ARIB STD-T63-31.102 V11.6.0

Characteristics of the Universal Subscriber Identity Module (USIM) application

(Release 11)

Refer to “Industrial Property Rights (IPR)” in the preface of ARIB STD-T63 for Related Industrial Property Rights. Refer to “Notice” in the preface of ARIB STD-T63 for Copyrights.

3GPP TS 31.102 V11.6.0 (2013-09)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application

(Release 11)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Keywords

UMTS, SIM, card, LTE

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

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

© 2013, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

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) 25
4.2.10 EF_{GID1} (Group Identifier Level 1) 26
4.2.11 EF_{GID2} (Group Identifier Level 2) 26
4.2.12 EF_{SPN} (Service Provider Name) 26
4.2.13 EF_{PUCT} (Price per Unit and Currency Table) 27
4.2.14 EF_{CBMI} (Cell Broadcast Message identifier selection) 28
4.2.15 EF_{ACC} (Access Control Class) 29
4.2.16 EF_{FPLMN} (Forbidden PLMNs) 29
4.2.17 EF_{LOCI} (Location Information) 30
4.2.18 EF_{AD} (Administrative Data) 31
4.2.19 Void 33
4.2.20 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download) 33
4.2.21 EF_{ECC} (Emergency Call Codes) 33
4.2.22 EF_{CBMIR} (Cell Broadcast Message Identifier Range selection) 35
4.2.23 EF_{PSLOCI} (Packet Switched location information) 35
4.2.24 EF_{FDN} (Fixed Dialling Numbers) 36
4.2.25 EF_{SMS} (Short messages) 37
4.2.26 EF_{MSISDN} (MSISDN) 38
4.2.27 EF_{SMSP} (Short message service parameters) 39
4.2.28 EF_{SMSS} (SMS status) 40
4.2.29 EF_{SDN} (Service Dialling Numbers) 41
4.2.30 EF_{EXT2} (Extension2) 42
4.2.31 EF_{EXT3} (Extension3) 42
4.2.32 EF_{SMSR} (Short message status reports) 42
4.2.33 EF_{ICI} (Incoming Call Information) 43
4.2.34 EF_{OCI} (Outgoing Call Information) 46
4.2.35 EF_{ICT} (Incoming Call Timer) 47
4.2.36 EF_{OCT} (Outgoing Call Timer) 48
4.2.37 EF_{EXT5} (Extension5) 48
4.2.38 EF_{CCP2} (Capability Configuration Parameters 2) 49
4.2.39 EF_{eMLPP} (enhanced Multi Level Precedence and Pre-emption) 49
4.2.40 EF_{AaeM} (Automatic Answer for eMLPP Service) 50
4.2.41 Void 51
4.2.42 $EF_{Hiddenkey}$ (Key for hidden phone book entries) 51

4.2.43 Void 52
4.2.44 EF_{BDN} (Barred Dialling Numbers) 52
4.2.45 EF_{EXT4} (Extension4) 52
4.2.46 EF_{CMI} (Comparison Method Information) 53
4.2.47 EF_{EST} (Enabled Services Table) 53
4.2.48 EF_{ACL} (Access Point Name Control List) 54
4.2.49 EF_{DCK} (Depersonalisation Control Keys) 54
4.2.50 EF_{CNL} (Co-operative Network List) 55
4.2.51 $EF_{START\text{-}HFN}$ (Initialisation values for Hyperframe number) 56
4.2.52 $EF_{THRESHOLD}$ (Maximum value of START) 57
4.2.53 $EF_{OPLMNwACT}$ (Operator controlled PLMN selector with Access Technology) 57
4.2.54 $EF_{HPLMNwAcT}$ (HPLMN selector with Access Technology) 58
4.2.55 EF_{ARR} (Access Rule Reference) 58
4.2.56 Void 59
4.2.57 EF_{NETPAR} (Network Parameters) 59
4.2.58 EF_{PNN} (PLMN Network Name) 61
4.2.59 EF_{OPL} (Operator PLMN List) 62
4.2.60 EF_{MBDN} (Mailbox Dialling Numbers) 63
4.2.61 EF_{EXT6} (Extension6) 64
4.2.62 EF_{MBI} (Mailbox Identifier) 64
4.2.63 EF_{MWIS} (Message Waiting Indication Status) 65
4.2.64 EF_{CFIS} (Call Forwarding Indication Status) 66
4.2.65 EF_{EXT7} (Extension7) 68
4.2.66 EF_{SPDI} (Service Provider Display Information) 68
4.2.67 EF_{MMSN} (MMS Notification) 69
4.2.68 EF_{EXT8} (Extension 8) 70
4.2.69 EF_{MMSICP} (MMS Issuer Connectivity Parameters) 71
4.2.70 EF_{MMSUP} (MMS User Preferences) 73
4.2.71 EF_{MMSUCP} (MMS User Connectivity Parameters) 74
4.2.72 $EF_{\mathbf{NIA}}$ (Network's Indication of Alerting) 74
4.2.73 $EF_{\mathbf{VGCS}}$ (Voice Group Call Service) 75
4.2.74 $EF_{\mathbf{VGCSS}}$ (Voice Group Call Service Status) 77
4.2.75 $EF_{\mathbf{VBS}}$ (Voice Broadcast Service) 77
4.2.76 $EF_{\mathbf{VBSS}}$ (Voice Broadcast Service Status) 79
4.2.77 $EF_{\mathbf{VGCSCA}}$ (Voice Group Call Service Ciphering Algorithm) 80
4.2.78 $EF_{\mathbf{VBSCA}}$ (Voice Broadcast Service Ciphering Algorithm) 81
4.2.79 EF_{GBABP} (GBA Bootstrapping parameters) 81
4.2.80 EF_{MSK} (MBMS Service Keys List) 82
4.2.81 EF_{MUK} (MBMS User Key) 83
4.2.82 Void 84
4.2.83 EF_{GBANL} (GBA NAF List) 84
4.2.84 EF_{EHPLMN} (Equivalent HPLMN) 85
4.2.85 $EF_{EHPLMNPI}$ (Equivalent HPLMN Presentation Indication) 85
4.2.86 $EF_{LRPLMNSI}$ (Last RPLMN Selection Indication) 86
4.2.87 EF_{NAFKCA} (NAF Key Centre Address) 86
4.2.88 EF_{SPNI} (Service Provider Name Icon) 87
4.2.89 EF_{PNNI} (PLMN Network Name Icon) 88
4.2.90 $EF_{NCP\text{-}IP}$ (Network Connectivity Parameters for USIM IP connections) 88
4.2.91 $EF_{EPSLOCI}$ (EPS location information) 91
4.2.92 EF_{EPSNSC} (EPS NAS Security Context) 93
4.2.93 EF_{UFC} (USAT Facility Control) 94
4.2.94 $EF_{NASCONFIG}$ (Non Access Stratum Configuration) 95
4.2.95 $EF_{UICCIARI}$ (UICC IARI) 97
4.2.96 EF_{PWS} (Public Warning System) 98
4.3 DFs at the USIM ADF (Application DF) Level 99
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 $EF_{\mathbf{SAI}}$ (SoLSA Access Indicator) 100
4.4.1.2 $EF_{\mathbf{SLL}}$ (SoLSA LSA List) 100
4.4.1.3 LSA Descriptor files 103
4.4.2 Contents of files at the DF PHONEBOOK level 104

4.4.2.1 EF_{PBR} (Phone Book Reference file) ... 104
4.4.2.2 EF_{IAP} (Index Administration Phone book) ... 106
4.4.2.3 EF_{ADN} (Abbreviated dialling numbers) ... 107
4.4.2.4 EF_{EXT1} (Extension1) ... 110
4.4.2.5 EF_{PBC} (Phone Book Control) ... 111
4.4.2.6 EF_{GRP} (Grouping file) ... 112
4.4.2.7 EF_{AAS} (Additional number Alpha String) ... 113
4.4.2.8 EF_{GAS} (Grouping information Alpha String) ... 114
4.4.2.9 EF_{ANR} (Additional Number) ... 114
4.4.2.10 EF_{SNE} (Second Name Entry) ... 116
4.4.2.11 EF_{CCP1} (Capability Configuration Parameters 1) ... 116
4.4.2.12 Phone Book Synchronisation ... 117
4.4.2.12.1 EF_{UID} (Unique Identifier) ... 117
4.4.2.12.2 EF_{PSC} (Phone book Synchronisation Counter) ... 118
4.4.2.12.3 EF_{CC} (Change Counter) ... 119
4.4.2.12.4 EF_{PUID} (Previous Unique Identifier) ... 119
4.4.2.13 EF_{EMAIL} (e-mail address) ... 120
4.4.2.14 Phonebook restrictions ... 121
4.4.3 Contents of files at the DF GSM-ACCESS level (Files required for GSM Access) ... 121
4.4.3.1 EF_{Kc} (GSM Ciphering key Kc) ... 121
4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS) ... 122
4.4.3.3 Void ... 122
4.4.3.4 EF_{CPBCCH} (CPBCCH Information) ... 122
4.4.3.5 $EF_{InvScan}$ (Investigation Scan) ... 123
4.4.4 Contents of files at the MexE level ... 124
4.4.4.1 $EF_{MexE\text{-}ST}$ (MexE Service table) ... 124
4.4.4.2 EF_{ORPK} (Operator Root Public Key) ... 125
4.4.4.3 EF_{ARPK} (Administrator Root Public Key) ... 126
4.4.4.4 EF_{TPRPK} (Third Party Root Public Key) ... 127
4.4.4.5 EF_{TKCDF} (Trusted Key/Certificates Data Files) ... 128
4.4.5 Contents of files at the DF WLAN level ... 128
4.4.5.1 EF_{Pseudo} (Pseudonym) ... 128
4.4.5.2 $EF_{UPLMNWLAN}$ (User controlled PLMN selector for I-WLAN Access) ... 129
4.4.5.3 $EF_{OPLMNWLAN}$ (Operator controlled PLMN selector for I-WLAN Access) ... 129
4.4.5.4 EF_{UWSIDL} (User controlled WLAN Specific Identifier List) ... 130
4.4.5.5 EF_{OWSIDL} (Operator controlled WLAN Specific IdentifierList) ... 131
4.4.5.6 EF_{WRI} (WLAN Reauthentication Identity) ... 131
4.4.5.7 EF_{HWSIDL} (Home I-WLAN Specific Identifier List) ... 132
4.4.5.8 $EF_{WEHPLMNPI}$ (I-WLAN Equivalent HPLMN Presentation Indication) ... 133
4.4.5.9 EF_{WHPI} (I-WLAN HPLMN Priority Indication) ... 133
4.4.5.10 $EF_{WLRPLMN}$ (I-WLAN Last Registered PLMN) ... 134
4.4.5.11 $EF_{HPLMNDAI}$ (HPLMN Direct Access Indicator) ... 134
4.4.6 Contents of files at the DF HNB level ... 135
4.4.6.1 Introduction ... 135
4.4.6.2 EF_{ACSGL} (Allowed CSG Lists) ... 135
4.4.6.3 EF_{CSGT} (CSG Type) ... 138
4.4.6.4 EF_{HNBN} (Home NodeB Name) ... 140
4.4.6.5 EF_{OCSGL} (Operator CSG Lists) ... 140
4.4.6.6 EF_{OCSGT} (Operator CSG Type) ... 142
4.4.6.7 EF_{OHNBN} (Operator Home NodeB Name) ... 143
4.4.7 Void ... 143
4.5 Contents of Efs at the TELECOM level ... 143
4.5.1 EF_{ADN} (Abbreviated dialling numbers) ... 143
4.5.2 EF_{EXT1} (Extension1) ... 143
4.5.3 EF_{ECCP} (Extended Capability Configuration Parameter) ... 143
4.5.4 EF_{SUME} (SetUpMenu Elements) ... 143
4.5.5 EF_{ARR} (Access Rule Reference) ... 144
4.5.6 EF_{ICE_DN} (In Case of Emergency – Dialling Number) ... 144
4.5.7 EF_{ICE_FF} (In Case of Emergency – Free Format) ... 144
4.5.8 EF_{RMA} (Remote Management Actions) ... 145
4.5.9 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC) ... 146
4.6 Contents of DFs at the TELECOM level ... 146

4.6.1 Contents of files at the $DF_{GRAPHICS}$ level 146
4.6.1.1 EF_{IMG} (Image) 146
4.6.1.2 EF_{IIDF} (Image Instance Data Files) 148
4.6.1.3 $EF_{ICE\_graphics}$ (In Case of Emergency – Graphics) 148
4.6.1.4 $EF_{LAUNCH\ SCWS}$ 149
4.6.1.5 EF_{ICON} 152
4.6.2 Contents of files at the $DF_{PHONEBOOK}$ under the $DF_{TELECOM}$ 153
4.6.3 Contents of files at the $DF_{MULTIMEDIA}$ level 153
4.6.3.1 EF_{MML} (Multimedia Messages List) 153
4.6.3.2 EF_{MMDF} (Multimedia Messages Data File) 156
4.7 Files of USIM 157

5 Application protocol 161
5.1 USIM management procedures 161
5.1.1 Initialisation 161
5.1.1.1 USIM application selection 161
5.1.1.2 USIM initialisation 161
5.1.1.3 GSM related initialisation procedures 163
5.1.2 Session termination 163
5.1.2.1 3G session termination 163
5.1.2.1.1 GSM termination procedures 163
5.1.2.2 3G session reset 163
5.1.3 USIM application closure 163
5.1.4 Emergency call codes 164
5.1.5 Language indication 164
5.1.6 Administrative information request 164
5.1.7 USIM service table request 164
5.1.8 Void 164
5.1.9 UICC presence detection 164
5.2 USIM security related procedures 164
5.2.1 Authentication algorithms computation 164
5.2.2 IMSI request 164
5.2.3 Access control information request 164
5.2.4 Higher Priority PLMN search period request 164
5.2.5 Location information 165
5.2.6 Cipher and Integrity key 165
5.2.7 Forbidden PLMN 165
5.2.8 Void 165
5.2.9 User Identity Request 165
5.2.10 GSM Cipher key 165
5.2.11 GPRS Cipher key 165
5.2.12 Initialisation value for Hyperframe number 165
5.2.13 Maximum value of START 165
5.2.14 HPLMN selector with Access Technology request 165
5.2.15 Packet Switched Location information 166
5.2.16 Cipher and Integrity key for Packet Switched domain 166
5.2.17 LSA information 166
5.2.18 Voice Group Call Services 166
5.2.19 Voice Broadcast Services 166
5.2.20 Generic Bootstrapping architecture (Bootstrap) 166
5.2.21 Generic Bootstrapping architecture (NAF Derivation) 166
5.2.22 MSK MIKEY Message Reception 167
5.2.23 MTK MIKEY Message Reception 167
5.2.24 Void 167
5.2.25 EHPLMN request 167
5.2.26 Last RPLMN Selection Indication request 167
5.2.29 Non Access Stratum Configuration 167
5.2.30 PWS Configuration 167
5.3 Subscription related procedures 168
5.3.1 Phone book procedures 168
5.3.1.1 Initialisation 168
5.3.1.2 Creation/Deletion of information 168

5.3.1.3 Hidden phone book entries 168
5.3.2 Dialling numbers 168
5.3.3 Short messages 170
5.3.4 Advice of charge 170
5.3.5 Capability configuration parameters 171
5.3.6 User controlled PLMN selector with Access Technology 171
5.3.7 Cell broadcast message identifier 171
5.3.8 Group identifier level 1 171
5.3.9 Group identifier level 2 171
5.3.10 Service provider name 171
5.3.11 Enhanced multi level precedence and pre-emption service 172
5.3.12 Cell broadcast message identifier ranges 172
5.3.13 Short message status report 172
5.3.14 APN Control List 172
5.3.15 Depersonalisation Control Keys 173
5.3.16 Co-operative Network List 173
5.3.17 CPBCCH information 173
5.3.18 Investigation Scan 173
5.3.19 Enabled Services Table Request 173
5.3.20 Operator controlled PLMN selector with Access Technology 173
5.3.21 HPLMN selector with Access Technology 173
5.3.22 Automatic Answer on eMLPP service 173
5.3.23 Network Parameter information 174
5.3.24 PLMN network name 174
5.3.25 Operator PLMN List 174
5.3.26 Message Waiting Indication 174
5.3.27 Call Forwarding Indication Status 174
5.3.28 Service Provider Display Information 174
5.3.29 MMS Notifications 174
5.3.30 MMS Issuer Connectivity Parameters 175
5.3.31 MMS User Preferences 175
5.3.32 MMS User Connectivity Parameters 175
5.3.33 Network's indication of alerting 175
5.3.34 Multimedia Messages Storage 175
5.3.35 Equivalent HPLMN Presentation Indication request 176
5.3.36 NAF Key Centre Address request 176
5.3.37 Service provider name Icon 176
5.3.38 PLMN network name Icon 176
5.3.39 ICE Information request 176
5.3.40 eCall Related Procedures 177
5.3.40.1 eCall Only support 177
5.3.40.2 eCall and Normal call support 177
5.3.41 SM-over-IP 177
5.3.42 UICC access to IMS 177
5.4 USAT related procedures 177
5.4.1 Data Download via SMS-PP 177
5.4.2 Image Request 177
5.4.3 Data Download via SMS-CB 178
5.4.4 Call Control by USIM 178
5.4.5 MO-SMS control by USIM 178
5.4.6 Data Download via USSD and USSD application mode 178
5.4.7 Additional TERMINAL PROFILE after UICC activation 178
5.4.8 Terminal Applications 178
5.4.9 Call control on EPS PDN connection by USIM 178
5.4.10 Communication Control for IMS by USIM 178
5.4.11 USAT Facility Control 179
5.4.12 Extended Terminal Applications 179
5.5 MexE related procedures 179
5.5.1 MexE ST 179
5.5.2 Operator root public key 179
5.5.3 Administrator root public key 179
5.5.4 Third Party root public key(s) 179

5.5.5 Trusted Key/Certificates Data Files 179
5.6 WLAN related procedures 180
5.6.1 WLAN Selection related Procedures 180
5.6.2 WLAN PLMN Selection related procedures 180
5.6.3 WLAN access authentication related procedures 180
5.6.4 WLAN access re-authentication related procedures 180
5.7 Network Connectivity Parameters for UICC IP connections related procedures 180
5.8 H(e)NB related procedures 180
5.8.1 CSG Access Control procedures 180
5.8.2 CSG Type related procedures 181
5.8.3 HNB name display related procedures 181

6 Security features 182
6.1 Authentication and key agreement procedure 182
6.2 Cryptographic Functions 182
6.3 GSM Conversion Functions 183
6.4 User verification and file access conditions 183

7 USIM Commands 183
7.1 AUTHENTICATE 183
7.1.1 Command description 183
7.1.1.1 3G security context 184
7.1.1.2 GSM security context 185
7.1.1.3 VGCS/VBS security context 185
7.1.1.4 GBA security context (Bootstrapping Mode) 185
7.1.1.5 GBA security context (NAF Derivation Mode) 186
7.1.1.6 MBMS security context (MSK Update Mode) 187
7.1.1.7 Void 188
7.1.1.8 MBMS security context (MTK Generation Mode) 188
7.1.1.9 MBMS security context (MSK Deletion Mode) 189
7.1.1.10 MBMS security context (MUK Deletion Mode) 189
7.1.1.11 Local Key Establishment security context (Key Derivation mode) 189
7.1.1.12 Local Key Establishment security context (Key Availability Check mode) 190
7.1.2 Command parameters and data 190
7.1.2.1 GSM/3G security context 192
7.1.2.2 VGCS/VBS security context 193
7.1.2.3 GBA security context (Bootstrapping Mode) 193
7.1.2.4 GBA security context (NAF Derivation Mode) 194
7.1.2.5 MBMS security context (All Modes) 194
7.1.2.6 Local Key Establishment security context (All Modes) 195
7.1.2.6.1 Local Key Establishment security context (Key Derivation mode) 195
7.1.2.6.2 Local Key Establishment security context (Key Availability Check mode) 197
7.2 Void 198
7.3 Status Conditions Returned by the USIM 198
7.3.1 Security management 198
7.3.2 Status Words of the Commands 199
7.4 Optional commands 200

8 Void 200

Annex A (informative): EF changes via Data Download or USAT applications 201

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 210

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA 213

Annex G (informative): Phonebook Example 214

Annex H (normative): List of SFI Values 218

H.1 List of SFI Values at the USIM ADF Level 218

H.2 List of SFI Values at the DF GSM-ACCESS Level 218

H.3 List of SFI Values at the DF WLAN Level 219

H.4 List of SFI Values at the DF HNB Level 219

Annex I (informative): USIM Application Session Activation/Termination 220

Annex J (informative): Example of MMS coding 221

J.1 Coding example for MMS User Preferences 221

J.2 Coding Example for MMS Issuer/User Connectivity Parameters 221

Annex K (informative): Examples of VService_Id coding 223

Annex L : USIM-INI and USIM-RN for Relay Nodes (normative) 224

L.1 Introduction 224

L.2 Application selection procedure 224

L.3 Secure channel operation 225

L.4 Support of commands 225

L.5 Storage of certificates 225

L.6 Relay Node files support 225

L.6.1 USIM-INI Files 225

L.6.1.1 EF_{CERT} (UICC Certificate) 225

L.6.2 USIM-RN Files 226

L.6.2.1 eF_{RNid} (Relay Node identifier) 226

L.6.2.2 EF_{SCCmax} (maximum value of Secure Channel Counter) 227

Annex M (informative): Change history 228

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".

[44] 3GPP TS 43.020: "Technical Specification Group Services and system Aspects; Security related network functions"

[45] 3GPP2 X.S0016-000-A v1.0: "3GPP2 Multimedia Messaging System MMS Specification Overview, Revision A"

[46] 3GPP TS 43.068: "Technical Specification Group Core Network; Voice Group Call Service (VGCS); Stage 2".

[47] 3GPP TS 33.110: "Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal".

[48] IETF RFC 3629 (2003): "UTF-8, a transformation format of ISO 10646".

[49] Open Mobile Alliance; OMA-TS-BCAST_SvcCntProtection
URL: http://www.openmobilealliance.org/

[50] ETSI TS TS 102 483 V8.1.0: "UICC-Terminal interface; Internet Protocol connectivity between UICC and Terminal".

[51] 3GPP TS 24.301: "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet Systems (EPS): Stage 3".

[52] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[53] 3GPP2 C.S0074-A v1.0: "UICC-Terminal Interface Physical and Logical Characteristics for cdma2000 Spread Spectrum Systems"

[54] 3GPP TS 22.220: "Service requirements for Home NodeBs and Home eNodeBs ".

[55] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3"

[56] IETF RFC 3261: "SIP: Session Initiation Protocol".

[57] IETF RFC 3629 (2003): "UTF-8, a transformation format of ISO 10646".

[58] 3GPP TS 24.285: "Allowed Closed Subscriber Group (CSG) list; Management Object (MO)"

[59] OMA Smartcard-Web-Server Approved Version 1.1 - 12 May 2009 (OMA-TS-Smartcard_Web_Server-V1_1-20090512-A).[60] ISO/IEC 15948:2003: "Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification".

[61] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

NOTE: Available from http://www.ietf.org/rfc/rfc2046.txt.

[62] ETSI TS 101 220 : "Smart Cards; ETSI numbering system for telecommunication application providers".

[63] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3"

[64] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[65] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)".

[66] ETSI TS 102 484 V10.1.0: "Smart Cards; Secure channel between a UICC and end-point terminal"

[67] ISO/IEC 7816-15:2004: "Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application"

[68] 3GPP TS 22.268: "Public Warning System (PWS) Requirements".

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

For the purposes of the present document, the following definition applies.

ADM: access condition to an EF which is under the control of the authority which creates this file.

> Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority
>
> The definition of access condition ADM does not preclude the administrative authority from using ALW, PIN, PIN2 and NEV if required.
>
> A terminal does not need to evaluate access conditions indicated as ADM in the present document.

PIN/ADM: A terminal is required to evaluate the access condition and verify it in order to access the EF if the access condition is set to PIN or PIN2.

EHPLMN: represents the Equivalent HPLMNs for network selection purposes. The behaviour of EHPLMNs is defined in TS 23.122 [31].

3.2 Symbols

For the purposes of the present document, the following symbols apply:

‖	Concatenation
⊕	Exclusive OR
f1	Message authentication function used to compute MAC
f1*	A message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ..., f5 and vice versa
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application Identifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
ASME	Access Security Management Entity
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
BER-TLV	Basic Encoding Rule - TLV
B-TID	Bootstrapping Transaction Identifier
CCP	Capability Configuration Parameter

CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
EPS	Evolved Packet System
FCP	File Control Parameters
FFS	For Further Study
GSM	Global System for Mobile communications
HE	Home Environment
HNB	Home NodeB
HeNB	Home eNodeB
IARI	IMS Application Reference Identifier
ICC	Integrated Circuit Card
ICE	In Case of Emergency
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	Identifier
Idi	Identity of the initiator
Idr	Identity of the responder
IEI	Information Element Identifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MBMS	Multimedia Broadcast/Multicast Service
MCC	Mobile Country Code
MexE	Mobile Execution Environment
MF	Master File
MGV-F	MTK Generation and Validation Function
MIKEY	Multimedia Internet KEYing
MM	Multimedia Message
MMI	Man Machine Interface
MMS	Multimedia Messaging Service
MMSS	MultiMode System Selection
MNC	Mobile Network Code
MODE	Indication packet switched/circuit switched mode
MSB	Most Significant Bit
MSK	MBMS Service Key
MTK	MBMS Traffic Key
MUK	MBMS User Key
NEV	NEVer
NPI	Numbering Plan Identifier
OCI	Outgoing Call Information
OCT	Outgoing Call Timer
PBID	Phonebook Identifier
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet switched
PS_DO	PIN Status Data Object
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM

RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment
SEQp	Sequence number for MGV-F stored in the USIM
SFI	Short EF Identifier
SGSN	Serving GPRS Support Node
SN	Serving Network
SQN	Sequence number
SRES	Signed RESponse calculated by a USIM
SW	Status Word
TLV	Tag Length Value
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
WLAN	Wireless Local Area Network
WSID	WLAN Specific Identifier
XRES	Expected user RESponse

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to TS 31.101 [11].

'XX':	Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4 Contents of the Files

This clause specifies the Efs for the 3GPP session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in an EF_{ADN} record.

A file is associated with attributes that depending of the file type indicates how data is to be accessed e.g. file size, record length etc. Although in the present document some files and data items stored in a file are indicated as having a fixed length; when reading such structures the terminal shall derive the length of the data item from the attributes provided in the file information i.e. not use the fixed value specified for the file in the present document. Although the terminal is able to read the entire structure it should only use those elements in the data item which is recognised by the terminal.

For any EF, when the SFI is not indicated in the description of the file it is not allowed to assign an SFI. If in the description of the file an SFI value is indicated the file shall support SFI. The SFI value shall be assigned by the card issuer. It is mandatory for Efs stating an SFI value ('YY') in the description of their structure to provide an SFI. For files where in the file description the SFI is indicated as 'Optional' the file may support an SFI.

For an overview containing all files see figures 4.1 and 4.2.

4.1 Contents of the Efs at the MF level

There are four Efs at the Master File (MF) level. These Efs are specified in TS 31.101 [11].

The information in EF_{PL} may be used by the ME for MMI purposes.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is available, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{LI,}$ whichever of these Efs is used (see clause 5.1.1). The CB message language is defined by the Data Coding Scheme (see TS 23.038 [5]) received with the CB message. The ME shall be

responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [5]) to the language coding as defined in ISO 639 [19] if it is necessary to check the language coding in EF_{PL}.

4.2 Contents of files at the USIM ADF (Application DF) level

The Efs in the USIM ADF contain service and network related information.

The File Ids '6F1X' (for Efs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the USIM ADF for administrative use by the card issuer.

4.2.1 EF_{LI} (Language Indication)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes. This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is available, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{PL,}$ whichever of these Efs is used (see clause 5.1.1). The CB message language is defined by the Data Coding Scheme (DCS: see TS 23.038 [5]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [5]) to the language coding as defined in ISO 639 [19] if it is necessary to check the language coding in EF_{PL}.

Identifier: '6F 05'	Structure: transparent	Optional
SFI: '02'		
File size: 2n bytes, (n ≥ 1)	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	1st language code (highest priority).	M	2 bytes
3 to 4	2nd language code	O	2 bytes
2n-1 to 2n	Nth language code (lowest priority).	O	2 bytes

Coding:

each language code is a pair of alpha-numeric characters, defined in ISO 639 [19]. Each alpha-numeric character shall be coded on one byte using the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0.

Unused language entries shall be set to 'FF FF'.

4.2.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent	Mandatory
SFI: '07'		
File size: 9 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

- Length of IMSI

Contents:
- the length indicator refers to the number of significant bytes, not including this length byte, required for the IMSI.

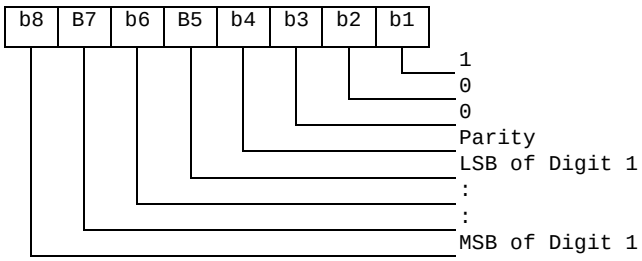
Coding:
- according to TS 24.008 [9].

- IMSI

Contents:
- International Mobile Subscriber Identity.

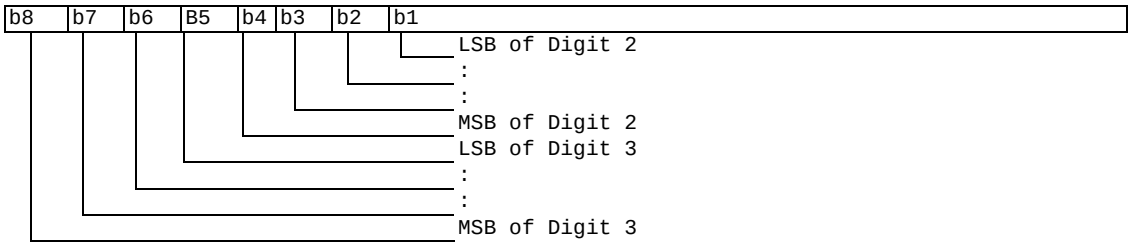
Coding:
- this information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:



For the parity bit, see TS 24.008 [9].

Byte 3:



etc.

4.2.3 EF_{Keys} (Ciphering and Integrity Keys)

This EF contains the ciphering key CK, the integrity key IK and the key set identifier KSI.

Identifier: '6F08'	Structure: transparent	Mandatory
SFI: '08'		
File size: 33 bytes	Update activity: high	

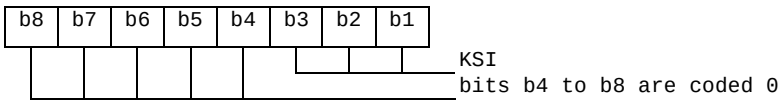
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Key set identifier KSI	M	1 byte
2 to 17	Ciphering key CK	M	16 bytes
18 to 33	Integrity key IK	M	16 bytes

- Key Set Identifier KSI.

Coding:



- Ciphering key CK.

Coding:

- the least significant bit of CK is the least significant bit of the 17th byte. The most significant bit of CK is the most significant bit of the 2nd byte.

- Integrity key IK.

Coding:

- the least significant bit of IK is the least significant bit of the 33rd byte. The most significant bit of IK is the most significant bit of the 18th byte.

4.2.4 EF_{KeysPS} (Ciphering and Integrity Keys for Packet Switched domain)

This EF contains the ciphering key CKPS, the integrity key IKPS and the key set identifier KSIPS for the packet switched (PS) domain.

Identifier: '6F09'	Structure: transparent	Mandatory
SFI: '09'		
File size: 33 bytes	Update activity: high	

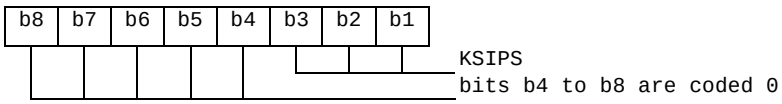
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Key set identifier KSIPS	M	1 byte
2 to 17	Ciphering key CKPS	M	16 bytes
18 to 33	Integrity key IKPS	M	16 bytes

- Key Set Identifier KSIPS.

Coding:



- Ciphering key CKPS.

Coding:

- the least significant bit of CKPS is the least significant bit of the 17th byte. The most significant bit of CKPS is the most significant bit of the 2nd byte.
- Integrity key IKPS.

Coding:

- the least significant bit of IKPS is the least significant bit of the 33rd byte. The most significant bit of IKPS is the most significant bit of the 18th byte.

4.2.5 $EF_{PLMNwAcT}$ (User controlled PLMN selector with Access Technology)

If service n° 20 is "available", this file shall be present.

This EF contains the coding for n PLMNs, where n is at least eight. This information is determined by the user and defines the preferred PLMNs of the user in priority order. The first record indicates the highest priority and the nth record indicates the lowest. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [31])

Identifier: '6F60'	Structure: transparent	Optional
SFI: '0A'		
File size: 5n (where n ≥8 bytes)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	M	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes
41 to 43	9th PLMN	O	3 bytes
44 to 45	9th PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	Nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	Nth PLMN Access Technology Identifier	O	2 bytes

- PLMN

Contents:

- Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

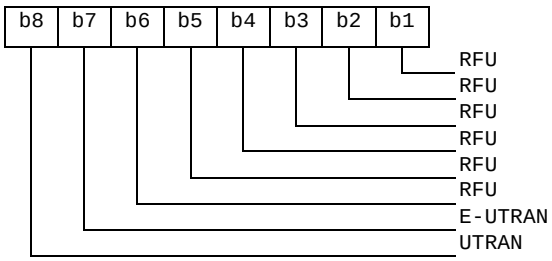
Coding:

- according to TS 24.008 [9].
- Access Technology Identifier:

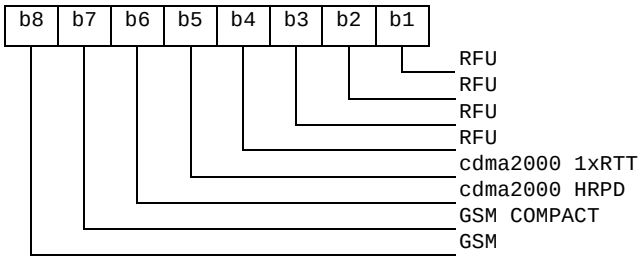
Coding:

- 2 bytes are used to select the access technology where the meaning of each bit is as follows:
  - bit = 1: access technology selected;
  - bit = 0: access technology not selected.

Byte5n-1:



Byte 5n:



4.2.6 EF_{HPPLMN} (Higher Priority PLMN search period)

This EF contains the interval of time between searches for a higher priority PLMN (see TS 22.011 [2]).

Identifier: '6F31'	Structure: transparent	Mandatory
SFI: '12'		
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Time interval	M	1 byte

- Time interval.

Contents:

the time interval between two searches.

Coding:

the time interval is coded in integer multiples of n minutes. The range is from n minutes to a maximum value. The value '00' indicates that no attempts shall be made to search for any higher priority PLMN. The encoding is:

- '00': No higher priority PLMN search attempts;
- '01': n minutes;
- '02': 2n minutes;
- : :
- 'YZ': (16Y+Z)n minutes (maximum value).

- All other values shall be interpreted by the ME as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to TS 22.011 [2].

4.2.7 EF_{ACMmax} (ACM maximum value)

If service n° 13 is "available", this file shall be present.

This EF contains the maximum value of the accumulated call meter.

Identifier: '6F37'	Structure: transparent	Optional
File size: 3 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Maximum value	M	3 bytes

- Maximum value.

Contents:

- maximum value of the Accumulated Call Meter (ACM).

Coding:

First byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Second byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Third byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For instance, '00' '00' '30' represents 2^5+2^4.

All ACM data is stored in the USIM and transmitted over the USIM/ME interface as binary.

ACMmax is not valid, as defined in TS 22.024 [3], if it is coded '000000'.

If a GSM application is present on the UICC and the ACMmax value is to be shared between the GSM and the USIM application this file shall be shared between the two applications.

4.2.8 EF_{UST} (USIM Service Table)

This EF indicates which services are available. If a service is not indicated as available in the USIM, the ME shall not select this service.

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, (X ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:

Service n°1:	Local Phone Book
Service n°2:	Fixed Dialling Numbers (FDN)
Service n°3:	Extension 2
Service n°4:	Service Dialling Numbers (SDN)
Service n°5:	Extension3
Service n°6:	Barred Dialling Numbers (BDN)
Service n°7:	Extension4
Service n°8:	Outgoing Call Information (OCI and OCT)
Service n°9:	Incoming Call Information (ICI and ICT)
Service n°10:	Short Message Storage (SMS)
Service n°11:	Short Message Status Reports (SMSR)
Service n°12:	Short Message Service Parameters (SMSP)
Service n°13:	Advice of Charge (AoC)
Service n°14:	Capability Configuration Parameters 2 (CCP2)
Service n°15:	Cell Broadcast Message Identifier
Service n°16:	Cell Broadcast Message Identifier Ranges
Service n°17:	Group Identifier Level 1
Service n°18:	Group Identifier Level 2
Service n°19:	Service Provider Name
Service n°20:	User controlled PLMN selector with Access Technology
Service n°21:	MSISDN
Service n°22:	Image (IMG)
Service n°23:	Support of Localised Service Areas (SoLSA)
Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
Service n°25:	Automatic Answer for eMLPP
Service n°26:	RFU
Service n°27:	GSM Access
Service n°28:	Data download via SMS-PP
Service n°29:	Data download via SMS-CB
Service n°30:	Call Control by USIM
Service n°31:	MO-SMS Control by USIM
Service n°32:	RUN AT COMMAND command
Service n°33:	shall be set to '1'
Service n°34:	Enabled Services Table
Service n°35:	APN Control List (ACL)
Service n°36:	Depersonalisation Control Keys
Service n°37:	Co-operative Network List
Service n°38:	GSM security context
Service n°39:	CPBCCH Information
Service n°40:	Investigation Scan
Service n°41:	MexE

Service n°42:	Operator controlled PLMN selector with Access Technology
Service n°43:	HPLMN selector with Access Technology
Service n°44:	Extension 5
Service n°45:	PLMN Network Name
Service n°46:	Operator PLMN List
Service n°47:	Mailbox Dialling Numbers
Service n°48:	Message Waiting Indication Status
Service n°49:	Call Forwarding Indication Status
Service n°50:	Reserved and shall be ignored
Service n°51:	Service Provider Display Information
Service n°52	Multimedia Messaging Service (MMS)
Service n°53	Extension 8
Service n°54	Call control on GPRS by USIM
Service n°55	MMS User Connectivity Parameters
Service n°56	Network's indication of alerting in the MS (NIA)
Service n°57	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
Service n°58	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
Service n°59	Pseudonym
Service n°60	User Controlled PLMN selector for I-WLAN access
Service n°61	Operator Controlled PLMN selector for I-WLAN access
Service n°62	User controlled WSID list
Service n°63	Operator controlled WSID list
Service n°64	VGCS security
Service n°65	VBS security
Service n°66	WLAN Reauthentication Identity
Service n°67	Multimedia Messages Storage
Service n°68	Generic Bootstrapping Architecture (GBA)
Service n°69	MBMS security
Service n°70	Data download via USSD and USSD application mode
Service n°71	Equivalent HPLMN
Service n°72	Additional TERMINAL PROFILE after UICC activation
Service n°73	Equivalent HPLMN Presentation Indication
Service n°74	Last RPLMN Selection Indication
Service n°75	OMA BCAST Smart Card Profile
Service n°76	GBA-based Local Key Establishment Mechanism
Service n°77	Terminal Applications
Service n°78	Service Provider Name Icon
Service n°79	PLMN Network Name Icon
Service n°80	Connectivity Parameters for USIM IP connections
Service n°81	Home I-WLAN Specific Identifier List
Service n°82	I-WLAN Equivalent HPLMN Presentation Indication
Service n°83	I-WLAN HPLMN Priority Indication
Service n°84	I-WLAN Last Registered PLMN
Service n°85	EPS Mobility Management Information
Service n°86	Allowed CSG Lists and corresponding indications
Service n°87	Call control on EPS PDN connection by USIM
Service n°88	HPLMN Direct Access
Service n°89	eCall Data
Service n°90	Operator CSG Lists and corresponding indications
Service n°91	Support for SM-over-IP
Service n°92	Support of CSG Display Control
Service n°93	Communication Control for IMS by USIM
Service n°94	Extended Terminal Applications
Service n°95	Support of UICC access to IMS
Service n°96	Non-Access Stratum configuration by USIM
Service n°97	PWS configuration by USIM

The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of the 3GPP.

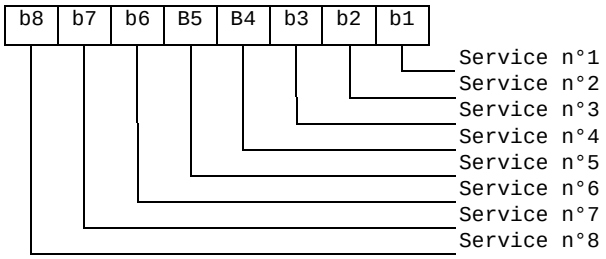
Service n°95 shall not be declared "available" if an ISIM application is present on the UICC.

Coding:

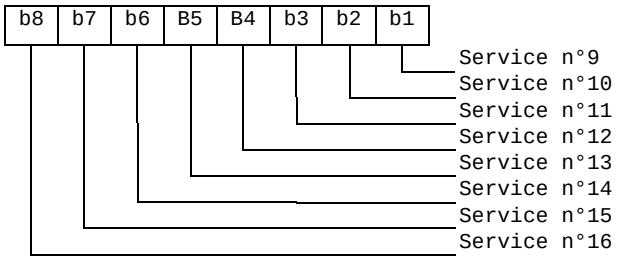
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

4.2.9 EF_{ACM} (Accumulated Call Meter)

If service n° 13 is "available", this file shall be present.

This EF contains the total number of units for both the current call and the preceding calls.

NOTE: The information may be used to provide an indication to the user for advice or as a basis for the calculation of the monetary cost of calls (see TS 22.086 [15]).

Identifier: '6F39'	Structure: cyclic	Optional
SFI: Optional		
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated count of units	M	3 bytes

NOTE: If a SFI is assigned, the recommended value is ‘1C’. However cards may exist that indicate another value. Therefore the terminal shall be able to handle other values.

- Accumulated count of units

Contents:
value of the ACM.
Coding:
see the coding of EF_{ACMmax}.

If a GSM application is present on the UICC and the ACM value is to be shared between the GSM and the USIM application this file shall be shared between the two applications.

4.2.10 EF_{GID1} (Group Identifier Level 1)

If service n° 17 is "available", this file shall be present.

This EF contains identifiers for particular USIM-ME associations. It can be used to identify a group of USIMs for a particular application.

Identifier: '6F3E'	Structure: transparent	Optional
File size: n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

4.2.11 EF_{GID2} (Group Identifier Level 2)

If service n° 18 is "available", this file shall be present.

This EF contains identifiers for particular USIM-ME associations. It can be used to identify a group of USIMs for a particular application.

Identifier: '6F3F'	Structure: transparent	Optional
File size: n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

NOTE: The structure of EF_{GID1} and EF_{GID2} is identical. They are provided to allow the network operator to enforce different levels of security dependant on an application.

4.2.12 EF_{SPN} (Service Provider Name)

If service n° 19 is "available", this file shall be present.

This EF contains the service provider name in text format and appropriate requirements for the display by the ME. The service provider name may also be provided in a graphical format in EF_{SPNI}. The ME shall use the service provider name in the text format or the graphical format or both to display the service provider name according to the rules defined in section 4.2.88.

Identifier: '6F46'	Structure: transparent	Optional
File Size: 17 bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Display Condition	M	1 byte
2 to 17	Service Provider Name	M	16 bytes

- Display Condition

Contents: display condition for the service provider name in respect to the registered PLMN (see TS 22.101 [24]).
Coding:

b8	b7	b6	b5	b4	b3	b2	b1

b1=0: display of registered PLMN name not required when registered PLMN is either HPLMN or a PLMN in the service provider PLMN list (see EF_{SPDI}).
B1=1: display of registered PLMN name required when registered PLMN is either HPLMN or a PLMN in the service provider PLMN list(see EF_{SPDI}).
B2=0: display of the service provider name is required when registered PLMN is neither HPLMN nor a PLMN in the service provider PLMN list(see EF_{SPDI}).
B2=1: display of the service provider name is not required when registered PLMN is neither HPLMN nor a PLMN in the service provider PLMN list(see EF_{SPDI}).
RFU (see TS 31.101)

- Service Provider Name

Contents:

service provider string

Coding:
the string shall use:

- either the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'.
- or one of the UCS2 code options defined in the annex of TS 31.101 [11].

4.2.13 EF_{PUCT} (Price per Unit and Currency Table)

If service n° 13 is "available", this file shall be present.

This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in TS 22.024 [3].

Identifier: '6F41'	Structure: transparent	Optional
File size: 5 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Currency code	M	3 bytes
4 to 5	Price per unit	M	2 bytes

- Currency code

Contents:
the alpha-identifier of the currency code.

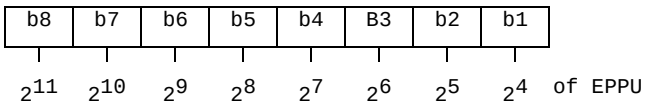
Coding:
bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0.

- Price per unit

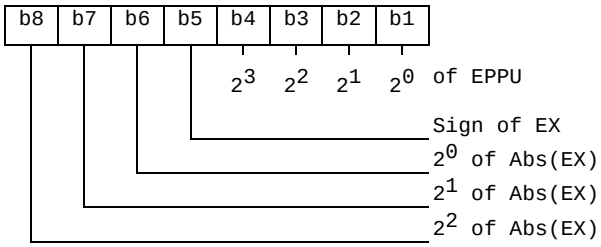
Contents:
price per unit expressed in the currency coded by bytes 1 to 3.

Coding:
byte 4 and bits b1 to b4 of byte 5 represent the Elementary Price per Unit (EPPU) in the currency coded by bytes 1 to 3. Bits b5 to b8 of byte 5 are the decimal logarithm of the multiplicative factor represented by the absolute value of its decimal logarithm (EX) and the sign of EX, which is coded 0 for a positive sign and 1 for a negative sign.

Byte 4:



Byte 5:



- The computation of the price per unit value is made by the ME in compliance with TS 22.024 [3] by the following formula:

price per unit = EPPU * 10^{EX}.

- The price has to be understood as expressed in the coded currency.

If a GSM application is present on the UICC and the PUCT information is to be shared between the GSM and the USIM application, then this file shall be shared between the two applications.

4.2.14 EF_{CBMI} (Cell Broadcast Message identifier selection)

If service n° 15 is "available", this file shall be present.

This EF contains the Message Identifier Parameters which specify the type of content of the cell broadcast messages that the subscriber wishes the UE to accept.

Any number of CB Message Identifier Parameters may be stored in the USIM. No order of priority is applicable.

Identifier: '6F45'	Structure: transparent	Optional
File size: 2 n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes

3 to 4	CB Message Identifier 2	O	2 bytes
:	:	:	:
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier

Coding:
- as in TS 23.041 [16], "Message Format on BTS-MS Interface - Message Identifier";
- values listed show the types of message which shall be accepted by the UE;
- unused entries shall be set to 'FF FF'.

4.2.15 EF_{ACC} (Access Control Class)

This EF contains the assigned access control class(es). The access control class is a parameter to control the access attempts. 15 classes are split into 10 classes randomly allocated to normal subscribers and 5 classes allocated to specific high priority users. For more information see TS 22.011 [2].

Identifier: '6F78'	Structure: transparent	Mandatory
SFI: '06'		
File size: 2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Access control classes	M	2 bytes

- Access control classes

Coding:
- each ACC is coded on one bit. An ACC is "allocated" if the corresponding bit is set to 1 and "not allocated" if this bit is set to 0. Bit b3 of byte 1 is set to 0.

Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1	
15	14	13	12	11	10	09	08	Number of the ACC (except for bit b3)

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	
07	06	05	04	03	02	01	00	Number of the ACC

4.2.16 EF_{FPLMN} (Forbidden PLMNs)

This EF contains the coding for n Forbidden PLMNs (FPLMN). It is read by the ME as part of the USIM initialization procedure and indicates PLMNs which the UE shall not automatically attempt to access.

A PLMN is written to the EF if a network rejects a Location Update with the cause "PLMN not allowed". The ME shall manage the list as follows.

When n FPLMNs are held in the EF, and rejection of a further PLMN is received by the ME from the network, the ME shall modify the EF using the UPDATE command. This new PLMN shall be stored in the nth position, and the existing list "shifted" causing the previous contents of the first position to be lost.

When less than n FPLMNs exist in the EF, storage of an additional FPLMN shall not cause any existing FPLMN to be lost.

Dependent upon procedures used to manage storage and deletion of FPLMNs in the EF, it is possible, when less than n FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The ME shall analyse all the EF for FPLMNs in any position, and not regard 'FFFFFF' as a termination of valid data.

Identifier: '6F7B'	Structure: transparent	Mandatory
SFI: '0D'		
File size: 3n bytes, (n≥ 4)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	PLMN 1	M	3 bytes
4 to 6	PLMN 2	M	3 bytes
7 to 9	PLMN 3	M	3 bytes
10 to 12	PLMN 4	M	3 bytes
:	:	:	:
(3n-2) to 3n	PLMN n	O	3 bytes

- PLMN

Contents:

Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:

according to TS 24.008 [9].

For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:

Bytes 7 to 9: '42' 'F6' '18'.

If storage for fewer than n PLMNs is required, the unused bytes shall be set to 'FF'.

4.2.17 EF_{LOCI} (Location Information)

This EF contains the following Location Information:

- Temporary Mobile Subscriber Identity (TMSI);
- Location Area Information (LAI);
- Location update status.

See clause 5.2.5 for special requirements when updating EF_{LOCI}.

Identifier: '6F7E'	Structure: transparent	Mandatory
SFI: '0B'		
File size: 11 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	TMSI	M	4 bytes
5 to 9	LAI	M	5 bytes
10	RFU	M	1 byte
11	Location update status	M	1 byte

- TMSI

Contents:

Temporary Mobile Subscriber Identity.

Coding:

according to TS 24.008 [9].

B8	b7	b6	b5	b4	B3	b2	b1
MSB							

- LAI

Contents:
Location Area Information.

Coding:
according to TS 24.008 [9].

Byte 5: first byte of LAI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- Location update status

Contents:
status of location update according to TS 24.008 [9].

Coding:
Byte 11:

Bits:	b3	b2	b1	
	0	0	0	: updated.
	0	0	1	: not updated.
	0	1	0	: PLMN not allowed.
	0	1	1	: Location Area not allowed.
	1	1	1	: reserved.

Bits b4 to b8 are RFU (see TS 31.101 [11]).

4.2.18 EF_{AD} (Administrative Data)

This EF contains information concerning the mode of operation according to the type of USIM, such as normal (to be used by PLMN subscribers for 3G operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication about how some ME features shall work during normal operation as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

Identifier: '6FAD'	Structure: transparent	Mandatory
SFI: '03'		
File size: 4+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	UE operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	M	1 byte
5 to 4+X	RFU	O	X bytes

- UE operation mode:

Contents:
mode of operation for the UE

Coding:

Initial value

- '00' normal operation.
- '80' type approval operations.
- '01' normal operation + specific facilities.
- '81' type approval operations + specific facilities.
- '02' maintenance (off line).
- '04' cell test operation.

