end of the file.

Create Record

Create Record

Command description.

The CREATE RECORD instruction allows the appending of a record (and to fill it) at the logical end of a Linear Fixed EF.

Records may be appended until the Max. number of records is reached.

After a create record operation, the Current Record is not modified.

Prerequisites.

- The last selected File must be a Linear Fixed EF.
- The AC for the CREATE group must be fulfilled.
- The EF should not be invalidated.
- The maximum number of records should not be reached.

Delete File

Delete File

Command description

This instruction allows the deletion of the specified EF within the current directory and at the condition it is the last created EFwithin the card.

It is not required to select the EF prior the Delete File instruction.

The last selected file remains the current one except when the EF to be deleted is the current one; in this case, after instruction execution, the current file will be changed to the parent DF of the deleted EF.

The EEPROM memory area used by the deleted EF becomes free to create an other file.

☞ **Note:** After deletion, the file created before the deleted file becomes the last created file and thus the delete process can be repeated several times up to the point the last created file is a DF.

☞ **Note:** During data download, if the commands script contents a DELETE FILE command for the SMS file, the status 6F00 is returned.

Prerequisites

- The AC for the Delete group of the parent directory must be fulfilled.

Read Directory

Read Directory

Command description.

The READ DIRECTORY instruction is used to retrieve File headers from the Directory File selected by the last select instruction.

Since a Directory File has the same structure as a Linear Fixed EF, the file header is accessed according to addressing modes described in the chapter "Addressing EFs"

Prerequisites.

- The last selected File must be a Directory (MF or DF).
- The AC for the READ group must be fulfilled.

Lock

Write lock (for SLE44C160S)

Command description

This instruction allows to write the locks in the Protected area.

All the locks for the SLE44C160S described in the following chapter are used. To set a binary lock, the data send has to be equal to FFh. Once a binary lock has been set, it is not allowed to change it.

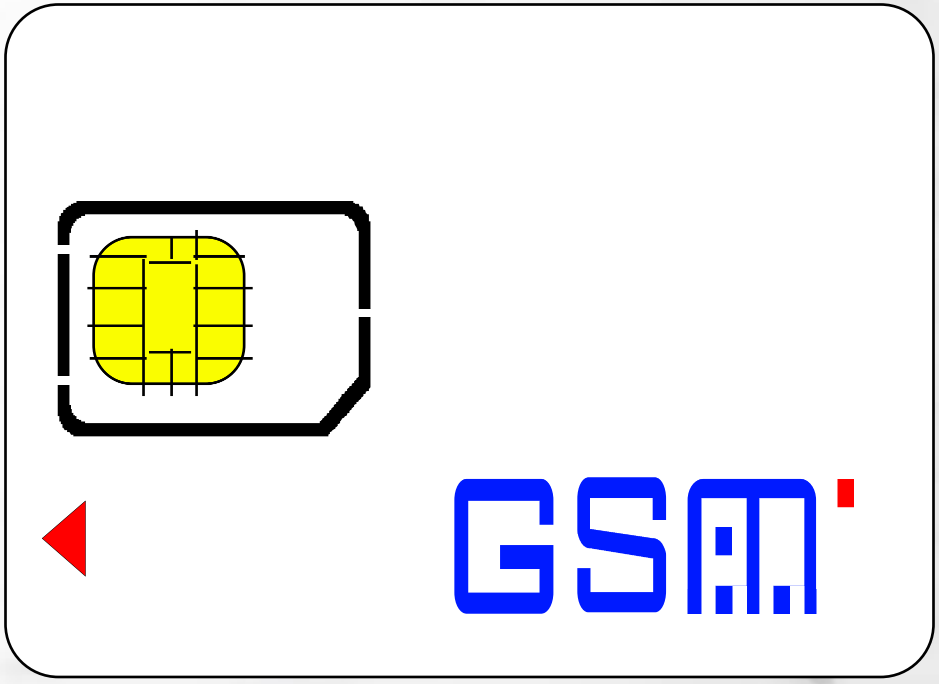
It is allowed to change Vst1,Vst2 and Vg.

The lock Vi allows to protect the locks against erasure.

Prerequisites

- This command is under control of the issuer code ISC1.

GSM SIM



Mobile Phone Services

ph1

- PLMN selection
- Abbreviated Dialling
- Short Messages
- Capability Configuration Parameters

ph1+

Language Preference

MSISDN storage

PLMN Selection
Abbreviated Dialing
Short Messages
Capability Configuration Parameters

ph2

- Language Preference
- Price Unit Currency Table
- MSISDN storage
- Call charge unit storage (AOC)
- Fixed Number Dialling
- Last Number Dialled

GSM SIM

- MF DF ID is 3F00
- DF Telecom ID is 7F10
- DF GSM ID is 7F20, however for phase 1 PCN (DCS1800), the DF ID is 7F21 and the GSM 900 DF ID is 7F20
- SIM COS usually implements automatic directory routing into 7F20 if 7F21 is selected
- File type MF=01, DF=02, EF = 04

