COMMON PCN HANDSET SPECIFICATION

CPHS Phase 2

Version Number: **4.2**
Date of Issue: **27 February 1997**
Document Reference: **CPHS4_2.WW6**

Authors		
Name	Organisation	Fax
Tim Haysom	Orange PCS Ltd.	+44 1454 618501
Richard Williams	Mercury One-2-One	+44 181 214 2898
Current Editor:	Orange PCS Ltd.	

Copies of this specification are available in .PDF format (requires Adobe Acrobat reader) or on paper.
For additional copies, please contact either author.

COMMON PCN
HANDSET SPECIFICATION
(CPHS)

Document History

Changes from version 3.0 to 3.1:

MPC 2, 5rev2, 6rev1, 7, 8, 10
U 1rev2, 2, 3, 4rev1, 6, 7rev1, 9
MIC 1rev1, 3rev3, 4rev1

Changes from version 3.1 to 3.2:

MPC 12
MIC 5, 6, 7, 8rev1
Revised terms and conditions

Changes from version 3.2 to 4.1

The document has been brought up to date and extended to introduce several new features:

Information Numbers
Shortform Operator Name String
CSP Extensions
Network and SP Lock
Language reset
Engineering mode and SW version restriction

The Service String Table definition has been removed in favour of Information numbers.

Changes from version 4.1 to 4.2

Version 4.1 incorrectly referred to the Information numbers datafield as 6F1X or 6F18. This has been changed to 6F19.

<div align="center">**COMMON PCN HANDSET SPECIFICATION**</div>

PART A - MARKETING REQUIREMENTS

A.1   INTRODUCTION AND HISTORY

In late 1989, three consortia were selected as providers of a new generation of Personal Communication services in the UK. These consortia formed an association, The Association of European PCN Operators ("The Association"), whose members as of January 1st 1991 were Mercury Personal Communications, Microtel and Unitel.

It was recognised and supported by The Association that the DCS 1800 standards defined by ETSI should form the basis upon which manufacturers should develop their technical specifications for handsets

The DCS1800 specifications provide for a minimum level of functional commonality between handsets and are intended to ensure that all PCN handsets will be compatible with the network services offered by each PCN operator, and that a defined group of basic services will be supported in a consistent manner across each of the members of the association.

In order to extend and promote DCS1800, the association agreed to produce a set of enhanced specifications known as the Common PCN handset Specification (CPHS) to provide significant benefits to manufacturers, end-users of PCN handsets and The Association.

The CPHS specifications were the result of detailed discussions and agreement within The Association. It was the agreed intention of The Association that the PCN handsets that each operator individually purchased were compliant with these requirements

During the initial launch of PCN networks in the UK, The Association sought to promote, encourage and endorse the use of CPHS handsets on their members networks.

It was not the intention of The Association to specify in detail how handsets should be designed or operated, but to address those elements of functionality deemed necessary to meet the defined objectives.

Issues such as handset size, weight, styling, individual choice of MMI, battery lifetime, etc. were left to the discretion of manufacturers seeking to establish differentiated positions in the developing PCN market.

A.2   OBJECTIVES

The objectives in proposing CPHS :

a)   The human interface shall be simple to use, intuitive, unambiguous and easy to learn. It shall be designed to enable the user to select handset features and network services with a minimum of education and selection delay.

        The number of keystrokes to access service and functions shall be minimised. As far as possible, the user shall not be required to memorise complex sequences of operations.

b)   Where possible, commonality of operation across GSM 900/1800/1900 networks should be utilised to simplify equipment design and provide economies of manufacturing scale.

c)   A minimum set of common services ("Core Services") shall be supported by a majority of network operators.

        A customer using a CPHS handset shall be able to access any of the Core Services in a consistent manner irrespective of which network the individual is operating on.

d)   It shall be possible to define subsets of the minimum set of common services on a SIM to personalise a user's subscription.

        The use of this is optional by the ME. If this feature is implemented the technique detailed in CPHS should be used so that the user may retain this personalisation across any similarly featured CPHS handsets that accept compatible sized SIMs.

A.3   Menu Display of Services

The handset may optionally recover from the SIM Customer Service Profile the subset of services available through the user's subscription and display the appropriate menu options accessible through the single command interface.

Additional items may also be included in these menus.

If the handset does not use the Customer Service Profile to display a subset of Core Services it shall display all the Core Services, along with any additional items, in the menus accessible through the Single Command Interface.

Where no Customer Service Profile is present on the SIM, the handset shall display all the Core Services along with any additional items.

A.4   Transportability of Services Information

It shall be possible for the service information specific to a user to be transportable between CPHS handsets.

This shall include:

-       User customised service strings.

-       Information related to a service (e.g. call forward number parameters where specified).

Optionally, on suitably featured CPHS handsets it may include:

-       Customer Service Profile (relevant core services)

A.5   INDICATORS

A.5.1   General

Indicators are required in association with key network services to alert the user on current system status and provide supplementary information.

Indicators shall be activated immediately upon receiving the appropriate activation signals from the network. No user actions should be required to activate an indicator.

Some indicators prompt user actions. These indicators should be activated in a way that enables single command responses from the user.

The indicators are listed below. These are not intended to be exhaustive and manufacturers may wish to offer handset solutions featuring additional indicators where these may prove of benefit to the PCN user.

A.5.2   Network Operator Name

The network operator's name shall be retrieved from the SIM and should be the primary display whenever the phone is turned on, and is not in use for selection of a handset or network service.

A.5.3   Home Country Roaming Indicator

An indicator ("ROAMING") may be provided to tell the user that operation is not on the home network but service is currently being provided on an alternative network. This indicator shall be a function of the handset and normal network operation and shall not rely on any additional network messages for activation.

A.5.4   Voice Message Waiting Indicator

CPHS defined standard formats for SMS messages advise the user that a voice message is awaiting retrieval from the user's voice mailbox. The handset may optionally use this standard format to distinguish between "voice" and "text" messages and provide separate indications according to the message types received.

Additionally the handset shall, as a minimum, provide a message received indication per directory number where ALS is available.

A.5.5   Diverted Call Indicator

An indication may be given to show that 'call forward unconditional' is active. If implemented this indication shall be displayed in idle mode.

A.5.6 Current Line Indicator

An indication shall be given to the user of the currently selected line, or in the case of an MT call, the active line.

A.6   ALTERNATE LINE SERVICE (ALS)

ALS provides the MS with the capability of associating two alternate lines with one IMSI. A user will be able to make and receive calls on either line as desired and will be billed separately for calls on each line. Each line will be associated with a separate directory number (MSISDN) and separate subscription profile. The operation of ALS is described in B.4.3.

Where ALS is available each directory number shall be treated separately from the point of view of basic and supplementary services, so that independent service sets may be assigned for each number. The exception is "Call Waiting", which shall be treated as applying to both directory numbers if either or both numbers carry a subscription to this service. In such cases, the handset shall generate a call waiting indication if a call arrives whilst either line is engaged on another call.

The user should be able to store and recover customised (alpha)numeric descriptions of the two lines. Where there is no user customised description, the handset shall display a default description of "Line 1" and "Line 2" for the two lines.

