ETSI/GSM

Released by: ETSI PT12

Date: July, 1994

Recommendation: GSM 11.11

Title: Specifications of the SIM-ME Interface

List of contents :

Original language: English

Number of pages: 132 (100 + 9 + 17 + 6)

1. SCOPE

Recommendation GSM 02.17 states the basic concept of a split of the MS into a removable SIM (Subscriber Identity Module) which contains all network related subscriber information and a ME (Mobile Equipment) which is the remaining part of the MS, and realizes all the functions common to all GSM subscribers.

The implementations stated in Recommendation GSM 02.17 are :

- IC card SIM;
- plug-in SIM.

The phases of the SIM life distinguished in Recommendation GSM 02.17 are :

- GSM network operation phase (also called GSM operations);
- administrative management phase.

This recommendation defines the interface of the ME with the SIM and the internal organization of the SIM related to the GSM network operation phase. The aspects relevant to the administrative management phase are left to each network operator discretion and are not addressed in this recommendation.

The reservations for the future GSM operational use are specified in clause 1.1, while those for the administrative management are specified in clause 1.2.

This recommendation does not specify any internal technical realization sketches.

This recommendation is divided into five parts :

- Definitions of the concepts introduced in the document;
- Description of the data and the algorithms to be stored within the SIM and the access control associated with each of them;
- Definition of the application protocol for communications between the SIM and the outside world;
- Description of the transmission protocol(s) to be used at the lower layers for communication;
- Description and specification of the physical characteristics.

NOTE : In case of discrepency between the text and the annexes, the text has priority.

1.1. Future GSM operational phase

The following codings are reserved for the future operational phase of the SIM.

Directories:

- application directories: 7F 1X, 7F 2X, 7F 6X

Data fields:

- 6F XX in all the above application directories, except 6F 1X in 7F 10, 7F 20 and 7F 21.
- data fields under the level root directory: 2F 1X.

Instruction codes:

- the instruction codes 0X with X ≠ 2, 4; 1X (for both ranges X shall be even).

Furthermore, in the respons data of the instructions STATUS and GET RESPONSE information areas are reserved (see clause 4.3.1).

Note: With X ranging from hex 0 to hex F.

1.2. Administrative management

The following codings are reserved for the administrative phase of the SIM.

Directories:

- application directories: 7F 4X

Data fields:

- data-fields under the level root directory: 2F EX except 2F E2 (ICC Identification)
- data-fields under the level application directory:
  - all data-fields (6F XX) in the directories 7F 4X
  - in the application directories 7F 10, 7F 20 and 7F 21 the data-fields 6F 1X

Instruction codes:

- the instruction codes A0 2A, A0 D0, A0 D2, A0 DE, A0 C4, A0 C6, A0 C8, A0 CA, A0 CC, A0 B4, A0 B6, A0 B8, A0 BA, A0 BC

Furthermore, in the respons data of the instructions STATUS and GET RESPONSE information areas are reserved (see clause 4.3.1).

Note: With X ranging from hex 0 to hex F.

2. DEFINITIONS AND ABBREVIATIONS

2.1. DEFINITIONS

(listed in alphabetic order)

Application

A set of services managed by an entity and offered to the user(s) of this set. It includes data, rules to handle them and the associated application protocol.

Application protocol

It describes the communication aspects between entities needed by the application.

Block

Contiguous data memory space which is allocated when requested for data-field. Each Block is linked to a unique binary data-field.

Data-field

A logical data area which contains information having the same security access conditions and data management characteristics.

A data-field may be either "binary" (non structured data-field composed of a fixed length block) or "formatted" (organised in logical records of fixed length).

Directory

Data-fields are grouped within directories.

GSM-application

This has been specified using data-fields and directories necessary to GSM operation. Two application directories have been defined to allow additional services and basic GSM functions to be handled by another application.

GSM-session

In the GSM application, this is the interval of time starting at the completion of the SIM activation procedure and ending either at the completion of the deactivation procedure or at the first instant the link between the SIM and the ME is interrupted for any reason.

Pattern

A string of bytes that is sought from the begining of records

Record

In the case of formatted data-fields, a record is a string of bytes handled as an entity by the SIM, containing application elementary data. Records are always of the same length in a specific data-field. A record may be selected by its number (position) in the data-field, or by searching throughout the data-field using the begining of the record as an argument.

SIM

Subscriber Identification Module. The SIM is used in GSM to handle securily identification and data related to a given subscriber. Other applications may exist in the removable module used as SIM.

2.2. ABBREVIATIONS

(listed in alphabetic order)

AD :	Application Directory
ADM :	Administrative phase in the life of the SIM
ADM/AUT :	a level of authorization defined by the authority who creates the data-field.
AUT :	Authority
BCCH :	Broadcast Control Channel
DF :	Data Field
FOR FS :	For Further Study
IDF :	Identifier of a data-field
LGTH :	Length of the data of the <data&parameters> in an instruction. This length is sent in the byte P3 of the instruction (see paragraph 4.4)
MMI :	Man Machine Interface
NET :	notation for procedures that are clearly not user dependant
PLMN :	Public Land Mobile Network
RACH :	Random Access Channel
RAU :	Reserved for Administrative Use
RD :	Root Directory
RFU :	Reserved for Future Use
SIM :	Subscriber Identification Module

3. SIM LOGICAL MEMORY ORGANIZATION

The SIM has two fundamental purposes as defined in Recommendation GSM 02.17:

- storing data (and controlling the access to this data),

- executing algorithms in secure conditions : for its maintask of authentication of the subscriber's identity according to Recommendation GSM 02.09.

3.1. DEFINITIONS OF DIRECTORIES AND DATA-FIELDS

Information is structured in data-fields grouped by directories.

All information contained in a data-field is of the same level of security management.

3.1.1. Directories

Data-fields are grouped in directories related to a specific application or service.

Application directories (AD) are under the root directory (RD). For the GSM-application, there are two application directories : the GSM directory (GSM-AD) and the Telecom directory (Tel-AD).

3.1.1.1. Structure of the directory

A directory is a functionnal grouping of data-fields and sub-directories. There may be access rules attached to the directory.

3.1.2. Data-fields

There are two types of Data-fields :

- binary Data-fields;
- formatted Data-fields.

3.1.2.1. Structure of binary data fields

A binary data-field is composed of a header and of a body part.

The header (which is managed by the SIM) contains :

* a data-field identifier used to select it among the others of the same application. This identifier consists of 2 bytes
* the type of the data-field : binary. (The type is coded on 1 byte)
* a security policy giving the conditions required to access the data contained in the data-field and to operate on it. This security policy is described in section 3.4.2. The security policy for each action is coded on 4 bits
* the length in bytes of the body part of the data-field (coded on two bytes).

The body of the data-field is a block containing data. Several funtional entities may exist in the block body of the same data-field. The ME should manage them separately if needed.

3.1.2.2. Structure of formatted data-fields

A formatted data-field is composed of a header and of a body part.

The header (which is managed by the SIM) contains :

* a data-field identifier used to select it among the others of the same application. This identifier consists of 2 bytes.
* the type of the data-field : formatted. (The type is coded on 1 byte)

* a security policy giving the conditions required to access the data contained in the data-field and to operate on it. This security policy is described in section 3.4.2. The security policy for each action is coded on 4 bits.

* the characteristics of the data-field : The record length (coded on one byte) and the length in bytes of the body part of the data field (coded on 2 bytes).

The body of a formatted data-field contains records. The first record is record 1.

3.1.2.3. Addressing data-fields

After a data-field has been selected, two addressing methods are possible to access the data contained in a data-field: relative addressing and logical addressing.

- Relative addressing is used for addressing binary data-fields. The SIM does not understand the semantics of the data inside the data-field, and it only performs actions on string of bytes. The SIM will perform actions in the data-field based on the block number, offset in the block, and the length of the string given by the ME.

- Logical addressing is used for addressing formatted data-fields.: The SIM is able to manage records within a formatted data-field. In a formatted data-field, the records are of fixed length.

For addressing records, there are 3 methods :

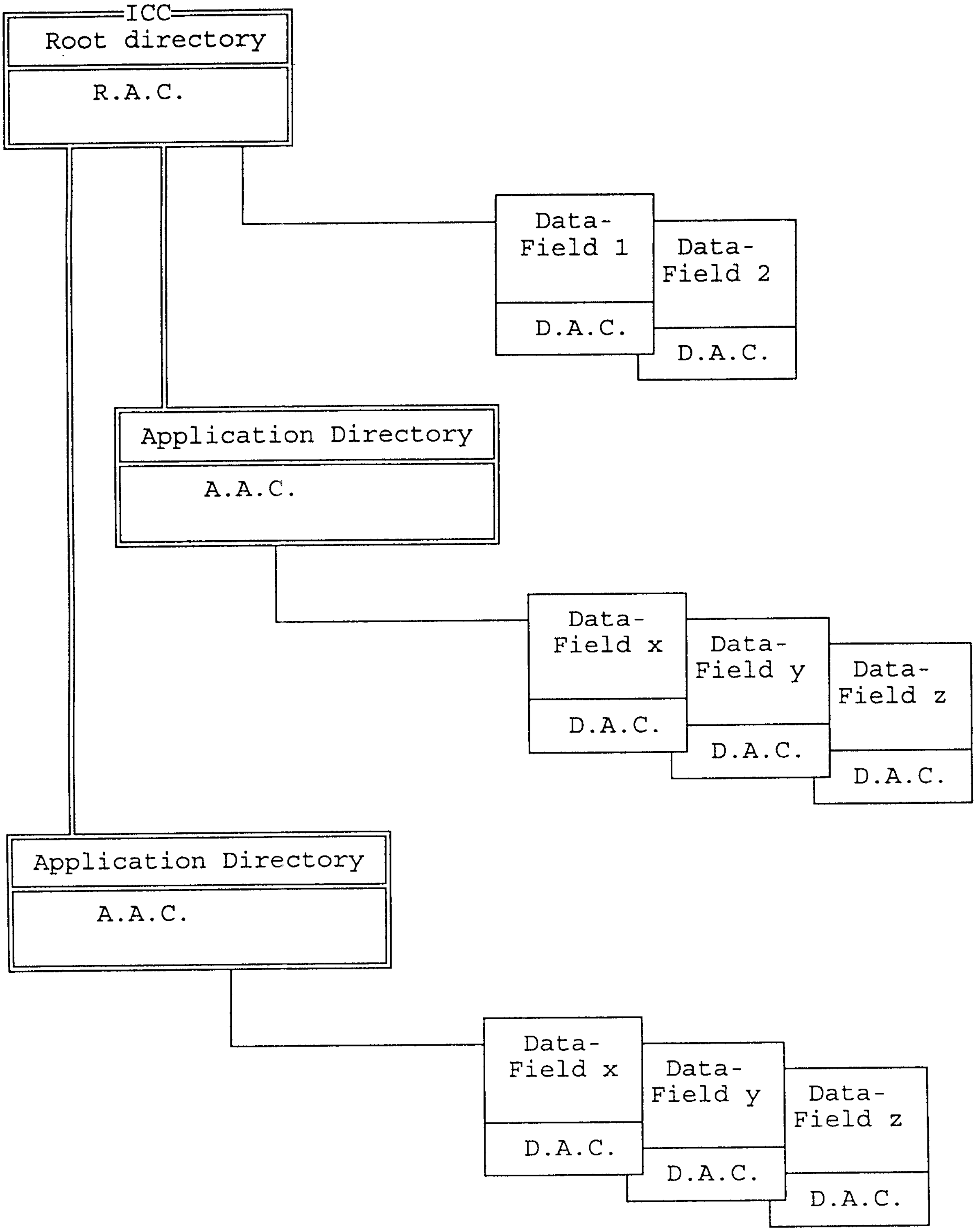
1) Using the record number.

2) Using a pointer positioned by previous instruction and modified according to the mode of the action.

3) By seeking for a pattern from the current pointer forward or backward in the data-field.

It is possible to mix these modes.

LOGICAL STRUCTURE - GENERAL CONCEPT



R.A.C =	Root Access Conditions (to be defined in administrative part)
A.A.C =	Application Access Conditions (to be defined in administrative part)
D.A.C =	Data-Field Access Conditions.

3.2. DEFINITION OF THE ACTIONS ON DIRECTORIES AND DATA-FIELDS

The actions defined below are those which may be invoked when the SIM is in GSM operations, i.e., associated with a ME. The actions which are needed for the daministrative management of the SIM are not addressed in this recommendation.

3.2.1. Definition of the actions on directories

In GSM operations, the only action allowed on directories is :

* Selection : action of selecting a specific directory by giving its identifier to the SIM. Once a directory is selected, all actions related to data-fields in GSM application will implicitly refer to this 'current' directory.

3.2.2. Definition of the actions on data-fields

3.2.2.1. General actions on data-fields

In GSM operations, the following actions are possible on data-fields :

* Selection : action of selecting a specific data-field by giving its identifier to the SIM. A selection of a data-field is done under the current directory. Once a data-field is selected, all actions will implicitly refer to this 'current' data-field.

Once the data-field has been selected, the SIM shall ensure that the security policy is fulfilled for each action described below :

* Updating: action by which data is changed. It may be a string of bytes in a binary data-field or a record in a formatted data-field.

  Note : the memory location is erased before the write occurs.

* Read: action by which information data are transferred from the SIM memory to the external world on the I/O line. This action may occur on a string of bytes or a record, depending on the data-field in which the action occurs.

* Seek: each action by which a search is made through a formatted data-field to locate a record. The seek will compare the given pattern with the begining of the record. When the pattern is found, the SIM sets a pointer at the found location in the current data-field where further actions such as read/update on the current record will be performed. If the pattern is not found, then the SIM will not change the pointer.

3.2.2.2. Definition of the actions on binary data-fields

In GSM operations, a binary data-field may be selected. Then, the ME can read or update strings of bytes in the block constituting the body of the data-field.

3.2.2.3. Definition of the actions on formatted data-fields

In GSM operations, a formatted data-field structured with records may be selected. Then, the ME can seek, read, update records (selected by their argument or their number) in the data-field. Reading and updating act upon a complete record and smaller groups of bytes cannot be individually accessed.

Where the pattern specified is not unique, the seek action will locate the first/next occurence of the pattern.

3.3. ALGORITHMS

The GSM Algorithms A3 and A8 are composed of an identifier and of a program. They are atomic in the sense that they are seen as a whole. The action performed by the SIM on these algorithms is to execute them.

3.4. SECURITY POLICY

3.4.1. Definition

Depending on the considered life phase of the SIM, different parties from the outside world may access and perform actions on the SIM.

The definition of the rules allowing a specific party to access the SIM and perform specific actions on specific data contained in the SIM is called a security policy. The access is allowed by the SIM only if the considered party has been successfully authenticated by the SIM.

An authentication of a specific party (if applicable) is carried out at the beginning of each invokation of the GSM-application. If this is successful, action on data-fields is allowed within the constraints of the security policy of each field.

Two kinds of authentication procedures between the ME and the SIM are envisaged in GSM operations:

1) passive authentication of the ME to the SIM : The procedure starts with the presentation of a secret code (e.g. a PIN) by the party. If the code presented corresponds with the one inside the SIM, then the authentication is successful.

2) active authentication of the SIM to the outside world : The outside world generates a random number and passes it to the SIM via the ME. A specific algorithm with a specific key and the random number is performed by the SIM and the result presented to the outside world. The same calculation is performed by the outside world. If the results agree,

the outside world considers that the SIM possesses the correct key and the authentication is successful.

When the SIM is in GSM network operation phase (i.e., when it is operated in association with a ME for GSM radiocommunications), the authentication procedure for the user (mobile subscriber) is a passive authentication, based on a PIN code as specified in Recommendation GSM 02.17.

The authentication procedures for the other parties (e.g. manufacturer, service provider, card issuer, SIM activator, delivering party, etc..), and when the SIM is in GSM administrative management phases (manufacturing, pre-personalization, personalization, etc..), are not addressed in this recommendation.

The authentication procedures of the SIM to the outside world is defined in Recommendation GSM 02.09 and Recommendation GSM 03.20. This is the main function of the SIM according to Recommendation GSM 02.17. In this case the SIM has to authenticate itself to the GSM PLMN.

Except when otherwise stated, an authentication is valid for the entire GSM-session. That is to say that, if an action on a given data-field is protected by an authentication, this action is permitted on this data-field if and only if such a successful authentication has taken place before, during the same GSM-session.

The security policy presented in this recommendation is restricted to those actions which are relevant to the GSM operations of the SIM.

3.4.2. Semantics of the data-field

A data-field shall contain only data with the same security policy. Therefore, the security policy is related to the actions allowed on all the data contained in this data-field.

The security policy is stored in the header of the data-field and describes for each possible action on the data-field the associated condition-level :

- Actions on data-fields in GSM operations are :
  * Read
  * Update
- Condition-levels are :
  * ALW(-ays possible): no authentication at all is required to perform the corresponding action on the data-field.
  * PIN: the action is possible on the data-field only if one of the following conditions is fulfilled :
    - a correct user PIN code has been already presented to the SIM during the current SIM session;

- the PIN enabled/disabled indicator is already set in position "disabled".

* ADM/AUT: the action is only possible on the data field if an authentication procedure reserved for use by the appropriate administrative authority during SIM administrative management phases has been successfully performed.

* NEV(er possible): this means that this action is never allowed.

The condition-levels refer to the SIM-ME interface and not to internal actions within the SIM.

Other condition-levels are possible (up to 16), but reserved.

Levels 2 and 3 are reserved for possible upgrading of SIM functions in GSM operation phase (for FS).

Levels 4 to 14 (11 different levels) are reserved for SIM administrative management (out of the scope of this document). When a security policy is quoted as adminitrative (and noted ADM/AUT in this document), the administrative authority can allocate any level between 4 and 14 at his own discretion.

Actions which have an ADM security level cannot be allocated a condition level coding of 0, 1, 2 and 3 which would allow access to these actions in GSM operations. It shall be impossible for the subscriber to violate the security policy of the GSM network operation phases defined in this recommendation. Therefore it shall be impossible for the subscriber to activate the administrative management of the SIM.

The condition level coding is :

```
* 0  : ALW
* 1  : PIN
* 2      |  Reserved for GSM
* 3      |  Future Use
* 4  : ADM/AUT
* ...
* 14 : ADM/AUT
* 15 : NEV
```

One byte is therefore required in the header to allocate a condition level for the two actions of the GSM operation phase (see section 4.3 (10) GET RESPONSE for an example).

3.4.3. Different phases of the life of the SIM

Two different phases for the life of the SIM are defined:

- GSM phase when the SIM is in communication with the ME.

- ADM phase when it is not a GSM phase. ADM phase may be constituted of different phases under the control of different authorities.

3.5. APPLICATION DATA ENCODING

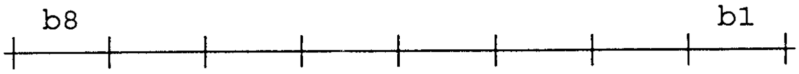
Information exchanged between the SIM and the ME and also exchanged between the ME and the network (through the air interface) is already encoded according to Rec. GSM 04.08.

In order to simplify the task of the ME, the data encoding at the SIM-ME interface shall be as far as possible the same as that at the air interface.

Note : the information which is not exchanged through the air interface is not encoded in Rec. GSM 04.08. Moreover, the information which is encoded at the air interface in less that one byte must be transcoded.

Notation :

In the following, the notation for a byte is :



b1 is the least significant bit of the byte (LSB)
b8 is the most significant bit of the byte (MSB)

Note : data-fields are not defined for those data that are accessed by specific instructions (ie : PIN)

Data-fields strings or records having a "NULL" value or cleared by the ME shall have all bits set to "1". When the ME reads the value "all 1" from the SIM, the data should be treated as undefined. After the administrative management phase, all data-fields shall have a defined value or be set to "NULL".

3.5.1. Description of the data-fields

In the following pages are described the different data-fields. The presentation is as follows :

1) The purpose of the data-field,

stating also if the data-field is subject to frequent updating

2) The Data-field attributes :

It specifies :

- the identifier
- the type of the data-field (binary or formatted)
- the security policy
- the record length (if the type is a formatted data-field)
- the block length (if the type is a binary data-field)

In the following pages, if no authorization is required, it will be presented by : ALW. (Always). The authorisation at the card-holder level will be represented by : PIN. All authorisations defined at administrative level by : ADM/AUT.

3) The structure of the data-field :

When necessary, a figure illustrates data (block or record) which will be exchanged between the ME and the SIM.

DATA-FIELD - 01: CARD-HOLDER RELATED INFORMATION

Encoding reserved for administrative purpose.

DATA-FIELD - AD: **ADMINISTRATIVE DATA-FIELD**

Purpose:

This Data-field contains the following information

the mode of operation according to the type of SIM, e.g., normal (to be used by PLMN subscribers for GSM operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases);

High update activity: **No**

Data-field attributes:

Identifier..........: 6F AD
Type................: Binary.
Security Policy...:
    Read : ALW.
    Update : ADM/AUT.
Block Length........: Fixed during management phase (three bytes defined up to now, other information may be stored in this field in the future, and will be coded on further bytes in the data-field).

Structure of the data-field:

Byte :		Initial value
1 :	MS operation mode	
	. normal operation	00
	. type approval operations	80
	. normal operation + specific facilities	01
	. type approval operations + specific facilities	81
	. maintenance (off line)	02
2-3 :	Additional information	
	. special facility number (if in byte 1: b1=1)	
	. ME manufacturer specific information (if in byte 1: b2=1)	

DATA-FIELD - E2: **IC CARD IDENTIFICATION**

Purpose:

This Data-field contains data identifying the SIM.

High update activity: **No**

Data-field attributes:

```
Identifier..........: 2F E2
Type................: Binary.
Security Policy...:
          Read         : ALW.
          Update       : NEV.
Block Length........: 10 bytes
```

Structure of the data-field:

Operators option.

DATA-FIELD - 38: **SIM SERVICE TABLE**

Purpose:

This Data-field is used to identify which are the allocated and active services in the SIM.

High update activity: No

Data-field attributes:

Identifier..........: 6F 38
Type................: Binary.
Security Policy...:
Read : PIN.
Update : ADM/AUT.
Block Length........: Fixed during administrative Management phase (two bytes are defined up to now)

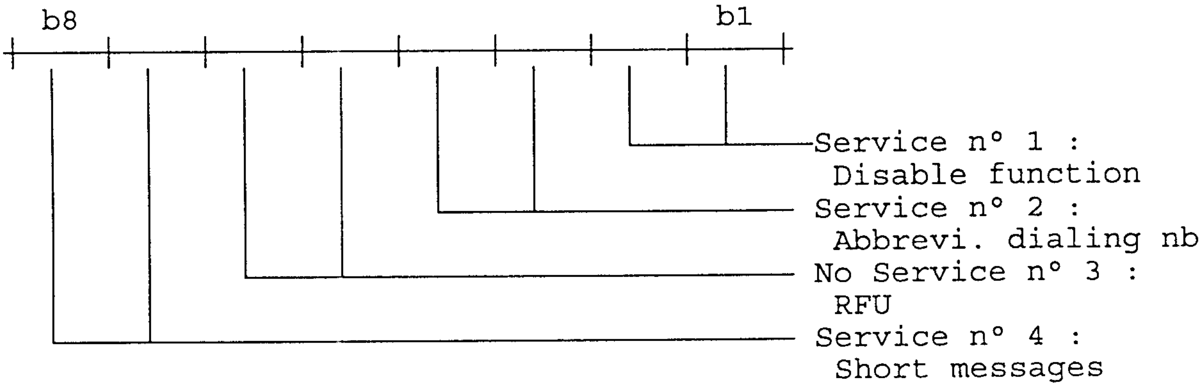
Structure of the data-field:

2 bits are used to describe each service :

first bit = 1 : service allocated in the card
first bit = 0 : service not allocated in the card

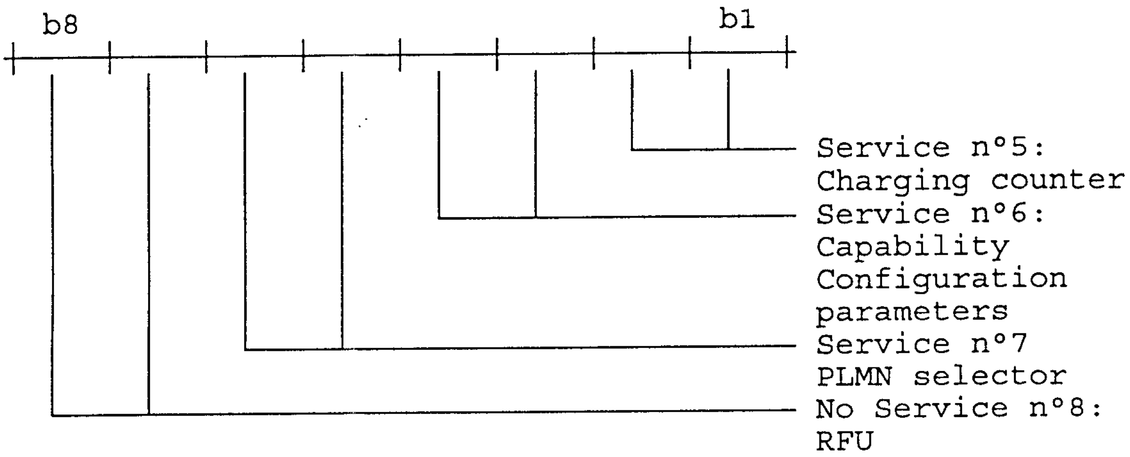
second bit = 1 : service activated in the card
second bit = 0 : service not activated in the card

First byte :

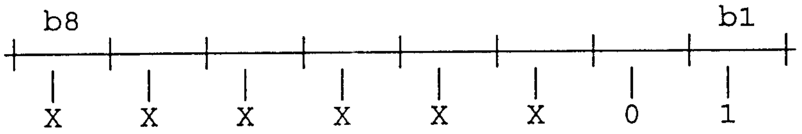


Note: For Service n° 3, the RFU bits are coded 00

Second byte :



example of coding (for the first byte):



means the service of "PIN-Disabling" is allocated but not activated.

Note : other services are possible in the future and will be coded on further bytes in the data-field.

DATA-FIELD - 07 : **IMSI.**

Purpose:

Storing the IMSI

High update activity: **No.**

Data-field attributes:

```
Identifier ........: 6F 07
Type...............: Binary.
Security Policy..:
          Read        : PIN.
          Update      : ADM/AUT.
Block Length........: 9 bytes
```

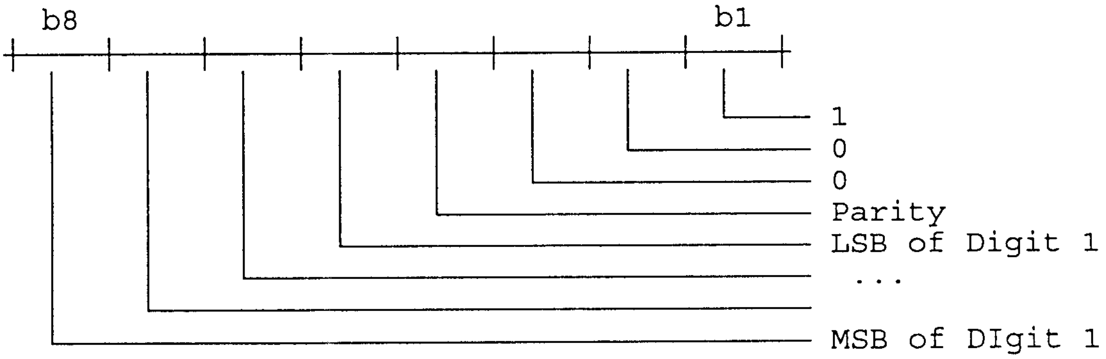
Structure of the data-field :

IMSI Data length = up to 15 digits stored on 9 bytes.

byte 1 : length of the contents of the Mobile Identity information element (in the present case IMSI) according to GSM 04.08 - section 10.5.

