GSM TECHNICAL SPECIFICATION

GSM 11.14

August 1996

Version 5.1.0

Source: ETSI TC-SMG

Reference: TS/SMG-091114Q

ICS: 33.060.50

Key words: Digital cellular telecommunications system, Global System for Mobile communications (GSM)

GSM

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface (GSM 11.14)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

Foreword

This Global System for Mobile communications Technical Specification (GTS) has been produced by the Special Mobile Group (SMG) Technical Committee (TC) of the European Telecommunications Standards Institute (ETSI).

This GTS defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) within the digital cellular telecommunications system (Phase 2/Phase 2+).

This GTS is a TC-SMG approved GSM technical specification version 5.

GTS are produced by TC-SMG to enable the GSM Phase 2 + specifications to become publicly available, prior to submission for the formal ETSI standards approval procedure to become European Telecommunications Standards (ETS). This ensures the earliest possible access to GSM Phase 2 + specifications for all Manufacturers, Network operators and implementors of the Global System for Mobile communications.

The contents of this GTS are subject to continuing work within TC-SMG and may change following formal TC-SMG approval. Should TC-SMG modify the contents of this GTS it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 5.x.y

where:

- y the third digit is incremented when editorial only changes have been incorporated in the specification;

- x the second digit is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.

The specification from which this GTS has been derived was originally based on CEPT documentation, hence the presentation of this GTS may not be entirely in accordance with the ETSI rules.

Reference is made within this TS to GSM-TSs (note).

NOTE: TC-SMG has produced documents which give the technical specifications for the implementation of the digital cellular telecommunications system. Historically, these documents have been identified as GSM Technical Specifications (GSM-TSs). These TSs may have subsequently become I-ETSs (Phase 1), or ETSs/ETSI Technical Reports (ETRs) (Phase 2). TC-SMG has also produced ETSI GSM TSs which give the technical specifications for the implementation of Phase 2+ enhancements of the digital cellular telecommunications system. These version 5.x.x GSM Technical Specifications may be referred to as GTSs.

Blank page

1 Scope

This Technical Specification defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME), and mandatory ME procedures, specifically for "SIM Application Toolkit".

SIM Application Toolkit is a set of commands and procedures for use during the network operation phase of GSM, in addition to those defined in GSM 11.11 [14].

Specifying the interface is to ensure interoperability between a SIM and an ME independently of the respective manufacturers and operators. The concept of a split of the Mobile Station (MS) into these elements as well as the distinction between the GSM network operation phase, which is also called GSM operations, and the administrative management phase are described in the Technical Specification GSM 02.17 [3].

This Technical Specification defines:

- the commands;

- the application protocol;

- the mandatory requirements on the SIM and ME for each procedure.

Unless otherwise stated, references to GSM also apply to DCS 1800.

This standard does not specify any aspects related to the administrative management phase. Any internal technical realization of either the SIM or the ME are only specified where these reflect over the interface. This standard does not specify any of the security algorithms which may be used.

This Technical Specification defines an enhancement for GSM Phase 2+ of the SIM/ME interface for GSM Phase 2. While all attempts have been made to maintain phase compatibility, any issues that specifically relate to Phase 1 should be referenced from within the relevant Phase 1 specification.

2 Normative references

This European Telecommunication Standard (ETS) incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to, or revisions of, any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] GSM 01.02 (ETR 99): "Digital cellular telecommunications system (Phase 2); General Description of a GSM PLMN".

[2] GSM 01.04 (ETR 100): "Digital cellular telecommunications system (Phase 2); Abbreviations and acronyms".

[3] GSM 02.17 (ETS 300 509): "Digital cellular telecommunications system (Phase 2); Subscriber identity modules, functional characteristics".

[4] GSM 02.30 (ETS 300 511): "Digital cellular telecommunications system (Phase 2); Man-Machine Interface (MMI) of the Mobile Station (MS)".

[5] GSM 03.38 (ETS 300 628): "Digital cellular telecommunication system (Phase 2); Alphabets and language-specific information".

[6] GSM 03.40 (ETS 300 536): "Digital cellular telecommunications system (Phase 2); Technical realization of the Short Message (SMS) Service Point-to-Point (PP)".

[7] GSM 03.41 (ETS 300 537): "Digital cellular telecommunications system (Phase 2); Technical realization of the Short Message Service Cell Broadcast (SMSCB)".

[8] GSM 04.08 (ETS 300 557): "Digital cellular telecommunications system (Phase 2); Mobile radio interface Layer 3 specification".

[9] GSM 04.11 (ETS 300 559): "Digital cellular telecommunications system (Phase 2); Point to Point (PP) Short Message Service (SMS) support on mobile radio interface".

[10] GSM 04.80 (ETS 300 564): "Digital cellular telecommunications system (Phase 2); Mobile radio interface layer 3; Supplementary services specification; Formats and coding".

[11] GSM 04.90 (ETS 300 572): "Digital cellular telecommunications system (Phase 2); Unstructured Supplementary Service Data (USSD) - Stage 3".

[12] GSM 07.05 (ETS 300 585): "Digital cellular telecommunications system (Phase 2); Use of Data Terminal Equipment - Data Circuit terminating Equipment (DTE - DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS)".

[13] GSM 09.91 (ETR 300 174): "Digital cellular telecommunications system (Phase 2); Interworking aspects of the SIM/ME interface between Phase 1 and Phase 2".

[14] GSM 11.11 (ETS 300 608): "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[15] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[16] ISO/IEC 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[17] ISO/IEC 7816-6 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 6 Inter-industry data elements".

[18] GSM 02.40 (ETS 300 512): "Digital cellular telecommunications system (Phase 2); Procedures for call progress indications".

[19] GSM 02.07 (ETS 300 505): "Digital cellular telecommunications system (Phase 2); Mobile Stations (MS) features".

[20] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of this standard, the following definitions apply. For further information and definitions refer to GSM 01.02 [1].

application: An application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols).

application protocol: The set of procedures required by the application.

card session: A link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.

data object: Information seen at the interface for which are defined a tag (identifier), a length and a value. Data objects can be either BER-TLV (objects that conform to the Basic Encoding Rules of ASN.1) or SIMPLE-TLV. In this specification, all BER-TLV data objects are "primitive": the value part consists only of SIMPLE-TLV data objects.

padding: One or more bits appended to a message in order to cause the message to contain the required number of bits or bytes.

proactive SIM: A SIM which is capable of issuing commands to the ME within the T=0 protocol.

SIM application toolkit: A set of applications and related procedures which may be used during a GSM session.

3.2 Abbreviations

For the purposes of this standard the following abbreviations apply. In addition to the following abbreviations used in this specification are listed in GSM 01.04 [2].

A3	Algorithm 3, authentication algorithm; used for authenticating the subscriber
A5	Algorithm 5, cipher algorithm; used for enciphering/deciphering data
A8	Algorithm 8, cipher key generator; used to generate K_C
A38	A single algorithm performing the functions of A3 and A8
ADN	Abbreviated Dialling Number
APDU	Application Protocol Data Unit
BCD	Binary Coded Decimal
CB	Cell Broadcast
CBMI	Cell Broadcast Message Identifier
CCP	Capability/Configuration Parameter
DCS	Digital Cellular System
DTMF	Dual Tone Multiple Frequency
EF	Elementary File
ETSI	European Telecommunications Standards Institute
etu	elementary time unit
FDN	Fixed Dialling Number
GSM	Global System for Mobile communications
ID	IDentifier
IEC	International Electrotechnical Commission
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
Kc	Cryptographic key; used by the cipher A5
Ki	Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8
lgth	The (specific) length of a data unit
LND	Last Number Dialled
ME	Mobile Equipment
MMI	Man Machine Interface
MS	Mobile Station
NPI	Numbering Plan Identifier
RAND	A RANDom challenge issued by the network
RFU	Reserved for Future Use
SIM	Subscriber Identity Module
SMS	Short Message Service
SRES	Signed RESponse calculated by a SIM
SS	Supplementary Service
SSC	Supplementary Service Control string
SW1/SW2	Status Word 1 / Status Word 2
TLV	Tag, length, value.

TON	Type Of Number
TP	Transfer layer Protocol
TS	Technical Specification
USSD	Unstructured Supplementary Service Data

3.3 Symbols

'0' to '9' and 'A' to 'F' The sixteen hexadecimal digits

4 Overview of SIM Application Toolkit

The SIM Application Toolkit provides mechanisms which allow applications, existing in the SIM, to interact and operate with any ME which supports the specific mechanism(s) required by the application.

The following mechanisms have been defined. These mechanisms are dependent upon the commands and protocols relevant to SIM Application Toolkit in GSM 11.11 [20].

4.1 Profile Download

Profile downloading provides a mechanism for the ME to tell the SIM what it is capable of. The ME knows what the SIM is capable of through the SIM Service Table and EF_{PHASE}.

4.2 Proactive SIM

Proactive SIM gives a mechanism whereby the SIM can initiate actions to be taken by the ME. These actions include:

- display text from the SIM to the ME
- send a short message
- set up a voice call to a number held by the SIM
- set up a data call to a number and bearer capabilities held by the SIM
- send a SS control or USSD string
- play tone in earpiece
- initiate a dialogue with the user
- SIM initialisation request and notification of changes to EF(s)

4.3 Data download to SIM

Data downloading to the SIM uses the transport mechanisms of SMS point-to-point and Cell Broadcast. Transferral of information over the SIM-ME interface uses the ENVELOPE command.

4.4 Menu selection

A set of possible menu entries is supplied by the SIM in a proactive SIM command. The menu selection mechanism is used to transfer the SIM application menu item which has been selected by the user to the SIM.

4.5 Call control by SIM

When this service is activated by the SIM, all dialled digit strings are first passed to the SIM before the ME sets up the call. The SIM has the ability to allow, bar or modify the call.

4.6 Security

Applications designed using the features in this specification may require methods to ensure data confidentiality, data integrity, and data sender validation, or any subset of these. Requirements for these mechanisms are defined in section 10. [This will be elaborated in joint meetings between SMG9 and SMG-SG].

5 Profile download

5.1 Procedure

The profile download instruction is sent by the ME to the SIM as part of the SIM initialisation procedure. This procedure is specified in GSM 11.11 [14]. In this procedure, the ME reads EF_{PHASE}. If the EF indicates that the SIM requires the ME to perform the profile download procedure, then the ME shall send, as the next instruction to be sent to the SIM, the TERMINAL PROFILE command as specified below. The profile sent by the ME shall state the facilities relevant to SIM Application Toolkit that are supported by the ME.

This procedure is important, as it is by this that the SIM knows what the ME is capable of, and the SIM can then limit its instruction range accordingly. If no command is sent by the ME, the SIM shall assume that the ME does not support SIM Application Toolkit.

5.2 Structure and coding of TERMINAL PROFILE

Direction: ME to SIM

The command header is specified in GSM 11.11 [14].

Command parameters/data:

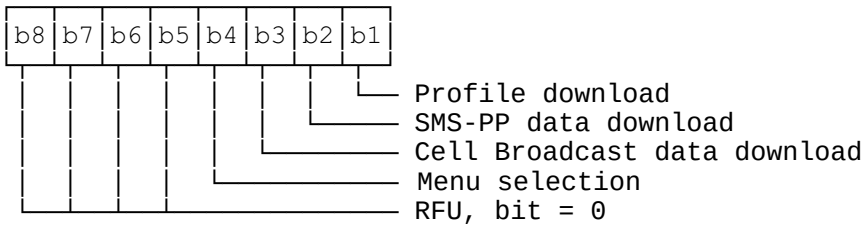
Description	Section	M/O	Length
Profile	-	M	lgth

- Profile:

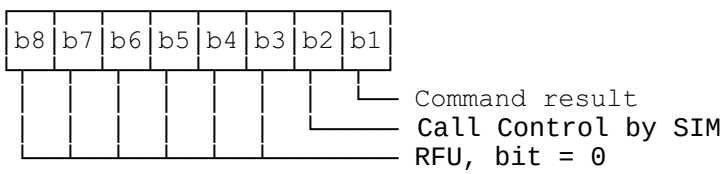
  Contents: The list of SIM Application Toolkit facilities that are supported by the ME.

