

ETSI TS 131 102 V10.15.0 (2018-01)



**Universal Mobile Telecommunications System (UMTS);
LTE;
Characteristics of the Universal Subscriber
Identity Module (USIM) application
(3GPP TS 31.102 version 10.15.0 Release 10)**

<https://standards.iteh.ai/catalog/standards/sist/186083d-2c6f-4d51-9d13-de64cb74cd56/etsi-ts-131-102-v10-15-0-2018-01>



ReferenceRTS/TSGC-0631102vaf0

KeywordsLTE,UMTS

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

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

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

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Intellectual Property Rights

Essential patents

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 (<https://ipr.etsi.org/>).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	10
Introduction	10
1 Scope	11
2 References	11
3 Definitions, symbols, abbreviations and coding conventions	14
3.1 Definitions	14
3.2 Symbols.....	14
3.3 Abbreviations	14
3.4 Coding Conventions.....	16
4 Contents of the Files.....	16
4.1 Contents of the Efs at the MF level.....	16
4.2 Contents of files at the USIM ADF (Application DF) level.....	17
4.2.1 EF _{LI} (Language Indication).....	17
4.2.2 EF _{IMSI} (IMSI)	18
4.2.3 EF _{Keys} (Ciphering and Integrity Keys)	19
4.2.4 EF _{KeysPS} (Ciphering and Integrity Keys for Packet Switched domain)	19
4.2.5 EF _{PLMNwAcT} (User controlled PLMN selector with Access Technology)	20
4.2.6 EF _{HPPLMN} (Higher Priority PLMN search period)	21
4.2.7 EF _{ACMmax} (ACM maximum value).....	22
4.2.8 EF _{UST} (USIM Service Table)	23
4.2.9 EF _{ACM} (Accumulated Call Meter).....	26
4.2.10 EF _{GID1} (Group Identifier Level 1)	26
4.2.11 EF _{GID2} (Group Identifier Level 2)	27
4.2.12 EF _{SPN} (Service Provider Name)	27
4.2.13 EF _{PUCT} (Price per Unit and Currency Table).....	28
4.2.14 EF _{CBMI} (Cell Broadcast Message identifier selection)	29
4.2.15 EF _{ACC} (Access Control Class).....	30
4.2.16 EF _{FPLMN} (Forbidden PLMNs).....	30
4.2.17 EF _{LOCI} (Location Information).....	31
4.2.18 EF _{AD} (Administrative Data).....	32
4.2.19 Void	34
4.2.20 EF _{CBMID} (Cell Broadcast Message Identifier for Data Download).....	34
4.2.21 EF _{ECC} (Emergency Call Codes)	34
4.2.22 EF _{CBMIR} (Cell Broadcast Message Identifier Range selection)	35
4.2.23 EF _{PSLOCI} (Packet Switched location information)	36
4.2.24 EF _{FDN} (Fixed Dialling Numbers)	37
4.2.25 EF _{SMS} (Short messages)	38
4.2.26 EF _{MSISDN} (MSISDN)	39
4.2.27 EF _{SMSP} (Short message service parameters).....	40
4.2.28 EF _{SMSS} (SMS status)	41
4.2.29 EF _{SDN} (Service Dialling Numbers).....	42
4.2.30 EF _{EXT2} (Extension2).....	43
4.2.31 EF _{EXT3} (Extension3).....	43
4.2.32 EF _{SMSR} (Short message status reports).....	43
4.2.33 EF _{ICI} (Incoming Call Information).....	44
4.2.34 EF _{OCI} (Outgoing Call Information).....	47
4.2.35 EF _{ICT} (Incoming Call Timer)	48
4.2.36 EF _{OCT} (Outgoing Call Timer)	49
4.2.37 EF _{EXT5} (Extension5).....	49
4.2.38 EF _{CCP2} (Capability Configuration Parameters 2)	50