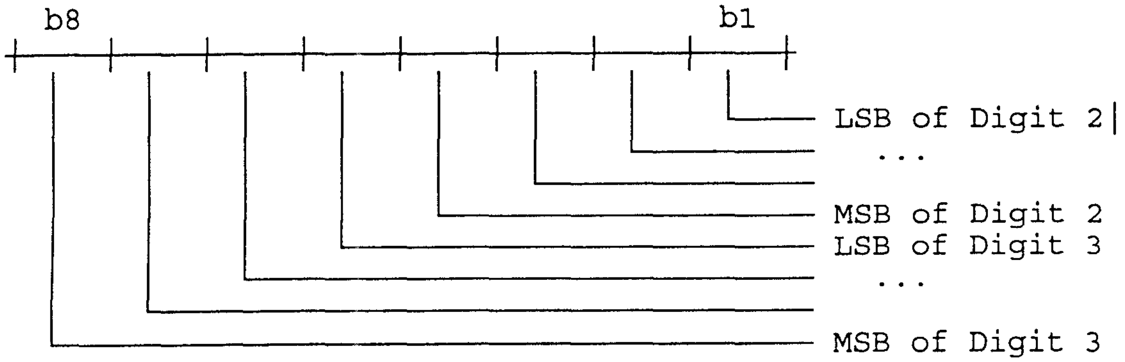
This information element is of variable length. The length indicator refers to the number of significant octets required for the IMSI, not including the length byte. If a network operator choose an IMSI of less than 15 digits, unused nibbles in this SIM data field shall be set to NULL.

byte 2 :

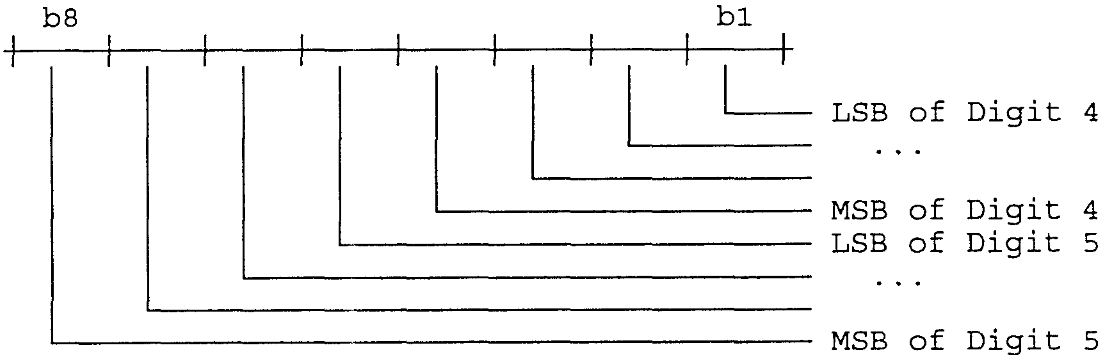


For the parity bit, see GSM 04.08

byte 3 :



byte 4 :



Etc.

DATA-FIELD - 7E: LOCATION INFORMATION : TMSI,LAI,TMSI TIME, UPDATE STATUS.

Purpose:

Storing TMSI, LAI, TMSI TIME, Location update status

High update activity: **Yes**

Data-field attributes:

Identifier .... : 6F 7E
Type................: Binary.
Security Policy..:
    Read : PIN.
    Update : PIN.
Block Length........: 11 bytes

Structure of the data-field:

* TMSI = 4 Bytes
Coding of the TMSI open for each operator.
If the TMSI is less than 4 bytes in length then the unused bits ahead of the MSB should be set to "0". Rec. GSM 04.08 Paragraph 10.5.1.3 refers.

* LAI = 5 Bytes

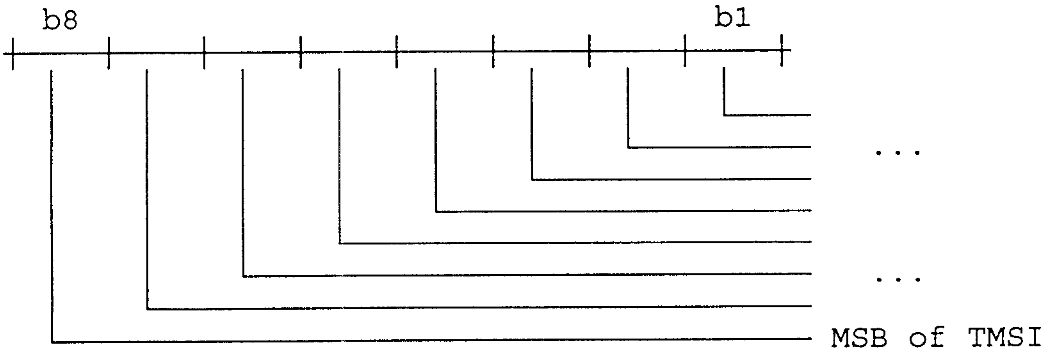
Rec. GSM 04.08 paragraph 10.5.1.3 refers.

* Current value of Periodic Location Updating Timer (T3212) = 1 byte.

* Location update status = 1 byte

Rec. GSM 04.08 paragraph 4.4.4. refers.

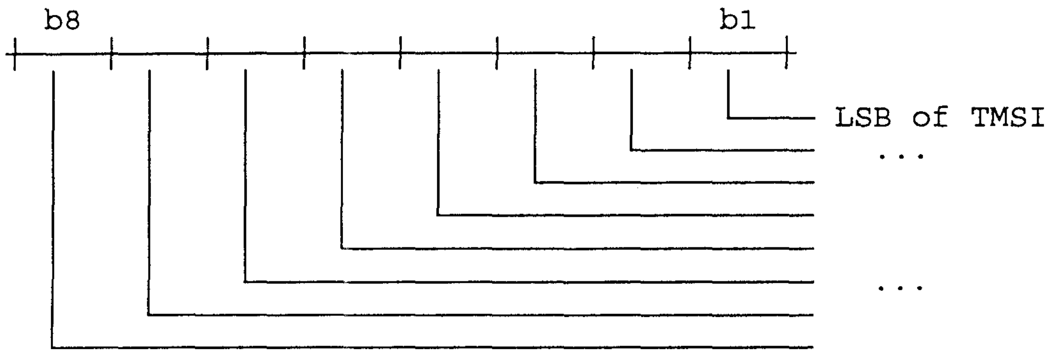
Byte 1 : First byte of TMSI



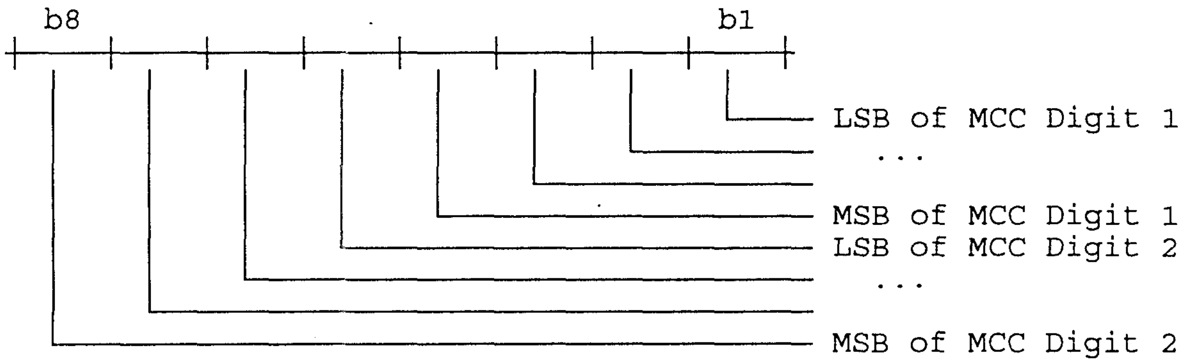
Byte 2 : second byte of TMSI

Byte 3 : third byte of TMSI

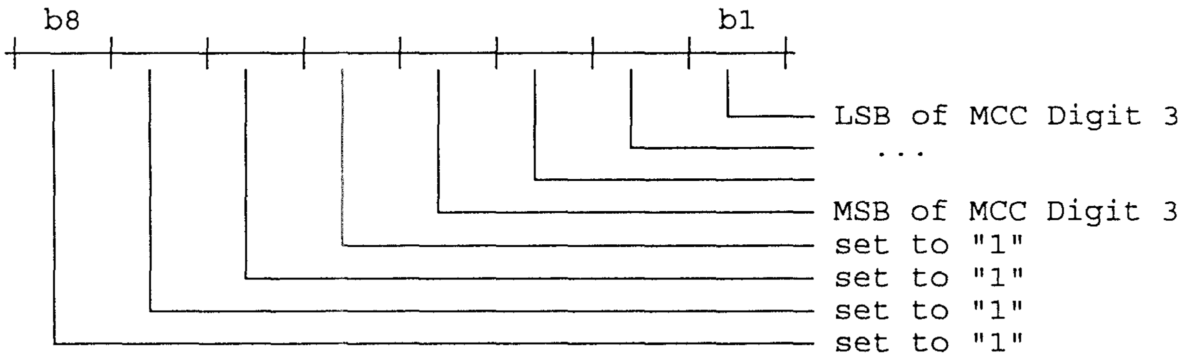
Byte 4 : Fourth byte of TMSI



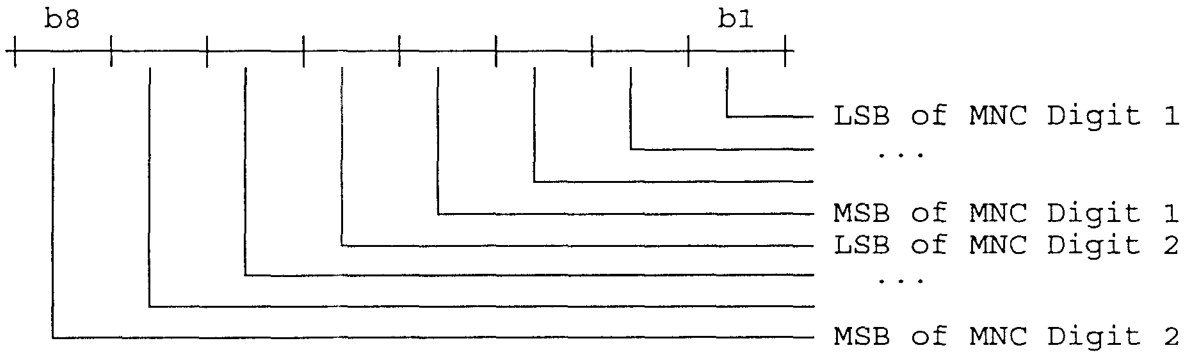
Byte 5 : First byte of LAI : MCC



Byte 6 : Second byte of LAI : MCC (continued)



Byte 7 : Third byte of LAI : MNC



Byte 8 : Fourth byte of LAI : LAC

Byte 9 : Fifth byte of LAI : LAC (continued)

Byte 10 : Current value of Periodic Location Updating Timer (T3212)

The value of the timer T3212 represents remaining time to expiry.

Coding of the T3212 value:

0 = the timer has expired.
1 to FE = remaining time to expiry (in deci-hours), binary coded.
FF = the timer is not running.

Byte 11 : Location update status

Bits :	b3	b2	b1	
	0	0	0	: updated
	0	0	1	: not updated
	0	1	0	: PLMN not allowed
	0	1	1	: Location Area not allowed
	1	1	1	: reserved

The bits b4 to b8 shall be set to zero.

DATA-FIELD - 20: **Key Kc and n**

Purpose:

Storage of encryption key Kc and ciphering key sequence number n.

Kc = 8 Bytes.
n = 1 Bytes (3 Bits Used)

High update activity: **Yes**

Data-field attributes:

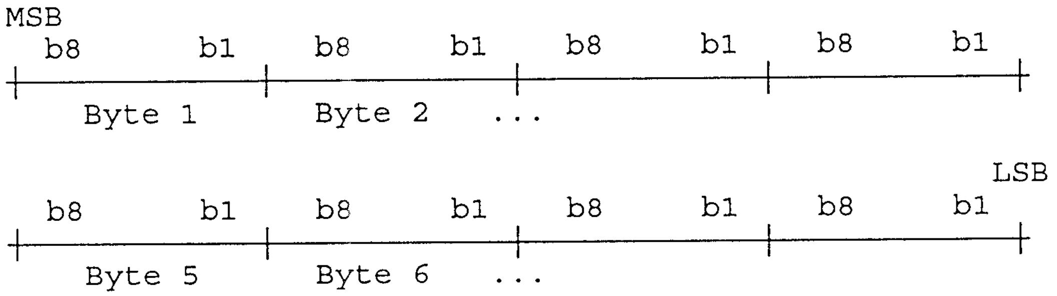
```
Identifier ........: 6F 20
Type...............: Binary.
Security Policy..:
          Read          : PIN.
          Update        : PIN.
Block Length........: 9 bytes
```

Structure of the data-field:

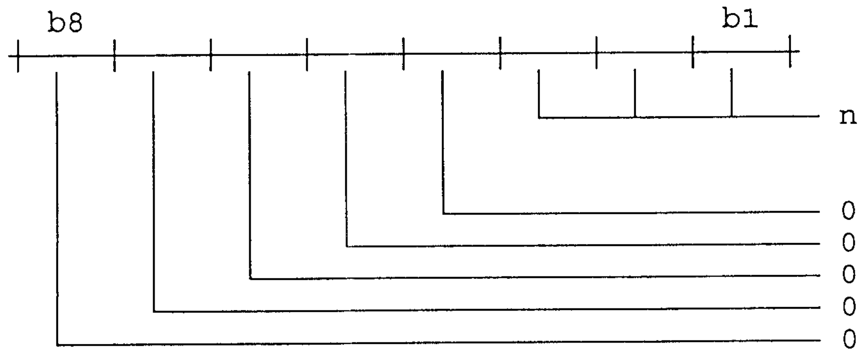
The LSB of Kc is the LSB of the eighth byte.
The MSB of Kc is the MSB of the first byte.

example : Kc = 'By1 By2 ... By8 '

In the memory of the SIM :



and n :



Note: TS GSM 04.08 defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administration phase.

DATA-FIELD - 30: **PLMN SELECTOR**

Purpose :

Storage is required for at least eight PLMN's, as specified by the PLMN operators. This information determined by the user/operator defines the preferred PLMN's of the user in priority order.

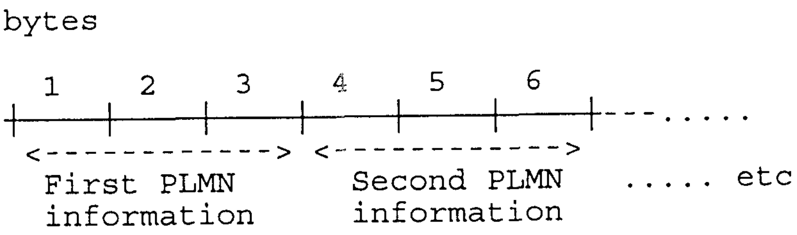
High update activity: **No.**

Data-field attributes:

Identifier ....: 6F 30
Type................: Binary.
Security Policy..:
Read : PIN
Update : PIN
Block Length......: Fixed during administrative management phase

Structure of the data-field:

Each PLMN information is coded as 3 bytes and structured with MNC (Mobile Network Code) and MCC (Mobile Country Code) digits (GSM 04.08 section 10.5.1.3. refers)



DATA-FIELD - 74: **BCCH INFORMATION**

Purpose:

Storing the BCCH information according to Rec. GSM 04.08.

BCCH storage may reduce the extent of a Mobile Stations search of BCCH carriers when selecting a cell. The BCCH carrier lists in an MS shall be in accordance with the procedures specified in recommendation GSM 04.08.

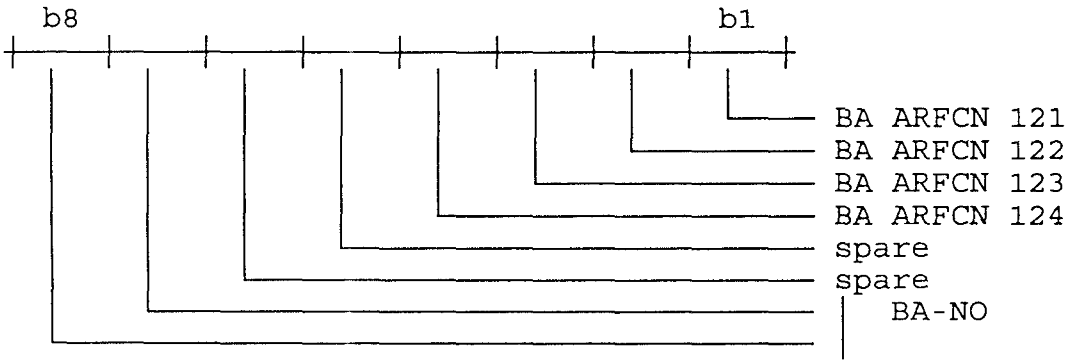
High update activity: **Yes**

Data-field attributes:

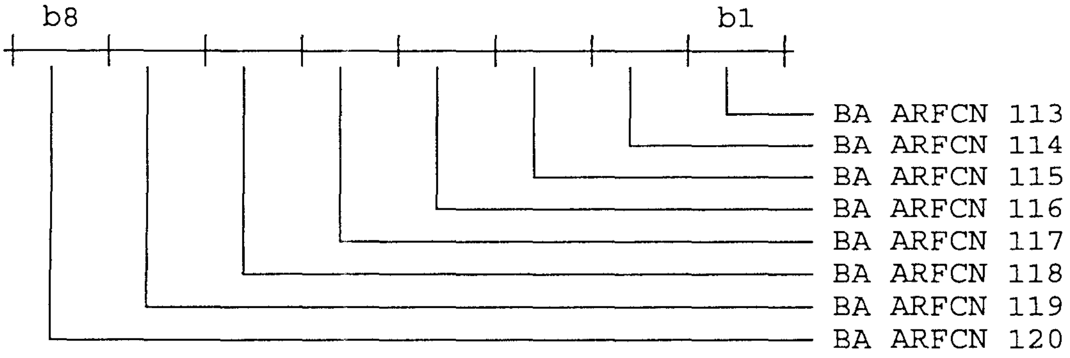
```
Identifier ........: 74
Type...............: Binary.
Security Policy..:
          Read        : PIN.
          Update      : PIN.
Block Length........: 16 bytes
```

Structure of the data-field :

Byte 1:

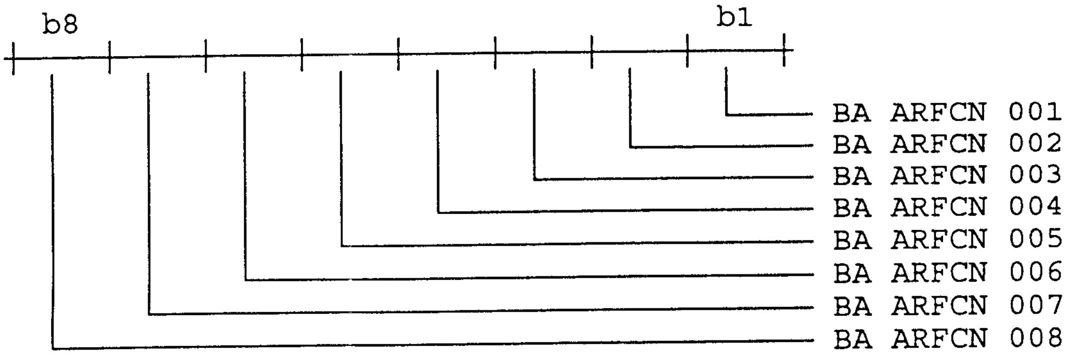


Byte 2:



...

Byte 16



Note :

BA-NO means BCCH allocation number.
BA ARFCN means allocation absolute radio frequency channel number N.
ARFCN means absolute radio frequency channel number N. N=1 corresponds to the lowest frequency.
For a RF channel with ARFCN = N belonging to the BCCH allocation the BA ARFCN bit is coded with a "1" ; N=1,2,...,124.
For a RF channel with ARFCN = N not belonging to the BCCH allocation the BA ARFCN bit is coded with a "0" ; N=1,2,...,124.

Reference : Rec. GSM 04.08 paragraph 10.5.2.13

DATA-FIELD - 78: **ACCESS CONTROL**

Purpose:

This data-field contains the access control class. The access control class is a parameter to control the RACH utilization. 15 classes are split into 10 classes randomly allocated to normal subscribers and 5 classes allocated to specific high priority users. For more information see Rec. GSM 02.11.

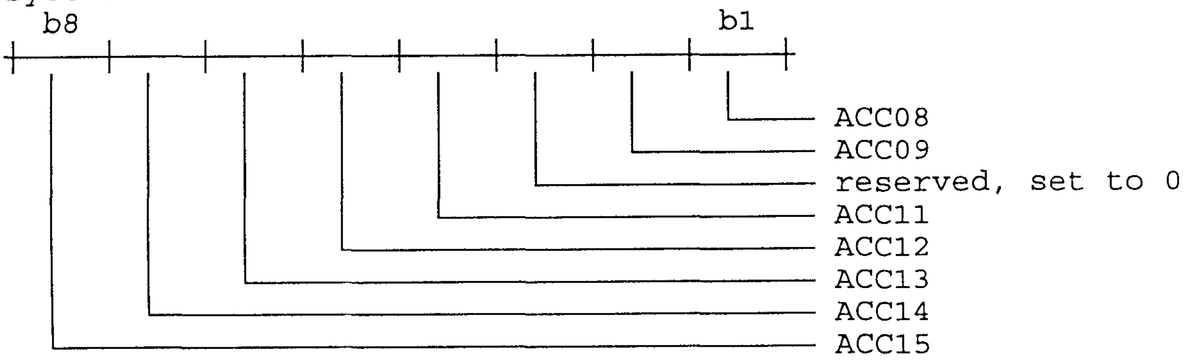
High update activity: No.

Data-field attributes:

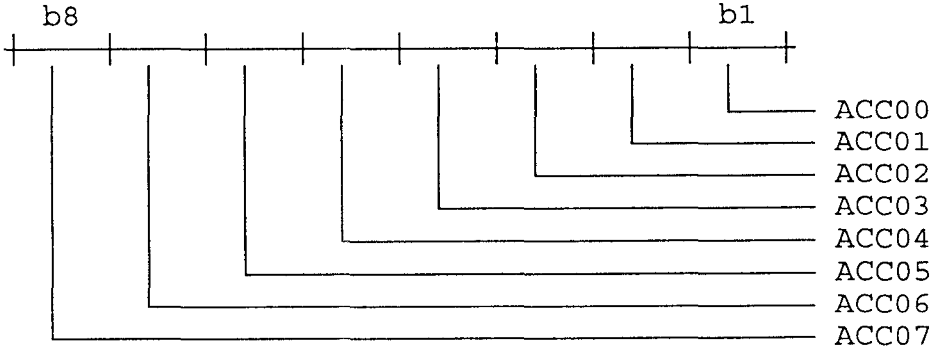
Identifier ....: 6F 78
Type........ : Binary.
Security Policy..:
  Read : PIN.
  Update : ADM/AUT.
Block Length........: 2 bytes

Structure of the data-field:

Byte 1:



Byte 2:



. ACCXX coded with "0" means "not allocated"
. ACCXX coded with "1" means "allocated"

DATA-FIELD - 3A: **ABBREVIATED DIALING NUMBER.**

Purpose:

This data-field contains

a) dialing numbers
b) associated alpha-tagging
c) a network/bearer capability identifier
d) an identifier reserved for future use.

The information is stored in records.

Each record contains

i) an alpha-identifier on (X) bytes. The value of X may vary from one SIM to another, but is identical for each record in the data-field;

ii) the telephone number information as defined in GSM 04.08 Fig 10.50 comprising

a) the number of up to 20 digits stored on 10 bytes
b) the type of number
c) the numbering plan identification

iii) a capability/configuration identification byte. This identifies the number of a record in data field 6F 3D which contains capability/configuration parameters associated with the dialling number and required for the call. This will be particularly useful for the set up of data calls. The use of this byte is optional, and can be set to NULL

iv) an identification byte reserved for future use, which shall be set to NULL.

High update activity: **No.**

Data-field attributes:

Identifier ....: 6F 3A
Type................: Formatted.
Security Policy..:
Read : PIN.
Update : PIN.

Record Length.......: (14 + X) bytes; using the instruction GET-RESPONSE the ME can determine the value of X.

Coding :

The alpha-tagging shall use ASCII with b8 set to 0. The telephone numbers shall be coded in BCD.

Structure of the data-field:

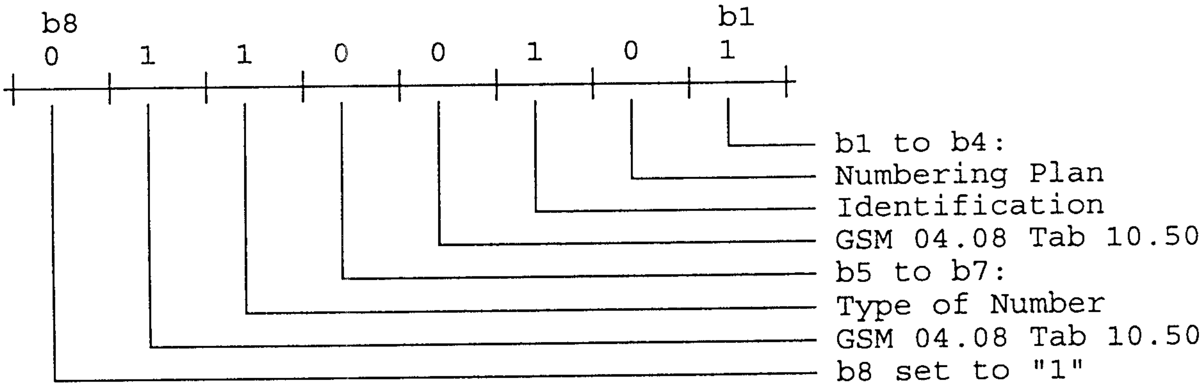
```
alpha identifier      telephone number    identifiers.
<... X bytes ......><..... 12 bytes .....><1 byte><1 byte>

I---I---I............I---I---I---I---I........I---I---I
 (a) (b)              (c) (d) (e) (f)          (g) (h)
```

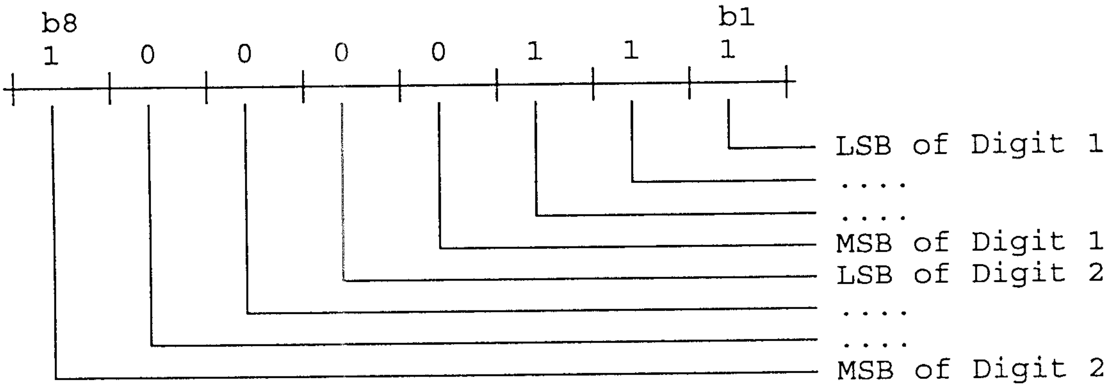
Byte a : first character of Alpha-identifier
Byte b : second character of Alpha-identifier

Byte c : length of BCD number contents (GSM 04.08 Fig 10.50)

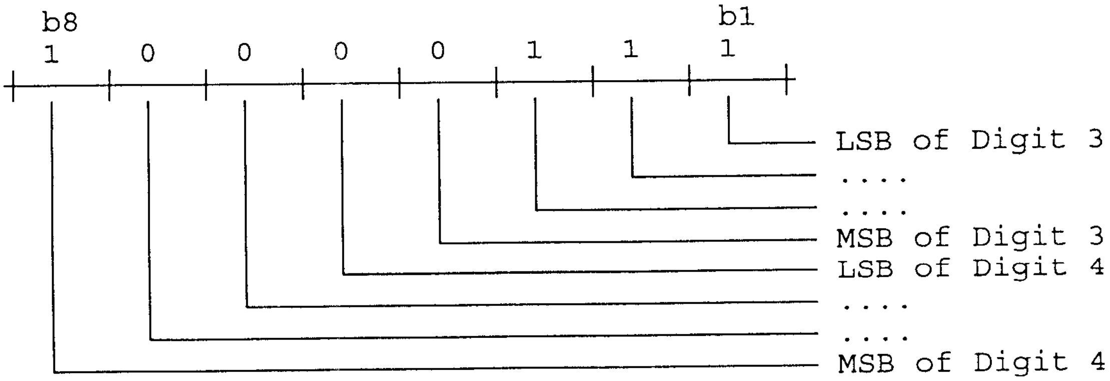
Byte d :



Byte e:



Byte f:



Byte g: Capability/Configuration Identification byte. This is coded in binary and gives the associated record number in data field 6F 3D.