  Coding:
  1 bit is used to code each facility:
  bit = 1: facility supported by ME
  bit = 0: facility not supported by ME

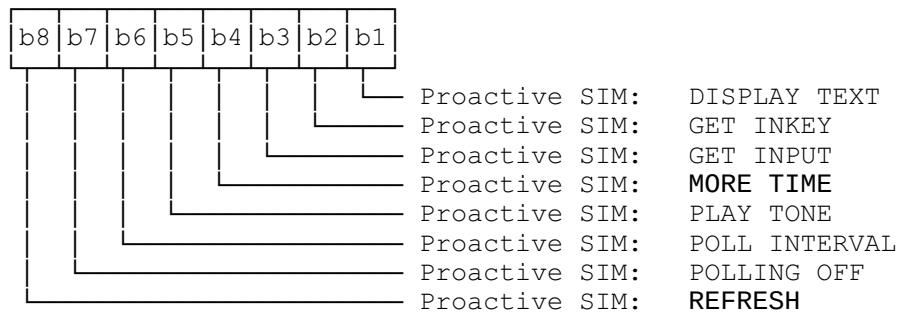
  First byte (Download):



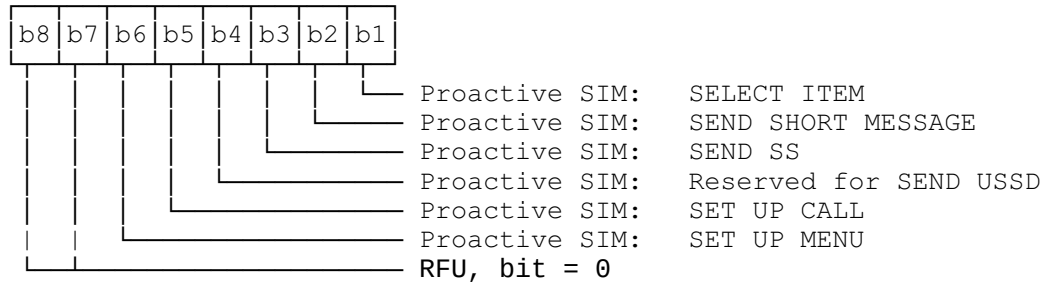
  Second byte (Other):



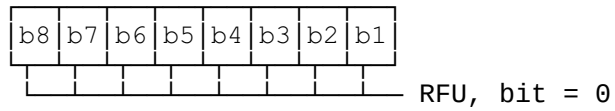
Third byte (Proactive SIM):



Fourth byte (Proactive SIM):



Subsequent bytes:



RFU bits, and all bits of subsequent bytes, are reserved to indicate future facilities. A SIM supporting only the features of SIM Application Toolkit defined here shall not check the value of RFU bits.

Response parameters/data: None.

6 Proactive SIM

6.1 Introduction

GSM 11.11 [14] defines that the ME communicates to the SIM using the T=0 protocol, which is specified in ISO/IEC 7816-3 [16]. The ME is always the "master", and initiates commands to the SIM, and therefore there is no mechanism for the SIM to initiate a communication with the ME. This limits the possibility of introducing new SIM features requiring the support of the ME, as the ME needs to know in advance what actions it should take.

The proactive SIM service provides a mechanism which stays within the protocol of T=0, but adds a new status response word SW1. This status response has the same meaning as the normal ending ('90 00'), and can be used with most of the commands that allow the normal ending, but it also allows the SIM to say to the ME "I have some information to send to you." The ME then uses the FETCH function to find out what this information is.

To avoid cross-phase compatibility problems, these functions shall only be used between a proactive SIM and an ME that supports the proactive SIM feature.

The SIM can issue a variety of commands through this mechanism, given in alphabetical order:

- DISPLAY TEXT, which displays text on screen (no more than 160 characters). A high priority is available, to replace anything else on screen.

- GET INKEY, which sends text to the display and requests a single character response in return. It is intended to allow a dialogue between the SIM and the user, particularly for selecting an option from a menu.

- GET INPUT, which sends text to the display and requests a response in return. It is intended to allow a dialogue between the SIM and the user.

- MORE TIME, which does not request any action from the ME. The ME is required to respond with TERMINAL RESPONSE (OK) as normal - see below. The purpose of the MORE TIME command is to provide a mechanism for the SIM Application Toolkit task in the SIM to request more processing time.

- PLAY TONE, which requests the ME to play a tone in its earpiece, ringer, or other appropriate loudspeaker.

- POLL INTERVAL, which negotiates how often the ME sends STATUS commands to the SIM during idle mode. Polling is disabled with POLLING OFF. Use of STATUS for the proactive SIM is described in GSM 11.11 [14].

- REFRESH, which requests the ME to carry out a SIM initialisation according to GSM 11.11 clause 11.2.1, and/or advises the ME that the contents or structure of EFs on the SIM have been changed.

- SELECT ITEM, where the SIM supplies a list of items, and the user is expected to choose one. The ME presents the list in an implementation-dependent way.

- SEND SHORT MESSAGE, which sends a short message or SMS-COMMAND to the network;

- SEND SS, which sends a SS request to the network;

- SEND USSD, which sends an USSD string to the network;

- SET UP CALL, of which there are three types:
  - Set up a call, but only if not currently busy on another call;
  - Set up a call, putting all other calls (if any) on hold;
  - Set up a call, disconnecting all other calls (if any);

  SET UP MENU, where the SIM supplies a list of items to be incorporated into the ME's menu structure.

The ME tells the SIM if the command was successful or not using the command result procedure defined in section 6.7. Responsibility for what happens after that (whether to repeat the command, try another one immediately, try again sometime later, or not to try again at all) lies with the SIM application. However, the SIM application needs to know why the command failed, so the ME provides the SIM with the result of the command.

Results are grouped into three main types:

- OK.

- Temporary problem. These results are further broken down into types of temporary problems, and specific causes. Generally, they indicate to the SIM that it may be worth trying again.

- Permanent problem. These results are again further broken down into types of permanent problems, and specific causes. Generally, they indicate to the SIM that it is not worth trying again during this GSM session.

6.2 Identification of proactive SIMs and of ME support

A proactive SIM shall be identified by having the proactive SIM service activated in the SIM Service Table (see GSM 11.11 [14]). An ME that supports proactive SIMs shall be identified as such when it sends a TERMINAL PROFILE command during SIM initialisation. The ME shall then send STATUS commands to the SIM at intervals determined by the poll interval procedure (see section 6.4.6).

A proactive SIM shall not send any command requests (status bytes SW1 SW2 = '91 XX') to a mobile that does not support the proactive SIM feature.

An ME that supports the proactive SIM feature shall not send proactive SIM related commands to a SIM that does not have the proactive SIM service activated.

6.3 General procedure

For all of the procedures that can end in '90 00' (indicating normal ending to the command), and which cannot end in '9F XX' (response data available from SIM), a proactive SIM operating with an ME that supports proactive SIMs may instead use the status response '91 XX'.

The response code '91 XX' shall indicate to the ME that the previous command has been successfully executed by the SIM in the same way as '90 00' (i.e. "OK"), but additionally it shall indicate response data which contains a command from the SIM for a particular ME procedure (defined in section 6.4).

The value 'XX' indicates the length of the response data. The ME shall use the FETCH command to obtain this data.

GSM 11.11 [20] shows how the SIM can initiate a proactive command in each of the five cases of transmission protocol identified in GSM 11.11 [14]. Some commands require the SIM to indicate that it has response data for the ME (through SW1/SW2 = '9F XX'), and the ME gets this data using the GET RESPONSE command.

When the ME has received a command from the SIM, it shall attempt to process the command immediately.

- If the command has been successfully executed, the ME shall inform the SIM immediately, using TERMINAL RESPONSE.

- If the command was not successfully executed, the ME shall inform the SIM immediately using TERMINAL RESPONSE with an error condition..

Responsibility for re-trying lies with the SIM application. The SIM application can make a judgement whether to send the same command again, to send a different one, or not to try again, from the information given by the ME in TERMINAL RESPONSE. If the SIM application wishes the ME to try again, it shall issue a new (identical) command.

6.4 Proactive SIM commands and procedures

6.4.1 DISPLAY TEXT

Four types are defined:

- Display normal priority text on screen (packed format);
- Display normal priority text on screen (unpacked format);
- Display high priority text on screen (packed format);
- Display high priority text on screen (unpacked format).

The ME shall reject normal priority text commands if the screen is currently being used for more than its normal stand-by display. If the command is rejected, the ME informs the SIM using TERMINAL RESPONSE (ME currently unable to process command - screen busy).

High priority text must be displayed on the screen immediately; the ME may return to the previous screen once the text from the SIM has been read.

6.4.2 GET INKEY

This command instructs the ME to display text, and to expect the user to enter a single character. Any response entered by the user shall be passed transparently by the ME to the SIM.

The text can be in one of two formats:

- packed format
- unpacked format

The response can be from one of two character sets. This is specified by the SIM:

- digits only (0-9, *, #, and +)
- characters from the SMS default alphabet

Upon receiving the command, the ME shall display the text. The ME shall allow the user to enter a single character in response.

- If the user presses END (or otherwise declines to respond, e.g. CLEAR), the ME shall give a null text string to the SIM, using TERMINAL RESPONSE.

- If the SIM requests a digit only, the ME shall only allow the user to enter a character from the digits 0-9, *, # and +. When the user has entered a digit, the ME shall pass the entered digit transparently to the SIM, using TERMINAL RESPONSE.

- If the SIM requests a character from the SMS default alphabet, the ME shall allow the user to enter a character using characters from this alphabet. When the user has entered a character, the ME shall pass the entered character transparently to the SIM, using TERMINAL RESPONSE.

  NOTE: If the MMI of the ME requires more than one keypress in order to select a character, it is an implementation decision for the ME manufacturer how to indicate completion (e.g. timeout, pressing SEND, OK). It may be useful to echo the input character on the display.

For both character sets, the response shall be coded using the SMS default alphabet in unpacked format.

6.4.3 GET INPUT

This command instructs the ME to display text, and that any response string entered by the user shall be passed transparently by the ME to the SIM.

The text can be in one of two formats:

- packed format
- unpacked format

The SIM indicates how many characters are expected for the response string, by giving a minimum and a maximum acceptable length.

The SIM specifies three variables for the response string it is expecting from the user:

- The response contains either digits only (0-9, *, # and +) or characters from the SMS default alphabet
- The response is either in an unpacked format or in a packed format
- The ME may display the text string being entered by the user (the response), or the ME shall hide (i.e. not display) the actual text string.

If the SIM requests that the user input (text string) is to be hidden, it is permissible for the ME to indicate the entry of characters, so long as the characters themselves are not revealed.

Upon receiving the command, the ME shall display the text. The ME shall allow the user to enter characters in response.

- The ME MMI is responsible for managing the entry of the correct number of characters.

- If the user presses END (or otherwise declines to respond), the ME shall give a null text string to the SIM, using TERMINAL RESPONSE.

- If the SIM requests digits only, the ME shall only allow the user to enter the digits 0-9, *, # and +. When the user presses SEND (or otherwise indicates completion), the ME shall pass the entered digit string transparently to the SIM, using TERMINAL RESPONSE.

- If the SIM requests characters from the SMS default alphabet, the ME shall allow the user to enter a character string using characters from this alphabet. When the user presses SEND (or otherwise indicates completion), the ME shall pass the entered text string transparently to the SIM, using TERMINAL RESPONSE.