All other values are RFU

- Additional information:

Contents:

additional information depending on the UE operation mode

Coding:

- specific facilities (if b1=1 in byte 1):

Byte 2 (first byte of additional information):

b8	b7	b6	b5	b4	b3	b2	b1	
								RFU (see TS 31.101)

Byte 3 (second byte of additional information):

b8	b7	b6	b5	b4	b3	b2	b1	
								b1=0: ciphering indicator feature disabled b1=1: ciphering indicator feature enabled
								b2: CSG Display Control bit, see below
								RFU (see TS 31.101)

b1 is used to control the ciphering indicator feature as specified in TS 22.101 [24].

b2 is used to indicate which CSGs the UE shall display during manual CSG selection. This bit corresponds to the value of OperatorCSGEntries_Only leaf described in TS 24.285 [58]. This bit shall be ignored when service n°92 is not "available".

- b2=0: for every PLMN not included in EF_OCSGL, or for which a CSG display indicator tag is not present, all available CSGs can be displayed without any restriction.
- b2=1: for every PLMN not included in EF_OCSGL or any PLMN for which a CSG display indicator tag is not present, only the available CSGs found in the Operator CSG list shall be displayed.

- ME manufacturer specific information (if b2=1 in byte 1):

Byte 2 (first byte of additional information):

B8	b7	b6	B5	B4	b3	b2	b1	
								Any value

Byte 3 (second byte of additional information):

B8	b7	b6	b5	B4	b3	b2	b1	
								Any value

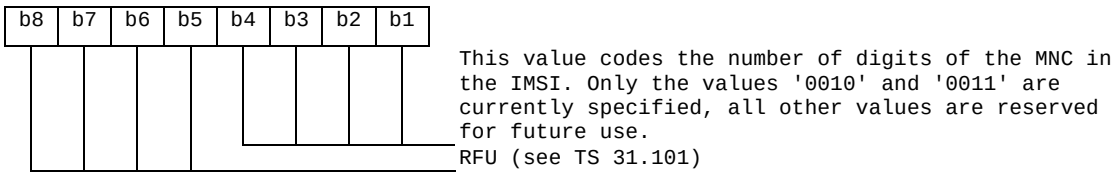
- Length of MNC in the IMSI:

Contents:

The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

Coding:

Byte 4:



4.2.19 Void

4.2.20 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download)

If service n° 29 is "available", this file shall be present.

This EF contains the message identifier parameters which specify the type of content of the cell broadcast messages which are to be passed to the USIM.

Any number of CB message identifier parameters may be stored in the USIM. No order of priority is applicable.

Identifier: '6F48'	Structure: transparent	Optional
SFI: '0E'		
File size: 2n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes
3 to 4	CB Message Identifier 2	O	2 bytes
:	:	:	:
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier.

Coding:

- as in TS 23.041 [16]. Values listed show the identifiers of messages which shall be accepted by the UE to be passed to the USIM.

Unused entries shall be set to 'FF FF'.

4.2.21 EF_{ECC} (Emergency Call Codes)

This EF contains emergency call codes.

Identifier: '6FB7'	Structure: linear fixed	Mandatory
SFI: '01'		
Record size: X+4 bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Emergency Call Code	M	3 bytes
4 to X+3	Emergency Call Code Alpha Identifier	O	X bytes
X+4	Emergency Service Category	M	1 byte

- Emergency Call Code.

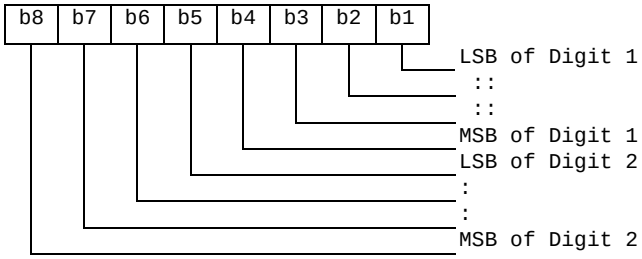
Contents:

- Emergency Call Code.

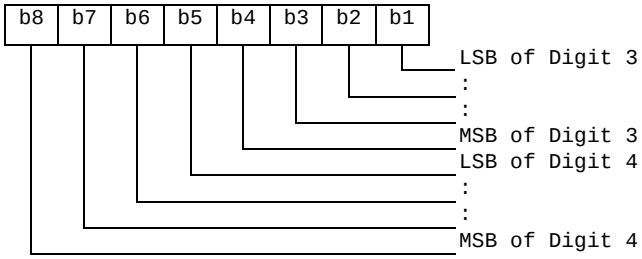
Coding:

- the emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of less than 6 digits is chosen, then the unused nibbles shall be set to 'F'.

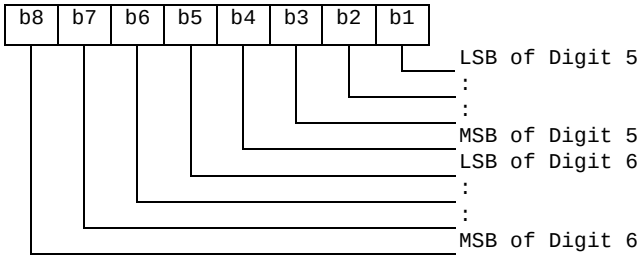
Byte 1:



Byte 2:



Byte 3:



- Emergency Call Code Alpha Identifier.

Contents:

Information about the dialled emergency number to be displayed to the user.

Coding:

this alpha-tagging shall use

either:

- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

Or

- one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

- Emergency Service Category.

Contents:

Information to be sent to the network indicating the category of the emergency call.

Coding:

Coding according to TS 24.008 [9].

4.2.22 EF_{CBMIR} (Cell Broadcast Message Identifier Range selection)

If service n° 16 is "available", this file shall be present.

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the UE to accept.

Any number of CB Message Identifier Parameter ranges may be stored in the USIM. No order of priority is applicable.

Identifier: '6F50'	Structure: transparent	Optional
File size: 4n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	CB Message Identifier Range 1	O	4 bytes
5 to 8	CB Message Identifier Range 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	CB Message Identifier Range n	O	4 bytes

- Cell Broadcast Message Identifier Ranges.

Contents:
- CB Message Identifier ranges:

Coding:
- bytes one and two of each range identifier equal the lower value of a cell broadcast range, bytes three and four equal the upper value of a cell broadcast range, both values are coded as in TS 23.041 [16] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the UE.

Unused entries shall be set to 'FF FF FF FF'.

4.2.23 EF_{PSLOCI} (Packet Switched location information)

This EF contains the following Location Information:

- Packet Temporary Mobile Subscriber Identity (P-TMSI);
- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);
- Routing Area Information (RAI);
- Routing Area update status.

Identifier: '6F73'	Structure: transparent	Mandatory
SFI: '0C'		
File size: 14 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	P-TMSI	M	4 bytes
5 to 7	P-TMSI signature value	M	3 bytes
8 to13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

- P-TMSI.

Contents:
Packet Temporary Mobile Subscriber Identity.

Coding:
according to TS 24.008 [9].

Byte 1: first byte of P-TMSI

b8	b7	B6	B5	B4	B3	b2	b1
MSB							

- P-TMSI signature value.

Contents:
Packet Temporary Mobile Subscriber Identity signature value.

Coding:
according to TS 24.008 [9].

Byte 5: first byte of P-TMSI signature value.

B8	b7	B6	B5	B4	B3	b2	b1
MSB							

- RAI

Contents:
Routing Area Information.

Coding:
according to TS 24.008 [9].

Byte 8: first byte of RAI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- Routing Area update status.

Contents:
status of routing area update according to TS 24.008 [9].

Coding:
byte 14:

Bits:	b3	b2	b1.	
	0	0	0	: updated.
	0	0	1	: not updated.
	0	1	0	: PLMN not allowed.
	0	1	1	: Routing Area not allowed.
	1	1	1	: reserved.

Bits b4 to b8 are RFU (see TS 31.101 [11]).

4.2.24 EF_{FDN} (Fixed Dialling Numbers)

If service n° 2 and/or service n° 89 is "available", this file shall be present.

This EF contains Fixed Dialling Numbers (FDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain an associated alpha-tagging. If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F3B'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 4.4.2.3), with the exception that extension records are stored in the EF_{EXT2}.

By default, destination addresses which are not in EF_{FDN} shall not be allowed on any CS bearer service/teleservice or SMS when FDN is enabled.

For the FDN procedures related to SMS see TS 22.101 [24] and TS 31.111 [12].

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.25 EF_{SMS} (Short messages)

If service n° 10 is "available", this file shall be present.

This EF contains information in accordance with TS 23.040 [6] comprising short messages (and associated parameters) which have either been received by the UE from the network, or are to be used as an UE originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

- Status.

Contents:

Status byte of the record which can be used as a pattern in the SEARCH RECORD command. For UE originating messages sent to the network, the status shall be updated when the UE receives a status report, or sends a successful SMS Command relating to the status report.

Coding:

```
b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1
                        X    X    0   free space
                        X    X    1   used space
                        0    0    1   message received by UE from network; message read
                        0    1    1   message received by UE from network; message to be
                                        read
                        1    1    1   UE originating message; message to be sent

                                      RFU (see TS 31.101 [11])
```

```
b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1
                  X    X    1    0    1   UE originating message; message sent to the network:
                  0    0    1    0    1     Status report not requested
                  0    1    1    0    1     Status report requested but not (yet) received;
                  1    0    1    0    1     Status report requested, received but not stored
                                                 in EF-SMSR;
                  1    1    1    0    1     Status report requested, received and stored
                                                 in EF-SMSR;

                                           RFU (see TS 31.101 [11])
```

- Remainder.

Contents:

This data item commences with the TS-Service-Centre-Address as specified in TS 24.011 [10]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in TS 23.040 [6], with identical coding and ordering of parameters.

Coding:

according to TS 23.040 [6] and TS 24.011 [10]. Any TP-message reference contained in an UE originated message stored in the USIM, shall have a value as follows:

	Value of the TP-message-reference:
message to be sent:	'FF'.
Message sent to the network:	the value of TP-Message-Reference used in the message sent to the network.

Any bytes in the record following the TPDU shall be filled with 'FF'.

It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the USIM the TS-Service-Centre-Address and the TPDU in bytes 2 to 176 without modification, except for the last byte of the TPDU, which shall not be stored.

4.2.26 EF_{MSISDN} (MSISDN)

If service n° 21 is "available", this file shall be present.

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain an associated alpha-tagging.

Identifier: '6F40'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of EF_{ADN}.

If the USIM stores more than one MSISDN number and the ME displays the MSISDN number(s) within the initialisation procedure then the one stored in the first record shall be displayed with priority.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.27 EF_{SMSP} (Short message service parameters)

If service n° 12 is "available", this file shall be present.

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the UE, the parameter in the USIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier.

Contents:

Alpha Tag of the associated SMS-parameter.

Coding:

see clause 4.4.2.3 (EF_{ADN}).

NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators.

Contents:

each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.

Coding:

allocation of bits:

bit number	Parameter indicated.
1	TP-Destination Address.
2	TS-Service Centre Address.
3	TP-Protocol Identifier.
4	TP-Data Coding Scheme.
5	TP-Validity Period.
6	reserved, set to 1.
7	reserved, set to 1.
8	reserved, set to 1.

Bit value	Meaning.
0	Parameter present.
1	Parameter absent.

- TP-Destination Address.

Contents and Coding:

as defined for SM-TL address fields in TS 23.040 [6].

- TP-Service Centre Address.

Contents and Coding:

as defined for RP-Destination address Centre Address in TS 24.011 [10].

- TP-Protocol Identifier.

Contents and Coding:

as defined in TS 23.040 [6].

- TP-Data Coding Scheme.

Contents and Coding:

as defined in TS 23.038 [5].

- TP-Validity Period.

Contents and Coding:

as defined in TS 23.040 [6] for the relative time format.

4.2.28 EF_{SMSS} (SMS status)

If service n° 10 is "available", this file shall be present.

This EF contains status information relating to the short message service.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

- Last Used TP-MR.

Contents:

- the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in TS 23.040 [6].

Coding:

- as defined in TS 23.040 [6].

- SMS "Memory Capacity Exceeded" Notification Flag.

Contents:

- this flag is required to allow a process of flow control, so that as memory capacity in the UE becomes available, the Network can be informed. The process for this is described in TS 23.040 [6].

Coding:

b1=1 means flag unset; memory capacity available;
b1=0 means flag set;
b2 to b8 are reserved and set to 1.

4.2.29 EF_{SDN} (Service Dialling Numbers)

If service n° 4 and or service n° 89 is "available", this file shall be present.

This EF contains special service numbers (SDN) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain associated alpha-tagging. If the service n° 89 is available this file will contain the eCall test and reconfiguration numbers that are used by an UE in eCall and normal service mode.

Identifier: '6F49'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1-X	Alpha identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 bytes
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension3 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 4.4.2.3), with the exception that extension records are stored in the EF_{EXT3} and capability/configuration parameters are stored in EF_{CCP2}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.30 EF_{EXT2} (Extension2)

If service n° 3 is "available", this file shall be present.

This EF contains extension data of an FDN (see FDN in 4.2.24).

Identifier: '6F4B'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 4.4.2.4 (EF_{EXT1}).

4.2.31 EF_{EXT3} (Extension3)

If service n° 5 is "available", this file shall be present.

This EF contains extension data of an SDN (see SDN in 4.2.29).

Identifier: '6F4C'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 4.4.2.4 (EF_{EXT1}).

4.2.32 EF_{SMSR} (Short message status reports)

If service n° 11 is "available", this file shall be present.

This EF contains information in accordance with TS 23.040 [6] comprising short message status reports which have been received by the UE from the network.

Each record is used to store the status report of a short message in a record of EF_{SMS}. The first byte of each record is the link between the status report and the corresponding short message in EF_{SMS}.

Identifier: '6F47'	Structure: linear fixed	Optional
Record length: 30 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	SMS record identifier	M	1
2 to 30	SMS status report	M	29 bytes

- SMS record identifier.

Contents:

- this data item identifies the corresponding SMS record in EF_{SMS}, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of EF_{SMS}.

Coding:

- '00' - empty record;
- '01' to 'FF' - record number of the corresponding SMS in EF_{SMS}.

- SMS status report:

Contents:

- this data item contains the SMS-STATUS-REPORT TPDU as specified in TS 23.040 [6], with identical coding and ordering of parameters.

Coding:

- according to TS 23.040 [6]. Any bytes in the record following the TPDU shall be filled with 'FF'.

4.2.33 EF_{ICI} (Incoming Call Information)

If service n°9 is "available", this file shall be present.

This EF is located within the USIM application. The incoming call information can be linked to the phone book stored under $DF_{TELECOM}$ or to the local phone book within the USIM. The EF_{ICI} contains the information related to incoming calls.

The time of the call and duration of the call are stored in this EF. This EF can also contain associated alpha identifier that may be supplied with the incoming call. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. The structure of this EF is cyclic, so the contents shall be updated only after a call is disconnected.

If CLI is supported and the incoming phone number matches a number stored in the phone book the incoming call information is linked to the corresponding information in the phone book. If the incoming call matches an entry but is indicated as hidden in the phone book the link is established but the information is not displayed by the ME if the code for the secret entry has not been verified. The ME shall not ask for the secret code to be entered at this point.

Optionally the ME may store the link to phone book entry in the file, so that it does not need to look again for a match in the phone book when it reuses the entry. But the ME will have to check that the incoming call number still exits in the linked phone book entry, as the link might be broken (entry modified). When not used by the ME or no link to the phone book has been found, this field shall be set to 'FFFFFF'.

The first byte of this link is used to identify clearly the phone book location either global (i.e. under $DF_{TELECOM}$) or local (i.e. USIM specific). To allow the reuse of the referring mechanism in further implementation of the phonebook under discussion, this byte can be used to indicate those.

For the current version of the phone book, the phone book entry is identified as follows:

- the record number in the EF_{PBR} which indicates the EF_{ADN} containing the entry;

- the record number inside the indicated EF_{ADN}.

The structure of EF_{ICI} is shown below. Coding scheme is according to EF_{ADN}

Structure of EF_{ICI}

Identifier: '6F80'	Structure: Cyclic	Optional
SFI: '14'		
Record length: X+28 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

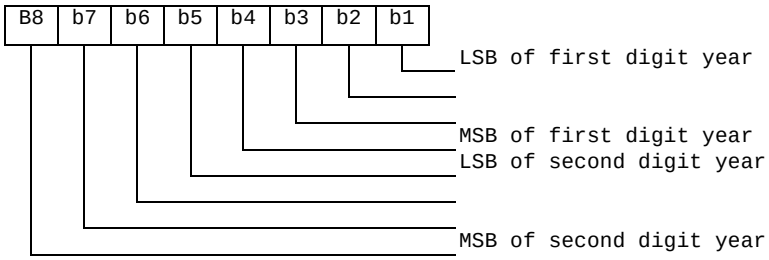
Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Incoming Call Number	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte
X+15 to X+21	Incoming call date and time (see detail 1)	M	7 bytes
X+22 to X+24	Incoming call duration (see detail 2)	M	3 bytes
X+25	Incoming call status (see detail 3)	M	1 byte
X+26 to X+28	Link to phone book entry (see detail 4)	M	3 bytes

NOTE: When the contents except incoming call status are invalid, they are filled with 'FF'.

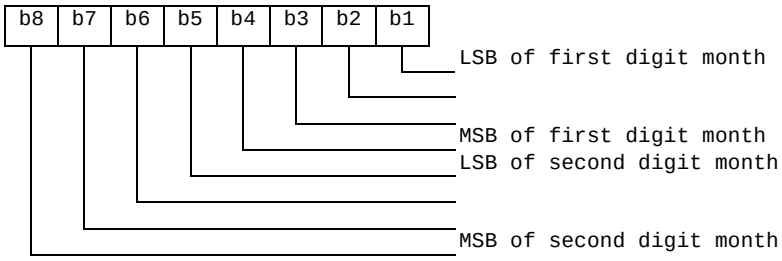
Detail 1 Coding of date and time.

Content:
the date and time are defined by the ME.

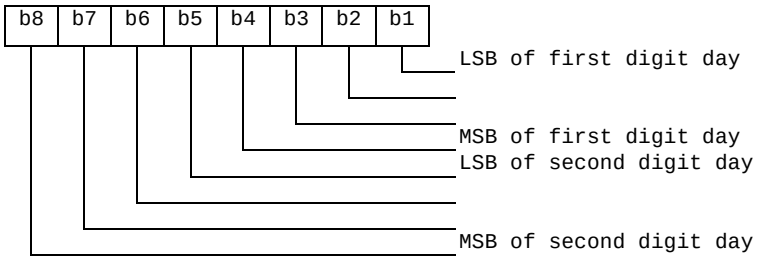
Coding:
it is according to the extended BCD coding from Byte1 to Byte 7. The first 3 bytes show year, month and day (yy.mm.dd). The next 3 bytes show hour, minute and second (hh.mm.ss). The last Byte 7 is Time Zone. The Time Zone indicates the difference, expressed in quarters of an hour, between the local time and GMT. Bit 4 in Byte 7 represents the algebraic sign of this difference (0: positive, 1: negative). If the terminal does not support the Time Zone, Byte 7 shall be "FF". Byte X+15: Year.



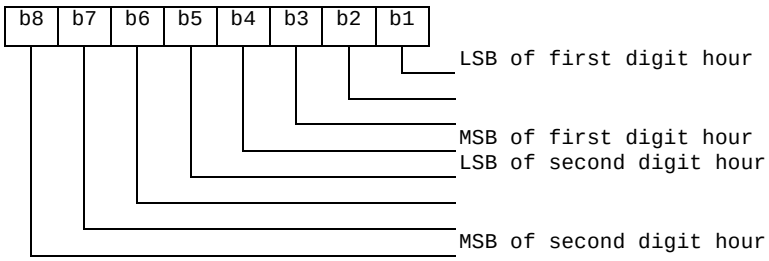
Byte X+16: Month



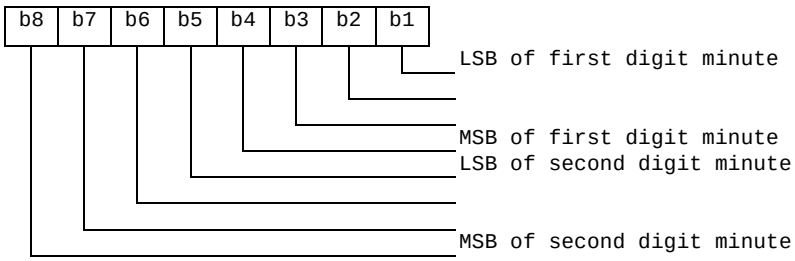
Byte X+17: Day



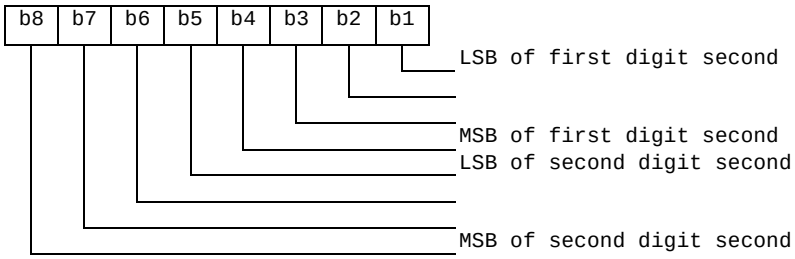
Byte X+18: Hour



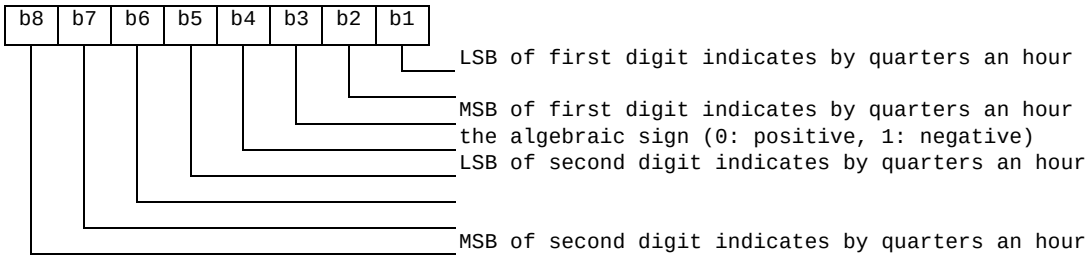
Byte X+19: Minute



Byte X+20: Second



Byte X+21: Time Zone



Detail 2 Coding of call duration.

Call duration is indicated by second.

Byte X+22:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Byte X+23:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Byte X+24:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For instance, '00' '00' '30' represents 2^5+2^4.

Detail 3 Coding of Call status.

Byte X+25:

b8	b7	b6	b5	b4	b3	b2	b1	
								Answered='0'/ Not Answered='1'
								RFU

Detail 4 Link to phone book entry

For the current implementation of the phone book the following coding applies:

Phone book reference.

Byte X+26:

b8	b7	b6	b5	b4	b3	b2	b1	
								0 Global Phone Book ($DF_{TELECOM}$)
								1 Local Phone Book (USIM Specific)
								RFU

EF_{PBR} record number:

- Byte X+27: Hexadecimal value.

EF_{ADN} record number:

- Byte X+28: Hexadecimal value.

4.2.34 EF_{OCI} (Outgoing Call Information)

If service n°8 is "available", this file shall be present.

This EF is located within the USIM application. The outgoing call information can be linked to the phone book stored under $DF_{TELECOM}$ or to the local phone book within the USIM. The EF_{OCI} contains the information related to outgoing calls.

The time of the call and duration of the call are stored in this EF. It may also contain associated alpha identifier. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. The structure of this file is cyclic, so the contents shall be updated only after a call is disconnected.

If the dialled phone number matches a number stored in the phone book the outgoing call information might be linked to the corresponding information in the phone book. The dialled number may match with a hidden entry in the phone

book. If the dialled number matches a hidden entry in the phone book the link is established but the information related to the phone book entry is not displayed by the ME, if the hidden code has not been verified. The ME shall not perform hidden code verification at this point.

Optionally, the ME may store the link to phone book entry in the file, so that it does not need to look again for a match in the phone book when it reuses the entry. But the ME will have to check that the outgoing call number still exists in the linked phone book entry, as the link might be broken (entry modified). When not used by the ME or no link to the phone book has been found, this field shall be set to 'FFFFFF'.

Coding scheme is according to EF_{ICI}.

Structure of EF_{OCI}

Identifier: '6F81'	Structure: Cyclic	Optional
SFI: '15'		
Record length: X+27 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Outgoing Call Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte
X+15 to X+21	Outgoing call date and time	M	7 bytes
X+22 to X+24	Outgoing call duration	M	3 bytes
X+25 to X+27	Link to Phone Book Entry	M	3 bytes

NOTE: When the contents are invalid, they are filled with 'FF'.

4.2.35 EF_{ICT} (Incoming Call Timer)

If service n°9 is "available", this file shall be present.

This EF contains the accumulated incoming call timer duration value for the current call and previous calls. The EF is USIM specific and resides within the USIM application.

This file should have only one entry.

Structure of EF_{ICT}

Identifier: '6F82'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated call timer value	M	3 bytes

Coding:

Accumulated call timer value is indicated by second.

Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For example, '00' '00' '30' represents 2^5+2^4.

4.2.36 EF_{OCT} (Outgoing Call Timer)

If service n°8 is "available", this file shall be present.

This EF contains the accumulated outgoing call timer duration value for the current call and previous calls. The EF is USIM specific and resides within the USIM application. The contents of this EF shall be updated only after a call is disconnected. The coding of this EF is the same as EF_{ICT}.

This file should have only one entry.

Structure of EF_{OCT}

Identifier: '6F83'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated call timer value	M	3 bytes

4.2.37 EF_{EXT5} (Extension5)

If service n° 44 is "available", this file shall be present.

This EF contains extension data of EF_{ICI}, EF_{OCI} and EF_{MSISDN} of the USIM application.

Identifier: '6F4E'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see EF_{EXT1}.

4.2.38 EF_{CCP2} (Capability Configuration Parameters 2)

If service n° 14 is "available", this file shall be present.

This EF contains parameters of required network and bearer capabilities and terminal configurations associated with a call established using a fixed dialling number, a barred dialling number, an MSISDN, a service dialling number, an incoming call, an outgoing call or an MBDN. It is referred by EF_{FDN}, EF_{BDN}, EF_{MSISDN}, EF_{SDN}, EF_{ICI}, EF_{OCI}, EF_{MBDN} and EF_{CFIS} at USIM ADF level.

Identifier: '6F4F'	Structure: linear fixed	Optional
SFI: '16'		
Record length: X bytes, X≥15	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information elements.

- Contents and Coding:
- see TS 24.008 [9]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the EF_{CCP2} record shall be Length of the bearer capability contents.
- unused bytes are filled with 'FF'.

4.2.39 EF_{eMLPP} (enhanced Multi Level Precedence and Pre-emption)

If service n° 24 is "available", this file shall be present.

This EF contains information about priority levels and fast call set-up conditions for the enhanced Multi Level Precedence and Pre-emption service that can be used by the subscriber.

Identifier: '6FB5'	Structure: transparent	Optional
File size: 2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Priority levels	M	1 byte
2	Fast call set-up conditions	M	1 byte

- Priority levels.

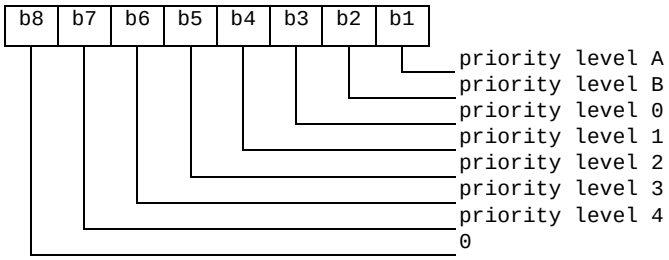
Contents:

- the eMLPP priority levels subscribed to.

Coding:

- each eMLPP priority level is coded on one bit. Priority levels subscribed to have their corresponding bits set to 1. Priority levels not subscribed to have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



NOTE: Priority levels A and B can not be subscribed to (see TS 22.067 [5] for details).

EXAMPLE 1: If priority levels 0, 1 and 2 are subscribed to, EF_{eMLPP} shall be coded '1C'.

- Fast call set-up conditions.

Contents:

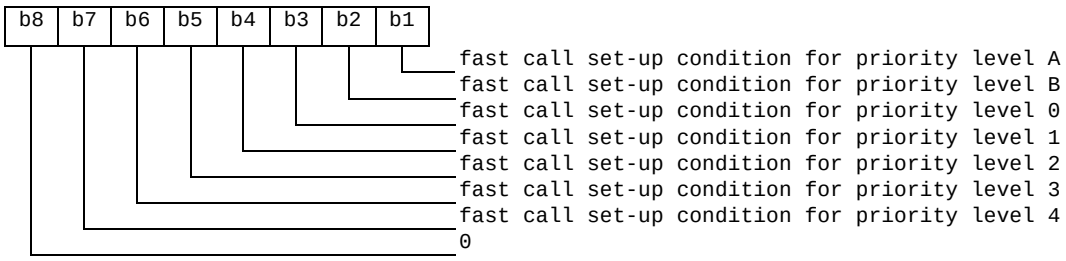
for each eMLPP priority level, the capability to use a fast call set-up procedure.

Coding:

each eMLPP priority level is coded on one bit. Priority levels for which fast call set-up is allowed have their corresponding bits set to 1. Priority levels for which fast call set-up is not allowed have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 2: fast call set-up condition for:

`



EXAMPLE 2: If fast call set-up is allowed for priority levels 0, and 1, then byte 2 of EF_{eMLPP} is coded '0C'.

4.2.40 EF_{AaeM} (Automatic Answer for eMLPP Service)

If service n° 25 is "available", this file shall be present.

This EF contains those priority levels (of the Multi Level Precedence and Pre-emption service) for which the ME shall answer automatically to incoming calls.

Identifier: '6FB6'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Automatic answer priority levels	M	1 byte

- Automatic answer priority levels.

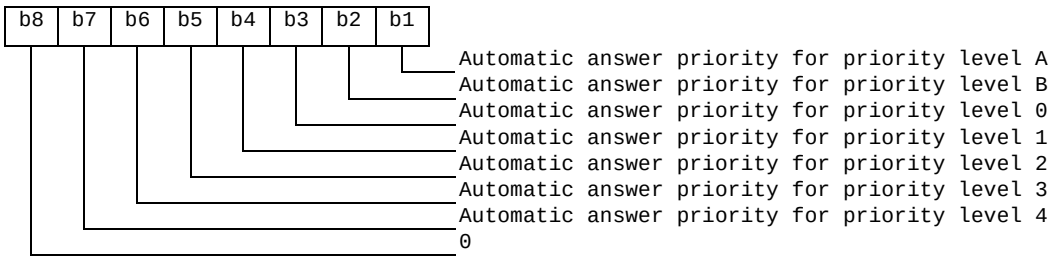
Contents:

- for each eMLPP priority level, the capability for the mobile station to answer automatically to incoming calls (with the corresponding eMLPP priority level).

Coding:

- each eMLPP priority level is coded on one bit. Priority levels allowing an automatic answer from the mobile station have their corresponding bits set to 1. Priority levels not allowing an automatic answer from the mobile station have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



EXAMPLE: If automatic answer is allowed for incoming calls with priority levels A, 0 and 1, then EF_{AaeM} is coded '0D'.

4.2.41 Void

4.2.42 $EF_{Hiddenkey}$ (Key for hidden phone book entries)

This EF contains the hidden key that has to be verified by the ME in order to display the phone book entries that are marked as hidden. The hidden key can consist of 4 to 8 digits.

Identifier: '6FC3'	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Hidden Key	M	4 bytes

- Hidden Key.

Coding:

- the hidden key is coded on 4 bytes using BCD coding. The minimum number of digits is 4. Unused digits are padded with 'F'.

NOTE 1: Digits are not swapped, i.e. for instance the key "1234" is coded as '12 34 FF FF'.

NOTE 2: The phone book entries marked as hidden are not scrambled by means of the hidden key. They are stored in plain text in the phone book.

4.2.43 Void

4.2.44 EF_{BDN} (Barred Dialling Numbers)

If service n° 6 is "available", this file shall be present.

This EF contains Barred Dialling Numbers (BDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging. As the BDN service relies on the Call Control feature, BDN shall only be available if Call Control is available. If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F4D'	Structure: linear fixed	Optional
Record length: X+15 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension4 Record Identifier	M	1 byte
X+15	Comparison Method Pointer	M	1 byte

For contents and coding of all data items, except for the Comparison Method Pointer, see the respective data items of EF_{ADN}, with the exception that extension records are stored in the EF_{EXT4} and capability/configuration parameters are stored in EF_{CCP2}. The Comparison Method Pointer refers to a record number in EF_{CMI}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.45 EF_{EXT4} (Extension4)

If service n° 7 is "available", this file shall be present.

This EF contains extension data of a BDN/SSC.

Identifier: '6F55'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 4.4.2.4 EF_{EXT1}.

4.2.46 EF_{CMI} (Comparison Method Information)

If service n° 6 is "available", this file shall be present.

This EF contains the list of Comparison Method Identifiers and alpha-tagging associated with BDN entries (see EF_{BDN}).

Identifier: '6F58'	Structure: linear fixed	Optional
Record length: X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	M	X bytes
X+1	Comparison Method Identifier	M	1 byte

- Alpha Identifier.
  Contents:
  Alpha-tagging of the associated Comparison Method Identifier.

  Coding:
  Same as the alpha identifier in EF_{ADN}.

- Comparison Method Identifier.

Contents:
- this byte describes the comparison method which is associated with a BDN record. Its interpretation is not specified but it shall be defined by the card issuers implementing the BDN feature on their USIMs.

Coding:
- binary; values from 0 to 255 are allowed.

The default coding 255 is reserved for empty field.

4.2.47 EF_{EST} (Enabled Services Table)

If service n° 2, 6, 34 or 35 is "available" (as indicated in the USIM Service Table), this file shall be present.

This EF indicates which services are enabled. If a service is not indicated as enabled in this table, the ME shall not select the service.

Identifier: '6F56'	Structure: transparent	Optional
SFI: '05'		
File size: X bytes, (X ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:	Service n°1:	Fixed Dialling Numbers (FDN)
	Service n°2:	Barred Dialling Numbers (BDN)
	Service n°3:	APN Control List (ACL)

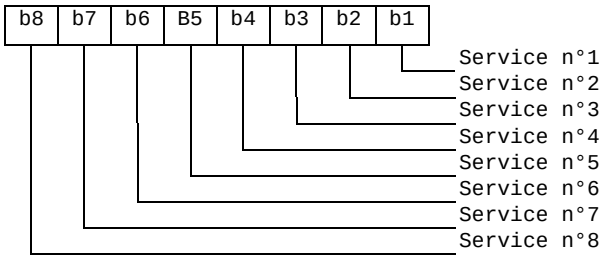
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then the EF shall also contain all bytes before that byte. Other services are possible in the future. The coding falls under the responsibility of the 3GPP.

Coding:

- 1 bit is used to code each service:
  - bit = 1: service activated;
  - bit = 0: service deactivated.
  - Unused bits shall be set to '0'.

A service which is listed in this table is enabled if it is indicated as available in the USIM Service Table (UST) and indicated as activated in the Enabled Services Tables (EST) otherwise this service is, either not available or disabled.

First byte:



etc.

4.2.48 EF_{ACL} (Access Point Name Control List)

If service n° 35 is "available", this file shall be present.

This EF contains the list of allowed APNs (Access Point Names). If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F57'	Structure: transparent	Optional
File size: X bytes (X>1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Number of APNs	M	1 byte
2 to X	APN TLVs	M	X-1 byte

For contents and coding of APN-TLV values see TS 23.003 [25]. The tag value of the APN-TLV shall be 'DD'. "Network provided APN" is coded with a TLV object of length zero.

4.2.49 EF_{DCK} (Depersonalisation Control Keys)

If service n° 36 is "available", this file shall be present.

This EF provides storage for the de-personalization control keys associated with the OTA de-personalization cycle of TS 22.022 [27].

Identifier: '6F2C'	Structure: transparent	Optional
File Size: 16 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	8 digits of network de-personalization control key	M	4 bytes
5 to 8	8 digits of network subset de-personalization control key	M	4 bytes
9 to 12	8 digits of service provider de-personalization control key	M	4 bytes
13 to 16	8 digits of corporate de-personalization control key	M	4 bytes

Empty control key bytes shall be coded 'FFFFFFFF'.

4.2.50 EF_{CNL} (Co-operative Network List)

If service n° 37 is "available", this file shall be present.

This EF contains the Co-operative Network List for the multiple network personalization services defined in TS 22.022 [27].

Identifier: '6F32'	Structure: transparent	Optional
File size: 6n bytes, (n ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 6	Element 1 of co-operative net list	M	6 bytes
:	:	:	:
6n-5 to 6n	Element n of co-operative net list	O	6 bytes

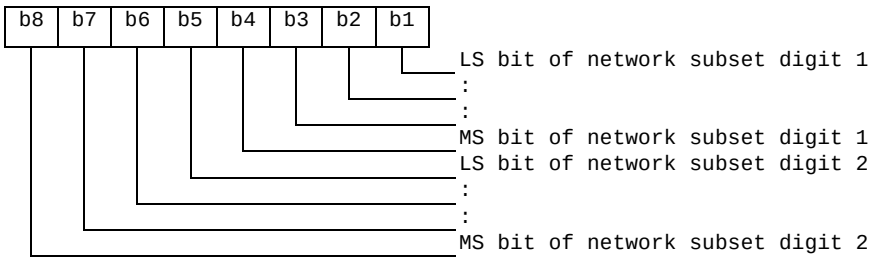
- Co-operative Network List.

Contents:
- PLMN network subset, service provider ID and corporate ID of co-operative networks.

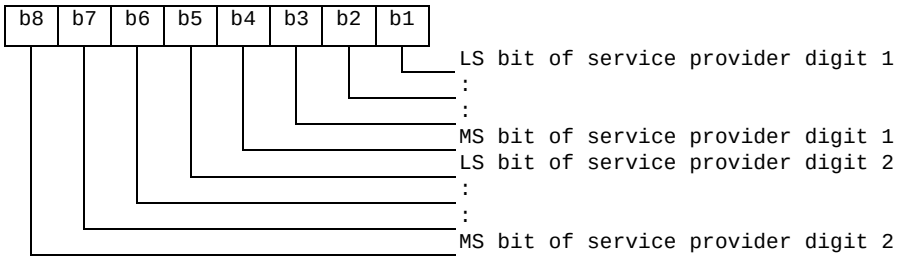
Coding:
- For each 6 byte list element.

Bytes 1 to 3: PLMN (MCC + MNC): according to TS 24.008 [9].

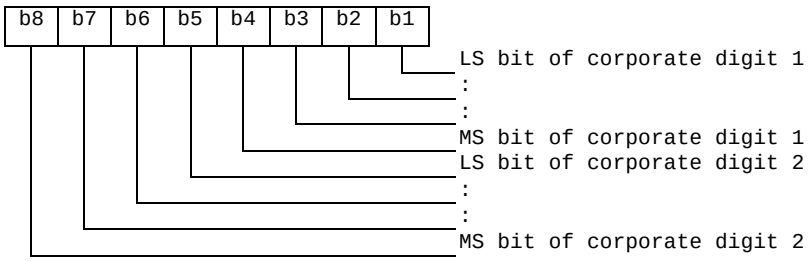
Byte 4:



Byte 5:



Byte 6:



- Empty fields shall be coded with 'FF'.
- The end of the list is delimited by the first MCC field coded 'FFF'.

4.2.51 $EF_{START\text{-}HFN}$ (Initialisation values for Hyperframe number)

This EF contains the values of $START_{CS}$ and $START_{PS}$ of the bearers that were protected by the keys in EF_{KEYS} or EF_{KEYSPS} at release of the last CS or PS RRC connection. These values are used to control the lifetime of the keys (see TS 33.102 [13]).

Identifier: '6F5B'	Structure: transparent	Mandatory
SFI: '0F'		
File size: 6 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	$START_{CS}$	M	3 bytes
4 to 6	$START_{PS}$	M	3 bytes

- $START_{CS}$
  Contents: Initialisation value for Hyperframe number – CS domain.

Coding: The LSB of $START_{CS}$ is stored in bit 1 of byte 3. Unused nibbles are set to 'F'.

- $START_{PS}$
  Contents: Initialisation value for Hyperframe number – PS domain.

Coding: As for $START_{CS}$.

4.2.52 $EF_{THRESHOLD}$ (Maximum value of START)

This EF contains the maximum value of $START_{CS}$ or $START_{PS}$. This value is used to control the lifetime of the keys (see TS 33.102 [13]).

Identifier: '6F5C'	Structure: transparent	Mandatory
SFI: '10'		
File size: 3 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Maximum value of $START_{CS}$ or $START_{PS}$.	M	3 bytes

- Maximum value of $START_{CS}$ or $START_{PS}$.

Coding: As for $START_{CS}$

4.2.53 $EF_{OPLMNwACT}$ (Operator controlled PLMN selector with Access Technology)

If service n° 42 is "available", this file shall be present.

This EF contains the coding for n PLMNs where n is determined by the operator. This information is determined by the operator and defines the preferred PLMNs in priority order. The first record indicates the highest priority and the nth record indicates the lowest. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [31])

Identifier: '6F61'	Structure: transparent	Optional
SFI: '11'		
File size: 5n bytes , (n ≥ 8)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes
41 to 43	9th PLMN	O	3 bytes
44 to 45	9th PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	N^{th} PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	N^{th} PLMN Access Technology Identifier	O	2 bytes

- PLMN.

Contents:

- Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:

- according to TS 24.008 [9].

- Access Technology Identifier:

Coding:

- See $EF_{PLMNwACT}$ for coding.

4.2.54 $EF_{HPLMNwAcT}$ (HPLMN selector with Access Technology)

If service n°43 is "available", this file shall be present.

The HPLMN Selector with access technology data field shall contain the HPLMN code, or codes together with the respected access technology in priority order (see TS 23.122 [31]).

Identifier: '6F62'	Structure: Transparent	Optional
SFI: '13'		
File size: 5n (n ≥ 1) bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	O	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	nth PLMN Access Technology Identifier	O	2 bytes

- PLMN

Contents:

Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:

according to TS 24.008 [47].

- Access Technology:

Contents: The Access Technology of the HPLMN that the ME will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

Coding:

- See $EF_{PLMNwACT}$ for coding.

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '17'		
Record Length: X bytes, (X > 0)	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4 [20]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.2.56 Void

4.2.57 EF_{NETPAR} (Network Parameters)

This EF contains information concerning the cell frequencies

Network Parameter storage may reduce the extent of the terminal search of FDD, TDD or GSM carriers when selecting a cell. The network parameters stored in the USIM shall be in accordance with the procedures specified in this clause.

The RF carrier frequency information is stored on 2 bytes and coded on 16 bits starting from 0,0 MHz. Each increment of the 16 bit value is an increment of 200 kHz in frequency. This allows the exact channel frequency to be stored in this data field making it independent of any band information. It is up to the terminal to associate the indicated frequency with a particular band, e.g. GSM 900, GSM 1800 etc. This means that a range from 0 to 13,1 GHz can be covered, with the resolution of 200 kHz. The frequency indicated is always the terminal receiver carrier frequency.

The EF provides a minimum storage capacity of 46 bytes in order to provide the capability of storing at least two cell information TLV objects, e.g. GSM/FDD or FDD/TDD in its minimum configuration, i.e. the terminal can rely on the required memory space for storing at least two cell information lists offering 8 GSM neighbour carrier frequencies and 8 Intra/Inter frequencies, respectively. In what configuration the available memory actually is being used is up to the terminal.

A terminal shall ignore a TLV object or the value of a carrier frequency which is beyond its capabilities, i.e. an FDD only terminal shall ignore the GSM related frequency information. When updating this file, the terminal shall update it with the current values available in the terminal. Updating of this file shall start from the beginning of the file. The terminal need not respect the structure of any information previously stored, i.e. an FDD only terminal may overwrite the GSM parameters stored in this file by another terminal.

The GSM cell information constructed TLV object contains the information of the BCCH channel frequency that the terminal is currently camped on, indicated by tag '80'. The constructed TLV object also contains an indication of up to 32 neighbour BCCH carrier frequencies indicated by tag '81'. In order to store a complete set of GSM network parameters, a total of 72 bytes is required. The terminal shall convert the BCCH channel information, as specified in TS 44.018 [28], received from the network into the corresponding frequency before storing it in the USIM.

The FDD cell information constructed TLV object contains the scrambling code information for the intra frequency carrier, tag '80', and the inter frequency scrambling codes, tag '81'. The intra frequency carrier information may contain up to 32 scrambling codes (m) while there is a limitation of the number of inter frequency scrambling codes (n1, n2, n3). The number of inter frequencies that can be indicated is limited to three and the total amount of scrambling codes for the inter frequencies is limited to 32 (n1+n2+n3 <= 32), i.e. if only one inter frequency carrier is indicated, it can contain up to 32 scrambling codes. If two or more inter frequency carriers are indicated, a total of 32 scrambling codes can be provided. How the information is split between the inter frequency carriers is determined by the terminal. In order to store a complete set of FDD cell information a total of 146 bytes is required. The terminal shall convert the UARFCN information, as specified in TS 25.101 [33], received from the network into the corresponding frequency before storing it in the USIM.

The TDD cell information constructed TLV object has the same structure as the FDD cell information TLV object.

NOTE: Currently there is no inter frequency cell information required for the TDD case.

Identifier: '6FC4'	Structure: transparent	Mandatory
File size: X bytes, (X ≥ 46)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	TLV object(s) containing GSM/FDD/TDD cell information	O	X

- EF_{NETPAR} Cell Information tags

Description	Value	Information Element size bytes
GSM Cell Information Tag	'A0'	1
Camping Frequency Tag	'80'	1
Camping Frequency Information		2
Neighbour Frequency Tag	'81'	1
Neighbour Frequency Information		2*m (8 <= m <= 32)
FDD Cell Information Tag	'A1'	1
Intra Frequency Information Tag	'80'	1
Scrambling code Information		2*m (8 <= m <= 32)
Inter Frequency Information Tag	'81'	1
Scrambling code information		2*(n1+n2+n3) (8 <= n1+n2+n3 <= 32)
TDD Frequency information Tag	'A2'	1
Intra Frequency Information Tag	'80'	1
Cell parameters ID		2*m (8 <= m <= 32)
Inter Frequency Information Tag	'81'	1
Cell parameters ID		2*(n1+n2+n3) (8 <= n1+n2+n3 <= 32)

- GSM Cell Information, if tag 'A0' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
GSM Cell Information Tag	'A0"	M	1
Length	'4+ (2+2*m) (<=70) '	M	1
Current camped cell BCCH frequency information tag	'80'	M	1
Length	'02'	M	1
Current camped BCCH frequency		M	2
Neighbour Cell BCCH Frequency information tag	'81'	O	1
Length	2*m (=< 32)	O	1
Neighbour BCCH carrier frequencies		O	2*m (8 <= m <= 32)

- FDD Cell Information. If tag 'A1' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
FDD Cell Information Tag	'A1'	M	1
Length	4+(2*m)+(4+2*n1)+(4+2*n2)+(4+2*n3) (<=144)	M	1
FDD Intra Frequency information tag	'80'	M	1
Length	2+2*m	M	1
Intra Frequency carrier frequency		M	2
Intra Frequency scrambling codes		M	2*m (8 <= m <= 32)
FDD Inter Frequency information tag (see NOTE 1)	'81'	O	1
Length	2+2*n (NOTE 2)	O	1
Inter Frequency carrier frequencies		O	2
Inter Frequency scrambling codes		O	2*n (NOTE 2)
NOTE 1: This TLV object may occur up to 3 times within the constructed TLV object depending how many inter frequencies are indicated NOTE 2: n is in this case n1, n2 or n3, 8 <= (n1+n2+n3)<=32			

- TDD Cell Information: If tag 'A2' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
TDD Cell Information Tag	'A2'	M	1
Length	4+(2*m)+(4+2*n1)+(4+2*n2)+(4+2*n3) (<=144)	M	1
TDD Intra Frequency information tag	'80'	M	1
Length	2+2*m	M	1
Intra Frequency carrier frequency		M	2
Intra Frequency scrambling codes		M	2*m (8 <= m <= 32)
TDD Inter Frequency information tag (see NOTE 1)	'81'	O	1
Length	2+2*n (NOTE 2)	O	1
Inter Frequency carrier frequencies		O	2
Inter Frequency scrambling codes		O	2*n (NOTE 2)
NOTE 1: This TLV object may occur up to 3 times within the constructed TLV object depending how many inter frequencies are indicated NOTE 2: n is in this case n1, n2 or n3, 8 <= (n1+n2+n3)<=32			

4.2.58 EF_{PNN} (PLMN Network Name)

If service n°45 is "available", this file shall be present.

This EF contains the full and short form versions of the network name for the registered PLMN. The ME shall use these versions in place of its own versions of the network name for the PLMN (stored in the ME's memory list), and also in place of the versions of the network name received when registered to the PLMN, as defined by TS 24.008 [9].

This file may also contain PLMN additional information to be displayed to the user during the Manual Network Selection procedures as defined in TS 23.122 [31].

If the EF_{OPL} is not present, then the first record in this EF is used for the default network name when registered in the HPLMN (if the EHPLMN list is not present or is empty) or an EHPLMN (if the EHPLMN list is present).

Identifier: '6FC5'	Structure: linear fixed	Optional
SFI: '19'		
Record length: X bytes; X ≥ 3	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Network name TLV objects	M	X bytes

- Network name TLV objects.
  The content and coding (Full name for network and Short name for network) is defined below, where the fields within the objects are defined in TS 24.008 [9]:

Coding of the Network name TLV objects

Length	Description	Status
1 byte	Full name for network IEI: '43' (This shall be the same as that used in the MM/GMM INFORMATION message).	M
1 byte	Length of Full name for network Name contents	M
Y bytes	Full name for network contents (Octets 3 to n of network name information element)	M
1 byte	Short name for network IEI: '45' (This shall be the same as that used in the MM/GMM INFORMATION message).	O
1 byte	Length of Short name for network	C1
Z bytes	Short name for network contents (Octets 3 to n of network name information element)	C1
1 byte	PLMN Additional Information tag ('80')	O
1 byte	Length of PLMN Additional Information	C2
W bytes	PLMN Additional Information (coded using one of the UCS2 code options as defined in TS 31.101 [11]).	C2
C1: this field shall be present if the short name for network IEI is present C2: this field shall be present if the PLMN Additional Information tag is present		

Unused bytes shall be set to 'FF'.

4.2.59 EF_{OPL} (Operator PLMN List)

If service n°46 is "available", this file shall be present.

This EF contains a prioritised list of Location Area Information (LAI) or Tracking Area Identity (TAI) identities that are used to associate a specific operator name contained in EF_{PNN} or EF_{PNNI} with the LAI/TAI. The ME shall use this EF in association with the EF_{PNN} in place of any network name stored within the ME's internal list and any network name received when registered to the PLMN, as defined by TS 24.008 [9] or TS 24.301 [51]. The PLMN Network Name may also be provided in a graphical format in EF_{PNNI}. The ME shall use the text format or the graphical format or both to display the service provider name according to the rules defined in section 4.2.89.

Identifier: '6FC6'	Structure: linear fixed	Conditional (see Note)
SFI: '1A'		
Record length: X bytes, (X ≥ 8)	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 7	Location Area Identity/Tracking Area Identity	M	7 bytes
8	PLMN Network Name Record Identifier	M	1 byte

NOTE: This file is mandatory if and only if EF_{PNN} is present.

- Location Area Identity/Tracking Area Identity

Contents:
Location Area Information, this comprises of the MCC, MNC and LAC
Tracking Area Identity, this comprises of the MCC, MNC and TAC

Coding:
PLMN : according to TS 24.008 [9]/TS 24.301 [51]
A BCD value of 'D' in any of the MCC and/or MNC digits shall be used to indicate a "wild" value for that corresponding MCC/MNC digit

LAC/TAC : according to TS 24.008 [9]/TS 24.301 [51]

Two values for the LAC/TAC are stored in order to allow a range of LAC/TAC values to be specified for a given PLMN. A value of '0000' stored in bytes 4 to 5 and a value of 'FFFE' stored in bytes 6 to 7 shall be used to indicate the entire range of LACs/TACs for the given PLMN. In the case where only a single LAC/TAC value is to be specified then the value stored in bytes 4 to 5 shall be identical to the value stored in bytes 6 to 7 for the given PLMN. If a range of LAC/TAC values are to be specified, then the value stored in bytes 4 to 5 shall be the start of the LAC/TAC range and the value stored in bytes 6 to 7 shall be the end of the LAC/TAC range for the given PLMN.

