# 3GPP TS 51.011 V5.0.0 (2001-12)

*Technical Specification*

## 3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 5)


Keywords
GSM, SIM, card

***3GPP***

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

# Contents

Foreword ..... 9
1 Scope ..... 10
2 References ..... 10
3 Definitions, abbreviations and symbols ..... 12
3.1 Definitions ..... 12
3.2 Abbreviations ..... 13
3.3 Symbols ..... 15
4 Physical characteristics ..... 15
5 Electronic signals and transmission protocols ..... 15
5.1 Electrical specifications ..... 16
5.2 Initial communication establishment procedures ..... 16
5.2.1 Error handling for speed enhancement ..... 16
5.3 Transmission protocols ..... 16
5.4 Clock ..... 16
6 Application and File structure ..... 17
6.1 SIM Application structure ..... 17
6.2 Void ..... 17
6.3 Void ..... 17
6.4 File types ..... 17
6.4.1 Dedicated files ..... 17
6.4.2 Elementary files ..... 17
6.4.2.1 Cyclic EF ..... 18
6.5 Methods for selecting a file ..... 18
7 Security features ..... 18
7.1 Authentication and cipher key generation procedure ..... 18
7.2 Algorithms and processes ..... 18
7.3 File access conditions ..... 18
8 Void ..... 19
9 Description of the commands ..... 20
9.1 Mapping principles ..... 20
9.2 Coding of the commands ..... 22
9.2.1 SELECT ..... 22
9.2.2 STATUS ..... 25
9.2.3 READ BINARY ..... 25
9.2.4 UPDATE BINARY ..... 25
9.2.5 READ RECORD ..... 25
9.2.6 UPDATE RECORD ..... 25
9.2.7 SEEK ..... 25
9.2.8 INCREASE ..... 26
9.2.9 VERIFY CHV ..... 27
9.2.10 CHANGE CHV ..... 27
9.2.11 DISABLE CHV ..... 27
9.2.12 ENABLE CHV ..... 28
9.2.13 UNBLOCK CHV ..... 28
9.2.14 INVALIDATE ..... 28
9.2.15 REHABILITATE ..... 28
9.2.16 RUN GSM ALGORITHM ..... 28
9.2.17 SLEEP ..... 29
9.2.18 GET RESPONSE ..... 29
9.2.19 TERMINAL PROFILE ..... 29

9.2.20 ENVELOPE ..... 29
9.2.21 FETCH ..... 29
9.2.22 TERMINAL RESPONSE ..... 29
9.3 Definitions and coding ..... 30
9.4 Status conditions returned by the card ..... 31
9.4.1 Responses to commands which are correctly executed ..... 31
9.4.2 Responses to commands which are postponed ..... 31
9.4.3 Memory management ..... 31
9.4.4 Referencing management ..... 31
9.4.5 Security management ..... 32
9.4.6 Application independent errors ..... 32
9.4.7 Commands versus possible status responses ..... 32
10 Contents of the Elementary Files (EF) ..... 33
10.1 Contents of the EFs at the MF level ..... 34
10.1.1 $EF_{ICCID}$ (ICC Identification) ..... 34
10.1.2 $EF_{PL}$ (Preferred language) ..... 34
10.2 DFs at the GSM application level ..... 34
10.3 Contents of files at the GSM application level ..... 34
10.3.1 $EF_{LP}$ (Language preference) ..... 34
10.3.2 $EF_{IMSI}$ (IMSI) ..... 35
10.3.3 $EF_{Kc}$ (Ciphering key Kc) ..... 36
10.3.4 $EF_{PLMNsel}$ (PLMN selector) ..... 37
10.3.5 $EF_{HPLMN}$ (HPLMN search period) ..... 37
10.3.6 $EF_{ACMmax}$ (ACM maximum value) ..... 38
10.3.7 $EF_{SST}$ (SIM service table) ..... 39
10.3.8 $EF_{ACM}$ (Accumulated call meter) ..... 41
10.3.9 $EF_{GID1}$ (Group Identifier Level 1) ..... 42
10.3.10 $EF_{GID2}$ (Group Identifier Level 2) ..... 42
10.3.11 $EF_{SPN}$ (Service Provider Name) ..... 43
10.3.12 $EF_{PUCT}$ (Price per unit and currency table) ..... 44
10.3.13 $EF_{CBMI}$ (Cell broadcast message identifier selection) ..... 45
10.3.14 $EF_{BCCH}$ (Broadcast control channels) ..... 45
10.3.15 $EF_{ACC}$ (Access control class) ..... 46
10.3.16 $EF_{FPLMN}$ (Forbidden PLMNs) ..... 46
10.3.17 $EF_{LOCI}$ (Location information) ..... 47
10.3.18 $EF_{AD}$ (Administrative data) ..... 48
10.3.19 $EF_{Phase}$ (Phase identification) ..... 50
10.3.20 $EF_{VGCS}$ (Voice Group Call Service) ..... 50
10.3.21 $EF_{VGCSS}$ (Voice Group Call Service Status) ..... 52
10.3.22 $EF_{VBS}$ (Voice Broadcast Service) ..... 53
10.3.23 $EF_{VBSS}$ (Voice Broadcast Service Status) ..... 55
10.3.24 $EF_{eMLPP}$ (enhanced Multi Level Pre-emption and Priority) ..... 55
10.3.25 $EF_{AAeM}$ (Automatic Answer for eMLPP Service) ..... 56
10.3.26 $EF_{CBMID}$ (Cell Broadcast Message Identifier for Data Download) ..... 57
10.3.27 $EF_{ECC}$ (Emergency Call Codes) ..... 57
10.3.28 $EF_{CBMIR}$ (Cell broadcast message identifier range selection) ..... 58
10.3.29 $EF_{DCK}$ De-personalization Control Keys ..... 59
10.3.30 $EF_{CNL}$ (Co-operative Network List) ..... 59
10.3.31 $EF_{NIA}$ (Network's Indication of Alerting) ..... 60
10.3.32 $EF_{KcGPRS}$ (GPRS Ciphering key KcGPRS) ..... 61
10.3.33 $EF_{LOCIGPRS}$ (GPRS location information) ..... 61
10.3.34 $EF_{SUME}$ (SetUpMenu Elements) ..... 63
10.3.35 $EF_{PLMNwAcT}$ (User controlled PLMN Selector with Access Technology) ..... 63
10.3.36 $EF_{OPLMNwAcT}$ (Operator controlled PLMN Selector with Access Technology) ..... 65
10.3.37 $EF_{HPLMNwAcT}$ (HPLMN Selector with Access Technology) ..... 65
10.3.38 $EF_{CPBCCH}$ (CPBCCH Information) ..... 66
10.3.39 $EF_{InvScan}$ (Investigation Scan) ..... 67
10.3.40 $EF_{RPLMNAcT}$ (RPLMN Last used Access Technology) ..... 68

10.3.41 $EF_{PNN}$ (PLMN Network Name) ..... 68
10.3.42 $EF_{OPL}$ (Operator PLMN List) ..... 69
10.3.43 $EF_{MBDN}$ (Mailbox Dialling Numbers) ..... 70
10.3.44 $EF_{MBI}$ (Mailbox Identifier) ..... 70
10.3.45 $EF_{MWIS}$ (Message Waiting Indication Status) ..... 71
10.3.46 $EF_{CFIS}$ (Call Forwarding Indication Status) ..... 72
10.3.47 $EF_{EXT5}$ (Extension5) ..... 73
10.3.48 $EF_{EXT6}$ (Extension6) ..... 73
10.3.49 $EF_{EXT7}$ (Extension7) ..... 74
10.3.50 $EF_{SPDI}$ (Service Provider Display Information) ..... 74
10.4 Contents of DFs at the GSM application level ..... 75
10.4.1 Contents of files at the GSM SoLSA level ..... 75
10.4.1.1 $EF_{SAI}$ (SoLSA Access Indicator) ..... 75
10.4.1.2 $EF_{SLL}$ (SoLSA LSA List) ..... 76
10.4.1.3 LSA Descriptor files ..... 78
10.4.2 Contents of files at the MExE level ..... 79
10.4.2.1 $EF_{MExE-ST}$ (MExE Service table) ..... 79
10.4.2.2 $EF_{ORPK}$ (Operator Root Public Key) ..... 80
10.4.2.3 $EF_{ARPK}$ (Administrator Root Public Key) ..... 82
10.4.2.4 $EF_{TPRPK}$ (Third Party Root Public key) ..... 82
10.4.2.5 Trusted Key/Certificates Data Files ..... 83
10.5 Contents of files at the telecom level ..... 83
10.5.1 $EF_{ADN}$ (Abbreviated dialling numbers) ..... 83
10.5.2 $EF_{FDN}$ (Fixed dialling numbers) ..... 87
10.5.3 $EF_{SMS}$ (Short messages) ..... 87
10.5.4 Capability configuration parameters ..... 88
10.5.4.1 $EF_{CCP}$ (Capability configuration parameters) ..... 88
10.5.4.2 $EF_{ECCP}$ (Extended Capability Configuration Parameters) ..... 89
10.5.5 $EF_{MSISDN}$ (MSISDN) ..... 89
10.5.6 $EF_{SMSP}$ (Short message service parameters) ..... 90
10.5.7 $EF_{SMSS}$ (SMS status) ..... 91
10.5.8 $EF_{LND}$ (Last number dialled) ..... 92
10.5.9 $EF_{SDN}$ (Service Dialling Numbers) ..... 93
10.5.10 $EF_{EXT1}$ (Extension1) ..... 93
10.5.11 $EF_{EXT2}$ (Extension2) ..... 95
10.5.12 $EF_{EXT3}$ (Extension3) ..... 95
10.5.13 $EF_{BDN}$ (Barred Dialling Numbers) ..... 95
10.5.14 $EF_{EXT4}$ (Extension4) ..... 96
10.5.15 $EF_{SMSR}$ (Short message status reports) ..... 96
10.5.16 $EF_{CMI}$ (Comparison Method Information) ..... 97
10.6 DFs at the telecom level ..... 98
10.6.1 Contents of files at the telecom graphics level ..... 98
10.6.1.1 $EF_{IMG}$ (Image) ..... 98
10.6.1.2 Image Instance Data Files ..... 100
10.7 Files of GSM ..... 100

11 Application protocol ..... 102
11.1 General procedures ..... 104
11.2 SIM management procedures ..... 104
11.2.1 SIM initialization ..... 104
11.2.2 GSM session termination ..... 106
11.2.3 Emergency Call Codes ..... 107
11.2.4 Language preference ..... 107
11.2.5 Administrative information request; ..... 107
11.2.6 SIM service table request ..... 107
11.2.7 SIM phase request ..... 107
11.2.8 SIM Presence Detection and Proactive Polling ..... 107
11.2.9 Preferred Language ..... 107
11.3 CHV related procedures ..... 108

11.3.1 CHV verification ..... 108
11.3.2 CHV value substitution ..... 108
11.3.3 CHV disabling ..... 108
11.3.4 CHV enabling ..... 109
11.3.5 CHV unblocking ..... 109
11.3.6 CHV procedures on a UICC Platform ..... 109
11.3.6.1 Mapping of CHV1 ..... 109
11.3.6.1.1 Single verification capable UICC (see TS 31.101 [57]) ..... 109
11.3.6.1.2 Multi verification capable UICC (see TS 31.101 [57]) ..... 109
11.3.6.1 Mapping of CHV2 ..... 110
11.4 GSM security related procedures ..... 110
11.4.1 GSM algorithms computation ..... 110
11.4.2 IMSI request ..... 110
11.4.3 Access control request ..... 110
11.4.4 HPLMN search period request ..... 110
11.4.5 Location information ..... 110
11.4.6 Cipher key ..... 110
11.4.7 BCCH information ..... 110
11.4.8 Forbidden PLMN ..... 110
11.4.9 LSA information ..... 111
11.4.10 GPRS Location information ..... 111
11.4.11 GPRS Cipher key ..... 111
11.5 Subscription related procedures ..... 111
11.5.1 Dialling numbers ..... 111
11.5.2 Short messages ..... 114
11.5.3 Advice of Charge (AoC) ..... 114
11.5.4 Capability configuration parameters ..... 114
11.5.5 PLMN selector ..... 115
11.5.6 Cell broadcast message identifier ..... 115
11.5.7 Group identifier level 1 ..... 115
11.5.8 Group identifier level 2 ..... 115
11.5.9 Service Provider Name ..... 115
11.5.10 Voice Group Call Services ..... 115
11.5.11 Voice Broadcast Services ..... 115
11.5.12 Enhanced Multi Level Pre-emption and Priority Service ..... 116
11.5.13 Cell Broadcast Message range identifier ..... 116
11.5.14 Depersonalisation Control Keys ..... 116
11.5.15 Short message status report ..... 116
11.5.16 Network's indication of alerting ..... 117
11.5.17 User controlled PLMN Selector with Access Technology ..... 117
11.5.18 Operator controlled PLMN Selector with Access Technology ..... 117
11.5.19 HPLMN Selector with Access Technology ..... 117
11.5.20 CPBCCH information ..... 117
11.5.21 Investigation Scan ..... 117
11.5.22 RPLMN last used Access Technology ..... 117
11.5.23 PLMN Network Name ..... 117
11.5.24 Operator PLMN List ..... 117
11.5.25 Message Waiting Indication ..... 118
11.5.26 Call Forwarding Indication Status ..... 118
11.5.27 Service Provider Display Information ..... 118
11.6 SIM Application Toolkit related procedures ..... 118
11.6.1 Initialization procedure ..... 118
11.6.2 Proactive polling ..... 118
11.6.3 Support of commands ..... 118
11.6.4 Support of response codes ..... 118
11.6.5 Command-response pairs ..... 119
11.6.6 Independence of normal GSM and SIM Application Toolkit tasks ..... 119
11.6.7 Use of BUSY status response ..... 119
11.6.8 Use of NULL procedure byte ..... 119

11.6.9 Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands ..... 119
11.6.10 Using the FETCH command ..... 119
11.6.11 Data Download via SMS-CB ..... 120
11.6.12 Data Download via SMS-PP ..... 120
11.6.13 Menu selection ..... 120
11.6.14 Call Control ..... 120
11.6.15 Proactive SIM ..... 120
11.6.16 Mobile Originated Short Message control by SIM ..... 120
11.6.17 SIM data download error ..... 120
11.6.18 Image Request ..... 120
11.7 MExE related procedures ..... 121
11.7.1 MExE ST ..... 121
11.7.2 Operator root public key ..... 121
11.7.3 Administrator root public key ..... 121
11.7.4 Third Party root public key(s) ..... 121

**Annex A (normative): Void ..... 122**

**Annex B (normative): Void ..... 122**

**Annex C (informative): FDN/BDN Procedures ..... 123**

**Annex D (informative): Suggested contents of the EFs at pre-personalization ..... 128**

**Annex E (informative): SIM application Toolkit protocol diagrams ..... 130**

**Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA ..... 137**

**Annex G (normative): Image Coding Schemes ..... 138**

G.1 Basic Image Coding Scheme ..... 138

G.2 Colour Image Coding Scheme ..... 139

**Annex H (normative): Coding of EFs for NAM and GSM-AMPS Operational Parameters . 141**

H.1 Elementary File Definitions and Contents ..... 141
H.1.1 $EF_{MIN}$ (Mobile Identification Number) ..... 141
H.1.2 $EF_{ACCOLC}$ (Access Overload Class) ..... 141
H.1.3 $EF_{SID}$ (System ID Of Home System) ..... 142
H.1.4 $EF_{IPC}$ (Initial Paging Channel) ..... 142
H.1.5 $EF_{GPI}$ (Group ID) ..... 143
H.1.6 $EF_{S\text{-}ESN}$ (SIM Electronic Serial Number) ..... 143
H.1.7 $EF_{COUNT}$ (Call Count) ..... 144
H.1.8 $EF_{PSID}$ (Positive/Favoured SID list) ..... 144
H.1.9 $EF_{NSID}$ (Negative/Forbidden SID List) ..... 145
H.1.10 $EF_{SPL}$ (Scanning Priority List) ..... 146
H.1.11 $EF_{NETSEL}$ (Network Selection Activation Flag) ..... 147
H.1.12 $EF_{CSID}$ (Current/Last Registered SID) ..... 148
H.1.13 $EF_{REG\text{-}THRESH}$ (Registration Threshold) ..... 148
H.1.14 $EF_{CCCH}$ (Current Control Channel) ..... 149
H.1.15 $EF_{LDCC}$ (Latest DCC) ..... 149
H.1.16 $EF_{GSM\text{-}RECON}$ (GSM Reconnect Timer) ..... 149
H.1.17 $EF_{AMPS\text{-}2\text{-}GSM}$ (AMPS to GSM Rescan Timing Table) ..... 150
H.1.18 $EF_{*FC1}$ (Feature Activation Codes) ..... 150
H.1.19 $EF_{AMPS\text{-}UI}$ (AMPS USAGE INDICATORS) ..... 151

H.2 Authentication Functionality ..... 152
H.2.1 A-KEY (ANSI-41 Authentication Key) ..... 152
H.2.2 SSD (Shared Secret Data) ..... 152

H.3 Authentication commands ..... 152
H.3.1 Generation of Authentication Signature Data and Ciphering Keys ..... 153
H.3.2 Validation and Storage of Entered A-Key's ..... 154
H.3.3 Ask Random Task ..... 154
H.3.4 Update Shared Secret Data ..... 155
H.3.5 Confirm Shared Secret Data ..... 155
H.3.6 CMEA Encryption of Voice Channel Data Digits ..... 155
H.3.7 SIM Status Codes ..... 156

**Annex I (informative): EF changes via Data Download or SIM Toolkit applications ..... 157**

**Annex J (informative): Tags defined in the present document ..... 159**

**Annex K (informative): Change history ..... 160**

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document 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 TS 02.17 [6].

The present document 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 and PCS 1900.

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

The present document 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 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] 3GPP TS 02.07: "Mobile Stations (MS) features".

[4] 3GPP TS 02.09: " Security aspects".

[5] 3GPP TS 22.011: " Service accessibility".

[6] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[7] 3GPP TS 22.024: " Description of Charge Advice Information (CAI)".

[8] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[9] 3GPP TS 22.086: "Advice of Charge (AoC) Supplementary Services - Stage 1".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 43.020: "Security related network functions".

[12] 3GPP TS 23.038: "Alphabets and language-specific information".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[15] 3GPP TS 04.08: "Mobile radio interface layer 3 specification".

[16] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

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

[18] ITU-T Recommendation E.118: "The international telecommunication charge card".

[19] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[20] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

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

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

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

[24] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

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

[26] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[27] 3GPP TS 11.14: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

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

[29] 3GPP TS 22.022: "Personalization of Mobile Equipment (ME); Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[33] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[34] GSM 11.19: "Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station - Land Station Compatibility Specification".

[42] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

[45] 3GPP TS 03.22: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] 3GPP TS 05.05: "Radio transmission and reception".

[47] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[48] 3GPP TS 04.18: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[49] 3GPP TS 04.60: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] 3GPP TS 23.057: "Mobile Execution Environment (MExE); Functional description; Stage 2".

[51] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode".

[52] 3GPP TS 31.102: "Characteristics of the USIM Application".

[53] 3GPP TS 22.101: "Service aspects; Service principles".

[54] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP) (Phase 2) - Stage 2".

[55] ETSI TS 102 221 "UICC-Terminal interface; Physical and logical characteristics"

[56] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[57] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

# 3 Definitions, abbreviations and symbols

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**access conditions:** set of security attributes associated with a file

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

**application protocol:** set of procedures required by the application

**card session:** 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:** latest MF or DF selected

**current EF:** latest EF selected

**data field:** obsolete term for Elementary File

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

**directory:** general term for MF and DF

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

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

**file identifier:** 2 bytes which address a file in the SIM

**GSM, DCS 1800 or PCS 1900 application:** set of security mechanisms, files, data and protocols required by GSM, DCS 1800 or PCS 1900

**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:** SIM having the format of an ID-1 card (see ISO 7816-1 [24])

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

**normal GSM operation:** relating to general, CHV related, GSM security related and subscription related procedures

**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:** Second format of SIM (specified in clause 4)

**proactive SIM:** SIM which is capable of issuing commands to the ME. Part of SIM Application Toolkit (see clause 11)

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

**record number:** number which identifies a record within an EF

**record pointer:** pointer which addresses one record in an EF

**root directory:** obsolete term for Master File

**SIM application toolkit procedures:** defined in TS 11.14 [27]

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, in addition to those listed in TR 21.905 [2]:

| | |
|---|---|
| A3 | Algorithm 3, authentication algorithm; used for authenticating the subscriber |
| A38 | A single algorithm performing the functions of A3 and A8 |
| A5 | Algorithm 5, cipher algorithm; used for enciphering/deciphering data |
| A8 | Algorithm 8, cipher key generator; used to generate $K_c$ |
| ACM | Accumulated Call Meter |
| ADM | Access condition to an EF which is under the control of the authority which creates this file |
| ADN | Abbreviated Dialling Number |
| AHAG | Ad-Hoc Authentication Group |
| A-Key | Authentication Key |
| ALW | ALWays |

| | |
|---|---|
| AMPS | Analogue Mobile Phone System |
| ANSI | American National Standards Institute |
| AoC | Advice of Charge |
| APDU | Application Protocol Data Unit |
| ATR | Answer To Reset |
| BCCH | Broadcast Control CHannel |
| BCD | Binary Coded Decimal |
| BDN | Barred Dialling Number |
| BTS | Base Transmitter Station |
| CB | Cell Broadcast |
| CBMI | Cell Broadcast Message Identifier |
| 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 |
| CNL | Co-operative Network List |
| CPBCCH | COMPACT Packet BCCH |
| CTS | Cordless Telephony System |
| DCK | De-personalization Control Keys |
| DCS | Digital Cellular System |
| DF | Dedicated File (abbreviation formerly used for Data Field) |
| DTMF | Dual Tone Multiple Frequency |
| ECC | Emergency Call Code |
| EF | Elementary File |
| EIA | Electronics Industries Alliance (North America) |
| eMLPP | enhanced Multi-Level Precedence and Pre-emption Service |
| 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 |
| IEI | Information Element Identifier |
| 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 |
| LSA | Localised Service Area |
| LSA ID | Localised Service Area Identity |
| 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 |
| MSB | Most Significant Bit |
| MSISDN | Mobile Station international ISDN number |
| NAM | Numeric Assignment Module |
| NET | NETwork |
| NEV | NEVer |
| NPI | Numbering Plan Identifier |

| | |
|---|---|
| OFM | Operational Feature Monitor |
| OPLMN | Operator Controlled PLMN (Selector List) |
| OTA | Over The Air |
| PDC | Personal Digital Communications |
| PIN/PIN2 | Personal Identification Number / Personal Identification Number 2 (obsolete terms for CHV1 and CHV2, respectively) |
| PLMN | Public Land Mobile Network |
| PPS | Protocol and Parameter 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 |
| SDN | Service Dialling Number |
| SID | System IDentity |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SoLSA | Support of Localised Service Area |
| SRES | Signed RESponse calculated by a SIM |
| SSC | Supplementary Service Control string |
| SW1/SW2 | Status Word 1 / Status Word 2 |
| TETRA | TErrestrial Trunk RAdio |
| TIA | Telecommunications Industries Association (North America) |
| 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 |
| VBS | Voice Broadcast Service |
| VGCS | Voice Group Call Service |
| VPLMN | Visited PLMN |

## 3.3 Symbols

For the purposes of the present document, the following symbols apply:

| | |
|---|---|
| '0' to '9' and 'A' to 'F' | the sixteen hexadecimal digits |
| Vcc | Supply voltage |
| Vpp | Programming voltage |

# 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 those specified for the UICC in TS 102 221 [55]

# 5 Electronic signals and transmission protocols

The present document contains references to the UICC/Terminal interface specification, TS 102 221 [55]. For the requirements of TS 102 221 [55] which are referenced by the present specification, the usage of the term "UICC" shall be equivalent to the term "SIM".

# 5.1 Electrical specifications

Electrical specifications of the SIM – ME interface shall be in accordance with TS 102 221 [55] with the following limitations.:

4MHz shall be the maximum clock speed specified for SIMs for 3V and below.

Power consumption during a SIM session and initial communication establishment i.e during the ATR shall not exceed the values defined for the ATR in TS 102 221 [55].

# 5.2 Initial communication establishment procedures

Initial communication establishment procedures shall be in accordance with TS 102 221 [55] with the following limitations.

Since 4MHz is the maximum clock speed specified for SIMs for 3V and below, the respective limitations on power consumption given in TS 102 221 [55] apply.

ATR content: The ME shall invoke the error handling as defined in TS 102 221 [55] if a SIM indicates other values than 0 or 255 in TC1. T=15 global interface parameters are optional. The coding of the historical bytes may not follow TS 102 221 [55] and need not to be interpreted by the ME.

PPS proceedures: Speed enhancement is optional for the SIM. However if speed enhancement is implemented at least F=512 and D=8 shall be supported.

Reset procedures: The SIM shall behave as a "Type 1 UICC".

Clock stop mode: The clock shall only be switched off subject to the conditions specified in the file characteristics (see clause 9.2.1). It is mandatory for a SIM operating at Class B or C operating conditions as defined in TS 102 221 [55] to support clock stop mode.

## 5.2.1 Error handling for speed enhancement

If the SIM does not answer the PPS request within the initial waiting time the ME shall reset the SIM. After two failed PPS attempts using F=512 and D=8 or values indicated in TA1, (no PPS response from the SIM) the ME shall initiate PPS procedure using default values. If this also fails (no PPS response from the SIM) the ME may proceed using default values without requesting PPS.

If the SIM does not support the values requested by the ME, the SIM shall respond to the PPS request indicating the use of default values.

# 5.3 Transmission protocols

Physical and Data link layer of the Transmission Protocols shall be in accordance with TS 102 221[55] with the following limitations.

The support of the Transmission Protocol T=0 is mandatory for ME and the SIM. All other protocols are optional. Use of other protocols than T=0 is not defined in the present document.

Procedure bytes '61' and '6C' shall not be used with GSM commands. Status byte '9F' is returned instead by the SIM to control exchanges between the Transport Layer of the terminal and the SIM.

# 5.4 Clock

If a frequency of 13/4 MHz is needed by the SIM to run the authentication procedure in the allotted time (see TS 03.20 [11]), or to process an ENVELOPE command used for SIM Data Download, 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.

# 6 Application and File structure

This clause describes the logical structure for a SIM if different from that specified in TS 102 221 [55],, the code associated with it, and the structure of files used.

## 6.1 SIM Application structure

Figure 3 shows the general structural relationships which may exist between files. The files are organized in a hierarchical structure and are of one of the types as defined in TS 102 221 [55]. These files may be either administrative or application specific. The operating system handles the access to the data stored in different files.

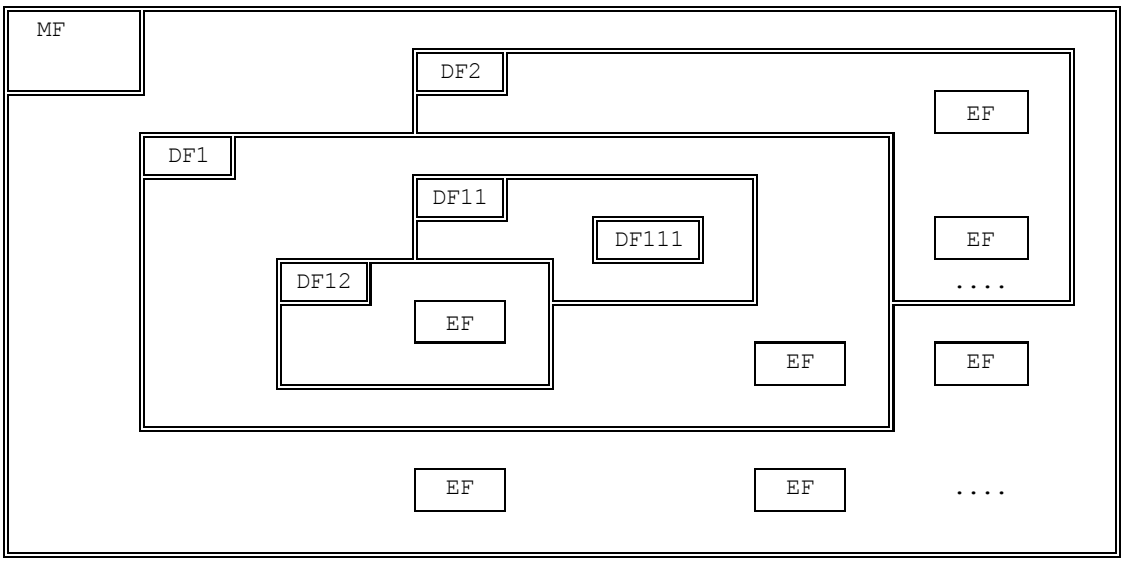



**Figure 3: Organization of memory**

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 Void

## 6.3 Void

## 6.4 File types

The SIM shall support the file types as defined in TS 102 221 [55] with the following limitations.

### 6.4.1 Dedicated files

The SIM does not support the operations that can be performed on an ADF as defined in TS 102 221 [55], although the SIM application DF is considered to be an ADF according to the definitions in TS 102 221 [55].

### 6.4.2 Elementary files

The SIM supports the elementary files as defined in TS 102 221 [55] with the following limitations

#### 6.4.2.1 Cyclic EF

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.

## 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 as specified in TS 102 221 [53] with the following exception:

- Only support selection by file ID referencing and the command parameters as specified in the present document.

# 7 Security features

The security aspects of GSM are described in the normative references TS 02.09 [4] and TS 03.20 [11]. 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 radio interface;
- file access conditions.

## 7.1 Authentication and cipher key generation procedure

This clause 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 TS 03.20 [11]. 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";

NOTE: Some Phase 1 and Phase 2 SIMs do not necessarily grant access when CHV1 is "disabled" and "blocked".

- 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 $DF_{TELECOM}$.

If the SIM application is based on a UICC platform (an IC card specified in TS 31.101 [57]), the CHVs may be mapped onto existing UICC key references.

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 Void

# 9 Description of the commands

The command description and structure is defined in TS 102 221 [55]. The coding of the CLA, INS and parameter bytes are according to TS 102 221 [55] with the limitations stated in the command description in the present document.This clause states the general principles for mapping the commands and responses onto Application Protocol Data Units which are used by the transmission protocol.

## 9.1 Mapping principles

The mapping of protocol T=0 with respect to the TPDU level is according to TS 102 221 with the following exceptions:

- The use of procedure byte '6C' for Case 2 commands as defined in TS 102 221 shall be replaced by the usage of '9F' as described in case 2b below. According to the present document the status byte '9F' triggers a GET RESPONSE command whereas the procedure byte '6C' in TS 102 221 triggers re-issuing of the same command.
- The use of procedure byte '61' for Case 4 commands as defined in TS 102 221 shall be replaced by the usage of '9F' as described in case 4 below. According to the present document the status byte '9F' triggers one GET RESPONSE command, which is optional for the ME, whereas the procedure byte '61' in TS 102 221 triggers one or more GET RESPONSE commands depending upon the procedure bytes following the GET RESPONSE command.

For some commands described in the present document 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:

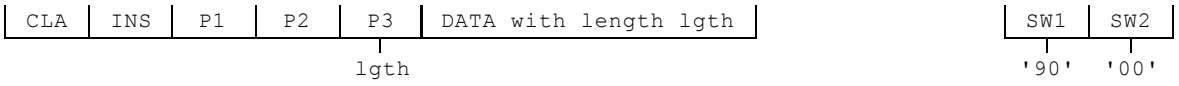
**Case 1: No input / No output**


**Case 2a: No input / Output of known length**

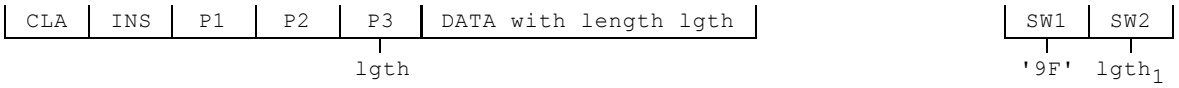

NOTE: lgth='00' causes a data transfer of 256 bytes.

**Case 2b: No Input / Output of unknown length**


**Case 3: Input / No output**




**Case 4: Input / Output of known or unknown length**



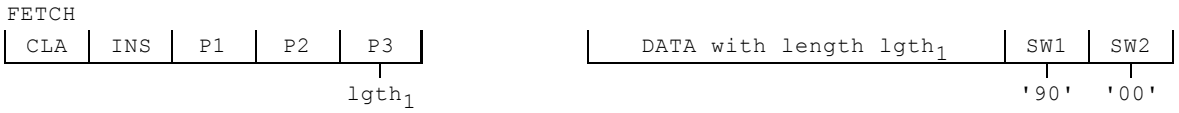


For case 4, in case of an ENVELOPE for SIM data download, SW1/SW2 may also indicate that there is response data with the value '9EXX', and the ME shall then send a GET RESPONSE command to get this response data.

The following diagrams show how the five cases of transmission protocol identified in the above diagrams can all be used to send pro-active SIM commands. For further information on the diagrams below see TS 11.14 [27].

**Case 1: No input / "OK" response with no output, plus additional command from SIM**

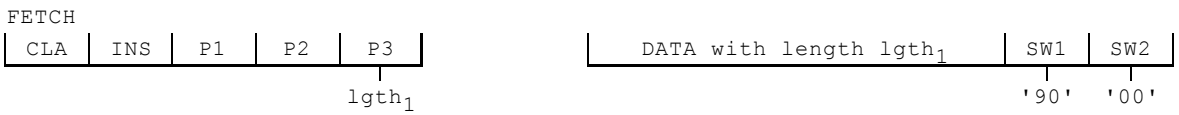

[Possible "normal GSM operation" command/response pairs]




NOTE: $lgth_1$='00' causes a data transfer of 256 bytes.

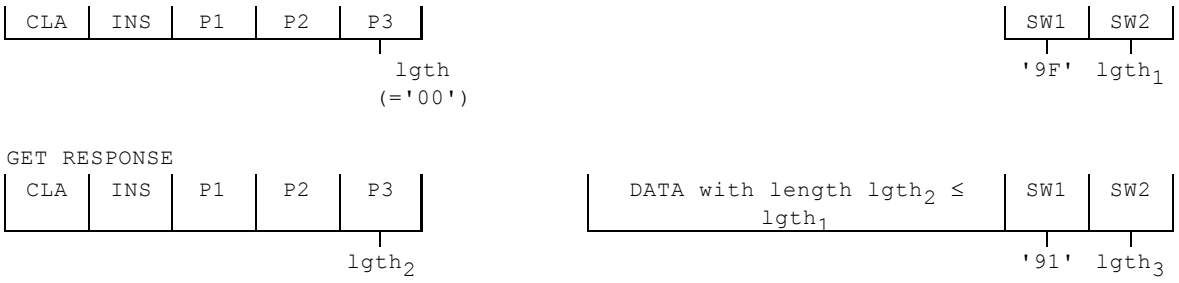
**Case 2a: No input / "OK" response with data of known length, plus additional command from SIM**


[Possible "normal GSM operation" command/response pairs]

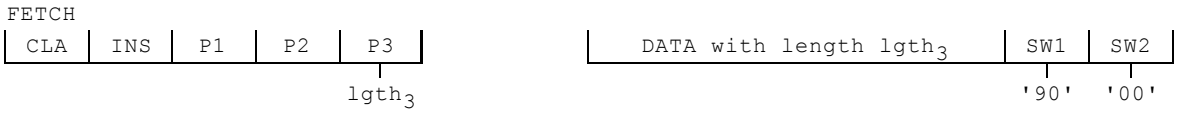



NOTE: lgth='00' causes a data transfer of 256 bytes. The same applies to $lgth_1$.