If the SIM requests the user input to be in packed format, then the ME shall pack the text according to GSM 03.38 [5] before submitting it to the SIM.

6.4.4 MORE TIME

This procedure is provided to allow the SIM Application Toolkit task in the SIM more time for processing, where the processing is so long that it is in danger of affecting normal GSM operation, and clock stop prevents processing to take place in the background.

The ME shall take no extraordinary action when it receives this command, and all other operations shall be unaffected. The ME shall conclude the command by sending TERMINAL RESPONSE (OK) to the SIM, as soon as possible after receiving the MORE TIME command.

6.4.5 PLAY TONE

This command instructs the ME to play an audio tone.

Upon receiving this command, the ME shall check if it is currently in, or in the process of setting up (SET-UP message sent to the network, see GSM 04.08 [8]), a speech call.

- If the ME is in, or is setting up a speech call, it shall superimpose the tone on top of the downlink audio (if any), for the duration given in the command. The progress or current state of the call shall not be affected in any way.

- If the ME is not in or setting up a speech call, it shall route the audio to the external ringer, or other appropriate audio device, and play the tone for the duration given in the command.

- If ME support for the specific tone requested is optional, and the ME does not support this particular tone, the ME shall inform the SIM using TERMINAL RESPONSE (Command beyond ME's capabilities).

This proactive command contains no information on how a call is progressing; therefore the ME shall not generate any verbal indication or display any text or graphical indication about the normal meaning of this tone (e.g. display "called subscriber busy"). If the SIM wishes to convey a meaning in text to the user, it shall do this through the alpha identifier data object.

If the ME is required to generate a supervisory tone due to the progress of the current call (e.g. the network sends the ME call control cause information) as defined in GSM 02.40 [18], then the call supervisory tone shall take precedence over the tone requested by the SIM.

6.4.6 POLL INTERVAL

This procedure negotiates the maximum interval of time between STATUS commands issued by the ME when in idle mode. The SIM requests the time interval it would like from then onwards, and the ME responds through TERMINAL RESPONSE with the maximum interval that it will use. This can be greater, less than, or exactly the same as requested by the SIM.

NOTE: Applications on the SIM should not request short time intervals for an extended period, as this will have an adverse effect on battery life.

6.4.7 RESET

The purpose of this command is to enable the ME to be notified of the changes to the SIM configuration that have occurred during a SIM application. It is up to the SIM application to ensure that this is done correctly.

The command is separated into four different codings:

- SIM Initialisation. This coding tells the ME to carry out SIM initialisation as it is defined in GSM 11.11 clause 11.2.1 only, starting after the CHV1 verification procedure. The ME shall not reset the SIM electrically.

- File Change Notification. This coding advises the ME of the identity of the EFs that have been changed (in structure and/or contents) in the SIM. This information can be used by the ME if there is an image of SIM EFs (e.g. the ADN file) in the ME's memory, to determine whether it needs to update this image.

- SIM Initialisation and File Change Notification. This is a combination of the first two codings above.

- SIM Initialisation and Full File Change Notification. This coding causes the ME to perform the SIM initialisation procedure of the first coding above and advises the ME that several EFs have been changed (in structure or contents) in the SIM. If there is an image of SIM EFs in the ME's memory, the ME shall completely update this image.

NOTE 1: If the SIM implements EF_{IMSI} and EF_{LOCI} invalidation (for the FDN procedure) during an ATR then, as an ATR cannot happen as a result of a REFRESH command, the invalidation of these fields would not occur. Such invalidation must therefore be carried out at a later stage before the ME selects the EF_{IMSI} or EF_{LOCI} (see clause GSM 11.11 clause 11.2.1).

NOTE 2: Many MEs copy an image of the SIM's memory to the ME at initialisation to speed up access to these fields during a GSM session. One of the purposes of this coding of the REFRESH command is to enable MEs to change such an image efficiently.

6.4.8 SET UP MENU

The SIM shall supply a set of menu items, which shall be integrated with the menu system (or other MMI facility) in order to give the user the opportunity to choose one of these menu items at his own discretion. Each item comprises a short identifier (used to indicate the selection) and a text string. The SIM shall include an alpha identifier which acts as a title for the list of menu items.

NOTE: The maximum amount of data sent in one proactive SIM command is 256 bytes. It is therefore unavoidable that there is trade-off between the number of items and the length of the descriptive text (the alpha identifier of the SET-UP MENU command and the text strings of the items), e.g. for an average length of 10 bytes per text string the maximum amount of items is 18.

The list of menu items shall then be part of the menu system of the ME and the user is allowed to select an item from this list. The presentation style is left as an implementation decision to the ME manufacturer.

When the ME has successfully integrated the list of menu items, it shall send TERMINAL RESPONSE (OK) to the SIM.

When the ME is not able to successfully integrate the list of menu items, it shall sent TERMINAL RESPONSE (Command beyond ME's capabilities).

Any subsequent SET-UP MENU command replaces the current list of menu items supplied in the previous SET-UP MENU command.

When the user has selected one of the menu items of this menu item list, then the ME shall use the Menu Selection mechanism to transfer the identifier of the selected menu item to the SIM.

6.4.9 SELECT ITEM

The SIM shall supply a set of items from which the user may choose one. Each item comprises a short identifier (used to indicate the selection) and a text string. Optionally the SIM may include an alpha identifier. The alpha identifier is intended to act as a title for the list of items.

NOTE: The maximum amount of data sent in one proactive SIM command is 256 bytes. It is therefore unavoidable that there is trade-off between the number of items and the length of the descriptive text (the alpha identifier of the SELECT ITEM command and the text strings of the items), e.g. for an average length of 10 bytes per text string the maximum amount of items is 18.

The ME shall present the list of text strings to the user, and allow the user to select an item from this list. The presentation style is left as an implementation decision to the ME manufacturer.

When the user has selected an item, the ME shall send TERMINAL RESPONSE (OK) to the SIM with the identifier of the item chosen.

If no item was selected, the ME shall send TERMINAL RESPONSE (OK) to the SIM with null as the identifier of the item chosen.

6.4.10 SEND SHORT MESSAGE

Two types are defined:

- A short message to be sent to the network in an SMS-SUBMIT message, or an SMS-COMMAND message, where the user data can be passed transparently;

- A short message to be sent to the network in an SMS-SUBMIT message where the text needs to be packed by the ME.

Where the text has been packed, the text string provided by the SIM shall not be longer than 160 characters. It shall use the SMS default 7-bit coded alphabet, packed into 8-bit octets, in accordance with GSM 03.38 [5]. The text length (which is part of the SMS TPDU) given by the SIM shall state the number of 7-bit characters in the text string. The command details shall indicate 'packing not required'.

8-bit data Short Messages may be sent by the SIM. The command shall indicate packing not required. The string shall not be longer than 140 bytes, and the length (in SMS TPDU) shall state the number of bytes in the string.

SMS commands may be sent by the SIM. These shall count as packed text message. The SMS TPDU from the SIM shall indicate SMS-COMMAND. The command details shall indicate 'packing not required'.

Where packing by the ME is required, the text string provided by the SIM shall not be longer than 160 characters. It shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [5] with bit 8 set to 0. The text length given by the SIM shall state the number of characters in the text string. The ME shall pack the text string in accordance with GSM 03.38 [5] before submitting the message to the network.

If the ME is capable of SMS-MO, then it shall send the data as a Short Message TPDU to the destination address. The ME shall give the result to the SIM using TERMINAL RESPONSE (indicating successful or unsuccessful transmission of the Short Message) after receiving an SMS RP-ACK or RP-Error from the network.

6.4.11 SEND SS

Upon receiving this command, the ME shall decide if it is able to execute the command. Examples are given below, but the list is not exhaustive:

- If the command is rejected because the ME is busy on a SS transaction, the ME informs the SIM using TERMINAL RESPONSE (ME unable to process command - currently busy on SS transaction);

- If the command is rejected because the ME does not support that Supplementary Service, the ME informs the SIM using TERMINAL RESPONSE (Command beyond ME's capabilities);

If the ME is able to send the SS request, the ME shall:

- Send the SS request immediately, without need to alert the user first. Optionally, the ME can give some audible or display indication concerning what is happening.

- Once a SS Return Result message not containing an error has been received from the network, the ME shall inform the SIM that the command has been successfully executed, using TERMINAL RESPONSE. This command shall include the contents of SS Return Result as additional data. Optionally, the ME may display the result on screen.

- If the command is rejected because the network cannot support or is not allowing the Supplementary Service request, the ME informs the SIM using TERMINAL RESPONSE (SS Return Result error code);

- If the SS request is unsuccessfully received by the network, the ME shall inform the SIM using TERMINAL RESPONSE (network currently unable to process command), and not retry to send the request.

6.4.12 SEND USSD

For further study.

6.4.13 SET UP CALL

Three types are defined:

- Set up a call, but only if not currently busy on another call;
- Set up a call, putting all other calls (if any) on hold;
- Set up a call, disconnecting all other calls (if any) first.

For each of these types, the SIM may request the use of an automatic redial mechanism according to the GSM 02.07 [19]. The SIM may also request an optional maximum duration for the redial mechanism. The ME shall attempt at least one call set-up.

In addition to the called party number, the command may contain capability configuration parameters (giving the bearer capability to request for the call) and the called party subaddress. The ME shall use these in its call set-up request to the network. The command may also include DTMF digits, which the ME shall send to the network after the call has connected.

Upon receiving this command, the ME shall decide if it is able to execute the command. Examples are given below, but the list is not exhaustive:

- If the command is rejected because the ME is busy on another call, the ME informs the SIM using TERMINAL RESPONSE (ME unable to process command - currently busy on call);

- If the command is rejected because the ME is busy on a SS transaction, the ME informs the SIM using TERMINAL RESPONSE (ME unable to process command - currently busy on SS transaction);

- If the command is rejected because the ME cannot support Call Hold, or because the ME does not support the capability configuration parameters requested by the SIM, the ME informs the SIM using TERMINAL RESPONSE (Command beyond ME's capabilities);

- If the command is rejected because the network cannot support or is not allowing Call Hold, the ME informs the SIM using TERMINAL RESPONSE (SS Return Result error code).

If the ME is able to set up the call on the serving network, the ME shall:

- Alert the user (as for an incoming call). Optionally, the ME can give some indication to the user concerning what is happening, perhaps using the alpha identifier in the command data from the SIM.

- If the user accepts the call, the ME shall then set up a call to the destination address given in the response data, with the relevant capability configuration parameters and called party subaddress (if provided by the SIM).

- If the user does not accept the call, or rejects the call, then the ME informs the SIM using TERMINAL RESPONSE (user did not accept call set-up request). The operation is aborted.

- Optionally, during call set-up, the ME can give some audible or display indication concerning what is happening.

- Once a CONNECT message has been received from the network (defined in GSM 04.08), the ME shall inform the SIM that the command has been successfully executed, using TERMINAL RESPONSE. Operation of the call then proceeds as normal.

If the first call set-up attempt is unsuccessful:

- If the SIM did not request redial then the ME shall inform the SIM using TERMINAL RESPONSE (network currently unable to process command), and not redial to set-up the call

- If the SIM requested redial, then the ME may automatically redial the call (depending on its capability/configuration). In this case, the ME shall not send a command result to the SIM concerning the first or any subsequent failed set-up attempts. If the call set-up has not been successful, and the ME is not going to perform any more redials, or the time elapsed since the first call set-up attempt has exceeded the duration requested by the SIM, then the ME shall inform the SIM using TERMINAL RESPONSE (network currently unable to process command), and the redial mechanism shall be terminated.

- If the user stops the call set-up attempt or the redial mechanism before a result is received from the network, the ME informs the SIM using TERMINAL RESPONSE (user cleared down call before connection or network release).

