EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 175-5

September 1996

Second Edition

Source: ETSI TC-RES

Reference: RE/RES-03027-5

ICS: 33.060.50

Key words: DECT, radio

Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Foreword 15

1 Scope 17

2 Normative references 17

3 Definitions and abbreviations 21
3.1 Definitions 21
3.2 Abbreviations 23

4 Overview of the NWK layer 25

5 Overview of procedures 26
5.1 General 26
5.2 Overview of Call Control (CC) 27
5.2.1 General 27
5.2.2 Call establishment 27
5.2.2.1 Call set-up 27
5.2.2.2 Service negotiation 28
5.2.3 Call connect 29
5.2.4 Call information 29
5.2.5 Service change 29
5.2.6 Call release 29
5.3 Overview of Supplementary Services (SS) 29
5.3.1 General 29
5.3.2 Keypad protocol 30
5.3.3 Feature key management protocol 30
5.3.4 Functional protocol 30
5.4 Overview of Connection Oriented Message Service (COMS) 31
5.4.1 General 31
5.4.2 COMS establishment 31
5.4.3 Service negotiation 31
5.4.4 COMS connect 32
5.4.5 COMS data transfer 32
5.4.6 COMS suspend and resume 32
5.4.7 COMS release 32
5.5 Overview of ConnectionLess Message Service (CLMS) 32
5.5.1 Fixed length message service 32
5.5.2 Variable length message service 33
5.6 Overview of Mobility Management (MM) 33
5.6.1 General 33
5.6.2 Identity procedures 33
5.6.3 Authentication procedures 34
5.6.4 Location procedures 34
5.6.5 Access rights procedures 34
5.6.6 Key allocation procedure 35
5.6.7 Parameter retrieval procedure 35
5.6.8 Ciphering related procedure 35
5.7 Overview of Link Control Entity (LCE) 35
5.7.1 General 35
5.7.2 Data Link Endpoint Identifier (DLEI) 36
5.7.3 Data link establishment 36
5.7.4 Data link re-establishment 37
5.7.5 Data link release 37

5.7.6 Data link suspend and resume 37
5.7.7 Queuing of messages 37
5.7.8 Request paging 37

6 Message functional definitions....38
6.1 Overview of message structures....38
6.1.1 Messages....38
6.1.2 Information elements....38
6.2 Message summaries....39
6.2.1 Summary of CC messages....39
6.2.2 Summary of CISS messages....39
6.2.3 Summary of COMS messages....40
6.2.4 Summary of CLMS messages 40
6.2.5 Summary of MM messages....41
6.2.6 Summary of LCE messages 41
6.3 S-FORMAT message functional contents 42
6.3.1 S-FORMAT message overview....42
6.3.2 CC-messages 43
6.3.2.1 {CC-SETUP}....43
6.3.2.2 {CC-INFO}....45
6.3.2.3 {CC-SETUP-ACK}....46
6.3.2.4 {CC-CALL-PROC}....47
6.3.2.5 {CC-ALERTING}....48
6.3.2.6 {CC-CONNECT}....49
6.3.2.7 {CC-CONNECT-ACK}....50
6.3.2.8 {CC-RELEASE} 50
6.3.2.9 {CC-RELEASE-COM} 51
6.3.2.10 {CC-SERVICE-CHANGE} 52
6.3.2.11 {CC-SERVICE-ACCEPT}....52
6.3.2.12 {CC-SERVICE-REJECT} 53
6.3.2.13 {CC-NOTIFY} 53
6.3.2.14 {IWU-INFO}....54
6.3.3 SS-messages (call related and call independent)....55
6.3.3.1 {FACILITY}....55
6.3.3.2 {HOLD} 55
6.3.3.3 {HOLD-ACK} 56
6.3.3.4 {HOLD-REJECT} 56
6.3.3.5 {RETRIEVE}....57
6.3.3.6 {RETRIEVE-ACK}....57
6.3.3.7 {RETRIEVE-REJECT}....58
6.3.3.8 {CISS-REGISTER}....58
6.3.3.9 {CISS-RELEASE-COM} 59
6.3.4 COMS-messages....59
6.3.4.1 {COMS-SETUP} 59
6.3.4.2 {COMS-INFO} 60
6.3.4.3 {COMS-ACK} 60
6.3.4.4 {COMS-CONNECT} 61
6.3.4.5 {COMS-RELEASE}....61
6.3.4.6 {COMS-RELEASE-COM}....62
6.3.4.7 {COMS-NOTIFY}....62
6.3.5 CLMS-message....63
6.3.5.1 {CLMS-VARIABLE}....63
6.3.6 MM-messages 64
6.3.6.1 {ACCESS-RIGHTS-ACCEPT}....64
6.3.6.2 {ACCESS-RIGHTS-REJECT}....64
6.3.6.3 {ACCESS-RIGHTS-REQUEST}....65
6.3.6.4 {ACCESS-RIGHTS-TERMINATE-ACCEPT}....65
6.3.6.5 {ACCESS-RIGHTS-TERMINATE-REJECT}....66
6.3.6.6 {ACCESS-RIGHTS-TERMINATE-REQUEST}....66
6.3.6.7 {AUTHENTICATION-REJECT}....67

6.3.6.8 {AUTHENTICATION-REPLY} 67
6.3.6.9 {AUTHENTICATION-REQUEST} 68
6.3.6.10 {CIPHER-REJECT} 68
6.3.6.11 {CIPHER-REQUEST} 69
6.3.6.12 {CIPHER-SUGGEST} 69
6.3.6.13 {DETACH} 70
6.3.6.14 {IDENTITY-REPLY} 70
6.3.6.15 {IDENTITY-REQUEST} 71
6.3.6.16 {KEY-ALLOCATE} 71
6.3.6.17 {LOCATE-ACCEPT} 72
6.3.6.18 {LOCATE-REJECT} 72
6.3.6.19 {LOCATE-REQUEST} 73
6.3.6.20 {MM-INFO-ACCEPT} 73
6.3.6.21 {MM-INFO-REJECT} 74
6.3.6.22 {MM-INFO-REQUEST} 74
6.3.6.23 {MM-INFO-SUGGEST} 75
6.3.6.24 {TEMPORARY-IDENTITY-ASSIGN} 75
6.3.6.25 {TEMPORARY-IDENTITY-ASSIGN-ACK} 76
6.3.6.26 {TEMPORARY-IDENTITY-ASSIGN-REJ} 76
6.3.7 LCE-messages 77
6.3.7.1 {LCE-PAGE-RESPONSE} 77
6.3.7.2 {LCE-PAGE-REJECT} 77
6.4 B-FORMAT message functional contents 77
6.4.1 B-FORMAT message overview 77
6.4.2 {LCE-REQUEST-PAGE} 78
6.4.3 {CLMS-FIXED} 79

7 S-FORMAT message structures 79
7.1 Overview 79
7.2 Protocol Discrimination (PD) element 80
7.3 Transaction Identifier (TI) element 80
7.4 Message type element 81
7.4.1 Messages for CC 82
7.4.2 Messages for SS 82
7.4.3 Messages for COMS 82
7.4.4 Messages for CLMS 82
7.4.5 Messages for MM 83
7.4.6 Messages for LCE 83
7.5 Other information elements 83
7.5.1 Coding rules 83
7.5.2 Extensions of codesets 85
7.5.3 Locking shift procedure 86
7.5.4 Non-locking shift procedure 86
7.5.5 Display and keypad elements 87
7.5.6 Repeated elements 87
7.6 Fixed length information elements 88
7.6.1 Summary 88
7.6.2 Sending complete and delimiter request 88
7.6.3 Repeat indicator 88
7.6.4 Basic service 89
7.6.5 Single display 89
7.6.6 Single keypad 90
7.6.7 Release reason 90
7.6.8 Signal 91
7.6.9 Timer restart 92
7.6.10 Test hook control 92
7.7 Variable length information elements 93
7.7.1 Summary 93
7.7.2 Allocation type 94
7.7.3 Alphanumeric 94

7.7.4 Auth type 96
7.7.5 Call attributes 97
7.7.6 Call identity 99
7.7.7 Called party number 100
7.7.8 Called party subaddress 101
7.7.9 Calling party number 102
7.7.10 Cipher info 103
7.7.11 Connection attributes 104
7.7.12 Connection identity 106
7.7.13 Duration 107
7.7.14 End-to-end compatibility 108
7.7.15 Facility 111
7.7.16 Feature activate 111
7.7.17 Feature indicate 114
7.7.18 Fixed identity 116
7.7.19 Identity type 117
7.7.20 Info type 118
7.7.21 InterWorking Unit (IWU) attributes 119
7.7.22 IWU packet 124
7.7.23 IWU to IWU 125
7.7.24 Key 127
7.7.25 Location area 128
7.7.26 Multi-display 129
7.7.27 Multi-keypad 129
7.7.28 NetWorK (NWK) assigned identity 129
7.7.29 Network parameter 130
7.7.30 Portable identity 131
7.7.31 Progress indicator 135
7.7.32 Rand 136
7.7.33 Rate parameters 136
7.7.34 Reject reason 138
7.7.35 RES 139
7.7.36 RS 139
7.7.37 Segmented info 140
7.7.38 Service change info 140
7.7.39 Service class 142
7.7.40 Set-up capability 142
7.7.41 Terminal capability 143
7.7.42 Transit delay 147
7.7.43 Window size 147
7.7.44 ZAP field 148
7.7.45 Escape to proprietary 148
7.7.46 Model identifier 149
7.7.47 MMS Generic Header 149
7.7.48 MMS Object Header 149
7.7.49 MMS Extended header 150
7.7.50 Time-Date 150
7.7.51 Ext h/o indicator 151

8 B-FORMAT message structures 152
8.1 General 152
8.2 LCE request paging messages 152
8.2.1 Short format message 154
8.2.2 Long format message 156
8.3 CLMS-FIXED messages 158
8.3.1 General message structure 158
8.3.2 Message elements 159
8.3.3 Standard message structures 160
8.3.3.1 General 160
8.3.3.2 Messages using 4-bit characters 160

8.3.3.3 Messages using 8-bit characters 161

9 Call Control (CC) procedures 161
9.1 General 161
9.2 Call Control (CC) states 164
9.2.1 States at PT 164
9.2.1.1 State T-00: "NULL" 164
9.2.1.2 State T-19: "RELEASE PENDING" 164
9.2.1.3 State T-10: "ACTIVE" 164
9.2.1.4 State T-01: "CALL INITIATED" 164
9.2.1.5 State T-02: "OVERLAP SENDING" 164
9.2.1.6 State T-03: "CALL PROCEEDING" 164
9.2.1.7 State T-04: "CALL DELIVERED" 164
9.2.1.8 State T-06: "CALL PRESENT" 164
9.2.1.9 State T-07: "CALL RECEIVED" 164
9.2.1.10 State T-08: "CONNECT PENDING" 164
9.2.2 States at FT 164
9.2.2.1 State F-00: "NULL" 164
9.2.2.2 State F-19: "RELEASE PENDING" 165
9.2.2.3 State F-10: "ACTIVE" 165
9.2.2.4 State F-01: "CALL-INITIATED" 165
9.2.2.5 State F-02: "OVERLAP SENDING" 165
9.2.2.6 State F-03: "CALL PROCEEDING" 165
9.2.2.7 State F-04: "CALL DELIVERED" 165
9.2.2.8 State F-06: "CALL PRESENT" 165
9.2.2.9 State F-07: "CALL RECEIVED" 165
9.2.3 Optional states (PT and FT) 166
9.2.3.1 States T-22 and F-22: "OVERLAP RECEIVING" 166
9.2.3.2 States T-23 and F-23: "INCOMING CALL PROCEEDING" 166
9.3 Call establishment procedures 166
9.3.1 PT initiated call establishment (outgoing call) 166
9.3.1.1 Call request 166
9.3.1.2 Call accept or reject 167
9.3.1.3 Selection of lower layer resources 168
9.3.1.4 Connection of U-plane 169
9.3.1.5 Overlap sending 169
9.3.1.6 Call proceeding 170
9.3.1.7 Call confirmation 170
9.3.1.8 Call connection 171
9.3.1.9 Expiry of timer <CC.04> 171
9.3.2 FT initiated call establishment (incoming call) 171
9.3.2.1 Call request 171
9.3.2.2 Call accept or reject 171
9.3.2.3 Selection of lower layer resources 172
9.3.2.4 Connection of U-plane 173
9.3.2.5 Overlap receiving 173
9.3.2.6 Call proceeding 173
9.3.2.7 Call confirmation 173
9.3.2.8 Call connection 174
9.3.2.9 Sending of <<TERMINAL-CAPABILITY>> 174
9.3.2.10 Expiry of timer <CC.04> 174
9.4 Call information procedures 174
9.5 Call release procedures 174
9.5.1 Normal call release 174
9.5.2 Abnormal call release 175
9.5.3 Release collisions 176
9.6 Service change procedures 176
9.6.1 General 176
9.6.2 Bandwidth changes (including reversals) 177
9.6.3 Service rerouting 177

9.6.4 Service suspension and resumption 177
9.7 Packet mode procedures 178
9.7.1 General 178
9.7.2 PT initiated access 178
9.7.3 FT initiated access 178
9.7.4 Packet mode suspend and resume 179
9.7.4.1 General 179
9.7.4.2 C-plane suspend and resume 179
9.7.4.3 U-plane suspend and resume 179

10 Supplementary Services procedures 180
10.1 General 180
10.2 Keypad protocol 180
10.3 Feature key management protocol 181
10.4 Functional protocol 181
10.4.1 Separate messages approach 181
10.4.1.1 Hold procedures 181
10.4.1.2 Retrieve procedures 182
10.4.1.3 Auxiliary states for hold and retrieve 182
10.4.2 Common information element approach 182
10.4.2.1 Call related procedures 182
10.4.2.2 Call independent procedures 183
10.4.2.3. Connectionless Supplementary Service (CLSS) procedure 183
10.5 Co-existence of multiple protocols 184
10.6 Application protocols 184
10.6.1 DECT standard functional supplementary services 184
10.6.2 DECT specific supplementary services 185
10.6.2.1 Queue management 185
10.6.2.2 Indication of subscriber number 186
10.6.2.3 Control of echo control functions 186
10.6.2.4 Cost information 186

11 Connection Oriented Message Service (COMS) 187
11.1 General 187
11.2 COMS states 187
11.2.1 States at PT 187
11.2.1.1 State TS-0: "NULL" 187
11.2.1.2 State TS-1: "CONNECT PENDING" 187
11.2.1.3 State TS-2: "RELEASE PENDING" 187
11.2.1.4 State TS-3: "ACTIVE" 187
11.2.2 States at FT 188
11.2.2.1 State FS-0: “NULL” 188
11.2.2.2 State FS-1: "CONNECT PENDING" 188
11.2.2.3 State FS-2: "RELEASE PENDING" 188
11.2.2.4 State FS-3: "ACTIVE" 188
11.3 COMS establishment procedures 188
11.3.1 PT initiated COMS establishment 188
11.3.1.1 COMS request 188
11.3.1.2 COMS connection 189
11.3.2 FT initiated COMS establishment 189
11.3.2.1 COMS request 189
11.3.2.2 COMS connection 189
11.4 COMS data transfer procedures 190
11.4.1 Procedure at the sending side 190
11.4.2 Procedure at the receiving side 190
11.5 COMS suspend and resume procedures 191
11.6 COMS release procedures 191
11.6.1 Normal COMS release 191
11.6.2 Release collisions 192

12 ConnectionLess Message Service (CLMS) 192
12.1 General 192
12.2 CLMS states 192
12.3 CLMS message transmission procedures 192
12.3.1 Fixed length messages 192
12.3.1.1 Procedure in the Fixed radio Termination (FT) 193
12.3.1.2 Procedure in the Portable radio Termination (PT) 193
12.3.2 Variable length messages 193
12.3.2.1 Procedure at the sending side 193
12.3.2.2 Procedure at the receiving side 194
12.3.2.3 Restrictions for portable side initiated messages 194

13 Mobility Management (MM) procedures 194
13.1 General 194
13.2 Identity procedures 195
13.2.1 Procedure for identification of PT 195
13.2.2 Procedure for temporary identity assignment 196
13.3 Authentication procedures 197
13.3.1 Authentication of a PT 198
13.3.2 Authentication of the user 199
13.3.3 Authentication of a FT 199
13.4 Location procedures 200
13.4.1 Location registration 200
13.4.2 Detach 202
13.4.3 Location update 202
13.5 Access rights procedure 203
13.5.1 Obtaining the access rights 203
13.5.2 Termination of access rights 204
13.6 Key allocation procedure 206
13.7 Parameter retrieval procedure 207
13.8 Ciphering related procedure 208

14 Link Control Entity (LCE) procedures 211
14.1 General 211
14.2 Connection oriented link control procedures 212
14.2.1 Link establishment 212
14.2.2 Direct PT initiated link establishment 212
14.2.3 Indirect (paged) FT initiated link establishment 213
14.2.4 Direct FT initiated link establishment (optional) 215
14.2.5 Link maintenance 215
14.2.6 Link suspend and resume 215
14.2.6.1 Link suspend 215
14.2.6.2 Link resume 216
14.2.7 Link release 216
14.2.7.1 NLR notification without "partial release" as release reason 216
14.2.7.2 NLR notification with "partial release" as release reason 217
14.3 Connectionless link control procedures 217
14.3.1 Message routing 217
14.3.2 Broadcast announce procedure 218
14.4 Procedure for collective and group ringing 218

15 Management procedures 219
15.1 Lower Layer Management Entity (LLME) 219
15.2 Service mapping and negotiation 220
15.2.1 General 220
15.2.2 Prioritised list negotiation 220
15.2.3 Exchanged attribute negotiation 221
15.2.4 Operating parameter negotiation 221
15.2.5 Peer attribute negotiation 221

15.3 Service modification procedures 222
15.4 Resource management 222
15.5 Management of MM procedures 222
15.6 Call ciphering management 223
15.7 External Handover 224
15.7.1 Handover candidate procedures 224
15.7.1.1 General 224
15.7.1.2 Handover candidate indication 224
15.7.1.3 Handover candidate retrieval 225
15.7.1.4 Target FP selection 225
15.7.2 Handover reference procedure 226
15.7.2.1 General 226
15.7.2.2 Handover reference indication 226
15.7.2.3 Handover reference retrieval 226
15.7.3 External handover suggested by FP 227
15.7.4 NWK layer set up procedure 227
15.7.4.1 Handover request 227
15.7.4.2 Handover confirm 227
15.7.4.3 Handover accept 227
15.7.4.4 Handover reject 227
15.7.4.5 Release of old connection 227
15.7.4.6 Handover Fall Back 228
15.7.5 U-plane handling 228
15.7.6 Ciphering procedure 228
15.8 Test management procedures 229
15.8.1 Test call back procedure 229
15.8.2 Test hook control procedures 229
15.8.3 Upper tester procedure 230

16 Primitives 230
16.1 Primitive types 230
16.2 Primitives to lower layer (DLC layer) 231
16.3 Primitives to IWU 231
16.3.1 Parameter definitions 231
16.3.2 MNCC primitives 231
16.3.2.1 MNCC_SETUP primitive 232
16.3.2.2 MNCC_SETUP_ACK primitive 232
16.3.2.3 MNCC_REJECT primitive 233
16.3.2.4 MNCC_CALL_PROC primitive 233
16.3.2.5 MNCC_ALERT primitive 234
16.3.2.6 MNCC_CONNECT primitive 234
16.3.2.7 MNCC_RELEASE primitive 234
16.3.2.8 MNCC_FACILITY primitive 235
16.3.2.9 MNCC_INFO primitive 235
16.3.2.10 MNCC_MODIFY primitive 235
16.3.2.11 MNCC_HOLD primitive 236
16.3.2.12 MNCC_RETRIEVE primitive 236
16.3.2.13 MNCC_IWU_INFO primitive 236
16.3.3 MNSS primitives 236
16.3.3.1 MNSS_SETUP primitive 237
16.3.3.2 MNSS_FACILITY primitive 237
16.3.3.3 MNSS_RELEASE primitive 237
16.3.4 MNCO primitives 237
16.3.4.1 MNCO_SETUP primitive 238
16.3.4.2 MNCO_CONNECT primitive 238
16.3.4.3 MNCO_INFO primitive 238
16.3.4.4 MNCO_ACK primitive 238
16.3.4.5 MNCO_RELEASE primitive 239
16.3.5 MNCL primitives 239
16.3.5.1 MNCL_UNITDATA primitive 239

16.3.6 MM primitives 239
16.3.6.1 MM_IDENTITY primitive 240
16.3.6.2 MM_IDENTITY_ASSIGN primitive 240
16.3.6.3 MM_AUTHENTICATE primitive 240
16.3.6.4 MM_LOCATE primitive 241
16.3.6.5 MM_DETACH primitive 241
16.3.6.6 MM_ACCESS_RIGHTS primitive 241
16.3.6.7 MM_ACCESS_RIGHTS_TERMINATE primitive 242
16.3.6.8 MM_KEY_ALLOCATE primitive 242
16.3.6.9 MM_INFO primitive 242
16.3.6.10 MM_CIPHER primitive 243

17 Handling of error and exception conditions 243
17.1 Protocol discrimination error 243
17.2 Message too short 243
17.3 Transaction identifier error 243
17.3.1 Illegal and unsupported transaction identifier value 243
17.3.2 Transaction identifier procedural errors and exception conditions 244
17.3.2.1 Unknown active CC call 244
17.3.2.2 Unknown active CISS call 244
17.3.2.3 Unknown active COMS call 244
17.3.2.4 Unknown active CLMS call 244
17.3.2.5 Unknown active MM transaction 244
17.3.2.6 Unknown active LCE transaction 244
17.3.3 Call Resource Contention 245
17.4 Message type or message sequence errors 245
17.4.1 CC message error 245
17.4.2 CISS message error 245
17.4.3 COMS or CLMS message error 245
17.4.4 MM message error 245
17.4.5 LCE message error 245
17.5 General information element errors 245
17.5.1 Information element out of sequence 245
17.5.2 Duplicated information elements 246
17.6 Mandatory information element errors 246
17.6.1 Mandatory information element missing in CC messages 246
17.6.2 Mandatory information element content error in CC messages 246
17.6.3 Mandatory information element error in COMS or CLMS messages 247
17.6.4 Mandatory information element error in MM messages 247
17.6.5 Mandatory information element error in LCE messages 247
17.7 Non-mandatory information element errors 247
17.7.1 Unrecognised information element 247
17.7.2 Non-mandatory information element content error 247
17.8 Data link reset 248
17.9 Data link failure 248

Annex A (normative): System parameters 249

A.1 CC timers 249

A.2 SS timers 249

A.3 COMS timers 250

A.4 CLMS timer 250

A.5 MM timers 250

A.6 LCE timers 252

A.7 NWK layer constants....252

A.8 Restart....252

Annex B (normative): CC state transition tables....253

B.1 CC state transitions at PT side....253
B.1.1 CC state table at PT side....253
B.1.2 CC transition procedures at PT side....253

B.2 CC state transitions at FT side....255
B.2.1 CC state table at FT side....255
B.2.2 CC transition procedures at FT side....256

Annex C (informative): DLC states as viewed by the LCE....258

Annex D (normative): DECT standard character sets....259

D.1 General....259

D.2 DECT standard 8-bit characters....259
D.2.1 General....259
D.2.2 Control codes....259
D.2.3 Standard IA5 codes....260
D.2.4 extended codes and escape to alternative character sets....260

D.3 DECT standard 4-bit characters....261

Annex E (normative): Default coding of <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> information elements for basic speech....262

Annex F (normative): Broadcast attributes coding....263

F.1 Higher Layer Capabilities....263

F.2 Extended Higher Layer Capabilities....263

Annex G (normative): Use of <<IWU-PACKET>> and <<IWU-TO-IWU>> information elements....264

G.1 General....264

G.2 Sending of <<IWU-PACKET>> elements....264
G.2.1 CC and MM use of <<IWU-PACKET>>....264
G.2.2 COMS and CLMS use of <<IWU-PACKET>>....264
G.2.3 Rejection of <<IWU-PACKET>> elements....264

G.3 Use of <<IWU-TO-IWU>> elements....264
G.3.1 Sending of <<IWU-TO-IWU>> elements....264
G.3.2 Rejection of <<IWU-TO-IWU>> elements....265

Annex H (normative): Transaction identifier flags (TIF) assignment in MM procedures....266

H.1 General....266

H.2 Nested procedures....266

H.3 Stand alone procedures....267
H.3.1 Location update procedure....267
H.3.2 Location registration procedure with temporary identity assignment....267
H.3.3 PT initiated cipher switching....267

H.3.4 Key allocation..... 268

Annex J (normative): Scrolling Behaviour 269

Annex K (informative): Bibliography..... 271

History 272

Blank page

Foreword

This second edition European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Annexes A, B, D, E, F, G, H, and J are normative in this ETS, and annexes C and K in this ETS are informative.

Further details of the DECT system may be found in ETR 015, ETR 043 and ETR 056.

This ETS forms part 5 of a series of 9 laying down the arrangements for the Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

Part 1: "Overview".

Part 2 "Physical layer (PHL)".

Part 3 "Medium Access Control (MAC) layer".

Part 4 "Data Link Control (DLC) layer".

Part 5: "Network (NWK) layer".

Part 6: "Identities and addressing".

Part 7: "Security features".

Part 8: "Speech coding and transmission".

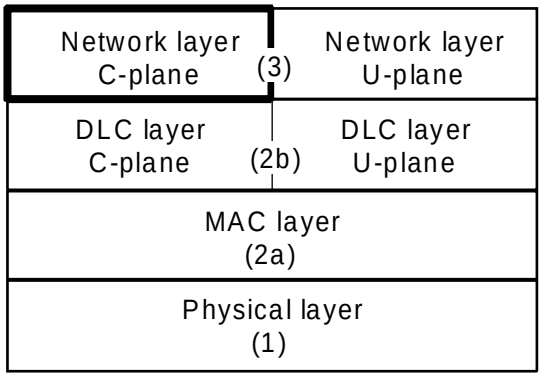
Part 9: "Public Access Profile (PAP)".

Transposition dates	
Date of adoption of this ETS:	6 September 1996
Date of latest announcement of this ETS (doa):	31 December 1996
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 June 1997
Date of withdrawal of any conflicting National Standard (dow):	30 June 1997

Blank page

1 Scope

This second edition ETS is part of the Digital Enhanced Cordless Telecommunications (DECT) Common Interface which specifies the Network (NWK) layer. The NWK layer is Part 5 of the DECT Common Interface standard and layer 3 of the DECT protocol stack.



This ETS only specifies the C-plane (control plane) of the DECT NWK layer. It contains no specification for the U-plane (user plane) because the U-plane is null for all services at the DECT NWK layer.

The C-plane contains all of the internal signalling information, and the NWK layer protocols are grouped into the following families of procedures:

- Call Control (CC);
- Supplementary Services (SS);
- Connection Oriented Message Service (COMS);
- ConnectionLess Message Service (CLMS);
- Mobility Management (MM);
- Link Control Entity (LCE).

This ETS uses the layered model principles and terminology as described in CCITT Recommendations X.200 [12] and X.210 [13].

2 Normative references

This European Telecommunication Standard (ETS) incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 175-1 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[2] ETS 300 175-2 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

[3] ETS 300 175-3 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[4] ETS 300 175-4 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".

[5] ETS 300 175-6 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[6] ETS 300 175-7 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[7] ETS 300 175-8 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech coding and transmission".

[8] ETS 300 175-9 (1996): "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 9: Public Access Profile (PAP)".

[9] I-ETS 300 176: "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Approval test specification".

[10] ETS 300 102-1 (1991): "Integrated Services Digital Network (ISDN); User-network interface layer 3 Specification for basic call control".

[11] I-ETS 300 022 (GSM Recommendation 04.08): "European digital cellular telecommunications system (phase 1); Mobile radio interface layer 3 specification".

[12] CCITT Recommendation X.200 (1988): "Reference Model of Open Systems Interconnection for CCITT applications".

[13] CCITT Recommendation X.210 (1988): "OSI layer service conventions".

[14] CCITT Recommendation T.50 (1988): "International Alphabet No. 5".

[15] ISO Publication 2022 (1986 E): "Information processing - ISO 7-bit and 8-bit coded character sets - Code extension techniques".

[16] ETS 300 133: "Paging Systems (PS); European Radio Message System (ERMES)".

[17] ETS 300 001: "Attachments to Public Switched Telephone Network (PSTN); General technical requirements for equipment connected to an analogue subscriber interface in the PSTN (candidate NET 4)".

[18] ETS 300 196-1: "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol".

[19] CCITT Recommendation Q.931 (1988): "Digital Subscriber Signalling System No.1; Network Link Layer".

[20] ETS 300 125: Integrated Services Digital Network (ISDN); User-network interface data link layer specification. Application of CCITT Recommendations Q.920/I.440 and Q.921/I.441.

[21] CCITT Recommendation T.71 (1988): "Link Access Protocol balanced (LAPB)".

[22] ISO Publication 8802-2: "Information processing systems - Local Area Networks Part 2: Logical Link Control".

[23] ISO Publication 8208: "Information processing systems - Data Communications X25 packet level protocol for data terminal equipment".

[24] ISO Publication 8348: "Information processing systems - Data Communications Network Service definition".

[25] ISO Publication 8473: "Information processing systems - Data Communications Protocol for providing the connectionless-mode network service".

[26] CCITT Recommendation X.244 (1988): "Protocol for the exchange of protocol identification during virtual call establishment on packet switched public data networks".

[27] CCITT Series V Recommendations (1988): Blue book, Fascicle VIII.1.

[28] CCITT Series X Recommendations (1988): Blue book. Fascicle VIII.

[29] CCITT Recommendation I.460 (1988): "Multiplexing, rate adaption and support of existing interfaces".

[30] ETS 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[31] ETS 300 207-1: "Integrated Services Digital Network (ISDN); Call Forwarding Busy (CFB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[32] ETS 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[33] ETS 300 092-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[34] ETS 300 093-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[35] ETS 300 097-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[36] ETS 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[37] ETS 300 359-1: "Integrated Services Digital Network (ISDN); Completion of Calls to Busy Subscriber (CCBS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[38] ETS 300 210-1: "Integrated Services Digital Network (ISDN); Freephone (FPH) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[39] ETS 300 182-1: "Integrated Services Digital Network (ISDN); Advice of Charge (AOC) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[40] ETS 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[41] ETS 300 055-1: "Integrated Services Digital Network (ISDN); Terminal Portability (TP) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[42] ETS 300 058-1: "Integrated Services Digital Network (ISDN); Call Waiting (CW) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[43] ETS 300 064-1: "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[44] ETS 300 052-1: "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[45] ETS 300 138-1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[46] ETS 300 369-1: "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[47] ETS 300 185-1: "Integrated Services Digital Network (ISDN); Conference Call add-on (CONF) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol". Part 1: Protocol Specification.

[48] ETS 300 141-1: "Integrated Services Digital Network (ISDN); Call Hold (HOLD) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

[49] ETS 300 188-1: "Integrated Services Digital Network (ISDN); Three Party (3PTY) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol". Part 1: Protocol Specification.

[50] CCITT Recommendation E.182: "Application of tones and recorded announcements in telephone services".

[51] I-ETS 300 021 (GSM 04.06): "European digital telecommunications system (phase 1); Mobile Station - Base Station System (MS-BSS) interface data link specification (GSM 04.06)".

[52] CCITT Recommendation X.25 (1988): "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[53] CCITT Recommendation T.70 (1988): "Network - independent basic transport service for telematic services".

[54] ISO Publication 1745 (1975): "Information processing - basic mode control procedures for data communication systems".

[55] ISO Publication 8859-1 (1987): "Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet N°1."

[56] ETS 300 755: ”Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT);Data Services Profile (DSP); Multimedia Messaging Service (MMS) with specific provision for facsimile services; (Service type F, class 2)”.

[57] ETS 300 757: ”Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Low rate messaging service; (Service type E, class 2)”.

[58] ETS 300 651: “Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Generic data link service; Service type C, class 2”.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply:

attach: See ETS 300 175-1 [1].

authentication of PT: The process whereby a DECT PT is positively verified to be a legitimate user of a particular FP

authentication of FT: The process whereby the identity of an FT is verified to a DECT PT.

authentication of user: The process whereby a DECT user is positively verified to be a legitimate user of a particular FP

NOTE 2: Authentication is generally performed at call set-up, but may also be done at any other time (e.g. during a call).

bearer service: See ETS 300 175-1 [1].

C-plane: See ETS 300 175-1 [1].

call: See ETS 300 175-1 [1].

Cordless Radio Fixed Part (CRFP): See ETS 300 175-1 [1].

DECT Network (DNW): See ETS 300 175-1 [1].

double duplex bearer : See ETS 300 175-1 [1].

End System (ES): See ETS 300 175-1 [1].

external handover: See ETS 300 175-1 [1].

Fixed Part (DECT Fixed Part) (FP): See ETS 300 175-1 [1].

Fixed radio Termination (FT): See ETS 300 175-1 [1].

geographically unique: See ETS 300 175-1 [1].

Global Network (GNW): See ETS 300 175-1 [1].

globally unique identity: See ETS 300 175-1 [1].

handover: See ETS 300 175-1 [1].

incoming call: See ETS 300 175-1 [1].

inter-cell handover: See ETS 300 175-1 [1].

internal call: A call between 2 users that does not make use of the local network resources.

internal handover: See ETS 300 175-1 [1].

interoperability: See ETS 300 175-1 [1].

interoperator roaming: See ETS 300 175-1 [1].

Interworking Unit (IWU): See ETS 300 175-1 [1].

intracell handover: See ETS 300 175-1 [1].

intraoperator roaming: See ETS 300 175-1 [1].

Local Network (LNW): See ETS 300 175-1 [1].

locally unique identity: See ETS 300 175-1 [1].

location area: See ETS 300 175-1 [1].

location registration: See ETS 300 175-1 [1].

Lower Layer Management Entity (LLME): See ETS 300 175-1 [1].

MAC connection (connection): See ETS 300 175-1 [1].

outgoing call: See ETS 300 175-1 [1].

paging: See ETS 300 175-1 [1].

paging area: See ETS 300 175-1 [1].

Portable Application (PA): See ETS 300 175-1 [1].

Portable Part (DECT Portable Part) (PP): See ETS 300 175-1 [1].

Portable radio Termination (PT): See ETS 300 175-1 [1].

Public Access Profile (PAP): See ETS 300 175-1 [1].

radio end point: See ETS 300 175-1 [1].

Radio Fixed Part (RFP): See ETS 300 175-1 [1].

registration: See ETS 300 175-1 [1].

Repeater Part (REP): See ETS 300 175-1 [1].

roaming: See ETS 300 175-1 [1].

roaming service: See ETS 300 175-1 [1].

segment: See ETS 300 175-1 [1].

segmentation: See ETS 300 175-1 [1].

service provider (telecommunications service provider): See ETS 300 175-1 [1].

sequencing (sequence numbering): See ETS 300 175-1 [1].

service call: A call initiated by a DECT PT for entering of FT related service and adjustment procedures in a transparent way.

subscriber (customer): See ETS 300 175-1 [1].

subscription registration: See ETS 300 175-1 [1].

Supplementary Service (SS): See ETS 300 175-1 [1].

teleservice: See ETS 300 175-1 [1].

TPUI domain: See ETS 300 175-1 [1].

U-plane: See ETS 300 175-1 [1].

user (of a telecommunication network): See ETS 300 175-1 [1].

Wireless Relay Station (WRS): See ETS 300 175-1 [1].

3.2 Abbreviations

For the purposes of this ETS the following abbreviations apply.

AC	Authentication Code
ACK	ACKnowledgement
ADPCM	Adaptive Differential Pulse Code Modulation
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity
ARQ	Automatic Repeat reQuest
BCD	Binary Coded Decimal
CBI	Collective Broadcast Identifier
CC	Call Control
CCITT	(the) International Telegraph and Telephone Consultative Committee
CI	Common Interface (standard)
CISS	Call Independent Supplementary Services
CK	Cipher Key
CODEC	COder-DECoder
CLMS	ConnectionLess Message Service
COMS	Connection Oriented Message Service
CRC	Cyclic Redundancy Check
CRFP	Cordless Radio Fixed Part
CRSS	Call Related Supplementary Services
CSPDN	Circuit Switched Public Data Network
C-Plane	Control Plane
C/L	ConnectionLess mode
C/O	Connection Oriented mode
DAM	DECT Authentication Module
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DLC	Data Link Control
DLEI	Data Link Endpoint Identifier (DLC layer)
DNW	DECT Network
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DTMF	Dual Tone Multi-Frequency

ES	End System
FP	Fixed Part
FT	Fixed radio Termination
HDB	Home Data Base
IA5	International Alphabet No.5 as defined by CCITT
IFEI	International Fixed Equipment Identity
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
ISDN	Integrated Services Digital Network
IWU	InterWorking Unit
K	authentication Key
KS	PP authentication Session Key
KS'	FP authentication Session Key
KSG	Key Stream Generator
KSS	Key Stream Segment
LAPC	a DLC layer C-plane protocol entity
LAN	Local Area Network
LCE	Link Control Entity
LCN	Logical Connection Number
LLME	Lower Layer Management Entity
LLN	Logical Link Number
LRMS	Low Rate Messaging Service
LSB	Least Significant Bit
MAC	Medium Access Control
MM	Mobility Management
MMS	Multimedia Messaging Service
MSB	Most Significant Bit
NLR	No Link Required
NWK	NetworK
PAP	Public Access Profile
PARI	Primary Access Rights Identity
PARK	Portable Access Rights Key
PBX(PABX)	Private (Automatic) Branch eXchange
PLI	Park Length Indicator
PMID	Portable part MAC IDentity (MAC layer)
PP	Portable Part
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
PT	Portable radio Termination
PUN	Portable User Number
PUT	Portable User Type
RAND-F	a RANdom challenge issued by a FT
RAND-P	a RANdom challenge issued by a PT
REP	Repeater Part
RES1	a RESponse calculated by a PT
RES2	a RESponse calculated by a FT
REP	REpeater Part
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RS	a value used to establish authentication session keys
SAP	Service Access Point
SARI	Secondary Access Rights Identity
SCK	Static Cipher Key
SDU	Service Data Unit
SMS	Short Message Service
SS	Supplementary Services
TARI	Tertiary Access Rights Identity
TCL	Telephone Coupling Loss
TDMA	Time Division Multiple Access
TI	Transaction Identifier

TPUI	Temporary Portable User Identity
UAK	User Authentication Key
UPI	User Personal Identification
U-Plane	User Plane
VDB	Visitors Data Base
WRS	Wireless Relay Station
XRES1	an eXpected RESponse calculated by a FT
XRES2	an eXpected RESponse calculated by a PT

4 Overview of the NWK layer

The DECT NWK layer (layer 3) protocol contains the following groups of functions (see figure 1).

Link Control Entity (LCE): the establishment, operation and release of a C-plane link between the fixed termination and every active portable termination.

Call Control (CC) entity: the establishment, maintenance and release of circuit switched calls.

Call Independent Supplementary Services (CISS) entity: the support of call independent supplementary services.

Connection Oriented Message Service (COMS) entity: the support of connection-oriented messages.

ConnectionLess Message Service (CLMS) entity: the support of connectionless messages.

Mobility Management (MM) entity: the management of identities, authentication, location updating, on-air subscription and key allocation.

In addition all of these C-plane entities interface to the Lower Layer Management Entity (LLME). This provides co-ordination of the operations between different NWK layer entities and also between the NWK layer and the lower layers.

The CC procedures and messages used in this protocol are based on the layer 3 procedures and messages defined in ETS 300 102-1 [10]. Many of the alterations adopted in prI-ETS 300 022 [11] have also been adopted here.

The other groups of procedures are also based on the similar groupings as defined in prI-ETS 300 022 [11].

Neither of these source documents can serve as a detailed reference for this ETS, because DECT contains many differences. These include:

a) the LCE, that provides a co-ordinated use of the layer 2 resources, including management of the broadcast services;

b) the advanced data capabilities of DECT, that include the capability for asymmetric calls and for multiple instances of a call.

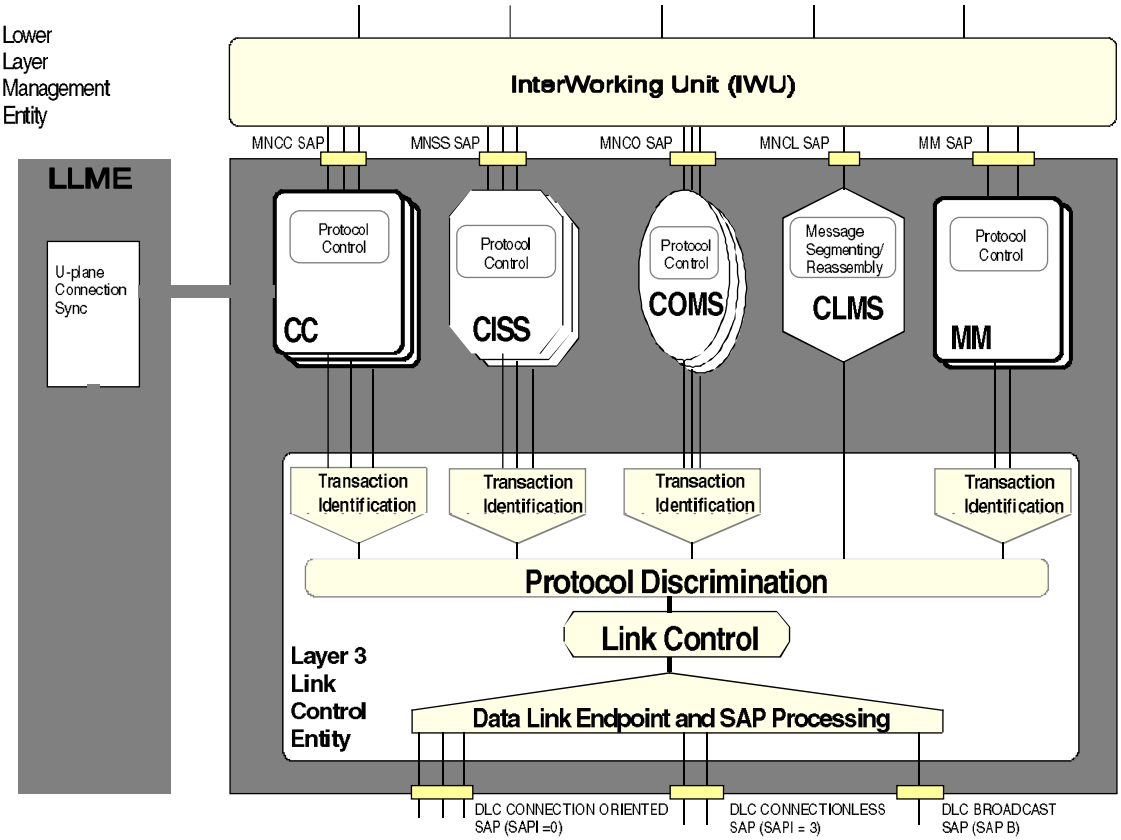
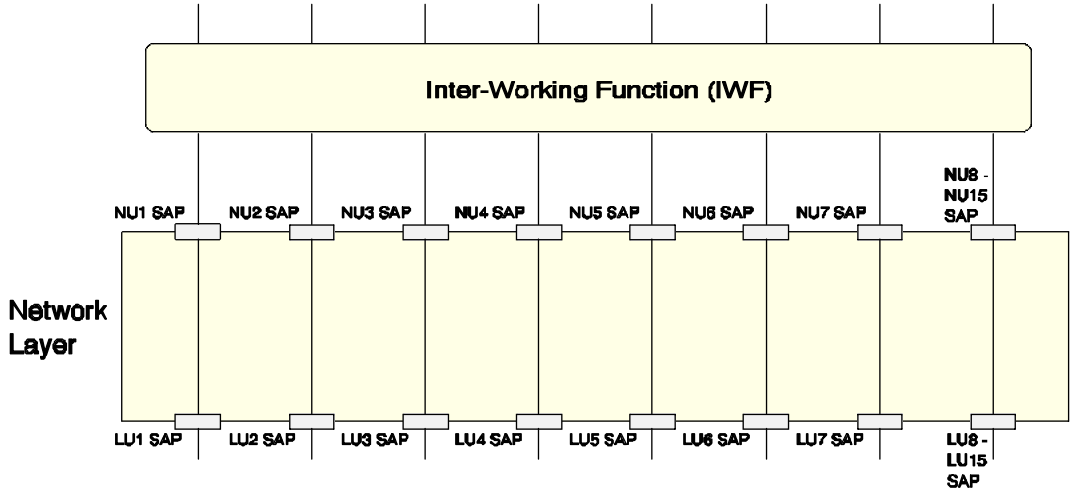


Figure 1: C-Plane model



The U-Plane is completely null at NWK Layer

Figure 2: U-Plane model

5 Overview of procedures

5.1 General

Each of the functional groupings (each entity) defined in clause 4 are described separately, and have its own set of procedures and messages.

This clause provides a short overview of the procedures and messages for each entity. The complete descriptions of messages appear in clause 6 and the detailed procedures appear in clauses 9 to 14. In the event of any conflict, the detailed message and procedure definitions shall take precedence.

As shown in the C-plane model (see figure 1) the LCE shall provide a common foundation for all the other "higher entities". The CC, CISS, COMS, CLMS and MM are collectively described as "higher entities". The LCE shall provide a message routing service to these "higher entities", using the combination of the Data Link Control (DLC) layer DLEI and the higher entity protocol discriminator element.

This ETS only considers the provision and co-ordination of services to a single PT. The provision of services to multiple PTs by one FT shall be understood to be based on independent operation, and is not considered any further in this ETS.

Within one PT, multiple instances of the CC, CISS and COMS entities may exist but there may be only two instances of the MM and one instance of the CLMS entities as shown in figure 1.

All of the procedures are based on the exchange of messages between peer entities. This ETS uses two distinct formats of message:

- S-FORMAT messages; these messages have a similar structure to ETS 300 102-1 [10] and prI-ETS 300 022 [11];

- B-FORMAT messages; these messages are specially coded to meet the physical constraints of the broadcast service. They are not similar to ETS 300 102-1 [10] messages.

The LCE shall provide a common routing service for messages to and from the separate entities using information that is explicit in every S-FORMAT message and implicit in every B-FORMAT message.

B-FORMAT messages shall only be used by the LCE and CLMS entities.

5.2 Overview of Call Control (CC)

5.2.1 General

CC is the main service instance. It provides a set of procedures that allow the establishment, maintenance and release of circuit switched services. It also provides support for all call related signalling.

Each instance of CC is termed a "call". This shall be associated with one or more U-plane service instances by the LLME. Both the CC service and the associated U-plane service are required to provide the complete service to a user.

5.2.2 Call establishment

5.2.2.1 Call set-up

Call set-up involves the exchange of some of the following information between the originator and the responding side of the call:

- International Portable User Identity (IPUI) (or group TPUI) (portable identity);

- Access Rights Identity (ARI) (fixed identity);

- called party number;

- interworking attributes;

- call attributes:

    - C-plane attributes (NWK layer and DLC layer);

    - U-plane attributes (DLC and MAC layers).

Call set-up can be originated by either side (FT or PT).

The IWU may request the CC entity to initiate a call set-up at any time. The CC shall then submit a call set-up message to the LCE, and the LCE shall determine which link establishment procedure is necessary (i.e. direct establishment, indirect establishment or none).

This first call set-up message shall define the transaction identifier for all subsequent messages (messages related to this call), and the management of these transaction identifiers is an independent task for each side.

The call set-up message may not contain all of the set-up information. If not, the remaining information shall be submitted in subsequent call information messages.

If the requested service is acceptable, the peer CC entity shall accept the set-up and shall respond with a positive message such as set-up acknowledge. This reply, and all future replies, adopt the transaction identifier defined by the initial call set-up message.

If the set-up is unacceptable to the peer entity, it shall reply with a call release message.

5.2.2.2 Service negotiation

Service negotiation may be supported during the call establishment phase. This possibility shall be indicated in the first call set-up message. The negotiation shall involve further peer-to-peer exchanges to determine an agreed set of service attributes.

5.2.3 Call connect

The call connect procedures are used to signal that the peer-to-peer U-plane communication has been enabled. These procedures provide signalling to/from the IWUs that the U-plane exchange has started.

This final acceptance of a call by the peer entity is signalled by sending a connect message. For FT initiated calls, the FT then responds with a connect acknowledge message.

There is no guarantee of peer-to-peer U-plane establishment until this procedure has completed.

5.2.4 Call information

The call information procedures may be invoked during call establishment and also as part of an established call (i.e. during the "ACTIVE" state).

These information exchange procedures shall always be supported. Their functions include the exchange of external information (for example, between a PP application and a FP interworking unit) in a series of one or more {CC-INFO} messages. This information is handled transparently by the CC protocol.

5.2.5 Service change

The service change procedures may only be invoked as part of an established call (i.e. during the "ACTIVE" state).

These service change procedures and the related service change messages are optional and should only be supported by equipment that also supports the related LLME (control) procedures. These procedures support a restricted set of modifications to the call. Each modification shall be offered to and accepted by the peer CC before it can be initiated.

5.2.6 Call release

The call release procedure is used to release all U-plane resources and all NWK layer C-plane resources associated with one call instance. The call release procedure can be invoked in two ways:

- directly, when the call ends properly;

- indirectly, when a call timer expires.

The call release message is submitted to the LCE which decides on the exact release procedure to be used. A release confirm message then provides confirmation from the peer CC entity that the release message has been accepted.

NOTE: If any other call instances are in use to this terminal, the C-plane link will be maintained by the LCE, and only the resources associated with this one instance will be released.

5.3 Overview of Supplementary Services (SS)

5.3.1 General

SSs provide additional capabilities to be used with bearer services and teleservices.

SSs are divided into two types:

- Call Related Supplementary Services (CRSS);

- Call Independent Supplementary Services (CISS).

CRSS are explicitly associated with a single instance of a CC entity. This association requires that all CRSS information elements are contained in messages that use the transaction identifier of that CC-instance. CRSS shall only be invoked within a CC instance at any phase of a CC, (establish, information or release) and multiple CRSS may be invoked within a single call.

CISS may refer to all CC instances (e.g. "call forward on busy") or they may relate to services that are unconnected to any CC instances. The messages for a CISS are invoked independent of any CC instance and are identified by using independent transaction identifiers that are directly allocated by the CISS entity.

An example of CISS is the charging procedures:

- negotiation of account details;
- charge sharing;
- reverse charging;
- advice of charge;
- charge confirmation (electronic receipt).

Three generic protocols are defined for the control of SSs, two of which are stimulus, the third being functional. These protocols are:

- the keypad protocol;

- the feature key management protocol;

- the functional protocol.

All three protocols can be used for both CRSS and CISS.

5.3.2 Keypad protocol

The keypad protocol is based on the use of the <<“KEYPAD”>> and <<“DISPLAY”>> information elements. The <<“KEYPAD”>> information element may be included in the {CC-SETUP} and {CC-INFO} messages and in the CISS messages. The <<“DISPLAY”>> information element may be included in various messages sent by the network to the user, as defined in subclause 6.3.

This protocol applies to SSs invocation in the user-to-network direction, and the keypad codes used for the invocation of an individual SS are network dependent.

The protocol is stimulus in the sense that it does not require any knowledge about the invoked SS by the PT or FT.

5.3.3 Feature key management protocol

The feature key management protocol is based on the use of the <<FEATURE-ACTIVATE>> and <<FEATURE-INDICATE>> information elements. The <<FEATURE-ACTIVATE>> information element may be included in various basic CC messages or CISS messages as specified in subclause 6.3, in the user-to-network direction. The <<FEATURE-INDICATE>> information element may be included in various basic CC messages or CISS messages in the network-to-user direction.

This protocol typically applies to SSs operation during calls but also allows for CISS control. CISS control is accomplished by sending an {CISS-REGISTER} or {FACILITY} message which contains a <<FEATURE-ACTIVATE>> information element. The user may send a <<FEATURE-ACTIVATE>> request at any time, and the network may send a <<FEATURE-INDICATE>> information element any time.

5.3.4 Functional protocol

Two categories of procedures are defined for the functional signalling for SSs. The first category, called the separate message approach, utilises separate message types to indicate a desired function. The hold and retrieve family of messages are identified for this category.

The second category, called the common information element procedure, utilises the <<FACILITY>> information element and applies only to SSs that do not require synchronisation of resources between the user and the network. A {FACILITY}, a {CISS-REGISTER} or an existing CC message is used to carry the <<FACILITY>> information element.

Both categories are specified in a symmetrical manner and can be signalled in the network-to-user and the user-to-network directions.

The protocol is functional in the sense that it requires the knowledge of the related SS by the PT or FT supporting it. This protocol, therefore, allows for autonomous operation by the DECT network, with no user (human) intervention. The protocol does not define the man-machine-interface.

5.4 Overview of Connection Oriented Message Service (COMS)

5.4.1 General

The COMS offers a point-to-point connection oriented packet service. This service only supports packet mode calls, and offers a faster (and simpler) call establishment than the CC entity. The COMS includes the ability for rapid suspension (and resumption) of the connection, this capability is provided to allow the lower layer resources to be released during periods of inactivity (this provides a function similar to the virtual connection mode of packet communications).

5.4.2 COMS establishment

COMS call set-up involves the exchange of some of the following information between the originator and the responding side of the call:

- TPUI or IPUI portable identity;

- ARI fixed identity;

- interworking attributes;

- COMS attributes (C-plane attributes for NWK layer and DLC layer).

COMS set-up can be originated by either side (FT or PT).

The IWU can request a COMS entity to initiate a call set-up at any time. The COMS then submits a call set-up message to the LCE. The LCE then decides if any link establishment procedures are necessary (i.e. direct establishment, indirect establishment or none).

This first COMS set-up message defines the transaction identifier for all subsequent messages (messages related to this call), and the management of these transaction identifiers is an independent task for each side.

If the COMS set-up is successful, the complete set-up message is delivered to the peer COMS entity, and if the call details are acceptable the peer responds with a connect message. This reply, and all future replies, adopt the transaction identifier defined by the initial call set-up message.

If the COMS set-up is unsuccessful, the originating entity will timeout. If the set-up is unacceptable to the peer entity it shall reply with a release message.

5.4.3 Service negotiation

Service negotiation may be supported during the call establishment phase. This possibility shall be indicated in the first call set-up message. The negotiation shall involve further peer-to-peer exchanges to determine an agreed set of service attributes.

5.4.4 COMS connect

The COMS connect procedures are used to signal that the interworking-to-interworking communication (C-plane) has been enabled. These procedures provide signalling to/from the IWUs that C-plane exchange has started.

This acceptance of a COMS call is signalled by the peer entity by sending a connect message, and the initiating side responds with a connect acknowledge message. There is no guarantee of end-to-end communication until this procedure has completed.

5.4.5 COMS data transfer

Following a successful connect, one or more packets of data can be transferred. Each packet is individually acknowledged when it is successfully delivered to the peer IWU. Long packets may be segmented, and are only delivered and acknowledged if all segments are received correctly.

The COMS data transfer allows for a small number of information (packet) formats. These formats may be used in any order, and in all cases the sequence of packets shall be preserved.

5.4.6 COMS suspend and resume

These procedures are optional. They use the same (C-plane) procedures as for CC to support suspension and resumption of the lower resources.

NOTE: This service is intended to support virtual data circuits such as for CCITT Recommendation X.25 [52] and for bursty data terminals, at low to medium data rates.

5.4.7 COMS release

The COMS release procedures are used to release all C-plane resources associated with one COMS instance. The release procedure can be invoked in two ways:

- directly, when the call ends properly;

- indirectly, when a call timer expires.

The COMS release message is submitted to the LCE which decides on the exact release procedures to be used. A release confirm message then provides confirmation from the peer COMS entity that the release message has been understood.

NOTE: If any other call instances are in use to this terminal, the C-plane link will be maintained by the LCE, and only the resources associated with this one instance will be released.

5.5 Overview of ConnectionLess Message Service (CLMS)

The CLMS offers a connectionless point-to-point or point-to-multipoint service. The CLMS may offer either or both of the following service types:

- fixed length message service;

- variable length message service.

5.5.1 Fixed length message service

This service only operates in the direction FT to PT. Messages are transmitted using the DLC broadcast services, and normally this should provide a more reliable service than the variable message service (see below) because broadcast transmissions are duplicated in the lower layers.

This service allows for the transport of structured or unstructured data, up to 160 bits.

NOTE: This is intended for group paging and broadcast information such as key system information.

5.5.2 Variable length message service

This service may operate in both directions. In the general case, a connection oriented link is not available, and the message is routed over a point-to-multipoint connectionless link.

NOTE: In the event that a connection oriented link already exists to the relevant PT, then the message may be routed over that (existing) link by the LCE.

In both cases successful delivery of the message shall not be acknowledged by the peer CLMS entity.

Only one variable message transaction to each PT is allowed at any one time.

5.6 Overview of Mobility Management (MM)

5.6.1 General

The MM entity handles functions necessary for the secure provision of DECT services and supports in particular incoming calls. These functions are necessary due to the mobile nature of the DECT user and due to highly probable fraudulent attacks upon the radio interface.

MM procedures are described in seven groups:

a) identity procedures;

b) authentication procedures;

c) location procedures;

d) access rights procedures;

e) key allocation procedure;

f) parameter retrieval procedure;

g) ciphering related procedure.

These groups are briefly described in this subclause. The MM procedures themselves are described in clause 13. The management of MM procedures including the use of an MM-procedure priority list to circumvent MM-state machine deadlocks, are described in subclause 15.5.

5.6.2 Identity procedures

The identity procedures are based on the DECT identities defined in ETS 300 175-6 [5].

The identity procedures serve three purposes:

- to request a PT to provide specific identification parameters to the FT;

- to assign a TPUI and/or a network assigned identity to a PT;

- to delete a TPUI and/or a network assigned identity in a PT.

PT identities (IPUI and TPUI) have an important relationship to FT identities:

- an IPUI is paired with one or more ARIs. The IPUI is usable on any fixed network that supports one (or more) of the paired ARIs;

- a TPUI is paired with one IPUI within one location area. The TPUI is only valid on FTs belonging to the associated location area.

The identity procedures are always initiated by the FT, and any one of them may be initiated at any time, including during a CC-call, CISS-call or COMS-call. However, the procedure may be triggered by a PT initiated event.

5.6.3 Authentication procedures

Authentication procedures can be used in both directions:

- PT authentication defines the mechanism that is used to provide the authentication of a PT to an FT;

- FT authentication defines the mechanism that is used to provide the authentication of an FT to a PT;

- user authentication defines the mechanism that is used to provide the authentication of the user to an FT.

The authentication procedures serve two purposes:

- to check that the identity provided by the PT or FT is a true identity;

- to provide a new ciphering key to the PT and FT.

5.6.4 Location procedures

The location procedures are necessary for incoming call provision. They are designed to allow the FT to minimise location database accesses in the event that duplicated or redundant messages are received from a PT.

The location procedures are concerned with two levels of location:

- locating; reporting the position of the PT in terms of location areas to the FT;

- detaching (attaching); reporting to the FT that the PT is not ready (ready) to receive calls.

Locating is a higher level than attaching. This means that a location registration can implicitly be regarded as an automatic attachment. Location registration without changing the location area is referred to as attaching, no separate message is defined.

NOTE: "Delocation" (defined as deletion of an entry in the external location database) is not a specified function for the air interface. The decision to "delocate" is specific to each FT. It should be possible to detach without "delocating".

Three location procedures are defined:

- location registration procedure for locating and attaching;

- detach procedure for detaching;

- location update procedure which is used by the FT to request from the PT to perform location updating, e.g. after location areas have been rearranged.

5.6.5 Access rights procedures

Two procedures are defined, one for obtaining the access rights and one for terminating the access rights.

The procedure for obtaining the access rights is used to load down the IPUI and the Portable Access Rights Key (PARK) to the PT.

Other service specific information may also be transferred during this procedure. This is stored at the handset for later retrieval by the system.

NOTE: This procedure does not transfer an authentication key. If a first key had been put in (e.g. an Authentication Code (AC)), then the key allocation procedure can be used to replace this first key by an other key (e.g. the User Authentication Key (UAK)).

The procedure for terminating the access rights is used to remove a specific IPUI and all information which is related to this IPUI from the PT and from the FT or to remove a PARK from the PT and the related access rights information from the FT.

5.6.6 Key allocation procedure

This procedure can be used to replace an Authentication Code (AC) by an UAK. For calculating the UAK a DECT Standard Authentication Algorithm (DSAA) is used. The AC that is used in this procedure should be as long as possible and should have at least 32 bits, but better 64 bits or more. After a successful key allocation, the used AC shall be erased.

5.6.7 Parameter retrieval procedure

This procedure uses the existing link between the PT and the FT to obtain additional information, which could be necessary to perform external handover to an other FT. In the case of an external handover, setting up a link to the new FT is done via the CC entity.

5.6.8 Ciphering related procedure

This procedure is used to define the cipher parameters and to engage or disengage ciphering of a connection.

5.7 Overview of Link Control Entity (LCE)

5.7.1 General

The LCE is the lowest entity in the NWK layer. It performs the following tasks:

a) supervision of lower layer link states for every data link endpoint in the C-plane;

b) downlink routing - routing of messages to different C-plane data link endpoints (instances of S-SAP);

c) uplink routing - routing of messages from different data link endpoints based on the protocol discriminator and the transaction identifier;

d) queuing of messages to all C-plane data link endpoints;

e) creation and management of {LCE-REQUEST-PAGE} messages, and submitting them to the B-SAP;

f) queuing and submission of other messages to the B-SAP;

g) assignment of new Data Link Endpoint Identifiers (DLEI) when a successful link establishment is indicated;

h) assignment of new NWL layer instances to existing data link endpoints;

i) reporting data link failures to all NWK layer instances that are using that link.

The link states as observed by the LCE are shown in annex C. These states are a combination of the DLC internal states plus the underlying connection. For example, the "LINK ESTABLISHED" state means that the DLC LAPC is established and the associated MAC connection is established.

