



**Universal Mobile Telecommunications System (UMTS);
LTE;
Characteristics of the Universal Subscriber
Identity Module (USIM) application
(3GPP TS 31.102 version 14.8.0 Release 14)**

PDF SCANNED FROM
<https://standards.iteh.ai/catalog/standards/sist/1b39011-9150-4d0b-8211-1001fd426051/sist/1b39011-9150-4d0b-8211-1001fd426051-201906>



Reference

RTS/TSGC-0631102ve80

Keywords

LTE,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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 2019.
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 a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

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 normative deliverables 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.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	12
Introduction	12
1 Scope	13
2 References	13
3 Definitions, symbols, abbreviations and coding conventions	17
3.1 Definitions	17
3.2 Symbols.....	17
3.3 Abbreviations	18
3.4 Coding Conventions.....	20
4 Contents of the Files.....	20
4.1 Contents of the EFs at the MF level	20
4.2 Contents of files at the USIM ADF (Application DF) level.....	20
4.2.1 EF _{LI} (Language Indication).....	21
4.2.2 EF _{IMSI} (IMSI)	21
4.2.3 EF _{Keys} (Ciphering and Integrity Keys)	22
4.2.4 EF _{KeysPS} (Ciphering and Integrity Keys for Packet Switched domain)	23
4.2.5 EF _{PLMNwAcT} (User controlled PLMN selector with Access Technology)	23
4.2.6 EF _{HPPLMN} (Higher Priority PLMN search period).....	25
4.2.7 EF _{ACMmax} (ACM maximum value).....	26
4.2.8 EF _{UST} (USIM Service Table).....	27
4.2.9 EF _{ACM} (Accumulated Call Meter).....	30
4.2.10 EF _{GID1} (Group Identifier Level 1).....	31
4.2.11 EF _{GID2} (Group Identifier Level 2).....	31
4.2.12 EF _{SPN} (Service Provider Name).....	31
4.2.13 EF _{PUCT} (Price per Unit and Currency Table).....	32
4.2.14 EF _{CBMI} (Cell Broadcast Message identifier selection)	33
4.2.15 EF _{ACC} (Access Control Class).....	34
4.2.16 EF _{FPLMN} (Forbidden PLMNs).....	34
4.2.17 EF _{LOCI} (Location Information).....	35
4.2.18 EF _{AD} (Administrative Data).....	36
4.2.19 Void	38
4.2.20 EF _{CBMID} (Cell Broadcast Message Identifier for Data Download).....	38
4.2.21 EF _{ECC} (Emergency Call Codes)	39
4.2.22 EF _{CBMIR} (Cell Broadcast Message Identifier Range selection)	40
4.2.23 EF _{PSLOCI} (Packet Switched location information)	40
4.2.24 EF _{FDN} (Fixed Dialling Numbers)	42
4.2.25 EF _{SMS} (Short messages)	42
4.2.26 EF _{MSISDN} (MSISDN)	44
4.2.27 EF _{SMSMSP} (Short message service parameters).....	44
4.2.28 EF _{SMSMSS} (SMS status)	46
4.2.29 EF _{SDN} (Service Dialling Numbers).....	46
4.2.30 EF _{EXT2} (Extension2).....	47
4.2.31 EF _{EXT3} (Extension3).....	47
4.2.32 EF _{SMSR} (Short message status reports).....	48
4.2.33 EF _{ICI} (Incoming Call Information).....	48
4.2.34 EF _{OCI} (Outgoing Call Information).....	52
4.2.35 EF _{ICT} (Incoming Call Timer)	53
4.2.36 EF _{OCT} (Outgoing Call Timer)	53
4.2.37 EF _{EXT5} (Extension5).....	54
4.2.38 EF _{CCP2} (Capability Configuration Parameters 2)	54