6.4.14 POLLING OFF

This command cancels the effect of any previous POLL INTERVAL commands.

6.5 Common elements in proactive SIM commands

6.5.1 Command number

The command number is to cater for the future possibility of multiple ongoing commands (i.e. when the SIM issues further commands before receiving the response to the ongoing command). The implications of such multiple ongoing commands have not been elaborated at this stage of the toolkit specification.

Each command issued by a proactive SIM during a GSM session shall have its own command number. Command numbers may take any hexadecimal value between '01' and 'FE'. The command number is held in the command details data object.

The SIM is responsible for assigning the command number.

The ME shall keep a record of the status of each command and its command number, until the ME gives the result of the command to the SIM, using TERMINAL RESPONSE. After this, the ME may erase all internal records concerning this command. The command number is then free for allocation by the SIM to a new command.

When the MS is powered off and on, the details of any ongoing command shall be reset. The ME shall not be expected to know the status of commands issued in a previous GSM session.

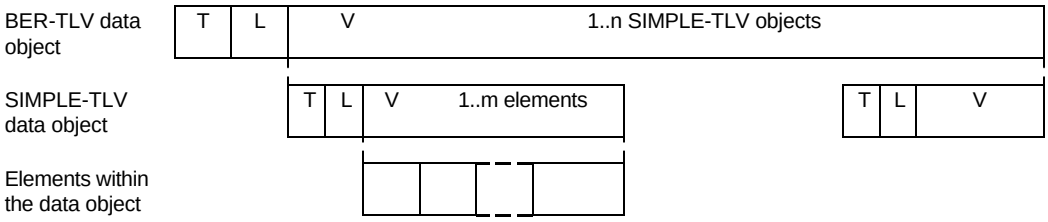
6.5.2 Device identities

This data object gives the devices which are the source and destination for the instruction. Only certain combinations of source and destination devices are allowed for each proactive command. These are given in section 13 of this document.

6.5.3 Alpha identifier in response data

Many of the commands include an alpha identifier data object. This is intended to be a short one or two word identifier for the ME to optionally display on screen along with any other indications, at the same time as the ME performs the SIM command. If longer text statements are required, which must be displayed on the screen, the SIM shall send a separate display command.

6.6 Structure of proactive SIM commands



Proactive SIM commands are sent across the interface as BER-TLV data objects. The tag is a constant value, length one byte, indicating it is a proactive SIM command.

The length is coded onto 1, or 2 bytes according to ISO 7816-6. The following table details this coding:

Length	**Byte 1**	**Byte 2**
0-127	length (‘00’ to ‘7F’)	not present
128-255	'81'	length (‘80’ to ‘FF’)

Any length within the APDU limits (up to 255 bytes) can thus be encoded on two bytes. This coding is chosen to remain compatible with ISO/IEC 7816-6 [17].

Any values for byte 1 or byte 2 that are not shown above shall be treated as an error and the whole message shall be rejected.

The value part of the BER-TLV data object consists of SIMPLE-TLV data objects, as shown in the sections below on individual commands. It is mandatory for SIMPLE-TLV data objects to be provided in the order given in this section for each command, but they do not necessarily need to be consecutive. (i.e., in the future, new SIMPLE-TLV data objects can be added to the middle of a command). The coding of SIMPLE-TLV data objects are specified later in this document.

The M/O columns specifies whether it is mandatory or optional for the sender to send that particular SIMPLE-TLV data object for compliance with the current version of this TS. The Min (Minimum Set) column describes whether it is necessary for the receiver to have received that particular SIMPLE-TLV data object to be able to attempt at least the most basic form of this command. The procedure for dealing with incomplete messages is described in section 6.9.

'00' and 'FF' are never used as tag values for BER-TLVs. Before, between or after BER-TLV data objects, '00' and 'FF' bytes without any meaning may occur (i.e. padding characters). This is in accordance with ISO/IEC 7816-6 [17]. The ME shall ignore them.

See ISO/IEC 7816-6 [17] for more information on data objects.

6.6.1 DISPLAY TEXT

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Text string	11.15	M	Y	C

6.6.2 GET INKEY

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Text string	11.15	M	Y	C

- Text string

Contents: text for the ME to display in conjunction with asking the user to respond

6.6.3 GET INPUT

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Text string	11.15	M	Y	C
Response length	11.11	M	Y	D

- Text string

Contents: text for the ME to display in conjunction with asking the user to respond

- Response length

Contents: the minimum and maximum acceptable lengths for the response from the user.

6.6.4 MORE TIME

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B

6.6.5 PLAY TONE

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D+E)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	O	N	C
Tone	11.16	O	N	D
Duration	11.8	O	N	E

- Tone

Contents: the standard supervisory tone or proprietary ME tone that the ME shall generate, either on its own or on top of the downlink audio path. If no tone is specified, then the ME shall default to "general beep".

NOTE: Some supervisory tones are optional for mobile equipment. See GSM 02.40 [18].

- Duration

Contents: the length of time for which the ME shall generate the tone, if the tone is continuous or repeatable. For single tones, the value of this data object shall be ignored by the ME. If no duration is specified, the ME shall default to a duration determined by the ME manufacturer.

6.6.6 POLL INTERVAL

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Duration	11.8	M	Y	C

- Duration

Contents: the maximum interval between two STATUS commands while in idle mode.

6.6.7 SET-UP MENU

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D1+D2+...Dn)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	M	Y	C
Item data object for item 1	11.9	M	Y	D1
Item data object for item 2	11.9	O	N	D2
.....	11.9	O	N	Dx
Item data object for last item in list	11.9	O	N	Dn

The SET-UP MENU command BER-TLV data object shall contain Item SIMPLE-TLV data objects. Each Item data object contains an item in the list, for the user to choose. The length of each Item data object may be different. Within a list, each Item shall have a unique item identifier.

6.6.8 SELECT ITEM

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D1+D2+...Dn)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	O	N	C
Item data object for item 1	11.9	M	Y	D1
Item data object for item 2	11.9	O	N	D2
.....	11.9	O	N	Dx
Item data object for last item in list	11.9	O	N	Dn

The SELECT ITEM command BER-TLV data object shall contain Item SIMPLE-TLV data objects. Each Item data object contains an item in the list, for the user to choose. The length of each Item data object may be different. Within a list, each Item shall have a unique item identifier.

6.6.9 SEND SHORT MESSAGE

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D+E)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	O	N	C
Address	11.1	O	N	D
SMS TPDU (SMS-SUBMIT or SMS-COMMAND)	11.13	M	Y	E

The address data object holds the RP_Destination_Address of the Service Centre. If no RP_Destination_Address is transferred, then the ME shall insert the default Service Centre address.

6.6.10 SEND SS

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	O	N	C
SS string	11.4	M	Y	D

6.6.11 Reserved for SEND USSD

6.6.12 SET UP CALL

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C+D+E+F+G)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
Alpha identifier	11.2	O	N	C
Address	11.1	M	Y	D
Capability configuration parameters	11.4	O	N	E
Called party subaddress	11.3	O	N	F
Duration	11.8	O	N	G

If the capability configuration parameters are not present, the ME shall assume the call is a speech call.

If the called party subaddress is not present, the ME shall not provide a called party subaddress to the network.

If the duration is not present, the SIM imposes no restrictions on the ME of the maximum duration of redials.

6.6.13 REFRESH

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B
File List	11.18	O	N	C

6.6.14 POLLING OFF

Description	Section	M/O	Min	Length
Proactive SIM command Tag	12.2	M	Y	1
Length (A+B)	-	M	Y	1 or 2
Command details	11.6	M	Y	A
Device identities	11.7	M	Y	B

6.7 Command results

Once the ME has made its attempt to execute a proactive command from the SIM, the ME shall inform the SIM of the success or otherwise of that command, by using TERMINAL RESPONSE. This message gives the command details, including the number of the command (see section 6.5.1), a general result, and sometimes more specific information.

Three overall categories of results are defined:

- Command performed successfully. This is returned by the ME for every successful command.

- Temporary problem with executing command. This is further defined below, but generally these indicate to the SIM that it is worth trying again later.

- Permanent problem with executing command. These are further defined below, but generally indicate that the same command will end in the same result if repeated during the same GSM session.

Successful commands are further defined as:

- Command performed successfully. There were no problems;
- Command performed with partial comprehension. Here the ME receives a command with one or more SIMPLE-TLV data objects that are unrecognised or unexpected, all of which do not have their ‘comprehension required’ flag set (section 12.3), but the parent BER-TLV data object still has the minimum set of SIMPLE-TLV data objects required to perform the command;
- Command performed, with missing information. The ME received at least the minimum set of component parts, but did not receive all of the parts that it believed mandatory for the SIM to send.

Temporary problems are further defined as:

- ME is currently unable to process the command. Specific causes for this are:
- the screen is busy;
- ME currently busy on a call;
- ME currently busy on SS transaction;
- no service is currently available;
- access control class barred on serving network
- no radio resource currently available
- not in speech call.
  If none of these can be made to apply, a "no cause can be given" value can be used.

- Network is currently unable to process the command. Specific cause values are the cause values given by the network, as defined in GSM 04.08 [8].

- The user did not accept the call set-up request. This is where the ME alerts the user before setting up a call, and the user either rejected or did not accept the "call".

- The user cleared down the call, before the call connected (CONNECT received from network, as defined in GSM 04.08 [8]) or before the network released the call.

Permanent problems are further defined as:

- Command is beyond ME's capabilities. This is sent by the ME when it understands what the SIM is asking it to do, but does not have the capability to do it, e.g. ME which only supports SMS asked to set up a call.

- Command type not understood by ME. This is sent by the ME when the SIM sends a command with the Type of Command byte set to a value the ME does not know. This is to allow future expansion of commands.

- Command data not understood by ME. This is sent by the ME when the command type is understood by the ME, but the related data object(s) are not, e.g. reserved values have been included in a data object, or one or more unknown SIMPLE-TLV data objects have a 'comprehension required' tag.

- SS Return Error. This is given to the SIM when the network returns a SS error in response to a previous SS command. Specific cause values are the same as given by the network in the Return Error message.

- SMS RP-ERROR. This is given to the SIM when the network returns an error in response to the ME trying to send a short message. Specific cause values are the same as the cause value of RP-Cause in an RP-ERROR message.

- Error, required values are missing. This is given when the command type is understood by the ME, but it does not receive the minimum set of SIMPLE-TLV data objects that it requires to perform the command. These components are shown by the 'Min' column in the command structure definitions.

6.8 Structure of TERMINAL RESPONSE

Direction: ME to SIM

The command header is specified in GSM 11.11 [14]. Length (A+B+C+D+E+F) is indicated by P3 of the header.

Command parameters/data:

Description	Section	M/O	Min	Length
Command details	11.6	M	Y	A
Device identities	11.7	M	N	B
Result	11.12	M	Y	C
Duration (only required in response to a POLL INTERVAL proactive command)	11.8	M/O	Y/N	D
Text string (only required in response to a GET INKEY or GET INPUT proactive command)	11.15	M/O	Y/N	E
Item identifier (only required in response to SELECT ITEM proactive command)	11.10	M/O	Y/N	F

- Command details: this data object shall be identical to the command details data object given by the SIM in the proactive command to which the ME is giving the result.

- Device identities: the ME shall set the device identities to
  Source: ME
  Destination: SIM

- Result: This data object holds the result of the proactive SIM command. . If the receiving SIM does not know the meaning of a value in the result, it shall assume that the command has failed.

- Duration: When the ME issues a successful TERMINAL RESPONSE for a POLL INTERVAL command, it shall state the polling interval it will be using in the Duration data object. All other types of TERMINAL RESPONSE do not need to include Duration. If one is included by the ME, the SIM shall ignore it.