5.7.2 Data Link Endpoint Identifier (DLEI)

Every message submitted to, or originated by, the LCE shall be routed to its correct DLEI. The necessary mapping should be based on two parameters:

- the IPUI or the assigned individual TPUI;

- the originating entity (CC, CISS, COMS, CLMS, MM or LCE), plus any associated transaction identifier.

This mapping should be defined as part of data link establishment.

NOTE 1: For group calls, there may be several alternative mappings (alternative acceptable values of IPUI). The link establishment procedures always creates a single mapping, but the selection procedures are not defined in this ETS.

NOTE 2: There is no DLEI defined for broadcast purposes. A broadcast DLEI is not required because broadcasts are clearly distinguished at the DLC and MAC layers by the use of a dedicated broadcast channel.

5.7.3 Data link establishment

A data link is only established in response to an explicit request from a higher entity. The necessary actions are slightly different at the FT and the PT.

The LCE shall request a suitable DLEI from the LLME in response to this request, using both

- the IPUI or the assigned individual TPUI;

- the originating entity (CC, CISS, COMS, CLMS, MM or LCE), plus any associated transaction identifier.

Having obtained a DLEI, the LCE procedure shall depend on the state of that link:

a) if the link is established, no action is required and any messages shall be immediately submitted using DL_DATA-req primitives;

b) if the link is not established, the LCE must determine the appropriate method of establishment. Two methods are defined:

   - direct establishment, for all PT initiations and for FT initiations where "fast DLC set-up" is supported;

   - indirect establishment, for all other cases, including failure of FT initiated "fast DLC set-up".

Indirect establishment uses the request paging procedures described in subclause 5.7.8.

If Class B operation is requested, and there is not an established Class B link, the LCE shall automatically attempt to establish (or resume) Class B operation on one link. If Class B establishment fails, but Class A operation is offered, the LCE shall proceed with Class A operation and shall notify the initiating entity.

NOTE: Refer to ETS 300 175-4 [4] for details of Class A and Class B link operation.

c) if link establishment fails, the LCE shall discard the message and shall notify the initiating entity of this failure.

Any messages from higher entities shall be queued by the LCE during link establishment, as defined in subclause 5.7.7.

5.7.4 Data link re-establishment

If the link associated with any active DLEI fails, the LCE shall notify all associated higher entities of this failure. Link re-establishment shall only be attempted in response to a request from one of these entities.

Link re-establishment may be requested at any time by one of the higher entities. The LCE shall immediately attempt to re-establish the link, and shall notify all higher entities of this event.

Any messages from higher entities shall be queued by the LCE during link re-establishment, as defined in subclause 5.7.7.

5.7.5 Data link release

Under normal conditions, a data link is only released if all higher entities associated with that link have been released.

The link may be maintained for a short period after the release of the last call.

5.7.6 Data link suspend and resume

The LCE controls the suspension and resumption of each C-plane data link in response to demands from the higher entities. A link suspension shall only be requested by a CC or COMS entity, and the link shall only be suspended if no other higher entities are active. The link shall be immediately resumed if a link is requested by any of the higher entities.

During the suspend and resume procedures, any messages from higher entities shall be queued by the LCE, as defined in subclause 5.7.7. The existence of queued messages for a suspended link should cause immediate resumption of that link.

5.7.7 Queuing of messages

Messages are only queued during link establishment, link re-establishment and during link suspend and resume procedures. Once a link has been established, messages should be sent as quickly as possible.

NOTE: Following successful link establishment, messages are not queued by the LCE, but they may still be queued by the DLC layer link entity (see ETS 300 175-4 [4]).

5.7.8 Request paging

Request paging is used to communicate to a portable termination that the DECT fixed termination wants to establish a link to it, wants to initiate a connectionless message service or wants a particular set of PPs to initiate ringing. The {LCE-REQUEST-PAGE} message contains very limited information (the main element is simply a shortened identity of the PT), a complete call establishment message is only exchanged after the link has been established.

NOTE: The {LCE-REQUEST-PAGE} message is a B-FORMAT message. Refer to subclause 8.2

In case of request for a link, upon receipt of a {LCE-REQUEST-PAGE} message, the LCE of the addressed PT initiates an immediate link establishment. The first message shall be a {LCE-PAGE-RESPONSE} message. This distinguishes it from an outgoing call PT initiated link establishment. This message shall contain the full IPUI of the responding PT.

A FT shall only initiate one of these procedures to any given IPUI (or TPUI) at any one time, and the LCE is required to maintain a record of outstanding requests, and to report their success or failure to the correct originating entity (CC, CISS, COMS or MM).

This procedure should not be used when a suitable link already exists to the chosen IPUI (or TPUI), and it is the responsibility of the LLME to determine if such a link exists.

In the case of request for ringing on receipt of the {LCE-REQUEST-PAGE} message indicating "ringing" the requested PPs shall initiate ringing without link establishment. Such shall be initiated upon following answer from one of the ringing PPs. Three types of ringing are considered, “Group” when only PPs that have been assigned the received connectionless group TPUI shall ring, "Collective" when all subscribed PPs shall ring and "Group Mask" when only PPs with assigned connectionless group TPUI that matches the received group mask shall ring.

6 Message functional definitions

6.1 Overview of message structures

6.1.1 Messages

Messages are the highest level of information grouping defined in the NWK layer. Each message contains a variable set of information relating to one (NWK layer) transaction of one entity. The relevant entity and the transaction number are identified by special elements that appear in every message.

Messages are divided into groups according to the originating entities (CC, CISS, COMS, CLMS, MM or LCE). A summary of all the possible messages for each group appears in subclause 6.2. These summaries includes both S-FORMAT messages and B-FORMAT messages.

The subclauses 6.3 and 6.4 list the allowed functional contents of each message. Each message is defined by a table that lists the mandatory and optional information elements for that message.

The functional contents for each S-FORMAT message are listed in subclause 6.3, and clause 7 contains coding details of the individual information elements for the S-FORMAT messages.

The functional contents for each B-FORMAT message are listed in subclause 6.4, and clause 8 contains coding details of the individual information elements for the B-FORMAT messages.

6.1.2 Information elements

Information elements are a lower level of information grouping, where the information usually relates to one specific aspect of the transaction. Elements are defined in a general way that allows elements to be (re)used within different messages. DECT defines three types of information elements:

- DECT specific information elements;

- DECT standard information elements;

- DECT transparent information elements.

DECT specific information elements are those elements that relate exclusively to the (internal) operation of the DECT protocol. These may refer to any or all of the layers.

DECT standard information elements are those elements that relate to the interaction of the DECT protocol with the IWUs and other higher layers. DECT standard information elements provide a standard mechanism for interoperation of PTs and FTs.

There are two DECT transparent information elements, <<IWU-TO-IWU>> and <<IWU-PACKET>>, corresponding to two possible structures of external information. These information elements are provided as a general mechanism for transporting external information that is of no (internal) relevance to the DECT protocol entities.

6.2 Message summaries

6.2.1 Summary of CC messages

Table 1: CC message summary (includes call related supplementary services)

	Dir.	Subclause
Call establishment messages		
{CC-SETUP}	Both	6.3.2.1
{CC-INFO}	Both	6.3.2.2
{CC-SETUP-ACK}	F=>P	6.3.2.3
{CC-CALL-PROC}	F=>P	6.3.2.4
{CC-ALERTING}	Both	6.3.2.5
{CC-NOTIFY}	F=>P	6.3.2.13
{CC-CONNECT}	Both	6.3.2.6
{CC-CONNECT-ACK}	Both	6.3.2.7
Call information phase messages		
{CC-INFO}	Both	6.3.2.2
{CC-SERVICE-CHANGE}	Both	6.3.2.10
{CC-SERVICE-ACCEPT}	Both	6.3.2.11
{CC-SERVICE-REJECT}	Both	6.3.2.12
{IWU-INFO}	Both	6.3.2.14
Call related supplementary services		
{FACILITY}	Both	6.3.3.1
{HOLD}	Both	6.3.3.2
{HOLD-ACK}	Both	6.3.3.3
{HOLD-REJECT}	Both	6.3.3.4
{RETRIEVE}	Both	6.3.3.5
{RETRIEVE-ACK}	Both	6.3.3.6
{RETRIEVE-REJECT}	Both	6.3.3.7
Call release messages		
{CC-INFO}	Both	6.3.2.2
{CC-RELEASE}	Both	6.3.2.8
{CC-RELEASE-COM}	Both	6.3.2.9

6.2.2 Summary of CISS messages

Table 2: CISS message summary

	Dir.	Subclause
CISS establishment messages		
{CISS-REGISTER}	Both	6.3.3.8
CISS information phase messages		
{FACILITY}	Both	6.3.3.1
CISS release messages		
{CISS-RELEASE-COM}	Both	6.3.3.9

6.2.3 Summary of COMS messages

Table 3: COMS message summary

	Dir.	Subclause
COMS establishment messages		
{COMS-SETUP}	Both	6.3.4.1
{COMS-CONNECT}	Both	6.3.4.4
{COMS-NOFIFY}	F=>P	6.3.4.7
COMS information phase messages		
{COMS-INFO}	Both	6.3.4.2
{COMS-ACK}	Both	6.3.4.3
COMS release messages		
{COMS-RELEASE}	Both	6.3.4.5
{COMS-RELEASE-COM}	Both	6.3.4.6

6.2.4 Summary of CLMS messages

Table 4: CLMS message summary

	Dir.	Subclause
CLMS information phase messages		
{CLMS-VARIABLE}	Both	6.3.5.1
{CLMS-FIXED}	F=>P	6.4.3

NOTE: {CLMS-FIXED} is a B-FORMAT message.

6.2.5 Summary of MM messages

Table 5: MM message summary

	Dir.	Subclause
Identity messages		
{TEMPORARY-IDENTITY-ASSIGN}	F=>P	6.3.6.24
{TEMPORARY-IDENTITY-ASSIGN-ACK}	P=>F	6.3.6.25
{TEMPORARY-IDENTITY-ASSIGN-REJ}	P=>F	6.3.6.26
{IDENTITY-REQUEST}	F=>P	6.3.6.15
{IDENTITY-REPLY}	P=>F	6.3.6.14
Authentication messages		
{AUTHENTICATION-REQUEST}	Both	6.3.6.9
{AUTHENTICATION-REPLY}	Both	6.3.6.8
{AUTHENTICATION-REJECT}	Both	6.3.6.7
Location messages		
{LOCATE-REQUEST}	P=>F	6.3.6.19
{LOCATE-ACCEPT}	F=>P	6.3.6.17
{LOCATE-REJECT}	F=>P	6.3.6.18
{DETACH}	P=>F	6.3.6.13
Access rights messages		
{ACCESS-RIGHTS-REQUEST}	P=>F	6.3.6.3
{ACCESS-RIGHTS-ACCEPT}	F=>P	6.3.6.1
{ACCESS-RIGHTS-REJECT}	F=>P	6.3.6.2
{ACCESS-RIGHTS-TERMINATE-REQUEST}	Both	6.3.6.6
{ACCESS-RIGHTS-TERMINATE-ACCEPT}	Both	6.3.6.4
{ACCESS-RIGHTS-TERMINATE-REJECT}	Both	6.3.6.5
Key allocation messages		
{KEY-ALLOCATE}	F=>P	6.3.6.16
Parameter retrieval messages		
{MM-INFO-SUGGEST}	F=>P	6.3.6.23
{MM-INFO-REQUEST}	P=>F	6.3.6.22
{MM-INFO-ACCEPT}	F=>P	6.3.6.20
{MM-INFO-REJECT}	F=>P	6.3.6.21
Ciphering messages		
{CIPHER-SUGGEST}	P=>F	6.3.6.12
{CIPHER-REQUEST}	F=>P	6.3.6.11
{CIPHER-REJECT}	Both	6.3.6.10

6.2.6 Summary of LCE messages

Table 6: LCE message summary

	Dir.	Subclause
LCE establishment messages		
{LCE-REQUEST-PAGE}	F=>P	6.4.2
{LCE-PAGE-RESPONSE}	P=>F	6.3.7.1
{LCE-PAGE-REJECT}	F=>P	6.3.7.2

NOTE: {LCE-REQUEST-PAGE} is a B-FORMAT message.

6.3 S-FORMAT message functional contents

6.3.1 S-FORMAT message overview

Each of the S-FORMAT message definitions includes:

a) a brief description of the message direction and use;

b) a table listing all the possible information elements that can be contained in the message. For each element, the table defines:

- the name of the information element;
- a reference to the subclause where the information element is defined;
- whether the inclusion of the information element is Mandatory (M) or Optional (O) or Not allowed (N). These inclusion rules are defined separately for each message direction. If the message is only specified for one direction, the elements are marked not applicable (-) for the other direction;
- the range of possible lengths of the information element, where "*" means the maximum length is undefined.

c) further explanatory notes as required.

The information elements are always listed in their order of appearance, this order is mandatory for all instances of the message. Receiver implementations shall take account of the possibility that further information elements may be inserted in the message tables in future editions of this standard.

6.3.2 CC-messages

6.3.2.1 {CC-SETUP}

This message is sent to initiate call establishment.

Message Type	Format	Directions
{CC-SETUP}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Portable identity		7.7.30	M	M	5-20
Fixed identity	11	7.7.18	M	M	5-20
NWK assigned identity		7.7.28	N	O	5-20
Basic service	1	7.6.4	M	M	2
Repeat Indicator	3	7.6.3	O	O	1
IWU attributes	1	7.7.21	M/N	M/N	5-12
Repeat Indicator	2	7.6.3	O	O	1
Call attributes	1,2	7.7.5	O	O	6-8
Repeat Indicator	3	7.6.3	O	O	1
Connection attributes	3	7.7.11	O	O	6-11
Cipher info		7.7.10	O	O	4-5
Connection identity		7.7.12	O	O	3-*
Repeat indicator	12	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
Repeat indicator	12	7.6.3	O	N	1
Progress Indicator		7.7.31	O	N	4
"Display"		7.5.5	O	N	2-*
"Keypad"	10	7.5.5	N	O	2-*
Signal	5	7.6.8	O	N	2
Feature Activate		7.7.16	N	O	3-4
Feature Indicate		7.7.17	O	N	4-*
Network parameter	8	7.7.29	O	O	4-*
Ext h/o indicator		7.7.51	O	N	4-*
Terminal capability		7.7.41	N	O	3-*
End-to-end compatib.	9	7.7.14	O	O	3-6
Rate parameters	7	7.7.33	O	O	5-7
Transit Delay	6	7.7.42	O	O	4
Window size	6	7.7.43	O	O	4
Calling Party Number		7.7.9	O	O	5-*
Called Party Number	10	7.7.7	O	O	4-*
Called Party Subaddr		7.7.8	O	O	4-*
Sending Complete	4	7.6.2	O	O	1
Repeat indicator	12	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<IWU-ATTRIBUTES>> is mandatory if the <<BASIC-SERVICE>> element indicates "other". Neither <<IWU-ATTRIBUTES>> nor <<CALL-ATTRIBUTES>> is allowed if the <<BASIC-SERVICE>> element indicates "default attributes".

NOTE 2: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<CALL-ATTRIBUTES>> indicating "prioritised list" for negotiation. Up to three versions of the <<CALL-ATTRIBUTES>> element may then follow. See subclause 15.2.

NOTE 3: If more than one connection is required, a list of <<CONNECTION-ATTRIBUTES>> and or <<IWU-ATTRIBUTES>> may be included preceded by the <<REPEAT-INDICATOR>> element indicating "non-prioritised list". If the <<CONNECTION-ATTRIBUTES>> or <<IWU-ATTRIBUTES>> elements are omitted, the attributes are indirectly defined by reference to the connection(s) indicated by the <<CONNECTION-IDENTITY>> element.

NOTE 4: Included if the PT or the FT optionally indicates that all information necessary for call establishment is included in the {CC-SETUP} message.

NOTE 5: Optionally included if the FT optionally provides additional information describing tones.

NOTE 6: Optionally included for data services whenever these parameters are applicable.

NOTE 7: Mandatory for call set-up of a rate adaption service (see ETS 300 175-4 [4]).

NOTE 8: Included only as part of external handover.

NOTE 9: Mandatory for services using LU6 (V.110/X.30 rate adaption).

NOTE 10: Called party number information may only be conveyed in the <<CALLED-PARTY-NUMBER>> element. The <<"KEYPAD">> element may only be included to convey other call establishment information.

NOTE 11: This information element may contain zero length contents if the setup message is used in an ARI-D (GSM) environment.

NOTE 12: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.2 {CC-INFO}

This message is used to transfer additional information between FT and PT both during and after call establishment.

Message Type	Format	Directions
{CC-INFO}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Location area	4	7.7.25	N	O	3-*
NWK assigned identity	4	7.7.28	N	O	5-20
Repeat indicator	5	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
Repeat indicator	5	7.6.3	O	N	1
Progress Indicator		7.7.31	O	N	4
"Display"		7.5.5	O	N	2-*
"Keypad"	1	7.5.5	N	O	2-*
Signal		7.6.8	O	N	2
Feature Activate		7.7.16	N	O	3-4
Feature Indicate		7.7.17	O	N	4-*
Network parameter	4	7.7.29	O	O	4-*
Ext h/o indicator		7.7.51	O	N	4-*
Called Party Number	1,3	7.7.7	O	O	4-*
Called Party Subaddr	3	7.7.8	O	O	4-*
Sending Complete	2	7.6.2	O	O	1
Test Hook Control		7.6.10	O	N	2
Repeat indicator	5	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The message may contain either the <<CALLED-PARTY-NUMBER>> element or the <<"KEYPAD">> element, but not both.

NOTE 2: Included if the PT optionally indicates completion of "OVERLAP SENDING" to the FT (or if the FT optionally indicates completion of "OVERLAP RECEIVING" to the PT).

NOTE 3: Address elements are only included in messages sent in the "OVERLAP SENDING" state.

NOTE 4: Included if requested as part of external handover.

NOTE 5: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.3 {CC-SETUP-ACK}

This message is sent to indicate that call establishment has been indicated, but additional information may be required.

Message Type	Format	Directions
{CC-SETUP-ACK}	S	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	-	½
Transaction Identifier		7.3	M	-	½
Message Type		7.4	M	-	1
Info type	3	7.7.20	O	-	3-*
Portable identity		7.7.30	O	-	5-20
Fixed identity		7.7.18	O	-	5-20
Location area		7.7.25	O	-	3-*
IWU attributes		7.7.21	O	-	5-12
Call Attributes	4	7.7.5	O	-	6-11
Connection attributes		7.7.11	O	-	3-*
Connection identity		7.7.12	O	-	3-*
Repeat indicator	7	7.6.3	O	-	1
Facility		7.7.15	O	-	2-*
Repeat indicator	7	7.6.3	O	-	1
Progress Indicator		7.7.31	O	-	4
"Display"		7.5.5	O	-	2-*
Signal	2	7.6.8	O	-	2
Feature Indicate		7.7.17	O	-	4-*
Network parameter	8	7.7.29	O	-	4-*
Ext h/o indicator		7.7.51	O	-	4-*
Transit Delay	5	7.7.42	O	-	4
Window size	5	7.7.43	O	-	4
Delimiter request	6	7.6.2	O	-	1
Repeat indicator	7	7.6.3	O	-	1
IWU-TO-IWU		7.7.23	O	-	4-*
IWU-PACKET		7.7.22	O	-	4-*
Escape to proprietary		7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: This message may be used in the direction P=>F when using the "INCOMING CALL PROCEEDING" operations.

NOTE 2: Included if the FT optionally provides additional information describing tones.

NOTE 3: Included if additional external handover parameters are requested.

NOTE 4: Included if prioritised list negotiation is used.

NOTE 5: Included if operational parameter negotiation is used.

NOTE 6: Included by the FT to request use of the <<SENDING-COMPLETE>> element by the PT.

NOTE 7: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.4 {CC-CALL-PROC}

This message indicates that the requested (onward) connection establishment has been initiated by the fixed side interworking unit.

Message Type	Format	Directions
{CC-CALL-PROC}	S	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	-	½
Transaction Identifier		7.3	M	-	½
Message Type		7.4	M	-	1
IWU attributes		7.7.21	O	-	5-12
Call Attributes	3	7.7.5	O	-	6-11
Connection attributes		7.7.11	O	-	3-*
Connection identity		7.7.12	O	-	3-*
Repeat indicator	5	7.6.3	O	-	1
Facility		7.7.15	O	-	2-*
Repeat indicator	5	7.6.3	O	-	1
Progress indicator		7.7.31	O	-	4
"Display"		7.5.5	O	-	2-*
Signal	2	7.6.8	O	-	2
Feature Indicate		7.7.17	O	-	4-*
Transit Delay	4	7.7.42	O	-	4
Window size	4	7.7.43	O	-	4
Repeat indicator	5	7.6.3	O	-	1
IWU-TO-IWU		7.7.23	O	-	4-*
IWU-PACKET		7.7.22	O	-	4-*
Escape to proprietary		7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: This message may be used in the direction P=>F when using the "INCOMING CALL PROCEEDING" operations.

NOTE 2: Included if the FT optionally provides additional information describing tones.

NOTE 3: Included if prioritised list negotiation is used.

NOTE 4: Included if operational parameter negotiation is used.

NOTE 5: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.5 {CC-ALERTING}

This message is used to indicate that an initiation of alerting has been reported to the sending entity.

Message Type	Format	Directions
{CC-ALERTING}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
IWU attributes		7.7.21	N	O	5-12
Call Attributes	2	7.7.5	O	O	6-11
Connection attributes		7.7.11	O	O	3-*
Connection identity		7.7.12	O	O	3-*
Repeat indicator	4	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
Repeat indicator	4	7.6.3	O	N	1
Progress Indicator		7.7.31	O	N	4
"Display"		7.5.5	O	N	2-*
Signal	1	7.6.8	O	N	2
Feature Indicate		7.7.17	O	N	4-*
Terminal capability		7.7.41	N	O	3-*
Transit Delay	3	7.7.42	O	O	4
Window size	3	7.7.43	O	O	4
Repeat indicator	4	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: Included if the FT optionally provides additional information describing tones.

NOTE 2: Included if prioritised list negotiation is used.

NOTE 3: Included if operational parameter negotiation is used.

NOTE 4: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.6 {CC-CONNECT}

This message is sent by the FT to indicate completion of the connection through the DECT network, and by the PT to request such completion.

Message Type	Format	Directions
{CC-CONNECT}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
IWU attributes		7.7.21	N	O	5-12
Call Attributes	2	7.7.5	O	O	6-11
Connection attributes		7.7.11	O	O	3-*
Connection identity		7.7.12	O	O	3-*
Repeat indicator	4	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
Repeat indicator	4	7.6.3	O	N	1
Progress Indicator		7.7.31	O	N	4
"Display"		7.5.5	O	N	2-*
Signal	1	7.6.8	O	N	2
Feature Indicate		7.7.17	O	N	4-*
Network parameter	8	7.7.29	O	N	4-*
Ext h/o indicator		7.7.51	O	N	4-*
Terminal capability		7.7.41	N	O	3-*
Transit Delay	3	7.7.42	O	O	4
Window size	3	7.7.43	O	O	4
Repeat indicator	4	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: Included if the FT optionally provides additional information describing tones.

NOTE 2: Included if prioritised list negotiation is used.

NOTE 3: Included if operational parameter negotiation is used.

NOTE 4: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.7 {CC-CONNECT-ACK}

This message is sent by the FT to confirm completion of the connection through the DECT network, following a {CC-CONNECT} message requesting such completion. This message is also sent by the PT to confirm connection of the call following a {CC-CONNECT} message in an external handover procedure.

Message Type	Format	Directions
{CC-CONNECT-ACK}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
"Display"		7.5.5	O	N	2-*
Feature Indicate		7.7.17	O	N	4-*
Repeat indicator	1	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-to-IWU>> information elements indicating "non-prioritised list".

6.3.2.8 {CC-RELEASE}

This message is sent to indicate that the sending entity wishes to release the call and the call references, and to request the receiving entity to complete a corresponding release after returning a {CC-RELEASE-COM} message.

Message Type	Format	Directions
{CC-RELEASE}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Release Reason		7.6.7	O	O	2
Repeat indicator	1	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
Repeat indicator	1	7.6.3	O	O	1
Progress indicator		7.7.31	O	O	4
"Display"		7.5.5	O	N	2-*
Feature Indicate		7.7.17	O	N	4-*
Repeat indicator	1	7.6.3	O	N	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, <<IWU-to-IWU>> and <<PROGRESS INDICATOR>> information elements indicating "non-prioritised list".

6.3.2.9 {CC-RELEASE-COM}

This message indicates that the sending entity has released the call and the call reference, and the receiving entity shall release the call and call reference.

Message Type	Format	Directions
{CC-RELEASE-COM}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Release Reason		7.6.7	O	O	2
Identity type	3	7.7.19	O	N	4
Location area	3	7.7.25	O	N	3-*
IWU attributes	1	7.7.21	O	O	5-12
Repeat indicator	4	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
"Display"		7.5.5	O	N	2-*
Feature Indicate		7.7.17	O	N	4-*
Network parameter	2	7.7.29	O	N	4-*
Repeat indicator	4	7.6.3	O	O	1
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<IWU-ATTRIBUTES>> element is only included if exchanged attribute negotiation is supported. See subclause 15.2.3.

NOTE 2: Mandatory when responding to an external handover release.

NOTE 3: Optional when responding to an external handover release.

NOTE 4: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, and <<IWU-to-IWU>> information elements indicating "non-prioritised list".

6.3.2.10 {CC-SERVICE-CHANGE}

This message is used to request a service change to an existing call.

Message Type	Format	Directions
{CC-SERVICE-CHANGE}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	5-20
IWU attributes	7.7.21	O	O	5-12
Service Change Info	7.7.38	M	M	4-5
Repeat Indicator 1	7.6.3	O	O	1
Connection Attributes 1	7.7.11	M/O	M/O	6-11
Connection identity 2	7.7.12	M/O	M/O	3-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: The <<CONNECTION-ATTRIBUTES>> element is mandatory for certain service changes. See subclause 9.6. If more than one connection is affected, a list of <<CONNECTION-ATTRIBUTES>> may be included preceded by the <<REPEAT-INDICATOR>> element indicating "non-prioritised list".

NOTE 2: The <<CONNECTION-IDENTITY>> element is mandatory for certain service changes. See subclause 9.6.

6.3.2.11 {CC-SERVICE-ACCEPT}

This message is used to accept a service change to an existing call.

Message Type	Format	Directions
{CC-SERVICE-ACCEPT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
IWU attributes	7.7.21	O	O	5-12
Connection identity 1	7.7.12	O	O	3-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: The <<CONNECTION-IDENTITY>> element is mandatory for certain service changes. See subclause 9.6.4.

6.3.2.12 {CC-SERVICE-REJECT}

This message is used to reject a service change to an existing call.

Message Type	Format	Directions
{CC-SERVICE-REJECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
IWU attributes	7.7.21	O	O	5-12
Connection attributes	7.7.11	O	O	6-11
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory.

6.3.2.13 {CC-NOTIFY}

This message is used to exchange internal protocol information without causing a state change.

Message Type	Format	Directions
{CC-NOTIFY}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.2.14 {IWU-INFO}

This message is used to exchange (or reject) external protocol information in a transparent manner.

Message Type	Format	Directions
{IWU-INFO}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Portable identity	7.7.30	O	O	5-20
MMS Generic Header	7.7.47	O	O	-*
MMS Object Header	7.7.48	O	O	-*
Repeat Indicator 1	7.6.3	O	O	1
MMS Extended Header	7.7.49	O	O	-*
Repeat Indicator 1	7.6.3	O	O	1
Time-Date	7.7.50	O	O	6-10
Repeat Indicator 1	7.6.3	O	O	1
Calling Party Number	7.7.9	O	O	5-*
Repeat Indicator 1	7.6.3	O	O	1
Called Party Number	7.7.7	O	O	4-*
Called Party Subaddr	7.7.8	O	O	4-*
Segmented info	7.7.37	O	O	4
Alphanumeric	7.7.3	O	O	4-*
Repeat Indicator 1	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<MMS EXTENDED HEADER>>, <<TIME-DATE>> and <<CALLING PARTY NUMBER>> and <<CALLED PARTY NUMBER>> information elements indicating "non-prioritised list".

6.3.3 SS-messages (call related and call independent)

6.3.3.1 {FACILITY}

This message may be sent to request or acknowledge a supplementary service. The supplementary service to be invoked, and its associated parameters, are specified in the <<FACILITY>> information element.

Message Type	Format	Directions
{FACILITY}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Repeat indicator 1	7.6.3	O	O	1
Facility	7.7.15	O	O	2-*
"Display"	7.5.5	O	N	2-*
"Keypad"	7.5.5	N	O	2-*
Feature Activate	7.7.16	N	O	3-4
Feature Indicate	7.7.17	O	N	4-*
Repeat indicator 1	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>>, and <<IWU-to-IWU>> information elements indicating "non-prioritised list".

6.3.3.2 {HOLD}

This message is sent by the FT or PT to request the hold function for an existing call.

Message Type	Format	Directions
{HOLD}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.3.3 {HOLD-ACK}

This message is sent by the FT or PT to indicate that the hold function has been successfully performed.

Message Type	Format	Directions
{HOLD-ACK}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.3.4 {HOLD-REJECT}

This message is sent by the FT or PT to indicate the denial of a request to hold a call.

Message Type	Format	Directions
{HOLD-REJECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Reject Reason	7.7.34	O	0	3
Repeat indicator 1	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-to-IWU>> information elements indicating "non-prioritised list".

6.3.3.5 {RETRIEVE}

This message is sent by the FT or PT to request the retrieval of a held call.

Message Type	Format	Directions
{RETRIEVE}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.3.6 {RETRIEVE-ACK}

This message is sent by the FT or PT to indicate that the retrieve function has been successfully performed.

Message Type	Format	Directions
{RETRIEVE-ACK}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.3.7 {RETRIEVE-REJECT}

This message is sent by the FT or PT to indicate the inability to perform the requested retrieve function.

Message Type	Format	Directions
{RETRIEVE-REJECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Reject Reason	7.7.34	O	O	3
Repeat indicator 1	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-to-IWU>> information elements indicating "non-prioritised list".

6.3.3.8 {CISS-REGISTER}

This message is sent by the FT or PT to assign a new TI for non-call associated transactions.

Message Type	Format	Directions
{CISS-REGISTER}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Repeat indicator 1	7.6.3	O	O	1
Facility	7.7.15	O	O	2-*
"Display"	7.5.5	O	N	2-*
"Keypad"	7.5.5	N	O	2-*
Feature Activate	7.7.16	N	O	3-4
Feature Indicate	7.7.17	O	N	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>> information elements indicating "non-prioritised list".

6.3.3.9 {CISS-RELEASE-COM}

This message indicates that the sending entity has released the CISS-transaction and the transaction identifier, and the receiving entity shall release the CISS-transaction and the transaction identifier.

Message Type	Format	Directions
{CISS-RELEASE-COM}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Release Reason		7.6.7	O	O	2
Repeat indicator	1	7.6.3	O	O	1
Facility		7.7.15	O	O	2-*
"Display"		7.5.5	O	N	2-*
"Keypad"		7.5.5	N	O	2-*
Feature Activate		7.7.16	N	O	3-4
Feature Indicate		7.7.17	O	N	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>> information elements indicating "non-prioritised list".

6.3.4 COMS-messages

6.3.4.1 {COMS-SETUP}

This message is used to initiate a COMS call.

Message Type	Format	Directions
{COMS-SETUP}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2.	M	M	½
Transaction Identifier		7.3.	M	M	½
Message Type		7.4.	M	M	1
Portable identity	1	7.7.30	M	M	5-20
Fixed identity	1	7.7.18	M	M	5-20
IWU attributes		7.7.21	M	M	5-12
Connection attributes		7.7.11	O	O	4-7
"Display"		7.5.5	O	N	2-*
Called Party Number		7.7.7	O	O	4-*
Called Party Subaddr		7.7.8	O	O	4-*
IWU-TO-IWU		7.7.23	O	O	4-*
IWU-PACKET		7.7.22	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: <<Portable identity>> and <<Fixed identity>> are mandatory for direct data link establishment (see subclause 14.2).

6.3.4.2 {COMS-INFO}

This message is used to transfer information as part of a COMS call.

Message Type	Format	Directions
{COMS-INFO}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Segmented info 1	7.7.37	O	O	4
Alphanumeric	7.7.3	O	O	4-*
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

NOTE 1: The <<SEGMENTED-INFO>> element is used if the complete information cannot be fitted into one message.

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.4.3 {COMS-ACK}

This message is used to acknowledge the successful receipt of a compete COMS message as received in one or more {COMS-INFO} messages.

Message Type	Format	Directions
{COMS-ACK}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.4.4 {COMS-CONNECT}

The message is used in signal acceptance of a COMS call.

Message Type	Format	Directions
{COMS-CONNECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
"Display"	7.5.5	O	N	2-*
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.4.5 {COMS-RELEASE}

This message is used to indicate that the sending entity wishes to release a COMS call.

Message Type	Format	Directions
{COMS-RELEASE}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
"Display"	7.5.5	O	N	2-*
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.4.6 {COMS-RELEASE-COM}

This message indicates that the sending entity has released the COMS call and that the receiving entity shall release all call references.

Message Type	Format	Directions
{COMS-RELEASE-COM}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
"Display"	7.5.5	O	N	2-*
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.4.7 {COMS-NOTIFY}

This message is used to exchange internal protocol information without causing a state change.

Message Type	Format	Directions
{COMS-NOTIFY}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.5 CLMS-message

6.3.5.1 {CLMS-VARIABLE}

Message Type	Format	Directions
{CLMS-VARIABLE}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	5-20
MMS Generic Header	7.7.47	O	O	-*
MMS Object Header	7.7.48	O	O	-*
Repeat Indicator	7.6.3	O	O	1
MMS Extended Header	7.7.49	O	O	-*
Repeat Indicator	7.6.3	O	O	1
Time-Date	7.7.50	O	O	6-10
Repeat Indicator	7.6.3	O	O	1
Calling Party Number	7.7.9	O	O	5-*
Repeat Indicator	7.6.3	O	O	1
Called Party Number	7.7.7	O	O	4-*
Called Party Subaddr	7.7.8	O	O	4-*
Segmented-Info 1	7.7.37	O	O	4
Alphanumeric	7.7.3	O	O	4-*
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: The <<SEGMENTED-INFO>> element is used if the complete information cannot be fitted into one message.

6.3.6 MM-messages

6.3.6.1 {ACCESS-RIGHTS-ACCEPT}

This message is sent by the FT to the PT to transfer the access rights parameters to the PT.

Message Type	Format	Directions
{ACCESS-RIGHTS-ACCEPT}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Portable identity	7.7.30	M	-	5-20
Repeat Indicator 1	7.6.3	O	-	1
Fixed identity (PARK) 1	7.7.18	M	-	5-20
Location area	7.7.25	O	-	3-*
AUTH-TYPE	7.7.4	O	-	5-6
Cipher info	7.7.10	O	-	4-5
ZAP field	7.7.44	O	-	3
Service class	7.7.39	O	-	3-*
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
N = Not allowed;
O = Optional;
- = not applicable.

NOTE 1: More than one PARK can by transmitted by using the <<REPEAT-INDICATOR>> information elements. In this case the coding for "non-prioritised list" should be used. Not more than 5 PARKs should be included.

6.3.6.2 {ACCESS-RIGHTS-REJECT}

This message is sent by the FT to the PT to indicate that the access rights parameters cannot be transferred.

Message Type	Format	Directions
{ACCESS-RIGHTS-REJECT}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Reject Reason	7.7.34	O	-	3
Duration	7.7.13	O	-	4
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
0 = Optional;
- = not applicable.

6.3.6.3 {ACCESS-RIGHTS-REQUEST}

This message is sent by the PT to the FT to request from the FT to send the access rights parameters in a subsequent {ACCESS-RIGHTS-ACCEPT} message.

Message Type	Format	Directions
{ACCESS-RIGHTS-REQUEST}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	5-20
AUTH-TYPE	7.7.4	-	O	5-6
Cipher info	7.7.10	-	O	4-5
Set-up capability	7.7.40	-	O	3-4
Terminal capability	7.7.41	-	O	3-*
IWU-TO-IWU	7.7.23	-	O	4-*
Model identifier	7.7.46	-	O	5
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.4 {ACCESS-RIGHTS-TERMINATE-ACCEPT}

This message is sent by the FT or PT to indicate that the access rights parameters have been erased.

Message Type	Format	Directions
{ACCESS-RIGHTS-TERMINATE-ACCEPT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory.

6.3.6.5 {ACCESS-RIGHTS-TERMINATE-REJECT}

This message is sent by the FT or PT to indicate that the access rights parameters have not been erased.

Message Type	Format	Directions
{ACCESS-RIGHTS-TERMINATE-REJECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Reject Reason	7.7.34	O	O	3
Duration	7.7.13	O	N	4
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

6.3.6.6 {ACCESS-RIGHTS-TERMINATE-REQUEST}

This message is sent by the FT or PT to request the erasure of the access rights parameters.

Message Type	Format	Directions
{ACCESS-RIGHTS-TERMINATE-REQUEST}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	5-20
Repeat Indicator	7.6.3	O	O	1
Fixed identity (PARK)	7.7.18	O	O	5-20
IWU-TO-IWU	7.7.23	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

A list of <<FIXED-IDENTITY>> information elements (PARKs) can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" shall be used. Not more than 3 PARKs should be included.

6.3.6.7 {AUTHENTICATION-REJECT}

This message is sent by the FT or PT to indicate that authentication has failed or cannot be done.

Message Type	Format	Directions
{AUTHENTICATION-REJECT}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Repeat Indicator 1	7.6.3	O	O	1
AUTH-TYPE 1	7.7.4	O	O	5-6
Reject Reason	7.7.34	O	O	3
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: Instead of one <<AUTH-TYPE>> information element also a prioritised list of <<AUTH-TYPE>> information elements can be included by using the <<REPEAT-INDICATOR>> information element. Not more than 3 <<AUTH-TYPE>> information elements should be included.

6.3.6.8 {AUTHENTICATION-REPLY}

This message is sent by the FT or PT to deliver a calculated response.

Message Type	Format	Directions
{AUTHENTICATION-REPLY}	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
RES 1	7.7.35	M	M	6
RS 1,2	7.7.36	M/O	N	10
ZAP field 3	7.7.44	N	M/O	3
Service class 4	7.7.39	N	M/O	3-*
Key	7.7.24	N	O	4-*
IWU-TO-IWU	7.7.23	O	O	4-*
Escape to proprietary	7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The length when a DECT Standard Authentication Algorithm (DSAA) is used.

NOTE 2: If this message is used in the FT authentication procedure and a DECT Standard Authentication Algorithm (DSAA) is used, then the <<RS>> information element is mandatory in the direction FT to PT. If this message is used in the key allocation procedure, then the <<RS>> information element should not be included.

NOTE 3: If the PT has stored a ZAP field that is related to the current active IPUI, than the <<ZAP-FIELD>> information element is mandatory in the direction PT to FT.

NOTE 4: If the PT has stored a service class that is related to the current active IPUI, than the <<SERVICE-CLASS>> information element is mandatory in the direction PT to FT.

6.3.6.9 {AUTHENTICATION-REQUEST}

This message is sent by the FT or PT to initiate authentication of the PT or FT identity.

Message Type	Format	Directions
{AUTHENTICATION-REQUEST}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
AUTH-TYPE		7.7.4	M	M	5-6
RAND	1	7.7.32	M	M	10
RES	1,3	7.7.35	N	M/O	6
RS	1,2	7.7.36	M/O	N	10
Cipher info		7.7.10	O	O	4-5
IWU-TO-IWU		7.7.23	O	O	4-*
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: The length when a DECT Standard Authentication Algorithm (DSAA) is used.

NOTE 2: If a DECT Standard Authentication Algorithm (DSAA) is used, then the <<RS>> information element is mandatory in the direction FT to PT.

NOTE 3: If this message is used in the key allocation procedure, then the <<RES>> information element is mandatory in the direction PT to FT.

6.3.6.10 {CIPHER-REJECT}

This message is sent by the PT or FT to indicate that the requested cipher switching cannot be done.

Message Type	Format	Directions
{CIPHER-REJECT}	S	Both

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	M	½
Transaction Identifier		7.3	M	M	½
Message Type		7.4	M	M	1
Repeat Indicator	1	7.6.3	O	O	1
Cipher info	1	7.7.10	O	O	4-5
Reject Reason		7.7.34	O	O	3
Escape to proprietary		7.7.45	O	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: Instead of one <<CIPHER-INFO>> information element, also a prioritised list of <<CIPHER-INFO>> information elements can be included by using the <<REPEAT-INDICATOR>> information element. Not more than 3 <<CIPHER-INFO>> information elements should be included.

6.3.6.11 {CIPHER-REQUEST}

This message is sent by the FT to engage or disengage ciphering of a connection.

Message Type	Format	Directions
{CIPHER-REQUEST}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Cipher info	7.7.10	M	-	4-5
Call Identity	7.7.6	O	-	3-4
Connection Identity	7.7.12	O	-	3-*
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.12 {CIPHER-SUGGEST}

This message is sent by the PT to request engaging or disengaging ciphering of a connection.

Message Type	Format	Directions
{CIPHER-SUGGEST}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Cipher info	7.7.10	-	M	4-5
Call Identity	7.7.6	-	O	3-4
Connection Identity	7.7.12	-	O	3-*
IWU-TO-IWU	7.7.23	-	O	4-*
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.13 {DETACH}

This message is sent by the PT to the FT to set a deactivation indication in the network.

Message Type	Format	Directions
{DETACH}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	5-20
NWK assigned identity	7.7.28	-	O	5-20
IWU-TO-IWU	7.7.23	-	O	4-*
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.14 {IDENTITY-REPLY}

This message is sent by the PT to the FT in response to an {IDENTITY-REQUEST} message providing the requested identity.

Message Type	Format	Directions
{IDENTITY-REPLY}	S	P=>F

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	-	M	½
Transaction Identifier		7.3	-	M	½
Message Type		7.4	-	M	1
Repeat Indicator	1	7.6.3	-	O	1
Portable identity	1	7.7.30	-	O	5-20
Repeat Indicator	2	7.6.3	-	O	1
Fixed identity	2	7.7.18	-	O	5-20
Repeat Indicator	3	7.6.3	-	O	1
NWK assigned identity	3	7.7.28	-	O	5-20
IWU-TO-IWU		7.7.23	-	O	4-*
Escape to proprietary		7.7.45	-	O	2-*

M = Mandatory;
O = Optional.

NOTE 1: More than one <<PORTABLE-IDENTITY>> information element can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" is used.

NOTE 2: More than one <<FIXED-IDENTITY>> information element can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" is used.

NOTE 3: More than one <<NWK-ASSIGNED-IDENTITY>> information element can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" is used.

NOTE 4: An {IDENTITY-REPLY} message without any information elements has the same meaning as an “{IDENTITY-REJECT}” message.

6.3.6.15 {IDENTITY-REQUEST}

This message is sent by the FT to the PT to request a PT to submit the specified identity to the FT.

Message Type	Format	Directions
{IDENTITY-REQUEST}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Repeat Indicator 1	7.6.3	M/N	-	1
Identity type 1	7.7.19	M	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
N = Not allowed;
O = Optional.

NOTE 1: More than one <<IDENTITY-TYPE>> information element can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" is used. Not more than 3 <<IDENTITY-TYPE>> information elements should be included.

6.3.6.16 {KEY-ALLOCATE}

This message is sent by the FT to the PT to replace an authentication code by an User Authentication Key (UAK).

Message Type	Format	Directions
{KEY-ALLOCATE}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Allocation type	7.7.2	M	-	4
RAND 1	7.7.32	M	-	10
RS 1	7.7.36	M	-	10
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory.

NOTE 1: The length when a DECT standard authentication algorithm is used.

6.3.6.17 {LOCATE-ACCEPT}

This message is sent by the FT to the PT to indicate that location updating or attach has been completed.

Message Type	Format	Directions
{LOCATE-ACCEPT}	S	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	-	½
Transaction Identifier		7.3	M	-	½
Message Type		7.4	M	-	1
Portable identity	1	7.7.30	M	-	2-20
Location area		7.7.25	M	-	3-*
NWK assigned identity		7.7.28	O	-	5-20
Ext h/o indicator		7.7.51	O	-	4-*
Duration		7.7.13	O	-	4
IWU-TO-IWU		7.7.23	O	-	4-*
Escape to proprietary		7.7.45	O	-	2-*

M = Mandatory;
O = Optional.

NOTE 1: This element may contain zero length contents if a new TPUI is not assigned.

6.3.6.18 {LOCATE-REJECT}

This message is sent by the FT to the PT to indicate that location updating or attach has failed.

Message Type	Format	Directions
{LOCATE-REJECT}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Reject Reason	7.7.34	O	-	3
Duration	7.7.13	O	-	4
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.19 {LOCATE-REQUEST}

This message is sent by the PT to the FT either to request update of its location file or to request attach.

Message Type	Format	Directions
{LOCATE-REQUEST}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	5-20
Fixed identity	7.7.18	-	O	5-20
Location area	7.7.25	-	O	3-*
NWK assigned identity	7.7.28	-	O	5-20
Cipher info	7.7.10	-	O	4-5
Set-up capability	7.7.40	-	O	3-4
Terminal capability	7.7.41	-	O	3-*
IWU-TO-IWU	7.7.23	-	O	4-*
Model identifier	7.7.46	-	O	5
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.20 {MM-INFO-ACCEPT}

This message is sent by the FT to the PT in response to a {MM-INFO-REQUEST} message providing the requested information.

Message Type	Format	Directions
{MM-INFO-ACCEPT}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Info type	7.7.20	O	-	3-*
Repeat Indicator	7.6.3	O	-	1
Fixed identity	7.7.18	O	-	5-20
Location area	7.7.25	O	-	3-*
NWK assigned identity	7.7.28	O	-	5-20
Network parameter	7.7.29	O	-	4-*
Duration	7.7.13	O	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.21 {MM-INFO-REJECT}

This message is sent by the FT to indicate to the PT that the requested information cannot be sent.

Message Type	Format	Directions
{MM-INFO-REJECT}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Reject Reason	7.7.34	O	-	3
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.22 {MM-INFO-REQUEST}

This message is sent by the PT to the FT to request information (e.g. regarding external handover) to be sent in a subsequent {MM-INFO-ACCEPT} message.

Message Type	Format	Directions
{MM-INFO-REQUEST}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Info type	7.7.20	-	M	3-*
Portable identity	7.7.30	-	O	5-20
Repeat indicator	7.6.3	-	O	1
Fixed identity	7.7.18	-	O	5-20
Location area	7.7.25	-	O	3-*
NWK assigned identity	7.7.28	-	O	5-20
Network parameter	7.7.29	-	O	4-*
IWU-TO-IWU	7.7.23	-	O	4-*
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.23 {MM-INFO-SUGGEST}

This message is sent by the FT to provide information to the PT or to suggest an action to the PT, e.g. to perform location updating or an external handover.

Message Type	Format	Directions
{MM-INFO-SUGGEST}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Info type	7.7.20	M	-	3-*
Fixed identity	7.7.18	O	-	5-20
Location area	7.7.25	O	-	3-*
NWK assigned identity	7.7.28	O	-	5-20
Network parameter	7.7.29	O	-	4-*
Ext h/o indicator	7.7.51	O	-	4-*
KEY	7.7.24	O	-	4-*
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.6.24 {TEMPORARY-IDENTITY-ASSIGN}

This message is sent by the FT to the PT to allocate a TPUI or a network assigned identity.

Message Type	Format	Directions
{TEMPORARY-IDENTITY-ASSIGN}	S	F=>P

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	½
Transaction Identifier	7.3	M	-	½
Message Type	7.4	M	-	1
Portable identity 1	7.7.30	O	-	5-20
Location area	7.7.25	O	-	3-*
NWK assigned identity 1	7.7.28	O	-	5-20
Duration	7.7.13	O	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: At least one identity information element is included in a {TEMPORARY-IDENTITY-ASSIGN} message.

6.3.6.25 {TEMPORARY-IDENTITY-ASSIGN-ACK}

This message is sent by the PT to the FT to indicate that allocation of a TPUI or network assigned identity has taken place.

Message Type	Format	Directions
{TEMPORARY-IDENTITY-ASSIGN-ACK}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
- = not applicable.

6.3.6.26 {TEMPORARY-IDENTITY-ASSIGN-REJ}

This message is sent by the PT to the FT to indicate that allocation of a TPUI or network assigned identity has failed.

Message Type	Format	Directions
{TEMPORARY-IDENTITY-ASSIGN-REJ}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Reject Reason	7.7.34	-	O	3
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.7 LCE-messages

6.3.7.1 {LCE-PAGE-RESPONSE}

This message is sent by the PT to the FT to indicate that it has received a {LCE-REQUEST-PAGE} message.

Message Type	Format	Directions
{LCE-PAGE-RESPONSE}	S	P=>F

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	5-20
Fixed identity	7.7.18	-	O	5-20
NWK assigned identity	7.7.28	-	O	5-20
Cipher info	7.7.10	-	O	4-5
Escape to proprietary	7.7.45	-	O	2-*

M = Mandatory;
O = Optional;
- = not applicable.

6.3.7.2 {LCE-PAGE-REJECT}

This message is sent by the FT to the PT to reject an unwanted response to a {LCE-REQUEST-PAGE} message.

Message Type	Format	Directions
{LCE-PAGE-REJECT}	S	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	-	½
Transaction Identifier		7.3	M	-	½
Message Type		7.4	M	-	1
Portable identity	1	7.7.30	M	-	5-20
Fixed identity		7.7.18	O	-	5-20
Reject Reason		7.7.34	O	-	3
Escape to proprietary		7.7.45	O	-	2-*

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: The <<PORTABLE-IDENTITY>> information element contains the full IPUI of the PT that is rejected.

6.4 B-FORMAT message functional contents

6.4.1 B-FORMAT message overview

Each of the B-FORMAT message definitions includes:

a) a brief description of the message direction and use;

b) a table listing all the possible information elements that can be contained in the message. For each element, the table defines:

   1) the name of the information element;

   2) a reference to the subclause where the information element is defined;

   3) whether the inclusion of the information element is Mandatory (M) or Optional (O) or Not allowed (N). These inclusion rules are defined separately for each message direction. If the message is only specified for one direction, the elements are marked not applicable (-) for the other direction;

   4) the range of possible lengths of the information element, where "*" means the maximum length is undefined.

c) further explanatory notes as required.

The information elements are always listed in their order of appearance, this order is mandatory for all instances of the message. Receiver implementations shall take account of the possibility that further information elements may be inserted in the message tables in future editions of this standard.

6.4.2 {LCE-REQUEST-PAGE}

This message is used by the LCE in the FT to request a PT to immediately establish a link to that FT.

Message Type	Format	Directions
{LCE-REQUEST-PAGE}	B	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
LCE Header		8.2	M	-	½
Long address	1	8.2	O	-	4
Short address	1	8.2	O	-	2

M = Mandatory;
O = Optional;
- = not applicable.

NOTE 1: The message must contain either a <<LONG-ADDRESS>> element or a <<SHORT-ADDRESS>> element.

6.4.3 {CLMS-FIXED}

This message is used by the CLMS in the FT to send application specific information to one or more PTs.

NOTE 1: This message will be fragmented into message sections suitable for transmission by the MAC broadcast message control services.

Message Type	Format	Directions
{CLMS-FIXED}	B	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
CLMS Header	1	8.3.2	M	-	½
Short address	2	8.3.2	M	-	2
Protocol Discriminator	2	8.3.2	M	-	1
Length Indicator	3	8.3.2	M/N	-	1
Data		8.3.2	M	-	1-20
Fill	4	8.3.2	O	-	0-3

M = Mandatory;
N = Not allowed;
O = Optional;
- = not applicable.

NOTE 1: This element appears in all message sections.

NOTE 2: These elements are mandatory for all {CLMS-FIXED} messages. They are contained in the first message section. Refer to subclause 12.3.1.

NOTE 3: The <<LENGTH-INDICATOR>> is mandatory for multi-section messages. It is not allowed for single-section messages. Refer to subclause 12.3.1.

NOTE 4: The fill field is used to adjust the total message length to an integral number of sections. Refer to subclause 8.3.

7 S-FORMAT message structures

7.1 Overview

The S-FORMAT message structures are based on the principles adopted in ETS 300 102-1 [10]. Similar modifications to those adopted in prI-ETS 300 022 [11] have also been used. The detailed coding of all elements is unique to this ETS.

Every message consists of the following parts:

a) protocol discriminator;

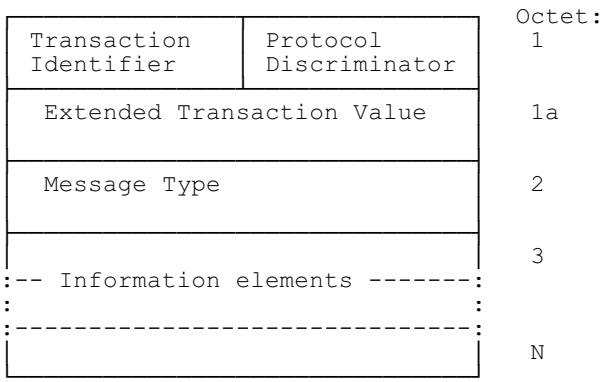
b) transaction identifier;

c) message type;

d) information elements.

Elements a), b) and c) shall be present in every message. Element d) is specific to each message type.

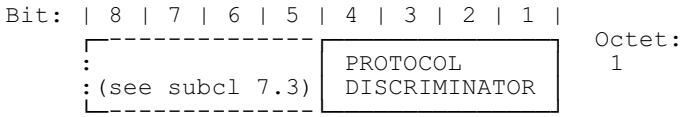
Elements a) and b) are combined into one octet (octet 1) of every message.



S-FORMAT message structures

NOTE: Octet 1a is optional, and should only be used on systems that require an extended transaction value.

7.2 Protocol Discrimination (PD) element



Protocol Discriminator (PD) bits

Protocol Discriminator (PD):

Bits: 4 3 2 1	Meaning
0 0 0 0	Link Control Entity (LCE) messages
0 0 1 1	Call Control (CC) messages (note 2)
0 1 0 0	Call Independent Supplementary Services (CISS) messages
0 1 0 1	Mobility Management (MM) messages
0 1 1 0	ConnectionLess Message Service (CLMS) messages
0 1 1 1	Connection Oriented Message Service (COMS) messages
1 - - -	Unknown protocol entity

All other values reserved.

NOTE 1: Only bit 4 of this protocol discriminator is used in the ECMA/ETSI sense. Bits 3 to 1 are used to provide discrimination between different entities within one protocol set.

NOTE 2: CC messages include Call Related Supplementary Service (CRSS) messages.

7.3 Transaction Identifier (TI) element

The Transaction Identifier (TI) is used to distinguish multiple parallel transactions (multiple activities) associated with one PT (one value of IPUI). The Transaction Identifier (TI) only applies to the associated value of Protocol Discriminator (PD), and the same value of transaction identity may be used by different protocol entities at the same time. A Transaction Identifier (TI) contains two fields, a Flag field (F) and a Transaction Value (TV) field.

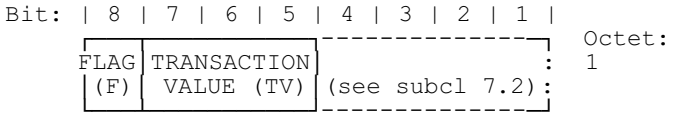
The allowable values of the Transaction Value (TV) depend on the associated Protocol Discriminator (PD) according to the following table.

Table 7: Allowable range of Transaction Identifiers (TIs)

Protocol Discriminator	Maximum number of parallel transactions	Allowable values of transaction value
LCE	1	'0' only
CC	7 + extend	'0' to '6' + extend
CISS	7	'0' to '6'
MM	1	'0' only
CLMS	1	'0' only
COMS	7	'0' to '6'
Unknown	Not defined	Not defined

The TI is assigned by the side that initiates the transaction (portable side or fixed side). The protocol entities on both sides have access to the full allowable range of transaction values as given above, The same TV can be used for two simultaneous transactions that are originated from opposite sides.

The TI value of "6" shall only be used for connectionless NWK layer transactions. For the procedures see subclause 10.4.2.3.



Transaction Identifier (TI) bits

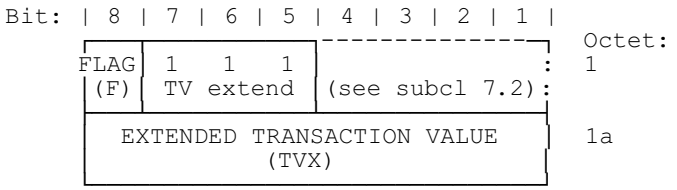
Transaction Flag (F):

F = 0 for message from transaction originator
F = 1 for message from transaction destination

Transaction Value (TV):

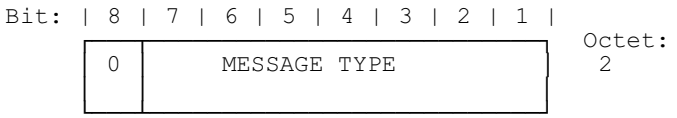
Bits: 7 6 5	Meaning
0 0 0	} Valid TV
to	
1 1 0	}
1 1 1	Reserved value (TV extension)

When the reserved value is used, the message shall contain an additional octet (octet 1b) containing an 8-bit Extended Transaction Value (TVX):



Extended Transaction Identifier (ETI) bits

7.4 Message type element



Message Identifier (MI)

The purpose of the message type is to identify the function of the message being sent. The message type is coded as shown in the following tables.

7.4.1 Messages for CC

Table 8: CC message type coding

CC message types	Bits 8	7	6	5	4	3	2	1
Reserved	0	0	0	0	0	0	0	0
{CC-ALERTING}	0	0	0	0	0	0	0	1
{CC-CALL-PROC}	0	0	0	0	0	0	1	0
{CC-SETUP}	0	0	0	0	0	1	0	1
{CC-CONNECT}	0	0	0	0	0	1	1	1
{CC-SETUP-ACK}	0	0	0	0	1	1	0	1
{CC-CONNECT-ACK}	0	0	0	0	1	1	1	1
{CC-SERVICE-CHANGE}	0	0	1	0	0	0	0	0
{CC-SERVICE-ACCEPT}	0	0	1	0	0	0	0	1
{CC-SERVICE-REJECT}	0	0	1	0	0	0	1	1
{CC-RELEASE}	0	1	0	0	1	1	0	1
{CC-RELEASE-COM}	0	1	0	1	1	0	1	0
{IWU-INFO}	0	1	1	0	0	0	0	0
{CC-NOTIFY}	0	1	1	0	1	1	1	0
{CC-INFO}	0	1	1	1	1	0	1	1

7.4.2 Messages for SS

Table 9: SS message type coding

CISS message types (call independ.)	Bits 8	7	6	5	4	3	2	1
{CISS-RELEASE-COM}	0	1	0	1	1	0	1	0
{FACILITY}	0	1	1	0	0	0	1	0
{CISS-REGISTER}	0	1	1	0	0	1	0	0
CRSS message types (call related)	8	7	6	5	4	3	2	1
{HOLD}	0	0	1	0	0	1	0	0
{HOLD-ACK}	0	0	1	0	1	0	0	0
{HOLD-REJECT}	0	0	1	1	0	0	0	0
{RETRIEVE}	0	0	1	1	0	0	0	1
{RETRIEVE-ACK}	0	0	1	1	0	0	1	1
{RETRIEVE-REJECT}	0	0	1	1	0	1	1	1
{FACILITY}	0	1	1	0	0	0	1	0

7.4.3 Messages for COMS

Table 10: COMS message type coding

COMS message types	Bits 8	7	6	5	4	3	2	1
{COMS-SETUP}	0	0	0	0	0	1	0	1
{COMS-CONNECT}	0	0	0	0	0	1	1	1
{COMS-NOTIFY}	0	0	0	0	1	0	0	0
{COMS-RELEASE}	0	1	0	0	1	1	0	1
{COMS-RELEASE-COM}	0	1	0	1	1	0	1	0
{COMS-INFO}	0	1	1	1	1	0	1	1
{COMS-ACK}	0	1	1	1	1	0	0	0

7.4.4 Messages for CLMS

Table 11: CLMS message type coding

CLMS message types	Bits 8	7	6	5	4	3	2	1
[{CLMS-FIXED}	** B-FORMAT message]							
{CLMS-VARIABLE}	0	0	0	0	0	0	0	1

7.4.5 Messages for MM

Table 12: MM message type coding

MM message types	Bits 8	7	6	5	4	3	2	1
{AUTHENTICATION-REQUEST}	0	1	0	0	0	0	0	0
{AUTHENTICATION-REPLY}	0	1	0	0	0	0	0	1
{KEY-ALLOCATE}	0	1	0	0	0	0	1	0
{AUTHENTICATION-REJECT}	0	1	0	0	0	0	1	1
{ACCESS-RIGHTS-REQUEST}	0	1	0	0	0	1	0	0
{ACCESS-RIGHTS-ACCEPT}	0	1	0	0	0	1	0	1
{ACCESS-RIGHTS-REJECT}	0	1	0	0	0	1	1	1
{ACCESS-RIGHTS-TERMINATE-REQUEST}	0	1	0	0	1	0	0	0
{ACCESS-RIGHTS-TERMINATE-ACCEPT}	0	1	0	0	1	0	0	1
{ACCESS-RIGHTS-TERMINATE-REJECT}	0	1	0	0	1	0	1	1
{CIPHER-REQUEST}	0	1	0	0	1	1	0	0
{CIPHER-SUGGEST}	0	1	0	0	1	1	1	0
{CIPHER-REJECT}	0	1	0	0	1	1	1	1
{MM-INFO-REQUEST}	0	1	0	1	0	0	0	0
{MM-INFO-ACCEPT}	0	1	0	1	0	0	0	1
{MM-INFO-SUGGEST}	0	1	0	1	0	0	1	0
{MM-INFO-REJECT}	0	1	0	1	0	0	1	1
{LOCATE-REQUEST}	0	1	0	1	0	1	0	0
{LOCATE-ACCEPT}	0	1	0	1	0	1	0	1
{DETACH}	0	1	0	1	0	1	1	0
{LOCATE-REJECT}	0	1	0	1	0	1	1	1
{IDENTITY-REQUEST}	0	1	0	1	1	0	0	0
{IDENTITY-REPLY}	0	1	0	1	1	0	0	1
{TEMPORARY-IDENTITY-ASSIGN}	0	1	0	1	1	1	0	0
{TEMPORARY-IDENTITY-ASSIGN-ACK}	0	1	0	1	1	1	0	1
{TEMPORARY-IDENTITY-ASSIGN-REJ}	0	1	0	1	1	1	1	1

7.4.6 Messages for LCE

Table 13: LCE message type coding

LCE message types	Bits 8	7	6	5	4	3	2	1
{LCE-PAGE-RESPONSE}	0	1	1	1	0	0	0	1
{LCE-PAGE-REJECT}	0	1	1	1	0	0	1	0
[{LCE-REQUEST-PAGE}	** B-FORMAT message]							

7.5 Other information elements

7.5.1 Coding rules

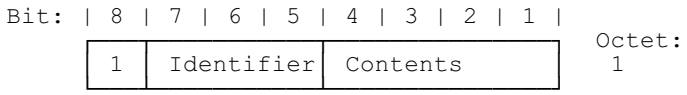
Two categories of information element are defined, fixed length and variable length. These categories are distinguished by the coding of bit 8 of the identifier octet.