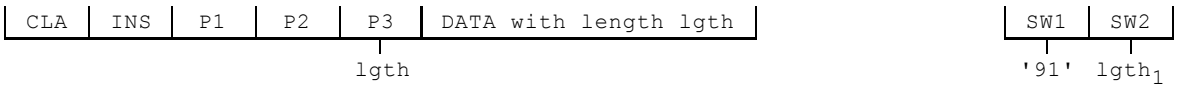
**Case 2b: No Input / "OK" response with data of unknown length, plus additional command from SIM**



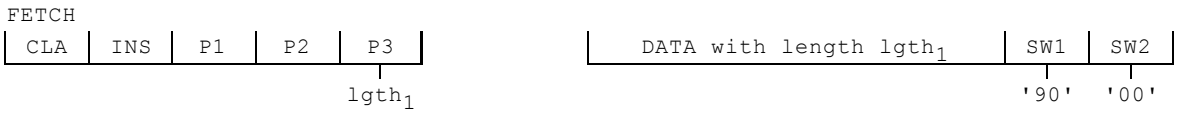

[Possible "normal GSM operation" command/response pairs]



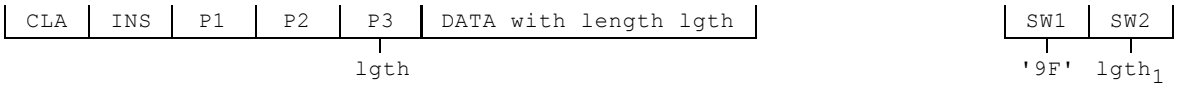

**Case 3: Input / "OK" response with no output data, plus additional command from SIM**




[Possible "normal GSM operation" command/response pairs]

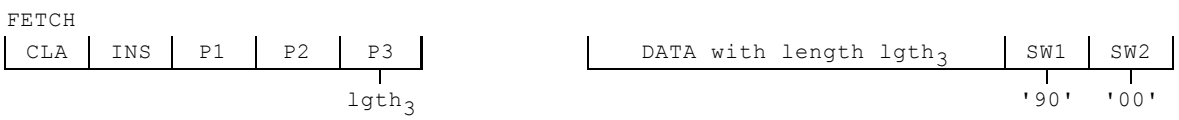



**Case 4: Input / "OK" response with data of known or unknown length, plus additional command from SIM**





[Possible "normal GSM operation" command/response pairs]




## 9.2 Coding of the commands

The commands are coded as specified in TS 102 221 [42] with the class byte set to 'A0'. In addition to the instruction codes specified TS 102 221 [55] the following codes are reserved:

GSM operational phase:

'1X' with X even, from X=6 to X=E.

Administrative management phase:

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

NOTE: This reservation may not be respected by other applications residing on a UICC or further evoluation of TS 102 221 [55].

## 9.2.1 SELECT

The SELECT command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1, P2 = '00'
- P3 = '02'

The response to the SELECT command with the parameters as specified is as follows:

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 clause 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 | $0 \leq lgth \leq 11$ |

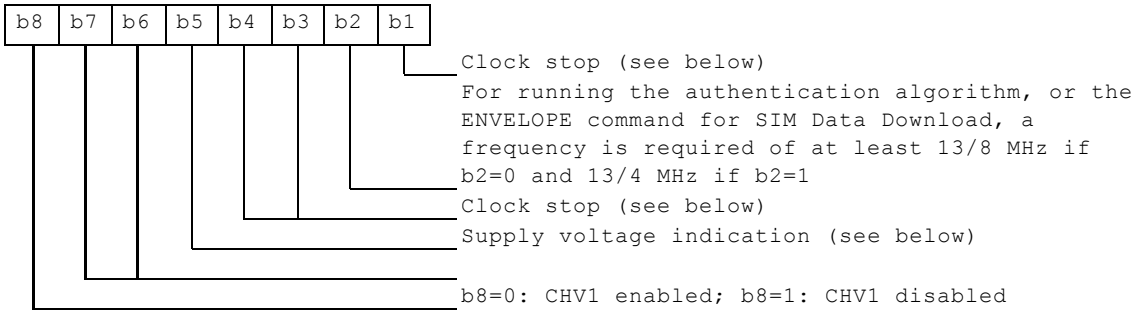
Bytes 1 - 22 are mandatory and shall be returned by the SIM. Bytes 23 and following are optional and may not be returned by the SIM.

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 |

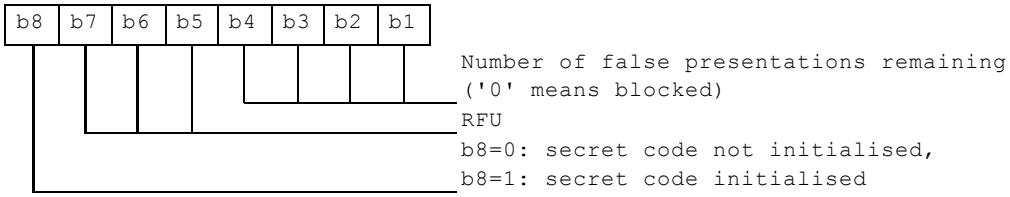
If bit b1 (column 1) is coded 1, stopping the clock is allowed at high or low level. In this case columns 2 (bit b3) and 3 (bit b4) give information about the preferred level (high or low, respectively) at which the clock may be stopped.

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.

The coding of the conditions for the supply voltage indication is as follows:

| SIM Supply Voltage | Bit 7 | Bit 6 | Bit 5 |
|---|---|---|---|
| 5V only SIM | 0 (RFU) [1] | 0 (RFU) [1] | 0 (RFU) [1] |
| 3V Technology SIM | 0 (RFU) [1] | 0 (RFU) [1] | 1 |
| 1.8V Technology SIM | 0 (RFU) [1] | 1 | 1 |
| Future Class | 1 | 1 | 1 |
| NOTE 1 The bits marked (RFU) are set to '0' and reserved for future use in the SIMs. The coding schemes relies on the fact that RFU bits are set to '0'. | | | |

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<br>(for transparent EF: the length of the body part of the EF)<br>(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 |
| 16 and following | RFU | - |

Bytes 1-14 are mandatory and shall be returned by the SIM.

Byte 15 is mandatory in case of linear fixed or cyclic EFs and shall be returned by the SIM.

Byte 15 is optional in case of transparent EFs and may not be returned by the SIM.

Byte 16 and following (when defined) are optional and may not be returned by the SIM.

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

The STATUS command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1, P2 = '00'

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

The READ BINARY command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- B8 in P1 shall be set to '0'

The response is according to the command parameters as defined in TS 102 221 [55].

## 9.2.4 UPDATE BINARY

The UPDATE BINARY command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- B8 in P1 shall be set to '0'

The response is according to the command parameters as defined in TS 102 221 [55].

### 9.2.5 READ RECORD

The READ RECORD command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

P2 = '02', '03', '04'

### 9.2.6 UPDATE RECORD

The UPDATE RECORD command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

P2 = '02', '03', '04'

The response is according to the command parameters, as defined in TS 102 221 [55]

### 9.2.7 SEEK

The instruction code 'A2' identifies the SEARCH RECORD command as defined in TS 102 221 [55]. In the present document the instruction code 'A2' is defined for the SEEK command for class 'A0'.

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.

| 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

The INCREASE command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'
- P3 = '03'

The response is according to the command parameters, as defined in TS 102 221 [55]

## 9.2.9 VERIFY CHV

The VERIFY CHV is identical to the VERIFY PIN command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P3 = '08'

NOTE: The functionality of the VERIFY CHV command is limited to CHV verification and can not be used to retrieve the retry counter value as specified in TS 102 221 [55].

Parameter P2 specifies the CHV:

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

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.10 CHANGE CHV

The CHANGE CHV is identical to the CHANGE PIN command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'

Parameter P2 specifies the CHV:

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

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.11 DISABLE CHV

The DISABLE CHV is identical to the DISABLE PIN command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P2 = '01'

NOTE: The functionality of the DISABLE CHV command is limited to CHV disabling and can not be used to indicate the use of an alternative CHV (global key reference) as specified in TS 102 221 [55].

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.12 ENABLE CHV

The ENABLE CHV is identical to the ENABLE PIN command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P2 = '01'

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.13 UNBLOCK CHV

The UNBLOCK CHV is identical to the UNBLOCK PIN command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'

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.

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.14 INVALIDATE

The INVALIDATE command is identical to the DEACTIVATE command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.15 REHABILITATE

The REHABILITATE command is identical to the ACTIVATE command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'

The response is according to the command parameters, as defined in TS 102 221 [55].

## 9.2.16 RUN GSM ALGORITHM

The RUN GSM ALGORITHM is identical to the AUTHENTICATE command as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'
- P3 = '10'

The structure of the Command parameters/data is as follows only for the specified parameters::

| Byte(s) | Description | Length |
|---|---|---|
| 1 - 16 | RAND | 16 |

The structure of the Response parameters/data is as follows only for the specified parameters:

| 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

This is an obsolete function used by Phase 1 MEs.

In order to achieve phase compatibility, 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;

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

### 9.2.18 GET RESPONSE

The GET RESPONSE command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

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

### 9.2.19 TERMINAL PROFILE

The TERMINAL PROFILE command is coded as specified in TS 102 221 [55] with the following limitations:

- Class = 'A0'

### 9.2.20 ENVELOPE

The ENVELOPE command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

### 9.2.21 FETCH

The FETCH command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

### 9.2.22 TERMINAL RESPONSE

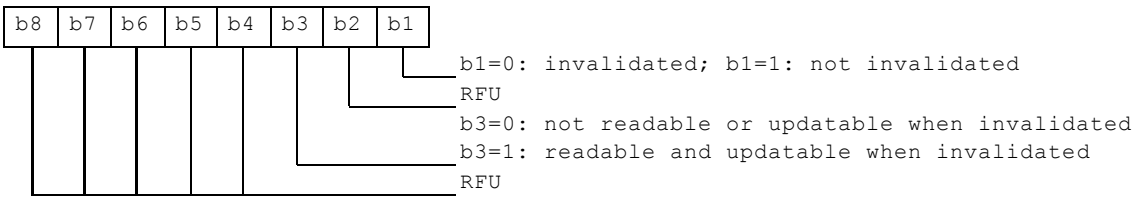
The TERMINAL RESPONSE command is coded as specified in TS 102 221 [55] with the following limitations:

Class = 'A0'

## 9.3 Definitions and coding

The coding conventions defined in TS 102 221 [55] applies with the following exceptions

**File status**




Bit b3 may be set to 1 in special circumstances when it is required that the EF can be read and updated even if the EF is invalidated, e.g. reading and updating the $EF_{ADN}$ when the FDN feature is enabled, or reading and updating the $EF_{BDN}$ when the BDN feature is disabled.

**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 ITU-T T.50 [20] 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**

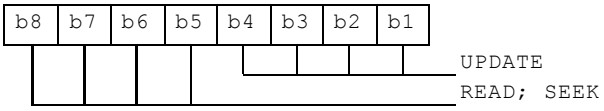
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command if class byte 'A0' is usedEach condition is coded on 4 bits as shown in table 10.

**Table 10: Access conditions**

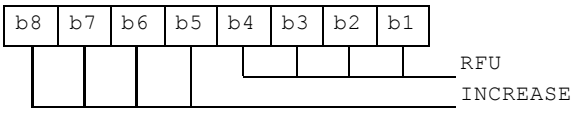
| | |
|---|---|
| ALW | '0' * |
| CHV1 | '1' * |
| CHV2 | '2' * |
| RFU | '3' |
| ADM | '4' |
| ..... | .. |
| ADM | 'E' |
| NEW | 'F' * |

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 the Access Condition bytes in the response data shall be the code applicable to that particular level.

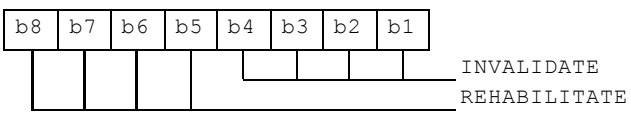
Byte 9:




Byte 10:




Byte 11:




## 9.4 Status conditions returned by the card

This clause 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 |
| '91' | 'XX' | - normal ending of the command, with extra information from the proactive SIM containing a command for the ME. Length 'XX' of the response data |
| '9E' | 'XX' | - length 'XX' of the response data given in case of a SIM data download error |
| '9F' | 'XX' | - length 'XX' of the response data |

### 9.4.2 Responses to commands which are postponed

| SW1 | SW2 | Error description |
|---|---|---|
| '93' | '00' | - SIM Application Toolkit is busy. Command cannot be executed at present, further normal commands are allowed. |

### 9.4.3 Memory management

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

### 9.4.4 Referencing management

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

### 9.4.5 Security management

| SW1 | SW2 | Error description |
|---|---|---|
| '98' | '02' | - no CHV initialized |
| '98' | '04' | - access condition not fulfilled<br>- unsuccessful CHV verification, at least one attempt left<br>- unsuccessful UNBLOCK CHV verification, at least one attempt left<br>- 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<br>- unsuccessful UNBLOCK CHV verification, no attempt left<br>- CHV blocked<br>- 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.

## 9.4.6 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 |
| NOTE 1: [#] These values of 'XX' are specified by ISO/IEC; at present the default value 'XX'='00' is the only one defined. | | |
| NOTE 2: [##] 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').

## 9.4.7 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 | | | | Busy | Mem Sta | | Refer. Status | | | | Security Status | | | | | | Application Independent Errors | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 90 | 91 | 9E | 9F | 93 | 92 | 92 | 94 | 94 | 94 | 94 | 98 | 98 | 98 | 98 | 98 | 98 | 67 | 6B | 6D | 6E | 6F |
| **Commands** | 00 | XX | XX | XX | 00 | 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 | * | * | | | | | * | | | | | | | | | | | * | * | | * | * |
| Terminal Profile | * | * | | | | * | * | | | | | | | | | | | * | * | | * | * |
| Envelope | * | * | * | * | * | * | * | | | | | | | | | | | * | * | | * | * |
| Fetch | * | | | | | | * | | | | | | | | | | | * | * | | * | * |
| Terminal Response | * | * | | | | * | * | | | | | | | | | | | * | * | | * | * |

The responses '91 XX', and '93 00' and '9E XX' can only be given by a SIM supporting SIM Application Toolkit, to an ME also supporting SIM Application Toolkit.

For the SEEK command the response '91 XX' can be given directly after a Type 1 SEEK command. Following the Type 2 SEEK command the SIM can give the response '91 XX' only after the GET RESPONSE command.

# 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 TS, 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' (TS 04.08 [15] 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 ITU-T T.50 [20], bit 8 of every byte shall be set to 0.

For an overview containing all files see figure 8.

## 10.1 Contents of the EFs at the MF level

The present document specifies only two Efs at the MF level. The presence of $EF_{DIR}$ on a SIM is optional. The present document does not specify the mechanism to select a SIM application using $EF_{DIR}$.

### 10.1.1 $EF_{ICCID}$ (ICC Identification)

This EF provides a unique identification number for the SIM. The structure of this EF is as defined in TS 102 221 [55]. Network operators issuing a SIM according to this document may use an identification number length of 20 bytes. SIM issued with identification number coded on 20 bytes may also have the digits in a byte not swapped.

### 10.1.2 $EF_{PL}$ (Preferred language)

The structure of this data field is as defined in TS 102 221 [55]. The presence of this file is optional for a SIM.

. This information may be used by the ME for MMI purposes.This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{LP}$, whichever of these EFs is used (see clause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see TS 23.038 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in $EF_{PL}$.

NOTE: This file is called $EF_{ELP}$ (Extended Langueage preference) in previous releases of the present document

## 10.2 DFs at the GSM application level

For compatibility with other systems based on the GSM switching platform and for special GSM services, DFs may be present as child directories of $DF_{GSM}$. The following have been defined:

| | |
|---|---|
| $DF_{IRIDIUM}$ | '5F30' |
| $DF_{GLOBALSTAR}$ | '5F31' |
| $DF_{ICO}$ | '5F32' |
| $DF_{ACeS}$ | '5F33' |
| $DF_{MExE}$ | '5F3C' |
| $DF_{EIA/TIA-553}$ | '5F40' |
| $DF_{CTS}$ | '5F60' |
| $DF_{SoLSA}$ | '5F70' |

Only the contents of $DF_{SoLSA}$ and $DF_{MExE}$ are specified in the present document. For details of the EFs contained in the $DF_{CTS}$, see TS 11.19 [34].

# 10.3 Contents of files at the GSM application level

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

## 10.3.1 $EF_{LP}$ (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.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows. When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{ELP}$, whichever of these EFs is used (see clause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see TS 23.038 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in $EF_{PL}$.

| 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 language codings contained in the Data Coding Scheme (see TS 23.038 [12]).

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

## 10.3.2 $EF_{IMSI}$ (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 TS 04.08 [15].

- IMSI

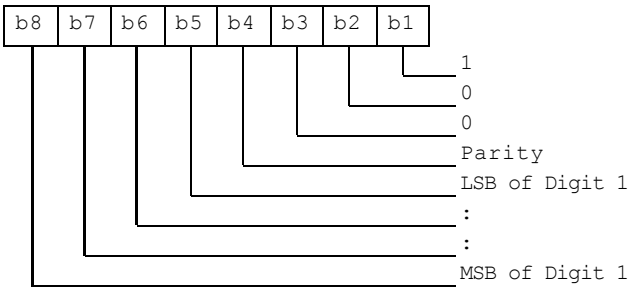
  Contents:

  International Mobile Subscriber Identity.

  Coding:

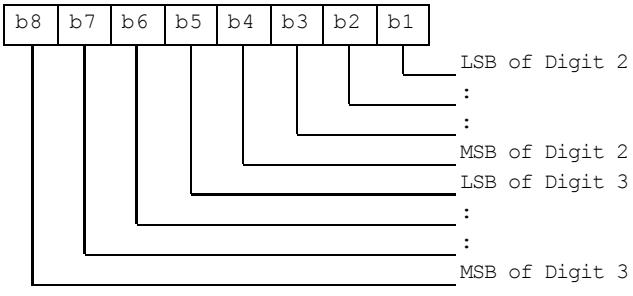
  This information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

  Byte 2:




  For the parity bit, see TS 04.08 [15].

  Byte 3:




  etc.

## 10.3.3 $EF_{Kc}$ (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 |

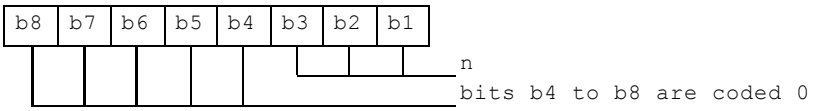
- Ciphering key Kc

  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:




NOTE: TS 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

## 10.3.4 $EF_{PLMNsel}$ (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 TS 04.08 [15].

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.

## 10.3.5 $EF_{HPLMN}$ (HPLMN search period)

This EF contains the interval of time between searches for the HPLMN (see TS 22.011 [5]).

| Identifier: '6F31' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 1 byte | Update activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE ADM<br>INVALIDATE ADM<br>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 TS 22.011 [5].

## 10.3.6 $EF_{ACMmax}$ (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 |

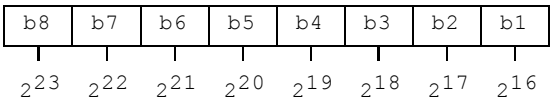
- Maximum value

Contents:

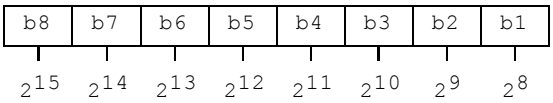
maximum value of the Accumulated Call Meter (ACM)

Coding:

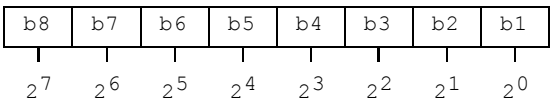
First byte:




Second byte:




Third byte:




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 TS 22.024 [7], if it is coded '000000'.

## 10.3.7 $EF_{SST}$ (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 |
| 6 | Services n°21 to n°24 | O | 1 byte |
| 7 | Services n°25 to n°28 | O | 1 byte |
| 8 | Services n°29 to n°32 | 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 |
| | Service n°18: | Service Dialling Numbers (SDN) |
| | Service n°19: | Extension3 |
| | Service n°20: | RFU |
| | Service n°21: | VGCS Group Identifier List ($EF_{VGCS}$ and $EF_{VGCSS}$) |
| | Service n°22: | VBS Group Identifier List ($EF_{VBS}$ and $EF_{VBSS}$) |
| | Service n°23: | enhanced Multi-Level Precedence and Pre-emption Service |
| | Service n°24: | Automatic Answer for eMLPP |
| | Service n°25: | Data download via SMS-CB |
| | Service n°26: | Data download via SMS-PP |
| | Service n°27: | Menu selection |
| | Service n°28: | Call control |
| | Service n°29: | Proactive SIM |
| | Service n°30: | Cell Broadcast Message Identifier Ranges |
| | Service n°31: | Barred Dialling Numbers (BDN) |
| | Service n°32: | Extension4 |
| | Service n°33: | De-personalization Control Keys |
| | Service n°34: | Co-operative Network List |
| | Service n°35: | Short Message Status Reports |
| | Service n°36: | Network's indication of alerting in the MS |
| | Service n°37: | Mobile Originated Short Message control by SIM |
| | Service n°38: | GPRS |
| | Service n°39: | Image (IMG) |
| | Service n°40: | SoLSA (Support of Local Service Area) |
| | Service n°41: | USSD string data object supported in Call Control |
| | Service n°42: | RUN AT COMMAND command |
| | Service n°43: | User controlled PLMN Selector with Access Technology |
| | Service n 44: | Operator controlled PLMN Selector with Access Technology |
| | Service n 45: | HPLMN Selector with Access Technology |
| | Service n 46: | CPBCCH Information |
| | Service n 47: | Investigation Scan |
| | Service n°48: | Extended Capability Configuration Parameters |
| | Service n°49: | MExE |
| | Service n°50: | RPLMN last used Access Technology |
| | Service n°51: | PLMN Network Name |
| | Service n°52: | Operator PLMN List |
| | Service n°53: | Mailbox Dialling Numbers |
| | Service n°54: | Message Waiting Indication Status |
| | Service n°55: | Call Forwarding Indication Status |
| | Service n°56: | Service Provider Display Information |

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 1: 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.

NOTE 2: As the BDN service relies on the Call Control feature, service n°31 (BDN) should only be allocated and activated if service n°28 (Call control) is allocated and activated.

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.

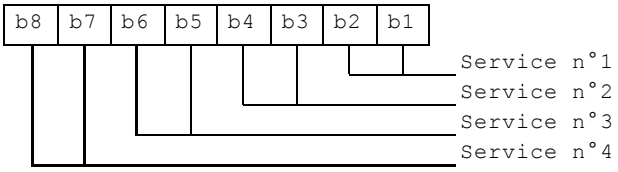
Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:

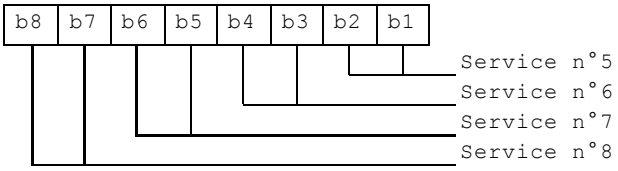
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

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

First byte:

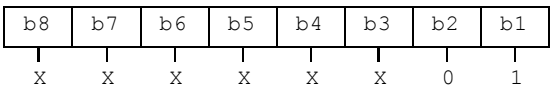



Second byte:




etc.

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




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.

If the SIM supports the BDN feature (BDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both $EF_{IMSI}$ and $EF_{LOCI}$ once during each GSM session and which forbids the REHABILITATE command to rehabilitate both $EF_{IMSI}$ and $EF_{LOCI}$ until the PROFILE DOWNLOAD procedure is performed indicating that the ME

supports the "Call control by SIM" facility. This mechanism shall be invoked by the SIM automatically if BDN is enabled. The invalidation of $EF_{IMSI}$ and $EF_{LOCI}$ shall occur at least before the next command following selection of either EF. BDN is enabled when the $EF_{BDN}$ is not invalidated.

## 10.3.8 $EF_{ACM}$ (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 TS 22.086 [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 $EF_{ACMmax}$

## 10.3.9 $EF_{GID1}$ (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 |

## 10.3.10 $EF_{GID2}$ (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.

## 10.3.11 $EF_{SPN}$ (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 |

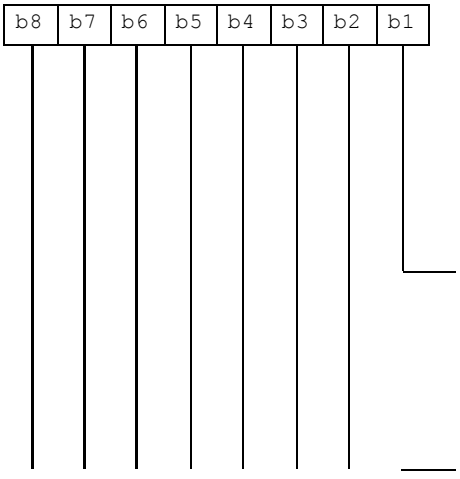
| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Display Condition | M | 1 byte |
| 2 - 17 | Service Provider Name | M | 16 bytes |

- Display Condition

  Contents: display condition for the service provider name in respect to the registered PLMN (see TS 02.0722.101 [53]).

  Coding: see below

  Byte 1:

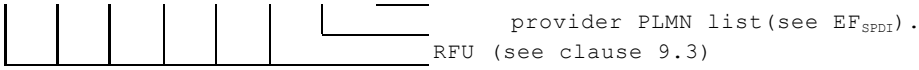



b1=0: display of registered PLMN not required when registered PLMN is either HPLMN or a PLMN in the Service Provider PLMNN List (see $EF_{SPDI}$).

b1=1: display of registered PLMN required when registered PLMN is either HPLMN or a PLMN in the Service Provider PLMN List (see $EF_{SPDI}$).

b2=0: display of the service provider name is required when registered PLMN is neither HPLMN nor a PLMN in the service provider PLMN list(see $EF_{SPDI}$).

b2=1: display of the service provider name is not required when registered PLMN is neither HPLMN nor a PLMN in the service




- Service Provider Name

  Contents: service provider string

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'; or

  - one of the UCS2 code options defined in annex B.

## 10.3.12 $EF_{PUCT}$ (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 TS 22.024 [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 TS 23.038 [12] with bit 8 set to 0.

- Price per unit

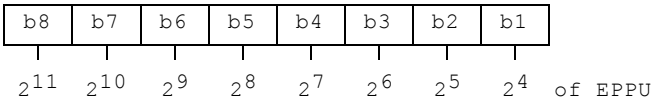
  Contents:

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

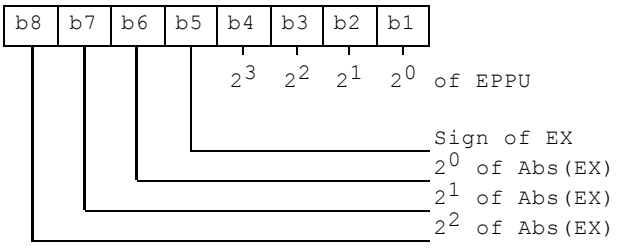
  Coding:

  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:




Byte 5:




The computation of the price per unit value is made by the ME in compliance with TS 22.024 [7] by the following formula:

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

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

## 10.3.13 $EF_{CBMI}$ (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:<br>READ CHV1<br>UPDATE CHV1<br>INVALIDATE ADM<br>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 TS 23.041, "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'.

## 10.3.14 $EF_{BCCH}$ (Broadcast control channels)

This EF contains information concerning the BCCH according to TS 04.08 [15].

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 TS 04.08 [15]. 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 TS 04.08 [15].

## 10.3.15 $EF_{ACC}$ (Access control class)

This EF contains the assigned access control class(es). TS 22.011 [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 TS 22.011 [5].

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

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

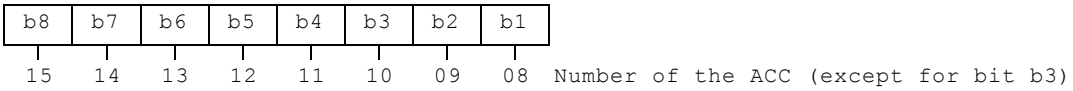
| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 2 | Access control classes | M | 2 bytes |

- Access control classes

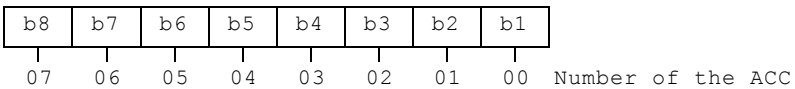
  Coding:

  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:




Byte 2:



## 10.3.16 $EF_{FPLMN}$ (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 TS 04.08 [15].

  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'.

## 10.3.17 $EF_{LOCI}$ (Location information)

This EF contains the following Location Information:

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

In the case when updating $EF_{LOCI}$ with data containing the TMSI value and the card reports the error '92 40' (Memory Problem), the ME shall terminate GSM operation.

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

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | CHV1 |

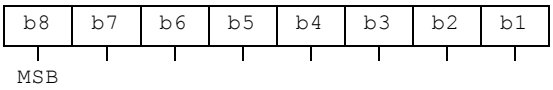
| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 4 | TMSI | M | 4 bytes |
| 5 - 9 | LAI | M | 5 bytes |
| 10 | TMSI TIME | M | 1 byte |
| 11 | Location update status | M | 1 byte |

- TMSI

Contents: Temporary Mobile Subscriber Identity

Coding: according to TS 04.08 [15].

Byte 1: first byte of TMSI

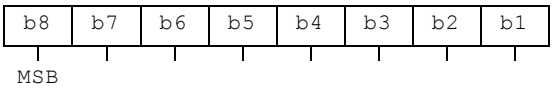



- LAI

Contents: Location Area Information

Coding: according to TS 04.08 [15].

Byte 5: first byte of LAI




- 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 TS 04.08 [15].

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 clause 9.3).

## 10.3.18 $EF_{AD}$ (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 as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

| 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 to 3 | Additional information | M | 2 bytes |
| 4 | length of MNC in the IMSI | O | 1 byte |
| 5 to 4+X | RFU | O | X bytes |

- MS operation mode

  Contents: mode of operation for the MS

  Coding:

  Initial value

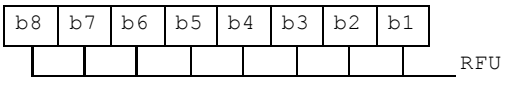
  - normal operation '00'
  - type approval operations '80'
  - normal operation + specific facilities '01'
  - type approval operations + specific facilities '81'
  - maintenance (off line) '02'
  - cell test operation '04'

- Additional information

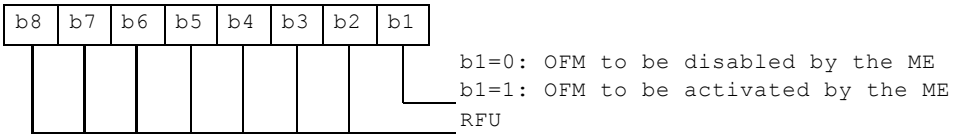
  Coding:

  - specific facilities (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):



Byte 3:




The OFM bit is used to control the Ciphering Indicator as specified in TS 02.07 [3]

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

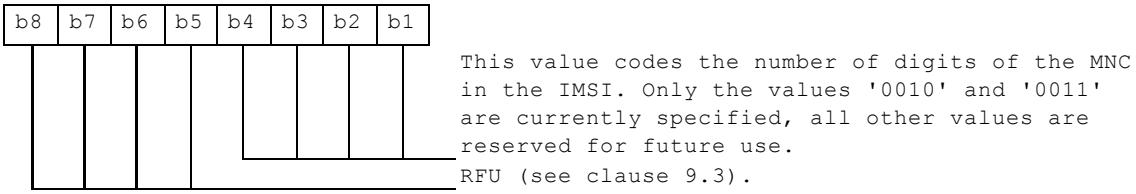
- Length of MNC in the IMSI :

Contents:

The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

Coding:

Byte 4:




## 10.3.19 $EF_{Phase}$ (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:<br>READ ALW<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

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

- SIM Phase

Coding:

'00': phase 1

'02': phase 2

'03': phase 2 and PROFILE DOWNLOAD required (see TS 11.14 [27]).

All other codings are reserved for specification by ETSI TC SMG. Codings '04' to '0F' indicate that the SIM supports, as a minimum, the mandatory requirements defined in this specification.

This phase identification does not preclude a SIM to support some features of a phase later than the one indicated in $EF_{Phase}$. For example : if $EF_{Phase}$ is coded '00', it may be assumed by the ME that some Phase 2 or Phase 2+ features are supported by this SIM; if $EF_{Phase}$ is coded '02' or '03', 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 or later with $EF_{Phase}$ being coded '02' or greater. Similarly, service n°31 (BDN) shall only be allocated and activated in SIMs with $EF_{Phase}$ being coded '03' or greater.

If $EF_{Phase}$ is coded '03' or greater, an ME supporting SIM Application Toolkit shall perform the PROFILE DOWNLOAD procedure, as defined in TS 11.14 [27].

## 10.3.20 $EF_{VGCS}$ (Voice Group Call Service)

This EF contains a list of those VGCS group identifiers the user has subscribed to. The elementary file is used by the ME for group call establishment and group call reception.

| Identifier: '6FB1' | Structure: transparent | Optional |
|---|---|---|
| File size: 4n bytes (n <= 50) | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 4 | Group ID 1 | M | 4 bytes |
| 5 - 8 | Group ID 2 | O | 4 bytes |
| : | : | : | : |
| (4n-3)-4n | Group ID n | O | 4 bytes |

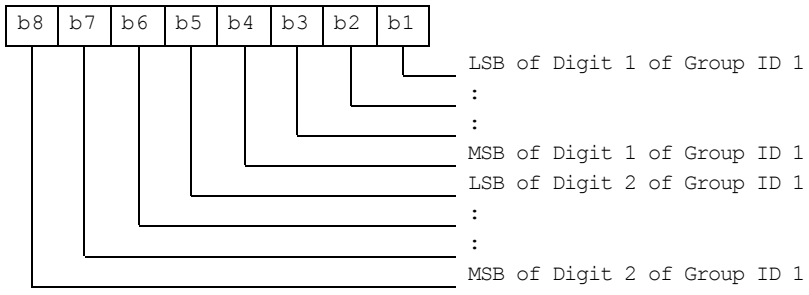
- Group ID

  Contents: VGCS Group ID, according to TS 23.003 [10]

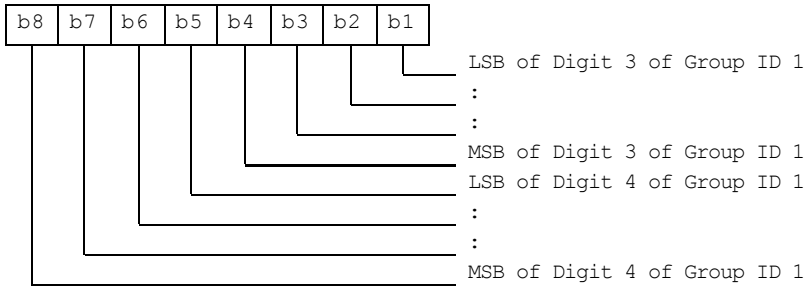
  Coding:

  The VGCS Group ID is of a variable length with a maximum length of 8 digits. Each VGCS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VGCS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VGCS Group ID Digit 1 is the most significant digit of the Group ID.