The handset shall provide an indication of the line on which incoming and outgoing service is being requested by audible and/or visual differentiation.

For outgoing calls, the handset shall enable the user to select the desired line via a single command interface.

A.7   EMERGENCY CALLING

As UK emergency services are accessed by dialling "999" (as well as "112"), UK PCN handsets shall enable both "999 SEND" and "112 SEND" calls to be processed without a valid SIM. If the handset is locked by use of a PIN, entering "999 SEND" or "112 SEND" must activate emergency calling. As a consequence PIN values beginning 112 or 999 shall not be presented by the ME to the SIM.

If the SIM is removed during an emergency call, the call shall continue.

Enhanced MMI for emergency calling over and above this minimum requirement may be provided.

PART B   TECHNICAL REQUIREMENTS

B.1   SCOPE

This part defines the common, minimum, set of technical requirements applicable to CPHS Mobile Stations.

These requirements are necessary:-

a)   To ensure that there is universal technical support for a minimum agreed set of features which will function on all GSM 900/ 1800 & 1900 networks.

b)   To clarify relevant areas of potential ambiguity or omissions in the GSM or DCS1800 specifications.

c)   To indicate clearly those areas of difference between the GSM and DCS1800 specifications in order to help MS manufacturers understand changes.

d)   To indicate additional requirements to GSM and DCS1800 for CPHS.

B.2   SIM Requirements

SIM fields relevant to the operation of DCS1800 are contained in a DCS1800 application directory. This is an alias directory of the GSM application directory to ensure compatibility when SIMs are transferred between 900, 1800 & 1900 MHz equipment. This is described in GSM 11.11.

B.3   OVERVIEW OF ADDITIONAL REQUIREMENTS FOR CPHS

These requirements are additional to the GSM 900 and DCS1800 recommendations. They apply to all products which are to be compliant with the CPHS specification.

B.3.1   Enhanced SIM Requirements

In addition to those SIM storage fields previously defined in DCS1800 to support existing MS features and services, the Association has defined the following fields :-

1)   Call Forwarding flag   (mandatory)
2)   Voice message waiting flag   (mandatory)
3)   PLMN operator name   (mandatory)
4)   Customer Service Profile (CSP)   (optional)
5)   CPHS Information   (mandatory)
6)   Mailbox Numbers   (optional)
7)   Information Numbers   (optional)

Full details of the operation of these features is contained in section B.4, "Detailed technical specifications of CPHS features". The directory structure of a CPHS SIM is shown in figure A.1.

The series of identifiers 6F 1X is reserved within GSM for "administrative use".

```
                        ┌─────────────────┐
                        │  Root Directory │
                        │                 │
                        │     3F 00       │
                        └─────────────────┘
              ┌──────────────────┼──────────────────┐
       ┌──────────┐    ┌─────────────────┐    ┌──────────┐
       │          │    │  GSM Directory  │    │          │
       │          │    │                 │    │          │
       │          │    │    7F 20/21     │    │          │
       └──────────┘    └─────────────────┘    └──────────┘
```
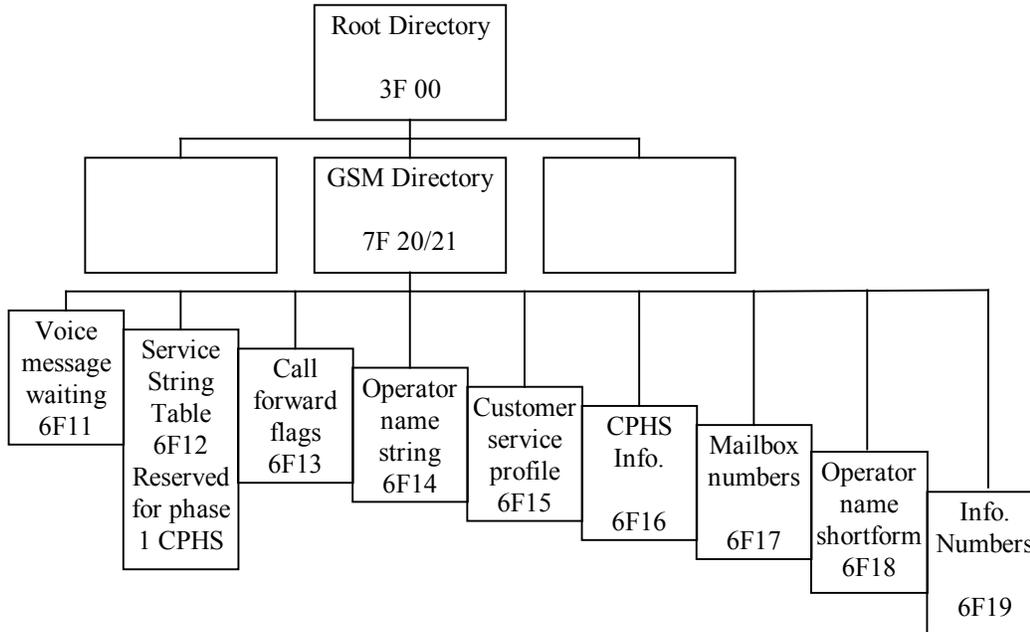
Figure 1 - CPHS specific datafields (see also GSM 11.11)

Voice message waiting 6F11 — Service String Table 6F12 Reserved for phase 1 CPHS — Call forward flags 6F13 — Operator name string 6F14 — Customer service profile 6F15 — CPHS Info. 6F16 — Mailbox numbers 6F17 — Operator name shortform 6F18 — Info. Numbers 6F19

B.3.1.1 CPHS Information

The CPHS Information data-field is needed to contain the CPHS phase of the SIM and to indicate which optional data-fields are present in the SIM.

DATA FIELD - 6F 16: CPHS INFORMATION

Purpose :

This data-field contains the CPHS phase of the SIM as well as the CPHS Service Table indicating which of the CPHS optional data-fields are present in the SIM card. The ME should read this data-field as part of the SIM initialisation procedure (see GSM 11.11) and it should only subsequently attempt to read or update an optional data-field if the data-field is indicated as being both allocated and activated in the CPHS Service Table.

Identifier: '6F16		Structure: transparent		Optional
File size: n bytes			Update activity: low	

Access Conditions:	
READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	CPHS Phase	M	1
2-3	CPHS Service Table	M	2
4-n	RFU	O	n-3

Structure of the data field:

Byte 1: CPHS phase, coded as:

01   phase 1
02   phase 2
        etc.

Byte 2: CPHS Service Table

b8	b7	b6	b5	b4	b3	b2	b1
OpName Shortform *(Phase 2 only)*		Mailbox Numbers *(All phases)*		SST *(Phase 1 only)*		CSP *(All phases)*	
Activated	Allocated	Activated	Allocated	Activated	Allocated	Activated	Allocated

Byte 3: CPHS Service Table continued

b8	b7	b6	b5	b4	b3	b2	b1
RFU		RFU		RFU		Information numbers *(Phase 2 only*	
0	0	0	0	0	0	Activated	Allocated

Service Allocated is indicated by as '1' in the lower bit of each service pair
Service Activated is indicated by as '1' in the upper bit of each service pair

Service Not Allocated is indicated by as '1' in the lower bit of each service pair
If the service is not allocated then the state of the activated bit has no meaning

Future optional services may be defined and shall be coded onto subsequent bytes

B.3.2 Indicators

To support the Core Services (defined in A.3.2), the following display indicators (and the associated SIM datafields) are needed.