NOTE: Although similar coding to ETS 300 102-1 [10] has been used this should not be assumed. Most information elements have been redefined and recoded and ETS 300 102-1 [10] should not be used as a detailed reference.

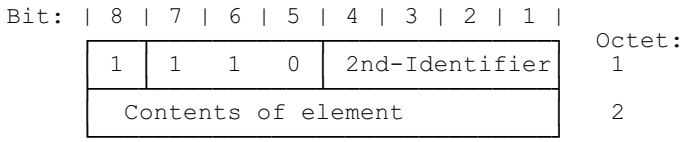
Fixed length information elements (bit 8 = "1")

The primary set of the fixed length information elements are single octet elements, where bits {4..1} contain the information. This corresponds to ETS 300 102-1 [10].

One single octet identifier is used to define a secondary set of 2 octet elements. For this secondary set only, bits {4..1} of the first octet define a secondary identifier (an extended identifier) that describes one of each double octet elements, see subclause 7.6.1. Octet 2 then contains a full octet of information.



Single octet information element



Double octet information element

Variable length information elements (bit 8 = "0")

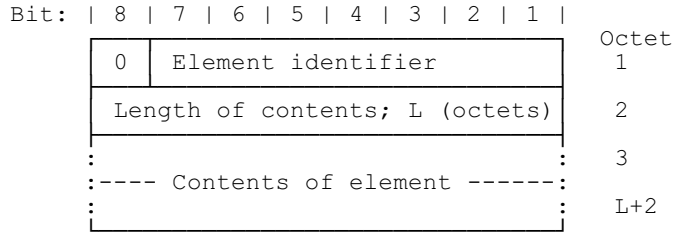
Variable length elements follow the principles defined in ETS 300 102-1 [10].

The descriptions of the variable length information elements are in subclause 7.7.2 onwards. There is a particular order of appearance for each variable length information element within a message. The code values of the variable length information element identifiers are assigned in ascending numerical order, according to the defined order of appearance of the elements in each message. This allows receiving equipment to detect the presence or absence of a particular information element without scanning through an entire message.

The second octet of all variable length elements indicates the total length of the contents of that element regardless of the coding of the first octet (i.e. the length is calculated starting from octet 3). This length is the natural binary coding of the number of octets of the contents, with the least significant bit in bit position 1.

An optional variable length information element may be present but empty (i.e. length of contents = "0"). This should be interpreted by the receiver as equivalent to that information element being absent.

Some information elements contain spare bits, these are generally indicated as being set to "0". In order to allow compatibility with future implementations, elements should not be rejected if these spare bits are set to "1".



Variable length information element

The following rules apply to the coding of the contents of variable length information elements:

1) the first character (the digit) in the octet number identifies one octet or a group of octets;

2) each octet group is a self contained entity. The second character (the letter) in the octet number identifies the position of the octet in the group. The internal structure of an octet group may be defined in alternative ways;

3) an octet group is formed by using some extension mechanism. The preferred extension mechanism is to use bit 8 of each octet in the group as an extension bit. The bit value "0" indicates that the group is extended into the next octet. The bit value "1" indicates that this is the last octet of the group.

In the coding descriptions that follow, the following conventions are used:

- one octet group is described as a sequence of zero or more octets with "0/1" on bit position 8, followed by one octet with "0/1 ext" or "1" on bit position 8;

- if any non-last octet of a described octet group has value 1, all subsequent octets shown for that octet are absent;

- an octet group showing "0/1 ext" in bit position 8 of the last octet of that group may be extended with additional octets in later versions of this ETS and equipment shall be prepared to receive such additional octets although the equipment need not to be able to act upon the contents of these octets;

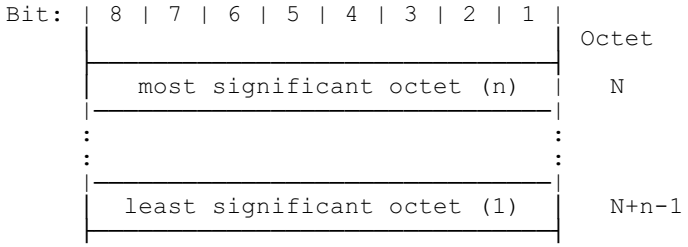
- an octet group showing "1" in bit position 8 of the last octet of that group will not be extended with additional octets in later versions of this ETS.

- An information element may be extended with additional octet groups in later versions of this ETS, and equipment shall be prepared to receive additional octet groups although the equipment need not be able to act upon the contents of these octet groups.

4) in addition to the extension mechanism described above, an octet group may be defined by an explicit length coding either using the value in octet 2 or including a second length coding. This mechanism may be used instead of, or as well as, the preferred mechanism described above;

5) in a few cases, this second length coding may define the length in bits (not octets). In this event the length of the octet group shall be minimum number of integral octets required to contain all the bits (i.e. the rounded-up value). The surplus bits shall be set to "0" by the sender and should be ignored by the receiver;

6) unless otherwise stated, all fields within an information element shall be coded with the natural binary value, with the least significant bit in the lowest numbered bit position. If a field spans more than 1 octet, the information shall be arranged with the most significant bits in the lower numbered octets.



Structure of long fields

7.5.2 Extensions of codesets

This ETS defines codeset "0". All elements listed in subclauses 7.6.1 and 7.7.1 belong to codeset "0".

One value of single octet information element is reserved for shift operations as described in subclauses 7.5.3 and 7.5.4. These shift operations allow an expansion of the information element coding structure to support 8 codesets.

Each codeset shall reserve the same value of single octet element for shifting from one codeset to another. The contents of this shift element identifies the codeset to be used for the next information element(s). The codeset in use at any time is referred to as the "active codeset". Codeset "0" (the codeset defined in this document) shall be the initially active codeset at the start of every message.

The following coding rules shall apply to all codesets:

- the same basic fixed/variable length information element coding split (using octet 1, bit 8) shall be used

- the same Identifier-Length-Contents format for variable length information elements shall be used.

- the same single/double octet coding (using octet 1, bits 5-7) for fixed length information elements shall be used.

- the same Shift fixed length information elements (according to requirements currently in subclaluse 7.5.2 to subclause 7.5.4) shall be used. Other fixed length information elements may be different.

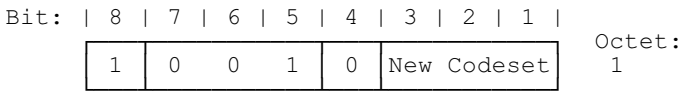
All equipment shall have the capability to recognise the shift element and to determine the length of the following information element(s). This shall enable the equipment to determine the start of a subsequent element. Equipment is not required to interpret any codesets except for codeset "0", elements from alternative codesets may be discarded without further action.

Two shift procedures shall be supported, locking shift and non-locking shift. Both procedures shall only apply to the message in which they appear (i.e. a shift shall not apply across message boundaries).

7.5.3 Locking shift procedure

The locking shift procedures uses the shift element to indicate the new active codeset. A "0" in bit position 4 indicates locking shift. The specified codeset remains active until another shift element appears or until the end of the message.

The locking shift procedure shall use the following element and coding:



Shift element (locking shift)

New (temporary) codeset identifier

Bits	3 2 1	Meaning
	0 0 0	Initial codeset (this ETS)
	0 0 1 }	Reserved
	0 1 0 }	
	0 1 1 }	
	1 - -	Escape for non-standard codeset

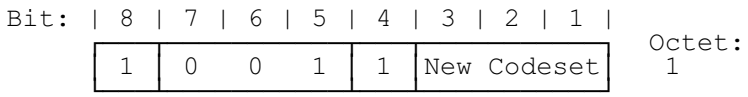
This procedure shall only be used to shift to a higher number codeset than the codeset being left.

7.5.4 Non-locking shift procedure

The non-locking shift procedures uses the shift element to indicate a temporary active codeset. A "1" in bit position 4 indicates non-locking shift. The specified codeset shall only apply to the next information element (or until the end of the message). After that information element the codeset shall revert to the previous (locked) active codeset.

A non-locking shift element shall not be transmitted directly before a locking shift element. If this combination is received it shall be treated as though the locking shift element only had been received.

The non-locking shift procedure shall use the following element and coding:



Shift element (non-locking)

New (temporary) codeset identifier:

as for locking shift: refer to subclause 7.5.3.

This procedure may be used to shift to a higher or lower numbered codeset than the codeset being left. A non-locking shift indicating the (currently) active codeset shall not of itself constitute an error.

7.5.5 Display and keypad elements

Display and keypad information can be carried in either a fixed length information element or a variable length information element:

Fixed Length	Variable Length
<< SINGLE-DISPLAY >>	<< MULTI-DISPLAY >>
<< SINGLE-KEYPAD >>	<< MULTI-KEYPAD >>

Whenever a message allows a <<"DISPLAY">> element or a <<"KEYPAD">> element to be included, this shall be understood to mean either one fixed length element << SINGLE ---- >> or one variable length element << MULTI ---- >> but not both.

All <<"KEYPAD">> and <<"DISPLAY">> elements shall contain zero or more characters from the DECT standard 8-bit character set as described in annex D.

NOTE: The DECT standard character set is based on the IA5 character set.

7.5.6 Repeated elements

Most messages shall only contain one appearance of a given information element. Two exceptions to this rule are allowed, and these exceptions are marked by the inclusion of the <<REPEAT-INDICATOR>> information element. Error handling on reception of unexpectedly repeated information elements is covered in subclause 17.5.2.

<<REPEAT-INDICATOR>>; coding 1.

The "non-prioritised list" coding is used when a message contains a list of repeated elements (containing different codings) which all are relevant. All elements in the list shall appear in immediate succession (i.e. there shall be no other elements in between the members of the list, and the <<REPEAT INDICATOR>> element shall immediately precede the first element of the list. These repeated lists are used for transferring a list of data, e.g. several Portable Access Rights Keys (PARKS) within one message.

<<REPEAT-INDICATOR>>; coding 2.

The "prioritised list" coding is used when a message contains a list of repeated elements (containing different codings) and inviting selection of one possibility. All elements in the list shall appear in immediate succession (i.e. there shall be no other elements in between the members of the list), and the <<REPEAT-INDICATOR>> element shall immediately precede the first element of the list. These repeated lists are used for negotiation of service, either at call establishment or during a service change.

7.6 Fixed length information elements

7.6.1 Summary

Table 14: Fixed length information elements coding

	Bits								Reference
Single Octet Elements	8	7	6	5	4	3	2	1	
Single Octet element	1	:	:	:	-	-	-	-	
Reserved	1	0	0	0	-	-	-	-	
Shift	1	0	0	1	-	-	-	-	7.5.3/7.5.4
Sending complete	1	0	1	0	0	0	0	1	7.6.2
Delimiter request	1	0	1	0	0	0	1	0	7.6.2
Repeat indicator	1	1	0	1	-	-	-	-	7.6.3
Double Octet element	1	1	1	0	-	-	-	-	
Double Octet Elements	8	7	6	5	4	3	2	1	
Basic Service	1	1	1	0	0	0	0	0	7.6.4
Release Reason	1	1	1	0	0	0	1	0	7.6.7
Signal	1	1	1	0	0	1	0	0	7.6.8
Timer Restart	1	1	1	0	0	1	0	1	7.6.9
Test Hook Control	1	1	1	0	0	1	1	0	7.6.10
Single-Display	1	1	1	0	1	0	0	0	7.6.5
Single-Keypad	1	1	1	0	1	0	0	1	7.6.6
Reserved (escape)	1	1	1	0	1	1	1	1	

7.6.2 Sending complete and delimiter request

The purpose of the <<SENDING-COMPLETE>> element is to optionally indicate completion of the called party number (see subclause 9.3.1.5).

The purpose of the <<DELIMITER-REQUEST>> element is to optionally request the peer to return a <<SENDING-COMPLETE>> element when the called party number is completed.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	1	0	0	0	0	1	1

SENDING-COMPLETE information element

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	1	0	0	0	1	0	1

DELIMITER-REQUEST information element

7.6.3 Repeat indicator

The purpose of the <<REPEAT-INDICATOR>> element is to indicate how repeated information elements shall be interpreted when included in a message. The <<REPEAT-INDICATOR>> element shall be included immediately before the first occurrence of the information element which will be repeated. See subclause 7.5.6.

NOTE: The use of the <<REPEAT-INDICATOR>> element in conjunction with an element that only appears once should not of itself constitute an error.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	1	0	1	Repeat indic.				1

REPEAT-INDICATOR information element

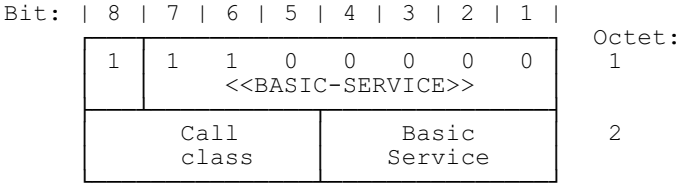
Repeat indicator coding (octet 1):

Bits	4 3 2 1	Meaning
	0 0 0 1	Non prioritised list. See subclause 7.5.6
	0 0 1 0	Prioritised list. See subclause 7.5.6

All other values reserved.

7.6.4 Basic service

The purpose of the <<BASIC-SERVICE>> element is to indicate the basic aspects of the service requested. This element allows the user to indicate the use of default attributes, thereby reducing the length of the set-up message.



BASIC-SERVICE information element

Call class (octet 2):

Bits	8 7 6 5	Meaning
	0 1 0 0	Message call set-up
	1 0 0 0	Normal call set-up
	1 0 0 1	Internal call (typically used in residential environments)
	1 0 1 0	Emergency call set-up
	1 0 1 1	Service call set-up
	1 1 0 0	External handover call set-up (see subclause 9.3.1.1)
	1 1 0 1	Supplementary service call set-up

All other values reserved.

Basic service (octet 2):

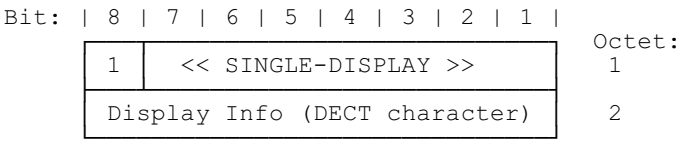
Bits	4 3 2 1	Meaning
	0 0 0 0	Basic speech default set-up attributes (see note and subclause 9.3.1.1)
	0 1 0 0	DECT GSM IWP profile (Phase 2)
	0 1 0 1	LRMS (E-profile) service [57]
	0 1 1 0	GSM IWP SMS
	1 1 1 1	Other (see subclause 9.3.1.1)

All other values reserved.

NOTE: The value of this field may be used in future standards to indicate "specific profile default setup attributes".

7.6.5 Single display

The purpose of the <<SINGLE-DISPLAY>> element is to convey display information that may be displayed by the PT. The <<SINGLE-DISPLAY>> element shall only contain DECT standard characters.

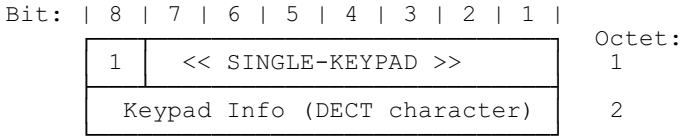


SINGLE-DISPLAY information element

NOTE: DECT characters are specified in annex D. These are based on IA5 characters.

7.6.6 Single keypad

The purpose of the <<SINGLE-KEYPAD>> element is to convey DECT standard characters e.g. as entered by means of a PT keypad.

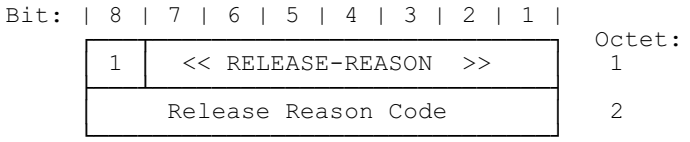


SINGLE-KEYPAD information element

NOTE: DECT characters are specified in annex D. These are based on IA5 characters.

7.6.7 Release reason

The purpose of the <<RELEASE-REASON>> element is to convey the cause of the release. This element shall be used whenever a specific coding is indicated in the procedures. The element should also be used in all other cases.



RELEASE-REASON information element

Release reason coding: general values

Value (hex)	Meaning (Reason)
00	Normal
01	Unexpected Message
02	Unknown Transaction Identifier
03	Mandatory information element missing
04	Invalid information element contents
05	Incompatible service
06	Service not implemented
07	Negotiation not supported
08	Invalid identity
09	Authentication failed
0A	Unknown identity
0B to 0C	Reserved
0D	Timer expiry
0E	Partial release
0F	Unknown

Release reason coding: user values

Value (hex)	Meaning (Reason)
10	User detached
11	User not in range
12	User unknown
13	User already active
14	User busy
15	User rejection
16 to 1F	Reserved

Release reason coding: external handover values

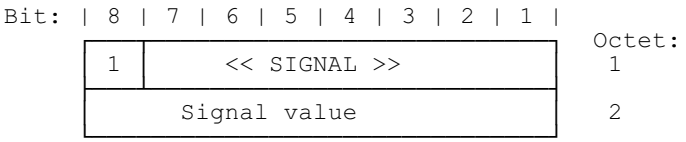
Value (hex)	Meaning (Reason)
20	Reserved
21	External Handover not supported
22	Network Parameters missing
23	External Handover release
24 to 2F	Reserved

Release reason coding: temporary overload values

Value (hex)	Meaning (Reason)
30	Reserved
31	Overload
32	Insufficient resources
33	Insufficient bearers available
34	IWU congestion
35 to 3F	Reserved

All other values reserved.

7.6.8 Signal



SIGNAL information element

Signal value coding (octet 2):

Bits 8 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0 0	dial tone on (note 3)
0 0 0 0 0 0 0 1	ring-back tone on (note 4)
0 0 0 0 0 0 1 0	intercept tone on (note 7)
0 0 0 0 0 0 1 1	network congestion tone on (note 6)
0 0 0 0 0 1 0 0	busy tone on (note 3)
0 0 0 0 0 1 0 1	confirm tone on (note 5)
0 0 0 0 0 1 1 0	answer tone on (note 5)
0 0 0 0 0 1 1 1	call waiting tone on (note 3)
0 0 0 0 1 0 0 0	off-hook warning tone on (note 5)
0 0 1 1 1 1 1 1	tones off
0 1 0 0 0 0 0 0	alerting on - pattern 0 (note 2)
0 1 0 0 0 0 0 1	alerting on - pattern 1 (note 2)
0 1 0 0 0 0 1 0	alerting on - pattern 2 (note 2)
0 1 0 0 0 0 1 1	alerting on - pattern 3 (note 2)
0 1 0 0 0 1 0 0	alerting on - pattern 4 (note 2)
0 1 0 0 0 1 0 1	alerting on - pattern 5 (note 2)
0 1 0 0 0 1 1 0	alerting on - pattern 6 (note 2)
0 1 0 0 0 1 1 1	alerting on - pattern 7 (note 2)
0 1 0 0 1 0 0 0	alerting on - continuous (note 1)
0 1 0 0 1 1 1 1	alerting off

All other values reserved.

A PT shall respond to all alerting patterns, but these may all produce the same sound.

NOTE 1: A FT may provide cadence following by sending an alternating sequence of alerting-on-continuous and alerting-off elements in {CC-INFO} messages while in the "CALL RECEIVED" state.

NOTE 2: The use of alerting patterns is FT dependent,; the resulting sound is PT dependent.

NOTE 3: This tone should be used in accordance with the description given in CCITT Recommendation E.182 [50].

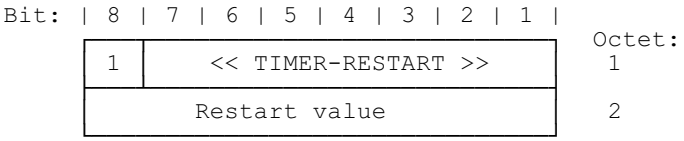
NOTE 4: This tone should be used in accordance with the "Ringing" tone description given in CCITT Recommendation E.182 [50].

NOTE 5: No description is provided for the use of this tone. This coding is included to provide alignment to the coding provided in ETS 300 102-1 [10].

NOTE 6: This tone should be used in accordance with the "congestion tone" description given in CCITT Recommendation E.182 [50].

NOTE 7: This tone should be used in accordance with the "intrusion tone" description given in CCITT Recommendation E.182 [50].

7.6.9 Timer restart



TIMER-RESTART information element

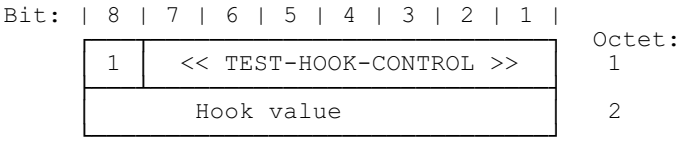
Restart value coding (octet 2):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	Restart timer
	0 0 0 0 0 0 0 1	Stop timer

All other values reserved.

7.6.10 Test hook control

The purpose of the <<TEST-HOOK-CONTROL>> element is to convey the remote control of the PT hook switch for testing.



TEST-HOOK-CONTROL information element

Hook value coding (octet 2):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	On-Hook
	0 0 0 0 0 0 0 1	Off-Hook

All other values reserved.

7.7 Variable length information elements

7.7.1 Summary

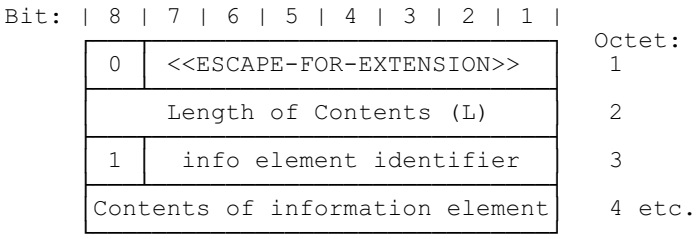
This table defines the coding that shall be used for the first octet of these elements, this octet uniquely identifies each element.

The reference number in the last column refers to the subclause where the detailed coding of the element shall be found.

Table 15: Variable length information element coding

	Bits								Reference
Variable Length Elements	8	7	6	5	4	3	2	1	
Info Type	0	0	0	0	0	0	0	1	7.7.20
Identity type	0	0	0	0	0	0	1	0	7.7.19
Portable identity	0	0	0	0	0	1	0	1	7.7.30
Fixed identity	0	0	0	0	0	1	1	0	7.7.18
Location area	0	0	0	0	0	1	1	1	7.7.25
NWK assigned identity	0	0	0	0	1	0	0	1	7.7.28
AUTH-TYPE	0	0	0	0	1	0	1	0	7.7.4
Allocation type	0	0	0	0	1	0	1	1	7.7.2
RAND	0	0	0	0	1	1	0	0	7.7.32
RES	0	0	0	0	1	1	0	1	7.7.35
RS	0	0	0	0	1	1	1	0	7.7.36
IWU attributes	0	0	0	1	0	0	1	0	7.7.21
Call attributes	0	0	0	1	0	0	1	1	7.7.5
Service change info	0	0	0	1	0	1	1	0	7.7.38
Connection attributes	0	0	0	1	0	1	1	1	7.7.11
Cipher info	0	0	0	1	1	0	0	1	7.7.10
Call identity	0	0	0	1	1	0	1	0	7.7.6
Connection identity	0	0	0	1	1	0	1	1	7.7.12
Facility	0	0	0	1	1	1	0	0	7.7.15
Progress indicator	0	0	0	1	1	1	1	0	7.7.31
MMS Generic Header	0	0	1	0	0	0	0	0	7.7.47
MMS Object Header	0	0	1	0	0	0	0	1	7.7.48
MMS Extended Header	0	0	1	0	0	0	1	0	7.7.49
Time-Date	0	0	1	0	0	0	1	1	7.7.50
Multi-Display	0	0	1	0	1	0	0	0	7.7.26
Multi-Keypad	0	0	1	0	1	1	0	0	7.7.27
Feature Activate	0	0	1	1	1	0	0	0	7.7.16
Feature Indicate	0	0	1	1	1	0	0	1	7.7.17
Network parameter	0	1	0	0	0	0	0	1	7.7.29
Ext h/o indicator	0	1	0	0	0	0	1	0	7.7.51
ZAP field	0	1	0	1	0	0	1	0	7.7.44
Service class	0	1	0	1	0	1	0	0	7.7.39
Key	0	1	0	1	0	1	1	0	7.7.24
Reject Reason	0	1	1	0	0	0	0	0	7.7.34
Set-up capability	0	1	1	0	0	0	1	0	7.7.40
Terminal capability	0	1	1	0	0	0	1	1	7.7.41
End-to-End compatibility	0	1	1	0	0	1	0	0	7.7.14
Rate parameters	0	1	1	0	0	1	0	1	7.7.33
Transit Delay	0	1	1	0	0	1	1	0	7.7.42
Window size	0	1	1	0	0	1	1	1	7.7.43
Calling Party Number	0	1	1	0	1	1	0	0	7.7.9
Called Party Number	0	1	1	1	0	0	0	0	7.7.7
Called Party Subaddr	0	1	1	1	0	0	0	1	7.7.8
Duration	0	1	1	1	0	0	1	0	7.7.13
Segmented info	0	1	1	1	0	1	0	1	7.7.37
Alphanumeric	0	1	1	1	0	1	1	0	7.7.3
IWU-to-IWU	0	1	1	1	0	1	1	1	7.7.23
Model identifier	0	1	1	1	1	0	0	0	7.7.46
IWU-PACKET	0	1	1	1	1	0	1	0	7.7.22
Escape to proprietary	0	1	1	1	1	0	1	1	7.7.45
Escape for extension	0	1	1	1	1	1	1	1	(note)
All other values are reserved									

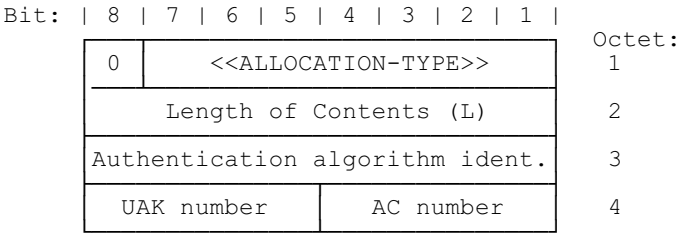
NOTE: When the <<ESCAPE-FOR-EXTENSION>> is used, the information element identifier is contained in octet 3 and the content of the information element follows in the subsequent octets as shown in the figure below.



Information element format using ESCAPE-FOR-EXTENSION

7.7.2 Allocation type

The purpose of the <<ALLOCATION-TYPE>> information element is to define the authentication parameters for the key allocation procedure.



ALLOCATION-TYPE information element

Authentication algorithm identifier coding (octet 3):

Bits 8 7 6 5 4 3 2 1 Meaning
0 0 0 0 0 0 0 1 DECT standard authentication algorithm 1
All other values reserved.

User Authentication Key (UAK) number coding (octet 4):

Bits 8 7 6 5 Meaning
Contains the binary coded number under which the allocated UAK shall be stored
If the MSB (bit 8) is set to 0, then the key shall be related to the active IPUI
If the MSB (bit 8) is set to 1, then the key shall be related to the active IPUI/PARK pair

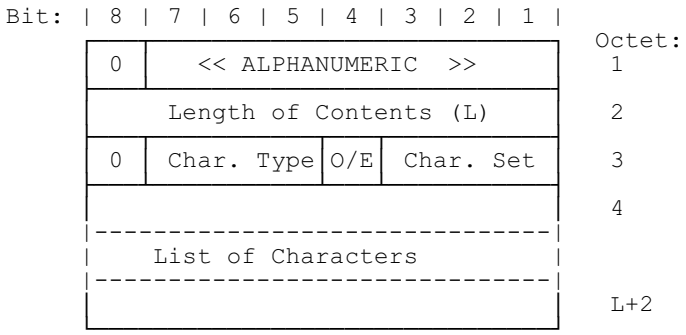
Authentication Code (AC) number (octet 4):

Bits 4 3 2 1 Meaning
Contains the binary coded number of the selected authentication code
If the MSB (bit 4) is set to 0, then the key shall be related to the active IPUI
If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair

7.7.3 Alphanumeric

The purpose of the <<ALPHANUMERIC>> element is to provide a transport mechanism for a family of alternative character sets in both directions.

This element shall not be used to carry dialling information.



ALPHANUMERIC information element

Character type coding:

Bits 7 6 5	Meaning (Character type)
0 0 0	User specific
0 0 1	Standard 8-bit characters
0 1 0	Standard 4-bit characters

All other values reserved.

Odd/even coding:

Bits 4	Meaning
0	Even number of characters
1	Odd number of characters

NOTE: The odd/even flag is only used when the character type is 4 bit. In all other cases it should be set to "even".

Standard 8-bit character set coding
Character set coding:

Bits 3 2 1	Meaning (Character set)
0 0 0	Reserved
0 0 1	DECT standard 8-bit characters (annex D)
0 1 0	IA5 characters (CCITT Recommendation T.50 [14])
0 1 1	Reserved (ISO Publication 2022 [15])
1 0 0	ERMES 7-bit characters (ETS 300 133-1 to -7 [16])
1 0 1	Reserved [CT2/CAI characters]
1 1 0	Standard ASCII (7 bit) characters (ANSI X 3.4-1986)

All 8-bit characters shall always be coded with one character per octet. Multiple characters shall be interpreted in the order of ascending octet numbers. Characters that are originally coded in less than 8-bits shall be padded up to 8-bits as follows:

- the original character is placed in the octet, with the least significant bit in bit position "1";

- any unused bit positions are filled with "0".

Standard 4-bit character set coding
Character set coding:

Bits 3 2 1	Meaning (Character set)
0 0 0	Reserved
0 0 1	DECT standard 4-bit characters (annex D)
1 0 0	ERMES 4-bit characters (ETS 300 133-1 to -7 [16])

All other values reserved.

4-bit characters shall always be coded with two characters per octet. Multiple characters shall be interpreted in the order of ascending octet numbers, and within each octet the high placed character (bits position 5-8) first.

7.7.4 Auth type

The purpose of the <<AUTH-TYPE>> information element is to define the authentication algorithm and the authentication key. In addition it may be used to send a ZAP increment command and/or to indicate if the cipher key shall be updated and/or sent.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< AUTH-TYPE >>							1
	Length of Contents (L)								2
	Authentication algorithm ident.								3
	Proprietary algorithm ident.								3a
	Auth. key type				Auth. key nr.				4
	INC	0	TXC	UPC	Cipher key nr.				5

AUTH-TYPE information element

Authentication algorithm identifier coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 1	DECT standard authentication algorithm 1
	0 1 0 0 0 0 0 0	GSM authentication algorithm
	0 1 1 1 1 1 1 1	Escape to proprietary algorithm identifier

All other values reserved.

Proprietary algorithm identifier (octet 3a):

This octet shall only be sent, when the authentication algorithm identifier coding (octet 3) indicates "escape to proprietary algorithm identifier".

Authentication Key (AK) type coding (octet 4):

Bits	8 7 6 5	Meaning
	0 0 0 1	User authentication key
	0 0 1 1	User personal identity
	0 1 0 0	Authentication code

All other values reserved.

NOTE: The User Personal Identity (UPI) is always used in combination with an User Authentication Key (UAK), therefore the key type UPI identifies always a pair of keys (UPI plus UAK).

Authentication Key (AK) number (octet 4):

Bits	4 3 2 1	Meaning

Contains the binary coded number of the selected Authentication Key (AK)
If the MSB (bit 4) is set to 0, then the key shall be related to the active IPUI
If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair

INC bit coding (octet 5):

Bits 8	Meaning
0	leave value of the ZAP field unchanged
1	increment value of the ZAP field

TXC bit coding (octet 5):

Bits 6	Meaning
0	do not include the derived cipher key in the {AUTHENTICATION-REPLY} message
1	include the derived cipher key in the {AUTHENTICATION-REPLY} message

UPC bit coding (octet 5):

Bits 5	Meaning
0	do not store the derived cipher key
1	store the derived cipher key under the given cipher key number

Cipher key number (octet 5):

Bits 4 3 2 1 Meaning

If the UPC bit is set to 1, then this field contains the binary coded number which is given to the newly derived cipher key
If the MSB (bit 4) is set to 0, then the key shall be related to the active IPUI
If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair
If the UPC bit is set to 0, then this field is not applicable and should be set to 0

NOTE: A derived cipher key is always related to the active IPUI and can be uniquely identified by the following three parameters, IPUI, cipher key type "derived" and cipher key number. A derived cipher key is not related to any specific cipher algorithm.

7.7.5 Call attributes

The purpose of the <<CALL-ATTRIBUTES>> element is to describe the higher layer service to be provided by the DECT protocol. The element may be repeated in a set-up message when using service negotiation.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< CALL-ATTRIBUTES >>							1
Length of Contents (L)								2
1	Coding std.	NWK Layer Attributes						3
1	C-plane class		C-plane routing					4
0/1	U-plane symm	LU identification						5
1	0 0 spare	LU identification F=>P direction						5a
0/1	U-plane class		U-plane frame type;					6
1	U-plane class F=>P		U-plane frame type; F=>P					6a

CALL-ATTRIBUTES information element

Coding standard (octet 3):

Bits	7 6	Meaning
	0 0	DECT standard coding

All other values reserved.

NWK layer attributes (octet 3):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	Undefined
	0 0 0 0 1	Basic speech
	0 1 0 0 0	DECT GSM IWP profile phase 2

All other values reserved.

C-plane class (octet 4):

Bits	7 6 5	Meaning
	0 0 0	Class U link; shared
	0 1 0	Class A link; shared
	1 0 0	Class B link; shared
	1 0 1	Class B link; independent

All other values reserved.

C-plane routing (octet 4):

Bits	4 3 2 1	Meaning
	0 0 0 0	C_S only
	0 0 0 1	C_S preferred / C_F accepted
	0 0 1 0	C_F preferred / C_S accepted
	0 1 0 0	C_F only
	1 1 0 0	C_F only; dedicated bearer (note)

All other values reserved.

NOTE: When "dedicated bearer" is indicated, at least one bearer of the MAC connection is reserved for the C_F channel (i.e. not to be used for U-plane information). Otherwise, the C_F channel may be routed to either a dedicated bearer or a non-dedicated bearer (a bearer that may also carry U-plane information) (see ETS 300 175-4 [4], subclause 9.5.1.2 for details of dedicated bearer operation).

U-plane symmetry (octet 5):

Bits	7 6	Meaning
	0 0	Symmetric
	1 0	Asymmetric

All other values reserved.

If symmetric, only octet 5 shall appear and this shall refer to both directions. If asymmetric octet 5 shall only refer to the direction P=>F and octet 5a shall refer to the direction F=>P.

LU identification (octet 5 and 5a):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 1	LU1
	0 0 0 1 0	LU2
	0 0 0 1 1	LU3
	0 0 1 0 0	LU4
	0 0 1 0 1	LU5
	0 0 1 1 0	LU6
	0 0 1 1 1	LU7
	0 1 0 0 0	}
	to	}reserved for LU8 to LU15
	0 1 1 1 1	}
	1 0 0 0 0	LU16

All other values reserved.

U-plane class (octets 6 and 6a):

Bits	7 6 5	Meaning
	0 0 0	Class 0 min_delay
	0 0 1	Class 0 normal_delay
	0 1 0	Class 1
	1 0 0	Class 2; Go_Back_N
	1 0 1	Class 2; SELective
	1 1 0	Class 3
	1 1 1	Not applicable

All other values reserved.

U-plane frame type (octets 6 and 6a):

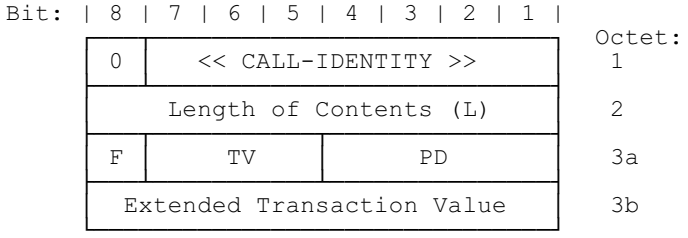
Bits	4 3 2 1	Meaning
	0 0 0 1	FU1
	0 0 1 0	FU2
	0 0 1 1	FU3
	0 1 0 0	FU4
	0 1 0 1	FU5
	0 1 1 0	FU6
	0 1 1 1	FU7

All other values reserved.

If symmetric is indicated in octet 5, only octet 6 shall appear and this shall refer to both directions. If asymmetric is indicated in octet 5, then octet 6 shall only refer to the direction P=>F and octet 6a shall refer to the direction F=>P.

7.7.6 Call identity

The purpose of the <<CALL-IDENTITY>> information element is to indicate the call identifier and the protocol discriminator of the calls to be ciphered.



CALL-IDENTITY information element

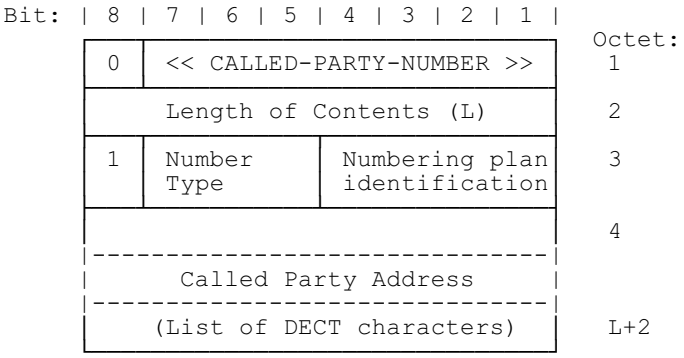
The fields in this element shall be used to identify the CC, MM or COMS call that is to be ciphered. It does this by encapsulating the transaction value and protocol discriminator of the relevant call. If this element is omitted, the ciphering shall be understood to apply to all active calls.

NOTE: In general, the TI and PD will be different from the TI and PD that appear at the beginning of the message.

- for flag and transaction value coding (octet 3a) see subclause 7.3 (transaction identifier element);
- for protocol discriminator coding (octet 3a) see subclause 7.2 (protocol discriminator element);
- for extended transaction value coding (octet 3b) see subclause 7.3 (transaction identifier element).

7.7.7 Called party number

The purpose of the <<CALLED-PARTY-NUMBER>> element is to identify the called party of a call in an en-bloc format.



CALLED-PARTY-NUMBER information element

Number type (octet 3):

Bits	7 6 5	Meaning
	0 0 0	Unknown
	0 0 1	International number
	0 1 0	National number
	0 1 1	Network specific number
	1 0 0	Subscriber number
	1 1 0	Abbreviated number
	1 1 1	Reserved for extension

All other values reserved.

Numbering plan identification (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	Unknown
	0 0 0 1	ISDN/telephony plan Rec. E.164/E.163 (note 1)
	0 0 1 1	Data plan Rec. X.121 (note 1)
	0 1 1 1	TCP/IP address (note 2)
	1 0 0 0	National standard plan (note 1)
	1 0 0 1	Private plan (note 1)
	1 0 1 1	Internet character format address (note 1)
	1 1 0 0	LAN MAC address (note 1)
	1 1 0 1	X.400 address (note 1)
	1 1 1 0	Profile service specific alphanumeric identifier (note 3)
	1 1 1 1	Reserved for extension

All other values reserved.

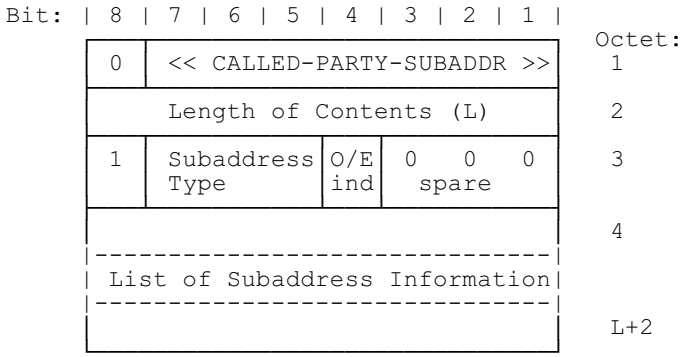
NOTE 1: Standard IA5 codes (see D.2.3) are used. Bit number 8 is zero.

NOTE 2 The address shall be indicated as a natural binary code.

NOTE 3 The significance and format is defined in the associated profile for the selected service.

7.7.8 Called party subaddress

The purpose of the <<CALLED-PARTY-SUBADDRESS>> element is to identify the subaddress of the called party of a call.



CALLED-PARTY-SUBADDRESS information element

Subaddress type (octet 3):

Bits	7 6 5	Meaning
	0 0 0	NSAP; CCITT Recommendation X.213/ISO Publication 8348 [24]
	0 1 0	User specified
	1 0 0	Profile service specific alphanumeric identifier (NOTE)

All other values reserved.

NOTE The significance and format is defined in the associated profile for the selected service.

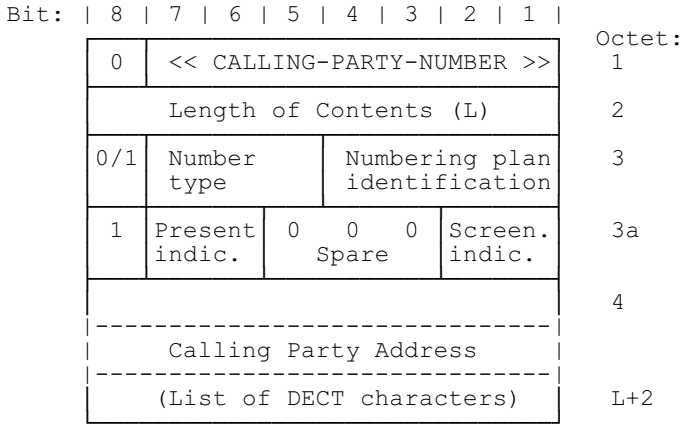
Odd/even (octet 3):

Bits	4	Meaning
	0	Even number of address signals
	1	Odd number of address signals

NOTE: The odd/even flag is used when the type of subaddress is "user specified" and the coding is Binary Coded Decimal (BCD). In all other cases it should be set to "even".

7.7.9 Calling party number

The purpose of the <<CALLING-PARTY-NUMBER>> element is to identify the calling party of a call in an en-bloc format.



CALLING-PARTY-NUMBER information element

Number type (octet 3):

Bits	7 6 5	Meaning
	0 0 0	Unknown
	0 0 1	International number
	0 1 0	National number
	0 1 1	Network specific number
	1 0 0	Subscriber number
	1 1 0	Abbreviated number
	1 1 1	Reserved for extension

All other values reserved.

Numbering plan identification (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	Unknown
	0 0 0 1	ISDN/telephony plan Rec. E.164/E.163 (note 1)
	0 0 1 1	Data plan Rec. X.121 (note 1)
	0 1 1 1	TCP/IP address (note 2)
	1 0 0 0	National standard plan (note 1)
	1 0 0 1	Private plan (note 1)
	1 0 1 1	Internet character format address (note 1)
	1 1 0 0	LAN MAC address (note 1)
	1 1 0 1	X.400 address (note 1)
	1 1 1 0	Profile service specific alphanumeric identifier (note 3)
	1 1 1 1	Reserved for extension

All other values reserved.

Presentation indicator (octet 3a):

Bits	7 6	Meaning
	0 0	Presentation allowed
	0 1	Presentation restricted
	1 0	Number not available
	1 1	Reserved.

Screening indicator (octet 3a):

Bits	2 1	Meaning
	0 0	User-provided, not screened
	0 1	User-provided, verified and passed
	1 0	User-provided, verified and failed
	1 1	Network provided.

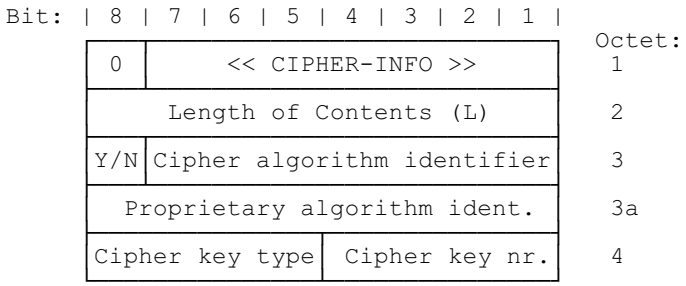
NOTE 1: Standard IA5 codes (see D.2.3) are used. Bit number 8 shall be set to zero.

NOTE 2 The address shall be indicated as a natural binary code.

NOTE 3 The significance and format is defined in the associated profile for the selected service.

7.7.10 Cipher info

The purpose of the <<CIPHER-INFO>> information element is to indicate if a call shall be ciphered or not. In the case of ciphering it defines the cipher algorithm and the cipher key.



CIPHER-INFO information element

Y/N bit coding (octet 3):

Bits	8	Meaning
	0	Disable ciphering
	1	Enable ciphering.

Cipher algorithm identifier coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 1	DECT standard cipher algorithm 1
	1 1 1 1 1 1 1	Escape to proprietary algorithm identifier

All other values reserved.

Proprietary algorithm identifier (octet 3a):

This octet shall only be sent, when the cipher algorithm identifier coding (octet 3) indicates "escape to proprietary algorithm identifier".

Cipher key type coding (octet 4):

Bits	8 7 6 5	Meaning
	1 0 0 1	Derived cipher key
	1 0 1 0	Static cipher key

All other values reserved.

Cipher key number (octet 4):

Bits 4 3 2 1 Meaning

Contains the binary coded number of the selected cipher key.
If the most significant bit (bit 4) is set to 0, then the key shall be related to the active IPUI.
If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair.

NOTE: Different sets of static cipher keys could be used in different systems.

7.7.11 Connection attributes

The purpose of the <<CONNECTION-ATTRIBUTES>> element is to describe the connections that are required for the requested service.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< CONNECTION-ATTRIBUTES >>							1
Length of Content (L)								2
1	Symmetry			Connection identity				3
0/1	0	0	Target bearers P=>F direction					4
0/1	0	1	Minimum bearers P=>F direction					4a
0/1	1	0	Target bearers F=>P direction					4b
1	1	1	Minimum bearers F=>P direction					4c
0/1	Slot size			MAC service				5
1	0	0	0	MAC service F=>P				5a
0/1 ext	CF chan. attributes			MAC packet lifetime				6
1	CF chan. atts F=>P			MAC packet lifetime F=>P				6a

CONNECTION-ATTRIBUTES information element

Symmetry:

Bits 7 6 5 Meaning

0 0 1 Symmetric connection
1 0 0 Asymmetric F to P with 1 duplex bearer
1 0 1 Asymmetric F to P with 2 target duplex bearers
1 1 0 Asymmetric P to F with 1 duplex bearer
1 1 1 Asymmetric P to F with 2 target duplex bearers
All other values reserved.

NOTE 1: A minimum of 1 duplex bearer is required for all asymmetric connections to provide the "pilot" bearer functions. Refer to ETS 300 175-3 [3].

Connection identity coding (octet 3):

Bits 4 3 2 1 Meaning

0 0 0 0 Unknown (not yet numbered)
1 N N N Advanced connection number NNN
All other values reserved.

NOTE 2: If already established, the (advanced) connection is identified using the Logical Connection Number (LCN) placed in position NNN.

Octets 4a, 4b and 4c are optional, but if present they shall appear in order shown. The following rules shall apply:

- if octet 4a is omitted, it shall be defaulted to the value given in octet 4;
- octets 4b and 4c shall be omitted if octet 3 indicates "symmetric";
- if octet 4c is omitted, it shall be defaulted to the value given in octet 4b.

NOTE 3: The meaning of octets 4, 4a, 4b and 4c is identified by the "bearer definition" coding in bits 7 and 6 as follows.

The Target and Minimum acceptable number of bearers specified in octet group 4 of this information element should be regarded as the range of bearers which is to be acceptable for the lifetime of the call (unless changed by a {CC-SERVICE-CHANGE} message procedure). The MAC may therefore dynamically change the number of MAC bearers during the lifetime of a call within these specified limits. If operation within the specified limits cannot be accomplished the call should be released.

Bearer definition coding (octets 4, 4a, 4b, 4c):

Bits 7 6	Meaning
0 0	Target number of bearers; P=>F direction
0 1	Minimum number of bearers; P=>F direction
1 0	Target number of bearers; F=>P direction
1 1	Minimum number of bearers; F=>P direction

Number of bearers coding (octets 4, 4a, 4b, 4c):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	No U-plane
n n n n n	Number of bearers ($1 \leq$ Number ≤ 31)

NOTE 4: The number of bearers is coded with the natural binary value, with the least significant bit in bit position "1". Allowable values are "1" to "31".

If symmetric is indicated in octet 3, only octet 5 and 6 shall appear and these shall refer to both directions. If asymmetric is indicated in octet 3, then octet 5 and 6 shall only refer to the direction P=>F and octets 5a and 6a shall refer to the direction F=>P.

In all of these fields the "number of bearers" coding refers to the total number of individual (simplex) bearers.

MAC slot size (octet 5):

Bits 7 6 5	Meaning
0 0 0	Half slot; j = 0.
1 0 0	full slot
1 0 1	double slot

All other values reserved.

MAC service (octets 5 and 5a):

Bits	4 3 2 1	Meaning
	0 0 0 0	I_N; minimum delay
	0 0 0 1	I_N; normal delay
	0 0 1 0	I_P; detect only
	0 0 1 1	I_P; Mod-2 correct

All other values reserved.

CF channel attributes (octets 6 and 6a):

Bits	7 6 5	Meaning
	0 0 0	C_F never (CS only)
	0 1 0	C_F Demand/1 bearer (interrupting)
	0 1 1	C_F Demand/2 bearers (interrupting)
	1 0 0	C_F Reserved/1 bearer (non-interrupting)
	1 0 1	C_F Reserved/2 bearers (non-interrupting)

All other values reserved.

NOTE 5: The C_F channel attributes indicate the intended usage of the C_F channel. In all cases the actual C_F usage is defined on a slot-by-slot basis for each connection by the DLC layer.

NOTE 6: The maximum packet lifetime (nnn) is only defined if the MAC service (octet 5 or 5a as appropriate) indicates IP error_correct. The value "nnn" defines the allowed values of maximum packet lifetime using the coding given in subclause 7.2.5.3.8 of ETS 300 175-3 [3]. In this coding nnn = (0) indicates unlimited lifetime, and nnn = (1..7) indicates the maximum lifetime in TDMA frames. In all other cases the "Not applicable" coding is used.

MAC packet lifetime (octets 6 and 6a):

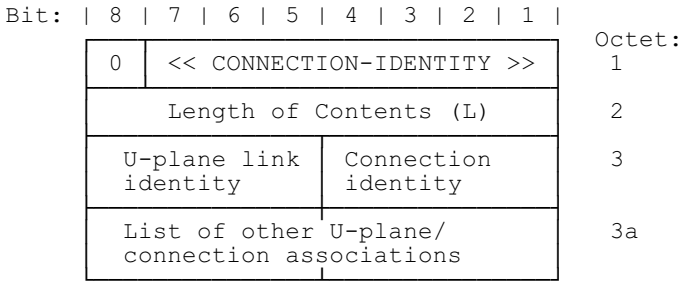
Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	1 n n n	Maximum packet lifetime (IP; Mod-2 operation only)

All other values reserved.

NOTE 7: The maximum packet lifetime (nnn) is coded with the natural binary value with the least significant bit in bit position "1". The allowable values are "0" to "7". The value "0" is interpreted as unlimited (i.e. infinite). The values "1" to "7" define the maximum lifetime in TDMA frames. Refer to ETS 300 175-3 [3] for the use of this attribute.

7.7.12 Connection identity

The purpose of the <<CONNECTION-IDENTITY>> element is to explicitly associate one or more U-plane link with an advanced connection (or connections).



CONNECTION-IDENTITY information element

Each octet defines an association between one U-plane link and one MAC connection. All associations refer to one call as identified by the transaction identifier (transaction identifier information element at the start of the message).

Connection identity coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Unknown (not yet numbered)
1 N N N	Advanced connection number NNN

All other values reserved.

NOTE 1: If already established, the (advanced) connection is identified using the Logical Connection Number (LCN) placed in position NNN.

U-plane link identity coding:

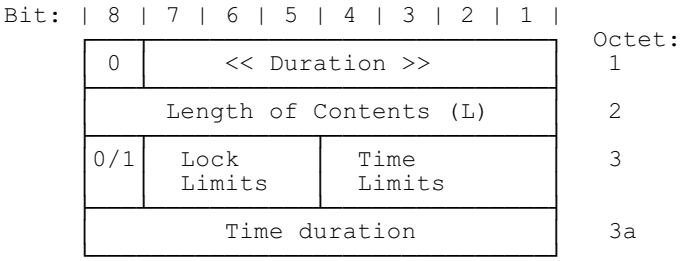
Bits 8 7 6 5	Meaning
0 0 0 0	Unnumbered link
1 N N N	Numbered link

For further study
All other values reserved.

NOTE 2: Most calls only contain 1 unnumbered U-plane link. Numbered links use the 3-bit U-plane Link Number (ULN) placed in position NNN. Refer to ETS 300 175-4 [4], subclause 13.2, for details of U-plane link number coding.

7.7.13 Duration

The purpose of the <<DURATION>> information element is to indication a time duration.



DURATION information element

Lock limits coding (octet 3):

Bits 7 6 5	Meaning
1 1 0	Temporary user limit (note 1)
1 1 1	No limits

NOTE 1: "Temporary user limit" indicates that a time limit applies when the PP leaves the locked state with the relevant FP (see ETS 300 175-6 [5]).

Time limits coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Erase (time limit zero)
0 0 0 1	Defined time limit 1
0 0 1 0	Defined time limit 2
0 1 0 0	Standard time limit (note 2)
1 1 1 1	Infinite

If a defined time limit is indicated, octet 3a shall follow.

NOTE 2: If a standard time limit is indicated, the standard time limit for the relevant procedure applies.

Time duration (octet 3a)

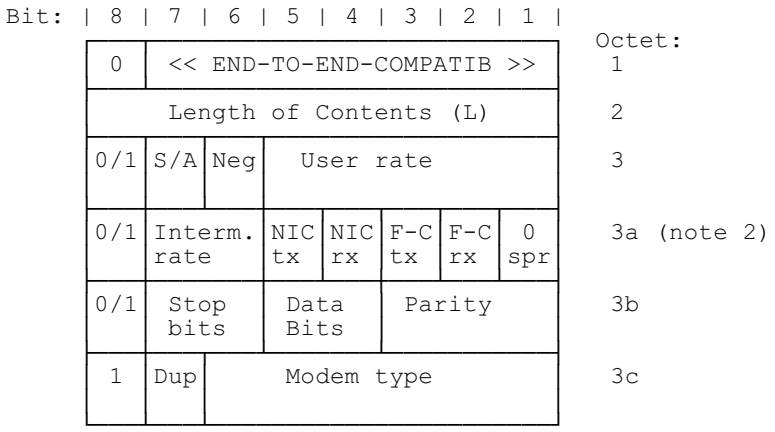
The time duration is binary coded (bit 1 being the least significant bit). The time duration defines time in units based on the MAC layer multiframes. Multiframes are defined in ETS 300 175-3 [3].

Defined time limit 1: 1 unit = 2E8 multiframes.
Defined time limit 2: 1 unit = 2E16 multiframes (note 3).

NOTE 3: This unit corresponds to the most significant octet of the multiframe counter that may be transmitted by FPs (see ETS 300 175-3 [3]).

7.7.14 End-to-end compatibility

The purpose of the <<END-TO-END-COMPATIBILITY>> element is to exchange some aspects of the end-to-end data terminal capabilities between PT and FT during call establishment.



END-TO-END-COMPATIBILITY information element

NOTE 1: This information element may only be included in a {CC-SETUP} message that also contains the <<IWU-ATTRIBUTES>> element.

NOTE 2: This octet is included if the service V.110/X.30 rate adaption is indicated in the <<IWU-ATTRIBUTES>>. Octet 3a may be included in other cases to extend into octets 3b and 3c but octet 3a should be ignored in these other cases.

Synchronous/Asynchronous (S/A) (octet 3):

Bits 7	Meaning
0	Synchronous
1	Asynchronous

NOTE 3: Octets 3a, 3b, 3c may be omitted if octet 3 indicates "synchronous" user rates.

Negotiation (Neg) (octet 3):

Bits 6	Meaning
0	In-band negotiation not possible
1	In band negotiation possible (note 4)

NOTE 4: "In band negotiation possible" is only used in the context of V.110/X.30 rate adaption.

User rate coding (octet 3):

Bits 5 4 3 2 1	Meaning	
0 0 0 0 1	0,6 kbit/s;	V.6 and X.1.
0 0 0 1 0	1,2 kbit/s;	V.6.
0 0 0 1 1	2,4 kbit/s;	V.6 and X.1.
0 0 1 0 0	3,6 kbit/s;	V.6.
0 0 1 0 1	4,8 kbit/s;	V.6 and X.1.
0 0 1 1 0	7,2 kbit/s;	V.6.
0 0 1 1 1	8,0 kbit/s;	I.460.
0 1 0 0 0	9,6 kbit/s;	V.6 and X.1.
0 1 0 0 1	14,4 kbit/s;	V.6.
0 1 0 1 0	16 kbit/s;	I.460.
0 1 0 1 1	19,2 kbit/s;	V.6.
0 1 1 0 0	32 kbit/s;	I.460.
0 1 1 1 0	48 kbit/s;	V.6 and X.1.
0 1 1 1 1	56 kbit/s;	V.6.
1 0 0 0 0	64 kbit/s;	X.1.
1 0 1 0 1	0,1345 kbit/s;	X.1.
1 0 1 1 0	0,1 kbit/s;	X.1.
1 0 1 1 1	0,075/1,2 kbit/s;	V.6 and X.1. (note 5)
1 1 0 0 0	1,2/0,075 kbit/s;	V.6 and X.1. (note 5)
1 1 0 0 1	0,050 kbit/s;	V.6 and X.1.
1 1 0 1 0	0,075 kbit/s;	V.6 and X.1.
1 1 0 1 1	0,110 kbit/s;	V.6 and X.1.
1 1 1 0 0	0,150 kbit/s;	V.6 and X.1.
1 1 1 0 1	0,200 kbit/s;	V.6 and X.1.
1 1 1 1 0	0,300 kbit/s;	V.6 and X.1.
1 1 1 1 1	12 kbit/s;	V.6.

All other values reserved.

NOTE 5: The first rate is the transmit rate in the forward direction of the call. The second rate is the transmit rate in the backward direction of the call.

NOTE 6: see CCITT V-series Recommendations [27].

see CCITT X-series Recommendations [28].

see CCITT I.460 Recommendation [29].

Intermediate rate (interim rate) (octet 3a):

Bits 7 6	Meaning
0 0	Not used
0 1	8 kbit/s
1 0	16 kbit/s
1 1	32 kbit/s

Network Independent Clock on transmission (NIC tx) (octet 3a):

Bits 5	Meaning
0	Not required to send data with network independent clock
1	Required to send data with network independent clock

NOTE 7: NIC tx refers to transmission in the forward direction of the call.

NOTE 8: See CCITT Recommendations V.110 [27] and X.30 [28].

Network Independent Clock on reception (NIC rx) (octet 3a):

Bits 4	Meaning
0	Cannot accept data with Network independent clock
1	Required to send data with Network independent clock

NOTE 9: NIC rx refers to transmission in the backward direction of the call.

NOTE 10: See CCITT Recommendations V.110 [27] and X.30 [28].

Flow-Control on transmission (F-C tx) (octet 3a):

Bits 3	Meaning
0	Not required to send data with flow control mechanism
1	Required to send data with flow control mechanism

NOTE 11: F-C tx refers to transmission in the forward direction of the call.

Flow-Control on reception (F-C rx) (octet 3a):

Bits 2	Meaning
0	Cannot accept data with flow control mechanism (i.e. sender does not support this optional procedure);
1	Can accept data with flow control mechanism (i.e. sender does support this optional procedure);

NOTE 12: F-C rx refers to transmission in the backward direction of the call.

Stop bits coding (octet 3b):

Bits 7 6	Meaning
0 0	Not used
0 1	1 bit
1 0	1,5 bits
1 1	2 bits

Data bits coding (octet 3b):

Bits 5 4	Meaning
0 0	Not used
0 1	5 bits
1 0	7 bits
1 1	8 bits

Parity coding (octet 3b):

Bits 3 2 1	Meaning
0 0 0	Odd
0 1 0	Even
0 1 1	None
1 0 0	Forced to 0
1 0 1	Forced to 1

All other values reserved.

Duplex mode (Dup) (octet 3c):

Bits 7	Meaning
0	Half duplex
1	Full duplex

Modem type (octet 3c):

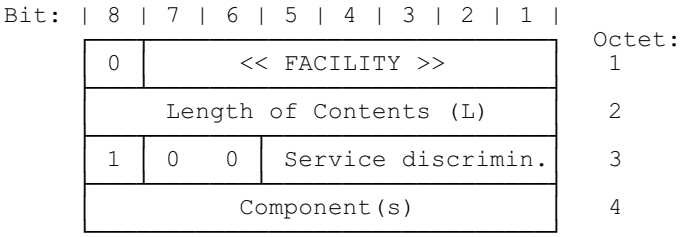
Bits	6 5 4 3 2 1	Meaning
	0 0 0 0 0 0	Reserved
	0 0 0 0 0 1	V.21
	0 0 0 0 1 0	V.22
	0 0 0 0 1 1	V.22 bis
	0 0 0 1 0 0	V.23
	0 0 0 1 0 1	V.26
	0 0 0 1 1 0	V.26 bis
	0 0 0 1 1 1	V.26 ter
	0 0 1 0 0 0	V.27
	0 0 1 0 0 1	V.27 bis
	0 0 1 0 1 0	V.27 ter
	0 0 1 0 1 1	V.29
	0 0 1 1 0 0	V.32
	0 0 1 1 0 1	V.35
	1 0 0 0 0 0 to	} Reserved for national use
	1 1 1 1 1 1	}

All other values reserved.

