Subscriber Identity Module (SIM)
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
Recommendation 11.11 defines two GSM Card Dimensions

ISO dimension Card

Plug-in SIM
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

<table>
<thead>
<tr>
<th>Commands</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>8</th>
<th>8</th>
<th>8</th>
<th>6</th>
<th>6</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>B</td>
<td>E</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Select</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Binary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Binary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seek</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify CHV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change CHV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable CHV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable CHV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unblock CHV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalidate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rehabilitate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run GSM Algorithm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sleep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Not applicable commands are marked with 'X' and applicable commands are marked with a blank space.*
<table>
<thead>
<tr>
<th>Access Condition</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Always / Free Access</td>
</tr>
<tr>
<td>1</td>
<td>CHV1 (PIN1)</td>
</tr>
<tr>
<td>2</td>
<td>CHV2 (PIN2)</td>
</tr>
<tr>
<td>3</td>
<td>Reserve</td>
</tr>
<tr>
<td>4,5..E</td>
<td>ADM (GSM operator)</td>
</tr>
<tr>
<td>F</td>
<td>Never (impossible)</td>
</tr>
</tbody>
</table>
GSM SIM: File Type

- **Header**
  - System Information

- **Body**
  - Sequence Of Byte
  - Application Data

- **Record #1**
- **Record #2**
- **Record #3**
- **Last Record #N**
- **Rest of records**

- **Transparent File**
  - File type 0

- **Linear File**
  - File type 1

- **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

<table>
<thead>
<tr>
<th>Function</th>
<th>MF</th>
<th>DF</th>
<th>EF transparent</th>
<th>EF linear fixed</th>
<th>EF cyclic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>STATUS</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>READ BINARY</td>
<td>*</td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPDATE BINARY</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ RECORD</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>UPDATE RECORD</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>SEEK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>INCREASE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>INVALIDATE</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>REHABILITATE</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>Lout</th>
<th>Data-out</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>B2</td>
<td>01=current</td>
<td>04</td>
<td>rec_length</td>
<td>data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02-FF = rec# 04</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>01=1st rec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>02=last rec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>03=previous</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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
The test algorithm employs bit-wise modulo 2 addition:

128 bits
SRES (32 bits)

128 bits
RAND

128 bits
Ki

XOR

128 bits

128 bits

Not Used

Kc (64 bits)
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

=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
*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

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>Lin</th>
<th>Data-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>DC</td>
<td>01=cursor</td>
<td>04</td>
<td>rec_length</td>
<td>data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02-FF = rec#</td>
<td>04</td>
<td></td>
<td>data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>01=1st rec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>02=last rec</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xx</td>
<td>03=previous</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note:

1. Last selected file must be a record file
2. Update access must be fulfilled
3. Lout must be record length
Verify CHV

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>Lin</th>
<th>Data-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>20</td>
<td>00</td>
<td>CHV# 08</td>
<td>CHV</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>Lin</th>
<th>Data-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>EA</td>
<td>00</td>
<td>00</td>
<td>Lin(&lt;20)</td>
<td>EF content</td>
</tr>
</tbody>
</table>

*Note:

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

<table>
<thead>
<tr>
<th>File Type</th>
<th>Allocated Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF</td>
<td>(Max. number of entries) * 16</td>
</tr>
<tr>
<td>Transparent EF</td>
<td>Max. number of bytes</td>
</tr>
<tr>
<td>Linear Fixed EF</td>
<td>If lock record is available for this file:</td>
</tr>
<tr>
<td></td>
<td>(Max. number of records) * (record length) +1 ^1</td>
</tr>
<tr>
<td></td>
<td>If lock record is not available for this file:</td>
</tr>
<tr>
<td></td>
<td>(Max. number of records) * (record length)</td>
</tr>
<tr>
<td>Cyclic EF</td>
<td>(Max. number of records) * (record length +1) ^2</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th></th>
<th>Transparent EF</th>
<th>Linear fixed EF</th>
<th>Cyclic EF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>(\checkmark)</td>
<td>(\checkmark)</td>
<td>(\checkmark)</td>
</tr>
<tr>
<td>Type 2</td>
<td>(\checkmark)</td>
<td>(\checkmark)</td>
<td></td>
</tr>
<tr>
<td>Type 3</td>
<td></td>
<td>(\checkmark)</td>
<td>(\checkmark)</td>
</tr>
</tbody>
</table>

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

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

Command description

This instruction allows the deletion of the specified EF within the current directory and at the condition it is the last created EF within 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 another 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 contains 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

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**

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

**Language Preference**

**MSISDN storage**

**PLMN Selection**

**Abbreviated Dialling**

**Short Messages**

**Capability Configuration Parameters**

**Language Preference**

**Price Unit Currency Table**

**MSISDN storage**

**Call charge unit storage (AOC)**

**Fixed Number Dialling**

**Last Number Dialed**
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

<table>
<thead>
<tr>
<th>Commands</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>XX</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Commands</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>9</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>XX</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