4.2.39	EF _{eMLPP} (enhanced Multi Level Precedence and Pre-emption).....	50
4.2.40	EF _{AaeM} (Automatic Answer for eMLPP Service).....	51
4.2.41	Void	52
4.2.42	EF _{Hiddenkey} (Key for hidden phone book entries)	52
4.2.43	Void	53
4.2.44	EF _{BDN} (Barred Dialling Numbers)	53
4.2.45	EF _{EXT4} (Extension4).....	53
4.2.46	EF _{CMi} (Comparison Method Information)	54
4.2.47	EF _{EST} (Enabled Services Table).....	54
4.2.48	EF _{ACL} (Access Point Name Control List)	55
4.2.49	EF _{DCK} (Depersonalisation Control Keys)	55
4.2.50	EF _{CNL} (Co-operative Network List).....	56
4.2.51	EF _{START-HFN} (Initialisation values for Hyperframe number).....	57
4.2.52	EF _{THRESHOLD} (Maximum value of START).....	58
4.2.53	EF _{OPLMNwACT} (Operator controlled PLMN selector with Access Technology)	58
4.2.54	EF _{HPLMNwACT} (HPLMN selector with Access Technology)	59
4.2.55	EF _{ARR} (Access Rule Reference).....	59
4.2.56	Void	60
4.2.57	EF _{NETPAR} (Network Parameters)	60
4.2.58	EF _{PNN} (PLMN Network Name)	62
4.2.59	EF _{OPL} (Operator PLMN List).....	63
4.2.60	EF _{MBDN} (Mailbox Dialling Numbers)	64
4.2.61	EF _{EXT6} (Extension6).....	65
4.2.62	EF _{MBI} (Mailbox Identifier).....	65
4.2.63	EF _{MWIS} (Message Waiting Indication Status)	66
4.2.64	EF _{CFIS} (Call Forwarding Indication Status).....	67
4.2.65	EF _{EXT7} (Extension7).....	69
4.2.66	EF _{SPDI} (Service Provider Display Information).....	69
4.2.67	EF _{MMSN} (MMS Notification)	70
4.2.68	EF _{EXT8} (Extension 8)	71
4.2.69	EF _{MMSICP} (MMS Issuer Connectivity Parameters)	72
4.2.70	EF _{MMSUP} (MMS User Preferences).....	74
4.2.71	EF _{MMSUCP} (MMS User Connectivity Parameters).....	75
4.2.72	EF _{NIA} (Network's Indication of Alerting)	75
4.2.73	EF _{VGCS} (Voice Group Call Service).....	76
4.2.74	EF _{VGCSS} (Voice Group Call Service Status)	78
4.2.75	EF _{VBS} (Voice Broadcast Service).....	78
4.2.76	EF _{VBSS} (Voice Broadcast Service Status).....	80
4.2.77	EF _{VGCSCA} (Voice Group Call Service Cipherring Algorithm)	81
4.2.78	EF _{VBSCA} (Voice Broadcast Service Cipherring Algorithm).....	82
4.2.79	EF _{GBABP} (GBA Bootstrapping parameters)	82
4.2.80	EF _{MSK} (MBMS Service Keys List)	83
4.2.81	EF _{MUK} (MBMS User Key).....	84
4.2.82	Void	85
4.2.83	EF _{GBANL} (GBA NAF List).....	85
4.2.84	EF _{EHPLMN} (Equivalent HPLMN)	86
4.2.85	EF _{EHPLMNPI} (Equivalent HPLMN Presentation Indication)	86
4.2.86	EF _{LRPLMNSI} (Last RPLMN Selection Indication).....	87
4.2.87	EF _{NAFKCA} (NAF Key Centre Address)	87
4.2.88	EF _{SPNI} (Service Provider Name Icon)	88
4.2.89	EF _{PNNI} (PLMN Network Name Icon)	89
4.2.90	EF _{NCP-IP} (Network Connectivity Parameters for USIM IP connections).....	89
4.2.91	EF _{EPSLOCI} (EPS location information)	92
4.2.92	EF _{EPSNSC} (EPS NAS Security Context).....	94
4.2.93	EF _{UFC} (USAT Facility Control).....	95
4.2.94	EF _{NASCONFIG} (Non Access Stratum Configuration)	96
4.2.95	EF _{UICCIARI} (UICC IARI).....	98
4.3	DFs at the USIM ADF (Application DF) Level	98
4.4	Contents of DFs at the USIM ADF (Application DF) level	99
4.4.1	Contents of files at the DF SoLSA level.....	99
4.4.1.1	EF _{SAI} (SoLSA Access Indicator).....	99

