



**Universal Mobile Telecommunications System (UMTS);
LTE;
Characteristics of the Universal Subscriber
Identity Module (USIM) application
(3GPP TS 31.102 version 15.5.0 Release 15)**



Reference

RTS/TSGC-0631102vf50

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.

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.....	12
Introduction	12
1 Scope	13
2 References	13
3 Definitions, symbols, abbreviations and coding conventions	17
3.1 Definitions	17
3.2 Symbols.....	18
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.....	21
4.2.1 EF _{LI} (Language Indication).....	21
4.2.2 EF _{IMSI} (IMSI)	22
4.2.3 EF _{Keys} (Ciphering and Integrity Keys)	23
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)	24
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)	28
4.2.9 EF _{ACM} (Accumulated Call Meter).....	31
4.2.10 EF _{GID1} (Group Identifier Level 1)	32
4.2.11 EF _{GID2} (Group Identifier Level 2)	32
4.2.12 EF _{SPN} (Service Provider Name)	33
4.2.13 EF _{PUCT} (Price per Unit and Currency Table).....	34
4.2.14 EF _{CBMI} (Cell Broadcast Message identifier selection)	35
4.2.15 EF _{ACC} (Access Control Class).....	35
4.2.16 EF _{FPLMN} (Forbidden PLMNs).....	36
4.2.17 EF _{LOCI} (Location Information).....	36
4.2.18 EF _{AD} (Administrative Data).....	37
4.2.19 Void	39
4.2.20 EF _{CBMID} (Cell Broadcast Message Identifier for Data Download).....	39
4.2.21 EF _{ECC} (Emergency Call Codes)	40
4.2.22 EF _{CBMIR} (Cell Broadcast Message Identifier Range selection)	41
4.2.23 EF _{PSLOCI} (Packet Switched location information)	42
4.2.24 EF _{FDN} (Fixed Dialling Numbers)	43
4.2.25 EF _{SMS} (Short messages)	43
4.2.26 EF _{MSISDN} (MSISDN)	45
4.2.27 EF _{SMSP} (Short message service parameters).....	45
4.2.28 EF _{SMSS} (SMS status)	47
4.2.29 EF _{SDN} (Service Dialling Numbers).....	47
4.2.30 EF _{EXT2} (Extension2).....	48
4.2.31 EF _{EXT3} (Extension3).....	48
4.2.32 EF _{SMSR} (Short message status reports).....	49
4.2.33 EF _{ICI} (Incoming Call Information).....	49
4.2.34 EF _{OCI} (Outgoing Call Information).....	53
4.2.35 EF _{ICT} (Incoming Call Timer)	53
4.2.36 EF _{OCT} (Outgoing Call Timer)	54
4.2.37 EF _{EXT5} (Extension5).....	55
4.2.38 EF _{CCP2} (Capability Configuration Parameters 2)	55
4.2.39 EF _{eMLPP} (enhanced Multi Level Precedence and Pre-emption).....	56