NOTE 13: see CCITT V-series Recommendations appear in [27].

7.7.15 Facility

The purpose of the <<FACILITY>> information element is to indicate the invocation and operation of supplementary services, identified by the corresponding operation value within the <<FACILITY>> information element.



FACILITY information element

Service discriminator coding:

Bits	5 4 3 2 1	Meaning
	1 0 0 0 1	Discriminator for supplementary service applications

All other values are reserved.

Regarding the coding and the use of the components, see ETS 300 196-1 [18].

7.7.16 Feature activate

The purpose of the <<FEATURE-ACTIVATE>> information element is to activate a feature as identified in the feature field.

Bit:	8	7	6	5	4	3	2	1	Octet:
0	<< FEATURE-ACTIVATE >>								1
Length of Contents (L)									2
0/1	Feature								3
1	Parameter								3a

FEATURE-ACTIVATE information element

Feature coding (octet 3):

Bits 7 6 5 4 3 2 1	Meaning	Parameter
0 0 0 1 1 1 1	external handover switch	no
0 1 0 0 0 0 0	queue entry request	no
0 1 1 0 0 0 0	indication of subscriber number	no
1 0 0 0 0 1 0	feature key	yes
1 0 0 0 1 0 0	specific line selection	yes
1 0 0 0 1 1 1	specific trunk carrier selection	yes
1 0 0 1 0 0 0	control of echo control functions	yes
1 1 0 0 0 0 0	cost information	yes
All other values reserved.		

External handover switch: indication from the PT to the FT that the call shall be immediately rerouted.

Queue entry request: request to enter outgoing call queue.

Indication of subscriber number: indication to the user of the subscriber number allocated to the user, e.g. during a temporary registration on a visited network.

Feature key:

Parameter (octet 3a)

Value (HEX)	Meaning
00	reserved
nn	feature key nn with 01 ≤ nn ≤ 7F

Specific line selection: the ability to select a specific line (internal or external) on which to make or receive a call.

Parameter (octet 3a):

Value (HEX)	Meaning
00	general selection
nn	selection nn with 01 ≤ nn ≤ 7F

Specific trunk carrier selection: the ability to select a specific trunk carrier for a call through a global network.

Parameter (octet 3a):

Value (HEX)	Meaning
00	default
nn	selection nn with 01 ≤ nn ≤ 7F

Control of echo control functions: the ability to connect or disconnect FP echo control functions, depending on e.g. the type of service and call routing information.

Parameter coding (octet 3a)

Bit 7 is reserved.

Bits 6 5	Meaning
0 0	option a) and b) disconnected (note 1)
0 1	only option a) connected (note 1)
1 0	only option b) connected (note 1)
1 1	no change (note 1)

Bits 4 3	Meaning
0 0	Disconnect for requirement 2 (note 2)
0 1	Connect · 9 dB for requirement 2 (note 2)
1 0	Connect reduced loss for requirement 2 (note 2)
1 1	No change for requirement 2 (note 2)

Bits 2 1	Meaning
0 0	Disconnect for requirement 1 (note 2)
0 1	Connect for requirement 1 (note 2)
1 0	Reserved for requirement 1 (note 2)
1 1	No change for requirement 1 (note 2)

NOTE 1: Refer to ETS 300 175-8 [7], subclause 7.4.1.2.

NOTE 2: Refer to ETS 300 175-8 [7], subclause 7.10.

Cost information: indication to the user of the call charge or call tariff. It may be used to invoke activation of this feature for all calls or on call-by-call basis. In the first case it is a Call Independent Supplementary Service (CISS) and the information element is placed in one of the CISS messages (see subclause 6.2.2). In the second case it is a Call Related Supplementary Service (CRSS) and the information element is placed in an allowed CC message as specified in subclause 6.3.

Parameter (octet 3a):

Bits 7 6 5	Meaning
0 0 1	DECT internal cost information
0 1 1	cost information for the complete connection

All other values reserved.

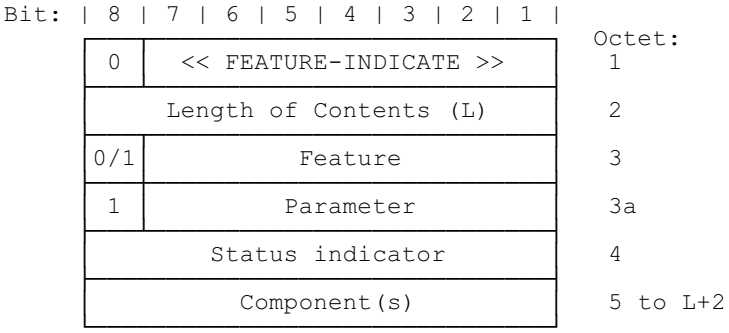
Parameter (octet 3a):

Bits 4 3 2 1	Meaning
0 0 0 0	tariff information
0 0 0 1	charging pulses during the call
0 0 1 0	calculated amount of charge at the end of the call

All other values reserved.

7.7.17 Feature indicate

The purpose of the <<FEATURE-INDICATE>> information element is to allow the FT to convey feature indications to the user regarding the status of an activated feature.



FEATURE-INDICATE information element

Feature coding (octet 3)

Bits	7 6 5 4 3 2 1	Meaning	Parameter
	0 0 0 1 1 1 1	external handover switch	no
	0 1 0 0 0 0 0	queue entry request	no
	0 1 1 0 0 0 0	indication of subscriber number	no
	1 0 0 0 0 1 0	feature key	yes
	1 0 0 0 1 0 0	specific line selection	yes
	1 0 0 0 1 1 1	specific trunk carrier selection	yes
	1 0 0 1 0 0 0	control of echo control functions	yes
	1 1 0 0 0 0 0	cost information	yes
	All other values reserved.		

The meaning of the features is the same as described in more detail for the <<FEATURE-ACTIVATE>> information element.

Parameter (octet 3a):

The parameter coding is the same as defined for the <<FEATURE-ACTIVATE>> information element.

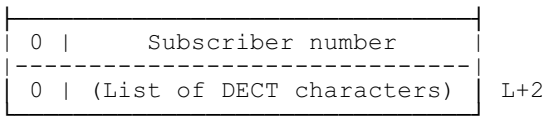
The status indicator field (octet 4) identifies the current status of an activated feature.

Status indicator coding:

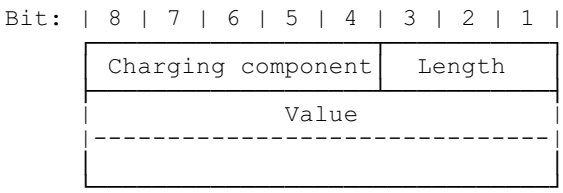
Bits	8 7 6 5 4 3 2 1	Status	Meaning
	1 0 0 0 0 0 0 0	Deactivated	Service request rejected
	1 0 0 0 0 0 0 1	Activated	Service request accepted, feature is activated
	1 0 0 0 0 0 1 1	Pending	Service request accepted, feature is pending
	1 0 0 0 0 1 0 0	Deactivated	Service busy
	1 0 0 0 0 1 1 0	Deactivated	Service unobtainable
	All other values reserved.		

Component coding (octet 5) for feature "queue entry request": the component consists of one octet. It gives the current position in the queue and is coded with the natural binary value.

Component coding (octet 5 to L+2) for feature "indication of subscriber number": the subscriber number shall be coded as a list of DECT standard characters as defined in annex D.



Component coding (octet 5 to L+2) for feature "cost information": when the <<FEATURE-INDICATE>> information element is used to carry "cost information" then one or more components can be included. Each of these components is coded as defined below:



Charging component coding:

Bits	8 7 6 5 4	Name	Meaning
	0 0 0 0 0	c0	reserved
	0 0 0 0 1	c1	units per interval
	0 0 0 1 0	c2	seconds per time interval
	0 0 0 1 1	c3	scaling factor
	0 0 1 0 0	c4	unit increment
	0 0 1 0 1	c5	units per data interval
	0 0 1 1 0	c6	segments per data interval
	0 0 1 1 1	c7	initial seconds per time interval
	0 1 0 0 0	c8	reserved
	0 1 0 0 1	c9	reserved
	0 1 0 1 0	c10	fixed cost for access to a specific network
	0 1 0 1 1	c11	calculated charged amount
	0 1 1 0 0	c12	fixed supplementary service cost
	0 1 1 0 1	c13	supplementary service cost per time interval
	0 1 1 1 0	c14	pulse
	0 1 1 1 1	c15	reserved
	1 0 - - -	c16-23	network proprietary components
	All other values reserved.		

Component c1: this component defines the number of unit increments per interval. It is set in terms of visited location area units per interval.

Component c2: this component defines the time interval for unitisation and is specified in seconds.

Component c3: this component defines the scaling factor to convert from visited location area units to home location area units. It is a dimensionless multiplier.

Component c4: this component defines the number of unit increments on receipt of the message containing the cost information. It is specified in units of the visited location area.

Component c5: this component defines the number of unit increments per data interval. It is set in terms of visited location area units per interval.

Component c6: this component defines the data usage interval for unitisation.

Component c7: this component defines the initial time interval for unitisation.

Component c10: this component defines a fixed cost for access to a specific network.

Component c11: this component defines the calculated cost in either the currency of the home location area or the visited location area.

Component c12: this component defines a fixed cost for a specific supplementary service.

Component c13: this component defines the cost per time interval for a specific supplementary service.

Component c14: this component represents one pulse.

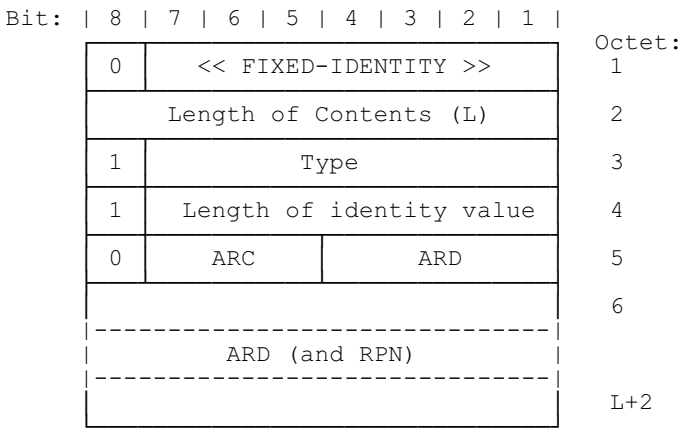
Length coding: this 3 bit number defines the length of the value field in octets and is coded with the natural binary value.

Value coding: this field contains the value of the charging components and is coded with the natural binary value.

Component	Resolution of the value
c1	0,1
c2	0,1
c3	0,01
c4	0,1
c5	0,1
c6	1,0
c7	0,1
c10	0,1
c11	0,1
c12	0,1
c13	0,1
c14	0,1

7.7.18 Fixed identity

The purpose of the <<FIXED-IDENTITY>> information element is to transport a DECT fixed identity or a Portable Access Rights Key (PARK). Refer to ETS 300 175-6 [5], describing identities and addressing.



FIXED-IDENTITY information element

Type coding (octet 3):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Access rights identity
0 0 0 0 0 0 1	Access rights identity plus radio fixed part number
0 1 0 0 0 0 0	Portable access rights key
All other values reserved.	

Length of identity value coding (octet 4): the length is defined in bits, and this is coded with the natural binary value. The least significant bit of the coding appears in bit position 1.

Length of identity value coding for identity type "ARI".
Length of identity value coding = 1 + (number of ARI bits).

Length of identity value coding for identity type "ARI + RPN":

Bits 7 6 5 4 3 2 1	Meaning
0 1 0 1 0 0 0	40 bits

Length of identity value coding for identity type "PARK":
Length of identity value = 1 + PARK length indicator

Access rights class coding (octet 5): refer to ETS 300 175-6 [5].

Access Rights Details (ARD) coding (octet 5 to L+2): refer to ETS 300 175-6 [5]. The MSB of the ARD is bit 4 in octet 5. The order of bit values progressively decreases as the octet number increases. Unused bits in the last octet should be coded as 0.

Radio fixed Part Number (RPN) (octet L+2): for identity type "ARI + RPN" also the RPN is contained, where the LSB of the RPN is bit 1 in octet L+2. For the identity types "ARI" and "PARK" no RPN is included.

7.7.19 Identity type

The purpose of the <<IDENTITY-TYPE>> information element is to indicate a specific identity type, e.g. used by the FT when requesting for a specific PT identity. Refer to ETS 300 175-6 [5].

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< IDENTITY-TYPE >>							1
Length of contents (L)								2
1	0	0	0	Identity group				3
1	Type							4

IDENTITY-TYPE information element

Identity group coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Portable identity
0 0 0 1	Network assigned identity
0 1 0 0	Fixed identity (also including the Portable Access Rights Key PARK)
1 1 1 1	Proprietary (application specific)

All other values reserved.

Type coding for identity group "portable identity" (octet 4):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	International Portable User Identity (IPUI)
0 0 1 0 0 0 0	International Portable Equipment Identity (IPEI)
0 1 0 0 0 0 0	Temporary Portable User Identity (TPUI)

All other values reserved.

Type coding for identity group "fixed identity" (also including PARK) (octet 4):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Access rights identity
0 0 0 0 0 0 1	Access rights identity plus radio fixed part number
0 1 0 0 0 0 0	Portable Access Rights Key (PARK)

All other values reserved.

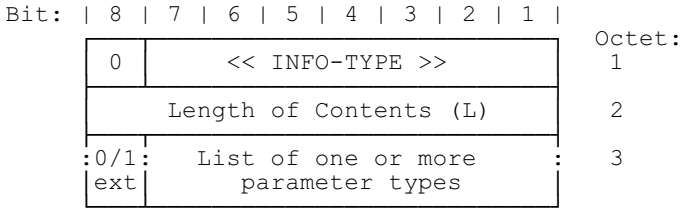
Type coding for identity group "network assigned identity" (octet 4):

Bits	7 6 5 4 3 2 1	Meaning
	1 1 1 0 1 0 0	GSM temporary mobile subscriber identity
	1 1 1 1 1 1 1	Proprietary (application specific)

All other values reserved.

7.7.20 Info type

The purpose of the <<INFO-TYPE>> information element is to indicate the type (or types) of requested or transmitted information.



INFO-TYPE information element

Parameter type coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	locate suggest
	0 0 0 0 1 0 0	authentication of PP failure
	0 0 0 1 0 0 0	external handover parameters (note)
	0 0 0 1 0 0 1	location area
	0 0 0 1 0 1 0	hand over reference
	0 0 0 1 0 1 1	multiframe and PSCN synchronised external handover candidate
	0 0 0 1 1 0 0	external handover candidate
	0 0 0 1 1 0 1	multiframe synchronised external handover candidate
	0 0 0 1 1 1 1	multiframe, PSCN and multiframe number synchronised external handover candidate
	0 0 0 1 1 1 0	non synchronised external handover candidate
	0 0 1 0 0 0 0	old fixed part identity
	0 0 1 0 0 0 1	old network assigned identity
	0 0 1 0 0 1 0	old network assigned location area
	0 0 1 0 0 1 1	old network assigned handover reference
	0 1 0 0 0 0 0	billing
	0 1 0 0 0 0 1	debiting
	0 1 0 0 0 1 0	CK transfer
	0 1 0 0 0 1 1	handover failed, reversion to old channel

All other values reserved.

NOTE: external handover parameters includes both handover reference and external handover candidate(s).

7.7.21 InterWorking Unit (IWU) attributes

The purpose of the <<IWU-ATTRIBUTES>> element is to provide a means for service compatibility information to be exchanged (e.g. between a PP application and a FP interworking unit). This element is transferred transparently by the DECT protocol entities.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< IWU-ATTRIBUTES >>							1
	Length of Contents (L)								2
	1	Coding Std.							3
									etc

IWU-ATTRIBUTES information element

Coding standard (octet 3):

Bits 7 6 Meaning
0 0 DECT standard coding
0 1 Profile defined coding
All other values reserved

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	0	Info. Transfer Capability					3
	1	Negotiation indicator		External Connection Type					4
	0/1	Trans mode		Information Transfer rate					5
	0/1	Unit rate		Rate Multiplier					5a
	0/1	Structure			Config		Estab.		5b
	0/1	Symm		Info. Trans. Rate. (Dest=>Originator)					5c
	1	Unit rate		Rate Multiplier (Dest=>Originator)					5d
	0/1	0	0	User protocol ID					6
	0/1	1	1	L3 protocol ID					6a
	0/1 ext	1	0	L2 protocol ID					6b

IWU-ATTRIBUTES information element for DECT standard coding

Information transfer capability (octet 3):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	Speech
0 1 0 0 0	Unrestricted digital information
0 1 0 0 1	Restricted digital information
1 0 0 0 0	3,1 kHz audio
1 0 0 0 1	7,0 kHz audio
1 0 1 0 0	Fax
1 1 0 0 0	Video

All other values reserved.

Negotiation indicator (octet 4):

Bits 7 6 5	Meaning
0 0 0	Negotiation not possible
1 0 0	Exchanged parameter negotiation
0 1 0	Peer attribute negotiation
1 1 0	Exchanged attribute negotiation and Peer attribute negotiation

All other values reserved.

External connection type (octet 4):

Bits 4 3 2 1	Meaning
0 0 0 0	Not applicable
0 0 0 1	Connection oriented
0 0 1 0	Permanent Virtual Circuit
0 0 1 1	Non-permanent Virtual Circuit
0 1 0 0	Datagram
1 0 0 0	Connectionless

All other values reserved.

Transfer mode (octet 5):

Bits 7 6	Meaning
0 0	Circuit mode
1 0	Packet mode
1 1	None (no transfer mode required)

All other values reserved.

Information transfer rate (octet 5 and 5c):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	Packet mode calls
0 1 0 1 0	16 kbit/s
0 1 0 1 1	32 kbit/s
1 0 0 0 0	64 kbit/s
1 0 0 0 1	2 x 64 kbit/s
1 0 0 1 1	384 kbit/s
1 1 1 1 0	Unspecified
1 1 1 1 1	Defined by rate multiplier

All other values reserved.

NOTE 1: When octet 5c is omitted, the transfer rate is symmetric. When octet 5c is included, the rate in octet 5 refers to the direction Orig=>Dest, and the rate in octet 5c refers to the reverse direction.

If the reserved coding "defined by rate multiplier" is used, then octet 5a shall follow. Octet 5d shall also follow if octet 5c is used (i.e. for asymmetric rates).

Structure (octet 5b)

Bits 7 6 5	Meaning
0 0 0	Default
0 0 1	8 kHz integrity
1 0 0	SDU integrity
1 1 1	Unstructured

All other values reserved.

If octet 5b is omitted, or the structure field is coded "default" the structure attribute shall be defaulted according to the following table:

Transfer mode	Transfer capability	Structure
circuit	speech	8 kHz integrity
circuit	restricted digital	8 kHz integrity
circuit	3,1 kHz audio	8 kHz integrity
circuit	7,0 kHz audio	8 kHz integrity
circuit	fax	8 kHz integrity
circuit	video	8 kHz integrity
packet	unrestricted digital	SDU integrity

Configuration (octet 5b):

Bits 4 3	Meaning
0 0	point-to-point

All other values reserved.

Establishment (octet 5b):

Bits 2 1	Meaning
0 0	demand

All other values reserved.

Unit rate (octet 5a and 5d):

Bits 7 6	Meaning
0 1	16 kbit/s steps
1 0	32 kbit/s steps
1 1	64 kbit/s steps

All other values reserved.

Rate multiplier (octet 5a and 5d):

Bits 5 4 3 2 1	Meaning
0 n n n n	Number of steps

All other values reserved.

NOTE 2: The number of steps (nnnn) relates to the unit rate defined in the same octet. The value is coded with the natural binary value, with the least significant bit in bit position "1". Allowable values for "number of steps" are "1" to "15".

Symmetry (octet 5c):

Bits 7 6	Meaning
0 0	bidirectional symmetric
1 0	unidirectional asymmetric
1 1	bidirectional asymmetric

All other values reserved.

All of the user protocol identifier (octets 6, 6a, 6b) are optional, but if present they shall appear in order shown. The meaning of each octet is identified by the coding of bits 7 and 6.

Protocol identifier coding (octets 6, 6a, 6b):

Bits 7 6	Meaning
0 0	User protocol IDentifier (ID)
1 1	L3 protocol ID
1 0	L2 protocol ID

All other values reserved.

User protocol ID (octet 6):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	User specific (escape)
0 0 0 0 1	V.110/X.30 rate adaption (note 6)
0 0 0 1 0	G.711 µ-law PCM
0 0 0 1 1	G.711 A-law PCM
0 0 1 0 0	G.721 ADPCM
0 0 1 0 1	H.221 and H.242
0 0 1 1 0	H.261 Video
0 0 1 1 1	Non-standard rate adaption
0 1 0 0 0	V.120 rate adaption
0 1 0 0 1	X.31 rate adaption
1 0 0 0 0	Group 3 fax
1 0 0 0 1	Group 4 fax
1 1 0 0 0	X.28/X.29

All other values reserved.

NOTE 3: If octet 6 indicates "V.110/X.30 rate adaption", the set-up message is also required to contain the <<END-TO-END-COMPATIBILITY>> element to define the attributes of the rate adaption service.

L3 protocol ID (octet 6a):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	User specific (escape)
0 0 0 1 0	ETS 300 102-1 [10]
0 0 1 1 0	CCITT Recommendation X.25 packet layer [52]
0 0 1 1 1	ISO Publication 8208 [23] (CCITT Recommendation X.25 packet level for DTE [52])
0 1 0 0 0	ISO Publication 8348 [24] (OSI C/O protocol)
0 1 0 0 1	ISO Publication 8473 [25] (OSI C/L service)
0 1 0 1 0	CCITT Recommendation T.70 [53], minimum network layer
1 0 0 1 0	GSM Recommendation 04.08 [11]

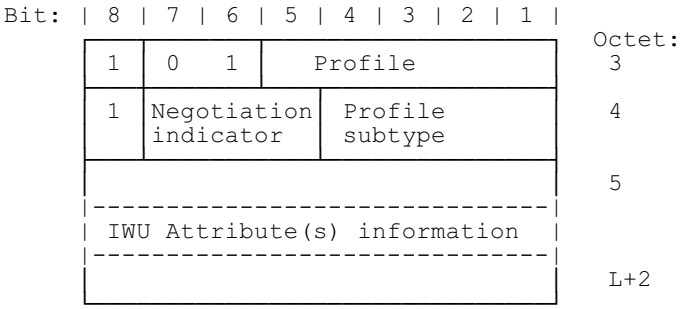
All other values reserved.

L2 protocol ID (octet 6b):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (escape)
	0 0 0 0 1	Basic mode ISO Publication 1745 [54]
	0 0 0 1 0	CCITT Recommendation Q.921/I.441 (LAP.D) [20]
	0 0 1 1 0	CCITT Recommendation X.25; link layer (LAP.B) [52]
	0 0 1 1 1	CCITT Recommendation X.25 [52] multilink
	0 1 0 0 0	Extended LAP.BNCCITT [21]
	0 1 1 0 0	ISO Publication 8802/2 (LAN LLC)[22]
	1 0 0 0 1	ISO Publication 8802/2 [22] (note 7)
	1 0 0 1 0	GSM Recommendation 04.06) [51]
	1 0 1 1 0	CCITT Recommendation V.42 [27] (LAP.M)

All other values reserved.

NOTE 4: ISO Publication 8802/x refers to LAN operation with a null Layer 2 protocol (LLC not implemented).



IWU-ATTRIBUTES information element for Profile defined coding standard

Profile (octet 3):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	A/B data profile
	0 0 0 0 1	C data profile
	0 0 0 1 0	D data profile
	0 0 0 1 1	E data profile
	0 0 1 0 0	F data profile
	0 1 0 0 0	GSM circuit mode NT
	0 1 0 0 1	GSM circuit mode T
	0 1 0 1 0	GSM packet mode
	0 1 0 1 1	GSM messaging
	0 1 1 0 0	GSM Facsimile service group 3

All other values reserved.

Negotiation indicator (octet 4):

Bits	7 6 5	Meaning
	0 0 0	Negotiation not possible
	1 0 0	Exchanged parameter negotiation
	0 1 0	Peer attribute negotiation
	1 1 0	Exchanged attribute negotiation and Peer attribute negotiation

All other values reserved.

Profile subtype (octet 4):

Bits 4 3 2 1	Meaning

The coding of the profile subtype is given in the interworking annexes for the services where they are used as indicated in the profile type identifier (octet 3) above.

IWU attribute(s) information (octets 4 to L+2):

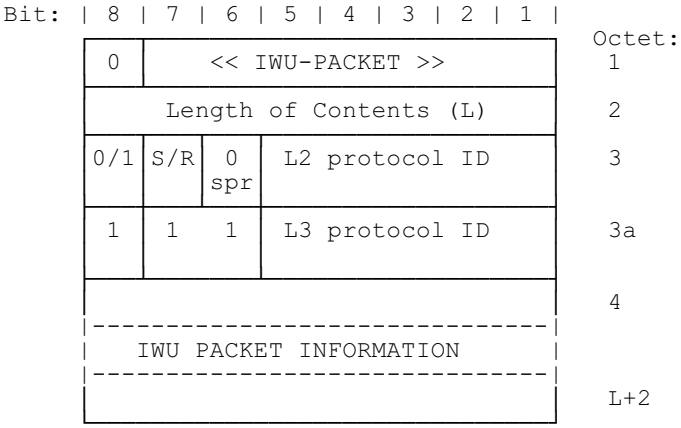
The coding of the IWU attributes is given in the interworking annexes for the services where they are used as indicated in the IWU type identifier (octet 3) above.

7.7.22 IWU packet

The purpose of the <<IWU-PACKET>> information element is to encapsulate any external frame or unstructured data such that it can be transported inside one or more CC, COMS or CLMS messages.

This element may be used to encapsulate octet structured frames (e.g. frames that have an original octet structure or have had all zero insertions and flag octets removed). If the frame (or data) is too large to fit into a single <<IWU-PACKET>> element, it shall be segmented into a series of <<IWU-PACKET>> elements that are associated using the <<SEGMENTED-INFO>> element.

Refer to annex G for more details on the use of this element.



IWU-PACKET information element

Send/Reject (S/R) bit (octet 3):

Bit 7	Meaning
0	Rejection of message
1	Transmission of message

NOTE 1: This send/reject bit is used to distinguish between the sending of a new messages (e.g. sent in the direction A=>B) and the rejection of a received message (e.g. message received by B can be rejected by sending "reject" code in direction B=>A).

L2 protocol ID coding (octet 3):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	User Specific (note 4)
0 0 0 0 1	Basic mode ISO Publication 1745 [54]
0 0 0 1 0	CCITT Recommendation Q.921/I.441 (LAP.D) [20]
0 0 1 1 0	CCITT Recommendation X.25 [52] link layer (LAP.B) [67]
0 0 1 1 1	CCITT Recommendation X.25 [52] multilink
0 1 0 0 0	Extended LAP.B [32]
0 1 1 0 0	ISO Publication 8802-22 (LAN LLC) [33]
1 0 0 0 1	ISO Publication 8802-2 [33] (note 3)
1 0 0 1 0	GSM Recommendation 04.06 [51]
1 0 1 1 0	CCITT Recommendation V.42 (LAP.M) [27]

All other values reserved.

L3 protocol ID coding (octet 3a):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	User specific (note 4)
0 0 0 1 0	ETS 300 102-1 [10]
0 0 1 1 0	CCITT Recommendation X.25, packet layer [52]
0 0 1 1 1	ISO Publication 8208 [23] (X.25 packet level for DTE [52])
0 1 0 0 0	ISO Publication 8348 [24] (OSI C/O protocol)
0 1 0 0 1	ISO Publication 8473 [25] (OSI C/L service)
0 1 0 1 0	CCITT Recommendation T.70 [53] (minimum NWK layer)
1 0 0 1 0	GSM Recommendation 04.08 [11]

All other values reserved.

NOTE 2: All the L2 protocol ID and L3 protocol ID codings are the same as the codings used for "DECT Standard coding" in the <<IWU-ATTRIBUTES>> element. See subclause 7.7.21.

NOTE 3: ISO Publication 8802-2 [22] refers to LAN operation with a null Layer 2 protocol (LLC not implemented).

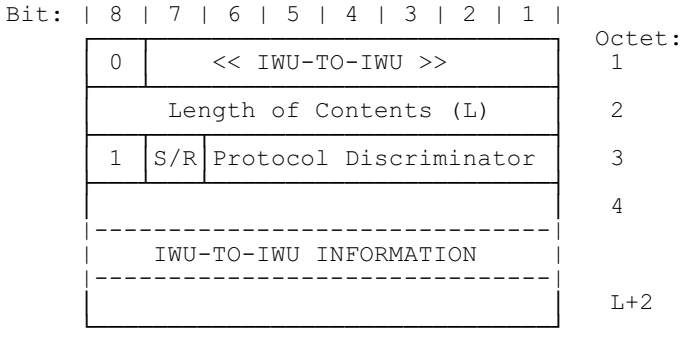
NOTE 4: The <<IWU-PACKET>> is structured according to the user needs.

7.7.23 IWU to IWU

The purpose of the <<IWU-TO-IWU>> element is to encapsulate any message or information element that cannot be interworked into one or more other DECT information element(s).

If the message or element is too large to fit into a single <<IWU-TO-IWU>> element, it shall be segmented into a series of <<IWU-TO-IWU>> elements that are associated using the <<SEGMENTED-INFO>> element.

Refer to annex G for more details on the use of this element.



IWU-TO-IWU information element

Send/Reject (S/R) bit:

Bits	7	Meaning
	0	Rejection of message
	1	Transmission of message

NOTE 1: This Send/Reject (S/R) bit is used to distinguish between the sending of a new message (e.g. sent in the direction A=>B) and the rejection of a received message (e.g. message received by B can be rejected by sending "reject" code in direction B=>A).

Protocol Discriminator (PD):

Bits	6 5 4 3 2 1	Meaning
	0 0 0 0 0 0	User Specific (note 2)
	0 0 0 0 0 1	OSI high layer protocols
	0 0 0 0 1 0	CCITT Recommendation X.244 [26] (note 3)
	0 0 0 1 0 0	IA5 characters
	0 0 0 1 1 1	CCITT Recommendation V.120 Rate adaption
	0 0 1 0 0 0	CCITT Recommendation Q.931 (I.451), message [19]
	0 0 1 0 0 1	CCITT Recommendation Q.931 (I.451), element(s) [19] (note 4)
	0 0 1 0 1 0	CCITT Recommendation Q.931 (I.451), partial message [19]. (note 5)
	0 1 0 0 0 0	GSM Recommendation 04.08, message [11]
	0 1 0 0 0 1	GSM Recommendation 04.08, element(s) [11] (note 4)
	0 1 0 1 0 0	MMS User Data element (E data profile [57])
	1 1 1 1 1 1	Unknown

All other values reserved.

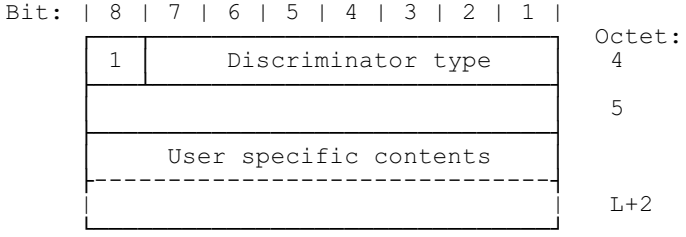
NOTE 2: The IWU information is structured as shown below.

NOTE 3: The IWU information is structured according to CCITT Recommendation X.244 [26] (CCITT Recommendation X.25 [52] call user data).

NOTE 4: If more than one element is included, they are interpreted in the order of appearance.

NOTE 5: The Q.931 (I.451) [19] partial message excludes the protocol discriminator and the call reference.

IWU-to-IWU information field (octets 4 to L+2) for Protocol Discriminator value "user specific".

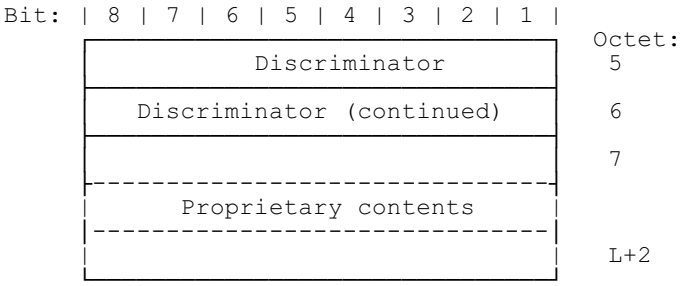


Discriminator type (octet 4):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	Unspecified
	0 0 0 0 0 0 1	EMC

All other values reserved

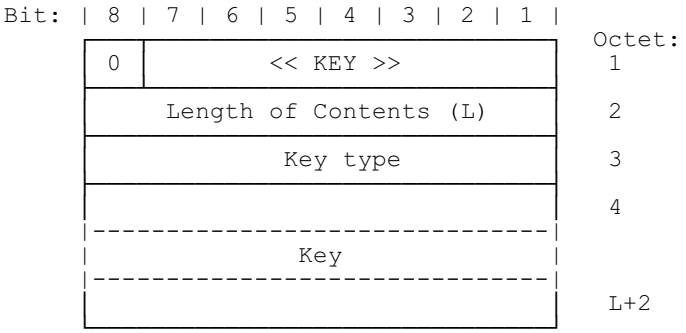
User specific contents field (octets 5 to L+2) for Discriminator type "EMC"



The discriminator consists of 2 octets (octets 5 and 6) and contains the EMC.

7.7.24 Key

The purpose of the <<KEY>> information element is to transfer a key. When sending the <<KEY>> information element a ciphered connection shall be used.



KEY information element

Key type coding (octet 3):

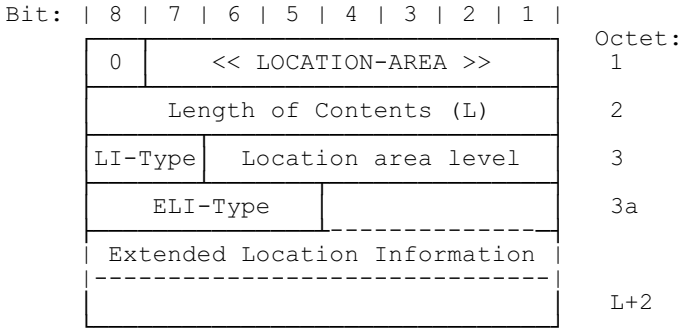
Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 1 0 0 0 0	Derived Cipher Key (DCK)
	All other values reserved.	

Key data field: the key data field contains the numeric value of the key. The length of the key data field is (L-1) octets as defined by the length indicator (octet 2). For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

NOTE: A key K1 with L1 > N bits can be mapped into a key K with N bits by taking the lower N bits of K1. A key K2 with L2 < N bits can be mapped into a key K with N bits by using: $K(i) = K2 (i \text{ modulo } L2)$, $0 \leq i \leq N-1$.

7.7.25 Location area

The purpose of the <<LOCATION-AREA>> information element is to provide an identification of the location area.



LOCATION-AREA information element

Location Information (LI) type coding (octet 3):

Bits 8 7	Meaning
0 0	Reserved
0 1	Location area level is included (octet 3) but no extended location information is included
1 0	Only extended location information (octet 3a to octet L+2) is included the value of the location area level (octet 3) is not a valid one
1 1	Location area level (octet 3) as well as extended location information (octet 3a to octet L+2) are included

Location area level for LA type 01 and 11 (octet 3):

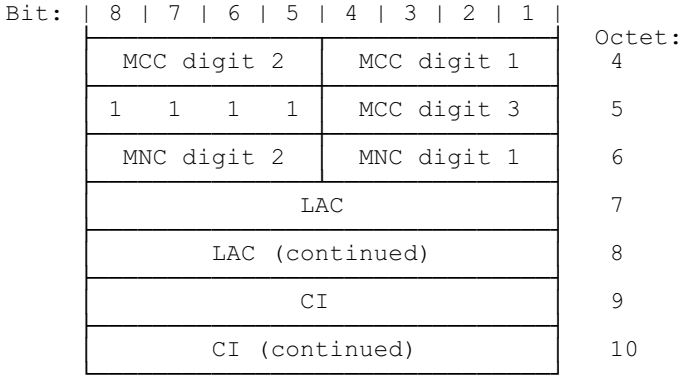
Contains a number which identifies how many bits of the RFPI are relevant for this location area. The bit count starts with the MSB of the RFPI.

Extended Location Information (ELI) type coding (octet 3a):

Bits 8 7 6 5	Meaning
0 1 1 1	GSM location information is requested and not included; bits 1 to 4 of octet 3a should be set to 1
1 1 1 1	GSM location information

All other values reserved.

GSM location information coding:

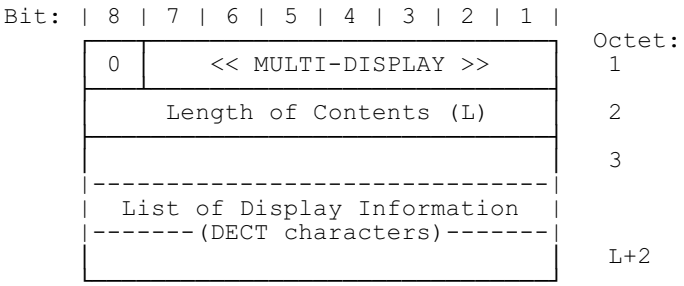


MCC: is the Mobile Country Code;
MNC: is the GSM Mobile Network Code;
LAC: is the GSM Location Area Code;
CI: is the GSM Cell Identity.

NOTE: The Cell Identity (CI) is needed for external handover.

7.7.26 Multi-display

The purpose of the <<MULTI-DISPLAY>> element is to supply a list of display information that may be displayed by the PT. Multi-display elements shall only contain DECT standard characters. Multiple characters shall be interpreted in the order of ascending octet numbers.

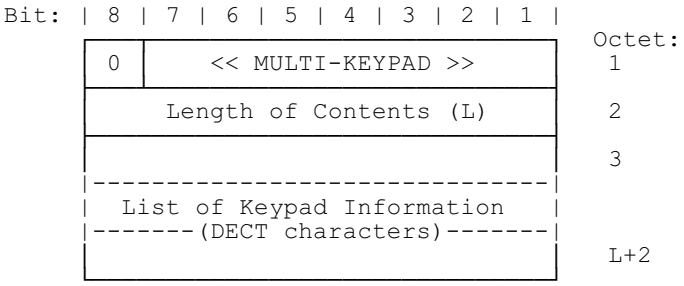


MULTI-DISPLAY information element

NOTE: DECT characters are specified in annex D. These are closely based on IA5 characters.

7.7.27 Multi-keypad

The purpose of the <<MULTI-KEYPAD>> element is to transport a list of keypad information e.g. entered by a PT keypad. Multi-keypad elements shall only contain DECT standard characters. Multiple characters shall be interpreted in the order of ascending octet numbers.

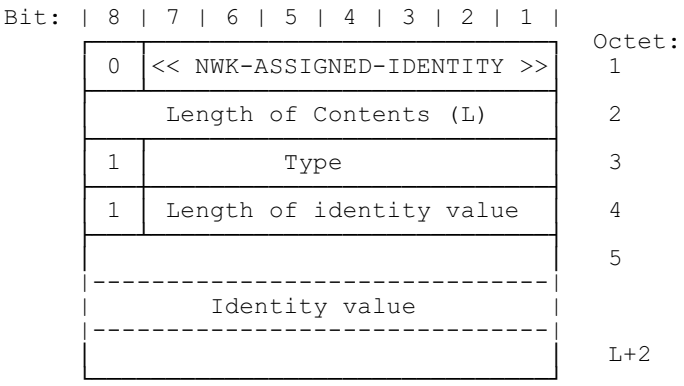


MULTI-KEYPAD information element

NOTE: DECT characters are specified in annex D. These are closely based on IA5 characters.

7.7.28 NetWorK (NWK) assigned identity

The purpose of the <<NWK-ASSIGNED-IDENTITY>> information element is to transport a network assigned identity.



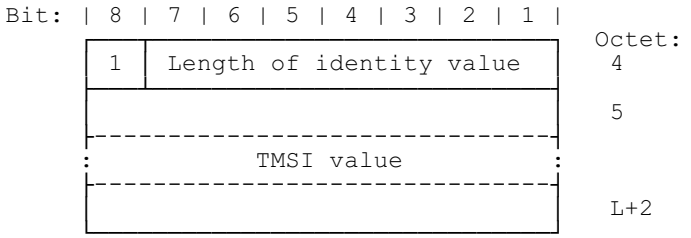
NWK-ASSIGNED-IDENTITY information element

Type coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	1 1 1 0 1 0 0	GSM Temporary Mobile Subscriber Identity (TMSI)
	1 1 1 1 1 1 1	Proprietary (application specific)
	All other values reserved.	

Length of identity value coding (octet 4): the length is defined in bits, and this is coded with the natural binary value. The least significant bit of the coding appears in bit position 1. Allowable values: 0 to 127.

Identity value coding for GSM-TMSI:

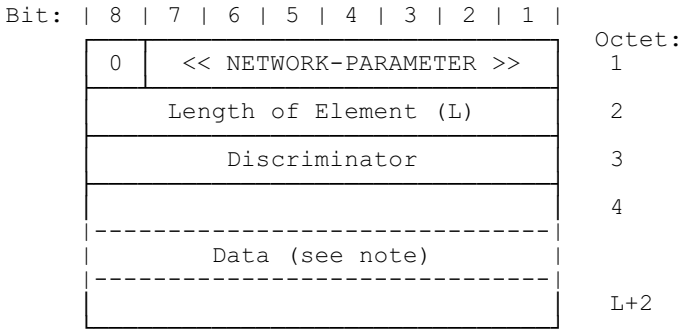


Length of identity value coding (octet 4): the length is defined in bits, and this is coded with the natural binary value. The least significant bit of the coding appears in bit position 1. Allowable values: 0 to 32.

TMSI value coding (octet 5 to L+2): the TMSI value shall not have more than 4 octets.

7.7.29 Network parameter

The purpose of the <<NETWORK-PARAMETER>> element is to carry network parameters.



NETWORK PARAMETER information element

Discriminator coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 1 1 0 1 0 0 0	Handover reference not required
	0 1 1 0 1 0 0 1	Handover reference, private network
	0 1 1 0 1 0 1 0	Handover reference, GSM network
	0 1 1 0 1 0 1 1	Handover reference, public network
	0 1 1 1 1 1 1 1	Proprietary
	1 1 1 0 1 0 1 0	Handover reference request, GSM network
	All other values reserved	

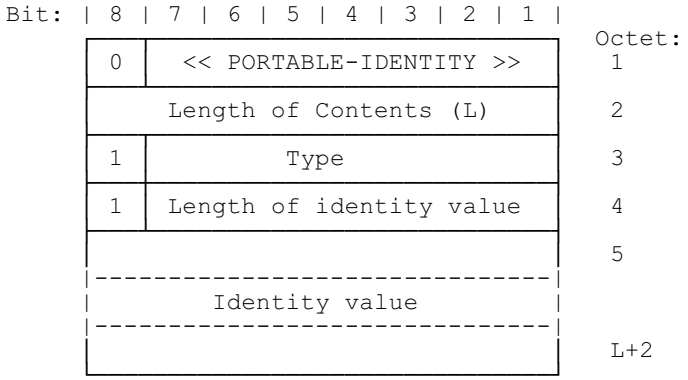
NOTE: The <data> field is not structured because information is passed transparently.

Data field coding for handover reference (octet 4):

The handover reference is coded using binary representation.

7.7.30 Portable identity

The purpose of the <<PORTABLE-IDENTITY>> information element is to transport a DECT portable identity. Refer to ETS 300 175-6 [5], describing identities and addressing.



PORTABLE-IDENTITY information element

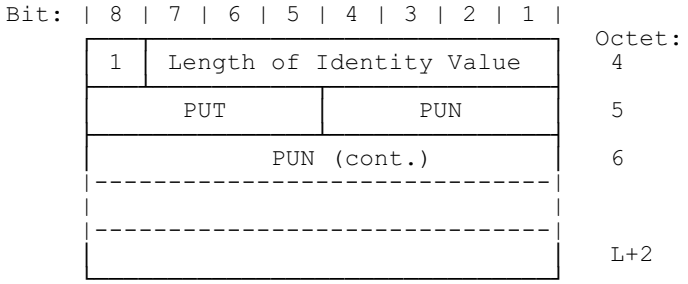
Identity type coding for portable identities (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	International Portable User Identity (IPUI)
	0 0 1 0 0 0 0	International Portable Equipment Identity (IPEI)
	0 1 0 0 0 0 0	Temporary Portable User Identity (TPUI)
	All other values reserved.	

Length of identity value coding (octet 4): the length is defined in bits, and this is coded with the natural binary value. The least significant bit of the coding appears in bit position 1.

Allowable values: 0 to 127.

Identity value coding for IPUIs:

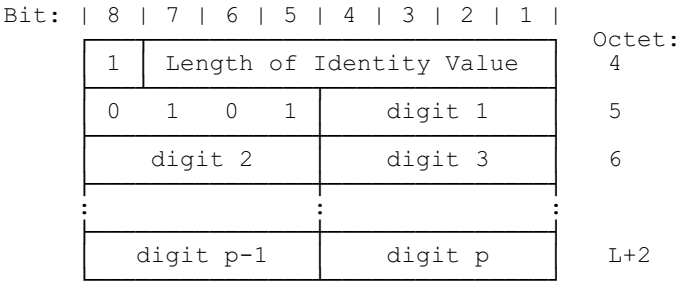


Length of identity value coding (octet 4): defines the number of valid IPUI bits.

Portable User Type (PUT) coding (octet 5): refer to ETS 300 175-6 [5]. The most significant bit is in bit position 8 in octet 5.

Portable User Number (PUN) coding (octet 5 to L+2): refer to ETS 300 175-6 [5]. The Most Significant Bit (MSB) is in bit position 4 in octet 5. For binary codings: the order of bit values progressively decreases as the octet number increases, and unused bits in the last octet shall be set to 0.

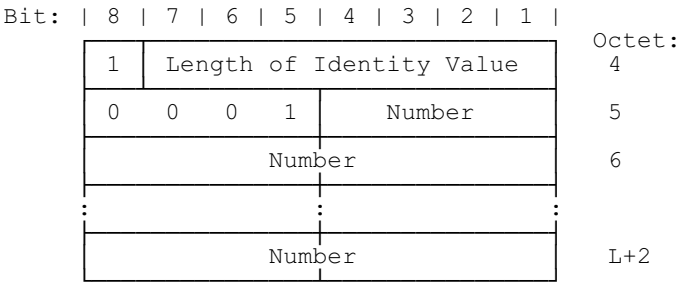
Identity value coding for IPUI S containing the PSTN or ISDN number:



Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 4 + 4 x p.

PSTN or ISDN number coding (octet 5 to L+2): the number is BCD coded and shall not exceed 15 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

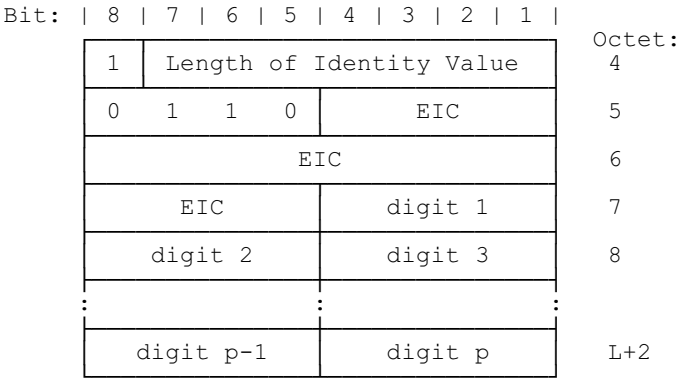
Identity value coding for IPUI O containing the private number:



Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals 4 + (0 to 60).

Private number coding number (octet 5 to L+2): the number is binary coded and shall not exceed 60 bits.

Identity value coding for IPUI T containing the equipment installer's code and private extended number:

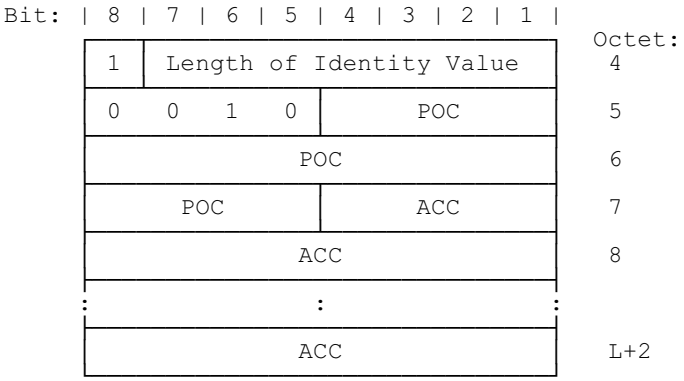


Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 20 + 4 x p.

Equipment Installer's Code (EIC) (octet 5 to 7): the EIC is binary coded and is 16 bits.

Private extended number coding (octet 7 to L+2): the number is BCD coded and shall not exceed 11 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

Identity value coding for IPUI P containing the public operator code and the account number:

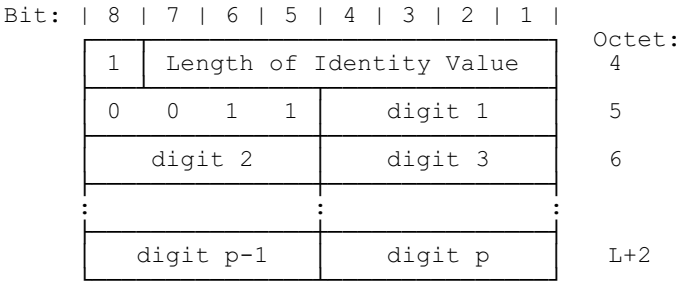


Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 20 + (0 to 80).

Public Operator Code (POC) (octet 5 to 7): the code is binary coded and is 16 bits.

ACCount number (ACC) coding (octet 7 to L+2): the number is binary coded and shall not exceed 80 bits.

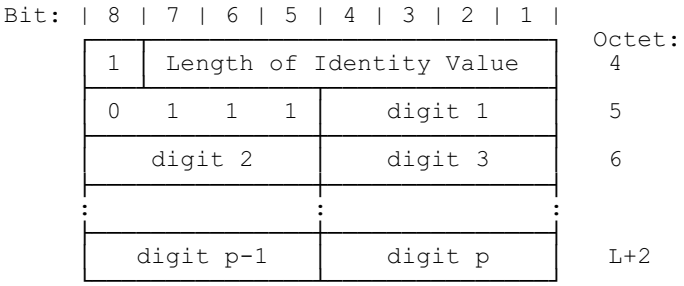
Identity value coding for IPUI Q containing the bank account number:



Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 4 + 4 x p.

Bank ACcount Number (BACN) coding (octet 5 to L+2): the number is BCD coded and shall not exceed 20 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

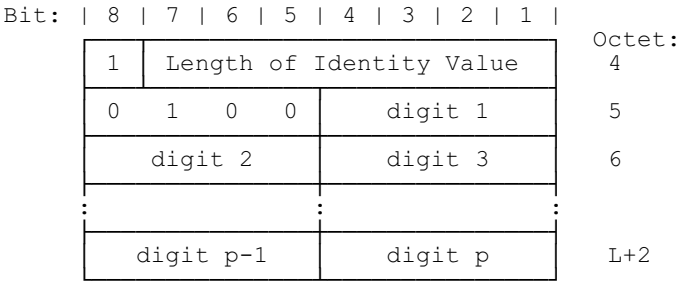
Identity value coding for IPUI U containing the credit card account number:



Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 4 + 4 x p.

Credit Card ACcount Number (CACN) coding (octet 5 to L+2): the number is BCD coded and shall not exceed 20 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

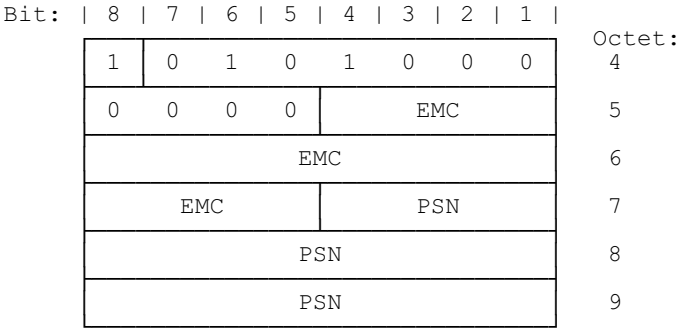
Identity value coding for IPUI R containing the GSM-IMSI:



Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 4 + 4 x p.

International Mobile Subscriber Identity (IMSI) coding (octet 5 to L+2): the number is BCD coded and shall not exceed 15 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

Identity value coding for the IPEI (same as for IPUI N):

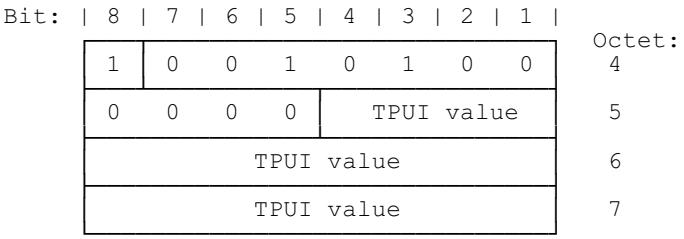


Length of identity value coding (octet 4): the number of valid bits for IPUI N containing the IPEI is 40.

Equipment Manufacturer Code (EMC) coding (octets 5 to 7): refer to ETS 300 175-6 [5]. The Most Significant Bit (MSB) is in bit position 4 in octet 5. The order of bit values progressively decreases as the octet number increases.

Portable Equipment Serial Number (PSN) coding (octets 7 to 9): refer to ETS 300 175-6 [5]. The most significant bit is in bit position 4 in octet 7. The order of bit values progressively decreases as the octet number increases.

Identity value coding for TPUI:

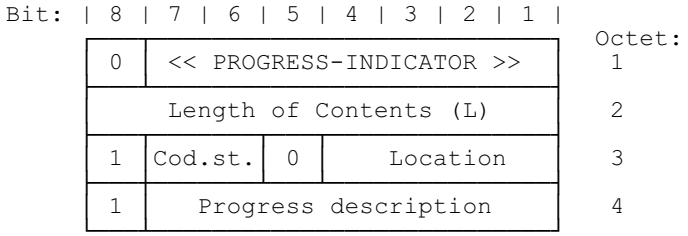


Length of identity value coding (octet 4): the number of valid bits for a TPUI is 20.

Temporary Portable User Identity (TPUI) coding (octet 5 to 7): Refer to ETS 300 175-6 [5]. The most significant bit is in bit position 4 in octet 5. The order of bit values progressively decreases as the octet number increases.

7.7.31 Progress indicator

The purpose of the <<PROGRESS-INDICATOR>> element is to describe an event which has occurred during the life of a call.



PROGRESS-INDICATOR information element

Coding standard coding (octet 3):

Bits	7 6	Meaning
	0 0	CCITT standardised coding, as described below
	0 1	reserved for other international standards
	1 0	national standard
	1 1	standard specific to identified location

Location coding (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	user
	0 0 0 1	private network serving the local user
	0 0 1 0	public network serving the local user
	0 1 0 0	public network serving the remote user
	0 1 0 1	private network serving the remote user
	0 1 1 1	international network
	1 0 1 0	network beyond interworking point
	1 1 1 1	not applicable

All other values are reserved.

Progress description coding (octet 4):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 1	Call is not end-to-end ISDN, further call progress info may be available in-band
	0 0 0 0 0 1 0	Destination address is non-ISDN
	0 0 0 0 0 1 1	Origination address is non-ISDN
	0 0 0 0 1 0 0	Call has returned to the ISDN
	0 0 0 0 1 0 1	Service change has occurred
	0 0 0 1 0 0 0	In-band information or appropriate pattern now available
	0 0 0 1 0 0 1	In-band information not available
	0 1 0 0 0 0 0	Call is end-to-end PLMN/ISDN

All other values reserved.

7.7.32 Rand

The purpose of the authentication parameter <<RAND>> information element is to provide a non predictable number to be used to calculate the authentication response signature.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< RAND >>							1
	Length of Contents (L)								2
	RAND Field								3
									L+2

RAND information element

NOTE: This information element is used for either the RAND-P or the RAND-F information. The actual contents are determined by the direction of transmission.

RAND field coding (octet 3 to L+2)
RAND shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

7.7.33 Rate parameters

The purpose of the <<RATE-PARAMETERS>> element is to indicate the requested attributes for the Basic Rate Adaption Service (BRAT).

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< RATE-PARAMETERS >>							1
	Length of Content (L)								2
	1	Symm		I	Class of service				3
	0/1	Ch 1 user rate P=>F			Ch 1. arrang. P=>F				4
	1	Ch 1 user rate F=>P			Ch 1. arrang. F=>P				4a
	0/1	Ch 2 user rate P=>F			Ch 2. arrang. P=>F				5
	1	Ch 2 user rate F=>P			Ch 2. arrang. F=>P				5a
	0/1	Ch 3 user rate P=>F			Ch 3. arrang. P=>F				6
	1	Ch 3 user rate F=>P			Ch 3. arrang. F=>P				6a

RATE-PARAMETERS information element

Symmetry (octet 3):

Bits	7 6	Meaning
	0 0	Symmetric
	1 0	Asymmetric

All other values reserved.

If symmetric, only octets 4, 5 and 6 shall appear and the rates shall apply to both directions. If asymmetric octets 4, 5 and 6 shall refer to the direction P=>F; and octets 4a, 5a and 6a shall refer to the direction F=>P.

If octets 5 or 6 is omitted the channel 2 rate and/or channel 3 rate shall be understood to be 0 kbit/s.

Interleaving (I) (octet 3):

Bits	5	Meaning
	0	Non-interleaved
	1	Interleaved

Class of service (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	I_N service
	0 0 1 0	I_P; Class 0 service
	0 1 0 0	I_P; Class 3 service; 0 % excess capacity
	0 1 0 1	I_P; Class 3 service; 25 % excess capacity
	0 1 1 0	I_P; Class 3 service; 50 % excess capacity
	0 1 1 1	I_P; Class 3 service; 100 % excess capacity

NOTE: The excess capacity indicated for the Class 3 services are target figures only. The actual excess capacity is defined by the connection used.

Channel arrangement (octets 4, 4a, 5, 5a, 6, 6a):

Bits	4 3 2 1	Meaning
	0 0 0 0	User defined
	0 0 0 1	B1
	0 0 1 0	B2
	1 0 0 0	D1

All other values reserved.

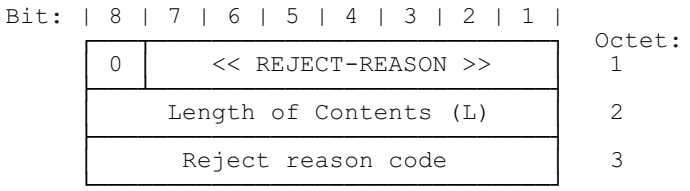
Channel rate coding (octets 4, 4a, 5, 5a, 6, 6a):

Bits	7 6 5	Meaning
	0 0 0	00 kbit/s (channel off)
	0 0 1	08 kbit/s
	0 1 0	16 kbit/s
	0 1 1	32 kbit/s
	1 0 0	64 kbit/s

All other values reserved.

7.7.34 Reject reason

The purpose of the <<REJECT-REASON>> information element is to indicate the reason why a request is rejected by the FT or PT.



REJECT-REASON information element

Reject reason coding (octet 3):

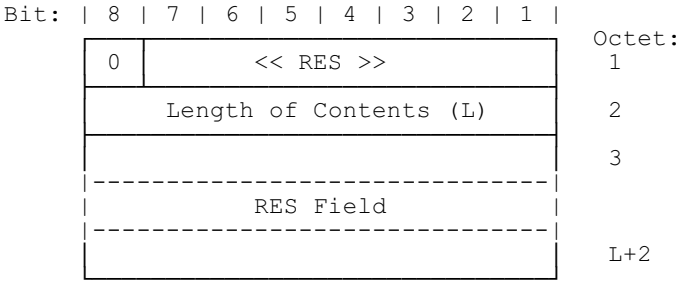
Value(hex)	Meaning(Reject reason)
01	TPUI unknown
02	IPUI unknown
03	network assigned identity unknown
05	IPEI not accepted
06	IPUI not accepted
10	authentication failed
11	no authentication algorithm
12	authentication algorithm not supported
13	authentication key not supported
14	UPI not entered
17	no cipher algorithm
18	cipher algorithm not supported
19	cipher key not supported
20	incompatible service
21	false LCE reply (no corresponding service)
22	late LCE reply (service already taken)
23	invalid TPUI
24	TPUI assignment limits unacceptable
2F	insufficient memory
30	overload (note)
40	test call back: normal, en-bloc
41	test call back: normal, piecewise
42	test call back: emergency, en-bloc
43	test call back: emergency, piecewise
5F	invalid message
60	information element error
64	invalid information element contents
70	timer expiry
76	PLMN not allowed
80	Location area not allowed
81	National roaming not allowed in this location area

All other values are reserved.

NOTE: If a {LCE-PAGE-REJECT} message with the <<REJECT-REASON>> "overload" is received, the portable part should try to access an other radio fixed part belonging to the same paging area.

7.7.35 RES

The purpose of the authentication parameter <<RES>> information element is to provide the calculated authentication response signature.



RES information element

NOTE: This information element is used for either the RES1 or the RES2 information. The actual contents are determined by the direction of transmission.