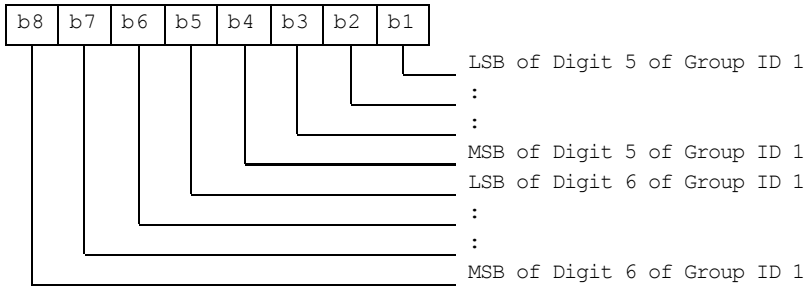
  Byte 1:



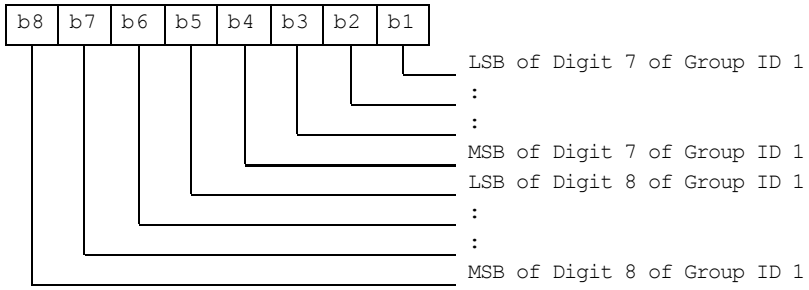
Byte 2:




Byte 3:



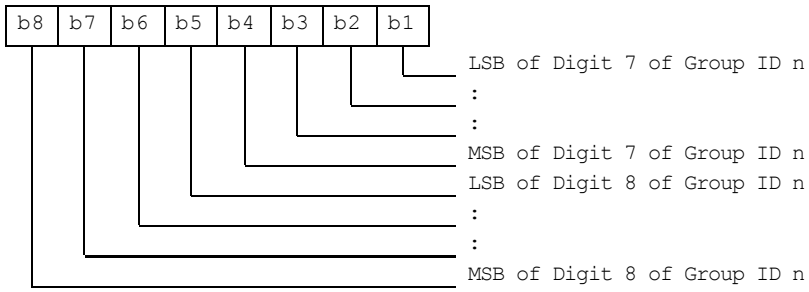

Byte 4:




:

: etc.....

Byte (4n-3)-4n:




If storage for fewer than the maximum possible number *n* of VGCS Group IDs, is required, the excess bytes shall be set to 'FF'.

## 10.3.21 $EF_{VGCSS}$ (Voice Group Call Service Status)

This EF contains the status of activation for the VGCS group identifiers. The elementary file is directly related to the $EF_{VGCS}$. This EF shall always be allocated if $EF_{VGCS}$ is allocated.

| Identifier: '6FB2' | Structure: transparent | Optional |
|---|---|---|
| File size: 7 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 7 | Activation/Deactivation Flags | M | 7 bytes |

- Activation/Deactivation Flags

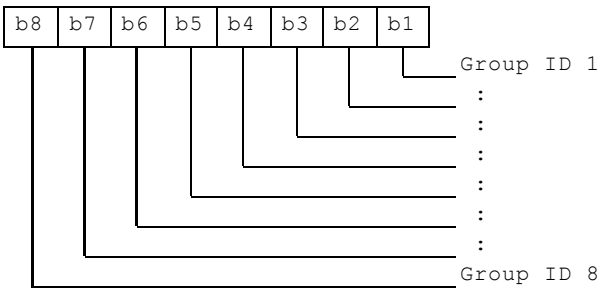
  Contents: Activation/Deactivation Flags of the appropriate Group IDs

  Coding:

  bit = 0 means - Group ID deactivated

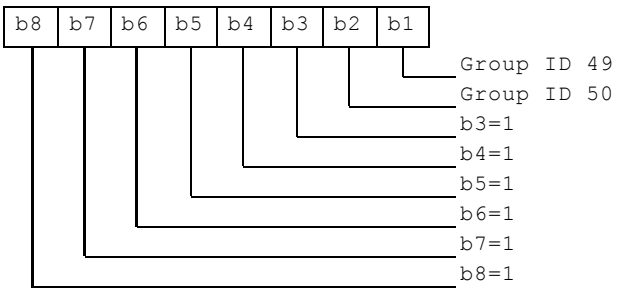
  bit = 1 means - Group ID activated

  Byte 1:




  etc : : : : : : : :

  Byte 7:




## 10.3.22 $EF_{VBS}$ (Voice Broadcast Service)

This EF contains a list of those VBS group identifiers the user has subscribed to. The elementary file is used by the ME for broadcast call establishment and broadcast call reception.

| Identifier: '6FB3' | Structure: transparent | Optional |
|---|---|---|
| File size: 4n bytes (n <= 50) | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 4 | Group ID 1 | M | 4 bytes |
| 5 - 2 | Group ID 2 | O | 4 bytes |
| : | : | : | : |
| (4n-3)-4n | Group ID n | O | 4 bytes |

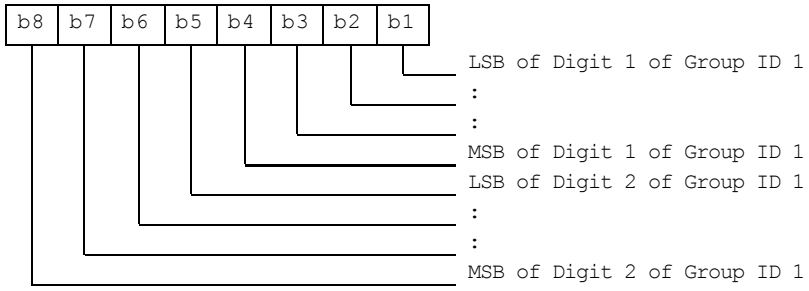
- Group ID

Contents: VBS Group ID, according to TS 23.003 [10]

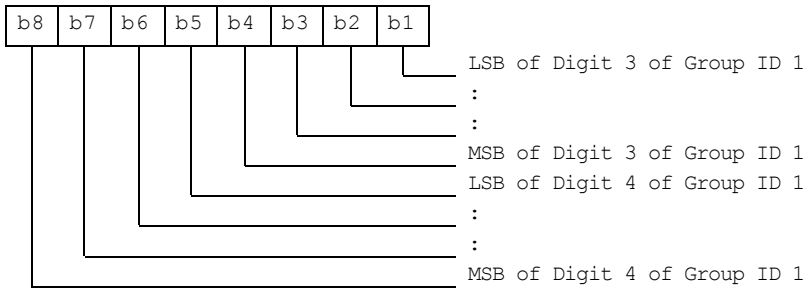
Coding:

The VBS Group ID is of a variable length with a maximum length of 8 digits. Each VBS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VBS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VBS Group ID Digit 1 is the most significant digit of the Group ID.

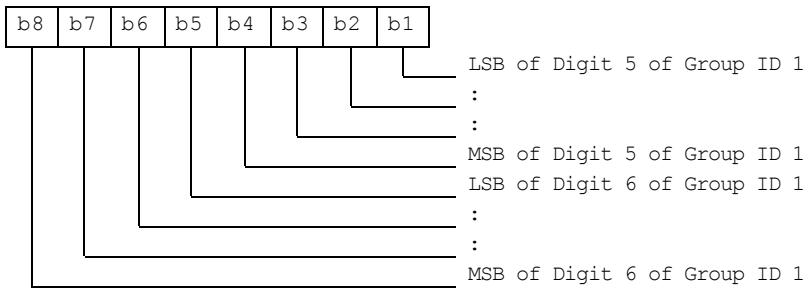
Byte 1:



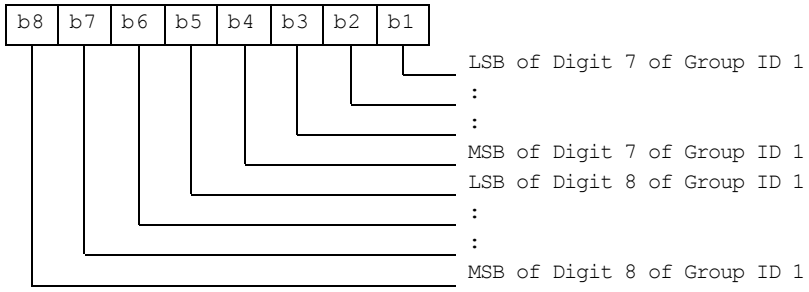

Byte 2:




Byte 3:

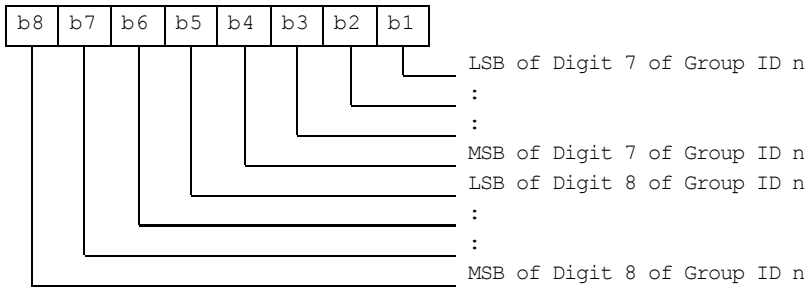


Byte 4:




:
: etc.....

Byte (4n-3)-4n:




If storage for fewer than the maximum possible number *n* of VBS Group IDs, is required, the excess bytes shall be set to 'FF'.

## 10.3.23 $EF_{VBSS}$ (Voice Broadcast Service Status)

This EF contains the status of activation for the VBS group identifiers. The elementary file is directly related to the $EF_{VBS}$. This EF shall always be allocated if $EF_{VBS}$ is allocated.

| Identifier: '6FB4' | Structure: transparent | Optional |
|---|---|---|
| File size: 7 bytes | Update activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 7 | Activation/Deactivation Flags | M | 7 bytes |

- Activation/Deactivation Flags

  Contents: Activation/Deactivation Flags of the appropriate Group IDs

  Coding:

  see coding of $EF_{VGCS}$

## 10.3.24 $EF_{eMLPP}$ (enhanced Multi Level Pre-emption and Priority)

This EF contains information about priority levels and fast call set-up conditions for the enhanced Multi Level Pre-emption and Priority service that which can be used by the subscriber.

| Identifier: '6FB5' | Structure: transparent | Optional |
|---|---|---|
| File size: 2 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

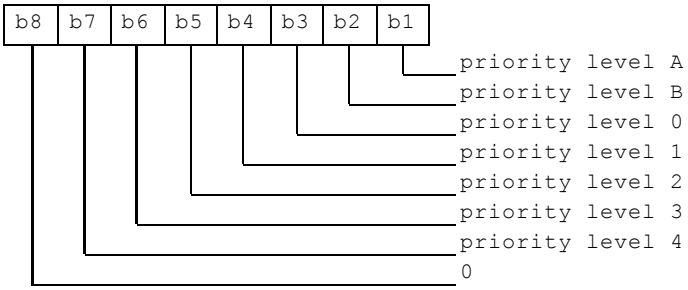
| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Priority levels | M | 1 byte |
| 2 | Fast call set-up conditions | M | 1 byte |

- Priority levels

  Contents: The eMLPP priority levels subscribed to.

  Coding: Each eMLPP priority level is coded on one bit. Priority levels subscribed to have their corresponding bits set to 1. Priority levels not subscribed to have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 1:




NOTE: Priority levels A and B can not be subscribed to (see TS 22.067 [42] for details).

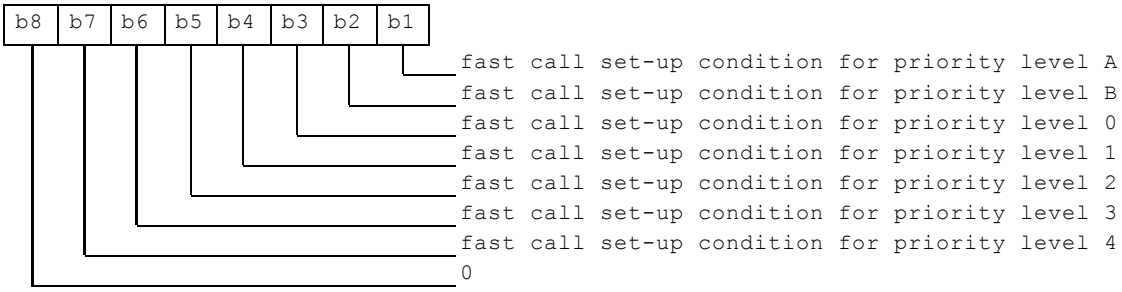
EXAMPLE 1: If priority levels 0, 1 and 2 are subscribed to, $EF_{eMLPP}$ shall be coded '1C'.

- Fast call set-up conditions

  Contents: For each eMLPP priority level, the capability to use a fast call set-up procedure.

  Coding: Each eMLPP priority level is coded on one bit. Priority levels for which fast call set-up is allowed have their corresponding bits set to 1. Priority levels for which fast call set-up is not allowed have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 2: fast call set-up condition for:




EXAMPLE 2: If fast call set-up is allowed for priority levels 0 and 1, then byte 2 of $EF_{eMLPP}$ is coded '0C'.

## 10.3.25 $EF_{AAeM}$ (Automatic Answer for eMLPP Service)

This EF contains those priority levels (of the Multi Level Pre-emption and Priority service) for which the mobile station shall answer automatically to incoming calls.

| Identifier: '6FB6' | Structure: transparent | Optional |
|---|---|---|
| File size: 1 byte | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Automatic answer priority levels | M | 1 byte |

- Automatic answer priority levels

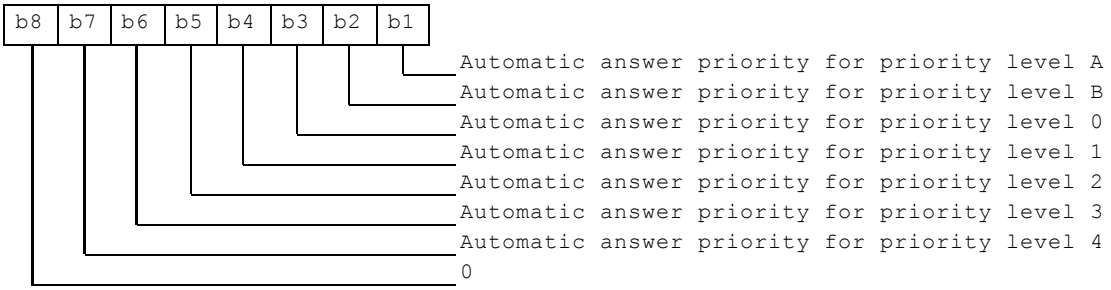
  Contents:

  For each eMLPP priority level, the capability for the mobile station to answer automatically to incoming calls (with the corresponding eMLPP priority level).

  Coding:

  Each eMLPP priority level is coded on one bit. Priority levels allowing an automatic answer from the mobile station have their corresponding bits set to 1. Priority levels not allowing an automatic answer from the mobile station have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 1:




EXAMPLE: If automatic answer is allowed for incoming calls with priority levels A, 0 and 1, then $EF_{AAeMLPP}$ is coded '0D'.

## 10.3.26 $EF_{CBMID}$ (Cell Broadcast Message Identifier for Data Download)

This EF contains the message identifier parameters which specify the type of content of the cell broadcast messages which are to be passed to the SIM.

Any number of CB message identifier parameters may be stored in the SIM. No order of priority is applicable.

| Identifier: '6F48' | Structure: transparent | Optional |
|---|---|---|
| File size: 2n bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| 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 TS 23.041 [14]. Values listed show the identifiers of messages which shall be accepted by the MS to be passed to the SIM.

  Unused entries shall be set to 'FF FF'.

## 10.3.27 $EF_{ECC}$ (Emergency Call Codes)

This EF contains up to 5 emergency call codes.

| Identifier: '6FB7' | Structure: transparent | Optional |
|---|---|---|
| File size: 3n (n ≤ 5) bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALW |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 3 | Emergency Call Code 1 | O | 3 bytes |
| 4 - 6 | Emergency Call Code 2 | O | 3 bytes |
| | | | |
| (3n-2) - 3n | Emergency Call Code n | O | 3 bytes |

- Emergency Call Code

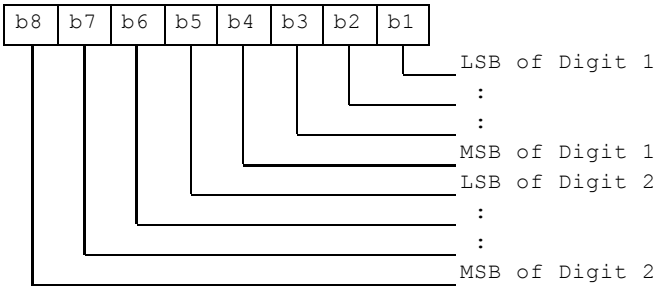
  Contents:

  Emergency Call Code

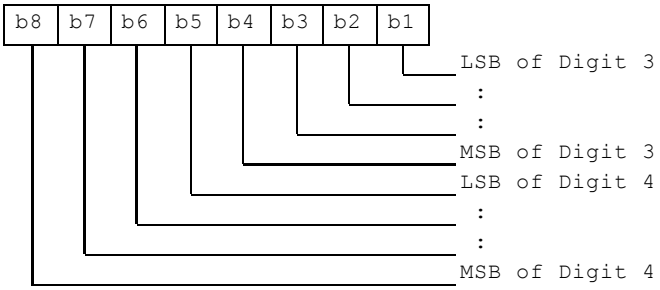
  Coding:

  The emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of less that 6 digits is chosen, then the unused nibbles shall be set to 'F'.

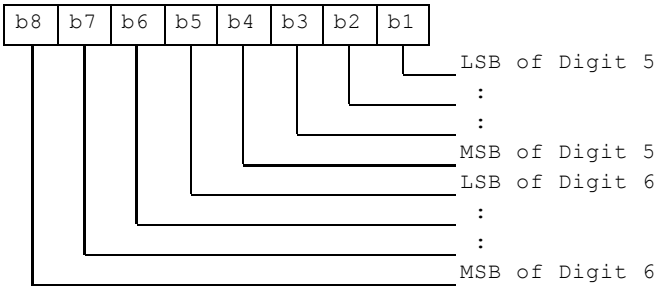
Byte 1:




Byte 2:




Byte 3:




## 10.3.28 $EF_{CBMIR}$ (Cell broadcast message identifier range selection)

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the MS to accept.

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

| Identifier: '6F50' | Structure: transparent | Optional |
|---|---|---|
| File size: 4n bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 4 | CB Message Identifier Range 1 | O | 4 bytes |
| 5 - 8 | CB Message Identifier Range 2 | O | 4 bytes |
| | | | |
| (4n-3) - 4n | CB Message Identifier Range n | O | 4 bytes |

- Cell Broadcast Message Identifier Ranges

  Contents:

CB Message Identifier ranges:

Coding:

bytes one and two of each range identifier equal the lower value of a cell broadcast range, bytes three and four equal the upper value of a cell broadcast range, both values are coded as in TS 23.041 [14] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the MS.

Unused entries shall be set to 'FF FF FF FF'.

## 10.3.29 $EF_{DCK}$ De-personalization Control Keys

This EF provides storage for the de-personalization control keys associated with the OTA de-personalization cycle of TS 22.022.

| Identifier: '6F2C' | Structure: transparent | Optional |
|---|---|---|
| File size: 16 bytes | Update activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE CHV1<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 4 | 8 digits of network de-personalization control key | M | 4 bytes |
| 5 to 8 | 8 digits of network subset de-personalization control key | M | 4 bytes |
| 9 to 12 | 8 digits of service provider de-personalization control key | M | 4 bytes |
| 13 to 16 | 8 digits of corporate de-personalization control key | M | 4 bytes |

Empty control key records shall be coded 'FFFFFFFF'.

## 10.3.30 $EF_{CNL}$ (Co-operative Network List)

This EF contains the Co-operative Network List for the multiple network personalization services defined in TS 22.022.

| Identifier: '6F32' | Structure: transparent | Optional |
|---|---|---|
| File size: 6n bytes | Update activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 6 | Element 1 of co-operative net list | O | 6 bytes |
| | | | |
| 6n-5 to 6n | Element n of co-operative net list | O | 6 bytes |

- Co-operative Network List

Contents:

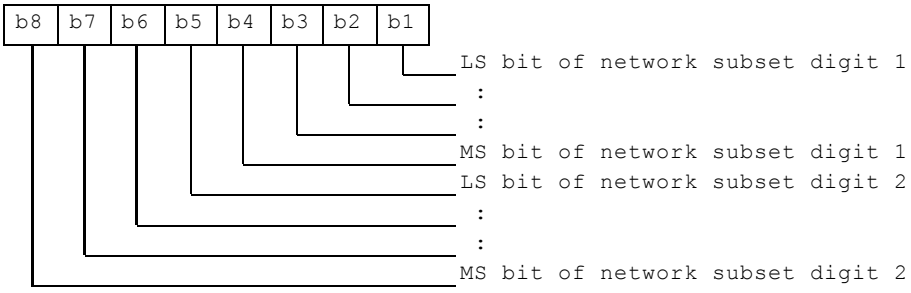
PLMN network subset, service provider ID and corporate ID of co-operative networks.

Coding:

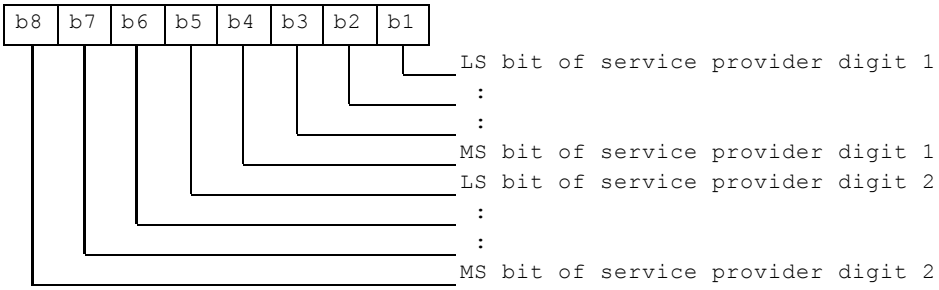
For each 6 byte list element

Byte 1 to 3 : PLMN (MCC + MNC) : according to TS 04.08 [15].

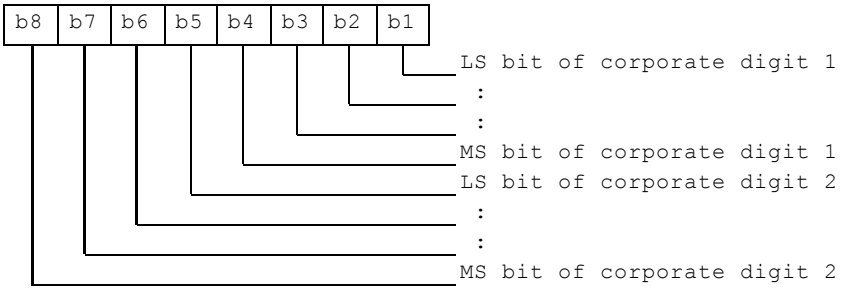
Byte 4:




Byte 5:




Byte 6:




Empty fields shall be coded with 'FF'.

The end of the list is delimited by the first MCC field coded 'FFF'.

## 10.3.31 $EF_{NIA}$ (Network's Indication of Alerting)

This EF contains categories and associated text related to the Network's indication of alerting in the MS service defined in TS 02.07 [3].

| Identifier: '6F51' | Structure: linear fixed | Optional |
|---|---|---|
| Record length : X+1 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Alerting category | M | 1 byte |
| 2 to X+1 | Informative text | M | X bytes |

- Alerting category

  Contents:

  category of alerting for terminating traffic.

  Coding:

  according to TS 04.08 [15]. Value 'FF' means that no information on alerting category is available.

- Informative text

  Contents:

  text describing the type of terminating traffic associated with the category.

  Coding:

  see the coding of the Alpha Identifier item of the $EF_{ADN}$ (clause 10.5.1). The maximum number of characters for this informative text is indicated in TS 02.07 [3].

## 10.3.32 $EF_{KcGPRS}$ (GPRS Ciphering key KcGPRS)

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see TS 23.060 [32]).

| Identifier: '6F52' | Structure: transparent | Optional |
|---|---|---|
| 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 KcGPRS | M | 8 bytes |
| 9 | Ciphering key sequence number n for GPRS | M | 1 byte |

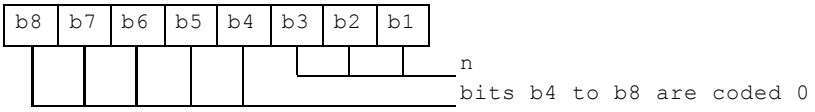
- Ciphering key KcGPRS

  Coding:

  The least significant bit of KcGPRS is the least significant bit of the eighth byte. The most significant bit of KcGPRS is the most significant bit of the first byte.

- Ciphering key sequence number n for GPRS

  Coding:




NOTE: TS 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

## 10.3.33 $EF_{LOCIGPRS}$ (GPRS location information)

This EF contains the following Location Information:

- Packet Temporary Mobile Subscriber Identity (P-TMSI);
- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);

- Routing Area Information (RAI);
- Routing Area update status.

| Identifier: '6F53' | Structure: transparent | Optional |
|---|---|---|
| File size: 14 bytes | Update activity: high | |
| Access Conditions:<br>READ CHV1<br>UPDATE CHV1<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

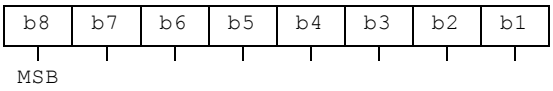
| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 4 | P-TMSI | M | 4 bytes |
| 5 – 7 | P-TMSI signature value | M | 3 bytes |
| 8 - 13 | RAI | M | 6 bytes |
| 14 | Routing Area update status | M | 1 byte |

- P-TMSI

  Contents: Packet Temporary Mobile Subscriber Identity

  Coding: according to TS 04.08 [15].

  Byte 1: first byte of P-TMSI

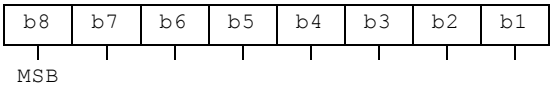



- P-TMSI signature value

  Contents: Packet Temporary Mobile Subscriber Identity signature value

  Coding: according to TS 04.08 [15].

  Byte 5: first byte of P-TMSI signature value

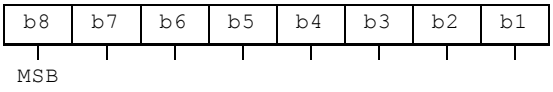



- RAI

  Contents: Routing Area Information

  Coding: according to TS 04.08 [15].

  Byte 8: first byte of RAI




- Routing area update status

  Contents: status of routing area update according to TS 04.08 [15].

  Coding:

  Byte 14:

  Bits: b3 b2 b1

0 0 0 : updated
0 0 1 : not updated
0 1 0 : PLMN not allowed
0 1 1 : Routing Area not allowed
1 1 1 : reserved

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

## 10.3.34 $EF_{SUME}$ (SetUpMenu Elements)

This EF contains Simple TLVs related to the menu title to be used by a SIM card supporting the SIM API when issuing a SET UP MENU proactive command.

| Identifier: '6F54' | Structure: transparent | Optional |
|---|---|---|
| File size: X+Y bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ADM |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - X | Title Alpha Identifier | M | X bytes |
| 1+X - X+Y | Title Icon Identifier | O | Y bytes |

- Title Alpha Identifier

  Contents:

  this field contains the Alpha Identifier Simple TLV defining the menu title text.

  Coding:

  according to TS 11.14 [27].

- Title Icon Identifier

  Contents:

  this field contains the Icon Identifier Simple TLV defining the menu title icon.

  Coding:

  according to GSM 11.14 [27].
  If not present the field shall be set to 'FF'.

  Unused bytes of this file shall be set to 'FF'.

## 10.3.35 $EF_{PLMNwAcT}$ (User controlled PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the user, defines the preferred PLMNs of the user in priority order. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [51]).

| Identifier:'6F60' | Structure: transparent | Optional |
|---|---|---|
| File size: 5n (n ≥ 8) bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 3 | 1st PLMN (highest priority) | M | 3 bytes |
| 4 to 5 | 1st PLMN Access Technology Identifier | M | 2 bytes |
| 6 to 8 | 2nd PLMN | M | 3 bytes |
| 9 to 10 | 2nd PLMN Access Technology Identifier | M | 2 bytes |
| : | : | | |
| 36 to 38 | 8th PLMN | M | 3 bytes |
| 39 to 40 | 8th PLMN Access Technology Identifier | M | 2 bytes |
| 41 to 43 | 9th PLMN | O | 3 bytes |
| 44 to 45 | 9th PLMN Access Technology Identifier | O | 2 bytes |
| : | : | | |
| (5n-4) to (5n-2) | Nth PLMN (lowest priority) | O | 3 bytes |
| (5n-1) to 5n | Nth PLMN Access Technology Identifier | O | 2 bytes |

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

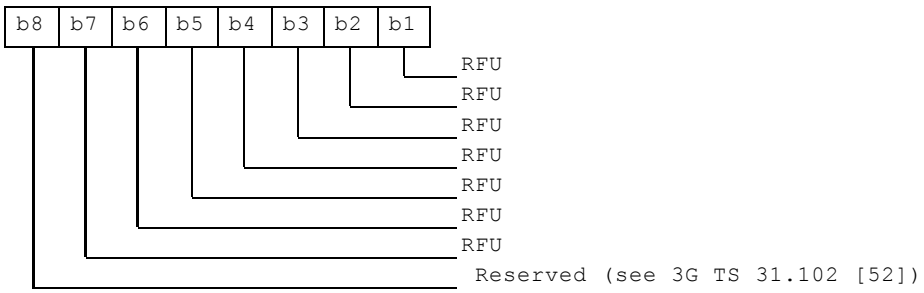
  according to TS 24.008 [47].

- Access Technologies

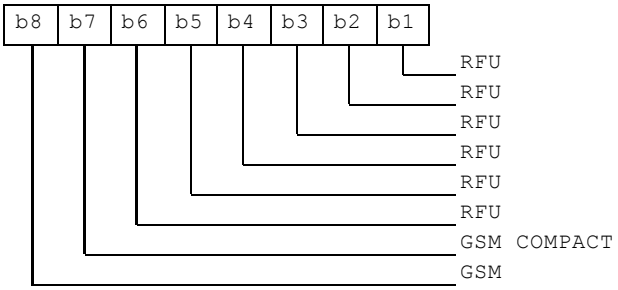
  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding:
  - 2 bytes are used to select the access technology where the meaning of each bit is as follows:
    - bit = 1: access technology selected;
    - bit = 0: access technology not selected.

Byte 5n-1:




Byte 5n:




The RFU bits are coded with '0' in the bit positions.

## 10.3.36 $EF_{OPLMNwAcT}$ (Operator controlled PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the operator, defines the preferred PLMNs of the operator in priority order. The EF also contains the Access Technologies for each PLMN in this list (see TS 23.122 [51]).

| Identifier: '6F61' | Structure: transparent | Optional |
|---|---|---|
| File size: 5n (n ≥ 8) bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 3 | 1st PLMN (highest priority) | M | 3 bytes |
| 4 to 5 | 1st PLMN Access Technology Identifier | M | 2 bytes |
| : | : | | |
| 36 to 38 | 8th PLMN | M | 3 bytes |
| 39 to 40 | 8th PLMN Access Technology Identifier | M | 2 bytes |
| 41 to 43 | 9th PLMN | O | 3 bytes |
| 44 to 45 | 9th PLMN Access Technology Identifier | O | 2 bytes |
| : | : | | |
| (5n-4) to (5n-2) | Nth PLMN (lowest priority) | O | 3 bytes |
| (5n-1) to 5n | Nth PLMN Access Technology Identifier | O | 2 bytes |

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

- Access Technologies

  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding: See $EF_{PLMNwAcT}$ for coding.

## 10.3.37 $EF_{HPLMNwAcT}$ (HPLMN Selector with Access Technology)

The HPLMN Selector with access technology data field shall contain the HPLMN code, or codes together with the respective access technology in priority order (see TS 23.122 [51]).

| Identifier: '6F62' | Structure: transparent | Optional |
|---|---|---|
| File size: 5n bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 3 | 1st PLMN (highest priority) | M | 3 bytes |
| 4 to 5 | 1st PLMN Access Technology Identifier | M | 2 bytes |
| 6 to 8 | 2nd PLMN | O | 3 bytes |
| 9 to 10 | 2nd PLMN Access Technology Identifier | O | 2 bytes |
| : | : | | |
| (5n-4) to (5n-2) | Nth PLMN (lowest priority) | O | 3 bytes |
| (5n-1) to 5n | Nth PLMN Access Technology Identifier | O | 2 bytes |

- PLMN
  Contents:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:
  according to TS 24.008 [47].

- Access Technology

  Contents: The Access Technology of the HPLMN that the MS will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

  Coding: See $EF_{PLMNwAcT}$ for coding.

## 10.3.38 $EF_{CPBCCH}$ (CPBCCH Information)

This EF contains information concerning the CPBCCH according to TS 04.18 [48] and TS 03.22 [45].

CPBCCH storage may reduce the extent of a Mobile Station's search of CPBCCH carriers when selecting a cell. The CPBCCH carrier lists shall be in accordance with the procedures specified in TS 04.18 [48], TS 04.60 [49] and TS 03.22 [45]. The MS stores CPBCCH information from the System Information 19 message, Packet System Information 3, and Packet System Information 3 bis on the SIM. The same CPBCCH carrier shall never occur twice in the list.

| Identifier: '6F63' | Structure: transparent | Optional |
|---|---|---|
| File size: 2n bytes | Update activity: high | |

Access Conditions:

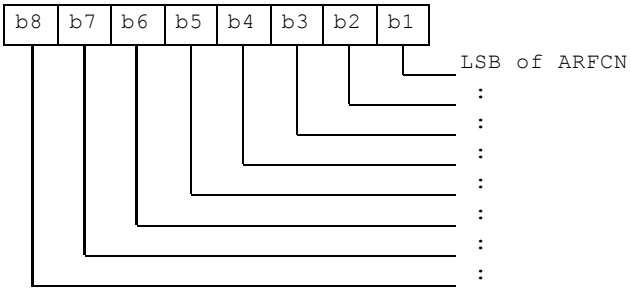
| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 2 | Element 1 of CPBCCH carrier list | M | 2 bytes |
| | | | |
| 2n-1 to 2n | Element n of CPBCCH carrier list | M | 2 bytes |

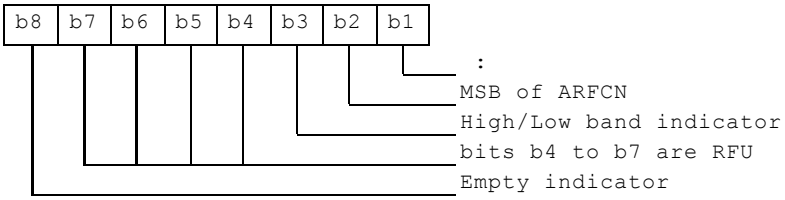
- Element in CPBCCH carrier list

  Coding:

  Byte 1: first byte of CPBCCH carrier list element




  Byte 2: second byte of CPBCCH carrier list element




  - ARFCN (10 bits) as defined in TS 05.05 [46].
  - High/Low band indicator: If the ARFCN indicates possibly a channel in the DCS 1800 or a channel in the PCS 1900 band, if the bit is set to '1' the channel is in the higher band (GSM 1900). If the bit is set to '0', the lower band (GSM 1800) is indicated. If ARFCN indicates a unique channel, this indicator shall be set to '0'.
  - Empty indicator: If this bit is set to '1', no CPBCCH carrier is stored in this position. If the Empty Indicator is set to '1', the content of the CPBCCH carrier field shall be ignored. The empty indicator shall also be used, and set to '1', if storage of fewer than maximum number n, of CPBCCH carrier fields is required.