4.2.40	EF _{AaeM} (Automatic Answer for eMLPP Service).....	57
4.2.41	Void	58
4.2.42	EF _{Hiddenkey} (Key for hidden phone book entries)	58
4.2.43	Void	58
4.2.44	EF _{BDN} (Barred Dialling Numbers)	58
4.2.45	EF _{EXT4} (Extension4).....	59
4.2.46	EF _{CMi} (Comparison Method Information)	59
4.2.47	EF _{EST} (Enabled Services Table).....	60
4.2.48	EF _{ACL} (Access Point Name Control List)	60
4.2.49	EF _{DCK} (Depersonalisation Control Keys)	61
4.2.50	EF _{CNL} (Co-operative Network List).....	61
4.2.51	EF _{START-HFN} (Initialisation values for Hyperframe number).....	63
4.2.52	EF _{THRESHOLD} (Maximum value of START).....	63
4.2.53	EF _{OPLMNwACT} (Operator controlled PLMN selector with Access Technology)	63
4.2.54	EF _{HPLMNwACT} (HPLMN selector with Access Technology)	64
4.2.55	EF _{ARR} (Access Rule Reference).....	65
4.2.56	Void	66
4.2.57	EF _{NETPAR} (Network Parameters)	66
4.2.58	EF _{PNN} (PLMN Network Name)	68
4.2.59	EF _{OPL} (Operator PLMN List).....	69
4.2.60	EF _{MBDN} (Mailbox Dialling Numbers)	70
4.2.61	EF _{EXT6} (Extension6).....	70
4.2.62	EF _{MBI} (Mailbox Identifier).....	71
4.2.63	EF _{MWIS} (Message Waiting Indication Status)	71
4.2.64	EF _{CFIS} (Call Forwarding Indication Status).....	73
4.2.65	EF _{EXT7} (Extension7).....	74
4.2.66	EF _{SPDI} (Service Provider Display Information)	75
4.2.67	EF _{MMSN} (MMS Notification)	75
4.2.68	EF _{EXT8} (Extension 8)	77
4.2.69	EF _{MMSICP} (MMS Issuer Connectivity Parameters).....	77
4.2.70	EF _{MMSUP} (MMS User Preferences)	80
4.2.71	EF _{MMSUCP} (MMS User Connectivity Parameters)	81
4.2.72	EF _{NIA} (Network's Indication of Alerting).....	81
4.2.73	EF _{VGCS} (Voice Group Call Service).....	82
4.2.74	EF _{VGCS} (Voice Group Call Service Status).....	84
4.2.75	EF _{VBS} (Voice Broadcast Service).....	84
4.2.76	EF _{VBSS} (Voice Broadcast Service Status).....	86
4.2.77	EF _{VGCS} (Voice Group Call Service Cipherring Algorithm).....	87
4.2.78	EF _{VB} (Voice Broadcast Service Cipherring Algorithm).....	88
4.2.79	EF _{GBABP} (GBA Bootstrapping parameters)	88
4.2.80	EF _{MSK} (MBMS Service Keys List)	89
4.2.81	EF _{MUK} (MBMS User Key).....	90
4.2.82	Void	91
4.2.83	EF _{GBANL} (GBA NAF List).....	91
4.2.84	EF _{EHPLMN} (Equivalent HPLMN)	92
4.2.85	EF _{EHPLMNPI} (Equivalent HPLMN Presentation Indication)	92
4.2.86	EF _{LRPLMNSI} (Last RPLMN Selection Indication).....	93
4.2.87	EF _{NAFKCA} (NAF Key Centre Address)	93
4.2.88	EF _{SPNI} (Service Provider Name Icon)	94
4.2.89	EF _{PNNI} (PLMN Network Name Icon)	95
4.2.90	EF _{NCP-IP} (Network Connectivity Parameters for USIM IP connections).....	95
4.2.91	EF _{EPSLOC} (EPS location information)	98
4.2.92	EF _{EPSNSC} (EPS NAS Security Context).....	100
4.2.93	EF _{UFC} (USAT Facility Control).....	101
4.2.94	EF _{NASCONFIG} (Non Access Stratum Configuration)	102
4.2.95	EF _{UICCIARI} (UICC IARI).....	106
4.2.96	EF _{PWS} (Public Warning System).....	107
4.2.97	EF _{FDNURI} (Fixed Dialling Numbers URI).....	107
4.2.98	EF _{BDNURI} (Barred Dialling Numbers URI).....	108
4.2.99	EF _{SDNURI} (Service Dialling Numbers URI).....	109
4.2.100	EF _{IWL} (IMEI(SV) White Lists)	110

