EUROPEAN
TELECOMMUNICATION
STANDARD

DRAFT
pr **ETS 300 608**

July 1999

Ninth Edition

Source: SMG

Reference: RE/SMG-091111PR9

ICS: 33.020

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

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 4.21.0)

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
Internet: secretariat@etsi.fr - http://www.etsi.org

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Telecommunication Standard (ETS) has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI), and is now submitted for the One-step Approval Procedure phase of the ETSI standards approval procedure.

This ETS specifies the Subscriber Identity Module (SIM) to Mobile Equipment (ME) interface within the digital cellular telecommunications system (Phase 2).

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

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This European Telecommunication Standard (ETS) defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of GSM as well as those aspects of the internal organization of the SIM which are related to the network operation phase. This 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 [6].

This ETS defines:

- the requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- the model which shall be used as a basis for the design of the logical structure of the SIM;
- the security features;
- the interface functions;
- the commands;
- the contents of the files required for the GSM application;
- the application protocol.

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

This ETS 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 ETS does not specify any of the security algorithms which may be used.

This ETS defines 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 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 Public Land Mobile Network (PLMN)".

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

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

[4] GSM 02.09 (ETS 300 506): "Digital cellular telecommunications system (Phase 2); Security aspects".

[5] GSM 02.11 (ETS 300 507): "Digital cellular telecommunications system (Phase 2); Service accessibility".

[6] GSM 02.17 (ETS 300 509): "Digital cellular telecommunications system (Phase 2); Subscriber Identity Modules (SIM), Functional characteristics".

[7] GSM 02.24 (ETS 300 510): "Digital cellular telecommunications system (Phase 2); Description of Charge Advice Information (CAI)".

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

[9] GSM 02.86 (ETS 300 519): "Digital cellular telecommunications system (Phase 2); Advice of charge (AoC) supplementary services - Stage 1".

[10] GSM 03.20 (ETS 300 534): "Digital cellular telecommunications system (Phase 2); Security related network functions".

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

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

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

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

[15] 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".

[16] GSM 09.91 (ETR 174): "Digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[17] CCITT Recommendation E.118: "The international telecommunications charge card".

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

[19] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, Information processing - ISO 7-bits coded characters set for information interchange).

[20] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[21] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[22] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[23] ISO 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[24] ISO 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

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

[26] GSM 11.12 (ETS 300 641): "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

3 Definitions, abbreviations and symbols

3.1 Definitions

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

access conditions: A set of security attributes associated with a file.

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.

current directory: The latest MF or DF selected.

current EF: The latest EF selected.

data field: Obsolete term for Elementary File.

Dedicated File (DF): A file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs).

directory: General term for MF and DF.

Elementary File (EF): A file containing access conditions and data and no other files.

file: A directory or an organized set of bytes or records in the SIM.

file identifier: The 2 bytes which address a file in the SIM.

GSM or DCS 1800 application: Set of security mechanisms, files, data and protocols required by GSM or DCS 1800.

GSM session: That part of the card session dedicated to the GSM operation.

IC card SIM: Obsolete term for ID-1 SIM.

ID-1 SIM: The SIM having the format of an ID-1 card (see ISO 7816-1 [23]).

Master File (MF): The unique mandatory file containing access conditions and optionally DFs and/or EFs.

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

plug-in SIM: A second format of SIM (specified in clause 4).

record: A string of bytes within an EF handled as a single entity (see clause 6).

record number: The number which identifies a record within an EF.

record pointer: The pointer which addresses one record in an EF.

root directory: Obsolete term for Master File.

3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply, in addition to the those 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
ACM	Accumulated Call Meter
ADN	Abbreviated Dialling Number
ADM	Access condition to an EF which is under the control of the authority which creates this file
ALW	ALWays
AoC	Advice of Charge
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BCCH	Broadcast Control CHannel
BCD	Binary Coded Decimal
BTS	Base Transmitter Station
CB	Cell Broadcast
CBMI	Cell Broadcast Message Identifier
CCITT	The International Telegraph and Telephone Consultative Committee (now also known as the ITU Telecommunications Standardization sector)
CCP	Capability/Configuration Parameter
CHV	Card Holder Verification information; access condition used by the SIM for the verification of the identity of the user
CLA	CLAss
DCS	Digital Cellular System
DF	Dedicated File (abbreviation formerly used for Data Field)
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
HPLMN	Home PLMN
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
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
LAI	Location Area Information; information indicating a cell or a set of cells
lgth	The (specific) length of a data unit
LND	Last Number Dialled
LSB	Least Significant Bit
MCC	Mobile Country Code
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MS	Mobile Station
MSISDN	Mobile Station international ISDN number
MSB	Most Significant Bit
NET	NETwork
NEV	NEVer
NPI	Numbering Plan Identifier
PIN/PIN2	Personal Identification Number / Personal Identification Number 2 (obsolete terms for CHV1 and CHV2, respectively)

PLMN	Public Land Mobile Network
PTS	Protocol Type Select (response to the ATR)
PUK/PUK2	PIN Unblocking Key / PIN2 Unblocking Key (obsolete terms for UNBLOCK CHV1 and UNBLOCK CHV2, respectively)
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
SSC	Supplementary Service Control string
SW1/SW2	Status Word 1 / Status Word 2
TMSI	Temporary Mobile Subscriber Identity
TON	Type Of Number
TP	Transfer layer Protocol
TPDU	Transfer Protocol Data Unit
TS	Technical Specification
UNBLOCK CHV1/2	value to unblock CHV1/CHV2
VPLMN	Visited PLMN

3.3 Symbols

For the purposes of this ETS, the following symbols apply.

Vcc	Supply voltage
Vpp	Programming voltage
'0' to '9' and 'A' to 'F'	The sixteen hexadecimal digits

4 Physical characteristics

Two physical types of SIM are specified. These are the "ID-1 SIM" and the "Plug-in SIM".

The physical characteristics of both types of SIM shall be in accordance with ISO 7816-1,2 [22, 23] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the GSM environment.

4.1 Format and layout

The information on the exterior of either SIM should include at least the individual account identifier and the check digit of the IC Card Identification (see clause 10, EF_{ICCID}).

4.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO 7816-1,2 [22, 23].

The card shall have a polarization mark (see GSM 02.07 [3]) which indicates how the user should insert the card into the ME.

The ME shall accept embossed ID-1 cards. The embossing shall be in accordance with ISO/IEC 7811 [21]. The contacts of the ID-1 SIM shall be located on the front (embossed face, see ISO/IEC 7810 [20]) of the card.

NOTE: Card warpage and tolerances are now specified for embossed cards in ISO/IEC 7810 [20].

4.1.2 Plug-in SIM

The Plug-in SIM has a width of 25 mm, a height of 15 mm, a thickness the same as an ID-1 SIM and a feature for orientation. (see figure A.1 in normative annex A for details of the dimensions of the card and the dimensions and location of the contacts).

Annexes A.1 and A.2 of ISO 7816-1 [23] do not apply to the Plug-in SIM.

Annex A of ISO 7816-2 [24] applies with the location of the reference points adapted to the smaller size. The three reference points P1, P2 and P3 measure 7,5 mm, 3,3 mm and 20,8 mm, respectively, from 0. The values in table A.1 of ISO 7816-2 [24] are replaced by the corresponding values of figure A.1.

4.2 Temperature range for card operation

The temperature range for full operational use shall be between -25°C and +70°C with occasional peaks of up to +85°C. "Occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

4.3 Contacts

4.3.1 Provision of contacts

ME: There shall not be any contacting elements in positions C4 and C8. Contact C6 need not be provided for Plug-in SIMs.

SIM: Contacts C4 and C8 need not be provided by the SIM. Contact C6 shall not be bonded in the SIM for any function other than supplying Vpp.

4.3.2 Activation and deactivation

The ME shall connect, activate and deactivate the SIM in accordance with the Operating Procedures specified in ISO/IEC 7816-3 [25].

For any voltage level, monitored during the activation sequence, or during the deactivation sequence following soft power-down, the order of the contact activation/deactivation shall be respected.

NOTE 1: Soft Power switching is defined in GSM 02.07 [3].

NOTE 2: It is recommended that whenever possible the deactivation sequence defined in ISO/IEC 7816-3 [25] should be followed by the ME on all occasions when the ME is powered down.

If the SIM clock is already stopped and is not restarted, the ME is allowed to deactivate all the contacts in any order, provided that all signals reach low level before Vcc leaves high level. If the SIM clock is already stopped and is restarted before the deactivation sequence, then the deactivation sequence specified in ISO/IEC 7816-3 [25] subclause 5.4 shall be followed.

When Vpp is connected to Vcc, as allowed by GSM (see clause 5), then Vpp will be activated and deactivated with Vcc, at the time of the Vcc activation/deactivation, as given in the sequences of ISO/IEC 7816-3 [25] subclauses 5.1 and 5.4.

The voltage level of Vcc, used by GSM, differs from that specified in ISO/IEC 7816-3 [25]. Vcc is powered when it has a value between 4,5 V and 5,5 V.

4.3.3 Inactive contacts

The voltages on contacts C1, C2, C3, C6 and C7 of the ME shall be between 0 and ± 0,4 volts referenced to ground (C5) when the ME is switched off with the power source connected to the ME. The measurement equipment shall have a resistance of 50 kohms when measuring the voltage on C2, C3, C6 and C7. The resistance shall be 10 kohms when measuring the voltage on C1.

4.3.4 Contact pressure

The contact pressure shall be large enough to ensure reliable and continuous contact (e.g. to overcome oxidisation and to prevent interruption caused by vibration). The radius of any curvature of the contacting elements shall be greater than or equal to 0,8 mm over the contact area.

Under no circumstances may a contact force be greater than 0,5 N per contact.

Care shall be taken to avoid undue point pressure to the area of the SIM opposite to the contact area. Otherwise this may damage the components within the SIM.

4.4 Precedence

For Mobile Equipment, which accepts both an ID-1 SIM and a Plug-in SIM, the ID-1 SIM shall take precedence over the Plug-in SIM (see GSM 02.17 [6]).

4.5 Static Protection

Considering that the SIM is a CMOS device, the ME manufacturer shall take adequate precautions (in addition to the protection diodes inherent in the SIM) to safeguard the ME, SIM and SIM/ME interface from static discharges at all times, and particularly during SIM insertion into the ME.

5 Electronic signals and transmission protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [25] unless specified otherwise. The following additional requirements shall be applied to ensure proper operation in the GSM environment.

The choice of the transmission protocol(s), to be used to communicate between the SIM and the ME, shall at least include that specified and denoted by T=0 in ISO/IEC 7816-3 [25].

The values given in the tables hereafter are derived from ISO/IEC 7816-3 [25], subclause 4.2 with the following considerations:

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

- This convention is different to the one used in ISO/IEC 7816-3 [25], which specifically defines an ICC for which its current conventions apply. The following clauses define the specific core requirements for the SIM, which provide also the basis for Type Approval. For each state ($V_{OH,}$ $V_{IH,}$ V_{IL} and V_{OL}) a positive current is defined as flowing out of the entity (ME or SIM) in that state.

- The high current options of ISO/IEC 7816-3 [25] for V_{IH} and V_{OH} are not specified for the SIM as they apply to NMOS technology requirements. No realization of the SIM using NMOS is foreseen.

5.1 Supply voltage Vcc (contact C1)

The SIM shall be operated within the following limits:

Table 1: Electrical characteristics of Vcc under normal operating conditions

Symbol	Minimum	Maximum	Unit
Vcc	4,5	5,5	V
Icc		10	mA

The current consumption of the SIM shall not exceed the value given in table 1 during any state (including activation and deactivation as defined in subclause 4.3.2).

When the SIM is in idle state (see below) the current consumption of the card shall not exceed 200 µA at 1 MHz and 25°C. If clock stop mode is allowed, then the current consumption shall also not exceed 200 µA while the clock is stopped.

The ME shall source the maximum current requirements defined above. It shall also be able to counteract spikes in the current consumption of the card up to a maximum charge of 40 nAs with no more than 400 ns duration and an amplitude of at most 200 mA, ensuring that the supply voltage stays in the specified range.

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

5.2 Reset (RST) (contact C2)

The ME shall operate the SIM within the following limits:

Table 2: Electrical characteristics of RST under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	Vcc-0,7	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0V (note)	0,6V
t_R t_F	C_{out} = C_{in} = 30 pF		400 µs
NOTE: To allow for overshoot the voltage on RST shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.3 Programming voltage Vpp (contact C6)

SIMs shall not require any programming voltage on Vpp. The ME need not provide contact C6. If the ME provides contact C6, then, in the case of the ID-1 SIM the same voltage shall be supplied on Vpp as on Vcc, while in the case of Plug-in SIMs the ME need not provide any voltage on C6. Contact C6 may be connected to Vcc in any ME but shall not be connected to ground.

5.4 Clock CLK (contact C3)

The SIM shall support 1 to 5 MHz. The clock shall be supplied by the ME. No "internal clock" SIMs shall be used.

If a frequency of 13/4 MHz is needed by the SIM to run the authentication procedure in the allotted time (see GSM 03.20 [10]), bit 2 of byte 1 in the file characteristics shall be set to 1. Otherwise a minimum frequency of 13/8 MHz may be used.

The duty cycle shall be between 40 % and 60 % of the period during stable operation.

The ME shall operate the SIM within the following limits:

Table 3: Electrical characteristics of CLK under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	0,7 x Vcc	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0V (note)	0,5 V
t_R t_F	C_{out} = C_{in} = 3 pF		9 % of period with a maximum of 0,5 µs
NOTE: To allow for overshoot the voltage on CLK shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.5 I/O (contact C7)

Table 4 defines the electrical characteristics of the I/O (contact C7). The values given in the table have the effect of defining the values of the pull-up resistor in the ME and the impedances of the drivers and receivers in the ME and SIM.

Table 4: Electrical characteristics of I/O under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{IH}	I_{IHmax} = ±20 µA (note 2)	0,7xVcc	Vcc+0,3 V
V_{IL}	I_{ILmax} = +1 mA	-0,3 V	0,8 V
V_{OH} (note 1)	I_{OHmax} = +20 µA	3,8 V	Vcc (note 3)
V_{OL}	I_{OLmax} = -1 mA	0 V (note 3)	0,4 V
t_R t_F	C_{out} = C_{in} = 30 pF		1 µs
NOTE 1: It is assumed that a pull-up resistor is used in the interface device (recommended value: 20 kohms).			
NOTE 2: During static conditions (idle state) only the positive value can apply. Under dynamic operating conditions (transmission) short term voltage spikes on the I/O line may cause a current reversal.			
NOTE 3: To allow for overshoot the voltage on I/O shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.6 States

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

- The SIM is in operating state when it executes a command. This state also includes transmission from and to the ME.
- The SIM is in idle state at any other time. It shall retain all pertinent data during this state.

The SIM may support a clock stop mode. The clock shall only be switched off subject to the conditions specified in the file characteristics (see clause 9).

Clock stop mode. An ME of Phase 2 or later shall wait at least 1860 clock cycles after having received the last character, including the minimum guard time (2 etu), of the response before it switches off the clock (if it is allowed to do so). It shall wait at least 744 clock cycles before it sends the first command after having started the clock.

To achieve phase compatibility, the following procedure shall be adhered to:

A SIM of Phase 2 or later shall always send the status information "normal ending of the command" after the successful interpretation of the command SLEEP received from a Phase 1 ME. An ME of Phase 2 or later shall not send a SLEEP command.

A Phase 1 ME shall wait at least 744 clock cycles after having received the compulsory acknowledgement SW1 SW2 of the SLEEP command before it switches off the clock (if it is allowed to do so). It shall wait at least 744 clock cycles before it sends the first command after having started the clock.

5.7 Baudrate

The baudrate for all communications shall be: (clock frequency)/372.

5.8 Answer To Reset (ATR)

The ATR is information presented by the SIM to the ME at the beginning of the card session and gives operational requirements.

5.8.1 Structure and contents

The following table gives an explanation of the characters specified in ISO/IEC 7816-3 [25] and the requirements for their use in GSM. The answer to reset consists of at most 33 characters. The ME shall be able to receive interface characters for transmission protocols other than T=0, historical characters and a check byte, even if only T=0 is used by the ME.

Table 5: ATR

Character	Contents	sent by the card	a) b) evaluation by the ME reaction by the ME
1. Initial character TS	coding convention for all subsequent characters (direct or inverse convention)	always	a) always b) using appropriate convention
2. Format character T0	subsequent interface characters, number of historical characters	always	a) always b) identifying the subsequent characters accordingly
3. Interface character (global) TA1	parameters to calculate the work etu	optional	a) always if present b) if TA1 is not '11', PTS procedure shall be used (see subclause 5.8.2)
4. Interface character (global) TB1	parameters to calculate the programming voltage and current	optional	a) always if present b) if PI1 is not 0, then reject the SIM (in accordance with subclause 5.10)
5. Interface character (global) TC1	parameters to calculate the extra guardtime requested by the card; no extra guardtime is used to send characters from the card to the ME	optional	a) always if present b) if TC1 is neither 0 nor 255, then reject the SIM (in accordance with subclause 5.10); see the note after the table
6. Interface character TD1	protocol type; indicator for the presence of inter-face characters, specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
7. Interface character (specific) TA2	not used for protocol T=0	optional	a) optional b) --------
8. Interface character (global) TB2	parameter to calculate the programming voltage	never	the allowed value of TB1 above defines that an external programming voltage is not applicable
9. Interface character (specific) TC2	parameters to calculate the work waiting time	optional	a) always if present b) using the work waiting time accordingly

(continued)

Table 5 (concluded): ATR

Character	Contents	sent by the card	a) b) evaluation by the ME reaction by the ME
10. Interface character TDi (i>1)	protocol type; indicator for the presence of interface characters, specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly
11. Interface character TAi, TBi, TCi (i>2)	characters which contain interface characters for other transmission protocols	optional	a) optional b) --------
12. Historical characters T1,...,TK	contents not specified in ISO/IEC	optional	a) optional b) --------
13. Check character TCK	check byte (exclusive - ORing)	not sent if only T=0 is indicated in the ATR; in all other cases TCK shall be sent	a) optional b) --------

NOTE: According to ISO/IEC 7816-3:1989/DAM2 (see annex D) N=255 indicates that the minimum delay is 12 etu for the asynchronous half-duplex character transmission protocol.