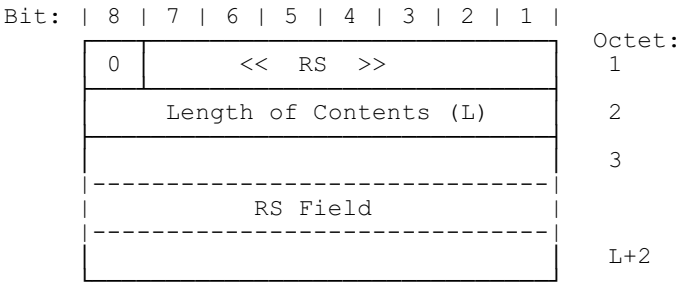
- RES field coding (octet 3 to 6);

- RES shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

7.7.36 RS

The purpose of the authentication parameter <<RS>> information element is to provide a number to be used together with <<RAND>> and the authentication key to calculate the authentication response signature.



RS information element

- RS field coding (octet 3 to L+2);

- RS shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

7.7.37 Segmented info

The purpose of the <<SEGMENTED-INFO>> element is to indicate that the message in which is occurs contains only part of a segmented information element. When used, this element shall always appear immediately before the segmented element to which it refers.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< SEGMENTED-INFO >>							1
	Length of Contents (L)								2
	F	No. of segments remaining							3
	0	Segmented element type							4

SEGMENTED-INFO information element

F bit coding:

Bit 8	Meaning
1	First segment follows
0	Subsequent segment follows

No of segments remaining: the number of remaining segments (including the following segment) that are still to be sent. This is coded with the natural binary value, with the least significant bit in position 1.

Segmented element type: the normal coding of the segmented information element (shall only refer to a variable length information element).

If the <<segmented-info>> information element is used, then it shall only permit message segmentation with respect to a single information element only.

7.7.38 Service change info

The purpose of the <<SERVICE-CHANGE-INFO>> element is to indicate the attributes of the proposed service change.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< SERVICE-CHANGE-INFO >>							1
	Length of Contents (L)								2
	0/1	Coding std.		M	Change Mode				3
	1	Extended change mode							3a
	1	A attributes			R	B attributes			4

SERVICE-CHANGE-INFO information element

Coding standard:

Bits 7 6	Meaning
0 0	DECT standard coding
All other values reserved.	

M (Master) coding:

Bits 5	Meaning
0	Initiating side is master
1	Receiving side is master

Change mode coding:

Bits 4 3 2 1	Meaning
0 0 0 0	None
0 0 0 1	Connection Reversal
0 0 1 0	Bandwidth change (see subclause 9.6)
0 1 0 0	Rerouting (of U-plane links) (see subclause 9.6)
0 1 1 0	Rerouting plus bandwidth change (see subclause 9.6)
1 0 0 0	Suspend
1 0 0 1	Resume
1 0 1 0	Voice/data change to data (note 1)
1 0 1 1	Voice/data change to voice (note 1)
1 1 0 0	IWU attribute change
1 1 1 0	Profile/ Basic service and IWU attributes change (note 1,2)
1 1 1 1	Reserved for extension (note 2)

All other values reserved.

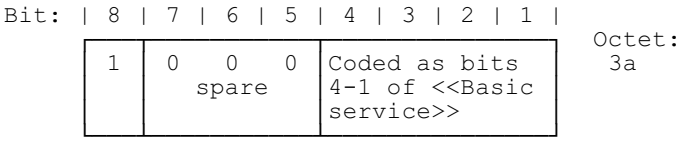
When using the reserved value, octet 3a shall follow containing extended coding of the service change.

Octet 4 shall only appear for "suspend" and "resume" codings.

NOTE 1: The procedures for the use of these codings are specified in the profiles for which such service changes can be supported, such as in the Mobility Class 2 Data Services Profiles.

NOTE 2: When using the “Profile/ Basic service and IWU attributes change” or “reserved” value, octet 3a follows. The coding of octet 3a is dependent on the change mode codings (octet 3).

Extended change mode for “Profile/ Basic service and IWU attributes change”:



Extended change mode for “reserved” is reserved for further standardisation.

A attributes coding:

Bits 7 6 5	Meaning
0 0 0	Not applicable
0 1 0	Maintain old connection(s)
0 1 1	Release old connection(s)

Reset (R) coding:

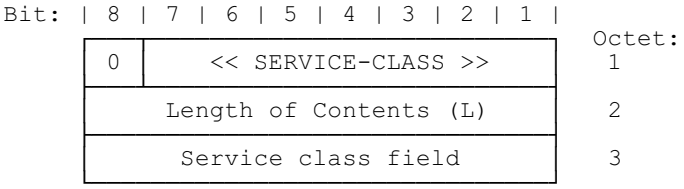
Bits 4	Meaning
0	Do not reset state variables
1	Reset state variables

B attributes coding:

Bits	3 2 1	Meaning
	0 0 0	Not applicable
	0 1 0	Interrupt data transfer
	0 1 1	Maintain data transfer

7.7.39 Service class

The purpose of the <<SERVICE-CLASS>> information element is to identify services which a PT is allowed to use.



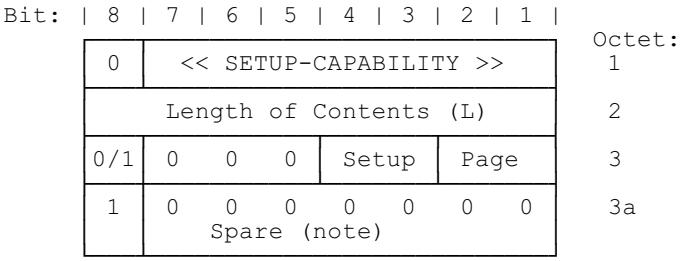
SERVICE-CLASS information element

Service class field coding (octet 3a):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 1	One nominated number only may be called
	0 0 0 0 0 0 1 0	As above and local calls are allowed
	0 0 0 0 0 0 1 1	As above and national calls are allowed
	0 0 0 0 0 1 0 0	As above and mobile and premium service calls are allowed
	0 0 0 0 0 1 0 1	As above and international calls are allowed
	0 0 0 0 0 1 1 0	As above and satellite services are allowed

7.7.40 Set-up capability

The purpose of the <<SETUP-CAPABILITY>> element is to convey some aspects of the PP call set-up capabilities to the FP during location registration.



SETUP-CAPABILITY information element

Page capability coding (octet 3):

Bits	2 1	Meaning
	0 1	Normal paging
	1 0	Fast paging

All other values reserved.

Set-up capability coding (octet 3):

Bits	4 3	Meaning
	0 1	Normal set-up
	1 0	Fast set-up

All other values reserved.

NOTE: Explicit provision for extension of this element is provided. Implementors should use the 0/1 ext flag (bit 8) to detect the use of additional octets in future versions.

7.7.41 Terminal capability

The purpose of the <<TERMINAL-CAPABILITY>> element is to convey some aspects of the PP capabilities to the FP during call establishment.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< TERMINAL-CAPABILITY >>							1
Length of Contents (L)								2
0/1	tone capab.			display capab.				3
0/1	echo param			N-REJ		A-VOL		3b
0/1	slot type capability							3c
0/1	Number of stored display characters (MS)							3d
0/1	Number of stored display characters (LS)							3e
0/1	Number of lines in (physical) display							3f
0/1	Number of characters / line							3g
0/1 ext	Scrolling behaviour field							3h
0/1	Profile indicator_1 note 9							4
0/1	Profile indicator_2 note 9							4a
0/1 ext	Profile indicator_3 note 9							4b
0/1	0 0 0 0 spare			control codes				5
0/1 ext	escape to 8 bit character sets_1 (note 9)							5a

TERMINAL-CAPABILITY information element

NOTE 1: Octet 3a is intentionally absent.

Display capability coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Not applicable
0 0 0 1	No display; (note 3)
0 0 1 0	Numeric (note 5)
0 0 1 1	Numeric-plus (note 5)
0 1 0 0	Alphanumeric (note 6)
0 1 0 1	Full display (note 7)

All other values reserved.

Tone capability coding (octet 3):

Bits	7 6 5	Meaning
	0 0 0	Not applicable
	0 0 1	No tone capability (note 3)
	0 1 0	dial tone only
	0 1 1	E.182 [50] tones supported (note 8)
	1 0 0	Complete DECT tones supported
	All other values reserved.	

Echo parameters (octet 3b):

Bits	7 6 5	Meaning
	0 0 0	Not applicable
	0 0 1	Minimum TCL (>34 dB); (note 3, note 4)
	0 1 0	Full TCL (>46 dB); (note 4)
	All other values reserved.	

Portable part ambient Noise REJection capability (N-REJ) (octet 3b):

Bits	4 3	Meaning
	0 0	Not applicable
	0 1	No noise rejection; (note 3, note 4)
	1 0	Noise rejection provided (note 4)
	1 1	Reserved

Adaptive VOLume control provision (A-VOL) (octet 3b):

Bits	2 1	Meaning
	0 0	Not applicable
	0 1	No PP adaptive volume control; (note 3)(note 4)
	1 0	PP adaptive volume control used (note 4)
	1 1	Disable FP adaptive volume control (note 4)

Slot type capability (octet 3c):

This is a bit pattern indicating the slot type capabilities. A "1" in a bit position indicates capability of the indicated slot type; a "0" indicates no capability.

Bit 1: Half slot; j = 0
Bit 4: Full slot; (note 3)
Bit 5: Double slot

All other bits are reserved, and should be set to "0".

Number of stored display characters (octets 3d, 3e):

Valid values for the number of stored display characters shall be in the range 0 to 16383.

Number of lines in (physical) display (octet 3f):

Valid values for the number of lines in the physical display shall be in the range 0 to 127.

Number of Characters per line (octet 3g):

Valid values of the number of characters per line in the physical display shall be in the range 0 to 127.

Scrolling Behaviour field (octet 3h):

The value in this field indicates a specific scrolling behaviour of the display.

Scrolling Behaviour coding (octet 3h):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Not specified
0 0 0 0 0 0 1	Scrolling behaviour type 1
0 0 0 0 0 1 0	Scrolling behaviour type 2

All other values reserved.

Scrolling Behaviour types 1 ,2

Details of scrolling behaviour are included in normative annex J.

Profile indicator (octet group 4):

This is a bit mapped octet group. A "1" indicates support for the specified profile. Reserved bits shall be set to zero and shall not be checked in the receiver.

Profile Indicator_1 Coding (Octet 4):

Bits 7 6 5 4 3 2 1	Meaning
x x x x x x 1	reserved
x x x x x 1 x	GAP/PAP supported
x x x x 1 x x	DECT/GSM interworking profile supported
x x x 1 x x x	ISDN supported
x x 1 x x x x	Data Services Profile E, Class 2
x 1 x x x x x	Data Services Profile A/B, Class 2
1 x x x x x x	Multi-bearers supported for the Data Services Profiles

Profile Indicator_2 Coding (Octet 4a):

Bits 7 6 5 4 3 2 1	Meaning
x x x x x x 1	Data Services Profile C, Class 2
x x x x x 1 x	Data Services Profile D, Class 2
x x x x 1 x x	Data Services Profile F, Class 2
x x x 1 x x x	DECT/GSM interworking - GSM Bearer service
x x 1 x x x x	DECT/GSM interworking - GSM SMS service
x 1 x x x x x	DECT/GSM interworking - GSM Facsimile service
1 x x x x x x	reserved

Profile Indicator_3 Coding (Octet 4b):

Bits 7 6 5 4 3 2 1	Meaning
x x x x x x 1	reserved
x x x x x 1 x	reserved
x x x x 1 x x	reserved
x x x 1 x x x	reserved
x x 1 x x x x	reserved
x 1 x x x x x	reserved
1 x x x x x x	reserved

Control Codes (octet 5):

This field indicates a set of DECT display control characters which the PT supports. Support for "clear display" control code is mandatory for all displays.

Control Codes coding(octet 5):

Bits 3 2 1	Meaning
0 0 0	Not specified
0 0 1	0CH (clear display)
0 1 0	Coding 001 plus 08H to 0BH and 0DH.
0 1 1	Coding 010 plus 02H, 03H, 06H, 07H, 19H, 1AH
1 0 0	Coding 011 plus 0EH, 0FH

All other values reserved.

NOTE 2: The display behaviour in response to some control codes may be dependent on the scrolling behaviour of the display.

Escape to 8 bit character sets_1 (octet 5a):

This bit mapped octet is used to indicate additional character sets which may be invoked by using escape sequences as defined in IS0 Publication 2022 [15]. A "1" indicates support for the specified character set and that the PT correctly interprets ISO Publication 2022 [15] escape sequences, see subclause D.2.4..

Escape to 8 bit character sets_1 coding(octet 5 a):

Bits 7 6 5 4 3 2 1	Meaning
x x x x x x 1	Latin alphabet no 1 supported ISO 8859-1 [55]
x x x x x 1 x	reserved
x x x x 1 x x	reserved
x x x 1 x x x	reserved
x x 1 x x x x	reserved
x 1 x x x x x	reserved
1 x x x x x x	reserved

NOTE 3: This capability is assumed as the default value unless otherwise specified by a service profile, if the <<TERMINAL-CAPABILITY>> information element is omitted.

NOTE 4: Refer to ETS 300 175-8 [7] for a definition of TCL, PP Adaptive VOLume (A-VOL) control, PP ambient Noise REJection (N-REJ) and the usage of these parameters.

NOTE 5: "Numeric" indicates support for at least the following characters: space, 0-9, *, #. "Numeric-plus" indicates support for at least the following characters: space, 0-9, *, #, a, b, c, d.

NOTE 6: "Alphanumeric" indicates support for at least the following characters: space, 0-9, *, #, a-z and A-Z.

NOTE 7: "Full display" indicates support for the full DECT character set. (i.e. displayable characters with character codes up to 7F).

NOTE 8: "E.182 [50] tones supported" indicates support of all of the E.182 [50] compatible tones identified in subclause 7.6.8.

NOTE 9: More octets may follow for the indication of further profiles or character sets.

7.7.42 Transit delay

The purpose of the <<TRANSIT-DELAY>> element is to indicate the allowable delay that shall be imposed for data transmitting the DECT subnetwork.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< TRANSIT-DELAY >>							1
Length of Content (L)								2
1	0	Forward Delay						3
1	0	Backward Delay						4

TRANSIT-DELAY information element

Forward delay (backward delay) octet 3 (and 4): the <<TRANSIT-DELAY>> shall be coded with the natural binary value, and the result placed in the octet with the least significant bit in position 1. Delay shall be calculated in steps of 1 TDMA frame (10 ms).

Allowable values are "1" to "63".

7.7.43 Window size

The purpose of the <<WINDOW-SIZE>> element is to indicate (and optionally to negotiate) the window size to be used for frame transmission.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< WINDOW-SIZE >>							1
Length of Content (L)								2
0/1 ext	Forward Value							3
0/1 ext	Maximum forward PDU length							3a
0/1 ext	Forward SDU length timer							3b
0/1 ext	Backward Value							4
0/1 ext	Maximum backward PDU length							4a
0/1 ext	Backward SDU LAPU timer							4b

WINDOW-SIZE information element

This information element may contain octet 3 and 4 only, only the FU window size is specified.

If octet group 4 is omitted, the backward values shall be understood to be equal to the forward values.

Forward value (backward value) octet 3 (and 4): the <<WINDOW-SIZE>> shall be coded with the natural binary value, and the result placed in the octet with the least significant bit in position 1. Allowable values are "1" to "127".

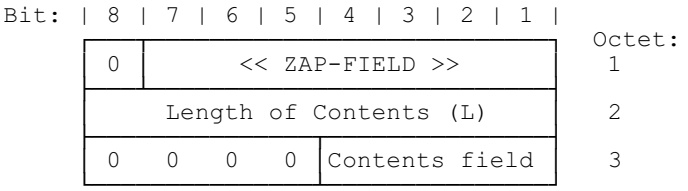
The value "0" shall be used to indicate "not applicable" in the event that no window size is defined for the forward direction.

Maximum forward (and backward) PDU length (octets 3a, 4a) is coded as natural binary value and the value of this field multiplied by 60 bytes shall give the maximum size of the PDU used by a profile.

Forward (and backward) SDU LAPU timer (octet 3b, 4b) value is coded as natural binary value and the value multiplied by the 10 TDMA frame time shall give the DLC layer <DLU.04> timer value This timer is defined in the C.2 data profile [58].

7.7.44 ZAP field

The purpose of the <<ZAP-FIELD>> information element is to provide the FT with the ZAP value, which is stored in the PT and is related to a subscription.

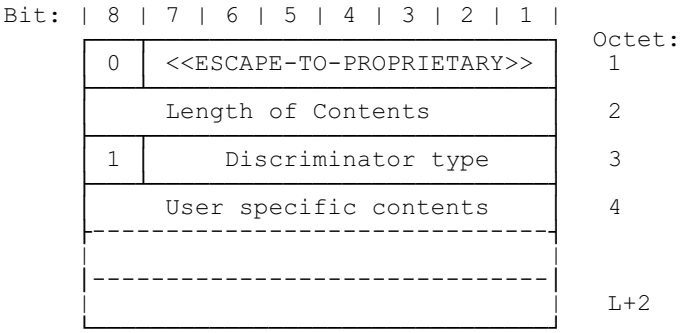


ZAP-FIELD information element

Contents field (octet 3);
Contains the 4 bit ZAP value.

7.7.45 Escape to proprietary

The purpose of the <<ESCAPE-TO-PROPRIETARY>> information element is to send non-standardised information inside a DECT message.



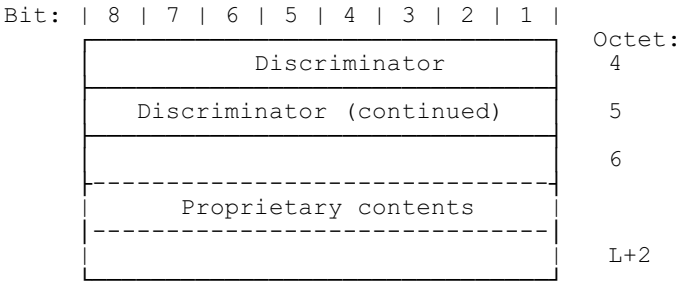
Information element format using ESCAPE-TO-PROPRIETARY

Discriminator type (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	Unspecified
	0 0 0 0 0 0 1	EMC

All other values reserved

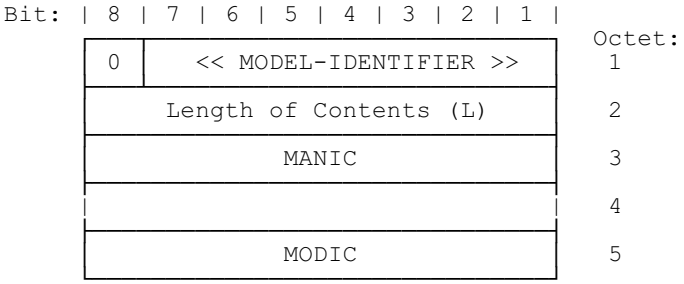
User specific contents field (octets 4 to L+2) for Discriminator type "EMC"



The discriminator consists of 2 octets (octets 4 and 5) and contains the EMC.

7.7.46 Model identifier

The purpose of <<MODEL-IDENTIFIER>> is to identify the model version of a DECT PT to the FT. This information element shall be sent from the portable to the base station during initial subscription and during location registration. It is not required during call setup and therefore does not result in an increased burdening of the CC-SETUP message.



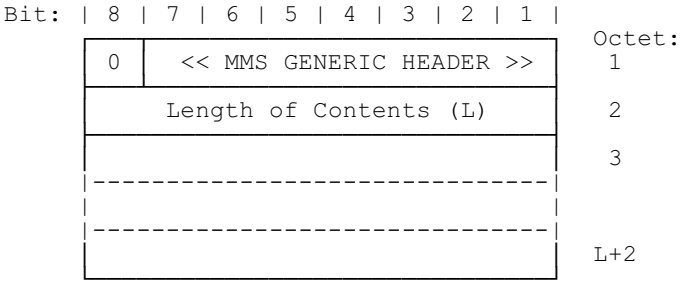
MODEL IDENTIFIER information element

MANIC coding (octets 3, 4): the field contains an EMC value allocated to a manufacturer. Generally the first allocated EMC value will be used. MANIC may be different to EMC in IPEI. The most significant bit of MANIC is in octet 3 bit 8.

MODIC coding (octet 5): the field contains an eight bit value, identifying the model version of the PT. The combination of MANIC and MODIC should be unique for each hardware/software variant of a PT. The most significant bit of MODIC is in octet 5 bit 8. 0 shall have the meaning of "model number not supported"

7.7.47 MMS Generic Header

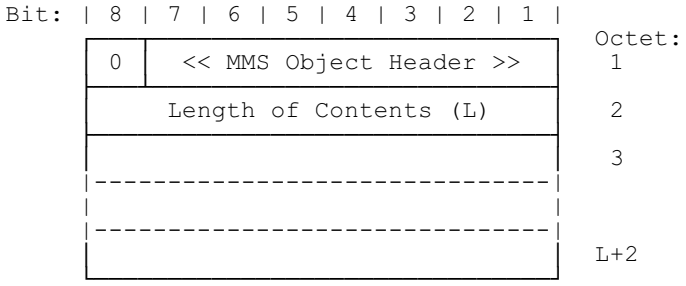
The usage and coding of the <<MMS Generic Header>> information element is defined in the F.2 Data services profile [56].



MMS GENERIC HEADER information element

7.7.48 MMS Object Header

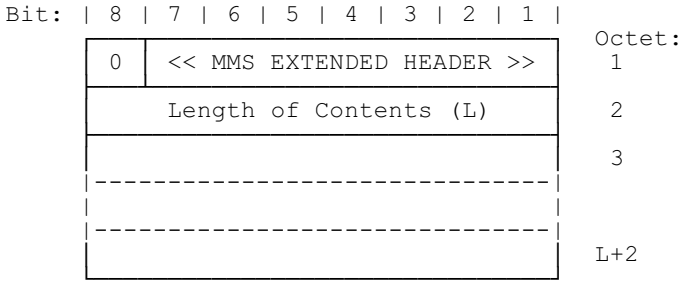
The usage and coding of the <<MMS Object Header>> information element is defined in the F.2 Data services profile [56].



MMS OBJECT HEADER information element

7.7.49 MMS Extended header

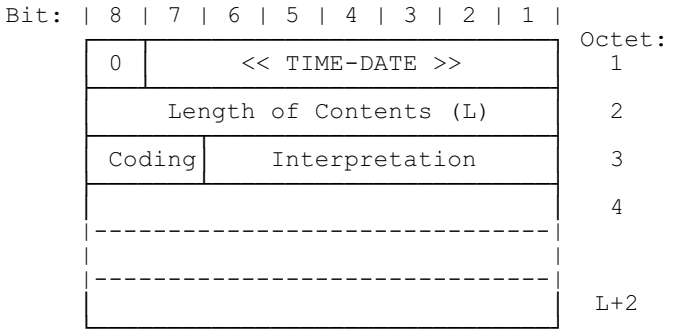
The usage and coding of the <<MMS Extended Header>> information element is defined in the F.2 Data services profile [56].



MMS EXTENDED HEADER information element

7.7.50 Time-Date

The usage and coding of the <<Time-Date>> is to provide a time and/or date.



TIME-DATE information element

Coding (octet 3):

Bits	8 7	Meaning
	0 1	Time
	1 0	Date
	1 1	Time and Date

All other values are reserved

Coding defines how the Time-Date element is structured. The coding value 1 1 " Time and date" indicates that the all fields in octets 4 - 10 of the element are present. The coding value 0 1 " Time" indicates that the octet 4 contains <Hour>, octet 5 <Minute>, octet 6 <Second> and octet 7 <Time Zone> field thus containing only the time information. The coding value 1 0 " Date" indicates that the octets 7 - 10 are omitted and the element contains only the date information. Coding 1 1 is the default value.

Interpretation (octet 3):

Bits 6 5 4 3 2 1	Meaning
0 0 0 0 0 0	The current time/date
0 0 0 0 0 1	Time duration (in Years, Months, Days and/or Hours, Minutes, Seconds, Time Zone = 0)
1 0 0 0 0 0	The time/date at which to start forwarding/delivering the MMS message (note)
1 0 0 0 0 1	The time/date the MMS user data was created (note)
1 0 0 0 1 0	The time/date the MMS user data was last modified (note)
1 0 0 0 1 1	The time/date the message was received by the MCE (note)
1 0 0 1 0 0	The time/date the message was delivered/accessed by the End Entity (note)
1 0 1 0 0 0	The time/date stamp for use as an identifier (note)

All other values are reserved

NOTE: These codings have specific meanings within the context of the MMS profiles (E.2 and F.2 Data Services [57], [56]).

Octets 4 - 6 coding (Time/Date element coding = 1 1 or 1 0)

Octet field	Digits (Semi octets)	Octet
Year	2	4
Month	2	5
Day	2	6

Octets 4 - 7 coding (Time/Date element coding = 0 1)

Octet field	Digits (Semi octets)	Octet
Hour	2	4
Minute	2	5
Second	2	6
Time Zone	2	7

Octets 7 - 10 coding (Time/Date element coding = 1 1)

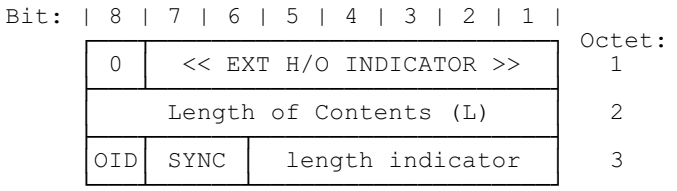
Octet field	Digits (Semi octets)	Octet
Hour	2	7
Minute	2	8
Second	2	9
Time Zone	2	10

The Time Zone indicates the difference, expressed in quarters of an hour, between the local time and GMT. In the first of the two semi-octets, the first bit represents the algebraic sign of this difference (0 : positive, 1 : negative).

The Time Zone code enables the receiver to calculate the equivalent time in GMT from the other semi-octets in the element, or indicate the time zone (GMT, GMT+1H etc.), or perform other similar calculations as required by the implementation.

7.7.51 Ext h/o indicator

The purpose of <<ext h/o indicator>> is to allow the PP to identify possible external handover candidates by comparing the PARI of the FP in use and the PARI of other FPs.



EXT H/O INDICATOR information element

length indicator coding (octet 3):

length indicator = 1+ ext h/o length indicator

The ext h/o length indicator defines how many bits of the ARI are relevant for evaluating the external handover candidate.

OID coding (octet 3)

Bits	8	Meaning
	0	Other fixed part IDs not available using parameter retrieval procedure
	1	Other fixed part IDs available using parameter retrieval procedure

SYNC coding (octet 3)

Bits	7 6	Meaning
	0 0	No synchronisation, or no information provided.
	0 1	Indicates that all identified FPs are multiframe synchronised
	1 0	Indicates that all identified FPs are multiframe and PSCN synchronised
	1 1	Indicates that all identified FPs are multiframe, multiframe number and PSCN synchronised

8 B-FORMAT message structures

8.1 General

The B-FORMAT messages shall only be originated by (and supplied to) either the LCE or the CLMS entity:

Message type	**Originator**
{LCE-REQUEST-PAGE}	LCE
{CLMS-FIXED}	CLMS

All the messages shall be fixed length, in order to allow simple mapping of the messages on to the lower layer broadcast channels (the MAC layer BS logical channel). Refer to ETS 300 175-3 [3].

All messages shall be sent to the B-SAP using the DL_BROADCAST-req or DL_EXPEDITED-req primitive. This shall use the broadcast service of the DLC.

The following formats are defined:

	Format	**Frame length (octets)**
-	short format	3 octets
-	long format	5 octets
-	extended format	5, 10, 15, 20, 25 or 30 octets

Extended format messages shall be sent in a single primitive.

NOTE: Fragmentation of the message (into slot size pieces) is performed by the MAC layer. Refer to ETS 300 175-3 [3].

8.2 LCE request paging messages

Request paging messages shall use one of the following formats:

a) short format;

b) long format.

When using short format messages, or long format messages with the IPUI address structure (see subclause 8.2.2), the following default values shall apply for the missing fields:

Target number of bearers:
default value = 1

Symmetry:
default value = symmetric connection

Slot type:
no default value is defined;
if missing, the PT may select any suitable slot type.

MAC connection type:
no default value is defined;
the PT may select any suitable connection type.

MAC packet lifetime:
default value = unlimited.

NOTE 1: The default values are chosen so that the short format message can be used to indicate most types of single bearer duplex connection. The only exception is I_p-error-correct services that require a different packet lifetime.

For multibearer connections, or for a single bearer connection with different attributes, the long format message with TPUI address structure should be used to supply the additional service attributes. The following default attributes shall apply to this message:

Minimum number of bearers:
default value = target number of bearers

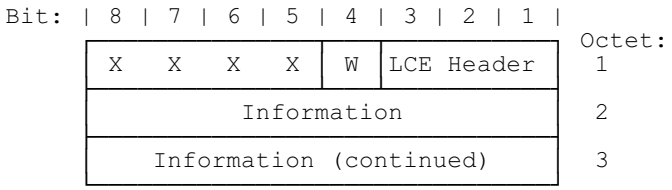
Otherwise, the LCE header coding "unknown" shall be used. In this event only a single bearer connection of unknown service type can be established and a subsequent service modification procedure is required. Refer to ETS 300 175-3 [3], subclause 10.2.4.3 for more details of service modification.

NOTE 2: A subsequent service modification is essential if the LCE header coding indicates "unknown" in order to define the wanted connection attributes. Service modification may also be used in other cases (e.g. to modify a known established connection).

8.2.1 Short format message

The short format message shall contain 20 bits of information, placed into a 3 octet frame.

Short format message



Short format message structure

W-bit

The W-bit coding in combination with the LCE header coding shall be used to distinguish different usage of the short format message, see below:

Bit 4
All values allowed

LCE header coding

The LCE header coding shall indicate the U-plane service (MAC service type) required. In addition it may indicate whether the message is used to start ringing at the portable part, see subclause 14.4:

Bits 3 2 1	U-plane service (MAC service type)
0 0 0	None
0 0 1	Unknown (MAC service type) & Ringing
0 1 0	Reserved
0 1 1	Unknown
1 0 0	I_N-min_delay
1 0 1	I_N-normal_delay
1 1 0	I_p-error-detect
1 1 1	I_p-error-correct

NOTE 1: The coding "none" indicates that no U-plane service is required. This should be used to indicate services that only require a C-plane (e.g. MM procedures).

If the paging message contains a connectionless TPUI, the U-plane coding may be used to indicate the expected service type. If the coding "unknown" is used, the PP should accept any suitable service at the indicated transmission. If the coding "none" is used, the PP should only accept C-plane connectionless services. The "none" coding is also used to announce CLMS messages.

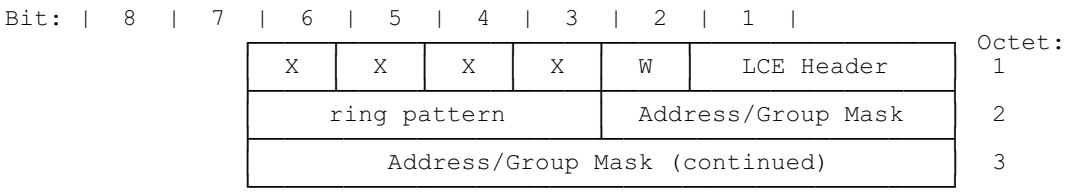
If the coding "Unknown (MAC service type) & Ringing" is used this shall be interpreted as request for ringing according to Collective/Group ringing procedure subclause 14.4 and the PP should request any suitable MAC service when it attempts to establish a link upon the outgoing call.

Octets 2 and 3

The content of octets 2 and 3 is dependent on the value of “W“ and “LCE Header“ and shall be interpreted as follows:

W	LCE Header	Octet 2 bits 5-8	Octet 2 bits 1-4	Octet 3
1	all except 001	lowest 16 bits of assigned TPUI or CBI		
0	all except 001	lowest 16 bits of default individual TPUI		
1	001	Ring pattern	group mask = sequence of ‘1s’ or/and ‘0s’	
0	001	Ring pattern	lowest 12 bits of the assigned connectionless group TPUI or CBI	

This reflects in two layouts of the short format paging currently defined:



Short format message for collective or group ringing request

Ring pattern

Bits 8 7 6 5	Meaning
0 0 0 0	alerting on - pattern 0 (NOTE 2)
0 0 0 1	alerting on - pattern 1 (NOTE 2)
0 0 1 0	alerting on - pattern 2 (NOTE 2)
0 0 1 1	alerting on - pattern 3 (NOTE 2)
0 1 0 0	alerting on - pattern 4 (NOTE 2)
0 1 0 1	alerting on - pattern 5 (NOTE 2)
0 1 1 0	alerting on - pattern 6 (NOTE 2)
0 1 1 1	alerting on - pattern 7 (NOTE 2)
1 0 0 0	alerting on - continuous
1 0 1 0	incoming call released by the FP (NOTE 3)
1 0 1 1	incoming call has been answered (NOTE 3)
1 1 1 1	alerting off
All other values reserved.	

A PT shall respond to all alerting patterns, but these may all produce the same sound.

NOTE 2: The use of alerting patterns is FT dependent; the resulting sound is PT dependent.

NOTE 3: The value does not represent a ring pattern but indicates stop of ringing.

Address/Group Mask

When used for group mask ringing this field shall include a sequence of 12 bits as group mask, see subclause 14.4.

When used for group ringing this field shall include the lowest 12 bits of the assigned connectionless group TPUI.

When used for Collective ringing this field shall include the last 12 bits of the CBI, see ETS 300 175-6 [5] subclause 6.3.1.

Short format message for all other cases

Bit: 8	7	6	5	4	3	2	1	Octet:
X	X	X	X	W	LCE Header			1
TPUI Address								2
TPUI Address (continued)								3

Short format message for all other cases

TPUI Address

This field shall include the lowest 16 bits of the TPUI, assigned or default, in accordance of the value of "W", or the lowest 16 bits of the CBI.

Refer to ETS 300 175-6 [5] for details of IPUI and TPUI.

For the address fields the order of bit values shall progressively decrease as the octet number increases.

8.2.2 Long format message

The long format message shall contain 36 bits of information, placed into a 5 octet frame. There are two structures for the long format message, and the chosen structure shall be indicated by the coding of the W bit:

Bit: 8	7	6	5	4	3	2	1	Octet:
X	X	X	X	W=1	LCE Header			1
Attributes				TPUI Address				2
TPUI Address (cont)								3
TPUI Address (cont)								4
Target bearers				MAC pkt life				5

TPUI address structure

Bit: 8	7	6	5	4	3	2	1	Octet:
X	X	X	X	W=0	LCE Header			1
IPUI Class				IPUI Address				2
IPUI Address (cont)								3
IPUI Address (cont)								4
IPUI Address (cont)								5

IPUI address structure

The address element shall be derived as follows:

W = "1": TPUI address element:
TPUI address = complete TPUI (20 bits).

W = "0": IPUI address element:
class = IPUI Class;
IPUI address = lowest 28 bits of IPUI.

For the address field, the order of bit values shall progressively decrease as the octet number increases.

LCE header coding:

refer to subclause 8.2.1.

Attributes coding:

The attributes field can contain two alternative codings, that are distinguished by the setting of bit 8. This means that a paging message can specify either the slot type for symmetric connections or the asymmetric parameter.

Slot type option:

Bits	8 7 6 5	Meaning
	0 0 0 0	Half slot; j = 0
	0 1 0 0	full slot
	0 1 0 1	double slot

Symmetry option:

Bits	8 7 6 5	Meaning
	1 0 0 1	Symmetric connection
	1 1 0 0	Asymmetric F to P with 1 duplex bearer
	1 1 0 1	Asymmetric F to P with 2 target duplex bearers
	1 1 1 0	Asymmetric P to F with 1 duplex bearer
	1 1 1 1	Asymmetric P to F with 2 target duplex bearers

All other values reserved.

NOTE 1: The default value is assumed for the missing option.

NOTE 2: A minimum of 1 duplex bearer is required for all asymmetric connections to provide the "pilot" bearer functions. Refer to ETS 300 175-3 [3].

Target bearers (advanced connections only):

Bits	8 7 6 5	Meaning
	0 0 0 0	Undefined: (pilot bearer only)
	N N N N	Target number of bearers required

NOTE 3: The target number of bearers (NNNN) is coded with the natural binary value with the least significant bit in bit position "5". The allowable values are "1" to "15".

The target number of bearers defines the total number of paired bearers to be used for the connection. For symmetric connections this refers to the total number of duplex bearers. For asymmetric connections this refers to the total number of duplex bearers PLUS the total number of double simplex bearers.

For asymmetric connections, the direction of the double simplex bearers, and the number of duplex bearers shall be defined by using the symmetry option for "attributes" field.

MAC packet life:

Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	1 n n n	Maximum packet lifetime (I_P; error_protect service only)

The maximum packet lifetime (nnn) is coded with the natural binary value with the least significant bit in bit position "1". The allowable values are "0" to "7". The value "0" shall be interpreted as unlimited (i.e. infinite). The values "1" to "7" define the maximum lifetime in TDMA frames. Refer to ETS 300 175-3 [3] for the use of this attribute.

8.3 CLMS-FIXED messages

8.3.1 General message structure

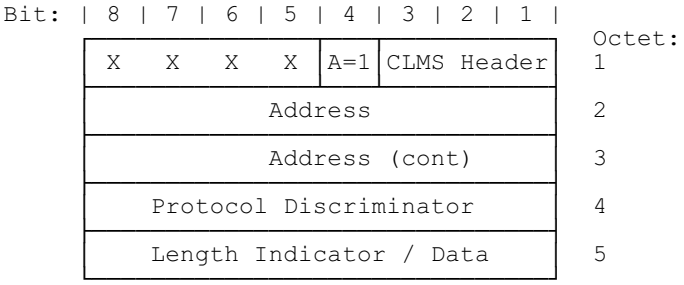
Each {CLMS-FIXED} message shall contain 1 or more message sections, where each section shall contain 36 bits of information in a 5 octet frame. {CLMS-FIXED} messages can only carry information equivalent to that contained in the <<ALPHANUMERIC>> information element (see subclause 7.7.3). {CLMS-FIXED} messages shall use the extended format.

The first section of each message shall contain addressing and control information. The remaining sections shall contain any data. The contents of any given section shall be indicated by the A bit.

Each message shall only comprise complete sections, up to a maximum of 6 sections (i.e. one address section followed by up to 5 data sections). All of the sections for a complete message shall be delivered in a single primitive, and should be received in a single primitive. Refer to subclause 12.3.1.

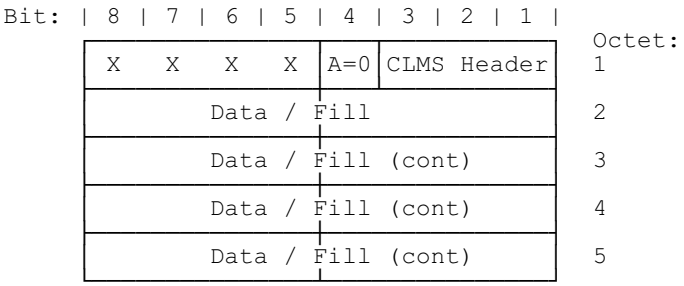
NOTE 1: The received message may be incomplete. Missing sections may not be detected by the lower layers before delivery. Missing sections may be detected by examining the length indicator element and/or the data segment numbers.

The possible data structures are defined by the protocol discriminator field, this shall use the same coding as octet 3 of the <<ALPHANUMERIC>> information element. This allows for either 8 bit characters, 4 bit characters or application specific codings.



CLMS-FIXED message structure: address section

NOTE 2: The contents of octets 5 is determined by the header coding.



CLMS-FIXED message structure: data section

8.3.2 Message elements

A-bit coding (octet 1):

A = "1" address section
A = "0" data section

CLMS header coding (octet 1):

The header coding is different for address sections and data sections. The address section allows two types of message to be defined, a DECT standard message or a general alphanumeric message. The basic structure of these messages is the same, but DECT standard messages provide standard codings for the message contents.

CLMS header coding for address section:

Bits 3 2 1	Message type	octet 4	octet 5
0 0 1	One section:	Standard	Data
0 1 0	Multi-section:	Standard	Length indicator
1 0 1	One section:	Alphanumeric	Data
1 1 0	Multi-section:	Alphanumeric	Length indicator

All other values reserved.

CLMS header coding for data section:

Bits 3 2 1	Meaning
n n n	Data section number

The first data section shall be numbered 000. The following sections shall be numbered in ascending order.

Address (octets 2 and 3 of address section):

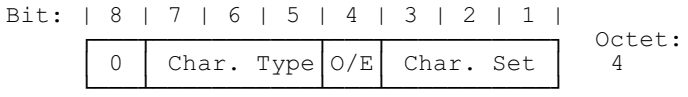
The address shall only be derived from a connectionless TPUI:

- address = lowest 16 bits of connectionless TPUI.

NOTE 1: The CLMS service requires the use of assigned TPUIs. Refer to ETS 300 175-6 [5].

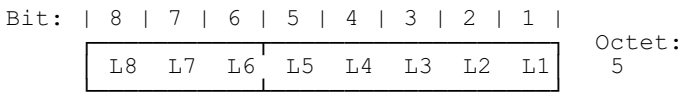
Protocol discriminator (octet 4 of address section):

Coding as for octet 3 of <<ALPHANUMERIC>>



Format of Protocol Discriminator (PD)

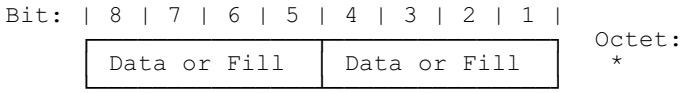
Length indicator (octet 5 of address section if multi-section): this indicates the total length of valid data in bits. The length shall be coded with the natural binary value, and the least significant bit placed in bit position 1.



Format of Length Indicator (LI)

NOTE 2: Each complete data segment contains 32 bits of valid data. Therefore the most significant 3-bits shall indicate the total number of data segments.

Data/Fill (octet 5 of address section if single-section and all data sections):



Format of Data/Fill

Each Data/Fill octet is used to carry the user information. This shall be formatted in accordance with the format indicated in the protocol discriminator octet.

All 8-bit data characters shall always be coded with one character per octet. Multiple characters shall be interpreted in the order of ascending octet numbers. Characters that are originally coded in less than 8-bits shall be padded up to 8-bits as follows:

- the original character is placed in the octet, with the least significant bit in bit position "1", and a unused bit positions are filled with "0".

4-bit data characters shall always be coded with two characters per octet. Multiple characters shall be interpreted in the order of ascending octet numbers, and within each octet the high placed character (bits position 5-8) first.

Fill characters (8-bit or 4-bit as appropriate) shall then be inserted to fill up the final octets.

A complete data segment that contains no valid data (i.e. fill only) shall not be transmitted.

8.3.3 Standard message structures

8.3.3.1 General

DECT standard messages shall only use one of the DECT standard character sets: either 4-bit characters or 8-bit characters. In both cases, the first character of the message shall be used as a message type identifier to define the meaning of the following characters.

8.3.3.2 Messages using 4-bit characters

Table 16: Messages using 4-bit characters

Message Type	1st char.	2nd char.	Other characters
Tone alert	0	0 to 9	not allowed
Other messages are for further standardisation			

Message type 0: tone alert: the second character identifies one of ten possible alerting tones. The use of tones by the FT, and the resulting sound at the PT shall not be defined in this ETS.

8.3.3.3 Messages using 8-bit characters

Table 17: Messages using 8-bit characters

Message Type	1st char.	2nd char.	Other characters
8-bit messages are for further standardisation			

9 Call Control (CC) procedures

9.1 General

The Call Control (CC) procedures provide mechanisms to support both circuit oriented and packet oriented services. Each independent service is called a "call" and this is controlled by an independent instance of CC. A CC always establishes circuit oriented lower resources to provide the service (i.e. uses the MAC layer connection oriented service). The CC represents a group of procedures covering all aspects of call establishment and release, and also covering a range of call related supplementary services (CRSS).

The protocol allows for multiple instances of a CC call at both the fixed termination and at the portable termination (for example, a PT may provide two or more simultaneous calls). These multiple instances are assumed to operate completely independently from each other. The possible existence of multiple instances is therefore ignored in the following clauses, which only describe the procedures for a single instance, denoted as the CC entity.

Figure 3 illustrates the states and transitions on the PT side.

Figure 4 illustrates the states and transitions on the FT side.

An alternative description of the CC state transitions is included in annex B. This contains a state transition table, plus a summary of the transition procedures. This annex is included as a shortform summary. In the event of any discrepancy, the main text (the following clauses) take precedence.

A reliable C-plane DLC link (LAPC) shall be available before any of these CC procedures can operate. The establishment and maintenance of this link is the responsibility of the LCE and is described in clause 14.

NOTE: A "LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. If a CC timer expires whilst in this state, the resulting release should be handled locally.

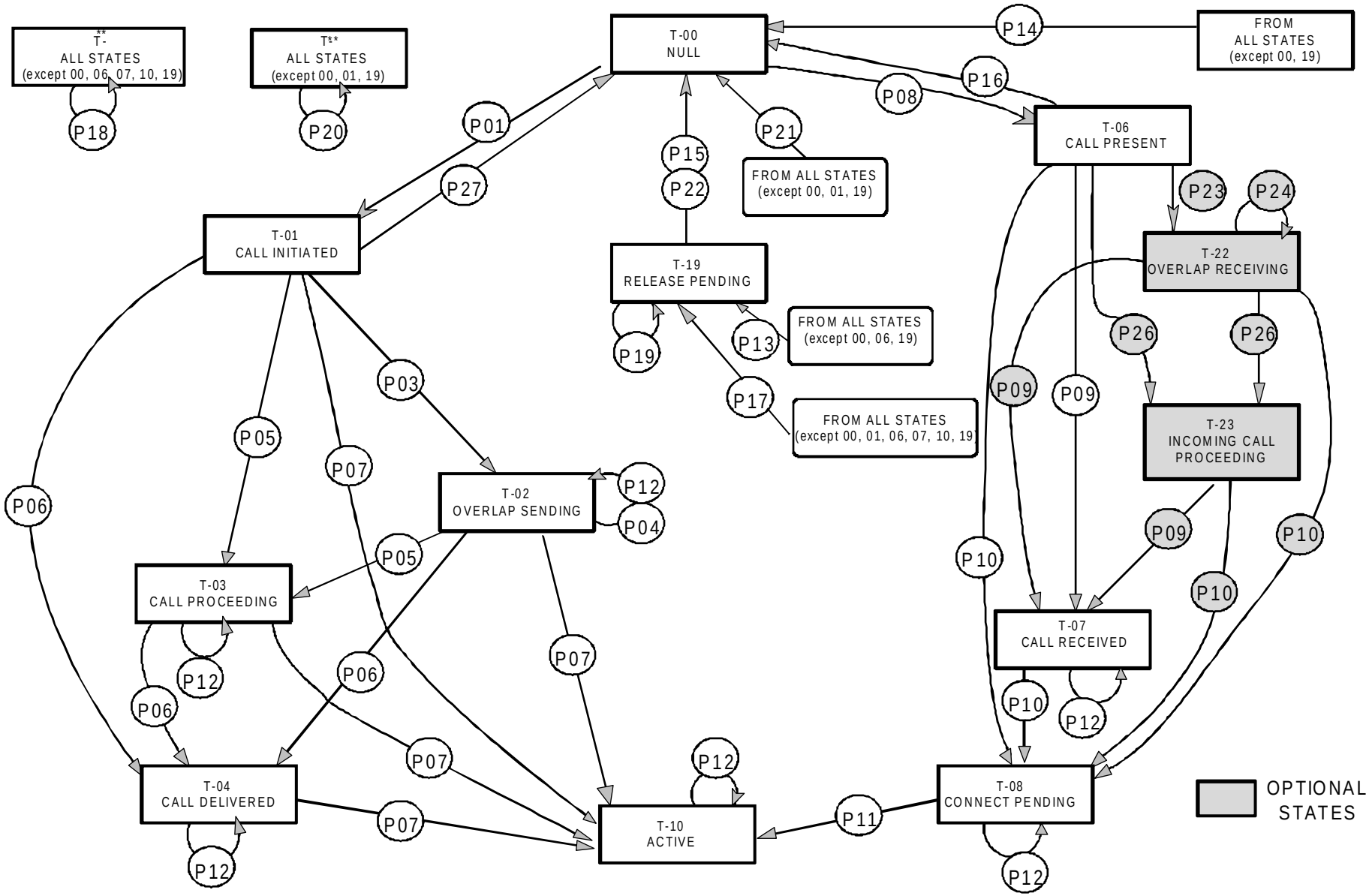


Figure 3: Call control states in the PT

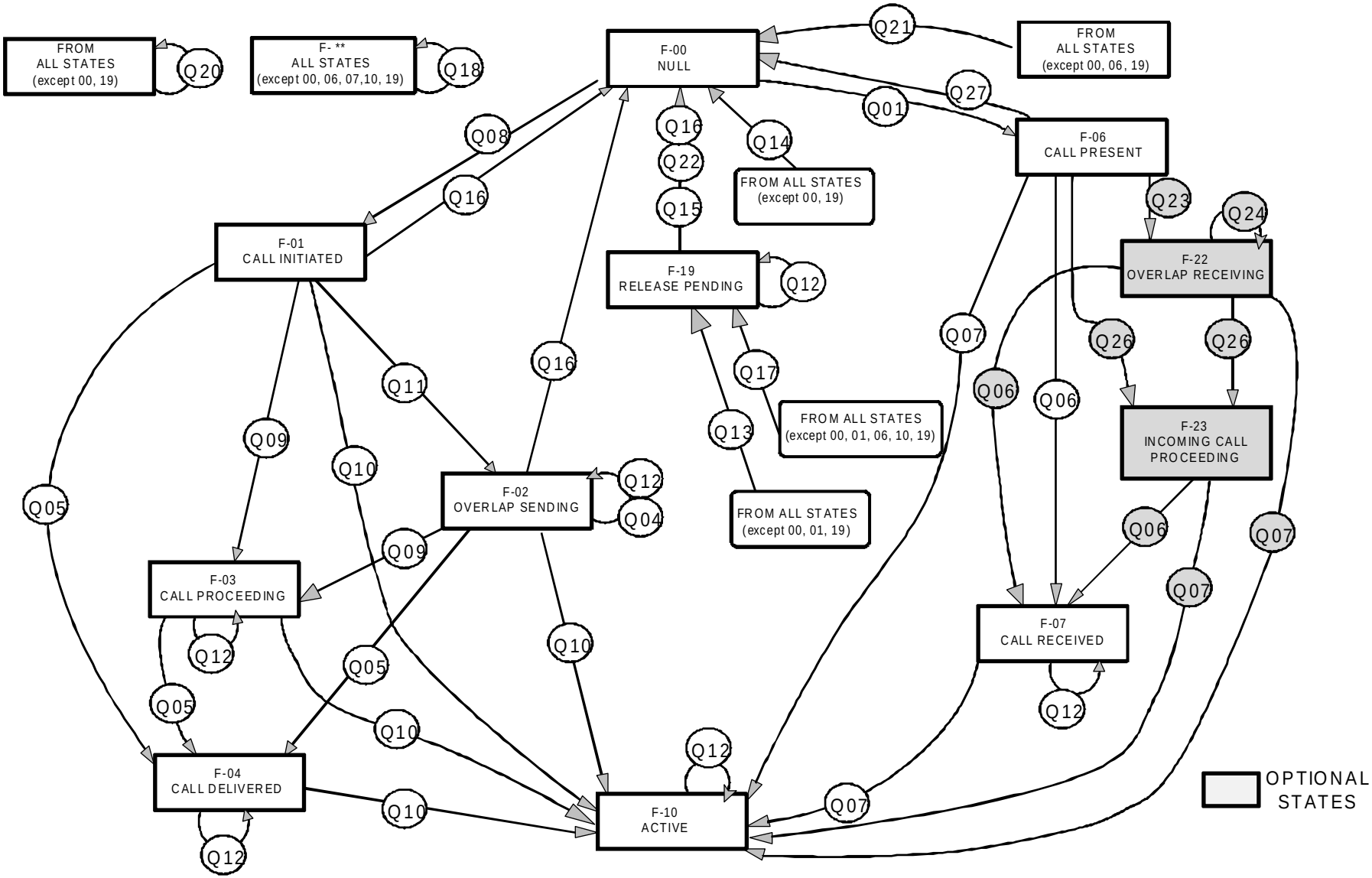


Figure 4: Call control states in the FT

9.2 Call Control (CC) states

9.2.1 States at PT

Central call states

9.2.1.1 State T-00: "NULL"

No call exists.

9.2.1.2 State T-19: "RELEASE PENDING"

The PT has sent a release message to the FT, but has not received a response.

9.2.1.3 State T-10: "ACTIVE"

a) The PT user has answered an incoming call;

b) the PT has received an indication that the FT has connected a PT outgoing call.

PT originated call states (outgoing call)

9.2.1.4 State T-01: "CALL INITIATED"

A PT initiated call has been started, by sending a set-up message to the FT.

9.2.1.5 State T-02: "OVERLAP SENDING"

An outgoing call is being established using "OVERLAP SENDING".

9.2.1.6 State T-03: "CALL PROCEEDING"

The PT has received a message from the FT to confirm that all set-up information has been received.

9.2.1.7 State T-04: "CALL DELIVERED"

The PT has received a message from the FT that indicates that called party alerting has been started.

PT terminated call states (incoming call)

9.2.1.8 State T-06: "CALL PRESENT"

The PT has received a set-up message from the FT, but has not yet responded.

9.2.1.9 State T-07: "CALL RECEIVED"

The PT has sent a message to the FT to report alerting of the user, but the user has not yet responded.

9.2.1.10 State T-08: "CONNECT PENDING"

The PT user has answered the call, but is waiting for a message from the FT giving confirmation of a U-plane connection (assumed to be an end-to-end connection).

9.2.2 States at FT

Central call states

9.2.2.1 State F-00: "NULL"

No call exists.

9.2.2.2 State F-19: "RELEASE PENDING"

The FT has sent a release message to the PT, but has not received a response.

9.2.2.3 State F-10: "ACTIVE"

a) The FT has allocated an incoming call to one PT;

b) the FT has sent a message to the PT reporting connection of an outgoing call (assumed to mean that the called party has answered the outgoing call).

NOTE: The ACTIVE state is typically used for intelligent networks when the connection is completed and for PSTN when the PT goes off hook.

PT originated call states (outgoing call)

9.2.2.4 State F-01: "CALL-INITIATED"

A PT initiated call set-up has been started. The FT has received a set-up message from the PT, but has not yet replied.

9.2.2.5 State F-02: "OVERLAP SENDING"

A PT initiated call is being established using "OVERLAP SENDING".

NOTE: The OVERLAP SENDING state is typically used when the DECT FT wants to receive more digits from the PT. The {CC-SETUP-ACK} can originally come from the network or just locally from the FT.

9.2.2.6 State F-03: "CALL PROCEEDING"

The FT has sent a message to the PT to confirm that all set-up information has been received.

NOTE: The CALL PROCEEDING state is typically used for telling the PT that the connected network is routing the call but has not started to alert.

9.2.2.7 State F-04: "CALL DELIVERED"

The FT has sent a message to the PT reporting that it has received notification that called party alerting has started.

NOTE The CALL DELIVERED state is typically used for telling the PT that the called party is alerting.

PT terminated call states (incoming call)

9.2.2.8 State F-06: "CALL PRESENT"

The FT has sent a set-up message to the PT, but has not yet received a satisfactory response.

9.2.2.9 State F-07: "CALL RECEIVED"

The FT has received a message from the PT to report that it is alerting the user (but the user has not yet responded).

9.2.3 Optional states (PT and FT)

The following states are optional. They are required for incoming calls, when DECT is being used as an intermediate network. In this case, the call is not terminated in the DECT portable termination, and these additional states are used to allow the call establishment procedures to interact with the attached network on the PT side.

9.2.3.1 States T-22 and F-22: "OVERLAP RECEIVING"

An incoming call is being established using "OVERLAP RECEIVING".

9.2.3.2 States T-23 and F-23: "INCOMING CALL PROCEEDING"

The PT has sent a message to the FT to confirm that all set-up information has been received.

9.3 Call establishment procedures

9.3.1 PT initiated call establishment (outgoing call)

PT initiated call establishment is started upon receipt of a MNCC_SETUP-req primitive by the CC entity at the PT side (P-CC). This primitive shall specify the type of call required.

9.3.1.1 Call request

Case A: normal call or internal call request

The CC entity in the PT (P-CC) starts a normal or internal call establishment by sending a {CC-SETUP} message to its peer CC entity in the FT (F-CC). This message is submitted to the LCE in the PT, and the P-CC entity enters the "CALL INITIATED" state and starts timer P<CC.03>.

The {CC-SETUP} message shall carry a full portable part identity (the IPUI) plus a full fixed part identity (the relevant ARI) according to the identity rules given in ETS 300 175-6 [5].

The {CC-SETUP} message shall contain the <<BASIC-SERVICE>> information element. This element shall indicate "normal set-up" or "internal call set-up" and may optionally indicate "basic speech default set-up attributes" (or other profile specific default attributes), in which case the service shall be defined by the defined default codings given in annex E or in the relevant profile specification when explicitly stated and no further <<IWU-ATTRIBUTES>> or <<CALL-ATTRIBUTES>> elements shall be included. Alternatively, if the service is indicated as "other", the set-up message shall also contain the <<IWU-ATTRIBUTES>>element, and optionally <<CALL-ATTRIBUTES>> element to fully define the required service, such that all the necessary resources can be reserved and installed by the FT and the interworking unit at the FT side (F-IWU).

NOTE 1: The set-up message may contain a list of attribute elements when using prioritised list negotiation. Refer to subclause 15.2.2.

The PT may include the <<TERMINAL-CAPABILITY>> element in the {CC-SETUP} message. If omitted the last available values (e.g. as received in {LOCATE-REQUEST} or {ACCESS-RIGHTS-REQUEST} should be assumed. Otherwise the default values shall be assumed.

NOTE 2: The action of a FT in response to an omitted <<TERMINAL-CAPABILITY>> element is not defined in this ETS. They should be defined in the relevant profiles specifications based on DECT CI.

Case B: emergency call request

Emergency call establishment uses the same CC procedures as normal call establishment, except that the call shall be indicated as an "emergency call" in the <<BASIC-SERVICE>> information element.

The <<BASIC-SERVICE>> element for an emergency call request shall always indicate the "default service attributes" (i.e. shall only request a single bearer speech call).

Emergency call requests shall only be supported for PT initiated call.

Case C: external handover request

Call establishment for external handover uses the same CC procedures as normal call establishment, except that the call shall be indicated as an "external handover" in the <<BASIC-SERVICE>> information element.

External handover call set-up is used in the direction P to F only.

Case D: Service call request

Call establishment for a service call uses the same CC procedures as normal or internal call establishment , except that the call shall be indicated as a "service call setup" in the <<BASIC-SERVICE>> information element.

Service call request shall only be supported for PT initiated calls

Case E: Supplementary Service call request

Call establishment for a supplementary service call uses the same CC procedures as normal or internal call establishment , except that the call shall be indicated as a "supplementary service call setup" in the <<BASIC-SERVICE>> information element.

Case F: Messaging call request

Call establishment for messaging call uses the same CC procedures as normal call establishment except that the call shall be indicated as a “Messaging call setup” in the <<BASIC SERVICE>> information element.

NOTE 1: The messaging call set up should be used for store and forward type of messaging applications.

9.3.1.2 Call accept or reject

Call accept:

Upon receipt of a {CC-SETUP} message, the F-CC shall enter the "CALL INITIATED" state. The F-CC entity shall examine the attributes defined in the {CC-SETUP} message and attempt to fulfil them. If it can meet the request, it shall issue a MNCC_SETUP-ind primitive to the interworking unit at the fixed side (F-IWU).

NOTE 1: Either the F-CC or the F-IWU may reject the call. The F-CC examines the <<CALL-ATTRIBUTES>> and the <<CONNECTION-ATTRIBUTES>> elements, and the F-IWU examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the F-IWU after it has been accepted by the F-CC. The call may also be rejected by the local network.

If the F-IWU accepts the call it is expected to reply with one of the following primitives:

a) a MNCC_SETUP_ACK-req primitive;

b) a MNCC_CALL_PROC-req primitive;

c) a MNCC_ALERT-req primitive;

d) a MNCC_CONNECT-req primitive.

Upon receipt of one of these primitives, the F-CC shall act according to subclauses 9.3.1.3 to 9.3.1.9.

Call reject:

If the F-CC cannot meet any of the set-up requests, or if the {CC-SETUP} message contains errors or inconsistencies, or if the F-IWU rejects the call by responding to the MNCC_SETUP-ind primitive with a MNCC_REJECT-req primitive, the FT shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the "NULL" state.

The MNCC_REJECT-req should include a release reason (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the PT shall act according to subclause 9.5.2.

NOTE 2: Call rejection may also occur as part of exchanged attribute service negotiation. Refer to subclause 15.2.3.

Expiry of timer <CC.03>

Timer P<CC.03> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {CC-NOTIFY} message. If timer P<CC.03> expires before a suitable reply (or a restart) is received, the P-CC should immediately reject the call by sending a {CC-RELEASE-COM} message, with the reason set to "timer expiry". It shall then issue a MNCC_REJECT-ind primitive indicating unacknowledged release (cause = local timer expiry) and shall enter the "NULL" state.

9.3.1.3 Selection of lower layer resources

The following procedures shall only be used when using advanced connections. The elements described in this subclause shall be omitted when using basic connections, and this omission shall be understood to indicate a basic connection.

The PT should indicate the lower layer resources (DLC U-plane link identifier and MAC connection identifier) by including a <<CONNECTION-IDENTITY>> element in the {CC-SETUP} message. If this element is included, the FT shall be obliged to use the indicated resources or shall reject the call.

NOTE 1: The attributes of the indicated connection may still be undefined (i.e. connection type "unknown") at this point. The attributes are subsequently defined by the MAC establishment procedures (PT initiated).