4.2.39	EF _{eMLPP} (enhanced Multi Level Precedence and Pre-emption).....	55
4.2.40	EF _{AaeM} (Automatic Answer for eMLPP Service).....	56
4.2.41	Void	57
4.2.42	EF _{Hiddenkey} (Key for hidden phone book entries)	57
4.2.43	Void	57
4.2.44	EF _{BDN} (Barred Dialling Numbers)	57
4.2.45	EF _{EXT4} (Extension4).....	58
4.2.46	EF _{CFMI} (Comparison Method Information)	58
4.2.47	EF _{EST} (Enabled Services Table).....	59
4.2.48	EF _{ACL} (Access Point Name Control List)	59
4.2.49	EF _{DCK} (Depersonalisation Control Keys)	60
4.2.50	EF _{CNL} (Co-operative Network List).....	60
4.2.51	EF _{START-HFN} (Initialisation values for Hyperframe number).....	62
4.2.52	EF _{THRESHOLD} (Maximum value of START).....	62
4.2.53	EF _{OPLMNwACT} (Operator controlled PLMN selector with Access Technology)	62
4.2.54	EF _{HPLMNwACT} (HPLMN selector with Access Technology)	63
4.2.55	EF _{ARR} (Access Rule Reference).....	64
4.2.56	Void	65
4.2.57	EF _{NETPAR} (Network Parameters)	65
4.2.58	EF _{PNN} (PLMN Network Name)	67
4.2.59	EF _{OPL} (Operator PLMN List).....	68
4.2.60	EF _{MBDN} (Mailbox Dialling Numbers)	69
4.2.61	EF _{EXT6} (Extension6).....	69
4.2.62	EF _{MBI} (Mailbox Identifier).....	70
4.2.63	EF _{MWIS} (Message Waiting Indication Status)	70
4.2.64	EF _{CFIS} (Call Forwarding Indication Status).....	72
4.2.65	EF _{EXT7} (Extension7).....	73
4.2.66	EF _{SPDI} (Service Provider Display Information).....	74
4.2.67	EF _{MMSN} (MMS Notification)	74
4.2.68	EF _{EXT8} (Extension 8)	76
4.2.69	EF _{MMSICP} (MMS Issuer Connectivity Parameters).....	77
4.2.70	EF _{MMSUP} (MMS User Preferences).....	79
4.2.71	EF _{MMSUCP} (MMS User Connectivity Parameters).....	80
4.2.72	EF _{NIA} (Network's Indication of Alerting).....	80
4.2.73	EF _{VGCS} (Voice Group Call Service).....	81
4.2.74	EF _{VGCS} (Voice Group Call Service Status).....	83
4.2.75	EF _{VBS} (Voice Broadcast Service).....	83
4.2.76	EF _{VBS} (Voice Broadcast Service Status).....	85
4.2.77	EF _{VGCSA} (Voice Group Call Service Ciphering Algorithm).....	86
4.2.78	EF _{VBSA} (Voice Broadcast Service Ciphering Algorithm).....	87
4.2.79	EF _{GBABP} (GBA Bootstrapping parameters).....	87
4.2.80	EF _{MSK} (MBMS Service Keys List)	88
4.2.81	EF _{MUK} (MBMS User Key).....	89
4.2.82	Void	90
4.2.83	EF _{GBANL} (GBA NAF List).....	90
4.2.84	EF _{EHPLMN} (Equivalent HPLMN)	91
4.2.85	EF _{EHPLMNP} (Equivalent HPLMN Presentation Indication)	91
4.2.86	EF _{LRPLMNSI} (Last RPLMN Selection Indication).....	92
4.2.87	EF _{NAFKCA} (NAF Key Centre Address)	92
4.2.88	EF _{SPNI} (Service Provider Name Icon)	93
4.2.89	EF _{PNNI} (PLMN Network Name Icon)	94
4.2.90	EF _{NCP-IP} (Network Connectivity Parameters for USIM IP connections).....	94
4.2.91	EF _{EPSLOCI} (EPS location information)	97
4.2.92	EF _{EPSNSC} (EPS NAS Security Context).....	99
4.2.93	EF _{UFC} (USAT Facility Control).....	100
4.2.94	EF _{NASCONFIG} (Non Access Stratum Configuration)	101
4.2.95	EF _{UICCIARI} (UICC IARI).....	105
4.2.96	EF _{PWS} (Public Warning System).....	106
4.2.97	EF _{FDNURI} (Fixed Dialling Numbers URI).....	106
4.2.98	EF _{BDNURI} (Barred Dialling Numbers URI).....	107
4.2.99	EF _{SDNURI} (Service Dialling Numbers URI).....	108