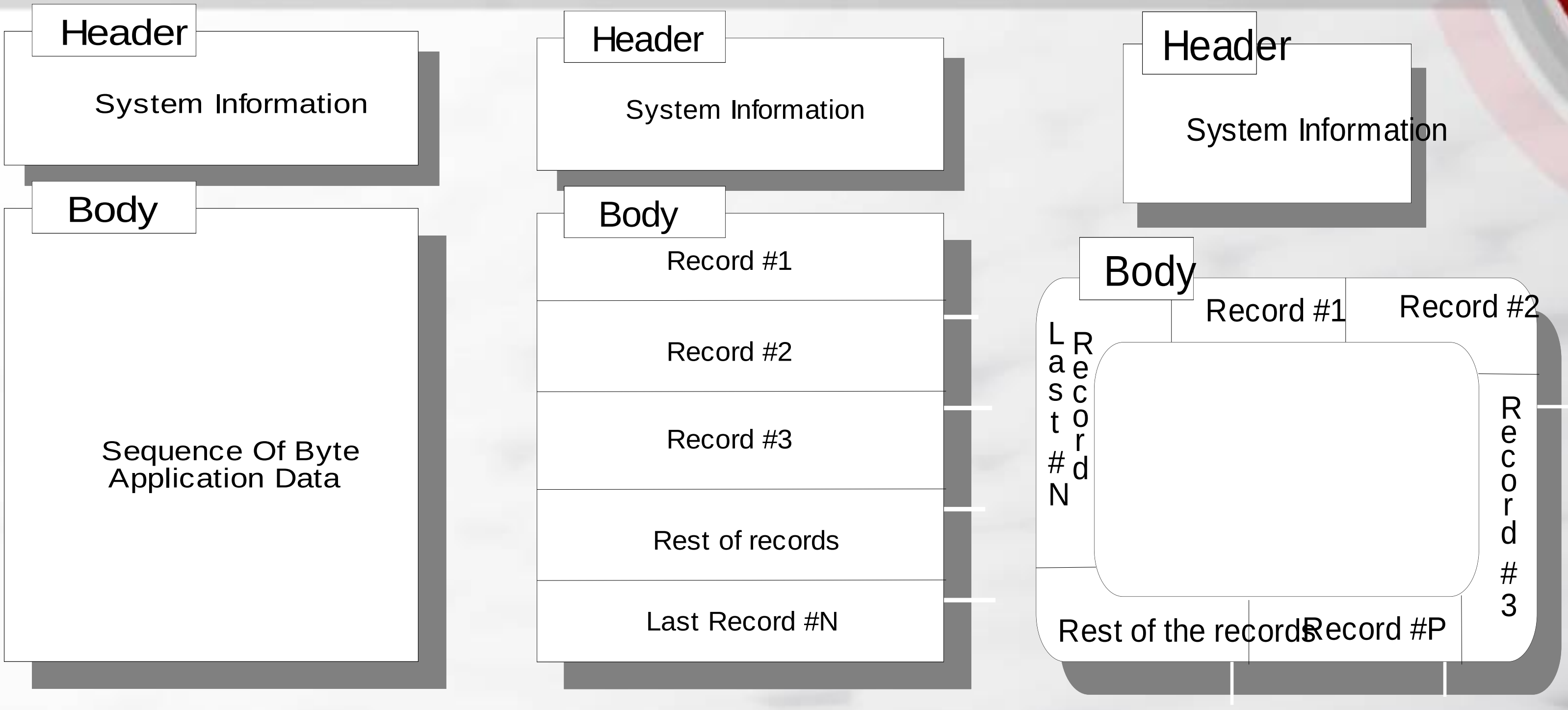
GSM SIM: GSM 11.11 Command Set

Commands	90 00	9F XX	92 0X	92 40	94 00	94 02	94 04	94 08	98 02	98 04	98 08	98 10	98 40	98 50	67 XX	6B XX	6D XX	6E XX	6F XX
Select		*		*			*								*	*		*	*
Status	*			*											*	*		*	*
Update Binary	*		*	*	*			*		*		*			*	*		*	*
Update Record	*		*	*	*	*		*		*		*			*	*		*	*
Read Binary	*			*	*			*		*		*			*	*		*	*
Read Record	*			*	*	*		*		*		*			*	*		*	*
Seek	*	*		*	*		*	*		*		*			*	*		*	*
Increase		*	*	*	*			*		*		*		*	*	*		*	*
Verify CHV	*		*	*					*	*	*		*		*	*		*	*
Change CHV	*		*	*					*	*	*		*		*	*		*	*
Disable CHV	*		*	*					*	*	*		*		*	*		*	*
Enable CHV	*		*	*					*	*	*		*		*	*		*	*
Unblock CHV	*		*	*					*	*	*		*		*	*		*	*
Invalidate	*		*	*	*					*		*			*	*		*	*
Rehabilitate	*		*	*	*					*		*			*	*		*	*
Run GSM Algorithm		*		*				*		*					*	*		*	*
Sleep	*														*	*		*	*
Get Response	*			*											*	*		*	*

GSM SIM: Access Conditions

Access Condition	Meaning
0	Always / Free Access
1	CHV1(PIN1)
2	CHV2 (PIN2)
3	Reserve
4,5..E	ADM (GSM operator)
F	Never (impossible)

GSM SIM: File Type



Transparent File **Linear File** **Cyclic File**

File type 0 **File type 1** **File type 3**

GSM SIM: File Access Type

- **Read** - read (all EFs) or search a file (Linear)
- **Update** - update (all EFs)
- **Increase** - increase value in cyclic EF
- **Rehabitate** - reverse invalidated EF using Rehabitate command
- **Invalidate** - an invalidated EF (using Invalidate command) cannot be accessed
- Other types of access outside the GSM 11.11 specification
  - Delete, data-download, lock, etc.