Alternatively <<CONNECTION-ATTRIBUTES>> elements may be used to postpone the establishment (or modification) of suitable connection(s) until the set-up is accepted (e.g. if the PT is attempting to set-up a second call using the C-plane resources of an existing call). In this event, the PT may include one or more <<CONNECTION-ATTRIBUTES>> elements in the {CC-SETUP} message; one element for each postponed connection. Each element contains a valid Logical Connection Number assignment (see ETS 300 175 - 4 [4]) if it refers to an established connection (i.e. a postponed modification).

If the <<CONNECTION-IDENTITY>> element is omitted, or if it contains one or more connection identities that are indicated as "unknown" (thereby indicating that the link associations are not defined) the FT shall nonetheless reserve all of the DLC resources upon accepting the call. The FT shall then associate these DLC resources (U-plane links) to the connections by using all of the PT defined associations, and adding FT defined associations for the remaining (unknown) link associations. It shall then confirm the complete set of associations by including a <<CONNECTION-IDENTITY>> element in the first response message (i.e. {CC-SETUP-ACK}, {CC-CALL-PROC}, {CC-ALERTING} or {CC-CONNECT}). This element may be omitted if all associations have been defined by the PT in the {CC-SETUP} message.

NOTE 2: The FT may also be required to modify existing connections as indicated by the <<CONNECTION-ATTRIBUTES>> elements. In this event, the <<CONNECTION-IDENTITY>> response indicates that this modification has been initiated.

NOTE 3: "Unknown" PT assignments are intended to allow FT choice when the indicated resources require FT modification of existing connections. "Unknown" assignments may also be used in other cases, provided that all possible associations are acceptable for the PT.

Upon receipt of the first message from the FT indicating acceptance of the set-up, the PT shall immediately establish all remaining connections (or modify existing connections) and shall associate all remaining U-plane links to complete the required service.

NOTE 4: In all cases, it is the responsibility of the PT to establish any new connections.

If any of the required resources are not available, the FT shall reject the call.

Both the <<CONNECTION-IDENTITY>> and the <<CONNECTION-ATTRIBUTES>> elements shall be omitted from all messages for a call establishment relating to a basic connection. If this basic connection is not already established when the {CC-SETUP} message is received, the call shall be rejected.

9.3.1.4 Connection of U-plane

The PT is not required to request the LLME to connect its receive U-plane unless it receives a message containing the <<PROGRESS-INDICATOR>> element indicating cause no. 8 ("In-band information or appropriate pattern is now available in band"). The FT should not assume that the PT has connected the U-plane unless this message has been sent.

NOTE: If this <<PROGRESS-INDICATOR>> element is not used, the PT may delay connection of the U-plane until receipt of the {CC-CONNECT} message. See subclause 9.3.1.8.

9.3.1.5 Overlap sending

"OVERLAP SENDING" is indicated if the F-CC receives a MNCC_SETUP_ACK-req primitive.

Upon receipt of this primitive, the F-CC shall send a {CC-SETUP-ACK} message to the P-CC. It shall then start timer F<CC.01> and shall enter the "OVERLAP SENDING" state. In this state it is waiting for a {CC-INFO} message (or messages) from the P-CC.

Upon receipt of the {CC-SETUP-ACK} message, the P-CC shall stop timer P<CC.03>, shall optionally start timer P<CC.04>. It shall then issue a MNCC_SETUP_ACK-ind primitive and shall enter the "OVERLAP SENDING" state.

The remainder of the set-up information should now be supplied by the PP application in a series of one or more MNCC_INFO-req primitives. The P-CC shall send this information in one or more {CC-INFO} messages.

The called party number shall be supplied by the PP application in one of two ways:

- en-bloc sending, where the called party number is sent in a single variable length <<CALLED-PARTY-NUMBER>> information element;

- piecewise sending, where the called party number is sent in a series of fixed or variable length <<"KEYPAD">> information elements, contained in one or more messages (one <<"KEYPAD">> element per message).

Only one method of sending shall be used within any one call.

NOTE 1: This ETS allows piecewise sending to include more than one character in each <<"KEYPAD">> information element.

NOTE 2: The length of the called party number is defined by the length of the <<CALLED-PARTY-NUMBER>> information element when this is used. If <<"KEYPAD">> information elements are used the length definition is specific to the F-IWU: it may be undefined, or it may be defined by the <<SENDING-COMPLETE>> information element.

Upon receipt of a {CC-INFO} message, the F-CC shall immediately forward the contents to the F-IWU in a MNCC_INFO-ind primitive, and shall restart timer F<CC.01>.

Call reject

If the F-CC cannot meet any of the set-up requests whilst in the "OVERLAP SENDING" state, or if a {CC-INFO} message contains errors or inconsistencies, or if the F-IWU rejects the call by responding to a MNCC_INFO-ind primitive with a MNCC_REJECT-req primitive, the FT shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the NULL state.

The MNCC_REJECT-req should include a release reason (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the PT shall act according to subclause 9.5.2.

9.3.1.6 Call proceeding

Upon receipt of the MNCC_CALL_PROC-req primitive, the F-CC shall stop timer F<CC.01>, shall enter the "CALL PROCEEDING" state and shall send a {CC-CALL-PROC} message to the P-CC. It shall then start timer F<CC.04> (if implemented).

Upon receipt of the {CC-CALL-PROC} message, the P-CC shall stop timer P<CC.03> if running and should start timer P<CC.04> (if implemented). It shall then issue a MNCC_CALL_PROC-ind primitive and shall enter the "CALL PROCEEDING" state.

The F-IWU may also issue this primitive without receiving a complete called party number. In this event, any (subsequent) dialling shall only appear in <<"KEYPAD">> information elements. For example, in the case of queue management, see subclause 10.6.2.

If timer F<CC.01> expires before a suitable primitive is received, the F-CC should immediately release the call using the release procedures defined in subclause 9.5.1. The {CC-RELEASE} message should contain the reason “TIMER-EXPIRY”.

9.3.1.7 Call confirmation

When the F-CC receives a MNCC_ALERT-req primitive (usually meaning that user alerting has been initiated at the called destination), the F-CC may send a {CC-ALERTING} message to the P-CC. This message shall only be sent if the U-plane resources are fully installed. The F-CC shall stop timer F<CC.01> if running and shall start timer F<CC.04> (if implemented). It shall then enter the "CALL DELIVERED" state.

Upon receipt of a {CC-ALERTING} message, the P-CC shall stop timer P<CC.03> if running, and should start timer P<CC.04> if not running and if implemented. It shall then issue a MNCC_ALERTING-ind primitive and shall enter the "CALL DELIVERED" state.

9.3.1.8 Call connection

Upon receiving a MNCC_CONNECT-req primitive (usually meaning that the call has been accepted by the destination), the F-CC shall request confirmation of the U-plane connection from the F-LLME. When the U-plane is confirmed, it shall stop timer F<CC.01> if running and shall send a {CC-CONNECT} message to the P-CC. It shall then enter the "ACTIVE" state.

On receipt of the {CC-CONNECT} message the P-CC shall request confirmation of the U-plane connection from the P-LLME. When the U-plane connection is confirmed, the P-CC shall stop timer P<CC.03> if running, stop timer P<CC.04> if used, and enter the "ACTIVE" state. It shall then issue a MNCC_CONNECT-ind primitive.

9.3.1.9 Expiry of timer <CC.04>

Timer P<CC.04> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {CC-NOTIFY} message. If timer P<CC.04> expires, the P-CC shall immediately release the call using the procedures described in subclause 9.5.1.

Equally, if timer F<CC.04> expires, the F-CC shall immediately release the call using the procedures described in subclause 9.5.1.

NOTE: The use of timer <CC.04> is optional for both PT and FT.

9.3.2 FT initiated call establishment (incoming call)

FT initiated call establishment is started upon receipt of a MNCC_SETUP-req primitive by the CC entity at the FT side (F-CC).

9.3.2.1 Call request

The F-CC entity starts the call establishment by sending a {CC-SETUP} message to its peer entity at the PT side (P-CC). This message is submitted to the LCE in the FT, and the F-CC enters "CALL PRESENT" state and starts timer F<CC.03>.

For individual calls, the {CC-SETUP} message shall carry a full portable part identity (the IPUI) plus a full fixed part identity (the relevant ARI) according to the identity rules given in ETS 300 175-6 [5]. For group calls the {CC-SETUP} message shall carry either one full portable part identity (one IPUI) or one group identity (one group TPUI) plus a full fixed part identity (the relevant ARI).

The {CC-SETUP} message shall contain the <<BASIC-SERVICE>> information element. This element shall indicate "normal set-up" and may optionally indicate "default service attributes", in which case the service shall be defined by the defined default codings given in annex E and no further <<IWU-ATTRIBUTES>> or <<CALL-ATTRIBUTES>> elements shall be included. Alternatively, if the service is indicated as "other", the set-up message shall also contain the <<IWU-ATTRIBUTES>> element, and optionally the <<CALL-ATTRIBUTES>> element to fully define the required service, such that all the necessary resources can be reserved and installed by the PT.

NOTE: The set-up message may contain a list of attribute elements when using prioritised list negotiation. Refer to subclause 15.2.2.

9.3.2.2 Call accept or reject

Call accept

Upon receipt of a {CC-SETUP} message the P-CC shall enter the "CALL PRESENT" state. The P-CC entity shall examine the attributes defined in the {CC-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCC_SETUP-ind primitive.

NOTE: Either the P-CC or an IWU application may reject the call. The P-CC examines the <<CALL-ATTRIBUTES>> and the <<CONNECTION-ATTRIBUTES>> elements, and the PP-IWU examine the <<IWU-ATTRIBUTES>> element. The call is only offered to the PP-IWU after it has been accepted by the P-CC.

If the PP-IWU accept the call, they are expected to respond to the P-CC with one of the following primitives:

For normal calls:

a) a MNCC_ALERT-req primitive;

b) a MNCC_CONNECT-req primitive.

For calls using "OVERLAP RECEIVING":

c) a MNCC_SETUP_ACK-req primitive;

d) a MNCC_CALL_PROC-req primitive.

Upon receipt of one of these primitives, the P-CC shall act according to subclauses 9.3.2.3 to 9.3.2.8.

Call reject

If the PT cannot meet any of the demands, or if the {CC-SETUP} message contains errors or inconsistencies, or if a MNCC_REJECT-req primitive is received in response to the MNCC_SETUP-ind primitive (thus indicating rejection by the PP-IWU), the P-CC entity shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the "NULL" state.

The MNCC_REJECT-req should include a release reason (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the FT shall act according to subclause 9.5.2.

Expiry of timer <CC.03>

If timer F<CC.03> expires before a suitable reply is received, the F-CC shall immediately reject the call by sending a {CC-RELEASE-COM} message, with the reason set to “TIMER-EXPIRY”. It shall then issue a MNCC_REJECT-ind primitive indicating unacknowledged release (cause = local timer expiry) to the F-IWU and shall enter the "NULL" state.

9.3.2.3 Selection of lower layer resources

The following procedures shall only be used for advanced connections. These elements shall be omitted when using basic connections, and this omission shall be understood to indicate a basic connection.

The FT may indicate the lower layer resources (DLC U-plane link identifier and MAC connection identifier) by including a <<CONNECTION-IDENTITY>> element in the {CC-SETUP} message. If this element is included, the PT shall be obliged to use the indicated resources or shall reject the call. The FT may also include the <<CONNECTION-ATTRIBUTES>> element to indicate other needed connections.

NOTE 1: The attributes of the indicated connection may still be undefined (i.e. connection type "unknown") at this point. The attributes are subsequently be defined by the MAC establishment procedures (FT initiated).

If the <<CONNECTION-ATTRIBUTES>> element indicates a connection identifier as "unknown", this indicates that the PT should immediately initiate the establishment of this connection prior to sending the first response message.

NOTE 2: The <<CONNECTION-ATTRIBUTES>> may also be used to indicate an existing connection that requires a bandwidth modification by the PT.

If the <<CONNECTION-IDENTITY>> element is omitted, or if it contains one or more connection identities that are indicated as "unknown" (thereby indicating that the link associations are not defined) the PT shall nonetheless reserve all of the DLC resources upon accepting the call. The PT shall then associate these DLC resources (U-plane links) to the connections by using all of the FT defined associations, and adding PT defined associations for the remaining (unknown) link associations. It shall then confirm the complete set of associations by including a <<CONNECTION-IDENTITY>> element in the first response message (i.e. {CC-ALERTING} or {CC-CONNECT}). This element may be omitted if all associations have been defined by the FT in the {CC-SETUP} message.

If suitable resources are not available and cannot be established the PT shall reject the call.

Both the <<CONNECTION-IDENTITY>> and the <<CONNECTION-ATTRIBUTES>> elements shall be omitted from all messages for a call establishment relating to a basic connection. If this basic connection is not already established when the {CC-SETUP} message is received, the call shall be rejected.

9.3.2.4 Connection of U-plane

The PT is not required to request the LLME to connect its receive U-plane unless it receives a message containing the <<PROGRESS-INDICATOR>> element indicating cause no. 8 ("in-band information or appropriate pattern is now available in band"). The FT should not assume that the PT has connected the U-plane unless this message has been sent.

NOTE: If this <<PROGRESS-INDICATOR>> element is not used, the PT may delay connection of the U-plane until receiving of the {CC-CONNECT-ACK} message. See subclause 9.3.2.8.

9.3.2.5 Overlap receiving

These procedures are optional, and shall only apply to PTs that implement this option.

9.3.2.6 Call proceeding

For FT initiated calls, the set-up message should normally contain sufficient information to complete the call. However the F-CC may also send any supplementary information (e.g. <<"DISPLAY">> information elements) in a subsequent {CC-INFO} message (or messages) in response to MNCC_INFO-req primitives from the F-IWU.

9.3.2.7 Call confirmation

Confirmation of the call is indicated when a MNCC_ALERT-req primitive is received at the P-CC (usually indicating that user altering has been initiated). Upon receipt of this primitive, the P-CC shall send a {CC-ALERTING} message to the F-CC and shall enter the "CALL RECEIVED" state.

The F-CC, upon receipt of the {CC-ALERTING} message shall stop timer F<CC.03> and shall start timer F<CC.04> (if implemented). It shall then issue a MNCC_ALERT-ind primitive and shall enter the "CALL RECEIVED" state.

Whilst in the "CALL-RECEIVED" state, the FT may send further information to the PT in one or more {CC-INFO} messages in response to further MNCC_INFO-req primitives. The PT should issue the contents of all these messages using MNCC_INFO-ind primitives.

NOTE: Cadence following of the PT alerting may be achieved by sending a sequence of <<SIGNAL>> elements in a series of {CC-INFO} messages.

9.3.2.8 Call connection

Connection of the call is indicated when an MNCC_CONNECT-req primitive is received by the P-CC (usually indicating that the call has been accepted by the PT user). Upon receipt of this primitive, the P-CC should request confirmation of the U-plane connection from the LLME and shall send a {CC-CONNECT} message to the F-CC. It shall then start timer P<CC.05> and enter the "CONNECT PENDING" state.

NOTE: If the U-plane is connected the receive path may be muted.

On receipt of the {CC-CONNECT} message the F-CC shall stop timer F<CC.03> if running and shall stop timer F<CC.04> if running (and if implemented). It then issues a MNCC_CONNECT-ind primitive to the F-IWU. On receipt of a MNCC_CONNECT-res primitive the FT shall request confirmation of the U-plane connection from the LLME and when confirmed it shall return a {CC-CONNECT-ACK} message to the PT and shall enter the "ACTIVE" state.

Upon receipt of the {CC-CONNECT-ACK} message the P-CC shall request the U-plane connection from the P-LLME, (if not already connected) and when confirmed it shall stop timer P<CC.05>, It then issues a MNCC_CONNECT-cfm primitive, and shall enter the "ACTIVE" state.

If timer P<CC.05> expires, the P-CC shall immediately release the call using the normal procedure described in subclause 9.5.1.

9.3.2.9 Sending of <<TERMINAL-CAPABILITY>>

The PT may include the <<TERMINAL-CAPABILITY>> element in its first response message. If omitted the last available values (e.g. as received in {LOCATE-ACCEPT} or {ACCESS-RIGHTS-REQUEST}) should be assumed. Otherwise the default values shall be assumed.

NOTE: The action of a FT in response to an omitted <<TERMINAL-CAPABILITY>> element is not defined in this ETS. They should be defined in the relevant profiles specifications based on DECT CI.

9.3.2.10 Expiry of timer <CC.04>

If timer F<CC.04> expires, the F-CC shall immediately release the call using the procedures described in subclause 9.5.1.

NOTE: The use of timer <CC.04> is optional.

9.4 Call information procedures

While in the "ACTIVE" state, the P-CC and F-CC shall immediately transfer any information received in MNCC_INFO-req primitives, using a series of one or more {CC-INFO} messages. Upon receipt of a {CC-INFO} message, the peer CC entity shall immediately issue the contents in a MNCC_INFO-ind primitive.

Service change procedures during the call information phase are described in subclause 9.6.

9.5 Call release procedures

9.5.1 Normal call release

The call release procedures may be started by the CC entity at either side at any time, upon receipt of a MNCC_RELEASE-req primitive or as a result of timer expiry as described in subclause 9.3.

NOTE 1: A MNCC_RELEASE-req primitive is an illegal response to a call set-up. The following normal call release procedure is not followed when responding to a call set-up. A FT in the "CALL INITIATED" or "OVERLAP SENDING" state responds as though rejecting the call set-up and should follow the procedures defined in subclauses 9.3.1.2 and 9.3.1.5 for PT initiated calls. A PT in the "CALL PRESENT" state responds as though rejecting the call set-up and should follow the procedures defined in subclause 9.3.2.2 for FT initiated calls.

To initiate a normal release, the starting entity sends a {CC-RELEASE} message, starts timer <CC.02>, and enters the "RELEASE PENDING" state. The release message may include an information element giving the reason for the release, if no reason is given "normal" release should be assumed.

Upon receipt of the {CC-RELEASE} message, the accepting side shall issue a MNCC_RELEASE-ind primitive to the IWU. Acceptance of the release by the IWU is indicated by a MNCC_RELEASE-res primitive. Upon receipt of this response, the CC shall send a {CC-RELEASE-COM} message. It shall then release all resources associated with the call and enter the "NULL" state.

Upon receipt of the {CC-RELEASE-COM} reply the initiating side shall issue a MNCC_RELEASE-cfm primitive indicating normal acknowledged release (cause = peer message). It shall then release all resources, stop timer <CC.02>, and enter the "NULL" state.

If timer <CC.02> expires before the receipt of a {CC-RELEASE-COM} message, the initiating side should immediately send a {CC-RELEASE-COM} message. It should then issue a MNCC_RELEASE-cfm primitive indicating an unacknowledged release (cause = local timer expiry) and should release all resources and enter the "NULL" state.

Prior to issuing the MNCC_RELEASE-res primitive, the responding side may submit a small number of MNCC_INFO-req primitives (thereby invoking {CC-INFO} messages). If a {CC-INFO} message is received by the initiating entity while in the "RELEASE PENDING" state it shall be indicated with a MNCC_INFO-ind primitive.

On receipt of MNCC_INFO-req primitive, when in F-19 state, the FT shall issue a {CC-INFO} message (e.g. thereby acknowledging supplementary services requested beforehand by the PT).

NOTE 2: The {DISCONNECT} message used by ETS 300 102-1 [10] has not been introduced. However, the normal call procedure provides a similar function by allowing limited information transfer to the release initiating entity.

Both sides shall report the completion of the release of the call to their respective LCEs. This report shall be given immediately after sending the last message, the LCE shall issue the final message to the DLC before releasing the lower layer resources.

NOTE 3: If a "partial" release has been indicated in the <<RELEASE-REASON>> information element (implying that a follow-on call is expected) the CC should request a delayed release from the LCE. In this event the link should be retained for a few seconds as described in subclause 14.2.7.

9.5.2 Abnormal call release

Abnormal release is indicated by the unexpected receipt of a {CC-RELEASE-COM} message (i.e. without a prior transmission of a {CC-RELEASE} message). This may occur in any state (except for the "NULL" or "RELEASE PENDING" states). At the FT side, an abnormal release can also be invoked by the receipt of an MNCC_REJECT-req primitive in the "RELEASE PENDING" state.

NOTE: The IWU should issue this primitive only in exceptional cases, eg when a RELEASE message is received from the Local network after a normal MNCC_RELEASE-req primitive has been issued.

Upon receipt of the unexpected {CC-RELEASE-COM} message the CC entity shall issue a MNCC_REJECT-ind primitive to indicate abnormal release (cause = peer message). It shall then release all resources, stop all timers, and enter the "NULL" state.

Upon receipt of the MNCC_REJECT-req primitive, the CC entity shall stop timer <CC.02>, send a {CC-RELEASE-COM} message, release all resources and enter the "NULL" state.

Both sides shall report the completion of the release of the call to their respective LCEs. This report shall be given immediately after sending the last message, the LCE shall issue the final message to the DLC before releasing the lower layer resources.

9.5.3 Release collisions

A release collision occurs when both sides of a call issue a {CC-RELEASE} message at the same time, such that at least one of these messages is received by a CC entity that is already in the "RELEASE PENDING" state.

If either CC entity receives a {CC-RELEASE} message, while in the "RELEASE PENDING" state, the normal release procedure is not followed by that CC entity. In this event, the CC entity shall stop timer <CC.02> and shall issue a MNCC_RELEASE-cfm primitive indicating normal acknowledged release (cause = peer message). It shall report this release to the LCE, and enter the "NULL" state.

9.6 Service change procedures

9.6.1 General

When in the "ACTIVE" state, service change procedures may be used to modify some of the existing service characteristics. This may include modification of the existing MAC connection(s) and/or the association of the call to a new MAC connection.

A service change may be indicated by the receipt of a MNCC_INFO-req primitive. Upon receipt of this primitive, the initiating CC entity sends a {CC-SERVICE-CHANGE} message to request the change. This message shall contain a complete description of the new (requested) service using the <<SERVICE-CHANGE-INFO>>.

NOTE 1: The <<SERVICE-CHANGE-INFO>> provides codings for a set of standard service changes. Complex service changes (in particular, a switch between 2 different service mappings) may be achieved using a combination of the suspend and resume.

Upon receipt of the {CC-SERVICE-CHANGE} message, the receiving entity shall attempt to meet the revised proposal. If the change is possible, the receiving entity shall immediately return a {CC-SERVICE-ACCEPT}. If the change is not acceptable, the receiving entity shall respond with a {CC-SERVICE-REJECT} message.

The {CC-SERVICE-CHANGE} message may specify the master side for activation of the proposed change at the MAC layer. This shall only apply if the change may be initiated from either side, in some cases the choice of master is implicit in the change.

NOTE 2: Service changes that involve modification of an asymmetric MAC connection can only be initiated from one side. In these cases the master side is defined in ETS 300 175-3 [3].

If the master is indicated as "receiving side", the receiving entity shall immediately activate the MAC layer changes after sending the {CC-SERVICE-ACCEPT} message. If the master is indicated as "sending side", the initiating entity shall activate the change immediately after receiving the {CC-SERVICE-ACCEPT} message.

All other changes shall be independently invoked immediately after sending or receiving the {CC-SERVICE-ACCEPT} message. Following completion of all changes, the initiating entity shall issue a MNCC_INFO-cfm primitive indicating success and the receiving entity shall issue a MNCC_INFO-ind primitive.

Service change rejection, as indicated by the sending and receipt of a {CC-SERVICE-REJECT} message, shall cause no immediate action at either side. The initiating entity shall issue a MNCC_INFO-cfm primitive indicating failure.

9.6.2 Bandwidth changes (including reversals)

The following procedures shall only be used for advanced connections.

Bandwidth changes shall be defined as changes that may be realised by modification of the existing MAC connection or connections. The <<CONNECTION-ATTRIBUTES>> element (or a list of elements) shall always be included to define the new connection bandwidths.

Bandwidth changes may be combined with establishment of new connections and/or rerouting of links by also including the <<CONNECTION-IDENTITY>> element to define the new associations. See also subclause 9.6.3.

The special case of connection reversal shall be identified using the reserved coding. Both the <<CONNECTION-ATTRIBUTES>> element and the <<CONNECTION-IDENTITY>> elements may be included to specify the new connection bandwidths and/or associations. If these elements are omitted, the reversal shall be understood to apply to all relevant connections.

9.6.3 Service rerouting

The following procedures shall only be used for advanced connections.

A {CC-SERVICE-CHANGE} message may alternatively request a rerouting of the DLC U-plane elements. This should only be used for packet services. The <<CONNECTION-IDENTITY>> element shall always be included to indicate the proposed connections.

The old (dis-associated) MAC connection may be released or may be maintained following an agreed rerouting. This decision shall be indicated in the <<SERVICE-CHANGE-INFO>> element. A maintained connection shall be immediately available for reuse, following completion of the service change procedure.

This procedure may be combined with a bandwidth change as described in subclause 9.6.2.

9.6.4 Service suspension and resumption

The following procedures shall only be used for advanced connections.

A {CC-SERVICE-CHANGE} message may alternatively request a suspension or resumption of the DLC U-plane elements. This should only be used for packet services.

The <<CONNECTION-IDENTITY>> element may be omitted for a suspend request, in which case the suspend shall be understood to apply to all relevant U-plane elements.

The <<CONNECTION-IDENTITY>> element shall always be included in a resume request to indicate the proposed connections. The resume request may also include <<CONNECTION-ATTRIBUTES>> elements to request establishment of new connections or modification of existing connections according to the set-up procedures defined in subclause 9.3.1.3. (PT initiated) or subclause 9.3.2.3. (FT initiated). If new connections and/or associations are required as part of the resume, these shall be confirmed in the {CC-SERVICE-ACCEPT} message using the <<CONNECTION-IDENTITY>> element as defined in subclause 9.3.1.3 or 9.3.2.3.

The associated MAC connection may be released or may be maintained following an agreed suspension. This decision shall be indicated in the <<SERVICE-CHANGE-INFO>> element. A maintained connection shall be immediately available for reuse, following completion of the service change procedure.

9.7 Packet mode procedures

9.7.1 General

The following procedures shall only be used for advanced connections.

This subclause describes the use of the CC procedures to offer a packet mode service.

The CC service may be accessed in one of two modes:

a) permanent access;

b) demand assigned access.

For permanent access, the resources of all layers remain allocated. For demand assigned access the lower layer resources (MAC and physical layers) may be released during periods of inactivity using the suspend and resume procedures.

9.7.2 PT initiated access

For outgoing data calls, the user shall decide whether a circuit switched or packet switched service is required. If circuit switched access is required (case A) the normal procedures defined in subclause 9.3. shall apply. The <<IWU-ATTRIBUTES>> information element shall be set appropriately.

If packet switched access is required (case B) the procedures defined in this subclause shall apply.

NOTE: The service requested may not be available. The FT will clear a request for unsupported services by sending a {CC-RELEASE-COM} message, with the reason set to "service not implemented".

Packet switched PT initiated access shall use the standard CC procedures with the following exceptions:

a) the procedures for overlap sending shall not apply;

b) the procedures for call proceeding shall not apply;

c) the procedures for call confirmation apply as follows:

- upon accepting the service requested in the {CC-SETUP} message, the FT shall return a {CC-CONNECT} message to the PT and shall enter the "ACTIVE" state;

- the {CC-CONNECT} message shall confirm installation of the requested U-plane entity;

- upon receipt of the {CC-CONNECT} message the PT shall enter the "ACTIVE" state and shall issue a MNCC_CONNECT-ind primitive.

9.7.3 FT initiated access

For incoming data calls, the IWU shall decide whether a circuit switched or packet switched service is required. If circuit switched access is required (case A) the normal procedures defined in subclause 9.3 shall apply. The <<IWU-ATTRIBUTES>> information element shall be set appropriately.

If packet switched access is required (case B) the procedures defined in this subclause shall apply.

NOTE: The requested service may not be available. The PT will clear a request for unsupported services by sending a {CC-RELEASE-COM} message, with the reason set to "service not implemented".

Packet switched FT initiated access shall use the standard CC procedures with the following exceptions:

a) the procedures for overlap receiving shall not apply;

b) the procedures for call alerting may apply, but the receipt of a {CC-ALERTING} message shall not cause the FT to issue a MNCC_ALERT-ind primitive.

9.7.4 Packet mode suspend and resume

9.7.4.1 General

A packet mode call may optionally be suspended. The suspend procedure allows the service attributes to be reserved such that the call can be resumed more rapidly.

The suspend and resume shall use two independent procedures:

- C-plane suspend and resume, under control of the LCE;

- U-plane suspend and resume, under control of the LLME.

These procedures may be invoked independently, once the relevant call is in the "ACTIVE" state.

9.7.4.2 C-plane suspend and resume

The CC entity may request the LCE to suspend a C-plane link at any time after reaching the "ACTIVE" state. No further messages should be submitted for that link as these will invoke an immediate resumption of the link.

NOTE: The DLC suspend and resume procedures are managed by the LCE. In the case of Class A operation, all resources associated with the link are released (i.e. suspension is equivalent to release). In the case of Class B operation, all MAC and physical layer resources are released, but the DLC C-plane resources are preserved. This allows for the link to be restarted with Class B operation.

9.7.4.3 U-plane suspend and resume

U-plane suspend and resume shall use the service change procedures as described in subclause 9.6. Any U-plane DLC instance may be suspended, provided that all NWK layer resources (in particular the CC transaction identifier) are preserved. A suspension shall always suspend all of the U-plane resources associated with the indicated CC instance (all resources related to the indicated TI).

Following acceptance of a service change indicating suspension of a service, all of the relevant U-plane resources shall be immediately suspended, all resources shall be preserved and all timers shall be stopped. Any associations to MAC connections shall then be removed.

Following acceptance of a service change indicating resumption of a service, the relevant U-plane resources shall be reassociated to a suitable open MAC connection. The U-plane operations shall then be resumed and all timers shall be restarted (and reset).

NOTE: The state variables of the U-plane link may be reset as part of link resumption.

10 Supplementary Services procedures

10.1 General

This clause describes the generic procedures for the control of all supplementary services at the user-network interface. The procedures may be used for the invocation and operation of supplementary services as part of either the CC or CISS protocol entities:

a) Call Related Supplementary Services (CRSS); that operate in association with an existing CC call(s), but do not influence the states at either side of the call;

b) Call Independent Supplementary Services (CISS); that operate outside of any CC calls.

Three generic protocols are defined for supplementary services:

	GENERIC NAME	PROTOCOL TYPE
1)	Keypad	Stimulus
2)	Feature key management	Stimulus
3)	Functional	Functional

10.2 Keypad protocol

The keypad protocol is based on the use of the following information elements:

- <<SINGLE-KEYPAD>> or <<MULTI-KEYPAD>> } <<"KEYPAD">>

- <<SINGLE-DISPLAY>> or <<MULTI-DISPLAY>> } <<"DISPLAY">>

The CRSS and CISS uses the generic keypad protocol as follows:

- the PT sends a <<"KEYPAD">> information element to invoke a service. This element contains network dependent access codes;

- the FT sends a <<"DISPLAY">> information element that gives an indication to the PT user about the service.

These elementary steps may be repeated several times, with the FT <<"DISPLAY">> element providing a prompt for the PT user. The semantics of this dialogue are not specified.

The CRSS keypad protocol can be invoked at any phase of the associated CC call. During the establishment phase, a <<"KEYPAD">> element may only be included in the {CC-SETUP} message or a {CC-INFO} message. Subsequent elements shall always be sent in a {CC-INFO} message. A <<"DISPLAY">> element may be included in any CC message in the F=>P direction except {CC-NOTIFY} and {IWU-INFO}.

The CISS keypad protocol can be used in any of the CISS messages.

If the FT is unable to support the requested supplementary service it shall ignore the request and no further action is required. It may optionally inform the user of this rejection with one or more display messages.

This protocol does not specify the keypad codes used for the invocation of these services. These codes shall be agreed in advance, and may either adopt a common set of access codes (specified elsewhere) or may be network dependent.

10.3 Feature key management protocol

The feature key management protocol is based on the use of the following information elements:

- <<FEATURE-ACTIVATE>>

- <<FEATURE-INDICATE>>

These elements may be included in various CC messages or CISS messages, as defined in clause 6 of this ETS.

The generic feature key management protocol is used as follows:

- the PT sends a <<FEATURE-ACTIVATE>> information element to invoke a service. This element contains a feature identifier number which the network then maps onto the corresponding service as indicated by that users service profile;

- the FT responds to the activation with a <<FEATURE-INDICATE>> information element. This element contains either a feature identifier number (that correlates to the original activation) or a status indicator that reports the status of the requested service.

The feature key management protocol can be used for both call related and call independent supplementary services.

For call related supplementary services the feature protocol can be invoked by sending a <<FEATURE-ACTIVATE>> element in the {CC-SETUP} message (only during the establishment phase of the call) or a {CC-INFO} message.

For call independent supplementary services the feature protocol is invoked by sending a <<FEATURE-ACTIVATE>> element in a CISS message.

10.4 Functional protocol

Two categories of procedures are defined for the functional signalling for supplementary services. The first category, called the separate message approach, utilises the hold and retrieve set of messages. The second category, called the common information element approach, utilises the <<FACILITY>> information element and applies only to supplementary services that do not require synchronisation of resources between the user and the network.

10.4.1 Separate messages approach

The messages defined in this subclause are specified as separate functional messages for invoking specific functions which require changes of the resources. The following messages are defined:

- {HOLD};
- {HOLD-ACK};
- {HOLD-REJECT};
- {RETRIEVE};
- {RETRIEVE-ACK};
- {RETRIEVE-REJECT}.

10.4.1.1 Hold procedures

The hold function should be invoked in association with an existing call. The invocation of the hold function does not affect the existing CC state but does affect the auxiliary state.

A call hold is requested on receipt of a MNCC_HOLD-req primitive by sending the {HOLD} message. It will place the auxiliary state in the "HOLD REQUEST" state. The responding entity will send a MNCC_HOLD-ind primitive to the IWU and on receipt of a MNCC_HOLD-res primitive without "reject reason" meaning that the operation was successful shall acknowledge the request with a {HOLD-ACK} message. This will result in the auxiliary state being put in the "CALL HELD" state. If the IWU answers with MNCC_HOLD-res primitive including "Reject reason" because the requested hold function cannot be obtained, then a {HOLD-REJECT} message will be returned. This will result in the auxiliary state returning to the "IDLE" state.

The receipt of either {HOLD-ACK} or {HOLD-REJECT} message shall be acknowledged to the IWU by a MNCC_HOLD-cfm primitive indicating the success/failure of the operation.

10.4.1.2 Retrieve procedures

The retrieve function is requested on receipt of a MNCC_RETRIEVE-req primitive by sending a {RETRIEVE} message. This message may be sent while the auxiliary state is in the "CALL-HELD" state. Upon the sending the auxiliary state would go to the "RETRIEVE REQUEST" state.

On receipt of a {RETRIEVE} message the peer entity shall issue a MNCC_RETRIEVE-ind primitive to the IWU.

If a MNCC_RETRIEVE-res primitive without "Reject reason" is received meaning the "RETRIEVE-REQUEST" is successful, the {RETRIEVE-ACK} message will be returned to the peer. The auxiliary state would then return to the "IDLE" state.

If a MNCC_RETRIEVE-res primitive including "Reject reason" is received meaning the "RETRIEVE REQUEST" is not successful, the {RETRIEVE-REJECT} message will be returned. The auxiliary state would then remain in the "CALL HELD" state.

The receipt of either {RETRIEVE-ACK} or {RETRIEVE-REJECT} message shall be acknowledged to the IWU by a MNCC_RETRIEVE-cfm primitive indicating the success/failure of the operation.

10.4.1.3 Auxiliary states for hold and retrieve

There are four auxiliary states associated with the hold and retrieve functions:

1) IDLE;
2) HOLD REQUEST;
3) CALL HELD;
4) RETRIEVE REQUEST.

10.4.2 Common information element approach

The common information element approach is based on the use of the information element:

- <<FACILITY>>.

10.4.2.1 Call related procedures

The CRSS uses the generic functional protocol as follows:

- either side (PT or FT) sends a <<FACILITY>> information element to invoke a service;

- the responding side replies by returning the same <<FACILITY>> element. This reply can either accept or reject the service.

If appropriate, either side can respond to a rejection of the service by releasing the CC call, using the procedures defined in clause 9.

The facility protocol can be invoked at any phase of the associated CC call. During the establishment phase, a <<FACILITY>> element in the P=>F direction may only be included in the {CC-SETUP}, {CC-INFO}, {CC-ALERTING}, {CC-RELEASE} or {CC-RELEASE-COM} message. A <<FACILITY>> element in the F=>P direction may be included in any CC message. A {FACILITY} message may be exchanged at any phase in the associated CC call.

10.4.2.2 Call independent procedures

The functional protocol is invoked by either side on receipt of a MNSS_SETUP-req primitive, by sending a {CISS-REGISTER} message which may contain a <<FACILITY>> information element. This first message is submitted to the LCE, and the LCE is responsible for providing a duplex link to the desired PT or FT, using the procedures defined in clause 14. The CISS transaction identifier for this CISS instance is defined by this first message.

The receipt of the {CISS-REGISTER} message at the peer side shall be acknowledged to the IWU with a MNSS_SETUP-ind primitive.

All subsequent exchanges shall use the {FACILITY} message containing a single <<FACILITY>> information element. A {FACILITY} message shall be sent on receipt of a MNSS_FACILITY-req primitive and shall be acknowledged to the peer IWU by a MNSS_FACILITY-ind primitive.

Each instance of the CISS is released on receipt of a MNSS_RELEASE-req primitive using a single unacknowledged {CISS-RELEASE-COM} message. At the receiving side on receipt of a {CISS-RELEASE-COM} message a MNSS_RELEASE-ind primitive is issued.

10.4.2.3. Connectionless Supplementary Service (CLSS) procedure

Normal operation

If a point-to-point DECT link is known to exist or can be established, a connectionless transport mechanism can be used using a reliable data link connection.

The connectionless transport mechanism is based on {FACILITY} messages. The CLSS procedure shall only use the dummy TI value 6 indicating "connectionless".

Before data can be sent the originating entity shall first establish, if not already available, a reliable data link connection between the user and the network using the DL_ESTABLISH-req service primitive as described in ETS 300 175-4 [4]. Completion of establishment of this connection is indicated by a DL_ESTABLISH-cfm primitive.

The {FACILITY} message is used to carry the "user" information, i.e. the component structures in the <<FACILITY>> information element. Structure and principals of coding and the procedures upon the components are described in ETS 300 196-1 [18] subclauses 8.1 and 8.2. Service specific coding is defined in the respective subclauses of the ISDN stage 3 standards for the supplementary services.

Exceptional procedures

If a <<FACILITY>> information element is received with an invalid protocol profile, the receiving entity shall discard the {FACILITY} message.

If a {FACILITY} message is received and it does not contain the <<FACILITY>> information element, the receiving entity shall disregard the {FACILITY} message.

When a message other than {FACILITY} is received using the connectionless TI, the receiving entity shall disregard the message.

If either protocol entity receives an indication that the data link has been released or that the data link has spontaneously been reset, then the procedures as they affect the higher layer protocol are outside the scope of this ETS.

NOTE: The handling of layer 2 errors is supplementary service dependent and shall therefore be specified in the individual supplementary services.

10.5 Co-existence of multiple protocols

Networks may support one or more of the three generic protocols. These protocols may allow alternative methods of invoking similar supplementary services.

In general, the keypad and feature key management protocols have only local network significance, while the functional protocol may have wider significance.

NOTE: The functional protocol is the preferred method of invoking a given service, if there is a choice of methods available.

10.6 Application protocols

10.6.1 DECT standard functional supplementary services

For the functional protocol the use of the application protocol defined for ISDN is recommended. The following SS are defined (see ETS 300 196-1 [18]):

- Malicious Call Identification (MCID), see ETS 300 130-1 [30];
- Call Forwarding Busy (CFB), see ETS 300 207-1 [31];
- Call Forwarding Unconditional (CFU), see ETS 300 207-1 [31];
- User to User Signalling (UUS), see ETS 300 286-1 [32];
- Calling Line Identification Presentation (CLIP), see ETS 300 092-1 [33];
- Calling Line Identification Restriction (CLIR), see ETS 300 093-1 [34];
- COnnected Line identification Presentation (COLP), see ETS 300 097-1 [35];
- COnnected Line identification Restriction (COLR), see ETS 300 098-1 [36];
- Completion of Calls to Busy Subscriber (CCBS), see ETS 300 359-1 [37];
- FreePHone (FPH), see ETS 300 210-1 [38];
- Advice Of Charge (AOC), see ETS 300 182-1 [39];
- SUBaddressing (SUB), see ETS 300 061-1 [40];
- Terminal Portability (TP), see ETS 300 055-1 [41];
- Call Waiting (CW), see ETS 300 058-1 [42];
- Direct Dialling In (DDI), see ETS 300 064-1 [43];
- Multiple Subscriber Number (MSN), see ETS 300 052-1 [44];
- Closed User Group (CUG), see ETS 300 138-1 [45];
- Explicit Call Transfer (ECT), see ETS 300 369-1 [46];
- Call Forwarding No Reply (CFNR), see ETS 300 207-1 [31];
- Call Deflection (CD), see ETS 300 207-1 [31];

- CONFerence call add-on (CONF), see ETS 300 185-1 [47];

- Call Hold (CH), see ETS 300 141-1 [48];

- Three ParTY (3PTY), see ETS 300 188-1 [49].

NOTE: For the keypad protocol no specific application protocol is identified.

10.6.2 DECT specific supplementary services

For DECT specific supplementary services the feature key management protocol is used.

The following supplementary services are defined:

- queue management;

- indication of subscriber number;

- control of echo control functions;

- cost information.

10.6.2.1 Queue management

This service can be used to register a PP in a queue for outgoing calls, e.g. in the case of a network congestion.

If an outgoing call is requested by a PT by sending a {CC-SETUP} message and no external line is available, then the FT can respond with an allowed CC-message, which can include <<"DISPLAY">> information and/or a <<PROGRESS-INDICATOR>> information element indicating cause no. 8 ("in-band information or appropriate pattern now available") to request the PT to connect the U-plane. Upon receipt of this element, the PT should request its LLME to connect the receive U-plane, so that the user can receive verbal information.

In response to the displayed and/or verbal information about the outgoing call queue, the user can request to enter the queue or release the call.

To enter the queue the PT shall send a <<FEATURE-ACTIVATE>> information element containing a "queue entry request" e.g. in a {CC-INFO} message.

Upon receipt of the "queue entry request" the FT shall respond with a <<FEATURE-INDICATE>> information element e.g. in a {CC-INFO} message to tell if the service request has been accepted and to indicate the position in the queue.

NOTE: The FT might have to send a <<TIMER-RESTART>> with a {CC-NOTIFY} message to avoid that the CC completion timer <CC.04> in the PT expires.

If the queue position changes, then the FT shall send a new <<FEATURE-INDICATE>> information element containing the updated information about the position in the outgoing call queue. The FT can also send display and/or voice information.

The FT may send a <<PROGRESS-INDICATOR>> information element indicating cause No. 9 ("in-band information not available") to inform the PT that the verbal information has concluded. Upon receipt of this element, the PT may disable the received audio (in particular, the speech codec and audio circuits may be disabled) but the U-plane shall remain connected.

The PT may exit the queue at any time by releasing the call.

As soon as the external line is free the FT proceeds with the normal call set up procedure, by giving a dial tone or by sending a {CC-CALL-PROC} message or a {CC-ALERTING} message or a {CC-CONNECT} message, depending on the status of the call.

10.6.2.2 Indication of subscriber number

The subscriber number shall be requested by sending a <<FEATURE-ACTIVATE>> information element with the feature coding "indication of subscriber number".

Upon receipt of the <<FEATURE-ACTIVATE>> information element the FT shall respond with a <<FEATURE-INDICATE>> information element indicating if the service is accepted or rejected. If the service is accepted and activated, then the subscriber number shall be sent in a <<FEATURE-INDICATE>> information element.

10.6.2.3 Control of echo control functions

This service is used to connect or disconnect fixed part echo control functions, depending on e.g. the type of service and call routing information. See also ETS 300 175-8 [7]. This service provides messages to control four FP echo control functions:

Requirement 1 and requirement 2:
(subclause 7.10 of ETS 300 175-8 [7]).

Option a) and option b):
(subclause 7.4.1.2 of ETS 300 175-8 [7]).

Requirement 1 is primarily designed to control the echo from the DECT hybrid in the case of a 2-wire connection.

Requirement 2 is primarily designed to control the echo from the far end hybrids.

Option a) is primarily designed to ensure that echo cancellers at the international switching centre are activated.

Option b) is designed for use with specific local networks (in particular connection to the GSM mobile or fixed network) to ensure that the effective TCL from the DECT network is always in excess of 46 dB.

The exact echo control function(s) to be used depend upon the type of interface and the type of local network to which DECT is connected. These echo control functions should be disconnected when not needed to optimise the speech quality. The connect/disconnect decision (for each function) depends upon the installation and/or routing information (on a per call basis).

Where possible, all echo control function should be fully controlled by the fixed part and in many cases may be preset at installation. For particular cases (e.g. disconnection of requirement 2 for internal PBX calls) this service allows the PP to over-ride the FP control.

NOTE: All possible PP control options are provided to allow for future developments, but most of these should not be required.

Control of echo functions on a per call basis is expected to use the call routing information. This can be provided by number analysis in the PP or FP. When number analysis is provided in the PP, the messages in subclause 7.7.16 may be used to transfer this information to the FP.

10.6.2.4 Cost information

This service can be used to obtain cost information such as tariffing, charging or charging pulses. It can furnish either DECT specific cost information or cost information for the complete connection including the DECT link.

The cost information shall be requested by sending a <<FEATURE-ACTIVATE>> information element with the feature coding "cost information".

The parameter in the <<FEATURE-ACTIVATE>> information element is used to request either DECT internal cost information or cost information for the complete connection and to choose between tariff information, charging pulses during the call or a calculated amount at the end of the call.

Upon receipt of the <<FEATURE-ACTIVATE>> information element the FT shall respond with a <<FEATURE-INDICATE>> information element indicating if the service is accepted or rejected. If the service is accepted and activated, then the cost information shall be sent in one or more <<FEATURE-INDICATE>> information elements containing charging components.

The support of this feature does not compel any specific tariffing principle.

11 Connection Oriented Message Service (COMS)

11.1 General

The connection oriented message service procedures only deal with packet switched connections. The COMS represents a group of procedures covering all aspects of packet mode call establishment, packet data transfer and release.

The protocol allows for multiple instances of a COMS call at both the fixed termination and at the portable termination. These multiple instances are assumed to operate completely independently from each other. The possible existence of multiple instances is therefore ignored in the following clauses, which only describe the procedures for a single instance.

A reliable C-plane DLC link (LAPC) shall be available before any of these COMS procedures can operate. The establishment and maintenance of this link is the responsibility of the LCE and is described in clause 14.

NOTE: A "LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. If a COMS timer expires whilst in this state, the resulting release should be handled locally.

11.2 COMS states

11.2.1 States at PT

11.2.1.1 State TS-0: "NULL"

No call exists.

11.2.1.2 State TS-1: "CONNECT PENDING"

The PT has sent a set-up message to the FT, but has not received a response.

11.2.1.3 State TS-2: "RELEASE PENDING"

The PT has sent a release message to the FT, but has not received a response.

11.2.1.4 State TS-3: "ACTIVE"

a) The PT has answered an incoming call;

b) the PT has received an indication that the FT has connected a PT outgoing call.

11.2.2 States at FT

11.2.2.1 State FS-0: “NULL”

No call exists.

11.2.2.2 State FS-1: "CONNECT PENDING"

The FT has sent a set-up message to the PT, but has not received a response.

11.2.2.3 State FS-2: "RELEASE PENDING"

The FT has sent a release message to the PT, but has not received a response.

11.2.2.4 State FS-3: "ACTIVE"

a) The FT has allocated an incoming call to one PT;

b) the FT has sent a message to the PT reporting connection of an outgoing call.

11.3 COMS establishment procedures

11.3.1 PT initiated COMS establishment

11.3.1.1 COMS request

PT initiated COMS establishment is started upon receipt of a MNCO_SETUP-req primitive from the interworking unit at the PT side.

The COMS entity (P-COMS) initiates COMS establishment by sending a {COMS-SETUP} message to its peer entity (F-COMS). This message is submitted to the LCE in the PT, and the P-COMS enters the "CONNECT PENDING" state and starts timer P<COMS.03>.

The {COMS-SETUP} message shall carry all details of the interworking attributes such that all the necessary resources can be reserved and installed by the F-COMS and the F-IWU.

Call accept

The F-COMS entity shall examine the attributes defined in the {COMS-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCO_SETUP-ind primitive to the F-IWU. The F-IWU is expected to reply with a MNCO_CONNECT-req primitive, if the call is acceptable.

NOTE: Either the F-COMS or a F-IWU may reject the COMS call. The F-COMS examines the <<CONNECTION-ATTRIBUTES>> element and the F-IWU examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the F-IWU after it has been accepted by the F-COMS.

Call reject

If the F-COMS cannot meet any of the set-up requests, or if the {COMS-SETUP} message contains errors or inconsistencies, or if the F-IWU replies with a MNCO-REJECT-req primitive, the FT shall reject the request by sending a {COMS-RELEASE-COM} message.

Set-up release

If timer P<COMS.03> expires before a suitable response is received, the P-COMS shall immediately release the call by sending a {COMS-RELEASE-COM} message, with the reason set to "timer expiry". It shall then issue a MNCO_RELEASE-ind primitive and shall enter the "NULL" state.

11.3.1.2 COMS connection

Upon receiving a MNCO_CONNECT-req primitive, the F-COMS shall complete the C-plane connection and shall send a {COMS-CONNECT} message to the P-COMS. It shall then enter the "ACTIVE" state.

On receipt of this message the P-COMS shall complete the C-plane connection. The P-COMS shall then stop timer P<COMS.03> and enter the "ACTIVE" state. It shall then issue a MNCO_CONNECT-ind primitive to the P-IWU.

11.3.2 FT initiated COMS establishment

11.3.2.1 COMS request

FT initiated COMS establishment is started upon receipt of a MNCO_SETUP-req primitive from the interworking unit at the FT side.

The COMS entity (F-COMS) initiates COMS establishment by sending a {COMS-SETUP} message to its peer entity (P-COMS). This message is submitted to the LCE in the FT, and the F-COMS enters the "CONNECT PENDING" state, and starts timer F<COMS.03>.

The {COMS-SETUP} message should carry all details of the interworking attributes such that all the necessary resources can be reserved and installed by the PT.

Call accept

The P-COMS entity shall examine the attributes defined in the {COMS-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCO_SETUP-ind primitive. A MNCO_CONNECT-req primitive will then be received in reply if the call is acceptable.

NOTE: Either the P-COMS or the PP higher layer application may reject the COMS call. The P-COMS examines the <<CONNECTION-ATTRIBUTES>> element and the PP higher layer application examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the PP higher layer application after it has been accepted by the P-COMS.

Call reject

If the P-COMS cannot meet any of the set-up requests, or if the {COMS-SETUP} message contains errors or inconsistencies, or if a MNCO-REJECT-req primitive is received, the P-COMS shall reject the request by sending a {COMS-RELEASE-COM} message.

Set-up release

If timer F<COMS.03> expires before a suitable response is received, the F-COMS shall immediately release the call by sending a {COMS-RELEASE-COM} message, with the reason set to "timer expiry". It shall then issue a MNCO_RELEASE-ind primitive to the F-IWU and shall enter the "NULL" state.

11.3.2.2 COMS connection

Upon receiving a MNCO_CONNECT-req primitive, the P-COMS shall complete the C-plane connection and shall send a {COMS-CONNECT} message to the P-COMS. It shall then enter the "ACTIVE" state.

On receipt of this message the F-COMS shall complete the C-plane connection. The F-COMS shall then stop timer F<COMS.03> and enter the "ACTIVE" state and shall issue a MNCO_CONNECT-ind primitive to the F-IWU.

11.4 COMS data transfer procedures

11.4.1 Procedure at the sending side

This service shall only support octet structured data, using any of the defined information elements. Unstructured data shall not be supported.

Upon receipt of a MNCO_INFO-req primitive the COMS shall attempt to map the parameters into one or more of the {COMS-INFO} message elements. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

If the resulting message exceeds the following limits the service data shall be segmented into two or more messages, and these messages shall be transmitted independently.

The following message limits should be used:

DOWNLINK: 58 octets;
UPLINK: 58 octets for full slot operation.

NOTE: These lower limits are chosen because the maximum information length of a LAPC UI frame, see ETS 300 174 - 4 [4] is 63 octets.

If the service data is segmented, each message shall contain the <<SEGMENTED-INFO>> information element, together with a duplicate of all of the mandatory elements. Each message should contain the maximum amount of service data (of user information).

The COMS shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery via the connection oriented S-SAP (SAPI="0"). The messages shall be delivered using DL_UNITDATA-req primitives, indicating the use of a Class U (unacknowledged) link.

After sending a complete message (of one or more segments) the COMS shall start timer <COMS.01> and shall wait for the final acknowledgement to be received from the peer COMS entity. No further messages shall be submitted until this acknowledgement is received. Upon receipt of this acknowledge, the COMS shall issue a MNCO_ACK-ind primitive to the IWU to indicate successful delivery.

If timer <COMS.01> expires the COMS shall resubmit the complete message starting from the first segment. Timer <COMS.01> shall be restarted after transmission of the complete message. If timer <COMS.01> expires a second time the service shall be released using the procedures defined in subclause 11.6.

11.4.2 Procedure at the receiving side

Upon receipt of a {COMS-INFO} message, the COMS shall check the contained address. If the address does not match any of the PT identities the message shall be discarded. If the address is valid, the COMS shall:

a) if the message does not contain the <<SEGMENTED-INFO>> information element it shall map the elements into the parameters of a MNCO_INFO-ind primitive. It shall immediately issue the resulting primitive via the MNCO-SAP;

b) if the message does contain the <<SEGMENTED-INFO>> element the COMS shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <COMS.00> seconds. Whenever a new segmented message is received, the COMS shall attempt to construct a complete message using all stored segmented messages that contain the same <<SHORT-ADDRESS>> and <<PROTOCOL-DISCRIMINATOR>> element coding. Any duplicate segmented messages should be discarded.

A complete message shall be identified by the receipt of all of the segments as indicated in the <<SEGMENTED-INFO>> elements. Upon detection of a complete series of segments, the COMS shall map the elements into the parameters of a MNCO_INFO-ind primitive. Duplicate mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<ALPHANUMERIC>> and/or <<IWU-PACKET>> elements shall be concatenated into a single message unit parameter. The COMS shall immediately issue the resulting primitive via the MNCO-SAP.

NOTE: The <<SEGMENTED-INFO>> element in each segmented message indicates the total number of segments belonging to the complete message, plus the number of segments remaining. The latter field should be used to sequence the segments.

Upon issuing the complete message to the IWU, the COMS shall immediately return a {COMS-ACK} message to its peer entity using the same Class U link as used for {COMS-INFO} messages.

11.5 COMS suspend and resume procedures

A COMS call may optionally be suspended. The suspend procedure allows the service attributes to be reserved such that the call can be resumed more rapidly.

The suspend and resume shall use the standard C-plane suspend and resume procedure under control of the LCE. See subclause 14.2.6.

The COMS entity may request the LCE to suspend a C-plane link at any time after reaching the "ACTIVE" state. No further messages should be submitted for that link as these will invoke an immediate resumption of the link.

NOTE: The DLC suspend and resume procedures are managed by the LCE. In the case of Class A operation, all resources associated with the link are released (i.e. suspension is equivalent to release). In the case of Class B operation, all MAC and physical layer resources are released, but the DLC C-plane resources are preserved. This allows for the link to be restarted with Class B operation.

The COMS service can be resumed by either side by submitting a new {COMS-INFO} message to the LCE. This resumption may use any suitable link.

A suspended COMS entity may be discarded without notification to the sender. Any subsequent resumption messages shall then be discarded without notification to the sender. A COMS entity may also be replaced with a new (re-established) COMS entity at any time (i.e. a COMS set-up that uses the transaction identifier of an existing entity) shall always take priority and shall over-write the existing values.

11.6 COMS release procedures

11.6.1 Normal COMS release

The COMS release procedures may be started by the COMS entity at either side at any time, upon receipt of a MNCO_RELEASE-req primitive. The starting entity sends a {COMS-RELEASE} message, starts timer <COMS.02>, and enters the "RELEASE PENDING" state. The release message may include an information element giving the reason for the release: if no reason is given "normal" release should be assumed.

Upon receipt of the {COMS-RELEASE} message, the accepting side shall immediately release all resources associated with the call. It then confirms completion of the release by sending a {COMS-RELEASE-COM} message, enters the "NULL" state, and issues a MNCO_RELEASE-ind primitive. The initiating side must wait for receipt of this {COMS-RELEASE-COM} message before it too can release all resources, stop timer <COMS.02>, and enter the "NULL" state. The initiating side shall then issue a MNCO_RELEASE-cfm primitive, indicating a normal (acknowledged) release. Both sides shall also record the release of the call in their respective LCEs.

If timer <COMS.02> expires before the receipt of a {COMS-RELEASE-COM} message, the initiating side shall release all resources, shall report the call as released to the LCE, and shall issue a MNCO_RELEASE-ind primitive indicating an abnormal time-out release.

11.6.2 Release collisions

A release collision occurs when both sides of a call issue a {COMS-RELEASE} message at the same time, such that at least one of these messages is received by a COMS entity that is already in the "RELEASE PENDING" state.

If either COMS entity receives a {COMS-RELEASE} message, while in the "RELEASE PENDING" state the normal release procedure is not followed by that COMS entity. In this event, the COMS entity immediately releases all the COMS resources, reports this release to the LCE and issues a MNCO_RELEASE-ind primitive indicating abnormal release.

12 ConnectionLess Message Service (CLMS)

12.1 General

The ConnectionLess Message Service procedures offer a connectionless packet service. The CLMS shall provide generic message formats that enable a single packet of differing types of user data to be transported. A single CLMS entity may handle messages from multiple applications.

All messages shall be handled sequentially, in the order of arrival, by a single CLMS entity. Each message shall be handled independently of all other messages. The following subclauses shall describe the procedures for the transmission and reception of one message.

There are two types of CLMS messages:

1) fixed length messages;

2) variable length messages.

Fixed length messages shall be routed via the broadcast service (B-SAP), and these messages shall conform to the fixed length operation specified for this service.

Variable length messages shall be routed via the LAPC services (S-SAP) where they may be routed via a connection oriented link (SAPI="0") or a connectionless link (SAPI="3"). In both cases unacknowledged link operation shall be used.

A connection oriented link shall only be used if a suitable link is already established. Otherwise a connectionless link should be used. The choice of link, and the establishment of these links is the responsibility of the LCE and is described in clause 14.

"LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. A link in this state shall not be used for the transport of CLMS messages.

12.2 CLMS states

No states shall be defined for the CLMS entity, the CLMS shall always be ready to transmit or receive a message.

12.3 CLMS message transmission procedures

12.3.1 Fixed length messages

Fixed length CLMS messages shall use the B-FORMAT message structure.

12.3.1.1 Procedure in the Fixed radio Termination (FT)

Upon receipt of a MNCL_UNITDATA-req primitive indicating fixed length operation, the CLMS shall attempt to map the parameters into {CLMS-FIXED} message elements, using one or more message sections as appropriate. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

The CLMS shall only insert <<FILL>> elements into the final message section in order to fill that final section.

NOTE 1: The total message length is limited by the maximum number of data sections, as defined in subclause 8.3.

NOTE 2: If the data completely fills the last data sections, no <<FILL>> element is added.

The CLMS shall then deliver all sections of the resulting message to the LCE for immediate delivery via the B-SAP. The message priority shall be set to "normal".

12.3.1.2 Procedure in the Portable radio Termination (PT)

Upon receipt of a {CLMS-FIXED} message, the CLMS shall check the contained address in the first section. If the address section is missing, or if the address does not match any of the PT identities the message shall be discarded.

If the address does match the CLMS shall map the remaining elements into the parameters of a MNCL_UNITDATA-ind primitive (removing any <<FILL>> elements). It shall immediately issue the resulting primitive via the MNCL-SAP.

12.3.2 Variable length messages

Variable length CLMS messages shall use the S-FORMAT message structure. However, the transaction value field is redundant and shall be set to "0" by the sending entity. This field should be ignored by the receiving entity. Four (4) complete CLMS message segments, equating to 176 characters shall be supported (this corrects the number of CLMS segments from three to four in ETS 300 175-9 [8] subclause 6.1.4 to allow for correct operation).

12.3.2.1 Procedure at the sending side

This service shall only support octet structured service data, using any one of the defined information elements. Unstructured data shall not be supported.

Upon receipt of a MNCL_UNITDATA-req primitive indicating variable length operation, the CLMS shall attempt to map the parameters into the {CLMS-VARIABLE} message elements. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

If the resulting message exceeds the following limits the service data shall be segmented into two or more messages, and these messages shall be transmitted independently.

The following message limits should be used:

DOWNLINK: 58 octets;
UPLINK: 58 octets for full slot operation.

NOTE: These lower limits are chosen because the maximum information length of a LAPC UI frame, see ETS 300 174 - 4 [4] is 63 octets.

If the service data is segmented, each message shall contain the <<SEGMENTED-INFO>> information element, together with a duplicate of all of the mandatory elements. Each message should contain the maximum amount of service data (of user information).

The CLMS shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery via the S-SAP.

12.3.2.2 Procedure at the receiving side

Upon receipt of a {CLMS-VARIABLE} message, the CLMS shall check the contained address. If the address does not match the message shall be discarded. If the address does match the CLMS shall:

a) if the message does not contain the <<SEGMENTED-INFO>> information element it shall map the elements into the parameters of a MNCL_UNITDATA-ind primitive. It shall immediately issue the resulting primitive via the MNCL-SAP;

b) if the message does contain the <<SEGMENTED-INFO>> element the CLMS shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <CLMS-00> seconds. Whenever a new segmented message is received, the CLMS shall attempt to construct a complete message using all stored segmented messages that contain the same <<SHORT-ADDRESS>> and <<PROTOCOL-DISCRIMINATOR> element coding. Any duplicate segmented messages may be discarded.