4.2.101	EF _{IPS} (IMEI(SV) Pairing Status).....	111
4.2.102	EF _{IPD} (IMEI(SV) of Pairing Device)	112
4.2.103	EF _{ePDGId} (Home ePDG Identifier).....	113
4.2.104	EF _{ePDGSelection} (ePDG Selection Information).....	114
4.2.104a	EF _{ePDGIdEm} (Emergency ePDG Identifier)	116
4.2.105	EF _{ePDGSelectionEm} (ePDG Selection Information for Emergency Services).....	116
4.2.106	EF _{FromPreferred} (From Preferred)	116
4.2.107	EF _{IMSCConfigData} (IMS Configuration Data)	117
4.2.108	EF _{TVCONFIG} (TV Configuration)	117
4.2.109	EF _{3GPPPSDATAOFF} (3GPP PS Data Off)	119
4.2.110	EF _{3GPPPSDATAOFFservicelist} (3GPP PS Data Off Service List).....	120
4.2.111	EF _{XCAPConfigData} (XCAP Configuration Data).....	120
4.2.112	EF _{EARFCNlist} (EARFCN list for MTC/NB-IOT UEs).....	121
4.3	DFs at the USIM ADF (Application DF) Level	122
4.4	Contents of DFs at the USIM ADF (Application DF) level	122
4.4.1	Contents of files at the DF SoLSA level.....	122
4.4.1.1	EF _{SAI} (SoLSA Access Indicator).....	122
4.4.1.2	EF _{SLL} (SoLSA LSA List).....	123
4.4.1.3	LSA Descriptor files	125
4.4.2	Contents of files at the DF PHONEBOOK level.....	126
4.4.2.1	EF _{PBR} (Phone Book Reference file)	127
4.4.2.2	EF _{IAP} (Index Administration Phone book).....	129
4.4.2.3	EF _{ADN} (Abbreviated dialling numbers)	129
4.4.2.4	EF _{EXT1} (Extension1)	132
4.4.2.5	EF _{PBC} (Phone Book Control).....	134
4.4.2.6	EF _{GRP} (Grouping file).....	135
4.4.2.7	EF _{AAS} (Additional number Alpha String).....	135
4.4.2.8	EF _{GAS} (Grouping information Alpha String).....	136
4.4.2.9	EF _{ANR} (Additional Number).....	136
4.4.2.10	EF _{SNE} (Second Name Entry).....	138
4.4.2.11	EF _{CCP1} (Capability Configuration Parameters 1).....	139
4.4.2.12	Phone Book Synchronisation	139
4.4.2.12.1	EF _{UID} (Unique Identifier).....	139
4.4.2.12.2	EF _{PSC} (Phone book Synchronisation Counter).....	140
4.4.2.12.3	EF _{CC} (Change Counter)	141
4.4.2.12.4	EF _{PUID} (Previous Unique Identifier)	142
4.4.2.13	EF _{EMAIL} (e-mail address)	142
4.4.2.14	Phonebook restrictions	143
4.4.2.15	EF _{PURI} (Phonebook URIs).....	143
4.4.3	Contents of files at the DF GSM-ACCESS level (Files required for GSM Access).....	144
4.4.3.1	EF _{Kc} (GSM Ciphering key Kc)	144
4.4.3.2	EF _{KcGPRS} (GPRS Ciphering key KcGPRS).....	145
4.4.3.3	Void.....	145
4.4.3.4	EF _{CPBCCCH} (CPBCCCH Information)	145
4.4.3.5	EF _{InvScan} (Investigation Scan)	146
4.4.4	Contents of files at the MexE level	147
4.4.4.1	EF _{MexE-ST} (MexE Service table)	147
4.4.4.2	EF _{ORPK} (Operator Root Public Key)	147
4.4.4.3	EF _{ARPK} (Administrator Root Public Key).....	149
4.4.4.4	EF _{TPRPK} (Third Party Root Public Key).....	150
4.4.4.5	EF _{TKCDF} (Trusted Key/Certificates Data Files).....	151
4.4.5	Contents of files at the DF WLAN level.....	151
4.4.5.1	EF _{Pseudo} (Pseudonym)	151
4.4.5.2	EF _{UPLMNWLAN} (User controlled PLMN selector for I-WLAN Access)	152
4.4.5.3	EF _{OPLMNWLAN} (Operator controlled PLMN selector for I-WLAN Access)	152
4.4.5.4	EF _{UWSIDL} (User controlled WLAN Specific Identifier List).....	153
4.4.5.5	EF _{OWSIDL} (Operator controlled WLAN Specific IdentifierList)	154
4.4.5.6	EF _{WRI} (WLAN Reauthentication Identity)	154
4.4.5.7	EF _{HWSIDL} (Home I-WLAN Specific Identifier List)	155
4.4.5.8	EF _{WEHPLMNPI} (I-WLAN Equivalent HPLMN Presentation Indication).....	155
4.4.5.9	EF _{WHPI} (I-WLAN HPLMN Priority Indication)	156
4.4.5.10	EF _{WLRPLMN} (I-WLAN Last Registered PLMN).....	156