4.2.100	EF _{IWL} (IMEI(SV) White Lists)	109
4.2.101	EF _{IPS} (IMEI(SV) Pairing Status).....	110
4.2.102	EF _{IPD} (IMEI(SV) of Pairing Device)	111
4.2.103	EF _{ePDGId} (Home ePDG Identifier).....	112
4.2.104	EF _{ePDGSelection} (ePDG Selection Information).....	113
4.2.104a	EF _{ePDGIdEm} (Emergency ePDG Identifier)	115
4.2.105	EF _{ePDGSelectionEm} (ePDG Selection Information for Emergency Services).....	115
4.2.106	EF _{FromPreferred} (From Preferred)	115
4.2.107	EF _{IMSCfgData} (IMS Configuration Data)	116
4.2.108	EF _{TVCONFIG} (TV Configuration)	116
4.2.109	EF _{3GPPPSDATAOFF} (3GPP PS Data Off)	118
4.2.110	EF _{3GPPPSDATAOFFservicelist} (3GPP PS Data Off Service List).....	118
4.2.111	EF _{XCAPConfigData} (XCAP Configuration Data).....	119
4.3	DFs at the USIM ADF (Application DF) Level	119
4.4	Contents of DFs at the USIM ADF (Application DF) level	120
4.4.1	Contents of files at the DF SoLSA level.....	120
4.4.1.1	EF _{SAI} (SoLSA Access Indicator).....	120
4.4.1.2	EF _{SLL} (SoLSA LSA List).....	121
4.4.1.3	LSA Descriptor files	123
4.4.2	Contents of files at the DF PHONEBOOK level.....	124
4.4.2.1	EF _{PBR} (Phone Book Reference file)	125
4.4.2.2	EF _{IAP} (Index Administration Phone book).....	127
4.4.2.3	EF _{ADN} (Abbreviated dialling numbers)	127
4.4.2.4	EF _{EXT1} (Extension1)	130
4.4.2.5	EF _{PBC} (Phone Book Control).....	132
4.4.2.6	EF _{GRP} (Grouping file).....	133
4.4.2.7	EF _{AAS} (Additional number Alpha String).....	133
4.4.2.8	EF _{GAS} (Grouping information Alpha String).....	134
4.4.2.9	EF _{ANR} (Additional Number).....	134
4.4.2.10	EF _{SNE} (Second Name Entry).....	136
4.4.2.11	EF _{CCP1} (Capability Configuration Parameters 1).....	137
4.4.2.12	Phone Book Synchronisation	137
4.4.2.12.1	EF _{UID} (Unique Identifier).....	137
4.4.2.12.2	EF _{PSC} (Phone book Synchronisation Counter).....	138
4.4.2.12.3	EF _{CC} (Change Counter)	139
4.4.2.12.4	EF _{PUID} (Previous Unique Identifier)	140
4.4.2.13	EF _{EMAIL} (e-mail address)	140
4.4.2.14	Phonebook restrictions	141
4.4.2.15	EF _{PURI} (Phonebook URIs).....	141
4.4.3	Contents of files at the DF GSM-ACCESS level (Files required for GSM Access).....	142
4.4.3.1	EF _{Kc} (GSM Cipherring key Kc)	143
4.4.3.2	EF _{KcGPRS} (GPRS Cipherring key KcGPRS).....	143
4.4.3.3	Void.....	144
4.4.3.4	EF _{CPBCCCH} (CPBCCCH Information)	144
4.4.3.5	EF _{InvScan} (Investigation Scan)	145
4.4.4	Contents of files at the MexE level	145
4.4.4.1	EF _{MexE-ST} (MexE Service table)	146
4.4.4.2	EF _{ORPK} (Operator Root Public Key)	146
4.4.4.3	EF _{ARPK} (Administrator Root Public Key)	148
4.4.4.4	EF _{TPRPK} (Third Party Root Public Key).....	149
4.4.4.5	EF _{TKCDF} (Trusted Key/Certificates Data Files).....	149
4.4.5	Contents of files at the DF WLAN level.....	150
4.4.5.1	EF _{Pseudo} (Pseudonym)	150
4.4.5.2	EF _{UPLMNWLAN} (User controlled PLMN selector for I-WLAN Access)	151
4.4.5.3	EF _{OPLMNWLAN} (Operator controlled PLMN selector for I-WLAN Access)	151
4.4.5.4	EF _{UWSIDL} (User controlled WLAN Specific Identifier List).....	152
4.4.5.5	EF _{OWSIDL} (Operator controlled WLAN Specific IdentifierList)	153
4.4.5.6	EF _{WRI} (WLAN Reauthentication Identity)	153
4.4.5.7	EF _{HWSIDL} (Home I-WLAN Specific Identifier List)	154
4.4.5.8	EF _{WEHPLMNPI} (I-WLAN Equivalent HPLMN Presentation Indication).....	155
4.4.5.9	EF _{WHPI} (I-WLAN HPLMN Priority Indication)	155
4.4.5.10	EF _{WLRPLMN} (I-WLAN Last Registered PLMN).....	156