A complete message shall be identified by the receipt of all of the segments as indicated in the <<SEGMENTED-INFO>> elements. Upon detection of a complete series of segments, the CLMS shall map the elements into the parameters of a MNCL_UNITDATA-ind primitive. Duplicate mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<ALPHANUMERIC>>, <<IWU-TO-IWU>> or <<IWU-PACKET>> information elements shall be concatenated into a single message unit parameter. The CLMS shall immediately issue the resulting primitive via the MNCL-SAP.

NOTE: The <<SEGMENTED-INFO>> element in each segmented message indicates the total number of segments belonging to the complete message, plus the number of segments remaining. The latter field should be used to sequence the segments.

12.3.2.3 Restrictions for portable side initiated messages

CLMS messages initiated from the portable side are subject to the special transmission restrictions given in ETS 300 175-3 [3] when using connectionless MAC services. These restrictions introduce extra delays for messages in excess of two segments.

13 Mobility Management (MM) procedures

13.1 General

This clause describes the procedures used for mobility management at the radio interface.

The main function of the Mobility Management (MM) is to support the mobility of portable parts, such as informing the network of its present location and providing user identity confidentiality.

The MM procedures are described in seven groups:

- identity procedures;
- authentication procedures;
- location procedures;
- access rights procedures;
- key allocation procedure;
- parameter retrieval procedure;
- ciphering related procedure.

Each of these procedures shall be treated as a separate transaction, with a single transaction identifier used for the whole procedure. The transaction identifier is assigned by the entity that initiates the procedure (the entity that sends the first message).

Two MM procedures are allowed at any one time, but they shall not both have been initiated by the same side. This limitation is enforced by the transaction identifiers, which allow only one value to be assigned by each side.

The priorities of the MM procedures are defined in subclause 15.5 which describes the management of MM procedures.

13.2 Identity procedures

The identity procedures can be used:

- to request a PT to provide specific identification parameters to the FT;
- to assign a temporary portable user identity to a PT;
- to delete a temporary portable user identity in a PT;
- to assign a network assigned identity to a PT;
- to delete a network assigned identity in a PT.

The identity procedures are initiated by the FT and can be used any time.

13.2.1 Procedure for identification of PT

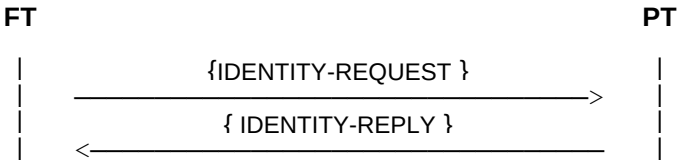
The identification procedure is used by the FT to request a PT to provide specific identification parameters to the FT e.g. the international portable user identity or the international portable equipment identity.

Upon receiving a MM_IDENTITY-req primitive the FT initiates the identification procedure by transferring an {IDENTITY-REQUEST} message to the PT and starts the timer <MM_ident.2>. The {IDENTITY-REQUEST} message specifies the type of the requested identity in the <<IDENTITY-TYPE>> information element. Optionally more than one <<IDENTITY-TYPE>> information element can be included by using the <<REPEAT-INDICATOR>> information element. Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {IDENTITY-REQUEST} message the PT issues a MM_IDENTITY-ind primitive. On receipt of a MM_IDENTITY-res primitive the PT sends back an {IDENTITY-REPLY} message which contains the identification parameters as requested by the FT. If more than one identity has been requested and not all of them can be provided, then the available ones shall be included in the {IDENTITY-REPLY} message. If none of the requested identification parameters can be provided, then the {IDENTITY-REPLY} message will contain no identification information. Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {IDENTITY-REPLY} message the FT shall stop the timer <MM_ident.2>. The FT issues a MM_IDENTITY-cfm primitive.

The identification procedure is supervised by the timer <MM_ident.2> in the FT. At the first expiry of timer <MM_ident.2> the FT should retransmit the {IDENTITY-REQUEST} message. If the timer <MM_ident.2> expires a second time the FT shall abort the procedure and release the transaction.



NOTE: An {IDENTITY-REPLY} message without any information elements has the function of an identity reject.

13.2.2 Procedure for temporary identity assignment

A temporary identity may be assigned either using the procedure for temporary identity assignment, described in this subclause or by the procedure for location registration, described in subclause 13.4.

Upon receiving a MM_IDENTITY_ASSIGN-req primitive the FT initiates the procedure by sending a {TEMPORARY-IDENTITY-ASSIGN} message to the PT. The FT starts the timer <MM_ident.1>.

The {TEMPORARY-IDENTITY-ASSIGN} message shall contain one <<PORTABLE-IDENTITY>> information element with the Temporary Portable User Identity (TPUI) and/or one <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity. When the message contains a <<PORTABLE-IDENTITY>> element, it may also contain an optional <<DURATION>> information element, which may contain a defined time limit and/or a lock limit for the newly assigned TPUI. It may also contain an optional <<IWU-TO-IWU>> information element. If the <<DURATION>> element is omitted, the default values of "infinite" time limit and "no limits" lock limit shall be assumed.

NOTE 1: The detailed coding of the <<DURATION>> element appears in subclause 7.7.13. Refer also to ETS 300 175-6 [5] for details of the application of time limits and lock limits to assigned TPUIs.

Upon receipt of a {TEMPORARY-IDENTITY-ASSIGN} message the PT issues a MM_IDENTITY_ASSIGN-ind primitive to the P-IWU.

The P-IWU replies with MM_IDENTITY_ASSIGN-res primitive indicating either "Accept" or "Reject" of the request.

On receipt of "Accept" indication PT shall send a {TEMPORARY-IDENTITY-ASSIGN-ACK} message to the FT.

On receipt of "Reject" indication PT shall send a {TEMPORARY-IDENTITY-ASSIGN-REJ} message to the FT. The {TEMPORARY-IDENTITY-ASSIGN-REJ} message can optionally contain the <<REJECT-REASON>> information element if such has been included in the "Reject" primitive.

The receipt of the {TEMPORARY-IDENTITY-ASSIGN-ACK} message should be understood by FT as following:

- PP has stored the received identities. If an individual TPUI has been assigned, then any previously assigned individual TPUI (for the relevant location area) has been replaced by the new one. If a network assigned identity has been assigned, then an earlier stored NWK assigned identity has been replaced by the new one.

- PP has erased the required identities if a <<DURATION>> information element with the value "Erase" was sent in the {TEMPORARY-IDENTITY-ASSIGN} message; (This will be the case as well if PP has no record for the identities required to be erased.)

The receipt of the {TEMPORARY-IDENTITY-ASSIGN-REJ} message should be understood by FT as following:

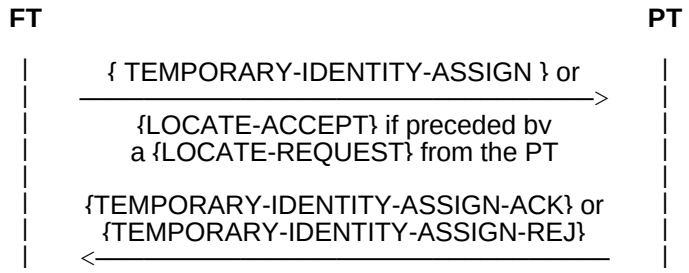
- PP has not stored the received identities as it is not capable of storing them;

- PP has not stored the received identities as it does not support the limits indicated in the <<DURATION>> element.

Upon receipt of a {TEMPORARY-IDENTITY-ASSIGN-ACK} message or a {TEMPORARY-IDENTITY-ASSIGN-REJ} message the FT shall stop the timer <MM_ident.1>. If a {TEMPORARY-IDENTITY-ASSIGN-ACK} message has been received the FT shall consider the assignment (or erasure) as successful. If a {TEMPORARY-IDENTITY-ASSIGN-REJ} message is received the FT shall consider the procedure to have failed. The FT issues a MM_IDENTITY_ASSIGN-cfm primitive indicating the outcome of the procedure.

NOTE 2: Each TPUI assignment is always associated to one specific IPUI and one specific location area.

The temporary identity assignment is supervised by the timer <MM_ident.1> in the FT. At the first expiry of timer <MM_ident.1> the FT should re transmit the {TEMPORARY-IDENTITY-ASSIGN} message. If the timer <MM_ident.1> expires a second time the FT shall abort the procedure and release the transaction. The FT then issues a MM_IDENTITY_ASSIGN-cfm primitive indicating failure of the procedure.



13.3 Authentication procedures

The authentication procedures can be used:

- to check that the identity provided by the PT is the correct identity;
- to authenticate the user;
- to check that the identity provided by the FT is the correct identity;
- to provide a new key for ciphering;
- to check the ZAP field provided by the PT;
- to send a ZAP command to the PT.

The authentication procedures are based on the use of the following information elements:

- <<AUTH-TYPE>>;
- <<RAND>>;
- <<RS>>;
- <<RES>>;
- <<ZAP-FIELD>>;
- <<REJECT-REASON>>.

13.3.1 Authentication of a PT

The authentication of a PT may be invoked by the FT in various cases e.g. when originating or terminating a call, activation or deactivation of a feature or supplementary service, location procedures or other MM procedures. Authentication can also be invoked during a call (in-call authentication).

Procedure for authenticating a PT:

Upon receiving a MM_AUTHENTICATE-req primitive the FT sends an {AUTHENTICATION-REQUEST} message which contains the <<AUTH-TYPE>> information element (defining the chosen authentication type and authentication key) and the <<RAND>> and <<RS>> information elements (two numbers necessary for calculating the response parameter). The <<RS>> information element is only mandatory, when a DECT standard authentication algorithm is used, for other algorithms it can be optional. The INC bit in the <<AUTH-TYPE>> information element can be used to ask the PT to increase its ZAP-register. The {AUTHENTICATION-REQUEST} message can also contain the optional <<CIPHER-INFO>> information element and an optional <<IWU-TO-IWU>> information element. The timer <MM_auth.1> is started.

Upon receipt of the {AUTHENTICATION-REQUEST} message PT issues a MM_AUTHENTICATE-ind primitive. The relevant ZAP field shall be incremented, if the INC bit in the <<AUTH-TYPE>> information element is set. If the value in the ZAP field was already at the maximum value of 0FH, then it shall be set to zero. Before incrementing the relevant ZAP field the IWU may issue a MM_AUTHENTICATE-req primitive thereby requesting PT to authenticate the FT - in this case the authentication of a PT with incrementing the ZAP field procedure, and authentication of a FT procedure shall be treated as nested procedures, see annex H, clause H.2. If the authentication of the FT fails, the ZAP field may not be incremented.

NOTE 1: A ZAP field is always related to one IPUI (subscription), as also an authentication key is always related to one IPUI. Therefore several ZAP fields can exist in the PT. In this procedure the relevant ZAP field is that, which is related to the same IPUI as the used authentication key.

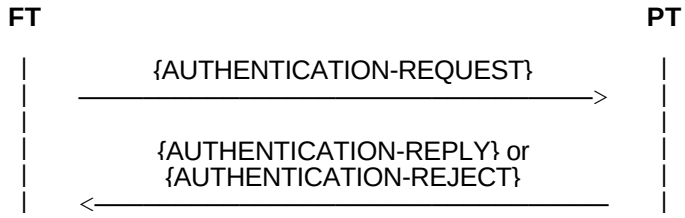
Upon receiving a MM_AUTHENTICATE-res primitive indicating "accept" the PT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result. If the PP has stored a ZAP field that is related to the current active IPUI, than also the <<ZAP-FIELD>> information element with the relevant ZAP value shall be included. If the PP has stored a "service class" that is related to the current active IPUI, then also the <<SERVICE-CLASS>> information element shall be included. If in the {AUTHENTICATION-REQUEST} message the TXC bit in the <<AUTH-TYPE>> information element was set, then the derived cipher key shall be sent using the <<KEY>> information element. An optional <<IWU-TO-IWU>> information element can also be included in the {AUTHENTICATION-REPLY} message. Upon receiving a MM_AUTHENTICATE-res primitive indicating "reject" the PT shall respond by sending an {AUTHENTICATION-REJECT} message containing the optional <<REJECT-REASON>> information element and one of a prioritised list of the optional <<AUTH-TYPE>> information element to propose an alternative algorithm or key.

The FT shall only request to send a derived cipher key (e.g. for GSM) when the DECT link is already ciphered.

Upon receipt of the {AUTHENTICATION-REPLY} message or the {AUTHENTICATION-REJECT} message the FT shall stop the timer <MM_auth.1> and issue a MM_AUTHENTICATE-cfm primitive indicating the outcome of the operation. The validity of the response shall be checked. If the FT has received an {AUTHENTICATION-REPLY} message, where the <<RES>> information element contains the correct result the PT authentication shall be considered as successful. If the FT has received an {AUTHENTICATION-REPLY} message where the <<RES>> information element contains the wrong result, then in cases where the Temporary Portable User Identity (TPUI) has been used the local network may decide to initiate the identity procedure. In any case the FT may optionally communicate the failed authentication to the PT in a subsequent NWK layer message, using a <<RELEASE-REASON>> or <<REJECT-REASON>> information element. The FT issues a MM_AUTHENTICATE-cfm primitive.

If a DECT standard authentication algorithm is used, then together with the authentication result a new ciphering key is calculated. If in this case the UPC-bit in the <<AUTH-TYPE>> information element is set, this new ciphering key shall be stored and shall be given the cipher key number as indicated in the <<AUTH-TYPE>> information element.

The procedure for authenticating a PT is supervised by the timer <MM_auth.1> in the FT. At the first expiry of timer <MM_auth.1> the FT should re transmit the {AUTHENTICATION-REQUEST} message. If the timer <MM_auth.1> expires a second time the FT shall abort the procedure and release the transaction.



13.3.2 Authentication of the user

The authentication of the user is combined with the authentication of a PT. Therefore the information elements and messages are the same as in subclause 13.3.1 above. The only difference is that in the <<AUTH-TYPE>> information element the use of a different key is indicated. In this case part of the key is added by the user via the keypad. This keypad entry is not transmitted over the air, but locally used by the PT to calculate the authentication key, K.

The procedure is equivalent to that one described in subclause 13.3.1 above. The timer that is used by the FT is called <MM_auth.2>, which has a longer period in order to enable the user to enter the User Personal Identity (UPI).

If user authentication procedure is started during an unfinished PT initiated procedure of lower priority, then the PT shall stop the timer of the unfinished lower priority procedure and start the <MM_auth.2> timer. The PT shall stop the <MM_auth.2> timer when it responds to the user authentication procedure by sending an {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message. If the <MM_auth.2> timer expires or is stopped and the lower priority procedure has not been finished in the meantime, then the timer of the interrupted lower priority procedure shall be restarted, see subclause 15.5.

13.3.3 Authentication of a FT

This authentication procedure is activated by the PT, typically when the FT is sending a ZAP-command.

Procedure for authenticating a FT:

Upon receiving a MM_AUTHENTICATE-req primitive the PT sends an {AUTHENTICATION-REQUEST} message which contains the <<AUTH-TYPE>> information element (defining the chosen authentication type) and the <<RAND>> information elements (a random number necessary for calculating the response parameter). It can also contain the optional <<CIPHER INFO>> information element and an optional <<IWU-TO-IWU>> information element. The timer <MM_auth.1> is started.

NOTE 1: The <<RES>> information element is only included when the {AUTHENTICATION-REQUEST} message is used for the key allocation procedure.

The FT, upon receiving the {AUTHENTICATION-REQUEST} message, issues an MM_AUTHENTICATE-ind primitive.

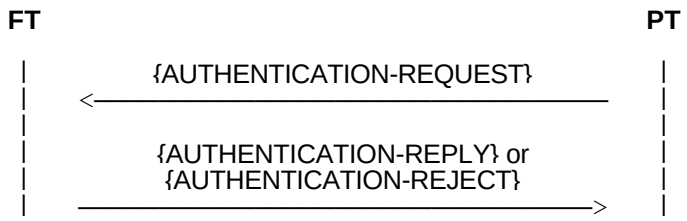
Upon receiving a MM_AUTHENTICATE-res primitive indicating "accept" the FT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result and the <<RS>> information element with a number necessary for calculating the response parameter. The <<RS>> information element is only mandatory when a DECT standard authentication algorithm is used, for other algorithms it can be optional. An optional <<IWU-TO-IWU>> information element can also be included in the {AUTHENTICATION-REPLY} message. Upon receiving a

MM_AUTHENTICATE-res primitive indicating "reject" the FT shall respond by sending an {AUTHENTICATION-REJECT} message containing one or a prioritised list of the optional <<AUTH-TYPE>> information element to propose an alternative algorithm or key and an optional <<REJECT-REASON>> information element.

Upon receipt of the {AUTHENTICATION-REPLY} message or the {AUTHENTICATION-REJECT} message the PT shall stop the timer <MM_auth.1> and issue a MM_AUTHENTICATE-cfm primitive indicating the outcome from the procedure. The validity of the response shall be checked. If the PT has received an {AUTHENTICATION-REPLY} message, where the <<RES>> information element contains the correct result the PT shall consider the FT authentication as successful.

NOTE 2: A cipher key should not be generated during FT authentication. If generated, it is not used.

The procedure for authenticating a FT is supervised by the timer <MM_auth.1> in the PT. At the first expiry of timer <MM_auth.1> the PT should retransmit the {AUTHENTICATION-REQUEST} message. If the timer <MM_auth.1> expires a second time the PT shall abort the procedure and release the transaction.



NOTE 3: The procedure for authenticating a FT has the highest priority under the MM procedures and can therefore always be initiated. It restarts the MM timer in the FT of any FT initiated and yet unfinished MM procedure. See also subclause 15.5.

13.4 Location procedures

Three location related procedures are defined, location registration (attach), detach and location update.

13.4.1 Location registration

The location registration procedure is used to indicate to the FT where the PT is located in terms of location areas, where a location area consists of part of one or several DECT systems.

The location registration procedure is based on the International Portable User Identity (IPUI) and is only carried out with respect to the IPUI that is active at the time. The location information that has been stored in association with inactive IPUIs is not effected.

NOTE 1: Location registration without changing the location area is referred to as attach, which is the process whereby a PT informs the FT that it is ready to receive incoming calls. Therefore the procedure for attach is the same as described in this subclause.

The location registration procedure is used as follows:

Upon receiving a MM_LOCATE-req primitive the PT sends a {LOCATE-REQUEST} message containing a <<PORTABLE-IDENTITY>> information element with its IPUI. If the location area has changed, then a <<FIXED-IDENTITY>> information element with the old ARI and a <<LOCATION-AREA>> information element with the old LAL shall be included. If the PT has Extended Location Information (ELI), then this shall also be included in the <<LOCATION-AREA>> information element (as LI-Type 11). If the PT has a network assigned identity, then this shall be sent within a <<NWK-ASSIGNED-IDENTITY>> information element. The {LOCATE-REQUEST} message can also contain an optional <<CIPHER-INFO>> information element, an optional <<SETUP-CAPABILITY>> information element, an optional <<TERMINAL-CAPABILITY>> information element and an optional <<IWU-TO-IWU>> information element. The timer <MM_locate.1> is started.

Upon receiving a {LOCATE-REQUEST} message the FT issues a MM_LOCATE-ind primitive. Upon receiving a MM_LOCATE-res primitive indicating "accept" the FT shall respond with a {LOCATE-ACCEPT} message containing the <<LOCATION-AREA>> information element with the location area level, a <<PORTABLE-IDENTITY>> information element with a new assigned individual TPUI of the PT and an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity.

If the FT does not want to assign TPUI it shall include the <<PORTABLE-IDENTITY>> information element with zero length contents (octet 2 = 0).

If the portable receives a <<Portable identity>> with zero length contents (octet 2 = 0), it shall maintain its currently assigned TPUI. If no TPUI has been previously assigned, it shall use its default TPUI.

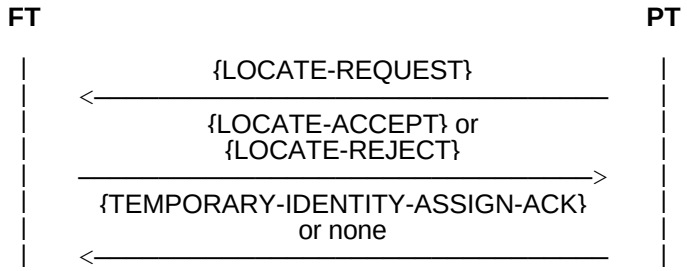
The message can also contain an optional <<DURATION>> information element, which may define for how long at least the location registration and the temporary identities, if provided, are valid. Optionally an <<IWU-TO-IWU>> information element can also be included in the {LOCATE-ACCEPT} message. If a TPUI or NWK assigned identity is included, then the {LOCATE-ACCEPT} message is used to start the procedure for temporary identity assignment as described in subclause 13.2.2. FT shall start timer <MM_ident.1>. Upon receiving a MM_LOCATE-res primitive indicating "reject" the FT shall respond with a {LOCATE-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receipt of the {LOCATE-ACCEPT} message or the {LOCATE-REJECT} message the PT shall stop the timer <MM_locate.1>. The PT issues a MM_LOCATE-cfm primitive. If a correct {LOCATE-ACCEPT} message has been received, the PP shall consider the location registration as successful and shall store the received location information. If the {LOCATE-ACCEPT} message contains a TPUI or/and a network assigned identity, then the PP shall consider this as a temporary identity assignment, and shall respond according to the identity assignment criteria defined in subclause 13.2.2. If it can accept the assignment, it shall store the identities and send back a MM_IDENTITY_ASSIGN-res primitive indicating "Accept" reflecting in a {TEMPORARY-IDENTITY-ASSIGN-ACK} message sent to the FT as described in subclause 13.2.2. If it cannot accept the assignment, it shall send back a MM_IDENTITY_ASSIGN-res primitive indicating "Reject" reflecting in a {TEMPORARY-IDENTITY-ASSIGN-REJ} message as described in subclause 13.2.2. On receipt of a {TEMPORARY-IDENTITY-ASSIGN-ACK} message or a {TEMPORARY-IDENTITY-ASSIGN-REJ} message as described in subclause 13.2.2 FT issues a MM_IDENTITY_ASSIGN-cfm primitive indicating the outcome of the assignment. On receipt of {TEMPORARY-IDENTITY-ASSIGN-ACK} message or {TEMPORARY-IDENTITY-ASSIGN-REJ} message the FT shall stop timer <MM_identity.1>. If timer <MM_ident.1> expires, the FT shall abort the procedure and release the transaction.

The complete location registration procedure shall be treated as a single transaction , even when it includes an identity assignment, see annex H, subclause H.3.2.

If a {LOCATE-REJECT} message has been received containing a <<DURATION>> information element, then the PT shall not initiate this procedure within this location area again before the defined time has passed. If the <<DURATION>> element indicates "Standard time limit" or cannot be understood, the PT shall wait a minimum of <MM_wait> minutes. The time starts with the reception of the {LOCATE-REJECT} message.

The location registration procedure is supervised by the timer <MM_locate.1> in the PT. At the first expiry of timer <MM_locate.1> the PT should retransmit the {LOCATE-REQUEST} message. If the timer <MM_locate.1> expires a second time the PT shall abort the procedure and release the transaction.



NOTE 2: For fast set up also location registration is needed. In this case the size of the location area is one cell.

13.4.2 Detach

Detach is the process whereby a PT informs the FT that it is not ready to receive incoming calls.

NOTE 1: Location registration without changing the location area is referred to as "attach". Therefore the procedure for attach is the same as described in subclause 13.4.1 for location registration.

The detach procedure is used as follows:

Upon receiving a MM_DETACH-req primitive the PT sends a {DETACH} message, containing the <<PORTABLE-IDENTITY>> information element with its IPUI or individual assigned TPUI. If the PT has got a network assigned identity, then this identity shall also be included, using a <<NWK-ASSIGNED-IDENTITY>> information element. Optionally an <<IWU-TO-IWU>> information element can also be included.

Upon receiving a {DETACH} message the FT issues a MM_DETACH-ind primitive.

NOTE 2: This message should have been preceded by a {LOCATE-REQUEST} message.

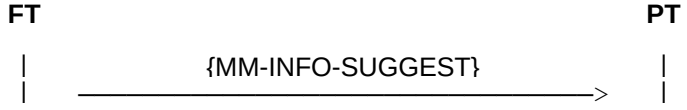
13.4.3 Location update

Location update is used by the FT to inform the PT of a modification of the location areas.

The location update procedure is used as follows:

Upon receiving a MM_INFO-req primitive the FT sends a {MM-INFO-SUGGEST} message, which contains an <<INFO-TYPE>> information element with the parameter type "locate suggest". Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues a MM_INFO-ind primitive. If the parameter type "locate suggest" is indicated in the <<INFO-TYPE>> information element, the PT shall initiate the location registration procedure as described in subclause 13.4.1.



The locate suggest and the following location registration procedure shall be treated as two different transactions, see annex H, subclause H.3.1.

13.5 Access rights procedure

13.5.1 Obtaining the access rights

The procedure for obtaining the access rights is used to load the International Portable User Identity (IPUI), the Portable Access Rights Key (PARK) and other service specific information into the PT.

The PT can then use the knowledge to:

- gain access to the system and make calls;
- recognise the system in order to receive calls.

The FT can then use the knowledge to:

- validate service requests from the PT; and
- allow certain classes of service;
- recognise calls for valid PTs in order to route calls to them.

If the access rights procedure is not supported by the FT, as indicated in the broadcast attributes and as defined in annex F, than the PT shall not initiate this procedure.

Procedure for obtaining the access rights:

Upon receiving a MM_ACCESS_RIGHTS-req primitive the PT initiates the procedure by sending an {ACCESS-RIGHTS-REQUEST} message and starts the timer <MM_access.1>. The {ACCESS-RIGHTS-REQUEST} message contains a <<PORTABLE-IDENTITY>> information element with an international portable user identity, e.g. IPUI type N with the portable's equipment number. The message can also contain an optional <<AUTH-TYPE>> information element, an optional <<CIPHER-INFO>> information element, an optional <<TERMINAL-CAPABILITY>> information element and an optional <<IWU-TO-IWU>> information element.

Upon receiving a {ACCESS-RIGHTS-REQUEST} message the FT issues a MM_ACCESS_RIGHTS-ind primitive. Upon receiving a MM_ACCESS_RIGHTS-res primitive indicating "accept" the FT shall respond by sending an {ACCESS-RIGHTS-ACCEPT} message containing a <<PORTABLE-IDENTITY>> information element with an international portable user identity and an <<FIXED-IDENTITY>> information element with the portable access rights key. Optionally a list of <<FIXED-IDENTITY>> information elements with further portable access rights keys can be included. Further optional information elements are the <<LOCATION-AREA>> information element with the location area level, the <<AUTH-TYPE>> information element which indicates the authentication algorithm and key, the <<CIPHER-INFO>> information element which indicates the cipher algorithm, the <<ZAP-FIELD>> information element with the ZAP value, the <<SERVICE-CLASS>> information element which defines the allowed service, and key and the <<IWU-TO-IWU>> information element with operator specific information.

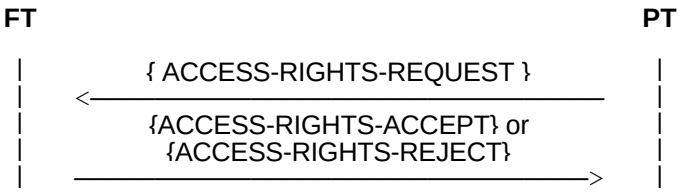
NOTE: For sending the user authentication key over the air the key allocation procedure can be used. That procedure needs a first key e.g. an authentication code which could be keyed in.

Upon receiving a MM_ACCESS_RIGHTS-res primitive indicating "reject" the FT shall respond by sending an {ACCESS-RIGHTS-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receipt of the {ACCESS-RIGHTS-ACCEPT} message or the {ACCESS-RIGHTS-REJECT} message the PT shall stop the timer <MM_access.1>. The PT issues a MM_ACCESS_RIGHTS-cfm primitive. If an {ACCESS-RIGHTS-ACCEPT} message has been received the PT shall store the received information.

If an {ACCESS-RIGHTS-REJECT} message has been received containing a <<DURATION>> information element, then the PT shall not initiate this procedure within this location area again before the defined time has passed. If the <<DURATION>> element cannot be understood or indicates "standard time limit" the PT shall wait a minimum of <MM_wait> minutes. The time starts with the reception of the {ACCESS-RIGHTS-REJECT} message.

The procedure for obtaining access rights is supervised by the timer <MM_access.1> in the PT. At the first expiry of timer <MM_access.1> the PT should retransmit the {ACCESS-RIGHTS-REQUEST} message. If the timer <MM_access.1> expires a second time the PT shall abort the procedure and release the transaction.



13.5.2 Termination of access rights

The procedure for terminating the access rights is used to remove a specific International Portable User Identity (IPUI) and all information which is related to this IPUI from the PT and FT.

The PT is then unable to:

- gain access to the system and make calls;

- recognise the system in order to receive calls.

The FT is then unable to:

- validate service requests from the PT and allow certain classes of service;

- recognise calls for valid PTs in order to route calls to them.

Procedure for terminating access rights initiated by the PT:

Upon receiving a MM_ACCESS_RIGHTS_TERMINATE-req primitive the PT initiates the procedure by sending an {ACCESS-RIGHTS-TERMINATE-REQUEST} message containing the <<PORTABLE-IDENTITY>> information element with the IPUI. The message can also contain an optional <<FIXED-IDENTITY>> information element with a portable access rights key and an optional <<IWU-TO-IWU>> information element. The timer <MM_access.2> is started.

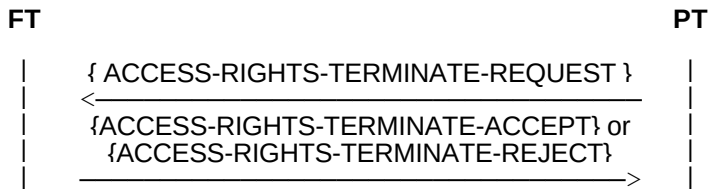
Upon receipt of an {ACCESS-RIGHTS-TERMINATE-REQUEST} message the FT issues a MM_ACCESS_RIGHTS_TERMINATE-ind primitive. The FT may receive a MM_AUTHENTICATE-req primitive triggering the authentication the PT rocedure before the terminate access rights request is answered - in this case termination of access rights procedure and authentication procedure shall be treated as nested procedures, see annex H, subclause H.2. If authentication of the PT is not successful, termination of access rights request should be rejected. If the {ACCESS-RIGHTS-TERMINATE-REQUEST} message contains a PARK, then the erasure of only this PARK is requested. If the {ACCESS-RIGHTS-TERMINATE-REQUEST} message contains no PARK, then the erasure of the IPUI and all data associated with this IPUI is requested. If the FT receives a MM_ACCESS_RIGHTS_TERMINATE-res primitive indicating "accept", then the FT shall respond by sending an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message. If the FT receives a MM_ACCESS_RIGHTS_TERMINATE-res primitive indicating "reject", then the FT shall respond by sending an {ACCESS-RIGHTS-TERMINATE-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receipt of an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message or an {ACCESS-RIGHTS-TERMINATE-REJECT} message the PT shall stop the timer <MM_access.2>. The PT issues a MM_ACCESS_RIGHTS_TERMINATE-cfm primitive. If an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message has been received, the PT shall consider the termination of access rights as successful and delete the same data in the PP, that the former {ACCESS-RIGHTS-TERMINATE-REQUEST} message requested to be deleted.

If an {ACCESS-RIGHTS-TERMINATE-REJECT} message has been received it shall be understood as the required data has not been deleted.

If an {ACCESS-RIGHTS-TERMINATE-REJECT} message has been received containing a <<DURATION>> information element, then the PP shall not initiate this procedure within this location area again before the defined time has passed. If the <<DURATION>> element indicates "standard time limit" or cannot be understood the PP shall wait a minimum of <MM_wait> minutes. The time starts with the reception of the {ACCESS-RIGHTS-TERMINATE-REJECT} message.

The PT initiated procedure for termination of access rights is supervised by the timer <MM_access.2> in the PT. At the first expiry of timer <MM_access.2> the PT should retransmit the {ACCESS-RIGHTS-TERMINATE-REQUEST} message. If the timer <MM_access.2> expires a second time the PT shall abort the procedure and release the transaction.



Procedure for termination of access rights initiated by the FT:

Upon receiving a MM_ACCESS_RIGHTS_TERMINATE-req primitive the FT initiates the procedure by sending a {ACCESS-RIGHTS-TERMINATE-REQUEST} message containing the <<PORTABLE-IDENTITY>> information element with the IPUI. The message can also contain an optional <<FIXED-IDENTITY>> information element with a portable access rights key and an optional <<IWU-TO-IWU>> information element. The timer <MM_access.2> is started.

Upon receipt of the {ACCESS-RIGHTS-TERMINATE-REQUEST} message the PT issues a MM_ACCESS_RIGHTS_TERMINATE-ind primitive. The PP should authenticate the FT - in this case termination of access rights procedure and authentication procedure shall be treated as nested procedures, see annex H, subclause H.2. If the authentication of the FT fails, then the PP should send an ACCESS-RIGHTS-TERMINATE-res indicating "Reject" resulting in an {ACCESS-RIGHTS-TERMINATE-REJECT} message containing the optional <<REJECT-REASON>> information element. Otherwise the PP shall, if the {ACCESS-RIGHTS-TERMINATE-REQUEST} message contains a PARK, erase this PARK and all data associated with this PARK and if the message contains no PARK, erase the IPUI and all data associated with this IPUI and send an MM_ACCESS_RIGHTS_TERMINATE-res indicating "Accept" resulting in an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message being sent back to the FT.

Upon receipt of the {ACCESS-RIGHTS-TERMINATE-ACCEPT} message or the {ACCESS-RIGHTS-TERMINATE-REJECT} message the FT shall stop the timer <MM_access.2>. The FT issues a MM_ACCESS_RIGHTS_TERMINATE-cfm primitive. If an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message has been received, the FT shall consider the termination of access rights as successful.

The FT initiated procedure for termination of access rights is supervised by the timer <MM_access.2> in the FT. At the first expiry of timer <MM_access.2> the FT should retransmit the {ACCESS-RIGHTS-TERMINATE-REQUEST} message. If the timer <MM_access.2> expires a second time the FT shall abort the procedure and release the transaction.

13.6 Key allocation procedure

Upon receiving a MM_KEY_ALLOCATE-req primitive the FT initiates the procedure by sending a {KEY-ALLOCATE} message which shall contain the <<ALLOCATION-TYPE>> information element which indicates the Authentication algorithm identifier, the Authentication code (AC) number to be used and the User authentication key (UAK) number to be derived. The message shall also contain the <<RAND>> information element with the 64-bit random number, RAND-F, and the <<RS>> information element with the 64-bit number RS. The timer <MM_key.1> is started.

NOTE 1: The authentication code which is used in this procedure should be as long as possible, at least 32 bits, but better if 64 bits or more are used.

Upon receipt of the {KEY-ALLOCATE} message the PT issues an MM_KEY_ALLOCATE-ind primitive. If the <<ALLOCATION-TYPE>> element is acceptable the PT shall use the indicated authentication code and the received numbers, RS and RAND-F, to calculate the authentication result RES1. The PT shall start timer <MM_auth.1> and respond by sending an {AUTHENTICATION-REQUEST} message including the <<AUTH-TYPE>> information element with the same parameters (Authentication algorithm identifier, Authentication key (AK) type indicating AC, Authentication code (AC) number) as indicated in the received <<ALLOCATION-TYPE>> information element. The PT shall also include the <<RES>> information element with the calculated result RES1 and the <<RAND>> information element with a 64-bit random number, RAND-P. If the received <<ALLOCATION-TYPE>> element is unacceptable the PT shall respond by sending an {AUTHENTICATION-REJECT} message.

Upon receipt of the {AUTHENTICATION-REJECT} message the FT shall stop the timer <MM_key.1> and consider that the key allocation procedure has failed.

Upon receipt of the {AUTHENTICATION-REQUEST} message the FT shall stop the timer <MM_key.1>. The value XRES1 is computed in the FT from the indicated authentication code, RAND-F and RS. The authentication of PT is considered as successful if RES1 = XRES1. If it is successful the FT shall use the original RS, the AC and the received random number RAND-P to calculate the authentication result, RES2. The FT shall store the reverse session key, KS', as new user authentication key under the UAK-number which was given in the <<ALLOCATION-TYPE>> information element in the {KEY-ALLOCATE} message. The FT marks the new UAK with “unconfirmed status”. The FT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result RES2. If the ‘authentication of the PT has failed´, the FT shall respond by sending an {AUTHENTICATION-REJECT} message.

Upon receipt of the {AUTHENTICATION-REJECT} message the PT shall stop the timer <MM_auth.1> and consider that the key allocation procedure as failed.

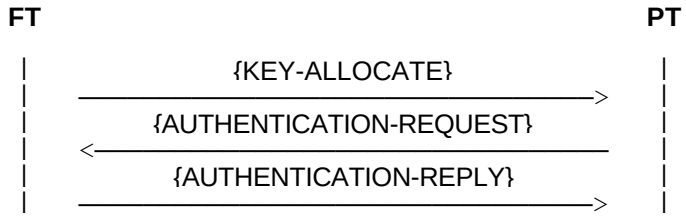
Upon receipt of the {AUTHENTICATION-REPLY} message the PT shall stop the timer <MM_auth.1>. The value XRES2 is computed in the PT from the indicated authentication code, RAND-P and the original RS. The authentication of FT is considered as successful if RES2 = XRES2. If it is successful the PT shall store the reverse session authentication key, KS', as new user authentication key under the UAK-number which was given in the <<ALLOCATE-TYPE>> information element in the {KEY-ALLOCATE} message and erase the used Authentication Code, AC. If the authentication of the FT has failed the PT shall retain the AC, and drop the call.

NOTE 2: The reverse Session authentication Key, KS', is an intermediate result during the calculation of RES2. Refer also to ETS 300 175-7 [7].

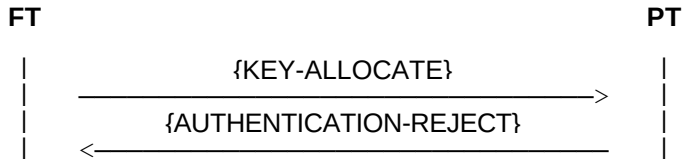
The FT shall keep the Authentication Code (AC), and shall try to use the UAK with “unconfirmed status” in a future PT authentication procedure. If this future authentication of the PT succeeds, then also the FT shall erase the AC, and the UAK will now obtain the “confirmed status”. If it fails the FT shall delete this UAK.

The key allocation procedure is supervised by the timer <MM_key.1> in the FT and by the timer <MM_auth.1> in the PT. At the first expiry of timer <MM_key.1> the FT should re transmit the {KEY-ALLOCATE} message. If the timer <MM_key.1> expires a second time the FT shall abort the procedure and release the transaction. If the timer <MM_auth.1> expires the PT shall abort the procedure and release the transaction.

successful case:



unsuccessful case:



This procedure shall not be used for roaming key allocation in a visited network.

NOTE 3: A possibility for roaming key allocation is that the visited system obtains a Session Key KS with the corresponding value RS from the home system. It can then use this session key for the authentication procedures whereas the PT can use its standard user authentication key together with RS and RAND to calculate the authentication result as normal. Refer also to ETS 300 175-7 [7].

The complete key allocation procedure shall be treated as a single transaction, see annex H, subclause H.3.4.

13.7 Parameter retrieval procedure

This procedure is used to exchange information between the FT and the PT. This information could be necessary for an external handover, where after having obtained this information the actual handover is done by the interworking unit via the call control entity and is not described in this subclause.

The procedure can be initiated by the FT or by the PT.

Procedure for parameter retrieval initiated by the FT:

Upon receiving a MM_INFO-req primitive the FT initiates the procedure by sending a {MM-INFO-SUGGEST} message. This message contains the <<INFO-TYPE>> information element which defines the suggested action. The coding "locate suggest" is used in the case of the location updating procedure which is described in subclause 13.4.3. One of the codings "external handover parameters", "location area", "hand over reference", "external handover candidate", "synchronised external handover candidate" and "non synchronised external handover candidate" is used for the external handover procedure which is described in subclause 15.7.

The {MM-INFO-SUGGEST} message can optionally also contain the following information elements:

<<FIXED-IDENTITY>> with the ARI of a proposed new FT;

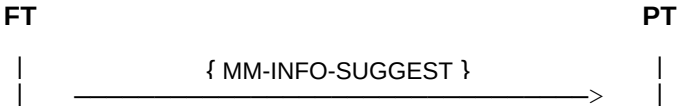
<<LOCATION-AREA>> with the identification of the current location area (extended location information);

<<NWK-ASSIGNED-IDENTITY>> with a network assigned identity;

<<NETWORK-PARAMETER>> with the value of a handover reference;

<<IWU-TO-IWU>> with application specific information.

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues this information directly to the IWU by issuing a MM_INFO-ind primitive.

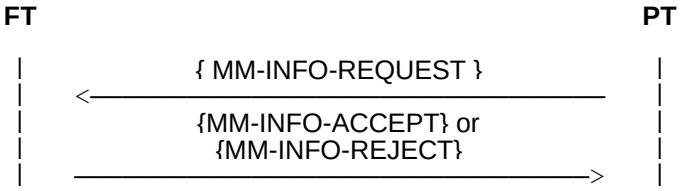


Procedure for parameter retrieval initiated by the PT:

Upon receiving a MM_INFO-req primitive the PT initiates the procedure by sending a {MM-INFO-REQUEST} message, which contains an <<INFO-TYPE>> information element which defines the requested parameter(s) and can contain a <<PORTABLE-IDENTITY>> information element with the IPUI or individual assigned TPUI, an optional <<FIXED-IDENTITY>> information element containing ARI or PARKs identifying candidate FPs, an optional <<LOCATION-AREA>> information element with a new location area identification (extended location information), an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity, an optional <<NETWORK-PARAMETER>> information element with the value of a handover reference and an optional <<IWU-TO-IWU>> information element.

Upon receiving a {MM-INFO-REQUEST} message the FT issues a MM_INFO-ind primitive. Upon receiving a MM_INFO-res primitive indicating "accept" the FT shall respond by sending a {MM-INFO-ACCEPT} message, which can include an <<INFO-TYPE>> information element which gives some more information about specific requested parameter(s), an optional <<FIXED-IDENTITY>> information element with the ARI of a new FT, an optional <<LOCATION-AREA>> information element with the current location area identification (extended location information), an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity, an optional <<NETWORK-PARAMETER>> information element with the value of a handover reference and an optional <<IWU-TO-IWU>> information element. Upon receiving a MM_INFO-res primitive indicating "reject" the FT shall respond by sending a {MM-INFO-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receiving a {MM-INFO-ACCEPT} message or a {MM-INFO-REJECT} message the PT issues a MM_INFO-cfm primitive.



13.8 Ciphering related procedure

This procedure is initiated by the FT or PT and is used to engage or disengage ciphering and in the case of engaging ciphering to define the cipher parameters.

NOTE 1: The real time start and stop of ciphering is done in the MAC layer and is always initiated by the PT.

Procedure for cipher-switching initiated by the FT:

Upon receiving a MM_CIPHER-req primitive the FT initiates the procedure by sending a {CIPHER-REQUEST} message to the PT. The {CIPHER-REQUEST} message contains a <<CIPHER-INFO>> information element with the clear/cipher flag and the identification of the cipher algorithm and cipher key. The message can also contain an optional <<CALL-IDENTITY>> information element, which identifies the call for which ciphering shall be engaged or disengaged, and an optional <<CONNECTION-IDENTITY>> information element, which identifies the connection where ciphering shall be engaged or disengaged. If neither the <<CALL-IDENTITY>> information element nor the <<CONNECTION-IDENTITY>> information element is included, then cipher-switching shall relate to all existing calls/connections between the FT and PT. Optionally an <<IWU-TO-IWU>> information element can be included. The cipher key is transferred with a DL_ENC-KEY.req primitive to the lower layer and the timer <MM_cipher.1> is started.

Upon receipt of the {CIPHER-REQUEST} message the PT issues a MM_CIPHER-ind primitive. The PT checks the clear/cipher flag and if it supports the indicated cipher algorithm and cipher key. The response of the PT is as indicated in the following table:

Table 18: Response to cipher switching initiated by the FT

		Current state	
		clear	ciphered
Wanted state	clear	none	EITHER Ciphering is disabled at the MAC layer OR {CIPHER-REJECT} message is sent to the FT (reject reason = incompatible service)
	ciphered	IF requested ciphering supported THEN ciphering is enabled at the MAC layer ELSE {CIPHER-REJECT} message is sent to the FT (reject reason = "no cipher algorithm" or "cipher algorithm not supported" or "cipher key not supported"	none (note 2)

NOTE 2: A change of the cipher parameters of an existing and already ciphered connection is not supported. It is however possible to switch, to clear, and to start ciphering with new parameters.

If the PT (upon receipt of an MM_CIPHER-res primitive indicating "Reject") responds by sending an {CIPHER-REJECT} message, then this message may contain one or a prioritised list of the optional <<CIPHER-INFO>> information element to propose an alternative algorithm or key and an optional <<REJECT-REASON>> information element.

Upon receipt of a DL_ENCRYPT.ind primitive from the lower layer or a {CIPHER-REJECT} message from the PT the FT shall stop the timer <MM_cipher.1>. The FT issues a MM_CIPHER-cfm primitive.

If a {CIPHER-REJECT} message has been received the FT can:

a) release the call; or

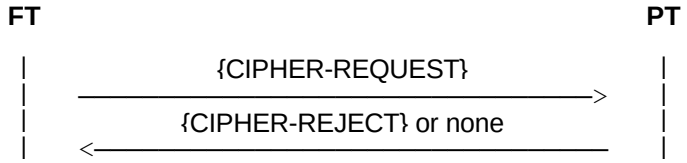
b) proceed in the existing mode;

In the case, that switching from clear to ciphered was requested, the FT has the following additional two options:

c) if the reject reason "cipher algorithm not supported" or the reject reason "cipher key not supported" was included, then the FT can send a new {CIPHER-REQUEST} message with a new <<CIPHER-TYPE>> information element. This element may have been received in the {CIPHER-REJECT} message;

d) if the reject reason "cipher key not supported" was included, then the FT can perform "authentication of the PT" (and thereby establish a new cipher key) and then send a new {CIPHER-REQUEST} message.

The procedure for FT initiated cipher-switching is supervised by the timer <MM_cipher.1> in the FT. At the first expiry of timer <MM_cipher.1> the FT should retransmit the {CIPHER-REQUEST} message. If the timer <MM_cipher.1> expires a second time the FT shall abort the procedure and release the transaction.



Procedure for cipher-switching initiated by the PT:

Upon receiving a MM_CIPHER-req primitive the PT initiates the procedure by sending a {CIPHER-SUGGEST} message to the FT. The {CIPHER-SUGGEST} message contains a <<CIPHER-INFO>> information element with the clear/cipher flag and the identification of the cipher algorithm and cipher key. The message can also contain an optional <<CALL-IDENTITY>> information element, which identifies the call for which ciphering shall be engaged or disengaged, and an optional <<CONNECTION-IDENTITY>> information element, which identifies the connection where ciphering shall be engaged or disengaged. If neither the <<CALL-IDENTITY>> information element nor the <<CONNECTION-IDENTITY>> information element is included, then cipher-switching shall relate to all existing calls/connections between the FT and PT. Optionally an <<IWU-TO-IWU>> information element can be included. The timer <MM_cipher.2> is started.

Upon receipt of the {CIPHER-SUGGEST} message the FT issues an MM_CIPHER-ind primitive to the IWU. The response of the FT is as indicated in the following table and depends on the "Accept/Reject flag" in the received MM_CIPHER-res primitive reflecting whether the requested service is supported.

Table 19: Response to cipher switching initiated by the PT

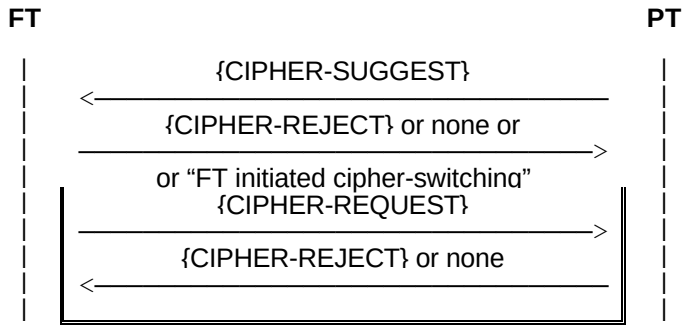
		Current state	
		clear	ciphered
Wanted state	clear	none	If clear is allowed THEN the “procedure for cipher-switching initiated by the FT” is started by sending {CIPHER-REQUEST} message ELSE {CIPHER-REJECT} message is sent to the PT
	ciphered	If requested ciphering supported THEN the “procedure for cipher-switching initiated by the FT” is started, sending {CIPHER-REQUEST} message ELSE {CIPHER-REJECT} message is sent to the PT	none (note 3)

NOTE 3: A change of the cipher parameters of an existing and already ciphered connection is not supported. It is however possible to switch to clear and to start ciphering with new parameters.

Upon receipt of a {CIPHER-REQUEST} message or a {CIPHER-REJECT} message from the FT the PT shall stop the timer <MM_cipher.2>. If a {CIPHER-REQUEST} message has been received, then the PT shall respond as described in the "procedure for cipher-switching initiated by the FT".

If a {CIPHER-REJECT} message has been received, than the PT can either release the call or proceed in the existing mode. In this case the PT issues a MM_CIPHER-cfm primitive indicating "reject".

The procedure for PT initiated cipher-switching is supervised by the timer <MM_cipher.2> in the PT. At the first expiry of timer <MM_cipher.2> the PT should retransmit the {CIPHER-SUGGEST} message. If the timer <MM_cipher.2> expires a second time the PT shall abort the procedure and release the transaction.



The complete procedure for cipher-switching initiated by the PT shall be treated as a single transaction, see annex H, subclause H.3.3.

14 Link Control Entity (LCE) procedures

14.1 General

The Link Control Entity (LCE) is the lowest entity in the NWK layer, and all messages to and from the higher entities pass through the LCE. There is a single LCE at both the FT and the PT.

The LCE controls independent links for each PT. The main function of this single LCE is the message routing task: there is no other interaction between the links. All the LCE procedures are described in terms of one link, and multiple instances of these procedures may be required for a complete FT implementation.

NOTE 1: The following procedures describe the message routing task in terms of two identities: IPUI and TPUI. This task implies a requirement for a local "LCE routing table" that contains the legal IPUI/TPUI associations. The procedures for the creation and management of this table are not defined in this ETS.

Each connection oriented link (each Class U, Class A or Class B value of LLN for every PT) can exist in one of four states. A pictorial overview of these states is given in annex C.

- "LINK RELEASED": the link is fully released.
- "LINK ESTABLISHED": the link is fully established, with a defined class of operation.
- "ESTABLISH PENDING": link establishment has been requested, but has not yet been confirmed.
- "RELEASE PENDING": link release has been requested, but has not yet been confirmed.

Each Class B link may support three additional states:

- "LINK SUSPENDED": the link is fully suspended.
- "SUSPEND PENDING": link suspend has been requested, but has not yet been confirmed.
- "RESUME PENDING": link resume has been requested, but has not yet been confirmed.

Each connectionless link (Class U only) can only exist in one state.

NOTE 2: Refer to ETS 300 175-4 [4] for a description of Class U, Class A and Class B links.

The LCE operation is described in two groups of procedures:

a) connection orientated link control;

b) connectionless link control.

14.2 Connection oriented link control procedures

14.2.1 Link establishment

The connection oriented link control procedures are concerned with the establishment, the maintenance, the optional suspension/resumption and the release of one or more DLC C-plane links to each PT, whenever there is a demand from a higher NWK layer entity. The message from each higher layer instance shall only be routed via one link, but multiple instances may share a single link, or may use separate links.

Each C-plane link shall only be maintained while there are continued demands from the higher entities. When these demands cease (i.e. when all relevant calls are released), the LCE shall release the associated DLC link(s).

The LCE shall immediately (re) establish a DLC C-plane link, in response to the arrival of a message from any of the higher entities. This establishment of a C-plane link is the most complex part of the LCE operation. Three establishment procedures are described:

- direct PT initiated link establishment;

- indirect (paged) FT initiated link establishment;

- direct FT initiated link establishment.

NOTE: The operation of the link establishment procedures may be dependent on stored information relating to the capabilities of PTs. This information storage is described as a "LCE location table" in the following subclauses. The structure of this table is not defined in this ETS.

Additional messages may be queued at the originating LCE during this set-up phase.

If a higher entity releases a call, whilst the initial messages are still queued (i.e. if the link is in the "ESTABLISH PENDING" state), the queued messages shall be discarded, and the link establishment shall be immediately terminated by issuing a DL_RELEASE-req primitive to the DLC layer.

14.2.2 Direct PT initiated link establishment

Direct PT initiated link establishment shall occur when the first service request is detected by the LCE in the PT. The LCE queues (stores) the associated messages, and shall issue a DL_ESTABLISH-req primitive via the S-SAP (SAPI="0"). This primitive shall specify the class of link required and may optionally include a SDU containing the first message.

Each DL_ESTABLISH-req primitive shall be interpreted as a request for a new independent link.

If link establishment is successful the DLC replies with a DL_ESTABLISH-cfm primitive. The LCE shall now mark the link as "LINK-ESTABLISHED" and shall send any queued messages using DL_DATA-req primitives via the S-SAP (SAPI="0").

If the F-LCE receives a DL_ESTABLISH-ind without an SDU, it should start timer <LCE.05>. This timer is stopped when a new higher entity message or DL_DATA-ind with an SDU is received. On expiry of timer <LCE.05>, when no higher entities are running, the LCE shall release the link immediately using the “abnormal” release procedure as specified in subclause 14.2.7.1

14.2.3 Indirect (paged) FT initiated link establishment

Indirect FT initiated link establishment is the normal method of FT initiated link establishment. It occurs when a new link request is received by the LCE, and no suitable link is available. As part of this request, the first message for a given PT should be passed to the LCE in the FT. The LCE shall queue (store) this initial message, and shall issue a {LCE-REQUEST-PAGE} message using either a DL_BROADCAST-req primitive or a DL_EXPEDITED-req primitive via the B-SAP. It shall then mark the link as in the "ESTABLISH PENDING" state, and shall start timer <LCE.03>.

No further indirect link establishment messages shall be generated for a PT that has a link in the "ESTABLISH PENDING" state. New requests shall be queued until the pending link establishment is either successful or has failed (timer <LCE.03> has expired).

The DL_EXPEDITED-req primitive shall only be used if the wanted PT is recorded as having a "FAST-PAGE" capability in the LCE location table. Otherwise the DL_BROADCAST-req primitive shall be used.

For individual messages, the identity used in this message shall be decided as follows:

a) the assigned individual TPUI shall be used if available. This may be transmitted in either the short address format or the long address format;

b) if an assigned individual TPUI is not available the identity shall depend on the address format used; either

   - the short address format shall be used. This shall contain the default individual TPUI; or

   - the long address format shall be used. This shall contain part of the IPUI.

For group messages, an assigned value of TPUI shall always be used.

Refer to ETS 300 175-6 [5] for details of IPUI and TPUI. Refer to subclause 8.2 of this ETS, for details of the corresponding message formats.

NOTE 1: The use of a default individual TPUI or an IPUI means that the identity is not guaranteed to be unique. This allows the possibility of causing false responses from PTs. Therefore the use of assigned individual TPUIs is recommended.

If the {LCE-REQUEST-PAGE} message is successfully received by the intended PT, it shall respond with a PT initiated link establishment, using the procedure defined in subclause 14.2.2. The DL_ESTABLISH-req primitive used by the PT shall contain a {LCE-PAGE-RESPONSE} message which shall contain a complete portable identity. The identity used shall be decided as follows:

- the complete IPUI shall always be used.

When the {LCE-REQUEST-PAGE} message contains the default individual TPUI, and the intended PT has an assigned TPUI available, the PT shall still respond with a PT initiated link establishment.

The PT response shall be regarded as a new transaction, and the LCE in the PT shall set the transaction identifier to indicate a PT initiated transaction. See subclause 7.3.

The {LCE-REQUEST-PAGE} message may contain extended details of the required MAC layer service (see subclause 8.2). In this event the responding PT may use these service details to start immediate establishment of the required service at the MAC layer. In all other cases, the responding PT shall only establish the minimum MAC layer service needed for a single C-plane link (i.e. a single duplex bearer).

The PT may respond to {LCE-REQUEST-PAGE} messages that contain a correct identity, even if the DLC reports an error for the message, but in this event only a single C-plane link shall be established.

NOTE 2: The possibility to reply to an errored message is allowed to improve the probability of getting the wanted response (i.e. by allowing an error) even though it also means that some false responses may exist. False responses are already possible because the use of shortened IPUIs is allowed.

If this indirect link establishment is successful the DLC at the FT shall deliver a DL_ESTABLISH-ind primitive to the originating LCE containing the {LCE-PAGE-RESPONSE} message. The LCE shall then check the identity contained in this response against a list of outstanding {LCE-REQUEST-PAGE} messages, and if the identity matches it shall mark the link as "LINK ESTABLISHED"; it shall stop timer <LCE.03> and shall send all the queued messages using DL_DATA-req primitives via the S-SAP (SAPI="0").

NOTE 3: The MAC layer identity, PMID, is directly related to the assigned individual TPUI (if used). This identity should be available via the LLME, and may be used to identify the matching {LCE-REQUEST-PAGE} message.

NOTE 4: The LCE should only provide a consistency check of the portable identity. Further checks of identities (for validation or authentication) may occur in the higher entities.

If the identity does not match, the LCE shall immediately reject the set-up by sending a {LCE-PAGE-REJECT} message, using a DL_DATA-req primitive via the S-SAP (SAPI="0") using the same DLEI as indicated by the primitive containing the {LCE-PAGE-RESPONSE}. This FT reply shall also use the same transaction value as used by the PT in the {LCE-PAGE-RESPONSE} message.

The LCE may use the {LCE-PAGE-REJECT} to report a invalid assigned TPUI (individual or group TPUI), by using the <<REJECT-REASON>> information element to indicate "invalid TPUI". Upon receipt of this reason the PT should immediately erase the assigned TPUI.

The LCE may use the {LCE-PAGE-REJECT} to request an automatic test call back, by setting the <<REJECT-REASON>> to test call back: normal/emergency, en-bloc or test call back: normal/emergency, piecewise. See subclause 15.8.

This unwanted link shall be immediately released using the "normal" release procedures defined in subclause 14.2.7.

NOTE 5: The {LCE-PAGE-REJECT} message is only sent over the point-to-point link that has been established by the responding PT. It is not a broadcast message.

NOTE 6: The {LCE-REQUEST-PAGE} message may address more than one portable, when using a group identity. In this case the {LCE-PAGE-REJECT} message should be used to reject a second (and any subsequent) responses.

If timer <LCE.03> expires before the wanted link is established, the LCE should resubmit the {LCE-REQUEST-PAGE} message. Resubmitted messages shall only be issued at a lower priority than other outstanding B-FORMAT messages. A message may be resubmitted a maximum of N300 times, before it is discarded. The link shall remain in the "ESTABLISH PENDING" state until the {LCE-REQUEST-PAGE} message is discarded, thereby preventing any other set-up attempts to the same PT. Upon discarding the message, the link shall be immediately marked as "LINK RELEASED" and the LLME shall be notified of the failure. A new indirect establishment may be initiated immediately.

NOTE 7: The failure of one or more indirect establishment attempts may be used to update the LCE location table such that future set-up requests are rejected. Any such action is not specified as part of this ETS.

If the call is released by the higher entity (usually as a result of a time-out) the message shall be immediately discarded, such that any subsequent responses shall be appear as unwanted responses, thereby invoking the reject procedures described above.

14.2.4 Direct FT initiated link establishment (optional)

Direct FT initiated link establishment can be used as an alternative to indirect FT initiated link establishment only when the intended PT has a valid entry in a LCE location table. This table entry must specify one RFP as the likely location of the wanted PT.

NOTE: The definition of "valid entry" is a local matter and is not specified in this ETS.

When the first message for a particular PT is passed to the LCE in the FT, the LCE queues (stores) the call set-up message, and issues a DL_ESTABLISH-req primitive directly to the DLC layer via the S-SAP (SAPI="0"). This primitive shall contain the correct routing information (to identify a single RFP), and this is used by the DLC layer to address the RFP to use for the set-up attempt.

If link establishment is successful the DLC replies with a DL_ESTABLISH-cfm primitive. The LCE shall now mark the link as "LINK ESTABLISHED", and it shall send the original call set-up message using a DL_DATA-req primitive via the S-SAP (SAPI="0").

If this direct link establishment fails, the originating LCE may reattempt using the indirect procedures described in subclause 14.2.3.

14.2.5 Link maintenance

Active link maintenance is the responsibility of the DLC layer, and no additional maintenance procedures are defined for the LCE.

The LCE has a passive responsibility to report any link failures. An unexpected link failure may occur at any time, resulting in an unexpected DL_RELEASE-ind primitive. The LCE shall report this failure immediately to all active entities. Link re-establishment shall only be attempted upon receipt of service demands from a higher entity.

NOTE: The mechanism for such reporting is internal to the DLC layer, and is not specified in this ETS.

14.2.6 Link suspend and resume

A link may be suspended in response to a request from the CC or COMS entity. This request shall only activate the DLC layer suspend procedure if no other higher entities are using the link (this includes other CC or COMS entities).

A link should be resumed in response to a request from any higher entity. The arrival of a message from any higher entity shall be regarded as a request for link resumption.

Support of the suspend and resume procedures by the LCE is only required when using Class B links.

NOTE: A Class A link cannot be suspended. The LLME may command the release of the Class A link when suspending a call, this provides an equivalent function to Class B suspend.

14.2.6.1 Link suspend

The suspend procedure may be initiated by the LCE at either side (FT or PT) by issuing a DL_SUSPEND-req primitive to the DLC layer. The LCE shall then mark the link as "SUSPEND PENDING" and shall start timer <LCE.04>. Any subsequent messages for this link shall be queued until a response is received from the DLC.