5.8.2 PTS procedure

Specifically related to this Technical Specification the PTS procedure according to ISO/IEC 7816-3 [25], clause 7, is applied, only if TA1 is not equal to '11', as follows:

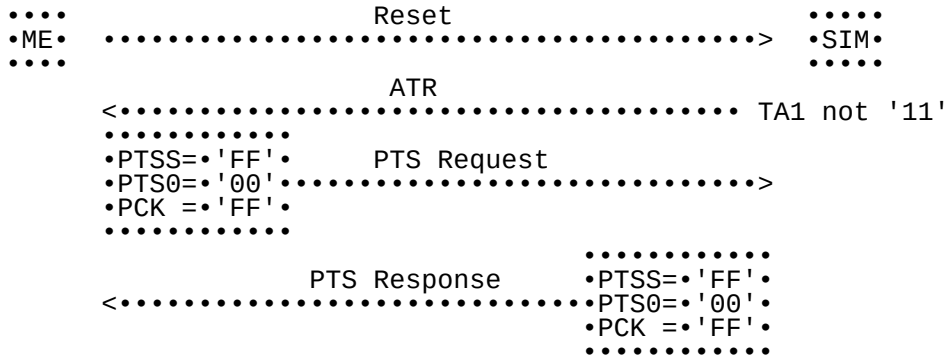


Figure 1: PTS procedure

PTS Request and PTS Response consist of the three (3) characters PTSS, PTSO and PCK of which PTSS is sent first.

After this procedure the protocol T=0 and the parameters F=372, D=1 and N=0 will be used.

5.9 Bit/character duration and sampling time

The bit/character duration and sampling time specified in ISO/IEC 7816-3 [25], subclauses 6.1.1 and 6.1.2, are valid for all communications.

5.10 Error handling

Following receipt of an ATR, which is not in accordance with this specification, e.g. because of forbidden ATR characters or too few bytes being transmitted, the ME shall perform a Reset. The ME shall not reject the SIM until at least three consecutive wrong ATRs are received.

During the transmission of the ATR and the protocol type selection, the error detection and character repetition procedure specified in ISO/IEC 7816-3 [25], subclause 6.1.3, is optional for the ME. For the subsequent transmission on the basis of T=0 this procedure is mandatory for the ME.

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

6 Logical Model

This clause describes the logical structure for a SIM, the code associated with it, and the structure of files used.

6.1 General description

Figure 2 shows the general structural relationships which may exist between files. The files are organized in a hierarchical structure and are of one of three types as defined below. These files may be either administrative or application specific. The operating system handles the access to the data stored in different files.

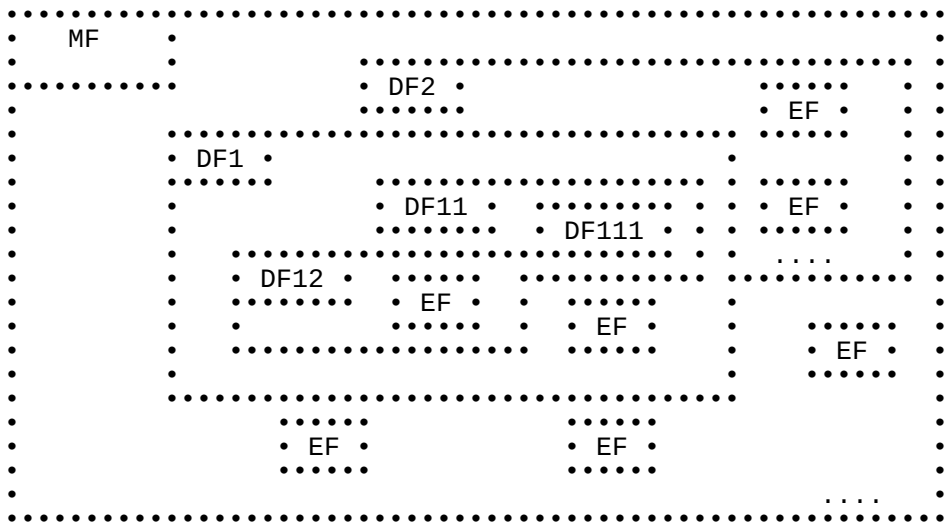


Figure 2: Organization of memory

Files are composed of a header, which is internally managed by the SIM, and optionally a body part. The information of the header is related to the structure and attributes of the file and may be obtained by using the commands GET RESPONSE or STATUS. This information is fixed during the administrative phase. The body part contains the data of the file.

6.2 File identifier

A file ID is used to address or identify each specific file. The file ID consists of two bytes and shall be coded in hexadecimal notation. They are specified in clause 10.

The first byte identifies the type of file, and for GSM is:

- '3F': Master File;
- '7F': Dedicated File;
- '2F': Elementary File under the Master File;
- '6F': Elementary File under a Dedicated File.

File IDs shall be subject to the following conditions:

- the file ID shall be assigned at the time of creation of the file concerned;
- no two files under the same parent shall have the same ID;
- a child and any parent, either immediate or remote in the hierarchy, e.g. grandparent, shall never have the same file ID.

In this way each file is uniquely identified.

6.3 Dedicated files

A Dedicated File (DF) is a functional grouping of files consisting of itself and all those files which contain this DF in their parental hierarchy (that is to say it consists of the DF and its complete "subtree"). A DF "consists" only of a header part.

Three DFs are defined in this specification:

- DF_{GSM} which contains the application for both GSM and/or DCS1800;
- DF_{IS41} which contains the applications for IS-41 as specified by ANSI T1P1;
- $DF_{TELECOM}$ which contains telecom service features.

All three files are immediate children of the Master File (MF) and may coexist on a multi-application card.

6.4 Elementary files

An Elementary File (EF) is composed of a header and a body part. The following three structures of an EF are used by GSM.

6.4.1 Transparent EF

An EF with a transparent structure consists of a sequence of bytes. When reading or updating, the sequence of bytes to be acted upon is referenced by a relative address (offset), which indicates the start position (in bytes), and the number of bytes to be read or updated. The first byte of a transparent EF has the relative address '00 00'. The total data length of the body of the EF is indicated in the header of the EF.

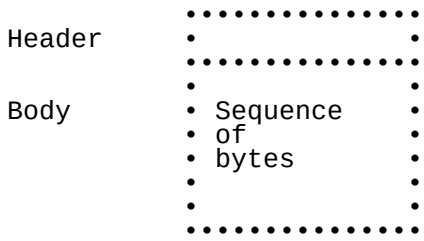


Figure 3: Structure of a transparent EF

NOTE: This structure was previously referred to as "binary" in GSM.

6.4.2 Linear fixed EF

An EF with linear fixed structure consists of a sequence of records all having the same (fixed) length. The first record is record number 1. The length of a record as well as this value multiplied by the number of records are indicated in the header of the EF.

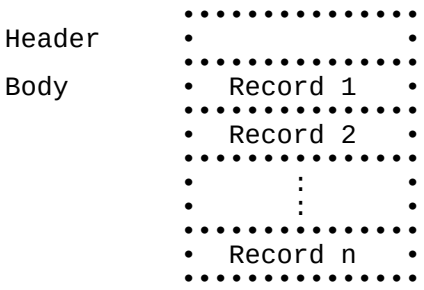


Figure 4: Structure of a linear fixed file

There are several methods to access records within an EF of this type:

- absolutely using the record number;
- when the record pointer is not set it shall be possible to perform an action on the first or the last record by using the NEXT or PREVIOUS mode;
- when the record pointer is set it shall be possible to perform an action on this record, the next record (unless the record pointer is set to the last record) or the previous record (unless the record pointer is set to the first record);
- by identifying a record using pattern seek starting
  - forwards from the beginning of the file;
  - forwards from the record following the one at which the record pointer is set (unless the record pointer is set to the last record);
  - backwards from the end of the file;
  - backwards from the record preceding the one at which the record pointer is set (unless the record pointer is set to the first record).

If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action.

NOTE 1: It is not possible, at present, to have more than 255 records in a file of this type, and each record cannot be greater than 255 bytes.

NOTE 2: This structure was previously referred to as "formatted" in GSM.

6.4.3 Cyclic EF

Cyclic files are used for storing records in chronological order. When all records have been used for storage, then the next storage of data shall overwrite the oldest information.

An EF with a cyclic structure consists of a fixed number of records with the same (fixed) length. In this file structure there is a link between the last record (n) and the first record. When the record pointer is set to the last record n, then the next record is record 1. Similarly, when the record pointer is set to record 1, then the previous record is record n. The last updated record containing the newest data is record number 1, and the oldest data is held in record number n.

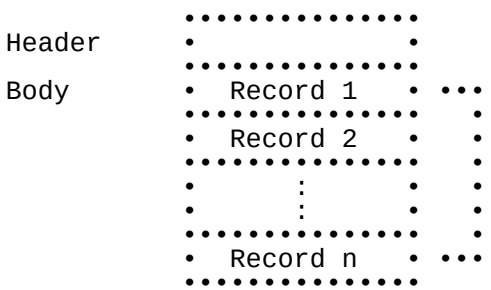


Figure 5: Structure of a cyclic file

For update operations only PREVIOUS record shall be used. For reading operations, the methods of addressing are Next, Previous, Current and Record Number.

After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last. If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action.

NOTE: It is not possible, at present, to have more than 255 records in a file of this type, and each record cannot be greater than 255 bytes.

6.5 Methods for selecting a file

After the Answer To Reset (ATR), the Master File (MF) is implicitly selected and becomes the Current Directory. Each file may then be selected by using the SELECT function in accordance with the following rules.

Selecting a DF or the MF sets the Current Directory. After such a selection there is no current EF. Selecting an EF sets the current EF and the Current Directory remains the DF or MF which is the parent of this EF. The current EF is always a child of the Current Directory.

Any application specific command shall only be operable if it is specific to the Current Directory.

The following files may be selected from the last selected file:

- any file which is an immediate child of the Current Directory;
- any DF which is an immediate child of the parent of the current DF;
- the parent of the Current Directory;
- the current DF;
- the MF.

This means in particular that a DF shall be selected prior to the selection of any of its EFs. All selections are made using the file ID.

The following figure gives the logical structure for the GSM application. GSM defines only one level of DFs under the MF.

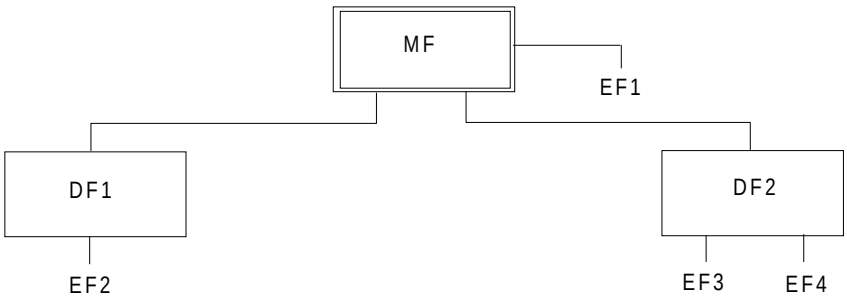


Figure 6: Logical structure

The following table gives the valid selections for GSM for the logical structure in figure 6. Reselection of the last selected file is also allowed but not shown.

Table 6: File selection

Last selected file	Valid Selections
MF	DF1, DF2, EF1
DF1	MF, DF2, EF2
DF2	MF, DF1, EF3, EF4
EF1	MF, DF1, DF2
EF2	MF, DF1, DF2
EF3	MF, DF1, DF2, EF4
EF4	MF, DF1, DF2, EF3

6.6 Reservation of file IDs

In addition to the identifiers used for the files specified in this ETS, the following file IDs are reserved for use by GSM.

Dedicated Files:
- administrative use:
  '7F 4X';
- operational use:
  '7F 10' ($DF_{TELECOM}$), '7F 20' (DF_{GSM}), '7F 21' ($DF_{DCS1800}$), '7F 22' (DF_{IS41}) and '7F 2X', where X ranges from '3' to 'F'.

Elementary files:
- administrative use:
  '6F XX' in the DFs '7F 4X';
  '6F 1X' in the DFs '7F 10', '7F 20', '7F 21';
  '2F 01', '2F EX' in the MF '3F 00';
- operational use:
  '6F 2X', '6F 3X', '6F 4X' in '7F 10' and '7F 2X';
  '2F 1X' in the MF '3F 00'.

In all the above X ranges, unless otherwise stated, from '0' to 'F'.

7 Security features

The security aspects of GSM are described in the normative references GSM 02.09 [4] and GSM 03.20 [10]. This clause gives information related to security features supported by the SIM to enable the following:

- authentication of the subscriber identity to the network;
- data confidentiality over the air interface;
- file access conditions.

7.1 Authentication and cipher key generation procedure

This subclause describes the authentication mechanism and cipher key generation which are invoked by the network. For the specification of the corresponding procedures across the SIM/ME interface, see clause 11.

The network sends a Random Number (RAND) to the MS. The ME passes the RAND to the SIM in the command RUN GSM ALGORITHM. The SIM returns the values SRES and Kc to the ME which are derived using the algorithms and processes given below. The ME sends SRES to the network. The network compares this value with the value of SRES which it calculates for itself. The comparison of these SRES values provides the authentication. The value Kc is used by the ME in any future enciphered communications with the network until the next invocation of this mechanism.

A subscriber authentication key Ki is used in this procedure. This key Ki has a length of 128 bits and is stored within the SIM for use in the algorithms described below.

7.2 Algorithms and processes

The names and parameters of the algorithms supported by the SIM are defined in GSM 03.20 [10]. These are:

- Algorithm A3 to authenticate the MS to the network;
- Algorithm A8 to generate the encryption key.

These algorithms may exist either discretely or combined (into A38) within the SIM. In either case the output on the SIM/ME interface is 12 bytes. The inputs to both A3 and A8, or A38, are Ki (128 bits) internally derived in the SIM, and RAND (128 bits) across the SIM/ME interface. The output is SRES (32 bits)/Kc (64 bits) the coding of which is defined in the command RUN GSM ALGORITHM in clause 9.

7.3 File access conditions

Every file has its own specific access condition for each command. The relevant access condition of the last selected file shall be fulfilled before the requested action can take place.

For each file:

- the access conditions for the commands READ and SEEK are identical;
- the access conditions for the commands SELECT and STATUS are ALWays.

No file access conditions are currently assigned by GSM to the MF and the DFs.

The access condition levels are defined in the following table:

Table 7: Access condition level coding

Level	Access Condition
0	ALWays
1	CHV1
2	CHV2
3	Reserved for GSM Future Use
4 to 14	ADM
15	NEVer

The meaning of the file access conditions is as follows:

ALWAYS: the action can be performed without any restriction;

CHV1 (card holder verification 1): the action shall only be possible if one of the following three conditions is fulfilled:

- a correct CHV1 value has already been presented to the SIM during the current session;
- the CHV1 enabled/disabled indicator is set to "disabled";
- UNBLOCK CHV1 has been successfully performed during the current session;

CHV2: the action shall only be possible if one of the following two conditions is fulfilled:

- a correct CHV2 value has already been presented to the SIM during the current session;
- UNBLOCK CHV2 has been successfully performed during the current session;

ADM: allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority;

The definition of access condition ADM does not preclude the administrative authority from using ALW, CHV1, CHV2 and NEV if required.

NEVER: the action cannot be performed over the SIM/ME interface. The SIM may perform the action internally.

Condition levels are not hierarchical. For instance, correct presentation of CHV2 does not allow actions to be performed which require presentation of CHV1. A condition level which has been satisfied remains valid until the end of the GSM session as long as the corresponding secret code remains unblocked, i.e. after three consecutive wrong attempts, not necessarily in the same card session, the access rights previously granted by this secret code are lost immediately. A satisfied CHV condition level applies to both DF_{GSM} and $DF_{TELECOM}$.

The ME shall determine whether CHV2 is available by using the response to the STATUS command. If CHV2 is "not initialized" then CHV2 commands, e.g. VERIFY CHV2, shall not be executable.

8 Description of the functions

This clause gives a functional description of the commands and their respective responses. Associated status conditions, error codes and their corresponding coding are specified in clause 9.

It shall be mandatory for all cards complying with this Standard to support all functions described in this Standard. The command GET RESPONSE which is needed for the protocol T=0 is specified in clause 9.

The following table lists the file types and structures together with the functions which may act on them during a GSM session. These are indicated by an asterisk (*).

Table 8: Functions on files in GSM session

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

8.1 SELECT

This function selects a file according to the methods described in clause 6. After a successful selection the record pointer in a linear fixed file is undefined. The record pointer in a cyclic file shall address the last record which has been updated or increased.

Input:
- file ID.

Output:
- if the selected file is the MF or a DF:
  file ID, total memory space available, CHV enabled/disabled indicator, CHV status and other GSM specific data;
- if the selected file is an EF:
  file ID, file size, access conditions, invalidated/not invalidated indicator, structure of EF and length of the records in case of linear fixed structure or cyclic structure.

8.2 STATUS

This function returns information concerning the current directory. A current EF is not affected by the STATUS function.

Input:
- none.

Output:
- file ID, total memory space available, CHV enabled/disabled indicator, CHV status and other GSM specific data (identical to SELECT above).

8.3 READ BINARY

This function reads a string of bytes from the current transparent EF. This function shall only be performed if the READ access condition for this EF is satisfied.

Input:
- relative address and the length of the string.

Output:
- string of bytes.

8.4 UPDATE BINARY

This function updates the current transparent EF with a string of bytes. This function shall only be performed if the UPDATE access condition for this EF is satisfied. An update can be considered as a replacement of the string already present in the EF by the string given in the update command.

Input:
- relative address and the length of the string;
- string of bytes.

Output:
- none.

8.5 READ RECORD

This function reads one complete record in the current linear fixed or cyclic EF. The record to be read is described by the modes below. This function shall only be performed if the READ access condition for this EF is satisfied. The record pointer shall not be changed by an unsuccessful READ RECORD function.

Four modes are defined:

CURRENT: The current record is read. The record pointer is not affected.

ABSOLUTE: The record given by the record number is read. The record pointer is not affected.

NEXT: The record pointer is incremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (next) shall read the first record and set the record pointer to this record.

If the record pointer addresses the last record in a linear fixed EF, READ RECORD (next) shall not cause the record pointer to be changed, and no data shall be read.

If the record pointer addresses the last record in a cyclic EF, READ RECORD (next) shall set the record pointer to the first record in this EF and this record shall be read.

PREVIOUS: The record pointer is decremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (previous) shall read the last record and set the record pointer to this record.

