ETSI TS 131 102 V14.7.0 (2019-05)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
Characteristics of the Universal Subscriber Identity Module (USIM) application
(3GPP TS 31.102 version 14.7.0 Release 14)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8710ec0d-30f0-4822-ab9b-a6651853d07f/etsi-ts-131-102-v14.7.0-2019-05

A GLOBAL INITIATIVE

Reference
RTS/TSGC-0631102ve70

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/d7178c0d-3000-4822-4b9a-a665183ad075/etsi-ts-131-102-v14.7.0-2019-05

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-4822-ab9b-a6651853d075/etsi-ts-131-102-v14-7-0-2019-05

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 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) 20
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_{SMSP} (Short message service parameters) 44
4.2.28 EF_{SMSS} (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) 52
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

ETSI STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/6f6178c0d-3040-4832-ab9b-ad5f8535d075/etsi-ts-131-102-v14.7.0-2019-05

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_{CMI} (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) 76
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_{VGCSS} (Voice Group Call Service Status) 83
4.2.75 EF_{VBS} (Voice Broadcast Service) 83
4.2.76 EF_{VBSS} (Voice Broadcast Service Status) 85
4.2.77 EF_{VGCSCA} (Voice Group Call Service Ciphering Algorithm) 86
4.2.78 EF_{VBSCA} (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 $EF_{EHPLMNPI}$ (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) 107
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8717f8c0d-3940-4f52-a9ba-651253d075/etsi-ts-131-102-v14.7.0-2019-05

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 $EF_{IMSConfigData}$ (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) 120
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 Ciphering key Kc) 142
4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS) 143
4.4.3.3 Void 143
4.4.3.4 EF_{CPBCCH} (CPBCCH Information) 143
4.4.3.5 $EF_{InvScan}$ (Investigation Scan) 144
4.4.4 Contents of files at the MexE level 145
4.4.4.1 $EF_{MexE-ST}$ (MexE Service table) 145
4.4.4.2 EF_{ORPK} (Operator Root Public Key) 145
4.4.4.3 EF_{ARPK} (Administrator Root Public Key) 147
4.4.4.4 EF_{TPRPK} (Third Party Root Public Key) 148
4.4.4.5 EF_{TKCDF} (Trusted Key/Certificates Data Files) 149
4.4.5 Contents of files at the DF WLAN level 149
4.4.5.1 EF_{Pseudo} (Pseudonym) 149
4.4.5.2 $EF_{UPLMNWLAN}$ (User controlled PLMN selector for I-WLAN Access) 150
4.4.5.3 $EF_{OPLMNWLAN}$ (Operator controlled PLMN selector for I-WLAN Access) 150
4.4.5.4 EF_{UWSIDL} (User controlled WLAN Specific Identifier List) 151
4.4.5.5 EF_{OWSIDL} (Operator controlled WLAN Specific IdentifierList) 152
4.4.5.6 EF_{WRI} (WLAN Reauthentication Identity) 152
4.4.5.7 EF_{HWSIDL} (Home I-WLAN Specific Identifier List) 153
4.4.5.8 $EF_{WEHPLMNPI}$ (I-WLAN Equivalent HPLMN Presentation Indication) 153
4.4.5.9 EF_{WHPI} (I-WLAN HPLMN Priority Indication) 154
4.4.5.10 $EF_{WLRPLMN}$ (I-WLAN Last Registered PLMN) 154
4.4.5.11 $EF_{HPLMNDAI}$ (HPLMN Direct Access Indicator) 155

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8717f8c0d-3940-45f7-ab9b-a6651253e075/etsi-ts-131-102-v14.7.0-2019-05