- PLMN Network Name Record Identifier

Contents:
Identifier of operator name to be displayed

Coding:
A value of '00' indicates that the name is to be taken from other sources, see TS 22.101 [24]

A value in the range '01' to 'FE' indicates the record number in EF_{PNN} that shall be displayed as the registered PLMN name. It also indicates the record number in EF_{PNNI} that may be displayed as the registered PLMN name icon.

NOTE: The intent of this file is to provide exceptions to the other sources of a network name. Care should be taken not to introduce too many PLMN entries. An excessive number of entries could result in a longer initialisation period.

4.2.60 EF_{MBDN} (Mailbox Dialling Numbers)

If service n°47 is "available", this file shall be present.

This EF contains dialling numbers to access mailboxes associated with Voicemail, Fax, Electronic Mail and other messages. It may also contain associated alpha-tags for each supported mailbox. Each dialling number shall be associated with a message waiting indication group type using EF_{MBI} (see TS 23.038 [5] for message waiting indication group types).

Identifier: '6FC7'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC contents	M	10 bytes
X+13	Capability/Configuration2 Record Identifier	M	1 byte
X+14	Extension 6 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 4.4.2.3), with the exception that extension records are stored in the EF_{EXT6} and with the exception that Capability/Configuration parameters are stored in the $EF_{CCP2.}$

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.61 EF_{EXT6} (Extension6)

This EF contains extension data of an MBDN (see MBDN in 4.2.60).

Identifier: '6FC8'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding, see clause 4.4.2.4 (EF_{EXT1}).

4.2.62 EF_{MBI} (Mailbox Identifier)

If service n°47 is "available", this file shall be present.

This EF contains information to associate mailbox dialling numbers in EF_{MBDN} with a message waiting indication group type and subscriber profile (as defined in TS 23.097 [36]). A message waiting indication group type may either be Voicemail, Fax, Electronic Mail, Other or Videomail (as defined in TS 23.040 [6]).

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile). Each record contains references to mailbox dialling numbers in EF_{MBDN} (one reference for each message waiting indication group type).

Identifier: '6FC9'	Structure: linear fixed	Optional
Record length: X bytes, (X ≥ 4)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Mailbox Dialling Number Identifier – Voicemail	M	1 byte
2	Mailbox Dialling Number Identifier – Fax	M	1 byte
3	Mailbox Dialling Number Identifier – Electronic Mail	M	1 byte
4	Mailbox Dialling Number Identifier – Other	M	1byte
5	Mailbox Dialling Number Identifier – Videomail	O	1 byte

- Mailbox Dialling Number Identifier (message waiting group type = Voicemail, Fax, Electronic Mail, Other or Videomail).

Contents:

Identifies the mailbox dialling number to be associated with message waiting type.

Coding:

'00' – no mailbox dialling number associated with message waiting indication group type.
'xx' – record number in EF_{MBDN} associated with message waiting indication group type.

4.2.63 EF_{MWIS} (Message Waiting Indication Status)

If service n°48 is "available", this file shall be present.

This EF contains the status of indicators that define whether or not a Voicemail, Fax, Electronic Mail, Other or Videomail message is waiting (as defined in TS 23.040 [6]). The ME uses the status after re-activation to determine whether or not to display the respective message-waiting indication on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in TS 23.097 [36] for MSP.

Identifier: '6FCA'	Structure: Linear fixed	Optional
Record length: X bytes, (X ≥ 5)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Message Waiting Indicator Status	M	1 byte
2	Number of Voicemail Messages Waiting	M	1 byte
3	Number of Fax Messages Waiting	M	1 byte
4	Number of Electronic Mail Messages Waiting	M	1 byte
5	Number of Other Messages Waiting	M	1 byte
6	Number of Videomail Messages waiting	O	1 byte

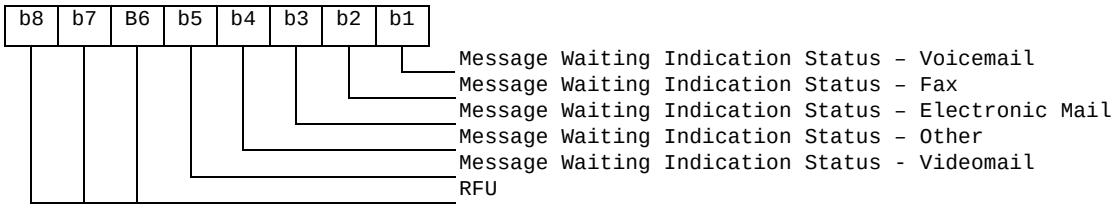
Message Waiting Indication Status

Contents:

Indicates the status of the message-waiting indication.

Coding:

The indicator status for each indicator type is 1 bit long and set as follows:
bit = 1: Set Indication Active
bit = 0: Set Indication Inactive



Number of Voicemail Messages Waiting
Contents:
Contains the number of voicemail messages waiting (see TS 23.040 [6]).

Coding:
Binary.

Number of Fax Messages Waiting
Contents:
Contains the number of fax messages waiting (see TS 23.040 [6]).

Coding:
Binary.

Number of Electronic Mail Messages Waiting
Contents:
Contains the number of electronic mail messages waiting (see TS 23.040 [6])

Coding:
Binary.

Number of Other Messages Waiting
Contents:
Contains the number of other messages waiting (see TS 23.040 [6]).

Coding:
Binary.

Number of Videomail Messages Waiting
Contents:
Contains the number of Videomail messages waiting (see TS 23.040 [6]).

Coding:
Binary.

4.2.64 EF_{CFIS} (Call Forwarding Indication Status)

If service n°49 is "available", this file shall be present.

This EF contains the status of indicators that are used to record whether call forward is active. The ME uses the status after re-activation to determine whether or not to display the respective Call Forwarding indicator on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in TS 23.097 [36] for MSP.

Identifier: '6FCB'	Structure: Linear Fixed	Optional
Record length: 16 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	MSP number	M	1 byte
2	CFU indicator status	M	1 byte
3	Length of BCD number	M	1 byte
4	TON and NPI	M	1 byte
5 to 14	Dialling Number	M	10 bytes
15	Capability/Configuration2 Record Identifier	M	1 byte
16	Extension 7 Record Identifier	M	1 byte

NOTE: For contents and coding of data items not detailed below, see the respective data items of EF_{ADN} (clause 4.4.2.3), Capability/Configuration2 Record Identifier and Extension 7 Record Identifier.

MSP number:

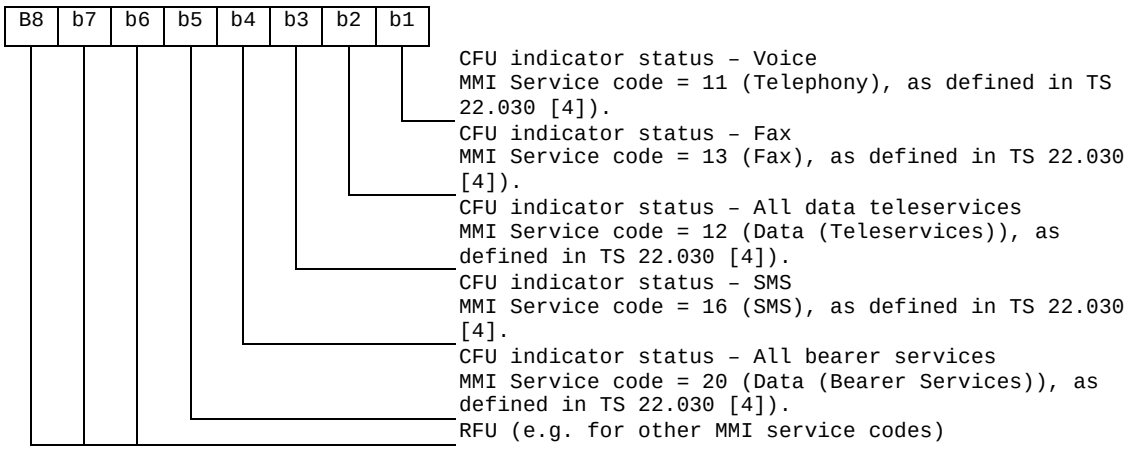
Contents:
The MSP number contains the Profile Identity of the subscriber profile. The Profile Identity shall be between 1and 4 as defined in TS 23.097 [36] for MSP.

Coding:
Binary.

CFU indicator status:

Contents:
Indicates the status of the call forward unconditional indicator. Service code = 21 (CFU) or 002 (for CFU part of all CF), as defined in TS 22.030 [4]

Coding:
The indicator status for each indicator type is 1 bit long and is set as follows:
bit = 1: Set indication active
bit = 0: Set indication inactive.



4.2.65 EF_{EXT7} (Extension7)

This EF contains extension data of a CFIS (Call Forwarding Indication Status - see 4.2.64).

Identifier: '6FCC'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 4.4.2.4 (EF_{EXT1}).

4.2.66 EF_{SPDI} (Service Provider Display Information)

If service n°51 is "available", this file shall be present.

This EF contains information regarding the service provider display i.e. the service provider PLMN list.

Identifier: '6FCD'	Structure: transparent	Optional
SFI: '1B'		
File size: x bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to x	TLV object(s) containing Service Provider information	M	x bytes

Tag Value	Tag Description
'A3'	Service provider display information Tag
'80'	Service provider PLMN list tag

The service provider display information object is a constructed TLV coded according to ISO/IEC 8825-1 [35].

- Service provider PLMN list

Contents:

This TLV contains a list of n PLMNs in which the Service Provider Name shall be displayed, as defined in clause 4.2.12 (EF_{SPN}).

Coding:

Description	M/O	Length
Service provider PLMN list tag	M	1 byte
Length (see note)	M	x bytes
1st PLMN entry	M	3 bytes
2nd PLMN entry	O	3 bytes
3rd PLMN entry	O	3 bytes
…		
nth PLMN entry	O	3 bytes
Note: the length is 3*n bytes, where n denotes the number of PLMN entries. The length can be coded on one or more bytes according to ISO/IEC 8825-1 [35].		

Each PLMN is coded as follows:

Mobile Country Code (MCC) followed by the Mobile Network Code (MNC) according to TS 24.008 [9]. In case a PLMN entry is not used, it shall be set to 'FF FF FF'.

4.2.67 EF_{MMSN} (MMS Notification)

If service n°52 is "available", this file shall be present.

This EF contains information in accordance with TS 23.140 [38] and X.S0016-000-A v1.0 [45] comprising MMS notifications (and associated parameters) which have been received by the UE from the network. A 3GPP terminal needs only to support the MMS implementation specified in TS 23.140 [38].

Identifier: '6FCE'	Structure: Linear fixed	Optional
Record length: 4+X bytes	Update activity: low	

Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM

Bytes	Description	M/O	Length
1 to 2	MMS Status	M	2 bytes
3	MMS Implementation	M	1 byte
4 to X+3	MMS Notification	M	X bytes
X+4	Extension file record number	M	1 byte

- MMS Status

Content:

The status bytes contain the status information of the notification.

Coding:

b1 indicates whether there is valid data or if the location is free. B2 indicates whether the MMS notification has been read or not. Bits b3-b4 of the first byte indicate the MM retrieval, MM rejection, or MM forwarding status, Bits b5-b8 of the first byte and the entire second byte are reserved for future use.

First byte:

b8	b7	b6	b5	b4	b3	b2	b1	
				X	X	X	0	Free space
				X	X	X	1	Used space
				X	X	0	1	Notification not read
				X	X	1	1	Notification read
				0	0	X	1	MM not retrieved
				0	1	X	1	MM retrieved
				1	0	X	1	MM rejected

```
|    |    |    |    1    1    X    1  MM forwarded
|    |    |    |                      Reserved for future use
|____|____|____|____________________
```

Second byte:

```
| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|____|____|____|____|____|____|____|____|
|    |    |    |    |    |    |    |    |  Reserved for future use
|____|____|____|____|____|____|____|____|
```

- MMS Implementation

Contents:

The MMS Implementation indicates the used implementation type, e.g. WAP.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	WAP implementation of MMS as defined in TS 23.140 [38]
2	Reserved for 3GPP2: M-IMAP implementation of MMS as defined in X.S0016-000-A v1.0 [45]
3	Reserved for 3GPP2: SIP implementation of MMS as defined in X.S0016-000-A v1.0 [45]
4-8	Reserved for future use

Bit value	Meaning
0	Implementation not supported.
1	Implementation supported.

- MMS Notification

Contents:

The MMS Notification contains the MMS notification.

Coding:

The MMS Notification is coded according to the MMS Implementation as indicated in Byte 3.

Any unused byte shall be set to 'FF'.

- Extension file record number

Contents:

- extension file record number. This byte identifies the number of a record in the EF_{EXT8} containing extension data for the notification information. The use of this byte is optional. If it is not used it shall be set to 'FF'.

Coding:

- binary.

4.2.68 EF_{EXT8} (Extension 8)

If service n°53 is "available", this file shall be present.

This EF contains extension data of a MMS Notification (Multimedia Messaging Service - see 4.2.67).

Identifier: '6FCF'	Structure: linear fixed	Optional
Record length: X+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to X+1	Extension data	M	X bytes
X+2	Identifier	M	1 byte

The structure of this EF is identical to the structure of EF_{EXT1} (see clause 4.4.2.4).

- Record type.

Contents:
type of the record, see clause 4.4.2.4

Coding:
according to the "additional data" type

- Extension data.

Contents:
additional data (MMS notification extension)

Coding:
the first byte of the extension data gives the number of bytes of the remainder of the MMS notification in this record. The following bytes contain the extension of the MMS notification.

- Identifier.

Contents:
identifier of the next extension record (in EXT8) to enable longer storage of information.

Coding:
record number of next record. 'FF' identifies the end of the chain.

4.2.69 EF_{MMSICP} (MMS Issuer Connectivity Parameters)

If service n°52 is "available", this file shall be present.

This EF contains values for Multimedia Messaging Connectivity Parameters as determined by the issuer, which can be used by the ME for MMS network connection. This file may contain one or more sets of Multimedia Messaging Issuer Connectivity Parameters. The first set of Multimedia Messaging Issuer Connectivity Parameters is used as the default set. Each set of Multimedia Messaging Issuer Connectivity Parameters may consist of one or more Interface to Core Network and Bearer information TLV objects, but shall contain only one MMS implementation TLV object, one MMS Relay/Server TLV object and one Gateway TLV object. The order of the Interface to Core Network and Bearer information TLV objects in the MMS Connectivity TLV object defines the priority of the Interface to Core Network and Bearer information, with the first TLV object having the highest priority.

Identifier: '6FD0'	Structure: Transparent	Optional
File Size: X_1+…+ X_n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X_1	MMS Connectivity Parameters TLV object	M	X_1 bytes
X_1+1 to X_1 + X_2	MMS Connectivity Parameters TLV object	O	X_2 bytes
…	…		
X_1+…+ X_{n-1}+1 to X_1+…+ X_n	MMS Connectivity Parameters TLV object	O	X_n bytes

MMS Connectivity Parameters tags

Description	Tag Value
MMS Connectivity Parameters Tag	'AB'
MMS Implementation Tag	'80'
MMS Relay/Server Tag	'81'
Interface to Core Network and Bearer Information Tag	'82'
GatewayTag	'83'
Reserved for 3GPP2: MMS Authentication Mechanism Tag	'84'
Reserved for 3GPP2: MMS Authentication User Name Tag	'85'

- MMS Connectivity Parameters contents

Description	Value	M/O	Length (bytes)
MMS Connectivity Parameters Tag	'AB'	M	1
Length	Note 1	M	Note 2
MMS Implementation Tag	'80'	M	1
Length	1	M	1
MMS Implementation Information	--	M	1
MMS Relay/Server Tag	'81'	M	1
Length	X1	M	Note 2
MMS Relay/Server Address	--	M	X1
MMS Authentication Mechanism Tag	'84'	C1	1
Length	X2	C1	Note 2
MMS Authentication Mechanism	--	C1	X2
MMS Authentication User Name Tag	'85'	C1	1
Length	X3	C1	Note 2
MMS Authentication User Name	--	C1	X3
1st Interface to Core Network and Bearer Information Tag (highest priority)	'82'	C2	1
Length	Y1	C2	Note 2
1st Interface to Core Network and Bearer information	--	C2	Y1
2nd Interface to Core Network and Bearer Information Tag	'82'	C2	1
Length	Y2	C2	Note 2
2nd Interface to Core Network and Bearer information	--	C2	Y2
…			
Nth Interface to Core Network and Bearer Information Tag (lowest priority)	'82'	C2	1
Length	Y3	C2	Note 2
Nth Interface to Core Network and Bearer information	--	C2	Y3
GatewayTag	'83'	O	1
Length	Z	O	Note 2
Gateway Information	--	O	Z
Note 1: This is the total size of the constructed TLV object. Note 2: The length is coded according to ISO/IEC 8825-1 [35]. C1: Reserved for 3GPP2: only present if M-IMAP or SIP indicated in tag 80. C2: Only present if WAP is indicated in tag 80.			

- MMS Implementation Tag '80'

See section 4.2.67 for contents and coding.

- MMS Relay/server Tag '81'

Contents:

The MMS relay/server contains the address of the associated MMS relay/server.

Coding:

The MMS relay/server address is coded according to the guideline provided in TS 23.140 [38].

- MMS Authentication Mechanism Tag '84'

Contents:

The MMS authentication mechanism contains the authentication mechanism used for M-IMAP and SIP.

Coding:

The MMS authentication mechanism is coded according to the guidelines provided in X.S0016-000-A v1.0 [45].

- MMS Authentication User Name Tag '85'

Contents:

The MMS Authentication User Name contains the authentication user name used for M-IMAP and SIP.

Coding:

The MMS authentication User Name is coded according to the guidelines provided in X.S0016-000-A v1.0 [45].

- Interface to Core Network and Bearer Information Tag '82'

Contents:

The Interface to Core Network and Bearer Information may contain the following information to set up the bearer: Bearer, Address, Type of address, Speed, Call type, Authentication type, Authentication id, Authentication password.
Coding:
The coding is according to the guideline provided in TS 23.140 [38].

- Gateway Tag '83'

Contents:
The Gateway may contain the following information; Address, Type of address, Port, Service, Authentication type, Authentication id and Authentication password.
Coding:
The coding is according to the guideline provided in TS 23.140 [38].

Unused bytes shall be set to 'FF'.

An Example for the coding of these parameters can be found in Annex J.2.

4.2.70 EF_{MMSUP} (MMS User Preferences)

If service n°52 is "available", this file shall be present.

This EF contains values for Multimedia Messaging Service User Preferences, which can be used by the ME for user assistance in preparation of mobile multimedia messages (e.g. default values for parameters that are often used).

Identifier: '6FD1'	Structure: Linear Fixed	Optional
Record Length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	MMS User Preference TLV Objects	M	X bytes

MMS User Preference tags

Description	Tag Value
MMS Implementation Tag	'80'
MMS User preference profile name Tag	'81'
MMS User Preference information Tag	'82'

MMS User Preference information

Description	Value	M/O	Length (bytes)
MMS Implementation Tag	'80'	M	1
Length	1	M	Note
MMS Implementation information	--	M	1
MMS User preference profile name Tag	'81'	M	1
Length	X	M	Note
MMS User profile name	--	M	X
MMS User Preference information Tag	'82'	M	1
Length	Y	M	Note
MMS User Preference information	--	M	Y
Note: The length is coded according to ISO/IEC 8825-1 [35]			

- MMS Implementation Tag '80'

For contents and coding see 4.2.67

- MMS User preference profile name Tag '81'

Contents:
Alpha tagging of the MMS user preference profile.

Coding:
this alpha-tagging shall use either:
- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified.

Or:
- one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

- MMS User Preference information Tag '82'

Contents:
The following information elements may be coded; Sender Visibility, Delivery Report, Read-Reply, Priority, Time of Expiry and Earliest Delivery Time.
Coding:
Depending upon the MMS implementation as indicated in Tag '80'.

An Example for the coding of these parameters can be found in Annex J.1.

4.2.71 EF_{MMSUCP} (MMS User Connectivity Parameters)

If service n°52 and n°55 are "available", this file shall be present.

This EF contains values for Multimedia Messaging Connectivity Parameters as determined by the user, which can be used by the ME for MMS network connection. This file may contain one or more sets of Multimedia Messaging User Connectivity Parameters. Each set of Multimedia Messaging User Connectivity Parameters may consist of one or more Interface to Core Network and Bearer information TLV objects, but shall contain only one MMS implementation TLV object, one MMS Relay/Server TLV object and one Gateway TLV object. The order of the Interface to Core Network and Bearer information TLV objects in the MMS Connectivity TLV object defines the priority of the Interface to Core Network and Bearer information, with the first TLV object having the highest priority.

Identifier: '6FD2'	Structure: Transparent	Optional
File Size: X_1+…+ X_n bytes	Update activity: low	

Access Conditions:

READ	PIN	
UPDATE	PIN/PIN2	
		(fixed during administrative management)
DEACTIVATE	ADM	
ACTIVATE	ADM	

Bytes	Description	M/O	Length
1 to X_1	MMS Connectivity Parameters TLV object	O	X_1 bytes
X_1+1 to X_1 + X_2	MMS Connectivity Parameters TLV object	O	X_2 bytes
…	…		
X_1+…+ X_{n-1}+1 to X_1+…+ X_n	MMS Connectivity Parameters TLV object	O	X_n bytes

For the contents and coding see 4.2.69

4.2.72 EF_{NIA} (Network's Indication of Alerting)

If service n°56 is "available", this file shall be present.

This EF contains categories and associated text related to the Network's indication of alerting in the MS service defined in TS 22.101 [24].

Identifier: '6FD3'	Structure: linear fixed	Optional
Record length : X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Alerting category	M	1 byte
2 to X+1	Informative text	M	X bytes

- Alerting category

Contents:

category of alerting for terminating traffic.

Coding:

according to TS 24.008 [9]. Value 'FF' means that no information on alerting category is available.

- Informative text

Contents:

text describing the type of terminating traffic associated with the category.

Coding:

see the coding of the Alpha Identifier item of the EF_{ADN}. The maximum number of characters for this informative text is indicated in TS 22.101 [24].

4.2.73 EF_{VGCS} (Voice Group Call Service)

If service n°57 is "available", this file shall be present.

This EF contains a list of those VGCS group identifiers the user has subscribed to. The elementary file is used by the ME for group call establishment and group call reception.

Identifier: '6FB1'	Structure: transparent	Optional
File size: 4n bytes, (1≤ n ≤ 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 4	Group ID 1	M	4 bytes
5 to 8	Group ID 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	Group ID n	O	4 bytes

- Group ID

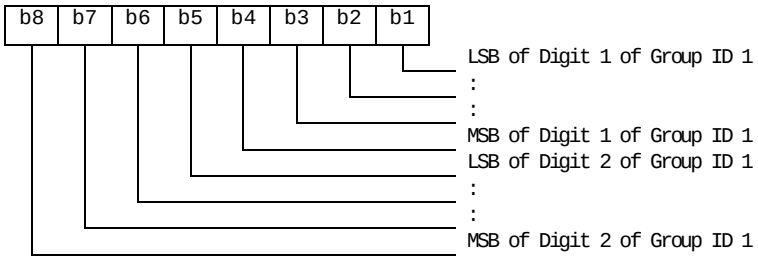
Contents: VGCS Group ID, according to TS 23.003 [25]

Coding:

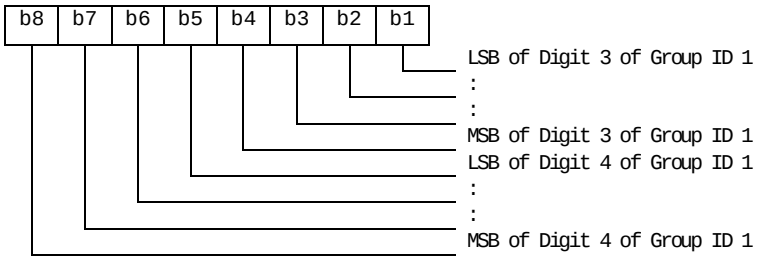
The VGCS Group ID is of a variable length with a maximum length of 8 digits. Each VGCS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code.

If a VGCS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VGCS Group ID Digit 1 is the most significant digit of the Group ID.

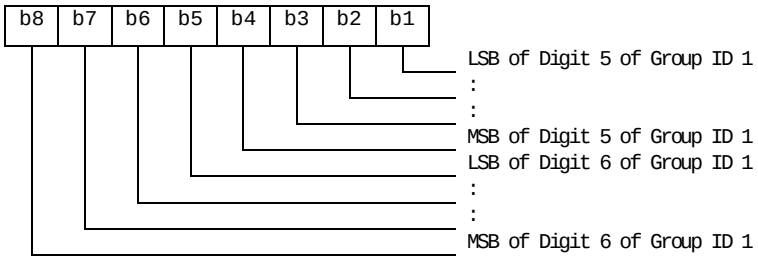
Byte 1:



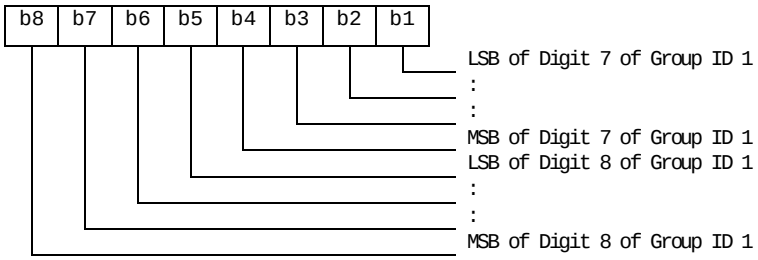
Byte 2:



Byte 3:

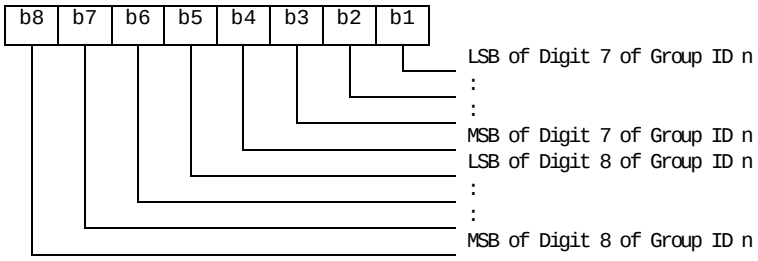


Byte 4:



:
: etc.....

Byte (4n-3) to 4n:



If storage for fewer than the maximum possible number *n* of VGCS Group Ids, is required, the excess bytes shall be set to 'FF'.

4.2.74 EF_{VGCSS} (Voice Group Call Service Status)

If service n°57 is "available", this file shall be present.

This EF contains the status of activation for the VGCS group identifiers. The elementary file is directly related to the EF_{VGCS}. This EF shall always be allocated if EF_{VGCS} is allocated.

Identifier: '6FB2'	Structure: transparent	Optional
File size: 7 bytes	Update activity: low	

Access Conditions:

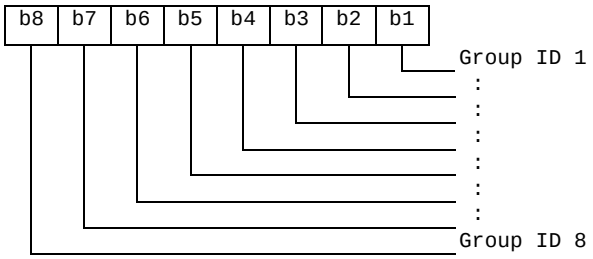
READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

Activation/Deactivation Flags

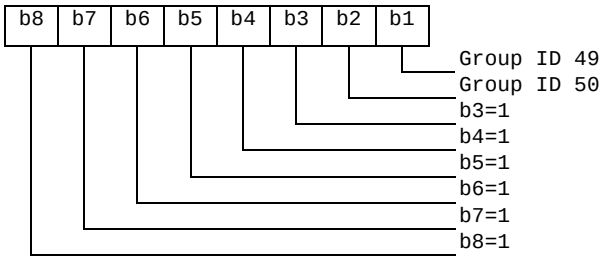
Contents: Activation/Deactivation Flags of the appropriate Group Ids
Coding: bit = 0 means - Group ID deactivated
bit = 1 means - Group ID activated

Byte 1:



etc : : : : : : : :

Byte 7:



4.2.75 EF_{VBS} (Voice Broadcast Service)

If service n°58 is "available", this file shall be present.

This EF contains a list of those VBS group identifiers the user has subscribed to. The elementary file is used by the ME for broadcast call establishment and broadcast call reception.

Identifier: '6FB3'	Structure: transparent	Optional
File size: 4n bytes, (1 ≤ n ≤ 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

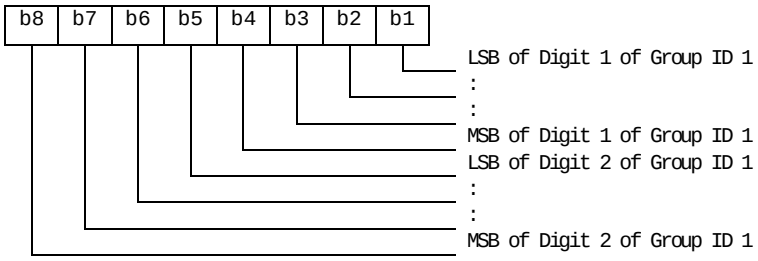
Bytes	Description	M/O	Length
1 to 4	Group ID 1	M	4 bytes
5 to 2	Group ID 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	Group ID n	O	4 bytes

Group ID

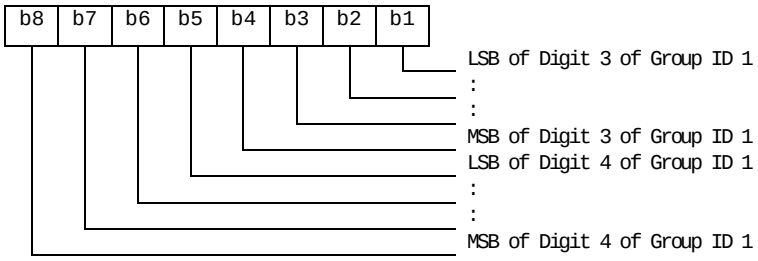
Contents: VBS Group ID, according to TS 23.003 [25]

Coding: The VBS Group ID is of a variable length with a maximum length of 8 digits. Each VBS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VBS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VBS Group ID Digit 1 is the most significant digit of the Group ID.

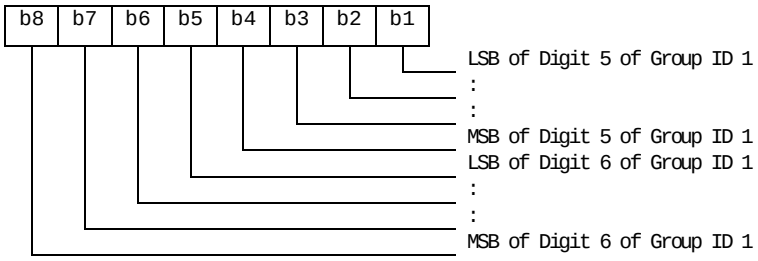
Byte 1:



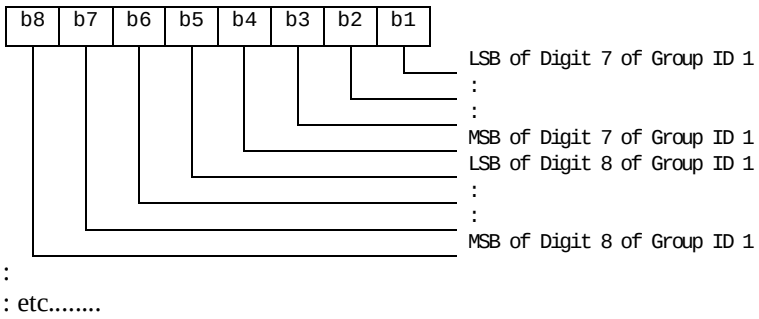
Byte 2:



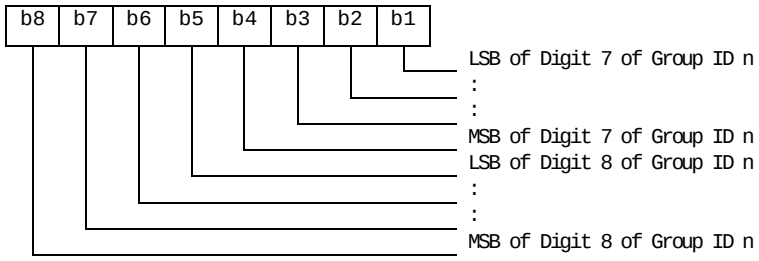
Byte 3:



Byte 4:



Byte (4n-3) to 4n:



If storage for fewer than the maximum possible number *n* of VBS Group Ids, is required, the excess bytes shall be set to 'FF'.

4.2.76 EF_{VBSS} (Voice Broadcast Service Status)

If service n°58 is "available", this file shall be present.

This EF contains the status of activation for the VBS group identifiers. The elementary file is directly related to the EF_{VBS}. This EF shall always be allocated if EF_{VBS} is allocated.

Identifier: '6FB4'	Structure: transparent	Optional
File size: 7 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

Activation/Deactivation Flags

Contents: Activation/Deactivation Flags of the appropriate Group Ids
Coding: see coding of EF_{VGCSS}

4.2.77 EF_{VGCSCA} (Voice Group Call Service Ciphering Algorithm)

If service n°64 is "available", this file shall be present.

This EF contains the ciphering algorithm identifiers for each of the Master Group Key (V_Ki) of each VGCS group that the user has subscribed to (defined in EF_{VGCS}).

Identifier: '6FD4'	Structure: transparent	Optional
File size: 2n bytes, (1 ≤ n ≤ 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group 1	M	1 byte
2	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group 1	M	1 byte
3	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group 2	O	1 byte
4	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group 2	O	1 byte
:	:	:	:
2n-1	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group n	O	1 byte
2n	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group n	O	1 byte

Ciphering Algorithm Identifier:

Contents: Ciphering Algorithm identifier for the specified Master Group Key of each Voice Call Group
Coding:

Value

‘00’ no ciphering
‘01’ ciphering with algorithm GSM A5/1
‘02’ ciphering with algorithm GSM A5/2
‘03’ ciphering with algorithm GSM A5/3
‘04’ ciphering with algorithm GSM A5/4
‘05’ ciphering with algorithm GSM A5/5
‘06’ ciphering with algorithm GSM A5/6
‘07’ ciphering with algorithm GSM A5/7
‘08’ to ‘FF’ RFU

4.2.78 EF_{VBSCA} (Voice Broadcast Service Ciphering Algorithm)

If service n°65 is "available", this file shall be present.

This EF contains the ciphering algorithm identifiers for each of the Master Group Key (V_Ki) of each VBS group that the user has subscribed to (defined in EF_{VBS}).

Identifier: '6FD5'	Structure: transparent	Optional
File size: 2n bytes, (1 ≤ n ≤ 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	VBS Group ciphering algorithm identifier for 1st V_Ki of Group 1	M	1 byte
2	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group 1	M	1 byte
3	VBS Group ciphering algorithm identifier for 1st V_Ki of Group 2	O	1 byte
4	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group 2	O	1 byte
:	:	:	:
2n-1	VBS Group ciphering algorithm identifier for 1st V_Ki of Group n	O	1 byte
2n	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group n	O	1 byte

Ciphering Algorithm Identifier:

Contents: Ciphering Algorithm identifier for the specified Master Group Key of each Voice Broadcast Group

Coding: See coding of EF_{VGCSCA}

4.2.79 EF_{GBABP} (GBA Bootstrapping parameters)

If service n°68 is "available", this file shall be present.

This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure.

Identifier: '6FD6'	Structure: transparent	Optional
File length: L+X+N+3 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of RAND (X)	M	1 byte
2 to (X +1)	RAND	M	X bytes
X+2	Length of B-TID (L)	M	1 byte
(X+3) to (X+2+L)	B-TID	M	L bytes
X+L+3	Length of key lifetime	M	1 byte
(X+L+4) to (X+L+N+3)	Key lifetime	M	N bytes

Length of RAND

Contents: number of bytes, not including this length byte, of RAND field

RAND

Contents: Random challenge used in the GBA_U bootstrapping procedure.
Coding: as defined in TS 33.103 [13]

Length of B-TID

Contents: number of bytes, not including this length byte, of B-TID field

B-TID

Content: Bootstrapping Transaction Identifier the GBA_U bootstrapped keys
Coding: As defined in TS 33.220 [42]

Length of key lifetime

Contents: number of bytes, not including this length byte, of key lifetime field

Key lifetime

Content: Lifetime of the GBA_U bootstrapped keys
Coding: As defined in TS 33.220 [42]

4.2.80 EF_{MSK} (MBMS Service Keys List)

If service n°69 is "available", this file shall be present.

A record of this EF contains the list of MBMS Service Keys (MSK) and associated parameters, which are related to an MBMS Key Domain. There are up to two MSKs per Key Domain ID/Key Group ID pair, where the Key Group ID is the Key Group part of the MSK ID as defined in TS 33.246 [43]. Two 4 byte MSK IDs stored within a record have the same value for the 2 byte Key Group part.

Identifier: '6FD7'	Structure: linear fixed	Optional
Record length: 8n+4 bytes, (n ≥ 2)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Key Domain ID	M	3 bytes
4	Number of stored MSK IDs and corresponding TS	M	1 byte
5 to 8	1st MSK ID	M	4 bytes
9 to 12	1st Time Stamp Counter (TS)	M	4 bytes
13 to 16	2nd MSK ID	M	4 bytes
17 to 20	2nd Time Stamp Counter (TS)	M	4 bytes
:	:	:	:
8(n-1)+5 to 8n	nth MSK ID	O (See Note)	4 bytes
8n+1 to 8n+4	nth Time Stamp Counter (TS)	C (See Note)	4 bytes

Note: In the current version of the specification, these bytes are RFU.

Key Domain ID:

Content: Identifier of the Domain of the BM-SC providing MBMS Service.
Coding: As defined in TS 33.246 [43]

Number of stored MSK IDs and corresponding TS:
Content: Number of stored MSK IDs and corresponding Time Stamp counter (TS) within the record, as defined in TS 33.246 [43]. This number shall not exceed the maximum limit of MSK IDs fixed in TS 33.246 [43] (e.g if the maximum number of MSK IDs is 2, then this byte may only take the following values: '00', '01', '02').
Coding: binary.

MSK ID:

Content: Identifier of MBMS Service Key (MSK) within a particular Key Domain.
Coding: As defined in TS 33.246 [43]

Time Stamp Counter (TS):

Content: Counter for MIKEY replay protection in MTK delivery. Each counter is associated with a particular MSK.
Coding: As defined in TS 33.246 [43]

Any unused bytes shall be set to 'FF'.

4.2.81 EF_{MUK} (MBMS User Key)

If service n°69 is "available", this file shall be present.

This EF contains the identifier of the MBMS User Key (MUK) that is used to protect the transfer of MBMS Service Keys (MSK). The file also contains the Time Stamp Counter associated with the MUK, which is used for Replay Protection in MSK transport messages. This EF shall not contain MUK IDs with the same Idi part.

Identifier: '6FD8'	Structure: linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Bytes
1 to Z	MBMS User Key TLV objects	M	1 to Z

MBMS User Key tags

Description	Tag Value
MUK ID Tag	'A0'
Time Stamp Counter Tag	'81'

MBMS User Key information

Description	Value	M/O	Length (bytes)
MUK ID Tag	'A0'	M	1
Length	X	M	Note
MUK Idr Tag	'80'	M	1
Lenght	A	M	Note
MUK Idr value	--	M	A
MUK Idi Tag	'82'	M	1
Lenght	W	M	Note
MUK Idi Value	-	M	W
Time Stamp Counter Tag	'81'	M	1
Length	Y	M	Note
Time Stamp Counter value	--	M	Y
Note: The length is coded according to ISO/IEC 8825-1 [35]			

- MUK ID Tag 'A0'. This constructed data object consists of the Idr, and the Idi

- Idr Tag '80'
Content:
Idr part of MBMS User Key (MUK).
Coding:
As defined in TS 33.246 [43]
- Idi Tag '82'
Content:
Idi part of MBMS User Key (MUK).
Coding:
As defined in TS 33.246 [43]

- Time Stamp Counter Tag '81'
Content:
Counter for MIKEY replay protection in MSK delivery. The counter is associated with the particular MUK. The length value is defined in TS 33.246 [43].
Coding:
As defined in TS 33.246 [43]

Unused bytes shall be set to 'FF'.

4.2.82 Void

4.2.83 EF_{GBANL} (GBA NAF List)

If service n°68 is "available", this file shall be present.

This EF contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure.

Identifier: '6FDA'	Structure: Linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z	NAF Key Identifier TLV objects	M	Z bytes

NAF Key Identifier tags

Description	Tag Value
NAF_ID Tag	'80'
B-TID Tag	'81'

NAF Key Identifier information

Description	Value	M/O	Length (bytes)
NAF_ID Tag	'80'	M	1
Length	X	M	Note
NAF_ID value	--	M	X
B-TID Tag	'81'	M	1
Length	Y	M	Note
B-TID value	--	M	Y
Note: The length is coded according to ISO/IEC 8825-1 [35]			

- NAF_ID Tag '80'

Contents:
Identifier of Network Application Function used in the GBA_U NAF Derivation procedure.
Coding:
As defined in TS 33.220 [42]

- B-TID Tag '81'

Content:
Bootstrapping Transaction Identifier of the GBA_U bootstrapped key
Coding:
As defined in TS 33.220 [42]

Unused bytes shall be set to 'FF'

4.2.84 EF_{EHPLMN} (Equivalent HPLMN)

If service n°71 is "available", this file shall be present.

This EF contains the coding for n EHPLMNs. The usage of EHPLMN is defined in TS 23.122 [31]. This data field may contain the HPLMN code derived from the IMSI as an EHPLMN entry.

Identifier: '6FD9'	Structure: transparent	Optional
SFI: '1D'		
File size: 3n, (n ≥1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st EHPLMN (highest priority)	M	3 bytes
4 to 6	2nd EHPLMN	O	3 bytes
:	:		
(3n-2) to (3n)	nth EHPLMN (lowest priority)	O	3 bytes

- EHPLMN

Contents:
- Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:
- according to TS 24.008 [9].

Unused entries shall be set to 'FF FF FF'

4.2.85 $EF_{EHPLMNPI}$ (Equivalent HPLMN Presentation Indication)

If service n°71 and service n°73 are "available", this file shall be present.

This EF contains an indication to the ME for the presentation of the available EHPLMN(s). The usage of the EHPLMN presentation indication is defined in TS 23.122 [31].

Identifier: '6FDB'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	EHPLMN Presentation Indication	M	1 byte

- EHPLMN Presentation Indication:
  Contents:
  EHPLMN display mode

Coding:
- '00' - No preference for the display mode
- '01' - Display the highest-priority available EHPLMN only
- '02' - Display all the available EHPLMNs
- All other values are RFU

4.2.86 $EF_{LRPLMNSI}$ (Last RPLMN Selection Indication)

If service n°74 is "available", this file shall be present.

This EF contains an indication to the ME for the selection of the RPLMN or the home network at switch on, or following recovery from lack of coverage. The usage of the Last RPLMN Selection Indication is defined in TS 23.122 [31].

Identifier: '6FDC'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Last RPLMN Selection Indication	M	1 byte

- Last RPLMN Selection Indication:
  Contents:
  Last RPLMN Selection Indication

Coding:
- '00' - The UE shall attempt registration on the last RPLMN at switch-on or recovery from out-of-coverage as described in TS 23.122 [31]
- '01' - The UE shall attempt registration either on the HPLMN or the last RPLMN at switch-on or recovery from out-of-coverage as described in TS 23.122 [31]
- All other values are RFU

4.2.87 EF_{NAFKCA} (NAF Key Centre Address)

If service n°68 and service n°76 are "available", this file shall be present.

This EF contains one or more NAF Key Centre addresses. The first record in the EF shall be considered to be of the highest priority. The last record in the EF shall be considered to be the lowest priority.

Identifier: '6FDD'	Structure: Linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z	NAF Key Centre TLV object	M	Z bytes

Unused bytes shall be set to 'FF'.

NAF Key Centre tags

Description	Tag Value
NAF Key Centre address Tag	**'80'**

NAF Key Centre information

Description	Value	M/O	Length (bytes)
NAF Key Centre address Tag	**'80'**	**M**	**1**
Length	**X**	**M**	**Note**
NAF Key Centre address value	**--**	**M**	**X**
Note: The length is coded according to ISO/IEC 8825-1 [35].			

- NAF Key Centre Address value (Tag '80')

  Contents:
  Fully qualified Domain Name (FQDN) of the NAF Key Centre used in the Local Key Establishment procedures (see TS 33.110 [47]).

  Coding:
  Encoded to an octet string according to UTF-8 encoding rules as described in IETF RFC 3629 [48].

4.2.88 EF_{SPNI} (Service Provider Name Icon)

If service n°78 is "available", this file shall be present.

This EF may contain one or several links to the service provider name icon. When more than one link is available, it is up to the ME to choose the link type to be used (e.g. the link type that is supported by the ME). The requirements for the display by the ME are defined in section 4.2.12.

Identifier: '6FDE'	Structure: transparent	Optional
File Size: X bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Icon TLV object(s)	M	X bytes

This file may contain one or several service provider name Icon TLV object(s). The coding of the service provider name Icon TLV objects is described hereafter:

Length	Description	Value	Status
1 byte	Icon Tag (See Note 1)	--	M
1 byte	Length (see Note 2)	Y+1	M
1 byte	Icon Qualifier	--	M
Y bytes	Icon Link	--	M
Note 1: The tag value indicates the type and format of the Icon Link that is provided in the TLV value field (e.g. Tag '80' indicates that the Icon link is a URI, while Tag '81' indicates that the Icon Link is the record number of the corresponding image in EF_{IMG}). Note 2: coded according to ISO/IEC 8825-1 [35].			

- Icon Tag
  Contents: Tag value.

  - When the Icon Link is an URI, the Tag value shall be set to '80'.

  - When the Icon Link is a pointer to the record number of the corresponding image in EF_{IMG}, the Tag value shall be set to '81'.

- All other values are RFU.

Coding: binary.

- Icon Qualifier

Contents: The icon qualifier indicates to the ME how the icon shall be used.

- '01' = icon is self-explanatory, i.e. if displayed, it replaces the corresponding name in text format.

- '02' = icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the corresponding name in text format.

- All other values are RFU.

Coding: binary.

- Icon Link

Contents: Link to the icon. This link shall point to a UICC resource.

Coding:

- When the Tag value indicates an URI (i.e. Tag = '80') , the Icon Link shall be encoded to an octet string according to UTF-8 encoding rules as described in IETF RFC 3629 [48] (e.g. http://127.0.0.1:3516/pub/files/spng.jpg).

- When the Tag value indicates that the Icon Link contains the record number of the corresponding image in EF_{IMG} (i.e. Tag = '81'), the Icon Link shall be encoded in binary.

4.2.89 EF_{PNNI} (PLMN Network Name Icon)

If service n°79 is "available", this file shall be present.

This EF contains one or several links to the PLMN network name icon. When more than one link is available in a record, it is up to the ME to choose the link type to be used (e.g. the link type that is supported by the ME).

Identifier: '6FDF'	Structure: linear fixed	Optional
Record length: X bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Icon TLV object(s)	M	X bytes

Each record may contain one or several PLMN network name Icon TLV object(s). The coding of the Icon TLV object(s) is described in EF_{SPNI}.

4.2.90 EF_{NCP-IP} (Network Connectivity Parameters for USIM IP connections)

If service n°80 is "available", this file shall be present.

This EF contains the network activation parameters to be used by the ME for establishing a data channel (e.g. PDP context activation) for UICC remote IP connectivity as described in ETSI TS 102 483 [50].

Each record contains a network connectivity parameters set. A network connectivity parameters set may comprise an Access Point Name, a Login and Password of the Access Point Name, a Data Destination Address Range and the Bearer Description. The priority order of the different Network Connectivity Parameters sets is the same as the order of the record numbers.

Each network connectivity parameters set provides a condition and the network connectivity parameters to be used when this condition is met:

- The network activation parameters present in a record shall be associated with this Data Destination Address Range in the same record (i.e. if a record contains a Data Destination Address Range, all IP packets that are sent by the UICC to any network destination address belonging to this Address Range shall transit through a network connection established using the parameters provided in that record).

  Note: A Data Destination Address Range TLV with a zero length prefix matches all addresses of the address type.

In a record, if the Access Point Name has a value part, the associated Login and Password may be provided. If supported by the ME, the Login and Password may be used for Access Point Name authentication. If only the Login is present, the ME shall use its default Password configuration if any. If the Login and Password are not present, the ME shall use its default Login/Password configuration if any. If no authentication is requested, the Login and Password shall be ignored. The Password TLV can only be provided in a record if a Login TLV is provided in the same record.

In any record, if the Access Point Name has no value part, the ME may use its default Access Point Name or the default subscription value together with the other network connectivity parameters of that record.

When present, the Bearer Description TLV provides recommended values for parameters that the ME should use to establish the data link for UICC remote IP connections. However if the ME or network does not support these values, the ME selects the most appropriate values.

Structure of EF_{NCP-IP}

Identifier: '6FE2'	Structure: linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to M	Data Destination Address Range TLV	M	M bytes
M+1 to M+N	Access Point Name TLV	M	N bytes
M+N+1 to M+N+O	Login TLV	C	O bytes
M+N+O+1 to M+N+O+P	Password TLV	C	P bytes
M+N+O+P+1 to M+N+O+P+Q	Bearer description TLV	C	Q bytes

- Access Point Name TLV
  Contents: Access Point Name provides information to the ME necessary to identify the Gateway entity which provides interworking with an external packet data network.

  Coding: the coding of the Access Point Name TLV object is described hereafter. The Access Point Name Value is coded as defined in TS 23.003 [25].

Length	Description	Value	Status
1 byte	Access Point Name Tag	80	M
1 byte	Length (see note 1)	X	M
1 byte	Access Point Name Value	--	M
Note 1: coded according to ISO/IEC 8825-1 [35].			

- Login TLV
  Contents: the login of the Access Point Name.

Coding: the coding of the Login TLV object is described hereafter. The Login Value is coded as for SMS Data coding scheme defined in TS 23.038 [5]. Parts of the data coding scheme other than the character set indication shall be ignored.

Length	Description	Value	Status
1 byte	Login Tag	81	M
1 byte	Length (see note 1)	X	M
1 byte	Login Value	--	M
Note 1: coded according to ISO/IEC 8825-1 [35].			

- Password TLV
  Contents: the password of the Access Point Name.

  Coding: the coding of the Password TLV object is described hereafter. The Password Value is coded as for SMS Data coding scheme defined in TS 23.038 [5]. Parts of the data coding scheme other than the character set indication shall be ignored.

Length	Description	Value	Status
1 byte	Password Tag	82	M
1 byte	Length (see note 1)	X	M
1 byte	Password Value	--	M
Note 1: coded according to ISO/IEC 8825-1 [35].			

- Data Destination Address Range TLV
  Contents: the data destination address or the range of data destination addresses.

  Coding: the coding of the Data Destination Address Range TLV object is described hereafter.

Length	Description	Value	Status
1 byte	Data Destination Address Range Tag	83	M
1 byte	Length (see note1)	X	M
1 byte	Type of Address	--	M
1 byte	Prefix length (in bits)	'00' to '20' for Ipv4 '00' to '80' for Ipv6	M
0 to 16 bytes	Prefix	--	
Note 1: coded according to ISO/IEC 8825-1 [35].			

  - Type of Address

    Contents: the type of data destination address range.

    Coding:

    - '21' = Ipv4 address range;
    - '57' = Ipv6 address range;
    - Other values are RFU.

  - Prefix length

    Contents: the number N of valid bits of the prefix of the address range. A prefix length of zero denotes the default "all IP addresses" range.