Byte h: Identification byte reserved for future use, which shall be set to NULL.

NOTES:

1) GSM 04.08 allows the number information field to be of variable length. However, the SIM requires that formated data fields contain records of equal length, and 10 bytes (20 nibbles of BCD information) are allocated for storage of digits. When Abbreviated Dialing Numbers require less than 20 digits, the excesss nibbles at the end of the record shall be set to "NULL".

2) The Abbreviated Dialing Number data-field is part of the Telecom Directory, therefore able to be used by both GSM and other applications on multi-function cards. If the non-GSM application does not recognize Type of Number (TON) and Number Plan Identification (NPI) then the information relating to the national dialing plan must be held within the digits field and the TON and NPI fields set to UNKNOWN. This format would be acceptable for GSM operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

   e.g. SIM storage of an International Number using E164 numbering plan

	TON	NPI	Digit field
GSM application	001	0001	abc...
Other application also compatible with GSM	000	0000	xxx...abc...

   where abc... denotes the subscriber number digits, and xxx... denotes a national prefix replacing TON and NPI.

3) When the ME acts upon an abbreviated dialling number data field sith a SEEK instruction in order to identify a character string in the alpha-identifier, it is the responsability of the ME to ensure that the number of characters used as SEEK parametes are less than or equal to the value of X (the number of bytes in the alpha-identifier) if the MMI allows the user to offer a greater number.

DATA-FIELD - 3D: **CAPABILITY/CONFIGURATION PARAMETERS.**

Purpose:

This data-field will store parameters of required network and bearer capabilities and ME configuration associated with a call established using an abbreviated number.

High update activity: **No.**

Data-field attributes:

Identifier ....: 6F 3D
Type................: formatted.
Security Policy..:
        Read   : PIN.
        Update   : PIN.
Record Length.......: 14 bytes

Structure of the data-field:

Each record will comprise 14 bytes

e.g.

- 10 bytes (GSM 04.08 fig 10.5.2 refers) for Network/bearer capability.
- 4 bytes (format For FS) for the ME user Interface configuration.

DATA-FIELD - 3E:

Purpose:

This data-field is reserved for future GSM use.

High update activity:

Data-field attributes:

```
Identifier ........: 6F 3E
Type................:
Security Policy..:
          Read         :
          Update       :
Record Length.......  :
```

Structure of the data-field:

DATA-FIELD - 3C: **SHORT MESSAGE(S) STORAGE.**

Purpose:

This data field contains information in accordance with GSM 03.40 comprising short messages (and associated parameters) which have either been received by the MS from the network, or are to be used as a MS originated message.

High update activity: **No.**

Data-field attributes:

Identifier ....: 6F 3C
Type................: Formatted
Security Policy...:
Read : PIN
Update : PIN

Record Length.......: 176 bytes

The number of short messages to be managed by the SIM is chosen during personalisation phase. Messages are stored in records.

Record Structure:

Byte 1 : Status Byte for the record which can be used as a pattern in the SEEK instruction.

b1 = 0	means "Free space"
b1 = 1	means "Used space"

b3	b2	Meaning
0	0	Message received by MS from network; message read
0	1	Message received by MS from network; message to be read
1	0	MS originating message; message sent to the network
1	1	MS originating message; message to be sent

b4 to b8 are reserved and set to "0".

When a record is free (b1 = 0) the byte shall have the value 00 HEX.

Bytes commencing with byte 2 contain the TS-Service-Centre-Address as specified in GSM 04.11. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in GSM 03.40, with identical coding and ordering of parameters.

Any TP-message reference contained in an MS originated message stored in the SIM, shall have a value as follows:

	Value of the TP-message-reference
message to be sent ....:	NULL

message sent to the network: the value of TP-Mesage-Reference used in the message sent to the network.

Any bytes in the record following the TPDU shall be filled with NULL.

DATA-FIELD -3B: **FIXED DIALING NUMBERS.**

Purpose:

Reserved for possible future definition of a fixed dialling feature (not relevant in GSM Phase 1).

High update activity: .

Data-field attributes:

```
Identifier .........: 6F 3B
Type................:
Security Policy..:
          Read          :
          Update        :

Record Length.......:
```

Coding :

Structure of the data-field:

DATA-FIELD - 39: **CHARGING COUNTER.**

Purpose:

Storing the information about the charge of the call(s). This information is just indicative for the user.

High update activity: **Yes**

Data-field attributes:

```
Identifier ........: 6F 39
Type................: Binary.
Security Policy..:
          Read         : PIN.
          Update       : PIN.
Block Length........: 02
```

Structure of the data-field:

FOR FURTHER STUDY

DATA-FIELD - 7B: **FORBIDDEN PLMNs**

Purpose:

Storage is required for four PLMNs. This data field will be read by the ME as part of the SIM initialisation procedure, and indicates PLMNs which the MS shall not automatically attempt to access.

A PLMN is written to the data field if a network (other than the HPLMN) rejects a Location Update with the cause "PLMN not allowed' .

The ME shall manage the list as a cyclic store, e.g., if four PLMNs are stored in the list and another rejected Location Update occurs then the oldest member of the list of PLMNs in the data field shall be lost. The modified data field is stored on the SIM by the ME using an UPDATE instruction. No manipulation of the list is undertaken by the SIM.

High update activity: **No.**

Data-field attributes:

```
Identifier .........: 6F 7B
Type................: Binary.
Security Policy..:
          Read        : PIN
          Update      : PIN

Block Length........: 12 bytes
```

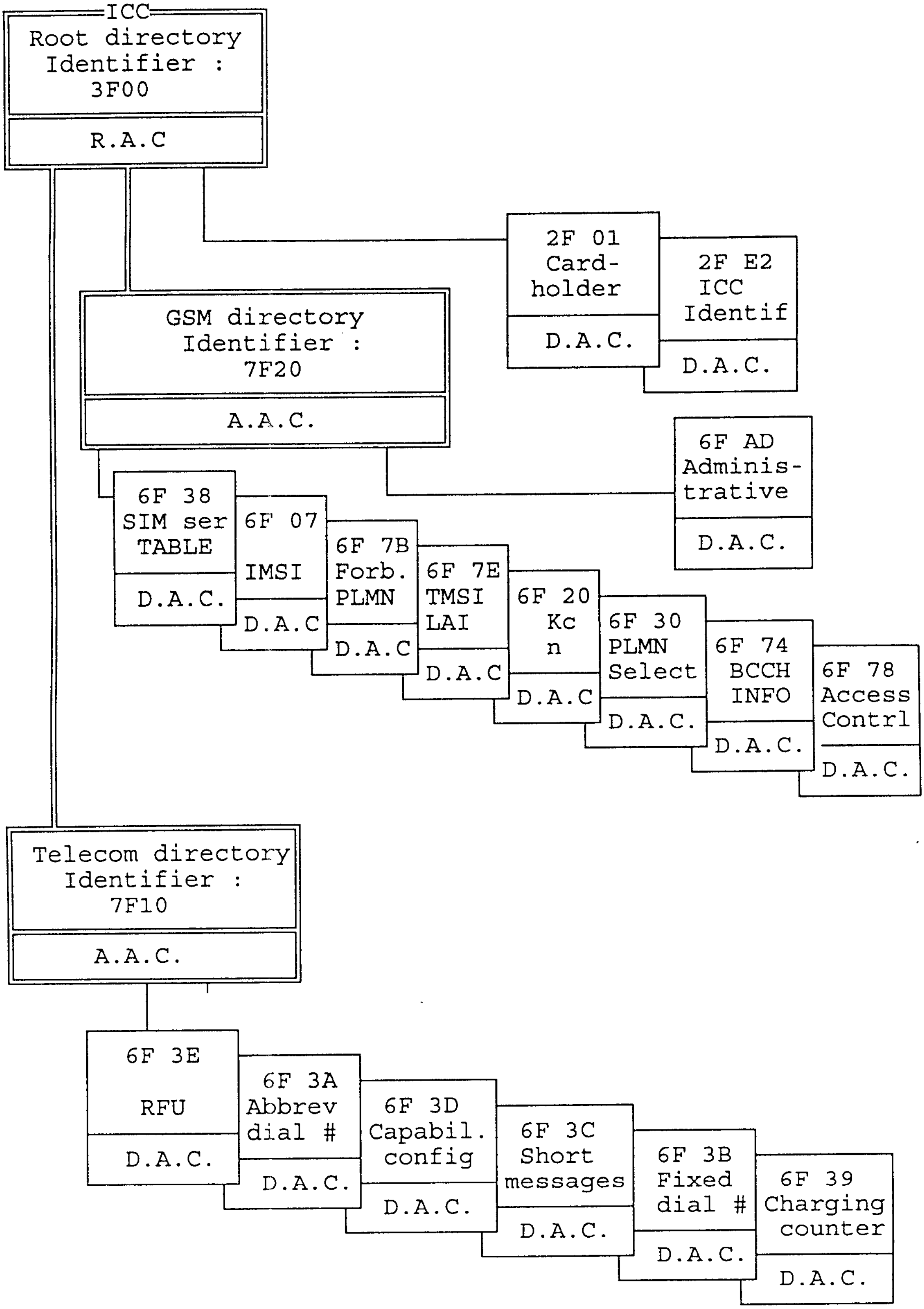
Structure of the data-field:

Each PLMN information is structured as the Mobile Country Code (MCC) and Mobile Network Code (MNC) as specified in GSM 04.08 paragraph 10.5.1.3. Three bytes are required for each PLMN. If storage for less than four PLMNs is required the excess bytes shall be set to NULL (FF Hex).

bytes

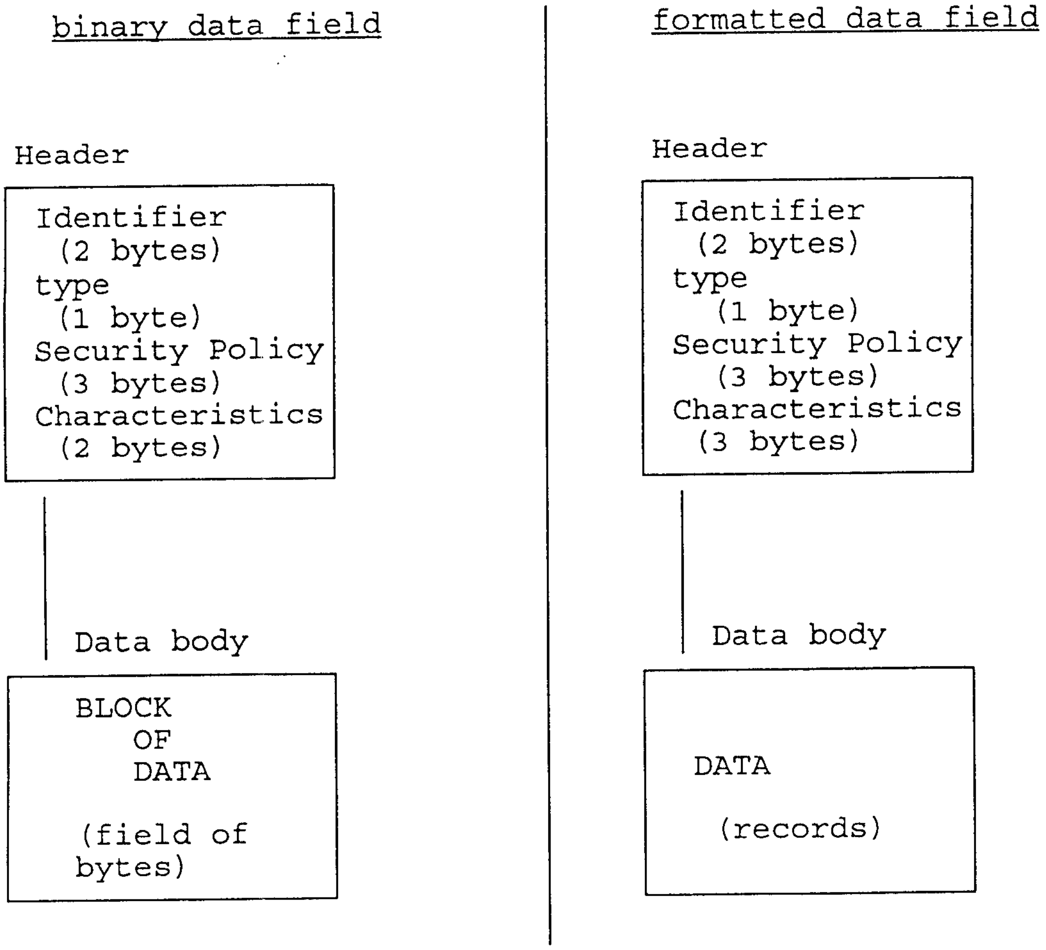
```
  1    2    3    4     5    6    7    8    9   10   11   12
I----I----I----I----I----I----I----I----I----I----I----I----I
< oldest PLMN > <  2nd PLMN   > <  3rd PLMN   > < newest PLMN >
```

SIM IMPLEMENTATION MODEL (Numbers are Hexadecimal)



R.A.C = Root Access Conditions
A.A.C = Application Access Conditions
D.A.C = Data-Field Access Conditions.
DF xx = Data-Field identifier.

DIFFERENT TYPES OF DATA-FIELDS



4. GSM APPLICATION PROTOCOL

4.1. GENERAL

In the GSM application protocol of the SIM, messages are exchanged with the ME (during GSM network operation phase), or any accepting device (during GSM administrative management phase). A message can be a command or a response.

- A GSM instruction (also called Command-Response Pair) will be a sequence made of one command and of the associated response. The response contains condition codes followed eventually by data.

- A GSM function is a process (here called a procedure) (accomplished by one or more GSM instruction(s) and resultant action(s)), which is used to perform all or part of an application-oriented task (cf future draft of ISO 7816/4). A procedure must be considered as a whole, that is to say that the corresponding function is achieved only and only if the procedure is completed. The ME shall guarantee that, when it is correctly operated (i.e., accordingly to the manufacturer's manual), the outside world cannot control any unspecified interruption of the sequence (if any) of instructions which realize the procedure, without implying the abort of the procedure itself.

- The GSM application protocol is specified in that a simultaneous opening (according to the evolution of international standards) of applications other than the GSM application is intended to be possible (e.g. multiservice IC cards, for FS).

4.2. FUNCTIONAL DESCRIPTION OF THE PROCEDURES AT THE SIM INTERFACE IN GSM OPERATIONS

When the SIM is involved in GSM network operations, it is interfaced with a ME; the general functions it provides are defined in Rec. GSM 02.17 (par. 2.2).

When the SIM is involved in GSM administrative management operations, it is interfaced with appropriate terminal equipment, here called a SIM Accepting Device (SIM-AD). The general functions it provides are left to each network operator discretion.

When the SIM is interfaced with a ME for the GSM application, the ME plays the role of the master and the SIM plays the role of the slave in the procedures.

Some procedures at the SIM-ME interface may be associated with MMI procedures; the descriptions hereafter do not intend to infer any specific MMI procedures. These MMI procedures are not part of the subject. However, in the list given below, they are marked as "MMI".

Some other procedures are clearly not user dependent; they are directly connected with the relations between the ME and the network. In the list given below, they are marked as "NET".

The list of procedures at the SIM-ME interface in GSM network operation is as follows :

A. SIM management procedures :

-	1. SIM initialization	MMI
-	2. SIM de-activation	MMI
-	3. SIM service table request	NET
-	4. Administrative information request	MMI
-	5. SIM identification request	MMI

B. User PIN code related procedures :

-	6. User PIN code verification	MMI
-	7. User PIN code substitution	MMI
-	8. User PIN code disabling	MMI
-	9. User PIN code reenabling	MMI
-	10.SIM unblocking procedure	MMI

C. GSM security related procedures :

-	11.GSM algorithms computation	NET
-	12.TMSI request	NET
-	13.LAI request	NET
-	14.TMSI updating	NET
-	15.LAI updating	NET
-	16.cipher key request	NET
-	17.cipher key updating	NET
-	18.ciph. key seq. number request	NET
-	19.ciph. key seq. number updating	NET
-	20.IMSI request	NET
-	21.TMSI time request	NET
-	22.TMSI time updating	NET
-	23.BCCH information request	NET
-	24.BCCH information updating	NET
-	25.Access control information request	NET
-	44.Forbidden PLMN information request	NET
-	45.Forbidden PLMN information updating	NET
-	46.Location update status request	NET
-	47.Location update status updating	NET

D. Mobile subscriber information related procedures :

-	26.short message storage	MMI
-	27.short message erasure	MMI
-	28.short message request	MMI
-	29.charging information updating	NET
-	30.charging information erasure	MMI
-	31.charging information request	MMI
-	32.abbreviated dialing number storage	MMI
-	33.abbreviated dialing number erasure	MMI
-	34.abbreviated dialing number request	MMI
-	35.Capability config. param. request	MMI
-	36.Capability config. param. updating	MMI
-	37.Capability config. param. erasure	MMI
-	42.PLMN selector request	NET
-	43.PLMN selector updating	MMI (*)

Note : services marked with a (*) may be ADM phase services.

The functions listed in Section A are mandatory to execute all the other SIM functions. A GSM-session of the SIM in the GSM application is the interval of time starting at the completion of the SIM activation procedure and ending either at the completion of the deactivation procedure, or at the first instant the link between the SIM and the ME is interrupted for any reason.

As specified in Rec. GSM 02.17, the procedures listed in Sections B and C are mandatory in the SIM (and consequently mandatory in the SIM-ME application protocol). According to Rec. GSM 02.17, the procedures listed in Section 4 are not mandatorily implemented in each SIM, but if they are implemented, it must be done in accordance with section D.

In what follows, each procedure is functionaly described.

The following procedures have to be implemented according to state diagrams and tables of the annexes.

1. SIM initialization procedure:

The ME asks the SIM for initialization of GSM service. The SIM initialization procedure is as follows.

The ME requests the PIN enabled/disabled indicator (not protected in reading). If the PIN enabled/disabled indicator is set "enabled", the ME starts the PIN code verification procedure. After the successful completion of this procedure, the SIM is ready to be operated for a session. If the PIN enabled/disabled indicator is set "disabled", the SIM is ready to be operated for a session.

Afterwards, the ME runs the following procedures:

- TMSI request
- LAI request
- cipher key request
- ciphering key sequence number request
- TMSI time request
- PLMN selector
- SIM capability request
- IMSI request
- administrative information request
- BCCH information request.
- forbidden PLMN information request
- access control information request
- location update status request

After these procedures are completed, the MS (i.e. the SIM and the ME together) is ready for GSM network operations.

2. SIM de-activation procedure :

(this procedure is not to be confused with the de-activation of the contacts in IS 7816/3)

The SIM de-activation procedure is initiated by the ME as follows.

The ME runs all the updating procedures which are necessary to transfer from the ME to the SIM the following subscriber related information:

- TMSI
- location area identification
- cipher key
- ciphering key sequence number
- TMSI time

- BCCH information
- advice of charge
- forbidden PLMN information
- location update status.

As soon as the SIM indicates that these procedures are completed, the ME-SIM link is de-activated. This means that any further procedure needs a SIM activation procedure first.

Finally, the ME deletes all these subscriber related information elements from its memory, according to Rec. GSM 02.17.

3. SIM service table request procedure :

The ME asks the SIM for GSM capability request procedure. The GSM capability request procedure in the SIM is as follows.

The SIM sends to the ME the list of mobile subscriber information related services (short message storage, charging information storage, abbreviated dialing number storage, fixed dialing number storage, barring of outgoing call, automatic PLMN selector) supported by the SIM.

4. Administrative information request :

The ME asks the SIM for administrative information (blocking counter, etc) request procedure. The SIM sends to the ME the information of the administrative information data-field.

5. SIM identification request :

The ME asks the SIM for SIM identification request procedure. The SIM sends to the ME the information of the SIM identification data-field.

6. User PIN code verification :

The ME asks the SIM for user PIN code verification procedure and sends the presented PIN to the SIM. The user PIN code verification procedure in the SIM is as follows.

The SIM compares the presented PIN with the PIN it has in memory. If they are identical, then the authentication is said to be succesful: the SIM sends "OK" to the ME and unlocks all the actions for the data-fields within the GSM application protected by PIN. This unlocking is valid for all the procedures in the GSM session. The counter of false successive PIN presentations (PIN error counter) is set to 0.

If the presented PIN and the PIN in memory are not identical, then the authentication is not successful. The SIM increments the PIN error counter. If the number of PIN errors is less than 3, the SIM allows the ME to offer a new PIN presentation during further procedures. If the value of the PIN error counter is greater or equal to 3, then the SIM is put in the status "blocked" and the SIM is no longer usable for GSM application in network operation until it is "unblocked".

7. User PIN code substitution :

The user PIN code substitution procedure requires that the ME has the "old" PIN and the "new" PIN proposed by the user (MMI). The ME asks the SIM for a user PIN code change and sends together the "old" PIN and the "new" PIN.

The SIM compares the presented old PIN with the PIN it has in memory. If they are identical, then the authentication is said to be succesful: the SIM sends "OK" to the ME and unlocks all the actions for the data-fields within the GSM application protected by PIN. This unlocking is valid for all the procedures in the GSM session. The counter of false successive PIN presentations (PIN error counter) is set to 0.

After the user "old" PIN has been verified successfully the SIM replaces the "old" PIN code stored in its memory by the "new" one.

If the "old" PIN and the PIN in memory are not identical, then the authentication is not successful and the procedure aborts. The SIM increments by one unit the PIN error counter. If the number of PIN errors is less than 3, the SIM allows the ME a new PIN presentation during a further procedure in the same GSM session. If the value of the PIN error counter is greater or equal to 3, then the SIM is put in the status called "blocked" and the SIM is no longer usable for GSM application in network operation until it is "unblocked".

8. User PIN code disabling :

The user PIN code disabling procedure requires that the ME has the PIN code (MMI). The ME asks the SIM for a user PIN code disabling and sends the user PIN code. The user PIN code disabling procedure in the SIM is as follows.

The SIM compares the presented PIN with the PIN it has in memory. If they are identical, then the authentication is said to be succesful: the SIM sends "OK" to the ME and unlocks all the actions for the data-fields within the GSM application protected by PIN. This unlocking is valid for all the procedures in the GSM session. The counter of false successive PIN presentations (PIN error counter) is set to 0.

After the user PIN code has been verified successfully, the SIM proceeds as follows. The SIM checks the PIN disabling allowed/not allowed indicator: if it is set "disabling not allowed", then the user PIN code disabling procedure is not allowed and the SIM tells that fact to the ME. If the PIN disabling allowed/not allowed indicator is set "disabling allowed", then the user PIN code disabling procedure is allowed and the SIM sets the PIN enabled/disabled indicator "disabled". All GSM data protected by a user PIN code verification (marked "PIN" in the security policy) are now accessible (as if they were marked "ALW" in those tables).

If the user PIN code authentication is not successful then the procedure aborts. The SIM increments by one unit the PIN error counter. If the value of the PIN error counter is less than 3, the SIM allows the ME a new PIN presentation during a further procedure in the same GSM session. If the number of PIN errors is greater or equal to 3, then the SIM is put in the status called "blocked" and the SIM is no longer usable for GSM application in network operation until it is unblocked.

9. User PIN code reenabling :

The ME asks the SIM for user PIN code reenabling procedure. The user PIN code reenabling procedure in the SIM is as follows.

The user PIN code reenabling procedure requires that the ME has the user PIN code (MMI). The ME asks the SIM for a user PIN code reenabling and sends the presented PIN code.

The SIM compares the presented PIN with the PIN it has in memory. If they are identical, then the authentication is said to be succesful: the SIM sends "OK" to the ME and unlocks all the actions for the data-fields within the GSM application protected by PIN. This unlocking is valid for all the procedures in the GSM session. The counter of false successive PIN presentations (PIN error counter) is set to 0.

After the user PIN code has been verified successfully the SIM set the PIN enabled/disabled indicator "enabled".

If the presented PIN and the PIN in memory are not identical, then the authentication is not successful and the procedure aborts. The SIM increments by one unit the PIN error counter. If the value of the PIN error counter is less than 3, the SIM allows the ME a new PIN presentation during a further procedure. If the number of PIN errors is greater or equal to 3, then the SIM is put in the status called "blocked" and the SIM is no longer usable for GSM application in network operation until it is "unblocked".

10. GSM application unblocking procedure :

The ME asks the SIM for GSM application unblocking procedure, sends the personal unblocking key and a new PIN code (i.e., chosen by the user). This can be done either if the PIN is blocked or not. The SIM unblocking procedure in the SIM is as follows.

The SIM checks the value of the unblocking error counter: if its value is greater or equal to 10, then the SIM tells the ME that unblocking is no longer possible. If the value of the unblocking error counter is less than 10, the SIM proceeds as follows.

The SIM compares the presented personal unblocking key with the one stored in its own memory. If they are identical, then the SIM unblocking is said to be succesful: the SIM sends "OK" to the ME and sets the new PIN code in its memory. The PIN error counter and the unblocking error counter are set to zero. The SIM status is set "unblocked".

All the actions for the data-fields protected by PIN are unlocked.

If the presented personal unblocking key and the one stored in the SIM memory are not identical, then the SIM unblocking is not successful. The SIM increments by one the unblocking error counter. If the value of the unblocking error counter is less than 10, the SIM asks the ME for a new personal unblocking key presentation. If the value of the unblocking error error counter is greater or equal to 10, then the SIM cannot be unblocked.

11. GSM algorithms computation :

The ME asks the SIM for GSM algorithms computation procedure and sends the number RAND. The GSM algorithms computation procedure in the SIM involves performing the two GSM security algorithms called A3 and A8 (see Rec. GSM 03.20 for the definitions). These algorithms are chosen at the PLMN operator's discretion and either A3 and A8 are two distinct algorithms or A3 and A8 are combined in one algorithm, here called A38. The procedure in the SIM is as follows.

a) A3 and A8 are distinct:

The SIM performs successively Algorithm A3 and Algorithm A8, both of them with the authentication key Ki kept in memory and with RAND as inputs. The output SRES of A3 and the output Kc of A8 are combined into one response, say SRES-Kc, which is sent to the ME when requested by a subsequent GET-RESPONSE instruction.

b) A3 and A8 are combined into A38 :

The SIM performs Algorithm A38, with the authentication key Ki kept in memory and with RAND as inputs. The output of A38 is one response (formed of two parts SRES and Kc). The whole response SRES-Kc is sent to the ME when requested by a subsequent GET-RESPONSE instruction.

The format of RAND is 128 bits (see GSM 04.08:10.5.3.1).
The format of SRES is 32 bits (see GSM 04.08:10.5.3.2).
The format of Kc is 64 bits (see GSM 03.20:Annex 3).
Therefore, the format of SRES-Kc is 96 bits.

note : the response SRES/Kc is identical for cases a) and b).

12. TMSI request :

The ME asks the SIM for TMSI request procedure. The TMSI request procedure in the SIM is as follows.

The SIM reads the value of TMSI it has in memory, and sends it to the ME.