GSM: Related Algorithm

- ❑ A3 is the card authentication algorithm
- ❑ A8 is the algorithm to compute session key Kc
- ❑ A5 is the algorithm to cipher voice data with Kc
- ❑ A3A8 algorithm is usually COM-128, if the operator is a signatory of GSM MOU, sometimes called MOU algorithm
- ❑ XOR or dummy algorithm used otherwise
- ❑ A4 is the algorithm to cipher Ki, using DES
- ❑ K4 is the key used by A4

GSM SIM: Commands & Files

Function	MF	DF	EF transparent	EF linear fixed	EF cyclic
SELECT	*	*	*	*	*
STATUS	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
INCREASE					*
INVALIDATE			*	*	*
REHABILITATE			*	*	*

GSM SIM: MF & Telecom DF

MF	File Id	Description	Type	Size	Value
0F44	'2F E2'	ICC identification	M, T	10	89-CC-nn..nn
Telecom DF					
1244	'6F 3B'	Fixed dialling numbers	O,L	(X+14)*n	'FF...FF'
1144	'6F 3C'	Short messages	0,L	176*n	'00FF...FF'
1144	'6F 3D'	Capability configuration	O,L	14	'FF...FF'
1144	'6F 40'	MSISDN storage	O,L	(X+14)*n	'FF...FF'
1144	'6F 42'	SMS parameters	O,L	(28+Y)	'FF...FF'
1144	'6F 43'	SMS status	O,T	2+X	'FF...FF'
1144	'6F 44'	Last number dialled	O,C	(X+14)*n	'FF...FF'
1144	'6F 4A'	Extension 1	O,L	13*n	'FF...FF'
1244	'6F 4B'	Extension 2	O,L	13*n	'FF...FF'

GSM SIM: GSM DF

GSM DF	File Id	Description	Type	Size	Value
0144	'6F 05'	Language preference	M,T	1 - n	'FF'
1441	'6F 07'	IMSI	M,T	9	mcc-mnc-msin
1144	'6F 20'	Ciphering key Kc	M,T	9	'FF...FF07'
1144	'6F 30'	PLMN selector	O,T	3n (n>=8)	'FF...FF'
1444	'6F 31'	HPLMN search period	M,T	1	'FF'
1144/1244	'6F 37'	ACM maximum value	O,T	3	'000000'
1444	'6F 38'	SIM service table	M,T	X (x>=2)	operator dependant
11144/11244	'6F 39'	Accumulated call meter	O,C	3	'000000'
1444	'6F 3E'	Group identifier level 1	O,T	1 - n	operator dependant
1444	'6F 3F'	Group identifier level 2	O,T	1 – n	operator dependant
1144/1244	'6F 41'	PUCT	O,T	5	'FFFFFF0000'
1144	'6F 45'	CBMI	O,T	2n	'FF...FF'
0444	'6F 46'	Service provider name	O.T	17	'FF...FF'
1144	'6F 74'	BCCH	M,T	16	'FF...FF'
1444	'6F 78'	Access control class	M,T	2	Last digit of IMSI
1144	'6F 7B'	Forbidden PLMNs	M,T	12	'FF...FF'
1141	'6F 7E	Location information	M,T	11	'FFFFFFFFxxFxxx0000FF01'
0444	'6F AD'	Administrative data	M,T	3+x	operator dependant (000000)
0444	'6F AE'	Phase identification	M,T	1	01,02,03 for phase 1,2,2+
1122	'6F 3A'	Abbreviated dialling #	O,L	(X+14)*n	'FF...FF'

ICC ID, EFID 2FE2

- ICCID may be 18 digit, 18+L, 19 or 19+L
- If ICC ID is less than 20 digits, pad F
- L is Luhn, a check digit
- Format is 89 CC nnn...nn, where CC = IDD country code, and n..n is defined by the operator
- ICC ID is not used by GSM; it is only for operator SIM management purposes
- Internally in SIM, digit is swapped (e.g. ICC ID 8965029903160027502 is coded as 985620993061007205F2)

Language Preference EFLP – 6F05

00	German
01	English
02	Italian
03	French
04	Spanish
05	Dutch
06	Swedish
07	Danish
08	Portuguese
09	Finnish
0A	Norwegian
0B	Greek
0C	Turkish
0F	Chinese

Default = FF..FF

EF6F07 – IMSI

- The International Mobile Subscriber ID comprises MCC-MNC-MSIN
  - MCC - mobile country code, 3 digit
  - MNC - mobile network code, 2 digit
  - MSIN - an HLR number followed by a sequence number
  - IMSI is 15 digits, if otherwise, pad with F
- MCC-MNC is the PLMN
- Internally in SIM, digits are swapped - 08x9xxxxxxxxxxxxx, (e.g. 525026401057750 is coded as 085952204610507705)

EF6F30 – PLMN Selector

- PLMN = MCC(3 digits) + MNC(2 digits)
- Internally in SIM, digits are swapped (e.g. suppose the PLMN is 246-81, it is coded as 42F618)
- TMSI-LAI, EF 6F7E also require PLMN coding as described
- 1st entry is the highest priority
- Used during automatic PLMN selection mode

EF6F38 – SIM Service Table

1. **CHV disable**
2. **ADN**
3. **FDN**
4. **SMS**
5. **AoC**
6. **CCP**
7. **PLMN**
8. **RFU**
9. **MSISDN**
10. **Ext 1**
11. **Ext 2**
12. **SMS Parameters**
13. **LDN**
14. **Cell Broadcast Msg ID**
15. **Group ID Level 1**
16. **Group ID Level 2**
17. **Service Provide Name**

- Byte 1, bit 0 = service 1; 0 not allocated, 1 allocated
- Bit 1 = service 1; 0 = not activated, 1=activated
- And so on...