    Coding: binary

  - Prefix

Contents: Prefix, i.e. the leftmost bits of the address range. All addresses where the leftmost N bits match the prefix belong to the address range.

Coding:

- the leftmost N bits encode the prefix of the address range. If N is not an integer multiple of 8, the prefix is right padded with zeroes to the next octet boundary.

- Bearer Description TLV
  Contents: bearer description.

  Coding: the coding of the Bearer Description TLV object is described hereafter. The Bearer Description Value is encoded as the value part of the "Bearer description" TLV data object defined in TS 31.111 [12].

Length	Description	Value	Status
1 byte	Bearer Description Tag	84	M
1 byte	Length (see note 1)	X	M
1 byte	Bearer Description Value	--	M
Note 1: coded according to ISO/IEC 8825-1 [35].			

Any unused bytes shall be set to 'FF'.

4.2.91 $EF_{EPSLOCI}$ (EPS location information)

If service n°85 is "available", this file shall be present.

This EF contains the following EPS location information:

- Globally Unique Temporary Identifier (GUTI);
- Last visited registered Tracking Area Identity (TAI);
- EPS update status.

Identifier: '6FE3'	Structure: transparent	Optional
SFI: '1E'		
File size: 18 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 12	GUTI	M	12 bytes
13 to17	Last visited registered TAI	M	5 bytes
18	EPS update status	M	1 byte

- GUTI.
  Contents:

  Globally Unique Temporary Identifier.

  Coding:

  as the GUTI part of the EPS mobile identity information element defined in TS 24.301 [51]. Byte 1 corresponds to "octet 2" of an EPS mobile identity information element containing a GUTI. Byte 12 corresponds to "octet 13" of an EPS mobile identity information element information element containing a GUTI.

  Byte 1: first byte of GUTI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- Last visited registered TAI
  Contents:

  Last visited registered Tracking Area Identity.

  Coding:

  as the content of the tracking area identity information element defined in TS 24.301 [51]. Byte 13 corresponds to "octet 2" of a tracking area identity information element. Byte 17 corresponds to "octet 6" of a tracking area identity information element.

  Byte 13: first byte of last visited registered TAI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- EPS update status.
  Contents:

  status of EPS update according to TS 24.301 [51].

  Coding:

  byte 18:

  Bits: b3 b2 b1.

b3	b2	b1	
0	0	0	: UPDATED.
0	0	1	: NOT UPDATED.
0	1	0	: ROAMING NOT ALLOWED.
0	1	1	: reserved.
1	0	0	: reserved.
1	0	1	: reserved.
1	1	0	: reserved.
1	1	1	: reserved.

  Bits b4 to b8 are RFU (see TS 31.101 [11]).

Unused bytes shall be set to 'FF'.

4.2.92 EF_{EPSNSC} (EPS NAS Security Context)

If service n°85 is "available", this file shall be present.

This EF contains the EPS NAS Security context as defined in TS 33.401 [52]. This file shall contain only one record.

Identifier: '6FE4'	Structure: linear fixed	Optional
SFI: '18'		
Record size: X bytes (X≥54)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	EPS NAS Security Context TLV Object	M	X bytes

EPS NAS Security Context tags

Description	Tag Value
EPS NAS Security Context Tag	'A0'

EPS NAS Security Context information

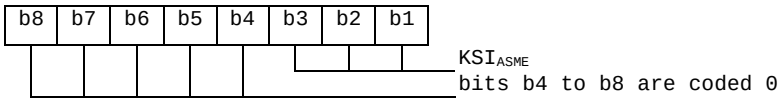
Description	Value	M/O	Length (bytes)
EPS NAS Security Context Tag	'A0'	M	1
Length (length of all subsequent data)	Y	M	Note 1
Key set identifier KSI_{ASME} Tag	'80'	M	1
Length	K	M	Note 1
Key set identifier KSI_{ASME}	--	M	K
ASME key (K_{ASME}) Tag	'81'	M	1
Length	L	M	Note 1
ASME key (K_{ASME})	--	M	L
Uplink NAS count Tag	'82'	M	1
Length	M	M	Note 1
Uplink NAS count	--	M	M
Downlink NAS count Tag	'83'	M	1
Length	N	M	Note 1
Downlink NAS count	--	M	N
Identifiers of selected NAS integrity and encryption algorithms Tag	'84'	M	1
Length	S	M	Note 1
Identifiers of selected NAS integrity and encryption algorithms	--	M	S
Note 1: The length is coded according to ISO/IEC 8825-1 [35]			

- Key set identifier KSI_{ASME} Tag '80'

  Contents:

  The ASME key set identifier as defined in TS 33.401 [52]. In this release the KSI_{ASME} is coded on 1 byte.

  Coding:



- ASME key (K_{ASME}) Tag '81'

Contents:

The ASME Key as defined in TS 33.401 [52]. In this release a valid ASME key is coded on 32 bytes. The ME shall treat any ASME key values stored in this EF as invalid if the ASME key set identifier indicates that no ASME key is available or if the length indicated in the ASME key TLV is set to '00',

Coding:

The most significant bit of K_{ASME} is the most significant bit of the 1st byte of this TLV value field. The least significant bit of K_{ASME} is the least significant bit of the last byte of this TLV value field.

- Uplink NAS count Tag '82'

Contents:

The uplink NAS count as defined in TS 33.401 [52]. In this release the Uplink NAS count is coded on 4 bytes.

Coding:

The most significant bit of the uplink NAS count is the most significant bit of the 1st byte of this TLV value field. The least significant bit of the uplink NAS count is the least significant bit of the last byte of this TLV value field.

- Downlink NAS count Tag '83'

Contents:

The downlink NAS count as defined in TS 33.401 [52]. In this release the downlink NAS count is coded on 4 bytes.

Coding:

The most significant bit of the downlink NAS count is the most significant bit of the 1st byte of this TLV value field. The least significant bit of the downlink NAS count is the least significant bit of the last byte of this TLV value field.

- Identifiers of selected NAS integrity and encryption algorithms Tag '84'

Contents:

The identifiers of selected NAS integrity and encryption algorithms as defined in TS 33.401 [52] and TS 24.301 [51]. In this release the identifiers of selected NAS integrity and encryption algorithms are coded on 1 byte.

Coding:

as the content of the NAS security algorithms information element defined in TS 24.301 [51].

Byte 1 of this TLV value field: first byte of the NAS security algorithms information element

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

Unused bytes shall be set to 'FF'.

In order to mark the stored EPS NAS security context as invalid, the record bytes shall be set to 'FF'.

4.2.93 EF_{UFC} (USAT Facility Control)

This EF contains data for USAT Facility Control related to AT commands for USAT (see TS 31.111 [12]).

Identifier: '6FE6'	Structure: transparent	Optional
File size: X bytes, (X ≥ 1)	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Facility list	M	X bytes

The facility list has the same format as the TERMINAL PROFILE defined in TS 31.111 [12].

By setting the corresponding bits to 1, the facility list defines facilities which can only be provided by the MT and which are not allowed to be provided by the TE.

If a TERMINAL PROFILE is longer than the facility list, for the purpose of facility control, the exceeding bytes of the TERMINAL PROFILE shall be compared according to the generic rules found in TS 31.111 [12].

4.2.94 $EF_{NASCONFIG}$ (Non Access Stratum Configuration)

If service n°96 is "available", this file shall be present. This EF contains NAS configuration parameters defined in TS 24.368 [65]. The parameters in $EF_{NASCONFIG}$ shall take precedence over the corresponding parameters stored in the ME's non-volatile memory.

Identifier: '6FE8'	Structure: transparent	Optional
File size: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z	NAS configuration parameter TLV objects	M	Z bytes

NAS configuration parameter information

Description	**Value**	**M/O/C**	**Length (bytes)**

NAS signalling priority Tag	'80'	O	1
Length	L1	C	Note 1
NAS signalling priority value	--	C	L1
NMO I Behaviour Tag	'81'	O	1
Length	L2	C	Note 1
NMO I Behaviour value	--	C	L2
Attach with IMSI Tag	'82'	O	1
Length	L3	C	Note 1
Attach with IMSI value	--	C	L3
Minimum Periodic Search Timer Tag	'83'	O	1
Length	L4	C	Note 1
Minimum Periodic Search Timer value	--	C	L4
Extended access barring Tag	'84'	O	1
Length	L5	C	Note 1
Extended access barring value	--	C	L5
Timer T3245 Behaviour Tag	'85'	O	1
Length	L6	C	Note 1
Timer T3245 Behaviour value	--	C	L6
Override NAS signalling low priority Tag	'86'	O	1
Length	L7	C	Note 1
Override NAS signalling low priority value	--	C	L7
Override Extended access barring Tag	'87'	O	1
Length	L8	C	Note 1
Override Extended access barring value	--	C	L8
Note 1 : The length is coded according to ISO/IEC 8825-1 [35] Note 2: C; if the Tag is present, this is mandatory.			

- NAS signalling priority

  Contents:

  As described in TS 24.368 [65], used to determine the NAS signalling priority included in NAS messages.

  Coding:

  As defined for the NAS_SignallingPriority leaf in TS 24.368 [65].

- NMO I Behaviour

  Content:

  As described in TS 24.368 [65], indicates whether the "NMO I, Network Mode of Operation I" indication is applied by the UE.

  Coding:

```
b8 b7 b6 b5 b4 b3 b2 b1
                       b1 value to be interpreted as defined for the
                       NMO_I_Behaviour leaf in TS 24.368 [65].

                       RFU (see TS 31.101 [11])
```

- Attach with IMSI

  Content:

  As described in TS 24.368 [65], indicates whether attach with IMSI is performed when moving to a non-equivalent PLMN.

  Coding:

```
b8 b7 b6 b5 b4 b3 b2 b1
                       b1 value to be interpreted as defined for the
                       AttachWithIMSI leaf in TS 24.368 [65].

                       RFU (see TS 31.101 [11])
```

- Minimum Periodic Search Timer

Content:

As described in TS 24.368 [65], gives a minimum value in minutes for the timer T controlling the periodic search for higher prioritized PLMNs. The content applies a minimum value that may override the value in file EF_{HPPLMN} (Higher Priority PLMN search period), as specified in TS 23.122 [31] clause 4.4.3.3.1.

Coding:

As defined for the MinimumPeriodicSearchTimer leaf in TS 24.368 [65].

- Extended access barring

Content:

As described in TS 24.368 [65], indicates whether the UE applies extended access barring.

Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
								b1 value to be interpreted as defined for ExtendedAccessBarring leaf in TS 24.368 [65].
								RFU (see TS 31.101 [11])

- Timer T3245 Behaviour

Content:

As described in TS 24.368 [65], indicates whether the timer T3245 and the related functionality is used by the UE.

Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
								b1 value to be interpreted as defined for Timer_T3245_Behaviour leaf in TS 24.368 [65].
								RFU (see TS 31.101 [11])

- Override NAS signalling low priority

Contents:

As described in TS 24.368 [65], used to determine whether the NAS signalling priority included in NAS messages can be overriden.

Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
								b1 value to be interpreted as defined for the Override_NAS_SignallingLowPriority leaf in TS 24.368 [65].
								RFU (see TS 31.101 [11])

- Override Extended access barring

Contents:

As described in TS 24.368 [65], used to determine whether the Extended access barring included in NAS messages can be overriden.

Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
								b1 value to be interpreted as defined for the Override_ ExtendedAccessBarring leaf in TS 24.368 [65].
								RFU (see TS 31.101 [11])

Unused bytes shall be set to 'FF'.

4.2.95 $EF_{UICCIARI}$ (UICC IARI)

If service n°95 is "available", this file shall be present.

As specified in TS 24.229 [63] a ME includes the list of IARIs for the IMS applications it intends to use when sending an initial registration or when sending subsequent registrations to the IMS in the form of a SIP REGISTER request.

This EF contains a list of IARIs associated with active applications installed on the UICC that are included in the SIP REGISTER request in accordance with the procedures of TS 24.229 [63].

NOTE: If this file is present in both the USIM and the ISIM, the file in the ISIM is used. It is assumed that the presence of this file in the USIM when an ISIM is present on the UICC is an incorrect configuration of the UICC.

Identifier: '6FE7'	Structure: linear fixed	Optional
Record length: X bytes.	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	IARI TLV object	M	X bytes

IARI TLV object:

Contents:

- The content and coding is defined below.

Coding of the IARI TLV objects

Length	Description	Value	Status
1 byte	IARI TLV TAG	'80'	M
1 byte	Length of IARI	Y	M
Y bytes	IARI value	-	M

- Coding:

  IMS Application Reference Identifier: shall be coded as specified in TS 24.229 [63].

Unused bytes shall be set to 'FF'.

4.2.96 EF_{PWS} (Public Warning System)

If service n°97 is "available", this file shall be present. This EF contains the configuration parameters for PWS, as defined in TS 22.268 [68].

Identifier: '6FEC'	Structure: transparent	Optional
File size: 1+Z bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z+1	PWS configuration	M	1+Z bytes

Contents:

Configuration for PWS

Coding:

First byte:

b8	b7	b6	b5	b4	b3	b2	b1

```
b1=0 process all PWS warning messages in HPLMN and
equivalent PLMNs
b1=1 ignore all PWS warning messages in HPLMN and
equivalent PLMNs
b2=0 process all PWS warning messages in VPLMNs
b2=1 ignore all PWS warning messages in VPLMNs
RFU (see TS 31.101 [11])
```

Successive bytes:

RFU (see TS 31.101 [11])

4.3 DFs at the USIM ADF (Application DF) Level

DFs may be present as child directories of USIM ADF. The following DFs are defined:

$DF_{PHONEBOOK}$ '5F3A' (see Note 2).

$DF_{GSM\text{-}ACCESS}$ '5F3B'.

DF_{MexE} '5F3C'.

DF_{WLAN} '5F40'.

DF_{HNB} '5F50'

DF_{SoLSA} '5F70'

DF_{BCAST} '5F80' (see Note 1).

Note 1: The DF identifier '5F80' is reserved for OMA BCAST Smart Card Profile [49]

Note 2: DF for application specific phonebook. This DF has the same structure as the $DF_{PHONEBOOK}$ under $DF_{TELECOM}$.

4.4 Contents of DFs at the USIM ADF (Application DF) level

4.4.1 Contents of files at the DF SoLSA level

This only applies if the Support of Localised Service Areas is supported, as indicated by Service Number 23 in the USIM Service Table and specified in TS 23.073 [23] .

The Efs contain information about the users subscribed local service areas.

4.4.1.1 EF_{SAI} (SoLSA Access Indicator)

This EF contains the 'LSA only access indicator'. This EF shall always be allocated if DF_{SoLSA} is present.

If the indicator is set, the network will prevent terminated and/or originated calls when the MS is camped in cells that are not included in the list of allowed LSAs in EF_{SLL}. Emergency calls are, however, always allowed.

The EF also contains a text string which may be displayed when the MS is out of the served area(s).

Identifier: '4F30'	Structure: transparent	Optional
File size: X + 1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	LSA only access indicator	M	1 byte
2 to X+1	LSA only access indication text	M	X bytes

- LSA only access indicator

Contents: indicates whether the MS is restricted to use LSA cells only or not.

Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
								b1=0: LSA only access not activated
								b1=1: LSA only access activated
								RFU

- LSA only access indication text

Contents: text to be displayed by the ME when it's out of LSA area.

Coding: the string shall use either

- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
- one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

4.4.1.2 EF_{SLL} (SoLSA LSA List)

This EF contains information describing the LSAs that the user is subscribed to. This EF shall always be allocated if DF_{SoLSA} is present.

Each LSA is described by one record that is linked to a LSA Descriptor file. Each record contains information of the PLMN, priority of the LSA, information about the subscription and may also contain a text string and/or an icon that identifies the LSA to the user. The text string can be edited by the user.

Identifier: '4F31'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	LSA name	O	X bytes
X+1	Configuration parameters	M	1 byte
X+2	RFU	M	1 byte
X+3	Icon Identifier	M	1 byte
X+4	Priority	M	1 byte
X+5 to X+7	PLMN code	M	3 bytes
X+8 to X+9	LSA Descriptor File Identifier	M	2 byte
X+10	LSA Descriptor Record Identifier	M	1 byte

- LSA name

  Contents: LSA name string to be displayed when the ME is camped in the corresponding area, dependant on the contents of the LSA indication for idle mode field.

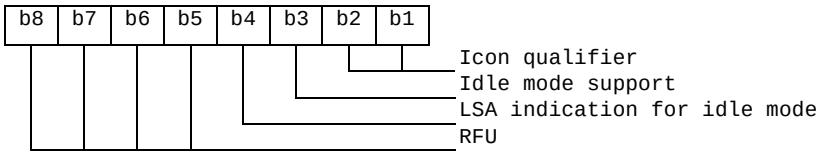
Coding: the string shall use either

- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
- one of theUCS2 code options defined in the annex of TS 31.101 [11].

- Configuration parameters

Contents: Icon qualifier, control of idle mode support and control of LSA indication for idle mode.

Coding:



Icon qualifier:

Contents: The icon qualifier indicates to the ME how the icon is to be used.

B2, b1: 00: icon is not to be used and may not be present
01: icon is self-explanatory, i.e. if displayed, it replaces the LSA name
10: icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the LSA name
11: RFU

Idle mode support:

Contents: The idle mode support is used to indicate whether the ME shall favour camping on the LSA cells in idle mode.

B3 = 0: Idle mode support disabled
b3 = 1: Idle mode support enabled

LSA indication for idle mode:

Contents: The LSA indication for idle mode is used to indicate whether or not the ME shall display the LSA name when the ME is camped on a cell within the LSA.

B4 = 0: LSA indication for idle mode disabled
b4 = 1: LSA indication for idle mode enabled

Bits b5 to b8 are RFU (see subclause 9.3).

- Icon Identifier

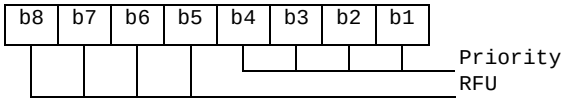
Contents: The icon identifier addresses a record in EF_{IMG}.

Coding: binary.

- Priority

  Contents: Priority of the LSA which gives the ME the preference of this LSA relative to the other LSAs.

  Coding:



'0' is lowest priority, 'F' is highest.

- PLMN code

Contents: MCC + MNC for the LSA.

Coding: according to TS 24.008 [9] and EF_{LOCI}.

- LSA Descriptor File Identifier:

Contents: these bytes identify the EF which contains the LSA Descriptors forming the LSA.

Coding: byte X+8: high byte of the LSA Descriptor file;
byte X+9: low byte of the LSA Descriptor file.

- LSA Descriptor Record Identifier:

Contents: this byte identifies the number of the first record in the LSA Descriptor file forming the LSA.

Coding: binary.

4.4.1.3 LSA Descriptor files

Residing under DF_{SoLSA}, there may be several LSA Descriptor files. These Efs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA Ids, as a list of LAC + Cis, as a list of Cis or as a list of LACs. As the basic elements (LSA ID, LAC + CI, CI and LAC) of the four types of lists are of different length, they can not be mixed within one record. Different records may contain different kinds of lists within the Efs. Examples of codings of LSA Descriptor files can be found in annex F.

Identifier: '4FXX'	Structure: linear fixed	Optional
Record length: n*X+2 bytes	Update activity: low	

Access Conditions:

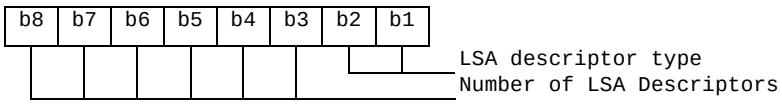
READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	LSA descriptor type and number	M	1 byte
2 to X+1	1st LSA Descriptor	M	X bytes
X+2 to 2X+1	2nd LSA Descriptor	M	X bytes
:	:	:	:
(n-1)*X+2 to n*X+1	nth LSA Descriptor	M	X bytes
n*X+2	Record Identifier	M	1 byte

- LSA descriptor type and number:

  Contents: The LSA descriptor type gives the format of the LSA descriptor and the number of valid LSA Descriptors within the record.

Coding:



LSA descriptor type:

Contents: Gives the format of the LSA Descriptors.

B2, b1: 00: LSA ID.
01: LAC + CI
10: CI
11: LAC

Number of LSA Descriptors:

Contents: Gives the number of valid LSA Descriptors in the record.

Coding: binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor

Contents: Dependant of the coding indicated in the LSA descriptor type:

- in case of LSA ID the field length 'X' is 3 bytes;
- in case of LAC + CI the field length 'X' is 4 bytes;
- in case of CI the field length 'X' is 2 bytes;
- in case of LAC the field length 'X' is 2 bytes.

Coding: according to TS 24.008 [9].

- Record Identifier:

  Contents: This byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

Coding: record number of next record. 'FF' identifies the end of the chain.

This file utilises the concept of chaining as for EF_{EXT1}.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of EF_{SAI} and EF_{SLL}. For the range of 'XX', see TS 31.101 [11].

4.4.2 Contents of files at the DF PHONEBOOK level

The Efs in the $DF_{PHONEBOOK}$ level contain phone book related features as required in TS 21.111 [1].

The UICC may contain a global phonebook, or application specific phonebooks, or both in parallel. When both phonebook types co-exist, they are independent and no data is shared. In this case, it shall be possible for the user to select which phonebook the user would like to access. To achieve this, the terminal shall support the global and the application specific phonebooks.

It is recommended that the terminal searches for the global phonebook located under $DF_{TELECOM}$ as its presence is not indicated anywhere in the USIM application.

The global phonebook is located in $DF_{PHONEBOOK}$ under $DF_{TELECOM.}$. Each specific USIM application phonebook is located in $DF_{PHONEBOOK}$ of its respective Application ADF_{USIM}. The organisation of files in $DF_{PHONEBOOK}$ under ADF_{USIM} and under DF $_{TELECOM}$ follows the same rules. Yet $DF_{PHONEBOOK}$ under ADF_{USIM} may contain a different set of files than $DF_{PHONEBOOK}$ under $DF_{TELECOM}$. All phonebook related Efs are located under their respective $DF_{PHONEBOOK}$. USIM specific phonebooks are dedicated to application specific entries. Each application specific phonebook is protected by the application PIN.

EF_{ADN} and EF_{PBR} shall always be present if the $DF_{Phonebook}$ is present. If any phonebook file other than EF_{ADN} or $EF_{EXT1,}$ is used, then EF_{PBC} shall be present.

If a GSM application resides on the UICC, the Efs ADN and EXT1 from one $DF_{PHONEBOOK}$ (defined at GSM application installation) are mapped to $DF_{TELECOM}$. Their file Ids are specified in TS 51.011 [18], i.e. EF_{ADN} = '6F3A' and EF_{EXT1} = '6F4A', respectively.

If the UICC is inserted into a terminal accessing the ADN and EXT1 files under $DF_{TELECOM}$; and a record in these files has been updated, a flag in the corresponding entry control information in the EF_{PBC} is set from 0 to 1 by the UICC. If the UICC is later inserted into a terminal that supports the global and/or application specific phonebook, the terminal shall check the flag in EF_{PBC} and if this flag is set, shall update the EF_{CC}, and then reset the flag. A flag set in EF_{PBC} results in a full synchronisation of the phonebook between an external entity and the UICC (if synchronisation is requested).

The EF structure related to the public phonebook is located under $DF_{PHONEBOOK}$ in $DF_{TELECOM}$. A USIM specific phonebook may exist for application specific entries. The application specific phonebook is protected by the application PIN. The organisation of files in the application specific phonebook follows the same rules as the one specified for the public phone book under $DF_{TELECOM}$. The application specific phonebook may contain a different set of files than the one in the public area under $DF_{TELECOM}$.

4.4.2.1 EF_{PBR} (Phone Book Reference file)

This file describes the structure of the phonebook. All Efs representing the phonebook are specified here (with the exception of EF_{PSC}, EF_{PUID} and EF_{CC}), together with their file identifiers (FID) and their short file identifiers (SFI), if applicable.

Certain kinds of Efs can occur more than once in the phonebook, e.g. there may be two entities of Abbreviated Dialling Numbers, EF_{ADN} and EF_{ADN1}. For these kinds of Efs, no fixed FID values are specified. Instead, the value '4FXX' indicates that the value is to be assigned by the card issuer. These assigned values are then indicated in the associated TLV object in EF_{PBR}.

The SFI value assigned to an EF which is indicated in EF_{PBR} shall correspond to the SFI indicated in the TLV object in EF_{PBR}.

The reference file is a file that contains information how the information in the different files is to be combined together to form a phone book entry. The reference file contains records. Each record specifies the structure of up to 254 entries in the phone book. Each phone book entry consists of data stored in files indicated in the reference file record. The entry structure shall be the same over all the records in the EF $_{PBR}$. If more than 254 entries are to be stored, a second record is needed in the reference file. The structure of a phone book entry is defined by different TLV objects that are stored in a reference file record. The reference file record structure describes the way a record in a file that is part of the phonebook is used to create a complete entry. Three different types of file linking exist.

Type 1 files: Files that contain as many records as the reference/master file (EF_{ADN}, EF_{ADN1}) and are linked on record number bases (Rec1 -> Rec1). The master file record number is the reference.

Type 2 files: Files that contain less entries than the master file and are linked via pointers in the index administration file (EF_{IAP}).

Type 3 files: Files that are linked by a record identifier within a record.

Table 4.1: Phone Book Reference file Constructed Tags

Tag Value	Constructed TAG Description
'A8'	Indicating files where the amount of records equal to master EF, type 1
'A9'	Indicating files that are linked using the index administration file, type 2. Order of pointer appearance in index administration EF is the same as the order of file Ids following this tag
'AA'	Indicating files that are linked using a record identifier, type 3. (The file pointed to is defined by the TLV object.)

The first file ID in the first record of EF_{PBR} indicated using constructed Tag 'A8' is called the master EF. Access conditions for all other files in the Phonebook structure using Tags 'A8', 'A9' or 'AA' is set to the same as for the master EF unless otherwise specified in the present document.

File Ids indicated using constructed Tag 'A8' is a type 1 file and contains the same number of records as the first file that is indicated in the data part of this TLV object. All files following this Tag are mapped one to one using the record numbers/Ids of the first file indicated in this TLV object.

File Ids indicated using constructed Tag 'A9' are mapped to the master EF (the file ID indicated as the first data object in the TLV object using Tag 'A8') using the pointers in the index administration file. The order of the pointers in the index administration file is the same as the order of the file Ids presented after Tag 'A9'. If this Tag is not present in the reference file record the index administration file is not present in the structure. In case the index administration file is not present in the structure it is not indicated in the data following tag 'A8'.

File Ids indicated using constructed Tag 'AA' indicate files that are part of the reference structure but they are addressed using record identifiers within a record in one or more of the files that are part of the reference structure. The length of the tag indicates whether the file to be addressed resides in the same directory or if a path to the file is provided in the TLV object.

Type 2 and type 3 files contain records that may be shared between several phonebook entries (except when otherwise indicated). The terminal shall ensure that a shared record is emptied when the last phonebook entry referencing it is modified in such a way that it doesn't reference the record anymore.

NOTE: in the current version of the specification, only type 3 files contain records that may be shared.

Each constructed Tag contains a list of primitive Tags indicating the order and the kind of data (e.g. ADN, IAP,…) of the reference structure.

The primitive tag identifies clearly the type of data, its value field indicates the file identifier and, if applicable, the SFI value of the specified EF. That is, the length value of a primitive tag indicates if an SFI value is available for the EF or not:

- Length = '02' Value: 'FID (2 bytes)'

- Length = '03' Value: 'FID (2 bytes)', 'SFI (1 byte)'

Table 4.2: Tag definitions for the phone book kind of file

Tag Value	TAG Description
'C0'	EF_{ADN} data object
'C1'	EF_{IAP} data object
'C2'	EF_{EXT1} data object
'C3'	EF_{SNE} data object
'C4'	EF_{ANR} data object
'C5'	EF_{PBC} data object
'C6'	EF_{GRP} data object
'C7'	EF_{AAS} data object
'C8'	EF_{GAS} data object
'C9'	EF_{UID} data object
'CA'	EF_{EMAIL} data object
'CB'	EF_{CCP1} data object

Table 4.3 (below) lists the allowed types for each kind of file:

Table 4.3: Presence of files as type

File name	Type 1	Type 2	Type 3
EF_{AAS}			X
EF_{ADN}	X		
EF_{ANR}	X	X	
EF_{EMAIL}	X	X	
EF_{EXT1}			X
EF_{GAS}			X
EF_{GRP}	X		
EF_{IAP}	X		
EF_{PBC}	X		
EF_{SNE}	X	X	
EF_{UID}	X		
EF_{CCP1}			X

Phone Book Reference file EF_{PBR} structure

Identifier: '4F30'	Structure: linear fixed	Conditional (see Note)
Record Length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	TLV object(s) for indicating Efs that are part of the phone book structure	M	X bytes

NOTE: This file is mandatory if and only if $DF_{Phonebook}$ is present.

At the end of each record, unused bytes, if any, shall be filled with 'FF'.

4.4.2.2 EF_{IAP} (Index Administration Phone book)

This file is present if Tag 'A9' is indicated in the reference file.

The EF contains pointers to the different records in the files that are part of the phone book. The index administration file record number/ID is mapped one to one with the corresponding EF_{ADN} (shall be record to record). The index administration file contains the same amount of records as EF_{ADN}. The order of the pointers in an EF_{IAP} shall be the same as the order of file Ids that appear in the TLV object indicated by Tag 'A9' in the reference file record. The amount of bytes in a record is equal to the number of files indicated the EF_{PBR} following tag 'A9'.

The value 'FF' is an invalid record number/ID and is used in any location in to indicate that no corresponding record in the indicated file is available.

The content of EF_{IAP} is set to 'FF' at the personalisation stage.

Index administration file EF_{IAP} structure

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'YY'		
Record Length: X bytes, (X ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record number of the first object indicated after Tag 'A9'	M	1 byte
2	Record number of the second object indicated after Tag 'A9'	C	1 byte
X	Record number of the xth object indicated after Tag 'A9'	C	1 byte

NOTE 1: This file is mandatory if and only if type 2 files are present.
NOTE 2: x^{th}-field marked with 'C' is mandatory if x^{th}-object indicated following tag 'A9' is present in EF_{PBR}

4.4.2.3 EF_{ADN} (Abbreviated dialling numbers)

This EF contains Abbreviated Dialling Numbers (ADN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'YY'		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration1 Record Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

NOTE: This file is mandatory if and only if $DF_{PHONEBOOK}$ is present.

- Alpha Identifier.

Contents:
- Alpha-tagging of the associated dialling number.

Coding:
- this alpha-tagging shall use either:
  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

  Or:
  - one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the ME can determine the value of X.

- Length of BCD number/SSC contents.

Contents:
- this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see clause 4.4.2.4).

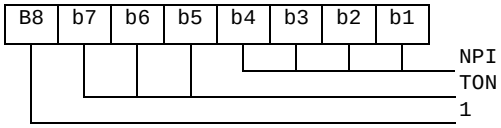
Coding:
- according to TS 24.008 [9].

- TON and NPI.

Contents:
- Type of number (TON) and numbering plan identification (NPI).

Coding:
- according to TS 24.008 [9]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see TS 24.008 [9]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.

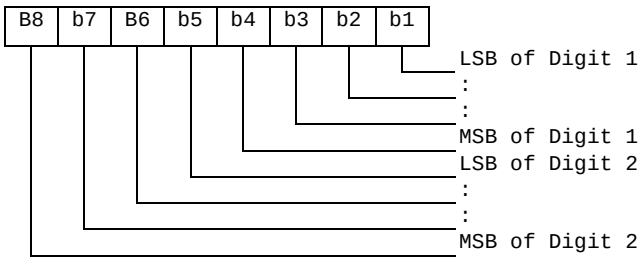


- Dialling Number/SSC String

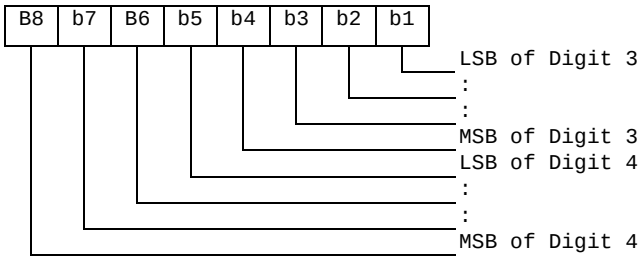
Contents:
- up to 20 digits of the telephone number and/or SSC information.

Coding:
- according to TS 24.008 [9], TS 22.030 [4] and the extended BCD-coding (see table 4.4). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the remainder is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the EF_{EXT1}. The record is identified by the Extension 1 Record Identifier. Excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3



Byte X+4:



etc.

- Capability/Configuration1 Record Identifier.

Contents:

- capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP1} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

Coding:

- binary.

- Extension1 Record Identifier.

Contents:

- extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.
- if the ADN/SSC requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see clause 4.4.2.4).

Coding:

- binary.

NOTE 3: EF_{ADN} in the public phone book under $DF_{TELECOM}$ may be used by USIM, GSM and also other applications in a multi-application card. If the non-GSM application does not recognise the use of Type of Number (TON) and Number Plan Identification (NPI), then the information relating to the national dialling plan shall be held within the data item dialling number/SSC and the TON and NPI fields set to UNKNOWN. This format would be acceptable for 3G operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

EXAMPLE: SIM storage of an International Number using E.164 [22] numbering plan.

	TON	NPI	Digit field.
USIM application	001	0001	abc...
Other application compatible with 3G	000	0000	xxx...abc...

where "abc..." denotes the subscriber number digits (including its country code), and "xxx..." denotes escape digits or a national prefix replacing TON and NPI.

NOTE 4: When the ME acts upon the EF_{ADN} with a SEARCH RECORD command in order to identify a character string in the alpha-identifier, it is the responsibility of the ME to ensure that the number of characters used as SEARCH RECORD parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 4.4: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
:	:
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (see TS 22.101 [24]).
'D'	"Wild" value. This will cause the MMI to prompt the user for a single digit (see TS 22.101 [24]).
'E'	RFU.
'F'	Endmark e.g. in case of an odd number of digits.

BCD values 'C', 'D' and 'E' are never sent across the radio interface.

NOTE 5: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 6: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see TS 22.101 [24]).

4.4.2.4 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC.

Extension data is caused by:

- an ADN/SSC which is greater than the 20 digit capacity of the ADN/SSC Elementary File or where common digits are required to follow an ADN/SSC string of less than 20 digits. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN/SSC Elementary File. The EXT1 record in this case is specified as additional data;

- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'YY'		
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

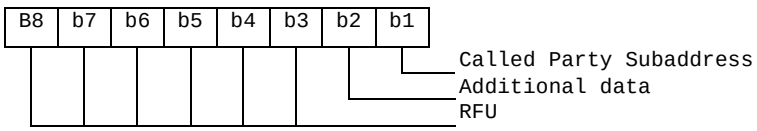
Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type.

Contents:

- type of the record.

Coding:



- b3 to b8 are reserved and set to 0;

- a bit set to 1 identifies the type of record;

- only one type can be set;

- '00' indicates the type "unknown" or "free".

The following example of coding means that the type of extension data is "additional data":

B8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	1	0

- Extension data.

Contents:
additional data or Called Party Subaddress depending on record type.

Coding:

Case 1, Extension1 record is additional data:

- The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC. The coding of remaining bytes is BCD, according to the coding of ADN/SSC. Unused nibbles at the end shall be set to 'F'. It is possible if the number of additional digits exceeds the capacity of the additional record to chain another record inside the EXT1 Elementary File by the identifier in byte 13. In this case byte 2 (first byte of the extension data) of all records for additional data within the same chain indicates the number of bytes ('01' to '0A') for ADN/SSC (respectively MSISDN, LND) within the same record unequal to 'FF'.

Case 2, Extension1 record is Called Party Subaddress:

- The subaddress data contains information as defined for this purpose in TS 24.008 [9]. All information defined in TS 24.008, except the information element identifier, shall be stored in the USIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier.

Contents:
identifier of the next extension record to enable storage of information longer than 11 bytes.

Coding:
record number of next record. 'FF' identifies the end of the chain.

- Example of a chain of extension records being associated to an ADN/SSC. The extension1 record identifier (Byte 14+X) of EF_{ADN} is set to 3.

	EF EXT1												
	Byte: 1	2	3	4	5	6	7	8	9	10	11	12	13
	Record Type	Extension data											Identifier
Record 1	01	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	FF
Record 2	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
▶ Record 3	02	0A	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	04
Record 4	02	04	xx	xx	xx	xx	FF	FF	FF	FF	FF	FF	06
Record 5	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
Record 6	01	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	01
⋮													

In this example, ADN/SSC is associated to additional data (records 3 and 4) which represent the last 27 or 28 digits of the whole ADN/SSC (the first 20 digits are stored in EF_{ADN}) and a called party subaddress whose length is more than 11 bytes (records 6 and 1).

4.4.2.5 EF_{PBC} (Phone Book Control)

This EF contains control information related to each entry in the phone book. This EF contains as many records as the EF_{ADN} associated with it (shall be record to record). Each record in EF_{PBC} points to a record in its EF_{ADN}. This file indicates the control information and the hidden information of each phone book entry.

The content of EF_{PBC} is linked to the associated EF_{ADN} record by means of the ADN record number/ID (there is a one to one mapping of record number/identifiers between EF_{PBC} and EF_{ADN}).

Structure of control file EF_{PBC}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'YY'		
Record length: 2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Entry Control Information	M	1 byte
2	Hidden Information	M	1 byte

NOTE: This file is mandatory if one or both of the following is true:
- hidden entries are supported
- a GSM SIM application is supported in the UICC.

- Entry Control Information.

Contents:

- provides some characteristics about the phone book entry e.g. modification by a terminal accessing the ADN and EXT1 files under $DF_{TELECOM}$ (see clause 4.4.2).

Coding:

b8	B7	b6	B5	b4	B3	b2	B1	
								Modified phonebook entry '1', no change '0'
								RFU (see TS 31.101)

- Hidden Information.

Contents:

indicates to which USIM application of the UICC this phone book entry belongs, so that the corresponding secret code can be verified to display the phone book entry. If the secret code is not verified, then the phone book entry is hidden.

Coding:

'00' – the phone book entry is not hidden;

'xx' – the phone book entry is hidden. 'xx' is the record number in EF_{DIR} of the associated USIM application.

4.4.2.6 EF_{GRP} (Grouping file)

This EF contains the grouping information for each phone book entry. This file contains as many records as the associated EF_{ADN}. Each record contains a list of group identifiers, where each identifier can reference a group to which the entry belongs.

Structure of grouping file EF_{GRP}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'YY'		
Record Length: X bytes (1 ≤ X ≤10)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Group Name Identifier 1	M	1 byte
2	Group Name Identifier 2	O	1 byte
X	Group Name Identifier X	O	1 byte

NOTE: This file is mandatory if and only if EF_{GAS} is present.

- Group Name Identifier x.

Content:
- indicates if the associated entry is part of a group, in that case it contains the record number of the group name in EF_{GAS}.
- One entry can be assigned to a maximum of 10 groups.

Coding:
- '00' – no group indicated;

'XX' – record number in EF_{GAS} containing the alpha string naming the group of which the phone book entry is a member.

4.4.2.7 EF_{AAS} (Additional number Alpha String)

This file contains the alpha strings that are associated with the user defined naming tags for additional numbers referenced in EF_{ANR}.

Structure of EF_{AAS}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: Optional		
Record length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha text string	M	X bytes

- Alpha text string.

Content:
- user defined text for additional number.

Coding:
- same as the alpha identifier in EF_{ADN}.

4.4.2.8 EF_{GAS} (Grouping information Alpha String)

This file contains the alpha strings that are associated with the group name referenced in EF_{GRP}.

Structure of EF_{GAS}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: Optional		
Record length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha text string	M	X bytes

NOTE: This file is mandatory if and only if EF_{GRP} is present.

- Alpha text string

Content:
- group names.

Coding:
- same as the alpha identifier in EF_{ADN}.

4.4.2.9 EF_{ANR} (Additional Number)

Several phone numbers and/or Supplementary Service Control strings (SSC) can be attached to one EF_{ADN} record, using one or several EF_{ANR}. The amount of additional number entries may be less than or equal to the amount of records in EF_{ADN}. The EF structure is linear fixed. Each record contains an additional phone number or Supplementary Service Control strings (SSC). This record cannot be shared between several phonebook entries. The first byte indicates whether the record is free or the type of additional number referring to the record number in EF_{AAS}, containing the text to be displayed. The following part indicates the additional number and the reference to the associated record in the EF_{ADN} file. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records.

Structure of EF_{ANR}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'YY'		
Record length: 15 or 17 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Additional Number Record identifier	M	1 byte
2	Length of BCD number/SSC contents	M	1 byte
3	TON and NPI	M	1 byte
4 to 13	Additional number/SSC String	M	10 bytes
14	Capability/Configuration1 Record Identifier	M	1 byte
15	Extension1 Record Identifier	M	1 byte
16	ADN file SFI	C	1 byte
17	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- Additional Number Record Identifier

Content:
- describes the type of the additional number defined in the file EF_{AAS}.

Coding:
- '00' – no additional number description;

'xx' – record number in EF_{AAS} describing the type of number (e.g. "FAX");
'FF' – free record.

- Length of BCD number/SSC contents

Contents:
- this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual additional number/SSC information length is greater than 11. When the additional number/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see clause 4.4.2.4).

Coding:
- same as the length of BCD number/SSC string byte in $EF_{ADN.}$

- TON and NPI.

Contents:
- Type of number (TON) and numbering plan identification (NPI).

Coding:
- same as the TON and NPI byte in $EF_{ADN.}$

- Additional number/SSC string

Content:
- up to 20 digits of the additional phone number and/or SSC information linked to the phone book entry.

Coding:
- same as the dialling number /SSC string in $EF_{ADN.}$

- Capability/Configuration1 Record Identifier.

Contents:
- This byte identifies the number of a record in the EF_{CCP1} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

Coding:
- binary.

- Extension1 Record Identifier.

Contents:
- extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.

if the number requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see clause 4.4.2.4).

Coding:
- binary.

- ADN file SFI.

Content:
- Short File identifier of the associated EF_{ADN} file.

Coding:
- as defined in the UICC specification.

- ADN file Record Identifier

Content:
- record identifier of the associated phone book entry.

Coding:
- 'xx' – record identifier of the corresponding ADN record.

4.4.2.10 EF_{SNE} (Second Name Entry)

The phone book also contains the option of a second name entry. The amount of second name entries may be less than or equal to the amount of records in EF_{ADN}. Each record contains a second name entry. This record cannot be shared between several phonebook entries.

Structure of EF_{SNE}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'YY'		
Record length: X or X+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier of Second Name	M	X bytes
X+1	ADN file SFI	C	1 byte
X+2	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- Alpha Identifier of Second Name.

Content:
- string defining the second name of the phone book entry.

Coding:
- as the alpha identifier for EF_{ADN}.

- ADN file SFI.

Content:
- Short File identifier of the associated EF_{ADN} file.

Coding:
- as defined in the UICC specification.

- ADN file Record Identifier

Content:
record identifier of the associated phone book entry.

Coding:
'xx' – record identifier of the corresponding ADN record.

4.4.2.11 EF_{CCP1} (Capability Configuration Parameters 1)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using a phone book entry.

Structure of EF_{CCP1}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'YY'		
Record length: X bytes, X ≥ 15	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information element.

Contents and Coding:
- see TS 24.008 [9]. The Information Element Identity (IEI) shall be excluded; i.e. the first byte of the EF_{CCP1} record shall be Length of the bearer capability contents.

"- unused bytes are filled with 'FF'

4.4.2.12 Phone Book Synchronisation

To support synchronisation of phone book data with other devices, the USIM may provide the following files to be used by the synchronisation method: a phone book synchronisation counter (PSC), a unique identifier (UID) and change counter (CC) to indicate recent changes.

If synchronisation is supported in the phonebook, then EF_{PSC}, EF_{UID}, EF_{PUID} and EF_{CC} are all mandatory.

4.4.2.12.1 EF_{UID} (Unique Identifier)

The EF_{UID} is used to uniquely identify a record and to be able to keep track of the entry in the phone book. The terminal assigns the (UID) when a new entry is created. The value of the UID does not change as long as the value of the PBID remains the same. The UID shall remain on the UICC, in EF_{UID}, until the PBID is regenerated. This means that when a phone book entry is deleted, the content of the linked information (e.g. ADN, E-MAIL,..) shall be set to the personalization value 'FF…FF'. But the UID-value of the deleted record shall not be used when a new entry is added to the phonebook until the PBID is regenerated, but it shall be set to a new value.

If/when the PBID is regenerated, all UIDs for the entry in the phone book shall be assigned new values starting from 1. If more than one EF_{UID} exists (i.e. multiple phone book file sets) then all values of UIDs used in that phone book shall be unique over all phone book file sets within that phone book. The new value of the UID for each entry shall then be kept until the PBID is regenerated again.

Structure of EF_{UID}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'YY'		
Record length: 2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Unique Identifier (UID) of Phone Book Entry	M	2 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- Unique Identifier of Phone Book Entry.

Content:
- number to unambiguously identify the phone book entry for synchronisation purposes.

Coding:
- hexadecimal value. At initialisation all UIDs are personalised to "00 00" (i.e. empty).

4.4.2.12.2 EF_{PSC} (Phone book Synchronisation Counter)

The phone book synchronisation counter (PSC) is used by the ME to construct the phone book identifier (PBID) and to determine whether the accessed phone book is the same as the previously accessed phone book or if it is a new unknown phone book (might be the case that there is one phonebook under DF-telecom and one phone book residing in a USIM-application). If the PSC is unknown, a full synchronisation of the phone book will follow.

The PSC is also used to regenerate the UIDs and reset the CC to prevent them from running out of range. When the UIDs or the CC has reached its maximum value, a new PSC is generated. This leads to a scenario where neither the CC nor the UIDs will run out of range.

The PSC shall be regenerated by the terminal if one of the following situation applies:
- the values of the UIDs have run out of range;
- the whole phone book has been reset/deleted;
- the value of the CC has run out of range.

Structure of EF_{PSC}

Identifier: '4F22'	Structure: transparent	Conditional (see Note)
SFI: 'YY'		
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Phone book synchronisation counter (PSC)	M	4 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- PSC: Unique synchronisation counter of Phone Book.

Content:
number to unambiguously identify the status of the phone book for synchronisation purposes.

Coding:
hexadecimal value.

The phone book identifier (PBID) coding based on the EF_{PSC} is described hereafter:

- For a phone book residing in DF-telecom:

- PBID = ICCid (10bytes) "fixed part" + 4 bytes (in EF_{PSC}) "variable part".

- For a phone book residing in an USIM application:

- PBID = 10 last bytes of (ICCid XOR AID) "fixed part" + 4 bytes (in EF_{PSC}) "variable part".

To be able to detect if the PSC needs to be regenerated (i.e. the variable part) the following test shall be made by the terminal before for each update of either the CC or the assignment of a new UID:

- Each time the terminal has to increment the value of the UID the following test is needed:

  - If UID = 'FF FF' then.

    {Increment **PSC** mod 'FF FF FF FF'; all the UIDs shall be regenerated}.

- Each time the terminal has to increment the value of CC the following test is needed:

  If CC = 'FF FF' then.

  {Increment **PSC** mod 'FF FF FF FF'; CC=0001}.

NOTE: If the phonebook is deleted then the terminal will change the **PSC** according to:

Incrementing **PSC** modulus 'FFFFFFFF'.

4.4.2.12.3 EF_{CC} (Change Counter)

The change counter (CC) shall be used to detect changes made to the phone book.

Every update/deletion of an existing phone book entry or the addition of a new phone book entry causes the terminal to increment the EF_{CC}. The concept of having a CC makes it possible to update the phone book in different terminals, which still are able to detect the changes (e.g. changes between different handset and/or 2nd and 3rd generation of terminals).

Structure of EF_{CC}

Identifier: '4F23'	Structure: transparent	Conditional (see Note)
SFI: 'YY'		
File size: 2 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Change Counter (CC) of Phone Book	M	2 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- Change Counter of Phone Book.

Content:
- indicates recent change(s) to phone book entries for synchronisation purposes.

Coding:
- hexadecimal value. At initialisation, CC shall be personalised to '00 00' (i.e. empty).

4.4.2.12.4 EF_{PUID} (Previous Unique Identifier)

The PUID is used to store the previously used unique identifier (UID). The purpose of this file is to allow the terminal to quickly generate a new UID, which shall then be stored in the EF_{UID}.

Structure of EF_{PUID}

Identifier: '4F24'	Structure: transparent	Conditional (see Note)
SFI: 'YY'		
File size: 2 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Previous Unique Identifier (PUID) of Phone Book Entry	M	2 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- Previous unique Identifier of Phone Book Entry.

Content:
- Previous number that was used to unambiguously identify the phone book entry for synchronisation purposes.

Coding:

- As for EF_{UID}

4.4.2.13 EF_{EMAIL} (e-mail address)

This EF contains the e-mail addresses that may be linked to a phone book entry. Several e-mail addresses can be attached to one EF_{ADN} record, using one or several EF_{EMAIL}. The number of email addresses may be equal to or less than the amount of records in EF_{ADN}. Each record contains an e-mail address. The first part indicates the e-mail address, and the second part indicates the reference to the associated record in the EF_{ADN} file. This record cannot be shared between several phonebook entries.

Structure of EF_{EMAIL}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'YY'		
Record length: X or X+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	E-mail Address	M	X bytes
:	:	:	:
:	:	:	:
X+1	ADN file SFI	C	1 byte
X+2	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- E-mail Address.

Content:
- string defining the e-mail address

Coding:
- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

- ADN file SFI.

Content:
- short File identifier of the associated EF_{ADN} file.

Coding:
- as defined in TS 31.101.

- ADN file Record Identifier.

Content:
- record identifier of the associated phone book entry.

Coding:
- binary.

4.4.2.14 Phonebook restrictions

This clause lists some general restrictions that apply to the phonebook:

- if an EF_{PBR} file contains more than one record, then they shall all be formatted identically on a type-by-type basis, e.g. if EF_{PBR} record #1 contains one type 1 e-mail then all EF_{PBR} records shall have one type 1 email;

- if an EF_{PBR} record contains more than one reference to one kind of file, such as two EF_{EMAIL} files, then they shall all be formatted identically on a type-by-type basis, e.g. if an EF_{PBR} record has 2 email addresses, then they shall have the same record size and the same number of records in each EF_{PBR} entry;

- an EF_{PBR} record may contain TLV entries indicating that the file exist as a type 1 and 2 file, e.g. a phonebook entry may have two emails, one with a one-to-one mapping (type 1) and one with a indirect mapping (type 2). Regardless of the type, files in all entries shall have the same record configuration;

- an EF_{PBR} record shall not contain more than one occurrence of a given kind of file indicated in tag 'AA' (type 3 link). For instance, an EF_{PBR} record may only contain one reference to an EF_{EXT1}.

4.4.3 Contents of files at the DF GSM-ACCESS level (Files required for GSM Access)

The Efs described in this clause are required for the USIM application to be able to access service through a GSM network.

The presence of this DF and thus the support of a GSM access is indicated in the 'USIM Service Table' as service no. '27' being available.

4.4.3.1 EF_{Kc} (GSM Ciphering key Kc)

If service n°27 is "available", this file shall be present.

This EF contains the ciphering key Kc and the ciphering key sequence number n for enciphering in a GSM access network.

Identifier: '4F20'	Structure: transparent	Optional
SFI: '01'		
File size: 9 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 8	Ciphering key Kc	M	8 bytes
9	Ciphering key sequence number n	M	1 byte

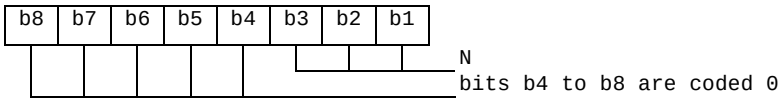
- Ciphering key Kc.

Coding:

- the least significant bit of Kc is the least significant bit of the eighth byte. The most significant bit of Kc is the most significant bit of the first byte.