- **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

<table>
<thead>
<tr>
<th>Access Condition</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Always / Free Access</td>
</tr>
<tr>
<td>1</td>
<td>CHV1(PIN1)</td>
</tr>
<tr>
<td>2</td>
<td>CHV2 (PIN2)</td>
</tr>
<tr>
<td>3</td>
<td>Reserve</td>
</tr>
<tr>
<td>4,5..E</td>
<td>ADM (GSM operator)</td>
</tr>
<tr>
<td>F</td>
<td>Never (impossible)</td>
</tr>
</tbody>
</table>
GSM SIM: File Type

- **Header**: Contains system information.
- **Body**: Includes sequence of byte application data.
- **Record #1**: First record.
- **Record #2**: Second record.
- **Record #3**: Third record.
- **Last Record #N**: Last record.
- **Rest of records**: Additional records.

**Transparent File**
- File type 0

**Linear File**
- File type 1

**Cyclic File**
- 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

<table>
<thead>
<tr>
<th>Function</th>
<th>MF</th>
<th>DF</th>
<th>EF transparent</th>
<th>EF linear fixed</th>
<th>EF cyclic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STATUS</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ BINARY</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPDATE BINARY</td>
<td></td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ RECORD</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>UPDATE RECORD</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>SEEK</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>INCREASE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>INVALIDATE</td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>REHABILITATE</td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
## GSM SIM: MF & Telecom DF

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

<table>
<thead>
<tr>
<th>GSM DF</th>
<th>File Id</th>
<th>Description</th>
<th>Type</th>
<th>Size</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0144</td>
<td>'6F 05'</td>
<td>Language preference</td>
<td>M,T</td>
<td>1 - n</td>
<td>'FF'</td>
</tr>
<tr>
<td>1441</td>
<td>'6F 07'</td>
<td>IMSI</td>
<td>M,T</td>
<td>9</td>
<td>'FF'...FF07</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 20'</td>
<td>Ciphering key Kc</td>
<td>M,T</td>
<td>9</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 30'</td>
<td>PLMN selector</td>
<td>O,T</td>
<td>3n (n&gt;=8)</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 31'</td>
<td>HPLMN search period</td>
<td>M,T</td>
<td>1</td>
<td>'FF'</td>
</tr>
<tr>
<td>1144/1244</td>
<td>'6F 37'</td>
<td>ACM maximum value</td>
<td>O,T</td>
<td>3</td>
<td>'000000'</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 38'</td>
<td>SIM service table</td>
<td>M,T</td>
<td>X (x&gt;=2)</td>
<td>operator dependant</td>
</tr>
<tr>
<td>11144/11244</td>
<td>'6F 39'</td>
<td>Accumulated call meter</td>
<td>O,C</td>
<td>3</td>
<td>'000000'</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 3E'</td>
<td>Group identifier level 1</td>
<td>O,T</td>
<td>1 - n</td>
<td>operator dependant</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 3F'</td>
<td>Group identifier level 2</td>
<td>O,T</td>
<td>1 – n</td>
<td>operator dependant</td>
</tr>
<tr>
<td>1144/1244</td>
<td>'6F 41'</td>
<td>PUCT</td>
<td>O,T</td>
<td>5</td>
<td>'FFFFFFF0000'</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 45'</td>
<td>CBMI</td>
<td>O,T</td>
<td>2n</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>0444</td>
<td>'6F 46'</td>
<td>Service provider name</td>
<td>O,T</td>
<td>17</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 74'</td>
<td>BCCH</td>
<td>M,T</td>
<td>16</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 78'</td>
<td>Access control class</td>
<td>M,T</td>
<td>2</td>
<td>Last digit of IMSI</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 7B'</td>
<td>Forbidden PLMNs</td>
<td>M,T</td>
<td>12</td>
<td>'FF'...FF</td>
</tr>
<tr>
<td>1141</td>
<td>'6F 7E'</td>
<td>Location information</td>
<td>M,T</td>
<td>11</td>
<td>'FFFFFFFFFxxFxxx0000FF01'</td>
</tr>
<tr>
<td>0444</td>
<td>'6F AD'</td>
<td>Administrative data</td>
<td>M,T</td>
<td>3+x</td>
<td>operator dependant (000000)</td>
</tr>
<tr>
<td>0444</td>
<td>'6F AE'</td>
<td>Phase identification</td>
<td>M,T</td>
<td>1</td>
<td>01,02,03 for phase 1,2,2+</td>
</tr>
<tr>
<td>1122</td>
<td>'6F 3A'</td>
<td>Abbreviated dialling #</td>
<td>O,L</td>
<td>(X+14)*n</td>
<td>'FF'...FF</td>
</tr>
</tbody>
</table>
ICC ID 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