4.4.6 Contents of files at the DF HNB level 155
4.4.6.1 Introduction 155
4.4.6.2 EF_{ACSGL} (Allowed CSG Lists) 155
4.4.6.3 EF_{CSGT} (CSG Type) 158
4.4.6.4 EF_{HNBN} (Home NodeB Name) 160
4.4.6.5 EF_{OCSGL} (Operator CSG Lists) 160
4.4.6.6 EF_{OCSGT} (Operator CSG Type) 162
4.4.6.7 EF_{OHNBN} (Operator Home NodeB Name) 163
4.4.7 Void 163
4.4.8 Contents of files at the DF ProSe level 163
4.4.8.1 Introduction 163
4.4.8.2 EF_{PROSE_MON} (ProSe Monitoring Parameters) 163
4.4.8.3 EF_{PROSE_ANN} (ProSe Announcing Parameters) 164
4.4.8.4 $EF_{PROSEFUNC}$ (HPLMN ProSe Function) 165
4.4.8.5 $EF_{PROSE\_RADIO\_COM}$ (ProSe Direct Communication Radio Parameters) 166
4.4.8.6 $EF_{PROSE\_RADIO\_MON}$ (ProSe Direct Discovery Monitoring Radio Parameters) 168
4.4.8.7 $EF_{PROSE\_RADIO\_ANN}$ (ProSe Direct Discovery Announcing Radio Parameters) 169
4.4.8.8 EF_{PROSE_POLICY} (ProSe Policy Parameters) 170
4.4.8.9 EF_{PROSE_PLMN} (ProSe PLMN Parameters) 172
4.4.8.10 EF_{PROSE_GC} (ProSe Group Counter) 173
4.4.8.11 EF_{PST} (ProSe Service Table) 175
4.4.8.12 EF_{PROSE_UIRC} (ProSe UsageInformationReportingConfiguration) 175
4.4.8.12 $EF_{PROSE\_GM\_DISCOVERY}$ (ProSe Group Member Discovery Parameters) 179
4.4.8.13 EF_{PROSE_RELAY} (ProSe Relay Parameters) 180
4.4.8.14 $EF_{PROSE\_RELAY\_DISCOVERY}$ (ProSe Relay Discovery Parameters) 181
4.4.9 Contents of files at the DF ACDC level 184
4.4.9.1 Introduction 184
4.4.9.2 EF_{ACDC_LIST} (ACDC List) 184
4.4.9.3 $EF_{ACDC\_OS\_CONFIG}$ (ACDC OS configuration) 185
4.4.10 Contents of files at the DF TV level 186
4.4.10.1 Introduction 186
4.4.10.2 EF_{TVUSD} (TV User Service Description) 186
4.5 Contents of Efs at the TELECOM level 187
4.5.1 EF_{ADN} (Abbreviated dialling numbers) 187
4.5.2 EF_{EXT1} (Extension1) 187
4.5.3 EF_{ECCP} (Extended Capability Configuration Parameter) 187
4.5.4 EF_{SUME} (SetUpMenu Elements) 188
4.5.5 EF_{ARR} (Access Rule Reference) 188
4.5.6 EF_{ICE_DN} (In Case of Emergency – Dialling Number) 188
4.5.7 EF_{ICE_FF} (In Case of Emergency – Free Format) 188
4.5.8 EF_{RMA} (Remote Management Actions) 189
4.5.9 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC) 190
4.6 Contents of DFs at the TELECOM level 190
4.6.0 List of DFs at the TELECOM level 190
4.6.1 Contents of files at the $DF_{GRAPHICS}$ level 190
4.6.1.1 EF_{IMG} (Image) 190
4.6.1.2 EF_{IIDF} (Image Instance Data Files) 192
4.6.1.3 $EF_{ICE\_graphics}$ (In Case of Emergency – Graphics) 192
4.6.1.4 Void 193
4.6.1.5 Void 193
4.6.2 Contents of files at the $DF_{PHONEBOOK}$ under the $DF_{TELECOM}$ 193
4.6.3 Contents of files at the $DF_{MULTIMEDIA}$ level 193
4.6.3.1 EF_{MML} (Multimedia Messages List) 193
4.6.3.2 EF_{MMDF} (Multimedia Messages Data File) 196
4.6.4 Contents of files at the DF_{MCPTT} level 196
4.6.4.1 EF_{MST} (MCPTT Service Table) 197
4.6.4.2 EF_{MCPTT_CONFIG} (MCPTT configuration data) 197
4.6.4.3 Void 198
4.6.4.4 Void 198
4.6.4.5 Void 198
4.6.5 Contents of files at the DF_{V2X} level 198

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-4822-ab9b-a6651853d075/etsi-ts-131-102-v14.7.0-2019-05