- Network Operator Name   (mandatory)
- Home Country Roaming   (optional)
- Voice Message Waiting   (mandatory)
- Diverted Calls   (optional)

B.4   DETAILED TECHNICAL SPECIFICATIONS OF CPHS SPECIFIC FEATURES.

This section defines details of the technical requirements (additional to the DCS1800 recommendations) which also apply to the CPHS products.

B.4.1　Service Accessibility

B.4.1.1 Display in Idle Mode

When the MS is in idle mode and registered with a PLMN (i.e. a location update has been accepted), the MS shall display the following:

Selection Method	Home PLMN	Roaming within Home Country	Roaming outside Home Country
Automatic	Name	HCR	MCC/MNC
Manual	Name	MCC/MNC	MCC/MNC

Where　　　　Name = Network operator name string as in section B.4.1.3
　　　　　　HCR　= A Home Country Roaming Indicator ("ROAMING")
　　　　　　　　　　may be displayed.
　　　　　　MCC　= Mobile Country Code
　　　　　　MNC　= Mobile Network Code

Notes:-

1　　It is allowable to temporarily remove the operator name to display other ME or system messages to the user.

2　　The decision on whether roaming is within or outside the home country is made on the basis of the MCC of the selected PLMN.

3　　Where MCC/MNC is shown in the table this is the minimum display acceptable. Additional procedures may be supported by a manufacturer whereby country and operator names can be displayed. It is preferable to use the latest version of the MoU list of operator names (SE.13) to display the applicable roaming operator.

B.4.1.2 Network Operator Name

Under some circumstances it is desired to show the PLMN operator's name on the MS display.

The name of the operator will be contained on the SIM issued to a subscriber in one or both of the CPHS datafields below.

The field structures to be used for the storage of these name strings are as follows:-

The ME may choose which name to use, dependent upon its display size and how well it can format the name.

DATA FIELD - 6F 14: OPERATOR NAME STRING

Purpose :

This data field contains the name of the PLMN operator who issued the SIM. This is read by the ME for display in idle mode.

Identifier: '6F14'	Structure: transparent		Optional
Record length: n bytes		Update activity: low	

Access Conditions:
  READ   CHV1
  UPDATE   ADM
  INVALIDATE   ADM
  REHABILITATE ADM			

Bytes	Description	M/O	Length
1 to n	PLMN name	M	n bytes

Coding:
The PLMN name shall be coded in default 7 bit alphabet (see GSM 03.40) with b8 set to 0. Unused bytes shall be set to 'FF'

DATA FIELD - 6F 18: OPERATOR NAME SHORTFORM

Purpose :

This data field contains a shortform of the name of the PLMN operator who issued the SIM. This is read by the ME for display in idle mode and is used instead of the Operator Name String by the ME if its display cannot accommodate the complete Operator Name String.

Identifier: '6F18'	Structure: transparent		Optional
Record length: 10 bytes		Update activity: low	

Access Conditions:
  READ   CHV1
  UPDATE   ADM
  INVALIDATE   ADM
  REHABILITATE ADM			

Bytes	Description	M/O	Length
1 to 10	Operator Name Shortform	M	10 bytes

Coding:
The Operator Name Shortform shall be coded in default 7 bit alphabet (see GSM 03.40) with b8 set to 0. Unused bytes shall be set to 'FF'

B.4.2 Voice Message Waiting

B.4.2.1 Voice Message Waiting Indicator

The GSM short message present indicator may be enhanced in order to distinguish between voice messages and normal text short messages. An agreed voice message format will be used by the network operators.

A handset manufacturer may use this format in order to provide a separate Voice Message Indicator.

The basic principle is that the short message originating entity address (associated with the Voice Messaging Centre), which is not used by the network, is used to select the handset indicator and control its condition (on or off).

The user data transported in a voice message waiting message shall consist of either:

(i)   a single space (character coded as 0100000 b7..b1 in the default alphabet in GSM 03.40), or;

(ii)   free-format text (coded in the default alphabet specified in GSM 03.40).

Where the user data consists only of a single space, the short message shall not be stored on the SIM but shall be used to select and control the indicator. If more user data is present the short message shall be used to select and control the indicator and shall be stored on the SIM as normal.

The indicator messages and the actions to be made on them shall be identified from the originating SME address. For Short Message, mobile terminated, the originating SME address is contained in the TS-Originating-Address parameter of the TS-Deliver primitive, and is transferred in the TP-Originating-Address element of the SMS-Deliver TPDU.

Beyond the specification of the originating SME address to be used for indicator short messages, the procedures for handling such messages in the MS, and for supporting such indicators from the network, are not specified.

The originating SME address field shall be coded as follows:

Octet 1   Address-Length (coded in binary)
                        constant value   00000100 (note 1)

Octet 2   Type-of-Address
               bit 8   always set to 1   1
               bits 7..5   type of number: 101 (alphanumeric)
               bits 4..1   numbering plan id: 0000

Octets 3-4   Address Value (note 2)

        Character 1
               bit 1   set/clear indicator
               0   clear
               1   set

bits 4..2   **type of indicator**
000   voice message waiting indicator
bits 7..5
001   constant value

____Character 2____
bit 1   **indicator identifier**
0   indicator 1
1   indicator 2
bits 7..2
000000   constant value

Notes:

(1)   Octet 1 has the value 4 (decimal) indicating that 4 semi-octets are used for the address-value part of the address field.

(2)   The alphanumeric character definitions and the packing of characters into octets in the Address field are as defined in GSM Rec. 03.40 Annex 2. Characters 1 and 2 are 7 bits in length.

(3)   Using this scheme the handset cannot differentiate between voice messaging centres.

(4)   This scheme gives independent control of indicators 1 and 2. For CPHS handsets indicator 1 is associated with line 1 and indicator 2 is associated with line 2.

(5)   The CPHS method of coding a voice message may be used in conjunction with the two GSM phase 2+ standardised methods using TP-DCS or TP-UD. These methods are described in GSM 03.38 and 03.40 V5+.

B.4.2.2 Voice Message Retrieval and Indicator Clearing

A voice message shall be retrieved using the procedure appropriate for that voice message centre. The dialling number of the voice mailbox can be found by the ME in the Mailbox Numbers data-field. The structure of this data-field is similar to the Abbreviated Dialling data-field so that different numbers can be stored against different bearer capabilities:

Data field 6F 17: Mailbox Numbers

Purpose: To store dialling numbers to be used for message retrieval from mailboxes. The Capability/Configuration Identification byte indicates the bearer capability required to access that mailbox. The alpha-tags serve no essential purpose but may be used by the MMI to indicate mailbox types (i.e. voice, fax, etc.).