- Text string: When the ME issues a successful TERMINAL RESPONSE for a GET INKEY or GET INPUT command, it shall supply the single character or the character string entered by the user in the Text string data object, no matter what type of string was entered. All other types of TERMINAL RESPONSE do not need to include Text string. If one is included by the ME, the SIM shall ignore it.

- Item identifier: When the ME issues a successful TERMINAL RESPONSE for a SELECT ITEM command, it shall supply the identifier of the item selected by the user in the Item identifier data object. All other types of TERMINAL RESPONSE do not need to include Item identifier. If one is included by the ME, the SIM shall ignore it.

  Under no circumstances shall the SIM wait indefinitely for a terminal response.

  Any future additional SIMPLE-TLV objects shall be included as Min = N and comprehension not required. This will ensure that any proactive command will end in a predictable way.

Response parameters/data: None.

6.9 Handling of unknown, unforeseen and erroneous messages

6.9.1 General

The procedures described in this section apply to the BER-TLV and SIMPLE-TLV data objects described in this TS. The purpose of this section is to allow greater flexibility in future versions of this document, and a greater predictability across different versions of this standard.

The procedures described here specify how the ME and SIM shall behave when they receive a proactive command or response that is not fully compliant with the standards by which it was designed. A response will be made to the SIM by means of the ‘general result’ field of the ‘result’

If the ME sends a TERMINAL RESPONSE to the SIM that contains values that the SIM does not understand, then the SIM shall issue the appropriate SW1 / SW2 error response. The current proactive transaction shall be considered complete and neither the ME or the SIM shall take no further action with regard to it. In this case, unless the ‘General result’ is ‘command performed...’ then the SIM shall assume that the command was not carried out and that a permanent error exists with regard to that particular proactive command. If the command was performed, but the ‘additional information on result’ field was not understood, then the SIM may attempt the command again at a later stage in the current GSM session.

If the SIM has enough information to proceed (i.e. it has received all the data objects of the Minimum set) then it shall do so.

6.9.2 Message too short

Any information received that is not a complete tag and length shall be ignored.

6.9.3 Missing minimum information

If a message is received that does not have all the mandatory elements in it, then if all of the minimum set elements are present then the receiver shall complete the command and report ‘command performed, with missing information’.

If the minimum set of elements is not complete, then the ME shall respond with ‘Error, required values are missing’.

6.9.4 Unknown Tag value

If a BER-TLV object is received that has a tag that is understood, but contains SIMPLE-TLV components that have unknown tags, then provided the minimum set condition is fulfilled, the 'comprehension required' bit of the tag shall determine how the receiving entity behaves.

If the comprehension required flag in an unknown tag is set to '1', and the ME either does not recognize or is not expecting one or more of the SIMPLE-TLV objects in the message, then it shall respond with 'Error, command data not understood by ME'.

If the comprehension required flag is set to '0', then the ME shall read the length field that follows and ignore that object. In this case the ME will be able to carry out the command without the SIMPLE-TLV components that it cannot understand. It shall respond with 'command performed, with missing information'.

6.9.5 Unexpected Tag value

If a BER-TLV object is received that contains elements that have recognisable tags, but which where not expected in the context of this message (for example, the ME sees SMS TDPU tag as part of TEXT FOR DISPLAY), then is shall discard that element. It shall then proceed as described for Unknown Tag values.

If a received object has a tag that has already been received, then the first instance shall be used and any subsequent instances shall be discarded.

6.9.6 Length errors

If the total lengths of the SIMPLE-TLV data objects are not consistent with the length given in the BER-TLV data object, then the whole BER-TLV data object shall be rejected. The result field in the TERMINAL RESPONSE shall have the error condition 'ME unable to process command'.

6.9.7 Contents not understood

If the contents of a SIMPLE-TLV data object contains a field with a value that is defined as reserved, then the whole SIMPLE-TLV data object shall be considered as invalid. It will then depend on the 'comprehension required' bit of the relevant tag as to whether the whole BER-TLV data object shall be rejected, or whether that particular SIMPLE-TLV data object shall be ignored.

If the contents of a BER-TLV object contains 'Spare' bits, then these shall be ignored.

6.9.8 Extended length data objects

If a SIMPLE-TLV data object has a length longer than expected (i.e. more information has been added), then the receiver shall ignore this extra information to the end of the object. The end of the object shall be found by looking at the 'length' field of that object.

NOTE: If comprehension of the extra bytes is required, this can be achieved by the use of a reserved coding in an earlier field.

7 Data download to SIM

7.1 SMS-PP data download

7.1.1 Procedure

If the service "data download via SMS Point-to-point" is allocated and activated in the SIM Service Table (see GSM 11.11 [14]), then the ME shall follow the procedure below:

- When the ME receives a Short Message with
  protocol identifier = SIM data download, and
  data coding scheme = class 2 message,
  then the ME shall pass the message transparently to the SIM using the ENVELOPE (SMS-PP DOWNLOAD) command as defined below.

- The ME shall not display the message, or alert the user of a short message waiting.

- The ME shall wait for an acknowledgement from the SIM. The SIM shall respond with:
  SW1 / SW2 = ‘90 00’, ‘91 XX’ or ‘9F XX’.

- If the SIM responds with ‘90 00’ or ‘91 XX’, the ME shall acknowledge the receipt of the short message to the network.

- If the SIM responds with ‘9F XX’, the ME shall use the GET RESPONSE command to get the response data. The response data from the SIM will be appended by the ME to the RP-ACK message it will send back to the network (see GSM 04.11[9]). The response data will be limited to 16 bytes.

If the service "data download via SMS-PP" is not allocated and activated in the SIM Service Table, and the ME receives a Short Message with the protocol identifier = SIM data download and data coding scheme = class 2 message, then the ME shall store the message in EF_{SMS} in accordance with GSM 11.11 [14].

NOTE: MEs not supporting SIM Application Toolkit are likely to store data download messages in EF_{SMS}, as if they were normal short messages.

7.1.2 Structure of ENVELOPE (SMS-PP DOWNLOAD)

Direction: ME to SIM

The command header is specified in GSM 11.11 [14].

Command parameters/data:

Description	Section	M/O	Min	Length
SMS-PP download tag	12.1	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Device identities	11.7	M	Y	A
Address	11.1	O	N	B
SMS TPDU (SMS-DELIVER)	11.13	M	Y	C

- Device identities: the ME shall set the device identities to
  Source: Network
  Destination: SIM

- Address: The address data object holds the RP_Originating_Address of the Service Centre (TS-Service-Centre-Address), as defined in GSM 04.11 [9].

Response parameters/data: None for this type of ENVELOPE command.

7.2 Cell Broadcast data download

7.2.1 Procedure

If the service "data download via SMS-CB" is allocated and activated in the SIM Service Table (see GSM 11.11 [14]), then the ME shall follow the procedure below:

- When the ME receives a new Cell Broadcast message, the ME shall compare the message identifier of the Cell Broadcast message with the message identifiers contained in EF_{CBMID}.

- If the message identifier is found in EF_{CBMID}, the cell broadcast page is passed transparently to the SIM using the ENVELOPE (CELL BROADCAST DOWNLOAD) command, as defined below. The ME shall not display the message.

- If the message identifier of the incoming cell broadcast message is not found in EF_{CBMID}, then the ME shall determine if the message should be displayed, by following the procedures in GSM 03.41 [7] and GSM 11.11 [14].

The ME shall identify new cell broadcast pages by their message identifier, serial number and page values.

7.2.2 Structure of ENVELOPE (CELL BROADCAST DOWNLOAD)

Direction: ME to SIM

The command header is specified in GSM 11.11 [14].

Command parameters/data:

Description	Section	M/O	Min	Length
Cell Broadcast Download tag	12.1	M	Y	1
Length (A+B)	-	M	Y	1 or 2
Device identities	11.7	M	Y	A
Cell Broadcast page	11.5	M	Y	B

- Device identities: the ME shall set the device identities to
  Source: Network
  Destination: SIM

Response parameters/data: None for this type of ENVELOPE command.

8 Menu Selection

A set of possible menu options can be supplied by the SIM using the proactive command SET UP MENU. If the SIM has sent this command, and the user subsequently chooses an option, the ME informs the SIM using this procedure.

8.1 Procedure

If the service ‘menu selection’ is allocated and activated in the SIM Service Table (see TS GSM 11.11 [14]), then the ME shall follow the procedure below.

- When the ME receives a menu selection from one of the menu items defined by a ‘SET-UP MENU’ command issued previously by the SIM it shall pass the identifier of the selected menu item to the SIM using the ENVELOPE(MENU SELECTION) command, as defined below.

8.2 Structure

Direction: ME to SIM

The command header is specified in TS GSM 11.11 [14]

Command parameters/data:

Description	Section	M/O	Min	Length
Menu Selection tag	12.1	M	Y	1
Length (A+B)	-	M	Y	1 or 2
Device identities	11.7	M	Y	A
Item identifier	11.10	M	Y	B

- Device identities: the ME shall set the device identities to
  Source: Keypad
  Destination: SIM

9 Call Control by SIM

9.1 Procedure for mobile originated calls

If the service "call control" is allocated and activated in the SIM Service Table (see GSM 11.11 [14]), then the ME shall follow the procedure below:

- For all call set-up attempts, the ME shall first pass the dialled digits and associated parameters to the SIM, using the ENVELOPE (CALL CONTROL) command defined below. The only exception is for redial attempts which are managed by the ME and only require the call set-up details to be passed to the SIM for the first attempt.

- The SIM shall respond with SW1 / SW2 = '90 00' or '9F XX'

- If the SIM responds with '90 00', the ME shall set up the call with the dialled digits and other parameters as sent to the SIM.

- If the SIM responds with '9F XX', the ME shall use the GET RESPONSE command to get the response data. The response data from the SIM shall indicate to the ME whether to set up the call as proposed, not set up the call, or instead set up a call using the data supplied by the SIM. It is mandatory for the ME to perform the call set-up request in accordance with the data from the SIM.

Optionally, the ME may indicate to the user that the call has been barred or changed.

The ME shall then follow the call set-up procedure defined in GSM 04.08 [8].

9.2 Procedure for Supplementary Services

If the service "call control" is allocated and activated in the SIM Service Table (see GSM 11.11 [14]), then for all supplementary service registrations or activations which include a destination number, the ME shall first pass the destination number to the SIM, using the ENVELOPE (CALL CONTROL) command defined below, as if the user wished to set up a call to the destination number.

The SIM shall respond in the same way as for dialled digits. The ME shall interpret the response as follows:

- If the SIM responds with '90 00', the ME shall send the supplementary service registration with the destination number as sent to the SIM.

- If the SIM responds with '9F XX', the ME shall use the GET RESPONSE command to get the response data. The response data from the SIM shall indicate to the ME whether to send the supplementary service registration as proposed, not send the SS registration, or instead send the SS registration using the data supplied by the SIM. It is mandatory for the ME to send the supplementary service registration in accordance with the data from the SIM.

Optionally, the ME may indicate to the user that the supplementary service registration has been barred or changed.

The ME shall then follow the supplementary service registration procedure defined in GSM 04.80 [10].

9.3 Interaction with Fixed Dialling Number

It is permissible for the Fixed Dialling Number service to be enabled (see GSM 11.11 [14]) at the same time as Call Control is allocated and activated in the SIM Service Table.

If FDN is enabled and Call Control is activated, the ME shall follow this procedure:

- The ME shall check that the number entered through the MMI is on the FDN list, in accordance with GSM 02.07 [19].

- If the MMI input does not pass the FDN check, the call shall not be set up.

- If the MMI input does pass the FDN check, the ME shall pass the dialled digits and other parameters to the SIM, using the ENVELOPE (CALL CONTROL) command.

- If the SIM responds with "allowed, no modification", the ME shall set up the call as proposed.

- If the SIM responds with "not allowed", the ME shall not set up the call.