4.4.1.2	EF _{SLL} (SoLSA LSA List)	99
4.4.1.3	LSA Descriptor files	102
4.4.2	Contents of files at the DF PHONEBOOK level	103
4.4.2.1	EF _{PBR} (Phone Book Reference file)	103
4.4.2.2	EF _{IAP} (Index Administration Phone book)	105
4.4.2.3	EF _{ADN} (Abbreviated dialling numbers)	106
4.4.2.4	EF _{EXT1} (Extension1)	109
4.4.2.5	EF _{PBC} (Phone Book Control)	110
4.4.2.6	EF _{GRP} (Grouping file)	111
4.4.2.7	EF _{AAS} (Additional number Alpha String)	112
4.4.2.8	EF _{GAS} (Grouping information Alpha String)	113
4.4.2.9	EF _{ANR} (Additional Number)	113
4.4.2.10	EF _{SNE} (Second Name Entry)	115
4.4.2.11	EF _{CCP1} (Capability Configuration Parameters 1)	115
4.4.2.12	Phone Book Synchronisation	116
4.4.2.12.1	EF _{UID} (Unique Identifier)	116
4.4.2.12.2	EF _{PSC} (Phone book Synchronisation Counter)	117
4.4.2.12.3	EF _{CC} (Change Counter)	118
4.4.2.12.4	EF _{PUID} (Previous Unique Identifier)	118
4.4.2.13	EF _{EMAIL} (e-mail address)	119
4.4.2.14	Phonebook restrictions	120
4.4.3	Contents of files at the DF GSM-ACCESS level (Files required for GSM Access)	120
4.4.3.1	EF _{Kc} (GSM Ciphering key Kc)	120
4.4.3.2	EF _{KcGPRS} (GPRS Ciphering key KcGPRS)	121
4.4.3.3	Void	121
4.4.3.4	EF _{CPBCCCH} (CPBCCCH Information)	121
4.4.3.5	EF _{InvScan} (Investigation Scan)	122
4.4.4	Contents of files at the MexE level	123
4.4.4.1	EF _{MexE-ST} (MexE Service table)	123
4.4.4.2	EF _{ORPK} (Operator Root Public Key)	124
4.4.4.3	EF _{ARPK} (Administrator Root Public Key)	125
4.4.4.4	EF _{TPRPK} (Third Party Root Public Key)	126
4.4.4.5	EF _{TKCDF} (Trusted Key/Certificates Data Files)	127
4.4.5	Contents of files at the DF WLAN level	127
4.4.5.1	EF _{Pseudo} (Pseudonym)	127
4.4.5.2	EF _{UPLMNWLAN} (User controlled PLMN selector for I-WLAN Access)	128
4.4.5.3	EF _{OPLMNWLAN} (Operator controlled PLMN selector for I-WLAN Access)	128
4.4.5.4	EF _{UWSIDL} (User controlled WLAN Specific Identifier List)	129
4.4.5.5	EF _{OWSIDL} (Operator controlled WLAN Specific IdentifierList)	130
4.4.5.6	EF _{WRI} (WLAN Reauthentication Identity)	130
4.4.5.7	EF _{HWSIDL} (Home I-WLAN Specific Identifier List)	131
4.4.5.8	EF _{WEHPLMNPI} (I-WLAN Equivalent HPLMN Presentation Indication)	132
4.4.5.9	EF _{WHPI} (I-WLAN HPLMN Priority Indication)	132
4.4.5.10	EF _{WLRPLMN} (I-WLAN Last Registered PLMN)	133
4.4.5.11	EF _{HPLMNDAI} (HPLMN Direct Access Indicator)	133
4.4.6	Contents of files at the DF HNB level	134
4.4.6.1	Introduction	134
4.4.6.2	EF _{ACSGL} (Allowed CSG Lists)	134
4.4.6.3	EF _{CSGT} (CSG Type)	137
4.4.6.4	EF _{HNBName} (Home NodeB Name)	139
4.4.6.5	EF _{OCSGL} (Operator CSG Lists)	139
4.4.6.6	EF _{OCSGT} (Operator CSG Type)	141
4.4.6.7	EF _{OHNBN} (Operator Home NodeB Name)	142
4.4.7	Void	142
4.5	Contents of Efs at the TELECOM level	142
4.5.1	EF _{ADN} (Abbreviated dialling numbers)	142
4.5.2	EF _{EXT1} (Extension1)	142
4.5.3	EF _{ECCP} (Extended Capability Configuration Parameter)	142
4.5.4	EF _{SUME} (SetUpMenu Elements)	142
4.5.5	EF _{ARR} (Access Rule Reference)	143
4.5.6	EF _{ICE_DN} (In Case of Emergency – Dialling Number)	143
4.5.7	EF _{ICE_FF} (In Case of Emergency – Free Format)	143