EF6F78 – Access Control Class

- 2 bytes (16 bits) of data represent 10 classes of normal subscribers & 5 classes of high priority users - operator, police, etc.
- 10 classes represented by bit 0 to bit 9 are randomly allocated
- The usual practice is to use the last digit of the IMSI to select the bit number to be set to 1
- Example values: 0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200

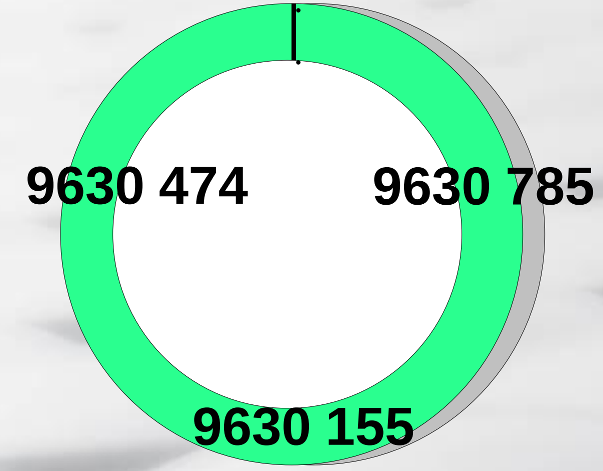
MSISDN

- Subscriber telephone number
- Can be displayed by the mobile
- Can store several numbers
- The subscriber can get a new SIM and keep the same number
- The subscriber can ask to change the MSISDN and keep the same card

Stored in the card for information only

LND: Last Number Dialed

- The phone stores the LND in a cyclic file of the SIM
- The subscriber uses a speed dialing mode to dial out the LND
- The oldest LND is overwritten when there is no more empty record



FDN: Fixed Dialing Numbers

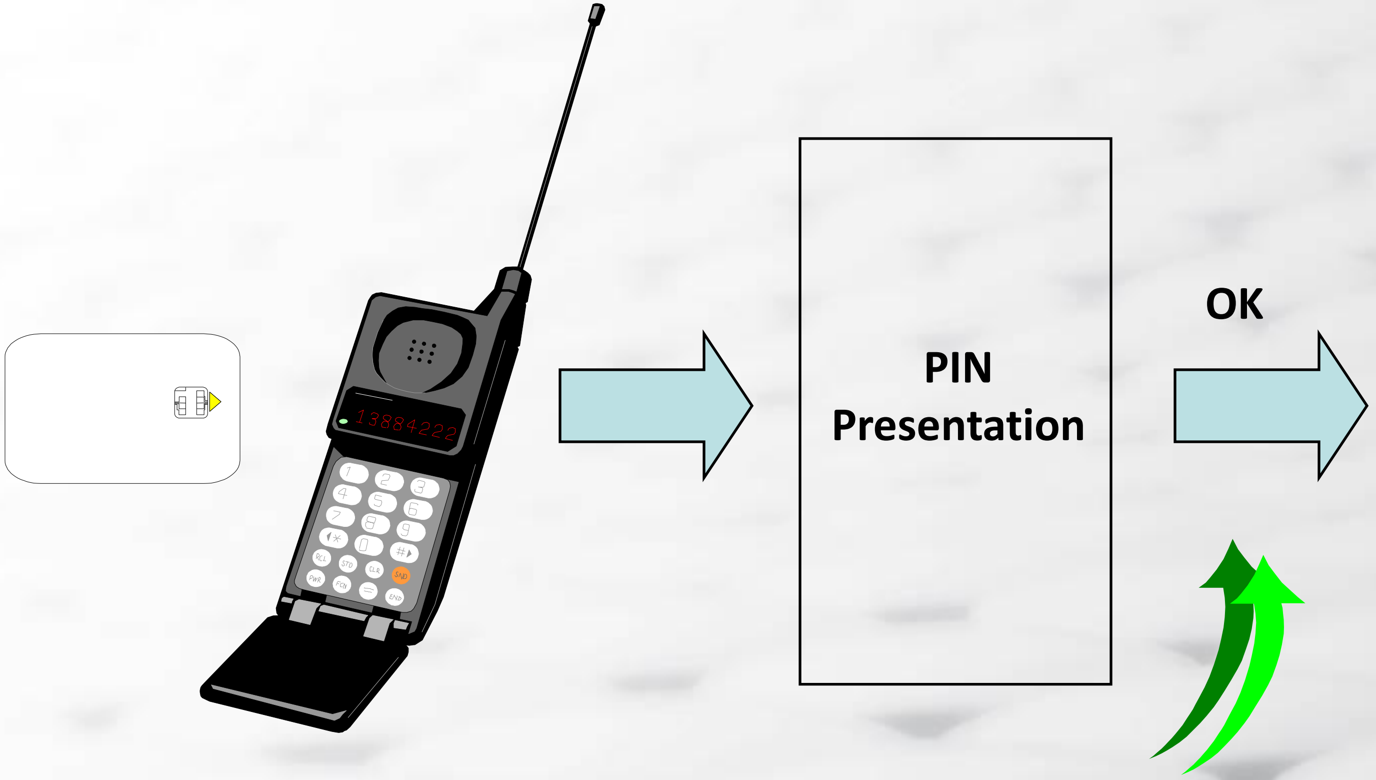
- ❑ Restrict the outgoing numbers to a list
- ❑ No restriction for the incoming calls
- ❑ A SIM card with the FDN activated doesn't work if the mobile doesn't support the feature.