## 10.3.39 $EF_{InvScan}$ (Investigation Scan)

This EF contains two flags used to control the investigation scan for higher prioritized PLMNs not offering voice services.

| Identifier: '6F64' | Structure: transparent | Optional |
|---|---|---|
| File size: 1 byte | Update activity: low | |

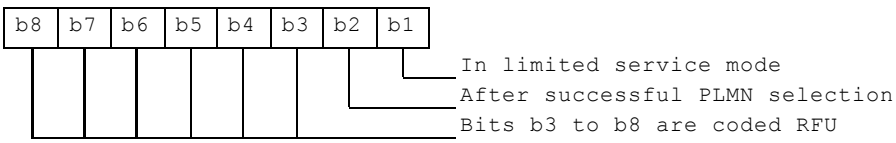
Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Investigation scan flags | M | 1 bytes |

- Investigation scan flags

  Coding:



A '1' in a bit position indicates that the investigation scan shall be performed for the condition corresponding to that bit position and a '0' that it shall not be performed.

If this elementary file is not present, no investigation scan shall be performed.

## 10.3.40 $EF_{RPLMNAcT}$ (RPLMN Last used Access Technology)

This EF contains the last used access technology for the Registered PLMN, RPLMN. (see TS 23.122 [50]). This EF shall contain only one access technology.

NOTE: One access technology means that only one bit is set in the entire field.

If this EF does not exist on the SIM, then the MS shall assume that RPLMN access technology is GSM.

| Identifier: '6F5F' | Structure: transparent | Optional |
|---|---|---|
| File size: 2+X bytes | Update activity: High | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 2 | Access Technology of RPLMN | M | 2 bytes |
| 3 to 2+X | RFU | O | X bytes |

- Access Technology

  Coding:

  - See $EF_{PLMNwAcT}$ for coding.

## 10.3.41 $EF_{PNN}$ (PLMN Network Name)

This EF contains the full and short form versions of the network name for the registered PLMN. The ME shall use these versions in place of its own versions of the network name for the PLMN (stored in the ME's memory list), and also in place of the versions of the network name received when registered to the PLMN, as defined by 3G TS 24.008 [47].

The first record in this EF is used for the default network name when registered to the HPLMN. Subsequent records are to be used for other network names.

| Identifier: '6FC5' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALWAYS |
| UPDATE | ADM |
| ACTIVATE | ADM |
| DEACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to X | Network name TLV objects | M | X bytes |

- Network Name TLV objects.
  The content and coding (Full name for network and Short name for network) is defined below, where the fields within the objects are defined in 3G TS 24.008 [47]:

**Coding of the Network Name TLV objects**

| Length | Description | Status |
|---|---|---|
| 1 byte | Full name for network IEI (This shall be the same as that used in the MM information message). | M |
| 1 byte | Length of Full name for network Name contents | M |
| Y bytes | Full name for network contents (Octets 3 to n of network name information element) | M |
| 1 byte | Short name for network IEI (This shall be the same as that used in the MM information message). | O |
| 1 byte | Length of Short name for network | C1 |
| Z bytes | Short name for network contents (Octets 3 to n of network name information element) | C1 |
| C1: this field shall be present if the short name for network IEI is present | | |

Unused bytes shall be set to 'FF'.

## 10.3.42 $EF_{OPL}$ (Operator PLMN List)

This EF contains a prioritised list of Location Area Information (LAI) identities that are used to associate a specific operator name contained in $EF_{PNN}$ with the LAI. The ME shall use this EF in association with the $EF_{PNN}$ in place of any network name stored within the ME's internal list and any network name received when registered to the PLMN, as defined by 3G TS 24.008 [47].

If the $EF_{PNN}$ is not present then this file shall not be present.

| Identifier: '6FC6' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X bytes, X >= 8 | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALWAYS |
| UPDATE | ADM |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 7 | Location Area Identity | M | 7 bytes |
| 8 | PLMN Network Name Record Identifier | M | 1 byte |

- Location Area Identity

  Contents:

  Location Area Information, this comprises of the MCC, MNC and two LACs

  Coding:

  PLMN: according to TS 24.008 [47]

  A BCD value of 'D' in any of the MCC and/or MNC digits shall be used to indicate a "wild" value for that corresponding MCC/MNC digit

  LAC : according to 3G TS 24.008 [47]

  Two values for the LAC are stored in order to allow a range of LAC values to be specified for a given PLMN. A value of '0000' stored in bytes 4 to 5 and a value of 'FFFE' stored in bytes 6 to 7 shall be used to indicate the entire range of LACs for the given PLMN. In the case where only a single LAC value is to be specified then the value stored in bytes 4 to 5 shall be identical to the value stored in bytes 6 to 7 for the given PLMN. If a

range of LAC values are to be specified, then the value stored in bytes 4 to 5 shall be the start of the LAC range and the value stored in bytes 6 to 7 shall be the end of the LAC range for the given PLMN.

- PLMN Network Name Record Identifier

  Contents:

  Identifier of operator name to be displayed

  Coding:

  A value of '00' indicates that the name is to be taken from other sources, see 3G TS 22.101 [53]

  A value in the range '01' to 'FE' indicates the record number in $EF_{PNN}$ that shall be displayed as the registered PLMN name

NOTE: The intent of this file is to provide exceptions to the other sources of a network name. Care should be taken not to introduce too many PLMN entries. An excessive number of entries could result in a longer initialisation period.

## 10.3.43 $EF_{MBDN}$ (Mailbox Dialling Numbers)

This EF contains dialling numbers to access mailboxes associated with Voicemail, Fax, Electronic Mail and other messages. It may also contain associated alpha-tags for each supported mailbox. Each dialling number shall be associated with a message waiting indication group type using $EF_{MBI}$ (see 3G TS 23.038 [12] for message waiting indication group types).

This EF is mandatory if $EF_{SST}$ indicates that the Mailbox Dialling Numbers service is available.

| Identifier: '6FC7' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X+14 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN/ADM<br>(fixed during administrative management) |
| DEACTIVATE | ADM |
| ACTIVATE | 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 contents | M | 10 bytes |
| X+13 | Extended Capability Configuration Parameters | M | 1 byte |
| X+14 | Extension 6 Record Identifier | M | 1 byte |

For contents and coding of all data items see the respective data items of the $EF_{ADN}$ (clause 10.5.1), with the exception that extension records are stored in the $EF_{EXT6}$ and with the exception that Capability/Configuration parameters are stored in the $EF_{ECCP}$

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

## 10.3.44 $EF_{MBI}$ (Mailbox Identifier)

This EF contains information to associate mailbox dialling numbers in $EF_{MBDN}$ with a message waiting indication group type and subscriber profile (as defined in 3G TS 23.097 [54]). A message waiting indication group type may either be Voicemail, Fax, Electronic Mail or Other (as defined in 3G TS 23.038 [12] for Data Coding Scheme).

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile). Each record contains references to mailbox dialling numbers in $EF_{MBDN}$ (one reference for each message waiting indication group type).

This EF is mandatory if $EF_{SST}$ indicates that the Mailbox Dialling Numbers service is available.

| Identifier: '6FC9' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X bytes, X>=4 | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN/ADM (fixed during administrative management) |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Mailbox Dialling Number Identifier – Voicemail | M | 1 byte |
| 2 | Mailbox Dialling Number Identifier – Fax | M | 1 byte |
| 3 | Mailbox Dialling Number Identifier – Electronic Mail | M | 1 byte |
| 4 | Mailbox Dialling Number Identifier – Other | M | 1byte |

- Mailbox Dialling Number Identifier (message waiting group type = Voicemail, Fax, Electronic Mail or Other).
  Contents:
  Identifies the mailbox dialling number to be associated with message waiting type.

  Coding:
  '00' – no mailbox dialling number associated with message waiting indication group type
  'xx' – record number in $EF_{MBDN}$ associated with message waiting indication group type

## 10.3.45 $EF_{MWIS}$ (Message Waiting Indication Status)

This EF contains the status of indicators that define whether or not a Voicemail, Fax, Electronic Mail or Other message is waiting (as defined in 3G TS 23.038 [12] for message waiting indication group types). The ME uses the status after re-activation to determine whether or not to display the respective message-waiting indication on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in 3G TS 23.097 [54] for MSP.

| Identifier: '6FCA' | Structure: Linear fixed | Optional |
|---|---|---|
| Record length: X bytes, X >= 5 | Update activity: high | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Message Waiting Indicator Status | M | 1 byte |
| 2 | Number of Voicemail Messages Waiting | M | 1 byte |
| 3 | Number of Fax Messages Waiting | M | 1 byte |
| 4 | Number of Electronic Mail Messages Waiting | M | 1 byte |
| 5 | Number of Other Messages Waiting | M | 1 byte |

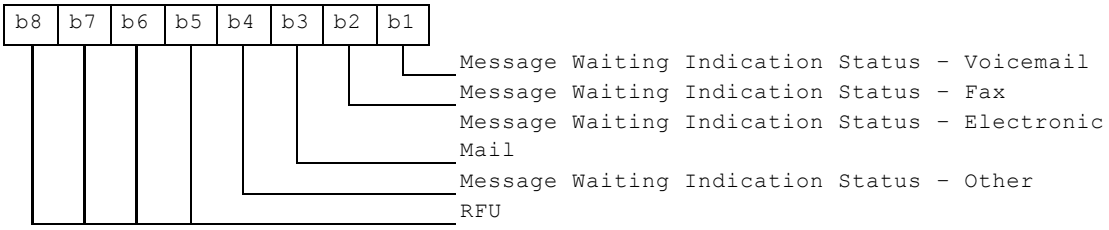
Message Waiting Indication Status
Contents:
Indicates the status of the message-waiting indication.

Coding:

The indicator status for each indicator type is 1 bit long and set as follows:

bit = 1: Set Indication Active

bit = 0: Set Indication Inactive




Number of Voicemail Messages Waiting

Contents:

Contains the number of voicemail messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

Number of Fax Messages Waiting

Contents:

Contains the number of fax messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

Number of Electronic Mail Messages Waiting

Contents:

Contains the number of electronic mail messages waiting (see 3G TS 23.040 [13])

Coding:

Binary.

Number of Other Messages Waiting

Contents:

Contains the number of other messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

## 10.3.46 $EF_{CFIS}$ (Call Forwarding Indication Status)

This EF contains the status of indicators that are used to record whether call forward is active. The ME uses the status after re-activation to determine whether or not to display the respective Call Forwarding indicator on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in 3G TS 23.097 [54] for MSP.

| Identifier: '6FCB' | Structure: Linear Fixed | Optional |
|---|---|---|
| Record length: 16 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | MSP number | M | 1 byte |
| 2 | CFU indicator status | M | 1 byte |
| 3 | Length of BCD number | M | 1 byte |
| 4 | TON and NPI | M | 1 byte |
| 5 to 14 | Dialling Number | M | 10 bytes |
| 15 | Extended Capability Configuration Parameters | M | 1 byte |
| 16 | Extension 7 Record Identifier | M | 1 byte |

NOTE: For contents and coding of data items not detailed below, see the respective data items of $EF_{ADN}$ (subclause 10.5.1), with the exception that Capability/Configuration parameters are stored in the $EF_{ECCP}$ and Extension 7 Record Identifier is used.

MSP number:

Contents:

The MSP number contains the Profile Identity of the subscriber profile. The Profile Identity shall be between 1and 4 as defined in 3G TS 23.097 [54] for MSP.

Coding:

Binary.

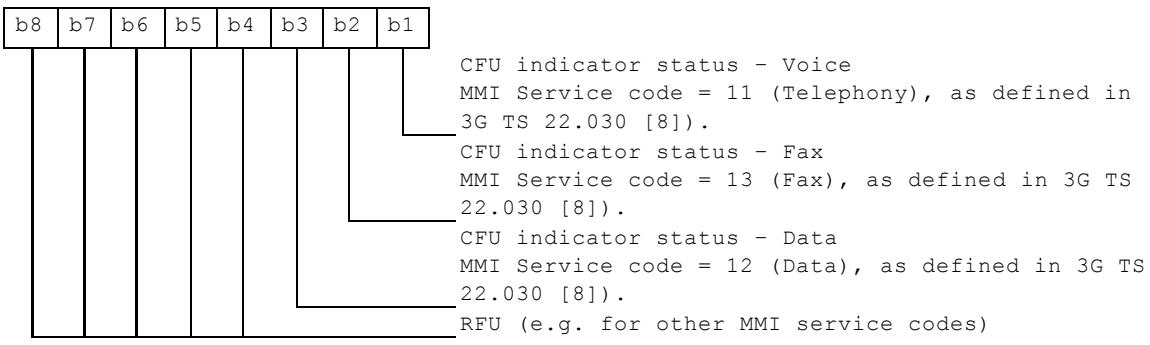
CFU indicator status:

Contents:

Indicates the status of the call forward unconditional indicator. Service code = 21 (CFU) or 002 (for CFU part of all CF), as defined in 3G TS 22.030 [8]

Coding:

The indicator status for each indicator type is 1 bit long and is set as follows:
bit = 1: Set indication active
bit = 0: Set indication inactive



## 10.3.47 $EF_{EXT5}$ (Extension5)

This EF is not used

## 10.3.48 $EF_{EXT6}$ (Extension6)

This EF contains extension data of an MBDN (see MBDN in 10.3.43).

| Identifier: '6FC8' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 13 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN/ADM<br>(fixed during administrative management) |
| DEACTIVATE | ADM |
| ACTIVATE | 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 clause 10.5.10 ($EF_{EXT1}$).

## 10.3.49 $EF_{EXT7}$ (Extension7)

This EF contains extension data of a CFIS (Call Forwarding Indication Status - see 10.3.46).

| Identifier: '6FCC' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 13 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN |
| DEACTIVATE | ADM |
| ACTIVATE | 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 clause 10.5.10 ($EF_{EXT1}$).

## 10.3.50 $EF_{SPDI}$ (Service Provider Display Information)

This EF contains information regarding the service provider display i.e. the service provider PLMN list.

| Identifier: '6FCD' | Structure: transparent | Optional |
|---|---|---|
| File size: x bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to x | TLV object(s) containing Service Provider Information | M | x bytes |

| Tag Value | Tag Description |
|---|---|
| 'A3' | Service Provider Display Information Tag |
| '80' | Service Provider PLMN List Tag |

The Service Provider Display Information object is a constructed TLV.

- Service Provider PLMN List
  Contents:
  This TLV contains a list of n PLMNs in which the Service Provider Name shall be displayed, as defined in subclause 10.3.11 ($EF_{SPN}$).

  Coding:

| Description | M/O | Length |
|---|---|---|
| Service Provider PLMN List tag | M | 1 byte |
| Length (see note) | M | x bytes |
| 1st PLMN entry | M | 3 bytes |
| 2nd PLMN entry | O | 3 bytes |
| 3rd PLMN entry | O | 3 bytes |
| … | | |
| nth PLMN entry | O | 3 bytes |
| Note: the length is 3*n bytes, where n denotes the number of PLMN entries. The length can be coded on one or more bytes. | | |

  Each PLMN is coded as follows:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC) according to TS 24.008 [47].
  In case a PLMN entry is not used, it shall be set to 'FF FF FF'.

# 10.4 Contents of DFs at the GSM application level

## 10.4.1 Contents of files at the GSM SoLSA level

This clause specifies the EFs in the dedicated file $DF_{SoLSA}$. It only applies if the SoLSA feature is supported (see TS 23.073 [33]).

The EFs contain information about the users subscribed local service areas.

### 10.4.1.1 $EF_{SAI}$ (SoLSA Access Indicator)

This EF contains the 'LSA only access indicator'. This EF shall always be allocated if $DF_{SoLSA}$ is present.

If the indicator is set, the network will prevent terminated and/or originated calls when the MS is camped in cells that are not included in the list of allowed LSAs in $EF_{SLL}$. Emergency calls are, however, always allowed.

The EF also contains a text string which may be displayed when the MS is out of the served area(s).

| Identifier: '4F30' | Structure: transparent | Optional |
|---|---|---|
| File size: X + 1 bytes | Update activity: low | |

Access Conditions:

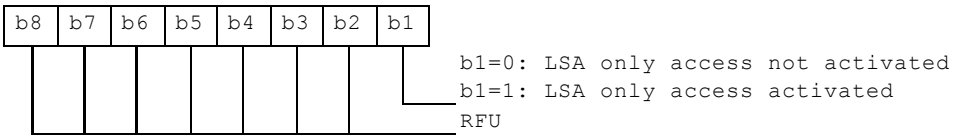
| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | LSA only access indicator | M | 1 byte |
| 2 to X+1 | LSA only access indication text | M | X bytes |

- LSA only access indicator

  Contents: indicates whether the MS is restricted to use LSA cells only or not.

  Coding:




- LSA only access indication text

  Contents: text to be displayed by the ME when it's out of LSA area.

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 coded options as defined in annex B.

### 10.4.1.2 $EF_{SLL}$ (SoLSA LSA List)

This EF contains information describing the LSAs that the user is subscribed to. This EF shall always be allocated if $DF_{SoLSA}$ is present.

Each LSA is described by one record that is linked to a LSA Descriptor file. Each record contains information of the PLMN, priority of the LSA, information about the subscription and may also contain a text string and/or an icon that identifies the LSA to the user. The text string can be edited by the user.

| Identifier: '4F31' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X + 10 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to X | LSA name | O | X bytes |
| X+1 | Configuration parameters | M | 1 byte |
| X+2 | RFU | M | 1 byte |
| X+3 | Icon Identifier | M | 1 byte |
| X+4 | Priority | M | 1 byte |
| X+5 to X+7 | PLMN code | M | 3 bytes |
| X+8 to X+9 | LSA Descriptor File Identifier | M | 2 byte |
| X+10 | LSA Descriptor Record Identifier | M | 1 byte |

- LSA name

  Contents: LSA name string to be displayed when the ME is camped in the corresponding area, dependant on the contents of the LSA indication for idle mode field.

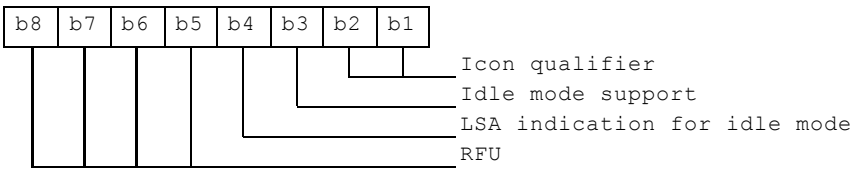
  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 coded options as defined in annex B.

- Configuration parameters

  Contents: Icon qualifier, control of idle mode support and control of LSA indication for idle mode.

  Coding:




Icon qualifier:

Contents: The icon qualifier indicates to the ME how the icon is to be used.

b2, b1: 00: icon is not to be used and may not be present
01: icon is self-explanatory, i.e. if displayed, it replaces the LSA name
10: icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the LSA name
11: RFU

Idle mode support:

Contents: The idle mode support is used to indicate whether the ME shall favour camping on the LSA cells in idle mode.

b3 = 0: Idle mode support disabled
b3 = 1: Idle mode support enabled

LSA indication for idle mode:

Contents: The LSA indication for idle mode is used to indicate whether or not the ME shall display the LSA name when the ME is camped on a cell within the LSA.

b4 = 0: LSA indication for idle mode disabled
b4 = 1: LSA indication for idle mode enabled

Bits b5 to b8 are RFU (see clause 9.3).

- Icon Identifier

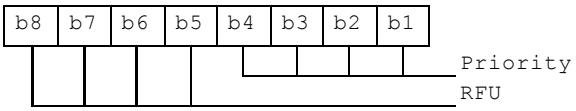
Contents: The icon identifier addresses a record in $EF_{IMG}$.

Coding: binary.

- Priority

Contents: Priority of the LSA which gives the ME the preference of this LSA relative to the other LSAs.

Coding:




'0' is lowest priority, 'F' is highest.

- PLMN code

Contents: MCC + MNC for the LSA.

Coding: according to GSM 04.08 [15] and $EF_{LOCI}$.

- LSA Descriptor File Identifier:

Contents: these bytes identify the EF which contains the LSA Descriptors forming the LSA.

Coding: byte X+8: high byte of the LSA Descriptor file;
byte X+9: low byte of the LSA Descriptor file.

- LSA Descriptor Record Identifier:

Contents: this byte identifies the number of the first record in the LSA Descriptor file forming the LSA.

Coding: binary.

### 10.4.1.3 LSA Descriptor files

Residing under $DF_{SoLSA}$, there may be several LSA Descriptor files. These EFs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA IDs, as a list of LAC + CIs, as a list of CIs or as a list of LACs. As the basic elements (LSA ID, LAC + CI, CI and LAC) of the four types of lists are of different length, they can not be mixed within one record. Different records may contain different kinds of lists within the EFs. Examples of codings of LSA Descriptor files can be found in annex F.

| Identifier: '4FXX' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: n*X+2 bytes | Update activity: low | |

Access Conditions:

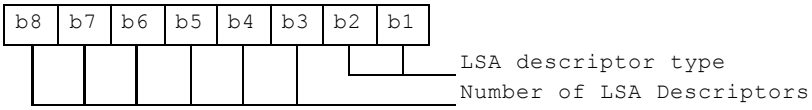
| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | LSA descriptor type and number | M | 1 byte |
| 2 to X+1 | 1st LSA Descriptor | M | X bytes |
| X+2 to 2X+1 | 2nd LSA Descriptor | M | X bytes |
| | | | |
| (n-1)*X+2 to n*X+1 | nth LSA Descriptor | M | X bytes |
| n*X+2 | Record Identifier | M | 1 byte |

- LSA descriptor type and number:

  Contents: The LSA descriptor type gives the format of the LSA descriptor and the number of valid LSA Descriptors within the record.

  Coding:




  LSA descriptor type:

  Contents: Gives the format of the LSA Descriptors.

  b2, b1: 00: LSA ID.
  01: LAC + CI
  10: CI
  11: LAC

  Number of LSA Descriptors:

  Contents: Gives the number of valid LSA Descriptors in the record.

  Coding: binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor

  Contents: Dependant of the coding indicated in the LSA descriptor type:

  - in case of LSA ID the field length 'X' is 3 bytes;
  - in case of LAC + CI the field length 'X' is 4 bytes;
  - in case of CI the field length 'X' is 2 bytes;

- in case of LAC the field length 'X' is 2 bytes.

Coding: according to TS 04.08 [15].

- Record Identifier:

Contents: This byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

Coding: record number of next record. 'FF' identifies the end of the chain.

This file utilises the concept of chaining as for $EF_{EXT1}$.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of $EF_{SAI}$ and $EF_{SLL}$. For the range of 'XX', see clause 6.6.

## 10.4.2 Contents of files at the MExE level

This clause specifies the EFs in the dedicated file DFMExE. It only applies if support of MExE by the SIM is supported (see TS 23.057 [50]).

The EFs in the Dedicated File DFMExE contain execution environment related information.

### 10.4.2.1 $EF_{MExE-ST}$ (MExE Service table)

This EF indicates which MExE 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: '4F40' | Structure: transparent | Optional |
|---|---|---|
| File size: X bytes, X ≥ 1 | 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 | O | 1 byte |
| etc. | | | |
| X | Services (4X-3) to (4X) | O | 1 byte |

-Services

Contents:
- Service n°1 : Operator root public key
- Service n°2 : Administrator root public key
- Service n°3 : Third party root public key
- Service n°4 : RFU

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.

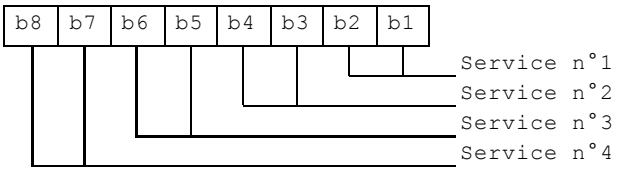
Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

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 clause 9.3.

First byte:




etc.

For an example of coding see clause 10.3.7

### 10.4.2.2 $EF_{ORPK}$ (Operator Root Public Key)

This EF contains the descriptor(s ) of certificates containing the Operator Root Public Key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MExE operator domain using a root public key held on the SIM. Each record of this EF contains one certificate descriptor.

For example, Operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

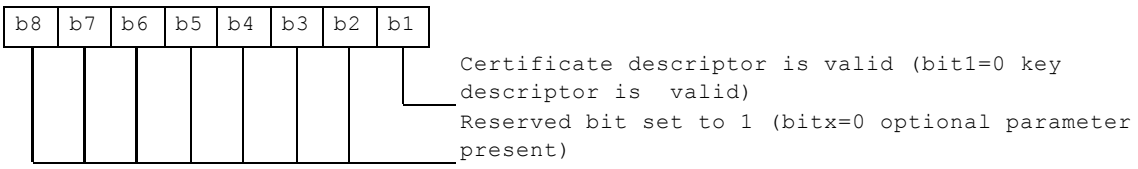
| Identifier: '4F41' | Structure: linear fixed | Optional |
|---|---|---|
| Record length : X + 10 bytes | Update activity: low | |

Access Conditions:

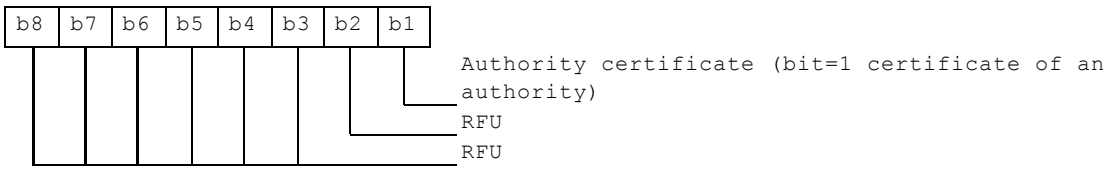
| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Parameters indicator | M | 1 byte |
| 2 | Flags | M | 1 byte |
| 3 | Type of certificate | M | 1 byte |
| 4 to 5 | Key/certificate file identifier | M | 2 bytes |
| 6 to 7 | Offset into key/certificate file | M | 2 bytes |
| 8 to 9 | Length of key/certificate data | M | 2 bytes |
| 10 | Key identifier length (k) | M | 1 byte |
| 11 to 10+k | Key identifier | M | k bytes |

- Parameter indicator
  Contents:
  The parameter indicator indicates if record is full and which optional parameters are present
  Coding: bit string




- Flags
  Contents:
  The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.
  Coding: bit string




- Type of certificate
  Contents:
  This field indicates the type of certificate containing the key.
  Coding: binary :
  0 : WTLS
  1 : X509
  2 : X9.68
  Other values are reserved for further use

- Key/certificate File Identifier
  Contents:
  these bytes identify an EF which is the key/certificate data file (see clause 10.7.5), holding the actual key/certificate data for this record.
  Coding:
  byte 4: high byte of Key/certificate File Identifier;
  byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File
  Contents:
  these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.
  Coding:
  byte 6: high byte of offset into Key/certificate Data File;
  byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data
  Contents:
  these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.
  Coding:
  byte 8: high byte of Key/certificate Data length;
  byte 9: low byte of Key/certificate Data length.

- Key identifier length
  Contents:
  This field gives length of key identifier
  Coding:
  binary

- Key identifier
  Contents:
  This field provides a means of identifying certificates that contain a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [50].
  Coding:
  octet string

NOTE: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

### 10.4.2.3 $EF_{ARPK}$ (Administrator Root Public Key)

This EF contains the descriptor(s ) of certificates containing the Administrator Root Public Key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator Root Public Key held on the SIM. Each record of this EF contains one certificate descriptor.

This file shall contain only one record.

| Identifier: '4F42' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X + 10 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Parameters indicator | M | 1 byte |
| 2 | Flags | M | 1 byte |
| 3 | Type of certificate | M | 1 byte |
| 4 to 5 | Key/certificate file identifier | M | 2 bytes |
| 6 to 7 | Offset into key/certificate file | M | 2 bytes |
| 8 to 9 | Length of key/certificate data | M | 2 bytes |
| 10 | Key identifier length (k) | M | 1 byte |
| 11 to 10+k | Key identifier | M | k bytes |

For contents and coding of all data items see the respective data items of the $EF_{ORPK}$ (clause 10.4.2.1).

### 10.4.2.4 $EF_{TPRPK}$ (Third Party Root Public key)

This EF contains descriptor(s ) of certificates containing the Third Party Root Public key (s). This EF shall only be allocated if the SIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held on the SIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.

For example, an operator may provide several Third Party root public keys.

| Identifier: '4F43' | Structure: linear fixed | Optional |
|---|---|---|
| Record length : X + 10 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Parameters indicator | M | 1 byte |
| 2 | Flags | M | 1 byte |
| 3 | Type of certificate | M | 1 byte |
| 4 to 5 | Key/certificate file identifier | M | 2 bytes |
| 6 to 7 | Offset into key/certificate file | M | 2 bytes |
| 8 to 9 | Length of key/certificate data | M | 2 bytes |
| 10 | Key identifier length (k) | M | 1 byte |
| 11 to 10+k | Key identifier | M | k bytes |
| 11+k to11+k | Certificate identifier length (m) | M | 1 byte |
| 12+k to 11+k+m | Certificate identifier | M | m bytes |

- Certificate identifier length
  Contents:
  This field gives length of certificate identifier
  Coding:
  binary

- Certificate identifier
  Contents:
  This field identify the issuer and provide a easy way to find a certificate. For more information about value and usage, see TS 23.057 [50].
  Coding:
  Octet string

For contents and coding of all other data items see the respective data items of the $EF_{ORPK}$ (clause 10.7.1).

### 10.4.2.5 Trusted Key/Certificates Data Files

Residing under $DF_{MExE}$, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

| Identifier: '4FXX' | Structure: transparent | Optional |
|---|---|---|
| Record length: Y bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to Y | Key/Certicates Data | M | Y bytes |

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by $EF_{TPRPK}$ (see clause 10.4.2.4).

The identifier '4FXX' shall be different from one key/certificate data file to the other. For the range of 'XX', see clause 6.6. The length Y may be different from one key/certificate data file to the other.

# 10.5 Contents of files at the telecom level

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

## 10.5.1 $EF_{ADN}$ (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 either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or

- one of the UCS2 coded options as defined in annex B.

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 has extension, 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 additional data being coded in the appropriate additional record itself (see clause 10.5.10).

  Coding:

  according to TS 04.08 [15].

- TON and NPI

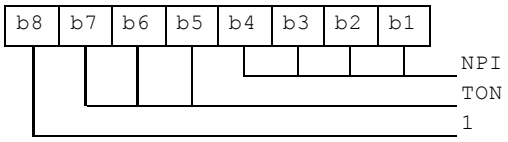
  Contents:

  Type of number (TON) and numbering plan identification (NPI).

  Coding:

  according to TS 04.08 [15]. 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 radio interface (see TS 04.08 [15]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.




- Dialling Number/SSC String

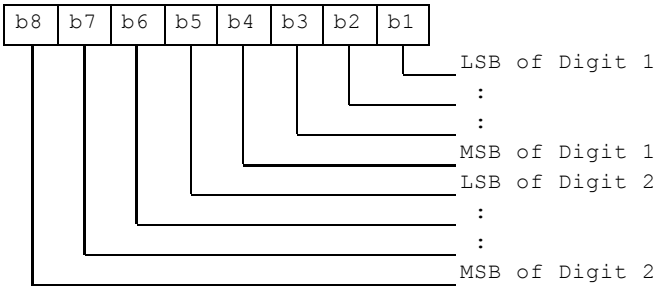
  Contents:

  up to 20 digits of the telephone number and/or SSC information.

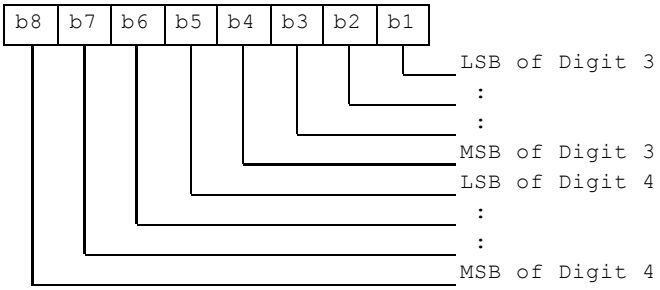
  Coding:

  according to TS 04.08 [15] , TS 22.030 [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 remainder 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'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the $EF_{EXT1}$. The record is identified by the Extension 1 Record Identifier. 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 additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  If the ADN/SSC requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside $EF_{EXT1}$ identifies the record of the appropriate called party subaddress (see clause 10.5.10).

  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 [19] 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 (TS 02.07 [3]) |
| 'D' | "Wild" value<br>This will cause the MMI to prompt the user for a single digit (see TS 02.07 [3]). |
| 'E' | Expansion digit ("Shift Key").<br>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<br>e.g. in case of an odd number of digits |

BCD values 'C', 'D' and 'E' are never sent across the radio 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 TS 02.07 [3]).

## 10.5.2 $EF_{FDN}$ (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 $EF_{ADN}$ (clause 10.5.1), 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 $EF_{ADN}$.

## 10.5.3 $EF_{SMS}$ (Short messages)

This EF contains information in accordance with TS 23.040 [13] 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. For MS originating messages sent to the network, the status shall be updated when the MS receives a status report, or sends a successful SMS Command relating to the status report.

Coding:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | |
|---|---|---|---|---|---|---|---|---|
| | | | | | X | X | 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 | 1 | 1 | MS originating message; message to be sent |
| | | | | | | | | RFU (see clause 9.3) |

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | |
|---|---|---|---|---|---|---|---|---|
| | | | X | X | 1 | 0 | 1 | MS originating message; message sent to the network: |
| | | | 0 | 0 | 1 | 0 | 1 | status report not requested |
| | | | 0 | 1 | 1 | 0 | 1 | status report requested but not (yet) received; |
| | | | 1 | 0 | 1 | 0 | 1 | status report requested, received but not stored in EF-SMSR; |
| | | | 1 | 1 | 1 | 0 | 1 | status report requested, received and stored in EF-SMSR; |
| | | | | | | | | RFU (see clause 9.3) |

- Remainder

Contents:

This data item commences with the TS-Service-Centre-Address as specified in TS 24.011 [16]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in TS 23.040 [13], with identical coding and ordering of parameters.

Coding:

according to TS 23.040 [13] and TS 24.011 [16]. 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.

## 10.5.4 Capability configuration parameters

### 10.5.4.1 $EF_{CCP}$ (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, an MSISDN, a last number dialled, a service dialling number or a barred dialling number.

For compatibility reasons, this file may be present for release 98 or earlier MEs in order to support Capability Configuration Parameters service.

| 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 TS 04.08 [15]. The Information Element Identity (IEI) shall be excluded. i.e. the first byte of the $EF_{CCP}$ record shall be Length of the bearer capability contents.

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

### 10.5.4.2 $EF_{ECCP}$ (Extended 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, an MSISDN, a last number dialled, a service dialling number, a barred dialling number, a mailbox dialling number or a call forwarding indication status number.

The number of records of the $EF_{ECCP}$ shall be equal to the number of records of the $EF_{CCP}$. Each record of the $EF_{CCP}$ shall have a corresponding record in the $EF_{ECCP}$ with the same record number.

If an ME has to update a record, then the ME shall update each record of both files, $EF_{CCP}$ with 10 bytes and $EF_{ECCP}$ with X bytes (X≥15).