4.5.8	EF _{RM} A (Remote Management Actions).....	144
4.5.9	EF _{PSISMSC} (Public Service Identity of the SM-SC).....	145
4.6	Contents of DFs at the TELECOM level.....	145
4.6.1	Contents of files at the DF _{GRAPHICS} level.....	145
4.6.1.1	EF _{IMG} (Image).....	145
4.6.1.2	EF _{IIDF} (Image Instance Data Files).....	147
4.6.1.3	EF _{ICE_graphics} (In Case of Emergency – Graphics).....	147
4.6.1.4	EF _{LAUNCH SCWS}	148
4.6.1.5	EF _{ICON}	151
4.6.2	Contents of files at the DF _{PHONEBOOK} under the DF _{TELECOM}	152
4.6.3	Contents of files at the DF _{MULTIMEDIA} level.....	152
4.6.3.1	EF _{MML} (Multimedia Messages List).....	152
4.6.3.2	EF _{M MDF} (Multimedia Messages Data File).....	155
4.7	Files of USIM.....	156
5	Application protocol.....	160
5.1	USIM management procedures.....	160
5.1.1	Initialisation.....	160
5.1.1.1	USIM application selection.....	160
5.1.1.2	USIM initialisation.....	160
5.1.1.3	GSM related initialisation procedures.....	161
5.1.2	Session termination.....	162
5.1.2.1	3G session termination.....	162
5.1.2.1.1	GSM termination procedures.....	162
5.1.2.2	3G session reset.....	162
5.1.3	USIM application closure.....	162
5.1.4	Emergency call codes.....	162
5.1.5	Language indication.....	163
5.1.6	Administrative information request.....	163
5.1.7	USIM service table request.....	163
5.1.8	Void.....	163
5.1.9	UICC presence detection.....	163
5.2	USIM security related procedures.....	163
5.2.1	Authentication algorithms computation.....	163
5.2.2	IMSI request.....	163
5.2.3	Access control information request.....	163
5.2.4	Higher Priority PLMN search period request.....	163
5.2.5	Location information.....	163
5.2.6	Cipher and Integrity key.....	163
5.2.7	Forbidden PLMN.....	164
5.2.8	Void.....	164
5.2.9	User Identity Request.....	164
5.2.10	GSM Cipher key.....	164
5.2.11	GPRS Cipher key.....	164
5.2.12	Initialisation value for Hyperframe number.....	164
5.2.13	Maximum value of START.....	164
5.2.14	HPLMN selector with Access Technology request.....	164
5.2.15	Packet Switched Location information.....	164
5.2.16	Cipher and Integrity key for Packet Switched domain.....	164
5.2.17	LSA information.....	165
5.2.18	Voice Group Call Services.....	165
5.2.19	Voice Broadcast Services.....	165
5.2.20	Generic Bootstrapping architecture (Bootstrap).....	165
5.2.21	Generic Bootstrapping architecture (NAF Derivation).....	165
5.2.22	MSK MIKEY Message Reception.....	165
5.2.23	MTK MIKEY Message Reception.....	165
5.2.24	Void.....	166
5.2.25	EHPLMN request.....	166
5.2.26	Last RPLMN Selection Indication request.....	166
5.2.29	Non Access Stratum Configuration.....	166
5.3	Subscription related procedures.....	166
5.3.1	Phone book procedures.....	166