Identifier: '6F17'		Structure: linear fixed		Optional
Record length: X+14 bytes			Update activity: low	

Access Conditions:
    READ   CHV1
    UPDATE   CHV1
    INVALIDATE   ADM
    REHABILITATE ADM				

Bytes	Description		M/O	Length
1 to X	Alpha Identifier		O	X bytes
X+1	Length of BCD number contents		M	1 byte
X+2	TON and NPI		M	1 byte
X+3 to X+12	Mailbox Number String		M	10 bytes
X+13	Capability/Configuration Identifier		M	1 byte
X+14	Extension1 Record Identifier		M	1 byte

For contents and coding of all data items see the respective data items of EF_{ADN} in GSM 11.11.

NOTE 1:   The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN} in GSM 11.11.

NOTE 2:   Optionally, if the ME does not support capabilities configuration identifiers, then the following convention shall be used:

                        Record 1   Line 1 mailbox
                        Record 2   Line 2 mailbox
                        Record 3   Data mailbox
                        Record 4   Fax mailbox

Message waiting indicator clearing can be achieved using the defined short message format or the handset may offer a means of clearing the indicator manually.

B.4.2.3 Voice Message Waiting Indicator Flags in the SIM

CPHS has defined flags in the SIM to store the state of these indicators.

The contents of these flags should be read on power up and used to set the indicators to the correct state.

The following is the definition (in the manner of GSM 11.11) of this field:-

The ME shall update the SIM flags immediately it detects a change in their status. This is to ensure that information is not lost, should power be cut to the ME.

DATA FIELD -6F 11: Voice message waiting flag

Purpose :

Storing the status of indicators that define whether a voice message is waiting. This status is used to set the message waiting indicator after re-activation of the handset. The use of this data field is optional at the discretion of the manufacturer.

Identifier: '6F11'		Structure: transparent		Optional
Record length: n bytes		Update activity: low		

Access Conditions:
    READ   CHV1
    UPDATE   CHV1
    INVALIDATE   ADM
    REHABILITATE ADM				

Bytes	Description		M/O	Length
1	Voice Message Waiting Indicator flags		M	1
2	Fax / Data Message Waiting Indicator flags		O	1
3-n	RFU		O	n-2

Structure of the Message Waiting flags

If a message is waiting, the nibble should contain A (HEX).
If no message is waiting the nibble should contain 5 (HEX)

Byte 1 Nibble 1 is used to store the status of the 'Line 1' message and nibble 2 that of 'Line 2'.
Byte 2 Nibble 1 is used to store the status of the 'Fax' message and nibble 2 that of 'data' status.

B.4.3   Alternate Line Service

The principle of network operation is to associate a series of MSISDNs against a single IMSI. An additional requirement to the GSM recommendations is the definition of an additional Teleservice and Bearer capability - See Appendix 2.

Within GSM each MSISDN can be associated with a different bearer capability to facilitate service interworking with a PSTN. For the purposes of providing dual speech services CPHS defines a second teleservice called 'Auxiliary Speech'.

The ISDN number used to route an incoming call determines whether the call is associated with the speech or auxiliary speech bearer capability. The translation from MSISDN to speech/auxiliary speech is done at the terminating MSC and is conveyed to the MS during call set up by means of the bearer capability information element. This shall be used by the handset to provide an indication of which line is being called, either by different ring tones and/or a clear display message such as "Line 2".

For outgoing calls the MS manufacturer must provide a means of selecting Line 1 or Line 2. The MS then selects the appropriate teleservice, either 'Telephony' or 'Auxiliary Telephony', and the appropriate bearer capability (speech or auxiliary speech respectively), dependent on whether Line 1 or Line 2 is selected.

The network will associate both of these teleservices with speech and associate the appropriate MSISDN with the call. It will itemise them separately on the billing records, allowing post processing into two separate bills.

Handset procedures which select the Line number implicitly select the corresponding Supplementary Service (SS) operations mode so that apply to the selected line. This allows, for example, barring and diverting of calls to be performed differently for each MSISDN number.

Where a SS operation is performed and no teleservice supplementary information byte is explicitly entered, then the MS will insert the correct teleservice (either Telephony or Auxiliary Telephony) depending on the line number currently selected.

Whenever a customer's MSISDN is displayed, the MSISDN of the active line shall be used.

Only one incoming call at a time is set up to the MS. Initiating the answer sequence (by pressing the 'send' key or its equivalent) will automatically answer the incoming call irrespective of which line has been selected.

For Mobile terminated calls, if Calling Number Identification is activated, the Calling Number Identification information must be displayed with the active line number during call ringing.

B.4.4   MSISDN/ Line Identification in SIM

The MSISDN/Line Identification feature shall be provided through the use of the MSISDN data-field.

When appropriate the ME displays the MSISDN of the active line. The MSISDN for a given line is distinguished using the Capabilities/Configuration byte included in the record. The alpha-tag in the record will contain a description of the line and its use by the ME is optional.

Optionally, if the ME does not support capabilities configuration identifiers, then the following convention shall be used:

Record 1	Line 1 MSISDN
Record 2	Line 2 MSISDN
Record 3	Data MSISDN
Record 4	Fax MSISDN

It is left to the manufacturer to provide a means for the user to personalise/interrogate this field.

B.4.5   Diverted Call Status Indicator

Whilst it is recognised that the status of the service in the network can only accurately be obtained by interrogation of the call forwarding Supplementary Service, an indication can be provided on the handset based on the last operation performed on that supplementary service.

An MS supporting this feature shall therefore set the Call Forward Unconditional indicator when the network confirms user execution of the "set call forward unconditional". It should be cleared when the network confirms execution of the "clear call forward unconditional" or "clear all call forward options".

To support ALS it is necessary to store the current state of the call forward unconditional options for both line 1 and line 2. Whether both indications are displayed simultaneously, or only the one corresponding to the currently selected handset mode (either line 1 or line 2) is a manufacturers option.

In order to retain the status of the indicators during periods when the equipment is turned off, (and/or the battery removed) CPHS has assigned flags for this purpose in the SIM.

For an MS supporting this feature the indicators must be set to match the stored status on powering up the MS, or when a network interrogation returns status information of this service.

The ME shall update the SIM flags immediately it detects a change in their status. This is to ensure that information is not lost, should power be cut to the ME.

The following wording (in the manner of 11.11) defines these fields:-

DATA FIELD -6F 13: Call forwarding flags

<u>**Purpose :**</u>

Storing the status of a MS flag that records whether or not call forward unconditional is active. The status may be used to set the forwarding indicators after re-activation of the handset.

Identifier: '6F13'	Structure: transparent		Optional
Record length: n bytes	Update activity: low		
Access Conditions: 　　READ　　　　　　　　CHV1 　　UPDATE　　　　　　　CHV1 　　INVALIDATE　　　　　ADM 　　REHABILITATE　　　ADM			

Bytes	Description	M/O	Length
1	Voice Call forward unconditional flags	M	1
2	Data/fax call forward unconditional flags	O	1
3-n	RFU	O	n-2

<u>Structure of the data field:</u>

If call forwarding unconditional is active the nibble should contain A (HEX).
If no call forwarding message is waiting the nibble should contain 5 (HEX)

Byte 1 Nibble 1 is used to indicate the "call forward unconditional" status for 'line 1' and nibble 2 for 'line 2'.
Byte 2 Nibble 1 is used to indicate the "call forward unconditional" status for 'fax' (MMI service code 13 from GSM 02.30) and nibble 2 that of 'data'. (comment which data??)