If an ME has to read a record, then the ME shall check the consistency between the record of the $EF_{ECCP}$ and the corresponding record of the $EF_{CCP}$ and update the record of the $EF_{ECCP}$ with the value of the corresponding record of the $EF_{CPP}$.

| Identifier: '6F4F' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X (X≥15) | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to X | Bearer capability information element | M | X bytes |

- Bearer capability information element

  Contents and Coding:

  see TS 24.008 [47]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the $EF_{ECCP}$ record shall be Length of the bearer capability contents.

  Unused bytes are filled with 'FF'.

## 10.5.5 $EF_{MSISDN}$ (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 $EF_{ADN}$.

## 10.5.6 $EF_{SMSP}$ (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 clause 10.5.1 ($EF_{ADN}$).

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 TS 23.040 [13].

- TP-Service Centre Address

  Contents and Coding: As defined for RP-Destination address Centre Address in TS 24.011 [16].

- TP-Protocol Identifier

  Contents and Coding: As defined in TS 23.040 [13].

- TP-Data Coding Scheme

  Contents and Coding: As defined in TS 23.038 [12].

- TP-Validity Period

  Contents and Coding: As defined in TS 23.040 [13] for the relative time format.

## 10.5.7 $EF_{SMSS}$ (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 TS 23.040 [13].

  Coding:

as defined in TS 23.040 [13].

- 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 TS 23.040 [13].

  Coding:

  b1=1 means flag unset; memory capacity available

  b1=0 means flag set

  b2 to b8 are reserved and set to 1.

## 10.5.8 $EF_{LND}$ (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 |

For contents and coding, see clause 10.5.1 $EF_{ADN}$.

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

## 10.5.9 $EF_{SDN}$ (Service Dialling Numbers)

This EF contains special service numbers (SDN) 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: '6F49' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X+14 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1-X | Alpha identifier | O | X bytes |
| X+1 | Length of BCD number/SSC contents | M | 1 bytes |
| X+2 | TON and NPI | M | 1 byte |
| X+3-X+12 | Dialling Number/SSC String | M | 10 bytes |
| X+13 | Capability/Configuration Identifier | M | 1 byte |
| X+14 | Extension3 Record Identifier | M | 1 byte |

For contents and coding of all data items see the respective data items of the $EF_{ADN}$ (clause 10.5.1), with the exception that extension records are stored in the $EF_{EXT3}$.

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

## 10.5.10 $EF_{EXT1}$ (Extension1)

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

- an ADN/SSC (MSISDN, LND) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, LND) Elementary File or where common digits are required to follow an ADN/SSC string of less than 20 digits. 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 additional 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:

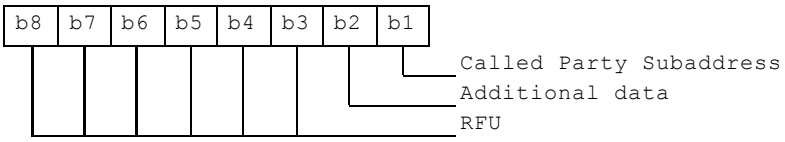
| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| 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:




  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 "additional data":

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

- Extension data

  Contents: Additional data or Called Party Subaddress depending on record type.

  Coding:

  Case 1, Extension1 record is additional data:

  The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC (respectively 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 additional digits exceeds the capacity of the additional record to chain another record inside the EXT1 Elementary File by the identifier in byte 13. In this case byte 2 (first byte of the extension data) of all records for additional data within the same chain indicates the number of bytes ('01' to '0A') for ADN/SSC (respectively MSISDN, LND) within the same record unequal to 'FF'.

  Case 2, Extension1 record is Called Party Subaddress:

  The subaddress data contains information as defined for this purpose in TS 04.08 [15]. All information defined in TS 04.08, 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 $EF_{ADN}$ 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 additional data (records 3 and 4) which represent the last 27 or 28 digits of the whole ADN/SSC (the first 20 digits are stored in $EF_{ADN}$) and a called party subaddress whose length is more than 11 bytes (records 6 and 1).

## 10.5.11 $EF_{EXT2}$ (Extension2)

This EF contains extension data of an FDN/SSC (see EXT2 in clause 10.5.2).

| 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 clause 10.5.10 $EF_{EXT1}$.

## 10.5.12 $EF_{EXT3}$ (Extension3)

This EF contains extension data of an SDN (see EXT3 in clause 10.5.9).

| Identifier: '6F4C' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 13 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| 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 clause 10.5.10 $EF_{EXT1}$.

## 10.5.13 $EF_{BDN}$ (Barred Dialling Numbers)

This EF contains Barred Dialling Numbers (BDN) 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: '6F4D' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X+15 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV2 |
| INVALIDATE | CHV2 / ADM (set at personalisation) |
| REHABILITATE | CHV2 / ADM (set at personalisation) |

| 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 | Extension4 Record Identifier | M | 1 byte |
| X+15 | Comparison Method Pointer | M | 1 byte |

For contents and coding of all data items, except for the Comparison Method Pointer, see the respective data items of the $EF_{ADN}$ (clause 10.5.1), with the exception that extension records are stored in the $EF_{EXT4}$. The Comparison Method Pointer refers to a record number in $EF_{CMI}$.

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

## 10.5.14 $EF_{EXT4}$ (Extension4)

This EF contains extension data of an BDN/SSC (see EXT4 in clause 10.5.13).

| Identifier: '6F4E' | 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 clause 10.5.10 $EF_{EXT1}$.

## 10.5.15 $EF_{SMSR}$ (Short message status reports)

This EF contains information in accordance with TS 23.040 [13] comprising short message status reports which have been received by the MS from the network.

Each record is used to store the status report of a short message in a record of $EF_{SMS}$. The first byte of each record is the link between the status report and the corresponding short message in $EF_{SMS}$.

| Identifier: '6F47' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 30 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | CHV1 |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | SMS record identifier | M | 1 |
| 2 - 30 | SMS status report | M | 29 bytes |

- SMS record identifier

  Contents:

  This data item identifies the corresponding SMS record in $EF_{SMS}$, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of $EF_{SMS}$.

  Coding:

  '00' - empty record

  '01' - 'FF' - record number of the corresponding SMS in $EF_{SMS}$.

- SMS status report

  Contents:

  This data item contains the SMS-STATUS-REPORT TPDU as specified in TS 23.040 [13], with identical coding and ordering of parameters.

  Coding:

  according to TS 23.040 [13]. Any bytes in the record following the TPDU shall be filled with 'FF'.

## 10.5.16 $EF_{CMI}$ (Comparison Method Information)

This EF contains a list of Comparison Method Identifiers and alpha-tagging associated with BDN entries (see $EF_{BDN}$). This EF shall always be present if $EF_{BDN}$ is present.

| Identifier: '6F58' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: X+1 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to X | Alpha Identifier | M | X bytes |
| X+1 | Comparison Method Identifier | M | 1 byte |

- Alpha Identifier

  Contents:

  Alpha-tagging of the associated Comparison Method Identifier

  Coding:

  Same as the alpha identifier in $EF_{ADN}$.

- Comparison Method Identifier

  Contents:

  this byte describes the comparison method which is associated with a BDN record. Its interpretation is not specified but it shall be defined by the operators implementing the BDN feature.

  Coding:

  '00' - 'FE' = Comparison Method Identifier.

  'FF' = Default method.

# 10.6 DFs at the telecom level

DFs may be present as child directories of $DF_{TELECOM}$. The following has been defined.

$DF_{GRAPHICS}$ '5F50'

## 10.6.1 Contents of files at the telecom graphics level

The EFs in the Dedicated File $DF_{GRAPHICS}$ contain graphical information.

### 10.6.1.1 $EF_{IMG}$ (Image)

Each record of this EF identifies instances of one particular graphical image, which graphical image is identified by this EF's record number.

Image instances may differ as to their size, having different resolutions, and the way they are coded, using one of several image coding schemes.

As an example, image k may represent a company logo, of which there are i instances on SIM, of various resolutions and perhaps encoded in several image coding schemes. Then, the i instances of the company's logo are described in record k of this EF.

| Identifier: '4F20' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 9n+2 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Number of Actual Image Instances | M | 1 byte |
| 2 to 10 | Descriptor of Image Instance 1 | M | 9 bytes |
| 11 to 19 | Descriptor of Image Instance 2 | O | 9 bytes |
| : | | | |
| 9 (n-1) + 2 to 9n + 1 | Descriptor of Image Instance n | O | 9 bytes |
| 9n + 2 | RFU | O | 1 byte |

- Number of Actual Image Instances

  Contents: this byte gives the number of actual image instances described in the following data items (i.e. unused descriptors are not counted).

  Coding: binary

- Image Instance Descriptor

  Contents: a description of an image instance

  Coding: see below

  Byte 1: Image Instance Width

  Contents:

  this byte specifies the image instance width, expressed in raster image points.

  Coding:

  binary.

  Byte 2: Image Instance Height

  Contents:

  this byte specifies the image instance height, expressed in raster image points.

  Coding:

  binary.

Byte 3: Image Coding Scheme

Contents:

this byte identifies the image coding scheme that has been used in encoding the image instance.

Coding:

'11' - basic image coding scheme as defined in annex G;

'21' - colour image coding scheme as defined in annex G;

other values are reserved for future use.

Bytes 4 and 5: Image Instance File Identifier

Contents:

these bytes identify an EF which is the image instance data file (see clause 10.6.1.2), holding the actual image data for this particular instance.

Coding:

byte 4: high byte of Image Instance File Identifier;

byte 5: low byte of Image Instance File Identifier.

Bytes 6 and 7: Offset into Image Instance File

Contents:

these bytes specify an offset into the transparent Image Instance File identified in bytes 4 and 5.

Coding:

byte 6: high byte of offset into Image Instance File;

byte 7: low byte of offset into Image Instance File

Bytes 8 and 9: Length of Image Instance Data

Contents:

these bytes yield the length of the image instance data, starting at the offset identified in bytes 6 and 7.

Coding:

byte 8: high byte of Image Instance Data length;

byte 9: low byte of Image Instance Data length.

NOTE: Transparent image instance data longer than 256 bytes may be read using successive READ BINARY commands.

### 10.6.1.2 Image Instance Data Files

Residing under $DF_{GRAPHICS}$, there may be several image instance data files. These EFs containing image instance data shall have the following attributes.

| Identifier: '4FXX' | Structure: transparent | Optional |
|---|---|---|
| Record length: Y bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | CHV1 |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to Y | Image Instance Data | M | Y bytes |

Contents and coding:

Image instance data are accessed using the image instance descriptors provided by $EF_{IMG}$ (see clause 10.6.1.1).

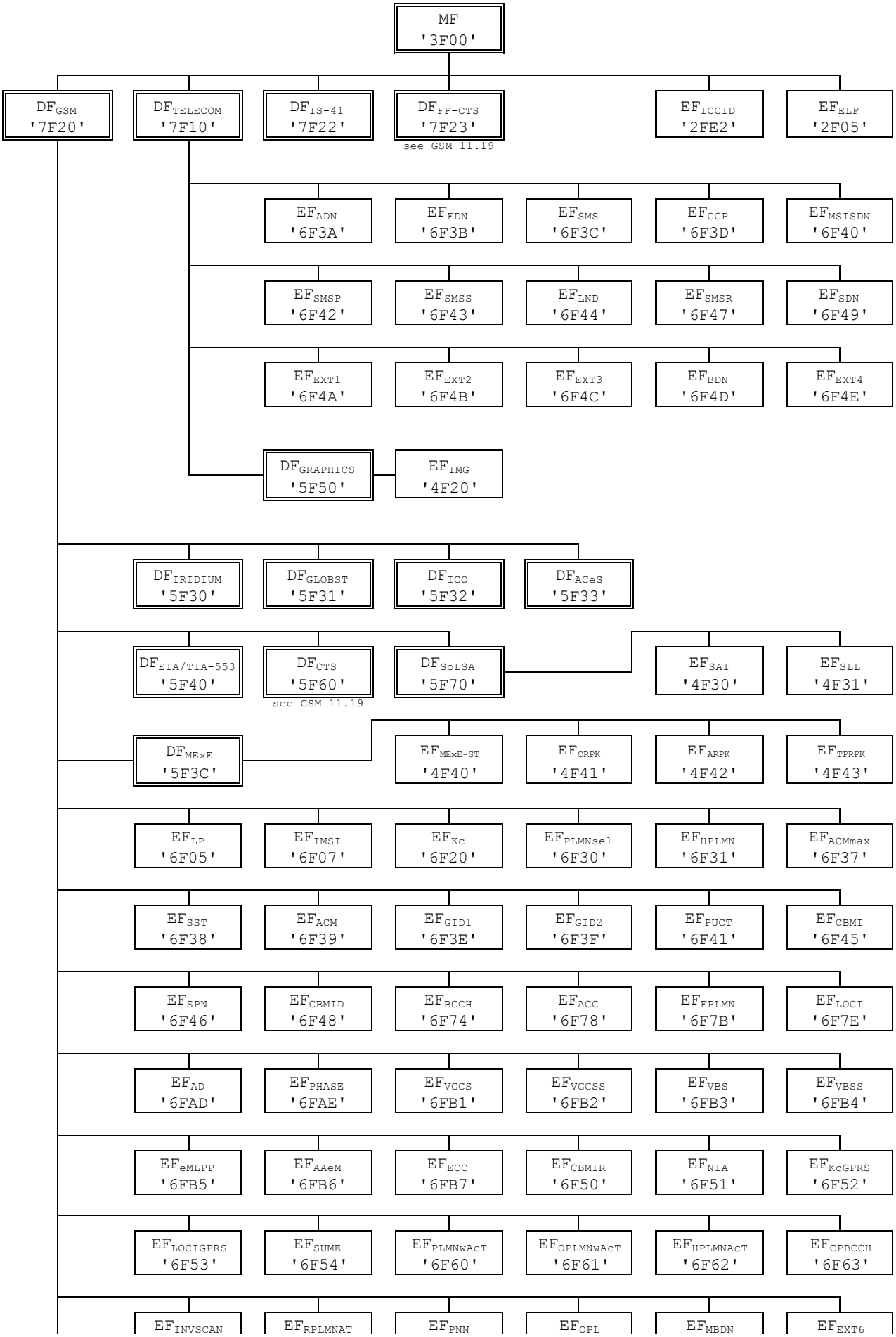
The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', see clause 6.6. The length Y may be different from one image instance data file to the other.

## 10.7 Files of GSM

This clause 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 DCS 1800 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 DCS 1800 application using the Phase 1 directory $DF_{DCS1800}$ coded '7F21'.

NOTE 2: To ensure backwards compatibility with those Phase 1 DCS 1800 MEs which have no means to select $DF_{GSM}$ two options have been specified. These options are given in GSM 09.91 [17].


MF
'3F00'
DF GSM
'7F20'
DF TELECOM
'7F10'
DF IS-41
'7F22'
DF FP-CTS
'7F23'
see GSM 11.19
EF ICCID
'2FE2'
EF ELP
'2F05'
EF ADN
'6F3A'
EF FDN
'6F3B'
EF SMS
'6F3C'
EF CCP
'6F3D'
EF MSISDN
'6F40'
EF SMSP
'6F42'
EF SMSS
'6F43'
EF LND
'6F44'
EF SMSR
'6F47'
EF SDN
'6F49'
EF EXT1
'6F4A'
EF EXT2
'6F4B'
EF EXT3
'6F4C'
EF BDN
'6F4D'
EF EXT4
'6F4E'
DF GRAPHICS
'5F50'
EF IMG
'4F20'
DF IRIDIUM
'5F30'
DF GLOBST
'5F31'
DF ICO
'5F32'
DF ACeS
'5F33'
DF EIA/TIA-553
'5F40'
DF CTS
'5F60'
see GSM 11.19
DF SoLSA
'5F70'
EF SAI
'4F30'
EF SLL
'4F31'
DF MExE
'5F3C'
EF MExE-ST
'4F40'
EF ORPK
'4F41'
EF ARPK
'4F42'
EF TPRPK
'4F43'
EF LP
'6F05'
EF IMSI
'6F07'
EF Kc
'6F20'
EF PLMNsel
'6F30'
EF HPLMN
'6F31'
EF ACMmax
'6F37'
EF SST
'6F38'
EF ACM
'6F39'
EF GID1
'6F3E'
EF GID2
'6F3F'
EF PUCT
'6F41'
EF CBMI
'6F45'
EF SPN
'6F46'
EF CBMID
'6F48'
EF BCCH
'6F74'
EF ACC
'6F78'
EF FPLMN
'6F7B'
EF LOCI
'6F7E'
EF AD
'6FAD'
EF PHASE
'6FAE'
EF VGCS
'6FB1'
EF VGCSS
'6FB2'
EF VBS
'6FB3'
EF VBSS
'6FB4'
EF eMLPP
'6FB5'
EF AAeM
'6FB6'
EF ECC
'6FB7'
EF CBMIR
'6F50'
EF NIA
'6F51'
EF KcGPRS
'6F52'
EF LOCIGPRS
'6F53'
EF SUME
'6F54'
EF PLMNwAcT
'6F60'
EF OPLMNwAcT
'6F61'
EF HPLMNAcT
'6F62'
EF CPBCCH
'6F63'
EF INVSCAN
EF RPLMNAT
EF PNN
EF OPL
EF MBDN
EF EXT6

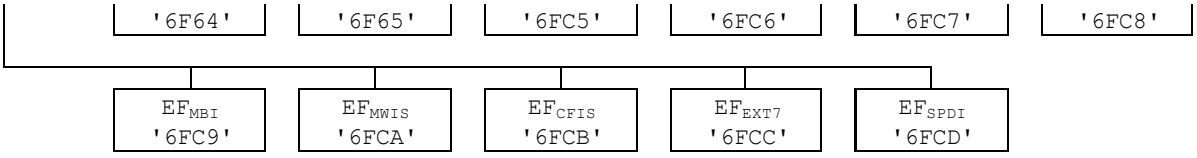



**Figure 8: File identifiers and directory structures of GSM**

# 11 Application protocol

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

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 role of the master and the SIM plays the role of the slave.

The SIM shall execute all GSM and SIM Application Toolkit commands or procedures in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the RUN GSM ALGORITHM is delayed in such a way which would result in the network denying or suspending service to the user.

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
- Emergency call codes request ME
- Extended language preference request 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
- GPRS Location Information NET
- Cipher key NET
- GPRS Cipher key NET
- BCCH information NET
- Forbidden PLMN information NET
- LSA information NET

Subscription related procedures:

- Dialling Numbers (ADN, FDN, MSISDN, LND, SDN, BDN) MMI/ME
- Short messages (SMS) MMI
- Advice of Charge (AoC) MMI
- Capability Configuration Parameters (CCP) MMI
- PLMN Selector MMI
- HPLMN Selector with Access Technology MMI
- User controlled PLMN Selector with Access Technology MMI
- Operator controlled PLMN Selector with Access Technology MMI
- RPLMN last used Access Technology MMI
- Investigation Scan request NET
- CPBCCH information NET

- 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
- Voice Group Call Service (VGCS) MMI/ME
- Voice Broadcast Service (VBS) MMI/ME
- Enhanced Multi Level Pre-emption and Priority (eMLPP) MMI/ME
- Depersonalisation Control Keys ME
- Short message status reports (SMSR) MMI
- Network's indication of alerting ME

SIM Application Toolkit related procedures:

- Data Download via SMS-CB (CBMID) NET
- Data Download via SMS-PP NET
- Menu selection MMI
- Call Control MMI/ME/NET
- Proactive SIM MMI/ME/NET
- Mobile Originated Short Message control by SIM MMI/ME/NET
- Image Request MMI/ME

MExE related procedures:

- Reading of MExE_ST ME
- Reading of root public keys on the SIM (ORPK, ARPK,TPRPK) ME/NET

The procedures listed in clause 11.2 are basically required for execution of the procedures in clauses 11.3, 11.4 and 11.5. The procedures listed in clauses 11.3 and 11.4 are mandatory (see TS 02.17 [6]). The procedures listed in clause 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 clause 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 clause 10.3.7). In all other cases this procedure shall not start.

## 11.1 General procedures

Procedures on different types of files shall be in accordance with TS 102 221 [55] with the limitation that the use of short file IDs is not supported by the SIM.

## 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 clause 4.3.2), the ME selects the Dedicated File $DF_{GSM}$ and optionally attempts to select $EF_{ECC}$ If $EF_{ECC}$ is available, the ME requests the emergency call codes.

The ME requests the Extended Language Preference. The ME only requests the Language Preference ($EF_{LP}$) if at least one of the following conditions holds:

- $EF_{PL}$ is not available;
- $EF_{PL}$ does not contain an entry corresponding to a language specified in ISO 639[30];
- the ME does not support any of the languages in $EF_{PL}$.

If both EFs are not available or none of the languages in the EFs is 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.

For a SIM requiring PROFILE DOWNLOAD, then the ME shall perform the PROFILE DOWNLOAD procedure in accordance with TS 11.14 [27]. When BDN is enabled on a SIM, the PROFILE DOWNLOAD procedure is used to indicate to the SIM whether the ME supports the "Call Control by SIM" facility. If so, then the SIM is able to allow the REHABILITATE command to rehabilitate $EF_{IMSI}$ and $EF_{LOCI}$.

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 SIM of Phase 2 or greater, 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 but with Call control by SIM facility shall not rehabilitate $EF_{IMSI}$ and/or $EF_{LOCI}$ if FDN is enabled in the SIM and therefore have no access to these EFs. GSM operation will therefore be prohibited;

  MEs without FDN capability and without Call control by SIM facility 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 these mechanisms which are used for control of services n°3 and n°31 by the use of SIMs for these services which always invalidate these two EFs at least before the next command following selection of either EF.

NOTE: When FDN and BDN are both enabled, and if the ME supports FDN but does not support the Call control by SIM facility, the rehabilitation of $EF_{IMSI}$ and $EF_{LOCI}$ will not be successful because of a restriction mechanism of the REHABILITATE command linked to the BDN feature.

When $EF_{IMSI}$ and $EF_{LOCI}$ are successfully rehabilitated, 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, subject to the service being supported both by the ME and the SIM:

- Administrative Information request;
- SIM Service Table request;

- IMSI request;
- Access Control request;
- HPLMN Search Period request;
- Investigation scan request;
- PLMN selector request;
- HPLMN Selector with Access Technology request;
- User controlled PLMN Selector with Access Technology request;
- Operator controlled PLMN Selector with Access Technology request;
- RPLMN last used Access Technology request;
- Location Information request;
- GPRS Location Information request;
- Cipher Key request;
- GPRS Cipher Key request;
- BCCH information request;
- CPBCCH information request;
- Forbidden PLMN request;
- LSA information request;
- CBMID request;
- Depersonalisation Control Keys request;
- Network's indication of alerting request.

If the SIM service table indicates that the proactive SIM service is active, then from this point onwards, the ME, if it supports the proactive SIM service, shall send STATUS commands at least every 30s during idle mode as well as during calls, in order to enable the proactive SIM to respond with a command. The SIM may send proactive commands (see TS 11.14 [27]), including a command to change the interval between STATUS commands from the ME, when in idle mode. In-call requirements for STATUS for SIM Presence Detection are unchanged by this command.

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 clause 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, subject to the service being supported both by the ME and the SIM:

- Location Information update;
- GPRS Location Information update;
- Cipher Key update;
- GPRS Cipher Key update;
- BCCH information update;

- CPBCCH information update;
- RPLMN last used Access Technology 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 Emergency Call Codes

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

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

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, CHV1 or CHV2.

### 11.2.4 Language preference

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

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

### 11.2.5 Administrative information request;

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

### 11.2.6 SIM service table request

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

### 11.2.7 SIM phase request

The ME performs the reading procedure with $EF_{Phase}$.

### 11.2.8 SIM Presence Detection and Proactive Polling

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.

If the ME supports the proactive SIM service, and the SIM has this service activated in its Service Table, then during idle mode the ME shall send STATUS commands to the SIM at intervals no longer than the interval negotiated with the SIM (see TS 11.14 [27]).

### 11.2.9 Preferred Language

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

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

## 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 if the CHV is "enabled", 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.

In the case of CHV1 the following procedure applies:

- if the CHV1 status is "blocked" and CHV1 is "enabled", the procedure ends and is finished unsuccessfully;
- if the CHV1 status is "blocked" but CHV1 is "disabled", the procedure ends and is finished successfully. The ME shall, however, accept SIMs which do not grant access rights when CHV1 is "blocked" and "disabled". In that case ME shall consider those SIMs as "blocked";
- if the CHV1 status is not "blocked" and CHV1 is "disabled", the procedure is finished successfully;
- if the CHV1 status is not "blocked" and CHV1 is "enabled", the ME uses the VERIFY CHV function. If the CHV1 presented by the ME is equal to the corresponding CHV1 stored in the SIM, the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the corresponding CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

In the case of CHV2 the following procedure applies:

- if the CHV2 status is "blocked", the procedure ends and is finished unsuccessfully;
- if the CHV2 status is not "blocked", the ME uses the VERIFY CHV function. If the CHV2 presented by the ME is equal to the corresponding CHV2 stored in the SIM, the procedure is finished successfully. If the CHV2 presented by the ME is not equal to the corresponding CHV2 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.

## 11.3.6 CHV procedures on a UICC Platform

If the SIM application is based on a UICC platform and the mapping of the CHVs onto existing UICC key references (used by a USIM application) takes place, the following additional procedures apply. These are in addition to the CHV procedures described above:

- after a third consecutive presentation of a wrong CHV or USIM PIN to which it is mapped, not necessarily in the same GSM or USIM session, the CHV and USIM PIN to which it is mapped become "blocked".

### 11.3.6.1 Mapping of CHV1

#### 11.3.6.1.1 Single verification capable UICC (see TS 31.101 [57])

If the PIN key reference of the USIM application (see 3G TS 31.102 [52]) that the CHV1 is mapped to is "enabled", CHV1 shall also be "enabled" for the SIM application and vice versa.

If the PIN key reference of the USIM application (see 3G TS 31.102 [52]) that the CHV1 is mapped to is "disabled", CHV1shall also be "disabled" for the SIM application and vice versa.

If the CHV1 status becomes "blocked", the PIN key reference of the USIM application that the CHV1 is mapped to becomes "blocked" and vice versa.

#### 11.3.6.1.2 Multi verification capable UICC (see TS 31.101 [57])

If the PIN key reference of the USIM application (see 3G TS 31.102 [52]) that the CHV1 is mapped to is "enabled", CHV1 shall also be "enabled" for the SIM application and vice versa. If the CHV1 status becomes "blocked", the PIN key reference of the USIM application that the CHV1 is mapped to also becomes "blocked".

If the PIN key reference of the USIM application (see 3G TS 31.102 [52]) that the CHV1 is mapped to is "disabled" and not replaced with the Universal PIN of the UICC (the usage qualifier of Universal PIN is set to '00' - "Do not Use Universal PIN"), CHV1shall also be "disabled" for the SIM application.

If the PIN key reference of the USIM application (see 3G TS 31.102 [52]) that the CHV1 is mapped to is "disabled" and replaced with the Universal PIN of the UICC (the usage qualifier of the Universal PIN is set to '08' -"Use Universal PIN"), CHV1 shall remain "enabled" for the SIM application. The CHV1 is now mapped to the Universal PIN. If the CHV1 presented by the ME is equal to the value of the Universal PIN stored in the UICC, the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the value of the Universal PIN stored in the UICC, the procedure ends and is finished unsuccessfully. If the CHV1 status becomes "blocked", the Universal PIN on the UICC also becomes "blocked", and vice versa.

### 11.3.6.1 Mapping of CHV2

CHV2 in the SIM application is mapped to the corresponding local key reference belonging to the USIM application to which the CHV1 is mapped. In the 2G operation mode, this PIN is considered to be global, in the 3G operation mode, it is seen as a being local.

## 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 clause 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 $EF_{PLMN}$.

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

### 11.4.9 LSA information

Request: The ME performs the reading procedure with $EF_{SAI}$, $EF_{SLL}$ and its associated LSA Descriptor files.

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

### 11.4.10 GPRS Location information

Requirement: Service n°38 "allocated and activated".

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

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

### 11.4.11 GPRS Cipher key

Requirement: Service n°38 "allocated and activated".

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

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

## 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 $EF_{FDN}$, $EF_{MSISDN}$, $EF_{LND}$, $EF_{BDN}$, $EF_{SDN}$, $EF_{MBDN}$ 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,

Service n°18 for SDN,

Service n°31 for BDN,

Service n°53 for MBDN)

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 clauses 10.5.1, 10.5.4 and 10.5.10):

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;

  Service n°19 for SDN;

  Service n°32 for BDN;

  Service n°53 for MBDN).

  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 "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional 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 additional data (see clauses 10.5.1 and 10.5.10).

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;
Service n°19 for SDN;
Service n°32 for BDN;
Service n°53 for MBDN).

If the length of the called party subaddress is less than or equal to 11 bytes (see TS 04.08 [15] 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 TS 04.08 [15] 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 additional 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 10.5.1) 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 $EF_{EXT1}$ ($EF_{EXT2,}$ $EF_{EXT6}$) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2, Extension6) records are noted by the ME. All Extension1 (Extension2, Extension6) 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 TS 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.

Invalidated ADNs may optionally still be readable and updatable depending on the file status (see clause 9.3)

The following three procedures are only applicable to service n°31 (BDN).

BDN capability request. The ME has to check the state of service n°31, i.e. if BDN is "enabled" or "disabled". BDN service is "enabled" only if service n°31 is allocated and activated, and $EF_{BDN}$ is not invalidated. In all other cases, the BDN service is "disabled".

BDN disabling. The BDN disabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN disabling procedure will not be executed successfully. To disable BDN capability, the ME

invalidates $EF_{BDN}$. The invalidate/rehabilitate flag of $EF_{BDN}$, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

BDN enabling. The BDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN enabling procedure will not be executed successfully. To enable BDN capability, the ME rehabilitates $EF_{BDN}$. The invalidate/rehabilitate flag of $EF_{BDN}$, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

Invalidated BDNs (when BDN capability is disabled) may optionally still be readable and updatable depending on the file status (see clause 9.3).

## 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 service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in $EF_{SMSR}$), the ME performs the reading procedure with the corresponding record in $EF_{SMSR}$. If the ME does not find a corresponding record in $EF_{SMSR}$, then the ME shall update the status of the SMS with '19' (status report requested, received but not stored in $EF_{SMSR}$).

If the short 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.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in $EF_{SMSR}$), the ME performs the erasure procedure for $EF_{SMSR}$ with the corresponding record in $EF_{SMSR}$.

## 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 $EF_{PLMNse1}$.

Update: The ME performs the updating procedure with $EF_{PLMNse1}$.

## 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 $EF_{SPN}$.

## 11.5.10 Voice Group Call Services

Requirement: Service n°18 "allocated and activated".

Voice Group Call Service

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

Voice Group Call Service Status

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

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

## 11.5.11 Voice Broadcast Services

Requirement: Service n°19 "allocated and activated".

Voice Broadcast Service

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

Voice Broadcast Service Status

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

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

## 11.5.12 Enhanced Multi Level Pre-emption and Priority Service

Requirement: Service n°18 "allocated and activated".

Enhanced Multi Level Pre-emption and Priority

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

Automatic Answer on eMLPP service

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

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

## 11.5.13 Cell Broadcast Message range identifier

Requirement: Service n°30 "allocated and activated".

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

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

## 11.5.14 Depersonalisation Control Keys

Requirement: Service n°33 "allocated and activated".

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

## 11.5.15 Short message status report

Requirement: Service n°35 "allocated and activated".

Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the seek function with $EF_{SMSR}$ to identify the record containing the appropriate status report. The ME performs the reading procedure with $EF_{SMSR}$.

Update: If a status report is received, the ME first seeks within the SMS record identifiers of $EF_{SMSR}$ for the same record number it used for the short message in $EF_{SMS}$. If such a record identifier is found in $EF_{SMSR}$, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in $EF_{SMSR}$ for storage. If no free entry is found the ME runs the Purge procedure with $EF_{SMSR}$. If there is still no free entry, the status report is not stored.

If the ME found an appropriate record in $EF_{SMSR}$ for storage, it updates the record with the status report setting the record identifier in $EF_{SMSR}$ to the appropriate record number of the short message in $EF_{SMS}$.

The status in $EF_{SMS}$ is updated accordingly (see clause 10.5.3) by performing the update procedure with $EF_{SMS}$.

Erasure: The ME runs the update procedure with $EF_{SMSR}$ by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of $EF_{SMSR}$. With each record the ME checks the corresponding short messages in $EF_{SMS}$. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in $EF_{SMSR}$), the ME shall perform the erasure procedure with the appropriate record in $EF_{SMSR}$.

## 11.5.16 Network's indication of alerting

Requirement: Service n°36 "allocated and activated".

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

## 11.5.17 User controlled PLMN Selector with Access Technology

Requirement: Service n°43"allocated and activated".

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

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

## 11.5.18 Operator controlled PLMN Selector with Access Technology

Requirement: Service n°44 "allocated and activated".

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

## 11.5.19 HPLMN Selector with Access Technology

Requirement: Service n°45 "allocated and activated".

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

## 11.5.20 CPBCCH information

Requirement: Service n°46 "allocated and activated".

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

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

## 11.5.21 Investigation Scan

Requirement: Service n°47 "allocated and activated".

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

## 11.5.22 RPLMN last used Access Technology

Requirement: Service n°50 "allocated and activated".

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

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

### 11.5.23 PLMN Network Name

Requirement: Service n°51 " allocated and activated ".

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

### 11.5.24 Operator PLMN List

Requirement: Service n°52 " allocated and activated ".

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

### 11.5.25 Message Waiting Indication

Requirement: Service n°54 " allocated and activated ".

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

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

### 11.5.26 Call Forwarding Indication Status

Requirement: Service n°55 " allocated and activated ".

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

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

### 11.5.27 Service Provider Display Information

Requirement: Services n°17 and 56 are "allocated and activated".

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

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

## 11.6 SIM Application Toolkit related procedures

SIM Application Toolkit is an optional feature. The higher level procedures, and contents and coding of the commands, are given in TS 11.14 [27]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this clause. A SIM or ME supporting SIM Application Toolkit shall conform to the requirements given in this clause.

### 11.6.1 Initialization procedure

A SIM supporting SIM Application Toolkit shall indicate this through relevant data in $EF_{Phase}$ and $EF_{SST}$, as defined in the relevant clauses above.

An ME supporting SIM Application Toolkit shall perform initialization as defined in the SIM Initialization clause above.

### 11.6.2 Proactive polling

An ME supporting proactive SIM (part of SIM Application Toolkit) shall support the polling procedure as defined above.

### 11.6.3 Support of commands

A SIM or ME supporting SIM Application Toolkit shall support the commands TERMINAL PROFILE, ENVELOPE, FETCH and TERMINAL RESPONSE.

These commands shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support these commands.

### 11.6.4 Support of response codes

A SIM or ME supporting SIM Application Toolkit shall support the response status words (SW1 SW2) '91 XX', and '93 00' and '9E XX'. The SIM shall send '9E XX' only to an ME indicating in TERMINAL PROFILE that it supports the handling of these status words.

These responses shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support them.

### 11.6.5 Command-response pairs

Using the terminology where the ME issues a command and the SIM a response, ending in status words SW1 SW2, a command-response pair is considered as a single transaction. Each transaction is initiated by the ME and terminated by the SIM. One transaction must be completed before the next one can be initiated. This protocol applies to SIM Application Toolkit in the same way as it does to normal operation.

### 11.6.6 Independence of normal GSM and SIM Application Toolkit tasks

Normal GSM operation (relating to general, CHV related, GSM security related, and subscription related procedures) and SIM Application Toolkit operation shall be logically independent, both in the SIM and in the ME.

Specifically, this means:

- the currently selected EF and current record pointer in the normal GSM task shall remain unchanged, if still valid, as seen by the ME, irrespective of any SIM Application Toolkit activity;
- between successive SIM Application Toolkit related command-response pairs, other normal GSM related command-response pairs can occur. The SIM Application Toolkit task status shall remain unchanged by these command-response pairs.