Controlled by PIN2

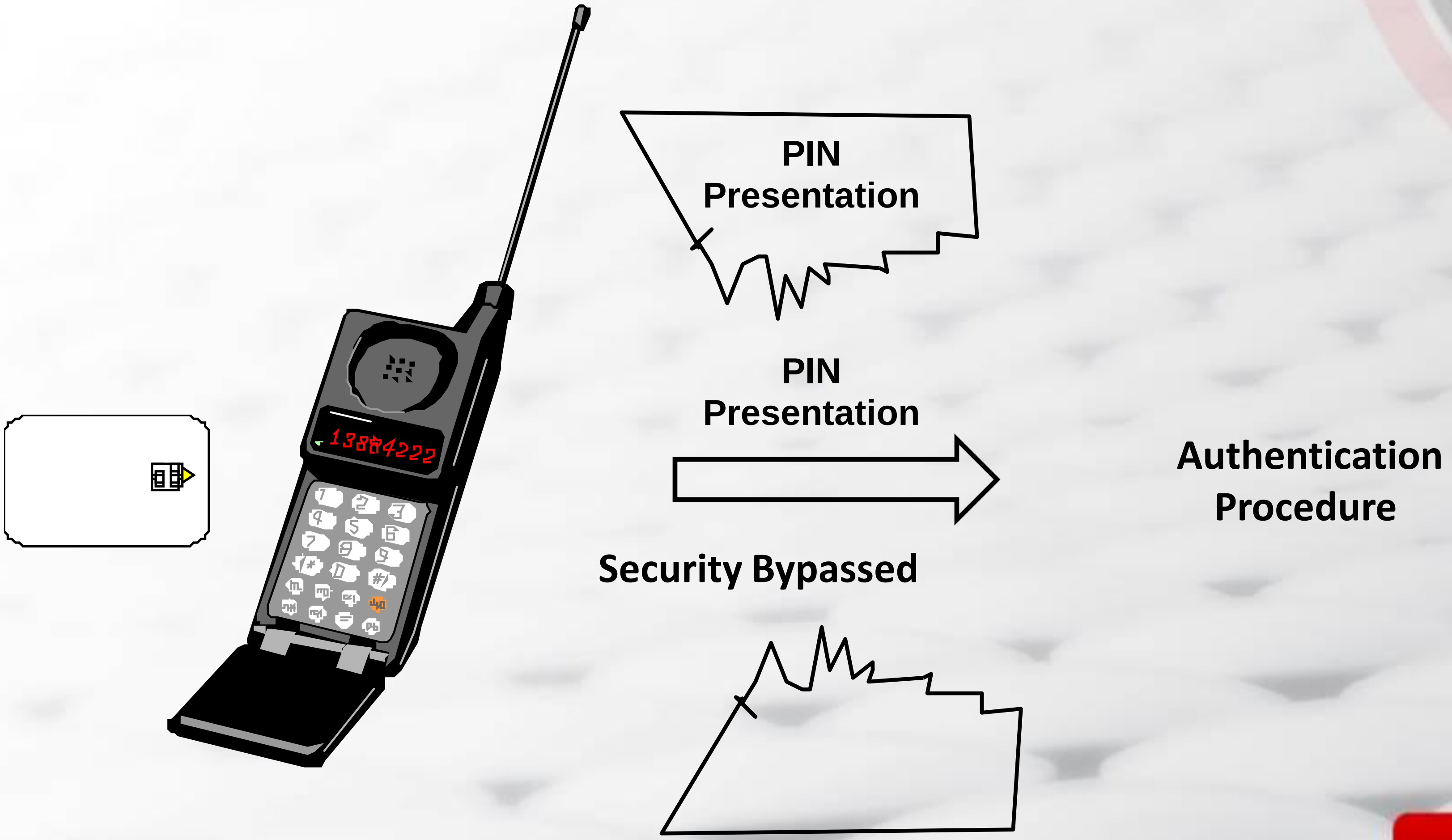
Dialing Number

- Stored in linear file, record length = X+14
- X is alphanumeric tag length, may be 0
- 14 bytes comprises:
  - 1 byte - length
  - 1 byte - 81
  - 10 bytes - telephone #, swapped & padded with F if less than 20 digits
  - 1 byte - FF, if capability configuration is not used
  - 1 byte – record number of the extension file, or FF, if not used