4.4.5.11	EF _{HPLMNDAI} (HPLMN Direct Access Indicator)	157
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
4.4.11	Contents of files at the DF _{5GS} level	189
4.4.11.1	Introduction	189
4.4.11.2	EF _{5GS3GPPLOCI} (5GS 3GPP location information)	189
4.4.11.3	EF _{5GSN3GPPLOCI} (5GS non-3GPP location information)	191
4.4.11.4	EF _{5GS3GPPNSC} (5GS 3GPP Access NAS Security Context)	191
4.4.11.5	EF _{5GSN3GPPNSC} (5GS non-3GPP Access NAS Security Context)	194
4.4.11.6	EF _{5GAUTHKEYS} (5G authentication keys)	194
4.4.11.7	EF _{UAC_AIC} (UAC Access Identities Configuration)	195
4.4.11.8	EF _{SUCI_Calc_Info} (Subscription Concealed Identifier Calculation Information EF)	196
4.4.11.9	EF _{OPL5G} (5GS Operator PLMN List)	197
4.4.11.10	EF _{NSI} (Network Specific Identifier)	198
4.4.11.	EF _{Routing_Indicator} (Routing Indicator EF)	199
4.5	Contents of Efs at the TELECOM level	199
4.5.1	EF _{ADN} (Abbreviated dialling numbers)	200
4.5.2	EF _{EXT1} (Extension1)	200
4.5.3	EF _{ECCP} (Extended Capability Configuration Parameter)	200
4.5.4	EF _{SUME} (SetUpMenu Elements)	200
4.5.5	EF _{ARR} (Access Rule Reference)	200
4.5.6	EF _{ICE_DN} (In Case of Emergency – Dialling Number)	200
4.5.7	EF _{ICE_FF} (In Case of Emergency – Free Format)	201
4.5.8	EF _{RMA} (Remote Management Actions)	202
4.5.9	EF _{PSISMSC} (Public Service Identity of the SM-SC)	202
4.6	Contents of DFs at the TELECOM level	202
4.6.0	List of DFs at the TELECOM level	202
4.6.1	Contents of files at the DF _{GRAPHICS} level	203
4.6.1.1	EF _{IMG} (Image)	203
4.6.1.2	EF _{IIDF} (Image Instance Data Files)	204
4.6.1.3	EF _{ICE_graphics} (In Case of Emergency – Graphics)	205

4.6.1.4	Void.....	205
4.6.1.5	Void.....	205
4.6.2	Contents of files at the DF _{PHONEBOOK} under the DF _{TELECOM}	205
4.6.3	Contents of files at the DF _{MULTIMEDIA} level.....	205
4.6.3.1	EF _{MML} (Multimedia Messages List).....	205
4.6.3.2	EF _{MMDf} (Multimedia Messages Data File).....	208
4.6.4	Contents of files at the DF _{MCS} level	209
4.6.4.1	EF _{MST} (MCS Service Table).....	209
4.6.4.2	EF _{MCS_CONFIG} (MCS configuration data).....	209
4.6.4.3	Void.....	210
4.6.4.4	Void.....	210
4.6.4.5	Void.....	210
4.6.5	Contents of files at the DF _{V2X} level	210
4.6.5.1	V2X configuration data related files	210
4.6.5.2	EF _{VST} (V2X Service Table).....	211
4.6.5.3	EF _{V2X_CONFIG} (V2X configuration data).....	211
4.7	Files of USIM.....	213
5	Application protocol.....	220
5.1	USIM management procedures	220
5.1.1	Initialisation	220
5.1.1.1	USIM application selection.....	220
5.1.1.2	USIM initialisation.....	220
5.1.1.3	GSM related initialisation procedures	221
5.1.2	Session termination.....	222
5.1.2.1	3G session termination.....	222
5.1.2.1.1	GSM termination procedures.....	222
5.1.2.2	3G session reset.....	222
5.1.3	USIM application closure	222
5.1.4	Emergency call codes	222
5.1.5	Language indication.....	222
5.1.6	Administrative information request	223
5.1.7	USIM service table request.....	223
5.1.8	Void.....	223
5.1.9	UICC presence detection	223
5.1.10	UICC interface in PSM.....	223
5.1.11	UICC interface during eDRX.....	223
5.1.12	UICC interface during MICO.....	224
5.2	USIM security related procedures	224
5.2.1	Authentication algorithms computation.....	224
5.2.2	IMSI request	224
5.2.3	Access control information request	225
5.2.4	Higher Priority PLMN search period request	225
5.2.5	Location information	225
5.2.6	Cipher and Integrity key	225
5.2.7	Forbidden PLMN.....	225
5.2.8	Void.....	225
5.2.9	User Identity Request.....	225
5.2.10	GSM Cipher key.....	225
5.2.11	GPRS Cipher key.....	225
5.2.12	Initialisation value for Hyperframe number.....	225
5.2.13	Maximum value of START	225
5.2.14	HPLMN selector with Access Technology request	225
5.2.15	Packet Switched Location information.....	226
5.2.16	Cipher and Integrity key for Packet Switched domain	226
5.2.17	LSA information.....	226
5.2.18	Voice Group Call Services	226
5.2.19	Voice Broadcast Services	226
5.2.20	Generic Bootstrapping architecture (Bootstrap)	226
5.2.21	Generic Bootstrapping architecture (NAF Derivation)	226
5.2.22	MSK MIKEY Message Reception.....	226
5.2.23	MTK MIKEY Message Reception	227