If the record pointer addresses the first record in a linear fixed EF, READ RECORD (previous) shall not cause the record pointer to be changed, and no data shall be read.

If the record pointer addresses the first record in a cyclic EF, READ RECORD (previous) shall set the record pointer to the last record in this EF and this record shall be read.

Input:
- mode, record number (absolute mode only) and the length of the record.

Output:
- the record.

8.6 UPDATE RECORD

This function updates one complete record in the current linear fixed or cyclic EF. This function shall only be performed if the UPDATE access condition for this EF is satisfied. The UPDATE can be considered as a replacement of the relevant record data of the EF by the record data given in the command. The record pointer shall not be changed by an unsuccessful UPDATE RECORD function.

The record to be updated is described by the modes below. Four modes are defined of which only PREVIOUS is allowed for cyclic files:

CURRENT: The current record is updated. The record pointer is not affected.

ABSOLUTE: The record given by the record number is updated. The record pointer is not affected.

NEXT: The record pointer is incremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (next) shall set the record pointer to the first record in this EF and this record shall be updated. If the record pointer addresses the last record in a linear fixed EF, UPDATE RECORD (next) shall not cause the record pointer to be changed, and no record shall be updated.

PREVIOUS: For a linear fixed EF the record pointer is decremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (previous) shall set the record pointer to the last record in this EF and this record shall be updated. If the record pointer addresses the first record in a linear fixed EF, UPDATE RECORD (previous) shall not cause the record pointer to be changed, and no record shall be updated.
For a cyclic EF the record containing the oldest data is updated, the record pointer is set to this record and this record becomes record number 1.

Input:
- mode, record number (absolute mode only) and the length of the record;
- the data used for updating the record.

Output:
- none.

8.7 SEEK

This function searches through the current linear fixed EF to find a record starting with the given pattern. This function shall only be performed if the READ access condition for this EF is satisfied. Two types of SEEK are defined:

Type 1 The record pointer is set to the record containing the pattern, no output is available.

Type 2 The record pointer is set to the record containing the pattern, the output is the record number.

NOTE: A Phase 1 SIM only executes type 1 of the SEEK function.

The SIM shall be able to accept any pattern length from 1 to 16 bytes inclusive. The length of the pattern shall not exceed the record length.

Four modes are defined:

- from the beginning forwards;
- from the end backwards;
- from the next location forwards;
- from the previous location backwards.

If the record pointer has not been previously set (its status is undefined) within the selected linear fixed EF, then the search begins:

- with the first record in the case of SEEK from the next location forwards or
- with the last record in the case of SEEK from the previous location backwards.

After a successful SEEK, the record pointer is set to the record in which the pattern was found. The record pointer shall not be changed by an unsuccessful SEEK function.

Input:
- type and mode;
- pattern;
- length of the pattern.

Output:
- type 1: none;
- type 2: status/record number

8.8 INCREASE

This function adds the value given by the ME to the value of the last increased/updated record of the current cyclic EF, and stores the result into the oldest record. The record pointer is set to this record and this record becomes record number 1. This function shall be used only if this EF has an INCREASE access condition assigned and this condition is fulfilled (see bytes 8 and 10 in the response parameters/data of the current EF, clause 9). The SIM shall not perform the increase if the result would exceed the maximum value of the record (represented by all bytes set to 'FF').

Input:
- the value to be added.

Output:
- value of the increased record;
- value which has been added.

8.9 VERIFY CHV

This function verifies the CHV presented by the ME by comparing it with the relevant one stored in the SIM. The verification process is subject to the following conditions being fulfilled:

- CHV is not disabled;
- CHV is not blocked.

If the access condition for a function to be performed on the last selected file is CHV1 or CHV2, then a successful verification of the relevant CHV is required prior to the use of the function on this file unless the CHV is disabled.

If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3.

If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented. After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Input:
- indication CHV1/CHV2, CHV.

Output:
- none.

8.10 CHANGE CHV

This function assigns a new value to the relevant CHV subject to the following conditions being fulfilled:

- CHV is not disabled;
- CHV is not blocked.

The old and new CHV shall be presented.

If the old CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and the new value for the CHV becomes valid.

If the old CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and the value of the CHV is unchanged. After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been performed successfully on the respective CHV.

Input:
- indication CHV1/CHV2, old CHV, new CHV.

Output:
- none.

8.11 DISABLE CHV

This function may only be applied to CHV1. The successful execution of this function has the effect that files protected by CHV1 are now accessible as if they were marked "ALWAYS". The function DISABLE CHV shall not be executed by the SIM when CHV1 is already disabled or blocked.

If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be disabled.

If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHV1 remains enabled. After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHV1 shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

Input:
- CHV1.

Output:
- none.

8.12 ENABLE CHV

This function may only be applied to CHV1. It is the reverse function of DISABLE CHV. The function ENABLE CHV shall not be executed by the SIM when CHV1 is already enabled or blocked.

If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be enabled.

If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHV1 remains disabled. After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHV1 shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

Input:
- CHV1.

Output:
- none.

8.13 UNBLOCK CHV

This function unblocks a CHV which has been blocked by 3 consecutive wrong CHV presentations. This function may be performed whether or not the relevant CHV is blocked.

If the UNBLOCK CHV presented is correct, the value of the CHV, presented together with the UNBLOCK CHV, is assigned to that CHV, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV is reset to its initial value 10 and the number of remaining CHV attempts for that CHV is reset to its initial value 3. After a successful unblocking attempt the CHV is enabled and the relevant access condition level is satisfied.

If the presented UNBLOCK CHV is false, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV shall be decremented. After 10 consecutive false UNBLOCK CHV presentations, not necessarily in the same card session, the respective UNBLOCK CHV shall be blocked. A false UNBLOCK CHV shall have no effect on the status of the respective CHV itself.

Input:
- indication CHV1/CHV2, the UNBLOCK CHV and the new CHV.

Output:
- none.

8.14 INVALIDATE

This function invalidates the current EF. After an INVALIDATE function the respective flag in the file status shall be changed accordingly. This function shall only be performed if the INVALIDATE access condition for the current EF is satisfied.

An invalidated file shall no longer be available within the application for any function except for the SELECT and the REHABILITATE functions.

Input:
- none.

Output:
- none.

8.15 REHABILITATE

This function rehabilitates the invalidated current EF. After a REHABILITATE function the respective flag in the file status shall be changed accordingly. This function shall only be performed if the REHABILITATE access condition for the current EF is satisfied.

Input:
- none.

Output:
- none.

8.16 RUN GSM ALGORITHM

This function is used during the procedure for authenticating the SIM to a GSM network and to calculate a cipher key. The card runs the specified algorithms A3 and A8 using a 16 byte random number and the subscriber authentication key Ki, which is stored in the SIM. The function returns the calculated response SRES and the cipher key Kc.

The function shall not be executable unless DF_{GSM} has been selected as the Current Directory and a successful CHV1 verification procedure has been performed (see 11.3.1).

Input:
- RAND.

Output:
- SRES, Kc.

The contents of Kc shall be presented to algorithm A5 by the ME in its full 64 bit format as delivered by the SIM.

8.17 SLEEP

This is an obsolete GSM function which was issued by Phase 1 MEs. The function shall not be used by an ME of Phase 2 or later.

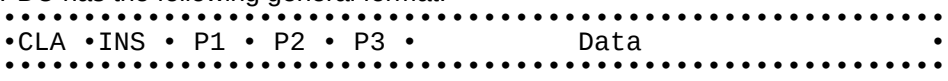
9 Description of the commands

This clause states the general principles for mapping the functions described in clause 8 onto Application Protocol Data Units which are used by the transmission protocol.

9.1 Mapping principles

An APDU can be a command APDU or a response APDU.

A command APDU has the following general format:



The response APDU has the following general format:

An APDU is transported by the T=0 transmission protocol without any change. Other protocols might embed an APDU into their own transport structure (ISO/IEC 7816-3 [25]).

The bytes have the following meaning:

- CLA is the class of instruction (ISO/IEC 7816-3 [25]), 'A0' is used in the GSM application;
- INS is the instruction code (ISO/IEC 7816-3 [25]) as defined in this subclause for each command;
- P1, P2, P3 are parameters for the instruction. They are specified in table 9. 'FF' is a valid value for P1, P2 and P3. P3 gives the length of the data element. P3='00' introduces a 256 byte data transfer from the SIM in an outgoing data transfer command (response direction). In an ingoing data transfer command (command direction), P3='00' introduces no transfer of data.
- SW1 and SW2 are the status words indicating the successful or unsuccessful outcome of the command.

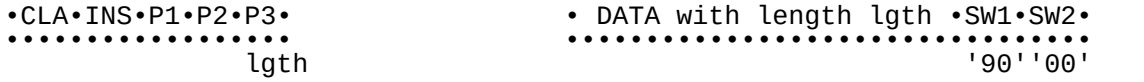
For some of the functions described in clause 8 it is necessary for T=0 to use a supplementary transport service command (GET RESPONSE) to obtain the output data. For example, the SELECT function needs the following two commands:

- the first command (SELECT) has both parameters and data serving as input for the function;
- the second command (GET RESPONSE) has a parameter indicating the length of the data to be returned.

If the length of the response data is not known beforehand, then its correct length may be obtained by applying the first command and interpreting the status words. SW1 shall be '9F' and SW2 shall give the total length of the data. Other status words may be present in case of an error. The various cases are:

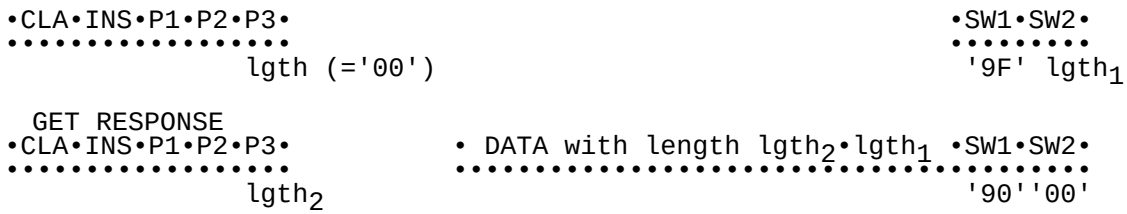
Case 1: No input / No output

Case 2: No input / Output of known length

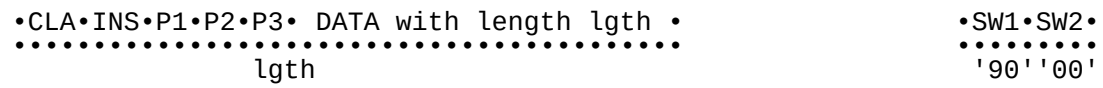


NOTE: lgth='00' causes a data transfer of 256 bytes.

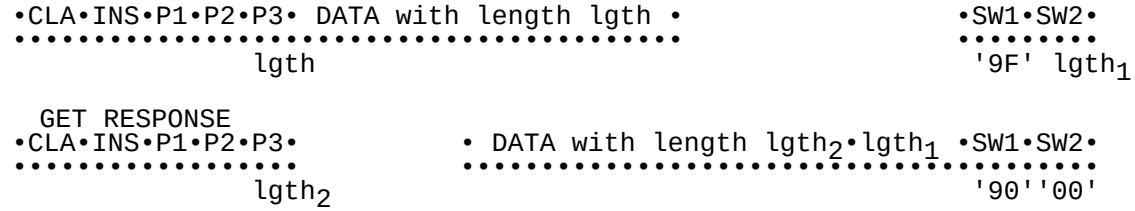
Case 3: No Input / Output of unknown length



Case 4: Input / No output



Case 5: Input / Output of known or unknown length



For cases 3 and 5, when SW1/SW2 indicates there is response data (i.e. SW1/SW2 = '9FXX'), then, if the ME requires to get this response data, it shall send a GET RESPONSE command as described in the relevant case above.

If the GSM application is one of several applications in a multi-application card, other commands with CLA not equal to 'A0' may be sent by the terminal. This shall not influence the state of the GSM application.

9.2 Coding of the commands

Table 9 below gives the coding of the commands. The direction of the data is indicated by (S) and (R), where (S) stands for data sent by the ME while (R) stands for data received by the ME. Offset is coded on 2 bytes where P1 gives the high order byte and P2 the low order byte. '00 00' means no offset and reading/updating starts with the first byte while an offset of '00 01' means that reading/updating starts with the second byte, ...

In addition to the instruction codes specified in table 9 the following codes are reserved:

GSM operational phase:
'1X' with X even.

Administrative management phase:
'2A', 'D0', 'D2', 'DE', 'C4', 'C6', 'C8', 'CA', 'CC', 'B4', 'B6', 'B8', 'BA' and 'BC'.

Table 9: Coding of the commands

COMMAND	INS	P1	P2	P3	S/R
SELECT	'A4'	'00'	'00'	'02'	S/R
STATUS	'F2'	'00'	'00'	lgth	R
READ BINARY	'B0'	offset high	offset low	lgth	R
UPDATE BINARY	'D6'	offset high	offset low	lgth	S
READ RECORD	'B2'	rec No.	mode	lgth	R
UPDATE RECORD	'DC'	rec No.	mode	lgth	S
SEEK	'A2'	'00'	type/mode	lgth	S/R
INCREASE	'32'	'00'	'00'	'03'	S/R
VERIFY CHV	'20'	'00'	CHV No.	'08'	S
CHANGE CHV	'24'	'00'	CHV No.	'10'	S
DISABLE CHV	'26'	'00'	'01'	'08'	S
ENABLE CHV	'28'	'00'	'01'	'08'	S
UNBLOCK CHV	'2C'	'00'	see NOTE	'10'	S
INVALIDATE	'04'	'00'	'00'	'00'	-
REHABILITATE	'44'	'00'	'00'	'00'	-
RUN GSM ALGORITHM	'88'	'00'	'00'	'10'	S/R
SLEEP	'FA'	'00'	'00'	'00'	-
GET RESPONSE	'C0'	'00'	'00'	lgth	R

NOTE: If the UNBLOCK CHV command applies to CHV1 then P2 is coded '00'; if it applies to CHV2 then P2 is coded '02'.

Definitions and codings used in the response parameters/data of the commands are given in subclause 9.3.

9.2.1 SELECT

COMMAND	CLASS	INS	P1	P2	P3
SELECT	'A0'	'A4'	'00'	'00'	'02'

Command parameters/data:

Byte(s)	Description	Length
1 - 2	File ID	2

Response parameters/data in case of an MF or DF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	Total amount of memory of the selected directory which is not allocated to any of the DFs or EFs under the selected directory	2
5 - 6	File ID	2
7	Type of file (see subclause 9.3)	1
8 - 12	RFU	5
13	Length of the following data (byte 14 to the end)	1
14 - 34	GSM specific data	21

GSM specific data:

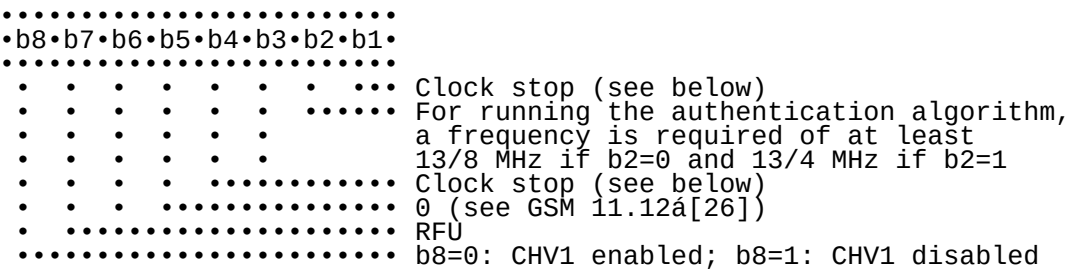
Byte(s)	Description	Length
14	File characteristics (see detail 1)	1
15	Number of DFs which are a direct child of the current directory	1
16	Number of EFs which are a direct child of the current directory	1
17	Number of CHVs, UNBLOCK CHVs and administrative codes	1
18	RFU	1
19	CHV1 status (see detail 2)	1
20	UNBLOCK CHV1 status (see detail 2)	1
21	CHV2 status (see detail 2)	1
22	UNBLOCK CHV2 status (see detail 2)	1
23	RFU	1
24 - 34	Reserved for the administrative management (optional)	0•lgth•11

NOTE 1: Byte 35 and following are RFU.

NOTE 2: The STATUS information of the MF, DF_{GSM} and $DF_{TELECOM}$ provide some identical application specific data, e.g. CHV status. On a multi-application card the MF should not contain any application specific data. Such data is obtained by terminals from the specific application directories. ME manufacturers should take this into account and therefore not use application specific data which may exist in the MF of a mono-application SIM.

Similarly, the Verify CHV command should not be executed in the MF but in the relevant application directory (e.g. DF_{GSM}).

Detail 1: File characteristics



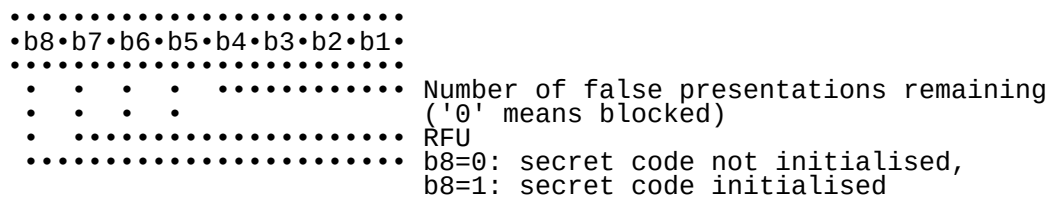
The coding of the conditions for stopping the clock is as follows:

Bit b1	Bit b3	Bit b4	
1	0	0	clock stop allowed, no preferred level
1	1	0	clock stop allowed, high level preferred
1	0	1	clock stop allowed, low level preferred
0	0	0	clock stop not allowed
0	1	0	clock stop not allowed, unless at high level
0	0	1	clock stop not allowed, unless at low level

If bit b1 (column 1) is coded 1, stopping the clock is allowed at high or low level. In this case columns 2 (bit b3) and 3 (bit b4) give information about the preferred level (high or low, resp.) at which the clock may be stopped.

If bit b1 is coded 0, the clock may be stopped only if the mandatory condition in column 2 (b3=1, i.e. stop at high level) or column 3 (b4=1, i.e. stop at low level) is fulfilled. If all 3 bits are coded 0, then the clock shall not be stopped.