PIN Code Enabled



PIN Code Disabled



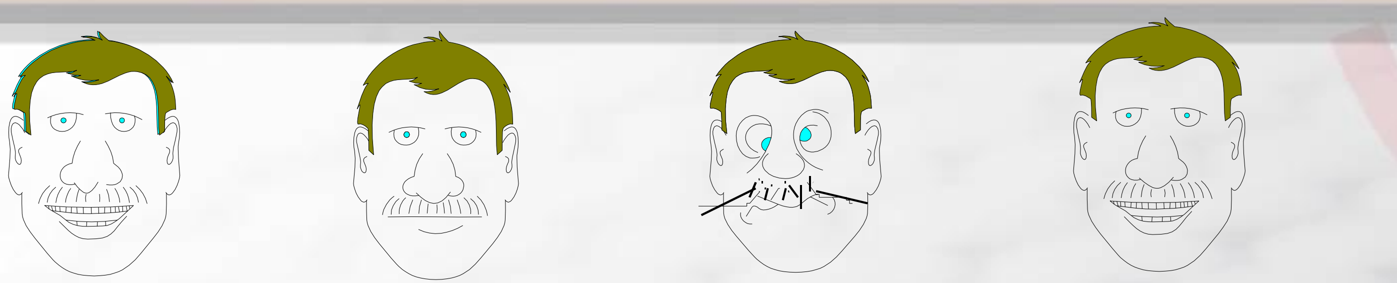
PIN Presentation

PIN Presentation

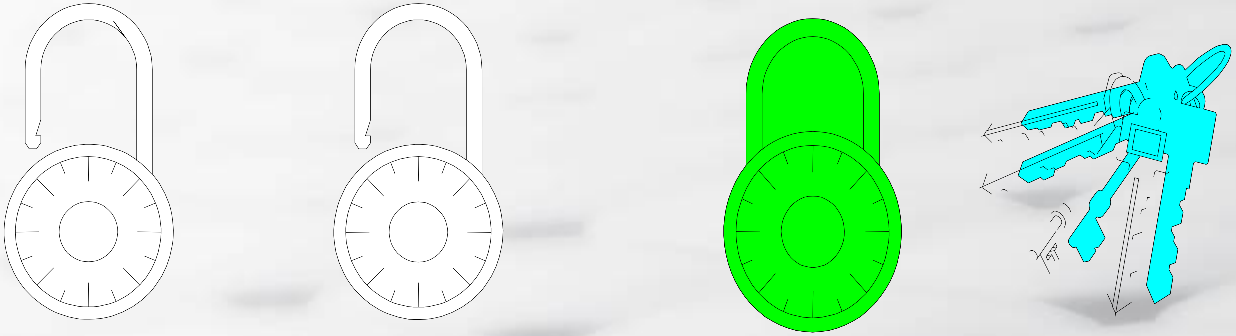
Authentication Procedure

Security Bypassed

Pin Unblocking

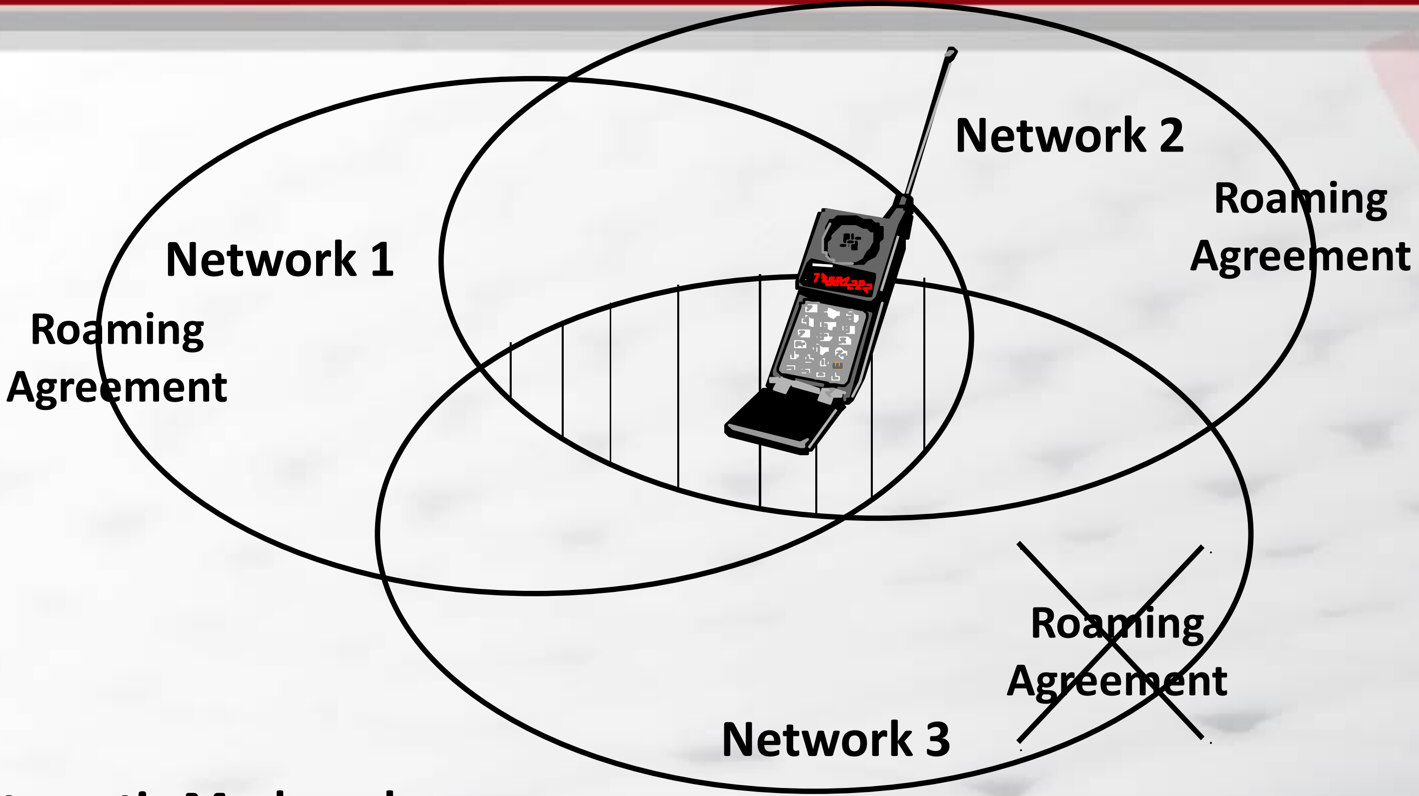


	PIN 1st try	PIN 2nd try	PIN 3rd try	PUK presentation
PIN counter	3 to 2	2 to 1	1 to 0	0 to 3



The number of PIN tries allowed before permanently locking the SIM Card depends on the Operator setting.