B.4.6   Information Numbers

The Information Numbers data-field is optional in the SIM. The Information Numbers information shall only be presented to the user when the CPHS-defined Customer Service Profile (CSP) data-field contains a Service Group Code (byte A) of D5 hex, with an associated byte B of FF hex.

The ME shall support user access to the "Information Number" data field stored on the SIM.

The MMI shall allow structured hierarchical access to entries within the field. An indication shall be made to the user that marked entries will be charged as premium rate services.

B 4.6.1 Technical Specification

This data-field is written to the card during preparation and contains a directory of useful numbers for information services with user friendly multilevel indexing for number selection. Each record is either an alphatagged number entry or an index name with a group of number entries associated with it.

The indexing is multilevel as illustrated below:

```
Index
level
                        TRAVEL              WEATHER         ENTERTAINMENT


Index
level                                                
-            TAXIS                  AIRPORTS   North   South    Ticketmaster
                                               323     597          562

Index
level      Computercabs  Dial-a-cab   Heathrow      Gatwick
-             111           132          345           651
```
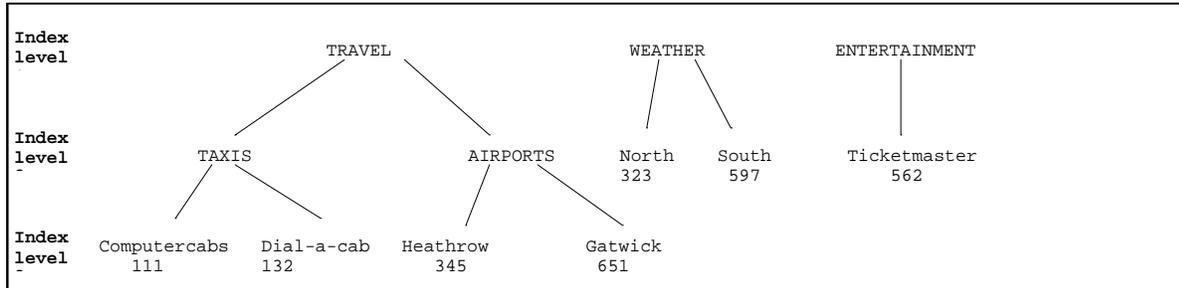
Figure 2   Multilevel Index Structure for Information Numbers

This is coded into the data-field by placing an index level identifier into each record, as shown schematically in the table below.

Index Level	Example Alpha-tag	Example Numbers
1	TRAVEL	null
2	TAXIS	null
3	Computercabs	111
3	Dial-a-cab	132
2	AIRPORTS	null
3	Heathrow	345
3	Gatwick	651
1	WEATHER	null
2	North	323
2	South	597
1	ENTERTAINMENT	null
2	Ticketmaster	562

Simplified Representation of Information Numbers Data-field

Index Name entries are distinguished from Number Entries by having null number values (i.e. length byte and Type of Number bytes set to FF). To speed searching through the table for options to display to the user, the number section of an Index Name entry may optionally contain a pointer to the next entry of the same index level. This feature will not be programmed into the SIM's at launch although it may be provided in later issues of SIM's.

In order to retain future flexibility and yet minimize memory space used in the SIM in the short term, neither the alpha-tag nor the number section of the records are given a fixed length. It is anticipated that three-digit numbers shall be put into the data-field and a number translation will occur within the network.

There shall be both a Premium Service Indicator and a Network Specific Indicator flag contained in each entry. The Premium Service Indicator shows whether the call will be charged at a premium

rate and this should be indicated to the customer prior to selection. The Network Specific Indicator marks a network specific entry that should not be presented to the user when the MS roams onto other networks.

Information Numbers only apply to speech call and have no line significance for the Alternate Line Service (ALS). Entries shall be selectable independently of whether the ME is in line 1 or line 2 mode. The bearer capability for the call requested from the network shall be taken from the current mode of the handset.

The Update Security policy for the data-field is set to "CHV1" to enable remote SIM personalization of the data-field in later phases of the network. This would be achieved by inserting entries into completely null records left in the middle of data-fields.   The ME shall not provide mechanisms for altering the alphatags and associated telephone numbers.

B.4.6.2 DATA FIELD -6F 19: Information Numbers

If the ME cannot find Identifier '6F19', it shall attempt to read identifier 'EA01' which may contain Information Numbers in older SIM cards.

Identifier: '6F19'		Structure: linear fixed		Optional
Record length: 5+Y+Z bytes		Update activity: low		

Access Conditions:
     READ   CHV1
     UPDATE   CHV1
     INVALIDATE   ADM
     REHABILITATE ADM				

Bytes	Description	M/O	Length
1	Alpha length	M	1 byte
2	Entry Status (defined below)	M	1 byte
3 to Y+2	Alpha Identifier	O	Y bytes
Y+3	Length of called party BCD number (04.08)	M	1 byte
Y+4	TON and NPI	M	1 byte
Y+5 to Y+Z+4	Digits section	M	Z bytes
Y+Z+5	Extension1 Record Identifier	M	1 byte

For the filled records, the above bytes shall be coded in the following way.

Alpha length	Number of bytes in the alpha-tag section of the record. This byte has the same value for each filled entry of the data-field.							
Entry Status	b8	b7	b6	b5	b4	b3	b2	b1
	1	1	Network Specific Indicator	Premium Service Indicator	Index Level Identifier			
	Bits 1 to 4 represent the Index Level Identifier for the entry. All level 1 entries are initially displayed by the ME to the user upon selection of Information Numbers featured by the user. Entries with a higher index level are only displayed to the user when the preceding entry with a lower index level has been selected. The coding is as follows:							

	bit 4 bit 1 0 0 0 1 Index level 1 0 0 1 0 Index level 2 0 0 1 1 Index level 3 etc. The Premium Service indicator is set to "1" when the entry, or whole group of entries associated with the index name, are charged at a premium rate. The ME should provide an indication of a Premium Service entry prior to number selection. The Network Specific Indicator is set to "1" for entries whose associated numbers are specific to the HPLMN and therefore should not be selectable when the handset is roaming on a VPLMN. It is applicable to index names and number entries.
Alpha-tag	The alpha-tag is coded in the short message alphabet given in GSM 03.40, with bit 8 set to zero. The number of bytes in this section (Y) is given by the Alpha length.
Length of called party BCD number contents	For Number Entries, this byte is equal to the number of significant bytes in the digits section (i.e., non-FF) plus the type of number byte. For Index Names, this byte is set to FF.
Type of Number, etc.	This byte is as specified in octet 3 of the called party BCD number information element of GSM 04.08 This byte is only used for number entries and not index names. It is set to FF for all index name entries.
Digits section	The number of bytes in this section can be deduced from the record length (given in Get Response after selection of the data-field) and the value of Y as follows: Z = Record Length - Y - 5 For Number Entries, the digits of the number are coded as BCD with digit 1 in bits 1 to 4 of byte g, digit 2 in bits 5 to 8 of byte g, digit 3 coded in bits 1 to 4 of byte g+1, etc. Unused nibbles at the end of the section shall have all their bits set to all 1. If the record contains an index name, the first byte may contain either the absolute record number of the next entry in the absolute record number of the next entry in the Information Numbers data-field which has the same index level, or a value of FF. All of the other bytes in this section are set to FF.
Extension1 Record Identifier	This is coded in binary and gives the associated record number in datafield 6F 3E. For records containing Index names, this byte is set for FF. Null records can be located between filled records, and are coded with all bytes in the new record set to FF. The ME shall ignore such null records and look at the following record for the next significant entry.