4.4.5.11	EF _{HPLMNDAI} (HPLMN Direct Access Indicator)	156
4.4.6	Contents of files at the DF HNB level	157
4.4.6.1	Introduction	157
4.4.6.2	EF _{ACSGL} (Allowed CSG Lists)	157
4.4.6.3	EF _{CSGT} (CSG Type)	160
4.4.6.4	EF _{HNB} (Home NodeB Name)	162
4.4.6.5	EF _{OCSGL} (Operator CSG Lists)	162
4.4.6.6	EF _{OCSGT} (Operator CSG Type)	164
4.4.6.7	EF _{OHNB} (Operator Home NodeB Name)	165
4.4.7	Void	165
4.4.8	Contents of files at the DF ProSe level	165
4.4.8.1	Introduction	165
4.4.8.2	EF _{PROSE_MON} (ProSe Monitoring Parameters)	165
4.4.8.3	EF _{PROSE_ANN} (ProSe Announcing Parameters)	166
4.4.8.4	EF _{PROSEFUNC} (HPLMN ProSe Function)	167
4.4.8.5	EF _{PROSE_RADIO_COM} (ProSe Direct Communication Radio Parameters)	168
4.4.8.6	EF _{PROSE_RADIO_MON} (ProSe Direct Discovery Monitoring Radio Parameters)	170
4.4.8.7	EF _{PROSE_RADIO_ANN} (ProSe Direct Discovery Announcing Radio Parameters)	171
4.4.8.8	EF _{PROSE_POLICY} (ProSe Policy Parameters)	172
4.4.8.9	EF _{PROSE_PLMN} (ProSe PLMN Parameters)	174
4.4.8.10	EF _{PROSE_GC} (ProSe Group Counter)	175
4.4.8.11	EF _{PST} (ProSe Service Table)	177
4.4.8.12	EF _{PROSE_UIRC} (ProSe UsageInformationReportingConfiguration)	177
4.4.8.12	EF _{PROSE_GM_DISCOVERY} (ProSe Group Member Discovery Parameters)	181
4.4.8.13	EF _{PROSE_RELAY} (ProSe Relay Parameters)	182
4.4.8.14	EF _{PROSE_RELAY_DISCOVERY} (ProSe Relay Discovery Parameters)	183
4.4.9	Contents of files at the DF ACDC level	186
4.4.9.1	Introduction	186
4.4.9.2	EF _{ACDC_LIST} (ACDC List)	186
4.4.9.3	EF _{ACDC_OS_CONFIG} (ACDC OS configuration)	187
4.4.10	Contents of files at the DF TV level	188
4.4.10.1	Introduction	188
4.4.10.2	EF _{TVUSD} (TV User Service Description)	188
4.5	Contents of Efs at the TELECOM level	189
4.5.1	EF _{ADN} (Abbreviated dialling numbers)	189
4.5.2	EF _{EXT1} (Extension1)	189
4.5.3	EF _{ECCP} (Extended Capability Configuration Parameter)	189
4.5.4	EF _{SUME} (SetUpMenu Elements)	190
4.5.5	EF _{ARR} (Access Rule Reference)	190
4.5.6	EF _{ICE_DN} (In Case of Emergency – Dialling Number)	190
4.5.7	EF _{ICE_FF} (In Case of Emergency – Free Format)	191
4.5.8	EF _{RMA} (Remote Management Actions)	191
4.5.9	EF _{PSISMSC} (Public Service Identity of the SM-SC)	192
4.6	Contents of DFs at the TELECOM level	192
4.6.0	List of DFs at the TELECOM level	192
4.6.1	Contents of files at the DF _{GRAPHICS} level	192
4.6.1.1	EF _{IMG} (Image)	192
4.6.1.2	EF _{IIDF} (Image Instance Data Files)	194
4.6.1.3	EF _{ICE_graphics} (In Case of Emergency – Graphics)	194
4.6.1.4	Void	195
4.6.1.5	Void	195
4.6.2	Contents of files at the DF _{PHONEBOOK} under the DF _{TELECOM}	195
4.6.3	Contents of files at the DF _{MULTIMEDIA} level	195
4.6.3.1	EF _{MML} (Multimedia Messages List)	195
4.6.3.2	EF _{MMDf} (Multimedia Messages Data File)	198
4.6.4	Contents of files at the DF _{MCPTT} level	199
4.6.4.1	EF _{MST} (MCPTT Service Table)	199
4.6.4.2	EF _{MCPTT_CONFIG} (MCPTT configuration data)	199
4.6.4.3	Void	200
4.6.4.4	Void	200
4.6.4.5	Void	200