Role of Preferred PLMN

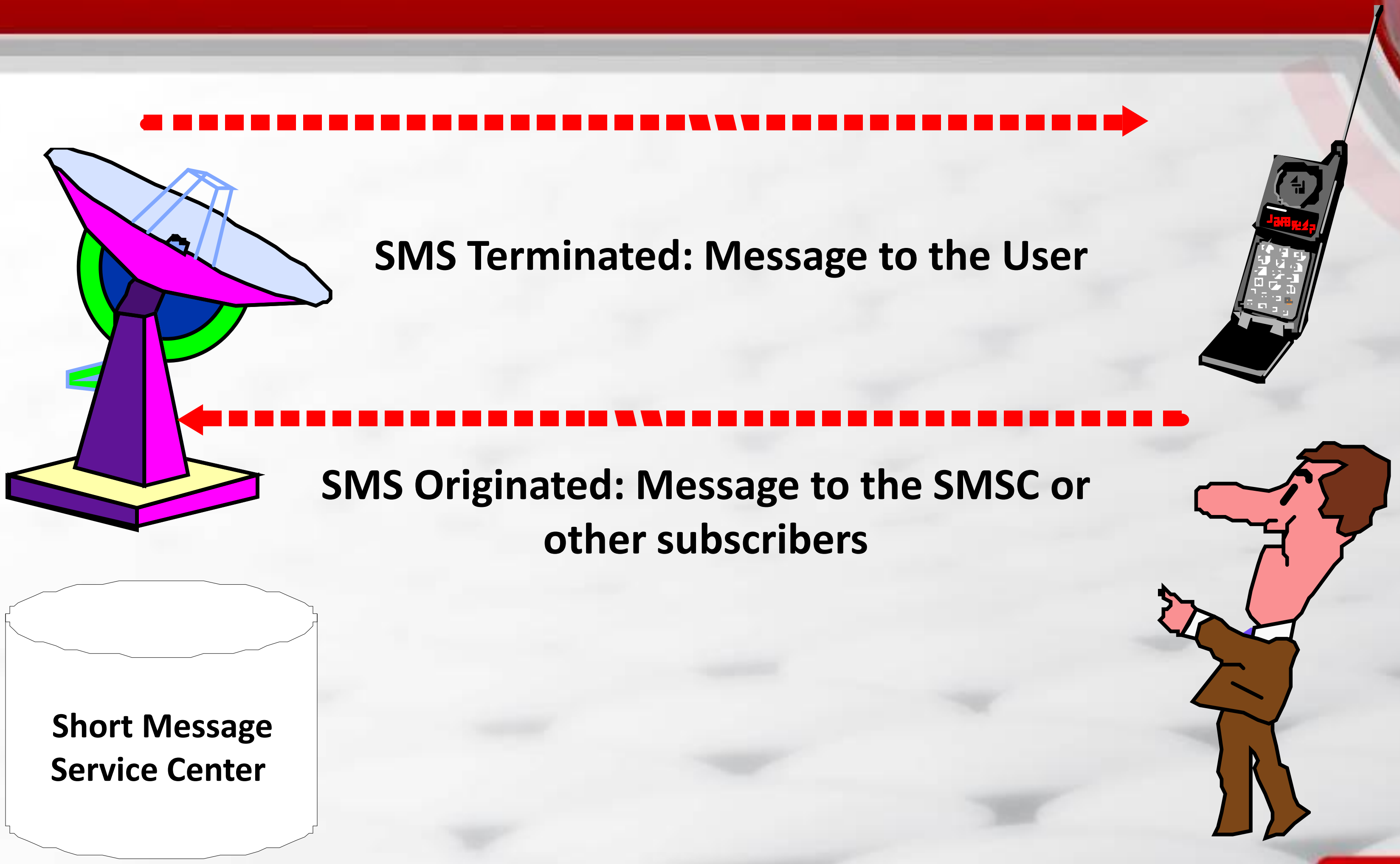


Automatic Mode only

PLMN A	PLMN B	PLMN C

Programmed according to Roaming Agreements

The SMS Channel



SMS Terminated: Message to the User

SMS Originated: Message to the SMSC or other subscribers

Short Message Service Center

AOC Mechanism

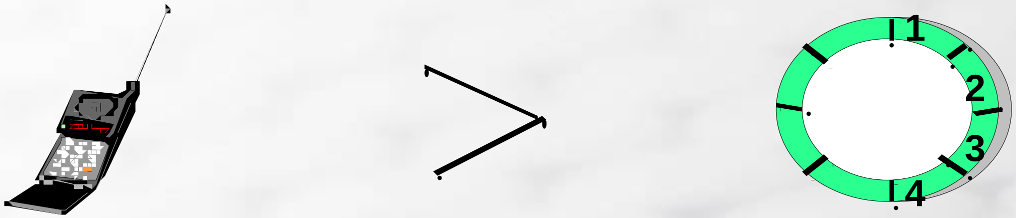
- Two types of services
  - AOC for information
  - AOC for charging

- Mechanism
  - ME increases the ACM (6F39, Accumulation Call Meter)
  - ME compares ACM and ACMMax (6F37), stops the call if necessary (only in AOC for charging)
  - Cost information given by PTUC (6F41,Price per Unit and Currency Table)

AOC feature is controlled by PIN2

AOC Mechanism: Role of the Phone

- The phone increases the Accumulation Call Meter (ACM)



- The phone compares ACM and ACM Max

If ACM > ACM Max,
Terminate the communication

Service Availability for AOC

	HLR Subscription		
SIM / ME Combinations	**Non – AoC**	**AoC (Information)**	**AoC (Charging)**
SIM Phase 1 / ME Phase 1	OK	Subscription incompatible with SIM but service may be allowed	Subscription incompatible with SIM
SIM Phase 1 / ME Phase 2	Ok	Subscription incompatible with SIM but service may be allowed	Subscription incompatible with SIM
SIM Phase 2 (AoC Allocated and Activated) / ME Phase 1	OK	Service allowed, but ACM will not be incremented	Chargeable calls will be rejected by Network (Note 1)
SIM Phase 2 (AoC Allocated and Activated) / ME Phase 2	OK	OK (Note 1)	OK
SIM Phase 2 (AoC not Activated) / ME Phase 1	OK	Subscription incompatible with SIM but service may be allowed	Subscription incompatible with SIM
SIM Phase 2 (AoC not Activated) / ME Phase 2	OK	Subscription incompatible with SIM but service may be allowed	Subscription incompatible with SIM

Note 1:** *The SIM Issuer is recommended to bar roaming to Phase 1 and Phase 2 networks not supporting AoC, to prevent calls being established and ACM not being incremented.

CPHS: Common PCN Handset Specification

- **Property of:** The Association of European PCN Operators (*Mercury/One-to-One and Hutchison/Orange, UK*)

- **Designed to:** CPHS aims at providing enhanced user interface and services that are above the standard DCS1800 specifications.

- **Specifications:** The specification is confidential and the current document is just a summary of the features which have to be supported by CPHS phones and by SIM personalization systems.