4.6.5.1 V2X configuration data related files 198
4.6.5.2 EF_{VST} (V2X Service Table) 199
4.6.5.3 EF_{V2X_CONFIG} (V2X configuration data) 199
4.7 Files of USIM 201

5 Application protocol 206
5.1 USIM management procedures 207
5.1.1 Initialisation 207
5.1.1.1 USIM application selection 207
5.1.1.2 USIM initialisation 207
5.1.1.3 GSM related initialisation procedures 208
5.1.2 Session termination 208
5.1.2.1 3G session termination 208
5.1.2.1.1 GSM termination procedures 209
5.1.2.2 3G session reset 209
5.1.3 USIM application closure 209
5.1.4 Emergency call codes 209
5.1.5 Language indication 209
5.1.6 Administrative information request 209
5.1.7 USIM service table request 209
5.1.8 Void 209
5.1.9 UICC presence detection 209
5.1.10 UICC interface in PSM 210
5.1.11 UICC interface during eDRX 210
5.2 USIM security related procedures 211
5.2.1 Authentication algorithms computation 211
5.2.2 IMSI request 211
5.2.3 Access control information request 211
5.2.4 Higher Priority PLMN search period request 211
5.2.5 Location information 211
5.2.6 Cipher and Integrity key 211
5.2.7 Forbidden PLMN 211
5.2.8 Void 211
5.2.9 User Identity Request 211
5.2.10 GSM Cipher key 211
5.2.11 GPRS Cipher key 211
5.2.12 Initialisation value for Hyperframe number 212
5.2.13 Maximum value of START 212
5.2.14 HPLMN selector with Access Technology request 212
5.2.15 Packet Switched Location information 212
5.2.16 Cipher and Integrity key for Packet Switched domain 212
5.2.17 LSA information 212
5.2.18 Voice Group Call Services 212
5.2.19 Voice Broadcast Services 212
5.2.20 Generic Bootstrapping architecture (Bootstrap) 213
5.2.21 Generic Bootstrapping architecture (NAF Derivation) 213
5.2.22 MSK MIKEY Message Reception 213
5.2.23 MTK MIKEY Message Reception 213
5.2.24 Void 213
5.2.25 EHPLMN request 213
5.2.26 Last RPLMN Selection Indication request 213
5.2.29 Non Access Stratum Configuration 213
5.2.30 PWS Configuration 214
5.3 Subscription related procedures 214
5.3.1 Phone book procedures 214
5.3.1.1 Initialisation 214
5.3.1.2 Creation/Deletion of information 214
5.3.1.3 Hidden phone book entries 214
5.3.2 Dialling numbers 214
5.3.3 Short messages 216
5.3.4 Advice of charge 216
5.3.5 Capability configuration parameters 217

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-482a-a9b0-bcf6518533d0/75/etsi-ts-131-102-v14.7.0-2019-05