13. LAI request :

The ME asks the SIM for LAI request procedure. The LAI request procedure in the SIM is as follows.

The SIM reads the value of LAI it has in memory, and sends it to the ME.

14. TMSI updating :

The ME asks the SIM for TMSI updating procedure and sends the updated value of TMSI. The TMSI updating procedure in the SIM is as follows.

The SIM stores the updated value of TMSI it received from the ME in the memory allocated to TMSI, in place of the former value of TMSI.

15. LAI updating :

The ME asks the SIM for LAI updating procedure and sends the updated value of LAI. The LAI updating procedure in the SIM is as follows.

The SIM stores the updated value of LAI it received from the ME in the memory allocated to LAI, in place of the former value of LAI.

16. Cipher key request :

The ME asks the SIM for cipher key request procedure. The cipher key request procedure in the SIM is as follows.

The SIM sends the value of the cipher key Kc it has in memory to the ME.

17. Cipher key updating :

The ME asks the SIM for cipher key updating procedure and sends the updated value of the cipher key Kc. The cipher key updating procedure in the SIM is this the right way round.

The SIM stores the updated value of Kc it received from the ME in the memory allocated to the cipher key, in place of the former value of Kc.

18. Ciphering key sequence number request :

The ME asks the SIM for ciphering key sequence number request procedure. The ciphering key sequence number request procedure in the SIM is as follows.

The SIM sends the value of the ciphering key sequence number (cipher key counter in Rec. GSM 02.17) it has in memory to the ME.

The format of the ciphering key sequence number is 3 bits but always uses one byte (see GSM 04.08: 10.5.1.2).

19. Ciphering key sequence number updating :

The ME asks the SIM for ciphering key sequence number updating procedure and sends the updated value of the ciphering key sequence number. The ciphering key sequence number updating procedure in the SIM is as follows.

The SIM stores the updated value of the ciphering key sequence number it received from the ME in the memory allocated to the ciphering key sequence number, in place of the former value of it.

The format of the ciphering key sequence number is 3 bits but always uses one byte (see GSM 04.08: 10.5.1.2).

20. IMSI request :

The ME asks the SIM for IMSI request procedure. The IMSI request procedure in the SIM is as follows.

The SIM reads the value of IMSI it has in memory, and sends it to the ME.

21. TMSI time request :

The ME asks the SIM for TMSI time request procedure. The TMSI time request procedure in the SIM is as follows.

The SIM reads the value of TMSI time it has in memory, and sends it to the ME.

22. TMSI time updating :

The ME asks the SIM for TMSI time updating procedure and sends the updated value of TMSI time. The TMSI time updating procedure in the SIM is as follows.

The SIM stores the updated value of TMSI time it received from the ME in the memory allocated to TMSI time, in place of the former value of TMSI time.

23. BCCH information request

The ME asks the SIM for BCCH request procedure. The BCCH request procedure in the SIM is as follows.

The SIM reads the value of BCCH it has in memory, and sends it to the ME.

24. BCCH information updating

The ME asks the SIM for BCCH updating procedure and sends the updated value of BCCH. The BCCH updating procedure in the SIM is as follows.

The SIM stores the updated value of BCCH it received from the ME in the memory allocated to BCCH, in place of the former value of BCCH.

25.Access control information request

The ME asks the SIM for Access control information request procedure. The Access control information request procedure in the SIM is as follows.

The SIM reads the value of the Access control information it has in memory, and sends it to the ME.

26. Short message storage :

The ME checks in the SIM service table that the short message storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for short message storage procedure and sends the short message to be stored. The short message storage procedure in the SIM is as follows.

The ME looks for the next available area to store the short message. If such a capacity is available, it sends the message to the SIM indicating in which area to store the message. After writing the message, the SIM sends back an acknowledgement to the ME.

If there is no available empty space in the SIM to store the received short message, a specific MMI will have to take place in order not to loose the message.

27. Short message erasure :

The ME checks in the SIM service table that the short message storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for short message erasure procedure and sends the identification of the message to be erased. The short message erasure procedure in the SIM is as follows.

The ME will select in the SIM the message area to free. Depending on the MMI, the message will be read or not before the area is marked as "free".

As soon as this is updated in the SIM, the memory allocated to this short message in the SIM is made available for a new incoming message, but the memory may still contain the old message until a new message is written.

28. Short message request :

The ME checks in the SIM service table that the short message storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for short message request procedure and sends the identification of the requested message. The short message request procedure in the SIM is as follows.

The SIM seeks for the identified message. If the message is found, the SIM sends the message to the ME.

If the identified short message is not found within the SIM memory, the SIM tells this fact to the ME.

29. Charging information updating : (FOR FS)

The ME checks in the SIM service table that the charging information storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for charging information updating procedure and sends the charging information. The charging information updating procedure in the SIM is as follows.

The SIM adds the charging information it received from the ME to the existing value charging information.

30. Charging information erasure : (FOR FS)

The ME checks in the SIM service table that the charging information storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for charging information erasure procedure. The charging information erasure procedure in the SIM is as follows.

The SIM sets to an initial value the charging information.

31. Charging information request : (FOR FS)

The ME checks in the SIM service table that the charging information storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for charging information request procedure. The charging information request procedure in the SIM is as follows.

The SIM sends to the ME the value of charging information it has in memory.

32. Abbreviated dialing number storage :

The ME checks in the SIM service table that the abbreviated dialing number storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for abbreviated dialing number storage procedure and sends the abbreviated dialing number identification and the complete information to be stored. The abbreviated dialing number storage procedure in the SIM is as follows.

The SIM checks that it has available storage capacity to store an abbreviated dialing number. If such a capacity is available, it stores the abbreviated dialing number identifier and the corresponding information it received from the ME in the memory allocated for this purpose. The SIM sends back an acknowledgement to the ME.

If the SIM has no available empty space to store the received abbreviated dialing number, it tells to the ME.

33. Abbreviated dialing number erasure :

The ME checks in the SIM service table that the abbreviated dialing number storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for abbreviated dialing number erasure procedure and sends the identification of the requested information to be erased. This identification may be an alphanumeric pattern contained in the abbreviated dialling number (refer to adressing data-field paragraph).

If the presented dialing number is the one to be erased, the ME requests the SIM for its erasure.

If the presented dialing number is not to be erased, the ME requests again the SIM for a further dialing number corresponding to the same identification or aborts this function.

34. Abbreviated dialing number request :

The ME checks in the SIM service table that the abbreviated dialing number storage capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for abbreviated dialing number request procedure and sends the identification of the requested information. This identifier may be an alphanumeric pattern contained in the abbreviated dialling number (refer to adressing data-fields paragraph) . The abbreviated dialing number request procedure in the SIM is as follows.

The SIM seeks for the identified dialing number. If the number is found, the SIM sends it to the ME.

If the identified dialing number is not found, the SIM tells the fact to the ME.

If no more phone numbers corresponding to the identification is found, the SIM tells the fact to the ME.

If the dialing phone number is not the correct one wanted by the user, the ME requests the SIM again for a further number corresponding to the same identification or aborts this function.

35. Capability configuration parameters request :

The ME checks in the SIM service table that the capability configuration parameters capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for capability configuration request procedure and sends the identification of the requested capability configuration parameter. The SIM seeks for the identified capability configuration parameter. If it is found, the SIM sends it to the ME.

36. Capability configuration parameters updating :

The ME checks in the SIM service table that the capability configuration parameters capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME asks the SIM for capability configuration updating procedure and sends the identification of the requested capability configuration parameter.

37. Capability configuration parameters erasure :

The ME checks in the SIM service table that the capability configuration parameters capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for capability configuration parameters erasure procedure and sends the identification of the number to be erased. This identification may be an alphanumeric pattern contained in the capability configuration parameters data-field.

The SIM seeks for the identified parameter. If one and only one number is found, the SIM sends it to the ME and asks the ME for a confirmation of erasure command.

42. PLMN selector request :

The ME checks in the SIM service table that the PLMN selector capability exists. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for PLMN selector request procedure. The PLMN selector request procedure in the SIM is as follows.

The SIM sends to the ME the contents of the PLMN selector it has in memory.

43. PLMN selector updating :

The ME checks in the SIM service table that the PLMN selector capability exists in the SIM. If not, the procedure does not start. If the capability exists, the ME proceeds as follows.

The ME asks the SIM for PLMN selector updating procedure and sends the updated value of the PLMN selector. The PLMN selector updating procedure in the SIM is as follows.

The SIM checks if this procedure is protected by an external authentication or not.

The proceeding of the PLMN selector updating procedure in case an external authentication is necessary is for Further Study.

If no external authentication is needed, then the SIM set the PLMN selector it has in memory at the updated value sent by the ME.

44. Forbidden PLMN information request

The ME asks the SIM for Forbidden PLMN information request procedure. The Forbidden PLMN information request procedure in the SIM is as follows.

The SIM reads the list of forbidden PLMNs it has in memory, and sends it to the ME.

45. Forbidden PLMN information updating

The ME asks the SIM for Forbidden PLMN information updating procedure and sends the list of forbidden PLMNs. The Forbidden PLMN information updating procedure in the SIM is as follows.

The SIM stores the updated list of forbidden PLMNs it received from the ME in the memory allocated to Forbidden PLMN, in place of the former value of forbidden PLMN.

46. Location update status request

The ME asks the SIM for Location update status request procedure. The Location update status request procedure in the SIM is as follows.

The SIM reads the value of Location update status it has in memory, and sends it to the ME.

47. Location update status updating

The ME asks the SIM for Location update status updating procedure and sends the updated location update status. The Location update status updating procedure in the SIM is as follows.

The SIM stores the updated value of the location update status it received from the ME in the memory allocated to Location update status, in place of the former value of location update status.

4.3. FUNDAMENTAL GSM INSTRUCTIONS

There are two types of GSM instructions. Those which shall be implemented into the ME and the SIM (here called MS instructions), and those which are implemented into the SIM-AD(s) and the SIM, and used during GSM administrative management phase (here called ADM instructions). The ADM instructions are not addressed in this recommendation.

The presentation of GSM instructions is as follows :

DEFINITION: the purpose of the instruction.

CONDITION OF USE: in what situation the instruction is allowed.

COMMAND PARAMETERS: data sent from the ME to the SIM in the association of the instruction.

RESPONSE PARAMETERS: data sent by the SIM to the ME in answering to the instruction.

STATUS INFORMATION: information that is sent back by the SIM, either if the action is performed or not.

Here is the list

Memory management:

- update successfull but after using an internal retry routine and "X" retries
- update impossible (memory problem)

Referencing management :

- no data-field selected
- unknown identifier or pattern not found
- out of range
- current directory or data-field unconsistent with the instruction

Security management :

- no secret code in the SIM
- acces security policy not fulfilled or secret code verification rejected
- in contradiction with PIN status
- secret code locked

Application independent errors :

- wrong instruction class given in the command
- unknown instruction code given in the command
- incorrect parameters P3
- incorrect parameters P1 or P2
- technical problem with no diagnostic given

Command correctly executed :

- normal ending of the command
- length "XX" of response data

4.3.1. MS instructions

The MS instructions are classified as follows.

Group Control :

- Select
- Select (Root Directory)
- Select (Application Directory)
- Select (Data-Field)
- Seek

Instruction Comments	Command Param./Data ———>	Response Param./data <———
Select	Object Identifier	
Seek	Mode, Identifier	

Class Group PIN :

- Verify-PIN
- Change-PIN
- Disable-PIN
- Reenable-PIN

Instruction	Command Param./Data	Response Param/Data
Comments	———>	<———
Verify PIN	PIN	
Change PIN	Old PIN, New PIN	
Disable PIN	PIN	
Reenable PIN	PIN	

Group Authentication :

- Run-SIM-Algorithm

Instruction	Command Param./Data	Response Param/Data
Comments	———>	<———
Run GSM alg.	RAND	

Group Read :

- Read-binary
- Read-record
- Get-Response

Instruction	Command Param./Data	Response Param./Data
Comments	———>	<———
Read-binary	offset,long	Data
Read-record	mode, record n°Data	
Get Response		Data (SRES/Kc) (Dir. char.) (Data-field char.)

Group Write :

- Update-binary
- Update-record

Instruction	Command Param/Data	Response Param/Data
Comments	———>	<———
Update-binary	offset,long Data	
Update-record	mode, record n° Data	

Group Management :

- Unblock GSM application
- Sleep
- Status

Instruction Comments	Command Param/Data ———>	Response Param/Data <———
Unblock GSM	Unblock. key, new PIN	
Sleep		
Status		Data

note 1 : To know which information of the field Command Param/Data is passed in the instruction and which one is passed as attributes of the instruction, see 4.4.1. the MS instruction encoding.

note 2 : instructions are always sent from the ME
<——— : Data expected from the SIM
———> : Data expected from the ME

(1) SELECT : (MS instruction)

DEFINITION :

The select instruction is always free. The Select instruction is used to select a specific object in (root directory, application directory, data-field) in the SIM.

CONDITION OF USE :

When the root directory or a data-field under the level of the selected root directory is selected, you are able to select :

- any application directory in the root directory
- any data-field under the level of the root directory.

When the current application directory or a data-field under the level of the current application directory is selected, you are able to select:

- any other application directory in the root directory
- the root directory
- any data-field in the current application directory.

Note : Once a particular object has been selected, an unlimited number of actions may be performed on this object (until another object is selected) without the need to re-select.

COMMAND PARAMETERS/DATA :

- The identifier of the object.

This identifier consists in the type of the object to be selected and the sub-identifier of the object

The type is on one byte and is coded :

- 3F : root directory
- 7F : application directory
- 2F : data-field under the level root directory
- 6F : data-field under the level application directory

The sub-identifier is coded on one byte in the GSM-application and follows the type

RESPONSE PARAMETERS/DATA :

It is optional to get the response which usually consists of the information within the header of the object. To get the response, one should use a GET-RESPONSE instruction just after the corresponding SELECT instruction.

STATUS INFORMATION :

See the tables of Section 4.4.3.

Note : Hereafter are described the Select(directory) and the Select(data-field) using this instruction Select.

Case 1 : SELECT(DIRECTORY)

DEFINITION :

This is an instruction which selects a specific directory in a multi-application card. For GSM application, 3 directories can be selected :

- the Root directory
- the Telecom directory
- the GSM directory

CONDITION OF USE :

This instruction is mandatory to have any action on the data-fields of a specific directory. When the SIM is activated, the root directory is implicitely selected.

COMMAND PARAMETERS/DATA :

- Identifier of the Directory (type and sub-identifier)

RESPONSE PARAMETERS/DATA :

- No response except the SW1 SW2 bytes. To have the possibiliy of reading the characteristics and the security policy of the directory, one uses a GET RESPONSE instruction. The definition of the characteristics and of the security policy of the directory is FOR FS (no use for the moment in the SIM-ME interface).

STATUS INFORMATION :

See the tables of Section 4.4.3.

note 1 : The use of the Telecom directory by other applications than the GSM application is FOR FS.

note 2 : Depending on the response, the ME may have to adapt its behaviour [i.e. PIN handling etc]

note 3 : In the case of multi-application cards, the use of this instruction to access other directories than the ones discussed in this document is FOR FS.

Case 2 : SELECT(DATA-FIELD)

DEFINITION :

This instruction looks for a data-field already existing in memory by positionning a pointer on this the data-field . It will then be possible to read, update or perform any specific action on the body of the data-field with the corresponding instruction (if the security policy allows the action).

CONDITION OF USE :

The corresponding directory shall have been selected before the invokation of this instruction.

COMMAND PARAMETERS/DATA :

Identifier of the data-field in the directory. This identifier consists of the type (6F) of data-field and of the sub-identifier which is coded on one byte in the GSM application..

RESPONSE PARAMETERS/DATA :

- No response except the SW1 SW2 bytes. To have the possibiliy of reading the characteristics and the security policy of the data-field contained in the header of the data-field, one uses a GET RESPONSE instruction. See this instruction to have the presentation of the header of the data-field at the SIM-ME interface.

STATUS INFORMATION :

See the tables of Section 4.4.3.

(2) SEEK (MS Instruction)

DEFINITION :

This instruction is used to locate a record in the data-field selected by the last "select data-field" instruction. This instruction searches through the current data-field to find a record containing the given argument. If the given pattern is found, the SIM sets a pointer to appropriate record. If the pattern is not found, the SIM will not change the pointer. If the pattern is not found and if the pointer was not set before the SEEK (from the next location-forward) or SEEK (from the previous location-backward), the pointer is still undefined.

CONDITION OF USE :

Within the GSM application, and according to the security policy, after a preliminary authentication if required.

The length of the pattern may be limited. If parameter P3 (LGTH) indicates a pattern-lenght greater than this limit or greater than the record length, the SIM shall send the status information "Incorrect parameter P3" (see the tables of section 4.4.3). The SIM shall accept at least any pattern-length between 1 and 16 bytes.

This instruction will be accepted by the SIM only on formatted data-fields.

The seek instruction will check if this request is in accordance with the security policy attached to the data-field. The seek instruction has the same security policy as the read record instruction. This security policy was given in the RESPONSE PARAMETERS/DATA of the select data-field instruction.

A READ-RECORD instruction allows to obtain the data of the found record to be read.

COMMAND PARAMETERS/DATA :

1) The mode :The data-field may be searched starting from the begining, the current location or from the end, and forward or backward looking for the argument given as the second parameter.

Four modes are defined :

- from the begining-forward coded Hex '00'
- from the next location-forward coded Hex '02'
  If the pointer has not been previously set within the selected data-field, the search begins on the first record of the selected data-field.
- from the previous location-backward coded Hex '03'
  If the pointer has not been previously set within the selected data-field, the search begins on the last record of the selected data-field.
- from the end-backward coded Hex '01'

2) The pattern : the argument given is searched in the data-field, assuming that it must be at the begining of a record.

RESPONSE PARAMETERS/DATA :

none.

STATUS INFORMATION :

See the tables of Section 4.4.3.

(3) VERIFY-PIN : (MS instruction)

DEFINITION :

This is an instruction which authenticates the user to the SIM by presenting the PIN.

CONDITION OF USE :

It is necessary to use this instruction once during a GSM-session with a successful result before having an action on a data-field protected by a PIN, except when the PIN is disabled. It is possible to use the instruction VERIFY-PIN after the selection of the root directory, a selection of an application directory or after the selection of a data-field in an application directory, except when the PIN is disabled or when the PIN is blocked. If the presented PIN is false when presented, the PIN error counter is adjusted accordingly. If the PIN is right, the PIN error counter is reset.

COMMAND PARAMETERS/DATA :

Value of the PIN.

"PIN" is coded on 8 bytes. Only numeric characters (0-9) shall be used, coded in CCITT 5 (ASCII) with b8 set to zero.

If the presented PIN has a length between 4 and 7 digits, the excess bytes shall be set to NULL by the ME.

Example : PIN = 5678

Byte 1: "Hex 35" in ASCII for the number 5 (first digit)

b8							b1
0	0	1	1	0	1	0	1

Byte 2: "Hex 36" in ASCII for the number 6

b8							b1
0	0	1	1	0	1	1	0

etc ...

Byte 8: "Hex FF" for NULL

b8							b1
1	1	1	1	1	1	1	1

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(4) CHANGE-PIN : (MS instruction)

DEFINITION :

This is an instruction that changes the PIN of the user.

CONDITION OF USE :

The PIN inside the SIM is only changed if the presented old PIN is correct. If the presented old PIN is not correct, then the PIN error counter is incremented.

The SIM will not execute the instruction CHANGE-PIN when the PIN is disabled or when the PIN is blocked.

COMMAND PARAMETERS/DATA :

Value of the old PIN and of the new PIN. (this order is important).

Structure of command data :

```
    "old PIN"          "nex PIN"

<     8 bytes     > <    8 bytes      >
I----I......I----I----I......I----I
 (a)         (b)  (c)         (d)
```

"old PIN" and "new PIN" are coded on 8 bytes. If the old PIN and the new PIN have a length between 4 and 7 digits, the excess bytes of each shall be set to NULL by the ME.

Example : old PIN = 5111 , new PIN = 6111

Byte a: "Hex 35" in ASCII for the number 5 (first digit)

b8							b1
0	0	1	1	0	1	0	1

Byte b: "Hex FF" for NULL

b8							b1
1	1	1	1	1	1	1	1

Byte c: "Hex 36" in ASCII for the number 6

b8							b1
0	0	1	1	0	1	1	0

Byte d: "Hex FF" for NULL

b8							b1
1	1	1	1	1	1	1	1

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(5) DISABLE-PIN : (MS instruction)

DEFINITION :

This is an instruction to disable the PIN verification.

CONDITION OF USE :

The SIM will not execute the instruction DISABLE PIN when the PIN is already disabled, or when the SIM is blocked.

COMMAND PARAMETERS/DATA :

Actual user PIN code.

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(6) REENABLE-PIN : (MS instruction)

DEFINITION :

This is an instruction that reenables the PIN checking by the user (opposite of the disable-PIN instruction).

CONDITION OF USE :

The SIM execute the instruction REENABLE PIN only when the PIN is disabled and the SIM not blocked.

COMMAND PARAMETERS/DATA :

Actual user PIN code.

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(7) RUN-GSM-ALGORITHM : (MS instruction)

DEFINITION :

This is an instruction to trigger the GSM algorithms of the SIM : A3 and A8.

This instruction needs to be followed by a GET-RESPONSE instruction in order to output the data SRES/Kc, which corresponds to the RAND value sent by the ME. If another instruction than the GET-RESPONSE follows the instruction RUN-GSM-ALGORITHM, the data SRES/Kc will be lost.

CONDITION OF USE :

To be executed, the GSM directory must have been previously selected as the current directory.

COMMAND PARAMETERS/DATA :

- A random number RAND given by the outside world.

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(8) READ-BINARY : (MS instruction)

DEFINITION :

This allows the SIM to read a string of bytes from a binary data-field.

CONDITION OF USE :

If the security policy of the data-field is not fulfilled, the instruction willbe rejected by the SIM.

COMMAND PARAMETERS/DATA :

- offset of the first byte of the string of bytes to be accessed within the data-field; coded on 2 bytes.
- number of bytes to read; coded on 1 byte.

RESPONSE PARAMETERS/DATA :

Data

STATUS INFORMATION :

See the tables of Section 4.4.3.

(9) READ RECORD (MS Instruction)

DEFINITION :

This instruction is used to read a record in the data-field selected by the last "select data-field" instruction.

CONDITION OF USE :

Within the GSM application, and according to the security policy of the data-field, after a preliminary authentication if required.

This instruction is used with formatted data-fields.

The read record instruction will check if this request is in accordance with the security policy attached to the data-field. This security policy was given in the RESPONSE PARAMETERS/DATA of the select data-field instruction.

Four modes are defined :

- CURRENT and ABSOLUTE modes : The pointer is not affected by this instruction. For READ (ABSOLUTE), the number of the record to read is given by P1; the reserved value P1 = 00 denotes the currrent record, i.e, for the READ (CURRENT).
- NEXT mode : the pointer will be incremented before the READ RECORD instruction is executed, and the pointed record will be read. If the pointer has not been previously set within the selected data-field, then READ (NEXT) will read the first record in the data-field and set the pointer to this record. If the pointer is already situated at the last record in the data-field, READ (NEXT) will not cause the pointer to be shifted, and no record data will be returned.
- PREVIOUS mode: the pointer will be decremented before the READ RECORD instruction is executed, and the pointed record will be read. If the pointer has not been previously set within the selected data-field, then READ (PREVIOUS) will read the last record in the data-field and set the pointer to this record. If the pointer is already situated at the first record in the data-field, READ (PREVIOUS) will not cause the pointer to be shifted, and no record data will be returned.

Note : The pointer is :

i) set by a SEEK instruction;

ii) set by READ (NEXT) and UPDATE (NEXT) on the first record in the data-field if a SEEK has not been performed on the selected data-field;

iii) set by READ (PREVIOUS) and UPDATE (PREVIOUS) on the last record in the data-field if a SEEK has not been performed on the selected data-field;

iv) modified by READ (PREVIOUS), UPDATE (PREVIOUS), READ (NEXT) and UPDATE (NEXT).

COMMAND PARAMETERS/DATA :

1) The record number for CURRENT and ABSOLUTE modes is given in P1. For the other modes P1 has no significance.

2) The mode is given by P2 as follows :

- CURRENT and ABSOLUTE mode : coded Hex 04;
- NEXT mode : coded Hex 02;
- PREVIOUS mode : coded Hex 03.

RESPONSE PARAMETERS/DATA :

The data of the record selected.

STATUS INFORMATION :

See the tables of Section 4.4.3.

(10) GET-RESPONSE : (MS instruction)

DEFINITION :

This instruction is used by the ME to receive data calculated or addressed by a previous instruction executed in the SIM.

CONDITION OF USE :

After a RUN-GSM-ALGORITHM instruction or after a SELECT (the instruction is optional). If the instruction GET RESPONSE is executed, it is mandatory that it is executed just after the instruction it is related to (no other instruction shall interfere with the command/response pair (see IS 7816-4), i.e. SELECT/GET RESPONSE). If the sequence of the command/response pair is not respected, the SIM shall send the Status Information "technical problem with no diagnostic given" as a reaction to the GET-RESPONSE

Note: Since the root directory is implicitly selected when the SIM is activated (cf. Clause 4.3.1 (1) SELECT DIRECTORY), the GET-RESPONSE instruction is allowed as the first instruction after activation.

COMMAND PARAMETERS/DATA :

None

RESPONSE PARAMETERS/DATA :

Case 1: After a RUN-GSM-ALGORITHM instruction:

As stated in paragraph 4.2 (clause C.11) the response data are SRES/Kc for GSM algorithm A3/A8. The overall format of SRES/Kc is 96 bits (12 bytes) and is described below:

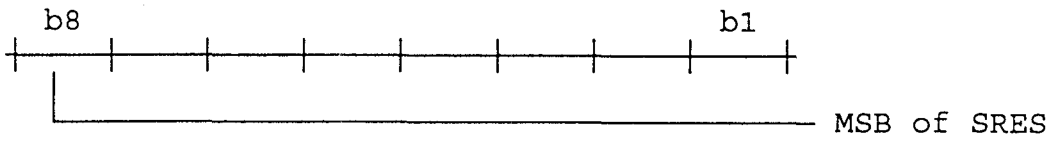
Byte	Description	Length
1-4	SRES (see detail 1)	4 bytes
5-12	Kc (see detail 2)	8 bytes

Byte 1 is the first one received by the ME as a response to the GET-RESPONSE instruction.

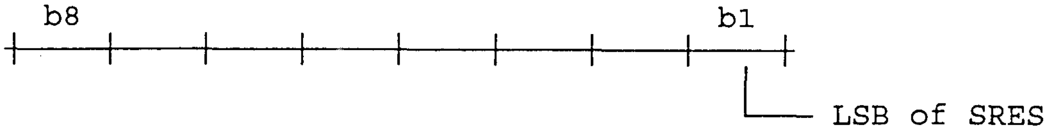
Detail 1: SRES encoding:

The coding of SRES is as stated in rec GSM 04.08, Table 10.40, i.e. byte 1 corresponds to octet 2, byte 2 to octet 3, byte 3 to octet 4 and byte 4 to octet 5, and:

Byte 1: Most significant byte:



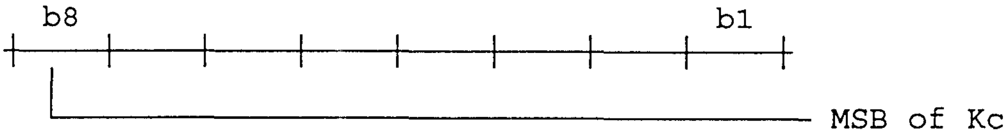
Byte 4:



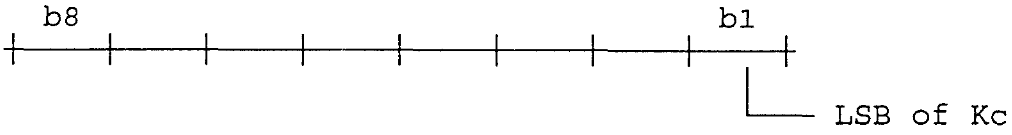
Detail 2: Kc encoding:

The Kc encoding is defined as follows:

Byte 5: Most significant byte:



Byte 12:



It must be noted that it is not assumed that the ME performs any checking or modification upon the contents of Kc which must be presented to algorithm A5 as it is delivered by the SIM in its 64 bits format. The way these data are used by A5 is part of the algorithm specification.