Detail 2: Status byte of a secret code



Response parameters/data in case of an EF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	File size (for transparent EF: the length of the body part of the EF) (for linear fixed or cyclic EF: record length multiplied by the number of records of the EF)	2
5 - 6	File ID	2
7	Type of file (see 9.3)	1
8	see detail 3	1
9 - 11	Access conditions (see 9.3)	3
12	File status (see 9.3)	1
13	Length of the following data (byte 14 to the end)	1
14	Structure of EF (see 9.3)	1
15	Length of a record (see detail 4)	1

NOTE: Byte 16 and following are RFU.

Detail 3: Byte 8

For transparent and linear fixed EFs this byte is RFU. For a cyclic EF all bits except bit 7 are RFU; b7=1 indicates that the INCREASE command is allowed on the selected cyclic file.

Detail 4: Byte 15

For cyclic and linear fixed EFs this byte denotes the length of a record. For a transparent EF, this byte shall be coded '00', if this byte is sent by the SIM.

9.2.2 STATUS

COMMAND	CLASS	INS	P1	P2	P3
STATUS	'A0'	'F2'	'00'	'00'	lgth

The response parameters/data are identical to the response parameters/data of the SELECT command in case of an MF or DF.

9.2.3 READ BINARY

COMMAND	CLASS	INS	P1	P2	P3
READ BINARY	'A0'	'B0'	offset high	offset low	lgth

Response parameters/data:

Byte(s)	Description	Length
1 - lgth	Data to be read	lgth

9.2.4 UPDATE BINARY

COMMAND	CLASS	INS	P1	P2	P3
UPDATE BINARY	'A0'	'D6'	offset high	offset low	lgth

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Data	lgth

9.2.5 READ RECORD

COMMAND	CLASS	INS	P1	P2	P3
READ RECORD	'A0'	'B2'	Rec.No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode, the record number is given in P1 with P1='00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the ME. To ensure phase compatibility between Phase 2 SIMs and Phase 1 MEs, the SIM shall not interpret the value given by the ME.

Response parameters/data:

Byte(s)	Description	Length
1 - lgth	The data of the record	lgth

9.2.6 UPDATE RECORD

COMMAND	CLASS	INS	P1	P2	P3
UPDATE RECORD	'A0'	'DC'	Rec.No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode; the record number is given in P1 with P1='00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the ME. To ensure phase compatibility between Phase 2 SIMs and Phase 1 MEs, the SIM shall not interpret the value given by the ME.

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Data	lgth

9.2.7 SEEK

COMMAND	CLASS	INS	P1	P2	P3
SEEK	'A0'	'A2'	'00'	Type/Mode	lgth

Parameter P2 specifies type and mode:

- 'x0' = from the beginning forward;
- 'x1' = from the end backward;
- 'x2' = from the next location forward;
- 'x3' = from the previous location backward

with x='0' specifies type 1 and x='1' specifies type 2 of the SEEK command.

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Pattern	lgth

There are no response parameters/data for a type 1 SEEK. A type 2 SEEK returns the following response parameters/data:

Byte(s)	Description	Length
1	Record number	1

9.2.8 INCREASE

COMMAND	CLASS	INS	P1	P2	P3
INCREASE	'A0'	'32'	'00'	'00'	'03'

Command parameters/data:

Byte(s)	Description	Length
1 - 3	Value to be added	3

Response parameters/data:

Byte(s)	Description	Length
1 - X	Value of the increased record	X
X+1 - X+3	Value which has been added	3

NOTE: X denotes the length of the record.

9.2.9 VERIFY CHV

COMMAND	CLASS	INS	P1	P2	P3
VERIFY CHV	'A0'	'20'	'00'	CHV No.	'08'

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV value	8

9.2.10 CHANGE CHV

COMMAND	CLASS	INS	P1	P2	P3
CHANGE CHV	'A0'	'24'	'00'	CHV No.	'10'

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	Old CHV value	8
9 - 16	New CHV value	8

9.2.11 DISABLE CHV

COMMAND	CLASS	INS	P1	P2	P3
DISABLE CHV	'A0'	'26'	'00'	'01'	'08'

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV1 value	8

9.2.12 ENABLE CHV

COMMAND	CLASS	INS	P1	P2	P3
ENABLE CHV	'A0'	'28'	'00'	'01'	'08'

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV1 value	8

9.2.13 UNBLOCK CHV

COMMAND	CLASS	INS	P1	P2	P3
UNBLOCK CHV	'A0'	'2C'	'00'	CHV No.	'10'

Parameter P2 specifies the CHV:

- 00 = CHV1;
- 02 = CHV2.

NOTE: The coding '00' for CHV1 differs from the coding of CHV1 used for other commands.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	UNBLOCK CHV value	8
9 - 16	New CHV value	8

9.2.14 INVALIDATE

COMMAND	CLASS	INS	P1	P2	P3
INVALIDATE	'A0'	'04'	'00'	'00'	'00'

9.2.15 REHABILITATE

COMMAND	CLASS	INS	P1	P2	P3
REHABILITATE	'A0'	'44'	'00'	'00'	'00'

9.2.16 RUN GSM ALGORITHM

COMMAND	CLASS	INS	P1	P2	P3
RUN GSM ALGORITHM	'A0'	'88'	'00'	'00'	'10'

Command parameters/data:

Byte(s)	Description	Length
1 - 16	RAND	16

Response parameters/data:

Byte(s)	Description	Length
1 - 4	SRES	4
5 - 12	Cipher Key Kc	8

The most significant bit of SRES is coded on bit 8 of byte 1. The most significant bit of Kc is coded on bit 8 of byte 5.

9.2.17 SLEEP

COMMAND	CLASS	INS	P1	P2	P3
SLEEP	'A0'	'FA'	'00'	'00'	'00'

NOTE: This command is used by Phase 1 MEs only.

9.2.18 GET RESPONSE

COMMAND	CLASS	INS	P1	P2	P3
GET RESPONSE	'A0'	'C0'	'00'	'00'	lgth

The response data depends on the preceding command. Response data is available after the commands RUN GSM ALGORITHM, SEEK (type 2), SELECT, and INCREASE. If the command GET RESPONSE is executed, it is required that it is executed immediately after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE). If the sequence is not respected, the SIM shall send the status information "technical problem with no diagnostic given" as a reaction to the GET RESPONSE.

Since the MF is implicitly selected after activation of the SIM, GET RESPONSE is also allowed as the first command after activation.

The response data itself is defined in the subclause for the corresponding command.

9.3 Definitions and coding

The following definitions and coding are used in the response parameters/data of the commands.

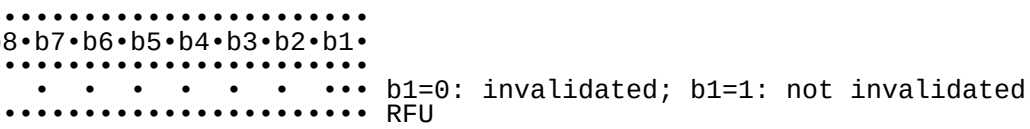
Coding

Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation the leftmost bit is the MSB.

RFU

In a GSM specific card all bytes which are RFU shall be set to '00' and RFU bits to 0. Where the GSM application exists on a multiapplication card or is built on a generic telecommunications card (e.g. TE9) then other values may apply. The values will be defined in the appropriate specifications for such cards. These bytes and bits shall not be interpreted by an ME in a GSM session.

File status



Structure of file

- '00' transparent;
- '01' linear fixed;
- '03' cyclic.

Type of File

- '00' RFU;
- '01' MF;
- '02' DF;
- '04' EF.

Coding of CHVs and UNBLOCK CHVs

A CHV is coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [19] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented CHV with 'FF' before sending it to the SIM.

The coding of the UNBLOCK CHVs is identical to the coding of the CHVs. However, the number of (decimal) digits is always 8.

Coding of Access Conditions

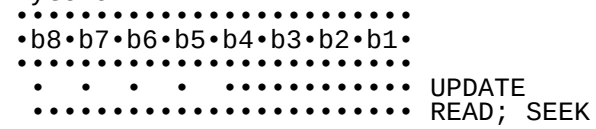
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command. Each condition is coded on 4 bits as shown in table 10.

Table 10: Access conditions

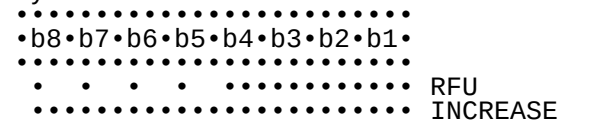
ALW	'0'*
CHV1	'1'*
CHV2	'2'*
RFU	'3'
ADM	'4'
.....	..
ADM	'E'
NEV	'F'*

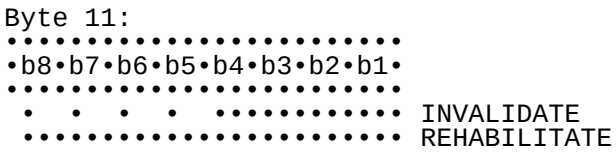
Entries marked "*" in the table above are also available for use as administrative codes in addition to the ADM access levels '4' to 'E' (refer to clause 7.3) if required by the appropriate administrative authority. If any of these access conditions are used, the code returned in Access Condition bytes in the response data shall be the code applicable to that particular level.

Byte 9:



Byte 10:





9.4 Status conditions returned by the card

This subclause specifies the coding of the status words SW1 and SW2.

9.4.1 Responses to commands which are correctly executed

SW1	SW2	Description
'90'	'00'	- normal ending of the command
'9F'	'XX'	- length 'XX' of the response data

9.4.2 Memory management

SW1	SW2	Error description
'92'	'0X'	- update successful but after using an internal retry routine 'X' times
'92'	'40'	- memory problem

9.4.3 Referencing management

SW1	SW2	Error description
'94'	'00'	- no EF selected
'94'	'02'	- out of range (invalid address)
'94'	'04'	- file ID not found - pattern not found
'94'	'08'	- file is inconsistent with the command

9.4.4 Security management

SW1	SW2	Error description
'98'	'02'	- no CHV initialised
'98'	'04'	- access condition not fulfilled - unsuccessful CHV verification, at least one attempt left - unsuccessful UNBLOCK CHV verification, at least one attempt left - authentication failed (see note)
'98'	'08'	- in contradiction with CHV status
'98'	'10'	- in contradiction with invalidation status
'98'	'40'	- unsuccessful CHV verification, no attempt left - unsuccessful UNBLOCK CHV verification, no attempt left - CHV blocked - UNBLOCK CHV blocked
'98'	'50'	- increase cannot be performed, Max value reached

NOTE: A Phase 1 SIM may send this error code after the third consecutive unsuccessful CHV verification attempt or the tenth consecutive unsuccessful unblocking attempt.

9.4.5 Application independent errors

SW1	SW2	Error description
'67'	'XX'	- incorrect parameter P3 (see note)
'6B'	'XX'#	- incorrect parameter P1 or P2 (see ##)
'6D'	'XX'#	- unknown instruction code given in the command
'6E'	'XX'#	- wrong instruction class given in the command
'6F'	'XX'#	- technical problem with no diagnostic given

These values of 'XX' are specified by ISO/IEC; at present the default value 'XX'='00' is the only one defined.

When the error in P1 or P2 is caused by the addressed record being out of range, then the return code '94 02' shall be used.

NOTE: 'XX' gives the correct length or states that no additional information is given ('XX' = '00').

9.4.6 Commands versus possible status responses

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Table 11: Commands and status words

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

10 Contents of the Elementary Files (EF)

This clause specifies the EFs for the GSM session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in a EF_{ADN} record.

EFs or data items having an unassigned value, or, which during the GSM session, are cleared by the ME, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is "deleted" during a GSM session by the allocation of a value specified in another GSM ETS, then this value shall be used, and the data item is not unassigned; e.g. for a deleted LAI in EF_{LOCI} the last byte takes the value 'FE' (GSM 04.08 [14] refers).

EFs are mandatory (M) or optional (O). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

When the coding is according to CCITT Recommendation T.50 [19], bit 8 of every byte shall be set to 0.

For an overview containing all files see figure 7.

10.1 Contents of the EFs at the MF level

There is only one EF at the MF level.

10.1.1 EF_{ICCID} (ICC Identification)

This EF provides a unique identification number for the SIM.

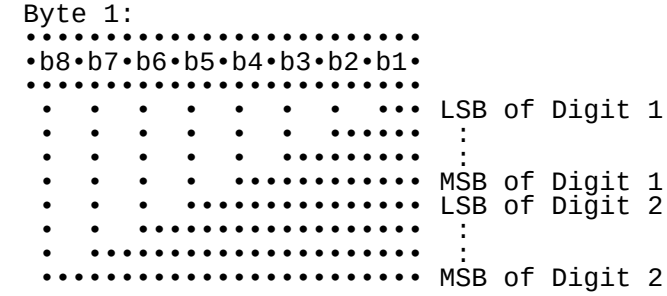
Identifier: '2FE2'	Structure: transparent	Mandatory
File size: 10 bytes	Update activity: low	

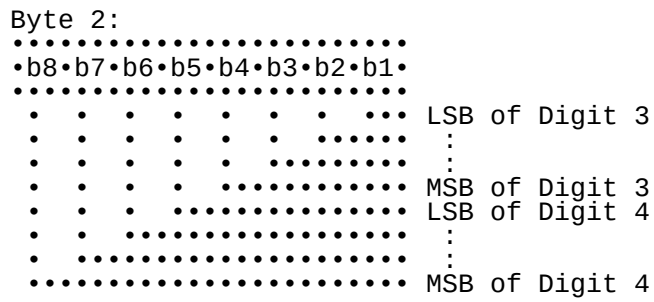
Access Conditions:

READ	ALWAYS
UPDATE	NEVER
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 10	Identification number	M	10 bytes

- Identification number
  Contents: according to CCITT Recommendation E.118 [17]. However, network operators who are already issuing Phase 1 SIM cards with an identification number length of 20 digits may retain this length.
  Purpose: card identification number.
  Coding: BCD, left justified and padded with 'F'; after padding the digits within a byte are swapped (see below). However, network operators who are already issuing Phase 1 SIM cards where the digits within a byte are not swapped may retain this configuration.





etc.

10.2 Contents of files at the GSM application level

The EFs in the Dedicated File DF_{GSM} contain network related information.

10.2.1 EF_{LP} (Language preference)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes and for short message handling (e.g. screening of preferred languages in SMS-CB).

When the CB Message Identifier capability is both allocated and activated the ME selects only those CB messages the language of which corresponds to one of the languages given in this EF. The CB message language is recognized according to GSM 03.41 by its data coding scheme.

Identifier: '6F05'	Structure: transparent	Mandatory
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	1st language code (highest prior.)	M	1 byte
2	2nd language code	O	1 byte
n	nth language code (lowest prior.)	O	1 byte

Coding: according to GSM 03.41 [13].

Using the command GET RESPONSE, the ME can determine the size of the EF.

10.2.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	CHV1

Bytes	Description	M/O	Length
1	length of IMSI	M	1 byte
2 - 9	IMSI	M	8 bytes

- length of IMSI
  Contents: The length indicator refers to the number of significant bytes, not including this length byte, required for the IMSI.
  Coding: according to GSM 04.08 [14].

- IMSI
  Contents: International Mobile Subscriber Identity.
  Coding: This information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

```
Byte 2:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •  •  ••• 1
 •  •  •  •  •  •  •••••• 0
 •  •  •  •  •  •  •••••••• 0
 •  •  •  •  •  ••••••••••• Parity
 •  •  •  •  •••••••••••••• LSB of Digit 1
 •  •  •••••••••••••••••••  :
 •  ••••••••••••••••••••••  :
 •••••••••••••••••••••••••• MSB of Digit 1

For the parity bit, see GSM 04.08á[14].

Byte 3:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •  •  ••• LSB of Digit 2
 •  •  •  •  •  •  •••••  :
 •  •  •  •  •  •••••••••  :
 •  •  •  •  •••••••••••• MSB of Digit 2
 •  •  •  •••••••••••••••• LSB of Digit 3
 •  •  •••••••••••••••••••  :
 •  ••••••••••••••••••••••  :
 •••••••••••••••••••••••••• MSB of Digit 3

etc.
```

10.2.3 EF_{Kc} (Ciphering key Kc)

This EF contains the ciphering key Kc and the ciphering key sequence number n.

Identifier: '6F20'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 8	Ciphering key Kc	M	8 bytes
9	Ciphering key sequence number n	M	1 byte

- Ciphering key Kc
  Coding: The least significant bit of Kc is the least significant bit of the eighth byte. The most significant bit of Kc is the most significant bit of the first byte.

- Ciphering key sequence number n
  Coding:

```
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •••••••• n
 •••••••••••••••••••••••• bits b4 to b8 are coded 0
```

NOTE: GSM 04.08 [14] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

10.2.4 $EF_{PLMNsel}$ (PLMN selector)

This EF contains the coding for n PLMNs, where n is at least eight. This information determined by the user/operator defines the preferred PLMNs of the user in priority order.

Identifier: '6F30'	Structure: transparent	Optional
File size: 3n (n•8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 - 3	1st PLMN (highest priority)	M	3 bytes
22 - 24	8th PLMN	M	3 bytes
25 - 27	9th PLMN	O	3 bytes
(3n-2)-3n	nth PLMN (lowest priority)	O	3 bytes

- PLMN
  Contents: Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding: according to GSM 04.08 [14].
  If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.
  For instance, using 246 for the MCC and 81 for the MNC and if this is the first and only PLMN, the contents reads as follows:
  Bytes 1-3: '42' 'F6' '18'
  Bytes 4-6: 'FF' 'FF' 'FF'
  etc.

10.2.5 EF_{HPLMN} (HPLMN search period)

This EF contains the interval of time between searches for the HPLMN (see GSM 02.11 [5]).

Identifier: '6F31'	Structure: transparent	Mandatory
File size: 1 byte	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Time interval	M	1 byte

- Time interval
  Contents: The time interval between two searches.
  Coding: The time interval is coded in integer multiples of n minutes. The range is from n minutes to a maximum value. The value '00' indicates that no attempts shall be made to search for the HPLMN. The encoding is:

  - '00': No HPLMN search attempts
  - '01': n minutes
  - '02': 2n minutes
  - : :
  - 'YZ': (16Y+Z)n minutes (maximum value)

  All other values shall be interpreted by the ME as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to GSM 02.11 [5].