4.6.5	Contents of files at the DF _{V2X} level	200
4.6.5.1	V2X configuration data related files	200
4.6.5.2	EF _{VST} (V2X Service Table).....	201
4.6.5.3	EF _{V2X_CONFIG} (V2X configuration data).....	201
4.7	Files of USIM.....	203
5	Application protocol.....	208
5.1	USIM management procedures	209
5.1.1	Initialisation	209
5.1.1.1	USIM application selection.....	209
5.1.1.2	USIM initialisation.....	209
5.1.1.3	GSM related initialisation procedures	210
5.1.2	Session termination.....	210
5.1.2.1	3G session termination.....	210
5.1.2.1.1	GSM termination procedures.....	211
5.1.2.2	3G session reset.....	211
5.1.3	USIM application closure	211
5.1.4	Emergency call codes	211
5.1.5	Language indication.....	211
5.1.6	Administrative information request	211
5.1.7	USIM service table request.....	211
5.1.8	Void.....	212
5.1.9	UICC presence detection	212
5.1.10	UICC interface in PSM.....	212
5.1.11	UICC interface during eDRX	212
5.2	USIM security related procedures	213
5.2.1	Authentication algorithms computation.....	213
5.2.2	IMSI request	213
5.2.3	Access control information request	213
5.2.4	Higher Priority PLMN search period request	213
5.2.5	Location information	213
5.2.6	Cipher and Integrity key	213
5.2.7	Forbidden PLMN.....	213
5.2.8	Void.....	213
5.2.9	User Identity Request.....	213
5.2.10	GSM Cipher key	214
5.2.11	GPRS Cipher key.....	214
5.2.12	Initialisation value for Hyperframe number.....	214
5.2.13	Maximum value of START.....	214
5.2.14	HPLMN selector with Access Technology request	214
5.2.15	Packet Switched Location information.....	214
5.2.16	Cipher and Integrity key for Packet Switched domain	214
5.2.17	LSA information.....	214
5.2.18	Voice Group Call Services	214
5.2.19	Voice Broadcast Services	215
5.2.20	Generic Bootstrapping architecture (Bootstrap)	215
5.2.21	Generic Bootstrapping architecture (NAF Derivation)	215
5.2.22	MSK MIKEY Message Reception.....	215
5.2.23	MTK MIKEY Message Reception	215
5.2.24	Void	215
5.2.25	EHPLMN request	215
5.2.26	Last RPLMN Selection Indication request	215
5.2.29	Non Access Stratum Configuration	216
5.2.30	PWS Configuration.....	216
5.3	Subscription related procedures	216
5.3.1	Phone book procedures	216
5.3.1.1	Initialisation	216
5.3.1.2	Creation/Deletion of information	216
5.3.1.3	Hidden phone book entries.....	216
5.3.2	Dialling numbers	217
5.3.3	Short messages.....	218
5.3.4	Advice of charge.....	219