Case 2: After a SELECT (Directory) instruction:

The response data contain information related to the selected directory. This information is exactly the same as that to be obtained by calling the STATUS instruction (see also the definition of the instruction STATUS).

Case 3: After a SELECT (Data Field) instruction

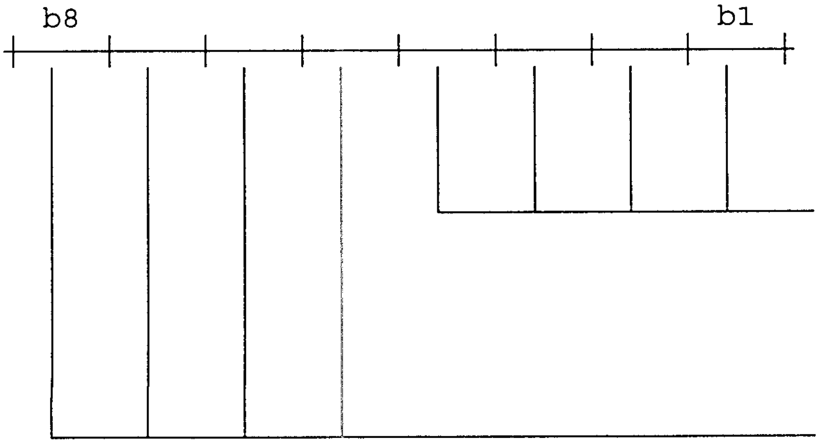
The response data contains information related to the selected data field. The format is described below:

Byte	Description	Length
1-2	RFU	2 bytes
3-4	Total memory space available (block size for binary DF) (record size * number of records for formatted DF)	2 bytes
5	Type identifier of current data-field	1 byte
6	Current data-field Sub-identifier	1 byte
7-8	RFU	2 bytes
9	Security policy in GSM operations (see detail 1	1 byte
10-12	Reserved for the administrative management	3 bytes
13	Length of following data (bytes 14 to the end)	1 byte
14	Data-field organization type (Hex '00' for binary) (Hex '01' for formatted)	1 byte
15	Record size, in bytes	1 byte

Note : All bytes which are RFU are set to zero .

Detail 1 : Security Policy

Byte 1:



bits 4-1
UPDATE
access condition
(0:ALW...F:NEVER)
(4-E: reserved for
the administrative
management)

bits 8-5
READ access cond.
(0:ALW...F:NEVER)
(4-E: reserved for
the administrative
management)

STATUS INFORMATION :

See the tables of Section 4.4.3.

(11) UPDATE-BINARY : (MS instruction)

DEFINITION :

Erase/Write

This is an instruction to replace a string of bytes in a binary data-field.

CONDITION OF USE :

- In the GSM application, this instruction is used in accordance to the security policy.

The corresponding data-field must have been selected before performing the update-binary.

COMMAND PARAMETERS/DATA :

- offset of the first byte of the string of bytes to be accessed within the data-field; coded on 2 bytes.
- number of bytes to be updated; coded on 1 byte.

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(12) UPDATE RECORD (MS Instruction)

DEFINITION :

This instruction is used to update a record in the data-field selected by the last "select data-field" instruction. This instruction erase the memory before the write is performed.

CONDITION OF USE :

Within the GSM application, and according to the security policy of the data-field, after a preliminary authentication if required.

This instruction is used with formatted data-fields.

The update record instruction will check if this request is in accordance with the security policy attached to the data-field. This security policy was given in the RESPONSE PARAMETERS/DATA of the associated select data-field instruction.

Four modes are defined :

- CURRENT and ABSOLUTE modes : The pointer is not affected by this instruction. For UPDATE (ABSOLUTE), the number of the record to update is given by P1; the reserved value P1 = 00 denotes the currrent record, i.e, for the UPDATE (CURRENT).

- NEXT mode : the pointer will be incremented before the UPDATE RECORD instruction is executed, and the pointed record will be updated. If the pointer has not been previously set within the selected data-field, then UPDATE (NEXT) will update the first record in the data-field and set the pointer to this record. If the pointer is already situated at the last record in the data-field, UPDATE (NEXT) will not cause the pointer to be shifted, and no record data will be updated.

- PREVIOUS mode : the pointer will be decremented before the UPDATE RECORD instruction is executed, and the pointed record will be updated. If the pointer has not been previously set within the selected data-field, then UPDATE (PREVIOUS) will update the last record in the data-field and set the pointer to this record. If the pointer is already situated at the first record in the data-field, UPDATE (PREVIOUS) will not cause the pointer to be shifted, and no record data will be updated.

Note : The pointer is :

i) set by a SEEK instruction;

ii) set by READ (NEXT) and UPDATE (NEXT) on the first record in the data-field if a SEEK has not been performed on the selected data-field;

iii) set by READ (PREVIOUS) and UPDATE (PREVIOUS) on the last record in the data-field if a SEEK has not been performed on the selected data-field;

iv) modified by READ (PREVIOUS), UPDATE (PREVIOUS), READ (NEXT) and UPDATE (NEXT).

COMMAND PARAMETERS/DATA :

1) The record number for CURRENT and ABSOLUTE modes is given in P1. For the other modes P1 has no significance.

2) The mode is given by P2 as follows :

- CURRENT and ABSOLUTE mode : coded Hex 04;
- NEXT mode : coded Hex 02;
- PREVIOUS mode : coded Hex 03.

RESPONSE PARAMETERS/DATA :

none.

STATUS INFORMATION :

See the tables of Section 4.4.3.

(14) UNBLOCK GSM APPLICATION : (MS instruction)

DEFINITION :

This instruction authenticates the user and establishes his new PIN .

This instruction is used to unblock the SIM when the user has locked his PIN after three false presentations or when the user has forgotten his PIN.

The PIN checking is enabled after a successful unblocking.

CONDITION OF USE :

If the presented UNBLOCKING KEY is false , the UNBLOCKING KEY error counter is adjusted accordingly. If the UNBLOCKING KEY presented is correct, its UNBLOCKING KEY error counter is reset.

COMMAND PARAMETERS/DATA :

Value of the UNBLOCKING KEY and of the new PIN (this order is important)

The UNBLOCKING KEY is coded on 8 bytes. Only numeric characters (0-9) shall be used, coded in CCITT 5 (ASCII) with b8 set to zero. For example : UNB. KEY = 56781234.

The new PIN is coded on 8 bytes. If the new PIN has a length between 4 and 7 digits, the excess bytes shall be set to NULL by the ME. For example : new PIN = 5111.

Structure of command data :

```
 "Unblocking key"   "new PIN"

<...8 bytes.....><...8 bytes.....>

I---I-.....-I---I---I-.......I---I
 (a)         (b) (c)          (d)
```

Byte a: Hex 35 in ASCII for the number 5 (first digit)

b8							b1
0	0	1	1	0	1	0	1

Byte b: Hex 34 in ASCII for the number 4 (last digit)

b8							b1
0	0	1	1	0	1	0	0

Byte c: "Hex 35" in ASCII for the number 5 (first digit)

b8							b1
0	0	1	1	0	1	0	1

Byte d: "Hex FF" for NULL

b8							b1
1	1	1	1	1	1	1	1

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(15) SLEEP : (MS instruction)

DEFINITION :

When the component do not have the "Full internal sleep mode" feature, this instruction is used to put the SIM into the Sleep mode.

CONDITION OF USE :

If the clock can be stopped (Clock Sleep mode), it is indicated in byte 1 of directory characterics given through a STATUS instruction.

COMMAND PARAMETERS/DATA :

None

RESPONSE PARAMETERS/DATA :

None

STATUS INFORMATION :

See the tables of Section 4.4.3.

(16) STATUS : (MS instruction)

DEFINITION :

This instruction gives information about the current secret codes (ISSUER, PIN, UNBLOCKING KEY...) as well as some information relative to the current Directory (Root directory or Application directory). It gives the same response than what is available through a GET RESPONSE after a SELECT of a directory.

CONDITION OF USE :

This instruction may be used at any time to obtain information about the context of the GSM application.

COMMAND PARAMETERS/DATA :

None

RESPONSE PARAMETERS/DATA :

Byte	Description	Length
1-2	RFU	2 bytes
3-4	Total memory space available	2 bytes
5	Type identifier of current directory	1 byte
6	Current directory Sub-identifier	1 byte
7-8	RFU	2 bytes
9	Security Policy of the directory: RFU	1 byte
10-12	Reserved for the administrative management	3 bytes
13	Length of following data (bytes 14 to the end)	1 byte
14	Directory characteristics (see detail 1)	1 byte
15	Number of sub-directories	1 byte
16	Number of data-fields in the current directory	1 byte
17	Number of secrete codes (X secrete codes, X between 2 and 16)	1 byte
18	RFU	1 byte
19	PIN status (see detail 2)	1 byte
20	UNBLOCKING KEY status	1 byte
21-23	Status of other secrete codes: RFU	3 bytes
24-34	Reserved for the administrative management	if X ≥ 5 X-5 bytes

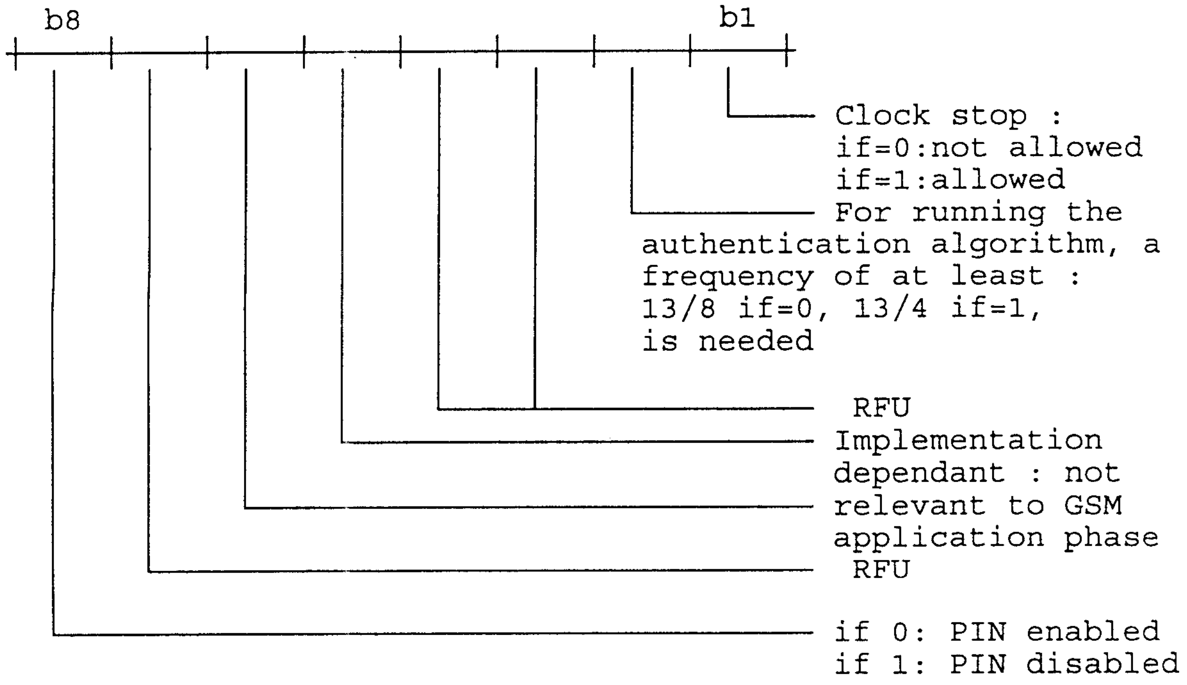
Note : if the data length requested in the command of the status instruction is lower than the maximum available length, only the requested length will be transfered in the response.

All bytes which are RFU are set to zero .
All bits which are RFU are set to zero.

Bytes 3, 4 and 15 shall not be interpreted by Phase 1 ME.

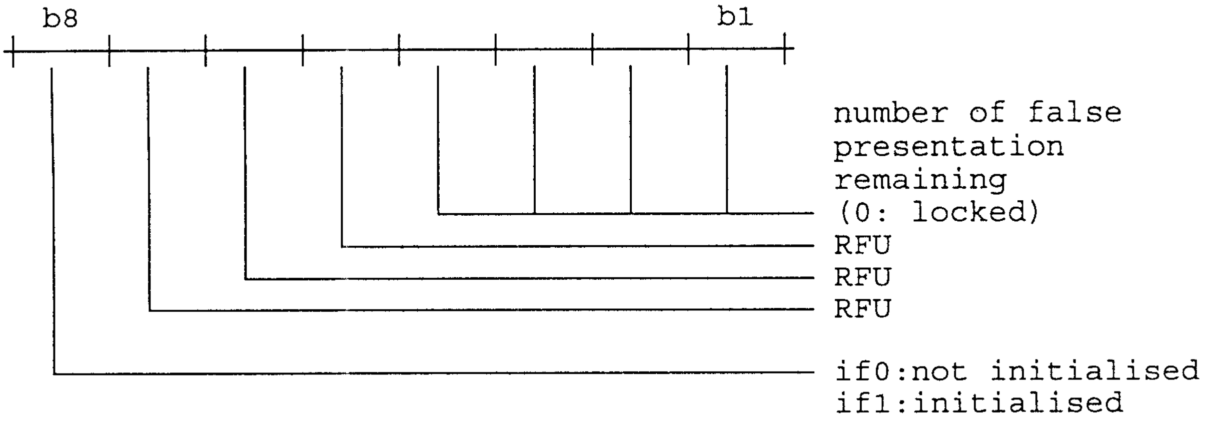
Detail 1 : directory characteristics

Byte 1:



Detail 2: For each secrete code the status byte is the following:

Byte 1:



STATUS INFORMATION :

See the tables of Section 4.4.3.

4.4. INSTRUCTION FORMAT AND ENCODING

4.4.1. Format

An instruction in GSM application consists of a command and the associated response pair.

The command has the format :

CLA : INS : P1 : P2 : P3 : <data & parameters>

The bytes of a command do not contain any transmission oriented information

where :

- CLA is the instruction class. A0 is used in GSM application
- INS is the instruction code within the instruction class
- P1,P2,P3 are parameters for the instruction. P3 gives the length of the exchange at the interface level. P1, P2 and P3 may have no values, depending on CLA/INS.
  Note : P1,P2&P3 are defined for each instruction previously.

The bytes CLA and INS are meaningfull for any value.

According to ISO standard 7816-3 :

P3 shall be the number of data bytes to be transmitted during the command, and P3 = hex "00" introduces a 256 byte data transfer from the SIM in an outgoing data transfer command (response direction). In an ingoing data transfer command (command direction), P3 = hex "00" introduces no transfer of data.

When P3 has a value greater than 1, the order of data bytes, transmitted on the SIM-ME I/O data line, shall be as specified in the definition of the data field in Section 3.

Note : As a result of a joint meeting of ISO/IEC/JTC1/SC17/WG4 and ISO/TC68/SC6/WG5, there is a proposition under study in ISO-IEC/JTC1/SC17/WG4 : "When byte P3 is hex "FF", the next two, L1, L2 , are respectively the most significant and the less significant part of the number of bytes to be transferred. Values beginning with hex "FFFFFF" are reserved for future use".

<data & parameters > are sent optionally.

A command always is answered by a response. A response have a length of 2 bytes minimum. It has the format :

<data & parameters> : SW1 : SW2

SW1, SW2 : two bytes giving the SIM status at the end of the instruction

<data & parameters > are sent optionnally.

When a response contains data or parameters, the order of data bytes, transmitted on the SIM-ME I/O data line, shall be as specified in the definition of the data field in Section 3.

4.4.2. MS Instruction encoding

All numbers are Hexadecimal ones in the table

NAME OF THE INSTRUCTION	CLASS	INS	P1	P2	P3
SELECT	A0	A4	00	00	02 (C)
SEEK	A0	A2	00	MODE	LGTH (C)
VERIFY PIN	A0	20	00	01	08 (C)
CHANGE PIN	A0	24	00	01	10 (C)
DISABLE PIN	A0	26	00	01	08 (C)
REENABLE PIN	A0	28	00	01	08 (C)
RUN GSM ALGORITHM	A0	88	00	00	10 (C)
READ BINARY	A0	B0	OFFSET	OFFSET	LGTH (R)
READ RECORD	A0	B2	RECORD	MODE	RECORD LGTH (R)
GET RESPONSE	A0	C0	00	00	LGTH (R)
UPDATE BINARY	A0	D6	OFFSET	OFFSET	LGTH (C)
UPDATE RECORD	A0	DC	RECORD NUMBER	MODE	RECORD LGTH (C)
UNBLOCK GSM APPLICATION	A0	2C	00	00	10 (C)
SLEEP	A0	FA	00	00	00 (C)
STATUS	A0	F2	00	00	LGTH (R)

Note : Other instructions with CLA not equal A0 may be sent without influencing the momentary state of GSM application, independant acceptation or rejection of the SIM.

COMMENTS ON THE TABLE :

- "CLA" is the class byte (to be defined by ISO if possible) A0 is proposed.

- parameters not used have been set to HEX 0. Some other implementations may use these parameters and consequently alter the behaviour of the instructions.

- "Offset" in READ-DATA and UPDATE-DATA means the relative position (in bytes) of the data to be acted upon within the data-field. In GSM application, "offset" is coded on 2 bytes, right justified, i.e.,

  Hex 00 00 means the 1st byte of the data-field,
  Hex 00 01 means the 2nd byte of the data-field,
  Hex 00 02 means the 3rd byte of the data-field,
  etc ...

- P3 is a length in byte except when equal 0

- LGTH : Length of the data attributes of the instruction.

- (C) : command direction
- (R) : response direction

4.4.3. Status encoding

According to ISO IS 7816-3, there are 2 status bytes called SW1 and SW2 in the response to an instruction.

The encoding of each bytes is expressed in Hex values.

The following tables show the status information elements associated to each GSM instruction (marked by "*") together with the encoding.

STATUS INFORMATION	SW1	SW2	SELECT	SEEK	VERIFY PIN	CHANGE PIN	DISABLE PIN	REENABLE PIN	UNBLOCK GSM	RUN GSM ALGOR	GET RESPONSE	READ BINARY	READ RECORD	UPDATE BINARY	UPDATE RECORD	STATUS	SLEEP
MEMORY MANAGEMENT																	
Update successfull but after using an internal retry routine X retries	92	0X			*	*	*	*	*					*	*		
Update impossible (memory problem)	92	40			*	*	*	*	*					*	*		
REFERENCING MANAGEMENT																	
No data field selected	94	00		*								*	*	*	*		
Unknown identifier Pattern not found	94	04	*	*													
Out of range	94	02											*		*		
Current directory or data field unconsistent with instruction	94	08		*						*		*	*	*	*		
SECURITY MANAGEMENT																	
No secret code in the SIM	98	02			*	*	*	*	*								
Access security policy not fullfilled Secret code verify rejected	98	04		*	*	*	*	*	*			*	*	*	*		
In contradiction with PIN status	98	08			*	*	*	*									
Secret code locked	98	40			*	*	*	*	*								

STATUS INFORMATION	SW1	SW2	SELECT	SEEK	VERIFY PIN	CHANGE PIN	DISABLE PIN	REENABLE PIN	UNBLOCK GSM	RUN GSM ALGOR	GET RESPONSE	READ BINARY	READ RECORD	UPDATE BINARY	UPDATE RECORD	STATUS	SLEEP
APPLICATION INDEPENDANT ERROR																	
Wrong instruction class given in the command	6E	XX	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Unknown instruction code given in the command	6D	XX															
Incorrect parameter P3 (if 'XX=00': no additional inform. if 'XX=/00': 'XX' gives correct length)	67	XX	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Incorrect parameter P1 or P2	6B	XX	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Technical problem with no diagnostic given (the command is aborted)	6F	XX	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
COMMAND CORRECTLY EXECUTED																	
Normal ending of the command	90	00		*	*	*	*	*	*		*	*	*	*	*	*	*
Length 'XX' of the response data	9F	XX	*							*							

5. SIM TRANSMISSION PROTOCOLS

5.1. TRANSMISSION PROTOCOL

The choice of the transmission protocol(s) to be used for communications between the SIM and the ME shall at least include that specified and denoted by T=0 in IS 7816-3.

5.2 ANSWER TO RESET

The answer to reset consists of at most 33 characters.

The ME shall be able to receive interface characters for other transmission protocols than T=0, historical characters and a check byte, even if only T=0 is used by the ME.

Character type/val	Contents	is sent by the card	a) evaluation by the ME b) reaction by the ME
1. Initial char. TS	conventions to code data bytes in all subsequent characters (direct or inverse convention)	always	a) always b) using appropriate convention
2. Format char. T0	subsequent interface characters number of historical characters	always	a) always b) identifying the subsequent characters accordingly
3. Interface char. (global) TA1	parameters to calculate the work etu	optional	a) always if present b) if TA1 is not "0001 0001" use PTS procedure (see clause 7, ISO 7816-3 or see below)
4. Interface char. (global) TB1	parameters to calculate the programming voltage and current	optional	a) always if present b) if PI1 is not 0 or not 5, then reject the SIM
5. Interface char. (global) TC1	parameters to calculate the extra guardtime requested by the card; no extra guard time is used to send characters from the card to ME	optional	a) always if present b) if TC1 is not 0 or not 255, then reject the SIM

Character type/val	Contents	is sent by the card	a) evaluation by the ME b) reaction by the ME
6. Interface char. TD1	protocol type; indicator for the presence of interface char., specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
7. Interface char. (specific) TA2	not used for protocol T=0	optional	a) not necessary b) --------------
8. Interface char. (global) TB2	parameter to calculate the programming voltage	optional	a) always if present b) if PI2 is not 50, then reject the SIM
9. Interface char. (specific) TC2	parameters to calculate the work waiting time	optional	a) always if present b) using the work waiting time accordingly
10. Interface char. TDi (i>1)	protocol type; indicator for the presence of interface char., specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
11. Interface char. TAi, TBi, TCi (i>2)	characters which contain interface characters for other transmission protocols	optional	a) not necessary b) -------------
12. Historical char. T1,...,TK	contents not specified in ISO	optional	a) not necessary b) -------------

Character type/val	Contents	is sent by the card	a) evaluation by the ME b) reaction by the ME
13. Check char. TCK	check byte (exclusive -ORing)	not sent if only T=0 is indicated in the ATR in all other cases TCK shall be sent	a) not necessary b) --------------

Specifically related to this recommendation the PTS procedure according to IS 7816-3, clause 7, is applied as follows:

```
          ME                                       SIM

(1)    (Reset of SIM) ------------->

(2)                                  <------- (Answer to reset)
                                          TA1 not '11'

(3)    (PTS request) -------------->
        PTSS='FF', PTSO='00', PCK='FF'

(4)                                  <------- (PTS response)
                                PTSS='FF', PTSO='00', PCK='FF'
```

Note : (PTS request) and (PTS response) consist of 3 characters, i.e., PTSS, PTSO and PCK, where PTSS is sent first.

After this procedure the protocol T=0 and the following parameters will be used:

F = 372 (for external clock cards), D=1, N=0 or 255.

5.3. ERROR HANDLING

If the ME receives a wrong "Answer to reset", it shall repeat the Reset between 2 and 5 times before rejecting the SIM.

5.4. BIT/CHARACTER DURATION AND SAMPLING TIME

The bit/character duration and sampling time specified in ISO 7816-3 chapter 6.1.2 are valid for all communication.

5.5. ERROR DETECTION AND CHARACTER REPETION

For the transmission of the Answer to Reset and the protocol type selection, the error detection and character repetition procedurre specified in ISO 7816-3 chapter 6.1.3 is optional for the ME.

For the subsequent transmission on the basis of T=0 this procedure is mandatory for the ME.

For the SIM the error detection and character repetition procedure is mandatory for all communication.

6. PHYSICAL CHARACTERISTICS AND LOW-LEVEL INTERFACE

Prefix : In view of the continuous effort to reduce the size and current consumption of the ME the figures given in this recommendation for power consumption and supply voltage should be revised not later than 1993. Figures to be aimed at are a supply voltage of 2.7 V to 5.5 V, a maximum current supply in the operating mode of 1 mA and 10 micro-A in idle state.

The international standards IS 7816/1, 2 and 3 shall apply as the basic interface specification between the SIM and the ME. Certain additional requirements are added in this section to ensure that the SIM will function properly in a GSM ME.

Two physical types of SIM are specified :

- IC card SIM : This type is identical to the card specified in the international standard IS 7816/1.

- Plug-in SIM : This is a smaller version of the IC card SIM. It is "obtained" by cutting away excessive plastic and adding a feature for orientation. The dimension of the contacts, which are the same as the IC card SIM, and their locations, are given in Figure 6.1. This type of SIM is primarily intended for hand-held telephones, but may also be used for other mobiles at the discretion of the ME manufacturer.

6.1. MECHANICAL INTERFACE

6.1.1. **Dimensions**

The mechanical interface between the IC card SIM and the ME shall be in accordance with IS 7816/1 and 2.

The mechanical interface between the plug-in SIM and the ME shall be in accordance with Figure 6.1. Section 4 of IS 7816/3 shall apply in principle. Annexes 1 and 2 of IS 7816/1 do not apply. Annex A of IS 7816-2 applies for the plug-in SIM with the three reference points P1, P2 and P3 measured 7.5 mm, 3.3 mm and 20.8 mm, respectively, from O.

6.1.2. Contacts

Contacts C4 and C8 dot not have to be provided by either type of SIM. There shall not be any contacting elements in the ME in positions C4 and C8.

In the case of the IC card SIM, the ME shall provide contact C6 and an idle state equal to the condition for Vcc. Contact C6 may be connected to Vcc in the ME.

In the case of the plug-in SIM, contact C6 need not be provided by the ME. If it is present in the ME, the programming voltage may not be provided. C6 shall not be connected to ground in the ME.

Contact C6 should not be bonded in the SIM if there is no corresponding bonding pad on the chip (that is in particular never to ground).

6.1.2.1. Contacting of the SIM

Care should be taken that, at deactivation of the SIM, no short circuit is caused in the SIM.

6.1.2.2. Contact pressure

The contact pressure of the contacting elements must be large enough to ensure contact even under extreme driving conditions. However, under no circumstances may a contact pressure be greater than .5 N per contact.

6.1.2.3. Shape of contacts for IC card SIM

The radius of curvature of the contacting elements shall be greater than or equal to .8 mm in the contact area on both axes. The shape of the contacting elements shall be such that no damage is caused by them being applied to the card.

6.1.3. Heat dissipation

The heat dissipation shall not exceed 55 mW for either type of SIM.

6.1.4. Environmental conditions

The SIM shall be fully operational in a temperature range from -25 °C to 70 °C with occasional peaks of up to 85 °C. Occasional means not more than four hours each time and not more than 100 times during the life time of the SIM.

6.1.5. Embossing of the IC SIM card SIM

The embossing of the IC card SIM shall be in accordance with ISO 7811-1 and 7811-3.

As specified in ISO 7816-2 the contacts of the IC card SIM may be located on either the front (embossed face, see ISO 7810) or the back of the card.

The mechanical interface of the ME shall accept embossed IC card SIM.

6.2. ELECTRICAL INTERFACE

6.2.1. Operating speed

The SIM shall support 1 to 5 MHz.
The clock shall be supplied by the ME. No "internal clock" SIMs shall be used.
The duty cycle shall be taken between 40% and 60%.
If a frequency of at least 13/4 MHz is needed by the SIM to run the authentication procedure in the allotted time (see Rec. GSM 03.20), bit b2 of byte 1 in the directory characteristics shall be set to 1. Otherwise a minimal frequency of 13/8 MHz can be used.