10.2.6 EF_{ACMmax} (ACM maximum value)

This EF contains the maximum value of the accumulated call meter. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F37'	Structure: transparent	Optional
File size: 3 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 3	Maximum value	M	3 bytes

- Maximum value
  Contents: maximum value of the Accumulated Call Meter (ACM)
  Coding:

```
First byte:
•••••••••••••••••••••••••••••••••
•b8 •b7 •b6 •b5 •b4 •b3 •b2 •b1 •
•••••••••••••••••••••••••••••••••
 •   •   •   •   •   •   •   •
 2^23 2^22 2^21 2^20 2^19 2^18 2^17 2^16

Second byte:
•••••••••••••••••••••••••••••••••
•b8 •b7 •b6 •b5 •b4 •b3 •b2 •b1 •
•••••••••••••••••••••••••••••••••
 •   •   •   •   •   •   •   •
 2^15 2^14 2^13 2^12 2^11 2^10 2^9  2^8

Third byte:
•••••••••••••••••••••••••••••••••
•b8 •b7 •b6 •b5 •b4 •b3 •b2 •b1 •
•••••••••••••••••••••••••••••••••
 •   •   •   •   •   •   •   •
 2^7  2^6  2^5  2^4  2^3  2^2  2^1  2^0
```

  For instance, '00' '00' '30' represents 2^5+2^4.

All ACM data is stored in the SIM and transmitted over the SIM/ME interface as binary.

ACMmax is not valid, as defined in GSM 02.24 [7], if it is coded '000000'.

10.2.7 EF_{SST} (SIM service table)

This EF indicates which services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the SIM, the ME shall not select this service.

Identifier: '6F38'	Structure: transparent	Mandatory
File size: X bytes, X•2	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Services n°1 to n°4	M	1 byte
2	Services n°5 to n°8	M	1 byte
3	Services n°9 to n°12	O	1 byte
4	Services n°13 to n°16	O	1 byte
5	Services n°17 to n°20	O	1 byte
etc.			
X	Services (4X-3) to (4X)	O	1 byte

- Services
  Contents:
  - Service n°1 : CHV1 disable function
  - Service n°2 : Abbreviated Dialling Numbers (ADN)
  - Service n°3 : Fixed Dialling Numbers (FDN)
  - Service n°4 : Short Message Storage (SMS)
  - Service n°5 : Advice of Charge (AoC)
  - Service n°6 : Capability Configuration Parameters (CCP)
  - Service n°7 : PLMN selector
  - Service n°8 : RFU
  - Service n°9 : MSISDN
  - Service n°10: Extension1
  - Service n°11: Extension2
  - Service n°12: SMS Parameters
  - Service n°13: Last Number Dialled (LND)
  - Service n°14: Cell Broadcast Message Identifier
  - Service n°15: Group Identifier Level 1
  - Service n°16: Group Identifier Level 2
  - Service n°17: Service Provider Name

For a phase 2 SIM, the EF shall contain at least two bytes which correspond to the Phase 1 services. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of ETSI.

NOTE: Service N°8 was used in Phase 1 for Called Party Subaddress. To prevent any risk of incompatibility Service N°8 should not be reallocated.

Coding:

2 bits are used to code each service:
first bit = 1: service allocated
first bit = 0: service not allocated
where the first bit is b1, b3, b5 or b7;
second bit = 1: service activated
second bit = 0: service not activated
where the second bit is b2, b4, b6 or b8.

Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see section 9.3.

```
First byte:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •  •••••• Service n°1
 •  •  •  •  •••••••••••• Service n°2
 •  •  ••••••••••••••••• Service n°3
 •••••••••••••••••••••••• Service n°4

Second byte:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •  •••••• Service n°5
 •  •  •  •  •••••••••••• Service n°6
 •  •  ••••••••••••••••• Service n°7
 •••••••••••••••••••••••• Service n°8
```

etc.

The following example of coding for the first byte means that service n°1 "CHV1-Disabling" is allocated but not activated:

```
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 X  X  X  X  X  X  0  1
```

If the SIM supports the FDN feature (FDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both EF_{IMSI} and EF_{LOCI} once during each GSM session. This mechanism shall be invoked by the SIM automatically if FDN is enabled. This invalidation shall occur at least before the next command following selection of either EF. FDN is enabled when the ADN is invalidated or not activated.

10.2.8 EF_{ACM} (Accumulated call meter)

This EF contains the total number of units for both the current call and the preceding calls.

NOTE: The information may be used to provide an indication to the user for advice or as a basis for the calculation of the monetary cost of calls (see GSM 02.86 [9]).

Identifier: '6F39'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INCREASE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 3	Accumulated count of units	M	3 bytes

- Accumulated count of units
  Contents: value of the ACM
  Coding: see the coding of EF_{ACMmax}

10.2.9 EF_{GID1} (Group Identifier Level 1)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3E'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - n	SIM group identifier(s)	O	n bytes

10.2.10 EF_{GID2} (Group Identifier Level 2)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3F'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - n	SIM group identifier(s)	O	n bytes

NOTE: The structure of EF_{GID1} and EF_{GID2} are identical. They are provided to allow the network operator to enforce different levels of security dependant on application.

10.2.11 EF_{SPN} (Service Provider Name)

This EF contains the service provider name and appropriate requirements for the display by the ME.

Identifier: '6F46'	Structure: transparent	Optional
File Size: 17 bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Display Condition	M	1 byte
2 - 17	Service Provider Name	M	16 bytes

- Display Condition
  Contents: display condition for the service provider name in respect to the registered PLMN (see GSM 02.07 [3])

Coding: see below

Byte 1:

Bit	b1	
	0	: display of registered PLMN not required
	1	: display of registered PLMN required

Bits b2 to b8 are RFU (see subclause 9.3)

- Service Provider Name

  Contents: service provider string to be displayed

  Coding: the string shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [11] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'.

10.2.12 EF_{PUCT} (Price per unit and currency table)

This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in GSM 02.24 [7]. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F41'	Structure: transparent	Optional
File size: 5 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 3	Currency code	M	3 bytes
4 - 5	Price per unit	M	2 bytes

- Currency code

  Contents: the alpha-identifier of the currency code.

  Coding: bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [11] with bit 8 set to 0.

- Price per unit

  Contents: price per unit expressed in the currency coded by bytes 1-3.

  Coding: Byte 4 and bits b1 to b4 of byte 5 represent the Elementary Price per Unit (EPPU) in the currency coded by bytes 1-3. Bits b5 to b8 of byte 5 are the decimal logarithm of the multiplicative factor represented by the absolute value of its decimal logarithm (EX) and the sign of EX, which is coded 0 for a positive sign and 1 for a negative sign.

```
Byte 4:
•••••••••••••••••••••••••••••••••
•b8 •b7 •b6 •b5 •b4 •b3 •b2 •b1 •
•••••••••••••••••••••••••••••••••
 •   •   •   •   •   •   •   •
 2^11 2^10 2^9  2^8  2^7  2^6  2^5  2^4   of EPPU

Byte 5:
•••••••••••••••••••••••••••••••••
•b8 •b7 •b6 •b5 •b4 •b3 •b2 •b1 •
•••••••••••••••••••••••••••••••••
 •   •   •   •   •   •   •   •
 •   •   •   •   2^3  2^2  2^1  2^0   of EPPU
 •   •   •   ••••••••••••••••••••• Sign of EX
 •   •   ••••••••••••••••••••••••• 2^0 of Abs(EX)
 •   ••••••••••••••••••••••••••••• 2^1 of Abs(EX)
 ••••••••••••••••••••••••••••••••• 2^2 of Abs(EX)
```

The computation of the price per unit value is made by the ME in compliance with GSM 02.24 [7] by the following formula:

price per unit = EPPU * 10^{EX}.

The price has to be understood as expressed in the coded currency.

10.2.13 EF_{CBMI} (Cell broadcast message identifier selection)

This EF contains the Message Identifier Parameters which specify the type of content of the cell broadcast messages that the subscriber wishes the MS to accept.

Any number of CB Message Identifier Parameters may be stored in the SIM. No order of priority is applicable.

Identifier: '6F45'	Structure: transparent	Optional
File size: 2n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 2	CB Message Identifier 1	O	2 bytes
3 - 4	CB Message Identifier 2	O	2 bytes
2n-1 - 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier
  Coding: as in GSM 03.41, "Message Format on BTS-MS Interface - Message Identifier".
  Values listed show the types of message which shall be accepted by the MS.
  Unused entries shall be set to 'FF FF'.

10.2.14 EF_{BCCH} (Broadcast control channels)

This EF contains information concerning the BCCH according to GSM 04.08 [14].

BCCH storage may reduce the extent of a Mobile Station's search of BCCH carriers when selecting a cell. The BCCH carrier lists in an MS shall be in accordance with the procedures specified in GSM 04.08 [14]. The MS shall only store BCCH information from the System Information 2 message and not the 2bis extension message.

Identifier: '6F74'	Structure: transparent	Mandatory
File size: 16 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 16	BCCH information	M	16 bytes

- BCCH information
  Coding: The information is coded as octets 2-17 of the "neighbour cells description information element" in GSM 04.08 [14].

10.2.15 EF_{ACC} (Access control class)

This EF contains the assigned access control class(es). GSM 02.11 [5] refers. The access control class is a parameter to control the RACH utilization. 15 classes are split into 10 classes randomly allocated to

normal subscribers and 5 classes allocated to specific high priority users. For more information see GSM 02.11 [5].

Identifier: '6F78'	Structure: transparent	Mandatory
File size: 2 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 2	Access control classes	M	2 bytes

- Access control classes
  Coding: Each ACC is coded on one bit. An ACC is "allocated" if the corresponding bit is set to 1 and "not allocated" if this bit is set to 0. Bit b3 of byte 1 is set to 0.

```
Byte 1:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 15 14 13 12 11 10 09 08  Number of the ACC (except for bit b3)

Byte 2:
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 07 06 05 04 03 02 01 00  Number of the ACC
```

10.2.16 EF_{FPLMN} (Forbidden PLMNs)

This EF contains the coding for four Forbidden PLMNs (FPLMN). It is read by the ME as part of the SIM initialization procedure and indicates PLMNs which the MS shall not automatically attempt to access.

A PLMN is written to the EF if a network rejects a Location Update with the cause "PLMN not allowed". The ME shall manage the list as follows.

When four FPLMNs are held in the EF, and rejection of a further PLMN is received by the ME from the network, the ME shall modify the EF using the UPDATE command. This new PLMN shall be stored in the fourth position, and the existing list "shifted" causing the previous contents of the first position to be lost.

When less than four FPLMNs exist in the EF, storage of an additional FPLMN shall not cause any existing FPLMN to be lost.

Dependent upon procedures used to manage storage and deletion of FPLMNs in the EF, it is possible, when less than four FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The ME shall analyse all the EF for FPLMNs in any position, and not regard 'FFFFFF' as a termination of valid data.

Identifier: '6F7B'	Structure: transparent	Mandatory
File size: 12 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 3	PLMN 1	M	3 bytes
4 - 6	PLMN 2	M	3 bytes
7 - 9	PLMN 3	M	3 bytes
10 - 12	PLMN 4	M	3 bytes

- PLMN
  Contents: Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding: according to GSM 04.08 [14].
  For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:
  Bytes 7-9: '42' 'F6' '18'
  If storage for fewer than 4 PLMNs is required, the unused bytes shall be set to 'FF'.

10.2.17 EF_{LOCI} (Location information)

This EF contains the following Location Information:

- Temporary Mobile Subscriber Identity (TMSI)
- Location Area Information (LAI)
- TMSI TIME
- Location update status

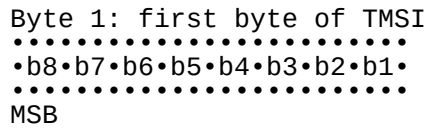
Identifier: '6F7E'	Structure: transparent	Mandatory
File size: 11 bytes	Update activity: high	

Access Conditions:

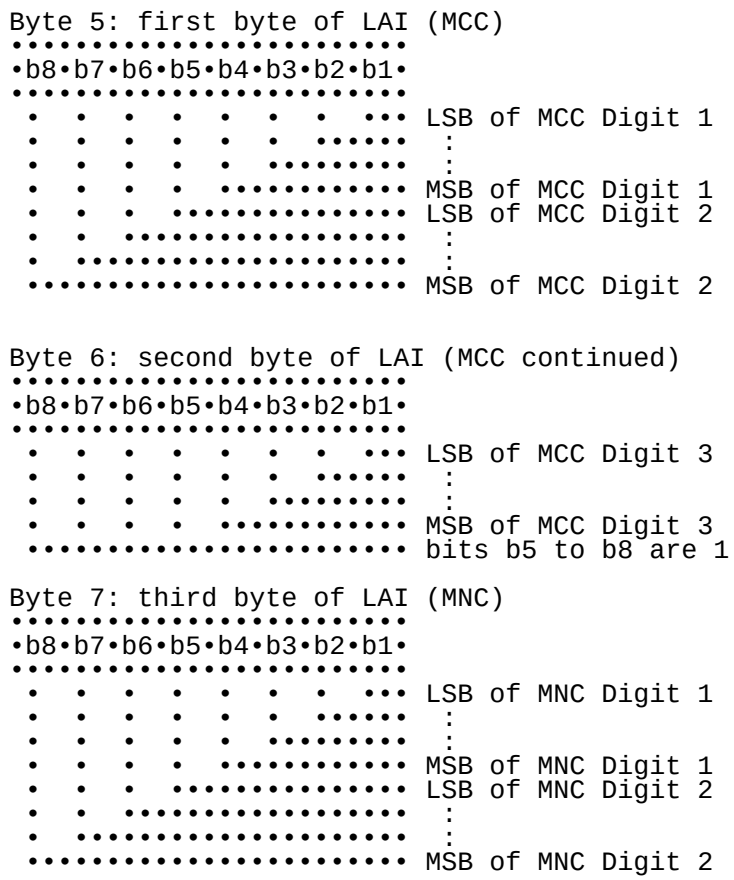
READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	CHV1

Bytes	Description	M/O	Length
1 - 4	TMSI	M	4 bytes
5 - 9	LAI	M	5 bytes
10	TMSI TIME	M	1 byte
11	Location update status	M	1 byte

- TMSI
  Contents: Temporary Mobile Subscriber Identity
  Coding: according to GSM 04.08 [14].



- LAI
  Contents: Location Area Information
  Coding: according to GSM 04.08 [14].



Byte 8: fourth byte of LAI (LAC)
Byte 9: fifth byte of LAI (LAC continued)

- TMSI TIME
  Contents: Current value of Periodic Location Updating Timer (T3212).
  This byte is used by Phase 1 MEs, but it shall not be used by Phase 2 MEs.

- Location update status
  Contents: status of location update according to GSM 04.08 [14].
  Coding:
  Byte 11:

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

  Bits b4 to b8 are RFU (see subclause 9.3).

10.2.18 EF_{AD} (Administrative data)

This EF contains information concerning the mode of operation according to the type of SIM, such as normal (to be used by PLMN subscribers for GSM operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication of whether some ME features should be activated during normal operation.

Identifier: '6FAD'	Structure: transparent	Mandatory
File size: 3+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

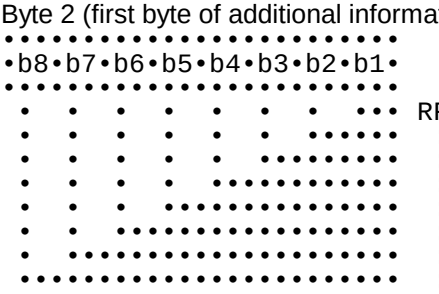
Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 - 3	Additional information	M	2 bytes
4 - 3+X	RFU	O	X bytes

- MS operation mode
  Contents: mode of operation for the MS
  Coding:
  Initial value

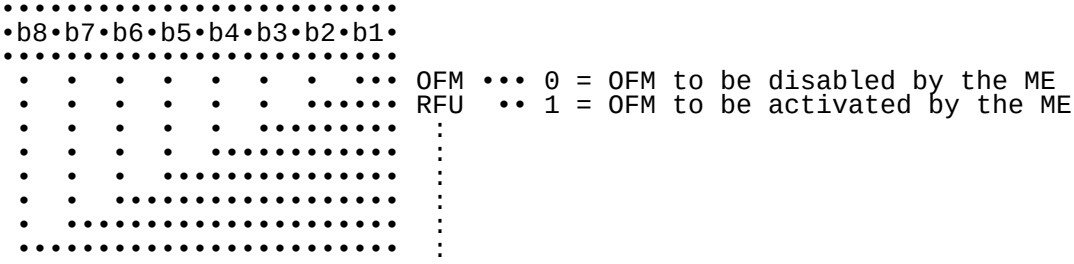
- normal operation	'00'
- type approval operations	'80'
- normal operation + specific facilities	'01'
- type approval operations + specific facilities	'81'
- maintenance (off line)	'02'
- cell test operation	'04'

- Additional information
  Coding:
  - special facility number (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):



  Byte 3:



  - ME manufacturer specific information (if b2=1 in byte 1).

10.2.19 EF_{Phase} (Phase identification)

This EF contains information concerning the phase of the SIM.

Identifier: '6FAE'	Structure: transparent	Mandatory
File size: 1 byte	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	SIM Phase	M	1 byte

- SIM Phase
  Coding:
  Phase 1: '00'
  Phase 2: '02'
  All other codings are reserved for specification by ETSI TC SMG. Codings '03', '04' to '0F' indicate that the SIM supports, as a minimum, the mandatory requirements defined in this specification.

If EF_{Phase} is coded '00', it may be assumed by the ME that some Phase 2 features are supported by this SIM. However, the services n°3 (FDN) and/or n°5 (AoC) shall only be allocated and activated in SIMs of phase 2 with EF_{Phase} being coded '02'.

10.3 Contents of files at the telecom level

The EFs in the Dedicated File $DF_{TELECOM}$ contain service related information.

10.3.1 EF_{ADN} (Abbreviated dialling numbers)

This EF contains Abbreviated Dialling Numbers (ADN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3A'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	CHV2
REHABILITATE	CHV2

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

- Alpha Identifier
  Contents: Alpha-tagging of the associated dialling number.
  Coding: this alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [11] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

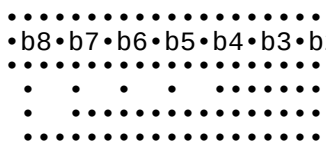
  NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the ME can determine the value of X.

- Length of BCD number/SSC contents

Contents: this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC requires more than 20 digits it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the overflow data being coded in the appropriate overflow record itself (see subclause 10.3.9).
Coding: according to GSM 04.08 [14].