- Ciphering key sequence number n

Coding:



NOTE: TS 24.008 [9] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

If service n°27 is "available", this file shall be present.

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see TS 23.060 [7]).

Identifier: '4F52'	Structure: transparent	Optional
SFI: '02'		
File size: 9 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 8	Ciphering key KcGPRS	M	8 bytes
9	Ciphering key sequence number n for GPRS	M	1 byte

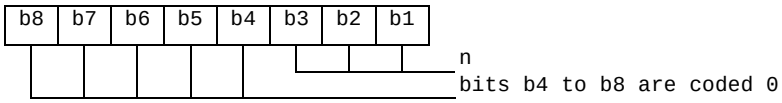
- Ciphering key KcGPRS.

Coding:

the least significant bit of KcGPRS is the least significant bit of the eighth byte. The most significant bit of KcGPRS is the most significant bit of the first byte.

- Ciphering key sequence number n for GPRS.

Coding:



NOTE: TS 24.008 [9] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.4.3.3 Void

4.4.3.4 EF_{CPBCCH} (CPBCCH Information)

If service n°39 is "available", this file shall be present.

This EF contains information concerning the CPBCCH according to TS 44.018 [28].

CPBCCH storage may reduce the extent of a Mobile Station's search of CPBCCH carriers when selecting a cell. The CPBCCH carrier lists shall be in accordance with the procedures specified TS 23.022 [29]. The MS stores CPBCCH information (from the System Information 19 message, Packet System Information 3, and Packet System Information 3 bis) on the USIM. The same CPBCCH carrier shall never occur twice in the list.

Identifier: '4F63'	Structure: transparent	Optional
File size: 2n bytes	Update activity: high	

Access Conditions:

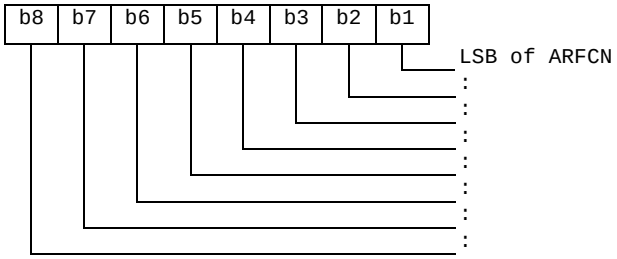
READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
:	:	:	:
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

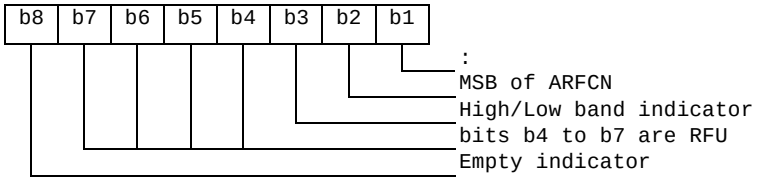
- Element in CPBCCH carrier list

Coding:

Byte 1: first byte of CPBCCH carrier list element



Byte 2: second byte of CPBCCH carrier list element



- ARFCN (10 bits) as defined in TS 45.005 [34].
- High/Low band indicator: If the ARFCN indicates possibly a channel in the DCS 1800 or a channel in the PCS 1900 band, if the bit is set to '1' the channel is in the higher band (GSM 1900). If the bit is set to '0', the lower band (GSM 1800) is indicated. If ARFCN indicates a unique channel, this indicator shall be set to '0'.
- Empty indicator: If this bit is set to '1', no valid CPBCCH carrier is stored in this position. If the Empty Indicator is set to '1', the content of the CPBCCH carrier field shall be ignored. The empty indicator shall also be used, and set to '1', if storage of fewer than maximum number n, of CPBCCH carrier fields is required.

4.4.3.5 $EF_{InvScan}$ (Investigation Scan)

If service n°40 is "available", this file shall be present.

This EF contains two flags used to control the investigation scan for higher prioritized PLMNs not offering voice services.

Identifier: '4F64'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Investigation scan flags	M	1 byte

- Investigation scan flags

Coding:

```
b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1
                                  |    |
                                  |    |____ In limited service mode
                                  |_________ After successful PLMN selection
                                             Bits b3 to b8 are coded RFU
```

A '1' in a bit position indicates that the investigation scan shall be performed for the condition corresponding to that bit position and a '0' that it shall not be performed.

If this elementary file is not present, no investigation scan shall be performed.

4.4.4 Contents of files at the MexE level

This clause specifies the Efs in the dedicated file DF_{MexE}. It only applies if the USIM supports MexE (see TS 23.057 [30]).

The presence of this DF is indicated in the 'USIM Service Table' as service no. '41' being available.

The Efs in the Dedicated File DF_{MexE} contain execution environment related information.

4.4.4.1 $EF_{MexE-ST}$ (MexE Service table)

If service n°41 is "available", this file shall be present.

This EF indicates which MexE services are available. If a service is not indicated as available in the USIM, the ME shall not select this service.

Identifier: '4F40'	Structure: transparent	Optional
File size: X bytes, X ≥ 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
etc.			
X	Services (8X-7) to (8X)	O	1 byte

-Services

Contents:	Service n°1:	Operator Root Public Key
	Service n°2:	Administrator Root Public Key
	Service n°3:	Third Party Root Public Key
	Service n°4:	RFU

Coding:

the coding rules of the USIM Service Table apply to this table.

4.4.4.2 EF_{ORPK} (Operator Root Public Key)

If service n°41 is "available", this file shall be present.

This EF contains the descriptor(s) of certificates containing the Operator Root Public Key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MexE operator domain using a root public key held in the USIM. Each record of this EF contains one certificate descriptor.

For example, an operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

Identifier: '4F41'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

- Parameter indicator

Contents:

The parameter indicator indicates if record is full and which optional parameters are present

Coding: bit string

b8	b7	b6	b5	b4	b3	b2	b1	
								Certificate descriptor is valid (bit1=0 key descriptor is valid)
								Reserved bit set to 1 (bitx=0 optional parameter present)

- Flags

Contents:

The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.

Coding: bit string

b8	b7	b6	b5	b4	b3	b2	b1	
								Authority certificate (bit=1 certificate of an authority)
								RFU
								RFU

- Type of certificate

Contents:

This field indicates the type of certificate containing the key.

Coding: binary:

0 : WTLS

1 : X509
2 : X9.68
Other values are reserved for further use

- Key/certificate File Identifier

Contents:
these bytes identify an EF which is the key/certificate data file (see clause 4.4.4.5), holding the actual key/certificate data for this record.

Coding:
byte 4: high byte of Key/certificate File Identifier;
byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File

Contents:
these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.

Coding:
byte 6: high byte of offset into Key/certificate Data File;
byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data

Contents:
these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.

Coding:
byte 8: high byte of Key/certificate Data length;
byte 9: low byte of Key/certificate Data length.

- Key identifier length

Contents:
This field gives length of key identifier

Coding:
binary

- Key identifier

Contents:
This field provides a means of identifying certificates that contain a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [30].

Coding:
octet string

NOTE: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

4.4.4.3 EF_{ARPK} (Administrator Root Public Key)

If service n°41 is "available", this file shall be present.

This EF contains the descriptor(s) of certificates containing the Administrator Root Public Key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator root public key held in the USIM. Each record of this EF contents one certificate descriptor.

This file shall contain only one record.

Identifier: '4F42'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

For contents and coding of all data items see the respective data items of the EF_{ORPK} (clause 4.4.4.2).

4.4.4.4 EF_{TPRPK} (Third Party Root Public Key)

If service n°41 is "available", this file shall be present.

This EF contains descriptor(s) of certificates containing the Third Party root public key (s). This EF shall only be allocated if the USIM issuer wishes to verify applications and certificates in the MexE Third Party domain using root public key(s) held in the USIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.

For example, an operator may provide several Third Party Root Public Keys.

Identifier:'4F43'	Structure: linear fixed	Optional
Record length: X + Y + 11 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes
11+X	Certificate identifier length (Y)	M	1 byte
12+X to 11+X+Y	Certificate identifier	M	Y bytes

- Certificate identifier length

Contents:
This field gives the length of the certificate identifier

Coding:
binary

- Certificate identifier

Contents:
This field identifies the issuer and provides an easy way to find a certificate. For more information about the value and usage see TS 23.057 [30].

Coding:
Octet string

For contents and coding of all other data items see the respective data items of the EF_{ORPK} (clause 4.4.4.2).

4.4.4.5 EF_{TKCDF} (Trusted Key/Certificates Data Files)

Residing under DF_{MexE}, there may be several key/certificates data files. These Efs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
File size: Y bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Y	Key/Certificate Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF_{TPRPK} (see clause 4.4.4.4).

The identifier '4FXX' shall be different from one key/certificate data file to another. For the range of 'XX', see TS 31.101 [11]. The length Y may be different from one key/certificate data file to another.

4.4.5 Contents of files at the DF WLAN level

This clause describes the additional files that are used for WLAN purposes.

DF_{WLAN} shall be present at the ADF_{USIM} level if either of the services nº59, nº60, nº61, nº62, nº63, nº66, n°81, n°82, n°83, n°84 or n°88 are "available" in the corresponding EF_{UST} (USIM Service Table).

4.4.5.1 EF_{Pseudo} (Pseudonym)

If service n°59 is "available", this file shall be present.

This EF contains a temporary user identifier (pseudonym) for subscriber identification. Pseudonyms may be provided as part of a previous authentication sequence. Pseudonyms are used as defined in TS 24.234 [40].

Identifier: '4F41'	Structure: Transparent	Optional
SFI : '01'		
File size: Y bytes (Y≥n+2)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	Pseudonym Length	M	2 bytes
3 to n+2	Pseudonym	M	n bytes

-Pseudonym Length

Contents:
- this byte gives the number of bytes of the following data item containing the Pseudonym value.

Coding:
- unsigned length coded on 2 bytes

- Pseudonym.

Contents:

-Pseudonym to be used as the username part of the NAI

Coding:

- As described for the user portion of the NAI in TS 33.234 [41]. Unused bytes shall be set to 'FF' and shall not be considered as a part of the value.

4.4.5.2 $EF_{UPLMNWLAN}$ (User controlled PLMN selector for I-WLAN Access)

If service n°60 is "available", this file shall be present.

This EF contains the coding for preferred PLMNs to be used for WLAN PLMN Selection. This information is determined by the user and defines the preferred PLMNs of the user in priority order. The first PLMN entry indicates the highest priority and the nth PLMN entry indicates the lowest. It shall be possible to store at least the number of PLMNs specified in TS 24.234 [40].

Identifier: '4F42'	Structure: transparent	Optional
SFI: '02'		
File size: 3n (where n ≥10)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 6	2nd PLMN	M	3 bytes
:	:		
28 to 30	10th PLMN	M	3 bytes
31 to 33	11th PLMN	O	3 bytes
:	:		
(3n-2) to 3n	N^{th} PLMN (lowest priority)	O	3 bytes

- PLMN

Contents:
- Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:
- according to TS 24.008 [9].

4.4.5.3 $EF_{OPLMNWLAN}$ (Operator controlled PLMN selector for I-WLAN Access)

If service n°61 is "available", this file shall be present.

This EF contains the coding for operator preferred PLMNs to be used for WLAN PLMN Selection. This information is determined by the operator and defines the operator preferred PLMNs in priority order. The first PLMN entry indicates the highest priority and the nth PLMN entry indicates the lowest. It shall be possible to store at least the number of PLMNs specified in TS 24.234 [40].

Identifier: '4F43'	Structure: transparent	Optional
SFI: '03'		
File size: 3n (where n ≥10)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 6	2nd PLMN	M	3 bytes
:	:		
28 to 30	10th PLMN	M	3 bytes
31 to 33	11th PLMN	O	3 bytes
:	:		
(3n-2) to 3n	Nth PLMN (lowest priority)	O	3 bytes

- PLMN

Contents:
- Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

Coding:
- according to TS 24.008 [9].

4.4.5.4 EF_{UWSIDL} (User controlled WLAN Specific Identifier List)

If service n°62 is "available", this file shall be present.

This file contains the user preferred list of WLAN specific identifier (WSID) for WLAN selection in priority order. The first record indicates the highest priority and the nth record indicates the lowest. This file is used for WLAN selection and shall store a list of at least the number of WSIDs specified in TS 24.234 [40].

Identifier: '4F44'	Structure: linear fixed	Optional
SFI: '04'		
Record size: X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of WSID	M	1 bytes
2 to X + 1	WSID	M	X bytes

-Length of WSID

Contents:
- this byte gives the number of bytes of the following data item containing the WSID.

Coding:
- unsigned length coded on one byte

-WSID

Contents:
- WLAN specific identifier (WSID) as defined in TS 24.234 [40].

Coding:
- binary. Unused bytes shall be set to 'FF' and not used either as a part of the value or for length calculation.

4.4.5.5 EF_{OWSIDL} (Operator controlled WLAN Specific IdentifierList)

If service n°63 is "available", this file shall be present.

This file contains the operator preferred list of WLAN specific identifier (WSID) for WLAN selection in priority order. The first record indicates the highest priority and the nth record indicates the lowest. This file is used for WLAN selection It shall be possible to store at least the number of PLMNs specified in TS 24.234 [40].

Identifier: '4F45'	Structure: linear fixed	Optional
SFI: '05'		
Record size: X + 1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of WSID	M	1 bytes
2 to X + 1	WSID	M	X bytes

-Length of WSID
Contents:
- this byte gives the number of bytes of the following data item containing the WSID.

Coding:
- unsigned length coded on one byte

-WSID
Contents:
- WLAN specific identifier (WSID) as defined in TS 24.234 [40].

Coding:
- binary. Unused bytes shall be set to 'FF' and not used either as a part of the value or for length calculation.

4.4.5.6 EF_{WRI} (WLAN Reauthentication Identity)

If service n°66 is "available", this file shall be present.

This EF contains a list of parameters linked to a re-authentication identity to be used in fast re-authentication. Re-authentication identities and related parameters (Master Key and Counter Value) are provided as part of a previous authentication sequence.

Identifier: '4F46'	Structure: Transparent	Optional
SFI: '06'		
File size: n bytes, (n ≥ J+K+L+6)	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Reauthentication Identity Tag '80'	M	1 byte
2	Re-authentication Identity Length	M	1 byte
3 to J+2	Re-authentication Identity Value	M	J bytes
J+3	Master Key Tag '81'	M	1 byte
J+4	Master Key Length	M	1 byte
J+5 to J+K+4	Master Key Value	M	K bytes
J+K+5	Counter Tag '82'	M	1 byte
J+K+6	Counter Length	M	1 byte
J+K+7 to J+K+L+6	Counter Value	M	L bytes

- Reauthentication Identity

Contents:
- Re-authentication identity TLV to be used as the username part of the NAI.

Coding:
Tag '80'
Unsigned length on 1 byte
Value: As described for the user portion of the NAI in TS 33.234 [41]. Unused bytes shall be set to 'FF' and shall not be considered as a part of the value.

- Master Key

Contents:
- Master Key TLV.

Coding:
Tag '81'
Unsigned length on 1 byte
Value: As described in TS 33.234 [41].

- Counter

Contents:
- Counter TLV

Coding:
Tag '82'
Unsigned length on 1 byte
Value: As described in TS 33.234 [41].

4.4.5.7 EF_{HWSIDL} (Home I-WLAN Specific Identifier List)

If service n°81 is "available", this file shall be present.

This file contains the Home I-WLAN specific identifier list (WSID list) for I-WLAN selection in priority order. The WSIDs in this list are known to connect to the HPLMN. The first record indicates the highest priority and the nth record indicates the lowest. This file is used for I-WLAN selection. It shall be possible to store at least the number of WSIDs specified in TS 24.234 [40].

Identifier: '4F47'	Structure: linear fixed	Optional
SFI: '07'		
Record size: X + 1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of WSID	M	1 bytes
2 to X + 1	WSID	M	X bytes

For contents and coding see EF_{OWSIDL}.

4.4.5.8 $EF_{WEHPLMNPI}$ (I-WLAN Equivalent HPLMN Presentation Indication)

If service n°82 is "available", this file shall be present.

This EF contains an indication to the ME for the presentation of the available EHPLMN(s) during I-WLAN selection procedures. The usage of the I-WLAN EHPLMN presentation indication is defined in TS 24.234 [40].

Identifier: '4F48'	Structure: transparent	Optional
SFI: '08'		
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	I-WLAN EHPLMN Presentation Indication	M	1 byte

- I-WLAN EHPLMN Presentation Indication:
  Contents:
  I-WLAN EHPLMN display mode

  Coding:
  - '00' - No preference for the display mode
  - '01' - Display the highest-priority available EHPLMN only
  - '02' - Display all the available EHPLMNs
  - All other values are RFU

4.4.5.9 EF_{WHPI} (I-WLAN HPLMN Priority Indication)

If service n°83 is "available", this file shall be present.

This EF contains an indication to the ME for the selection of the I-WLAN EHPLMN or the I-WLAN last Registered PLMN. The usage of the I-WLAN HPLMN Priority Indication file is defined in TS 24.234 [40].

Identifier: '4F49'	Structure: transparent	Optional
SFI: '09'		
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	I-WLAN Last RPLMN Selection Indication	M	1 byte

- I-WLAN Last RPLMN Selection Indication:
  Contents:
  I-WLAN Last RPLMN Selection Indication

  Coding:
  - '00' - The UE shall attempt registration on the last I-WLAN RPLMN as described in TS 24.234 [40]
  - '01' - The UE shall attempt registration on the I-WLAN home network as described in TS 24.234 [40]
  - All other values are RFU

4.4.5.10 $EF_{WLRPLMN}$ (I-WLAN Last Registered PLMN)

If service n°84 is "available", this file shall be present.

This EF contains I-WLAN Last Registered PLMN Selection. The usage of the I-WLAN Last Registered PLMN is defined in TS 24.234 [40].

Identifier: '4F4A'	Structure: transparent	Optional
SFI: '0A'		
File size: 3 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	I-WLAN Last Registered PLMN	M	3 bytes

- I-WLAN Last Registered PLMN
  Contents:
  - Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:
- according to TS 24.008 [9].

4.4.5.11 $EF_{HPLMNDAI}$ (HPLMN Direct Access Indicator)

If service n°88 is "available", this file shall be present.

This EF contains HPLMN Direct Access related informations. The usage of the HPLMN Direct Access Indicator file is defined in TS 23.234 [40].

Identifier: '4F4B'	Structure: transparent	Optional
SFI: '0B'		
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	HPLMN Direct Access Indication	M	1byte

- HPLMN Direct Access Indication:
  Contents:
  HPLMN Direct Access Indication

  Coding:
  - '00' – HPLMN Direct Access Indicator is disabled
  - '01' – HPLMN Direct Access Indicator is enabled

- All other values are RFU

4.4.6 Contents of files at the DF HNB level

4.4.6.1 Introduction

This clause describes the additional files that are used for Home (e)NodeB purposes.

DF_{HNB} shall be present at the ADF_{USIM} level if service nº86 and/or service nº90 isare "available" in EF_{UST} .

4.4.6.2 EF_{ACSGL} (Allowed CSG Lists)

If service n°86 is "available", this file shall be present.

This EF contains the coding for CSG ID belonging to the Allowed CSG lists. Furthermore, for each CSG ID in the list, a link to the corresponding HNB name and CSG Type may be provided.

Identifier: '4F81'	Structure: linear fixed	Optional
SFI: '01'		
Record length: X	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	CSG Lists TLV object	M	X bytes
Note: The CSG List in different records may contain the same PLMN			

The CSG List TLV object shall contain only one PLMN TLV object, Tag '80', and at least one CSG information TLV, Tag '81'. A record may contain one or more CSG List TLV objects. This means that all CSG Ids in one CSG List TLV object belong to the same PLMN.

CSG List Tags

Description	Tag Value

CSG List TLV object Tag	'A0'

CSG List information

Description	Value	M/O	Length (bytes)
CSG List Tag	'A0'	M	1
Length	Y	M	Note
PLMN Tag	'80'	M	1
Length	A	M	Note
PLMN	--	M	A
CSG Information Tag	'81'	M	1
Length	W	M	Note
CSG Information	-	M	W
Note: The length is coded according to ISO/IEC 8825-1 [35]			

- PLMN Tag '80'

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

CSG Information Tag '81'

.

Tag '81' Coding:

1	CSG Type indication	M	1 byte
2	HNB Name indication	M	1 byte
3 to W	CSG ID	M	W-2 bytes
Note: The length of the CSG ID is calculated from the TLV object length			

- CSG Type indication

  Contents:

  the CSG Type for the subsequent CSG ID.

  Coding:

  a value of '00' indicates that the CSG Type is to be taken from other sources (e.g. stored in the non-volatile memory of the ME). A value in the range '01' to 'FE' indicates the record number in EF_{CSGT} that shall be displayed as the CSG Type.

- HNB Name indication

  Contents:

  the HNB name for the subsequent CSG ID.

  Coding:

  a value of '00' indicates that the HNB name is to be taken from other sources (e.g. broadcasted by the Home Node B or stored in the non-volatile memory of the ME). A value in the range '01' to 'FE' indicates the record number in EF_{HNBN} that shall be displayed as the HNB name.

- CSG ID

  Contents:

CSG ID which is part of the allowed CSG list.

Coding:

the CSG ID shall be encoded as defined in TS 23.003 [25]. The CSG ID is coded left justified, i.e. the most significant bit of the CSG ID is coded on bit 8 of byte 3, over the number of bits as specified in TS 23.003 [25] using bytes 3 to W . The unused rightmost bits of byte W shall be set 1.

Unused bytes shall be set to 'FF'.

4.4.6.3 EF_{CSGT} (CSG Type)

If service n°86 is "available", this file shall be present.

This EF contains the CSG Type. The CSG Type is defined in TS 22.220 [54]. The association between a CSG ID and the corresponding CSG Type is provided in EF_{ACSGL}. The CSG Type may be provided in text or in graphic format.

Identifier: '4F82'	Structure: linear fixed	Optional
SFI: '02'		
Record length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	CSG Type TLV objects	M	X bytes

CSG Type tags

Description	Tag Value
Text CSG Type Tag	'89'
Graphics CSG Type Tag	'80' or '81'

CSG Type information

Contents:

CSG Type contains either Text CSG Type or Graphic CSG Type or both the Graphic and Text CSG Types

Coding:

Text CSG Type:

Description	Value	M/O	Length (bytes)
Text CSG Type Tag	'89'	M	1
Length	K	M	Note
Text CSG Type	--	M	K
Note: The length is coded according to ISO/IEC 8825-1 [35].			

Graphic CSG Type:

Description	Value	M/O	Length (bytes)
Graphic CSG Type Tag	'80' or '81'	M	1
Length	K + 1	M	Note 1
Graphic CSG Type Icon Qualifier	--	M	1
Graphic CSG Type Icon Link	--	M	K (Note 2)
Note 1: The length is coded according to ISO/IEC 8825-1 [35]. Note 2: The tag value indicates the type and format of the Icon Link that is provided in the TLV value field (e.g. Tag '80' indicates that the Icon link is a URI, while Tag '81' indicates that the Icon Link is the record number of the corresponding image in EF_{IMG}).			

- Text CSG Type Tag '89'

Contents:

Tag value for the CSG Type in text format.

Coding:

- '89' = the Text CSG Type is coded using one of the UCS2 code options as defined in TS 31.101 [11].

- Graphic CSG Type Tag

Contents:

Tag value for the CSG Type in graphic format with the Icon Qualifier or an Icon Link

Coding:

- '80' = the Graphic CSG Type Icon Link is an URI

- '81' = the Graphic CSG Type Icon Link is a pointer to the record number of the corresponding image in EF_{IMG},

- All other values are RFU.

- Graphic CSG Type Icon Qualifier
Contents:

The icon qualifier indicates to the ME how the icon shall be used.

Coding:

- '01' = icon is self-explanatory, i.e. if displayed, it replaces the corresponding name in text format.

- '02' = icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the corresponding name in text format.

- All other values are RFU.

- Graphic CSG Type Icon Link
Contents:

Link to the icon. This link shall point to a UICC resource.

Coding:

- When the Tag value indicates an URI (i.e. Tag = '80') , the Icon Link shall be encoded to an octet string according to UTF-8 encoding rules as described in IETF RFC 3629 [48] (e.g. http://127.0.0.1:3516/pub/files/csgtype.jpg).

- When the Tag value indicates that the Icon Link contains the record number of the corresponding image in EF_{IMG} (i.e. Tag = '81'), the Icon Link shall be encoded in binary.

Unused bytes shall be set to 'FF'.

4.4.6.4 EF_{HNBN} (Home NodeB Name)

If service n°86 is "available", this file shall be present.

This EF contains the HNB name. The HNB name is defined in TS 22.220 [54]. HNB name is a common name referring to HNB/HeNB. The association between a CSG ID and the corresponding HNB name is provided in EF_{ACSGL}.

Identifier: '4F83'	Structure: linear fixed	Optional
SFI: '03'		
Record length: X bytes; X ≥ 3	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	HNB Name TLV object	M	X bytes

HNB Name tags

Description	Tag Value
HNB Name Tag	'80'

HNB Name information

Description	Value	M/O	Length (bytes)
HNB Name Tag	'80'	M	1
Length	K	M	Note
HNB Name	--	M	K
Note 1: The length is coded according to ISO/IEC 8825-1 [35].			

- HNB Name Tag '80'

  Contents:

  name of the HNB or HeNB.

  Coding:

  coded using one of the UCS2 code options as defined in TS 31.101 [11].

Unused bytes shall be set to 'FF'.

4.4.6.5 EF_{OCSGL} (Operator CSG Lists)

If service n°90 is "available", this file shall be present.

This EF contains the coding for CSG Ids belonging to the Operator CSG lists. Furthermore, for each CSG ID in the list, a link to the corresponding HNB name and CSG type may be provided. Within one PLMN the first occurrence of CSG ID indicates the highest priority CSG ID and the last occurrence indicates the lowest.

NOTE 1: There is no requirement for the ME to take the priority into account.

Additionally, if service n°92 is "available", this EF allows the HPLMN to control, on a per PLMN basis, which available CSGs are displayed by the ME during a manual CSG selection. If there is no CSG display indicator for a PLMN, the ME shall display the available CSGs according to the value in EF_{AD} byte 3 bit 2.

NOTE 2: Operators should ensure that all CSG display indicators have the same value if the same PLMN is used in multiple CSG List TLV objects.

Identifier: '4F84'	Structure: linear fixed	Optional
SFI: '04'		
Record length: Y bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Operator CSG List TLV objects	M	X bytes
Note: The CSG List in different records may contain the same PLMN			

The Operator CSG List TLV object shall contain only one PLMN TLV object, Tag '80', and at least one Operator CSG information TLV, Tag '81'. A record may contain one or more Operator CSG List TLV objects. This means that all CSG Ids in one Operator CSG List TLV object belong to the same PLMN.
Additionally, the Operator CSG List TLV object may contain one CSG Display Indicator TLV object, if service n°92 is available.

CSG List Tags

Description	Tag Value
Operator CSG List TLV object Tag	'A0'

CSG List information

Description	Value	M/O	Length (bytes)
CSG List Tag	'A0'	M	1
Length	Y	M	Note
PLMN Tag	'80'	M	1
Length	A	M	Note
PLMN	--	M	A
CSG Information Tag	'81'	M	1
Length	W	M	Note
CSG Information	-	M	W
CSG Display indicator tag	'82'	O	1
Length	Z	O	Note
CSG Display indicator	-	O	Z
Note: The length is coded according to ISO/IEC 8825-1 [35]			

- PLMN Tag '80'

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

- CSG Information Tag '81'

  Tag '81' Coding:

1	CSG Type indication	M	1 byte
2	HNB Name indication	M	1 byte
3 to W	CSG ID	M	W-2 bytes
Note: The length of the CSG ID is calculated from the TLV object length			

  - CSG Type indication

Contents:

the CSG Type for the subsequent CSG ID.

Coding:

a value of '00' indicates that the CSG Type is to be taken from other sources (e.g. stored in the non-volatile memory of the ME). A value in the range '01' to 'FE' indicates the record number in EF_{CSGT} that shall be displayed as the CSG Type.

- HNB Name indication

Contents:

the HNB name for the subsequent CSG ID.

Coding:

a value of '00' indicates that the HNB name is to be taken from other sources (e.g. broadcasted by the Home Node B or stored in the non-volatile memory of the ME). A value in the range '01' to 'FE' indicates the record number in EF_{HNBN} that shall be displayed as the HNB name.

- CSG ID

Contents:

CSG ID which is part of the allowed CSG list.

Coding:

the CSG ID shall be encoded as defined in TS 23.003 [25]. The CSG ID is coded left justified, i.e. the most significant bit of the CSG ID is coded on bit 8 of byte 3, over the number of bits as specified in TS 23.003 [25] using bytes 3 to W. The unused rightmost bits of byte W shall be set 1.

- CSG display indicator Tag '82':

Coding:
- '00' All available CSG Ids can be displayed during a manual CSG selection
- '01' Only CSG Ids contained in Operator CSG lists shall be displayed during a manual CSG selection

Unused bytes shall be set to 'FF'

4.4.6.6 EF_{OCSGT} (Operator CSG Type)

If service n°90 is "available", this file shall be present.

This EF contains the Operator CSG Types. The CSG Type is defined in TS 22.220 [54]. The association between an Operator CSG ID and the corresponding Operator CSG Type is provided in EF_{OCSGL}. The Operator CSG Type may be provided in text or in graphic format.

Identifier: '4F85'	Structure: linear fixed	Optional
SFI: '05'		
Record length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	CSG Type TLV objects	M	X bytes

For coding see EF_{CSGT}

4.4.6.7 EF_{OHNBN} (Operator Home NodeB Name)

If service n°90 is "available", this file shall be present.

This EF contains the Operator HNB names. The HNB name is defined in TS 22.220 [54]. HNB Name is a common name referring to HNB/HeNB. The association between an Operator CSG ID and the corresponding Operator HNB name is provided in EF_{OCSGL}.

Identifier: '4F86'	Structure: linear fixed	Optional
SFI: '06'		
Record length: X bytes; X ≥ 3	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	HNB Name TLV object	M	X bytes

For coding see EF_{HNBN}

4.4.7 Void

4.5 Contents of Efs at the TELECOM level

The Efs in the Dedicated File $DF_{TELECOM}$ contain service related information.

4.5.1 EF_{ADN} (Abbreviated dialling numbers)

In case of a present GSM application on the UICC the first EF_{ADN} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F3A') to $DF_{TELECOM}$ to ensure backwards compatibility.

A 3G ME shall not access this file. The information is accessible for a 3G ME in EF_{ADN} under $DF_{PHONEBOOK.}$

4.5.2 EF_{EXT1} (Extension1)

In case of a present GSM application on the UICC the first EF_{EXT1} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F4A') to $DF_{TELECOM}$ to ensure backwards compatibility.

A 3G ME shall not access this file. The information is accessible for a 3G ME in EF_{EXT1} under $DF_{PHONEBOOK.}$

4.5.3 EF_{ECCP} (Extended Capability Configuration Parameter)

In case of a present GSM application on the UICC the first EF_{CCP1} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F4F') to $DF_{TELECOM}$ to ensure backwards compatibility. There shall not be any EF_{CCP} (with a file-id of '6F3D') under $DF_{TELECOM}$ because otherwise a GSM terminal could create inconsistencies within the phonebook.

A 3G ME shall not access this file. The information is accessible for a 3G ME in EF_{CCP1} under $DF_{PHONEBOOK.}$

4.5.4 EF_{SUME} (SetUpMenu Elements)

This File is defined in ETSI TS 102 222 [39], and has the file identifier '6F54'.

4.5.5 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the $DF_{TELECOM}$ in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at $DF_{Telecom}$-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
Record length: X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4 [20]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR}, any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.5.6 EF_{ICE_DN} (In Case of Emergency – Dialling Number)

This EF contains one or more records containing number formatted ICE information, according to TS 22.101 [24].

This file shall be deactivated if the user does not wish the ICE information contained in this file to be available and activated if the user wishes the ICE information in this file to be available.

Structure of EF_{ICE_DN} at $DF_{Telecom}$-level

Identifier: '6FE0'	Structure: Linear fixed	Optional
SFI: Optional		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	PIN
DEACTIVATE	PIN or Issuer Specified PIN (see Note)
ACTIVATE	PIN or Issuer Specified PIN (see Note)

Bytes	**Description**	**M/O**	**Length**
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration1 Record Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

Note: The Issuer Specified PIN is a PIN with a global key reference (see TS 31.101 [11]) specified by the card Issuer.

Coding:

As for EF_{ADN}

4.5.7 EF_{ICE_FF} (In Case of Emergency – Free Format)

This EF contains one or more records containing free formatted ICE information, according to TS 22.101 [24].

This file shall be deactivated if the user does not wish the ICE information contained in this file to be available and activated if the user wishes the ICE information in this file to be available.

Structure of EF_{ICE_FF} at $DF_{Telecom}$-level

Identifier: '6FE1'	Structure: Linear fixed	Optional
SFI: Optional		
Record length: >=X+Y bytes	Update activity: low	
Access Conditions: READ ALWAYS UPDATE PIN DEACTIVATE PIN or Issuer Specified PIN (see Note) ACTIVATE PIN or Issuer Specified PIN (see Note)		

Bytes	Description	M/O	Length
1 to X	ICE Free Format Label TLV	M	X bytes
X+1 to X+Y	ICE Free Format Content TLV	M	Y bytes

Note: The Issuer Specified PIN is a PIN with a global key reference (see TS 31.101 [11]) specified by the card Issuer.

- ICE Free Format Label TLV

Contents:
This TLV contains a label that summarises the type of content that is contained in the associated ICE Free Format Content TLV (e.g. "medical alert information").

Coding:
ICE Free Format Label TLV is coded as follows:
Tag value is '80'
Length is coded according to ISO/IEC 8825-1 [35].
Value is as for value part of the text string TLV in 3GPP TS 31.111 [12]. If the length is 0 and there is no value part then the terminal shall interpret this as no label is used.

- ICE Free Format Content TLV

Contents:
This TLV contains a ICE Free Format Content (e.g. "Allergy to work").

Coding:
ICE Free Format Content TLV is coded as follows:
Tag value is '81'
Length is coded according to ISO/IEC 8825-1 [35].
Value is as for value part of the text string TLV in 3GPP TS 31.111 [12]. If the length is 0 and there is no value part then the terminal shall interpret this as no label is used.

Padding: unused bytes in each record shall be set to 'FF'.

4.5.8 EF_{RMA} (Remote Management Actions)

This File is defined in ETSI TS 102 222 [39], and has the file identifier '6F53'.

4.5.9 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC)

This file shall be present if and only if service n°12 and n°91 are "available".

This EF contains the Public Service Identity of the SM-SC (either a SIP URI or tel URI) that the ME shall use to submit SMS over IP as defined in 24.341 [55].

Identifier: '6FE5'	Structure: linear fixed	Optional
File size: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	URI TLV data object	M	X bytes

- URI

  Contents:

  - SIP URI or tel URI of the Public Service Identity of the SM-SC.

  Coding:

  - For contents and syntax of URI TLV data object values see IETF RFC 3261 [56]. The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [57]. The tag value of the URI TLV data object shall be '80'.

4.6 Contents of DFs at the TELECOM level

DFs may be present as child directories of $DF_{TELECOM}$. The following DFs have been defined:

- $DF_{GRAPHICS}$ '5F50'.
- $DF_{PHONEBOOK}$ '5F3A'.

(DF for public phone book. This DF has the same structure as $DF_{PHONEBOOK}$ under ADF USIM).

- $DF_{MULTIMEDIA}$ '5F3B'.
- DF_{MMSS} '5F3C'

(The contents of DF for MMSS are defined in C.S0074-A [53]. This DF for MMSS is not applicable to 3GPP only terminals).

4.6.1 Contents of files at the $DF_{GRAPHICS}$ level

The Efs in the Dedicated File $DF_{GRAPHICS}$ contain graphical information.

4.6.1.1 EF_{IMG} (Image)

Each record of this EF identifies instances of one particular graphical image, which graphical image is identified by this EF's record number.

Image instances may differ as to their size, having different resolutions, and the way they are coded, using one of several image coding schemes.

As an example, image k may represent a company logo, of which there are i instances in the UICC, of various resolutions and perhaps encoded in several image coding schemes. Then, the i instances of the company's logo are described in record k of this EF.

Identifier: '4F20'	Structure: linear fixed	Optional
Record length: 9n+1 or 9n+2 bytes, (n ≥ 1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Number of Actual Image Instances	M	1 byte
2 to 10	Descriptor of Image Instance 1	M	9 bytes
11 to 19	Descriptor of Image Instance 2	O	9 bytes
:	:	:	:
9(n-1)+2 to 9n+1	Descriptor of Image Instance n	O	9 bytes
9n + 2	RFU (see TS 31.101 [11])	O	1 byte

- Number of Actual Image Instances.

Contents:
- this byte gives the number of actual image instances described in the following data items (i.e. unused descriptors are not counted).

Coding:
- binary.

- Image Instance Descriptor

Contents:
- a description of an image instance.

Coding:
- Byte 1: Image Instance Width

Contents:
- this byte specifies the image instance width, expressed in raster image points.

Coding:
- binary.

Byte 2: Image Instance Height.

Contents:
- this byte specifies the image instance height, expressed in raster image points.

Coding:
- binary.

Byte 3: Image Coding Scheme.

Contents:
- this byte identifies the image coding scheme that has been used in encoding the image instance.

Coding:
- '11' - basic image coding scheme as defined in annex B;
- '21' - colour image coding scheme as defined in annex B;
- '22' - colour image coding scheme with transparency as defined in annex B;
  other values are reserved for future use.

Bytes 4 and 5: Image Instance Data File Identifier.

Contents:
- these bytes identify an EF which is the image instance data file (see clause 4.6.1.2), holding the actual image data for this particular instance.

Coding:
- byte 4: high byte of Image Instance Data File Identifier;
- byte 5: low byte of Image Instance Data File Identifier.

Bytes 6 and 7: Offset into Image Instance Data File.

Contents:
- these bytes specify an offset into the transparent Image Instance Data File identified in bytes 4 and 5. The data for this image instance is found starting at this offset in the Image Instance Data File.

Coding:
- byte 6: high byte of offset into Image Instance Data File;
  byte 7: low byte of offset into Image Instance Data File.

Bytes 8 and 9: Length of Image Instance Data.

Contents:
- these bytes yield the length of the image instance data, starting at the offset identified in bytes 6 and 7. For the colour image coding scheme, as defined in annex B, the length of image instance data excludes the CLUT.

Coding:
- byte 8: high byte of Image Instance Data length;
- byte 9: low byte of Image Instance Data length.

NOTE: Transparent image instance data longer than 256 bytes may be read using successive READ BINARY commands.

4.6.1.2 EF_{IIDF} (Image Instance Data Files)

Residing under $DF_{GRAPHICS}$, there may be several image instance data files. Each Image Instance Data File contains data for one or more image instances. These Efs containing image instance data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
File size: Y bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Y	Image Instance Data	M	Y bytes

Contents and coding:
- Image instance data are accessed using the image instance descriptors provided by EF_{IMG} (see clause 4.6.1.1).

The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', TS 31.101 [11]. The length Y may be different from one image instance data file to the other.

4.6.1.3 $EF_{ICE\_graphics}$ (In Case of Emergency – Graphics)

This EF contains ICE graphical information, according to TS 22.101 [24].

This file shall be deactivated if the user does not wish the ICE information contained in this file to be available and activated if the user wishes the ICE information in this file to be available.

For this EF the Total File Size data object shall be present within the FCP template in order for the ME to fit the picture to the available memory.

Structure of $EF_{ICE\_graphics}$ at $DF_{graphics}$-level

Identifier: '4F21'	Structure: BER-TLV	Optional
SFI: Optional		
Record length: X	Update activity: low	
Access Conditions: READ ALWAYS UPDATE PIN DEACTIVATE PIN or Issuer Specified PIN (see Note) ACTIVATE PIN or Issuer Specified PIN (see Note)		

Bytes	Description	M/O	Length
1 to X	ICE graphics Data object	M	X bytes

Note: The Issuer Specified PIN is a PIN with a global key reference (see TS 31.101 [11]) specified by the card Issuer.

- ICE graphics Data Object

Coding of the ICE graphics Data Objects

Length	Description	Coding	Status
1 to T bytes (T ≤ 3)	ICE graphics Data Object tag	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 to L (L ≤ 4)	ICE graphics Data Object length	As defined in TS 31.101 [11] for BER-TLV structured files	M
X-L-T bytes	ICE graphics Content	JPEG format	M

4.6.1.4 $EF_{LAUNCH\ SCWS}$

Support of this EF is mandatory for a UICC that supports the Smart Card Web Server [59].

This EF contains the data for one or more launch facilities. A ME that supports the launch feature of the Smart Card Web Server shall read at least one of the launch facilities stored in $EF_{LAUNCH\ SCWS}$ and shall integrate them within the MMI in order to give the user the opportunity to launch a browser session with the Smart Card Web Server.

The launch facility comprises an alpha identifier, a browser identity, a URL and zero or more icon descriptors. The ME shall present as many launch facilities to the user as it is able, starting with the first one, according to the following rules:

- If no icon descriptor is provided, the ME shall use a ME specific default icon to present the launch facility to the user. The ME may also display the alpha identifier together with the icon.
- If one or more icon descriptor(s) is/are provided, the ME may use the icon descriptors and, if required, the icon data retrieved from the referenced EF_{ICON} to decide which of the icons is most appropriate for its menu system. If the ME is able to use this data, if required so after appropriate resizing, it shall use the icon data to present the launch pad to the user. If indicated in the Icon Qualifier the ME may also display the alpha identifier together with the icon. If the icon data is not usable by the ME, a default launch mechanism shall be used. The fact that the icon data from one of the referenced EF_{ICON} was retrieved may be used by the UICC as an indication that the launch pad is presented to the user.
- As a minimum, terminals shall support the following icon format:
  - PNG as specified in ISO/IEC 15948 [60];
  - Icon size 32 x 32 pixel;
  - indexed colour information with 8 bits per pixel.

When the USIM sends a REFRESH proactive command for this file, the procedure given above shall be followed.

Structure of EF_{LAUNCH_SCWS} at $DF_{graphics}$-level

Identifier: '4F 01'	Structure: transparent	Optional
SFI: Optional		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to M	Launch SCWS TLV object(s)	O	M bytes

This file may contain one or several Launch SCWS TLV object(s). Each Launch SCWS TLV object may contain one or more Icon Descriptor TLVs. The first URL TLV Object shall contain the Smart Card Web Server home page. The coding of the Launch SCWS TLV objects is described hereafter:

Length	Description	Value	Status
1 byte	Launch SCWS Tag	'A0'	M
(14+X+W+Z)	Length (see Note 2)	-	M
1 byte	URL Tag	'80'	M
1 byte	Length (see Note 2)	-	M
W byte	URL (starting page)	-	M
1 byte	Alpha Identifier Tag	'81'	O
1 byte	Length (see Note 2)	-	C
X byte	Alpha Identifier	-	C
1 byte	Browser Identity Tag	'82'	O
1 byte	Length (see Note 2)	-	C
1 byte	Browser Identity	-	C
1 byte	Icon Descriptor Tag	'83' or '84' (see Note 1)	O
1 byte	Length (see Note 2)	-	C
5+Z byte	Icon Descriptor	-	C

Note 1: The tag value indicates the type and format of the Icon Link that is provided in the TLV value field (e.g. Tag '83' indicates that the Icon link is a URI, of which there shall only be one instance, while Tag '84' indicates that the Icon Link is the EF_{ICON} file ID).
Note 2: coded according to ISO/IEC 8825-1 [35].
Note 3: C; if the Tag is present, this is mandatory.

- URL Tag '80':

  Contents:

  The URL shall point to a page of the Smart Card Web Server [59].

  Coding:

According to TS 31.111 [12]

- Alpha Identifier Tag '81':

  Contents:

  The alpha identifier contains the text to be displayed by the ME together with a non-self-explanatory icon.

  Coding:

  According to TS 31.111 [12]

- Browser Identity Tag '82':

  Contents:

  The browser identity contains information about the type of browser to be used (e.g. HTML or WML browser).

Coding:

According to TS 31.111 [12]

- Icon Descriptor Tag '83' or '84':

The icon descriptor TLV contains information about the icon.

- When the Icon Link is an URI, the Tag value shall be set to '83'.

Length	Description	Value
1 byte	Icon Descriptor Tag	'83'
1 byte	Length	-
1 byte	Icon Qualifier	-
Z	Icon Link	-

- When the Icon Link is a pointer to the EF_{ICON} file ID which contains the icon data (see clause 4.6.1.5), the Tag value shall be set to '84'.

Length	Description	Value
1 byte	Icon Descriptor Tag	'84'
1 byte	Length	-
1 byte	Icon Qualifier	-
1 byte	Icon Coding Scheme	-
1 byte	Icon Width	-
1 byte	Icon Height	-
1 byte	Bits per Pixel	-
Z	Icon Link	-

- Icon Qualifier:

- Contents:
  - The icon qualifier indicates how the icon shall be used by the terminal.
- Coding:
  - bit 1: 0 = icon is self-explanatory, i.e. if displayed, it replaces the alpha identifier;

    1 = icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the alpha identifier.
  - bits 2 to 8 = 0 RFU.

- Icon Coding Scheme:

- Contents:
  - this byte identifies the image coding scheme that has been used in encoding the icon.
- Coding: Reference to a media type as defined in RFC 2046 [61] and registered with IANA at http://www.iana.org/assignments/media-types/.
  - '00' - other media type as defined in EF_{ICON};
    '01' - "image/png";
    '02' - "image/jpeg";
    '03' - "image/gif";
    '04' - "image/tiff";
    '05' - "image/vnd.microsoft.icon";
    all other values - RFU.

- Icon Width:

- Contents:
  - this byte specifies the icon width, expressed in pixel.
- Coding:
  - binary.

- Icon Height:

- Contents:
  - this byte specifies the icon height, expressed in pixel.
- Coding:
  - binary.

- Bits per pixel:

- Contents:
  - this byte specifies the number of bits that are used to code each pixel.
- Coding:
  - binary.

- Icon Link:

- Contents:
  - Link to the icon. This link shall point to a UICC resource.
- Coding:

  - When the Tag value indicates an URI (i.e. Tag = '83') , the Icon Link shall be encoded to an octet string according to UTF-8 encoding rules as described in IETF RFC 3629 [48] (e.g. http://127.0.0.1:3516/pub/files/smartcardicon.jpg). The URI shall point to a page of the Smart Card Web Server [59].

  - When the Tag value indicates that the Icon Link contains file ID of the corresponding icon in EF_{ICON} (i.e. Tag = '84'), the Icon Link shall be encoded in binary.

  NOTE: Care has to be taken that the information in the icon descriptor matches the data retrieved from the referenced EF_{ICON}. Otherwise the terminal may revert to default behaviour.

4.6.1.5 EF_{ICON}

This EF contains the data for one icon.

Structure of EF_{ICON} at $DF_{graphics}$-level

Identifier: '4F XX'	Structure: transparent	Optional
SFI: Optional		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O/C	Length
1 to M	Media type TLV (tag = '80')	C	M bytes
M+1 to M+N	Icon data TLV (tag = '81')	M	N bytes
M+N+1 to X	'FF' padding	O	X-M-N bytes

If no reference in $EF_{LAUNCH\ SCWS}$ points to it, an icon file may contain arbitrary values.

Media type and icon data are coded as BER TLVs as defined in TS 101 220 [3]. The media type TLV shall be present if no media type is specified in the icon coding scheme of the entry in $EF_{LAUNCH\ SCWS}$ that points to this file, else it is optional.

Media type value part:

- Contents:
  - Text string specifying the icon encoding.
- Coding:
  - As defined in RFC 2046 [61] and registered with IANA at http://www.iana.org/assignments/media-types/ e.g. "image/png".

Icon data value part:

- Contents:
  - The graphical data of the icon.
- Coding:
  - Binary data as defined for the respective media type.

4.6.2 Contents of files at the $DF_{PHONEBOOK}$ under the $DF_{TELECOM}$

This DF has the same structure as $DF_{PHONEBOOK}$ under the ADF_{USIM}.

4.6.3 Contents of files at the $DF_{MULTIMEDIA}$ level

The Efs in the Dedicated File $DF_{MULTIMEDIA}$ contain multimedia information. This DF shall be present if service n°67 is available, i.e. if the card supports MMS storage.

4.6.3.1 EF_{MML} (Multimedia Messages List)

If service n°67 is "available", this file shall be present.

This file contains information about the MM data stored in EF_{MMDF}. MM information are encapsulated in a BER-TLV data object. Each data object in EF_{MML} points to a corresponding MM in EF_{MMDF}.

Identifier: '4F47'	Structure: BER-TLV	Optional
	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	MM Descriptor Data Object(s)	M	X bytes

- MM Descriptor Data Object
  The content and coding are defined below:

Coding of the MM Descriptor Data Objects

Length	Description	Coding	Status
1 to A bytes (A ≤ 3)	MM Descriptor Data Object tag	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 to B bytes (B ≤ 4)	MM Descriptor Data Object length	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 byte	MMS Implementation tag '80'		M
1 byte	MMS Implementation length		M
1 byte	MMS Implementation	See below	M
1 byte	MM File Identifier / SFI tag '81'		M
1 byte	MM File Identifier / SFI length		M
1 or 2 bytes	MM File Identifier / SFI	See below	M
1 byte	MM Content Data Object Tag tag '82'		M
1 byte	MM Content Data Object Tag length		M
1 to C bytes (C ≤ 3)	MM Content Data Object Tag	See below	M
1 byte	MM Size tag '83'		M
1 byte	MM Size length		M
1 to D bytes (D ≤ 4)	MM Size in bytes	See below	M
1 byte	MM Status tag '84'		M
1 byte	MM Status length		M
2 bytes	MM Status	See below	M
1 byte	MM Alpha Identifier tag '85'		M
1 byte	MM Alpha Identifier length		M
1 to E bytes	MM Alpha Identifier	See below	M

- MMS Implementation

Contents:

The MMS Implementation indicates the used implementation type, e.g. WAP.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	WAP implementation of MMS
2 to 8	Reserved for future use

Bit value	Meaning
0	Implementation not supported.
1	Implementation supported.

- MM File Identifier / SFI

Contents:

file identifier or SFI of EF_{MMDF} which contains the actual MM message. If the length of this TLV object is equal to 1 then the content indicates the SFI of the EF_{MMDF}, the SFI is coded on b1 to b5. Otherwise the TLV contains the file identifier.

Coding:

according to TS 31.101 [11].

- MM Content Data Object Tag

Contents:

tag indentifying a MM (i.e. identifying a data object) within EF_{MMDF}.

Coding:

according to TS 31.101 [11].

- MM Size

Contents:

size of the corresponding MM stored in EF_{MMDF}.

Coding:

according to TS 31.101 [11].

- MM Status

Contents:

The status bytes contain the status information of the stored Multimedia Message.

Coding:

First byte:

bit b1 indicates whether the MM has been read or not. Bit b2 indicates the MM forwarding status. Bit b3 indicates whether it is a received MM or an originated MM. Bits b4 to b8 are reserved for future use.