### 11.6.7 Use of BUSY status response

If for any reason the SIM Application Toolkit task of the SIM cannot process an ENVELOPE command issued by the ME at present (e.g. other SIM Application Toolkit processes are already running, and this additional one would cause an overload), the SIM can respond with a status response of '93 00'. The ME may re-issue the command at a later stage.

The BUSY status response has no impact on normal GSM operation.

### 11.6.8 Use of NULL procedure byte

The NULL procedure byte provides a mechanism for the SIM to obtain more time before supplying the response part of a command-response pair, during which time the ME is unable to send further commands to the SIM.

If a SIM Application Toolkit activity in the SIM runs for too long, this may prevent the ME from sending "normal GSM" commands which are time-critical, e.g. RUN GSM ALGORITHM. A MORE TIME command is defined in TS 11.14 [27], which ensures that the SIM Application Toolkit task in the SIM gets more processing time, while at the same time freeing the SIM/ME interface. This should be used in preference to NULL procedure bytes ('60').

### 11.6.9 Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands

These commands are part of the set used by SIM Application Toolkit. The use of the these commands, the occasions where they are required, and the command and response parameters associated with the commands, are specified in TS 11.14 [27]. The ME completes the command parameters/data of the relevant command and sends the command to the SIM. The transmitted data is processed by the SIM in a specific way depending on the tag value in the command parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support these commands.

### 11.6.10 Using the FETCH command

This command is used by SIM Application Toolkit. The use of the this command, the occasions where it is required, and the command and response parameters associated with the command, are specified in TS 11.14 [27]. It is similar in function to GET RESPONSE, in that it requests response parameters from the SIM, following a '91 XX' status response. The transmitted response data from the SIM is processed by the ME in a specific way depending on the tag value in the response parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support this command.

### 11.6.11 Data Download via SMS-CB

Requirement: Service n°25 "allocated and activated".

The ME shall perform the reading procedure with $EF_{CBMID}$. On receiving a cell broadcast message with an identifier which matches an identifier in $EF_{CBMID}$, the ME shall pass the CB message to the SIM using the ENVELOPE command. If a match is not found and service no. 14 is "allocated and activated", then the message identifier is checked against those in $EF_{CBMI}$.

### 11.6.12 Data Download via SMS-PP

Requirement: Service n°26 "allocated and activated".

The procedures and commands for Data Download via SMS-PP are defined in TS 11.14 [27].

### 11.6.13 Menu selection

Requirement: Service n°27 "allocated and activated".

The procedures and commands for Menu Selection are defined in TS 11.14 [27].

### 11.6.14 Call Control

Requirement: Service n°28 "allocated and activated".

The procedures and commands for Call Control are defined in TS 11.14 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control in the TERMINAL PROFILE command. When BDN is enabled, the Call control facility of the ME is used by the SIM to support the BDN service.

### 11.6.15 Proactive SIM

Requirement: Service n°29 "allocated and activated".

The procedures and commands for Proactive SIM, at the application level, are defined in TS 11.14 [27].

### 11.6.16 Mobile Originated Short Message control by SIM

Requirement: Service n°37 "allocated and activated".

The procedures and commands for Mobile Originated Short Message control by SIM are defined in TS 11.14 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Mobile Originated Short Message control by SIM in the TERMINAL PROFILE command.

### 11.6.17 SIM data download error

In case of an ENVELOPE for SIM data download, the SIM can respond with the status words '9E XX' to indicate that response data is available. The ME shall use the GET RESPONSE command to get the response data. The ME shall then send transparently to the network this response data, using the error procedure of the transport mechanism.

### 11.6.18 Image Request

Requirement: Service n°39 "allocated and activated".

The ME sends the identification of the information to be read. The ME shall analyse the data of $EF_{IMG}$ (clause 10.6.1.1) to identify the files containing the image's instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete image instance data.

## 11.7 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands, are given in TS 23.057 [50]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this clause. A SIM or ME supporting MExE shall conform to the requirements given in this clause.

### 11.7.1 MExE ST

Requirement: Service n°49 (MExE) "allocated and activated".
Request: The ME performs the reading procedure with $EF_{MExE\_ST}$.

### 11.7.2 Operator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°1 ($EF_{ORPK}$)" allocated and activated".
Request: The ME performs the reading procedure with $EF_{ORPK}$. The ME shall analyse the data of $EF_{ORPK}$ (clause 10.7.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

### 11.7.3 Administrator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°2 ($EF_{ARPK}$) "allocated and activated".
Request: The ME performs the reading procedure with $EF_{ARPK}$. The ME shall analyse the data of $EF_{ARPK}$ (clause 10.7.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

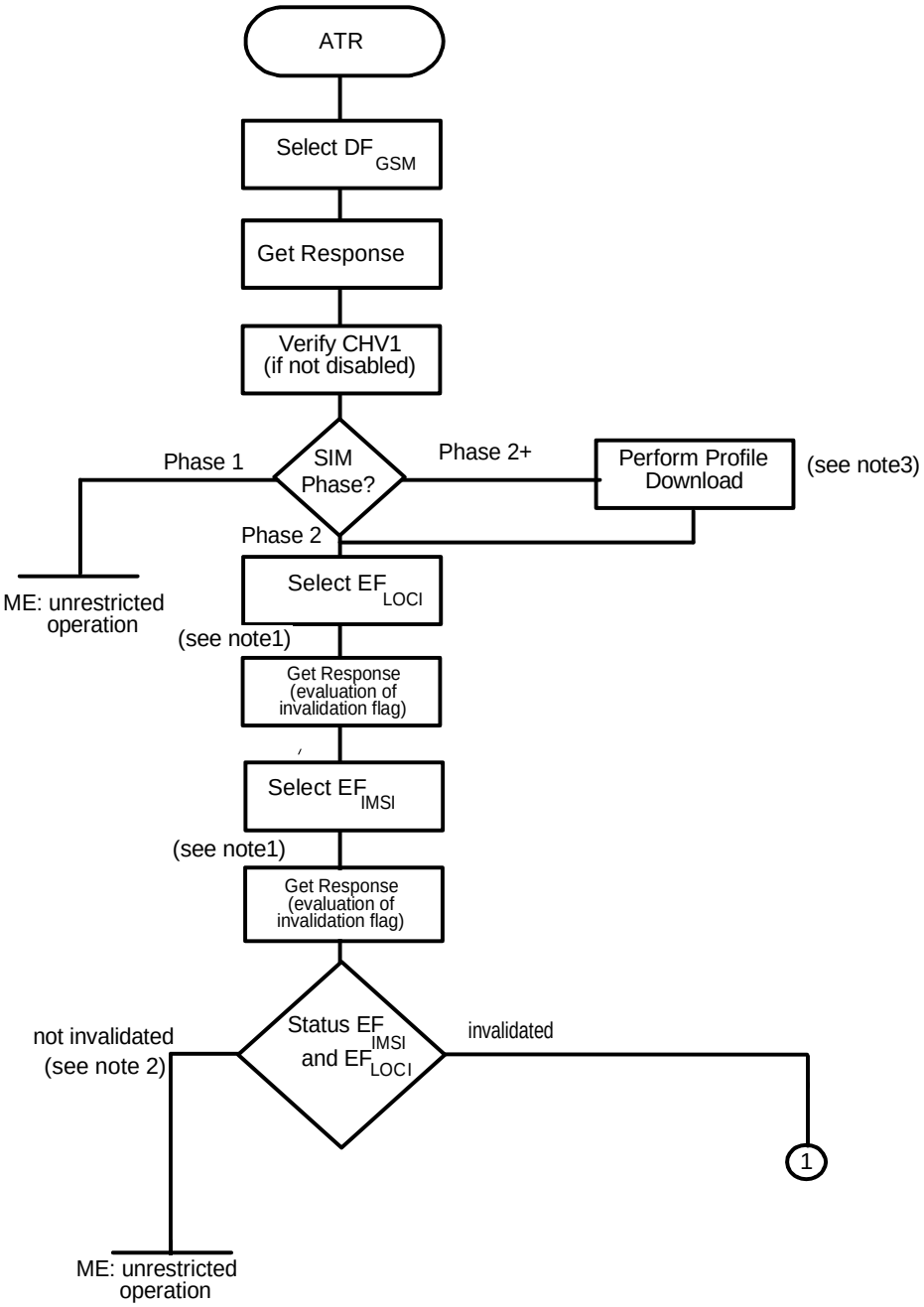
### 11.7.4 Third Party root public key(s)

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°3 ($EF_{TPRPK}$) "allocated and activated".
Request: The ME performs the reading procedure with $EF_{TPRPK}$. The ME shall analyse the data of $EF_{TPRPK}$ (clause 10.7.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

# Annex A (normative):
# Void

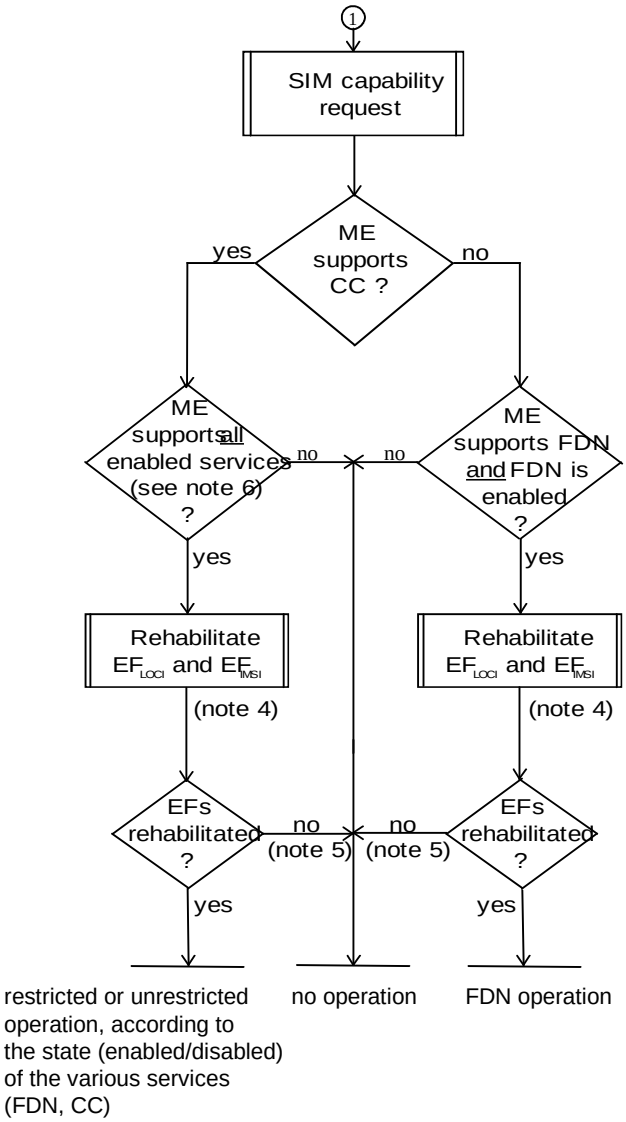
# Annex B (normative):
# Void

# Annex C (informative): FDN/BDN Procedures




NOTE 1: In case of enabled FDN and/or enabled BDN, the EF has been invalidated by the SIM at no later than this stage.
NOTE 2: Invalidation of only one of the two EFs is not allowed for FDN and BDN.
NOTE 3: For SIMs with enabled BDN this procedure is used to check whether the ME supports the Call Control by the SIM facility.

**Figure C.1a: Example of an Initialization Procedure of a FDN/BDN SIM (see clause 11.2.1)**




NOTE 4: In case of "BDN enabled", the SIM only allows rehabilitation of the $EF_{IMSI}$ and $EF_{LOCI}$, if the ME has indicated its CC-capability to the SIM (by PROFILE_DOWNLOAD).

NOTE 5: Possibility for future "restricting" services to use the internal SIM mechanism of invalidation of $EF_{IMSI}$ and $EF_{LOCI}$.

NOTE 6: If the ME does not support all enabled services (e.g. FDN, BDN), it does not operate. In case of enabled BDN, the support of the "Call Control Feature" by the ME is sufficient for operation. For future use, there may be additional "restricting" services, which are not known to the ME. In that case the ME will perform the subsequent rehabilitation procedure but will fail to rehabilitate $EF_{IMSI}$ and $EF_{LOCI}$ (see note 4).

**Figure C.1b: Example of an Initialization Procedure of a FDN/BDN SIM (continued)**

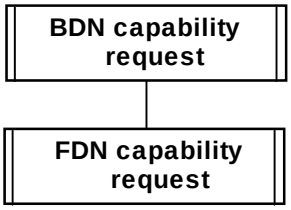



**Figure C.2: SIM capability request**

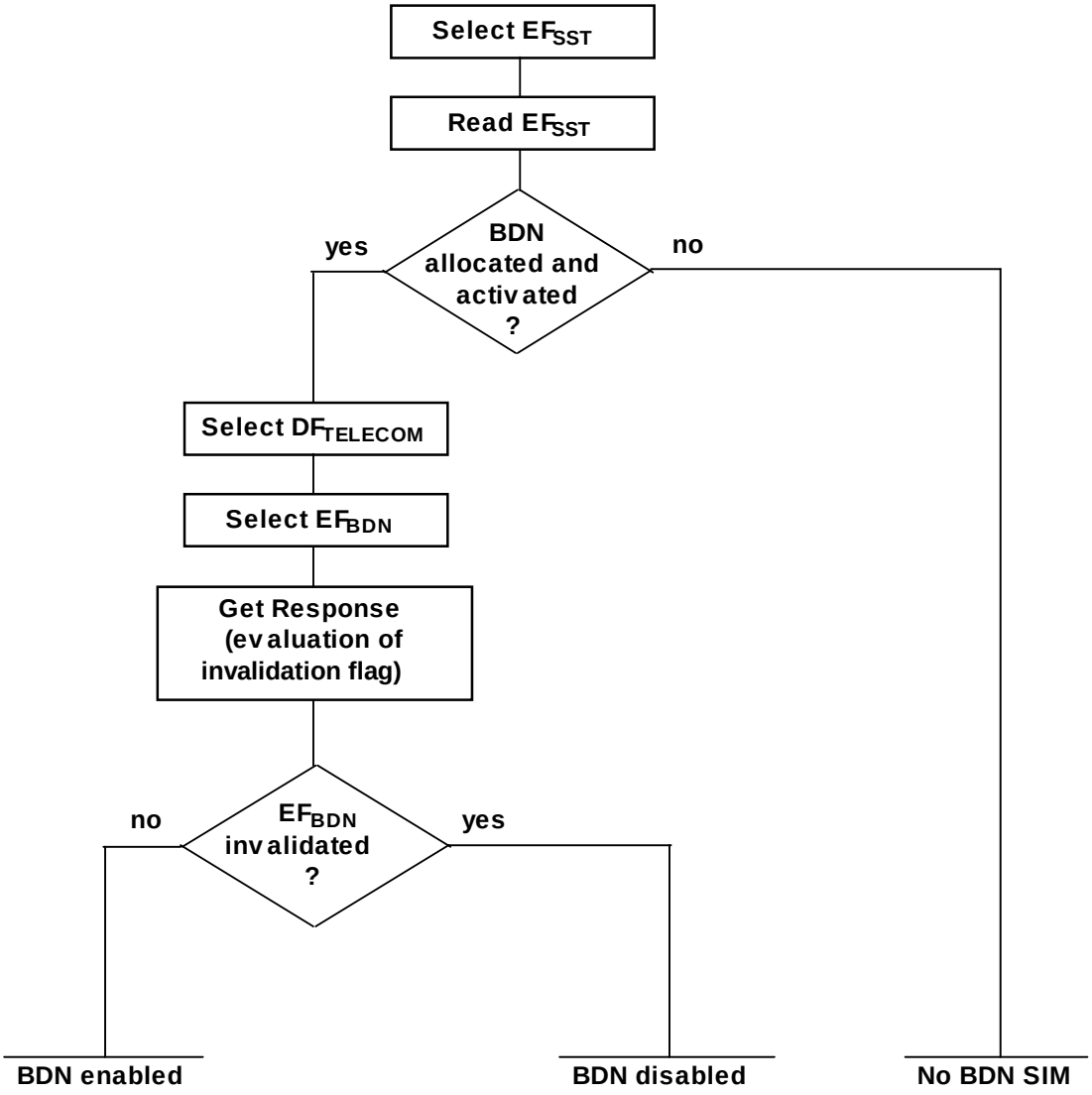
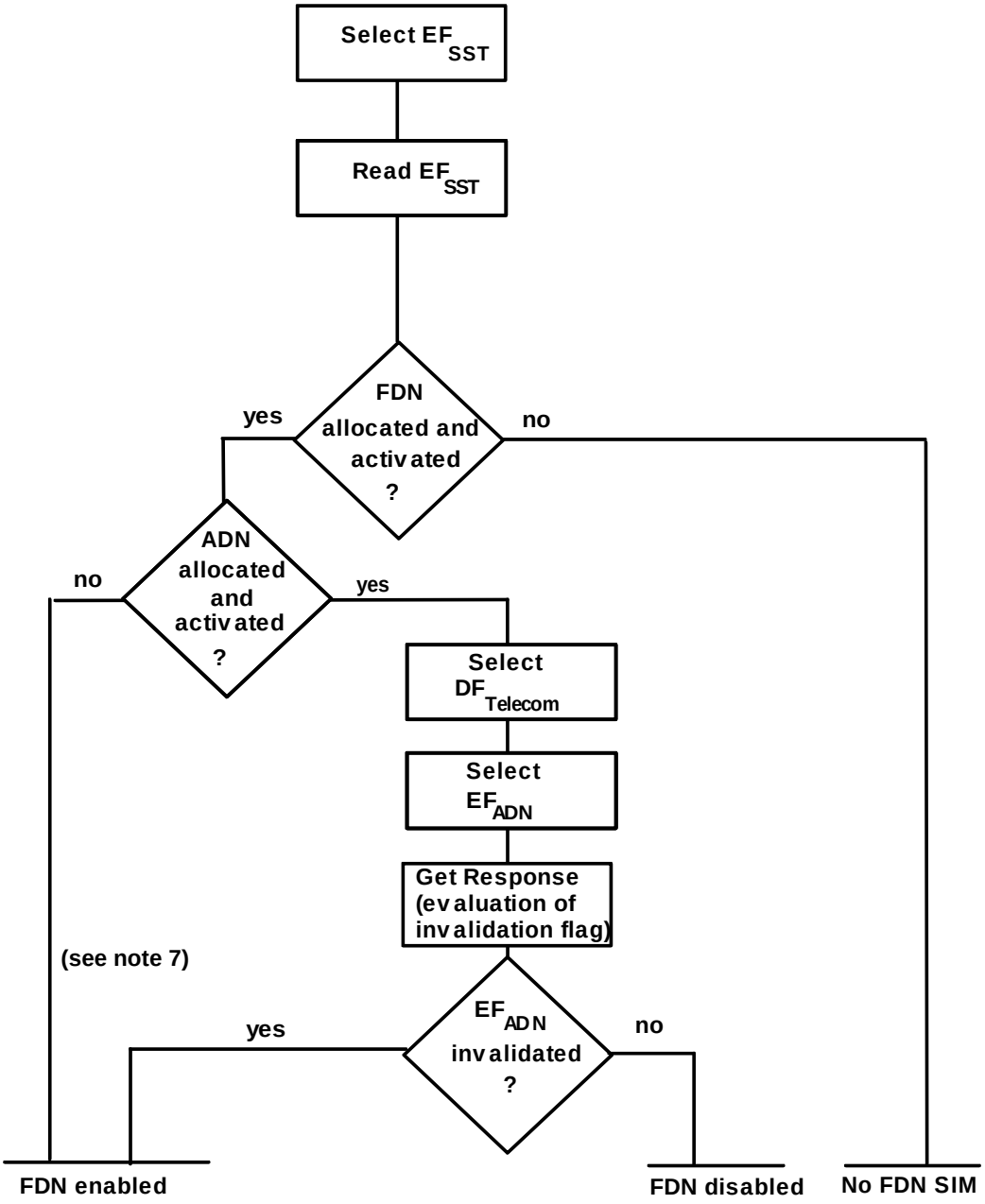
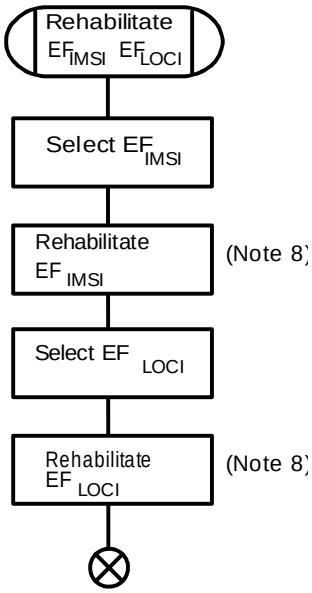



**Figure C.3: BDN capability request (see clause 11.5.1)**




NOTE 7: In this case FDN is enabled without the possibility of disabling.

**Figure C.4: FDN capability request (see clause 11.5.1)**




NOTE 8: If BDN is enabled in the SIM, and if the Profile download procedure has not indicated that the ME supports Call Control, the EF is not rehabilitated by the SIM.

**Figure C.5: Procedure to rehabilitate GSM files**

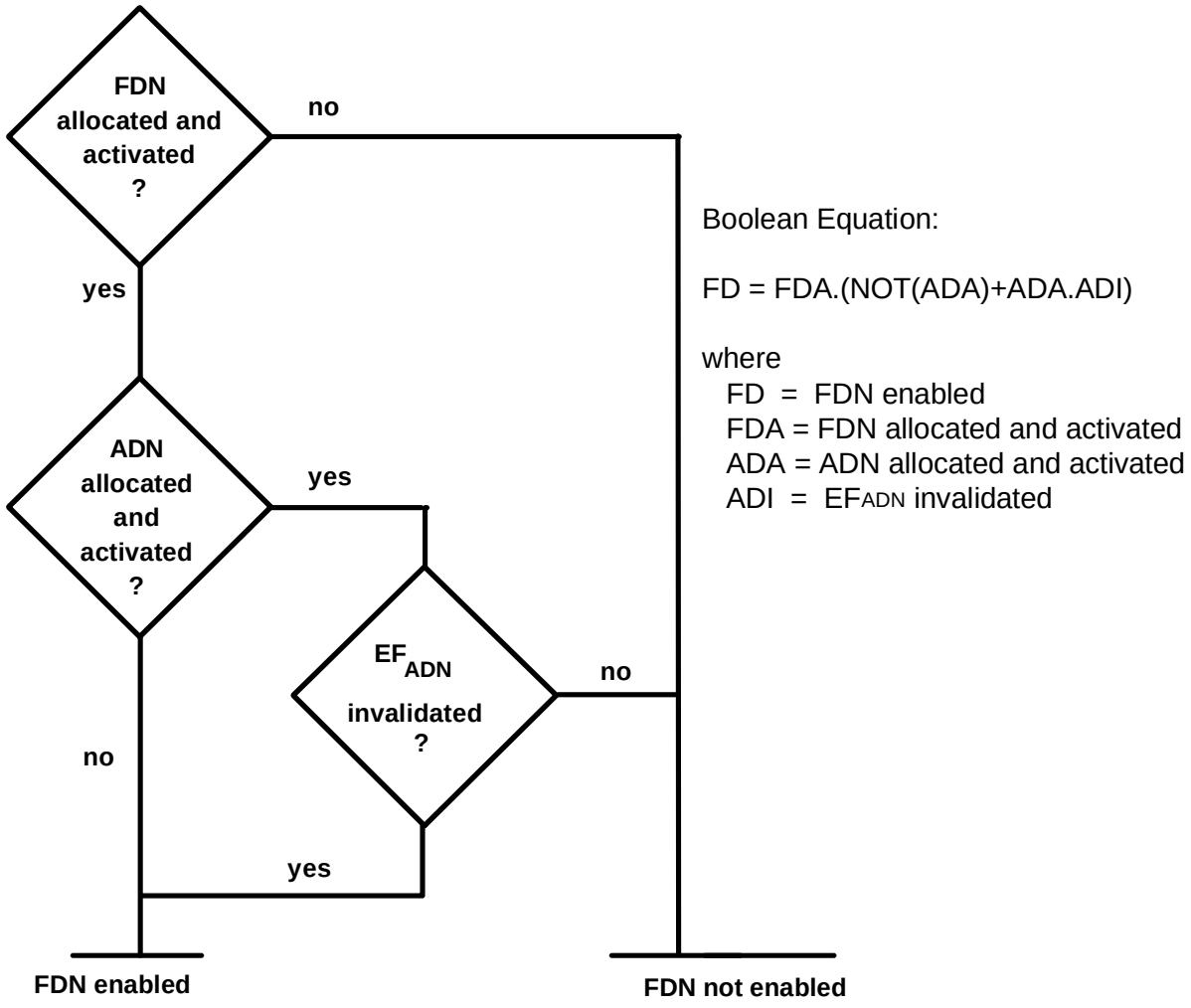



**Figure C.6: Coding for state of FDN**

# Annex D (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 |
|---|---|---|
| '2FE2' | ICC identification | operator dependant (see 10.1.1) |
| '2F05' | Extended Language preference | 'FF…FF' |
| '6F05' | Language preference | 'FF' |
| '6F07' | IMSI | operator dependant (see 10.3.2) |
| '6F20' | Ciphering key Kc | 'FF...FF07' |
| '6F30' | PLMN selector | 'FF...FF' |
| '6F31' | HPLMN search period | 'FF' |
| '6F37' | ACM maximum value | '000000' (see note 1) |
| '6F38' | SIM service table | operator dependant (see 10.3.7) |
| '6F39' | Accumulated call meter | '000000' |
| '6F3E' | Group identifier level 1 | operator dependant |
| '6F3F' | Group identifier level 2 | operator dependant |
| '6F41' | PUCT | 'FFFFFF0000' |
| '6F45' | CBMI | 'FF...FF' |
| '6F46' | Service provider name | 'FF...FF' |
| '6F48' | CBMID | 'FF...FF' |
| '6F49' | Service Dialling Numbers | 'FF...FF' |
| '6F74' | BCCH information | 'FF...FF' |
| '6F78' | Access control class | operator dependant (see 10.3.15) |
| '6F7B' | Forbidden PLMNs | 'FF...FF' |
| '6F7E | Location information | 'FFFFFFFF xxxxxx 0000 FF 01'<br>(see note 2) |
| '6FAD' | Administrative data | operator dependant (see 10.3.18) |
| '6FAE' | Phase identification | see 10.3.16 |
| '6F3A' | Abbreviated dialling numbers | 'FF...FF' |
| '6F3B' | Fixed dialling numbers | 'FF...FF' |
| '6F3C' | Short messages | '00FF...FF' |
| '6F3D' | Capability configuration parameters | 'FF...FF' |
| '6F40' | MSISDN storage | 'FF...FF' |
| '6F42' | SMS parameters | 'FF...FF' |
| '6F43' | SMS status | 'FF...FF' |
| '6F44' | Last number dialled | 'FF...FF' |
| '6F47' | Short message status reports | '00FF…FF' |
| '6F4A' | Extension 1 | 'FF...FF' |
| '6F4B' | Extension 2 | 'FF...FF' |
| '6F4C' | Extension 3 | 'FF...FF' |
| '6F4D' | Barred dialling numbers | 'FF...FF' |
| '6F4E' | Extension 4 | 'FF...FF' |
| '6F4F' | Extended capability configuration parameters | 'FF...FF' |
| '6F51' | Network's indication of alerting | 'FF...FF' |
| '6F52' | GPRS Ciphering key KcGPRS | 'FF...FF07' |
| '6F53' | GPRS Location Information | 'FFFFFFFF FFFFFF xxxxxx 0000 FF 01'<br>(see note 2) |
| '6F54' | SetUpMenu Elements | operator dependant (see 10.3.34) |
| '6F58' | Comparison method information | 'FF…FF' |
| '6F60' | User controlled PLMN Selector with Access Technology | 'FFFFFF0000..FFFFFF0000' |
| '6F61' | Operator controlled PLMN Selector with Access Technology | 'FFFFFF0000..FFFFFF0000' |
| '6F62' | HPLMN Selector with Access Technology | 'FFFFFF0000..FFFFFF0000' |
| '6F63' | CPBCCH information | 'FF..FF' |
| '6F64' | Investigation Scan | '00' |
| '6F65' | RPLMN last used Access Technology | '0000' |

**Continued**

| File Identification | Description | Value |
|---|---|---|
| '4F20' | Image data | '00FF...FF' |
| '4F30' | SoLSA Access Indicator) | '00FF...FF' |
| '4F31' | SoLSA LSA List | 'FF...FF' |
| '6FC5' | PLMN Network Name | Operator dependant |
| '6FC6' | Operator PLMN List | Operator dependant |
| '6FC7' | Mailbox Dialling Numbers | Operator dependant |
| '6FC8' | Extension 6 | '00 FF...FF' |
| '6FC9' | Mailbox Identifier | Operator dependant |
| '6FCA' | Message Waiting Indication Status | '00 00 00 00 00' |
| '6FCB' | Call Forwarding Indication Status | 'xx 00 FF...FF' |
| '6FCC' | Extension 7 | '00 FF...FF' |
| '6FCD' | Service Provider display Information | 'FF...FF' |

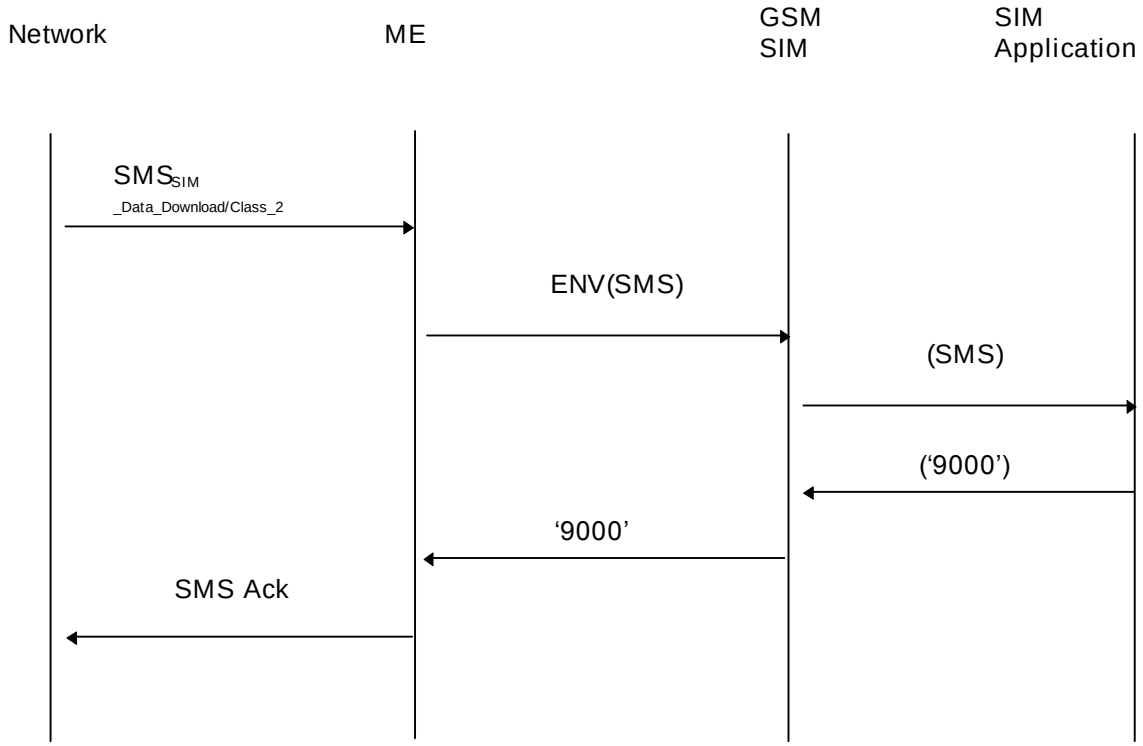
NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update $EF_{ACM}$ if the units to be added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

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 04.08 [15].

# Annex E (informative): SIM application Toolkit protocol diagrams

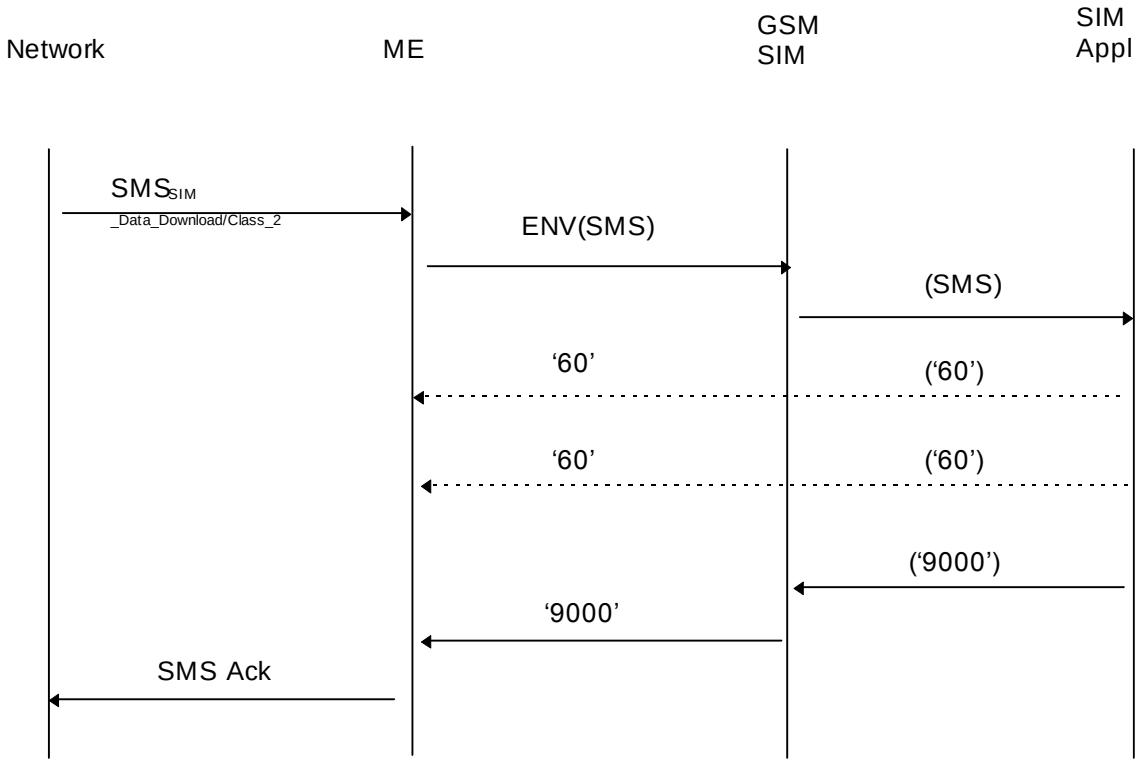
The diagrams in this annex are intended to illustrate the data protocols of the SIM toolkit application in various situations. The SIM application is shown as initiated by SMS Data Download messages. Other possibilities exist (as defined in TS 11.14) such as data entry from a menu selection.

**Case 1: Simple**




This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed immediately by the SIM application. This requires no ME action except to acknowledge the SMS.