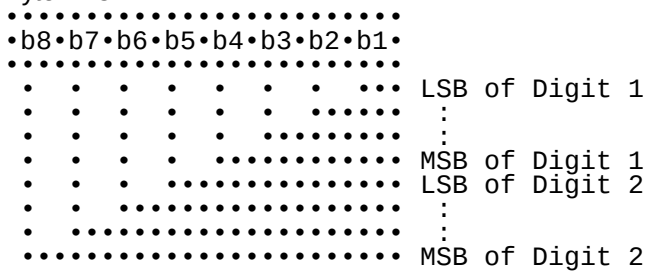
- TON and NPI
Contents: Type of number (TON) and numbering plan identification (NPI).
Coding: according to GSM 04.08 [14]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the air interface (see GSM 04.08 [14]). Accordingly, the ME should not interpret the value 'FF' and not send it over the air interface.

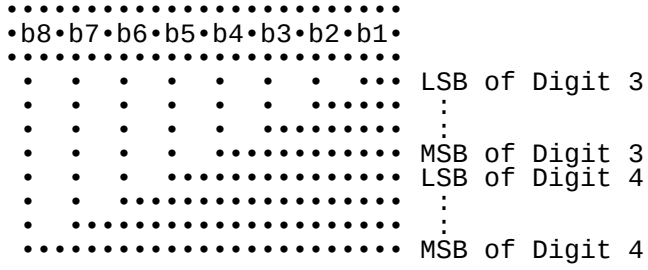


- Dialling Number/SSC String
Contents: up to 20 digits of the telephone number and/or SSC information.
Coding: according to GSM 04.08 [14] , GSM 02.30 [8] and the extended BCD-coding (see table 12). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the overflow data is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3



Byte X+4:



etc.

- Capability/Configuration Identifier
Contents: capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.
Coding: binary.

- Extension1 Record Identifier

Contents: extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or an overflow. The use of this byte is optional. If it is not used it shall be set to 'FF'.
If the ADN/SSC requires both overflow and called party subaddress, this byte identifies the overflow record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see subclause 10.3.9).
Coding: binary.

NOTE 3: As EF_{ADN} is part of the $DF_{TELECOM}$ it may be used by GSM and also other applications in a multi-application card. If the non-GSM application does not recognize the use of Type of Number (TON) and Number Plan Identification (NPI), then the information relating to the national dialling plan must be held within the data item dialling number/SSC and the TON and NPI fields set to UNKNOWN. This format would be acceptable for GSM operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

Example: SIM storage of an International Number using E.164 [18] numbering plan

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

where "abc..." denotes the subscriber number digits (including its country code), and "xxx..." denotes escape digits or a national prefix replacing TON and NPI.

NOTE 4: When the ME acts upon the EF_{ADN} with a SEEK command in order to identify a character string in the alpha-identifier, it is the responsibility of the ME to ensure that the number of characters used as SEEK parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 12: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (GSM 02.07 [3])
'D'	"Wild" value This will cause the MMI to prompt the user for a single digit (see GSM 02.07 [3]).
'E'	Expansion digit ("Shift Key"). It has the effect of adding '10' to the following digit. The following BCD digit will hence be interpreted in the range of '10'-'1E'. The purpose of digits in this range is for further study.
'F'	Endmark e.g. in case of an odd number of digits

BCD values 'C', 'D' and 'E' are never sent across the air interface.

NOTE 5: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 6: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see GSM 02.07 [3]).

10.3.2 EF_{FDN} (Fixed dialling numbers)

This EF contains Fixed Dialling Numbers (FDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3B'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (subclause 10.3.1), with the exception that extension records are stored in the EF_{EXT2}.

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

10.3.3 EF_{SMS} (Short messages)

This EF contains information in accordance with GSM 03.40 [12] comprising short messages (and associated parameters) which have either been received by the MS from the network, or are to be used as an MS originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

- Status
  Contents: Status byte of the record which can be used as a pattern in the SEEK command.
  Coding:

```
•••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
•••••••••••••••••••••••
 •  •  •  •  •  0  0  0   free space
 •  •  •  •  •  x  x  1   used space
 •  •  •  •  •  0  0  1   message received by MS from network;
 •  •  •  •  •              message read
 •  •  •  •  •  0  1  1   message received by MS from network;
 •  •  •  •  •              message to be read
 •  •  •  •  •  1  0  1   MS originating message;
 •  •  •  •  •              message sent to the network
 •  •  •  •  •  1  1  1   MS originating message; message to be sent
 •  •  •  •  •
 ••••••••••••••••••••••   RFU (see subclause 9.3)
```

- Remainder

  Contents: This data item commences with the TS-Service-Centre-Address as specified in GSM 04.11 [15]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in GSM 03.40 [12], with identical coding and ordering of parameters.

  Coding: according to GSM 03.40 [12] and GSM 04.11 [15]. Any TP-message reference contained in an MS originated message stored in the SIM, shall have a value as follows:

	Value of the TP-message-reference
message to be sent:	'FF'
message sent to the network:	the value of TP-Message-Reference used in the message sent to the network.

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

  It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the SIM the TS-Service-Centre-Address and the TPDU in bytes 2-176 without modification, except for the last byte of the TPDU, which shall not be stored.

10.3.4 EF_{CCP} (Capability configuration parameters)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, MSISDN or a last number dialled.

Identifier: '6F3D'	Structure: linear fixed	Optional
Record length: 14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved - see below	M	4 bytes

- Bearer capability information element

  Contents and Coding: see GSM 04.08 [14].

  - Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the ME.

10.3.5 EF_{MSISDN} (MSISDN)

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F40'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

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

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

NOTE 1: If the SIM stores more than one MSISDN number and the ME displays the MSISDN number(s) within the initialization procedure then the one stored in the first record shall be displayed with priority.

NOTE 2: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.3.6 EF_{SMSP} (Short message service parameters)

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the MS, the parameter in the SIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier
  Contents: Alpha Tag of the associated SMS-parameter.
  Coding: See 10.3.1 (EF_{ADN}).

  NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators
  Contents: Each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.
  Coding: Allocation of bits:

Bit number	Parameter indicated
1	TP-Destination Address
2	TS-Service Centre Address
3	TP-Protocol Identifier
4	TP-Data Coding Scheme
5	TP-Validity Period
6	reserved, set to 1
7	reserved, set to 1
8	reserved, set to 1

Bit value	Meaning
0	Parameter present
1	Parameter absent

- TP-Destination Address
  Contents and Coding: As defined for SM-TL address fields in GSM 03.40 [12].

- TP-Service Centre Address
  Contents and Coding: As defined for RP-Destination address Centre Address in GSM 04.11 [15].

- TP-Protocol Identifier
  Contents and Coding: As defined in GSM 03.40 [12].

- TP-Data Coding Scheme
  Contents and Coding: As defined in GSM 03.38 [11].

- TP-Validity Period
  Contents and Coding: As defined in GSM 03.40 [12] for the relative time format.

10.3.7 EF_{SMSS} (SMS status)

This EF contains status information relating to the short message service.

The provision of this EF is associated with EF_{SMS}. Both files shall be present together, or both absent from the SIM.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

- Last Used TP-MR.
  Contents: the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in GSM 03.40 [12].
  Coding: as defined in GSM 03.40 [12].

- SMS "Memory Capacity Exceeded" Notification Flag.
  Contents: This flag is required to allow a process of flow control, so that as memory capacity in the MS becomes available, the Network can be informed. The process for this is described in GSM 03.40 [12].
  Coding:
  b1=1 means flag unset; memory capacity available
  b1=0 means flag set
  b2 to b8 are reserved and set to 1.

10.3.8 EF_{LND} (Last number dialled)

This EF contains the last numbers dialled (LND) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F44'	Structure: cyclic	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INCREASE	NEVER
INVALIDATE	ADM
REHABILITATE	ADM

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

Contents and coding: see EF_{ADN}.

The value of X in EF_{LND} may be different to both the value of X in EF_{ADN} and of X in EF_{FDN}.

If the value of X in EF_{LND} is longer than the length of the α-tag of the number to be stored, then the ME shall pad the α-tag with 'FF'. If the value of X in EF_{LND} is shorter than the length of the α-tag of the number to be stored, then the ME shall cut off excessive bytes.

10.3.9 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC, an MSISDN, or an LND. Extension data is caused by:

- an ADN/SSC (MSIDSN, LND) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, LND) Elementary File. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN/SSC (MSISDN, LND) Elementary File. The EXT1 record in this case is specified as overflow data;
- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: '6F4A'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type
  Contents: type of the record
  Coding:

```
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 •  •  •  •  •  •  •  ••• Called Party Subaddress
 •  •  •  •  •  •  •••••• Overflow data
 •••••••••••••••••••••••• RFU
```

  b3-b8 are reserved and set to 0;
  a bit set to 1 identifies the type of record;
  only one type can be set;
  '00' indicates the type "unknown".

  The following example of coding means that the type of extension data is "overflow data":

```
••••••••••••••••••••••••
•b8•b7•b6•b5•b4•b3•b2•b1•
••••••••••••••••••••••••
 0  0  0  0  0  0  1  0
```

- Extension data
  Contents: Overflow data or Called Party Subaddress depending on record type.
  Coding:
  Case 1, Extension1 record is overflow data:
  The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC (resp. MSISDN, LND). The coding of remaining bytes is BCD, according to the coding of ADN/SSC (MSISDN, LND). Unused nibbles at the end have to be set to 'F'. It is possible if the number of overflow digits exceeds the capacity of the overflow record to chain another record inside the EXT1 Elementary File by the identifier in byte 13.
  Case 2, Extension1 record is Called Party Subaddress:
  The subaddress data contains information as defined for this purpose in GSM 04.08 [14]. All information defined in GSM 04.08 [14], except the information element identifier, shall be stored in the SIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these

records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier
  Contents: identifier of the next extension record to enable storage of information longer than 11 bytes.
  Coding: record number of next record. 'FF' identifies the end of the chain.

  Example of a chain of extension records being associated to an ADN/SSC. The extension1 record identifier (Byte 14+X) of ADN/SSC is set to 3.

No of Record	Type	Extension Data	Next	Record
.	.	.	.	
.	.	.	.	
Record 3	'02'	xx xx	'06'	>•••••••••••
Record 4	'xx'	xx xx	'xx'	•
Record 5	'01'	xx xx	'FF'	<•••••••• •
Record 6	'01'	xx xx	'05'	<•••••••••••
.	.	.	.	
.	.	.	.	

In this example ADN/SSC is associated to an overflow (record 3) and a called party subaddress whose length is more than 11 bytes (records 6 and 5).

10.3.10 EF_{EXT2} (Extension2)

This EF contains extension data of an FDN/SSC (see EXT1 in 10.3.9).

Identifier: '6F4B'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 10.3.9 EF_{EXT1}.

10.4 Files of GSM (figure 7)

This subclause contains a figure depicting the file structure of the SIM. DF_{GSM} shall be selected using the identifier '7F20'. If selection by this means fails, then DCS1800 MEs shall, and optionally GSM MEs may then select DF_{GSM} with '7F21'.

NOTE 1: The selection of the GSM application using the identifier '7F21', if selection by means of the identifier '7F20' fails, is to ensure backwards compatibility with those Phase 1 SIMs which only support the DCS1800 application using the Phase 1 directory $DF_{DCS1800}$ coded '7F21'.

NOTE 2: To ensure backwards compatibility with those Phase 1 DCS1800 MEs which have no means to select DF_{GSM} two options have been specified. These options are given in GSM 09.91 [16].

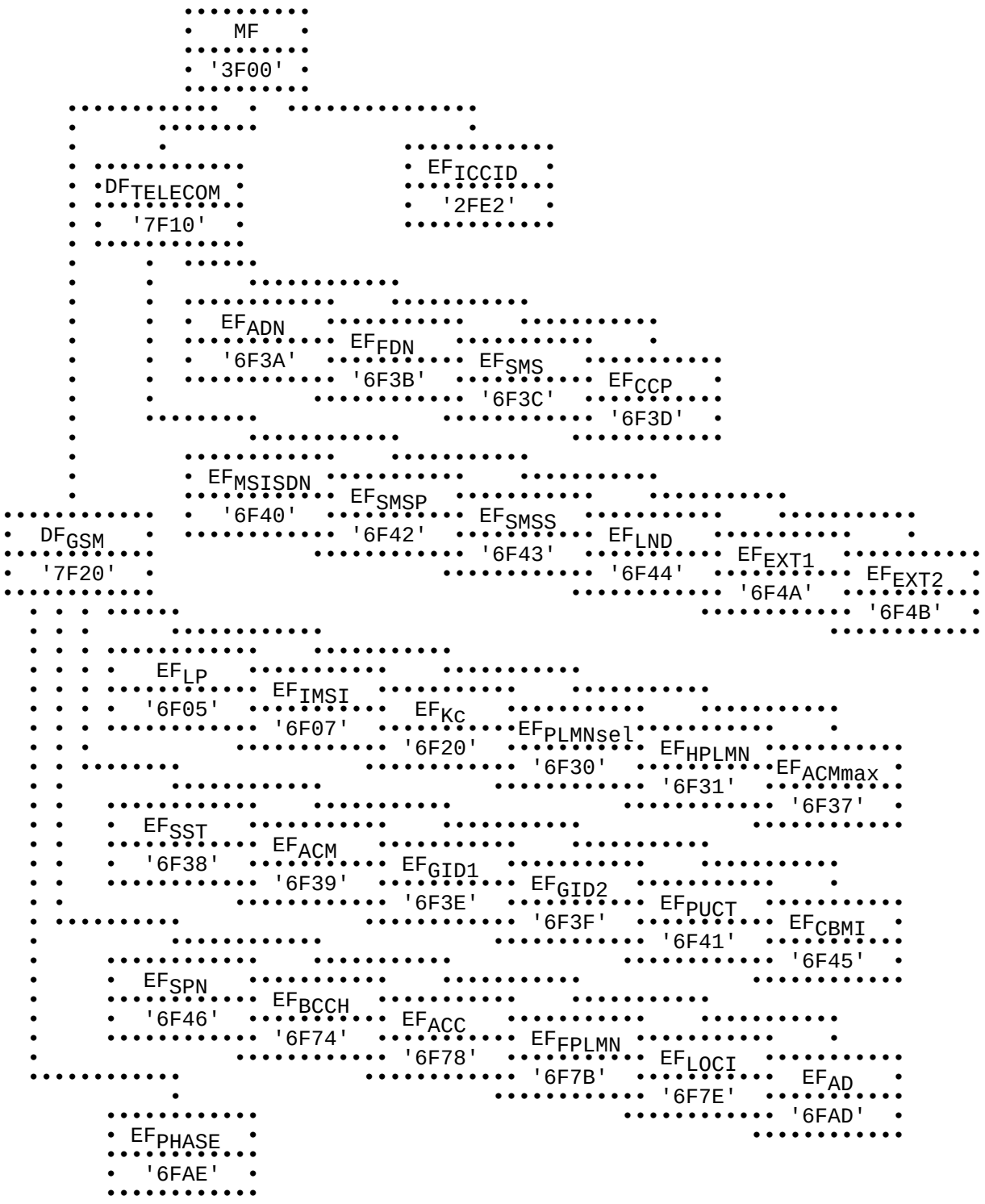


Figure 7: File identifiers and directory structures of GSM

11 Application protocol

When involved in GSM administrative management operations, the SIM interfaces with appropriate terminal equipment. These operations are outside the scope of this standard.

When involved in GSM network operations the SIM interfaces with an ME with which messages are exchanged. A message can be a command or a response.

- A GSM command/response pair is a sequence consisting of a command and the associated response.

- A GSM procedure consists of one or more GSM command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The ME shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself.

- A GSM session of the SIM in the GSM application is the interval of time starting at the completion of the SIM initialization procedure and ending either with the start of the GSM session termination procedure, or at the first instant the link between the SIM and the ME is interrupted.

During the GSM network operation phase, the ME plays the rôle of the master and the SIM plays the rôle of the slave.

Some procedures at the SIM/ME interface require MMI interactions. The descriptions hereafter do not intend to infer any specific implementation of the corresponding MMI. When MMI interaction is required, it is marked "MMI" in the list given below.

Some procedures are not clearly user dependent. They are directly caused by the interaction of the MS and the network. Such procedures are marked "NET" in the list given below.

Some procedures are automatically initiated by the ME. They are marked "ME" in the list given below.

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

General Procedures:

- Reading an EF ME
- Updating an EF ME
- Increasing an EF ME

SIM management procedures:

- SIM initialization ME
- GSM session termination ME
- Language preference request ME
- Administrative information request ME
- SIM service table request ME
- SIM phase request ME

CHV related procedures:

- CHV verification MMI
- CHV value substitution MMI
- CHV disabling MMI
- CHV enabling MMI
- CHV unblocking MMI

GSM security related procedures:

-	GSM algorithms computation	NET
-	IMSI request	NET
-	Access control information request	NET
-	HPLMN search period request	NET
-	Location Information	NET
-	Cipher key	NET
-	BCCH information	NET
-	Forbidden PLMN information	NET

Subscription related procedures:

-	Dialling Numbers (ADN, FDN, MSISDN, LND)	MMI/ME
-	Short messages (SMS)	MMI
-	Advice of Charge (AoC)	MMI
-	Capability Configuration Parameters (CCP)	MMI
-	PLMN Selector	MMI
-	Cell Broadcast Message Identifier (CBMI)	MMI
-	Group Identifier Level 1 (GID1)	MMI/ME
-	Group Identifier Level 2 (GID2)	MMI/ME
-	Service Provider Name (SPN)	ME

The procedures listed in subclause 11.2 are basically required for execution of the procedures in subclauses 11.3, 11.4 and 11.5. The procedures listed in subclauses 11.3 and 11.4 are mandatory (see GSM 02.17 [6]). The procedures listed in 11.5 are only executable if the associated services, which are optional, are provided in the SIM. However, if the procedures are implemented, it shall be in accordance with subclause 11.5.

If a procedure is related to a specific service indicated in the SIM Service Table, it shall only be executed if the corresponding bits denote this service as "allocated and activated" (see subclause 10.2.7). In all other cases this procedure shall not start.

11.1 General procedures

11.1.1 Reading an EF

The ME selects the EF and sends a READ command. This contains the location of the data to be read. If the access condition for READ is fulfilled, the SIM sends the requested data contained in the EF to the ME. If the access condition is not fulfilled, no data will be sent and an error code will be returned.