5.3.6 User controlled PLMN selector with Access Technology 217
5.3.7 Cell broadcast message identifier 217
5.3.8 Group identifier level 1 217
5.3.9 Group identifier level 2 217
5.3.10 Service provider name 217
5.3.11 Enhanced multi level precedence and pre-emption service 218
5.3.12 Cell broadcast message identifier ranges 218
5.3.13 Short message status report 218
5.3.14 APN Control List 218
5.3.15 Depersonalisation Control Keys 219
5.3.16 Co-operative Network List 219
5.3.17 CPBCCH information 219
5.3.18 Investigation Scan 219
5.3.19 Enabled Services Table Request 219
5.3.20 Operator controlled PLMN selector with Access Technology 219
5.3.21 HPLMN selector with Access Technology 219
5.3.22 Automatic Answer on eMLPP service 219
5.3.23 Network Parameter information 219
5.3.24 PLMN network name 220
5.3.25 Operator PLMN List 220
5.3.26 Message Waiting Indication 220
5.3.27 Call Forwarding Indication Status 220
5.3.28 Service Provider Display Information 220
5.3.29 MMS Notifications 220
5.3.30 MMS Issuer Connectivity Parameters 221
5.3.31 MMS User Preferences 221
5.3.32 MMS User Connectivity Parameters 221
5.3.33 Network's indication of alerting 221
5.3.34 Multimedia Messages Storage 221
5.3.35 Equivalent HPLMN Presentation Indication request 222
5.3.36 NAF Key Centre Address request 222
5.3.37 Service provider name Icon 222
5.3.38 PLMN network name Icon 222
5.3.39 ICE Information request 222
5.3.40 eCall Related Procedures 222
5.3.40.1 eCall Only support 222
5.3.40.2 eCall and Normal call support 223
5.3.40.3 Change of eCall mode 223
5.3.41 SM-over-IP 223
5.3.42 UICC access to IMS 224
5.3.43 TV Configuration 224
5.3.44 3GPP PS Data Off related procedures 224
5.3.45 3GPP PS Data Off service list related procedures 224
5.4 USAT related procedures 224
5.4.1 Data Download via SMS-PP 224
5.4.2 Image Request 224
5.4.3 Data Download via SMS-CB 224
5.4.4 Call Control by USIM 224
5.4.5 MO-SMS control by USIM 225
5.4.6 Data Download via USSD and USSD application mode 225
5.4.7 Additional TERMINAL PROFILE after UICC activation 225
5.4.8 Terminal Applications 225
5.4.9 Call control on EPS PDN connection by USIM 225
5.4.10 Communication Control for IMS by USIM 225
5.4.11 USAT Facility Control 225
5.4.12 Extended Terminal Applications 225
5.4.13 USAT application pairing procedure 225
5.5 MexE related procedures 226
5.5.1 MexE ST 226
5.5.2 Operator root public key 226
5.5.3 Administrator root public key 226
5.5.4 Third Party root public key(s) 226

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-4822-ab9b-a6651853d075/etsi-ts-131-102-v14.7.0-2019-05

5.5.5 Trusted Key/Certificates Data Files 226
5.6 WLAN related procedures 227
5.6.1 WLAN Selection related Procedures 227
5.6.2 WLAN PLMN Selection related procedures 227
5.6.3 WLAN access authentication related procedures 227
5.6.4 WLAN access re-authentication related procedures 227
5.7 Network Connectivity Parameters for UICC IP connections related procedures 227
5.8 H(e)NB related procedures 227
5.8.1 CSG Access Control procedures 227
5.8.2 CSG Type related procedures 228
5.8.3 HNB name display related procedures 228
5.9 ProSe related procedures 229
5.9.1 ProSe Direct Discovery Provisioning parameters 229
5.9.2 HPLMN ProSe Function address 229
5.9.3 ProSe direct communication related Procedures 229
5.9.4 ProSe direct discovery related Procedures 229
5.9.5 ProSe direct communication related Procedures 229
5.9.6 ProSe direct communication related Procedures 229
5.9.7 ProSe Group Counter related Procedures 229
5.9.8 ProSe Usage Information Reporting Configuration related Procedures 229
5.9.9 ProSe Group Member Discovery related Procedures 230
5.9.10 ProSe Relay related Procedures 230
5.10 ePDG Selection related procedures 230
5.10.1 Home ePDG Identifier 230
5.10.2 ePDG Selection Information 230
5.10.3 ePDG configuration information configured but empty 230
5.11 ACDC related procedures 230
5.11.1 ACDC Configuration 230
5.12 MCPTT related procedures 231
5.12.1 MCPTT configuration 231
5.12.2 Void 231
5.12.3 Void 231
5.12.4 Void 231
5.13 ePDG Selection for Emergency Services related procedures 231
5.13.1 Emergency ePDG Identifier 231
5.13.2 ePDG Selection Information for Emergency Services 231
5.13.3 ePDG configuration information for Emergency Services configured but empty 231
5.13.4 From Preferred related procedures 231
5.13.5 IMS Configuration Data related procedures 231
5.13.6 XCAP Configuration Data related procedures 232
5.14 V2X related procedures 232
5.14.1 V2X configuration 232

6 Security features 232
6.1 Authentication and key agreement procedure 232
6.2 Cryptographic Functions 233
6.3 GSM Conversion Functions 233
6.4 User verification and file access conditions 233