5.3.1.1	Initialisation	166
5.3.1.2	Creation/Deletion of information	166
5.3.1.3	Hidden phone book entries.....	167
5.3.2	Dialling numbers	167
5.3.3	Short messages.....	169
5.3.4	Advice of charge.....	169
5.3.5	Capability configuration parameters	169
5.3.6	User controlled PLMN selector with Access Technology	170
5.3.7	Cell broadcast message identifier	170
5.3.8	Group identifier level 1	170
5.3.9	Group identifier level 2.....	170
5.3.10	Service provider name	170
5.3.11	Enhanced multi level precedence and pre-emption service	170
5.3.12	Cell broadcast message identifier ranges	170
5.3.13	Short message status report.....	170
5.3.14	APN Control List.....	171
5.3.15	Depersonalisation Control Keys	171
5.3.16	Co-operative Network List	171
5.3.17	CPBCCCH information.....	171
5.3.18	Investigation Scan.....	172
5.3.19	Enabled Services Table Request.....	172
5.3.20	Operator controlled PLMN selector with Access Technology	172
5.3.21	HPLMN selector with Access Technology.....	172
5.3.22	Automatic Answer on eMLPP service.....	172
5.3.23	Network Parameter information	172
5.3.24	PLMN network name.....	172
5.3.25	Operator PLMN List.....	172
5.3.26	Message Waiting Indication	172
5.3.27	Call Forwarding Indication Status	173
5.3.28	Service Provider Display Information	173
5.3.29	MMS Notifications	173
5.3.30	MMS Issuer Connectivity Parameters	173
5.3.31	MMS User Preferences	174
5.3.32	MMS User Connectivity Parameters	174
5.3.33	Network's indication of alerting.....	174
5.3.34	Multimedia Messages Storage	174
5.3.35	Equivalent HPLMN Presentation Indication request.....	174
5.3.36	NAF Key Centre Address request.....	174
5.3.37	Service provider name Icon.....	175
5.3.38	PLMN network name Icon	175
5.3.39	ICE Information request	175
5.3.40	eCall Related Procedures	175
5.3.40.1	eCall Only support	175
5.3.40.2	eCall and Normal call support.....	175
5.3.40.3	Change of eCall mode.....	176
5.3.41	SM-over-IP	176
5.3.42	UICC access to IMS	176
5.4	USAT related procedures	176
5.4.1	Data Download via SMS-PP.....	176
5.4.2	Image Request	176
5.4.3	Data Download via SMS-CB.....	176
5.4.4	Call Control by USIM.....	177
5.4.5	MO-SMS control by USIM	177
5.4.6	Data Download via USSD and USSD application mode.....	177
5.4.7	Additional TERMINAL PROFILE after UICC activation	177
5.4.8	Terminal Applications	177
5.4.9	Call control on EPS PDN connection by USIM	177
5.4.10	Communication Control for IMS by USIM.....	177
5.4.11	USAT Facility Control.....	177
5.4.12	Extended Terminal Applications	177
5.5	MexE related procedures.....	178
5.5.1	MexE ST.....	178

5.5.2	Operator root public key	178
5.5.3	Administrator root public key	178
5.5.4	Third Party root public key(s)	178
5.5.5	Trusted Key/Certificates Data Files	178
5.6	WLAN related procedures	178
5.6.1	WLAN Selection related Procedures	178
5.6.2	WLAN PLMN Selection related procedures	179
5.6.3	WLAN access authentication related procedures	179
5.6.4	WLAN access re-authentication related procedures	179
5.7	Network Connectivity Parameters for UICC IP connections related procedures	179
5.8	H(e)NB related procedures	179
5.8.1	CSG Access Control procedures	179
5.8.2	CSG Type related procedures	180
5.8.3	HNB name display related procedures	180
6	Security features	180
6.1	Authentication and key agreement procedure	181
6.2	Cryptographic Functions	181
6.3	GSM Conversion Functions	181
6.4	User verification and file access conditions	182
7	USIM Commands	182
7.1	AUTHENTICATE	182
7.1.1	Command description	182
7.1.1.1	3G security context	183
7.1.1.2	GSM security context	183
7.1.1.3	VGCS/VBS security context	184
7.1.1.4	GBA security context (Bootstrapping Mode)	184
7.1.1.5	GBA security context (NAF Derivation Mode)	185
7.1.1.6	MBMS security context (MSK Update Mode)	185
7.1.1.7	Void	187
7.1.1.8	MBMS security context (MTK Generation Mode)	187
7.1.1.9	MBMS security context (MSK Deletion Mode)	188
7.1.1.10	MBMS security context (MUK Deletion Mode)	188
7.1.1.11	Local Key Establishment security context (Key Derivation mode)	188
7.1.1.12	Local Key Establishment security context (Key Availability Check mode)	189
7.1.2	Command parameters and data	189
7.1.2.1	GSM/3G security context	191
7.1.2.2	VGCS/VBS security context	192
7.1.2.3	GBA security context (Bootstrapping Mode)	192
7.1.2.4	GBA security context (NAF Derivation Mode)	193
7.1.2.5	MBMS security context (All Modes)	193
7.1.2.6	Local Key Establishment security context (All Modes)	194
7.1.2.6.1	Local Key Establishment security context (Key Derivation mode)	194
7.1.2.6.2	Local Key Establishment security context (Key Availability Check mode)	196
7.2	Void	197
7.3	Status Conditions Returned by the USIM	197
7.3.1	Security management	197
7.3.2	Status Words of the Commands	198
7.4	Optional commands	199
8	Void	199
Annex A (informative):	EF changes via Data Download or USAT applications	200
Annex B (normative):	Image Coding Schemes	204
B.1	Basic Image Coding Scheme	204
B.2	Colour Image Coding Scheme	205
B.3	Colour Image Coding Scheme with Transparency	206
Annex C (informative):	Structure of the Network parameters TLV objects	207