11.1.2 Updating an EF

The ME selects the EF and sends an UPDATE command. This contains the location of the data to be updated and the new data to be stored. If the access condition for UPDATE is fulfilled, the SIM updates the selected EF by replacing the existing data in the EF with that contained in the command. If the access condition is not fulfilled, the data existing in the EF will be unchanged, the new data will not be stored, and an error code will be returned.

11.1.3 Increasing an EF

The ME selects the EF and sends an INCREASE command. This contains the value which has to be added to the contents of the last updated/increased record. If the access condition for INCREASE is fulfilled, the SIM increases the existing value of the EF by the data contained in the command, and stores the result. If the access condition is not fulfilled, the data existing in the EF will be unchanged and an error code will be returned**.**

NOTE: The identification of the data within an EF to be acted upon by the above procedures is specified within the command. For the procedures in subclauses 11.1.1 and 11.1.2 this data may have been previously identified using a SEEK command, e.g. searching for an alphanumeric pattern.

11.2 SIM management procedures

Phase 2 MEs shall support all SIMs which comply with the mandatory requirements of Phase 1, even if these SIMs do not comply with all the mandatory requirements of Phase 2. Furthermore, Phase 2 MEs shall take care of potential incompatibilities with Phase 1 SIMs which could arise through use of inappropriate commands or misinterpretation of response data. Particular note should be taken of making a false interpretation of RFU bytes in a Phase 1 SIM having contradictory meaning in Phase 2; e.g. indication of EF invalidation state.

11.2.1 SIM initialization

After SIM activation (see subclause 4.3.2), the ME selects the Dedicated File DF_{GSM} and requests the Language Preference. If this EF is not available or the languages in the EF are not supported then the ME selects a default language. It then runs the CHV1 verification procedure.

If the CHV1 verification procedure is performed successfully, the ME then runs the SIM Phase request procedure. If the ME detects a SIM of Phase 1, it shall omit the following procedures relating to FDN and continue with the Administrative Information request. The ME may omit procedures not defined in Phase 1 such as HPLMN Search Period request.

For a Phase 2 SIM, GSM operation shall only start if one of the two following conditions is fulfilled:

- if EF_{IMSI} and EF_{LOCI} are not invalidated, the GSM operation shall start immediately;
- if EF_{IMSI} and EF_{LOCI} are invalidated, the ME rehabilitates these two EFs.
  MEs without FDN capability shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} and therefore have no access to these EFs. GSM operation will therefore be prohibited. It is this mechanism which is used for control of service n°3 by the use of SIMs for this service which always invalidate these two EFs at least before the next command following selection of either EF;
  If the FDN capability procedure indicates that:
  i) FDN is allocated and activated in the SIM; and FDN is set "enabled", i.e. ADN "invalidated" or not activated; and the ME supports FDN;
  or ii) FDN is allocated and activated in the SIM; and FDN is set "disabled", i.e. ADN "not invalidated";
  or iii) FDN is not allocated or not activated;

then GSM operation shall start.

In all other cases GSM operation shall not start.

Afterwards, the ME runs the following procedures:

- Administrative Information request
- SIM Service Table request
- IMSI request
- Access Control request
- HPLMN Search Period request
- PLMN selector request
- Location Information request
- Cipher Key request
- BCCH information request
- Forbidden PLMN request

After the SIM initialization has been completed successfully, the MS is ready for a GSM session.

11.2.2 GSM session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in subclause 4.3.2.

The GSM session is terminated by the ME as follows:

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

- Location Information update
- Cipher Key update
- BCCH information update
- Advice of Charge increase
- Forbidden PLMN update

As soon as the SIM indicates that these procedures are completed, the ME/SIM link may be deactivated.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the GSM Session, and the value has not changed until GSM session termination, the ME may omit the respective update procedure.

11.2.3 Language preference

Request: The ME performs the reading procedure with EF_{LP}.

Update: The ME performs the updating procedure with EF_{LP}.

11.2.4 Administrative information request;

The ME performs the reading procedure with EF_{AD}.

11.2.5 SIM service table request

The ME performs the reading procedure with EF_{SST}.

11.2.6 SIM phase request

The ME performs the reading procedure with EF_{PHASE}.

11.2.7 SIM Presence Detection

As an additional mechanism, to ensure that the SIM has not been removed during a card session, the ME sends, at frequent intervals, a STATUS command during each call. A STATUS command shall be issued within all 30 second periods of inactivity on the SIM-ME interface during a call. Inactivity in this case is defined as starting at the end of the last communication or the last issued STATUS command. If no response data is received to this STATUS command, then the call shall be terminated as soon as possible but at least within 5 seconds after the STATUS command has been sent. If the DF indicated in response to a STATUS command is not the same as that which was indicated in the previous response, or accessed by the previous command, then the call shall be terminated as soon as possible but at least within 5 seconds after the response data has been received.This procedure shall be used in addition to a mechanical or other device used to detect the removal of a SIM.

11.3 CHV related procedures

A successful completion of one of the following procedures grants the access right of the corresponding CHV for the GSM session. This right is valid for all files within the GSM application protected by this CHV.

After a third consecutive presentation of a wrong CHV to the SIM, not necessarily in the same GSM session, the CHV status becomes "blocked" and the access right previously granted by this CHV is lost immediately.

An access right is not granted if any of the following procedures are unsuccessfully completed or aborted.

11.3.1 CHV verification

The ME checks the CHV status. If the CHV status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV status is not "blocked", the ME reads the CHV enabled/disabled indicator. If this is "disabled", the procedure is finished successfully.

If the CHV status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the VERIFY CHV function. If the CHV presented by the ME is equal to the corresponding CHV stored in the SIM, the procedure is finished successfully. If the CHV presented by the ME is not equal to the corresponding CHV stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.2 CHV value substitution

The ME checks the CHV status. If the CHV status is "blocked" or "disabled", the procedure ends and is finished unsuccessfully.

If the CHV status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the CHANGE CHV function. If the old CHV presented by the ME is equal to the corresponding CHV stored in the SIM, the new CHV presented by the ME is stored in the SIM and the procedure is finished successfully.

If the old CHV and the CHV in memory are not identical, the procedure ends and is finished unsuccessfully.

11.3.3 CHV disabling

Requirement: Service n°1 "allocated and activated".

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "disabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the DISABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "disabled" and the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.4 CHV enabling

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "enabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "disabled", the ME uses the ENABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "enabled" and the procedure is finished successfully. If the CHV presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.5 CHV unblocking

The execution of the CHV unblocking procedure is independent of the corresponding CHV status, i.e. being blocked or not.

The ME checks the UNBLOCK CHV status. If the UNBLOCK CHV status is "blocked", the procedure ends and is finished unsuccessfully.

If the UNBLOCK CHV status is not "blocked", the ME uses the UNBLOCK CHV function. If the UNBLOCK CHV presented by the ME is equal to the corresponding UNBLOCK CHV stored in the SIM, the relevant CHV status becomes "unblocked" and the procedure is finished successfully. If the UNBLOCK CHV presented by the ME is not equal to the corresponding UNBLOCK CHV stored in the SIM, the procedure ends and is finished unsuccessfully.

11.4 GSM security related procedures

11.4.1 GSM algorithms computation

The ME selects DF_{GSM} and uses the RUN GSM ALGORITHM function (see 8.16). The response SRES-Kc is sent to the ME when requested by a subsequent GET RESPONSE command.

11.4.2 IMSI request

The ME performs the reading procedure with EF_{IMSI}.

11.4.3 Access control request

The ME performs the reading procedure with EF_{ACC}.

11.4.4 HPLMN search period request

The ME performs the reading procedure with EF_{HPLMN}.

11.4.5 Location information

Request: The ME performs the reading procedure with EF_{LOCI}.

Update: The ME performs the updating procedure with EF_{LOCI}.

11.4.6 Cipher key

Request: The ME performs the reading procedure with EF_{Kc}.

Update: The ME performs the updating procedure with EF_{Kc}.

11.4.7 BCCH information

Request: The ME performs the reading procedure with EF_{BCCH}.

Update: The ME performs the updating procedure with EF_{BCCH}.

11.4.8 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{FPLMN}.

Update: The ME performs the updating procedure with EF_{FPLMN}.

11.5 Subscription related procedures

11.5.1 Dialling numbers

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCP} and EF_{EXT1} as described in the procedures below, but also to EF_{FDN}, EF_{MSISDN} and EF_{LND} and their associated extension files. If these files are not allocated and activated, as denoted in the SIM service table, the current procedure shall be aborted and the appropriate EFs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Requirement: Service n°2 "allocated and activated"
(Service n°3 for FDN, Service n°9 for MSISDN, Service n°13 for LND)

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the description of the EFs in subclauses 10.3.1, 10.3.4 and 10.3.9):

i) The ME identifies the Alpha-tagging, Capability/Configuration Identifier and Extension1 Record Identifier.

ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:

- if a "+" is found, the TON identifier is set to "International";

- if 20 or less "digits" remain, they shall form the dialling number/SSC string;

- if more than 20 "digits" remain, the procedure shall be as follows:

  Requirement:
  Service n°10 "allocated and activated"
  (Service n°10 applies also for MSISDN and LND; Service n°11 for FDN).

  The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

  The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "overflow data". The first byte of the Extension1 record is set with the number of bytes of the remaining overflow data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing overflow data (see subclauses 10.3.1 and 10.3.9).

iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:

  Requirement:
  Service n°10 "allocated and activated"
  (Service n°10 applies also for MSISDN and LND; Service n°11 for FDN)

  If the length of the called party subaddress is less than or equal to 11 bytes (see GSM 04.08 [14] for coding):
  The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
  The ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".

  If the length of the called party subaddress is greater than 11 bytes (see GSM 04.08 [14] for coding):
  The ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted.
  The ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1} record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the SIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

NOTE 1: For reasons of memory efficiency the ME is allowed to analyse all Extension1 records to recognize if the overflow or subaddress data to be stored is already existing in EF_{EXT1}. In this case the ME may use the existing chain or the last part of the existing chain from more than one ADN (LND, MSISDN). The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

Erasure: The ME sends the identification of the information to be erased. The content of the identified record in EF_{ADN} is marked as "free".

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} (subclause 10.3.1) to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

Purge: The ME shall access each EF which references EF_{EXT1} (EF_{EXT2}) for storage and shall identify records in these files using extension data (overflow data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2) records are noted by the ME. All Extension1 (Extension2) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'.

NOTE 2: Dependent upon the implementation of the ME, and in particular the possibility of erasure of ADN/SSC records by Phase 1 MEs, which have no knowledge of the EF_{EXT1}, it is possible for Extension1 records to be marked as "used space" (not equal to 'FF'), although in fact they are no longer associated with an ADN/SSC record.

The following three procedures are only applicable to service n°3 (FDN).

FDN capability request. The ME has to check the state of service n°3, i.e. if FDN is "enabled" or "disabled". In case of enabled FDN, the ME has to switch to a restrictive terminal mode (see GSM 02.07). To ascertain the state of FDN, the ME checks in EF_{SST} whether or not ADN is activated. If ADN is not activated, service n°3 is enabled. If ADN is activated, the ME checks the response data of EF_{ADN}. If EF_{ADN} is invalidated, service n°3 is enabled. In all other cases service n°3 is disabled.

FDN disabling. The FDN disabling procedure requires that CHV2 verification procedure has been performed successfully and that ADN is activated. If not, FDN disabling procedure will not be executed successfully. To disable FDN capability, the ME rehabilitates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°3. If ADN is not activated, disabling of FDN is not possible and thus service n°3 is always enabled (see FDN capability request).

NOTE 3: If FDN is disabled (by rehabilitating EF_{ADN}) using an administrative terminal then the FDN disabling procedure of this administrative terminal need also to rehabilitate EF_{IMSI} and EF_{LOCI} to ensure normal operation of the SIM in a phase 1 ME or a phase 2 ME which does not support FDN.

FDN enabling. The FDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, FDN enabling procedure will not be executed successfully. To enable FDN capability, the ME invalidates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°3 (see FDN capability request). If ADN is not activated, service n°3 is always enabled.

11.5.2 Short messages

Requirement: Service n°4 "allocated and activated".

Request: The SIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.
If this message is not found within the SIM memory, the SIM indicates that to the ME.

Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.

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

Erasure: The ME will select in the SIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the SIM is made available for a new incoming message. The memory of the SIM may still contain the old message until a new message is stored in this area.

11.5.3 Advice of Charge (AoC)

Requirement: Service n°5 "allocated and activated".

Accumulated Call Meter.

Request: The ME performs the reading procedure with EF_{ACM}. The SIM returns the last updated value of the ACM.

Initialization: The ME performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The ME performs the reading procedure with EF_{ACMmax}.

Initialization: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The ME performs the reading procedure with EF_{PUCT}.

Update: The ME performs the updating procedure with EF_{PUCT}.

11.5.4 Capability configuration parameters

Requirement: Service n°6 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CCP}.

Update: The ME performs the updating procedure with EF_{CCP}.

Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP} is marked as "free".

11.5.5 PLMN selector

Requirement: Service n°7 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNsel}$.

Update: The ME performs the updating procedure with $EF_{PLMNsel}$.

11.5.6 Cell broadcast message identifier

Requirement: Service n°14 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CBMI}.

Update: The ME performs the updating procedure with EF_{CBMI}.

11.5.7 Group identifier level 1

Requirement: Service n°15 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID1}

11.5.8 Group identifier level 2

Requirement: Service n°16 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID2}

11.5.9 Service Provider Name

Requirement: Service n°17 "allocated and activated".

Request: The ME performs the reading procedure with EF_{SPN}.

Annex A (normative): Plug-in SIM

This annex specifies the dimensions of the Plug-in SIM as well as the dimensions and location of the contacts of the Plug-in SIM. For further details of the Plug-in SIM see clause 4.

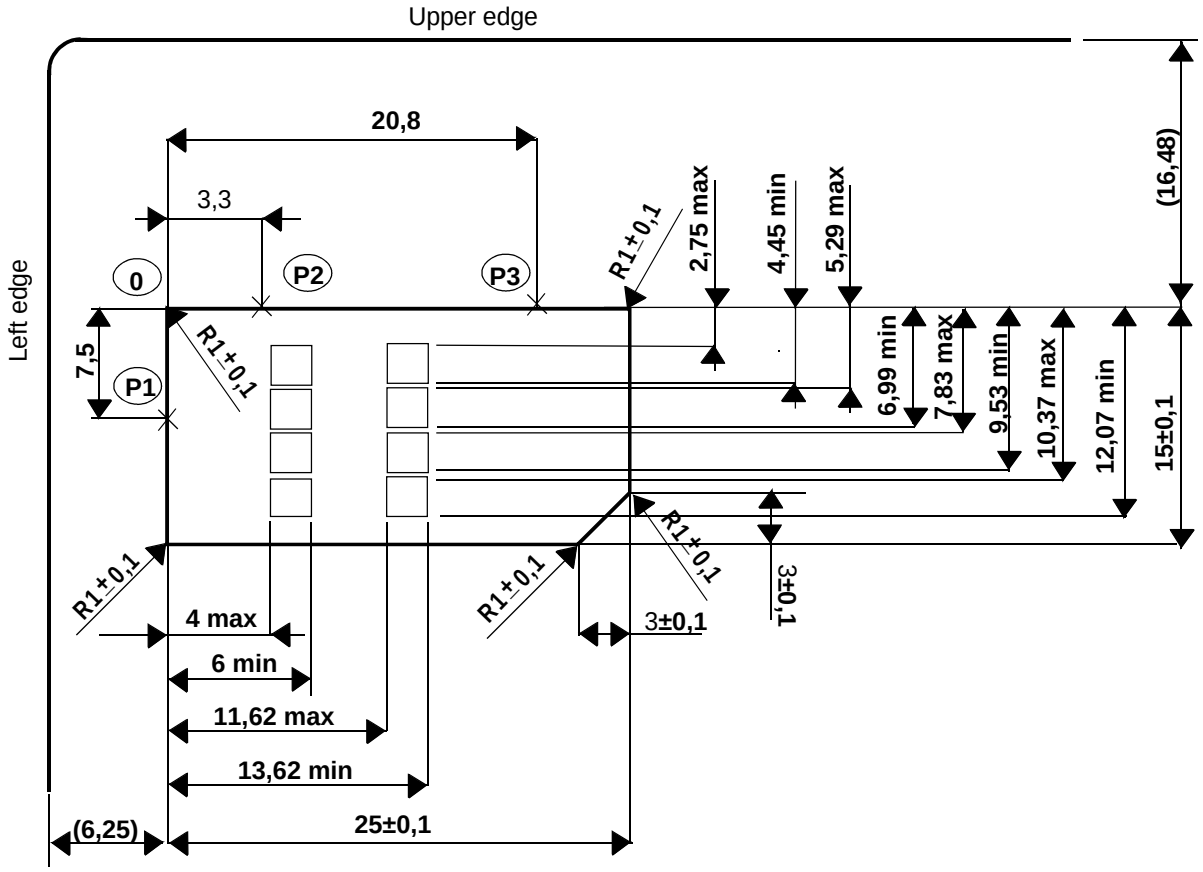
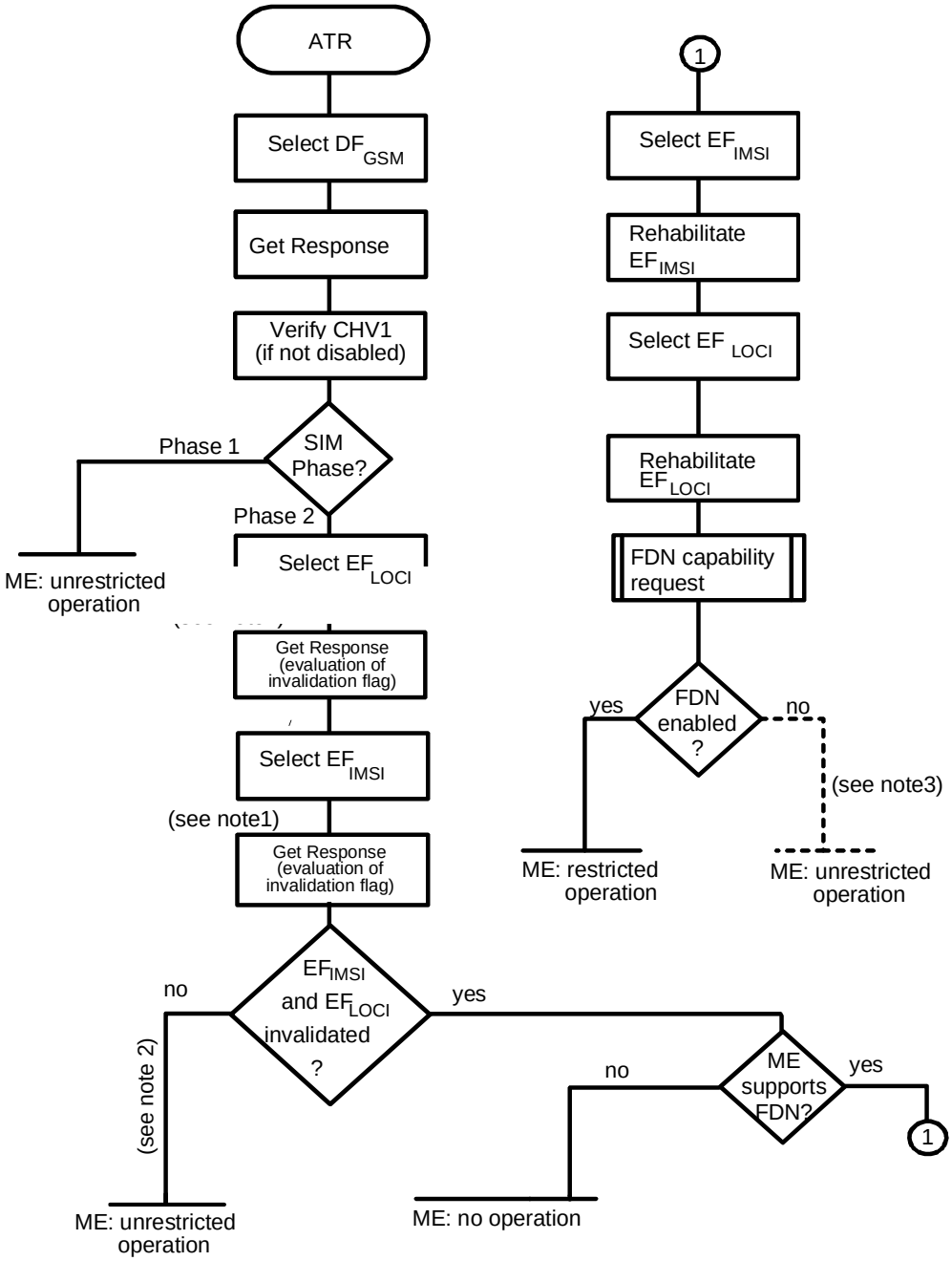


Figure A.1: Plug-in SIM

NOTE: The Plug-in SIM may be "obtained" by cutting away excessive plastic of an ID-1 SIM. The values in parenthesis in figure A.1 show the positional relationship between the Plug-in and the ID-1 SIM and are for information only.