The ME manufacturers are reminded to take Clause 4.2.5 of IS 7816/3 into account when implementing a frequency change.

6.2.2. Baudrate

The baudrate for all communication shall be :

(clock frequency) / 372 .

6.2.3. Voltage

The supply voltage Vcc shall be 5 V +/- 10% .
For the programming voltage Vpp, see Section 6.1.2.

6.2.4. I/O (Contact C7)

The table below defines the electrical characteristics of the I/O (Contact C7).

The values are derived from ISO/IEC 7816-3, subclause 4.2 with the following considerations:

- V_{OH} and V_{OL} always refer to the device (ME or SIM) which is driving the interface. V_{IH} and V_{IL} always refer to the device (ME or SIM) which is operating as a receiver on the interface.

- ISO/IEC 7816-3 specifically defines an ICC for which the current conventions in subclause 4.2 apply. For each state (V_{OH}, V_{IH}, V_{IL} and V_{OL}) this specification defines a positive current as flowing out of the entity (ME or SIM) in that state.

- The high current options of ISO/IEC 7816-3 for V_{IH} and V_{OH} are not specified for the SIM as they apply to NMOS technology requirements. No realisation of the SIM using NMOS is foreseen.

The values given in the table have the effect of defining the values of the pull-up resistor in the ME and the impedances of the drivers and receivers in the ME and SIM.

The following table gives the electrical characteristics of I/O under normal operating conditions.

Symbol	Conditions	Minimum	Maximum
V_{IH}	I_{IHmax} = ±20µA[2)]	0,7xVcc	Vcc+0,3V
V_{IL}	I_{ILmax} = +1mA	-0,3V	0,8V
V_{OH}[1)]	I_{OHmax} = +20µA	3,8V	Vcc
V_{OL}	I_{OLmax} = -1ma	0V	0,4V
t_R t_F	C_{out} = C_{in} = 30pF		1µS

1) It is assumed that a pull-up resistor is used in the interface device (recommended value: 20kohms).

2) During static conditions (idle state) only the positive value can apply. Under dynamic operating conditions (transmission) short term voltage spikes on the I/O line may cause a current reversal.

6.2.5. Mode of operation

There are two states for the SIM while the power supply is on:

The SIM is in operating state when it executes an instruction. This state also encludes transmission from and to the ME;

The SIM is in idle state at any other time.

The SIM shall retain all pertinent data during the idle state.

In order to avoid additional traffic flow over the air interface no SIM shall be used where the transition from the idle state to the operating state has to be followed by the authentication procedure.

To reduce the power consumption the SIM should support a sleep mode when it is in idle state. Three types of sleep mode are to be distinguished :

* "Full internal sleep mode" : the chip manages by itself the sleep mode;

- "Instruction sleep mode" : solution which needs the "SLEEP" instruction;

- "Clock sleep mode" : solution which incorporates stopping the clock.

In order to simplify matters, the following procedure shall always be implemented.

The ME shall always send a "SLEEP" instruction even if the SIM has an internal sleep mode. The ME shall wait at least 2 elementary time units after having received the compulsory acknowledgement SW1 SW2 of the "SLEEP" instruction before it switches off the clock (if it is allowed to do so). It shall wait at least 2 elementary time units before it sends the first instruction after having started the clock.

Even if the SIM has an internal sleep mode, it shall always send the status information "normal ending of the command" after the successful interpretation of the instruction "SLEEP".

The clock may only be switched off if bit b1 of byte 1 in the directory characteristics is set to 1. Those chips for which the stop of the clock could cause security problems shall have this bit set to 0.

6.2.6. Supply current

The current consumption of the SIM shall not exceed 10 mA. The supply current shall not exceed 200 microA at 1 MHz and 25°C when the SIM is in sleep mode.

Due to technology, spikes in the supply current can occur, the amplitude of which can be a multiple of the average current consumption. The power supply shall be able to counteract spikes up to a maximum charge of 40 nAs with no more than 400 ns duration and an amplitude of at most 200 mA, ensuring that the supply voltage stays in the specified range.

Note: A possible solution would be to place a capacitor (e.g. 100 nF, ceramic) as close as possible to the contacting elements.

6.2.7. Activation sequence of SIM contacts

When the MS is soft powered on, the contacts shall be activated according to ISO/IEC 7816-3:1989 section 5.1. For any voltage level, monitored during the activation sequence, the order of contact activation shall be respected.

6.2.8. De-activation sequence of SIM contacts

When the MS is soft powered off, the contacts shall be de-activated according to ISO/IEC 7816-3:1989 section 5.4. For any voltage level, monitored during the deactivation sequence, the order of contact deactivation shall be respected.

Note: Soft Power Switching is defined in TS GSM 02.07.

6.2.9. Inactive SIM/ME Contacts

The voltages on contacts C1, C2, C3, C6 and C7 of the ME shall be between 0 and +/-0.4 volts referenced to ground (C5) when the ME is switched off with the power source connected to the ME. The measurement equipment shall have a resistance of 50 kohms when measuring the voltage on C2, C3, C6 and C7. The resistance shall be 10 kohms when measuring the voltage on C1.

ANNEX 1

SIM SCENARIOS

1. INTRODUCTION

This document describes several SIM-ME procedures of the GSM operation phase by using the instructions and the data-fields defined in recommendation GSM 11.11.

The HOST/USER-ME exchanges are added in the scenarios for illustrative purposes.

The exchanges are shown only in situations where the communication exchanges are correct.

2. DESCRIPTION OF SIM-ME PROCEDURES

2.1. SIM ACTIVATION

HOST/USER	ME	SIM
	Reset Status of the card	Answer to Reset <——
	Card OK SELECT Directory GSM [7F 20] ——> GET RESPONSE*	Current Directory GSM. Return GSM directory structure <——

(USER)
PIN code input
——>
	If PIN required
	Ask for PIN
	<——
	VERIFY PIN
	——>
		Compare PIN code
		if not OK
		Ratif = Ratif + 1

	IMSI Request SELECT data-field (IMSI) DF [6F 07] ——> GET RESPONSE* READB	Current DF [6F 07] Return DF [6F 07] structure <—— Return IMSI <——

* SW1 and SW2 of the SELECT command return the length of the GET RESPNSE informations.

HOST/USER	ME	SIM
	SIM capability request SELECT data-field (SIM service table) DF [6F 38] ——> GET RESPONSE* READB	Current DF [6F 38] Return DF [6F 38] structure <—— Return SIM service table <——
	PLMN request SELECT data-field (PLMN) DF [6F 30] ——> GET RESPONSE* READB	Current DF [6F 30] Return DF [6F 30] structure <—— Return PLMN <——
	Other Requests SELECT data-field (BCCH) DF [6F 74] or (RACH) DF [6F 78] ——> GET RESPONSE* READB	Current DF [6F ??] Return DF [6F ??] structure <—— Return BCCH or Return RACH <——

* SW1 and SW2 of the SELECT command return the length of the GET RESPNSE informations.

HOST/USER	ME	SIM
(HOST) Connection acknowledge ——> Receive IMSI AUTHENTIFICATION (Rand,n) ——>	Call HOST <—— Send IMSI to HOST <——	
	RUN SIM AUTHENTICATION (Rand) ——> GET RESPONSE*	Run inatrenal algorithm (Rand,Ki) Send Kc and SRES <——
(HOST) Receive SRES Authentication OK ——>	Send SRES to HOST <——	

* SW1 and SW2 of the RUN SIM AUTHENTIFICATION return the length of the GET RESPONSE informations

HOST/USER	ME	SIM
	Cipher key and sun. var. store	
	SELECT data-field (Kc,n) Dir GSM [6F 20] ——>	
		Current DF [6F 20]
	GET RESPONSE*	Return DF [6F 20] structure <——
	UPDATEB ——>	
		Update OK
(HOST)		
	TMSI Update	
New TMSI,LAI,TMSI time ——>		
	SELECT data-field (TMSI) Dir GSM [6F 7E] ——>	
		Current DF [6F 7E]
	GET RESPONSE*	Return DF [6F 7E] structure <——
	UPDATEB ——>	
		Update OK
End of normal activation procedure		

* SW1 and SW2 of the SELECT command return the length of the GET RESPONSE informations.

2.2. PIN SUBSTITUTION

USER	ME	SIM
PIN substitution request Old PIN New PIN ——>		
	CHANGE PIN Old PIN New PIN ——>	
		Compare PIN code If not OK Ratif = Ratif + 1
	Change PIN code OK	

2.3. PIN CODE DISABLING

USER	ME	SIM
PIN disabling request PIN code ——>		
	DISABLE PIN PIN code ——>	
		If disable, PIN option is available Compare PIN code If not OK Ratif = Ratif + 1
	PIN code disabled OK	

2.4. PIN CODE ENABLING

USER	ME	SIM
PIN enabling request PIN code ——>		
	REENABLE PIN PIN code ——>	
		If disable, PIN option is available Compare PIN code If not OK Ratif = Ratif + 1
	PIN code reenable OK	

2.5. LOCAL INFORMATION UPDATE

HOST	ME	SIM
New TMSI,LAI,TMSI time ——>		
	SELECT data-field (TMSI) Dir GSM [6F 7E] ——>	
		Current DF [6F 7E]
	GET RESPONSE*	
		Return DF [6F 7E] structure <——
	UPDATEB ——>	
		Update OK

* SW1 and SW2 of the SELECT command return the length of the GET RESPONSE informations.

Same item for the following data-field:

Data-field BCCH DF [6F 74]
Data-field KC,n DF [6F 20]
Data-field Abbreviated dialling number DF [6F 3A]
Data-field Capability parameters DF [6F 3D]
Data-field Short message DF [6F 3C]
Data-field Fixed dialling number DF [6F 3B]
Data-field Charging counter DF [6F 39]

2.6. SHORT MESSAGE STORAGE

HOST	ME	SIM
Short Message storage Message ——>		
	Check SIM CAPABILITY TABLE, Short Message storage available	
	SELECT Directory Telecom [7F 10] ——>	
		Current directory Telecom
	GET RESPONSE*	Return Telecom directory structure <——
	SELECT data-field (Short Message) DF [6F 3C] ——>	
		Current DF [6F 3C]
	GET RESPONSE*	Return DF [6F 3C] structure <——
	SEEK first record free ——>	
		Current record is the first record free
	UPDATER (Short Message) ——>	
		Update OK
	SELECT directory GSM [7F 20] ——>	
		Current directory GSM
	GET RESPONSE*	Return GSM directory structure <——

* SW1 and SW2 of the SELECT command return the length of the GET RESPONSE informations.

2.7. SHORT MESSAGE ERASURE

HOST	ME	SIM
Short Message erasure request ——>		
	Check SIM CAPABILITY TABLE, Short Message storage available	
	SELECT Directory Telecom [7F 10] ——>	
		Current directory Telecom
	GET RESPONSE*	
		Return Telecom directory structure <——
	SELECT data-field (Short Message) DF [6F 3C] ——>	
		Current DF [6F 3C]
	GET RESPONSE*	
		Return DF [6F 3C] structure <——
	SEEK record to be erased ——>	
		Current record is the record to be erased
	UPDATER (00 00 ...) ——>	
		Update OK
	SELECT Directory GSM [7F 20] ——>	
		Current Directory GSM
	GET RTESPONSE*	
		Return GSM directory structure <——

* SW1 and SW2 of the SELECT command return the length of the GET RESPONSE informations.

ANNEX 2

SIM SDL PROCEDURE CHARTS

STATUS DEFINITIONS AND GENERAL NOTE FOR SIM SDL PROCEDURE CHARTS

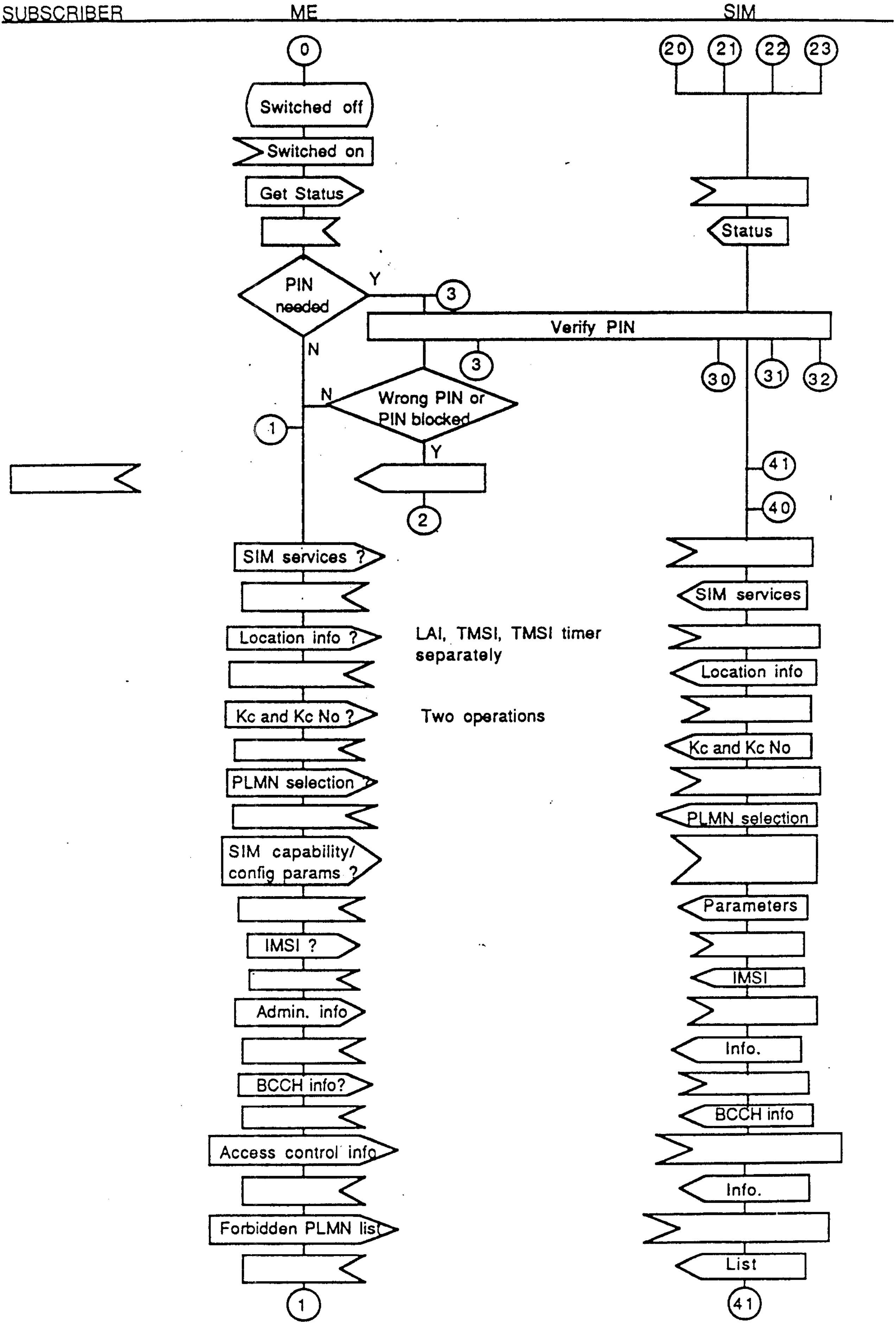
Statust definitions

0 - ME switched off
1 - ME ready for registration
2 - MS service blocked by SIM
3 - ME ready to ask subscriber for PIN
4 - ME switched on and equipped with SIM
5 - MS ready to make calls
6 - MS in call set-up phase
7 - MS in call phase
8 - MS needs LOC UPD

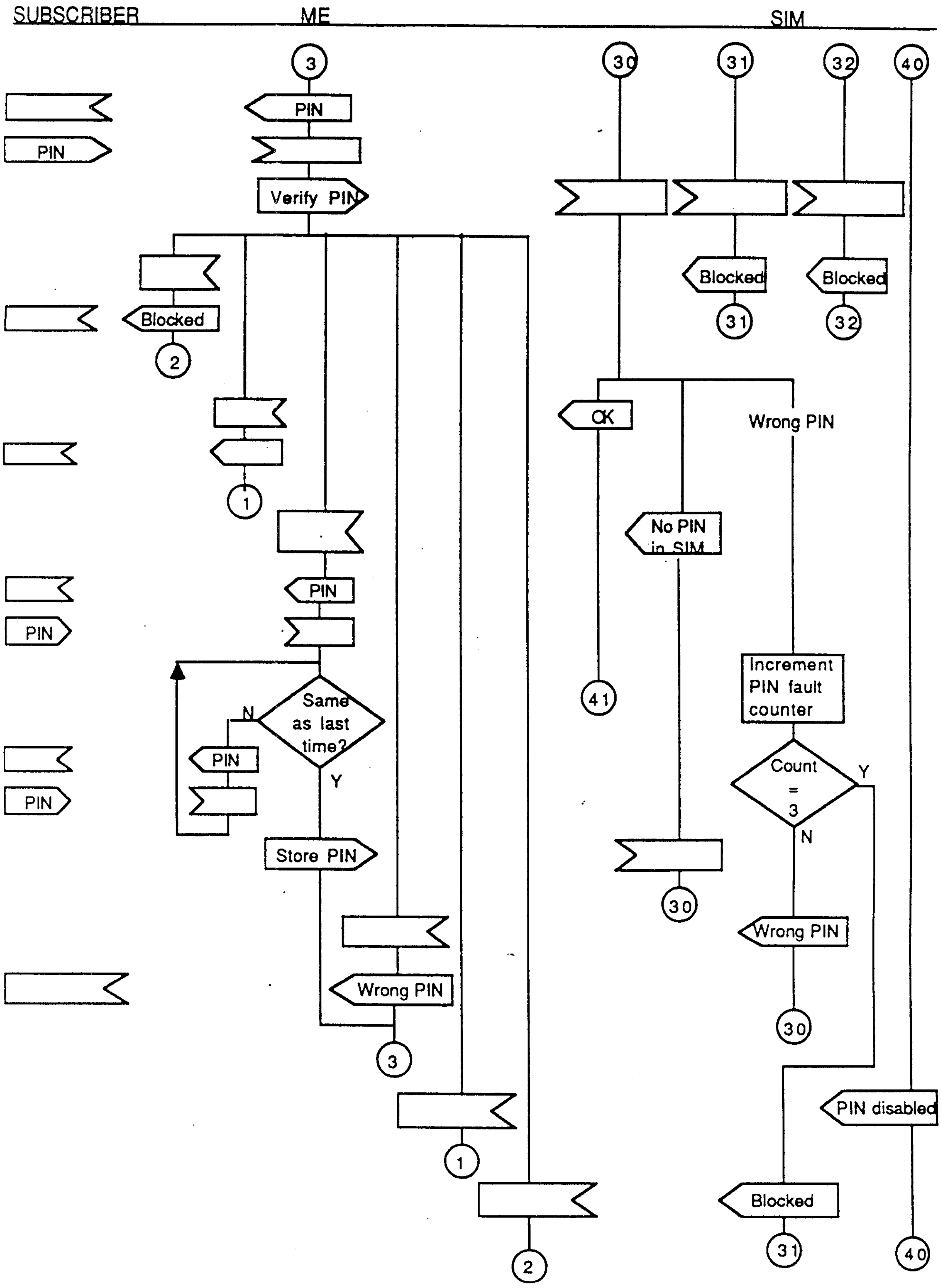
SIM statuses are as defined for the SIM State Transition Diagram.

General note

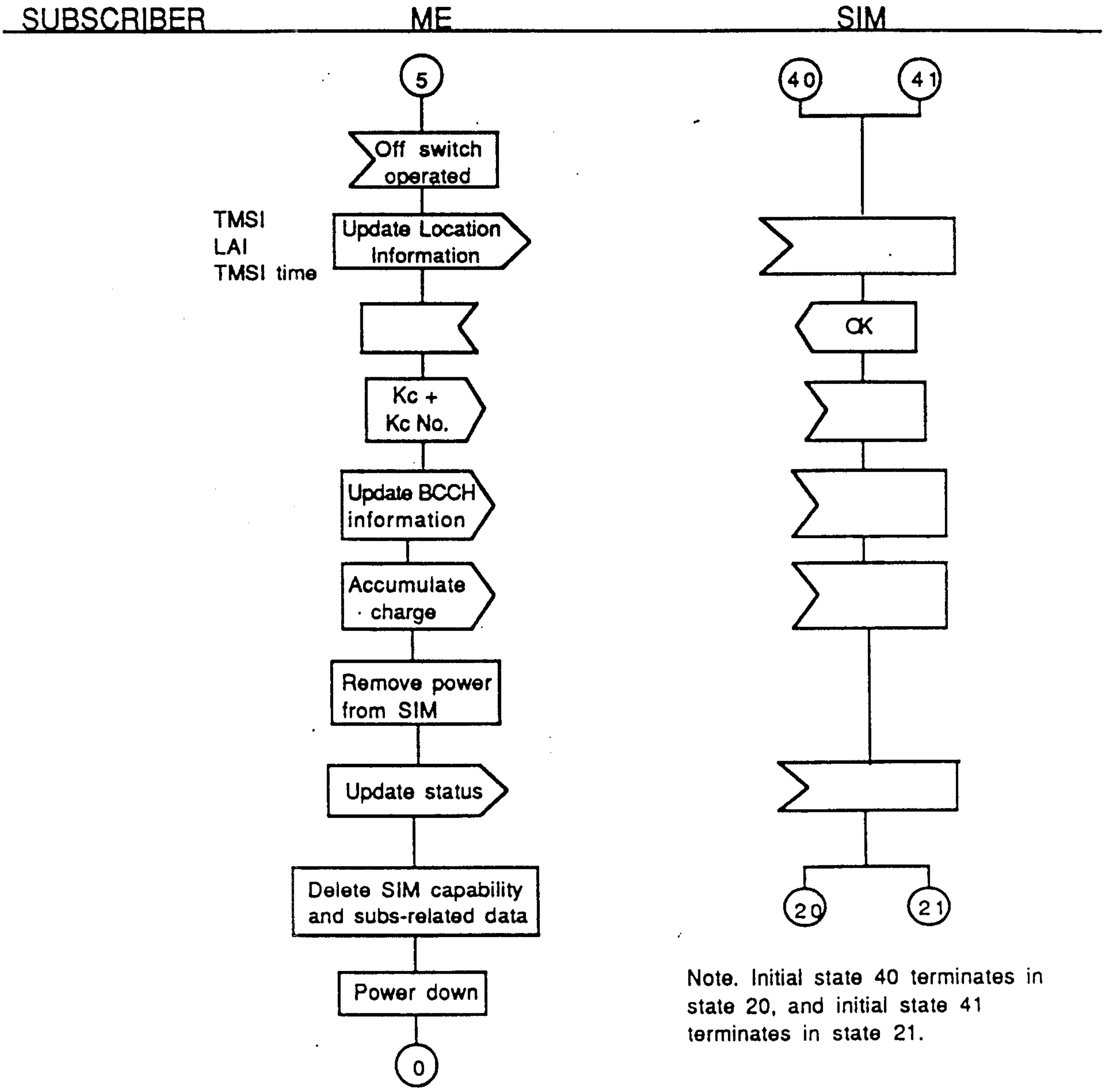
Emergency calls ("112", see GSM 02.30) can be attempted at any time when the ME is switched on, except during call and call set-up phases.



OPENING PROCEDURES

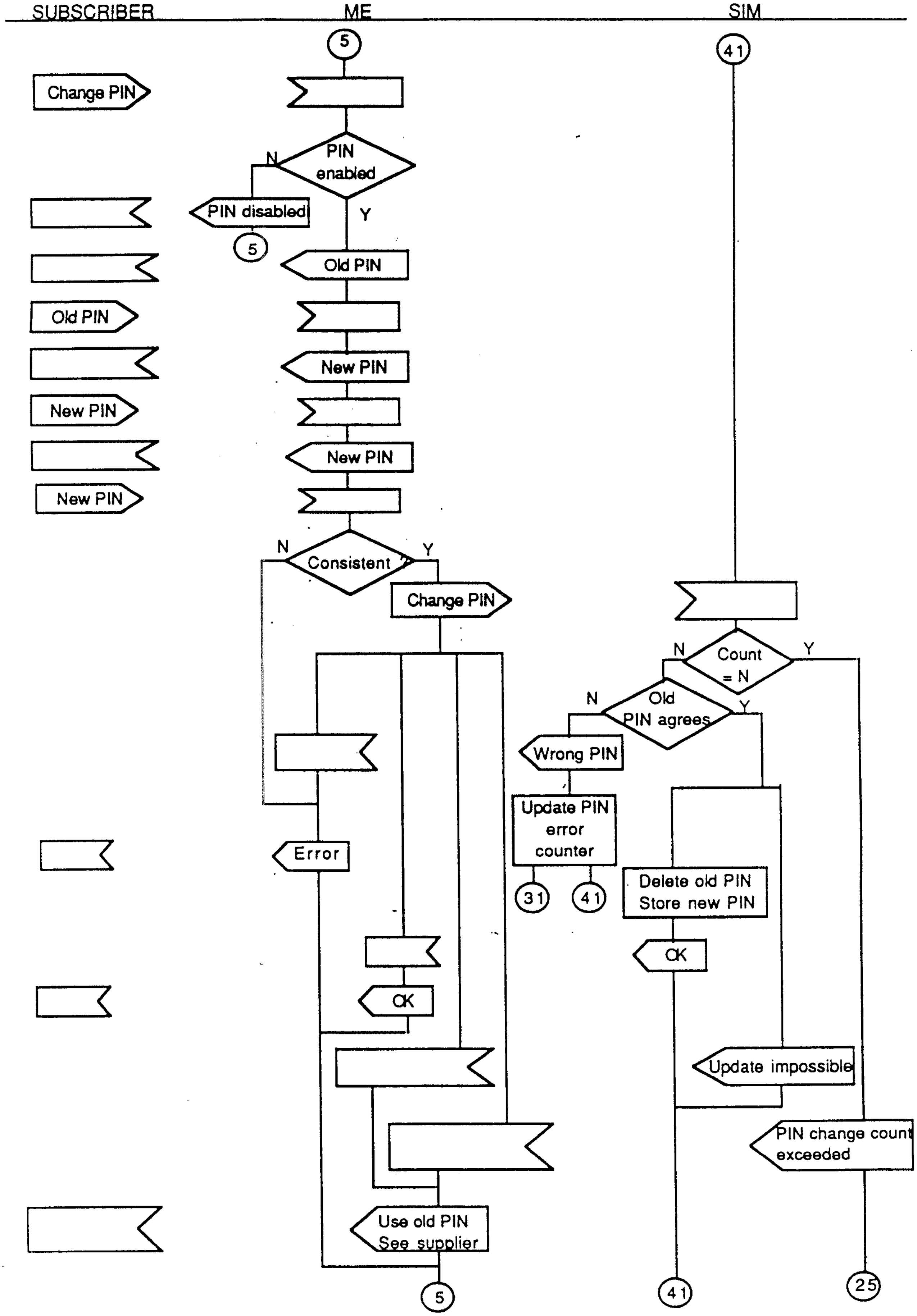

SUBSCRIBER
ME
SIM
3
30
31
32
40
PIN
PIN
Verify PIN
Blocked
Blocked
Blocked
2
31
32
OK
Wrong PIN
1
No PIN in SIM
PIN
PIN
41
Increment PIN fault counter
Same as last time?
N
Y
PIN
PIN
Count = 3
Y
N
Store PIN
30
Wrong PIN
Wrong PIN
30
3
PIN disabled
1
Blocked
2
31
40

VERIFY PIN

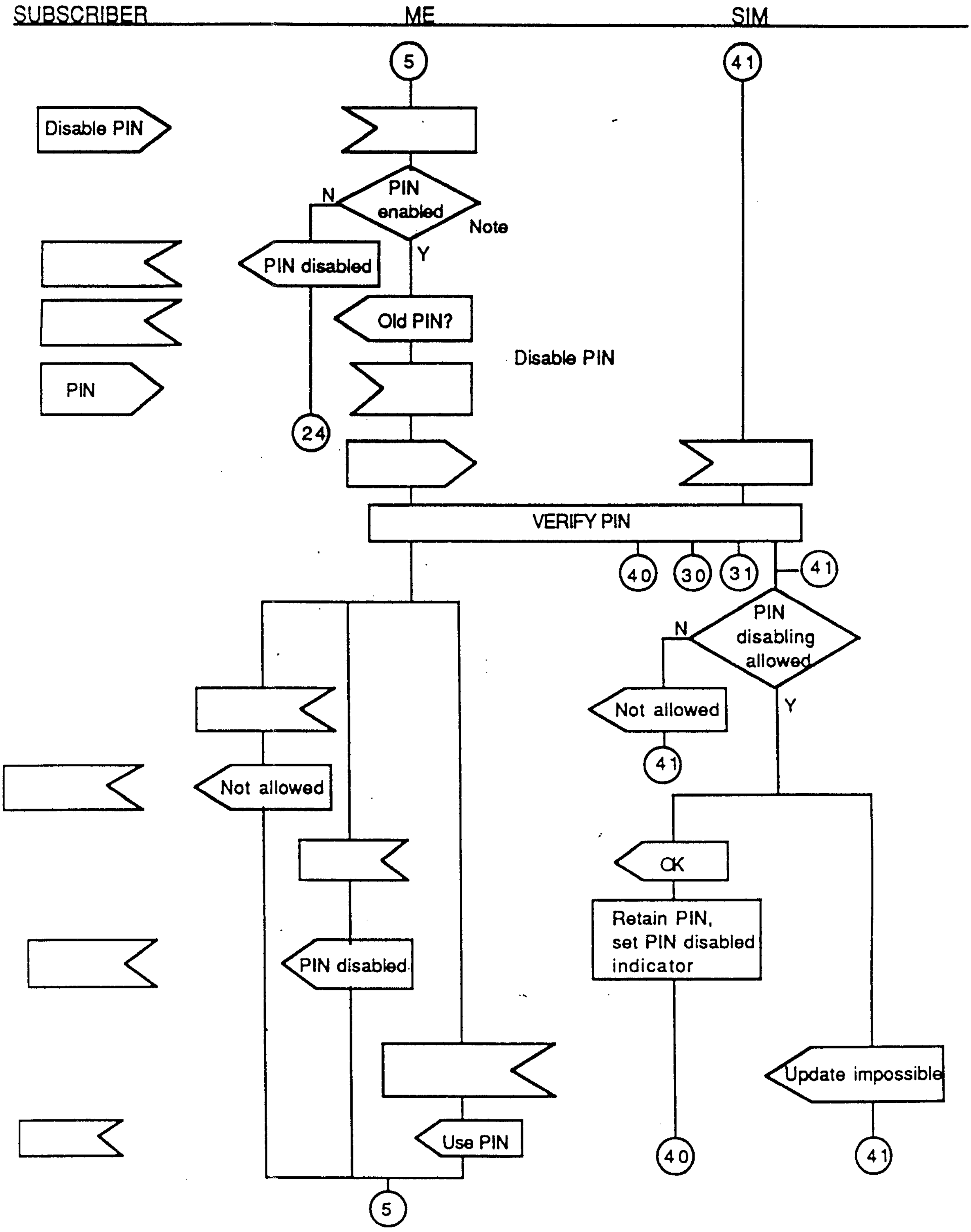


Note. Initial state 40 terminates in state 20, and initial state 41 terminates in state 21.