**Case 2: Simple with short delay**

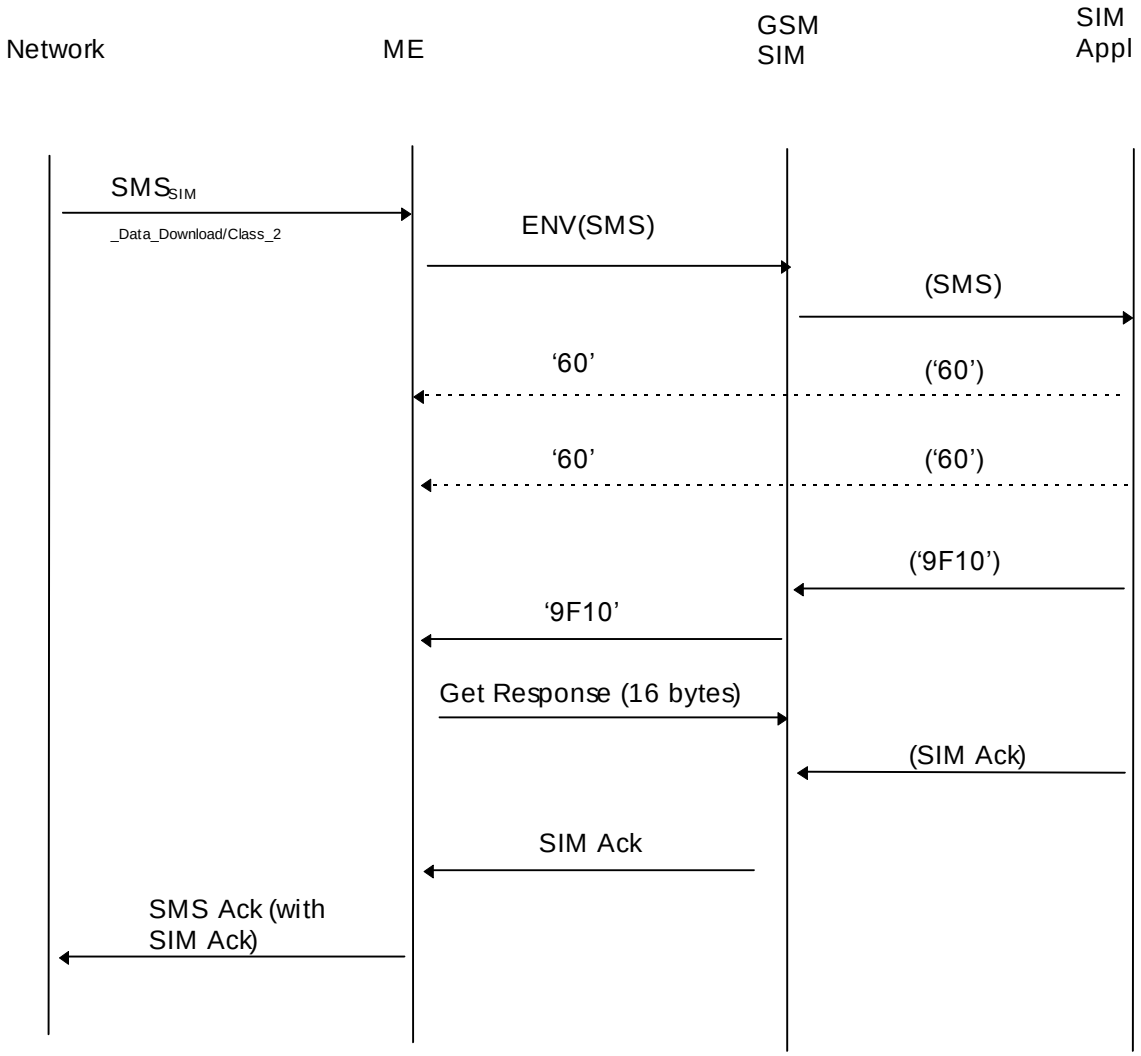



This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. The processing time is "not long" and is obtained by the SIM application sending "null procedure bytes" to the ME. Each byte has the effect of restarting the work waiting time so that the ME does not abort the transaction before the SIM application has finished processing the command(s) sent in the SMS.

**Guidelines on timings:**

1. The SMS Ack must be sent back before the network times out and sends the SMS again.
2. Use of null procedure bytes must not be excessive as during this time the ME is unable to issue normal GSM commands to the SIM.

**Case 3: Simple with short delay and SIM Acknowledgement**

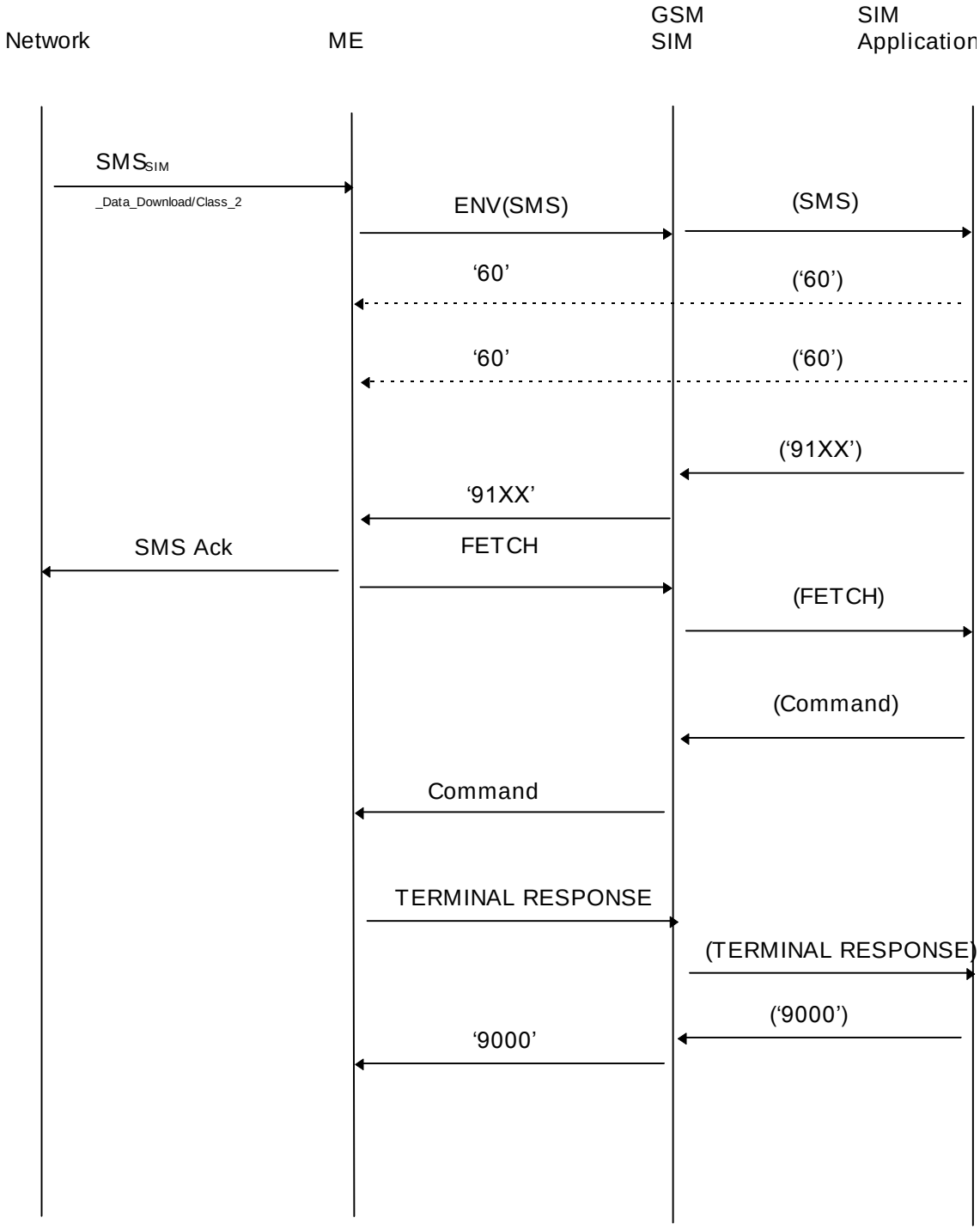



This shows the same case as previously where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. However in this case the SIM application has SIM acknowledgement data to include in the SMS acknowledgement being returned to the network by the ME.

**Guideline on timings:**

The SMS Ack must be sent back before the network times out and sends the SMS again.

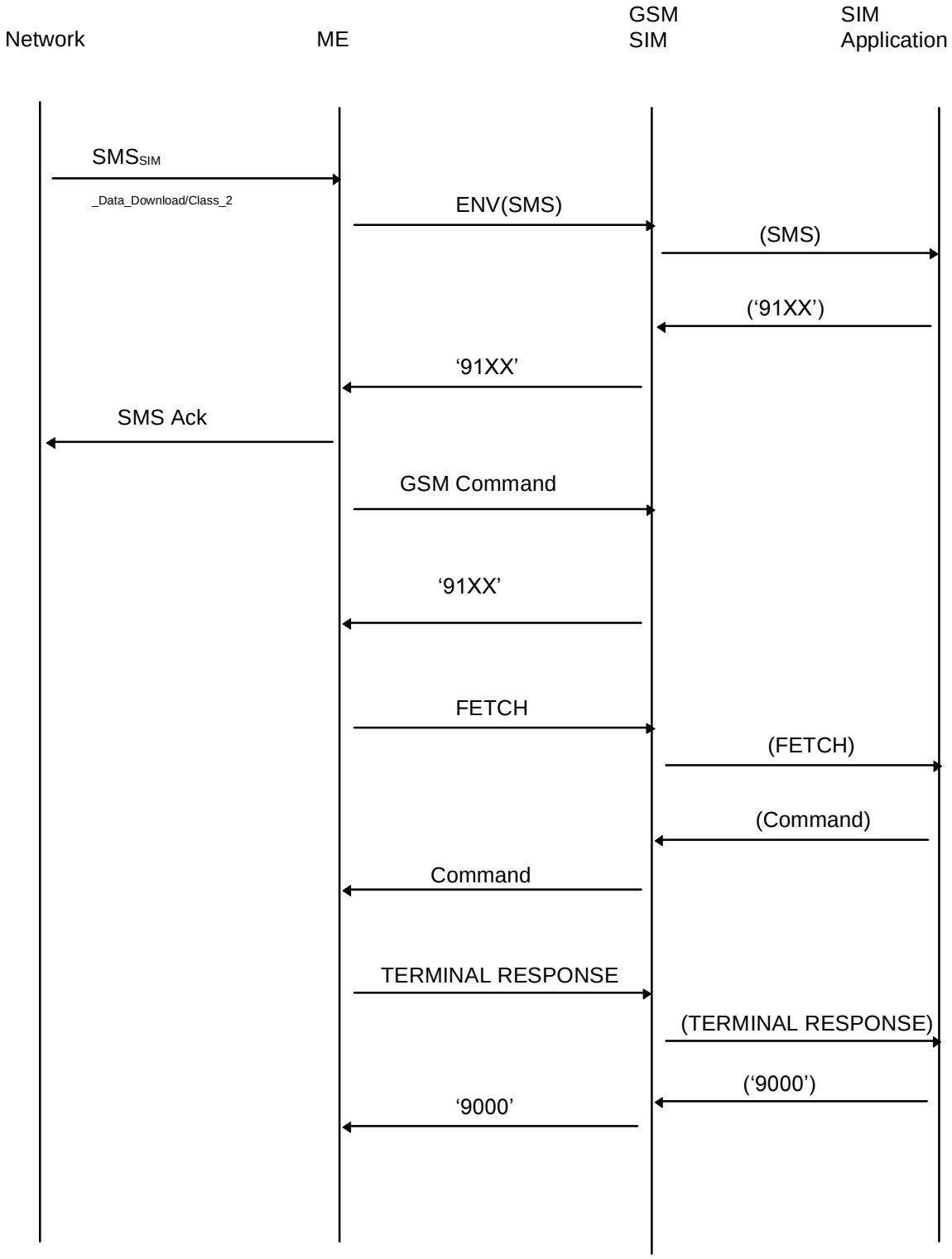
**Case 4: A Toolkit command generated by the SIM application as a result of an SMS from the network**




This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE).

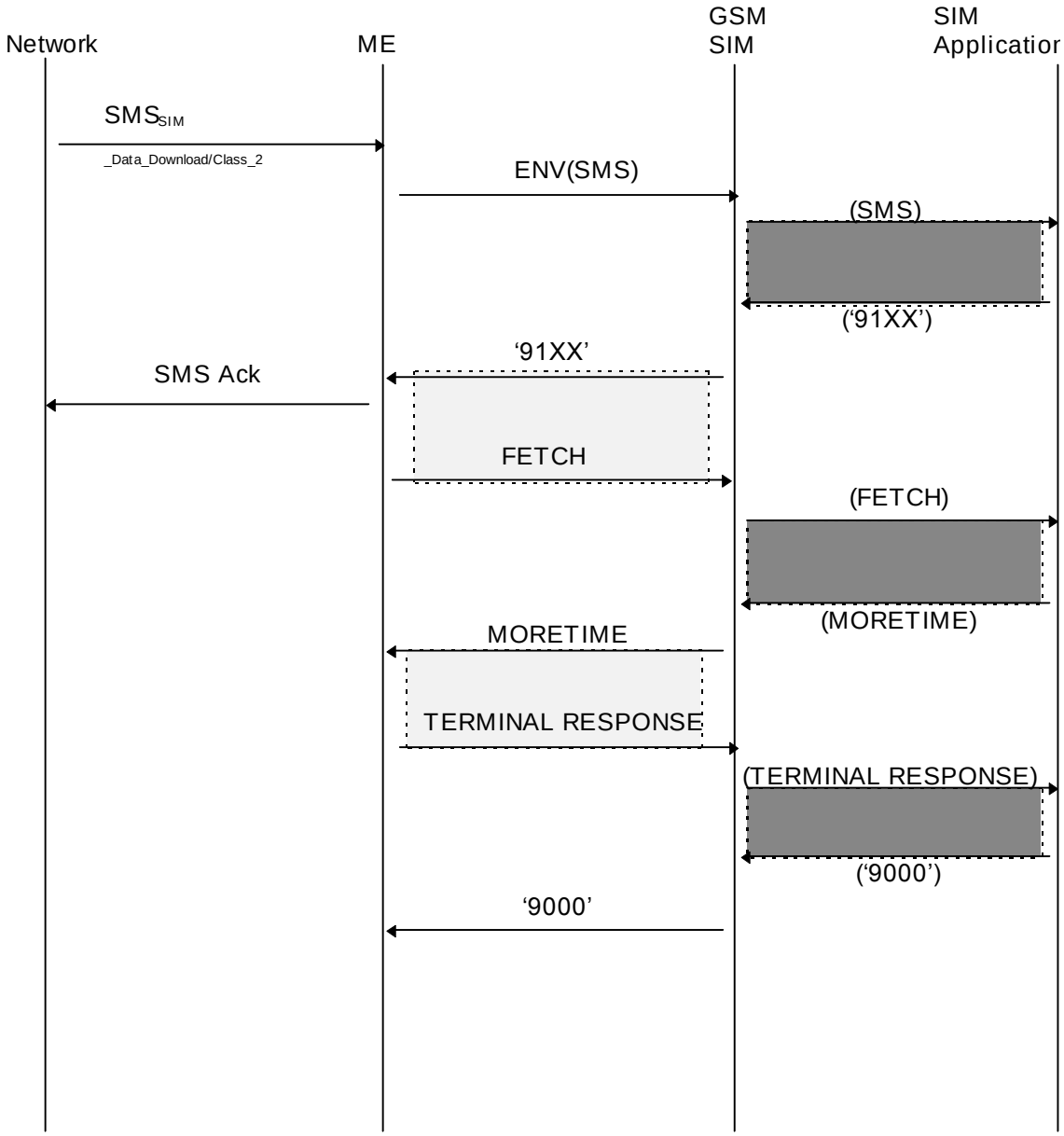
NOTE: If a positive acknowledgement to the network of completion of execution of the instructions given in the SMS message is required then the SIM application can issue a command to the ME to send a MO SMS.

**Case 5: A normal GSM command requires processing before the ME can respond to the 91XX from the SIM**




This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE). However a normal GSM command requires processing before the ME can FETCH the command which the SIM is waiting to give it. The response to the normal GSM command is '91XX' in this case to remind the ME of the outstanding SIM application command request.

**Case 6: MORE TIME Command**

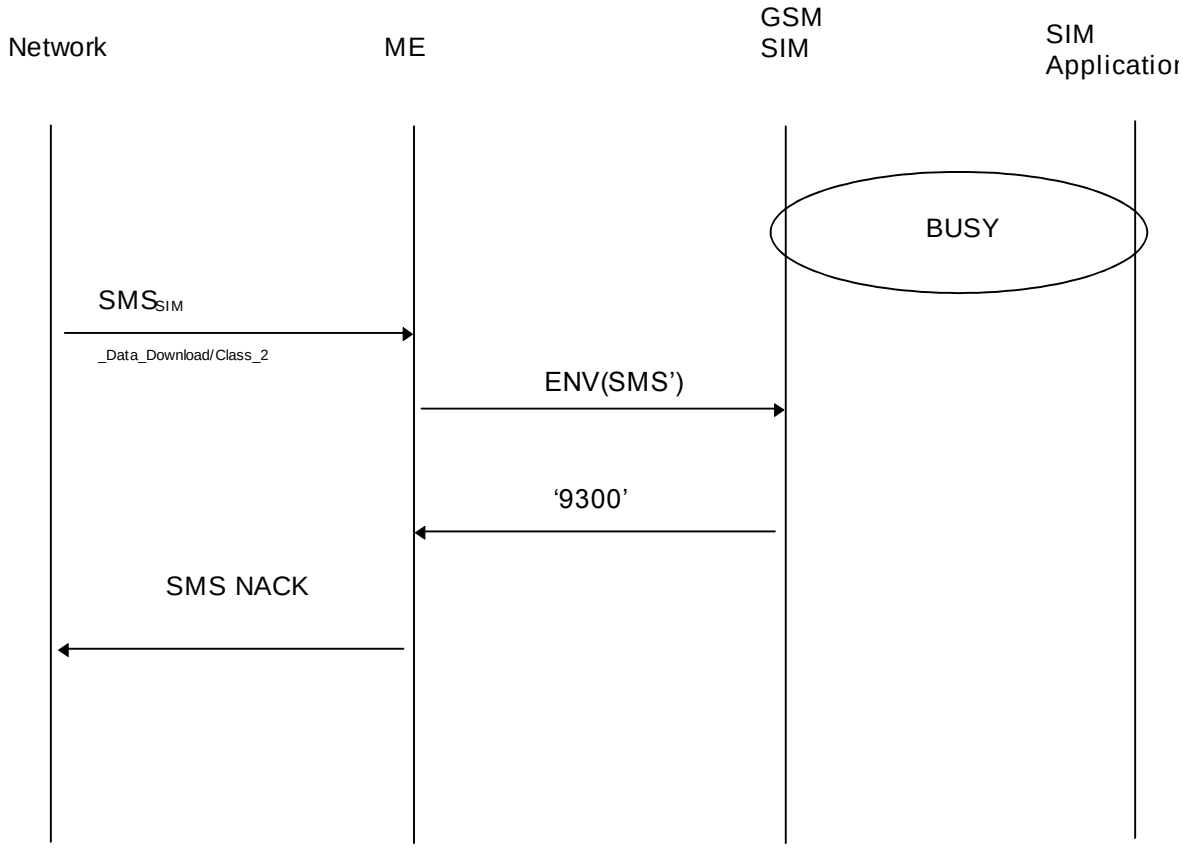



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and requires a considerable period of time to be processed by the SIM application. In this case the use of null procedure bytes only is inappropriate as the ME must be given the opportunity to process normal GSM commands. The opportunities gained by the SIM application for processing, and the opportunities for normal GSM commands are shown in the diagram above. The sequence of 91XX, FETCH and MORETIME commands can be repeated if required.

Opportunities to process normal GSM commands are shown thus:

Opportunities for SIM application processing are shown thus:

**Case 7: SIM Application Busy**




While the SIM application is busy processing a SMS for the SIM application arrives from the network and is sent to the SIM by the ME in the usual manner. The SIM operating system recognizes that the SIM application is busy, and it sends a busy response ('9300') to the ME. The ME then sends negative acknowledgement to the network. The responsibility for a retry rests with the network.

# Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSA IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSA IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:

| | | | |
|---|---|---|---|
| LSA descriptor type = LSA ID and number = 2 (1 byte) | LSA ID (3 bytes) | LSA ID (3 bytes) | Identifier (1 byte) |

2nd record:

| | | | | |
|---|---|---|---|---|
| LSA descriptor type = CI and number = 3 (1 byte) | CI (2 bytes) | CI (2 bytes) | CI (2 bytes) | Identifier (1 byte) |

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1st record:

| | | | |
|---|---|---|---|
| LSA descriptor type = LSA ID and number = 1 (1 byte) | LSA ID (3 bytes) | 'FF' | Identifier (1 byte) |

2nd record:

| | | | |
|---|---|---|---|
| LSA descriptor type = CI and number = 2 (1 byte) | CI (2 bytes) | CI (2 bytes) | Identifier (1 byte) |

# Annex G (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.


## G.1 Basic Image Coding Scheme

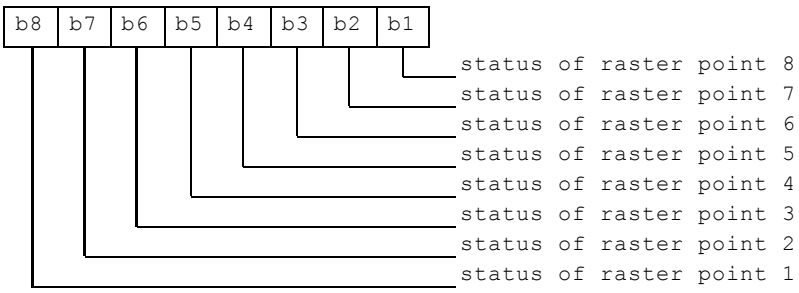
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

| Byte(s) | Description | Length |
|---|---|---|
| 1 | image width = X | 1 |
| 2 | image height = Y | 1 |
| 3 to K+2 | image body | K |

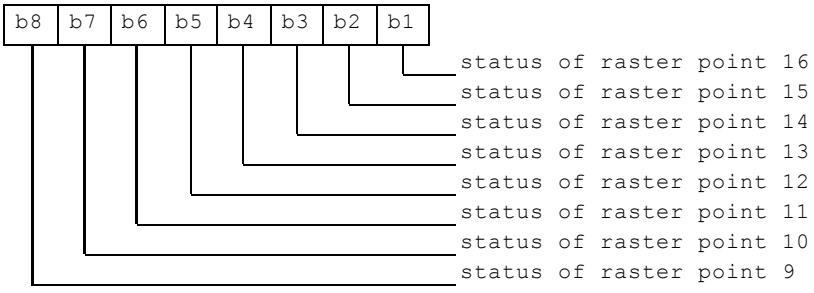
Coding of image body:

The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:




Byte 2:




etc.

Unused bits shall be set to 1

# G.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

| Byte(s) | Description | Length |
|---|---|---|
| 1 | Image width = X | 1 |
| 2 | Image height = Y | 1 |
| 3 | Bits per raster image point = B | 1 |
| 4 | Number of CLUT entries = C | 1 |
| 5 to 6 | Location of CLUT (Colour Look-up Table) | 2 |
| 7 to K+6 | Image body | K |

- Bits per raster image point:

  Contents:

  The number B of bits used to encode references into the CLUT, thus defining a raster image point's colour.

  B shall have a value between 1 and 8.

  Coding:

  Binary.

- Number of entries in CLUT:

  Contents:

  The number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1.

  C shall have a value between 1 and 2**B.

  Coding:

  Binary. The value 0 shall be interpreted as 256.

- Location of CLUT:

  Contents:

  This item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

  Coding:

  Byte 1: high byte of offset into Image Instance File.

  Byte 2: low byte of offset into Image Instance File.

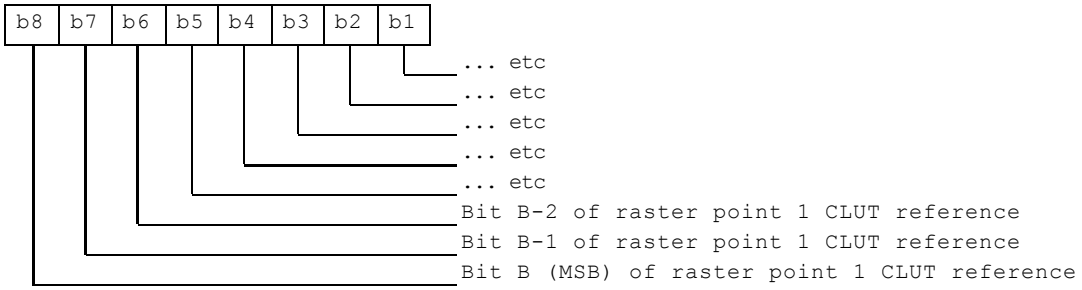
- Image body:

  Coding:

  Each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour.

  The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:




etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

C CLUT entries defining one colour each.

Coding:

The C CLUT entries are arranged sequentially:

| Byte(s) of CLUT | CLUT Entry |
|---|---|
| 1-3 | entry 0 |
| ... | ... |
| 3*(C-1) +1 to 3*C | Entry C-1 |

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

| Byte(s) of CLUT enty | Intensity of Colour |
|---|---|
| 1 | Red |
| 2 | Green |
| 3 | Blue |

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

# Annex H (normative): Coding of EFs for NAM and GSM-AMPS Operational Parameters

If the EIA/TIA-553 DF is provisioned on the SIM, then EFs specified in this annex and indicated as mandatory under the DF shall be provided. TIA/EIA-41 [40] based radio access systems should use this DF for storage of NAM parameters.

All quantities shown in the EF descriptions abide by the following rules unless otherwise specified:

- all unused bits of allocated parameters shall be set by default to 0;
- all unused bytes in a series of values (e.g. Partner, Favoured, or Forbidden SID List) should be set by default to 'FF'.

## H.1 Elementary File Definitions and Contents

### H.1.1 $EF_{MIN}$ (Mobile Identification Number)

This EF contains the Mobile Identification Number (MIN). The MIN is a 34-bit number used to address the mobile station across the AMPS and the TIA/EIA-136 air interfaces, and to identify the mobile station's home network. See TIA/EIA-136-005 [36] for further details on MIN.

| Identifier: '4F88' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 5 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV2 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 – 2 | MIN2 | M | 2 bytes |
| 3 – 5 | MIN1 | M | 3 bytes |

The MIN field is coded as follows:

- 6 most significant bits are unused;
- next 10 bits are MIN2;
- 24 least significant bits are MIN1;
- default MIN is '00 00 00 00 00' or 'FF FF FF FF FF'. In either case the ME shall interpret this as an invalid MIN and shall not transmit this value over the radio interface.

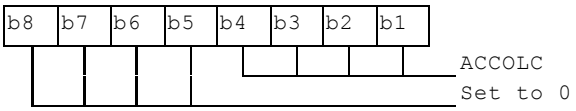
### H.1.2 $EF_{ACCOLC}$ (Access Overload Class)

This file contains the Access Overload Class (ACCOLC). The ACCOLC is a 4-bit indicator used to identify which overload class field controls the access attempts by the mobile station. See EIA/TIA-553 [41] for further details on ACCOLC.

| Identifier: '4F89' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 1 byte | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV2 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | ACCOLC<br>(possible values from '00' to '0F') | M | 1 byte |

Byte 1:




Initial value shall be '00'.

## H.1.3 $EF_{SID}$ (System ID Of Home System)

This file contains the system identity of the home system. The SID is a 15-bit number that uniquely identifies an AMPS or TIA/EIA-41 system. See EIA/TIA-553 [41] for further details on Home SID.

| Identifier: '4F80' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 2 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV2 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1-2 | System ID of Home System (SID)<br>( Most significant bit = 0) | M | 2 bytes |

The default value shall be '0000'.

## H.1.4 $EF_{IPC}$ (Initial Paging Channel)

The Initial (First) Paging Channel contains two 11-bit first paging channels (FIRSTCHP p-pri and FIRSTCHP p-sec) used to identify the channel number of the first paging channel when the mobile station is 'home'. See EIA/TIA-553 [41] for further details on First (Initial) Paging Channel.

| Identifier: '4F82' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 2-4 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV2 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 - 2 | FIRSTCHPpri (Initial Paging Channel) | M | 2 bytes |
| 3 – 4 | FIRSTCHPp-sec | O | 2 bytes |

- In the absence of the FIRSTCHPp-sec, the mobile station shall default to '02C4' if the primary channel = '014D' or '02E1' if the primary channel = '014E'

- A file size of 4 bytes may not be backwards compatible with the current dual-mode mobile equipment

The default of FISRTCHPpri value shall be '014D' for A systems, or '014E' for B systems.

## H.1.5 $EF_{GPI}$ (Group ID)

This file defines a subset of the most significant bits of the system identification (SID) that is used to identify a group of cellular systems for local control purposes. If the local control option is enabled within the mobile station and the bits of the home system identification that comprise the group identification match the corresponding bits of the SID read by the mobile station over the air, then the Local Control status shall be enabled. Otherwise, the Local Control status shall be disabled. Refer to EIA/TIA-553 [41] for additional details.

| Identifier: '4F81' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 1 byte | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV2 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Group ID | M | 1 byte |

- Group ID default value for North America = '0A'.

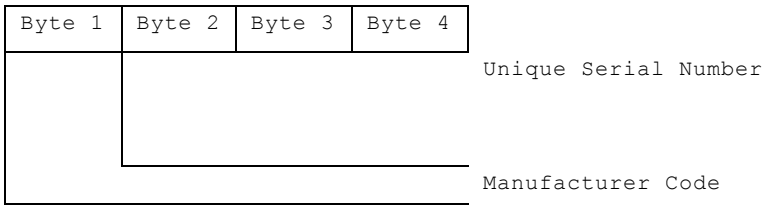
## H.1.6 $EF_{S\text{-}ESN}$ (SIM Electronic Serial Number)

This file stores a 32-bit electronic serial number (ESN) that is unique to the GSM-ANSI-136 SIM. The S-ESN can be unrelated to the ESN of any host equipment to which the GSM-ANSI-136 SIM may be attached. The S-ESN can be used for registration in conjunction with the MIN. The S-ESN may also be used in conjunction with the A-key and CAVE algorithm for authentication. See the ANSI-136 Usage Indicator file for details on the ESN usage indicator which specifies to the mobile equipment how the S-ESN should be used. See EIA/TIA-553 [41] for details on the ESN as it applies to registration and authentication.

The contents of this EF shall not be changed by any over-the-air procedures.

| Identifier: '4F8B' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 4 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | NEVER | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 – 4 | SIM ESN | M | 4 bytes |




The default value shall be 'FF FF FF FF'.

## H.1.7 $EF_{COUNT}$ (Call Count)

This file contains the CALL COUNT parameter. The CALL COUNT is used as a simple 'clone' detector in TIA/EIA-136 and AMPS modes. During the network access signalling in AMPS and other TIA/EIA-41 based networks, the SIM reports its CALL COUNT value to the network. If the value is consistent with the network perception of the CALL COUNT for that SIM, then the network will likely grant access based on the authentication process. During an AMPS or other TIA/EIA-41 based systems call, the value of the CALL COUNT may be incremented upon a command from the network. The value of the CALL COUNT, when incremented, is incremented by 1 using the INCREASE command. See EIA/TIA-553 [41] for further details on COUNTs-p.

| Identifier: '4F83' | Structure: Cyclic | Mandatory |
|---|---|---|
| File size: 3*N bytes | Update Activity: high | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| Most Recent Record | CALL COUNT | M | 3 bytes |
| --- | | … | … |
| Rec N | . . . | M | 3 bytes |

- File shall be initialised '00 00 00'
- Minimum file size is 2 records

## H.1.8 $EF_{PSID}$ (Positive/Favoured SID list)

This file contains a list of Favoured SIDs for use in identifying Favoured service providers while performing network selection (intelligent roaming).

| Identifier: '4F85' | Structure: transparent | Optional |
|---|---|---|
| File size: 2*N bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 – 2 | Favoured SID 1 | M | 2 bytes |
| … | Favoured SID 2 | O | … |
| (2N-1) – (2N) | Favoured SID N | O | 2 bytes |

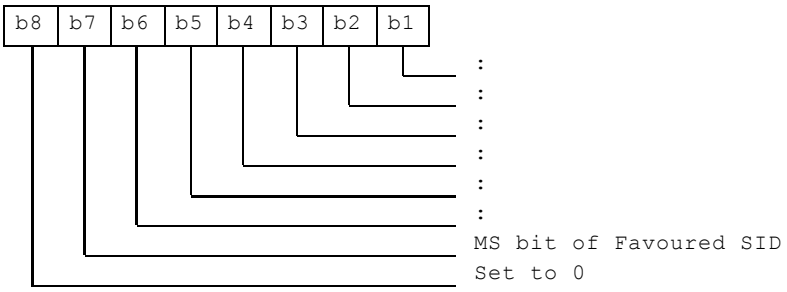
EOF (End of File) is indicated by 'FFFF'. An entry with all zeros is considered filler.

The most significant bit of the Favoured SID field is not used and it is set to 0.

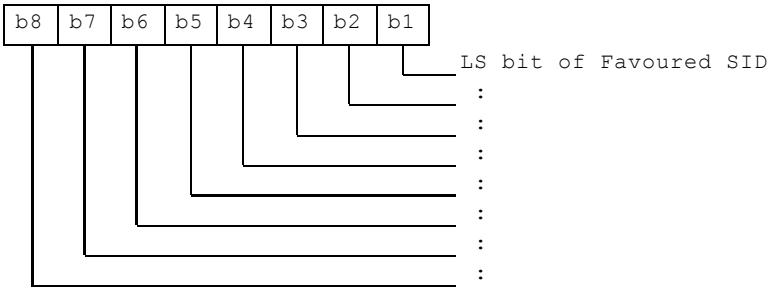
Coding of the Favoured SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:




Byte 2:




## H.1.9 $EF_{NSID}$ (Negative/Forbidden SID List)

This file contains a list of Forbidden SIDs, for use in identifying Forbidden service providers while performing network selection (intelligent roaming).

| Identifier: '4F84' | Structure: transparent | Optional |
|---|---|---|
| File size: 2*N bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 – 2 | Forbidden SID 1 | M | 2 bytes |
| … | Forbidden SID 2 | O | … |
| (2N-1) – (2N) | Forbidden SID N | O | 2 bytes |

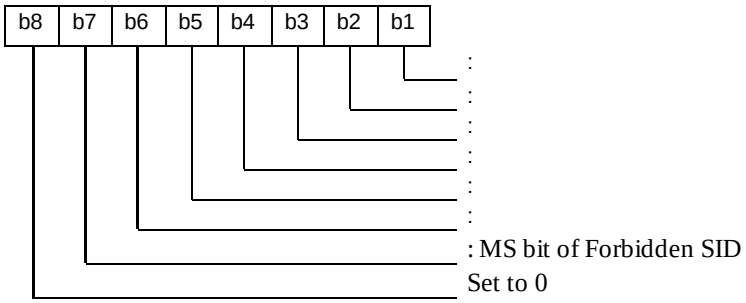
EOF (End of File) is indicated by 'FFFF.' An entry with all zeros is considered filler.

The most significant bit of the Forbidden SID field is not used and it is set to 0.