Annex B (informative): FDN Procedures

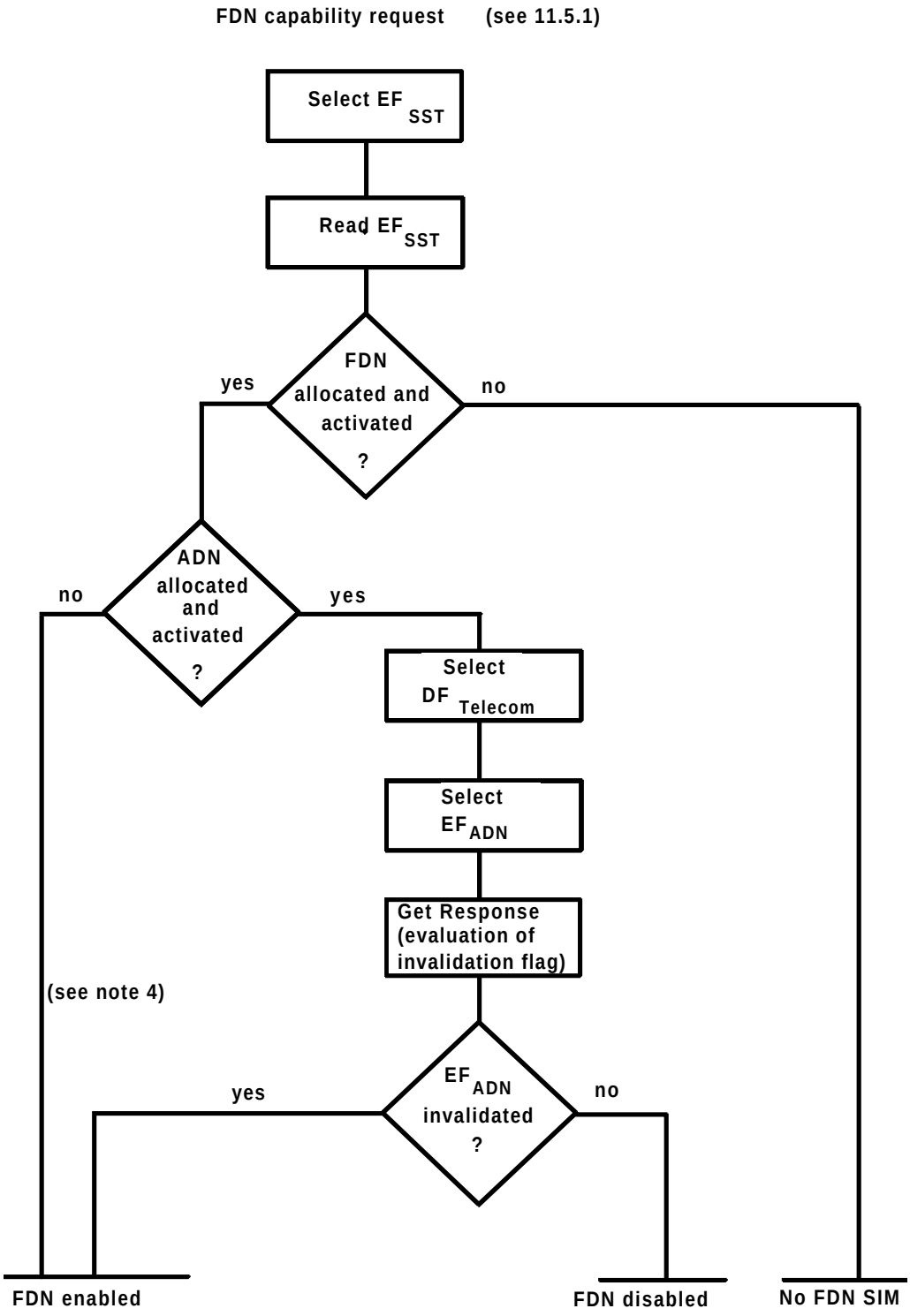
Example of an Initialisation Procedure of a FDN SIM **(see 11.2.1)**



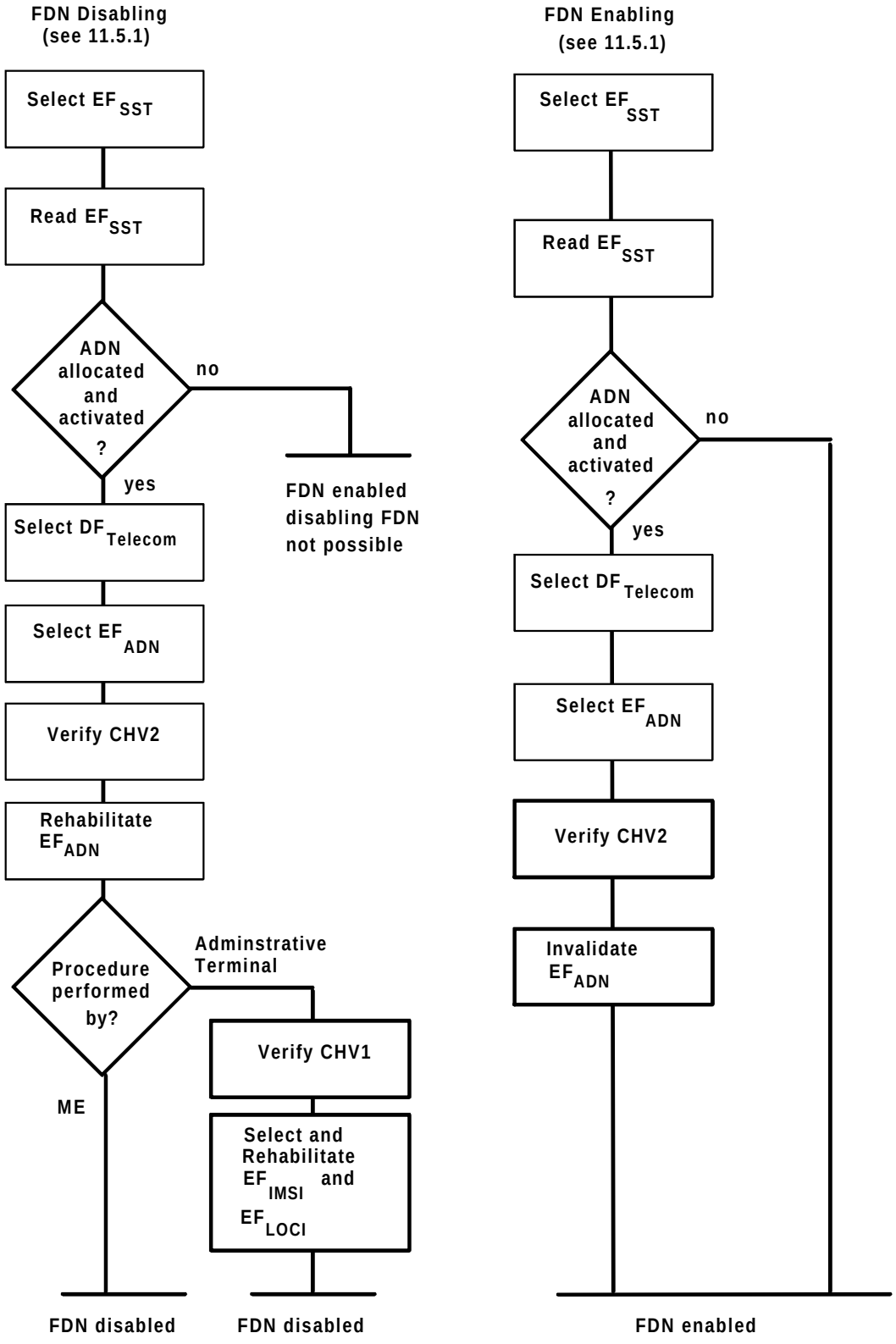
NOTE 1: In case of enabled FDN the SIM shall set the EF to “invalidated” at no later than this stage (see 10.2.7).

NOTE 2: Invalidation of only one of the two EFs is not allowed for FDN.

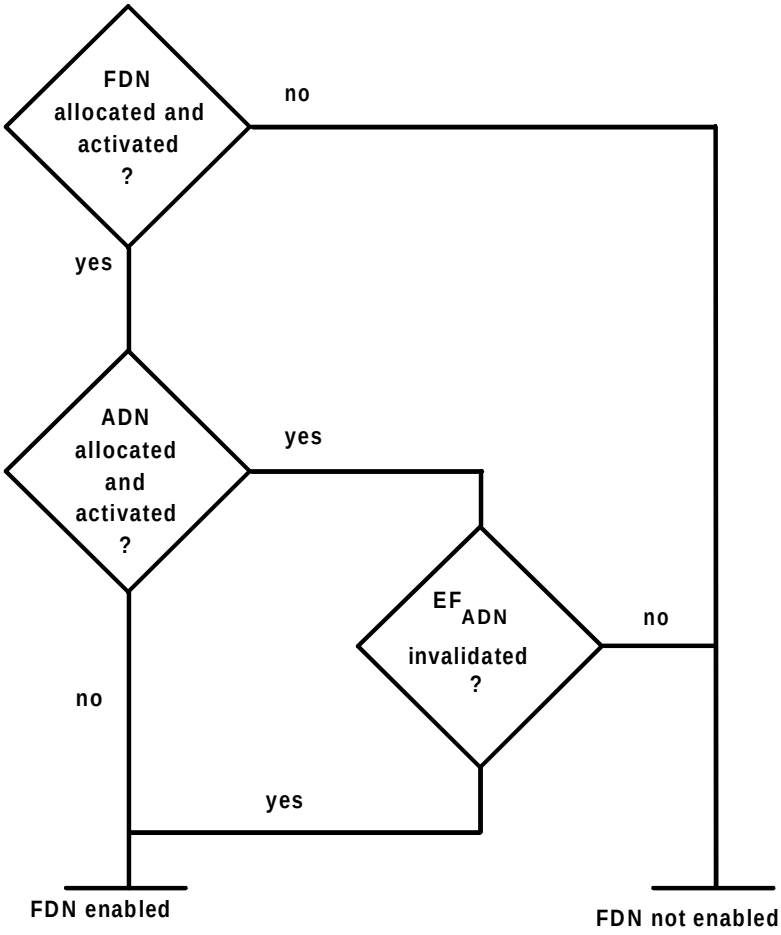
NOTE 3: Abnormal state. Internal SIM mechanism of invalidating EF_{MS} and EF_{LOCI} is expected to occur if FDN is enabled



NOTE 4: In this case FDN is enabled without the possibility of disabling.


FDN Disabling
(see 11.5.1)
Select EF SST
Read EF SST
ADN allocated and activated ?
no
FDN enabled disabling FDN not possible
yes
Select DF Telecom
Select EF ADN
Verify CHV2
Rehabilitate EF ADN
Procedure performed by?
Adminstrative Terminal
Verify CHV1
Select and Rehabilitate EF IMSI and EF LOCI
ME
FDN disabled
FDN disabled
FDN Enabling
(see 11.5.1)
Select EF SST
Read EF SST
ADN allocated and activated ?
no
yes
Select DF Telecom
Select EF ADN
Verify CHV2
Invalidate EF ADN
FDN enabled

Coding for state of FDN



Boolean equation:

FD = FDA . (NOT(ADA) + ADA . ADI)

with

FD = FDN enabled
FDA = FDN allocated and activated
ADA = ADN allocated and activated
ADI = EF_{ADN} invalidated

Annex C (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F E2'	ICC identification	operator dependant (see 10.1.1)
'6F 05'	Language preference	'FF'
'6F 07'	IMSI	operator dependant (see 10.2.2)
'6F 20'	Ciphering key Kc	'FF...FF07'
'6F 30'	PLMN selector	'FF...FF'
'6F 31'	HPLMN search period	'FF'
'6F 37'	ACM maximum value	'000000' (see note 1)
'6F 38'	SIM service table	operator dependant (see 10.2.7)
'6F 39'	Accumulated call meter	'000000'
'6F 3E'	Group identifier level 1	operator dependant
'6F 3F'	Group identifier level 2	operator dependant
'6F 41'	PUCT	'FFFFFF0000'
'6F 45'	CBMI	'FF...FF'
'6F 46'	Service provider name	'FF...FF'
'6F 74'	BCCH	'FF...FF'
'6F 78'	Access control class	operator dependant (see 10.1.12)
'6F 7B'	Forbidden PLMNs	'FF...FF'
'6F 7E	Location information	'FFFFFFFF xxFxxx 0000 FF 01' (see note 2)
'6F AD'	Administrative data	operator dependant (see 10.2.15)
'6F AE'	Phase identification	see 10.2.16
'6F 3A'	Abbreviated dialling numbers	'FF...FF'
'6F 3B'	Fixed dialling numbers	'FF...FF'
'6F 3C'	Short messages	'00FF...FF'
'6F 3D'	Capability configuration parameters	'FF...FF'
'6F 40'	MSISDN storage	'FF...FF'
'6F 42'	SMS parameters	'FF...FF'
'6F 43'	SMS status	'FF...FF'
'6F 44'	Last number dialled	'FF...FF'
'6F 4A'	Extension 1	'FF...FF'
'6F 4B'	Extension 2	'FF...FF'

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxFxxx stands for any valid MCC and MNC, coded according to GSM 04.08 [14].

Annex D (informative): Bibliography

1) EN 726-3 (1994): "Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use Part 3: Application independent card requirements".

2) EN 726-4 (1994): "Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use Part 4: Application independent card related terminal requirements".

3) ISO/IEC 7816-3/A2 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols",: "Protocol type select".

Annex E (Informative): Change History

This annex lists all change requests approved for this document since meeting #13 of ETSI SMG.

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s13	122/95	14/95	4.13.1	A001		2	3	HPLMN Search Period Timer	4.14.0
	122/95	14/95		A003		2	1	SIM-ME Association	
s15	515/95	100/95	4.14.0	A004		2	1	Display of Service Provider Name by the ME	4.15.0
s16	708/95	168/95	4.15.0	A005		2	2	Location of contact area on embossed ID-1 SIMs	4.16.0
	708/95	168/95		A007		2	2	Use of "Wild Characters" in SMS-CB	
s18	260/96	45/96	4.16.0	A015		2	F	SIM presence detection clarification	4.17.0
	261/96	54/96		A017		2	F	Reponse codes and coding of SIM service table	
	262/96	55/96		A019		2	F	Reference to International Standards	
s19	373/96	105/96	4.17.0	A022		2	D	Clarification of clock stop timing	4.18.0
s20	702/96	207/96	4.18.0	A030		2	D	RFU bit taken into use in GSM 11.12	4.18.1
s21	101/97	97/057	4.18.1	A035		2	D	Administrative Access Conditions	4.18.2
s22	356/97	162/97	4.18.2	A043	1	2	F	Clarification of electrical/mechanical SIM/ME interface	4.19.0
s25	98-0157	98p093	4.19.0	A060	1	2	F	Clarification of removal of the SIM	4.20.0
s26	98-0398	98p261	4.20.0	A067		2	D	Addition of file ID for IS-41 as requested by ANSI T1P1.2	4.20.1
s29	P-99-414	9-99-201	4.20.1	A087		2	F	Alignment with GSM 02.07 regarding the OFM bit	4.21.0

History

Document history		
January 1995	First Edition	
July 1995	Amendment 1 to First Edition of ETS 300 608	
January 1996	Second Edition	
May 1996	Third Edition	
December 1996	Fourth Edition	
May 1997	Fifth Edition	
August 1997	Sixth Edition	
January 1998	Seventh Edition	
May 1998	One-step Approval Procedure (Eighth Edition)	OAP 9841: 1998-05-20 to 1998-10-16
October 1998	Eighth Edition	
July 1999	One-step Approval Procedure (Ninth Edition)	OAP 9952: 1999-07-28 to 1999-11-26