- If the SIM responds with "allowed with modifications", the ME shall set up the call in accordance with the response from the SIM. If the modifications involve changing the dialled digits, the ME shall not re-check this modified number against the FDN list.

If the user wishes to enable or disable Fixed Dialling Number, the ME shall follow the procedure in GSM 11.11 [14]. The state of the Call Control service shall have no effect on this procedure.

9.4 Structure of ENVELOPE (CALL CONTROL)

Direction: ME to SIM

The command header is specified in GSM 11.11 [14].

Command parameters/data:

Description	Section	M/O	Min	Length
Call control tag	12.1	M	Y	1
Length (A+B+C+D)	-	M	Y	1 or 2
Device identities	11.7	M	Y	A
Address	11.1	M	Y	B
Capability configuration parameters	11.4	O	N	C
Called party subaddress	11.3	O	N	D

- Device identities: the ME shall set the device identities to
  Source: ME
  Destination: SIM

- Address: The address data object holds the Called Party Number, as defined in GSM 04.08 [8], to which the ME is proposing setting up the call. For supplementary service registrations, this data object holds the destination number.

- Capability configuration parameters: This contains the Bearer capabilities that the ME is proposing to send to the network. If this data object is not present, this shall indicate a speech call.

- Called party subaddress: This contains the called party subaddress that the ME is proposing to send to the network. If one is not present, this shall indicate that the ME is proposing not to send this information element to the network.

Response parameters/data:

It is permissible for the SIM to provide no response data, by responding with SW1 / SW2 = '90 00'. If the SIM does not provide any response data, then this shall have the same meaning as "allowed, no modification".

Description	Section	M/O	Min	Length
Call control result	-	M	Y	1
Length (A+B+C)	-	M	Y	1 or 2
Address	11.1	O	N	A
Capability configuration parameters	11.4	O	N	B
Called party subaddress	11.3	O	N	C

- Call control result

Contents: the command that the SIM gives to the ME concerning whether to allow, bar or modify the proposed call.

Coding:

'00' = Allowed, no modification
'01' = Not allowed
'02' = Allowed with modifications

- Address: This data object is only required if the SIM requests the call details to be modified. If the address data object is not present, then the ME shall assume the called party address (or destination number) is not to be modified.

- Capability configuration parameters: This data object is only required if the SIM requests the call details to be modified. If the capability configuration parameters are not present, then the ME shall assume the parameters are not to be modified.

- Called party subaddress: This data object is only required if the SIM requests the call details to be modified. If the called party subaddress is not present, then the ME shall assume the subaddress is not to be modified. If the subaddress supplied by the SIM is a null data object, then the ME shall not provide a called party subaddress to the network. A null data object shall have length = '00' and no value part.

It is mandatory for the SIM to provide at least one of the optional data objects if it has set the Call control result to "allowed with modifications".

10 Security requirements

To be defined.

11 SIMPLE-TLV data objects

This section specifies the coding of the SIMPLE-TLV data objects, which are contained in a BER-TLV data object. SIMPLE-TLV data objects may be transferred across the interface in either direction. A SIMPLE-TLV data object consists of a tag of length one byte, a length indicator, which gives the number of bytes in the value field, and a value part of variable length, whose contents, meaning and coding are given below.

Tag codings are given in section 12.3 for all SIMPLE-TLV data objects.

'00' and 'FF' are never used as tag values for SIMPLE-TLVs. Before, between or after SIMPLE-TLV data objects, '00' and 'FF' bytes without any meaning may occur (i.e. padding characters). The receiving entity shall ignore them. This is in alignment with ISO 7816-4 [17].

11.1 Address

Byte(s)	Description	Length
1	Address tag	1
2	Length (x)	1
3	TON and NPI	1
4 - x+2	Dialling number string	x-1

TON/NPI is coded as for EF_{ADN}.

Dialling number string is coded as for EF_{ADN}, and may include DTMF separators and DTMF digits, which the ME shall send in the same way as for EF_{ADN}.

See GSM 11.11 [14] for the coding of all EFs.

11.2 Alpha identifier

Byte(s)	Description	Length
1	Alpha identifier tag	1
2	Length (X)	1
3 - X+2	Alpha identifier of X characters	X

The alpha identifier is coded as for EF_{ADN}.

See GSM 11.11 [14] for the coding of all EFs.

11.3 Called party subaddress

Byte(s)	Description	Length
1	Called party subaddress tag	1
2	Length (x)	1
3 - x+2	Called party subaddress	X

Called party subaddress contains information as defined for this purpose in GSM 04.08 [8]. All information defined in GSM 04.08 shall be given in the value part of the data object, except the information element identifier and the length of called party subaddress contents (which is given by the length part of the data object).

11.4 Capability configuration parameters

Byte(s)	Description	Length
1	Capability configuration parameters tag	1
2	Length (X)	1
3 - X+2	Capability configuration parameters	X

Capability configuration parameters are coded as for EF_{CCP}. If it is being provided by the SIM, the SIM shall supply all information required to complete the Bearer Capability Information Element in the Call Set-up message, see GSM 04.08 [8]. Any unused bytes at the end of the value part shall be coded 'FF'.

See GSM 11.11 [14] for the coding of all EFs.

11.5 Cell Broadcast Page

Byte(s)	Description	Length
1	Cell Broadcast page tag	1
2	Length = '58' (88 decimal)	1
3 - 90	Cell Broadcast page	88

The Cell Broadcast page is formatted in the same way as described in GSM 03.41 [7].

11.6 Command details

Byte(s)	Description	Length
1	Command details tag	1
2	Length = ‘03’	1
3	Command number	1
4	Type of command	1
5	Command Qualifier	1

- Command number

For contents and coding, see section 6.5.1.

- Type of command:

Contents: The Type of Command specifies the required interpretation of the data objects which follow, and the required ME procedure.

Coding:

- '01’ = REFRESH;
- '02' = MORE TIME;
- '03' = POLL INTERVAL;
- ‘04’ = POLLING OFF;

- '10' =SET UP CALL,
- '11' = SEND SS;
- '12' = Reserved for SEND USSD;
- '13' = SEND SHORT MESSAGE,

- '20' = PLAY TONE;
- '21' = DISPLAY TEXT,
- '22' = GET INKEY,
- '23' = GET INPUT,
- '24' = SELECT ITEM,
- '25' = SET UP MENU.
- '26' to 'FF' are reserved values

The ME shall respond to reserved values with the result "Command type not understood"

- Command Qualifier:

Contents: Qualifiers specific to the command.

Coding:

- REFRESH;
  '00' =SIM Initialisation and Full File Change Notification;
  '01' = File Change Notification;
  '02' = SIM Initialisation and File Change Notification;
  '03' = SIM Initialisation.

- MORE TIME;
  The byte shall be set to '00'.

- POLL INTERVAL;
  The byte shall be set to '00'.

- POLLING OFF;
  The byte shall be set to '00'.

- SET UP CALL,
  '00' = set up call, but only if not currently busy on another call;
  '01' = set up call, but only if not currently busy on another call, with redial;
  '02' = set up call, putting all other calls (if any) on hold ;
  '03' = set up call, putting all other calls (if any) on hold, with redial;
  '04' = set up call, disconnecting all other calls (if any);
  '05' = set up call, disconnecting all other calls (if any), with redial;
  '06' to 'FF' = Reserved;

- SEND SS;
  The byte shall be set to '00'.

- Reserved for SEND USSD;

- SEND SHORT MESSAGE,
  bit 1: 0 = packing not required
  1 = SMS packing by the ME required
  bits 2-7 = 0 (Reserved);

- PLAY TONE;
  The byte shall be set to '00'.

- DISPLAY TEXT,
  '00' = normal priority
  '01' = high priority
  '02' to 'FF' = Reserved;

- GET INKEY,
  - bit 1 0 = digits (0-9, *, # and +) only
    1 = SMS default alphabet;
  - bits 2-7 = 0 (Reserved)

- GET INPUT,
  - bit 1 0 = digits (0-9, *, #, and +) only
    1 = SMS default alphabet;
  - bit 2 = 0 (Reserved)
  - bit 3 0 = ME may echo user input on the display
    1 = user input shall not be revealed in any way (see note)
  - bit 4 0 = user input to be in unpacked format
    1 = user input to be in SMS packed format
  - bits 5 to 8 = 0 (Reserved)

- SELECT ITEM.
  The byte shall be set to ‘00’.

- SET UP MENU.
  The byte shall be set to ‘00’.

NOTE: Where user input is not to be revealed, the ME may provide an indication of key entries, such as by displaying "*"s.

The ME shall respond to reserved values with the result "Command type not understood".

11.7 Device identities

Byte(s)	Description	Length
1	Device identities tag	1
2	Length = '02'	1
3	Source device identity	1
4	Destination device identity	1

- Source device identity

Contents: the source device for information held in the data objects which follow.

- Destination device identity

Contents: the destination device for information held in the data objects which follow.

NOTE: Only some combinations of Type of Command, Data Download type and Device identities are allowed. These are defined later in section 13.

Coding: both Source and Destination device identities are coded as follows:
- '01' = Keypad
- '02' = Display
- '03' = Earpiece
- '81' = SIM
- '82' = ME
- '83' = Network

All other values are reserved.

11.8 Duration

Byte(s)	Description	Length
1	Duration tag	1
2	Length = '02'	1
3	Time unit	1
4	Time interval	1

- Time unit

Contents: time unit used; minutes, seconds or tenths of seconds.
Coding:

'00' Minutes
'01' Seconds
'02' Tenths of seconds

All other values are reserved.

- Time interval

Contents: the length of time required, expressed in units.
Coding:

The time interval is coded in integer multiples of the time unit used. The range is from 1 unit to 255 units. The encoding is:

- '00': reserved
- '01': 1 unit
- '02': 2 units
- : :
- 'FF': 255 units

11.9 Item

Byte(s)	Description	Length
1	Item tag	1
2	Length (X)	1
3	Identifier of item	1
4 - X+2	Text string of item	X - 1

The identifier is a single byte between '01' and 'FF'. Each item must have a unique identifier within an Item list.

The text string is coded using the SMS default alphabet padded to 8 bits per character, in the same way as the alpha identifier for EF_{ADN}. Any unused bytes at the end of the value part shall be coded 'FF'.

11.10 Item identifier

Byte(s)	Description	Length
1	Item identifier tag	1
2	Length = '01'	1
3	Identifier of item chosen	1

The identifier is a single byte between '01' and 'FF', exactly the same as for the Item data object. A null item identifier is coded '00'.

11.11 Response length

Byte(s)	Description	Length
1	Response length tag	1
2	Length = '02'	1
3	Minimum length of response	1
4	Maximum length of response	X - 1

The range of length is between '00' and 'FF'. A minimum length coding of '00' indicates that there is no minimum length requirement; a maximum length coding of 'FF' indicates that there is no maximum length requirement. If a fixed length is required the minimum and maximum values are identical.

11.12 Result

Byte(s)	Description	Length
1	Result tag	1
2	Length (X)	1
3	General result	1
4 - X+2	Additional information on result	X-1

- General result

Contents: General result specifies the result and indicates appropriate SIM action:

Coding:
- '00' = Command performed successfully;
- '01' = Command performed with partial comprehension;
- '02' = Command performed, with missing information.

- '20' = ME currently unable to process command;
- '21' = Network currently unable to process command;
- '22' = User did not accept call set-up request
- '23' = User cleared down call before connection or network release;

- '30' = Command beyond ME's capabilities;
- '31' = Command type not understood by ME;
- '32' = Command data not understood by ME;
- '33' = Command number not known by ME;
- '34' = SS Return Error;
- '35' = SMS RP-ERROR.
- '36' = Error, required values are missing.

All other values are reserved and shall be treated by the SIM as '20'.