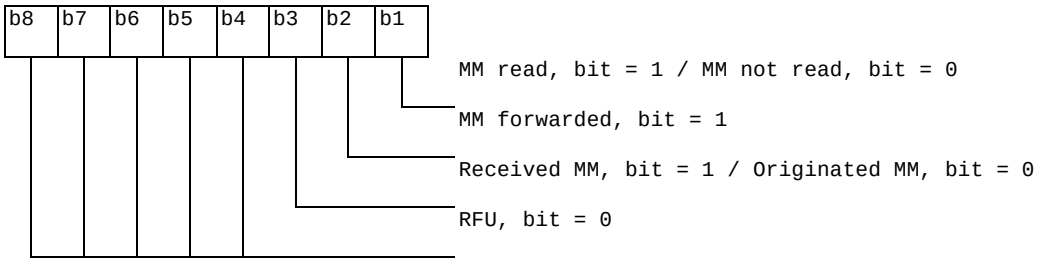
Second byte:

Coding of the second byte depends on whether the MM has been identified as a received MM or originated MM in the first byte:

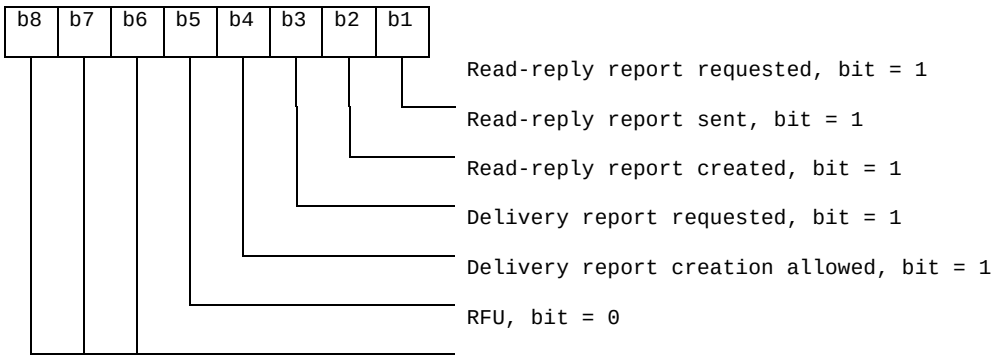
- Received MM coding:
  bits b1 and b2 are used to provide information on Read-reply reports. Bits b3 to b8 are reserved for future use.

- Originated MM coding:
  bit b1 is used to provide information on Delivery-report. Bits b2 to b8 are reserved for future use.

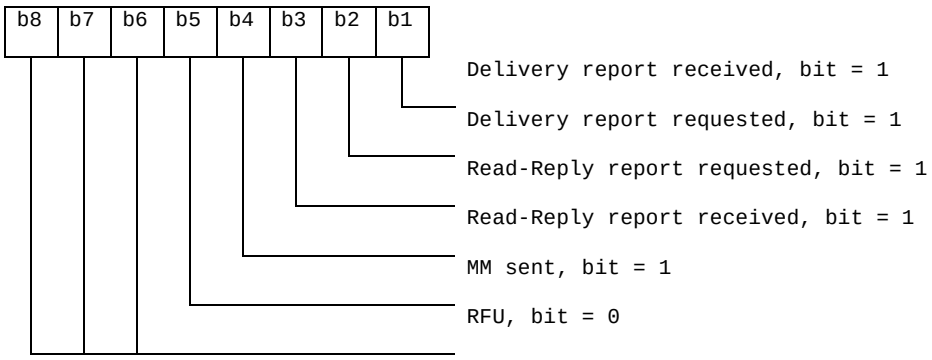
First byte:



Second byte coding for Received MM:



Second byte coding for Originated MM:



- MM Alpha Identifier

Contents:

information about the MM to be displayed to the user (e.g. sender, subject, date etc).

Coding:

this alpha identifier shall use either:

- the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF';
- or one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

4.6.3.2 EF_{MMDF} (Multimedia Messages Data File)

If service n°67 is "available", this file shall be present.

Residing under $DF_{MULTIMEDIA}$, this EF contains Multimedia Messages data. The structure of this EF is BER-TLV (see TS 31.101 [11]). Each MM in this file is identified by a tag. The tag value for a particular MM in this file is stored in EF_{MML}.

Identifier: '4F48'	Structure: BER-TLV	Optional
	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	MM Content Data Object(s)	M	X bytes

- MM Content Data Object
  The content and coding are defined below:

Coding of the MM Content Data Objects

Length	Description	Coding	Status
1 to T bytes (T ≤ 3)	MM Content Data Object tag	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 to L (L ≤ 4)	MM Content Data Object length	As defined in TS 31.101 [11] for BER-TLV structured files	M
X-L-T bytes	MM Content	According to MMS Implementation	M

Contents:
The Multimedia Message content consists of MM headers and a message body. The content of the Multimedia Message data depends on whether the MM has been identified as a received MM or an originated MM:

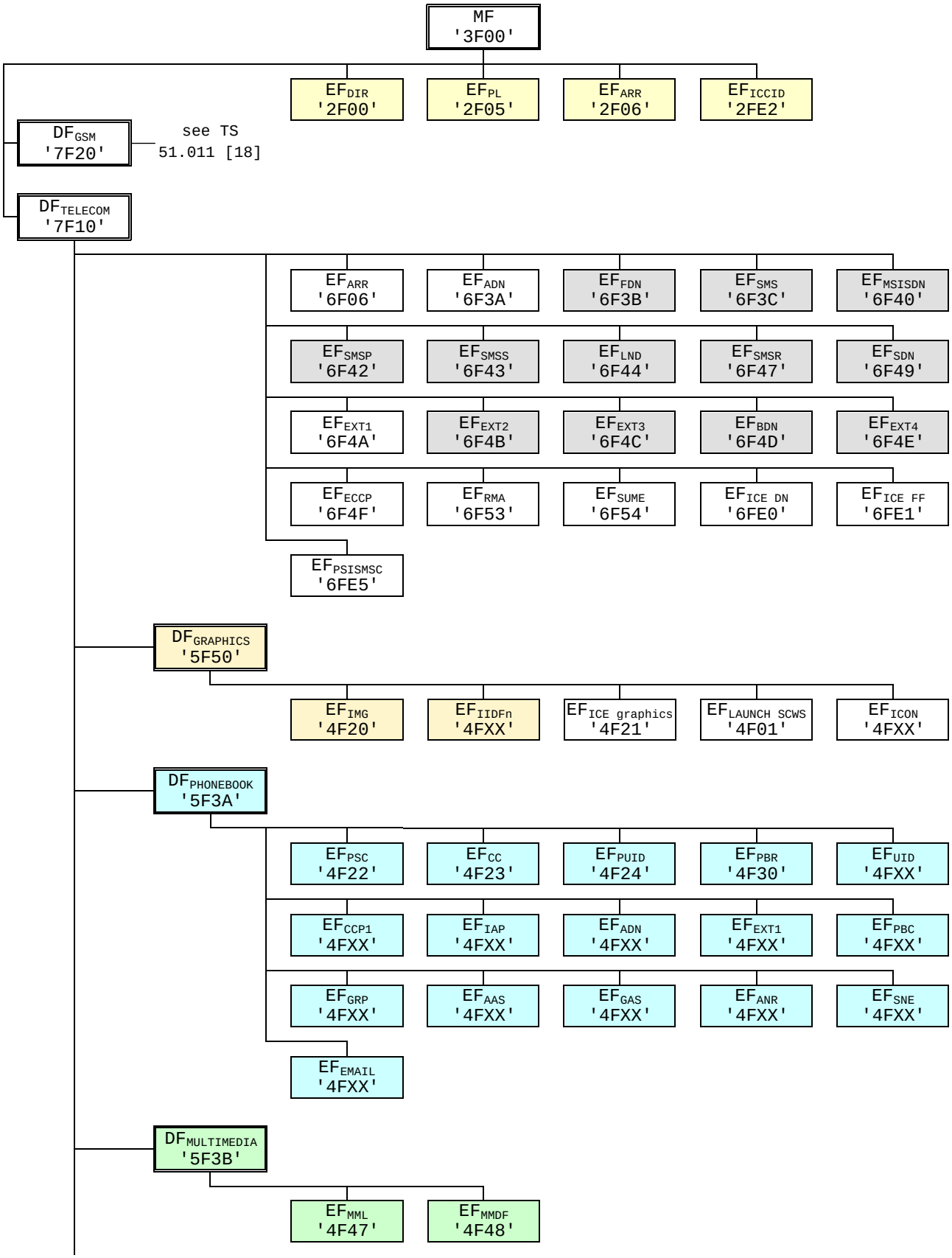
- For a received message, the stored Multimedia Message data consists of the information elements (i.e. relevant MM control information and MM content) of the MM1_retrieve.RES (see TS 23.140 [38]).

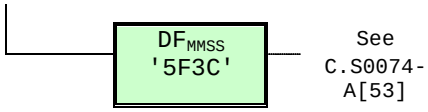
- For an originated message, the stored Multimedia Message data consists of the information elements (i.e. relevant MM control information and MM content) of the MM1_submit.REQ (see TS 23.140 [38]).

Coding:
The MM data encapsulation scheme and encoding rules are defined by the MMS Implementation.

4.7 Files of USIM

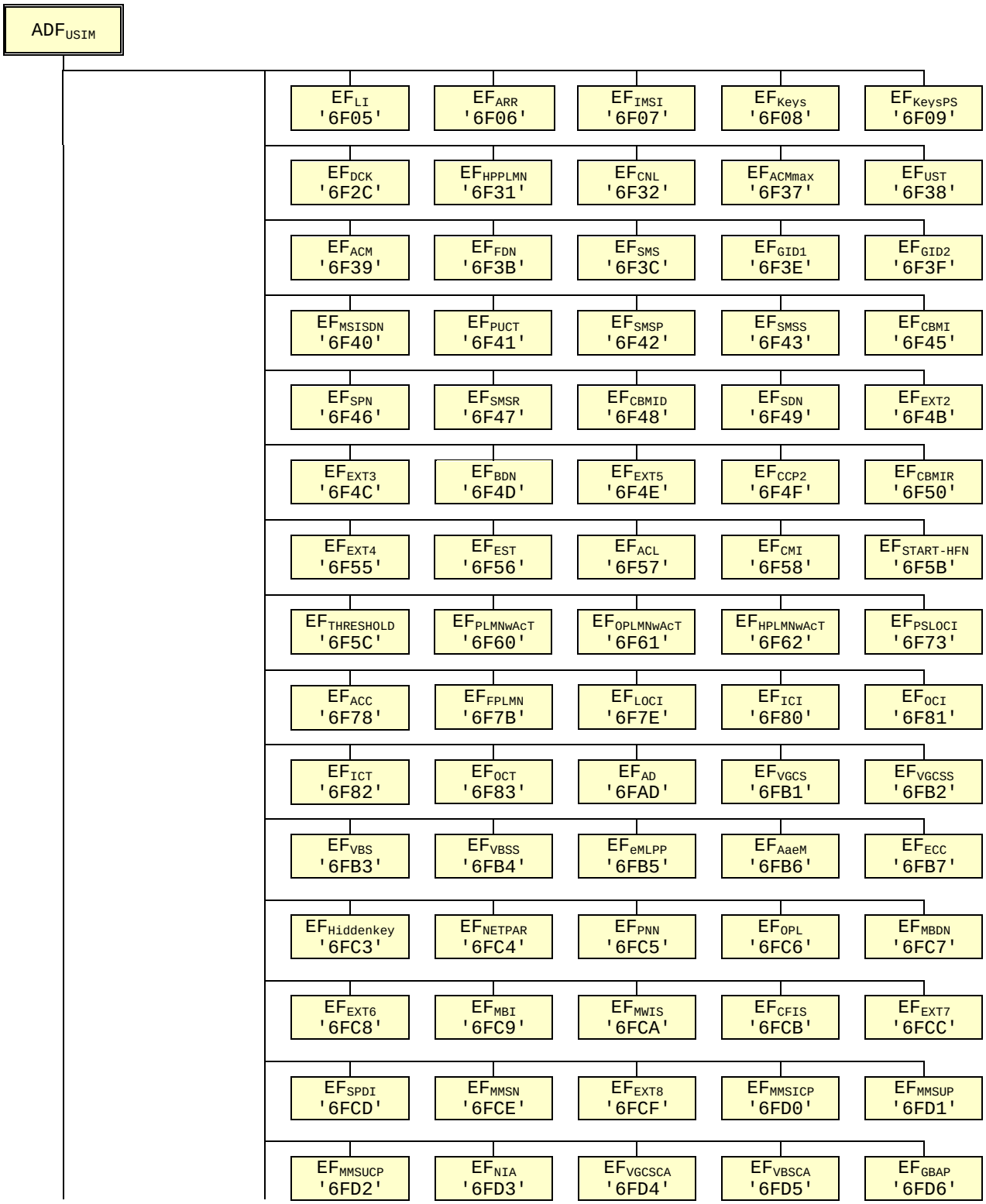
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.

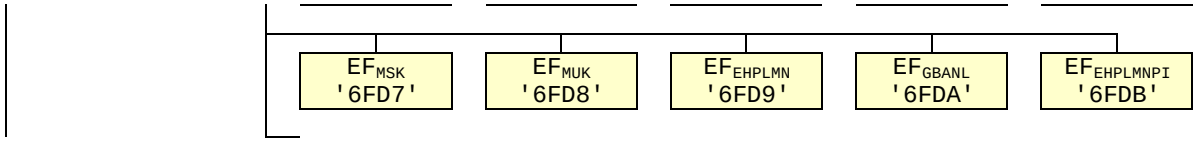


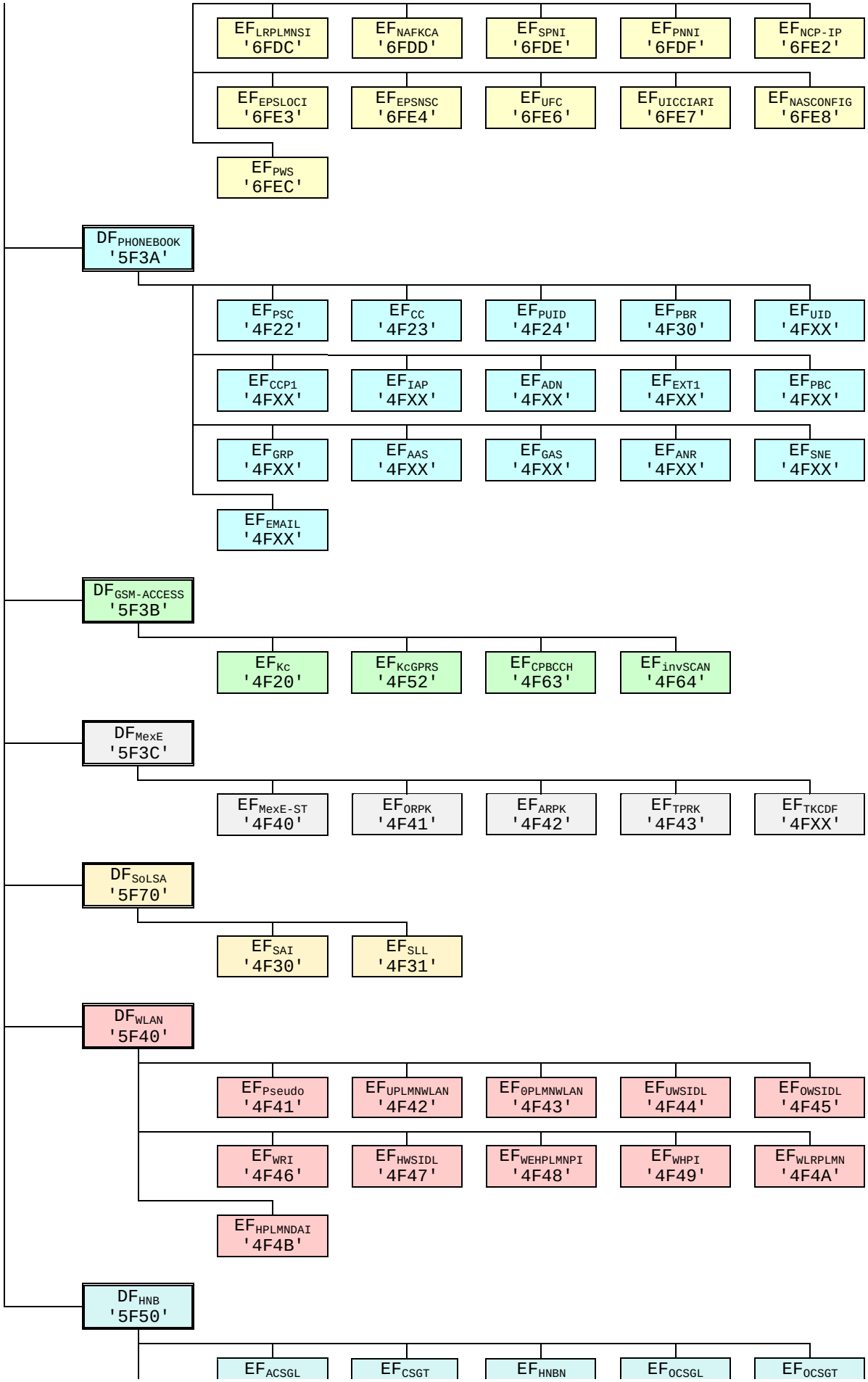


NOTE 1: Files under $DF_{TELECOM}$ with shaded background are defined in TS 51.011 [18].
NOTE 2: The value '6F65' under ADFUSIM was used in earlier versions of this specification, and should not be re-assigned in future versions.
NOTE 3: Files under DF_{MMSS} are defined in C.S0074-A [53].

Figure 4.1: File identifiers and directory structures of UICC




EF MSK
'6FD7'
EF MUK
'6FD8'
EF EHPLMN
'6FD9'
EF GBANL
'6FDA'
EF EHPLMNPI
'6FDB'


EF LRPLMNSI '6FDC'
EF NAFKCA '6FDD'
EF SPNI '6FDE'
EF PNNI '6FDF'
EF NCP-IP '6FE2'
EF EPSLOCI '6FE3'
EF EPSNSC '6FE4'
EF UFC '6FE6'
EF UICCIARI '6FE7'
EF NASCONFIG '6FE8'
EF PWS '6FEC'
DF PHONEBOOK '5F3A'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF UID '4FXX'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
DF GSM-ACCESS '5F3B'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
DF MexE '5F3C'
EF MexE-ST '4F40'
EF ORPK '4F41'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
DF SoLSA '5F70'
EF SAI '4F30'
EF SLL '4F31'
DF WLAN '5F40'
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF OPLMNWLAN '4F43'
EF UWSIDL '4F44'
EF OWSIDL '4F45'
EF WRI '4F46'
EF HWSIDL '4F47'
EF WEHPLMNPI '4F48'
EF WHPI '4F49'
EF WLRPLMN '4F4A'
EF HPLMNDAI '4F4B'
DF HNB '5F50'
EF ACSGL
EF CSGT
EF HNBN
EF OCSGL
EF OCSGT

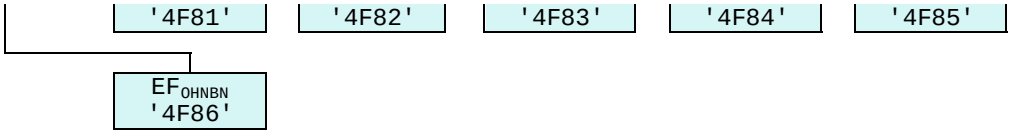


Figure 4.2: File identifiers and directory structures of USIM

5 Application protocol

The requirements stated in the corresponding section of TS 31.101 [11] apply to the USIM application.

The procedures listed in clause "USIM management procedures" are required for execution of the procedures in the subsequent clauses "USIM security related procedures" and "Subscription related procedures". The procedures listed in clauses "USIM security related procedures" are mandatory. The procedures listed in "Subscription related procedures" are only executable if the associated services, which are optional, are provided in the USIM. However, if the procedures are implemented, it shall be in accordance with clause "Subscription related procedures".

If a procedure is related to a specific service indicated in the USIM Service Table, it shall only be executed if the corresponding bits denote this service as "service available" (see clause "EF_{UST}"). In all other cases the procedure shall not start.

5.1 USIM management procedures

If a USIM application is present on the UICC, a 3GPP ME shall only use the USIM application regardless of the radio access technology in use. In this case, a possibly existing SIM application shall never be used by a 3GPP ME.

5.1.1 Initialisation

5.1.1.1 USIM application selection

After UICC activation (see TS 31.101 [11]), the ME selects a USIM application. If no EF_{DIR} file is found or no USIM applications are listed in the EF_{DIR} file, the ME may then try to select the GSM application as specified in TS 51.011 [18].

NOTE: there may be cards that need to be reset before selecting the GSM application.

After a successful USIM application selection, the selected USIM (AID) is stored on the UICC. This application is referred to as the last selected USIM application. The last selected USIM application shall be available on the UICC after a deactivation followed by an activation of the UICC.

If a USIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a USIM application. Furthermore if a USIM application is selected using a partial DF name as specified in TS 31.101 [11] indicating in the SELECT command the last occurrence the UICC shall select the USIM application stored as the last USIM application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

5.1.1.2 USIM initialisation

The ME requests the emergency call codes. For service requirements, see TS 22.101 [24].

The ME requests the Language Indication. The preferred language selection shall always use the EF_{LI} in preference to the EF_{PL} at the MF unless any of the following conditions applies:

- if the EF_{LI} has the value 'FFFF' in its highest priority position, then the preferred language selection shall be the language preference in the EF_{PL} at the MF level according the procedure defined in TS 31.101 [11];

- if the ME does not support any of the language codes indicated in EF_{LI}, or if EF_{LI} is not present, then the language selection shall be as defined in EF_{PL} at the MF level according the procedure defined in TS 31.101 [11];
- if neither the languages of EF_{LI} nor EF_{PL} are supported by the terminal, then the terminal shall use its own internal default selection.

The ME then runs the user verification procedure. If the procedure is not performed successfully, the USIM initialisation stops.

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

The ME performs the Enabled Services Table Request.

In case FDN is enabled, an ME which does not support FDN shall allow emergency calls but shall not allow MO-CS calls and MO-SMS.

If BDN is enabled, an ME which does not support Call Control shall allow emergency calls but shall not allow MO-CS calls.

If ACL is enabled, an ME which does not support ACL shall not send any APN to the network.

If all these procedures have been performed successfully then 3G session shall start. In all other cases 3G session shall not start.

Afterwards, the ME runs the following procedures if the ME and the USIM support the related services:

- IMSI request;
- Access control information request;
- Higher Priority PLMN search period request;
- EHPLMN request
- HPLMN selector with Access Technology request;
- User controlled PLMN selector with Access Technology request;
- Operator controlled PLMN selector with Access Technology request;
- GSM initialisation requests;
- Location Information request for CS-and/or PS-mode and/or EPS;
- Cipher key and integrity key request for CS- and/or PS-mode;
- EPS NAS Security Context request for EPS;
- Forbidden PLMN request;
- Initialisation value for hyperframe number request;
- Maximum value of START request;
- CBMID request;
- Depending on the further services that are supported by both the ME and the USIM the corresponding Efs have to be read.

After the USIM initialisation has been completed successfully, the ME is ready for a 3G session and shall indicate this to the USIM by sending a particular STATUS command.

5.1.1.3 GSM related initialisation procedures

If GSM access is enabled the following procedures shall be performed if the applicable service is enabled and if the ME supports the GSM compact access technology.

- Investigation Scan request;
- CPBCCH information request.

5.1.2 Session termination

5.1.2.1 3G session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [11].

The 3G session is terminated by the ME as follows.

The ME shall indicate to the USIM by sending a particular STATUS command that the termination procedure is starting.

The ME then runs all the procedures which are necessary to transfer the following subscriber related information to the USIM, if the ME and the USIM support the related services:

- Location Information update for CS-and/or PS-domain and/or EPS.
- Cipher Key and Integrity Key update for CS-and/or PS-domain.
- EPS NAS Security Context update for EPS domain.
- Advice of Charge increase.
- Forbidden PLMN update.
- GSM Termination procedures.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the 3G session, and the value has not changed until 3G session termination, the ME may omit the respective update procedure.

To actually terminate the session, the ME shall then use one of the mechanisms described in TS 31.101 [11].

5.1.2.1.1 GSM termination procedures

If GSM access is enabled the following termination procedures shall be performed if the applicable service is enabled.

- CPBCCH information update (if the ME supports the GSM compact access technology);

5.1.2.2 3G session reset

The ME shall follow the 3G session termination procedure defined above except that the ME shall use the Application session reset procedure as described in TS 31.101 [11] instead of one of the mechanisms to terminate the session.

5.1.3 USIM application closure

After termination of the 3G session as defined in 5.1.2 the USIM application may be closed by closing the logical channels that are used to communicate with this particular USIM application.

5.1.4 Emergency call codes

Request: The ME performs the reading procedure with EF_{ECC}. If EF_{ECC} does not contain any valid number, the ME shall use the emergency numbers it stores for use in setting up an emergency call without a USIM.

Update: The ME performs the updating procedure with EF_{ECC}.

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, PIN or PIN2.

5.1.5 Language indication

Request: The ME performs the reading procedure with EF_{LI}.

Update: The ME performs the updating procedure with EF_{LI}.

5.1.6 Administrative information request

The ME performs the reading procedure with EF_{AD}.

5.1.7 USIM service table request

The ME performs the reading procedure with EF_{UST}.

5.1.8 Void

5.1.9 UICC presence detection

The ME checks for the presence of the UICC according to TS 31.101 [11] within all 30 s periods of inactivity on the UICC-ME interface during a call. If the presence detection according to TS 31.101 [11] fails the call shall be terminated as soon as possible but at least within 5s after the presence detection has failed. Here a call covers a circuit switched call, and/or an active PDP context.

5.2 USIM security related procedures

5.2.1 Authentication algorithms computation

The ME selects a USIM application and uses the AUTHENTICATE command (see 7.1.1). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

After a successful AUTHENTICATE command, the ME shall perform cipher and integrity key update procedure.

5.2.2 IMSI request

The ME performs the reading procedure with EF_{IMSI}.

5.2.3 Access control information request

The ME performs the reading procedure with EF_{ACC}.

5.2.4 Higher Priority PLMN search period request

The ME performs the reading procedure with EF_{HPPLMN}.

5.2.5 Location information

Request: The ME performs the reading procedure with EF_{LOCI}.

Update: The ME performs the updating procedure with EF_{LOCI}.

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '6581' (Memory Problem), the ME shall terminate 3G operation.

5.2.6 Cipher and Integrity key

Request: The ME performs the reading procedure with EF_{Keys}.

Update: The ME performs the updating procedure with EF_{Keys}.

5.2.7 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{FPLMN}.

Update: The ME performs the updating procedure with EF_{FPLMN}.

5.2.8 Void

5.2.9 User Identity Request

The ME selects a USIM and performs the reading procedure with EF_{IMSI}.

5.2.10 GSM Cipher key

Requirement: Service n°27 "available".

Request: The ME performs the reading procedure with EF_{Kc}.

Update: The ME performs the updating procedure with EF_{Kc}.

5.2.11 GPRS Cipher key

Requirement: Service n°27 "available".

Request: The ME performs the reading procedure with EF_{KcGPRS}.

Update: The ME performs the updating procedure with EF_{KcGPRS}.

5.2.12 Initialisation value for Hyperframe number

Request: The ME performs the reading procedure with $EF_{START\text{-}HFN}$.

Update: The ME performs the updating procedure with $EF_{START\text{-}HFN}$.

5.2.13 Maximum value of START

Request: The ME performs the reading procedure with $EF_{THRESHOLD}$.

5.2.14 HPLMN selector with Access Technology request

Request: The ME performs the reading procedure with $EF_{HPLMNwAcT.}$

5.2.15 Packet Switched Location information

Request: The ME performs the reading procedure with EF_{PSLOCI}.

Update: The ME performs the updating procedure with EF_{PSLOCI}.

5.2.16 Cipher and Integrity key for Packet Switched domain

Request: The ME performs the reading procedure with EF_{KeysPS}.

Update: The ME performs the updating procedure with EF_{KeysPS}.

5.2.17 LSA information

Requirement: Service n°23 "available".

Request: The ME performs the reading procedure with EF_{SAI}, EF_{SLL} and its associated LSA Descriptor files.

Update: The ME performs the updating procedure with EF_{SLL}.

5.2.18 Voice Group Call Services

Requirement: Service n°57 "available".

Voice Group Call Service

Request: The ME performs the reading procedure with EFVGCS.

Voice Group Call Service Status

Request: The ME performs the reading procedure with EFVGCSS.

Update: The ME performs the updating procedure with EFVGCSS.

5.2.19 Voice Broadcast Services

Requirement: Service n°58 "available".

Voice Broadcast Service

Request: The ME performs the reading procedure with EF_{VBS}.

Voice Broadcast Service Status

Request: The ME performs the reading procedure with EF_{VBSS}.

Update: The ME performs the updating procedure with EF_{VBSS}.

5.2.20 Generic Bootstrapping architecture (Bootstrap)

The ME uses the AUTHENTICATE command in GBA security context (Bootstrapping Mode) (see 7.1.1). The response is sent to the ME.

After a successful GBA_U Procedure, the ME shall update the B-TID field and the Key Life Time field in EF_{GBABP}

5.2.21 Generic Bootstrapping architecture (NAF Derivation)

The ME shall first read EF_{GBABP}. The ME then uses the AUTHENTICATE command in GBA security context (NAF Derviation Mode) (see 7.1.1). The response is sent to the ME.

5.2.22 MSK MIKEY Message Reception

The ME performs the reading of EF_{MUK} and retrieves the Time Stamp Counter Value associated with the involved MUK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [43].

5.2.23 MTK MIKEY Message Reception

The ME performs the reading of EF_{MSK} and retrieves the Time Stamp Counter Value associated with the involved MSK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [43].

5.2.24 Void

5.2.25 EHPLMN request

Requirement: Service n°71 "available".

Request: The ME performs the reading procedure with EF_{EHPLMN}.

5.2.26 Last RPLMN Selection Indication request

Requirement: Service n°74 "available".

Request: The ME performs the reading procedure with $EF_{LRPLMNSI}$.

5.2.27 EPS Location Information

Requirement: Service n°85 "available".

Request: The ME performs the reading procedure with $EF_{EPSLOCI}$.

Update: The ME performs the updating procedure with $EF_{EPSLOCI.}$

5.2.28 EPS NAS Security Context

Requirement: Service n°85 "available".

Request: The ME performs the reading procedure with EF_{EPSNSC}.

Update: The ME performs the updating procedure with $EF_{EPSNSC.}$

In order to prevent UICC memory wear out due to excessive writing, the update of EPS NAS security context shall be according to the rules and procedures specified in TS 33.401 [52].

5.2.29 Non Access Stratum Configuration

Requirement: Service n°96 "available".

Request: The ME performs the reading procedure with $EF_{NASCONFIG}$.

The parameters in $EF_{NASCONFIG}$ shall take precedence over the parameters stored in the ME non-volatile memory.

5.2.30 PWS Configuration

Requirement: Service n°97 "available".

Request: The ME performs the reading procedure with EF_{PWS}.

5.3 Subscription related procedures

5.3.1 Phone book procedures

5.3.1.1 Initialisation

The ME first reads the content of EF_{PBR} to determine the configuration phonebook. If the EF_{IAP} file is indicated in EF_{PBR} following tag 'A8' the ME reads the content of EF_{IAP} in order to establish the relation ship between the content in the files indicated using tag 'A9' and files indicated by tag 'A8'. The ME may read the contents of the phone book related files in any order.

5.3.1.2 Creation/Deletion of information

In order to avoid unlinked data to introduce fragmentation of the files containing phone book data the following procedures shall be followed when creating a new entry in the phone book. The data related to EF_{ADN} is first stored in the relevant record. As the record number is used as a pointer the reference pointer is now defined for the entry. The rule for storing additional information for an entry is that the reference pointer shall be created before the actual data is written to the location.

In case of deletion of a complete or part of an entry the data shall be deleted first followed by the reference pointer for that data element. In case of deletion of a complete entry the contents of EF_{ADN} is the last to be deleted.

5.3.1.3 Hidden phone book entries

If a phone book entry is marked as hidden by means of EF_{PBC} the ME first prompts the user to enter the 'Hidden Key'. The key presented by the user is compared against the value that is stored in the corresponding $EF_{Hiddenkey}$. Only if the presented and stored hidden key are identical the ME displays the data stored in this phone book entry. Otherwise the content of this phone book entry is not displayed by the ME.

Even if the terminal does not support the Hidden Key Procedures, a hidden phone book entry shall not be displayed by the terminal.

Request: The ME performs the reading procedure with $EF_{Hiddenkey}$.

Update: The ME performs the updating procedure with $EF_{Hiddenkey}$.

5.3.2 Dialling numbers

Requirements:

- Service n°1 "available" for ADN located under the local phonebook;
- Presence of EF_{ADN} in EF_{PBR} for ADN located under the global phonebook;
- Presence of EF_{ANR} in EF_{PBR} for ANR;
- Service n°2 "available" for FDN;
- Service n°21 "available" for MSISDN;
- Service n°4 "available" for SDN;
- Service n°6 "available" for BDN;
- Service n°8 "available" for EFOCI;
- Service n°9 "available" for EFICI.

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCP1} and EF_{EXT1} as described in the procedures below, but also to EF_{ANR}, EF_{FDN}, EF_{MSISDN}, EF_{BDN}, EF_{SDN}, EF_{OCI}, EF_{ICI}, and EF_{MBDN} and their associated extension files. If these files are not "available", as denoted in the USIM service table, the current procedure shall be aborted and the appropriate Efs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the definition of the relevant Efs in the present document):

i) The ME identifies the Alpha-tagging, Capability/Configuration1 Record Identifier and Extension1 Record Identifier.

ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:

- if a "+" is found, the TON identifier is set to "International";

- if 20 or less "digits" remain, they shall form the dialling number/SSC string;

- if more than 20 "digits" remain, the procedure shall be as follows:

- The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

- The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data.

iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:

- If the length of the called party subaddress is less than or equal to 11 bytes (see TS 24.008 [9] for coding):

- The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

- The ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".

- If the length of the called party subaddress is greater than 11 bytes (see TS 24.008 [9] for coding):

  - The ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted.

  - The ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1} record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the USIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

For reasons of memory efficiency, the ME may analyse all Extension1 records to recognise if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case, the ME may use the existing chain or the last part of the existing chain from more than one ADN. The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

Erasure: The ME sends the identification of the information to be erased. The content of the identified record in EF_{ADN} is marked as "free".

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP1}. If necessary, then the ME performs the reading procedure on these Efs to assemble the complete ADN/SSC.

Purge: The ME shall access each EF which references EF_{EXT1} (EF_{EXT2}, EF_{EXT6}) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2, Extension6) records are noted by the ME. All Extension1 (Extension2, Extension6) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'.

The following three procedures are only applicable to service n°2 (FDN).

FDN capability request. The ME shall check the state of service n°2, i.e. if FDN is "enabled" or "disabled". If FDN is enabled, the ME shall only allow outgoing calls as defined in the fixed number dialling description in TS 22.101 [24]. To ascertain the state of FDN, the ME shall check in EF_{UST} and EF_{EST} if FDN is enabled (service activated and available). In all other cases service n°2 is disabled.

FDN enabling is done by activating the FDN service in EF_{EST}.

FDN disabling is done by deactivating the FDN service in EF_{EST}.

The following three procedures are only applicable to service n°6 (BDN).

- BDN capability request. The ME shall check the state of service n°6, i.e. if BDN is "enabled" or "disabled". To ascertain the state of BDN, the ME shall check in EF_{UST} and EF_{EST} if BDN is "enabled" (service available and activated). In all other cases, the BDN service is "disabled".
- BDN enabling is done by activating the BDN service in EF_{EST}.
- BDN disabling is done by deactivating the BDN service in EF_{EST}.

5.3.3 Short messages

Requirement: Service n°10 "available".

Request: The USIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.

If service n°10 is "available" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the reading procedure with the corresponding record in EF_{SMSR}. If the ME does not find a corresponding record in EF_{SMSR}, then the ME shall update the status of the SMS with '15' (status report requested, received but not stored in EF_{SMSR}).

If the short message is not found within the USIM memory, the USIM indicates that to the ME.

Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.

If there is no available empty space in the USIM to store the received short message, a specific MMI will have to take place in order not to loose the message.

Erasure: The ME will select in the USIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the USIM is made available for a new incoming message. The memory of the USIM may still contain the old message until a new message is stored in this area.

If service n°11 is "available" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

5.3.4 Advice of charge

Requirement: Service n°13 "available".

Accumulated Call Meter.

Request: The ME performs the reading procedure with EF_{ACM}. The USIM returns the last updated value of the ACM.

Initialisation: The ME performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The ME performs the reading procedure with EF_{ACMmax}.

Initialisation: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The ME performs the reading procedure with EF_{PUCT}.

Update: The ME performs the updating procedure with EF_{PUCT}.

5.3.5 Capability configuration parameters

Requirement: Service n°14 "available".

Request: The ME performs the reading procedure with EF_{CCP2}.

Update: The ME performs the updating procedure with EF_{CCP2}.

Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP2} is marked as "free".

5.3.6 User controlled PLMN selector with Access Technology

Requirement: Service n°20 "available".

Request: The ME performs the reading procedure with $EF_{PLMNwACT}$.

Update: The ME performs the updating procedure with $EF_{PLMNwACT}$.

5.3.7 Cell broadcast message identifier

Requirement: Service n°15 "available".

Request: The ME performs the reading procedure with EF_{CBMI}.

Update: The ME performs the updating procedure with EF_{CBMI}.

5.3.8 Group identifier level 1

Requirement: Service n°17 "available".

Request: The ME performs the reading procedure with EF_{GID1}.

5.3.9 Group identifier level 2

Requirement: Service n°18 "available".

Request: The ME performs the reading procedure with EF_{GID2}.

5.3.10 Service provider name

Requirement: Service n°19 "available".

Request: The ME performs the reading procedure with EF_{SPN}.

5.3.11 Enhanced multi level precedence and pre-emption service

Requirement: Service n°24 "available".

Request: The ME performs the reading procedure with EF_{eMLPP}.

5.3.12 Cell broadcast message identifier ranges

Requirement: Service n°16 "available".

Request: The ME performs the reading procedure with EF_{CBMIR}.

Update: The ME performs the updating procedure with EF_{CBMIR}.

5.3.13 Short message status report

Requirement: Service n°11 "available".

Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the search record function with EF_{SMSR} to identify the record containing the appropriatestatus report. The ME performs the reading procedure with EF_{SMSR}.

Update: If a status report is received, the ME first seeks within the SMS record identifiers of EF_{SMSR} for the same record number it used for the short message in EF_{SMS}. If such a record identifier is found in EF_{SMSR}, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the ME runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.

If the ME found an appropriate record in EF_{SMSR} for storage, it updates the record with the status report setting the record identifier in EF_{SMSR} to the appropriate record number of the short message in EF_{SMS}.

The status in EF_{SMS} is updated accordingly by performing the update procedure with EF_{SMS}.

Erasure: The ME runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the ME checks the corresponding short messages in EF_{SMS}. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in EF_{SMSR}), the ME shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

5.3.14 APN Control List

Requirement: Service n°35 "available".

Request: The ME performs the reading procedure with EF_{ACL}.

Update: The ME performs the updating procedure with EF_{ACL}.

Enabling: The ME activates service n°3 in EF_{EST} (bit n°3 set to "1").

Disabling: The ME deactivates service n°3 in EF_{EST} (bit n°3 set to "0").

When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EF_{ACL} before requesting this PDP context activation from the network. If the APN is not present in EF_{ACL}, the ME shall not request the corresponding PDP context activation from the network.

In the case that the APN Control List is enabled and no APN is indicated in the PDP context request, indicating that a network provided APN is to be used, then the ME shall only request the PDP context activation if "network provided APN" is contained within EF_{ACL}.

If the APN Control List service is enabled and the ME is to provide an APN as part of attach for PDN connectivity, then the ME shall verify that the APN value is present in the EF_{ACL} and if it is not the ME shall not proceed with the attach procedure. If the APN Control List service is enabled and the ME does not indend to provide an APN as part of the attach for PDN connectivity and use a network provided APN, the ME shall not check if "network provided APN" is contained within EF_{ACL}.

5.3.15 Depersonalisation Control Keys

Requirement: Service n°36 "available".

Request: The ME performs the reading procedure with EF_{DCK}.

5.3.16 Co-operative Network List

Requirement: Service n°37 "available".

Request: The ME performs the reading procedure with EF_{CNL}.

5.3.17 CPBCCH information

Requirement: Service n°39 "available".

Request: The ME performs the reading procedure with EF_{CPBCCH}.

Update: The ME performs the updating procedure with EF_{CPBCCH}.

5.3.18 Investigation Scan

Requirement: Service n°40 "available".

Request: The ME performs the reading procedure with $EF_{InvScan}$.

5.3.19 Enabled Services Table Request

Requirement: Service n°2, 6, 34 or 35 "available".

Request: The ME performs the reading procedure with EF_{EST}.

Update: The ME performs the updating procedure with EF_{EST}.

5.3.20 Operator controlled PLMN selector with Access Technology

Requirement: Service n°42 "available".

Request: The ME performs the reading procedure with $EF_{OPLMNwACT}$

5.3.21 HPLMN selector with Access Technology

Requirement: Service n°43 "available".

Request: The ME performs the reading procedure with EFHPLMNwACT

5.3.22 Automatic Answer on eMLPP service

Requirement: Service n°25 "available"

Request: The ME performs the reading procedure with EF_{AaeM}.

Update: The ME performs the updating procedure with EF_{AaeM}.

5.3.23 Network Parameter information

Request: The ME performs the reading procedure with EF_{NETPAR}.

Update: The ME performs the updating procedure with EF_{NETPAR}.

5.3.24 PLMN network name

Requirement: Service n°45 "available".

Request: The ME performs the reading procedure with EF_{PNN}.

5.3.25 Operator PLMN List

Requirement: Service n°46 "available".

Request: The ME performs the reading procedure with EF_{OPL}

5.3.26 Message Waiting Indication

Requirement: Service n°48 "available".

Request: The ME performs the reading procedure with EF_{MWIS}.

Update: The ME performs the updating procedure with EF_{MWIS}.

5.3.27 Call Forwarding Indication Status

Requirement: Service n°49 "available".

Request: The ME performs the reading procedure with EF_{CFIS}.

Update: The ME performs the updating procedure with EF_{CFIS}.

5.3.28 Service Provider Display Information

Requirement: Service n°19 and 51 are "available".

Request: The ME performs the reading procedure with EF_{SPDI}.

Update: The ME performs the updating procedure with EF_{SPDI}.

5.3.29 MMS Notifications

Requirement: Service n°52 "available".

Request: The ME sends the identification of the information to be read, then the ME performs the reading procedure with $EF_{MMSN.}$ If Service n°53 is available the ME shall analyse the data of EF_{MMSN} to ascertain, whether additional data is associated in EF_{EXT8}. If necessary, then the ME performs the reading procedure on EF_{EXT8} to assemble the complete MMS notification.

Update: The ME analyses and assembles the MMS notification to be stored as follows:

- if the MMS notification contains not more bytes than the maximum possible number for EF_{MMSN} then the ME looks for the next available area to store the MMS notification. If such an area is available, it performs the updating procedure with EF_{MMSN}.

- if the MMS notification contains <u>more</u> bytes than the maximum possible number for EF_{MMSN} then the ME seeks for a sufficient number of free records in EF_{EXT8} to store the complete MMS notification.

  - If there is not a sufficient number of EF_{EXT8} records marked as "free" to store the complete MMS notification, the procedure is aborted.

- Otherwise, the ME performs the updating procedure and stores as many bytes as possible in EF_{MMSN}. The Extension file record number of EF_{MMSN} is coded with the associated record number in the EF_{EXT8}. The remaining bytes are stored in the selected EF_{EXT8} record where the type of the record is then set to "additional data". The second byte of the EF_{EXT8} record is set with the number of bytes of the remaining additional data. It is possible, if the number of additional digits exceeds the capacity of the additional record, to chain another record inside the EF_{EXT8} by the identifier in the last byte of the record. In this case byte 2 of each record for additional data within the same chain indicates the number of bytes within the same record.

  The ME is only allowed to store extension data in unused records of EF_{EXT8}

  If there is no available empty space in the USIM to store the MMS notification, it is up to ME implementation how the notification is handled.

Erasure: The ME will select in the USIM the MMS notification to be erased. Depending on the MMI, the MMS notification may be read before the area is marked as "free". The memory of the USIM may still contain the old MMS notification until a new message is stored. If Service n°53 is available all associated records in EF_{EXT8} are then marked by the ME as "free" by setting them to 'FF'.

5.3.30 MMS Issuer Connectivity Parameters

Requirement: Service n°52 "available".

Request: the ME performs the reading procedure with EF_{MMSICP}.

Update: The ME performs the updating procedure with $EF_{MMSICP.}$

5.3.31 MMS User Preferences

Requirement: Service n°52 "available".

Request: the ME performs the reading procedure with EF_{MMSUP}.

Update: The ME performs the updating procedure with $EF_{MMSUP.}$

5.3.32 MMS User Connectivity Parameters

Requirement: Service n°52 and n°55 "available".

Request: the ME performs the reading procedure with EF_{MMSUCP}.

Update: The ME performs the updating procedure with $EF_{MMSUCP.}$

5.3.33 Network's indication of alerting

Requirement: Service n°56 "available".

Request: The ME performs the reading procedure with EF_{NIA}.

5.3.34 Multimedia Messages Storage

If the terminal supports Multimedia Message Storage on the USIM, then the following procedures apply.

As defined in TS 23.140 [38] a Multimedia Message consists of content, or multimedia objects, and headers to describe various properties of that content. An MM is stored in EF_{MMDF}, a BER-TLV structured file.

A list of multimedia messages is stored in the BER-TLV file $EF_{MML}$where each data object identifies one Multimedia Message stored in $EF_{MMDF.}$

Prerequisite: Service n°67 "available".

Request: The ME performs the reading procedures on EF_{MML} to verify the presence and to get the location information of the targeted MM. Then the ME performs the reading procedure of the EF_{MMDF} file to get the MM.

Update: The ME chooses a free identity (i.e. not listed in EF_{MML}) for the multimedia message and check for available space in the EF_{MMDF} file. This procedure could be done for each update or once at the startup of the UE and after a REFRESH command involving one of the $DF_{MULTIMEDIA}$ files. Then the ME performs the following procedures:

If there is no available empty space in the EF_{MMDF} file to store the MM, the procedure is aborted and the user is notified.

Else, the ME stores the MM in EF_{MMDF}, then updates the information in EF_{MML} accordingly.

Erasure: After a successful deletion of an MM in EF_{MMDF} the terminal updates the information in EF_{MML} accordingly.

5.3.35 Equivalent HPLMN Presentation Indication request

Requirement: Service n°73 "available".

Request: The ME performs the reading procedure with $EF_{EHPLMNPI}$.

5.3.36 NAF Key Centre Address request

Requirement: Service n°68 and service n°76 "available".

Request: The ME performs the reading procedure with EF_{NAFKCA}.

5.3.37 Service provider name Icon

Requirement: Service n°19 and service n°78 "available".

Request: The ME performs the reading procedure with EF_{SPN} and EF_{SPNI}.

5.3.38 PLMN network name Icon

Requirement: Service n°45 and service n°79 "available".

Request: The ME performs the reading procedure with EF_{PNN} and EF_{PNNI}.

5.3.39 ICE Information request

The ICE information shall be accessible even when the security features of the UE or UICC have been enabled. The ICE access procedure is described in TS 22.030 [4]. The terminal shall discover that the ICE feature is supported by the ability to select one of the ICE files i.e. EF_{ICE_DN}, EF_{ICE_FF} or $EF_{ICE\_graphics}$.

Request: The terminal performs the read procedure with EF_{ICE_DN} and/or EF_{ICE_FF} and/or $EF_{ICE\_graphics}$.

Update: The terminal performs the update procedure with EF_{ICE_DN} and/or EF_{ICE_FF} and/or $EF_{ICE\_graphics}$.

Disable ICE display: The terminal performs the deactivate procedure consecutively on all the supported files (EF_{ICE_DN}, EF_{ICE_FF} and $EF_{ICE\_graphics}$).

Enable ICE display: The terminal performs the activate procedure consecutively on all the supported files (EF_{ICE_DN}, EF_{ICE_FF} and $EF_{ICE\_graphics}$).

The content of the EF_{ICE_DN}, EF_{ICE_FF} and $EF_{ICE\_graphics}$ shall be preserved when enabling and disabling the ICE display.

5.3.40 eCall Related Procedures

The eCall feature on the USIM provides two numbers, a test number and a reconfiguration number, to the terminal to be used with the eCall. eCall support on the USIM is indicated in the service table when service '89' is "available".

Depending on the type of eCall support, EF_{FDN} or EF_{SDN} is used to provide the eCall functionality.

5.3.40.1 eCall Only support

Requirement: Service n° 89 and Service n° 2 are "available" and FDN service is enabled in EF_{EST}.

Request: The ME performs the reading procedure with EF_{FDN}.

If eCall only calls are supported, then EF_{FDN} shall only contain two entries. The first entry shall contain the eCall test number and the second entry shall contain the eCall reconfiguration number. A terminal in eCall only mode performs the FDN related procedures.

5.3.40.2 eCall and Normal call support

Requirement: Service n° 89 and Service n° 4 are "available".

Request: The ME performs the reading procedure with EF_{SDN}.

If eCall and normal calls are supported, then the last two entries of EF_{SDN} shall contain the eCall test number and the eCall reconfiguration number respectively. A terminal in eCall and normal mode performs the SDN related procedures.

5.3.41 SM-over-IP

Requirement: Service n°12 and n°91 "available".

Request: the ME performs the reading procedure with $EF_{PSISMSC}$.

Update: The ME performs the updating procedure with $EF_{PSISMSC}$.

5.3.42 UICC access to IMS

Requirement: Service n°95 is "available" and the ISIM application defined in TS 31.103 [64] is not present on the UICC.

Request: The terminal performs the reading procedure with $EF_{UICCIARI}$.

The procedures and command for "UICC access to IMS" are defined in TS 31.111 [12]. An ME supporting UICC access to IMS shall perform the reading procedure with $EF_{UICCIARI}$ prior to sending a registration to the IMS.

5.4 USAT related procedures

5.4.1 Data Download via SMS-PP

Requirement: USIM Service n°28 "available".

The procedures and commands for Data Download via SMS-PP are defined in TS 31.111 [12].

5.4.2 Image Request

The terminal sends the identification of the information to be read. The terminal shall analyse the data of EF_{IMG} to identify the files containing the instances of the image. If necessary, then the terminal performs READ BINARY commands on these files to assemble the complete image instance data.

5.4.3 Data Download via SMS-CB

Requirement: USIM Service n°29 "available".

The ME shall perform the reading procedure with EF_{CBMID}, and add the message identifiers to the Cell Broadcast search list. On receiving a cell broadcast message the procedure defined in TS 31.111 [12] applies.

5.4.4 Call Control by USIM

Requirement: USIM Service n°30 "available".

The procedures and commands for Call Control by USIM are defined in TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control by USIM in the TERMINAL PROFILE command.

5.4.5 MO-SMS control by USIM

Requirement: USIM Service n°31 "available".

The procedures and commands for MO-SMS control by USIM are defined in TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports MO-SMS control by USIM in the TERMINAL PROFILE command.

5.4.6 Data Download via USSD and USSD application mode

Requirement: Service n°70 "available".

The procedures and commands for Data Download via USSD and USSD application mode are defined in TS 31.111 [12].

5.4.7 Additional TERMINAL PROFILE after UICC activation

Requirement: USIM Service n°72 "available".

The procedures and commands for Additional TERMINAL PROFILE after UICC activation are defined in TS 31.111 [12] and allow the ME to send multiple Terminal Profile downloads.

5.4.8 Terminal Applications

Requirement: Service n°77 "available"

The procedures and commands for "Terminal Applications" are defined in TS 31.111 [12]

5.4.9 Call control on EPS PDN connection by USIM

Requirement: USIM Service n°87 "available".

The procedures and commands for Call control on EPS PDN connection by USIM are defined in TS 31.111 [12].

5.4.10 Communication Control for IMS by USIM

Requirement: USIM Service n°93 "available".

The procedures and commands for Communication Control for IMS by USIM are defined in TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Communication Control for IMS by USIM in the TERMINAL PROFILE command.

5.4.11 USAT Facility Control

Requirement: The ME supports the USAT over AT feature specified in TS 31.111 [12].

Request: The ME performs the reading procedures of EF_{UFC}.

5.4.12 Extended Terminal Applications

Requirement: Service n°77 and n°94 "available"

The procedures and commands for "Extended Terminal Applications" are defined in TS 31.111 [12].