SIM DEACTIVATION

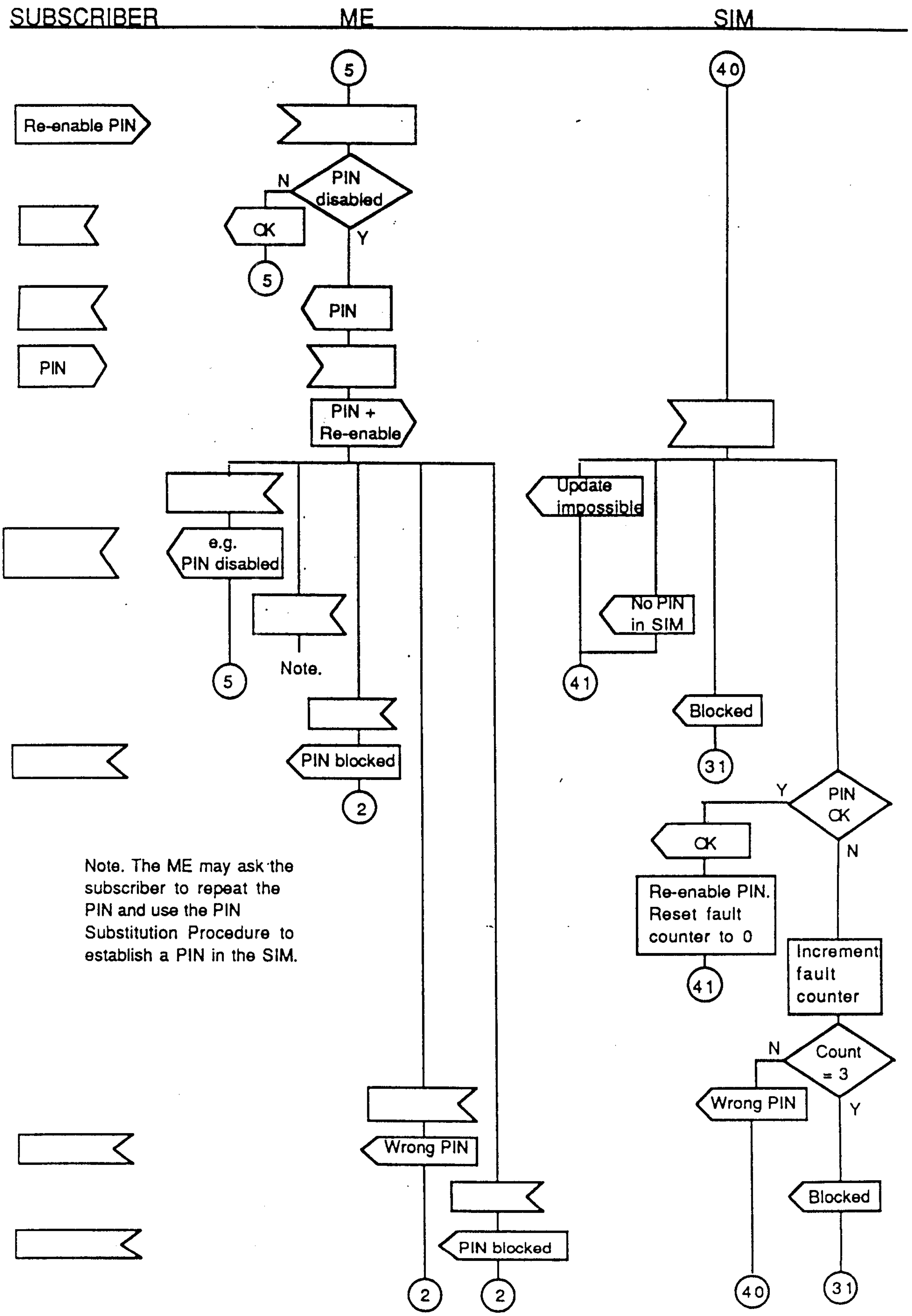


USER PIN CODE SUBSTITUTION



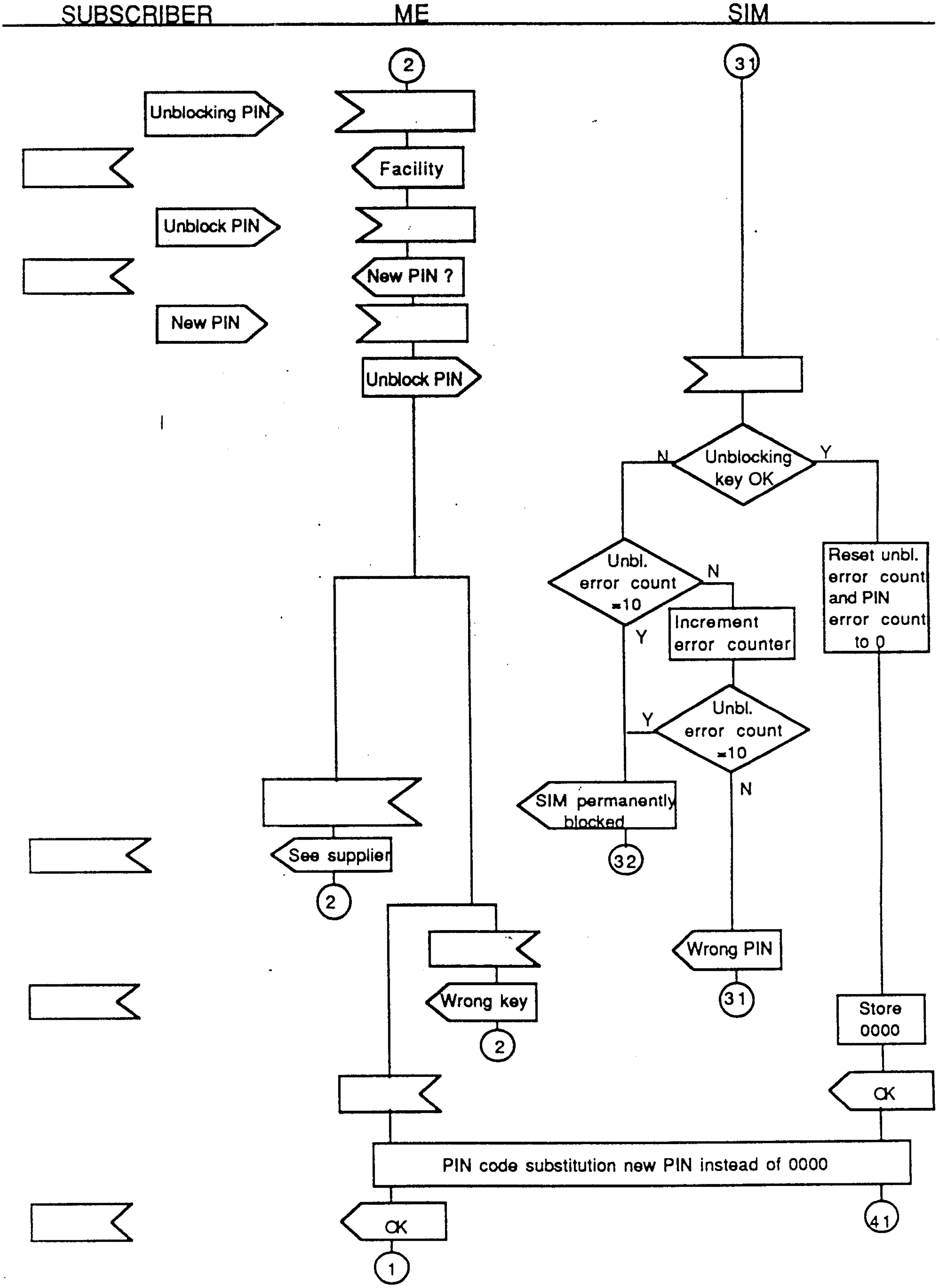
Note. If the ME does not implement the facility of stopping interaction with the SIM when the PIN is disabled, "PIN disabled" would be returned as a status reply from the SIM.

DISABLE PIN FACILITY

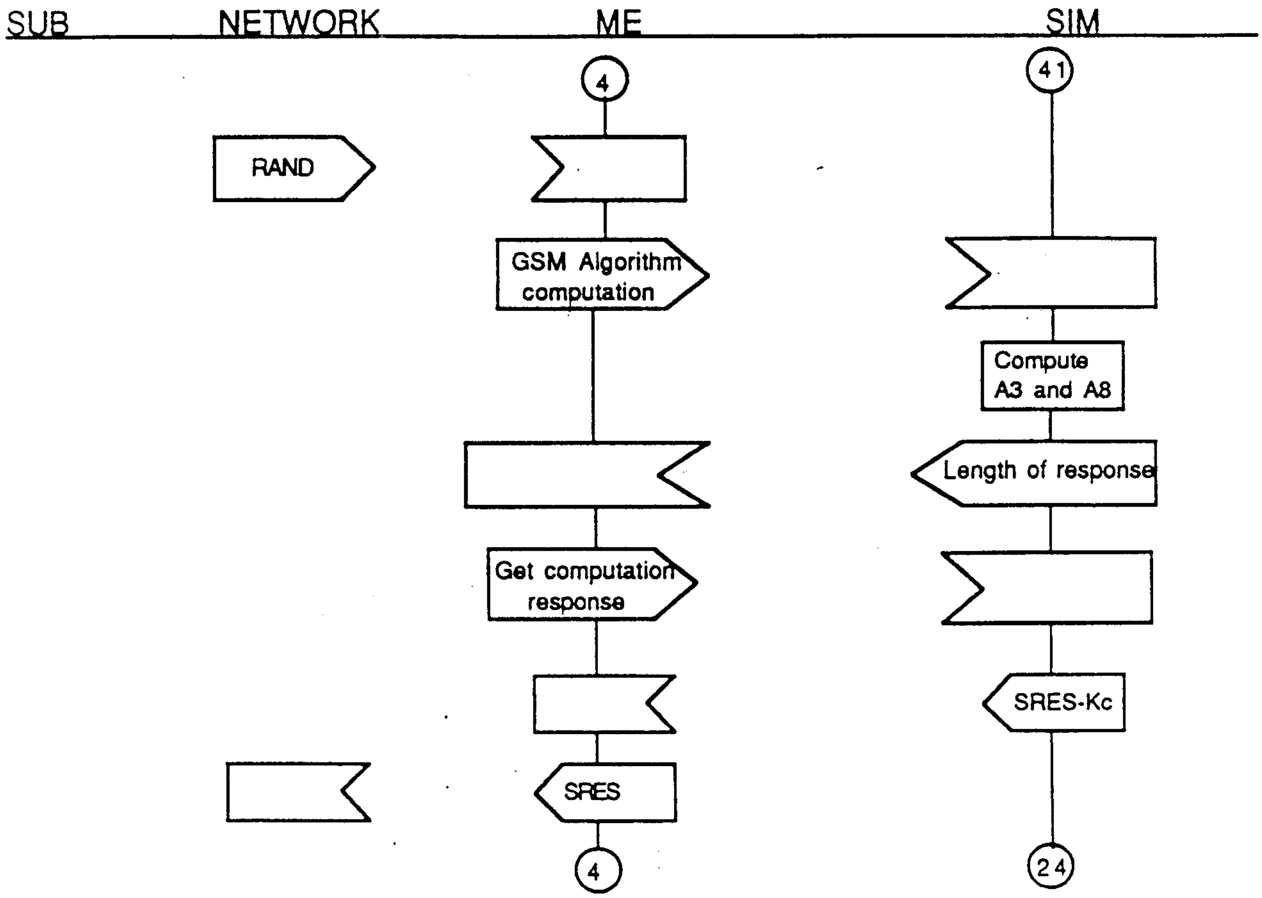


Note. The ME may ask the subscriber to repeat the PIN and use the PIN Substitution Procedure to establish a PIN in the SIM.

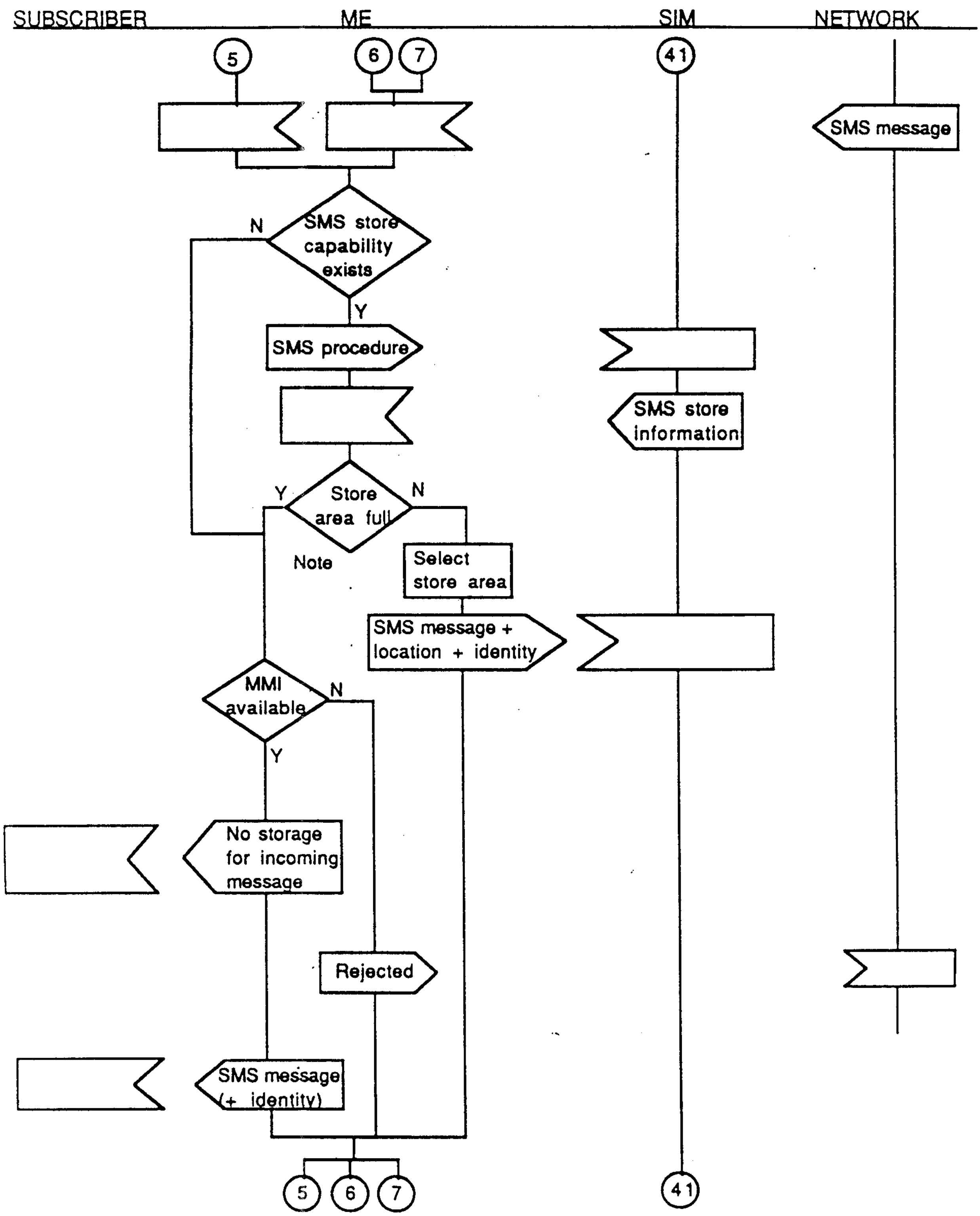
PIN RE-ENABLING



SIM UNBLOCKING

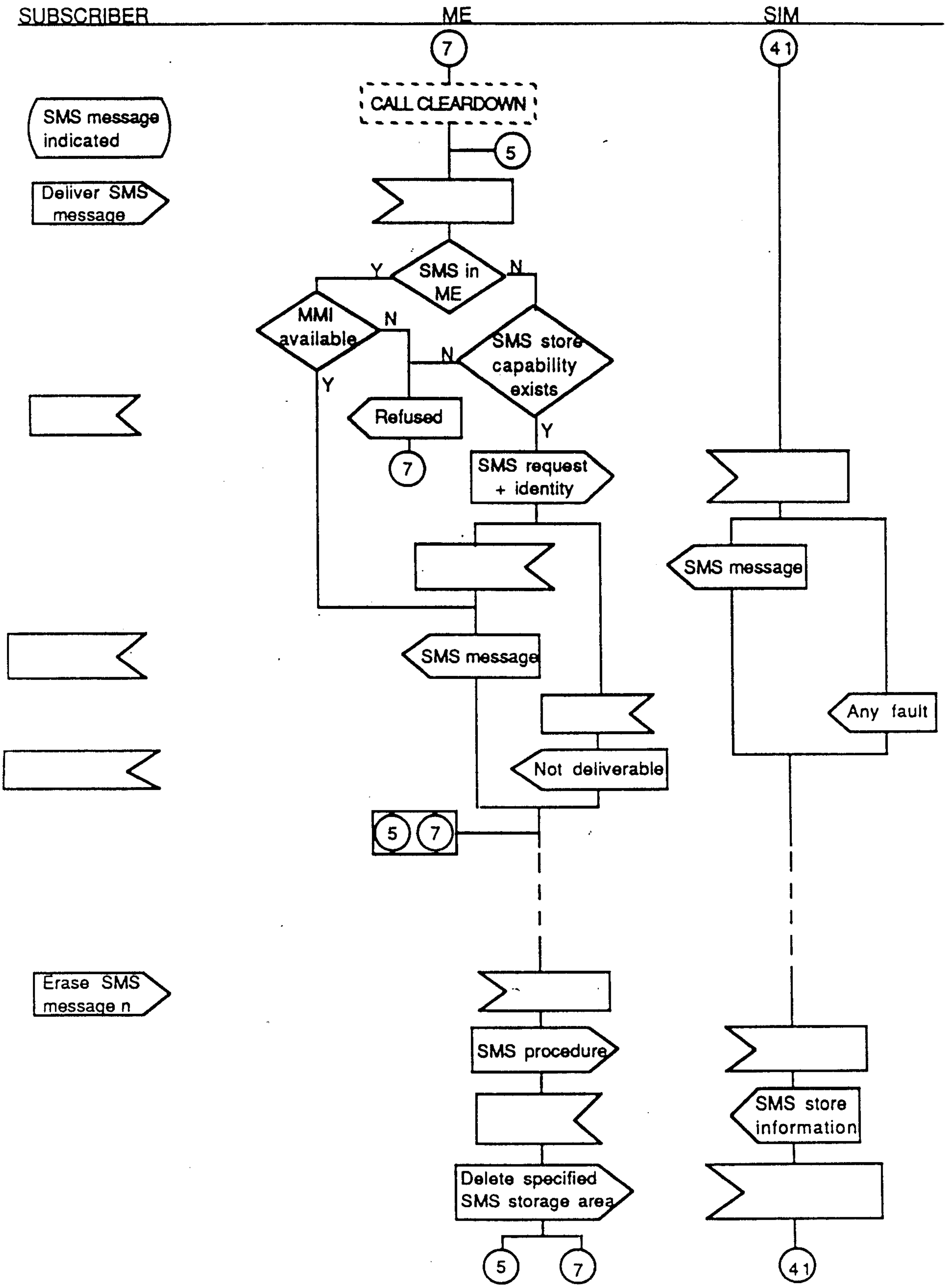


Note. If the SIM quotes a parameter or response fault in its replies to the MS, the MS may re-try. If it cannot, or the retry fails, the MS may tell the subscriber that authentication has failed.

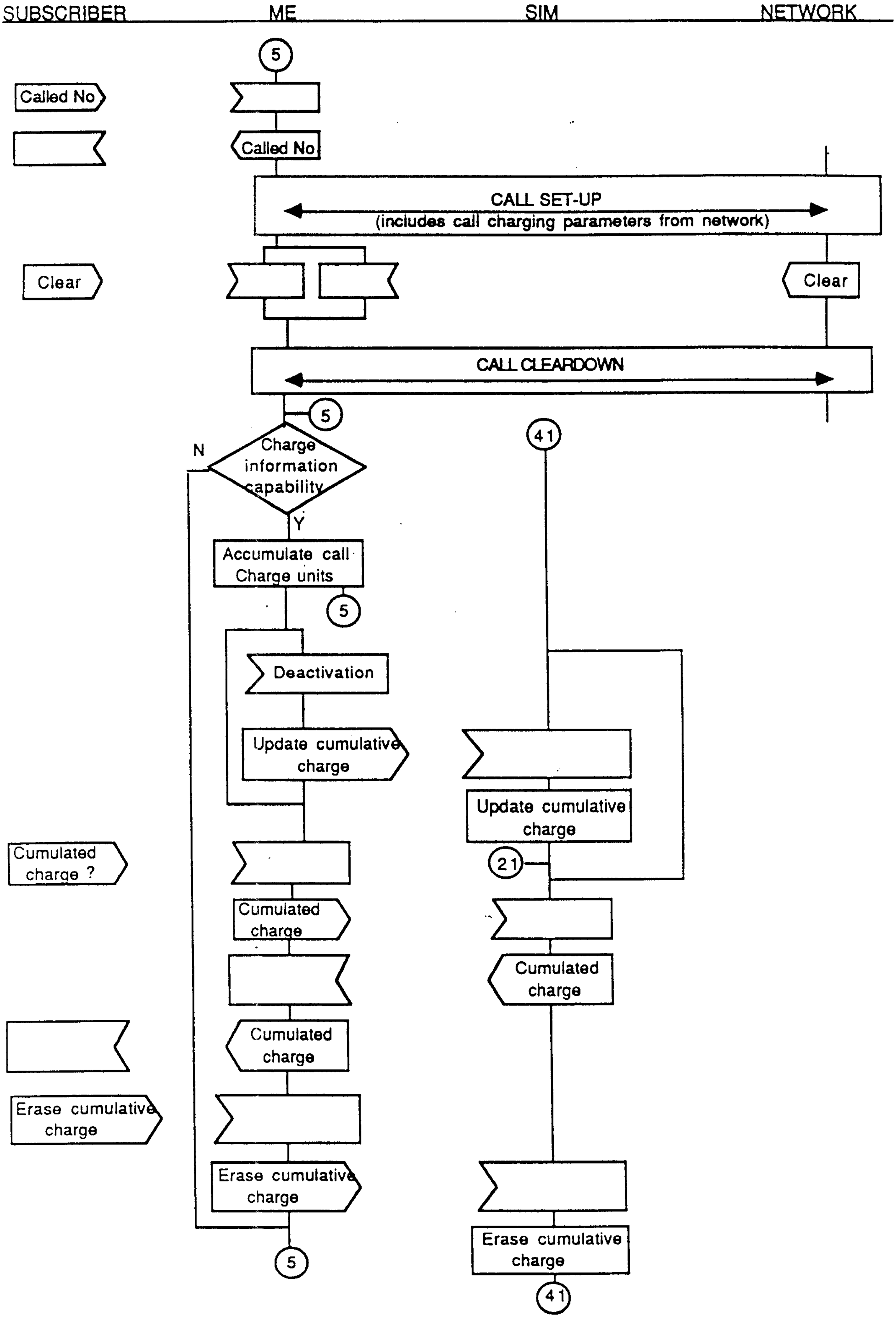


Note. It is here assumed that only the SIM is incapable of storing the message.Procedures for clearing space in the SIM are dependent on ME implementation.