5.2.24	Void	227
5.2.25	EHPLMN request	227
5.2.26	Last RPLMN Selection Indication request	227
5.2.29	Non Access Stratum Configuration	227
5.2.30	PWS Configuration.....	227
5.2.33	NSI request	228
5.3	Subscription related procedures	228
5.3.1	Phone book procedures.....	228
5.3.1.1	Initialisation	228
5.3.1.2	Creation/Deletion of information	228
5.3.1.3	Hidden phone book entries.....	228
5.3.2	Dialling numbers	228
5.3.3	Short messages.....	230
5.3.4	Advice of charge.....	231
5.3.5	Capability configuration parameters.....	231
5.3.6	User controlled PLMN selector with Access Technology	231
5.3.7	Cell broadcast message identifier	231
5.3.8	Group identifier level 1	231
5.3.9	Group identifier level 2.....	231
5.3.10	Service provider name	232
5.3.11	Enhanced multi level precedence and pre-emption service	232
5.3.12	Cell broadcast message identifier ranges	232
5.3.13	Short message status report.....	232
5.3.14	APN Control List.....	232
5.3.15	Depersonalisation Control Keys	233
5.3.16	Co-operative Network List	233
5.3.17	CPBCCCH information.....	233
5.3.18	Investigation Scan.....	233
5.3.19	Enabled Services Table Request.....	233
5.3.20	Operator controlled PLMN selector with Access Technology	233
5.3.21	HPLMN selector with Access Technology.....	233
5.3.22	Automatic Answer on eMLPP service.....	234
5.3.23	Network Parameter information	234
5.3.24	PLMN network name.....	234
5.3.25	Operator PLMN List.....	234
5.3.26	Message Waiting Indication	234
5.3.27	Call Forwarding Indication Status	234
5.3.28	Service Provider Display Information	234
5.3.29	MMS Notifications	234
5.3.30	MMS Issuer Connectivity Parameters	235
5.3.31	MMS User Preferences	235
5.3.32	MMS User Connectivity Parameters	235
5.3.33	Network's indication of alerting.....	235
5.3.34	Multimedia Messages Storage	235
5.3.35	Equivalent HPLMN Presentation Indication request.....	236
5.3.36	NAF Key Centre Address request.....	236
5.3.37	Service provider name Icon	236
5.3.38	PLMN network name Icon	236
5.3.39	ICE Information request	236
5.3.40	eCall Related Procedures.....	237
5.3.40.1	eCall Only support	237
5.3.40.2	eCall and Normal call support.....	237
5.3.40.3	Change of eCall mode.....	237
5.3.41	SM-over-IP	238
5.3.42	UICC access to IMS	238
5.3.43	TV Configuration.....	238
5.3.44	3GPP PS Data Off related procedures	238
5.3.45	3GPP PS Data Off service list related procedures	238
5.3.46	EARFCN list for MTC/NB-IOT UEs	238
5.3.47	SUCI Calculation information procedure	238
5.3.48	SUCI Calculation by the USIM procedure	239
5.3.49	Control plane-based Steering of Roaming related procedures.....	239