5.5 MexE related procedures

MexE is an optional feature. The higher level procedures, and contents and coding of the commands are given in TS 23.057 [30]. Procedures relating to the transmission of commands and responses across the USIM/ME interface are given in this clause. A USIM or ME supporting MexE shall conform to the requirements given in this clause.

5.5.1 MexE ST

Requirement: Service n°41 (MexE) "available".

Request: The ME performs the reading procedure with $EF_{MexE\text{-}ST}$

5.5.2 Operator root public key

Requirement: Service n°41 (MexE) "available" and MexE ST service n°1 (EF_{ORPK}) "available".

Request: The ME performs the reading procedure with EF_{ORPK}. The ME shall analyse the data of EF_{ORPK} (clause 4.4.1.4.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.3 Administrator root public key

Requirement: Service n°41 (MexE) "available" and MexE ST service n°2 (EF_{ARPK}) "available".

Request: The ME performs the reading procedure with $EF_{ARPK.}$ The ME shall analyse the data of EF_{ARPK} (clause 4.4.1.4.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

5.5.4 Third Party root public key(s)

Requirement: Service n°41 (MexE) "available" and MexE ST service n°3 (EF_{TPRPK}) "available".

Request: The ME performs the reading procedure with $EF_{TPRPK.}$ The ME shall analyse the data of EF_{TPRPK} (clause 4.4.1.4.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.5 Trusted Key/Certificates Data Files

Requirement: Service n°41 (MexE) "available".

Request: The ME performs the reading procedure with $EF_{TKCDF.}$ The ME shall analyse the data of EF_{TKCDF} and, if necessary, perform READ BINARY commands on these files

5.6 WLAN related procedures

5.6.1 WLAN Selection related Procedures

Requirement: service n°62 or n°63 or n°81 or n°82 or n°83 or n°84 or n°88 "available"

The ME shall read the User, Home and Operator controlled WSIDs, the I-WLAN Equivalent HPLMN Presentation Indication, I-WLAN HPLMN Priority Indication, the I-WLAN Last Registered PLMN and the HPLMN Direct Access Indicationfrom the corresponding list files (i.e. EF_{UWSIDL}, EF_{HWSIDL}, EF_{OWSIDL}, $EF_{WEHPLMNPI}$, $EF_{WLRPLMN}$, EF_{WHPI} and $EF_{HPLMDAI}$)to perform WLAN selection procedures as described in TS 24.234 [40].

The user may change the User controlled WSIDs.

5.6.2 WLAN PLMN Selection related procedures

Requirement: service n°60 or nº61 "available"

The ME shall read the User controlled PLMN selector and/or Operator controlled PLMN selector in $EF_{PLMNWLAN}$ and $EF_{OPLMNWLAN}$ respectively for WLAN PLMN Selection procedures as described in TS 24.234 [40].

The user may change the User controlled PLMN selector for WLAN.

5.6.3 WLAN access authentication related procedures

Requirement: service n°59 "available"

When the ME tries a full authentication, it shall inspect if a valid Pseudonym is available in $EF_{Pseudo.}$and use it as the user name portion of the NAI for WLAN access authentication following the procedures described in TS 24.234 [40].

The ME shall manage pseudonyms as defined in TS 24.234 [40].

5.6.4 WLAN access re-authentication related procedures

Requirement: service n°66 "available"

When the ME tries a fast re-authentication, it shall inspect if a valid reauthentication identity is available in EF_{WRI} and use it as the user name portion of the NAI for WLAN access re-authentication following the procedures described in TS 24.234 [40].

The ME shall manage re-authentiction identities, Master Key and counter values as described in TS 24.234 [40].

5.7 Network Connectivity Parameters for UICC IP connections related procedures

The EF_{NCP-IP} access procedures are described in ETSI TS 102 483 [50].

Request: The terminal performs the read procedure with EF_{NCP-IP} before establishing a remote data link for UICC remote IP connectivity as described in ETSI TS 102 483 [50].

Refresh: The terminal performs the refresh procedure with EF_{NCP-IP}.

5.8 H(e)NB related procedures

5.8.1 CSG Access Control procedures

Requirement: Service n°86 is "available"

Request: The terminal performs the read procedure with EF_{ACSGL}.

Update: The terminal performs the updating procedure with EF_{ACSGL}

The ME shall read the allowed CSG Ids from EF_{ACSGL} in order to perform H(e)NB selection procedures. The lists in EF_{ACSGL} shall take precedence over the list stored in the ME non-volatile memory.

Requirement: Service n°90 is "available"

Request: The terminal performs the read procedure with with EF_{OCSGL}.

The ME shall read the Operator CSG Ids from EF_{OCSGL} in order to perform H(e)NB selection procedures. The list in EF_{OCSGL} shall take precedence over the list stored in the ME non-volatile memory.

Requirement: Service n°92 is "available"

In case of a manual CSG cell selection, the ME shall read EF_{AD} and CSG Lists Display Indicators from EF_{OCSGL} and display CSG Ids accordingly. The configuration in EF_{OCSGL} shall take precedence over the configuration stored in the ME non-volatile memory.

If service n°92 is not "available", in case of a manual CSG cell selection, all available CSGs may be displayed without any restriction.

5.8.2 CSG Type related procedures

Requirement: Service n°86 is "available"

Request: The terminal performs the read procedure with EF_{ACSGL} and EF_{CSGT}.

Update: The terminal performs the updating procedure with EF_{ACSGL}

The ME shall discover the association between the selected CSG ID and a CSG Type from EF_{ACSGL}. If this association exists, the provided CSG Type shall be displayed.

Requirement: Service n°90 is "available"

Request: The terminal performs the read procedure with EF_{OCSGL} and EF_{OCSGT}.

The ME shall discover the association between the selected CSG ID and either a CSG Type from EF_{ACSGL} or an Operator CSG Type from EF_{OCSGL}. The Operator CSG Type has precedence.

5.8.3 HNB name display related procedures

Requirement: Service n°86 is "available"

Request: The terminal performs the read procedure with EF_{ACSGL} and EF_{HNBN}.

Update: The terminal performs the updating procedure with EF_{ACSGL} and EF_{HNBN}.

The ME shall discover the association between the selected CSG ID and a HNB name from EF_{ACSGL}. If this association exists, the provided HNB name shall be displayed.

Requirement: Service n°90 is "available"

Request: The terminal performs the read procedure with EF_{OCSGL} and EF_{OHNBN}.

The ME shall discover the association between the selected CSG ID and either a HNB Name from EF_{ACSGL} or an Operator HNB from EF_{OCSGL}. The Operator HNB Name has precedence. If this association exists, the HNB Name shall be displayed.

Requirement: Service n°92 is "available"

In case of a manual CSG cell selection, the ME shall read EF_{AD} and the CSG Lists Display Indicators from EF_{OCSGL} and display HNB Name accordingly. The configuration in EF_{OCSGL} shall take precedence over the configuration stored in the ME non-volatile memory.

If service n°92 is not "available", in case of a manual CSG cell selection, all available CSGs may be displayed without any restriction.

6 Security features

The security aspects of 3G are specified in TS 33.102 [13] and TS 33.103 [14]. This clause gives information related to security features supported by the USIM to enable the following:

- authentication of the USIM to the network;
- authentication of the network to the USIM;
- authentication of the user to the USIM;
- data confidentiality over the radio interface;
- file access conditions;
- conversion functions to derive GSM parameters.

6.1 Authentication and key agreement procedure

This clause gives an overview of the authentication mechanism and cipher and integrity key generation which are invoked by the network. For the specification of the corresponding procedures across the USIM/ME interface see clause 5.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition, the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication. SQN_{HE} is a counter in the HLR/AuC, individual for each user and SQN_{MS} denotes the highest sequence number the USIM has ever accepted.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector and sends the parameters RAND and AUTN (authentication token) to the user. Each authentication token consists of the following components: a sequence number SQN, an Authentication Management Field (AMF) and a message authentication code MAC over the RAND, SQN and AMF.

The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed. The USIM also computes CK and IK. The established keys CK and IK will be used by the ME to perform ciphering and integrity functions.

A permanent secret key K is used in this procedure. This key K has a length of 128 bits and is stored within the USIM for use in the algorithms described below. Also more than one secret key K can be stored in the USIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

6.2 Cryptographic Functions

The names and parameters of the cryptographic functions supported by the USIM are defined in TS 33.102 [13]. These are:

f1:	a message authentication function for network authentication used to compute XMAC;
f1*:	a message authentication function for support to re-synchronisation with the property that no valuable information can be inferred from the function values of f1* about those of f1, ..., f5, f5* and vice versa;
f2:	a message authentication function for user authentication used to compute SRES;
f3:	a key generating function to compute the cipher key CK;
f4:	a key generating function to compute the integrity key IK;
f5:	a key generating function to compute the anonymity key AK (optional);

f5*: a key generating function to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of f5* about those of f1, f1*, f2, ..., f5 and vice versa.

These cryptographic functions may exist either discretely or combined within the USIM.

6.3 GSM Conversion Functions

To gain GSM access, the USIM provides the conversion functions c2 and c3. These functions derive the required GSM parameters (SRES, cipher key Kc) from available 3G parameters.

6.4 User verification and file access conditions

The security architecture as defined in TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use a global key reference as PIN and local key reference as PIN2. For access to $DF_{TELECOM}$ the PIN shall be verified. Access with PIN2 is limited to the ADF(USIM).
- The only valid values for the usage qualifier are '00' (verification requirement is not used) and '08' (user authentication knowledge based (PIN)) as defined in ISO/IEC 7816-4 [20].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

7 USIM Commands

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- a 3G security context, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or
- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN)
- a VGCS/VBS security context, when VGCS/VBS authentication data is available
- a GBA_U security context, when a GBA bootstrapping procedure is requested
- a MBMS security context, when a MBMS security procedure is requested
- a Local Key Establishment security context, when a Local Key Establishment procedure is requested.

The function is used in GSM or 3G security context during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is used in VGCS/VBS security context during the procedure for retrieving the VGCS/VBS Short Term Key (VSTK) used by the terminal in establishing VGCS/VBS calls.

The function is used in GBA security context in two different modes:

a) Bootstrapping Mode: during the procedure for mutual authenticating of the USIM and the Bootstrapping Server Function (BSF) and for deriving bootstrapped key material from the AKA run.

b) NAF Derivation Mode: during the procedure for deriving Network Application Function (NAF) specific keys from previous bootstrapped key material.

The function is used in MBMS security context in two different modes:

a) MSK Update Mode: during the procedure for updating an MBMS Service Key (MSK).

b) MTK Generation Mode: during the procedure for retrieving the MBMS Traffic Key (MTK) used by the terminal to decrypt MBMS data.

The function is related to a particular USIM and shall not be executable unless the USIM application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

7.1.1.1 3G security context

The USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Then the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the USIM abandons the function.

Next the USIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in TS 33.102 [13].

NOTE: This implies that the USIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, where:
$AUTS = Conc(SQN_{MS}) \| MACS;$
$Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the USIM; and.
$MACS = f1^*_K(SQN_{MS} \| RAND \| AMF)$ where:
RAND is the random value received in the current user authentication request;
the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HE specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see TS 33.102 [13].

If Service n°27 is "available", the USIM calculates the GSM response parameter K_C, using the conversion function defined in TS 33.102 [13].

Input:

- RAND, AUTN (AUTN:= SQN ⊕ AK || AMF || MAC).

Output:

- RES, CK, IK if Service n°27 is "not available".

Or

- RES, CK, IK, K_C if Service n°27 is "available".

Or

- AUTS.

7.1.1.2 GSM security context

USIM operation in an GSM security context is supported if Service n°38 is "available".

The USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Next the USIM calculates the GSM response parameters SRES and K_C, using the conversion functions defined in TS 33.102 [13].

Input:

- RAND.

Output:

- SRES; K_C.

7.1.1.3 VGCS/VBS security context

USIM operation in a VGCS/VBS security context is supported if both Service n°57 and Service n°64 are “available” (VGCS security context) or if both Service n°58 and Service n°65 are "available" (VBS security context).

The USIM computes the Short Term Key (VSTK) associated with a particular VGCS/VBS Group Identifier (Group_Id). For this computation, the USIM uses the Voice Group (for VGCS) or Broadcast Group (for VBS) Key (V_Ki) identified by their respective Group_Id and Master Group Key Identifier (VK_Id). The USIM retrieves the Group_Id and the service flag (VGCS or VBS) from the received Voice Service Identifier (Vservice_Id).

NOTE: The Group_Id has a variable length according to TS 43.068 [46].

The USIM shall first search if the Group_Id corresponds to a stored VGCS Group Identifier in EF_{VGCS} or a stored VBS Group Identifier in EF_{VBS}.

Then, the USIM shall retrieve the V_Ki corresponding to the given Group_Id and VK_Id.

Then the USIM uses V_Ki and VSTK_RAND as input parameters for the A8_V key derivation function (as defined in TS 43.020 [44]) in order to compute and returns VSTK.

Input:

- Vservice_Id, VK_Id, VSTK_RAND

Output:

- VSTK.

7.1.1.4 GBA security context (Bootstrapping Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the RAND and AUTN*. The USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN $\oplus$ AK) $\oplus$ AK.

The USIM calculates IK = $f4_K$ (RAND) and MAC (by performing the MAC modification function described in TS 33.220 [42]). Then the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC previously produced. If they are different, the USIM abandons the function.

Then the USIM performs the checking of AUTN* as in UMTS security context. If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, which is computed as in UMTS security context.

If the sequence number is considered in the correct range, the USIM computes RES = $f2_K$ (RAND) and the cipher key CK = $f3_K$ (RAND).

The USIM then derives and stores GBA_U bootstrapped key material from CK, IK values. The USIM shall also stores RAND in the RAND field of EF_{GBABP}

The USIM stores GBA_U bootstrapped key material from only one bootstrapping procedure. The previous bootstrapped key material, if present, shall be replaced by the new one. This key material is linked with the data contained in EF_{GBABP} : RAND, which is updated by the USIM and B-TID, which shall be further updated by the ME.

NOTE: According to TS 33.220 [42], NAF-specific keys that may be stored on the USIM are not affected by this bootstrapping operation.

RES is included in the command response after flipping the least significant bit.

Input:

- RAND, AUTN*

Output:

- RES

or

- AUTS

7.1.1.5 GBA security context (NAF Derivation Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the NAF_ID and IMPI.

The USIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [42] using the key material from the previous GBA_U bootstrapping procedure.

If no key material is available this is considered as a GBA Bootstrapping failure and the USIM abandons the function. The status word ‘6985’ (Conditions of use not satisfied) is returned.

Otherwise, the USIM stores Ks_int_NAF and associated B-TID together with NAF_ID. The Ks_int_NAF keys related to other NAF_Ids, which are already stored in the USIM, shall not be affected. The USIM updates EF_{GBANL} as follows:

- If a record with the given NAF_ID already exists, the USIM updates the B-TID field of this record with the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF derivation procedure.
- If a record with the given NAF_ID does not exist, the USIM uses an empty record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure.

NOTE: According to TS 33.220 [42], the USIM can contain several Ks_int_NAF together with the associated B-TID and NAF_ID, but there is at most one pair of Ks_int_NAF and associated B-TID stored per NAF_ID.

- In case no empty record is available the USIM shall overwrite an existing record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure. To determine the record to overwrite, the USIM shall construct a list of record numbers by storing in the list first position the record number of the last used (i.e. involved in an Authentication command) or derived Ks_int_NAF and by shifting down the remaining list elements. The last record number in this list corresponds to the record to overwrite when the USIM runs out of free records. If an existing record corresponding to a Ks_int_NAF key in use is overwritten, the application Ks_int_NAF shall not be affected (e.g. in case a Ks_int_NAF was put into use as an MBMS MUK key, the MUK key shall continue to be available for the MBMS application).

Then, the USIM returns Ks_ext_NAF.

Input:

- NAF_ID, IMPI

Output:

- Ks_ext_NAF

7.1.1.6 MBMS security context (MSK Update Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the MIKEY packet containing an MSK update message. First, the USIM uses the MUK ID to identify the Ks_int_NAF corresponding with a previous bootstrapping procedure.

The USIM shall check if a new NAF derivation procedure involving the received Idi in the MIKEY message has been performed or if it is the first time that this Idi is used. If this check cannot be performed because the corresponding Ks_int_NAF key was overwritten, the USIM abandons the function and returns the status word '6985' (Conditions of use not satisfied). In case of a new NAF derivation procedure or a new Idi, the USIM shall store the last bootstrapped Ks_int_NAF as the last generated MUK and update EF_{MUK} as follows:

- If a record with the received Idi (included in the MUK ID: see TS 33.246 [43]) value is already present, then the MUK ID is stored in the corresponding field of this record, and the associated Time Stamp Counter (TS) field is reset. Additionally, the USIM internally stores the last successfully used MUK (i.e. MUK that was used during the last successful MSK update procedure), along with its MUK ID for further use (e.g. to detect Key freshness failure).

- If a record with the received Idi does not exist, the USIM uses an empty record to include the MUK ID, and reset the associated TS field.

- In case there is no empty record available in EF_{MUK} the USIM abandons the function and the status word '9867' (Authentication error, no available memory space in EF_{MUK}) is returned.

NOTE: In case no empty record in EF_{MUK} is available the ME should run a MUK Deletion Mode procedure to free entries in EF_{MUK} before running an MSK Update Mode procedure that involves a new MUK key.

NOTE: In case the ME receives the status word '6985', the ME should derive the required Ks_int_NAF key. In case the corresponding bootstrapping key Ks is still available, the ME should invoke the Authenticate command in "GBA - NAF derivation Mode" before invoking again the AUTHENTICATE command in "MBMS - MSK Update Mode". In case the corresponding bootstrapping key has been updated, the ME should put the new B-TID into use.

If the received MUK ID does not correspond to the last generated MUK (i.e. last bootstrapped MUK) then the USIM proceeds as follows:

- If the received MUK ID corresponds to the last successfully used MUK then the USIM uses this MUK to verify the integrity of the message. If the verification is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC). If the verification is successful, the USIM abandons the function and returns the status word '9865' (Key Freshness Failure), indicating to the ME that the received MIKEY message is protected using the last successfully used MUK that does not correspond to the last generated MUK (the new B-TID shall be put into use: see TS 33.246 [43]). In this case, the USIM shall not return a MIKEY verification message.

- Otherwise, this is considered as a bootstrapping failure (incorrect MUK) and the USIM abandons the function. The status word ‘6A88’ (Referenced data not found) is returned.

Otherwise, if the received MUK ID corresponds to the last generated MUK, the USIM uses the MUK value for MSK validation and derivation functions as described in TS 33.246 [43]. If the validation is unsuccessful, the status word '9862' (Authentication error, incorrect MAC) is returned and the USIM abandons the function.

After a successful MSK Update procedure the USIM stores the received credentials (e.g. MSK and/or Key Validity data) and updates EF_{MSK} as follows:

- If a record with the received Key Domain ID and Key Group part (i.e. Key Group part of the MSK ID) already exists, USIM stores the older MSK ID (if any) and its associated TS as the 2nd MSK ID and TS. The newer MSK ID is stored as the 1st MSK ID. In case the received MSK message has the same MSK ID as a stored MSK, the TS associated to this stored MSK is stored as the 1st TS. Otherwise, the 1st TS value is reset. The number of stored MSK IDs and corresponding TS shall be set to '02' if the USIM stores two different MSK IDs. The USIM shall not store two MSK IDs with the same Key Number part in the same record.

- If a record with the received Key Domain ID and Key Group part does not exist, the USIM uses an empty record to include those values. The received MSK ID is stored as the 1st MSK ID and the associated TS is reset. The 2nd MSK ID and the associated TS are set to 'FF FF'. The number of stored MSK IDs and corresponding TS shall be

set to '01'. In case there is no empty record available in EF_{MSK} the USIM abandons the function and the status word '9866' (Authentication error, no available memory space) is returned.

- In the case of a BM-SC solicited pull procedure (i.e. when the Key Number part of the MSK ID is set to 0x0), EF_{MSK} is not updated.

NOTE: In case no empty record is available the ME should run an MSK Deletion Mode procedure to free entries in EF_{MSK} before running an MSK Update Mode procedure that contains a new MSK key.

Then, the USIM stores the Time Stamp field (retrieved from the MIKEY message) in its corresponding field under EF_{MUK}.

The USIM stores internally the last successfully used MUK along with its MUK ID for further use. This MUK may be used beyond its GBA validity (i.e. after the derivation of a new Ks_int_NAF resulting from a new bootstrap procedure) to verify the integrity of a MIKEY message in order to detect a synchronization failure. This may occur if the last derived Ks_int_NAF did not reach the BM-SC.

The MSK is not necessarily updated in the MIKEY message, since a MSK transport message can be sent e.g. to update the Key Validity data or as part of a BM-SC solicited pull procedure. In such a case the USIM shall use the status word '9000' to inform the ME that the MIKEY message validation using the last generated MUK has succeeded.

Finally, if the V-bit in the HDR field of the received MIKEY message is set then the USIM shall produce a MSK Verification Message as described in TS 33.246 [43]. In this case the command response is the MIKEY verification message.

Input:

- MIKEY message

Output:

- MIKEY message

or

- None

7.1.1.7 Void

7.1.1.8 MBMS security context (MTK Generation Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the MIKEY message containing an MBMS MTK and a Salt key (if Salt key is available). First, the USIM retrieves the MSK with the Key Domain ID and the MSK ID given by the Extension payload of the MIKEY message (as described in TS 33.246 [43]).

If the needed MSK does not exist, this is considered as a MSK failure and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

If the key validity data of the MSK indicates an invalidated MSK (i.e. SEQl is greater than SEQu) then the USIM returns the status word '6985' (Conditions of use not satisfied) and abandons the function. SEQl and SEQu are defined in TS 33.246 [43].

Otherwise, the USIM performs the MBMS Generation and Validation Function (MGV-F) as described in TS 33.246 [43] using MSK.

If the USIM detects that the given MTK ID is invalid, this is considered as a SEQp freshness failure and the USIM abandons the function. The status word '9865' (Key freshness failure) is returned.

If the integrity validation of the MIKEY message is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC).

After successful MGV_F procedure the USIM stores the Time Stamp field (retrieved from the MIKEY message) as the Time Stamp Counter (TS) associated with the involved MSK under EF_{MSK}

The USIM also stores MTK ID (retrieved from the MIKEY message) as the SEQl associated with MSK.

Then, the USIM returns MTK and Salt key (if Salt key is available).

Input:

- MIKEY message

Output:

- MTK and Salt (if available).

7.1.1.9 MBMS security context (MSK Deletion Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the Key Domain ID and the Key Group part of the MSK ID. The USIM shall identify in the EF_{MSK} the record containing MSK IDs having this Key Domain ID and Key Group part.

If no record is identified, the USIM abandons the function and returns the status word '6A88' (Referenced data not found).

If a record is found, the USIM shall delete all corresponding MSKs and set to 'FF' the bytes of this record.

Input:

- Key Domain ID, MSK ID Key Group part

Output:

- None.

7.1.1.10 MBMS security context (MUK Deletion Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM shall identify in EF_{MUK} the record containing the received MUK ID.

If no record is identified, the USIM abandons the function and returns the status word '6A88' (Referenced data not found).

If a record is found, the USIM shall delete the corresponding MUK and set to 'FF' the bytes of this record. If a corresponding Ks_int_NAF key is present (i.e. with the same NAF_ID), it shall be deleted and its corresponding record in EF_{GBANL} shall be set to 'FF'. In case the corresponding Ks key is present (i.e. with the same B-TID), it shall be deleted and the content of EF_{GBABP} shall be set to 'FF'.

Input:

MUK ID TLV

Output:

- None

7.1.1.11 Local Key Establishment security context (Key Derivation mode)

USIM operations in this security context are supported if service n°68 and service n°76 are "available".

The USIM receives the NAF_ID corresponding to the NAF Key Centre, the Terminal_ID, the Terminal_appli_ID, the UICC_appli_ID, RANDx, the Counter Limit value and the MAC as described in TS 33.110 [47].

The USIM uses the NAF_ID to identify the Ks_int_NAF associated to the NAF Key Centre. If no valid Ks_int_NAF is available, this is considered as a Key Establishment failure and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

If the Ks_local key derivation is not authorized by the local UICC policy (e.g. Terminal_appli_ID/UICC_appli_ID association not authorized or Terminal_ID value not authorized), the USIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the USIM retrieves the appropriate Ks_int_NAF, derives Ks_local as described in TS 33.110 [47]. The USIM verifies the MAC value received from the Terminal as described in TS 33.110 [47]:

- If the verification is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC).
- If the verification is successful, the USIM stores Ks_local and associated parameters Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx and the Ks_local Counter Limit. The USIM returns the Local Key Establishment Operation Response TLV (indicating a successful Key Derivation operation) and a response MAC, which is derived as described in TS 33.110 [47].

The minimum number of Local keys that can be stored by the USIM shall be defined by the service provider at the pre-issuance of the card.

In case the maximum number of Local Key was already reached or there is not enough available memory in the USIM, the USIM shall overwrite a Local Key and its associated data in order to store the new one. To determine the Ks_local to overwrite, the USIM shall construct a list of Ks_local identifiers by storing in the list first position the Ks_local identifier of the last used or derived Ks_local and by shifting down the remaining list elements. The last Ks_local identifier in this list corresponds to the Ks_local to overwrite when the USIM runs out of free memory or when the maximum number of Ks_local keys is reached. If an existing Ks_local in use is overwritten, the application using Ks_local shall not be affected.

Input:

- Local Key Establishment Mode (Key Derivation mode), Counter Limit, request MAC, Key Identifier (i.e. NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx)

Output:

- Key Derivation operation status, response MAC.

7.1.1.12 Local Key Establishment security context (Key Availability Check mode)

USIM operations in this security context are supported if service n°68 and service n°76 are "available".

The USIM receives a Ks_local identifier. The USIM checks if a corresponding valid Ks_local is available. If a valid Ks_local key is available the Local Key Establishment Operation Response TLV (indicating a successful Key Availability Check operation) is returned. In case no valid Ks_local key is available the command fails and the status word '6A88' (Referenced data not found) is returned.

Input:

Local Key Establishment Mode (Key Availability Check mode), Key identifier (i.e. NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx).

Output:

- Key Availability Check Operation Status.

7.1.2 Command parameters and data

This command can be used with an EVEN or an ODD instruction (INS) code. The EVEN instruction code can be used when the challenge data provided by the terminal is not TLV encapsulated data and the length of the challenge data provided by the terminal is less than 256 bytes.

The ODD instruction code shall be used with the security context specified in table 2, when challenge and response data is TLV encapsulated regardless of their length. Terminals and UICCs that do not support security context requiring TLV format (e.g. MBMS), do not have to support AUTHENTICATE command with ODD instruction code.

EVEN INS code

Code	Value
CLA	As specified in TS 31.101 [11]
INS	'88'
P1	'00'
P2	See table 1 below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Table 1: Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'----- XXX'	Authentication context: 000 GSM context 001 3G context 010 VGCS/VBS context 100 GBA context

All other codings are RFU.

ODD INS code

The authentication data and the authentication response data are encapsulated in BER-TLV objects structured using tag '73' for BER-TLV structured data and tag '53' otherwise.

How this command can chain successive blocks of authentication data, or authentication response data is described in TS 31 101 [11].

If P1 indicates "First block of authentication data" or "Next block of authentication data":

Input:

- Authentication data encapsulated in a BER-TLV data object.

Output:

- None.

Code	Value
CLA	As specified in TS 31.101 [11]
INS	'89'
P1	As specified in TS 31.101 [11]
P2	See table 2 below
Lc	Length of the subsequent data field
Data	Authentication related data
Le	Not present

If P1 indicates "First block of authentication response data" or "Next block of authentication response data":

Input:

- None.

Output:

- Authentication response data encapsulated in a BER-TLV data object.

Code	Value
CLA	As specified in TS 31.101 [11]
INS	'89'
P1	As specified in TS 31.101 [11]
P2	See table 2 below
Lc	Not present
Data	Not present
Le	Length of the response data

Parameter P1 is used to control the data exchange between the terminal and the UICC as defined in TS 31.101 [11].

Parameter P2 specifies the authentication context as follows:

Table 2: Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'----- XXX'	Authentication context: 101 MBMS context 110 Local Key Establishment mode

All other codings are RFU.

Command parameters/data:

7.1.2.1 GSM/3G security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (see note)	1
(L1+3) to (L1+L2+2)	AUTN (see note)	L2
Note: Parameter present if and only if in 3G security context.		

The coding of AUTN is described in TS 33.102 [13]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, 3G security context, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5
(L3+L4+L5+5)	Length of K_C (= 8) (see note)	1
(L3+L4+L5+6 to (L3+L4+L5+13)	K_C (see note)	8
Note: Parameter present if and only if Service n°27 is "available".		

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, 3G security context, synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [13]. The most significant bit of AUTS is coded on bit 8 of byte 3.

Response parameters/data, case 3, GSM security context, command successful:

Byte(s)	Description	Length
1	Length of SRES (= 4)	1
2 to 5	SRES	4
6	Length of K_C (= 8)	1
7 to 14	K_C	8

The most significant bit of SRES is coded on bit 8 of byte 2. The most significant bit of Kc is coded on bit 8 of byte 7.

7.1.2.2 VGCS/VBS security context

Byte(s)	Description	Length
1	Length of Vservice_Id	1
2 to 5	Vservice_Id	4
6	Length of VK_Id	1
7	VK_Id	1
8	Length of VSTK_RAND (L1)	1
9 to L1+8	VSTK_RAND	L1

Vservice_Id is coded in the same way as the octets 2-5 in the Descriptive group or broadcast call reference information element as defined in TS 24.008 [9].

An Example for the coding of Vservice_Id can be found in Annex K.

The coding of VK_Id is as follows:

Coding of VK_Id

Coding b8-b1	Meaning
'00000001'	Corresponds to the 1st group key
'00000010'	Corresponds to the 2nd group key

The coding of VSTK_RAND is described in TS 43.020 [44]. The VSTK_RAND shall be inserted left-aligned into the L1 bytes, with unused bits to the right set to zero.

Response parameters/data, VGCS/VBS security context, command successful:

Byte(s)	Description	Length
1	"Successful VGCS/VBS operation" tag = 'DB'	1
2	Length of VSTK (16)	1
3 to 18	VSTK	16

7.1.2.3 GBA security context (Bootstrapping Mode)

Byte(s)	Description	Length
1	“GBA Security Context Bootstrapping Mode” tag = ‘DD’	1
2	Length of RAND (L1)	1
3 to (L1+2)	RAND	L1
(L1+3)	Length of AUTN (L2)	1
(L1+4) to (L1+L2+3)	AUTN	L2

Response parameters/data, GBA security context (Bootstrapping Mode), synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

AUTS coded as for UMTS Security context.

Response parameters/data, GBA security context (Bootstrapping Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of RES (L)	1
3 to (L+2)	RES	L

RES coded as for UMTS Security context.

7.1.2.4 GBA security context (NAF Derivation Mode)

Byte(s)	Description	Length
1	“GBA Security Context NAF Derivation Mode” tag = ‘DE’	1
2	Length of NAF_ID (L1)	1
3 to (L1+2)	NAF_ID	L1
(L1+3)	Length of IMPI (L2)	1
(L1+4) to (L1+L2+3)	IMPI	L2

Response parameters/data, GBA security context (NAF Derivation Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of Ks_ext_NAF (L)	1
3 to (L+2)	Ks_ext_NAF	L

Coding of Ks_ext_NAF as described in TS 33.220 [42].

7.1.2.5 MBMS security context (All Modes)

Byte(s)	Description	Coding	Length
1	MBMS Data Object tag (‘53’)	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to 1+A bytes (A ≤ 4)	MBMS Data Object length (L1)	As defined in TS 31.101 [11] for BER-TLV data object	A
A+2	MBMS Security Context Mode	See below	1
A+3 to (A+L1+1)	MIKEY message or Key Domain ID || MSK ID Key Group part or MUK ID TLV		L1-1

Only the MIKEY message shall be transmitted in the MBMS security context mode '01' or '02'.

Only the Key Domain ID (coded on 3 bytes as described in TS 33.246 [43]) concatenated with the Key Group part of the MSK ID (coded on two bytes as described in TS 33.246 [43] where the last transmitted byte represents the least significant byte of the Key Group part) shall be transmitted in the MBMS security context mode '03'.

Only the MUK ID TLV shall be transmitted in the MBMS security context mode '04'. The MUK ID TLV, containing the MUK Idr and MUK Idi only, shall be encoded as described in clause 4.2.81.

Parameter MBMS Security Context Mode specifies the MBMS mode in which MBMS security procedure is performed as follows:

Coding of MBMS Security Context Mode

Coding	Meaning
'01'	MSK Update Mode
'02'	MTK Generation Mode
'03'	MSK Deletion Mode
'04'	MUK Deletion Mode

Response parameters/data, MBMS security context (MSK Update Mode), command successful:

Byte(s)	Description	Coding	Length
1	MBMS operation response Data Object tag ('53')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to 1+A bytes (A ≤ 4)	MBMS operation response Data Object length (L)	As defined in TS 31.101 [11] for BER-TLV data object	A
A+2	"Successful MBMS operation" tag = 'DB' (see note 1)		1
A+3 to (A+L+1)	MIKEY message (see note 1)		L-1
NOTE 1: Parameter present if a MIKEY verification message is returned. Otherwise, the USIM returns "53 01 DB"			

Response parameters/data, MBMS security context (MTK Generation Mode), command successful:

Byte(s)	Description	Coding	Length
1	MBMS operation response Data Object tag ('53')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to 1+A bytes (A ≤ 4)	MBMS operation response Data Object length (L)	As defined in TS 31.101 [11] for BER-TLV data object	A
A+2	"Successful MBMS operation" tag = 'DB'		1
A+3 to (A+L+1)	MTK || Salt (if Salt key is available)		L-1

Response parameters/data, MBMS security context (MSK and MUK Deletion Mode), command successful:

Byte(s)	Description	Coding	Length
1	MBMS operation response Data Object tag ('53')	As defined in TS 31.101 [11] for BER-TLV data object	1
2	MBMS operation response Data Object length	As defined in TS 31.101 [11] for BER-TLV data object	1
3	"Successful MBMS operation" tag = 'DB'		1

The coding of parameters is described in TS 33.246 [43].

Note: The constructed TLV tag value 'AE' is used by OMA BCAST Smart Card Profile [49] for the encapsulation of command and response parameters/data.

7.1.2.6 Local Key Establishment security context (All Modes)

The Local Key Establishment Control TLV is included in the command data to indicate the security context mode. The Local Key Establishment Control TLV is also included in the response data to indicate the operation status.

Table 3: Coding of the Local Key Establishment Control TLV

Tag Value	Length	Value / Meaning
'80'	Coded according to ISO/IEC 8825-1 [35]	Local Key Establishment context: '01': Key Derivation mode '02': Key Availability Check mode Operation Status: 'DB': Successful Operation

7.1.2.6.1 Local Key Establishment security context (Key Derivation mode)

Command parameters/data:

Byte(s)	Description	Coding	Length
1	Key Derivation Data Object tag ('73')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to A+1 bytes (A ≤ 4)	Key Derivation Data Object length (L)	As defined in TS 31.101 [11] for BER-TLV data object	A
A+2 to (A+L+1)	Key Derivation Data Object		L

- Key Derivation Data Object content: The TLVs defined in table 4 are included in the Key Derivation Data Object.

Table 4: Coding of the Key Derivation Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in section 7.1.2.6. The value field shall be set to '01'	M	B
Counter Limit tag	'81'	M	1
Length	C	M	Note 1
Counter Limit	Coded as defined in TS 33.110 [47]	M	C
Request MAC tag	'82'	M	1
Length	D	M	Note 1
Request MAC	Coded as defined in TS 33.110 [47]	M	D (see Note 3)
Key Identifier tag	'A0'	M	1
Length	E (see Note 2)	M	Note 1
NAF_ID tag	'83'	M	1
Length	F	M	Note 1
NAF_ID	Coded as defined in TS 33.220 [42]	M	F
Terminal_ID tag	'84'	M	1
Length	G	M	Note 1
Terminal_ID	Coded as defined in TS 33.110 [47]	M	G
Terminal_appli_ID tag	'85'	M	1
Length	H	M	Note 1
Terminal_appli_ID	Coded as defined in TS 33.110 [47]	M	H
UICC_appli_ID tag	'86'	M	1
Length	I	M	Note 1
UICC_appli_ID	Coded as defined in TS 33.110 [47]	M	I
RANDx tag	'87'	M	1
Length	J	M	Note 1
RANDx	Coded as defined in TS 33.110 [47]	M	J (see Note 4)

Note 1: The length is coded according to ISO/IEC 8825-1 [35].
Note 2: The Key Identifier TLV is a constructed TLV containing the following primitive TLVs: NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID and RANDx. E is the length of the constructed Key Identifier value.
Note 3: The most significant bit of the request MAC is coded on bit 8 of the first byte following the MAC Length.
Note 4: The most significant bit of the RANDx is coded on bit 8 of the first byte following the RANDx Length.

Response parameters/data, Local Key Establishment security context (Key Derivation mode), command successful:

Byte(s)	Description	Coding	Length
1	Key Derivation Operation Response Data Object tag ('73')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to A1+1 bytes (A1 ≤ 4)	Key Derivation Operation Response Data Object length (L1)	As defined in TS 31.101 [11] for BER-TLV data object	A1
A1+2 to (A1+L1+1)	Key Derivation Operation Response Data Object		L1

Key Derivation Operation Response Data Object content: The TLVs defined in table 5 are included in the Key Derivation Operation Response Data Object.

Table 5: Coding of the Key Derivation Operation Response Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in section 7.1.2.6. The value field shall be set to 'DB'	M	B
Response MAC tag	'82'	M	1
Length	C	M	Note 1
Response MAC	Coded as defined in TS 33.110 [47]	M	C (see Note 2)
Note 1: The length is coded according to ISO/IEC 8825-1 [35]. Note 2: The most significant bit of the response MAC is coded on bit 8 of the first byte following the MAC length.			

7.1.2.6.2 Local Key Establishment security context (Key Availability Check mode)

Command parameters/data:

Byte(s)	Description	Coding	Length
1	Key Availability Check Data Object tag ('73')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to 1+A bytes (A ≤ 4)	Key Availability Check Data Object length (L)	As defined in TS 31.101 [11] for BER-TLV data object	A
A+2 to (A+L+1)	Key Availability Check Data Object		L

- Key Availability Check Data Object content: The TLVs defined in table 6 are included in the Key Availability Check Data Object.

Table 6: Coding of the Key Availability Check Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in section 7.1.2.6. The value field shall be set to '02'	M	B
Key Identifier TLV	Coded as defined in section 7.1.2.6.1	M	C

Response parameters/data, Local Key Establishment security context (Key Availability Check mode), command successful:

Byte(s)	Description	Coding	Length
1	Key Availability Check Operation Response Data Object tag ('73')	As defined in TS 31.101 [11] for BER-TLV data object	1
2 to 1+A1 bytes (A1 ≤ 4)	Key Availability Check Operation Response Data Object length (L1)	As defined in TS 31.101 [11] for BER-TLV data object	A1
A1+2 to (A1+L1+1)	Key Availability Check Operation Response Data Object		L1

- Key Availability Check Operation Response Data Object content: The TLV defined in table 7 is included in the Key Availability Check Operation Response Data Object.

Table 7: Coding of the Key Availability Check Operation Response Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in section 7.1.2.6. The value field shall be set to 'DB'	M	B

7.2 Void

7.3 Status Conditions Returned by the USIM

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This clause specifies the coding of the status bytes in the following tables, in addition to the ones defined in TS 31.101 [11].

7.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC
'98'	'64'	- Authentication error, security context not supported
'98'	'65'	- Key freshness failure
'98'	'66'	- Authentication error, no memory space available
'98'	'67'	- Authentication error, no memory space available in EF_{MUK}

7.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
98 65	*
98 66	*
98 67	*
62 00	*
62 81	
62 82	
62 83	
62 F1	*
62 F3	*
63 CX	
63 F1	*
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

7.4 Optional commands

The following command is optional for the USIM application:

- GET CHALLENGE command as defined in TS 31.101 [11].

Note: OMA BCAST Smart Card Profile [49] defines a command using instruction code INS '1B'

8 Void

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

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a USAT Application, is advisable. Updating of certain Efs "over the air" such as EF_{ACC} could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain Efs are marked "No"; under no circumstances should "over the air" changes of these Efs be considered.

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'4F01'	Launch SCWS	Yes
'4F20'	Image data	Yes
‘4F20’	GSM Ciphering key Kc	No
'4FXX'	Image Instance data Files	Yes
'4F21'	ICE graphics	Yes
'4FXX'	Icon	Yes
'4FXX'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4FXX'	Capability configuration parameters 1	Yes
'4F30'	SoLSA Access Indicator	Caution
'4F31'	SoLSA LSA List	Caution
'4FXX'	LSA Descriptor files	Caution
‘4F52’	GPRS Ciphring key KcGPRS	No
'4F63'	CPBCCH Information	No
'4F64’	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'4F41'	Pseudonym	Caution
'4F42'	User controlled PLMN selector for I-WLAN	No
'4F43'	Operator controlled PLMN selector for I-WLAN	Caution
'4F44'	User controlled WSID List	No
'4F45'	Operator controlled WSID List	Caution
'4F46'	WLAN Reauthentication Identity	No
4F47'	Home I-WLAN Specific Identifier List	Yes
'4F47'	Multimedia Messages List	Yes
'4F48'	I-WLAN Equivalent HPLMN Presentation Indication	Yes
'4F48'	Multimedia Messages Data File	Yes
'4F49'	I-WLAN HPLMN Priority Indication	Yes
'4F4A'	I-WLAN Last Registered PLMN	Caution
'4F4B'	HPLMN Direct Access Indicator	Yes
'4F81'	Allowed CSG lists	Yes
'4F82'	CSG Type	Yes
'4F83'	HNB name	Yes
'4F84'	Operator CSG lists	Yes
'4F85'	Operator CSG Type	Yes
'4F86'	Operator HNB name	Yes

File identification	Description	Change advised
'6F05'	Language indication	Yes
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Caution
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes (Note 2)
'6F3C'	Short messages	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes (Note 2)
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F54'	SetUp Menu Elements	Yes
'6F55'	Extension 4	Yes
'6F56'	Enabled services table	Caution
'6F57'	Access point name control list	Yes
'6F58'	Comparison method information	Yes
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F73'	Packet switched location information	Caution (Note 1)
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC3'	Key for hidden phone book entries	No
'6FC4'	Network Parameters	No
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator Network List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes

File identification	Description	Change advised
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
'6FCE'	MMS Notification	Yes
'6FCF'	Extension 8	Yes
'6FD0'	MMS Issuer Connectivity Parameters	Yes
'6FD1'	MMS User Preferences	Yes
'6FD2'	MMS User Connectivity Parameters	Yes
'6FD3'	Network's indication of alerting (NIA)	Caution
'6FD4'	Voice Group Call Service Ciphering Algorithm	Yes
'6FD5'	Voice Broadcast Service Ciphering Algorithm	Yes
'6FD6'	GBA Bootstrapping parameters	Caution
'6FD7'	MBMS Service Keys List	Caution
'6FD8'	MBMS User Key	Caution
'6FD9'	EHPLMN	Caution
'6FDA'	GBA NAF List	Caution
'6FDB'	EHPLMN Presentation Indication	Caution
'6FDC'	Last RPLMN Selection Indication	Caution
'6FDD'	NAF Key Centre Address	Caution
'6FDE'	Service Provider Name Icon	Yes
'6FDF'	PLMN Network Name Icon	Yes
'6FE0'	In Case of Emergency – Dialling Number	Yes
'6FE1'	In Case of Emergency – Free Format	Yes
'6FE2'	Network Connectivity Parameters for UICC IP connections	Yes
'6FE3'	EPS location information	Caution (Note 1)
'6FE4'	EPS NAS Security Context	Caution
'6FE5'	Public Service Identity of the SM-SC	Yes
'6FE6'	USAT Facility Control	Caution
'6FE7'	UICC IARI	Caution (Note 3)
'6FE8'	Non Access Stratum Configuration	Yes
'6FE9'	UICC certificate	Yes
'6FEA'	Relay Node ID	Yes
'6FEB'	Max value of Secure Channel counter	Caution
'6FEC'	Public Warning System	Yes

NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI}, EF_{PSLOCI} and $EF_{EPSLOCI}$ accordingly.

NOTE2: This file may contain eCALL related test and reconfiguration numbers.

NOTE3: If $EF_{UICCIARI}$ is changed, the UICC shall issue a REFRESH command as defined in TS 31.111. The ME shall read the updated list of IARIs associated with active applications installed on the UICC.

Annex B (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.

1	x
(x * (y-1) + 1)	(x * y)

B.1 Basic Image Coding Scheme

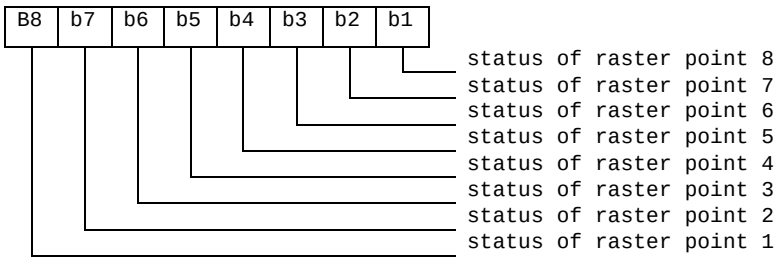
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

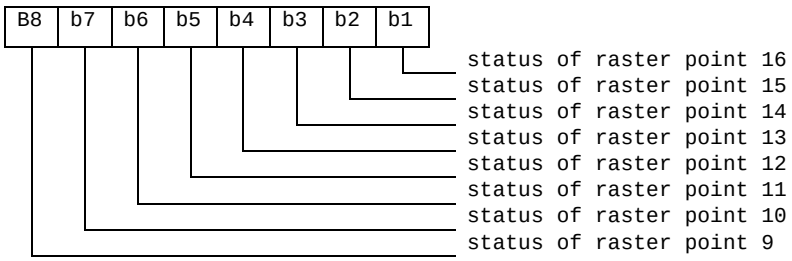
Coding of image body:

- The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:



etc.

Unused bits shall be set to 1.

B.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

Bits per raster image point:

Contents:
- the number B of bits used to encode references into the CLUT, thus defining a raster image point's colour. B shall have a value between 1 and 8.

Coding:
- binary.

Number of entries in CLUT:
Contents:
- the number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1. C shall have a value between 1 and 2**B.

Coding:
- binary. The value 0 shall be interpreted as 256.

Location of CLUT:

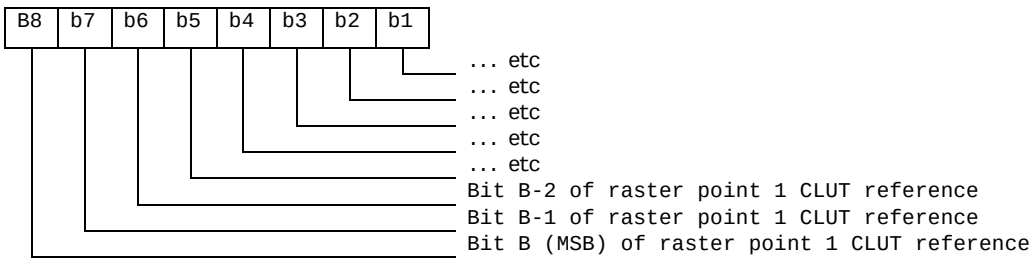
Contents:
- this item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

Coding:
- Byte 1: high byte of offset into Image Instance File.
- Byte 2: low byte of offset into Image Instance File.

Image body:

Coding:
- each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour. The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:



etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:
- C CLUT entries defining one colour each.

Coding:
- the C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
3*(C-1) +1 to 3*C	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT entry	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

B.3 Colour Image Coding Scheme with Transparency

This coding scheme is identical to the Colour Image Coding Scheme as defined in appendix B.2, with the following exception:

- Entry number C-1in the colour look-up table (CLUT), where C is the number of entries in the CLUT, defines transparency. Raster image points which point to this entry are transparent, so that the underlying colour in the display is shown.

The three colour-coding bytes of entry number C-1 in the CLUT are of no importance when referenced from images using the '22' coding scheme.

NOTE: Two different descriptors in the EF_{IMG} file with Image Coding Scheme '21' and '22' may point to the same actual image instance. In that case, the descriptor with Image Coding Scheme '21' would describe an image where a raster image point pointing to entry number C-1 in the CLUT would have the colour described in that CLUT entry, while the descriptor with Image Coding Scheme '22' would describe an image where a raster image point pointing to entry number C-1 in the CLUT is transparent.