7 USIM Commands 233
7.1 AUTHENTICATE 233
7.1.1 Command description 233
7.1.1.1 3G security context 234
7.1.1.2 GSM security context 235
7.1.1.3 VGCS/VBS security context 235
7.1.1.4 GBA security context (Bootstrapping Mode) 235
7.1.1.5 GBA security context (NAF Derivation Mode) 236
7.1.1.6 MBMS security context (MSK Update Mode) 237
7.1.1.7 Void 238
7.1.1.8 MBMS security context (MTK Generation Mode) 238
7.1.1.9 MBMS security context (MSK Deletion Mode) 239
7.1.1.10 MBMS security context (MUK Deletion Mode) 239

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8717f8c0d-3040-4b52-a99b-e651f553f075/etsi-ts-131-102-v14.7.0-2019-05

7.1.1.11 Local Key Establishment security context (Key Derivation mode) 240
7.1.1.12 Local Key Establishment security context (Key Availability Check mode) 240
7.1.2 Command parameters and data 241
7.1.2.1 GSM/3G security context 242
7.1.2.2 VGCS/VBS security context 243
7.1.2.3 GBA security context (Bootstrapping Mode) 244
7.1.2.4 GBA security context (NAF Derivation Mode) 244
7.1.2.5 MBMS security context (All Modes) 245
7.1.2.6 Local Key Establishment security context (All Modes) 246
7.1.2.6.1 Local Key Establishment security context (Key Derivation mode) 246
7.1.2.6.2 Local Key Establishment security context (Key Availability Check mode) 248
7.2 Void 249
7.3 Status Conditions Returned by the USIM 249
7.3.1 Security management 249
7.3.2 Status Words of the Commands 250
7.4 Optional commands 251

8 Void 251

Annex A (informative): EF changes via Data Download or USAT applications 252

Annex B (normative): Image Coding Schemes 257

B.1 Basic Image Coding Scheme 257

B.2 Colour Image Coding Scheme 258

B.3 Colour Image Coding Scheme with Transparency 259

Annex C (informative): Structure of the Network parameters TLV objects 260

Annex D (informative): Tags defined in 31.102 261

Annex E (informative): Suggested contents of the EFs at pre-personalization 267

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA 272

Annex G (informative): Phonebook Example 273

Annex H (normative): List of SFI Values 277

H.1 List of SFI Values at the USIM ADF Level 277

H.2 List of SFI Values at the DF GSM-ACCESS Level 277

H.3 List of SFI Values at the DF WLAN Level 278

H.4 List of SFI Values at the DF HNB Level 278

H.5 List of SFI Values at the DF ProSe Level 278

H.6 List of SFI Values at the DF ACDC Level 278

H.7 List of SFI Values at the DF MCPTT Level 279

H.8 List of SFI Values at the DF V2X Level 279

Annex I (informative): USIM Application Session Activation/Termination 280

Annex J (informative): Example of MMS coding 281

J.1 Coding example for MMS User Preferences 281
J.2 Coding Example for MMS Issuer/User Connectivity Parameters 281

Annex K (informative): Examples of VService_Id coding 283

Annex L (normative): USIM-INI and USIM-RN for Relay Nodes 284

L.1 Introduction 284
L.2 Application selection procedure 284

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-4802-abfb-a6641853d075/etsi-ts-131-102-v14-7-0-2019-05

L.3 Secure channel operation....285
L.4 Support of commands....285
L.5 Storage of certificates....285
L.6 Relay Node files support....285
L.6.1 USIM-INI Files....285
L.6.1.1 EF_{CERT} (UICC Certificate)....285
L.6.2 USIM-RN Files....286
L.6.2.1 eF_{RNid} (Relay Node identifier)....286
L.6.2.2 EF_{SCCmax} (maximum value of Secure Channel Counter)....287

Annex M (normative): USIM application dedicated for IOPS....288
M.1 Introduction....288
M.2 Features of the USIM dedicated for IOPS....288
M.3 Selection mechanisms....288

Annex N (informative): Change history....289

History....294

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/87178c0d-30f0-4822-ab9b-a6651853d075/etsi-ts-131-102-v14.7.0-2019-05

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4822-ab9b-a6651853d075/etsi-ts-131-102-v14.7.0-2019-05