5.3.50	5GS Operator PLMN List.....	239
5.3.51	Routing Indicator procedure for ME.....	239
5.4	USAT related procedures	239
5.4.1	Data Download via SMS-PP.....	239
5.4.2	Image Request	239
5.4.3	Data Download via SMS-CB.....	239
5.4.4	Call Control by USIM.....	239
5.4.5	MO-SMS control by USIM	239
5.4.6	Data Download via USSD and USSD application mode.....	240
5.4.7	Additional TERMINAL PROFILE after UICC activation	240
5.4.8	Terminal Applications	240
5.4.9	Call control on EPS PDN connection by USIM	240
5.4.10	Communication Control for IMS by USIM.....	240
5.4.11	USAT Facility Control.....	240
5.4.12	Extended Terminal Applications	240
5.4.13	USAT application pairing procedure	240
5.4.14	Call control on PDU Session by USIM	241
5.5	MexE related procedures.....	241
5.5.1	MexE ST.....	241
5.5.2	Operator root public key	241
5.5.3	Administrator root public key.....	241
5.5.4	Third Party root public key(s).....	241
5.5.5	Trusted Key/Certificates Data Files.....	242
5.6	WLAN related procedures.....	242
5.6.1	WLAN Selection related Procedures	242
5.6.2	WLAN PLMN Selection related procedures	242
5.6.3	WLAN access authentication related procedures	242
5.6.4	WLAN access re-authentication related procedures	242
5.7	Network Connectivity Parameters for UICC IP connections related procedures	242
5.8	H(e)NB related procedures.....	243
5.8.1	CSG Access Control procedures.....	243
5.8.2	CSG Type related procedures.....	243
5.8.3	HNB name display related procedures.....	243
5.9	ProSe related procedures	244
5.9.1	ProSe Direct Discovery Provisioning parameters.....	244
5.9.2	HPLMN ProSe Function address.....	244
5.9.3	ProSe direct communication related Procedures.....	244
5.9.4	ProSe direct discovery related Procedures.....	244
5.9.5	ProSe direct communication related Procedures.....	244
5.9.6	ProSe direct communication related Procedures.....	244
5.9.7	ProSe Group Counter related Procedures	244
5.9.8	ProSe Usage Information Reporting Configuration related Procedures	245
5.9.9	ProSe Group Member Discovery related Procedures	245
5.9.10	ProSe Relay related Procedures	245
5.10	ePDG Selection related procedures	245
5.10.1	Home ePDG Identifier	245
5.10.2	ePDG Selection Information.....	245
5.10.3	ePDG configuration information configured but empty	245
5.11	ACDC related procedures	246
5.11.1	ACDC Configuration.....	246
5.12	MCS related procedures	246
5.12.1	MCS configuration	246
5.12.2	Void.....	246
5.12.3	Void.....	246
5.12.4	Void.....	246
5.13	ePDG Selection for Emergency Services related procedures	246
5.13.1	Emergency ePDG Identifier.....	246
5.13.2	ePDG Selection Information for Emergency Services.....	246
5.13.3	ePDG configuration information for Emergency Services configured but empty	246
5.13.4	From Preferred related procedures.....	247
5.13.5	IMS Configuration Data related procedures	247
5.13.6	XCAP Configuration Data related procedures.....	247