Annex D (informative):	Tags defined in 31.102	208
Annex E (informative):	Suggested contents of the EFs at pre-personalization	211
Annex F (informative):	Examples of coding of LSA Descriptor files for SoLSA	215
Annex G (informative):	Phonebook Example	216
Annex H (normative):	List of SFI Values.....	220
H.1	List of SFI Values at the USIM ADF Level.....	220
H.2	List of SFI Values at the DF GSM-ACCESS Level.....	220
H.3	List of SFI Values at the DF WLAN Level.....	221
H.4	List of SFI Values at the DF HNB Level	221
Annex I (informative):	USIM Application Session Activation/Termination	222
Annex J (informative):	Example of MMS coding.....	223
J.1	Coding example for MMS User Preferences.....	223
J.2	Coding Example for MMS Issuer/User Connectivity Parameters.....	223
Annex K (informative):	Examples of VService_Id coding.....	225
Annex L : USIM-INI and USIM-RN for Relay Nodes (normative).....		226
L.1	Introduction	226
L.2	Application selection procedure	226
L.3	Secure channel operation.....	227
L.4	Support of commands.....	227
L.5	Storage of certificates.....	227
L.6	Relay Node files support	227
L.6.1	USIM-INI Files.....	227
L.6.1.1	EF _{CERT} (UICC Certificate)	227
L.6.2	USIM-RN Files.....	228
L.6.2.1	eF _{RNid} (Relay Node identifier).....	228
L.6.2.2	EF _{SCCmax} (maximum value of Secure Channel Counter)	229
Annex M (informative):	Change history	230
History		234

Foreword

This Technical Specification (TS) 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.

Introduction

The present document defines the Universal Subscriber Identity Module (USIM) application. This application resides on the UICC, an IC card specified in TS 31.101 [11]. In particular, TS 31.101 [11] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

TS 31.101 [11] is one of the core documents for this specification and is therefore referenced in many places in the present document.

1 Scope

The present document defines the USIM application for 3G telecom network operation.

The present document specifies:

- specific command parameters;
- file structures;
- contents of Efs (Elementary Files);
- security functions;
- application protocol to be used on the interface between UICC (USIM) and ME.

This is to ensure interoperability between a USIM and an ME independently of the respective manufacturer, card issuer or operator.

The present document does not define any aspects related to the administrative management phase of the USIM. Any internal technical realisation of either the USIM or the ME is only specified where these are reflected over the interface. The present document does not specify any of the security algorithms which may be used.

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] 3GPP TS 21.111: "USIM and IC Card Requirements".
- [2] 3GPP TS 22.011: "Service accessibility".
- [3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".
- [4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".
- [5] 3GPP TS 23.038: "Alphabets and language".
- [6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".
- [7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".
- [9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".
- [10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".
- [11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".
- [12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".
- [13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

- [14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".
- [15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".
- [16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".
- [17] 3GPP TS 02.07: "Mobile Stations (MS) features".
- [18] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".
- [19] ISO 639 (1988): "Code for the representation of names of languages".
- [20] ISO/IEC 7816-4: "Integrated circuit cards, Part 4: Organization, security and commands for interchange".
- [21] Void.
- [22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".
- [23] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".
- [24] 3GPP TS 22.101: "Service aspects; service principles".
- [25] 3GPP TS 23.003: "Numbering, Addressing and Identification".
- [26] Void.
- [27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".
- [28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol".
- [29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".
- [30] 3GPP TS 23.057: "Mobile Execution Environment (MexE);Functional description; Stage 2".
- [31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode".
- [32] Void.
- [33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".
- [34] 3GPP TS 45.005: "Radio Transmission and Reception".
- [35] ISO/IEC 8825-1 (2008): "Information technology – ASN.1 encoding rules : Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".
- [36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)".
- [37] Void.
- [38] 3GPP TS 23.140 Release 6: "Multimedia Messaging Service (MMS); Functional description; stage 2".
- [39] ETSI TS 102 222 V7.1.0: "Administrative commands for telecommunications applications".
- [40] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols;Stage 3".
- [41] 3GPP TS 33.234: "3G Security; Wireless Local Area Network (WLAN) interworking security".
- [42] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".
- [43] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service".