5.3.5	Capability configuration parameters	219
5.3.6	User controlled PLMN selector with Access Technology	219
5.3.7	Cell broadcast message identifier	220
5.3.8	Group identifier level 1	220
5.3.9	Group identifier level 2	220
5.3.10	Service provider name	220
5.3.11	Enhanced multi level precedence and pre-emption service	220
5.3.12	Cell broadcast message identifier ranges	220
5.3.13	Short message status report	220
5.3.14	APN Control List	221
5.3.15	Depersonalisation Control Keys	221
5.3.16	Co-operative Network List	221
5.3.17	CPBCCCH information	221
5.3.18	Investigation Scan	221
5.3.19	Enabled Services Table Request	222
5.3.20	Operator controlled PLMN selector with Access Technology	222
5.3.21	HPLMN selector with Access Technology	222
5.3.22	Automatic Answer on eMLPP service	222
5.3.23	Network Parameter information	222
5.3.24	PLMN network name	222
5.3.25	Operator PLMN List	222
5.3.26	Message Waiting Indication	222
5.3.27	Call Forwarding Indication Status	222
5.3.28	Service Provider Display Information	223
5.3.29	MMS Notifications	223
5.3.30	MMS Issuer Connectivity Parameters	223
5.3.31	MMS User Preferences	223
5.3.32	MMS User Connectivity Parameters	224
5.3.33	Network's indication of alerting	224
5.3.34	Multimedia Messages Storage	224
5.3.35	Equivalent HPLMN Presentation Indication request	224
5.3.36	NAF Key Centre Address request	224
5.3.37	Service provider name Icon	224
5.3.38	PLMN network name Icon	225
5.3.39	ICE Information request	225
5.3.40	eCall Related Procedures	225
5.3.40.1	eCall Only support	225
5.3.40.2	eCall and Normal call support	226
5.3.40.3	Change of eCall mode	226
5.3.41	SM-over-IP	226
5.3.42	UICC access to IMS	226
5.3.43	TV Configuration	227
5.3.44	3GPP PS Data Off related procedures	227
5.3.45	3GPP PS Data Off service list related procedures	227
5.4	USAT related procedures	227
5.4.1	Data Download via SMS-PP	227
5.4.2	Image Request	227
5.4.3	Data Download via SMS-CB	227
5.4.4	Call Control by USIM	227
5.4.5	MO-SMS control by USIM	227
5.4.6	Data Download via USSD and USSD application mode	228
5.4.7	Additional TERMINAL PROFILE after UICC activation	228
5.4.8	Terminal Applications	228
5.4.9	Call control on EPS PDN connection by USIM	228
5.4.10	Communication Control for IMS by USIM	228
5.4.11	USAT Facility Control	228
5.4.12	Extended Terminal Applications	228
5.4.13	USAT application pairing procedure	228
5.5	MexE related procedures	229
5.5.1	MexE ST	229
5.5.2	Operator root public key	229
5.5.3	Administrator root public key	229

5.5.4	Third Party root public key(s).....	229
5.5.5	Trusted Key/Certificates Data Files.....	229
5.6	WLAN related procedures.....	230
5.6.1	WLAN Selection related Procedures.....	230
5.6.2	WLAN PLMN Selection related procedures.....	230
5.6.3	WLAN access authentication related procedures.....	230
5.6.4	WLAN access re-authentication related procedures.....	230
5.7	Network Connectivity Parameters for UICC IP connections related procedures.....	230
5.8	H(e)NB related procedures.....	231
5.8.1	CSG Access Control procedures.....	231
5.8.2	CSG Type related procedures.....	231
5.8.3	HNB name display related procedures.....	231
5.9	ProSe related procedures.....	232
5.9.1	ProSe Direct Discovery Provisioning parameters.....	232
5.9.2	HPLMN ProSe Function address.....	232
5.9.3	ProSe direct communication related Procedures.....	232
5.9.4	ProSe direct discovery related Procedures.....	232
5.9.5	ProSe direct communication related Procedures.....	232
5.9.6	ProSe direct communication related Procedures.....	232
5.9.7	ProSe Group Counter related Procedures.....	233
5.9.8	ProSe Usage Information Reporting Configuration related Procedures.....	233
5.9.9	ProSe Group Member Discovery related Procedures.....	233
5.9.10	ProSe Relay related Procedures.....	233
5.10	ePDG Selection related procedures.....	233
5.10.1	Home ePDG Identifier.....	233
5.10.2	ePDG Selection Information.....	233
5.10.3	ePDG configuration information configured but empty.....	234
5.11	ACDC related procedures.....	234
5.11.1	ACDC Configuration.....	234
5.12	MCPTT related procedures.....	234
5.12.1	MCPTT configuration.....	234
5.12.2	Void.....	234
5.12.3	Void.....	234
5.12.4	Void.....	234
5.13	ePDG Selection for Emergency Services related procedures.....	234
5.13.1	Emergency ePDG Identifier.....	234
5.13.2	ePDG Selection Information for Emergency Services.....	235
5.13.3	ePDG configuration information for Emergency Services configured but empty.....	235
5.13.4	From Preferred related procedures.....	235
5.13.5	IMS Configuration Data related procedures.....	235
5.13.6	XCAP Configuration Data related procedures.....	235
5.14	V2X related procedures.....	235
5.14.1	V2X configuration.....	235
6	Security features.....	235
6.1	Authentication and key agreement procedure.....	236
6.2	Cryptographic Functions.....	236
6.3	GSM Conversion Functions.....	236
6.4	User verification and file access conditions.....	237
7	USIM Commands.....	237
7.1	AUTHENTICATE.....	237
7.1.1	Command description.....	237
7.1.1.1	3G security context.....	238
7.1.1.2	GSM security context.....	238
7.1.1.3	VGCS/VBS security context.....	239
7.1.1.4	GBA security context (Bootstrapping Mode).....	239
7.1.1.5	GBA security context (NAF Derivation Mode).....	240
7.1.1.6	MBMS security context (MSK Update Mode).....	240
7.1.1.7	Void.....	242
7.1.1.8	MBMS security context (MTK Generation Mode).....	242
7.1.1.9	MBMS security context (MSK Deletion Mode).....	243