B.4.7 Customer Service Profile

The Customer Service Profile (CSP) is a list on the SIM which indicates the services which are customer accessible using the single command interface. Each of these services has a related bit within the CSP. Each of these CSP bits allows the ME to present only the menu item(s) relevant to that service to the user.

The use of the CSP to control the MMI is in addition to the MMI procedures defined in GSM 02.30. The ME should not use the CSP to prevent access to services by these procedures.

B.4.7.1 Bit Significance of Customer Service Profile entries

An entry in the Customer Service Profile consists of two bytes. The first byte is a Service Group Code which is used to associate related services together within the CSP.

Each bit of the second byte has specific significance. A bit set to '1' indicates that the service is customer accessible via the single command interface, a bit set to '0' indicates that it is not.

Unused bits are set to '0'

The following table shows the bit significance for each Service Group code:-

Byte A
<hex>

Byte B
<--binary-------------------------------------->

Service Group Code	Service	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
01	Call offering	CFU	CFB	CFNRy	CFNRc	CT			
02	Call Restriction	BOAC	BOIC	BOIC exHC	BAIC	BIC Roam			
03	Other Supp Services	MPTY	CUG	AoC	Pref. CUG	CUG OA			
04	Call Completion	HOLD	CW	CCBS	User User Signalling				
05	Teleservices	SM/MT	SM/MO	SM/CB	Reply path	Del. Conf	Protocol ID	Validity Period	
06	CPHS Teleservices	ALS							
07	CPHS Features	Reserved (SST in phase 1 CPHS)							
08	Number Identif.	CLIP	Reserved	CoLR	CoLP	MCI		CLI send	CLI block
09	Phase 2+ services	GPRS	HSCSD	Voice Group call	Voice Broadcast Service	Multiple Subscriber Profile	Multiple Band		
C0	ValueAdded Services	PLMN MODE	VPS	SM/MO PAGING	SM/MO EMAIL	Fax	Data	Reserved	Language
D5	Information Numbers	Information Numbers							

The service abbreviations used above are:

CFU   Call Forwarding Unconditional   SM/MO   Short Message - Mobile Originated

CFB	Call Forwarding On User Busy	SM/CB	Short Message - Cell Broadcast
CFNRy	Call Forwarding on No Reply	Reply path	Restricts menu options for the ability to set reply path active on outgoing Short Messages
CFNRc	Call Forwarding On User Not Reachable	Del. Conf	SMS Delivery Confirmation
CT	Call Transfer	ALS	Alternate Line Service
BOAC	Barring of All Outgoing Calls	CLIP	Calling Line Identification Presentation
BOIC	Barring of Outgoing International Calls	CLIR	Calling Line Identification Restriction
BOIC-exHC	Barring of Outgoing International Calls except those directed to the Home PLMN country	CoLP	Connected Line Identification Presentation
BAIC	Barring of All Incoming Calls when Roaming Outside the Home PLMN country	CoLR	Connected Line Identification Restriction
MPTY	Multi-Party Service	MCI	Malicious Call Indicator
CUG	Closed User Group	CLI block	CLI per call mode - default send CLI - menu to block CLI
AoC	Advice Of Charge	CLI send	CLI per call mode - default block CLI - menu to send CLI
Pref. CUG	Preferential CUG	PLMN mode	Restriction of menu options for manual PLMN selection
CUG OA	CUG Outgoing Access	VPS	Restriction of menu options for Voice Mail or other similar menus
HOLD	Call Hold	SM/MO paging	Restriction of menu options for the ability to send Short messages with type Paging
CW	Call Waiting	SM/MO Email	Restriction of menu options for the ability to send Short messages with type Email
CCBS	Completion of Call to Busy Subscriber	Fax	Restriction of menu options for Fax calls
SM/MT	Short Message - Mobile Terminated	Data	Restriction of menu options for Data calls
Information Numbers	The ME shall only present Information numbers to the user if this field is set to FF.	Protocol ID	Restriction of menus for SMS Protocol ID options
Validity Period	Restriction of menus for SMS Validity period options	GPRS	Menus concerned with GPRS functionality
User User Signalling	Restriction of menus allowing use of user to user signalling	Multiple Band	Restriction of menus allowing user to select a particular GSM 900/ 1800 or 1900 band
Multiple Subscriber Profile	Phase 2+ multiple subscriber profile menus	Voice Broadcast Service	ASCI Voice broadcast service menus

Voice Group call	ASCI Voice Group call menus	Language	Restriction of menus allowing the user to change language.
HSCSD	Menus concerned with High Speed Circuit Switched Data functionality		

Bits 5,6 & 7 of service group 01 specify the conditional call forwarding menus. If they are all set to '1', only one "conditional" call forwarding menu shall be provided which will set all three individual conditional services. If any are set to zero, then the respective individual menus shall be provided.

Service Group codes in the range 08 hex ... BF hex inclusive are reserved for future use.

Service Group codes in the range C1 hex ... FF hex inclusive are for operator specific use. The service groups and services for these codes can be defined by individual network operators.

 If a ME encounters a Service Group code it does not recognise it should ignore it.

If a defined service group is absent from the table in the CSP then none of the services of that service group shall be offered in the menu.

The handset may provide other services which are outside the scope of the CSP defined above.

Each entry in the Customer Service Profile consists of two bytes; byte A carries the Service Group code, whilst byte B defines the provisioned services.

An example of an entry in the CSP is {01 C0 (HEX)}

This indicates that some 'Call Offering' services are to be presented to the customer, but only the menu names relating to CFU (Call Forwarding Unconditional) and CFB (Call Forward on User Busy).

Entries are packed consecutively into a list. Within the CSP datafield it shall be allowable for service groups to be listed in any order.

The SIM field defined for this purpose is detailed as follows :-

DATA FIELD- 6F 15: Customer Service Profile

Purpose :

Storing a list of service options which are relevant to that specific customer.

Identifier: '6F15'		Structure: transparent		Optional
Record length: X bytes		Update activity: low		

Access Conditions:
    READ   CHV1
    UPDATE   CHV1
    INVALIDATE   ADM
    REHABILITATE ADM				

Bytes	Description		M/O	Length
1 to 18	CPHS defined Customer Service Profile		M	18
19-X	RFU		O	X-18

Byte								
1	2	3	4	..	..	..	X-1	X
A1	B1	A2	B2	..	..	..	A(X/2)	B(X/2)

Each CSP entry consists of two bytes :-

    Byte A - The service group code defined in CPHS B.4.7.1
    Byte B - The services byte defined in CPHS B.4.7.1

B.4.8   Network and Service Provider Lock

B.4.8.1 Introduction

This section specifies the functional requirements for the handset in-regard to the implementation of a lock to ensure that handsets can be locked onto a specific network, or Service Provider as desired. This specification is aligned to the ETSI 02.22 recommendations on 'Personalisation of GSM Mobile Equipment (ME) Mobile functionality specification'.