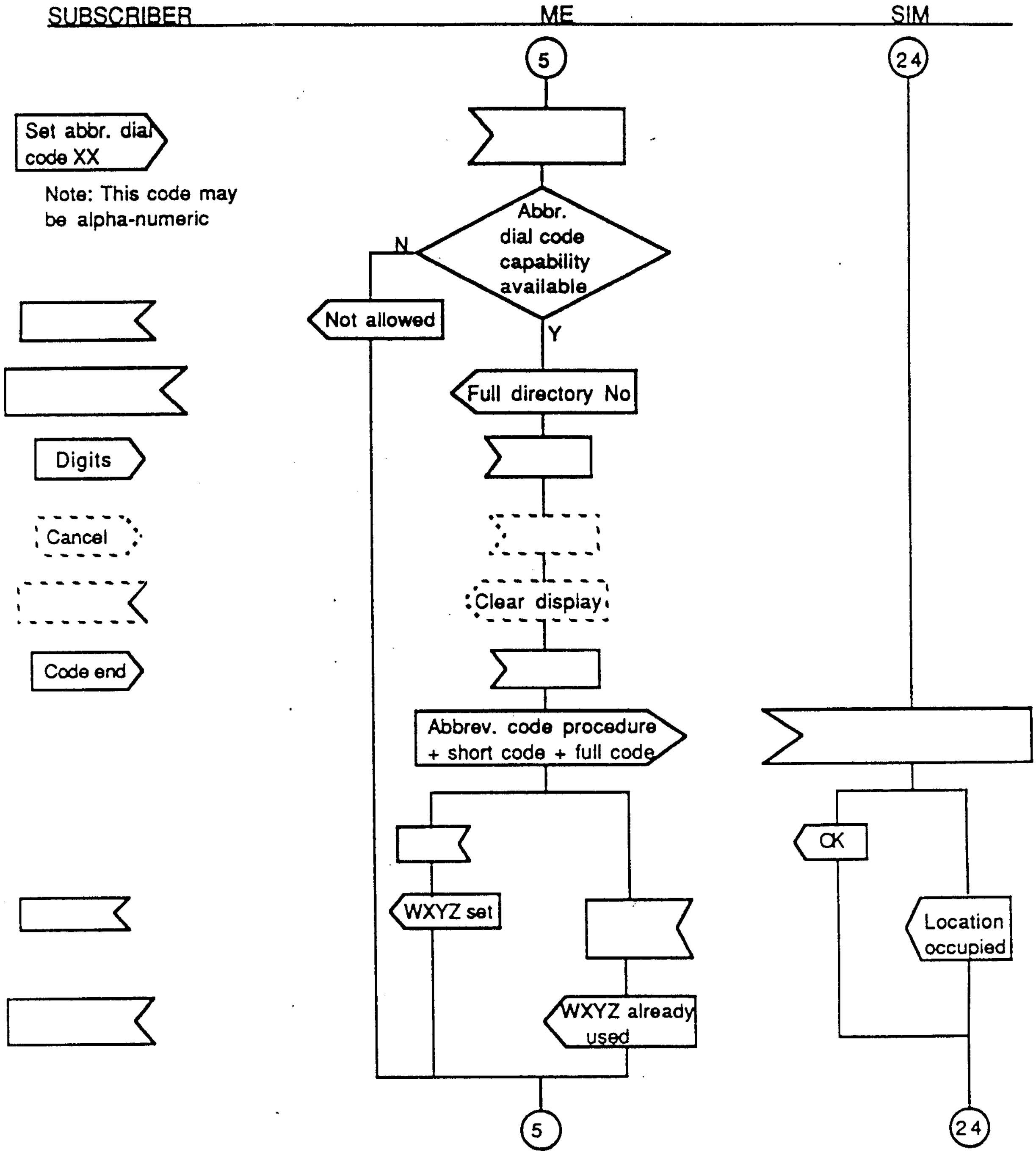
SMS MESSAGE RECEPTION AND STORAGE IN SIM



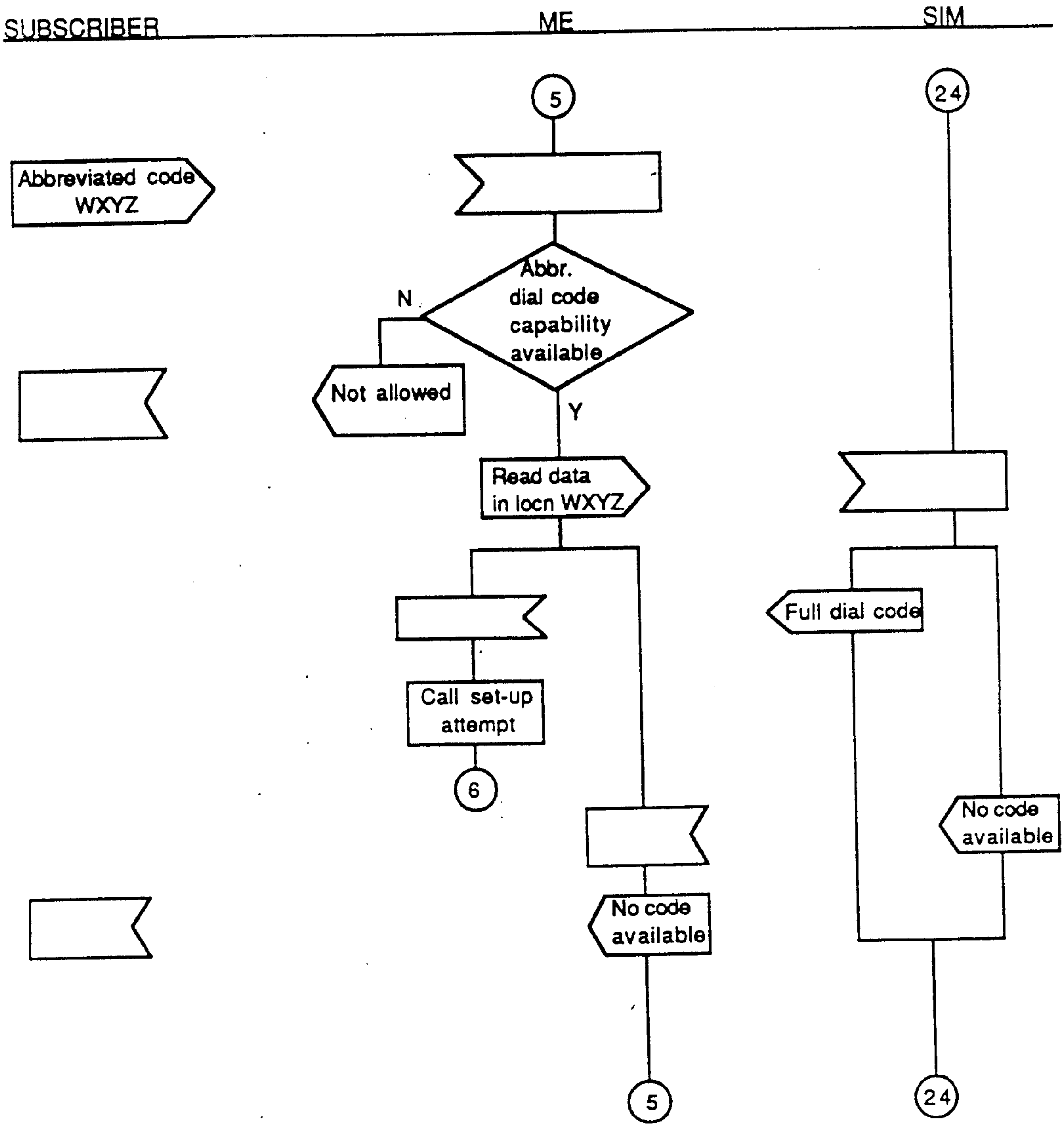
SMS MESSAGE DELIVERY AND ERASURE



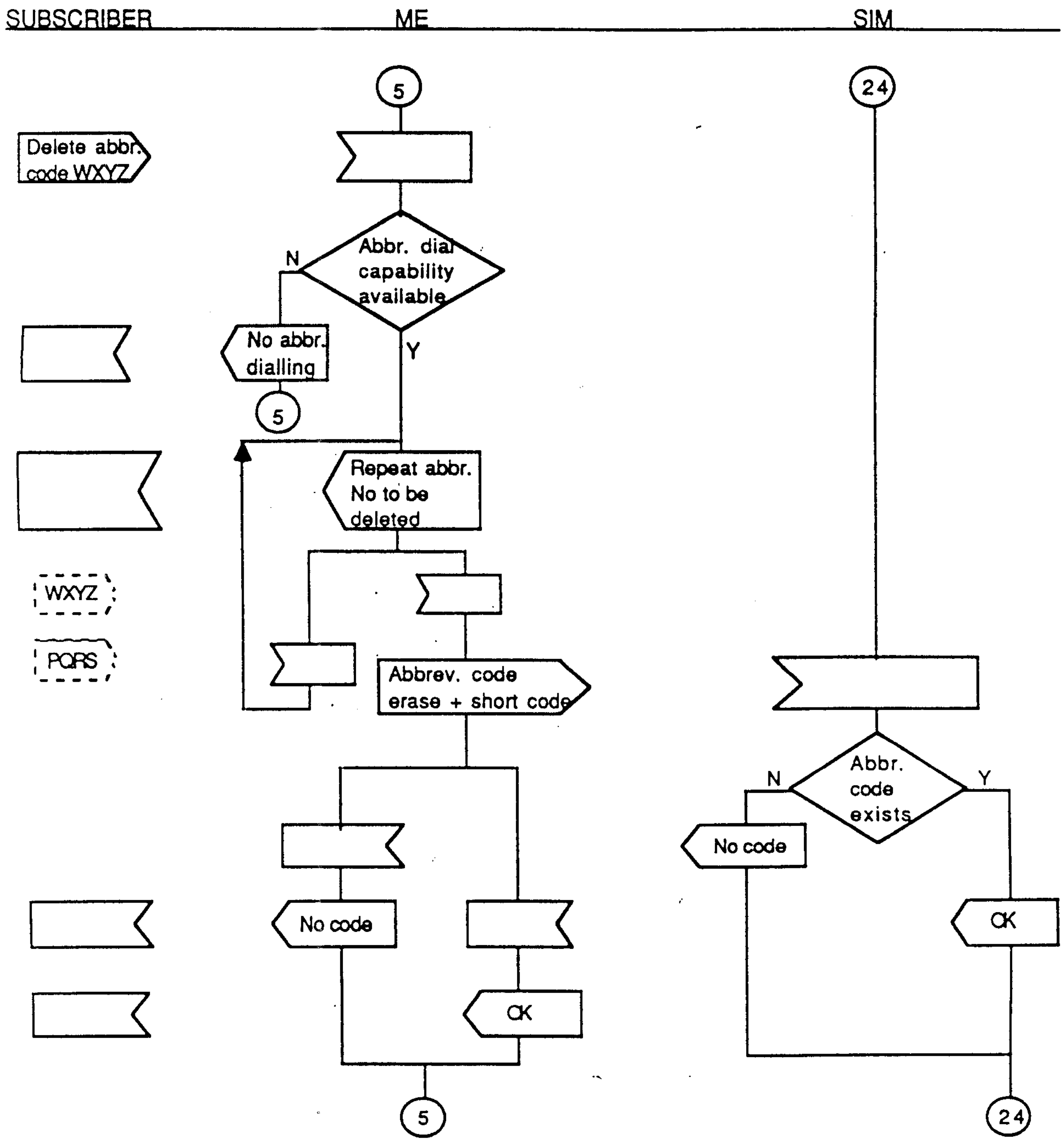
CUMULATIVE CHARGE PROCEDURES



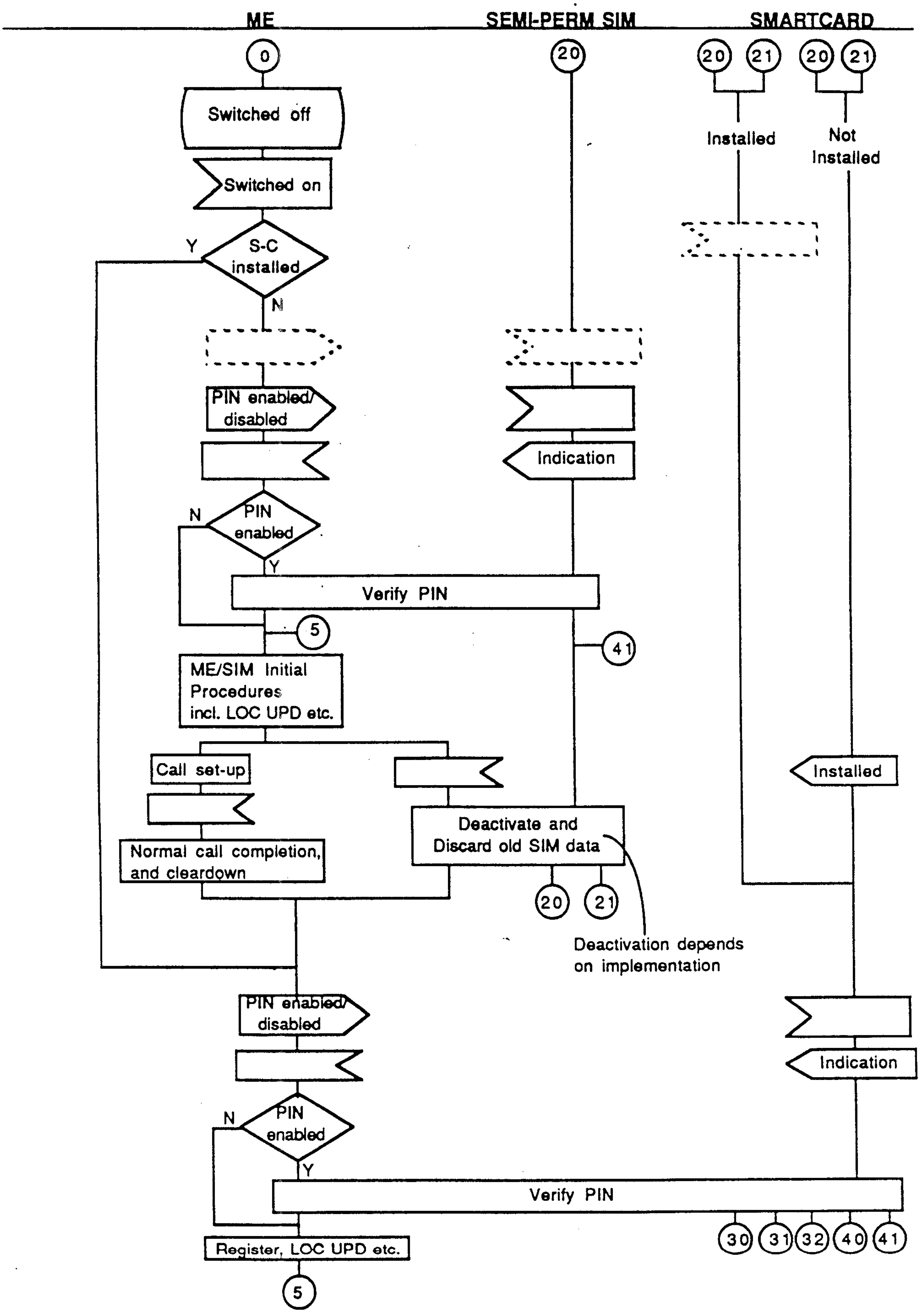
ABBREVIATED DIALLING NUMBER STORAGE



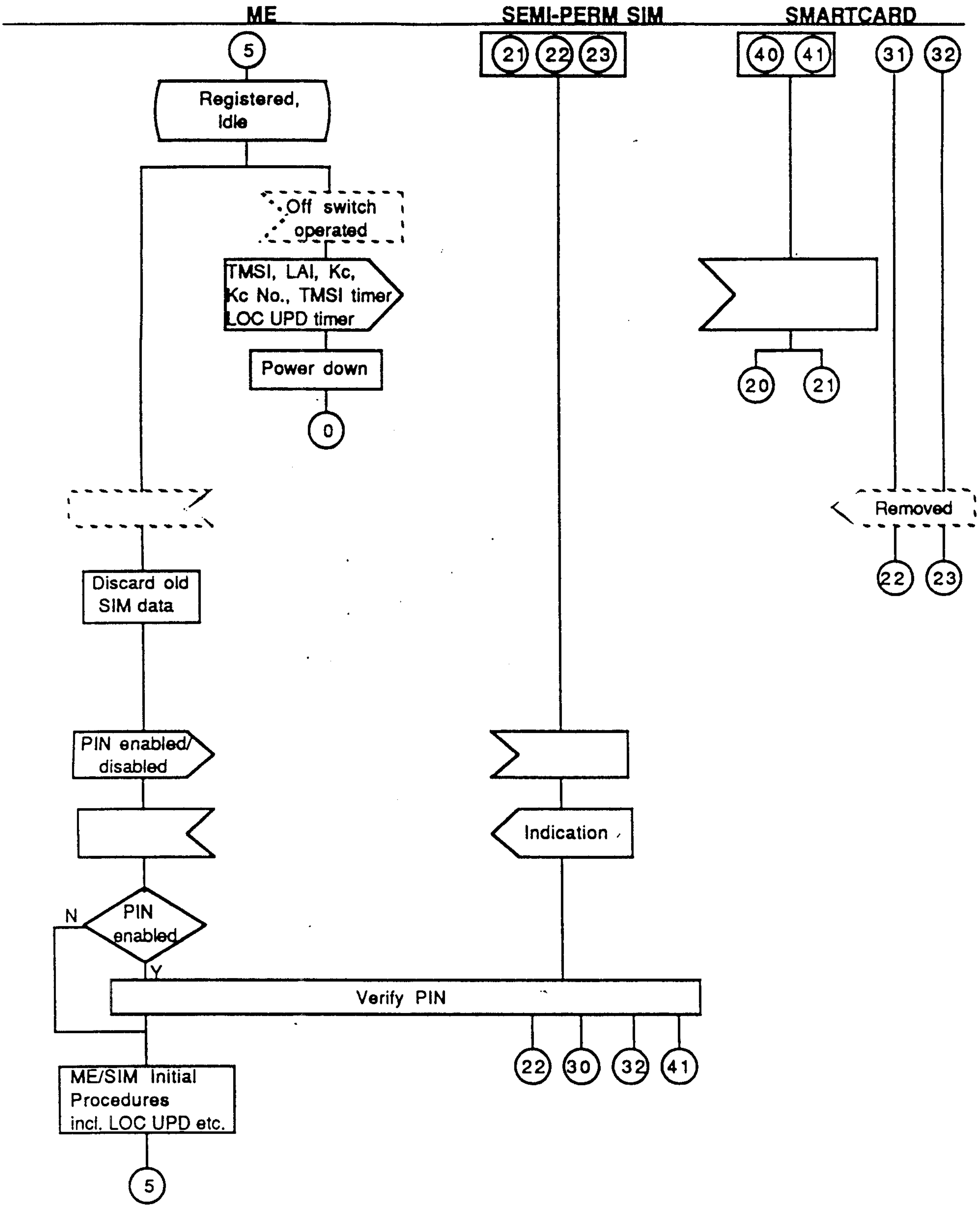
ABBREVIATED DIALLING NUMBER REQUEST



ABBREVIATED DIALLING CODE ERASURE



PROTOCOL FOR ME WITH SEMI-PERMANENT AND SMARTCARD SIM FACILITIES 1 of 2



PROTOCOL FOR ME WITH SEMI-PERMANENT AND SMARTCARD SIM FACILITIES
SWITCH OFF AND SMARTCARD REMOVAL 2 OF 2

ANNEX 3

Annex 3

SIM STATE TRANSITION DIAGRAM

The task of the SIM STATE TRANSITION DIAGRAM is to describe different states of the SIMs and the events which result in state-transitions. The reason to distinguish different SIM-states is to define at which state a specific ME-instruction can be performed. Therefore a STATE/INSTRUCTION ATTACHMENT TABLE is appended to the STATE TRANSITION DIAGRAM showing the relations between SIM-States and ME-Instructions.

Description of SIM-States:

STATE 20: This state is characterized by the following items:

- The SIM is deactivated; that means the SIM is unpowered.
- The PIN check has been disabled during a previous session or during the phase of the administrative management of the SIM by the network operator.
- This SIM is not blocked neither unusable.

STATE 21: This state is characterized by the following items:

- The SIM is deactivated.
- The PIN check is enabled.
- The SIM is not blocked neither unusable.

STATE 22: This state is characterized by the following items:

- The SIM is deactivated.
- The SIM is blocked as a result of 3 failed PIN verification attempts.
- The SIM is still usable.

STATE 23: This state is characterized by the following items:

- The SIM is deactivated.
- The SIM is unusable for GSM-application as a consequence of 10 failed unblocking attempts.

STATE 30: This state is characterized by the following items:

- The SIM is activated; that means the SIM is powered.
- The PIN check is enabled; therefore the PIN has to be verified before the subscriber gets access to the network.
- The MS is in offline-operation; that means the communication between SIM and ME is restricted to local operations, - the network is not accessed.

STATE 31: This state is characterized by the following items:

- The SIM is activated.
- The SIM is blocked; therefore only specific instruction for unblocking and status-request are executable in that state.
- The MS is in offline operation.

STATE 32: This state is characterized by the following items:

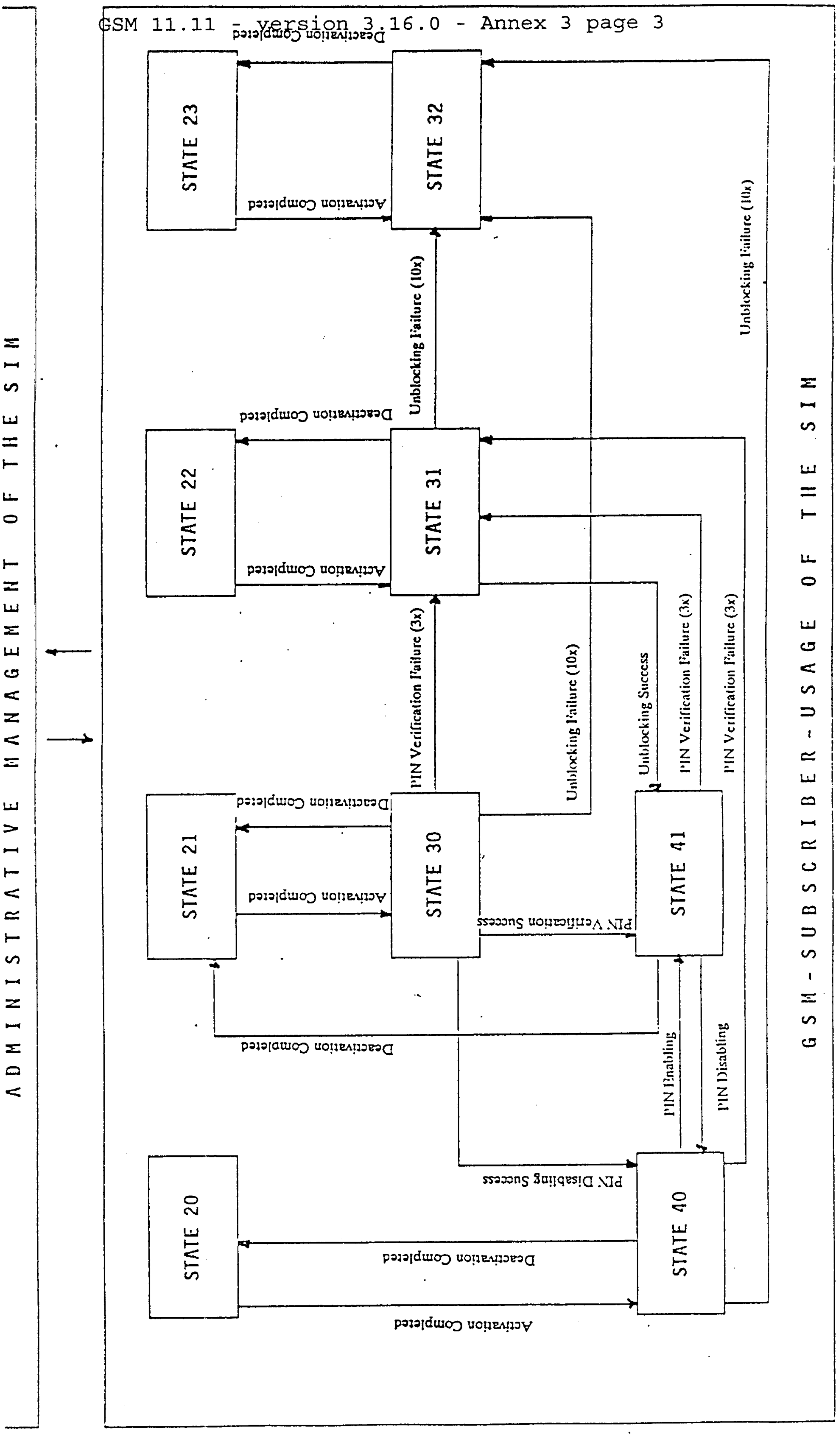
- The SIM is activated.
- The SIM is forever unusable for the GSM-application, as a consequence of 10 failed unblocking attempts. So in this state it is only possible to change between the states 23 and 32 by activating and deactivating the SIM. There is no possibility to return to normal operation again.

STATE 40: This state is characterized by the following items:

- The SIM is activated.
- The PIN check is disabled. Therefore the SIM changes directly to this STATE 40 after its activation.
- The MS is in online-operation; that means the MS may have access to the network. Therefore most of the instructions defined for the GSM-application are executable during this state.

STATE 41: This state is characterized by the following items:

- The SIM is activated.
- The PIN check is enabled.
- The MS is in online-operation.
- This state can be reached through states 30, 31 and 40 after a successful PIN verification or PIN enabling procedure.


ADMINISTRATIVE MANAGEMENT OF THE SIM
GSM-SUBSCRIBER-USAGE OF THE SIM
STATE 20
STATE 21
STATE 22
STATE 23
STATE 30
STATE 31
STATE 32
STATE 40
STATE 41
Activation Completed
Deactivation Completed
Activation Completed
Deactivation Completed
Activation Completed
Deactivation Completed
Activation Completed
Deactivation Completed
Deactivation Completed
PIN Verification Failure (3x)
Unblocking Failure (10x)
Unblocking Failure (10x)
Unblocking Failure (10x)
Unblocking Success
PIN Verification Failure (3x)
PIN Verification Failure (3x)
PIN Verification Success
PIN Disabling Success
PIN Enabling
PIN Disabling

STATE/INSTRUCTION-ATTACHMENT

INSTRUCTION	STATE								
	20	21	22	23	30	31	32	40	41
read administrative data-field	-	-	-	-	X	X	X	X	X
update administrative data-field	-	-	-	-	o	o	o	o	o
read IC card identification	-	-	-	-	X	X	X	X	X
update IC card identification	-	-	-	-	-	-	-	-	-
read SIM service table	-	-	-	-	-	-	-	X	X
update SIM service table	-	-	-	-	o	o	o	o	o
read IMSI	-	-	-	-	-	-	-	X	X
update IMSI	-	-	-	-	o	o	o	o	o
read location information	-	-	-	-	-	-	-	X	X
update location information	-	-	-	-	-	-	-	X	X
read key Kc and n	-	-	-	-	-	-	-	X	X
update key Kc and n	-	-	-	-	-	-	-	X	X

INSTRUCTION	STATE								
	20	21	22	23	30	31	32	40	41
read PLMN selector	-	-	-	-	-	-	-	X	X
update PLMN selector	-	-	-	-	-	-	-	X	X
read BCCH information	-	-	-	-	-	-	-	X	X
update BCCH information	-	-	-	-	-	-	-	X	X
read forbidden PLMNs	-	-	-	-	-	-	-	X	X
update forbidden PLMNs	-	-	-	-	-	-	-	X	X
read access control	-	-	-	-	-	-	-	X	X
update access control	-	-	-	-	o	o	o	o	o
read/seek abbreviated dialing number	-	-	-	-	-	-	-	X	X
update abbreviated dialing number	-	-	-	-	-	-	-	X	X
read/seek capability/configuration parameters	-	-	-	-	-	-	-	X	X
update capability/configuration parameters	-	-	-	-	-	-	-	X	X
read/seek short message storage	-	-	-	-	-	-	-	X	X
update short message storage	-	-	-	-	-	-	-	X	X
read/seek fixed dialing numbers	-	-	-	-	-	-	-	X	X
update fixed dialing numbers	-	-	-	-	-	-	-	X	X

INSTRUCTION	STATE								
	20	21	22	23	30	31	32	40	41
read called party subaddresses	-	-	-	-	-	-	-	X	X
update called party subaddresses	-	-	-	-	-	-	-	X	X
read charging counter	-	-	-	-	-	-	-	X	X
update charging counter	-	-	-	-	-	-	-	X	X
run GSM algorithm/get response	-	-	-	-	-	-	-	X	X
status	-	-	-	-	X	X	X	X	X
sleep	-	-	-	-	X	X	X	X	X
unblock GSM-application	-	-	-	-	X	X	-	X	X
verify PIN	-	-	-	-	X	-	-	-	-
change PIN	-	-	-	-	X	-	-	-	X
disable PIN	-	-	-	-	X	-	-	-	X
enable PIN	-	-	-	-	-	-	-	X	-
select/get response	-	-	-	-	X	X	X	X	X

Explanation:

- It is not allowed to invoke this instruction during that state.
x It is allowed to invoke this instruction during that state.
o It is in the responsibility of the PLMN-operator in which state the instruction is executable.