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

Structure of the GSM network parameter TLV object, 0<= m <=32

Tag	Length	Tag Currently Camped Frequency	Length	BCCH Frequency downlink		Tag Neighbour BCCH Frequency	Length	BCCH Neighbour Frequency 1		BCCH Neighbour Frequency 2		……		BCCH Neighbour Frequency m	
'A0'		'80'	'02'			'81'									

Structure of the FDD network parameter TLV object, 0 <= m <= 32

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier		Primary Scrambling code 1		Primary Scrambling code m		Tag Inter frequency carrier	Length	Inter Frequency downlink carrier		Primary Scrambling code n1	
'A1'		'80'								'81'					

Structure of the TDD network parameter TLV object, 0 <= m <= 32

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier		Primary Scrambling code 1		Primary Scrambling code m		Tag Inter frequency carrier	Length	Inter Frequency downlink carrier		Primary Scrambling code n1	
'A2'		'80'								'81'					

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'53'	MBMS Data Object	AUTHENTICATE command parameter, in MBMS security context
'53'	MBMS operation response Data Object The following tags are encapsulated within '53' 'DB' successful MBMS operation tag	Response to AUTHENTICATE command, in MBMS security context
'73'	Key Derivation Data Object The following tags are encapsulated within '73' '80' Local Key Establishment Control tag '81' Counter limit tag '82' Request MAC tag '83' NAF_ID tag '84' Terminal_ID tag '85' Terminal_appli_ID_tag '86' UICC_appli_ID tag '87' RANDx tag 'A0' Key Identifier tag	AUTHENTICATE command parameter, in Local Key Establishment security context
'73'	Key Derivation Operation Response Object The following tags are encapsulated within '73' '80' Local Key Establishment Control tag '82' Request MAC tag	Response to AUTHENTICATE command, in Local Key Establishment security context
'73'	Key Availability Check Data Object The following tags are encapsulated within '73' '80' Local Key Establishment Control tag 'A0' Key Identifier tag	AUTHENTICATE command parameter in Local Key Establishment security context
'80'	NAF_ID tag	GBA NAF List (EF_{GBANL})
'80'	NAF Key Centre address tag	NAF Key Centre Address (EF_{NAFKCA})
'80'	Icon Tag (Icon link is URI)	Service Provider Name Icon (EF_{SPNI})
'80'	Reauthentication Identity tag	WLAN Reauthentication Identity (EF_{WRI})
'80'	Graphics CSG Type tag (Icon link is URI)	CSG Type (EF_{CSGT})
'80'	HNB Name tag	Home NodeB Name (EF_{HNBN})
'80'	ICE Free Format Label tag	In Case of Emergency – Free Format ($_{EFICE\text{-}FF}$)
'81'	B-TID tag	GBA NAF List (EF_{GBANL})
'81'	Icon Tag (Icon link is record number)	Service Provider Name Icon (EF_{SPNI})
'81'	Master key tag	WLAN Reauthentication Identity (EF_{WRI})
'81'	Time Stamp counter tag	MBMS User Key (EF_{MUK})
'81'	Graphics CSG Type tag (Icon link is record number)	CSG Type (EF_{CSGT})
'81'	ICE Free Format Content tag	In Case of Emergency – Free Format ($_{EFICE\text{-}FF}$)
'82'	Counter tag	WLAN Reauthentication Identity (EF_{WRI})
'89'	Text CSG Type tag	CSG Type (EF_{CSGT})
'A0'	MUK ID tag The following tags are encapsulated within 'A0' '80' MUk IDr tag '82' MUk IDi tag	MBMS User Key (EF_{MUK})
'A0'	EPS NAS security Context tag The following tags are encapsulated within 'A0' '80' Key set identifier KSI_{ASME} Tag '81' ASME key (K_{ASME}) Tag '82' Uplink NAS count Tag '83' Downlink NAS count Tag '84' Identifiers of selected NAS integrity and encryption algorithms Tag	EPS NAS Security Context (EF_{EPSPSC})
'A0'	CSG List TLV object tag The following tags are encapsulated within 'A0'	Allowed CSG List (EF_{ACSGL}) Operator CSG List (EF_{OCSGL})

	'80' PLMN tag '81' CSG Information tag	
'A0'	GSM cell information The following tags are encapsulated within 'A0': '80' GSM Camping Frequency Information data object '81' GSM Neighbour Frequency Information data object	Network Parameters (EF_{NETPAR})
'A1'	FDD cell information The following tags are encapsulated within 'A1': '80' FDD Intra Frequency Information data object '81' FDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'A2'	TDD cell information The following tags are encapsulated within 'A2': '80' TDD Intra Frequency Information data object '81' TDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'A3'	Service provider display information The following tags are encapsulated within 'A3': '80' Service provider PLMN list	Service Provider Display Information (EF_{SPDI})
'A8'	Indicator for type 1 EFs (amount of records equal to master EF) The following tags are encapsulated within 'A8': 'C0' EF_{ADN} data object 'C1' EF_{IAP} data object 'C3' EF_{SNE} data object 'C4' EF_{ANR} data object 'C5' EF_{PBC} data object 'C6' EF_{GRP} data object 'C9' EF_{UID} data object 'CA' EF_{EMAIL} data object	Phone Book Reference File (EF_{PBR})
'A9'	Indicator for type 2 EFs (EFs linked via the index administration file) The following tags are encapsulated within 'A9': 'C3' EF_{SNE} data object 'C4' EF_{ANR} data object 'CA' EF_{EMAIL} data object	Phone Book Reference File (EF_{PBR})
'AA'	Indicator for type 3 EFs (EFs addressed inside an object using a record identifier as a pointer) The following tags are encapsulated within 'AA': 'C2' EF_{EXT1} data object 'C7' EF_{AAS} data object 'C8' EF_{GAS} data object 'CB' EF_{CCP1} data object	Phone Book Reference File (EF_{PBR})
'AB'	MMS Connectivity Parameters: The following are encapsulated under 'AB': '80' MMS Implementation Tag '81' MMS Relay/Server Tag '82' Interface to core network and bearer Tag '83' Gateway Tag '84' Reserved for 3GPP2: MMS Authentication Mechanism Tag '85' Reserved for 3GPP2: MMS Authentication User Name Tag	MMS Connectivity Parameters (EF_{MMSICP} / EF_{MMSUCP})
'DB'	Successful 3G authentication	Response to AUTHENTICATE
'DB'	Successful VGCS/VBS operation authentication tag	Response to AUTHENTICATE
'DB'	Successful GBA operation tag	Response to AUTHENTICATE
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DD'	Access Point Name	APN Control List (EF_{ACL})
'DD'	GBA Security Context Bootstrapping Mode tag	AUTHENTICATE command parameter, in GBA security context
'DE'	GBA Security Context NAF Derivation Mode tag	Response to AUTHENTICATE

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825-1 [35]

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

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2F00'	Application directory	Card issuer/operator dependent
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependent
'2FE2'	ICC identification	operator dependent
'4F01'	Launch SCWS	Operator dependent
'4F20'	Image data	'00FF...FF'
'4F20'	GSM Ciphering key Kc	'FF...FF07'
'4FXX'	Image instance data files	'FF…FF'
'4F21'	ICE graphics	'FF…FF'
4FXX'	Icon	Operator dependent
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependent
'4F30'	SoLSA Access Indicator	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'4FXX'	LSA Descriptor files	'FF…FF'
'4FXX'	Capability configuration parameters 1	'FF…FF'
'4F52'	GPRS Ciphring key KcGPRS	'FF...FF07'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'4F41'	Pseudonym	'00FF…FF'
'4F42'	User Controlled PLMN selector for I-WLAN	'FF…FF'
'4F43'	Operator Controlled PLMN selector for I-WLAN	Operator dependent
'4F44'	User Controlled WSID list	'00FF…FF'
'4F45'	Operator controlled WSID list	Operator dependent
'4F46'	WLAN Reauthentication Identity	'FF…FF'
'4F47'	Home I-WLAN Specific Identifier List	Operator dependent
'4F47'	Multimedia Messages List	'FF…FF'
'4F48'	I-WLAN Equivalent HPLMN Presentation Indication	Operator dependent
'4F48'	Multimedia Messages Data File	'FF…FF'
'4F49'	I-WLAN HPLMN Indication	Operator dependent
'4F4A'	I-WLAN Last Registered PLMN	'FFFFFF'
'4F4B'	HPLMN Direct Access Indicator	Operator dependent
'4F81'	Allowed CSG lists	Operator dependent
'4F82'	CSG Type	Operator dependent
'4F83'	HNB name	Operator dependent
'4F84'	Operator CSG lists	Operator dependent
'4F85'	Operator CSG Type	Operator dependent
'4F86'	Operator HNB name	Operator dependent
'6F05'	Language indication	'FF…FF'

'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Card issuer/operator dependent
'6F07'	IMSI	Operator dependent
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependent
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependent
'6F3F'	Group identifier level 2	Operator dependent
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependent
'6F47'	Short message status reports	'00FF…FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'
'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F54'	SetUp Menu Elements	Operator dependent
'6F55'	Extension 4	'00FF...FF'
'6F56'	Enabled services table	Operator dependent
'6F57'	Access point name control list	'00FF…FF'
'6F58'	Comparison method information	'FF…FF'
'6F5B'	Initialisation value for Hyperframe number	'F0 00 00 F0 00 00'
'6F5C'	Maximum value of START	Operator dependent
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependent
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF…FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF…FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependent
'6FB1'	Voice Group Call Service	Operator dependent
'6FB2'	Voice Group Call Service Status	Operator dependent
'6FB3'	Voice Broadcast Service	Operator dependent
'6FB4'	Voice Broadcast Service Status	Operator dependent
'6FB5'	EMLPP	Operator dependent
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependent
'6FC3'	Key for hidden phone book entries	'FF…FF'
'6FC4'	Network Parameters	'FF…FF'
'6FC5'	PLMN Network Name	Operator dependent
'6FC6'	Operator Network List	Operator dependent

'6FC7'	Mailbox Dialling Numbers	Operator dependent
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependent
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider Display Information	
'6FCE'	MMS Notification	'00 00 00 FF…FF'
'6FCF'	Extension 8	'00FF...FF'
'6FD0'	MMS Issuer Connectivity Parameters	'FF…FF'
'6FD1'	MMS User Preferences	'FF…FF'
'6FD2'	MMS User Connectivity Parameters	'FF…FF'
'6FD3'	Network's Indication of Alerting (NIA)	'FF...FF'
'6FD4'	Voice Group Call Service Ciphering Algorithm	'00…00'
'6FD5'	Voice Broadcast Service Ciphering Algorithm	'00…00'
'6FD6'	GBA Bootstrapping parameters	'FF…FF'
'6FD7'	MBMS Service Keys List	'FF…FF'
'6FD8'	MBMS User Key	'FF…FF'
'6FD9'	EHPLMN	'FF…FF' or xxxxxx (see Note 2)
'6FDA'	GBA NAF List	'FF…FF'
'6FDB'	EHPLMN Presentation Indication	'00'
'6FDC'	Last RPLMN Selection Indication	'00'
'6FDD'	NAF Key Centre Address	'FF…FF'
'6FDE'	Service Provider Name Icon	'00 FF…FF'
'6FDF'	PLMN Network Name Icon	'00 FF…FF'
'6FE0'	In Case of Emergency – Dialling Number	Operator dependent
'6FE1'	In Case of Emergency – Free Format	Operator dependent
'6FE2'	Network Connectivity Parameters for UICC IP connections	Operator dependent
'6FE3'	EPS location information	'FFFFFFFFFFFFFFFFFFFFFFFF xxxxxx0000 01' (see note 2)
'6FE4'	EPS NAS Security Context	'FF…FF'
'6FE5'	Public Service Identity of the SM-SC	Operator dependent
'6FE6'	USAT Facility Control	'80 1E 60 C0 1E 90 00 80 04 00 00 00 00 00 00 00 00 F0 00 00 00 00 40 00 00 00 00 00 00 80'
'6FE7'	UICC IARI	Operator dependent
'6FE8'	Non Access Stratum Configuration	Operator dependent
'6FE9'	UICC certificate	Card Issuer / Operator dependent
'6FEA'	Relay Node ID	Operator dependent
'6FEB'	Max value of Secure Channel counter	FF..FF
'6FEC'	Public Warning System	Operator dependent

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [9].

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

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSa IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSa IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:

LSA descriptor type = LSA ID and number = 2 (1 byte)	LSA ID (3 bytes)	LSA ID (3 bytes)	Identifier (1 byte)

2nd record:

LSA descriptor type = CI and number = 3 (1 byte)	CI (2 bytes)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1st record:

LSA descriptor type = LSA ID and number = 1 (1 byte)	LSA ID (3 bytes)	'FF'	Identifier (1 byte)

2nd record:

LSA descriptor type = CI and number = 2 (1 byte)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

Annex G (informative): Phonebook Example

This example phonebook has more than 254 entries. Additional number (3 additional numbers) information, second name and e-mail information can be added to each ADN entry. In addition each entry has a 2 byte Unique ID (UID) attached to it. The phonebook also contains three files that are shared EF_{EXT1}, EF_{AAS} and EF_{GAS}. These files are addressed from inside a file. EF_{EXT1} is addressed via $EF_{ADN,}$ EF_{ADN1}, EF_{AAS} is addressed via $EF_{ANRA,}$ EF_{ANRA1}, EF_{ANRB}, EF_{ANRB1}, EF_{ANRC}, EF_{ANRC1} and EF_{GAS} is addressed via $EF_{GRP,}$ EF_{GRP1}. The phonebook supports two levels of grouping and hidden entries in $EF_{PBC.}$

Two records are needed in the phonebook reference file PBR '4F30' for supporting more than 254 entries. The content of the phonebook reference file PBR '4F30' records is as shown in table G.2. The structure of the $DF_{PHONEBOOK}$ is shown in table G.1.

The content of phonebook entries in the range from 1-508 is described in the tables G.3 and G.4.

Table G.1: Structure of EFs inside $DF_{PHONEBOOK}$

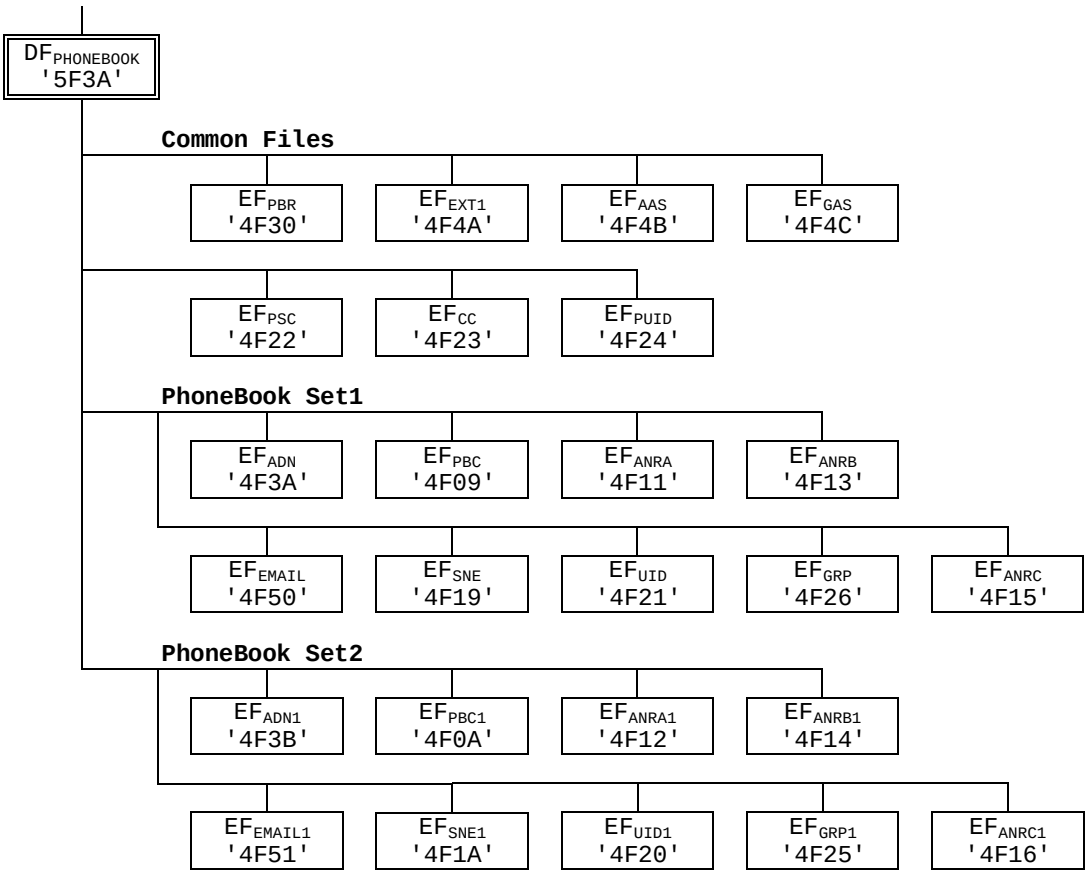


Table G.2: Contents of EF_{PBR}

Rec 1 Tag'A8' L='2D' (for Phonebook Set1)

Tag'C0'	L='03'	'4F3A'	'01'	Tag'C5'	L='03'	'4F09'	'02'	Tag'C6'	L='03'	'4F26'	'03'
Tag'C4'	L='03'	'4F11'	'04'	Tag'C4'	L='03'	'4F13'	'05'	Tag'C4'	L='03'	'4F15'	'06'
Tag'C3'	L='03'	'4F19'	'07'	Tag'C9'	L='03'	'4F21'	'12'	Tag'CA'	L='03'	'4F50'	'09'
Tag'AA'	L='0F'										
Tag'C2'	L='03'	'4F4A'	'08'	Tag'C7'	L='03'	'4F4B'	'14'	Tag'C8'	L='03'	'4F4C'	'15'

Rec 2 Tag'A8' L='2D' (for Phonebook Set 2)

Tag'C0'	L='03'	'4F3B'	'0A'	Tag'C5'	L='03'	'4F0A'	'0B'	Tag'C6'	L='03'	'4F25'	'0C'
Tag'C4'	L='03'	'4F12'	'0D	Tag'C4'	L='03'	'4F14'	'0E'	Tag'C4'	L='03'	'4F16'	'0F'
Tag'C3'	L='03'	'4F1A'	'10'	Tag'C9'	L='03'	'4F20'	'13'	Tag'CA'	L='03'	'4F51'	'11'
Tag'AA'	L='0F'										
Tag'C2'	L='03'	'4F4A'	'08'	Tag'C7'	L='03'	'4F4B'	'14'	Tag'C8'	L='03'	‘4F4C	'15'

Table G.3: Structure of the 254 first entries in the phonebook

Phone book entry	ADN '4F3A' SFI '01'		PBC '4F09' SFI '02'	GRP '4F26' SFI '03'	ANRA '4F11' SFI '04'	ANRB '4F13' SFI '05'	ANRC '4F15' SFI '06'	SNE '4F19' SFI '07'	UID '4F21' SFI '12'	EXT1 '4F4A' SFI '08'	AAS '4F4B' SFI '14'	GAS '4F4C' SFI '15'	EMAIL '4F50' SFI '09'
# 1	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID rec N° 3)	Rec n°1 Rec n°3 '00'	ANRA Rec n°1	ANRB Rec n°1	ANRC Rec n°1	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 2	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA Rec n°2	ANRB Rec n°2	ANRC Rec n°2	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 3													
:													
:													
:													
# 254													

Table G.4: Structure of phone book entries 255 to 508 (Rec 1-254)

Phone book entry	ADN1 '4F3B' SFI '0A'		PBC1 '4F0A' SFI '0B'	GRP1 '4F25' SFI '0C'	ANRA1 '4F12' SFI '0D'	ANRB1 '4F14' SFI '0E'	ANRC1 '4F16' SFI '0F'	SNE1 '4F1A' SFI '10'	UID1 '4F20' SFI '13'	EXT1 '4F4A' SFI '08'	AAS '4F4B' SFI '14'	GAS '4F4C' SFI '15'	EMAIL1 '4F51' SFI '11'
#255	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '03'	Hidden (AID Rec n° 3)	Rec n°1 Rec n°3 '00'	ANRA1 Rec n°1	ANRB1 Rec n°1	ANRC1 Rec n°1	Second Name Alpha String	UID	Rec '03'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#256	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2B'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA1 Rec n°2	ANRB1 Rec n°2	ANRC1 Rec n°2	Second Name Alpha String	UID	Rec '2B'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#257													
:													
:													
:													
#508													

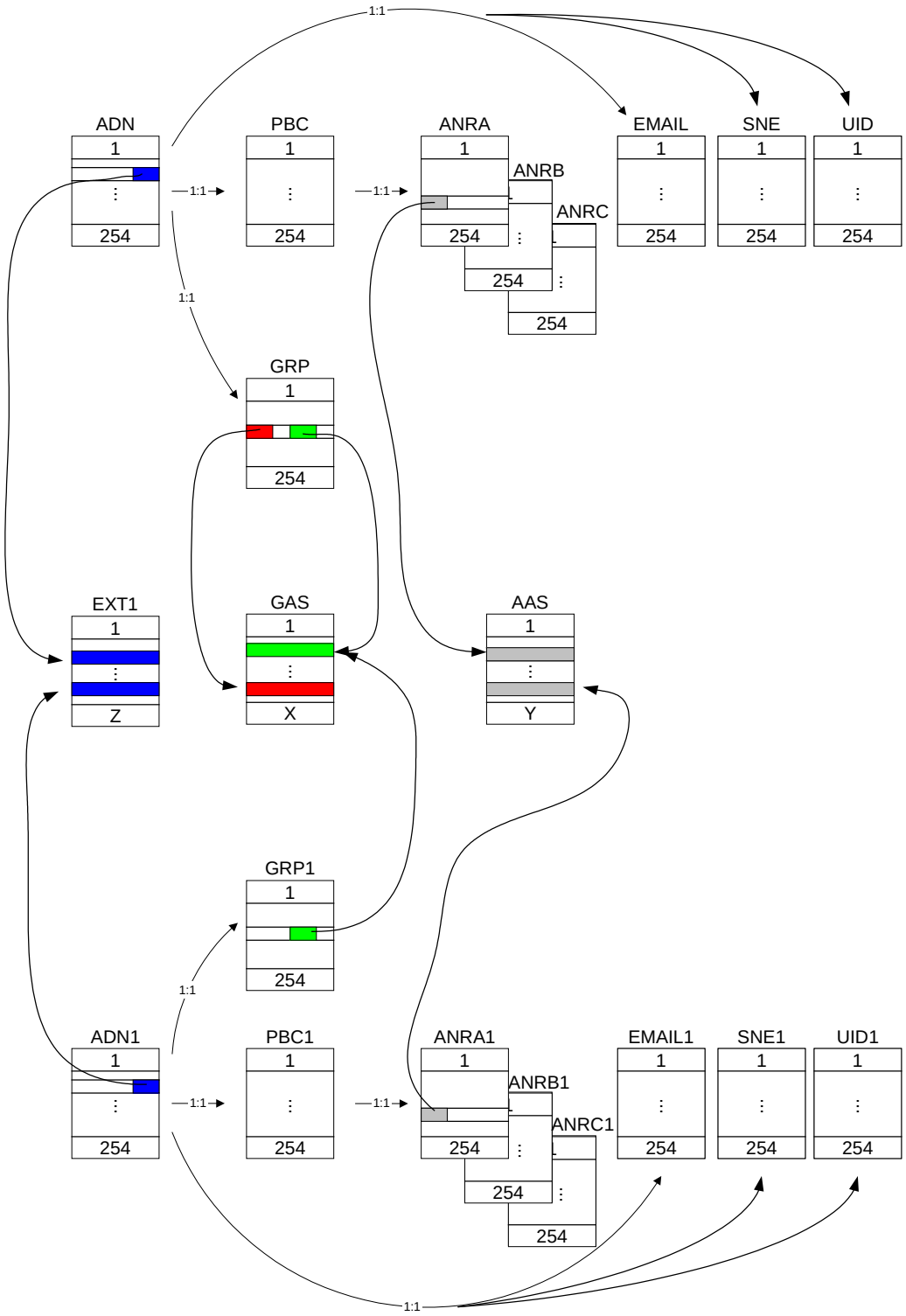


Figure G.1: Structure and Relations of the Example Phone Book

Annex H (normative): List of SFI Values

This annex lists SFI values assigned in the present document.

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

File Identification	SFI	Description
'6FB7'	'01'	Emergency call codes
'6F05'	'02'	Language indication
'6FAD'	'03'	Administrative data
'6F38'	'04'	USIM service table
'6F56'	'05'	Enabled services table
'6F78'	'06'	Access control class
'6F07'	'07'	IMSI
'6F08'	'08'	Ciphering and integrity keys
'6F09'	'09'	Ciphering and integrity keys for packet switched domain
'6F60'	'0A'	User PLMN selector
'6F7E	'0B'	Location information
'6F73'	'0C'	Packet switched location information
'6F7B'	'0D'	Forbidden PLMNs
'6F48'	'0E'	CBMID
'6F5B'	'0F'	Hyperframe number
'6F5C'	'10'	Maximum value of hyperframe number
'6F61'	'11'	Operator PLMN selector
'6F31'	'12'	Higher Priority PLMN search period
'6F62'	'13'	Preferred HPLMN access technology
'6F80'	'14'	Incoming call information
'6F81'	'15'	Outgoing call information
'6F4F'	'16'	Capability configuration parameters 2
'6F06'	'17'	Access Rule Reference
'6FC5'	'19'	PLMN Network Name
'6FC6'	'1A'	Operator Network List
'6FCD'	'1B'	Service Provider Display Information
'6F39'	'1C'	Accumulated Call Meter (see note)
'6FD9'	'1D'	Equivalent HPLMN
'6FE3'	'1E'	EPS location information
'6FE4'	'18'	EPS NAS Security Context
NOTE: When used the value '1C' shall be used as SFI for EF_{ACM}, for compatibility reasons the terminal shall accept other values.		

All other SFI values are reserved for future use.

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

File Identification	SFI	Description
'4F20'	'01'	GSM Ciphering Key Kc
'4F52'	'02'	GPRS Ciphering Key KcGPRS

All other SFI values are reserved for future use.

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

File Identification	SFI	Description
'4F41'	'01'	Pseudonym
'4F42'	'02'	User controlled PLMN for WLAN
'4F43'	'03'	Operator controlled PLMN for WLAN
'4F44'	'04'	User controlled WSID list
'4F45'	'05'	Operator controlled WSID list
'4F46'	'06'	WLAN Reauthentication Identity
'4F47'	'07'	Home I-WLAN Specific Identifier List
'4F48'	'08'	I-WLAN Equivalent HPLMN Presentation Indication
'4F49'	'09'	I-WLAN HPLMN Priority Indication
'4F4A'	'0A'	I-WLAN Last Registered PLMN
'4F4B'	'0B'	HPLMN Direct Access Indicator

All other SFI values are reserved for future use.

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

File Identification	SFI	Description
'4F81'	'01'	Allowed CSG lists
'4F82'	'02'	CSG Type
'4F83'	'03'	HNB name
'4F84'	'04'	Operator CSG lists
'4F85'	'05'	Operator CSG Type
'4F86'	'06'	Operator HNB name

All other SFI values are reserved for future use.

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

The purpose of this annex is to illustrate the different Application Session procedures.

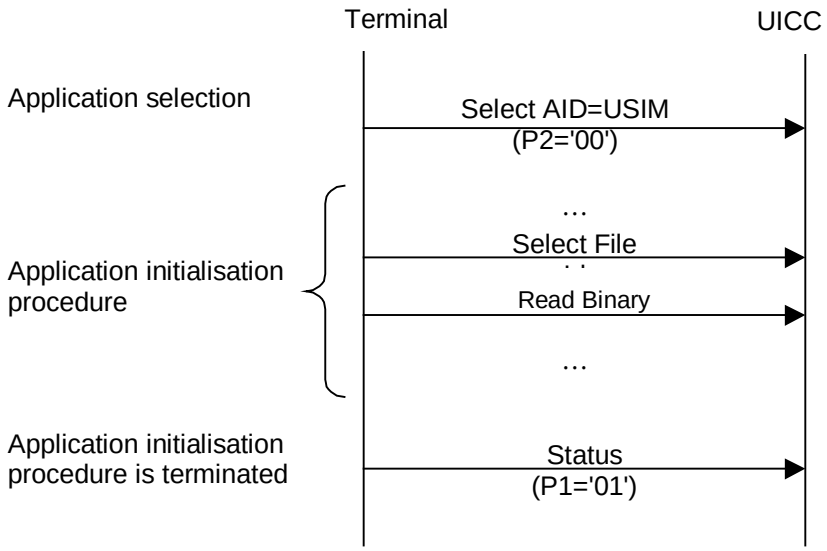


Figure I.1 USIM Application Session Activation procedure

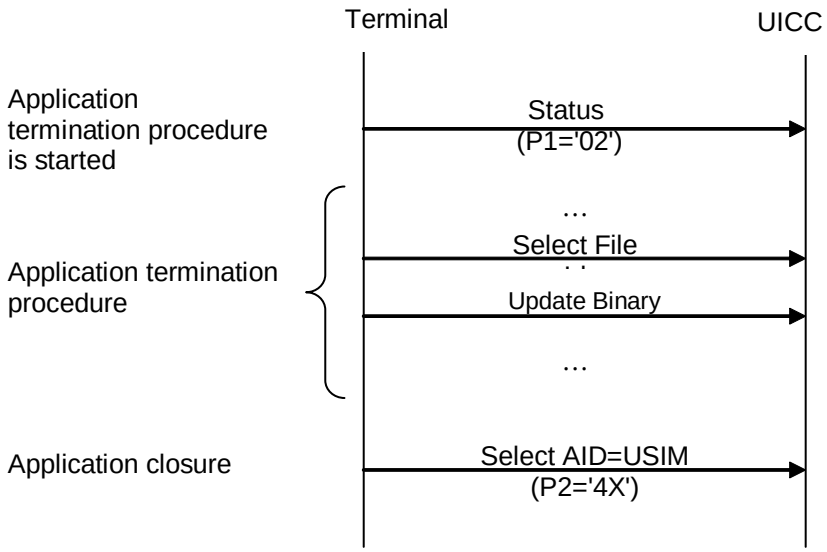


Figure I.2 USIM Application Session Termination procedure

Annex J (informative): Example of MMS coding

This annex gives an example for the coding of MMS User Preferences, while the MMS User Information Preference parameters are coded according to the WAP implementation of MMS.

J.1 Coding example for MMS User Preferences

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "(WAP")

0x81 MMS User Preference Profile Name Tag

0x0E (Length = "14")

43 68 72 69 73 74 6D 61 73 20 43 61 72 64

(profile name = "Christmas Card"; 14 characters, 14 Bytes)

0x82 MMS User Information Preference Information Tag

0x19 (Length = "25")

0x14 0x80 (visibility: = "hide"; 2 Bytes)

0x06 0x80 (delivery report: = "yes"; 2 Bytes)

0x10 0x80 (read-reply: = "yes"; 2 Bytes)

0x0F 0x81 (priority: = "normal"; 2 Bytes)

0x07 0x07 0x80 0x05 0x11 0x22 0x33 0x44 0x55
(Delivery-Time-Tag, Value-Length, Absolute-Token-Tag, Date-Value-Length, Date-Value; 9 Bytes)

0x08 0x06 0x81 0x04 0x55 0x22 0x33 0x44
(Expiry Tag, Value-Length, Relative-Token-Tag, Delta-Second-Value-Length, Delta-Second-Value; 8 Bytes)

J.2 Coding Example for MMS Issuer/User Connectivity Parameters

0xAB MMS Connectivity Parameters Tag

0x81 0x88 (Length = "136") (Length bytes greater than 127 are coded onto 2 bytes according to ISO/IEC 8825-1 [35])

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "WAP"; 1 Byte)

0x81 MMS Relay/Server Tag

0x17 (Length = "23")

0x68 0x74 0x74 0x70 0x3A 0x2F 0x2F 0x6D 0x6D 0x73 0x2D 0x6F 0x70 0x65 0x72 0x61 0x74 0x6F 0x72 0x2E 0x63 0x6F 0x6D
(MMS Relay/Server information = "http://mms-operator.com"; 23 characters; 23 Bytes)

0x82 Interface to Core Network and Bearer Tag

0x32 (Length = "50")

0x10 0xAA (bearer = "GSM-CSD"; 2 Bytes)

0x08 0x2B 0x34 0x39 0x35 0x33 0x34 0x31 0x39 0x30 0x36 0x00
(address = "+495341906", 12 Bytes)

0x09 0x87 (type of address = "E164"; 2 Bytes)

0x25 0xC5 (speed = "autobauding"; 2 Bytes)

0x0A 0x90 (call type = "ANALOG_MODEM"; 2 Bytes)

0x0C 0x9A (authentication type = "PAP"; 2 Bytes)

0x0D 0x64 0x75 0x6D 0x6D 0x79 0x11 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x0E 0x64 0x75 0x6D 0x6D 0x79 0x11 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

0x83 Gateway Tag

0x36 (Length = "54")

0x20 0x31 0x37 0x30 0x2E 0x31 0x38 0x37 0x2E 0x35 0x31 0x2E 0x33 0x00
(address = "170.187.51.3"; 14 Bytes)

0x21 0x85 (type of address = "IPv4"; 2 Bytes)

0x23 0x39 0x32 0x30 0x33 0x00 (port = "9203"; 6 Bytes)

0x24 0xCB (service = "CO-WSP"; 2 Bytes)

0x19 0x9C (authentication type = "HTTP BASIC"; 2 Bytes)

0x1A 0x64 0x75 0x6D 0x6D 0x79 0x11 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x1B 0x64 0x75 0x6D 0x6D 0x79 0x11 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

Annex K (informative): Examples of VService_Id coding

This annex gives examples for the coding of VService_Id,

It is assumed that:

- acknowledgement flag bit is set to 0;
- the call priority bits are set to 0.

GroupId	Content of EF_{VBS} or EF_{VGCs}	VService_Id(vbs)	VService_Id(vgcs)
00000000	F0FFFFFF	00000000	00000010
00000001	F1FFFFFF	00000020	00000030
00000012	21FFFFFF	00000180	00000190
00000123	21F3FFFF	00000F60	00000F70
00001234	2143FFFF	00009A40	00009A50
00012345	2143F5FF	00060720	00060730
00123456	214365FF	003C4800	003C4810
01234567	214365F7	025AD0E0	025AD0F0
12345678	21436587	178C29C0	178C29D0
99999999	99999999	BEBC1FE0	BEBC1FF0
13452670	31546207	19A8AFC0	19A8AFD0

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

L.1 Introduction

USIM-RN and USIM-INI are used for Relay Node network connections establishment.

USIM-INI, if present on the UICC, and USIM-RN include at least all mandatory files defined for a USIM in the present document, with the exception of files related to emergency calls.

Editor's note: It is FFS whether the list of files mandatory to support can be reduced further.

USIM-INI is only required in case of a certificate based solution as described in TS 33.401 [52].

For the certificate-based solution, the UICC shall support BIP-UICC server mode (see TS 31.111 [12]) and may support the Inter-Chip USB UICC/terminal interface (see TS 31.101 [11]) to perform the TLS handshake.

The USIM-RN is used to ensure a one to one binding with the Relay Node. The security architecture for Relay Nodes is defined in TS 33.401 [52].

L.2 Application selection procedure

Application selection is performed according to the procedures defined in clause 5.1.1.1. The following provisions apply:

When using pre-shared keys, only a USIM-RN is required, and the Relay Node will establish directly a secure channel with USIM-RN. It is assumed that the Relay Node knows the "3G application code" within the PIX value reserved for 3GPP USIM-RN.

When using certificate based procedure, the UICC inserted in the Relay Node shall contains two USIMs, the USIM-RN and USIM-INI. In case initial provisioning is required, the Relay Node will first select USIM-INI, either by direct application selection or by use of the EF_DIR file.

1. Direct application selection: with full or with partial AID. It is assumed that the Relay Node knows the "3G application code" within the PIX value reserved for 3GPP USIM-INI.

2. By use of the EF_DIR file: The Relay Node identifies the USIM-INI, which is characterised by an AID with a "3G application code" within the PIX value reserved for 3GPP USIM-INI, see TS 31.101 [11], and selects the USIM-INI by AID. The AID of the USIM-RN is characterised by an AID with a "3G application code" within the PIX value reserved for 3GPP USIM-RN, see TS 31.101 [11]. If the only applications present in EF_DIR are a USIM-RN and a USIM-INI, the terminal omits user presentation and proceeds to application selection.

The USIM applications USIM-INI and USIM-RN are not simultaneously active. USIM-INI is used to establish an initial network connection and USIM-INI is deactivated once the network related operations are finished. USIM-INI is deactivated prior to activating USIM-RN.

USIM-INI may be selected on any logical channel, see TS 31.101 [11]. Prior to selecting USIM-RN a new logical channel shall be opened using the MANAGE CHANNEL command as specified in TS 31.101 [11], an application to application secure channel can only be established on a logical channel different from channel 0. USIM-RN is then selected on the new logical channel.

USIM-RN shall be configured to support implicit and explicit application selection. The Relay Node will first select USIM-INI, according to the application selection mechanisms specified in TS 31.101 [11]. When the USIM-RN is selected explicitly, the Relay Node shall send a SELECT by AID APDU command in clear text prior to secure channel establishment. The implicit selection mechanism is performed by specifying USIM-RN AID in the MANAGE SECURE CHANNEL – Establish Master SA command.

L.3 Secure channel operation

The USIM-RN shall allow communication only via "Secured APDU" secure channel as defined in ETSI TS 102 484 [66].

NOTE: The above implies in particular that the AUTHENTICATE command to the USIM-RN is not executed outside the secure channel.In case the pre-shared key solution is used to establish the secure channel only the USIM-RN is required for establishing the connection, and the Relay Node will establish directly a secure channel with the USIM-RN before attaching to the network. The initial network connection using USIM-INI is not required in this case, and hence USIM-INI is not required.

In case the certificate based solution is used, the UICC inserted in the Relay Node shall contain two USIMs, USIM-RN and USIM-INI. A TLS handshake shall be used to provide key material for the Master SA for the secured APDU protocol, according to ETSI TS 102 484 [66].

L.4 Support of commands

The Relay Node may limit the set of APDU commands encapsulated in TRANSACT DATA command to the strict minimum (READ BINARY, READ RECORD, SELECT, STATUS, UPDATE BINARY, UPDATE RECORD, AUTHENTICATE).

The Relay Node and the UICC shall support letter class 'e' toolkit commands for BIP, see TS 31.111 [12]. In order to support toolkit the TERMINAL PROFILE, TERMINAL RESPONSE, ENVELOPE and FETCH commands need to be supported. These commands are not issued on the secure channel. According to TS 31.111 [12], USAT commands shall be sent on logical channel 0.

L.5 Storage of certificates

If the UICC supports the certificate based procedure, the UICC shall be provisioned with the UICC certificate and the root certificate. The UICC certificate, which is used as a server certificate in the TLS handshake, is stored in EF_{CERT} in USIM-INI as it needs to be accessed by the RN for reading the CRL distribution point before establishing the secure channel, for details cf. TS 33.401 [52]. The root certificate, which is used to verify the RN certificate in the TLS handshake, is only needed for UICC-internal purposes and need not be stored in an EF.

L.6 Relay Node files support

L.6.1 USIM-INI Files

L.6.1.1 EF_{CERT} (UICC Certificate)

This file contains the UICC Certificate.

Identifier: '6FE9'	Structure: transparent	Optional
File size: N bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
X	UICC Certificate	M	X

The format is as specified in TS 33.401 [52].

L.6.2 USIM-RN Files

L.6.2.1 eF_{RNid} (Relay Node identifier)

This EF contains the Relay Node identifier the USIM-RN is bound to, see TS 33.401 [52].

An USIM-RN shall contain this file. The content of this file is not intended to be read on UICC-RN interface. It serves as a storage location for the Relay Node identifier to which the UICC is bound. The file content is described for the purpose of Over-The-Air update.

Identifier: '6FEA'	Structure: transparent	Optional
File size: N bytes	Update activity: low	

Access Conditions:

READ	ADM
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
	Country Tag '80'	O	1 byte
	Country Length = 2	C	1 byte
	Country code (ASCII characters)	C	2 bytes
	Organization Tag '81'	M	1 byte
	Organization Length	M	1 byte
	Organization name (characters coded in UTF8)	M	K bytes
	Common Name Tag '82'	M	1 byte
	Common Name Length	M	1 byte
	Common Name (characters coded in UTF8)	M	L bytes
	Serial Number Tag '82'	O	1 byte
	Serial Number Length	C	1 byte
	Serial Number (characters coded in ASCII)	C	M bytes

NOTE: C: if the Tag is present, this is mandatory

L.6.2.2 EF_{SCCmax} (maximum value of Secure Channel Counter)

This EF contains the maximum number of transaction allowed with the same Connection SA, when a secure channel is established. When the counter value in TRANSACT DATA command reaches the maximum value, the terminal shall derive new key material using Manage Secure Channel APDU – establish SA – Connection SA, see ETSI TS 102.484 [66].

An USIM with an Application ID in the USIM-RN range shall contain this file.

Identifier: '6FEB'	Structure: transparent	Optional
File size: 8 bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
8	Secure Channel counter	M	8 byte

NOTE: The value of the Secure channel counter is set at personalisation. It is not intended to be updated or modified as a result of establishing a new Connection SA.

Annex M (informative): Change history

The table below indicates all CRs that have been incorporated into the present document since it was initially approved.

TSG # / Date	TSG Doc.	WG doc	CR	Rev	Cat	Subject/Comment	New
TP-27						Creation of Rel-7 version based on v6.9.0	7.0.0
TP-27	TP-050018	T3-050189	0264	1	F	Correction to overcome IMSI number space limitation – inclusion of EHPLMN	7.0.0
CT-28	CP-050136	C6-050402	0277		A	ISO/IEC 7816-series revision	7.1.0
CT-28	CP-050139	C6-050370	0272			Essential correction of the phonebook (access to mapped filed & "hidden key" coding)	7.1.0
CT-28	CP-050139	C6-050372	0285		A	Added EF_ARR under DF_TELECOM	7.1.0
CT-28	CP-050139	C6-050374	0280		A	Modifications regarding WLAN	7.1.0
CT-28	CP-050139	C6-050376	0282		A	Alignment of MBMS procedures with TS 33.246	7.1.0
CT-28	CP-050139	C6-050404	0287		A	Number of stored MSKs	7.1.0
CT-28	CP-050139	C6-050478	0289		A	Essential correction of phonebook support	7.1.0
CT-28	CP-050139	C6-050483	0291		A	Corrections to eMLPP and AAeM	7.1.0
CT-28	CP-050139	C6-050406	0278		F	Correction to EF-HPLMN	7.1.0
CT-29	CP-050460	C6-050689	0294	2	F	Clarification on ADM access condition	7.2.0
CT-29	CP-050460	C6-050729	0295	2	F	Editorial corrections	7.2.0
CT-30	CP-050499	C6-050876	0298		F	Clarifications in DF_PHONEBOOK level	7.3.0
CT-30	CP-050499	C6-050898	0297		A	NAF Id alignment with TS 33.246	7.3.0
CT-31	CP-060018	C6-060158	0304	1	A	Addition of mandatory UST services id references for VGCS/VBS security context definition	7.4.0
CT-31	CP-060023	C6-060119	0299		C	Change to allow PNN segmentation of the HPLMN and EHPLMN support	7.4.0
CT-31	CP-060023	C6-060122	0302		F	Indication of services in the USIM	7.4.0
CT-31	CP-060023	C6-060184	0305		C	Correction of service numbers associated to the UST	7.4.0
CT-31	CP-060156	C6-060121	0301	1	A	Padding of VSTK_RAND	7.4.0
-	-	-	-	-	-	MCC Completion of implementation of C6-060184	7.4.1
CT-32	CP-060239	C6-060277	0308		A	USAT related procedures - Additional Terminal Profile	7.5.0
CT-32	CP-060239	C6-060279	0310		a	VService_Id coding examples	7.5.0
CT-33	CP-060385	C6-060601	0318	1	F	Essential correction of the authenticate command in order to process message longer than 255 bytes	7.6.0
CT-34	CP-060541	C6-060781	0320	1	A	Correction of the MSK Update procedures	7.7.0
CT-34	CP-060541	C6-060808	0322	2	A	Clarification of the USIM behavior when MSK key is not updated	7.7.0
CT-34	CP-060541	C6-060785	0324	1	A	Correction of MBMS Security Context description	7.7.0
CT-34	CP-060541	C6-060764	0327	-	A	Correction of the references to a non-exisiting table in Authenticate command description	7.7.0
CT-34	CP-060541	C6-060817	0332	-	A	Correction of the MUK Update procedures	7.7.0
CT-34	CP-060547	C6-060788	0331	-	F	Correction of the Tables in section 7.1.2.5	7.7.0
CT-35	CP-070072	C6-070059	0340	-	F	Correction of the EHPLMN SFI	7.8.0
CT-35	CP-070067	C6-070120	0334	2	B	Presentation of EHPLMN	7.8.0
CT-35	CP-070067	C6-070133	0336	2	B	Last RPLMN Selection Indication	7.8.0
CT-35	CP-070071	C6-070123	0339	1	A	MSK management procedures	7.8.0
CT-36	CP-070305	C6-070311	0341	1	B	Presentation of additional information in manual selection mode	7.9.0
CT-36	CP-070299	C6-070310	0349	1	F	Correction of EF-IMG and EF-IIDF	7.9.0
CT-36	CP-070464	-	0350	1	A	GBA NAF Keys and MUKs storage policy	7.9.0
2007-06	-	-	-	-	-	Correction to implementation of '0x' as '04' in 7.1.2.5 (MCC)	7.9.1
CT-37	CP-070620	C6-070417	0347	3	B	Key Establishment mechanism: alignment with TS 33.110	7.10.0
CT-37	CP-070611	C6-070434	0352	-	A	Inconsistency in the MSK update procedures	7.10.0
CT-38	CP-070840	C6-070523	0355	-	F	Correction of reference to 3GPP TS 23.140	7.11.0
CT-38	CP-070840	C6-070586	0354	-	F	Completion of missing "Terminal Applications" entry in the UST	7.11.0
CT-38	CP-070841	C6-070884	0343	5	B	Reservation of parameters for OMA BCAST Smart Card Profile	8.0.0
CT-39	CP-080166	C6-080063	0365	1	A	MBMS security – Authentication error 9866	8.1.0
CT-39	CP-080167	C6-080059	0362	1	A	Add the support of EHPLMN in the automatic network selection	8.1.0
CT-39	CP-080168	C6-080014	0360	-	F	Correction of UST due to error in CR implementation	8.1.0
CT-39	CP-080168	C6-080064	0366	1	B	Correction of typo in the description of one of the fields of EFMBI.	8.1.0
CT-39	CP-080168	C6-080070	0357	3	B	Storage of SPN and PNN in graphic format Note: changes to clauses 5.3.10 and 5.3.24 have been moved to new sections with appropriate names.	8.1.0
CT-40	CP-080385	C6-080147	0368	1	F	Clarification of content of EFUID	8.2.0
CT-41	CP-080582	C6-080273	0372	-	A	Authentication of GBA	8.3.0
CT-41	CP-080642	C6-080266	0373	2	B	Introduction of ICE information in the UICC	8.3.0
CT-41	CP-080642	C6-080289	0375	2	B	Configuration of Network Connectivity parameters for UICC	8.3.0

						remote IP connections	
CT-41	CP-080642	C6-080245	0376	-	B	Introduction of new access technologies for LTE	8.3.0
CT-42	CP-080904	C6-080469	0374	5	B	Storage of EPS Mobility Management parameters	8.4.0
CT-42	CP-080904	C6-080468	0380	4	B	USIM provisioning for home (e)NodeB	8.4.0
CT-42	CP-080904	C6-080444	0382	1	B	Support for LTE in the EF-Operator PLMN	8.4.0
CT-42	CP-080909	C6-080409	0383	-	F	Correction to Example for MMS Issuer/User Connectivity Parameters	8.4.0
CT-42	CP-080961	----------	0385	2	B	Addition of I-WLAN related files and procedures	8.4.0
CT-43	CP-090188	C6-090007	0386	-	F	Removal of KNASint and KNASenc in EFEPSNSC	8.5.0
CT-43	CP-090188	C6-090056	0387	1	F	Correction of EF EPSNSC	8.5.0
CT-43	CP-090188	C6-090077	0390	-	B	Support of EPS in USAT: extension of Call control	8.5.0
CT-43	CP-090192	C6-090074	0388	1	B	HPLMN Direct Access Indicator for I-WLAN	8.5.0
CT-43	CP-090198	C6-090080	0384	5	F	Correction of Network Connectivity parameters for UICC remote IP connections (Email approval)	8.5.0
CT-44	CP-090451	C6-090110	0391	-	F	correction of coding of suggested contents of the EF_EPSLOCI at pre-personalization	8.6.0
CT-44	CP-090451	C6-090188	0392	2	F	correction of update status via Data Download or USAT Application for EF_EPSLOCI and EF_EPSNSC	8.6.0
CT-44	CP-090479	----------	0396	2	D	Editorial modifications of File structure overview	8.6.0
CT-44	CP-090479	----------	0398	2	A	Correction of wrong file names	8.6.0
CT-44	CP-090451	C6-090112	0399	-	F	Removal of NH and NCC parameters from EFEPSNSC	8.6.0
CT-44	CP-090451	C6-090116	0400	-	F	Correction for EPS in USIM security related procedures	8.6.0
CT-44	CP-090451	C6-090160	0405	-	C	Allowed CSG List updateable by ME	8.6.0
CT-45	CP-090712	C6-090305	0402	1	F	eCALL related enhancements	8.7.0
CT-45	CP-090712	C6-090301	0406	1	F	Correction of coding of CSG ID	8.7.0
CT-45	CP-090713	C6-090309	0409	2	F	Essential correction of EFSPDI encoding	8.7.0
CT-45	CP-090714	C6-090304	0412	3	F	Align files at Telecom level according to TS 102 222	9.0.0
CT-45	CP-090714	C6-090307	0416	2	B	Support For Multimode System Selection Storage	9.0.0
CT-46	CP-090991	C6-090415	0423	-	F	Correction to application session termination	9.1.0
CT-46	CP-090991	C6-090423	0428	-	D	Editorial correction on tables in NAF Key Centre tag and NAF Key Centre information	9.1.0
CT-46	CP-090992	C6-090440	0425	-	A	Correction of incorrect tag value	9.1.0
CT-46	CP-090990	C6-090460	0410	3	B	Introduction of operator controlled CSG list for H(e)NB	9.1.0
CT-46	CP-090990	C6-090500	0427	1	A	Correction of Allowed CSG list	9.1.0
CT-47	CP-100187	C6-100031	0429	-	F	Correction to EF_ACSGL access condition	9.2.0
CT-47	CP-100187	C6-100055	0431	-	F	Correction to informative Annex D	9.2.0
CT-47	CP-100188	C6-100111	0432	-	B	Introduction of Indicator for Inhibition of Allowed CSG List	9.2.0
CT-47	CP-100189	C6-100115	0433	-	B	Introduction of ICE (In Case of Emergency) graphics files	9.2.0
CT-48	CP-100391	C6-100260	0434	1	F	ICE graphics related procedure	9.3.0
CT-49	CP-100585	C6-100403	0446		A	Introduction of an ISIM EF to support Public Service Identity for SMS over IP	9.4.0
CT-49	CP-100586	C6-100358	0443		A	Update of reference to ETSI TS 102 483	9.4.0
CT-49	CP-100587	C6-100328	0438		F	Alignment of HNB and HeNB to the service requirements	9.4.0
CT-49	CP-100587	C6-100387	0439	1	F	Update reference to 3GPP2 specifications	9.4.0
CT-50	CP-100826	C6-100596	0450	1	F	Correction to Issuer specified PIN for ICE files	9.5.0
CT-50	CP-100827	C6-100617	0448	1	F	Allocation of File ID for EF_ICE-graphics	9.5.0
CT-50	CP-100827	C6-100618	0451	1	F	ETSI SCP specification reference update	9.5.0
CT-50	CP-100826	C6-100643	0466		A	Correction of EF_EPSNSC content description	9.5.0
CT-50	CP-100823	C6-1006428	0462	1	B	Communication control for IMS procedures in USIM	10.0.0
CT-51	CP-110236	C6-110191	0464	5	B	Introduction of Smart Card Web Server launch functionality	10.1.0
CT-51	CP-110239	C6-110062	0467	1	B	Addition of an EF for USAT facility control	10.1.0
CT-51	CP-110244	C6-110089	0469	1	B	Addition of 'Extended Terminal Application' support in EF_UST	10.1.0
CT-51	CP-110244	C6-110064	0470	1	D	Correction to coding of EF_MMSICP	10.1.0
CT-51	CP-110242	C6-110092	0471		F	CSG lists display Control	10.1.0
CT-51	CP-110297		0472	3	B	Introduction of the IARI list in the USIM	10.1.0
CT-51	CP-110302		0473	7	B	Non-Access Stratum (NAS) configuration parameters	10.1.0
CT-51	CP-110235	C6-110160	0475	1	B	Procedures for Relay Node USIM	10.1.0
CT-52	CP-110516	----------	0482	2	A	Essential correction to EPS NAS security context update	10.2.0
CT-52	CP-110527	----------	0479	3	C	Priority for NAS configuration parameters	10.2.0
CT-53	CP-110593	C6-110414	0483	2	A	Clarification of ACL in EPS Network	10.3.0
CT-53	CP-110703		0485	2	F	Correction to NAS configuration parameters coding	10.3.0
CT-53	CP-110595	C6-110411	0484	1	F	Correction of service required for EF-EST to be present	11.0.0
CT-55	CP-120173		0503	1	A	Correction of EF_ICON references in EF_LAUNCH_SCWS	11.1.0
CT-55	CP-120143	C6-120074	0504	1	D	Corrections in the section DFs at the USIM ADF level	11.1.0
CT-55	CP-120181		0510		A	Correction to Allowed CSG list and Operator CSG list coding	11.1.0
CT-55	CP-120145	C6-120091	0509		A	Update of reference to ETSI TS 102 484	11.1.0
CT-55	CP-120145	C6-120096	0511		A	Correction to EF_UICCIARI section number	11.1.0
CT-55	CP-120145	C6-120100	0512		A	FID allocation and other corrections to USIM for Relay Nodes	11.1.0
CT-56	CP-120385	C6-120221	0516		A	Correction to reference for CSG Type in EFCSGT	11.2.0
CT-56	CP-120386	C6-120277	0519	1	B	Adding new NAS configuration parameter for SIMTC	11.2.0
CT-57	CP-120620	C6-120440	0535	1	A	Update of reference to ASN.1 coding specification	11.3.0
CT-58	CP-120866	C6-120565	0546		A	Correction of update activity for EF_MSK	11.4.0

CT-58	CP-120867	C6-120610	0536	2	A	HPLMN or RPLMN selection clarification	11.4.0
CT-58	CP-120867	C6-120574	0539	1	A	Clarification for CSG Display Control during manual selection	11.4.0
CT-58	CP-120867	C6-120604	0517	2	B	Addition of EF with PWS configuration	11.4.0
CT-60	CP-130361	C6-130196	0558	1	A	Essential correction of CSG Type coding description	11.5.0
CT-61	CP-130530	C6-130378	0561	2	A	Handling of Multiple CSG ID display indicators for same PLMN id	11.6.0