B.4.8.2 Acronyms and Abbreviations

    * ALOCK   Autolock Criterion
    * LES   Lock Enable Status
    * GID1   Group Identifier field 1
    * SIMUC   SIM Unlocking code
    * SP   Service Provider
    * MSPID   Service Provider Identification field held in ME
    * SPL   Subsidy Protection Lock
    * To   Time-out interval counter
    * UAC   Unlock Attempt Counter

B.4.8.3 Fundamental requirements for the Service Provider Lock Mechanism

1.   It shall be possible to lock a handset to the HPLMN only.
2.   It shall be possible to lock a handset to a specific service provider.
3.   It shall be possible for a user to unlock the handset such that it will work on any network or any service provider at any time if in possession of the correct unlocking code.
4.   The locking mechanism shall be securely implemented in the ME such that attempts to guess the unlocking codes will be restricted through the implementation of a time-out period between accepting unlock attempts.
5.   Each time the wrong unlock code is entered the length of the time-out interval will increase.
6.   The internally stored data connected with the operation of the lock shall be held securely in non volatile memory. Within the phone this shall be done in such a manner that it is not economically possible to change codes and all reasonable precautions shall be taken to ensure that simple alterations to the EEPROM do not defeat the lock operation. As a minimum the same security precautions shall be taken as needed to satisfy the MoU rules on IMEI security. (e.g. Encryption, multiple bit settings, codes derived from IMEI, integrity checks, physical device encapsulation or other techniques.)
7.   The ME shall examine the lock Enable status at each power on or change of SIM card and if the lock is active follow the given algorithms before allowing service to be given.
8.   Whilst the lock is not active the ME shall automatically test for a card matching Automatic Lock criteria and if matched shall copy the contents of the GID1 field into the handset permanent EEPROM memory (MSPID) and activate the lock.
9.   The ME shall allow normal operation irrespective of lock status for Type Approval SIMs (MCC 001, MNC 01).
10. The ME shall prompt the user to enter their Special Code if the lock is active and an MCC and MNC of the IMSI inserted is other than 001-01 or the HPLMN.
11. For an HPLMN SIM, the ME shall check the status of the lock. If active the GID1 field shall be compared to the MSPID (i.e. the version copied to the ME non volatile memory at the point of autolocking). For SIM GID1 of FF or for matching SPID and MSPID normal service

shall be allowed. For non matching GID1 and MSPID the ME shall prompt the user to enter the unlocking code and only allow emergency calls can be made.

12.   If the correct unlocking code is entered by the user then the ME shall be permanently unlocked and shall allow operation with any network SIM irrespective of the GID1 values.

13.   The Special Code shall be either :-

i)   Randomly assigned to the ME at the time of manufacture and notified to the HPLMN operator on computer files accompanying the shipment giving IMEI information etc.

ii)   Algorithmically derived at the time of manufacture from the IMEI assigned to that ME using an algorithm to be proposed by the Supplier and agreed by the HPLMN operator.

iii)   Algorithmically derived at turn on by the ME from the IMEI assigned to that ME at the time of manufacture using an algorithm to be proposed by the Supplier and agreed by HPLMN operator.

14.   The Autolock operation shall only operate once in the life of the ME.

B.4.8.4 Operation of the SP Lock

The operation of the SP Lock is shown in detail on the flowchart attached. The stages of operation are described below.

B.4.8.4.1   MCC/MNC Lock.

When a handset is produced, it shall have a bit (or bits) in EEPROM to tell its operating system that the MCC/MNC lock is enabled (SPL = active). This bit shall always be active at manufacture. The MCC/MNC data shall be set to the HPLMN operators values at time of manufacture. In this way the handset is already locked to HPLMN SIMs after the completion of the manufacture process.

B.4.8.4.2   SP Lock

The SIM will be provisioned with a Service Provider ID contained within the GID1 field. The SIM will be paired with the handset (At the distribution warehouse for instance), and to avoid there being problems with acceptance testing of ME's performed using test SIMs, the ME shall read the SP lock data from GID1 and store this into the protected MSPID EEPROM field only if specific Autolock criteria are met. Details of the Autolock criteria are given below.

Normal customer SIMs will be such that they fulfill the Autolock criteria and cause the GID1 values to be read, encrypted and stored into an area of ME internal non-volatile memory (MSPID) when the ME is first turned on with the customer card inserted. After first operation of Autolock the Lock Enable Status bit (LES) is set indicating that the 'one shot' locking has been carried out.

From this point on, only HPLMN SIMs that contain this SP code shall be allowed to work with this handset until such time as the ME is unlocked. (Except type approval 001-01 test SIMs)

B.4.8.5 Unlocking The Subsidy Protection Lock

The ME shall be populated with at least an 8 digit SP unlocking code that is either calculated from the IMEI (and optionally the GID1 field contents), or is randomly populated.

If the MCC/MNC lock is on (SPL = active) and a SIM of another network is inserted, then the ME shall deny service and request the entry of the SP unlocking code. The ME checks the value of the code entered. If it is correct, then the MCC/MNC lock status bit(s) forming SPL shall be cleared.

If the code is incorrect, then the periodic timeout interval which must be waited before subsequent unlock attempts are accepted shall be increased.

The initial timout period is 30 seconds. This shall double at each incorrect attempt until a maximum value of 2048 * 30 seconds (approximately 17 hours).

NOTE It is preferable that the unlocking of the SP and MNC/MCC are simultaneous and upon entry of the same unlocking code.

B.4.8.6 Requirements of the SIM

The GID1 field details can be found in GSM 11.11 version 4.14 or later.
The field in directory 7F 20 / 21 and has identifier 6F 3E

B.4.8.7 Autolock Criteria

The Autolock operation shall take place only when the SIM inserted meets all the following criteria:-

i)   The IMSI has an MNC and MCC corresponding to the HPLMN Operator.
ii)   The access class is anything other than 15
iii) There is a GID1 on the SIM which is allocated and activated and whose value lies in the range 00 to FE inclusive
iv)   The operator name string stored on the SIM is not equal to 'GOODS-IN'

B.4.8.8 Security handling details

The SP Lock is necessary to protect the handset subsidy value on each ME sold.
The details of the implementation are therefore considered to be high security risk pieces of information for which special handling measures shall be taken as follows:-

i)   Within the Supplier's premises the number of people with knowledge of the implementation and data storage details shall be kept to an absolute minimum.
ii)   The algorithms and other information used to generate the lock codes applicable to individual ME's shall be held securely and only executable versions shall be available to production staff. Access to the source routines shall be by controlled access by authorised staff only.
      Any executable version should not be able to be copied and run on separate PC equipment. Acceptable measures to prevent this include the use of hardware keys to limit the operation of the code to individual machines.
iii) No plain storage of codes and flags shall be available in the ME. These should be held in encrypted form preferably with integrity check bits built in, or with cross checking between data stored in different physical devices. In the event of detecting a mismatch in data or check bits indicating that a fraudulent attempt has been made to alter the data, the ME shall immediately enter the disabled state.
iv)   The Supplier shall take all reasonable measures to ensure that no pieces of equipment are supplied to third parties, including approved third party test and repair centres, which allow security codes to be read or altered.
v)   The Supplier shall ensure that there are no versions of code supplied to any world market which would be able to be loaded on the same hardware platform and which do not take account of the SPL flags.