<table>
<thead>
<tr>
<th>Code</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>German</td>
</tr>
<tr>
<td>01</td>
<td>English</td>
</tr>
<tr>
<td>02</td>
<td>Italian</td>
</tr>
<tr>
<td>03</td>
<td>French</td>
</tr>
<tr>
<td>04</td>
<td>Spanish</td>
</tr>
<tr>
<td>05</td>
<td>Dutch</td>
</tr>
<tr>
<td>06</td>
<td>Swedish</td>
</tr>
<tr>
<td>07</td>
<td>Danish</td>
</tr>
<tr>
<td>08</td>
<td>Portuguese</td>
</tr>
<tr>
<td>09</td>
<td>Finnish</td>
</tr>
<tr>
<td>0A</td>
<td>Norwegian</td>
</tr>
<tr>
<td>0B</td>
<td>Greek</td>
</tr>
<tr>
<td>0C</td>
<td>Turkish</td>
</tr>
<tr>
<td>0F</td>
<td>Chinese</td>
</tr>
</tbody>
</table>

**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)
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                  | 9. MSISDN                     |
| 2. ADN                          | 10. Ext 1                     |
| 3. FDN                          | 11. Ext 2                     |
| 4. SMS                          | 12. SMS Parameters            |
| 5. AoC                          | 13. LDN                       |
| 7. PLMN                         | 15. Group ID Level 1          |
| 8. RFU                          | 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*
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 Presentation

OK

Authentication Procedure
PIN Code Disabled

PIN Presentation

Security Bypassed

Authentication Procedure
Pin Unblocking

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

<table>
<thead>
<tr>
<th>PIN counter</th>
<th>PIN 1st try</th>
<th>PIN 2nd try</th>
<th>PIN 3rd try</th>
<th>PUK presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3 to 2</td>
<td>2 to 1</td>
<td>1 to 0</td>
<td>0 to 3</td>
</tr>
</tbody>
</table>

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

Automatic Mode only

<table>
<thead>
<tr>
<th>PLMN A</th>
<th>PLMN B</th>
<th>PLMN C</th>
</tr>
</thead>
</table>

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 ACMMMax (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

<table>
<thead>
<tr>
<th>SIM / ME Combinations</th>
<th>Non – AoC</th>
<th>AoC (Information)</th>
<th>AoC (Charging)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM Phase 1 / ME Phase 1</td>
<td>OK</td>
<td>Subscription incompatible with SIM but service may be allowed</td>
<td>Subscription incompatible with SIM</td>
</tr>
<tr>
<td>SIM Phase 1 / ME Phase 2</td>
<td>Ok</td>
<td>Subscription incompatible with SIM but service may be allowed</td>
<td>Subscription incompatible with SIM</td>
</tr>
<tr>
<td>SIM Phase 2 (AoC Allocated and Activated) / ME Phase 1</td>
<td>OK</td>
<td>Service allowed, but ACM will not be incremented</td>
<td>Chargeable calls will be rejected by Network (Note 1)</td>
</tr>
<tr>
<td>SIM Phase 2 (AoC Allocated and Activated) / ME Phase 2</td>
<td>OK</td>
<td>OK (Note 1)</td>
<td>OK</td>
</tr>
<tr>
<td>SIM Phase 2 (AoC not Activated) / ME Phase 1</td>
<td>OK</td>
<td>Subscription incompatible with SIM but service may be allowed</td>
<td>Subscription incompatible with SIM</td>
</tr>
<tr>
<td>SIM Phase 2 (AoC not Activated) / ME Phase 2</td>
<td>OK</td>
<td>Subscription incompatible with SIM but service may be allowed</td>
<td>Subscription incompatible with SIM</td>
</tr>
</tbody>
</table>

*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.*
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)
<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1144</td>
<td>'6F 11'</td>
<td>Voice Msg Waiting Flag</td>
<td>O,T</td>
<td>1+n</td>
<td>'55'</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 13'</td>
<td>Call Forwarding Flag</td>
<td>O,T</td>
<td>1+n</td>
<td>'55'</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 14'</td>
<td>Operator Name String</td>
<td>O,T</td>
<td>N</td>
<td>'...FF..FF'</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 15'</td>
<td>Customer Service Profile</td>
<td>O,T</td>
<td>18+n</td>
<td>'00ff 02ff 03ff 04ff 05ff 06ff 07ff 08ff ff'</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 16'</td>
<td>CPHS Information</td>
<td>O,T</td>
<td>3+n</td>
<td>'02F303'</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 17'</td>
<td>CPHS Mailbox Number</td>
<td>O,T</td>
<td>X+14</td>
<td>'FF..FF'</td>
</tr>
<tr>
<td>1444</td>
<td>'6F 18'</td>
<td>CPHS Operator Name</td>
<td>O,T</td>
<td>10</td>
<td>'...FF..FF'</td>
</tr>
<tr>
<td>1144</td>
<td>'6F 19'</td>
<td>CPHS Information #</td>
<td>O,T</td>
<td>5+y+z</td>
<td></td>
</tr>
</tbody>
</table>
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
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.)
- **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?