

ETSI TS 151 011 V4.15.0 (2005-06)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Specification of the Subscriber Identity Module -
Mobile Equipment (SIM-ME) interface
(3GPP TS 51.011 version 4.15.0 Release 4)**



Reference

RTS/TSGC-0651011v4f0

Keywords

GSM

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2005.
All rights reserved.

DECT™, PLUGTESTS™ and UMTS™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the TIPHON logo are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Intellectual Property Rights

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

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

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Contents

Intellectual Property Rights	2
Foreword.....	2
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.....	15
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	16
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.....	23
9.2.2 STATUS	25
9.2.3 READ BINARY	25
9.2.4 UPDATE BINARY	25
9.2.5 READ RECORD	26
9.2.6 UPDATE RECORD	26
9.2.7 SEEK	26
9.2.8 INCREASE.....	27
9.2.9 VERIFY CHV	27
9.2.10 CHANGE CHV	27
9.2.11 DISABLE CHV	28
9.2.12 ENABLE CHV	28
9.2.13 UNBLOCK CHV.....	28
9.2.14 INVALIDATE.....	28
9.2.15 REHABILITATE	29
9.2.16 RUN GSM ALGORITHM	29
9.2.17 SLEEP	29

9.2.18	GET RESPONSE.....	29
9.2.19	TERMINAL PROFILE.....	29
9.2.20	ENVELOPE.....	30
9.2.21	FETCH.....	30
9.2.22	TERMINAL RESPONSE.....	30
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	32
9.4.2	Responses to commands which are postponed	32
9.4.3	Memory management	32
9.4.4	Referencing management	32
9.4.5	Security management.....	32
9.4.6	Application independent errors.....	33
9.4.7	Commands versus possible status responses	33
10	Contents of the Elementary Files (EF)	34
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.....	35
10.3.1	EF _{LP} (Language preference)	35
10.3.2	EF _{IMSI} (IMSI).....	36
10.3.3	EF _{Kc} (Cipherring key Kc).....	37
10.3.4	EF _{PLMNsel} (PLMN selector)	37
10.3.5	EF _{HPPLMN} (Higher Priority PLMN search period)	38
10.3.6	EF _{ACMmax} (ACM maximum value)	38
10.3.7	EF _{SST} (SIM service table)	40
10.3.8	EF _{ACM} (Accumulated call meter).....	42
10.3.9	EF _{GID1} (Group Identifier Level 1).....	43
10.3.10	EF _{GID2} (Group Identifier Level 2).....	43
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)	46
10.3.15	EF _{ACC} (Access control class)	46
10.3.16	EF _{FPLMN} (Forbidden PLMNs).....	47
10.3.17	EF _{LOCI} (Location information)	47
10.3.18	EF _{AD} (Administrative data).....	49
10.3.19	EF _{Phase} (Phase identification)	50
10.3.20	EF _{VGCS} (Voice Group Call Service).....	51
10.3.21	EF _{VGCS} (Voice Group Call Service Status)	52
10.3.22	EF _{VBS} (Voice Broadcast Service).....	53
10.3.23	EF _{VBS} (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).....	58
10.3.28	EF _{CBMIR} (Cell broadcast message identifier range selection)	59
10.3.29	EF _{DCCK} De-personalization Control Keys	59
10.3.30	EF _{CNL} (Co-operative Network List).....	60
10.3.31	EF _{NIA} (Network's Indication of Alerting)	61
10.3.32	EF _{KcGPRS} (GPRS Cipherring key KcGPRS).....	62
10.3.33	EF _{LOCIGPRS} (GPRS location information).....	62
10.3.34	EF _{SUME} (SetUpMenu Elements)	63
10.3.35	EF _{PLMNwAcT} (User controlled PLMN Selector with Access Technology).....	64
10.3.36	EF _{OPLMNwAcT} (Operator controlled PLMN Selector with Access Technology)	66
10.3.37	EF _{HPLMNwAcT} (HPLMN Selector with Access Technology).....	66
10.3.38	EF _{CPBCCH} (CPBCCH Information)	67
10.3.39	EF _{InvScan} (Investigation Scan)	68
10.3.40	Void	69
10.3.41	EF _{PNN} (PLMN Network Name)	69