NOTE: General results 0X' and '1X' indicate that the command has been performed. Results '2X' indicate to the SIM that it may be worth re-trying the command at a later opportunity. Results '3X' indicate that it is not worth the SIM re-trying with an identical command, as it will only get the same response. However, the decision to retry lies with the SIM application.

- Additional information

Contents: For the general result "Command performed successfully", some proactive commands require additional information in the command result. This is defined in the sections below. For the general results '20', '21', '34' and '35', it is mandatory for the ME to provide a specific cause value as additional information, as defined in the sections below. For the other general results, the ME may optionally supply additional information. If additional information is not supplied, then the length of the value part of the data object need only contain the general result.

11.12.1 Additional information for SEND SS

When the ME issues a successful COMMAND RESULT for a SEND SS proactive command, it shall also include the Operation Code and Parameters included in the Return Result component from the network, as additional information.

The first byte of the additional information shall be the SS Return Result Operation code, as defined in GSM 04.11 [9].

The rest of the additional information shall be the SS Return Result Parameters, as defined in GSM 04.11 [9].

11.12.2 Additional information for ME problem

For the general result "ME currently unable to process command", it is mandatory for the ME to provide additional information, the first byte of which to be as defined below:

- '00' = No specific cause can be given;
- '01' = Screen is busy;
- '02' = ME currently busy on call;
- '03' = ME currently busy on SS transaction;
- '04' = No service;
- '05' = Access control class bar;
- '06' = Radio resource not granted;
- '07' = Not in speech call.

All other values shall be interpreted by the SIM as '00'.

NOTE: The coding '00' shall only be used by the ME if no others apply.

11.12.3 Additional information for network problem

For the general result "network currently unable to process command", it is mandatory for the ME to provide additional information. The first byte shall be the cause value of the Cause information element returned by the network (as defined in GSM 04.08 [8]). Bit 8 shall be set to '1'. One further value is defined:

- '00' = No specific cause can be given.

All other values shall be interpreted by the SIM as '00'.

NOTE: The coding '00' shall only be used by the ME if no others apply.

11.12.4 Additional information for SS problem

For the general result "SS Return Error", it is mandatory for the ME to provide additional information. The first byte shall be the error value given in the Facility (Return result) information element returned by the network (as defined in GSM 04.80 [10]). One further value is defined:

- '00' = No specific cause can be given.

All other values shall be interpreted by the SIM as '00'.

NOTE: The coding '00' shall only be used by the ME if no others apply.

11.12.5 Additional information for SMS problem

For the general result "SMS RP-ERROR", it is mandatory for the ME to provide additional information. The first byte shall be the cause value given in the RP-Cause element of the RP-ERROR message returned by the network (as defined in GSM 04.11 [9]), with bit 8 = 0. One further value is defined:

- '00' = No specific cause can be given.

All other values shall be interpreted by the SIM as '00'.

NOTE: Specific cause '00' shall only be used by the ME if no others apply.

11.13 SMS TPDU

Byte(s)	Description	Length
1	SMS TPDU tag	1
2	Length (X)	1
3 - X+2	SMS TPDU	X

The TPDU is formatted as described in GSM 03.40 [6].

Where the TPDU is being sent from the SIM to the ME (to be forwarded to the network), and where it includes a TP-Message-Reference which is to be incremented by the MS for every outgoing message, the TP-Message-Reference as provided by the SIM need not be the valid value. TP-Message-Reference shall be checked and corrected by the ME to the value described in GSM 03.40 [6].

11.14 SS string

Byte(s)	Description	Length
1	SS string tag	1
2	Length (X)	1
3	TON and NPI	1
4 - X+2	SS string	X - 1

TON/NPI and SS control string are coded as for EF_{ADN}, where the ADN record relates to a Supplementary Service Control string. See GSM 11.11 [14] for the coding of EF_{ADN}.

11.15 Text string

Byte(s)	Description	Length
1	Text string tag	1
2	Length (X)	1
3	Data coding scheme	1
4 - X+2	Text string of X-1 characters	X-1

A null text string shall be coded with Length = '00', and no Value part.

Data coding scheme is coded as for SMS Data coding scheme defined in GSM 03.38 [5].

11.15.1 Coding of text in unpacked format

This is indicated by the data coding scheme having a value of 8 bit data. Other parts of the data coding scheme shall be ignored.

This string shall be no longer than 160 characters, and use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [5] with bit 8 set to 0. It may or may not include formatting characters, but all such formatting characters shall be taken from the set given in the SMS alphabet.

NOTE: This is exactly the same format as is used for EF_{ADN} alpha-identifiers. It is also the same as SMS messages that have been "unpacked".

11.15.2 Coding of text in packed format

This is indicated by the data coding scheme having a value of 7 bit GSM default alphabet. Other parts of the data coding scheme shall be ignored.

This string shall be no longer than 160 characters, and use the SMS default 7-bit coded alphabet, packed into 8-bit octets, as defined in GSM 03.38 [5]. It may or may not include formatting characters, but all such formatting characters shall be taken from the set given in the SMS alphabet.

NOTE: This is the same format as is used in SMS messages to and from the network.

11.16 Tone

Byte(s)	Description	Length
1	Tone tag	1
2	Length = '01'	1
3	Tone	1

- Tone

Contents: Tones can be either the standard supervisory tone, as defined in GSM 02.40 [18], or proprietary tones defined by the ME manufacturer. The code values for proprietary tones shall be supported by the ME. If proprietary tones are not supported the ME shall map these codings to tones that it can generate. The tones to be used are left as an implementation decision by the manufacturer.

Coding:

Standard supervisory tones:
'01' Dial tone
'02' Called subscriber busy
'03' Congestion
'04' Radio path acknowledge
'05' Radio path not available / Call dropped
'06' Error / Special information
'07' Call waiting tone
'08' Ringing tone

ME proprietary tones:
'10' General beep
'11' Positive acknowledgement tone
'12' Negative acknowledgement or error tone

All other values are reserved.

11.17 Reserved for USSD string

11.18 File List

Byte(s)	Description	Length
1	File List tag	1
2	Length (X) of bytes following	1
3	Number of files (n)	1
4 to X+2	Files	X-1

Number of files:

This is the number of files that will be described in the following list.

Files:

Full paths are given to files. Each of these must be at least 4 octets in length (e.g. '3F002FE2' or '3F007F206FAD'). Each entry in the file description is composed of two bytes, where the first byte identifies the type of file (see GSM 11.11).

An entry in the file description shall therefore always begin with '3FXX'. There can be any number of Dedicated File entries between the Master File and Elementary File. There shall be no delimiters between files, as this is implied by the fact that the full path to any EF starts with '3FXX' and ends with an Elementary type file.

12 Tag values

This section specifies the tag values used to identify the BER-TLV and SIMPLE-TLV data objects used in this specification.

12.1 BER-TLV tags in ME to SIM direction

Description	Length of tag	Value
SMS-PP download tag	1	'D1'
Cell Broadcast download tag	1	'D2'
Menu Selection tag	1	'D3'
Call control tag	1	'D4'

12.2 BER-TLV tags in SIM TO ME direction

Description	Length of tag	Value
Proactive SIM command tag	1	'D0'

12.3 SIMPLE-TLV tags in both directions

8	7	6	5	4	3	2	1
CR	T	T	T	T	T	T	T

CR: Comprehension required for this object. (See section 6.9.4 for a description of the use of the CR flag.)

CR	Value
Comprehension required	1
Comprehension not required	0

Description	Length of tag	CR	Value (T) (‘01’ - ‘7E’)
Command details tag	1	1	'01'
Device identity tag	1	1	'02'
Result tag	1	1	'03'
Duration tag	1	1	'04'
Alpha identifier tag	1	1	'05'
Address tag	1	1	'06
Capability configuration parameters tag	1	1	'07'
Called party subaddress tag	1	1	'08'
SS string tag	1	1	'09'
Reserved for USSD string tag	1	1	'0A'
SMS TPDU tag	1	1	'0B'
Cell Broadcast page tag	1	1	'0C'
Text string tag	1	1	'0D'
Tone tag	1	1	'0E'
Item tag	1	1	'0F'
Item identifier tag	1	1	'10'
Response length tag	1	1	'11'
Address tag	1	1	‘12’
Menu selection tag	1	1	‘13’
File List tag	1	1	‘14’

13 Allowed Type of command and Device identity combinations

Only certain types of commands can be issued with certain device identities. These are defined below:

Command description	Source	Destination
CALL CONTROL	ME	SIM
CELL BROADCAST DOWNLOAD	Network	SIM
COMMAND RESULT	ME	SIM
DISPLAY TEXT	SIM	Display
GET INKEY	SIM	ME
GET INPUT	SIM	ME
MENU SELECTION	Keypad	SIM
MORE TIME	SIM	ME
PLAY TONE	SIM	Earpiece (see note 1)
POLLING OFF	SIM	ME
POLL INTERVAL	SIM	ME
PROFILE DOWNLOAD	ME	SIM
REFRESH	SIM	ME
SELECT ITEM	SIM	ME
SEND SHORT MESSAGE	SIM	Network
SEND SS	SIM	Network
SEND USSD	SIM	Network
SET UP CALL	SIM	Network
SET UP MENU	SIM	ME
SMS-PP DOWNLOAD	Network	SIM

NOTE: The ME may route the tone to other loudspeakers (external ringer, car kit) if more appropriate.

Annex A (normative): Mandatory support of SIM Application Toolkit by Mobile Equipment

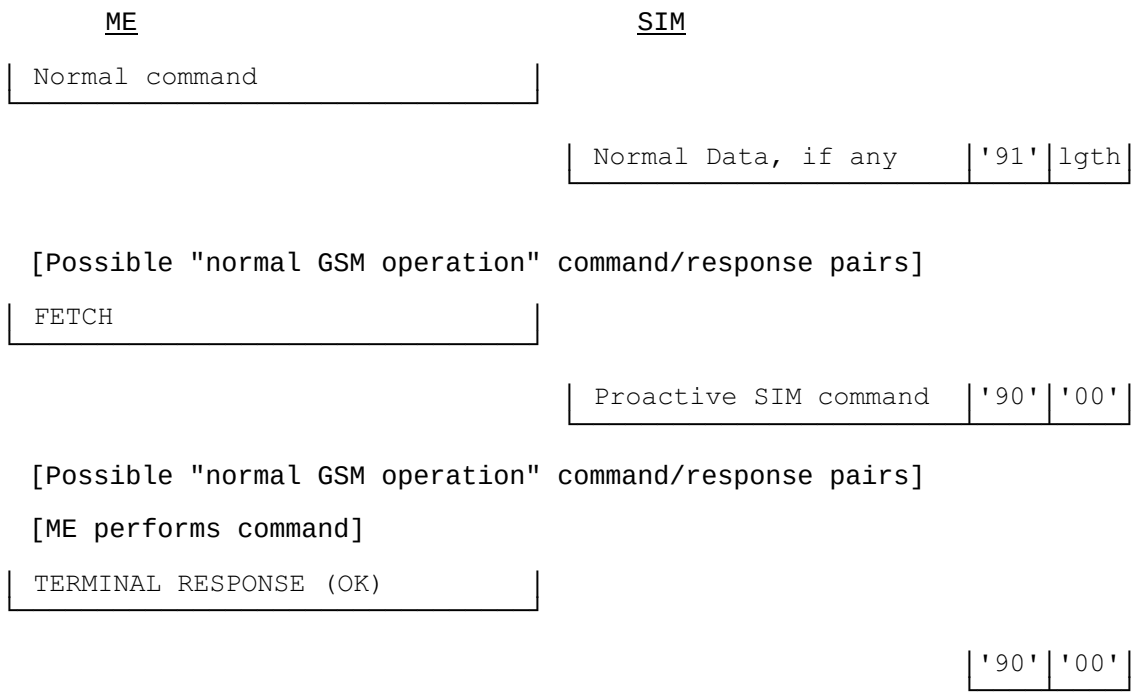
Support of SIM Application Toolkit is optional for Mobile Equipment. However, any ME claiming to support SIM Application Toolkit need not support all toolkit functions, but shall support all functions within a class as given in the table below:

		Classes		
Command description		1	2	3
CALL CONTROL			X	X
CELL BROADCAST DOWNLOAD			X	X
DISPLAY TEXT			X	X
GET INKEY			X	X
GET INPUT			X	X
MENU SELECTION			X	X
MORE TIME			X	X
PLAY TONE			X	X
POLLING OFF			X	X
POLL INTERVAL			X	X
REFRESH		X	X	X
SELECT ITEM			X	X
SEND SHORT MESSAGE			X	X
SEND SS			X	X
SEND USSD				X
SET UP CALL			X	X
SET UP MENU			X	X
SMS-PP DOWNLOAD		X	X	X
SET UP MENU			X	X

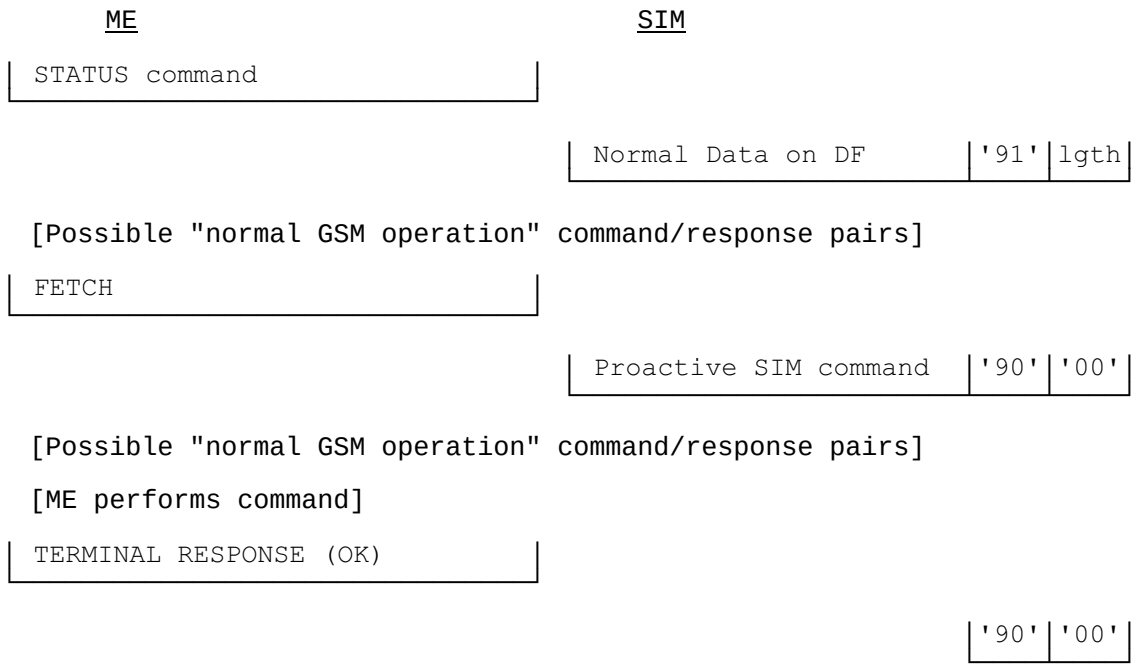
Annex B (informative): Example command sequences for proactive SIM

This section shows example APDU sequences for proactive SIM commands, and is for information only.

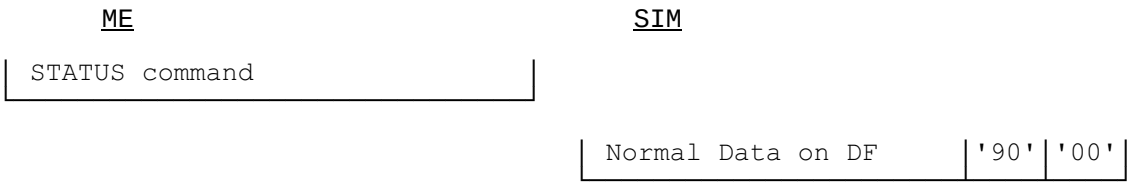
Case 1: Proactive SIM request following a normal command from the ME



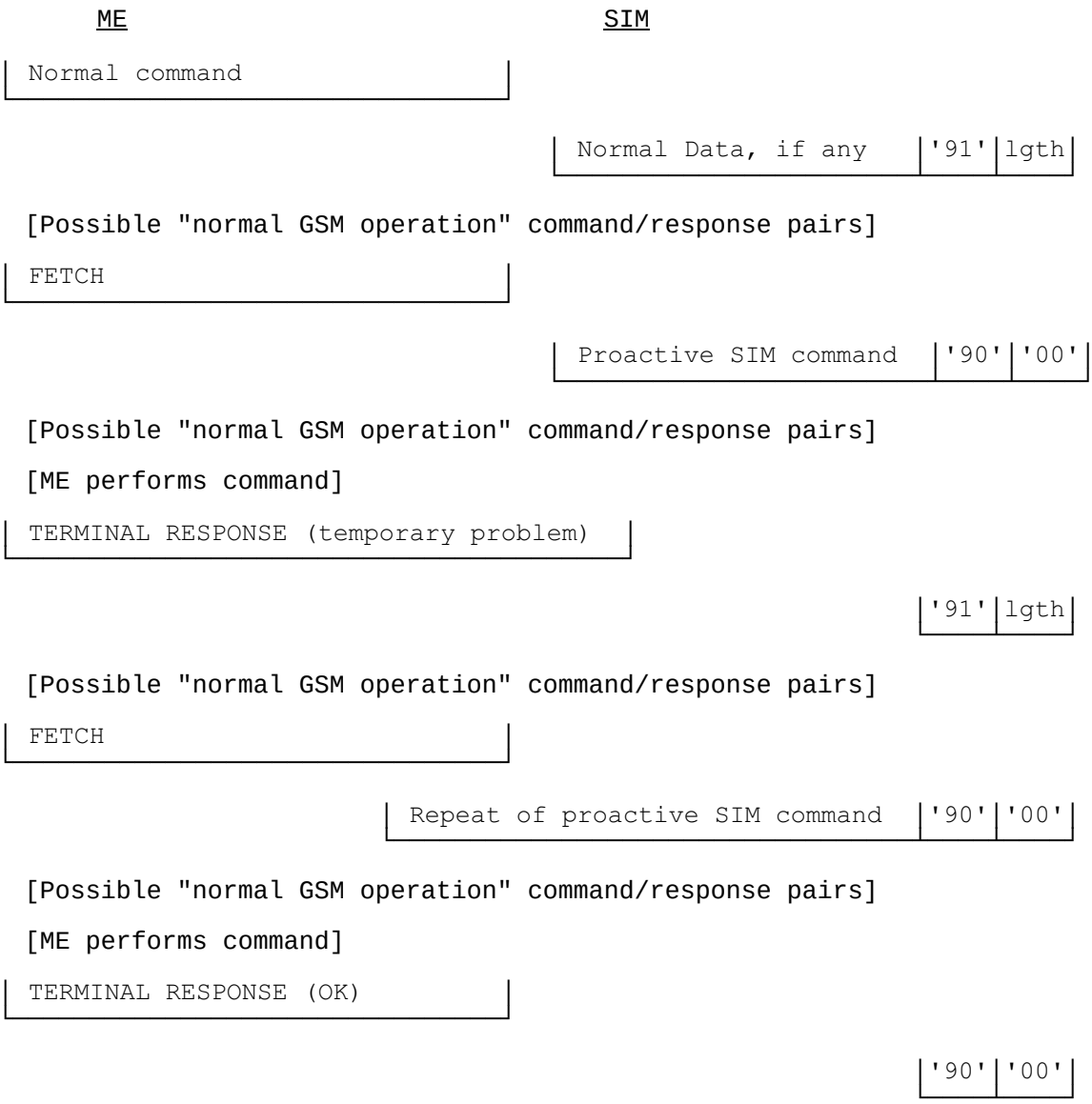
Case 2: Proactive SIM request following a (polling) STATUS command from the ME



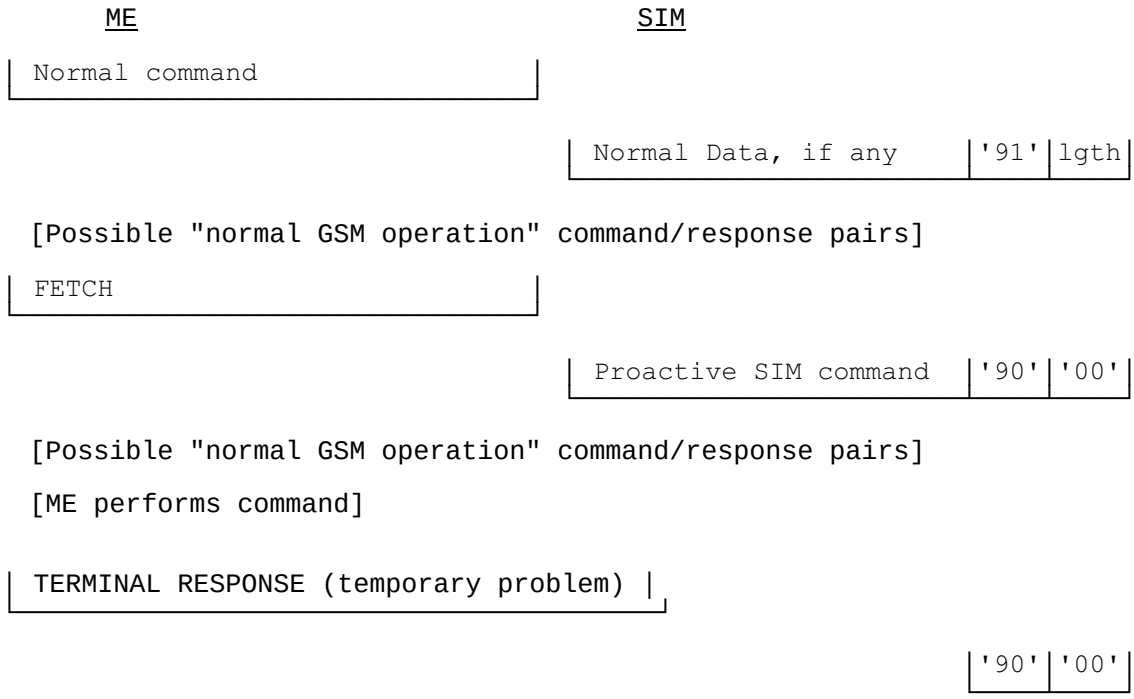
Case 3: STATUS command from ME, not followed by any proactive SIM request



Case 4: Unsuccessful proactive SIM request, followed by SIM asking the ME to retry



Case 5: Unsuccessful proactive SIM request, and the SIM does not ask for the ME to retry



Annex C (informative): Example of DISPLAY TEXT Proactive SIM Command

Example of DISPLAY TEXT Proactive SIM Command
(BER-TLV Data Object)

Byte#	Value (Hex)	Description
1	D0	Proactive SIM command tag
2	0E	length
3	01	command details tag
4	02	length
5	01	command number
6	60	Display text(normal priority)
7	02	Device identity tag
8	02	length
9	81	source : SIM
10	02	destination : Display
11	0D	Text string tag
12	04	length
13 - 16		text string

History

Change history					
Date/ SMG No.	**TDoc. No.**	**CR. No.**	**Section Affected**	**New version**	**Subject**
SMG#19	515/96	A001	Various	5.1.0	SIM Application Toolkit (refresh command)

Document history	
August 1996	Publication of version 5.1.0

ISBN 2-7437-0835-2
Dépôt légal : Août 1996