- **Functionality of CPHS version 4.2 (Phase 2, Feb. 1997)**

CPHS Files

1144	‘6F 11’	Voice Msg Waiting Flag	O,T	1+n	‘55’
1144	‘6F 13’	Call Forwarding Flag	O,T	1+n	‘55’
1444	‘6F 14’	Operator Name String	O,T	N	‘...FF..FF’
1144	‘6F 15’	Customer Service Profile	O,T	18+n	‘00ff 02ff 03ff 04ff 05ff 06ff 07ff 08ff fcff’
1444	‘6F 16’	CPHS Information	O,T	3+n	‘02F303’
1144	‘6F 17’	CPHS Mailbox Number	O,T	X+14	‘FF..FF’
1444	‘6F 18’	CPHS Operator Name	0,T	10	‘...FF..FF’
1144	‘6F 19’	CPHS Information #’	O,T	5+y+z	

Common PCN Handset Specification

- **Indicators** – messages displayed by the phone in order to alert the user about the status of the following network services:
  - **Network Operator Name**
    displayed when the phone is turned on
  - **Home Country Roaming Indicator**
    displayed when the current network is not HPLMN
  - **Voice Message Waiting Indicator**
    displayed together with line identification where ALS is available
  - **Call Waiting Indicator**
    displayed when a call arrives while another is engaged
  - **Diverted Call Indicator displayed**
    when call forward unconditional is active
  - **Current Line Indicator**
    displays currently selected line, where ALS is available

Common PCN Handset Specification

- **Alternate Line Service (ALS)** – two subscriptions (2 MSISDNs, 2 subscription profiles) with one SIM (1 IMSI).
  - The user is able to make and receive calls on either line as desired.
  - Barring or diverting of calls can be performed differently for each MSISDN.
  - Within GSM, each MSISDN can be associated with a different bearer capability to facilitate service interworking with a PSTN.
  - For the purposes of providing dual speech services, CPHS defines a second teleservice called ‘Auxiliary Speech’ (MSISDN 1 = Line 1 = “speech”, MSISDN 2 = Line 2 = “Auxiliary speech”).

Common PCN Handset Specification

- Emergency Calling
  - **112** is the standard emergency number.
  - CPHS adds **999**, which can also be dialed without a valid SIM.
  - **Rejected PIN**

    CPHS phones reject PIN values beginning with 112 or 999!

Common PCN Handset Specification

- **CPHS SIM Files** – CPHS SIM may contain the following files (Identifiers 6F11 through 6F19, all optional) under the GSM directory (7F20/7F21):
  - 1. **CPHS Information**

    6F16, transparent

    1 byte for CPHS Phase (01/02)

    2 bytes for CPHS Service Table (SST/Ph. 1, OpName Shortform and Information Numbers/Ph. 2, Mailbox Numbers and CSP/All phases)
  - 2. **Operator Name String**

    6F14, transparent

    n bytes for HPLMN name
  - 3. **Operator Name Shortform**

    6F18, transparent

    10 bytes for shortform of the HPLMN name, to be displayed if the ME cannot display the complete Operator Name string
  - 4. **Mailbox Numbers**

    6F17, linear fixed

    X+14 bytes per record for list of mailbox numbers (e.g. Line 1 mailbox, Line 2 mailbox, Fax mailbox, etc.)

Common PCN Handset Specification

- **CPHS SIM Files**
  - 5. **Voice Message Waiting Flag**

    6F11, transparent

    1 byte for Voice Message Waiting Indicator flags (Lines 1/2)

    1 optional byte for Fax/Data Message Waiting Indicator flags

    CPS use the TP-OA field (not used by the network) of the SME to indicate the type of indicator and the corresponding line.
  - 6. **Call Forwarding Flags**

    6F13, transparent

    1 byte for Voice Call forward unconditional flags (Lines 1/2)

    1 optional byte for Fax/Data Call forward unconditional flags
  - 7. **Information Numbers**

    6F19, linear fixed

    n bytes per record (alpha identifier, TON/NPI, digits, extension 1 record identifier)

    Each record gives an entry in a hierarchical structure containing phone numbers of various information services.

Common PCN Handset Specification

- **CPHS SIM Files**
  - 8. **Customer Service Profile (CSP)**

    6F15, transparent

    22 bytes for 11 groups of services (group code/allocated services)

    Reading this file, the phone knows the exhaustive list of services.

    The Service String Table is not used in CPHS Phase 2 (identifier 6F12, reserved for Phase 1).

    SIM lock is supported by CPHS, but in a standard way (GSM 02.22, GSM 11.11).

CPHS does not support SIM data download (e.g. through SMS).

Multi IMSI

- **Purpose:**
  - In places where a Roaming Agreement is not established, there is a need to establish other alternatives to Roaming, hence **Multi IMSI** is used.

- **Origin:**
  - Operators within the Country (e.g. INDIA) grouped together to form their own association to provide an alternative form of Roaming Service to users who need to travel within designated regions/states.

- **Usage:**
  - Users need to power off and on to re-register their mobiles to the new network in the new region where the current network is out of reach.

SIM Lock

- **ME-SIM Lock**
  - This feature controls the ability of the MS to access networks, in consideration of whether the ME matches the SIM based on one or more of the following criteria:

    Subscriber identity (IMSI)

    Group identifier level 1 (e.g. Service Provider identity)

    Group identifier level 2

    PLMN identity (MCC+MNC)
  - One or more of these criteria may be activated. When any are activated, the ME shall be locked to the SIM, such that the MS shall only make network registration attempts when there exists a bit-exact match between corresponding data elements on the ME and the SIM for each of the activated criteria.
  - Secure means shall be provided to prevent unauthorized changes to the lock status or the contents of any of the data fields above on the SIM or the ME.

Questions?