5.14	V2X related procedures.....	247
5.14.1	V2X configuration.....	247
5.15	UAC Access Identities related procedures.....	247
5.15.1	UAC Access Identities Configuration.....	247
6	Security features.....	247
6.1	Authentication and key agreement procedure.....	248
6.2	Cryptographic Functions.....	248
6.3	GSM Conversion Functions.....	248
6.4	User verification and file access conditions.....	248
7	USIM Commands.....	249
7.1	AUTHENTICATE.....	249
7.1.1	Command description.....	249
7.1.1.1	3G security context.....	249
7.1.1.2	GSM security context.....	250
7.1.1.3	VGCS/VBS security context.....	250
7.1.1.4	GBA security context (Bootstrapping Mode).....	251
7.1.1.5	GBA security context (NAF Derivation Mode).....	251
7.1.1.6	MBMS security context (MSK Update Mode).....	252
7.1.1.7	Void.....	254
7.1.1.8	MBMS security context (MTK Generation Mode).....	254
7.1.1.9	MBMS security context (MSK Deletion Mode).....	254
7.1.1.10	MBMS security context (MUK Deletion Mode).....	255
7.1.1.11	Local Key Establishment security context (Key Derivation mode).....	255
7.1.1.12	Local Key Establishment security context (Key Availability Check mode).....	256
7.1.2	Command parameters and data.....	256
7.1.2.1	GSM/3G security context.....	258
7.1.2.2	VGCS/VBS security context.....	258
7.1.2.3	GBA security context (Bootstrapping Mode).....	259
7.1.2.4	GBA security context (NAF Derivation Mode).....	260
7.1.2.5	MBMS security context (All Modes).....	260
7.1.2.6	Local Key Establishment security context (All Modes).....	261
7.1.2.6.1	Local Key Establishment security context (Key Derivation mode).....	261
7.1.2.6.2	Local Key Establishment security context (Key Availability Check mode).....	263
7.2	Void.....	264
7.3	Status Conditions Returned by the USIM.....	264
7.3.1	Security management.....	264
7.3.2	Status Words of the Commands.....	265
7.4	Optional commands.....	266
7.5	GET IDENTITY.....	266
7.5.1	Command description.....	266
7.5.1.1	SUCI context.....	266
7.5.2	Command parameters and data.....	267
7.5.2.1	SUCI context.....	267
8	Void.....	268
Annex A (informative):	EF changes via Data Download or USAT applications.....	269
Annex B (normative):	Image Coding Schemes.....	274
B.1	Basic Image Coding Scheme.....	274
B.2	Colour Image Coding Scheme.....	275
B.3	Colour Image Coding Scheme with Transparency.....	276
Annex C (informative):	Structure of the Network parameters TLV objects.....	277
Annex D (informative):	Tags defined in 31.102.....	278
Annex E (informative):	Suggested contents of the EFs at pre-personalization.....	284
Annex F (informative):	Examples of coding of LSA Descriptor files for SoLSA.....	289

Annex G (informative):	Phonebook Example	290
Annex H (normative):	List of SFI Values.....	294
H.1	List of SFI Values at the USIM ADF Level.....	294
H.2	List of SFI Values at the DF GSM-ACCESS Level.....	294
H.3	List of SFI Values at the DF WLAN Level.....	295
H.4	List of SFI Values at the DF HNB Level	295
H.5	List of SFI Values at the DF ProSe Level	295
H.6	List of SFI Values at the DF ACDC Level.....	295
H.7	List of SFI Values at the DF MCS Level	296
H.8	List of SFI Values at the DF V2X Level.....	296
H.9	List of SFI Values at the DF 5GS Level	296
Annex I (informative):	USIM Application Session Activation/Termination.....	297
Annex J (informative):	Example of MMS coding.....	298
J.1	Coding example for MMS User Preferences.....	298
J.2	Coding Example for MMS Issuer/User Connectivity Parameters.....	298
Annex K (informative):	Examples of VService_Id coding.....	300
Annex L (normative):	USIM-INI and USIM-RN for Relay Nodes.....	301
L.1	Introduction	301
L.2	Application selection procedure	301
L.3	Secure channel operation.....	302
L.4	Support of commands.....	302
L.5	Storage of certificates.....	302
L.6	Relay Node files support.....	302
L.6.1	USIM-INI Files.....	302
L.6.1.1	EF _{CERT} (UICC Certificate)	302
L.6.2	USIM-RN Files.....	303
L.6.2.1	e _{FRNid} (Relay Node identifier).....	303
L.6.2.2	EF _{SCCmax} (maximum value of Secure Channel Counter)	304
Annex M (normative):	USIM application dedicated for IOPS.....	305
M.1	Introduction	305
M.2	Features of the USIM dedicated for IOPS.....	305
M.3	Selection mechanisms.....	305
Annex N (informative):	Change history	306
History		312

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.