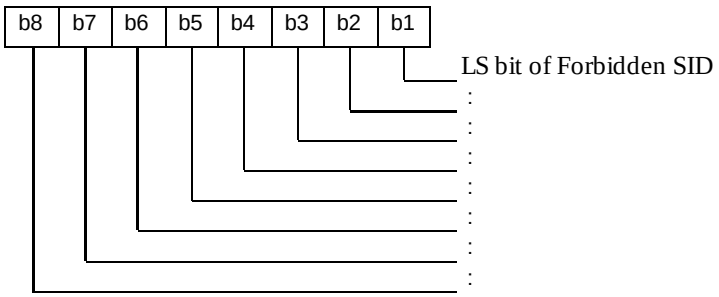
Coding of the Forbidden SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:




Byte 2:




## H.1.10 $EF_{SPL}$ (Scanning Priority List)

This file contains the Scanning Priority List. The Scanning Priority List is an array that defines the various types of systems that can be found. It also acts as a reference table, pointing to the various data structures in the SIM. This file is for backwards compatibility with GSM/AMPS mobile equipment. A Mobile Station supporting both TIA/EIA -136 and EIA/TIA-553 [41] is not expected to support this EF for network selection.

| Identifier: '4F87' | Structure: transparent | Optional |
|---|---|---|
| File size: 27 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Value 1 | M | 1 byte |
| 2 – 3 | Pointer 1 | M | 2 bytes |
| … | | | |
| … | | | |
| 25 | Value 9 | M | 1 byte |
| 26 – 27 | Pointer 9 | M | 2 bytes |

- The position of the pointers is fixed in this file. Highest priority level is 1, lowest priority level is 7. No two entries can have the same priority level with the exception the last two fields (Forbidden PLMNs and Negative SIDs) which both will have a value of 0. Default values are in parentheses. The values 1 or 2 shall reside in the first position (Home PLMN), and the second position (Last registered PLMN) shall contain a higher priority than position 3 (Preferred PLMNs List ) and 4 (Any Other PLMNs).

Format:

| Priority Value | Pointer | Reserved For |
|---|---|---|
| 1 – 7 (2) | SIM ('6F07') | Home PLMN |
| 1 – 7 (1) | SIM ('6F7E') | Last Registered PLMN |
| 1 – 7 (3) | SIM ('6F30') | Preferred PLMNs List |
| 1 – 7 (6) | 0 | Any Other PLMNs |
| 1 – 7 (4) | SIM ('4F80') | Home SID |
| 1 – 7 (5) | SIM ('4F85') | Positive SIDs List |
| 1 – 7 (7) | 0 | Any Other SIDs |
| 0 | SIM ('6F7B') | Forbidden PLMNs List |
| 0 | SIM ('4F84') | Negative SIDs List |

Constraints on the Priority List:

Mandatory PLMN priority order (highest to lowest):

Home PLMN or Last Registered PLMN, Preferred PLMNs, Any Other PLMNs

Mandatory SID priority order (highest to lowest):

Home SID, Positive SIs, Any Other SIDs.

## H.1.11 $EF_{NETSEL}$ (Network Selection Activation Flag)

This file contains the Network Selection Activation Flag. This flag is used to enable/disable the Manual Mode and some MMI functionality within the ME.

| Identifier: '4F86' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 1 byte | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV1 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Network Selection Activation Flag | M | 1 byte |

Enables / disables Manual Mode and some MMI functionality within the ME, in both AMPS and GSM modes.

Default value = 05 Hex.

Coding:

Bit 0 =0 GSM Manual Mode disabled

=1 GSM Manual Mode enabled (default)

Bit 1 =0 AMPS Manual Mode disabled (default)

=1 AMPS Manual Mode enabled

Bit 2 =0 Scanning Sequence Flags disabled

=1 Scanning Sequence Flags enabled (default)

Bit 3 =0 Disallow home only AMPS selection (default)

=1 Allow home only AMPS selection

Bits 4 through 7 are not used and set to zero.

## H.1.12 $EF_{CSID}$ (Current/Last Registered SID)

This file contains the SIDsp value. The most significant bit is unused and set to 0.

| Identifier: '4F8C' | Structure: transparent | | Optional |
|---|---|---|---|
| File size: 2 bytes | Update Activity: low | | |
| Access Conditions: | | | |
| READ | CHV1 | | |
| UPDATE | CHV1 | | |
| INVALIDATE | ADM | | |
| REHABILITATE | ADM | | |
| Bytes | Description | M/O | Length |
| 1 -2 | SIDsp | M | 2 bytes |

The default value shall be 'FFFF'.

## H.1.13 $EF_{REG-THRESH}$ (Registration Threshold)

This file contains the NXTREGsp value, specified in EIA/TIA-553 [41]. The three most significant bits are unused and are set to 0.

| Identifier: '4F8D' | Structure: transparent | | Optional |
|---|---|---|---|
| File size: 3 bytes | Update Activity: low | | |
| Access Conditions: | | | |
| READ | CHV1 | | |
| UPDATE | CHV1 | | |
| INVALIDATE | ADM | | |
| REHABILITATE | ADM | | |
| Bytes | Description | M/O | Length |
| 1 – 3 | NXTREGsp value | M | 3 bytes |

- (Default value = '00 00 00')

## H.1.14 $EF_{CCCH}$ (Current Control Channel)

This file contains the Current Control Channel information related to the Last Paging Control Channel on which the AMPS phone camped on.

| Identifier: '4F8E' | Structure: transparent | | Optional |
|---|---|---|---|
| File size: 2 bytes | Update Activity: low | | |
| Access Conditions: | | | |
| READ | CHV1 | | |
| UPDATE | CHV1 | | |
| INVALIDATE | ADM | | |
| REHABILITATE | ADM | | |
| Bytes | Description | M/O | Length |
| 1 – 2 | Current Control Channel | M | 2 bytes |

- (Default value = '0000')

## H.1.15 $EF_{LDCC}$ (Latest DCC)

This file contains the DCC value associated with the saved Current Control Channel.

| Identifier: '4F8F' | Structure: transparent | Optional |
|---|---|---|
| File size: 1 byte | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | CHV1 | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | DCC<br>(Default value = '00') | M | 1 byte |

## H.1.16 $EF_{GSM-RECON}$ (GSM Reconnect Timer)

This file specifies, in seconds, the time the ME should remain scanning the GSM-1900 spectrum, after loss of service from a GSM-1900 system, before any scanning of the AMPS spectrum is allowed.

| Identifier: '4F90' | Structure: transparent | Optional |
|---|---|---|
| File size: 2 bytes | Update Activity: low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1-2 | GSM Reconnect Timer<br>(Default value = '00 3C' = 60 seconds) | M | 2 bytes |

## H.1.17 $EF_{AMPS-2-GSM}$ (AMPS to GSM Rescan Timing Table)

The EF specifies, in minutes, a series of (typically increasing) intervals for scanning the GSM-1900 spectrum, used while in-service on an AMPS network while in Dual-Mode operation. The time is measured from the end of the last GSM-1900 scan to the start of the next GSM-1900 scan. If the table is not completely filled (i.e. the end-of-table value 'FF' is found), the last filled value may be repeated indefinitely. If a value of 'F0' is encountered, the table is terminated, as are all rescans to GSM until the current AMPS system is lost.

| Identifier: '4F91' | Structure: transparent | Optional |
|---|---|---|
| File size: 10 bytes | Update Activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | First Rescan Attempt Interval (Default = '02') | M | 1 byte |
| 2 | Second Rescan Attempt Interval (Default = '03') | M | 1 byte |
| 3 | Third Rescan Attempt Interval (Default = '04') | M | 1 byte |
| 4 | Fourth Rescan Attempt Interval (Default = '05') | M | 1 byte |
| 5 | Fifth Rescan Attempt Interval (Default = '06') | M | 1 byte |
| 6 | Sixth Rescan Attempt Interval (Default = 'FF') | M | 1 byte |
| 7 | Seventh Rescan Attempt Interval (Default = 'FF') | M | 1 byte |
| 8 | Eighth Rescan Attempt Interval (Default = 'FF') | M | 1 byte |
| 9 | Ninth Rescan Attempt Interval (Default = 'FF') | M | 1 byte |
| 10 | Tenth Rescan Attempt Interval (Default = 'FF') | M | 1 byte |

## H.1.18 $EF_{*FC1}$ (Feature Activation Codes)

This file contains the feature code table as specified in EIA/TIA-553 [41].

| Identifier: '4F8A' | Structure: transparent | Optional |
|---|---|---|
| File size: 2 bytes | Update Activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1-2 | Default value 'B990'. | M | 2 bytes |

## H.1.19 $EF_{AMPS-UI}$ (AMPS USAGE INDICATORS)

This file contains usage indicators for local control and extended address method.

| Identifier: 4F93 | File Type: Transparent | Optional |
|---|---|---|
| File size: 2 bytes (minimum) | Update Activity: Low | |
| Access Conditions: | | |
| READ | CHV1 | |
| UPDATE | ADM | |
| INVALIDATE | ADM | |
| REHABILITATE | ADM | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Number of Services (S) | M | 1 byte |
| 2 | Services n°1 to n°8 | M | 1 byte |

-Services:

Contents

Service n°1 : Local Control Indicator (see Note 1)

Service n°2 : Extended Address Method indicator – included in any access attempts (see Note 2)

Services n3°-n°8 : RFU

- Number of Services

Contents:

This byte refers to the number of services defined in the following byte.

Coding:

This byte is coded as BCD

Services

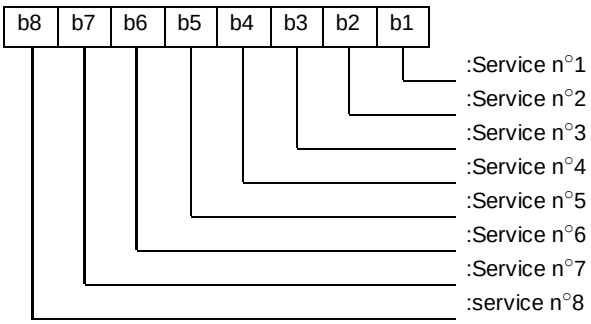
Contents:

This byte describes the services

Coding:

- One bit is used to code each service
- If the bit = 0: service is not enabled
- If the bit = 1: service is enabled
- The bits for services not yet defined shall be set to RFU. For coding of RFU see clause 9.3.

Byte 2:



NOTE 1: The Local Control Indicator is a means provided within the mobile station to enable or disable the local control option. Local Control is a mechanism that allows a cellular system to customise operation for home mobile stations, and for those roaming mobile stations whose home systems are members of a group, by sending local orders with the order field set to local control (which informs the mobile station to examine the local control field), and by sending one or both of two local control global action overhead messages.

A group of systems could be formed by participating systems agreeing to a common set of local control protocols and whose system identifications (SID) are recognised by mobile stations as a common group.

NOTE 2: The Extended Address Method indicator determines if the extended address word must be included in all access attempts.

# H.2 Authentication Functionality

## H.2.1 A-KEY (ANSI-41 Authentication Key)

The A-Key is only accessible to the algorithm used for Key generation. The A-Key may be programmed into the SIM directly by the service provider, or it may be programmed into the SIM through a specific over the air procedure. The A-Key is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in the present document. The SIM command A-KEY_VALIDATION is used to store the A-Key on the SIM.

## H.2.2 SSD (Shared Secret Data)

The Shared Secret Data is accessible only to the Authentication and the Key Generation functions. SSD is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in the present document.

An additional Status Code is defined for SSD updating as follows:

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

# H.3 Authentication commands

It is necessary to provide six interfaces to the CAVE Algorithm and Secret Data areas, as listed below:

- Generation of Authentication Signature data, and generation of ciphering keys.
- Validation and storage of entered A-Key's
- Ask Random task (generates RANDBS)
- Update Shared Secret Data (Generates SSD_A_NEW, SSD_B_NEW and AUTHBS values)
- Confirm Shared Secret Data (Updates SSD values)
- CMEA Encryption of voice channel data digits

NOTE: For each task, the expected normal (i.e. success) status code is listed in the status word description. A list of possible error codes that apply to all tasks can be found in the SIM Status Codes.

The interpretation of these instruction codes (INS in the table below) is valid only for class A0.

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| Internal_Authenticate | 'A0' | '88' | '00' | '00' | '0F' |
| AKEY_validation | 'A0' | '86' | '00' | '00' | '12' |
| Ask_Random | 'A0' | '8A' | '00' | '00' | '04' |
| Update_SSD | 'A0' | '84' | '00' | '00' | '0C' |
| Confirm_SSD | 'A0' | '82' | '00' | '00' | '03' |
| CMEA_encrypt | 'A0' | '8C' | '00' | '00' | 'nn' |

## H.3.1 Generation of Authentication Signature Data and Ciphering Keys

This task produces an Authentication response, and shall be used during mobile Registrations, Originations, Terminations, R_Data messages, SPACH Confirmations, and for the Unique Challenge-Response Procedure. If Byte 0, Bit 1 is set, the SIM should also generate key bits after completing the Authentication function. Some of those ciphering octets may be passed back to the ME for use with supplementary crypto mechanisms which reside in the ME. This task requires the following input parameters:

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| Internal_Authenticate | 'A0' | '88' | '00' | '00' | '0F' |

Coding::

Byte 0 Process Control Byte

Bit 0 0=RANDs, 1= RANDU

Bit 1 Generate Key Bits flag (0= No, 1= Yes)

Bit 2 Load Internal key flag:

(0= pass all generated key bytes to handset, 1= load first 8 bytes of generated keys internally to SIM, pass all remaining key bytes to ME)

Bits 3-7 Unused, future expansion

Bytes 1-4 RANDs (for Registrations, Originations, and Terminations)

or

Bytes 1-3 RANDU (for Unique Challenge-Response Procedures)
Byte 4 = 0 (MIN2 will be filled in by SIM)

Byte 5 Digits Length (in bits, =0, 4, 8, 12, 16, 20 or 24,

= 4 x number of digits in bytes 6-8)

Bytes 6-8 =0,0,0 (for Registrations, Terminations, Unique Challenge Response Procedures)

= Last Dialed Digits, unused bits filled with 0's (for Originations). If more than 6 digits are dialed, these are the last 6 digits in the origination string. If less than 6 digits are dialed, MIN1 will be filled in by the SIM for the unused bits.

Byte 9 Use ME ESN (='00')

Bytes 10-13 ESN

Byte 14 Key_size (=0 if Byte 0, Bit 1= 0, =8 (or more) if Byte 0, Bit 1 = 1)

The output of this task shall be:

Status Bytes: SW1 ('9F' if success)

SW2 ('nn' if success)

('nn' is 03+Key_size if Byte 0, Bit 2 above =0, 03+Key_size-08 if Byte 0, Bit 2 above =1)

## H.3.2 Validation and Storage of Entered A-Key's

With manual entry of the A-key, the input A-Key must be validated prior to its storage in the SIM. If successful, the A-key is saved in the SIM and the COUNTsp and Shared Secret Data (SSD) are reset to zero. This task requires the following input parameters:

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| AKEY_validation | 'A0' | '86' | '00' | '00' | '12' |

Coding:

Bytes 0 - 12

Authentication digits string (first digit in Most-Significant nibble of byte 0, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)

Byte 13 Use ME ESN ('00')

Bytes 14-17 ESN

The output of this task shall be:

Status Bytes: SW1 ('90' if success)

SW2 ('00' if success)

## H.3.3 Ask Random Task

This task is used to generate the RANDBS random value. This task must be executed prior to updating the Shared Secret Data (SSD). The value RANDSeed must be generated by the ME prior to calling this task. This task requires the following input parameters:

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| Ask_Random | 'A0' | '8A' | '00' | '00' | '04' |

Coding:

Bytes 0-3 RANDSeed

The output of this task shall be:

Status Bytes: SW1 ('9F' if success)

SW2 ('04' if success)

## H.3.4 Update Shared Secret Data

This task is used to generate the preliminary new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) and the AUTHBS value. The Ask Random Task (see above) must be executed prior to this routine. The task requires the following input parameters:

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| Update_SSD | 'A0' | '84' | '00' | '00' | '0C' |

Coding:

Bytes 0-6 RANDSSD

Byte 7 Use ME ESN (='00')

Bytes 8-11 ESN

The output of this task shall be:

Status Bytes: SW1 ('90' if success, '98' if failure)

SW2 ('00' if success, '04' if failure)

## H.3.5 Confirm Shared Secret Data

This task is used to validate the new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) by comparing the internally computed AUTHBS with the AUTHBSs received from the system. If successful, the SSD_A and SSD_B values will be updated to match the SSD_A_NEW and SSD_B_NEW values, respectively The task requires the following input parameters:

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| Confirm_SSD | 'A0' | '82' | '00' | '00' | '03' |

Coding:

Bytes 0-2 AUTHBSs

The output of this task shall be:

Status Bytes: SW1 ('90' if success)

SW2 ('00' if success)

## H.3.6 CMEA Encryption of Voice Channel Data Digits

This task is used when the MS is on a Voice Channel, to encrypt and decrypt some portions of digital messages transmitted to the BS. These will occur for the following messages:

- Called Address Message (in response to a hookflash, up to 4 bytes per word, 4 words, total of 16 bytes)

| Task Name | CLA | INS | P1 | P2 | Lc |
|---|---|---|---|---|---|
| CMEA_encrypt | 'A0' | '8C' | '00' | '00' | 'nn' |

where 'nn' is hex value of data length n

Coding:

Bytes 0 - (n-1) The n-byte data to be encoded, max. size = 32 bytes.

The output of this task shall be:

Status Bytes: SW1 ('9F' if success)

SW2 (='nn' if success) ('nn' is hex value of data length n)

## H.3.7 SIM Status Codes

The following status codes, returned by the SIM in response to the execution of any of the tasks specified in the present document, are valid. The first hex value is returned in SW1, the second hex value in SW2.

**Success Codes:**

90, 00 Generic success code

9F, xx Success, xx bytes of data available to be read via "Get_Response" task.

**Error Codes:**

92, 40 Error, memory problem

94, 08 Error, file is inconsistent with the command

98, 04 Error, no CHV1 has been presented successfully

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

67, xx Error, incorrect parameter P3 (ISO code)

6B, xx Error, incorrect parameter P1 or P2 (ISO code)

6D, xx Error, unknown instruction code given in the command (ISO code)

6E, xx Error, wrong instruction class given in the command (ISO code)

6F, xx Error, technical problem with no diagnostic given (ISO code)

6F, 00 Error, invalid input parameters to authentication computation

# Annex I (informative): EF changes via Data Download or SIM Toolkit applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by SIM Toolkit Application (e.g. by using the SIM API), is advisable. Updating of certain EFs, "over the air" such as $EF_{ACC}$ could result in unpredictable behaviour of the MS; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

| File identification | Description | Change advised |
|---|---|---|
| '2F05' | Extended Language preference | Yes |
| '2FE2' | ICC identification | No |
| '4F20' | Image data | Yes |
| '4Fxx' | Image Instance data Files | Yes |
| '6F05' | Language preference | Yes |
| '6F07' | IMSI | Caution (note) |
| '6F20' | Ciphering key Kc | No |
| '6F2C' | De-personalization Control Keys | Caution |
| '6F30' | PLMN selector | Caution |
| '6F31' | HPLMN search period | Caution |
| '6F32' | Co-operative network | Caution |
| '6F37' | ACM maximum value | Yes |
| '6F38' | SIM service table | Caution |
| '6F39' | Accumulated call meter | Yes |
| '6F3A' | Abbreviated dialling numbers | Yes |
| '6F3B' | Fixed dialling numbers | Yes |
| '6F3C' | Short messages | Yes |
| '6F3D' | Capability configuration parameters | Yes |
| '6F3E' | Group identifier level 1 | Yes |
| '6F3F' | Group identifier level 2 | Yes |
| '6F40' | MSISDN storage | Yes |
| '6F41' | PUCT | Yes |
| '6F42' | SMS parameters | Yes |
| '6F43' | SMS status | Yes |
| '6F44' | Last number dialled | Yes |
| '6F45' | CBMI | Caution |
| '6F46' | Service provider name | Yes |
| '6F47' | Short message status reports | Yes |
| '6F48' | CBMID | Yes |
| '6F49' | Service Dialling Numbers | Yes |
| '6F4A' | Extension 1 | Yes |
| '6F4B' | Extension 2 | Yes |
| '6F4C' | Extension 3 | Yes |
| '6F4D' | Barred dialling numbers | Yes |
| '6F4E' | Extension 4 | Yes |
| '6F50' | CBMIR | Yes |
| '6F51' | Network's indication of alerting | Caution |
| '6F52' | GPRS Ciphering key KcGPRS | No |
| '6F53' | GPRS Location Information | Caution |
| '6F58' | Comparison method information | |
| '6F60' | User controlled PLMN Selector with Access Technology | see 3GPP TS 22.011 |
| '6F61' | Operator controlled PLMN Selector with Access Technology | Caution |
| '6F62' | HPLMN Selector with Access Technology | Caution |
| '6F63' | CPBCCH information | No |
| '6F64' | Investigation scan | Caution |
| '6F65' | RPLMN last used Access Technology | No |
| '6F74' | BCCH information | No |
| '6F78' | Access control class | Caution |
| '6F7B' | Forbidden PLMNs | Caution |
| '6F7E' | Location information | No (note) |

**Continued.....**

| File identification | Description | Change advised |
|---|---|---|
| '6FAD' | Administrative data | Caution |
| '6FAE' | Phase identification | Caution |
| '6FB1' | Voice Group Call Service | Yes |
| '6FB2' | Voice Group Call Service Status | Yes |
| '6FB3' | Voice Broadcast Service | Yes |
| '6FB4' | Voice Broadcast Service Status | Yes |
| '6FB5' | Enhanced Multi Level Pre-emption and Priority | Yes |
| '6FB6' | Automatic Answer for eMLPP Service | Yes |
| '6FB7' | Emergency Call Codes | Caution |
| '6FC5' | PLMN Network Name | Yes |
| '6FC6' | Operator PLMN List | Yes |
| '6FC7' | Mailbox Dialling Numbers | Yes |
| '6FC8' | Extension 6 | Yes |
| '6FC9' | Mailbox Identifier | Caution |
| '6FCA' | Message Waiting Indication Status | Caution |
| '6FCB' | Call Forwarding Indication Status | Caution |
| '6FCC' | Extension 7 | Yes |
| '6FCD' | Service Provider Display Information | Yes |
| NOTE: If $EF_{IMSI}$ is changed, the SIM should issue REFRESH as defined in TS 11.14 [27] and update $EF_{LOCI}$ accordingly. | | |

# Annex J (informative): Tags defined in the present document

| Tag | Name of Data Element | Usage |
|---|---|---|
| 'A3' | Service provider display information<br>The following tags are encapsulated within 'A3':<br>'80' Service provider PLMN list | Service Provider Display Information ($EF_{SPDI}$) |

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825 [56]

# Annex K (informative): Change history

This annex lists all change requests approved for the present document since the first phase2+ version was approved by ETSI SMG.

| Meeting | Plenary tdoc | WG tdoc | VERS | CR | RV | Rel-ease | CAT | SUBJECT | Resulting Version |
|---|---|---|---|---|---|---|---|---|---|
| s16 | 709/95 | 154/95 | 4.15.0 | A008 | | R96 | 1 | SIM Speed Enhancement | 5.0.0 |
| s17 | 062/96 | 147/95 | 5.0.0 | A006 | | R96 | B | Service Dialling Numbers | 5.1.0 |
| | 060/96 | 06/96 | | A009 | | R96 | B | ASCI for VGCS and VBS | |
| | 060/96 | 06/96 | | A010 | | R96 | B | ASCI for eMLPP | |
| | 059/96 | 204/95r | | A013 | | R96 | C | Interaction betw een FDNs and ADNs | |
| | 061/96 | 05/96 | | A014 | | R96 | D | Correction of baud rate for SIM Speed enhancement | |
| s18 | 263/96 | 57/96 | 5.1.0 | A011 | 3 | R96 | B | SIM Application Toolkit protocol enhancements | 5.2.0 |
| | 260/96 | 45/96 | | A016 | | R96 | A | SIM presence detection clarification | |
| | 261/96 | 54/96 | | A018 | | R96 | A | Reponse codes and coding of SIM service table | |
| | 262/96 | 55/96 | | A020 | | R96 | A | Reference to International Standards | |
| s19 | 374/96 | 102/96 | 5.2.0 | A012 | | R96 | C | Contacting elements | 5.3.0 |
| | 373/96 | 105/96 | | A023 | | R96 | A | Clarification of clock stop timing | |
| | 409/96 | 107/96 | | A024 | 1 | R96 | B | Emergency Call Codes (ECC) | |
| | 374/96 | 108/96 | | A025 | | R96 | C | Using ranges of CBMIs | |
| s20 | 580/96 | 206/96 | 5.3.0 | A021 | | R96 | B | Barred Dialling Numbers | 5.4.0 |
| | 734/96 | 197/96 | | A026 | | R96 | B | Addition of Cooperative Netw ork List EF | |
| | 734/96 | 197/96 | | A027 | | R96 | B | Addition of ME Depersonalisation feature and EF | |
| | 702/96 | 207/96 | | A031 | | R96 | D | RFU bit taken into use in GSM 11.12 | |
| s21 | 101/97 | 97/079 | 5.4.0 | A032 | 2 | R96 | D | Ammendment to BDN diagrams in Annex B | 5.5.0 |
| | 101/97 | 97/086 | | A033 | 1 | R96 | B | DFs for MSS/ PCS1900/other use | |
| | 101/97 | 97/056 | | A034 | | R96 | C | Reading of EFDCK during SIM initialisation | |
| | 101/97 | 97/058 | | A036 | | R96 | D | Administrative Access Conditions | |
| | 101/97 | 97/059 | | A037 | | R96 | B | Format of EFCNL to include fields for Corporate Personal. Code | |
| | 101/97 | 97/089 | | A041 | | R96 | B | Administrative Data field | |
| s22 | 356/97 | 183/97 | 5.5.0 | A042 | | R97 | B | Extended language preference | 5.6.0 |
| | 356/97 | 163/97 | | A044 | 1 | R96 | A | Clarification of electrical/mechanical SIM/ME interface | |
| | 356/97 | 179/97 | | A045 | | R96 | D | Security procedures for 2nd level; DFs located under DF GSM | |
| | 356/97 | 187/97 | | A047 | | R96 | F | Number of bytes returned after a SELECT command | |
| | 356/97 | 093/97 | | A048 | | R96 | D | Serivce table and "radio interface" | |
| | 356/97 | 109/97 | | A049 | | R96 | F | Update Access condition of EFDCK (aligns 11.11 & 02.22) | |
| s23 | 788/97 | 97/249 | 5.6.0 | A046 | 2 | R97 | B | Short Message Status Reports | 5.7.0 |
| | 788/97 | 97/243 | | A050 | | R96 | F | Addition of SDN and BDN in the description of EFCCP | |
| | 788/97 | 97/259 | | A051 | 1 | R97 | C | SIM and ME behaviour w hen SIM is disabled and blocked | |
| | 788/97 | 97/262 | | A053 | | R96 | F | Response data following an ENVELOPE command | |
| | 788/97 | 97/260 | | A054 | | R96 | F | Coding of EFPhase | |
| | 788/97 | 97/271 | | A055 | | R97 | C | Changes to Dialling Number Files and extensions | |
| | 788/97 | 97/261 | | A056 | | R97 | B | Netw ork's indication of alerting in the MS | |
| s24 | 97-0886 | 97/365 | 5.7.0 | A052 | 2 | R97 | b | Introduction of UCS2 | 5.8.0 |
| | 97-0886 | 97/383 | | A057 | | R97 | c | MO SMS control by SIM | |
| *At SMG #25, it was decided to create a version 6.0.0 of every specification that contained at least one release '97 work item and a version 7.0.0 of every specification that contained at least one release '98 work item.* | | | | | | | | | |
| s25 | 98-0157 | 98p052 | 5.8.0 | A058 | 2 | R97 | B | Addition of EFs for GPRS | 6.0.0 |
| | 98-0157 | 98p108 | | A059 | | R97 | F | Clarification regarding EFCCP records | |
| | 98-0157 | 98p094 | | A061 | 1 | R96 | A | Clarification of removal of the SIM | |
| s26 | 98-0398 | 98p228 | 6.0.0 | A062 | 2 | R98 | B | Icons - addition of EF IMG and DF GRAPHICS | 7.0.0 |
| | 98-0398 | 98p227 | | A064 | | R98 | B | Operation of ME w ith multiple card readers | |
| | 98-0400 | 98p237 | | A065 | | R98 | F | Deletion of all release 97 markers from the R98 version | |
| | 98-0398 | 98p240 | | A066 | | R97 | F | RP-ACK RP-ERROR for SIM data dow nload error | |
| | 98-0398 | 98p263 | | A069 | | R97 | D | Allocation of file ID for IS-41 | |
| | | | | | | | | | |

(continued)

## Change History (continued)

| Meeting | Plenary tdoc | WG tdoc | VERS | CR | RV | Release | CAT | SUBJECT | Resulting Version |
|---|---|---|---|---|---|---|---|---|---|
| s27 | 98-0671 | 98p339 | 7.0.0 | A071 | | R98 | C | Enhanced image coding schemes (colour icons) | 7.1.0 |
| | 98-0671 | | | A072 | 1 | R98 | D | Addition of reference to PCS 1900 | |
| s28 | P-99-185 | 9-99-076 | 7.1.0 | A073 | 1 | R98 | F | Alignment with 2nd edition of ISO/IEC 7816-3 (1997) | 7.2.0 |
| | P-99-185 | 9-99-037 | | A074 | | R98 | B | Addition of SoLSA data fields | |
| | P-99-185 | 9-99-066 | | A075 | 1 | R98 | B | Addition of CTS fields | |
| | P-99-185 | 9-99-095 | | A076 | 1 | R98 | B | Definition of a file containing the title of the main menu | |
| | P-99-185 | 9-99-072 | | A077 | | R98 | C | USSD format indication in the SIM Service Table | |
| | P-99-185 | 0-99-093 | | A078 | | R98 | B | Informative annex on EF changes | |
| | P-99-185 | 9-99-097 | | A080 | | R98 | C | Additional GPRS field | |
| | P-99-188 | | | A082 | | R98 | D | Deletion of $(.....)$ release markers | |
| s29 | P-99-412 | 9-99-163 | 7.2.0 | A083 | 1 | R98 | C | EF IMSI changes via data download or SIM toolkit application | 8.0.0 |
| | P-99-412 | 9-99-180 | | A084 | | R98 | F | Addition of RUN AT COMMAND to the SIM service table | |
| | P-99-412 | 9-99-208 | | A085 | | R99 | C | Alignment of maximum of records in a linear fixed file in | |
| s30 | P-99-670 | 9-99-260 | 8.0.0 | A089 | | R99 | A | Correction for coding of SoLSA "Priority" field | 8.1.0 |
| | P-99-670 | 9-99-277 | | A090 | | R99 | D | Clarification of the Ciphering Indicator disable bit in the EFad | |
| | P-99-670 | 9-99-281 | | A091 | | R99 | F | Introduction of a new DF for the TIA/EIA-136 technology | |
| | P-99-670 | 9-99-294 | | A092 | 1 | R99 | B | Addition of EF definitions under the PCS 1900 DF | |
| | P-99-670 | 9-99-310 | | A093 | | R99 | F | Clarification about "Memory Problem" error for $EF_{LOCI}$ update | |
| | P-99-670 | 9-99-300 | | A094 | | R99 | F | Execution time of SIM toolkit procedures | |
| | P-99-670 | 9-99-311 | | A095 | | R99 | B | Introduction of a new DF for the TIA/EIA-95 technology | |
| | P-99-670 | 9-99-258 | | A097 | | R99 | A | Clarification of Optional Status for GPRS files | |
| s31 | P-00-137 | 9-00-0088 | 8.1.0 | A098 | | R99 | F | Clarification of interactions for CBS and the language files | 8.2.0 |
| | P-00-137 | 9-00-0092 | | A101 | | R99 | F | Correction to coding of ASCI EF eMLPP. | |
| | P-00-137 | 9-00-0095 | | A104 | | R99 | F | Addition of coding for ASCI Efs (VGCS and VBS) | |
| | P-00-137 | 9-00-0098 | | A107 | | R99 | F | Correction of the byte numbering related to EF LOCIGPRS | |
| | P-00-137 | 9-00-0133 | | A108 | | R99 | F | Corrections and additions to DF-5F40 | |
| | P-00-137 | 9-00-0146 | | A109 | 1 | R99 | F | Clarification of manual entry of the A-Key. | |
| | P-00-137 | 9-00-0151 | | A110 | | R99 | D | Addition of reference to the File ID as used in the TETRA | |
| | P-00-137 | 9-00-0163 | | A111 | 1 | R99 | B | COMPACT Cell Selection | |
| | P-00-137 | 9-00-0155 | | A112 | | R99 | B | COMPACT Cell Selection - Investigation Scan indicator for | |
| | P-00-139 | 9-00-0161 | | A113 | | R99 | B | Enhancement to CCP coding (CR number incorrect in P-00- | |
| | P-00-139 | 9-00-0159 | | A114 | | R99 | B | Enhancement of BDN feature (CR number incorrect in P-00- | |
| s32 | P-00-296 | 9-00-0232 | 8.2.0 | A120 | | R99 | B | DFs for MExE | 8.3.0 |
| | P-00-296 | 9-00-0276 | | A122 | | R99 | C | HPLM length | |
| | P-00-296 | 9-00-0275 | | A123 | | R99 | A | LAI, RAI and CNL : alignment with GSM 04.08 | |
| | P-00-296 | 9-00-0273 | | A124 | | R99 | F | PLMN Selection Corrections regarding RFU bits | |
| *Following the closure of ETSI SMG and the agreement of the 3GPP in July 2000 to undertake responsibility for remaining GSM specifications, the change requests listed below were approved by 3GPP TSG-T. This change in responsibility also changed the specification number from "GSM 11.11" to "3GPP TS 11.11".* | | | | | | | | | |
| TP-09 | TP-000176 | 9-00-0253 | 8.3.0 | A116 | | R99 | F | PLMN Selection Corrections and additions for EDGE | 8.4.0 |
| | TP-000176 | 9-00-0269 | | A119 | | R99 | C | Addition of RPLMN file | |
| | TP-000148 | T3-000479 | | A126 | | R99 | F | Standardise the current GAIT commands and reserving | |
| TP-11 | TP-010038 | T3-010047 | 8.4.0 | A127 | | R99 | F | Addition of file ID for indicating iDEN access technology | 8.5.0 |
| | TP-010038 | T3-010045 | | A128 | | R99 | F | Correction to default HPLMN RAT | |
| | At TSG-T #11, it was agreed that all existing release 99 specifications should be reissued as release 4 specifications so as to create a complete set of release 4 specifications. Further more, it was agreed to change the specification number of all GSM-only specifications from AA.BB to (AA+40).0BB. Thus GSM 11.11 changed to 3GPP TS 51.011. At the same time, the version numbering scheme was harmonised with 3G specifications so that all release 4 specifications have a version number 4.x.y. The contents of TS 51.011 v4.0.0 are identical to GSM 11.11 v8.5.0 | | | | | | | | 4.0.0 |
| TP-12 | TP-010109 | T3-010373 | 4.0.0 | 002 | | Rel-4 | F | Introduction of selected USIM features in to the SIM | 4.1.0 |
| TP-13 | TP-010203 | T3-010583 | 4.1.0 | 003 | | Rel-4 | F | EF EXT1: Clarification of Length Indicator for Additional Data | 4.2.0 |
| TP-14 | TP-010244 | T3-010744 | 4.2.0 | 004 | | Rel-4 | F | Collection of corrections | 5.0.0 |
| | TP-010244 | T3-010747 | | 005 | | Rel-4 | F | Alignment of SPN feature between 2G and 3G | |
| | TP-010244 | T3-010773 | | 006 | | Rel-4 | D | Restructuring of TS 51.011 to be based on TS 102 221 | |
| | TP-010244 | T3-010795 | | 007 | | Rel-5 | F | CHV mapping and handling between USIM- and SIM- | |
| | TP-010244 | T3-010797 | | 008 | | Rel-4 | F | Correction to EF(OPL ) | |