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).....	71
10.3.45	EF _{MWIS} (Message Waiting Indication Status)	72
10.3.46	EF _{CFIS} (Call Forwarding Indication Status).....	73
10.3.47	EF _{EXT5} (Extension5).....	74
10.3.48	EF _{EXT6} (Extension6).....	74
10.3.49	EF _{EXT7} (Extension7).....	74
10.3.50	EF _{SPDI} (Service Provider Display Information)	74
10.3.51	EF _{MMSN} (MMS Notification)	75
10.3.52	EF _{EXT8} (Extension 8)	77
10.3.53	EF _{MMSICP} (MMS Issuer Connectivity Parameters)	77
10.3.54	EF _{MMSUP} (MMS User Preferences)	79
10.3.55	EF _{MMSUCP} (MMS User Connectivity Parameters)	80
10.4	Contents of DFs at the GSM application level	81
10.4.1	Contents of files at the GSM SoLSA level	81
10.4.1.1	EF _{SAI} (SoLSA Access Indicator).....	81
10.4.1.2	EF _{SLL} (SoLSA LSA List)	82
10.4.1.3	LSA Descriptor files	84
10.4.2	Contents of files at the MExE level	85
10.4.2.1	EF _{MExE-ST} (MExE Service table).....	85
10.4.2.2	EF _{ORPK} (Operator Root Public Key).....	86
10.4.2.3	EF _{ARPK} (Administrator Root Public Key).....	88
10.4.2.4	EF _{TPRPK} (Third Party Root Public key)	88
10.4.2.5	Trusted Key/Certificates Data Files	89
10.5	Contents of files at the telecom level.....	89
10.5.1	EF _{ADN} (Abbreviated dialling numbers).....	89
10.5.2	EF _{FDN} (Fixed dialling numbers).....	93
10.5.3	EF _{SMS} (Short messages)	93
10.5.4	Capability configuration parameters	94
10.5.4.1	EF _{CCP} (Capability configuration parameters).....	94
10.5.4.2	EF _{ECCP} (Extended Capability Configuration Parameters).....	95
10.5.5	EF _{MSISDN} (MSISDN)	95
10.5.6	EF _{SMSP} (Short message service parameters).....	96
10.5.7	EF _{SMSS} (SMS status)	97
10.5.8	EF _{LND} (Last number dialled).....	98
10.5.9	EF _{SDN} (Service Dialling Numbers)	99
10.5.10	EF _{EXT1} (Extension1)	99
10.5.11	EF _{EXT2} (Extension2)	101
10.5.12	EF _{EXT3} (Extension3)	101
10.5.13	EF _{BDN} (Barred Dialling Numbers)	101
10.5.14	EF _{EXT4} (Extension4)	102
10.5.15	EF _{SMSR} (Short message status reports).....	102
10.5.16	EF _{CMI} (Comparison Method Information).....	103
10.6	DFs at the telecom level	104
10.6.1	Contents of files at the telecom graphics level.....	104
10.6.1.1	EF _{IMG} (Image).....	104
10.6.1.2	Image Instance Data Files	106
10.7	Files of GSM	106
11	Application protocol.....	108
11.1	General procedures.....	110
11.2	SIM management procedures	110
11.2.1	SIM initialization	110
11.2.2	GSM session termination.....	112
11.2.3	Emergency Call Codes.....	113
11.2.4	Language preference.....	113
11.2.5	Administrative information request;	113
11.2.6	SIM service table request.....	113
11.2.7	SIM phase request.....	113
11.2.8	SIM Presence Detection and Proactive Polling	113
11.2.9	Preferred Language.....	113

11.3	CHV related procedures	113
11.3.1	CHV verification	114
11.3.2	CHV value substitution.....	114
11.3.3	CHV disabling	114
11.3.4	CHV enabling	114
11.3.5	CHV unblocking.....	115
11.4	GSM security related procedures	115
11.4.1	GSM algorithms computation.....	115
11.4.2	IMSI request	115
11.4.3	Access control request	115
11.4.4	Higher Priority PLMN search period request	115
11.4.5	Location information	115
11.4.6	Cipher key.....	115
11.4.7	BCCH information.....	115
11.4.8	Forbidden PLMN.....	116
11.4.9	LSA information.....	116
11.4.10	GPRS Location information	116
11.4.11	GPRS Cipher key.....	116
11.5	Subscription related procedures	116
11.5.1	Dialling numbers	116
11.5.2	Short messages.....	119
11.5.3	Advice of Charge (AoC).....	119
11.5.4	Capability configuration parameters	120
11.5.5	PLMN selector.....	120
11.5.6	Cell broadcast message identifier	120
11.5.7	Group identifier level 1	120
11.5.8	Group identifier level 2.....	120
11.5.9	Service Provider Name	120
11.5.10	Voice Group Call Services	120
11.5.11	Voice Broadcast Services	121
11.5.12	Enhanced Multi Level Pre-emption and Priority Service	121
11.5.13	Cell Broadcast Message range identifier	121
11.5.14	Depersonalisation Control Keys	121
11.5.15	Short message status report.....	121
11.5.16	Network's indication of alerting.....	122
11.5.17	User controlled PLMN Selector with Access Technology	122
11.5.18	Operator controlled PLMN Selector with Access Technology.....	122
11.5.19	HPLMN Selector with Access Technology.....	122
11.5.20	CPBCCCH information.....	122
11.5.21	Investigation Scan.....	122
11.5.22	Void	122
11.5.23	PLMN Network Name.....	122
11.5.24	Operator PLMN List.....	123
11.5.25	Message Waiting Indication	123
11.5.26	Call Forwarding Indication Status	123
11.5.27	Service Provider Display Information	123
11.5.28	MMS Notifications	123
11.5.29	MMS Issuer Connectivity Parameters	124
11.5.30	MMS User Preferences.....	124
11.5.31	MMS User Connectivity Parameters	124
11.6	SIM Application Toolkit related procedures	124
11.6.1	Initialization procedure	124
11.6.2	Proactive polling.....	124
11.6.3	Support of commands	124
11.6.4	Support of response codes	125
11.6.5	Command-response pairs.....	125
11.6.6	Independence of normal GSM and SIM Application Toolkit tasks	125
11.6.7	Use of BUSY status response	125
11.6.8	Use of NULL procedure byte	125
11.6.9	Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands.....	125
11.6.10	Using the FETCH command.....	126
11.6.11	Data Download via SMS-CB.....	126