In this way it shall not be possible to re-boot the HPLMN operators phones with other available versions of code and defeat the security of the SP lock.
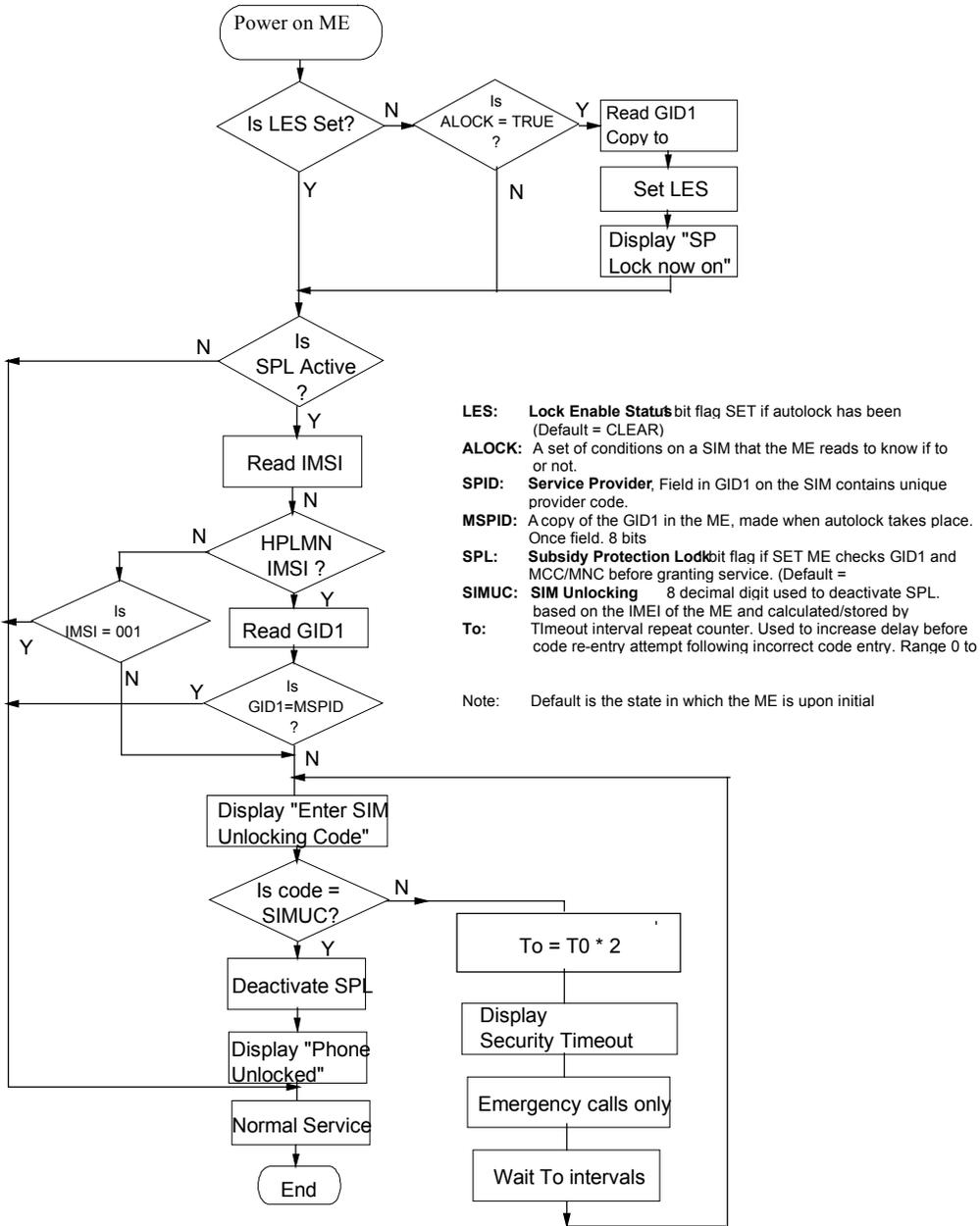

Figure 3 - Flow chart of Network and SP Lock functionality

B.4.9 Language Reset

It is often the case that handsets can be set into a language mode which the user does not understand and can find it extremely difficult to reset to a language which is readable. This specification provides a simple mechanism whereby a handset can be set to a language of choice or to an automatic mode whereby it sets itself to the language determined by the MCC of the IMSI stored on the SIM card.

When a code is entered in the format specified below, it shall set itself into the language indicated, provided that language is supported. If the language is not supported, then the automatic mode shall be entered.

```
*# <international dialling code (minimum 4 digits)> #
                    FOLLOWED BY "SEND"
```

E.g. If the user wishes to select English, then *#0044# shall be entered. If the user wishes to select Finnish, then *#0358# shall be entered.

In the situation where a language may be indicated by two or more country codes (e.g. English; UK, USA, Australia etc.), the handset shall implement either all applicable codes, or the one which is most applicable to the destined market.

Automatic mode shall be entered by entering *#0000# followed by "SEND".

B.4.10 Engineering Mode and SW version indication

It is common for a network operator to require the handset to support an engineering mode, whereby details of signal level, cell ID, carrier number etc. are displayed to the user. It is also common for the operator to require the handset to give its SW version to the user when a specific code is given.

However, this information shall not be given to a normal subscriber. It is imperative that the ME can determine an "authorised" user from a normal subscriber. This is done by checking the access class field on the SIM. If the subscriber has access class 15 (PLMN staff), then applicable codes may be used to determine the SW version or to display an engineering mode

B.4.11 SIM Toolkit

In order to utilise fully the provisions of the Phase 2+ SIM toolkit features, it is recommended that ME manufacturers implement class 3 SIM Toolkit functionality as soon as practically possible

Appendix 1

Modifications to GSM Recs. to support ALS

This page contains details of the additions to GSM recommendations 02.30, 04.08 and 09.02 made in order to support Alternate Line Service. Note that the information below does not include all other GSM specified values and should be used as an addendum to the GSM specifications.

02.30

An additional MMI service code is defined to give the new ALS teleservice "Auxiliary telephony.

```
Telecommunication Service                          MMI Service Code

Teleservices

All teleservices                                    10
Telephony                                           11
Auxiliary Telephony                                 89
All data teleservices                               12
.................
```

04.08

The bearer capability information element is modified to give an additional "information transfer capability"

```
Information transfer capability (octet 3)
Bits
3 2 1

0 0 0      speech
0 1 1      facsimile group 3
1 1 0      auxiliary speech (note)
1 1 1      alternate speech/facsimile group 3
.......

Note:      This value is treated by the network as speech.
```

09.02

An additional teleservice code is added to those which are currently specified.

TeleServiceCode	
Contents	Meaning
00000000	All teleservices
00010000	Speech transmission
00010001	Telephony
00010010	Emergency calls
11010000	Auxiliary speech
11010001	Auxiliary telephony
....	....