7.1.1.10	MBMS security context (MUK Deletion Mode).....	243
7.1.1.11	Local Key Establishment security context (Key Derivation mode)	243
7.1.1.12	Local Key Establishment security context (Key Availability Check mode)	244
7.1.2	Command parameters and data.....	244
7.1.2.1	GSM/3G security context.....	246
7.1.2.2	VGCS/VBS security context.....	247
7.1.2.3	GBA security context (Bootstrapping Mode)	247
7.1.2.4	GBA security context (NAF Derivation Mode)	248
7.1.2.5	MBMS security context (All Modes).....	248
7.1.2.6	Local Key Establishment security context (All Modes).....	249
7.1.2.6.1	Local Key Establishment security context (Key Derivation mode).....	249
7.1.2.6.2	Local Key Establishment security context (Key Availability Check mode)	251
7.2	Void.....	252
7.3	Status Conditions Returned by the USIM	252
7.3.1	Security management.....	252
7.3.2	Status Words of the Commands.....	253
7.4	Optional commands.....	254
8	Void.....	254
Annex A (informative): EF changes via Data Download or USAT applications		255
Annex B (normative): Image Coding Schemes.....		260
B.1	Basic Image Coding Scheme.....	260
B.2	Colour Image Coding Scheme	261
B.3	Colour Image Coding Scheme with Transparency.....	262
Annex C (informative): Structure of the Network parameters TLV objects.....		263
Annex D (informative): Tags defined in 31.102.....		264
Annex E (informative): Suggested contents of the EFs at pre-personalization		270
Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA		275
Annex G (informative): Phonebook Example		276
Annex H (normative): List of SFI Values.....		280
H.1	List of SFI Values at the USIM ADF Level.....	280
H.2	List of SFI Values at the DF GSM-ACCESS Level.....	280
H.3	List of SFI Values at the DF WLAN Level.....	281
H.4	List of SFI Values at the DF HNB Level	281
H.5	List of SFI Values at the DF ProSe Level	281
H.6	List of SFI Values at the DF ACDC Level.....	281
H.7	List of SFI Values at the DF MCPTT Level	282
H.8	List of SFI Values at the DF V2X Level.....	282
Annex I (informative): USIM Application Session Activation/Termination		283
Annex J (informative): Example of MMS coding.....		284
J.1	Coding example for MMS User Preferences.....	284
J.2	Coding Example for MMS Issuer/User Connectivity Parameters.....	284
Annex K (informative): Examples of VService_Id coding.....		286
Annex L (normative): USIM-INI and USIM-RN for Relay Nodes		287
L.1	Introduction	287

L.2	Application selection procedure	287
L.3	Secure channel operation.....	288
L.4	Support of commands.....	288
L.5	Storage of certificates.....	288
L.6	Relay Node files support	288
L.6.1	USIM-INI Files.....	288
L.6.1.1	EF _{CERT} (UICC Certificate)	288
L.6.2	USIM-RN Files.....	289
L.6.2.1	eF _{RNid} (Relay Node identifier).....	289
L.6.2.2	EF _{SCCmax} (maximum value of Secure Channel Counter).....	290
Annex M (normative): USIM application dedicated for IOPS		291
M.1	Introduction	291
M.2	Features of the USIM dedicated for IOPS.....	291
M.3	Selection mechanisms.....	291
Annex N (informative): Change history		292
History		297

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/1b39d911-9150-4d0b-8211-1001fd42603b/etsi-ts-131-102-v14.8.0-2019-06>

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.