11.6.12	Data Download via SMS-PP.....	126
11.6.13	Menu selection.....	126
11.6.14	Call Control.....	126
11.6.15	Proactive SIM.....	126
11.6.16	Mobile Originated Short Message control by SIM.....	126
11.6.17	SIM data download error.....	126
11.6.18	Image Request.....	127
11.7	MExE related procedures.....	127
11.7.1	MExE ST.....	127
11.7.2	Operator root public key.....	127
11.7.3	Administrator root public key.....	127
11.7.4	Third Party root public key(s).....	127
Annex A (normative):	Void.....	128
Annex B (normative):	Void.....	129
Annex C (informative):	FDN/BDN Procedures.....	130
Annex D (informative):	Suggested contents of the EFs at pre-personalization.....	135
Annex E (informative):	SIM application Toolkit protocol diagrams.....	138
Annex F (informative):	Examples of coding of LSA Descriptor files for SoLSA.....	145
Annex G (normative):	Image Coding Schemes.....	146
G.1	Basic Image Coding Scheme.....	146
G.2	Colour Image Coding Scheme.....	147
Annex H (normative):	Coding of EFs for NAM and GSM-AMPS Operational Parameters.....	149
H.1	Elementary File Definitions and Contents.....	149
H.1.1	EF _{MIN} (Mobile Identification Number).....	149
H.1.2	EF _{ACCOLC} (Access Overload Class).....	149
H.1.3	EF _{SID} (System ID Of Home System).....	150
H.1.4	EF _{IPC} (Initial Paging Channel).....	150
H.1.5	EF _{GPI} (Group ID).....	151
H.1.6	EF _{S-ESN} (SIM Electronic Serial Number).....	151
H.1.7	EF _{COUNT} (Call Count).....	152
H.1.8	EF _{PSID} (Positive/Favoured SID list).....	152
H.1.9	EF _{NSID} (Negative/Forbidden SID List).....	153
H.1.10	EF _{SPL} (Scanning Priority List).....	154
H.1.11	EF _{NETSEL} (Network Selection Activation Flag).....	155
H.1.12	EF _{CSID} (Current/Last Registered SID).....	156
H.1.13	EF _{REG-THRESH} (Registration Threshold).....	156
H.1.14	EF _{CCCH} (Current Control Channel).....	157
H.1.15	EF _{LDCC} (Latest DCC).....	157
H.1.16	EF _{GSM-RECON} (GSM Reconnect Timer).....	157
H.1.17	EF _{AMPS-2-GSM} (AMPS to GSM Rescan Timing Table).....	158
H.1.18	EF _{*FCI} (Feature Activation Codes).....	158
H.1.19	EF _{AMPS-UI} (AMPS USAGE INDICATORS).....	159
H.2	Authentication Functionality.....	160
H.2.1	A-KEY (ANSI-41 Authentication Key).....	160
H.2.2	SSD (Shared Secret Data).....	160
H.3	Authentication commands.....	160
H.3.1	Generation of Authentication Signature Data and Cipherring Keys.....	161
H.3.2	Validation and Storage of Entered A-Key's.....	162
H.3.3	Ask Random Task.....	162
H.3.4	Update Shared Secret Data.....	163
H.3.5	Confirm Shared Secret Data.....	163

H.3.6	CMEA Encryption of Voice Channel Data Digits	163
H.3.7	SIM Status Codes	164
Annex I (informative):	EF changes via Data Download or SIM Toolkit applications	165
Annex J (informative):	Tags defined in the present document	168
Annex K (informative):	Example of MMS coding	169
K.1	Coding example for MMS User Preferences	169
K.2	Coding Example for MMS Issuer/User Connectivity Parameters	169
Annex L (informative):	Change History	171
History		172

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 3GPP TS 42.017 [6]. The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols are all defined in accordance with the 3GPP TS 31.101 [55] except when stated otherwise in the present document.

The present document defines:

- 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.

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] Void.
- [4] 3GPP TS 42.009: "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)".