At the receiving side, a request for suspension is indicated with a DL_SUSPEND-ind primitive. The receiving LCE may either accept or reject the suspension, and shall immediately indicate its' decision using a DL_SUSPEND-res primitive. If the suspension is accepted, the receiving LCE shall immediately mark the link as "LINK SUSPENDED". No further messages shall then be submitted, without first invoking link resumption. If the suspension is rejected the receiving LCE shall take no further action and may immediately continue with normal message transmission.

Acceptance or rejection of the suspension shall be indicated to the initiating LCE using a DL_SUSPEND-cfm primitive. Upon receipt of DL_SUSPEND-cfm primitive indicating acceptance, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK SUSPENDED".

NOTE: If there are any queued messages the link should be immediately resumed.

Upon receipt of a DL_SUSPEND-cfm primitive indicating rejection, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK ESTABLISHED". If there are any queued messages these shall be immediately transmitted using DL_DATA-req primitives.

14.2.6.2 Link resume

The resume procedure can be initiated by the LCE at either side (FT or PT) by issuing a DL_RESUME-req primitive to the DLC layer. The LCE shall then mark the link as "RESUME PENDING" and shall start timer <LCE.04>. All messages for this link shall be queued until a response is received from the DLC.

At the receiving side, a request for resumption is indicated with a DL_RESUME-ind primitive. The receiving LCE shall either accept the resumption or shall reject the resumption by immediately releasing the link using the "abnormal" release procedures described in subclause 14.2.7.

If the resumption is accepted, the receiving LCE shall immediately return a DL_RESUME-res primitive and shall mark the link as "LINK ESTABLISHED". Successful resumption shall be reported to the initiating LCE with a DL_RESUME-cfm primitive, and on receipt of this primitive, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK ESTABLISHED". Any queued messages shall be immediately transmitted using DL_DATA-req primitives.

Rejection is indicated to both the receiving LCE and the initiating LCE with DL_RELEASE primitives as described in subclause 14.2.7. In this event, the initiating LCE shall stop timer <LCE.04> and both entities shall mark the link as "LINK RELEASED".

NOTE: Either LCE may subsequently attempt to re-establish the link using the procedures defined in subclause 14.2.1.

14.2.7 Link release

If a higher layer entity no longer requires the link, it shall indicate this to the LCE by means of notification "NLR" (no link required). This notification shall contain a release reason, indicating whether or not the entity requires the link to be still maintained for some time. If the link needs to be maintained for some time, the release reason shall be "partial release".

14.2.7.1 NLR notification without "partial release" as release reason

If the higher layer entity issues an NLR notification without "partial release" as release reason, then the LCE shall examine whether no other higher layer entities are using it and no LCE timers are running. If this is the case, then the LCE shall release the link using either the "normal" release procedure or the "abnormal" release procedure.

NOTE: The "normal" release is a conditional release that allows the DLC to complete transmission of any outstanding messages before releasing the link. The "abnormal" release is a request for an unconditional (immediate) release where any outstanding messages are discarded without notification. Use of the "normal" release procedure is recommended.

"Normal" release shall be initiated by the LCE at either side (FT or PT) by issuing a DL_RELEASE-req primitive to the DLC layer with the release mode parameter indicating "normal". The LCE shall then mark the link as "RELEASE PENDING", and shall start timer <LCE.01>. The DLC layer shall reply with a DL_RELEASE-cfm primitive to indicate completion of the release, and the LCE shall then mark the link as "LINK RELEASED", and shall stop timer <LCE.01>.

The DL_RELEASE-cfm primitive shall indicate the release mode achieved. A "normal" release shall indicate that the release has been successfully completed (e.g. successful acknowledgement of a Class B link released). An "abnormal" release shall indicate either an unacknowledged Class B release, or an unexpected upward release.

If timer <LCE.01> expires before the DL_RELEASE-cfm primitive is received, the initiating entity shall immediately initiate the "abnormal" release procedure as described below.

"Abnormal" release shall be initiated by the LCE at either side (FT or PT) by issuing a DL_RELEASE-req primitive to the DLC layer with the release mode parameter indicating "abnormal". The LCE shall then mark the link as "RELEASE PENDING". The DLC layer shall reply with a DL_RELEASE-cfm primitive to indicate completion of the release, and the LCE shall then mark the link as "LINK RELEASED".

A link shall not be re-established whilst in the "RELEASE PENDING" state.

14.2.7.2 NLR notification with "partial release" as release reason

If the higher layer entity issues an NLR notification with "partial release" as release reason, then the LCE shall start (or re-start if already running) timer <LCE.02>. On expiry of <LCE.02>, and if no other higher entities are using the link, and no other LCE timers are running, the LCE shall release the link immediately using the "abnormal" release procedure as specified in subclause 14.2.7.1. No action shall be taken on expiry of <LCE.02> if any other higher entities are using the link, or if any other LCE timers are running.

If CC wants to clear a call using "partial release", it shall first execute a normal call release procedure as specified in subclause 9.5.1, using "partial release" in the <<RELEASE-REASON>> information element in the {CC-RELEASE} message. Thereafter it shall issue an NLR notification with "partial release" as reason parameter.

CISS and CLMS shall always indicate "partial release" in their NLR notifications. MM shall always indicate "partial release" in the NLR notification, except after a location registration procedure with TPUI assignment has been made.

14.3 Connectionless link control procedures

14.3.1 Message routing

A single connectionless link may exist in the direction FT => PT or PT => FT. This link shall only be used by the CLMS entity.

No establishment or maintenance procedures shall be defined for this link, and the state of suitable lower resources shall be ignored by the LCE. CLMS messages shall be immediately submitted to the DLC unless the broadcast announcement procedure described in subclause 14.3.2 is used.

NOTE 1: The LLME is assumed to be responsible for establishing connectionless resources in all lower layers whenever required.

CLMS messages should be sent on the connectionless link using a DL_UNIT_DATA-req primitive via the connectionless S-SAP (SAPI="3"). However, if a suitable connection oriented link already exists in the "LINK ESTABLISHED" state, a CLMS message may be submitted over that link using a DL_UNIT_DATA-req primitive via the connection oriented S-SAP (SAPI="0").

A connection oriented link shall not be established to only carry CLMS messages.

CLMS messages may be received via either the connectionless or the connection oriented SAP (SAPI="0" or "3"). Messages shall be passed to the CLMS in their order of arrival.

NOTE 2: There are restrictions on the maximum message lengths for all CLMS messages (refer to subclause 12.3.2.1). These restrictions apply directly to the CLMS operation, and no checking of message lengths is required in the LCE.

14.3.2 Broadcast announce procedure

CLMS messages in the direction FT to PT may optionally be queued in the LCE while an automatic announcement is broadcast.

This procedure shall not be used if the CLMS message is being routed over a connection oriented link (SAPI="0").

Upon receipt of a message requiring an announcement, the LCE may queue the message. It shall then immediately issue a {LCE-REQUEST-PAGE} message indicating "none" (refer to message coding in subclause 8.2.1.) using a DL_BROADCAST-req or DL_EXPEDITED-req primitive via the B-SAP.

NOTE: The primitive is chosen according to the set-up attributes of the relevant portable. See also subclause 14.2.3.

The {LCE-REQUEST-PAGE} message shall contain the same value of connectionless TPUI as used in the CLMS message.

The LCE shall then start timer <LCE.03>, and upon expiry of this timer it shall submit the CLMS message using a DL_UNIT_DATA-req primitive via the S-SAP (SAPI="3").

14.4 Procedure for collective and group ringing

On receipt of a request from the local network for an incoming call an FP-IWU may decide to ring part or all of its PPs prior to forwarding the call.

In this case the FP-IWU shall request the LCE to send a request for ringing indicating which PPs shall ring. Either the group mask shall be used to ring all PPs having an assigned conectionless group TPUI matching the group mask, or the connectionless TPUI shall be used to ring the PPs having this connectionless TPUI assigned, or the Collective Broadcast Identifier shall be used to ring all PPs.

Upon this request the FT LCE shall send a special {LCE-REQUEST-PAGE} message see subclause 8.2.1, thereby requesting all or part of the subscribed PPs as indicated to start ringing.

At the PT side on receipt of the {LCE-REQUEST-PAGE} message indicating "ringing" the LCE shall inform the P-IWU of the request.

Depending on the type of ringing requested the PP shall react as following:

If group mask ringing was requested the PP shall compare the received group mask to its assigned connectionless group TPUI (if any). The PP shall start ringing if the assigned connectionless group TPUI has in the last 12 bits ‘1s’ at the same bits where the mask has ‘1s’ and shall not care for the settings of the bits in which the mask has ‘0s’. The PP shall not ring if it has ‘0’ in any bit position in which the relative bit in the mask has ‘1’.

Example 1

PP's group TPUI 12 last bits = '1100 0111 1111'
Group mask received = '1100 0011 1111'
Comparison decision: 'MAP', PP shall ring.
(The mask requires '1' in bits 1, 2, 3 ,4, 5, 6, 11 and 12, the group TPUI has them set; bits 7 to 10 "don't care" bits.)

Example 2

PP's group TPUI 12 last bits = '1100 0111 1111'
Group mask received = '1111 0011 1111'
Comparison decision: 'NOT MAP', PP shall not ring.
(The mask requires '1' in bits 1, 2, 3 ,4, 5, 6, 9, 10, 11 and 12, the group TPUI has bits 9 and 10 set to '0'; bits 7 and 8 "don't care" bits.)

NOTE 1: The P-IWU reaction in the event of another call being in progress when collective or group ringing occurrsis up to the IWU. For example if at the time some PPs have already established a call (e.g. two PPs having internal call) the {LCE-REQUEST-PAGE} may be interpreted as an unexpected message from those PPs and ringing need not be initiated.

Similarly, The P-IWU reaction upon in the event of a call setup during collective or group ringing is also up to the IWU. For example it may reject the call-setup or it may stop ringing and allows the call setup to proceed.

NOTE 2: By choosing a specific Group mask and group TPUIs allocation an FP may ring one or several PP groups at a time.

If group ringing was requested the PP shall ring if the received connectionless group TPUI is equal to the last 12 bits of its assigned connectionless group TPUI (if any).

If Collective ringing was requested (see subclause 8.2.1) the PP shall check first whether the Address field equals FFFH (CBI), and if it is true the PP shall start ringing.

When a user answers the ringing, the "off hook" shall trigger an outgoing call request. The {CC-SETUP} message shall be submitted to the P-LCE, triggering by this a direct PT link establishment, see subclause 14.2.2. When the link is established the {CC-SETUP} message shall be passed to the F-LCE.

On receipt of the {CC-SETUP} message at the FT side an MNCC_SETUP-ind primitive shall be sent to the F-IWU.

At the FP-IWU this outgoing call is directly mapped to the awaiting incoming call and an MNCC_CONNECT-req primitive shall be issued to the FT which shall send a {CC-CONNECT} message to the PT.

In this case or if FP decides to release the incoming call, the F-IWU shall inform the LCE that ringing is not any longer required and the LCE shall immediately send a new {LCE-REQUEST-PAGE} message indicating 'incoming call released from the FP" or "incoming call has been answered" as appropriate, thereby requesting ringing to be stopped.

Upon receipt of this message the not answering PPs shall stop ringing.

NOTE 3: To avoid infinite ringing (e.g. PP goes out of range and is not reachable for the "ring off" message) a timer should be implemented in the P-IWU. The recommended value is 120 sec.

15 Management procedures

15.1 Lower Layer Management Entity (LLME)

The Lower Layer Management Entity (LLME) shall contain the following groups of procedures that are relevant to the operation of the NWK layer:

Service mapping and negotiation: mapping of the user service demands into information elements and procedures of the internal protocols. Exchange of information elements during call set-up to negotiate and agree the exact service details.

Service modification: management of service modifications (including suspension and resumption) in response to changing service demands.

Resource management: coordination of the installation and control of the lower layer resources in response to service demands.

Management of MM procedures: coordination of different Mobility Management (MM) procedures to avoid deadlock conditions.

Call ciphering management: coordination of ciphering functions between the Mobility Management (MM) entity and one or more Call Control (CC) entities.

External handover management: procedures to support the transfer of parameters related to external handover.

Test management: procedures to support testing of equipment.

15.2 Service mapping and negotiation

15.2.1 General

The LLME is required to map the external service demands (as indicated by the MNCC_SETUP primitive) into internal service instances. Negotiation of acceptable services may be performed at the same time using the following procedures the Call Control (CC) establishment phase.

The LLME shall map the interworking (user) service details into internal service demands and both the external attributes and the resulting internal attributes may be negotiated. If the negotiation is successful, only the agreed service details shall be passed to the lower layers (via the LLME) to invoke U-plane service installation.

Service negotiation may involve one or more of the following procedures:

a) the prioritised list procedure to negotiate the <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> elements;

b) the exchanged attribute procedure to negotiate the <<IWU-ATTRIBUTES>> element;

c) the operating parameter procedure to negotiate the <<WINDOW-SIZE>> and/or the <<TRANSIT-DELAY>> elements;

d) the peer determined negotiation procedure to negotiate the <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> elements.

15.2.2 Prioritised list negotiation

Prioritised list negotiation allows up to three choices of service mapping to be offered by the initiating entity by including repeated <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> information elements into the {CC-SETUP} message as follows:

- a <<REPEAT-INDICATOR>> element indicating "prioritised list"; followed by

- a prioritised list of up to 3 <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> elements.

Upon receipt of this message, the peer entity should choose the highest priority option that it can support, and shall confirm that choice returning the appropriate <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> elements in the first response message (i.e. {CC-SETUP-ACK}, {CC-CALL-PROC}, {CC-ALERTING} or {CC-CONNECT}). If none of the offered mappings are acceptable, the call shall be released using the normal release procedures.

15.2.3 Exchanged attribute negotiation

Exchanged attribute negotiation may be supported by interworking units in addition to or instead of prioritised list negotiation. Exchanged attribute negotiation provides a mechanism for peer (receiving) entities to suggest alternative service attributes in response to an unacceptable set-up request. This response is designed to provide additional information to the initiating entity such that a subsequent reattempt (using modified service attributes) is more likely to succeed.

Exchanged attribute negotiation shall only be invoked by the receiving IWU if support of this capability is indicated in the <<IWU-ATTRIBUTES>> element (as contained in the {CC-SETUP} message), and if none of the proposed services in the {CC-SETUP} message are acceptable. In this event, the IWU shall reject the call by issuing a MNCC_REJECT-req primitive. It may include one alternative service description in this rejection using an <<IWU-ATTRIBUTES>> element indicating "exchanged parameter negotiation". This description shall indicate an alternative service from the services that are supported by that IWU. An MNCC_REJECT-req primitive which includes the <<IWU-ATTRIBUTES>> element (thus indicating it wishes to initiate the exchanged attribute negotiation procedure) and <<CONNECTION ATTRIBUTES>> shall always indicate a <<RELEASE-REASON>> of 'Partial release', thereby indicating that the lower layer (LCE) resources should be maintained (see subclause 14.2.7).

In the event that no alternative mapping is possible, the <<IWU-ATTRIBUTES>> element may either be omitted or, if included, it shall contain a copy of the received <<IWU-ATTRIBUTES>> element that has been modified to indicate "negotiation not possible". If exchanged parameter negotiation is not supported, the <<IWU-ATTRIBUTES>> element shall be omitted and the <<RELEASE-REASON>> element shall be included indicating "negotiation not supported".

Upon receipt of a response indicating "exchanged parameter negotiation" the initiating entity shall issue the proposed alternative service mapping to the initiating IWU in a MNCC_REJECT-ind primitive (cause = peer message). The call shall nonetheless be released, and any subsequent reattempt shall be treated as a new call instance.

15.2.4 Operating parameter negotiation

Operating parameter negotiation may be supported as part of all data services. The procedure shall involve the following information elements:

- <<WINDOW-SIZE>>;

- <<TRANSIT-DELAY>>.

If the initiating side includes one (or more) of these parameters in the {CC-SETUP} message, the peer side shall check that the offered parameters are acceptable before accepting the call. The peer side may negotiate a reduced value for one or more of the parameters by returning the modified elements in the first response message (i.e. {CC-SETUP-ACK}, {CC-CALL-PROC}, {CC-ALERTING} or {CC-CONNECT}). This message may also return unmodified parameters as formal acceptance of these unmodified values.

In all cases, the peer side shall only return a value less than or equal to the initial offer, and the initiating side should normally accept any reduced value. In exceptional circumstances, where the reduced value gives an unacceptable grade of service, the initiating side may release the call.

15.2.5 Peer attribute negotiation

Peer determined attribute negotiation may be supported by interworking units in addition to or instead of prioritised list negotiation and/or exchanged attribute negotiation. It provides a mechanism whereby the call initiating entity allows the peer (receiving) entity to redefine some of the <<IWU-ATTRIBUTES>> parameters given in the {CC-SETUP} message without requiring the release and re-establishment of the initiated call. This procedure represents a combination of the Prioritised list negotiation and the Exchanged attributes procedures.

Peer determined attribute negotiation shall only be invoked by the receiving IWU if support of this capability is indicated in the <<IWU-ATTRIBUTES>> element (as contained in the {CC-SETUP} message), and if none of the proposed services in the {CC-SETUP} message are acceptable. In this event, the IWU/ PP application may choose to continue the call setup procedure by including one alternative service description in the <<IWU-ATTRIBUTES>> element in the first response message (i.e. {CC-SETUP-ACK}, {CC-CALL-PROC}, {CC-ALERTING} or {CC-CONNECT}). The peer entity shall in offering the alternative <<IWU-ATTRIBUTES>> element not change the codings of octets 3 and 4 of that element from those which it received in the <<IWU-ATTRIBUTES>> in the {CC-SETUP} message. If the peer entity cannot support the attributes specified in these octets or in any other part of the {CC-SETUP} message excluding the <<IWU-ATTRIBUTES>> , or if it does not support these procedures the call shall be released using the normal release procedures.

The initiating entity shall indicate its acceptance of these new attributes by proceeding with the normal call setup procedures. If it cannot support the new attributes the call shall be released using the normal release procedures.

15.3 Service modification procedures

Service modification procedures provide for a restricted set of modifications to an existing "ACTIVE" call, as described in subclause 9.6.

The LLME is required to map the new service demands (as indicated by the MNCC_INFO primitive) into internal service change procedures, and the resulting mapping shall be exchanged using the {CC-SERVICE-CHANGE} message.

Following acceptance of the change, the LLME shall map the U-plane modifications into lower layer service modifications and the agreed service details shall be passed to the lower layers (via the LLME) to invoke U-plane service modification.

The LLME may also invoke C-plane suspension via the LCE.

15.4 Resource management

All the DECT network resources shall be managed and coordinated within the LLME. This subclause shall only describe coordination of the resources associated with a single portable part. Any broader coordination (such as may be required in complex fixed parts) is not described.

C-plane resources are managed via the LCE, U-plane resources are managed directly via the LLME. In both cases, the detailed management procedures are not specified as part of this ETS, because of the need to allow considerable implementation flexibility.

15.5 Management of MM procedures

In order to avoid possible deadlocks between different Mobility Management (MM) procedures the following rules apply:

- two MM procedures are allowed at any one time, but they shall not both have been initiated by the same side;

- if a MM procedure has not yet been finished, then a second MM procedure may only be initiated if the second MM procedure has a higher priority than the first MM procedure.

If a second procedure with higher priority is invoked by the side which has not invoked the first unfinished procedure, then the other side shall accept this second higher priority procedure and respond, without waiting for a completion of the lower priority procedure. In this case, completion of the higher priority procedure restarts the timer of the lower priority procedure. If the higher priority procedure is a FT initiated user authentication procedure, then the PT shall stop the timer of an unfinished PT initiated lower priority procedure and start the <MM_auth.2> timer. The PT shall stop the <MM_auth.2> timer when it responds to the user authentication procedure by sending an {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message. If the <MM_auth.2> timer expires or is stopped and the lower priority procedure has

not been finished in the meantime, then the timer of the interrupted lower priority procedure shall be restarted.

If a procedure with higher priority is invoked by the side which has already invoked a lower priority procedure, which is not yet finished, then the lower priority procedure shall be cancelled.

Priority level 1 (highest priority):

- authentication of a FT.

Priority level 2 (medium priority):

- access rights terminate, FT initiated;
- authentication of a PT;
- authentication of the user;
- ciphering related, FT initiated;
- identification of PT;
- key allocation;
- location update;
- parameter retrieval, FT initiated;
- temporary identity assignment.

Priority level 3 (lowest priority):

- access rights;
- access rights terminate, PT initiated;
- ciphering related, PT initiated;
- detach;
- location registration;
- parameter retrieval, PT initiated.

The procedures of priority level 1 and 3 are PT initiated. The procedures of priority level 2 are FT initiated.

For the transaction identifier flags assignment in case of nested or stand alone MM procedures see annex H.

For some procedures external to the MM entity, typically CC and COMS procedures, the FT can decide to perform MM procedures prior to executing the PT-initiated CC/COMS procedures. For instance the FT may want to authenticate the PT prior to sending an acknowledgement on a {CC-SETUP} message. These "interrupting" MM procedures might take more time than the expiry time of the running timers in the CC/COMS entity.

To prevent CC/COMS state machines from waiting on a response delayed by MM procedures, the FT has the possibility to restart the CC/COMS timers in the PT. To cause a timer restart, the LLME should request the CC (or COMS) entity at the FT side to send a {CC-NOTIFY} message containing the <<TIMER-RESTART>> information element.

15.6 Call ciphering management

Call ciphering shall be invoked using the MM procedures described in subclause 13.8. Each MM procedure may be used to enable or disable ciphering of one instance of CC or COMS.

When a cipher change is requested, the LLME shall relay the relevant call references (TI plus PD) from the CC to the MM for inclusion in the <<CALL-IDENTITY>> element.

Following successful reception of a cipher request, the receiving side LLME shall immediately invoke ciphering on all relevant MAC connections, and if successful shall mark the connection as ciphered.

The initiating entity shall take no direct action, but shall monitor the ciphering of all relevant MAC connections, and if successful shall mark the connection as ciphered.

Once ciphered, the connection shall only be handed over to a second ciphered connection.

15.7 External Handover

External handover is the process of switching a call in progress from one Fixed Part (FP-1) to another Fixed Part (FP-2). This means the handover occurs between two independent systems, where each system has its own lower layers of protocol and has an independent set of network layer Service Access Points (SAPs). To make external handover possible, a common management entity above the two fixed parts is necessary.

This subclause describes DECT procedures which can be used as part of the CC entity to support external handover. It does not specify how the fixed network performs the handover switching and it does not define the criteria that should be used to decide when to make a handover.

Handover candidate information is required to identify FPs to which external handover may be attempted. The procedures for obtaining handover candidates are defined in subclause 15.7.1. A handover reference (network parameter) is, in general, required to enable the network to re-connect the new DECT connection to the existing call. Procedures for obtaining the handover reference are specified in 15.7.2.

External handover is PP initiated. However, the FP can maintain control by means of the handover candidate and handover reference procedures. The FP may also suggest that a PP initiates an external handover (see subclause 15.7.3).

NOTE: In some configurations, the handover candidate procedures may be combined with the handover reference procedures. However, the combination of these procedures is not suitable for network configurations in which the handover reference depends on the target FP selected by the PP.

The procedures for set-up of a DECT connection to a new FP, and release of the old connection are defined in subclause 15.7.4.

Procedures for ciphering during an external handover are described in subclause 15.7.6.

15.7.1 Handover candidate procedures

15.7.1.1 General

Before external handover can occur, the PP has to obtain handover candidates information from the FP. This enables a PP to determine to which FPs it may make an external handover. The FP may provide synchronisation information, which may enable the PP to establish the new bearer, and re-initiate ciphering more rapidly.

The external handover candidate information may be obtained using either or both of the sub procedures: handover candidate indication (15.7.1.2), and, handover candidate retrieval (15.7.1.3).

15.7.1.2 Handover candidate indication

The FP shall provide the PP with an <<ext h/o indicator>> in {CC-SETUP}, {CC-SETUP-ACK}, {CC-CONNECT}, {CC-INFO}, {LOCATE-ACCEPT} or {MM-INFO-SUGGEST}. Besides candidate FPs, the <<ext h/o indicator>> indicates if the identities of other FPs are available using the handover candidate retrieval procedure.

NOTE: The use of the {CC-INFO} message is preferred if inclusion of handover candidates in {CC-SETUP} would result in segmentation of the message.

Handover candidate information provided in a CC message should be regarded as call specific. Handover candidate information provided in {LOCATE-ACCEPT} or {MM-INFO-SUGGEST} is valid until a change of location area.

Following a successful external handover to a new FP, any external handover candidate information stored in the PP should be considered invalid, and new handover candidate information should be obtained before attempting any further external handovers.

The FP should ensure that the indicated candidate FPs support external handover from the current FP. If the current FP supports encryption, then the FP should ensure that the indicated candidate FPs support encryption.

15.7.1.3 Handover candidate retrieval

The PP shall not invoke this procedure if the external handover bit in the broadcast attributes, is set to 0. If the PP has received an <<ext h/o indicator>> with an OID field set to zero, the PP shall not initiate this procedure.

The PP sends an {MM-INFO-REQUEST} message with an <<info type>> information element indicating "external handover parameters". The information element may more explicitly request "multiframe synchronised external handover candidate", "multiframe, PSCN and multiframe number synchronised external handover candidate", "multiframe and PSCN synchronised external handover candidate" or "non-synchronised external handover candidate". If the PP has identified a possible candidate FP for external handover, this should be indicated in a <<fixed identity>> information element.

NOTE 1: the info types "multiframe synchronised external handover candidate", "multiframe, PSCN and multiframe number synchronised external handover candidate" and "multiframe and PSCN synchronised external handover candidate" are not mutually exclusive. For example, the FP response to a request for "multiframe synchronised external handover candidate" should include FPs from all of the above categories.

The FP should respond with an {MM-INFO-ACCEPT} containing <<info type>> and one or more <<fixed identity>> information elements containing ARIs or PARKs to identify the FPs to which external handover may be attempted. The FP may also include a handover reference in a <<network parameter>> information element.

NOTE 2: If a PARK is included, it identifies (in conjunction with the park length indicator) a range of PARIs (not SARIs or TARIs) which may be targeted for external handover. The PARK{y} included shall only be used for external handover candidate selection; it does not affect location registration. If an ARI is included, it indicates the PARIs (not SARIs or TARIs) of FPs which may be targeted for external handover.

Following a successful external handover to a new FP, any external handover candidate information stored in the PP should be considered invalid, and new handover candidates should be obtained before attempting any further external handovers.

The FP should ensure that the identified candidate FPs support external handover from the current FP. If the current FP supports encryption, then the FP should ensure that the identified candidate FPs support encryption.

The FP may respond with {MM-INFO-REJECT} if it is unable to provide any of the requested information.

15.7.1.4 Target FP selection

A PP shall not attempt external handover unless FP-1 (the current FP) has indicated that the external handover to FP-2 (the candidate FP) will be supported.

NOTE: The external handover bit indicates that external handover is possible to some FPs, but does not specify to which FPs external handover is possible. An indication of external handover supported in the broadcast attributes of a candidate FP does not guarantee that external handover is possible from the current FP.

The PP may determine which FPs it may attempt external handover to by comparing the PARI of the FP in use with the PARIs of other FPs and determining if they match in the bits indicated by the ext h/o length indicator derived from the <<ext h/o indicator>> information element.

If the PP has retrieved the identities of suitable candidate FPs, it may attempt an external handover to the indicated FPs. The retrieved identities indicate the PARIs of FPs which may be used for external handover.

15.7.2 Handover reference procedure

15.7.2.1 General

By default, a PP shall assume that a handover reference is required for external handover. An FP may indicate that a handover reference is not required using a specific coding of the <<network parameter>> information element.

The <<network parameter>> is transferred as described in subclauses 15.7.2.2 and/or 15.7.2.3.

15.7.2.2 Handover reference indication

An FP connected to a network supporting external handover should send <<network parameter>> in a {CC-SETUP}, {CC-SETUP-ACK}, {CC-CONNECT} or {CC-INFO} message.

If no handover reference is required, the FP shall indicate this to the PP by sending the <<network parameter>> information element indicating “Handover reference not required”.

A PP supporting the external handover procedure shall be capable of storing the data in the transmitted <<network parameter>> information element in volatile memory. The minimum PP storage requirement is 10 bytes (11 bytes if discriminator field is included). The PP may be capable of storing more than 10 bytes.

NOTE: The <<network parameter>> information element should be limited in length as much as is practicable.

15.7.2.3 Handover reference retrieval

If the PP wants to initiate an external handover, and has no handover reference, and the PP has not received <<network parameter>> indicating “handover reference not required”, the PP shall retrieve a handover reference prior to initiating the external handover.

NOTE 1 This procedure applies when the PP did not receive the <<network parameter>> during call establishment or when the PP was unable to store the complete handover reference in volatile memory.

The PP shall apply the parameter retrieval procedure as described in subclause 13.7 to retrieve a handover reference from FP-1. The PP shall indicate “handover reference” or “external handover parameters” in the <<info type>> information element within the {MM-INFO-REQUEST}. The PP should include the identity (if available) of its proposed external handover candidate in the {MM-INFO-REQUEST} message. The FP shall respond with a {MM-INFO-ACCEPT} containing a handover reference within the <<network parameter>> information element.

NOTE 2: In some networks, it may not be possible to provide a handover reference until the FP knows the identity of the candidate FP selected by the PP.

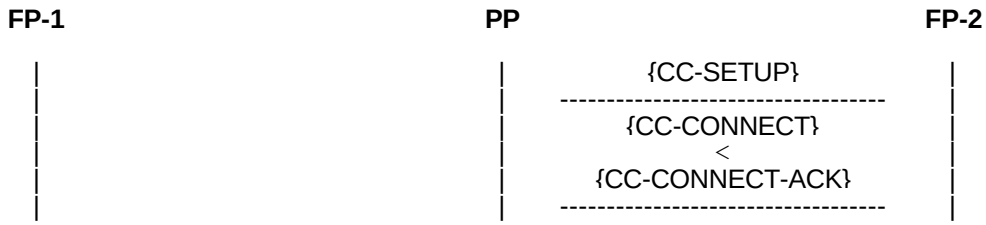
The FP may respond with {MM-INFO-REJECT} if it is unable to provide any of the requested information.

15.7.3 External handover suggested by FP

The FP has the option to propose an external handover by using the FP initiated procedure for parameter retrieval, sending {MM-INFO-SUGGEST} containing all the information (handover reference, handover candidate) necessary to enable the PP to initiate an external handover. The PP should then initiate a handover using the procedures of 15.7.4.

15.7.4 NWK layer set up procedure

In the following description FP-1 is the FP in use prior to handover. FP-2 is the FP in use after handover. It is assumed that the PP already has the necessary FP identities and handover reference.



15.7.4.1 Handover request

The PP shall start the network layer set up procedure by sending to the FP-2 the {CC-SETUP} message indicating in the <<BASIC-SERVICE>> <Call class> field the external handover call setup (coding 1100), and including the <<NETWORK-PARAMETER>> if required.

15.7.4.2 Handover confirm

The FP-2 shall send a {CC-CONNECT} message to the PP, to show confirmation of the handover by the network. FP-2 should start timer <CC.05>.

15.7.4.3 Handover accept

The PP shall send a {CC-CONNECT-ACK} message to the FP-2, to indicate to the network that the PP accepts the handover. On receipt of {CC-CONNECT-ACK} the FP-2 stops timer <CC.05> (if used). If the timer <CC.05> expires before {CC-CONNECT-ACK} is received, the FP-2 should immediately release the new connection following the release procedures defined in subclause 9.5.1.

NOTE: The receipt of {CC-CONNECT-ACK} is used to control the speech path.

15.7.4.4 Handover reject

The FP-2 may reject the handover request by responding with a {CC-RELEASE-COM} to the handover request.

NOTE: Because the connection could revert to FP-1, the PP should not erase the handover candidate/handover reference for use with FP-1 until the external handover is complete.

15.7.4.5 Release of old connection

The release procedure with the FP-1 shall be initiated as soon as the connection with the FP-2 has been established. After the FP-2 has received the {CC-CONNECT-ACK} message, the FP-1 shall initiate the release of the old connection by sending a {CC-RELEASE} message. The PP shall reply with a {CC-RELEASE-COM} message. If the PP has not received the {CC-RELEASE} message from FP-1 N400 seconds after {CC-CONNECT-ACK} message has been sent, it shall release the old link by sending a {CC-RELEASE} message. The {CC-RELEASE} message should contain a <<release reason>> indicating “external handover release“. The FP-1 shall reply with a {CC-RELEASE-COM} message.

15.7.4.6 Handover Fall Back

The PP may cancel the external handover until the {CC-CONNECT-ACK} message has been sent. The PP initiates the release procedure sending a {CC-RELEASE} message to FP-2. The {CC-RELEASE} message should contain a <<release reason>> indicating „external handover release". The FP-2 shall reply with a {CC-RELEASE-COM} message. The PP shall not stop the transmission of U-plane data until the {CC-RELEASE-COM} message is received.

NOTE 1: During the handover procedure, the radio conditions may change such that the PP prefers not to proceed with the handover but remain connected to the FP-1.

NOTE: 2 Because the connection could revert to FP-1, the PP should not erase the handover candidate/handover reference for use with FP-1 until the external handover is complete.

15.7.5 U-plane handling

External handover also involves re-routing the U-plane. The table below shows the recommended receive and transmit path connections for PP and FPs.

Step	Event	Action	PP receive path	PP transmit path	FP receive path
1	PP sends {CC-SETUP}	PP starts transmission on new connection	FP-1	FP-1 and FP-2	FP-1
2	FP-2 sends {CC-CONNECT}	FP-2 starts transmission	FP-1	FP-1 and FP-2	FP-1 or FP-2
3	PP receives {CC-CONNECT}		FP-1	FP-1 and FP-2	FP-1 or FP-2
4	PP sends {CC-CONNECT-ACK}	PP starts receiving on new connection	FP-2	FP-1 and FP-2	FP-1 or FP-2
5	FP-2 receives {CC-CONNECT-ACK}	FP-2 attaches to new connection.	FP-2	FP-1 and FP-2	FP-2
6	PP receives {CC-RELEASE}	PP releases old connection	FP-2	FP-2	FP-2

15.7.6 Ciphering procedure

If the connection to the FP-1 was ciphered, the connection to FP-2 shall also be ciphered. The PP may initiate ciphering at any time but it should do it as soon as possible after receipt of {CC-CONNECT}.

NOTE: The PP may have to delay the initiation of ciphering until the old connection is released if it contains only a single cipher engine.

If the connection to FP-1 was ciphered, and the PP initiated ciphering fails, the connection shall be released by the PP.

If FP-2 initiates ciphering, it shall not send {CIPHER-REQUEST} before {CC-CONNECT-ACK} has been received. If the PP receives {CIPHER-REQUEST} before the old connection is released, and is not able to simultaneously support ciphering on both connections, it may either release the old connection by sending a {CC-RELEASE-COM} message, or switch the old connection to clear mode.

If the connection to FP-1 was ciphered, and the FP-2 initiated ciphering fails, the connection shall be released by FP-2.

Ciphering of the old connection need not be stopped before the setup of the new connection.

For ciphering on the new connection, the same algorithm and key values which were used on the old connection from the PP to the FP-1 may be used. Alternatively a new authentication may be performed, resulting in a new cipher key.

For the description of the procedure see ETS 300 175-5 subclause 13.8.

15.8 Test management procedures

The test management procedures are defined to allow for automatic testing of equipment without requiring manual intervention. These procedures shall be disabled during normal operation, but when provided they shall be active during the test standby mode.

NOTE: The procedures for entering equipment into the test standby mode are defined in ETS 300 175-3 [3].

The following procedures are defined:

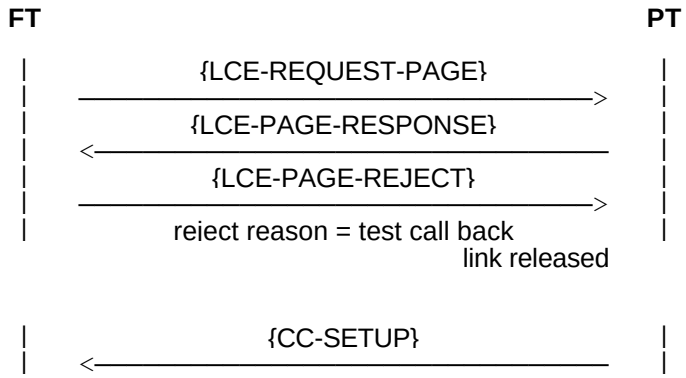
Test call back: the automatic generation of an outgoing call requested by the lower tester.

Test hook control: the remote control of the PTs hook switch by the lower tester. This allows automatic answering of incoming calls and automatic clearing of both incoming and outgoing calls.

Upper tester: the remote invocation of the FTs MM procedures by the lower tester.

15.8.1 Test call back procedure

The test call back procedure is used to request a PT to automatically call back. This is achieved by using the normal paging procedures, and then using {LCE-PAGE-REJECT} message including the <<REJECT-REASON>> element = test call back as below:



Upon receipt of the {LCE-PAGE-REJECT} message including the <<REJECT-REASON>> element = test call back, the PT shall perform the link release procedure as per subclause 14.2.7, and then perform PT initiated call establishment as for a normal/emergency call request depending on the coding of reject reason.

The time taken for the PT to send {CC-SETUP} message upon receipt of the {LCE-PAGE-REJECT} message including the <<REJECT-REASON>> element = test call back shall be less than 10 seconds.

Dialling shall be initiated either as en-bloc or piecewise from the PT depending on the coding of reject reason and whether the PT implements piecewise dialling. Digits dialled shall be as per manufacturers declaration.

15.8.2 Test hook control procedures

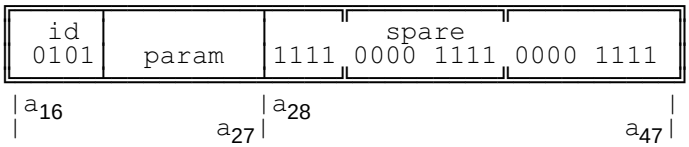
Upon receipt of {CC-INFO} message during PT Call Control (CC) state T07 containing the <<TEST-HOOK-CONTROL>> element indicating hook value "off-hook", the PT shall act as though a MNCC_CONNECT-req primitive had been received and shall respond according to the procedures defined in subclause 9.3.2.8.

Upon receipt of a {CC-INFO} message during PT Call Control (CC) states T02, T03, T04, T10, T08 containing a <<TEST-HOOK-CONTROL>> element indicating hook value "on-hook", the PT shall act as though a MNCC_RELEASE-req primitive had been received and shall release the call according to the procedures defined in subclause 9.5.1.

15.8.3 Upper tester procedure

The upper tester procedure is used to invoke FT MM procedures as requested by the lower tester. This procedure should be implemented in the case where the MM procedures can not be invoked by other means at the test house (as declared by the manufacturer).

The LLME receives from the MAC layer the MAC test message {NETWORK-TEST}. Refer to ETS 300 175-3 [3]. The coding of this message is defined below:



where: "id" indicates a NWK layer test message;
"a_{ii}" indicates the bit positions in the MAC message.

param	MM procedure invoked
0000 1100	Identification of PT
0000 1110	Temporary identity assignment
0000 0000	Authentication of PT
0000 0001	Authentication of user
0000 1010	Location update
0000 0100	Terminating access rights (FT initiated)
0000 0010	Key allocation
0000 1000	Parameter retrieval (info-suggest)
0000 0110	Ciphering (cipher-request)
other codes	reserved

Upon receipt of the MAC test message, the LLME shall unconditionally invoke the indicated MM procedure within 2 seconds, by proceeding as though the equivalent MM primitive had been received. The MM procedure invoked shall use parameters as per manufacturers declaration.

16 Primitives

16.1 Primitive types

Four primitive types may be used:

-req (request)
for a higher layer to request service from a lower layer;

-cfm (confirm)
for the layer providing the service to confirm that the activity has been completed;

-ind (indication)
for a layer providing a service to notify the next higher layer of any specific service related activity;

-res (response)
for a layer to acknowledge receipt of an indication primitive from the next lower layer.

The defined types for each category of primitive are shown as a list in curly brackets.

EXAMPLE: 7 MNCC_RELEASE- {req,cfm,ind }.

In this example, the defined types are request, confirm and indicate (but not response).

NOTE: These primitives are defined only for the purpose of describing layer-to-layer interactions. The primitives are defined as an abstract list of parameters, and their concrete realisation may vary between implementations. No formal testing of primitives is intended. The following primitive definitions have no normative significance.

16.2 Primitives to lower layer (DLC layer)

The primitives used for communication to the DLC layer are described in ETS 300 175-4 [4].

16.3 Primitives to IWU

This subclause summarises the primitives between the interworking unit and the NWK layer together with the list of associated parameters.

16.3.1 Parameter definitions

Endpoint identifiers: all primitives shall contain an endpoint identifier. This identifier shall be used to distinguish primitives related to different instances of call. The coding and use of these identifiers is a local matter, and is not defined in this ETS. An identifier is defined for each entity as follows:

- Call Control Endpoint Identifier (CCEI);
- Supplementary Services Endpoint Identifier;
- COMS Endpoint Identifier (COEI);
- CLMS Endpoint Identifier (CLEI);
- Mobility Management Endpoint Identifier.

Message unit: each piece of higher layer (peer-to-peer) information that is included in the primitive is called a message unit. A series of one or more message units may be associated with each primitive where each separate unit is related to one information element in the corresponding NWK layer message. The list of message units is derived from the message definitions (clause 6) by reference to the information elements that may contain information from (or to) the IWU.

NOTE: The operations across the IWU/NWK layer boundary should be such that a layer sending a message can assume a temporal order of the bits within the message unit, and that the layer receiving the primitive can reconstruct the message with its assumed temporal order.

16.3.2 MNCC primitives

The following primitives are used:

1 MNCC_SETUP- {req, ind };
2 MNCC_SETUP_ACK- {req, ind };
3 MNCC_REJECT- {req, ind };
4 MNCC_CALL_PROC- {req, ind };
5 MNCC_ALERT- {req, ind };
6 MNCC_CONNECT- {req, cfm, ind };
7 MNCC_RELEASE- {req, cfm, ind, res };
8 MNCC_FACILITY- {req, ind };
9 MNCC_INFO- {req, ind };
10 MNCC_INFO- {req, cfm, ind };
11 MNCC_HOLD- {req, ind };
12 MNCC_RETRIEVE- {req, ind };
13 MNCC_IWU_INFO- {req, ind }.

16.3.2.1 MNCC_SETUP primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Basic Service	A	-	A	-
IWU attributes	O	-	O	-
Cipher info	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Signal	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
Terminal capability	O	-	O	-
End-to-end compatibility	O	-	O	-
Rate parameters	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
Calling party number	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
Sending complete	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.2 MNCC_SETUP_ACK primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Info type	O	-	O	-
Location area	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
Delimiter request	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.3 MNCC_REJECT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Cause	N	-	A	-
Message units (possible elements)				
Release reason	A	-	A	-
Identity type	O	-	O	-
Location area	O	-	O	-
IWU attributes	O	-	O	-
Facility	O	-	O	-
Display	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

The "cause" parameter shall indicate one of the following values:

- peer message (a valid peer message was received);
- local timer expiry (a local timer has expired).

The coding of this parameter is a local matter and is not specified in this ETS.

16.3.2.4 MNCC_CALL_PROC primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.5 MNCC_ALERT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Terminal capability	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.6 MNCC_CONNECT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	-
Message units (possible elements)				
Facility	O	N	O	-
Progress indicator	O	N	O	-
Display	O	O	O	-
Signal	O	N	O	-
Feature indicate	O	O	O	-
Terminal capability	O	N	O	-
Transit delay	O	N	O	-
Window size	O	N	O	-
IWU-to-IWU	O	O	O	-
IWU-packet	O	O	O	-

A = Always;
O = Optional;
"-" = not applicable;
N = Not allowed.

16.3.2.7 MNCC_RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Cause	N	A	N	N
Message units (possible elements)				
Release reason	O	O	O	O
Identity type	N	O	N	O
Location area	N	O	N	O
IWU attributes	N	O	N	O
Facility	O	O	O	O
Display	O	O	O	O
Feature indicate	O	O	O	O
Network parameter	N	O	N	O
IWU-to-IWU	O	O	O	O
IWU-packet	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

The "cause" parameter shall indicate one of the following values:

- peer message (a valid peer message was received);
- local timer expiry (a local timer has expired).

The coding of this parameter is a local matter and is not specified in this ETS.

16.3.2.8 MNCC_FACILITY primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.9 MNCC_INFO primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Location area	O	-	O	-
NWK assigned identity	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Signal	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
Sending complete	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.2.10 MNCC_MODIFY primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	-
Success/Failure flag	N	A	A	-
Message units (possible elements)				
Service change info	A	O	A	-

A = Always;
O = Optional;
"-" = not applicable.

The Success/Failure flag shall indicate the outcome of the service modification.

16.3.2.11 MNCC_HOLD primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Message units (possible elements)				
Display	O	O	O	O
Reject reason	N	O	N	O

A = Always;
O = Optional;
N = Not allowed.

16.3.2.12 MNCC_RETRIEVE primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Message units (possible elements)				
Display	O	O	O	O
Reject reason	N	O	N	O

A = Always;
O = Optional;
N = Not allowed.

16.3.2.13 MNCC_IWU_INFO primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Alphanumeric	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.3 MNSS primitives

The following primitives are used:

1 MNSS_SETUP- {req, ind };
2 MNSS_FACILITY- {req, ind };
3 MNSS_RELEASE- {req, ind }.

16.3.3.1 MNSS_SETUP primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)				
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.3.2 MNSS_FACILITY primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)				
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.3.3 MNSS_RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)				
Release reason	O	-	O	-
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.4 MNCO primitives

The following primitives are used:

1 MNCO_SETUP- {req, ind };
2 MNCO_CONNECT- {req, ind };
3 MNCO_INFO- {req, ind };
4 MNCO_ACK { ind };
5 MNCO_RELEASE- {req, cfm, ind }.

16.3.4.1 MNCO_SETUP primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)				
IWU attributes	A	-	A	-
Display	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.4.2 MNCO_CONNECT primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)				
Display	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.4.3 MNCO_INFO primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)				
Display	O	-	O	-
Alphanumeric	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.4.4 MNCO_ACK primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	-	-	A	-
Message units (possible elements)				
Display	-	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.4.5 MNCO_RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	A	A	-
Message units (possible elements)				
Release reason	O	O	O	-
Display	O	O	O	-
IWU-TO-IWU	O	O	O	-
IWU-packet	O	O	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.5 MNCL primitives

The following primitives are used:

1 MNCL_UNITDATA- {req, ind }.

16.3.5.1 MNCL_UNITDATA primitive

PARAMETER	REQ	CFM	IND	RES
CLMS Endpoint Identifier (CLEI)	A	-	A	-
CLMS Message type (note 1)	A	-	A	-
Message units (possible elements)				
Alphanumeric	O	-	O	-
IWU-TO-IWU (note 2)	O	-	O	-
IWU-packet (note 2)	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

NOTE 1: The CLMS message type parameter specifies the message format to be used, fixed or variable.

NOTE 2: If the CLMS message type is fixed, then only the Alphanumeric message unit is used.

16.3.6 MM primitives

The following primitives are used:

1	MM_IDENTITY	{req, cfm, ind, res };
2	MM_IDENTITY_ASSIGN	{req, cfm, ind, res };
3	MM_AUTHENTICATE	{req, cfm, ind, res };
4	MM_LOCATE	{req, cfm, ind, res };
5	MM_DETACH	{req, ind, };
6	MM_ACCESS_RIGHTS	{req, cfm, ind, res };
7	MM_ACCESS_RIGHTS_TERMINATE	{req, cfm, ind, res };
8	MM_KEY_ALLOCATE	{req, ind, };
9	MM_INFO	{req, cfm, ind, res };
10	MM_CIPHER	{req, cfm, ind, res }.

16.3.6.1 MM_IDENTITY primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Message units (possible elements)				
Identity type	A	N	A	N
Portable identity	N	O	N	O
Fixed identity	N	O	N	O
NWK assigned identity	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

16.3.6.2 MM_IDENTITY_ASSIGN primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	N
Message units (possible elements)				
Portable identity	O	N	O	N
NWK assigned identity	O	N	O	N
Duration	O	N	O	N
Reject reason	N	O	N	O
IWU-TO-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.3 MM_AUTHENTICATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
AUTH-TYPE	A	O	A	O
RAND	A	N	A	N
RES	O	O	O	O
RS	O	O	O	O
Cipher info	O	O	O	O
ZAP field	N	O	N	O
Service class	N	O	N	O
Key	N	O	N	O
Reject reason	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.4 MM_LOCATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
Portable identity	A	O	A	O
Fixed identity	O	N	O	N
Location area	O	O	O	O
NWK assigned identity	O	O	O	O
Cipher info	O	N	O	N
Reject reason	N	O	N	O
Set-up capability	O	N	O	N
Terminal capability	O	N	O	N
Duration	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.5 MM_DETACH primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	-	A	-
Message units (possible elements)				
Portable identity	A	-	A	-
NWK assigned identity	O	-	O	-
IWU-TO-IWU	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable.

16.3.6.6 MM_ACCESS_RIGHTS primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
Portable identity	A	O	A	O
Fixed identity	N	O	N	O
Location area	N	O	N	O
AUTH-TYPE	O	O	O	O
Cipher info	O	O	O	O
Terminal capability	O	N	O	N
ZAP field	N	O	N	O
Service class	N	O	N	O
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.7 MM_ACCESS_RIGHTS_TERMINATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
Portable identity	A	N	A	N
Fixed identity	O	N	O	N
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-to-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.8 MM_KEY_ALLOCATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	-	A	-
Message units (possible elements)				
Allocate type	A	-	A	-
RAND	A	-	A	-
RS	A	-	A	-

A = Always;
"-" = not applicable.

16.3.6.9 MM_INFO primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
Info type	A	O	A	O
Portable identity	O	N	O	N
Fixed identity	O	O	O	O
Location area	O	O	O	O
NWK assigned identity	O	O	O	O
Network parameter	O	O	O	O
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-to-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.10 MM_CIPHER primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (note)	N	A	N	A
Message units (possible elements)				
Cipher info	A	O	A	O
Call identity	O	N	O	N
Connection identity	O	N	O	N
Reject reason	N	O	N	O
IWU-to-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

17 Handling of error and exception conditions

All procedures transferring signalling information by using the values of protocol discriminators defined in this ETS (see subclause 7.2) are applicable only to those messages which pass the checks described in subclauses 17.1 through 17.7.

Detailed error and exception handling procedures are implementation dependent and may vary. However, capabilities facilitating the orderly treatment of error or/and exception conditions are provided for in this section and shall be provided in each implementation.

Subclauses 17.1 through 17.7 are listed in order of precedence.

17.1 Protocol discrimination error

When a message is received with a protocol discriminator value that indicates a service that is not supported by the receiving entity, or that is coded as "unknown protocol entity", that message shall be ignored. "Ignore" means to do nothing, as if the message had never been received.

NOTE: Messages using the protocol discriminator values "unknown protocol entity" are expected to be routed to external (application specific) protocols. However, such coding represents an exception with regard to the protocols defined in this ETS.

17.2 Message too short

When a message is received that is too short to contain a complete <<MESSAGE-TYPE>> information element, that message shall be ignored.

17.3 Transaction identifier error

17.3.1 Illegal and unsupported transaction identifier value

If the transaction identifier information element octet 1, bits 7 to 5 indicate an illegal value for the transaction value (i.e. a value that is not allowed in subclause 7.3),, then the message shall be ignored.

If the transaction identifier information element octet 1, bits 7 to 5 indicate the reserved value for TV extension, and if extended TVs are not supported by the receiving equipment, then the message shall be ignored.

17.3.2 Transaction identifier procedural errors and exception conditions

17.3.2.1 Unknown active CC call

Whenever any message except {CC-SETUP}, {CC-RELEASE}, {CC-RELEASE-COM} or (for FPs or PPs supporting the service change procedures of subclause 9.6) {CC-SERVICE-CHANGE} is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, clearing should be initiated by sending a {CC-RELEASE-COM} message with release reason "unknown transaction identifier", using the same (unknown) transaction identifier in the returned message.

When a {CC-RELEASE} or a {CC-RELEASE-COM} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, no action should be taken.

When a {CC-SETUP} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, and with a transaction identifier flag incorrectly set to "1", this message shall be ignored.

When a {CC-SERVICE-CHANGE} message is received specifying a transaction identifier which is not recognised as relating to an active call, this message shall be ignored.

When a {CC-SETUP} message is received specifying a transaction identifier which is recognised as relating to an active call or to a call in progress, this {CC-SETUP} message shall be ignored.

17.3.2.2 Unknown active CISS call

Whenever a CISS entity receives a {FACILITY} message specifying a transaction identifier which is not recognised as relating to an active CISS-call or to a call in progress, clearing is initiated by sending a {CISS-RELEASE-COM} message with release reason "unknown transaction identifier", using the same (unknown) transaction identifier in the returned message.

17.3.2.3 Unknown active COMS call

Whenever any message except {COMS-RELEASE} or {COMS-RELEASE-COM} is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, clearing shall be initiated by sending a {COMS-RELEASE-COM} message with release reason "unknown transaction identifier", using the same (unknown) transaction identifier in the returned message.

When a {COMS-RELEASE} or a {COMS-RELEASE-COM} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, no action should be taken.

17.3.2.4 Unknown active CLMS call

Not applicable (there is no "ACTIVE" state for a CLMS call).

17.3.2.5 Unknown active MM transaction

Whenever a MM message is received neither specifying a transaction identifier which is recognised as relating to an initiated MM procedure nor being an allowed message initiating a new MM procedure, then this message should be ignored.

17.3.2.6 Unknown active LCE transaction

When a {LCE-PAGE-RESPONSE} message is received with a transaction identifier flag incorrectly set to “1”, this message should be ignored.

17.3.3 Call Resource Contention

When a {CC-SETUP} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress , one of two conditional actions shall be taken:

- if the resources exist to service the received call setup request, the request shall be handled as specified in subclauses 9.3.1 and 9.3.2.

- if the resources do not exist to service the received call setup request, the request shall be rejected by sending a {CC-RELEASE-COM} message which should contain the release reason "insufficient resources", using the same (unknown) transaction value in the returned message.

17.4 Message type or message sequence errors

17.4.1 CC message error

Whenever an unexpected message, except {CC-RELEASE} or {CC-RELEASE-COM}, or an unrecognised message is received in any state, the message shall be ignored. Therefore no alternative abnormal release is allowed.

When an unexpected {CC-RELEASE} message is received (e.g. if a previous message was corrupted by undetected transmission errors), the message shall not be ignored, and the normal release procedures as specified in subclause 9.5.1 shall be followed.

When an unexpected {CC-RELEASE-COM} message is received, the message shall not be ignored, and the abnormal release procedures as specified in subclause 9.5.2 shall be followed.

17.4.2 CISS message error

Whenever an unexpected message, or an unrecognised message is received in any state, the message should be ignored.

17.4.3 COMS or CLMS message error

Whenever an unexpected message, or an unrecognised message is received in any state, the message should be ignored.

17.4.4 MM message error

Whenever an unexpected message, or an unrecognised message is received in any state, the message should be ignored.

17.4.5 LCE message error

Whenever an unrecognised message is received, it should be ignored.

17.5 General information element errors

The general information element error procedures may also apply to information elements in codesets other than codeset "0". In that case, the release reason information element defined for codeset "0" may be used to indicate errors in information elements other than those in codeset "0" by applying the locking or non-locking shift procedures as described in subclause 7.5.4.

17.5.1 Information element out of sequence

A variable length information element which has a code value lower than the code value of the variable length information element preceding it shall be considered as an out of sequence information element.

If a message is received that contains an out of sequence information element, this information element may be ignored, and the receiving entity may continue to process the message. If this information is mandatory, and the receiving entity chooses to ignore this out of sequence information element, then the error handling procedure for missing mandatory information elements as described in subclause 17.6.1 shall be followed. If the ignored information element is non-mandatory, the receiving entity shall continue to process the message.

NOTE: An implementation may choose to process all the information elements received in a message regardless of the order in which they are placed.

17.5.2 Duplicated information elements

If an information element is repeated in a message in which repetition of the information element is not expected, only the contents of information element appearing first shall be handled and all subsequent repetitions of the information element shall be ignored. When repetition of the information elements is permitted, only the contents of permitted information elements shall be handled. If the limit on repetition of information elements is exceeded, the contents of information elements appearing first up to the limit of repetitions shall be handled and all subsequent repetitions of the information element shall be ignored.

17.6 Mandatory information element errors

17.6.1 Mandatory information element missing in CC messages

When a message other than {CC-SETUP}, CC-RELEASE} or {CC-RELEASE-COM} is received which has one or more mandatory information elements missing, the normal release procedure as described in subclause 9.5.1 should be invoked. In this case, the {CC-RELEASE} message should use the release reason "mandatory information element missing".

Alternatively, the receiving entity may choose to maintain the call in which case no action should be taken on the message and no state change should occur.

When a {CC-SETUP} or {CC-RELEASE} message is received which has one or more mandatory information elements missing, a {CC-RELEASE-COM} message with release reason set to "mandatory information element missing" should be returned.

When a {CC-RELEASE-COM} message is received with a <<RELEASE-REASON>> information element missing, it shall be assumed that a {CC-RELEASE-COM} message was received with release reason "normal".

17.6.2 Mandatory information element content error in CC messages

When a message other than {CC-SETUP}, {CC-RELEASE} or {CC-RELEASE-COM} is received which has one or more mandatory information elements with invalid content, the normal release procedure as described in subclause 9.5.1 should be invoked. In this case the {CC-RELEASE} message should use the release reason "invalid information element contents".

Alternatively, the receiving entity may choose to maintain the call in which case no action should be taken on the message and no state change should occur.

When a {CC-SETUP} or {CC-RELEASE} message is received which has one or more mandatory information elements with invalid content, a {CC-RELEASE-COM} message shall be returned. The message should indicate release reason "invalid information element contents" .

When a {CC-RELEASE-COM} message is received with invalid content of the <<RELEASE-REASON>> information element, it will be assumed that a {CC-RELEASE-COM} message was received with release reason "normal".

This subclause shall also apply to mandatory information elements with a length exceeding the maximum length (as given in clause 6).

17.6.3 Mandatory information element error in COMS or CLMS messages

When a message is received which has one or more mandatory information elements missing or has one or more mandatory information elements with invalid content, the message should be ignored.

Alternatively, when a {COMS-SETUP} message is received which has one or more mandatory information elements missing or with invalid content, a {COMS-RELEASE-COM} message with release reason "mandatory information element missing" or "invalid information element contents" as appropriate may be returned.

17.6.4 Mandatory information element error in MM messages

When a message is received which has one or more mandatory information elements missing or has one or more mandatory information elements with invalid content, the message should be ignored.

However, if the received message was a {TEMPORARY-IDENTITY-ASSIGN}, {AUTHENTICATION-REQUEST}, {LOCATE-REQUEST}, {ACCESS-RIGHTS-REQUEST}, {ACCESS-RIGHTS-TERMINATE-REQUEST}, {MM-INFO-REQUEST} or {CIPHER-REQUEST} message, then the corresponding reject message should be returned with the reject reason indicating "information element error" in the case of a missing mandatory information element, or indicating "invalid information element contents" in the case of a mandatory information element with a content error.

17.6.5 Mandatory information element error in LCE messages

When a message is received which has one or more mandatory information elements missing or has one or more mandatory information elements with invalid content, the message should be ignored.

However, if the received message is {LCE-PAGE-RESPONSE}, clearing shall be initiated by sending a {LCE-PAGE-REJECT} message.

17.7 Non-mandatory information element errors

The following subclauses identify actions on information elements not recognised as mandatory.

17.7.1 Unrecognised information element

Action shall only be taken on the message and those information elements which are recognised and have valid content.

Subsequent actions in the event of an unrecognised information element are therefore determined by the sender of the unrecognised information elements.

17.7.2 Non-mandatory information element content error

When a message is received which has one or more non-mandatory information elements with invalid content, action shall only be taken on the message and those information elements which are recognised and have valid content. All other elements shall be discarded.

This subclause shall also apply to non-mandatory information elements with a length exceeding the maximum length (as given in clause 6).

There are two exception to this treatment. The <<IWU-TO-IWU>> and <<IWU-PACKET>> information elements may be truncated and processed.

NOTE: The length of the <<IWU-TO-IWU>> and <<IWU-PACKET>> elements is variable up to several octets. These elements are deliberately placed at the end of all appropriate messages, such that they will be the first elements to suffer truncation in the event of buffer overflow.

17.8 Data link reset

Whenever the LCE is informed of a spontaneous data link layer reset by means of the DL_ESTABLISH-ind primitive, the following procedures apply:

a) for CC calls in the "OVERLAP SENDING" and "OVERLAP RECEIVING" states, the entity shall initiate the normal release procedures as given in subclause 9.5.1. with release reason "unknown";

b) for CC calls in the "ACTIVE", "RELEASE PENDING" or "NULL" states no action shall be taken;

c) for CC calls in the remaining establishment phase (states T-01, T-03, T-04, T-05, T-06, T-07, T-08, T-23 and F-01, F-03, F-04, F-06, F-07, F-23) and in any of the service change states, the call shall be maintained subject to the procedures contained in clause 9;

d) for MM transactions, the transaction shall be maintained subject to the procedures contained in clause 13.

17.9 Data link failure

Whenever a LCE is notified by its data link entity via the DL_RELEASE-ind primitive that there is a data link layer failure, the following procedure shall apply:

a) any calls not in the "ACTIVE" state shall be cleared internally;

b) if the DL_RELEASE-ind primitive indicates "normal" release, any calls in the "ACTIVE" state shall also be cleared internally;

c) if the DL_RELEASE-ind primitive indicates "abnormal" release, any calls in the "ACTIVE" state may be maintained, in which case the LCE should request link re-establishment from the DLC layer.

In case c), if the LCE requests DLC link re-establishment, it shall do this immediately by sending a DL_ESTABLISH-req primitive and shall start timer <LCE.04>. This shall only occur if at least one call is in the "ACTIVE" state. Otherwise, the LCE shall clear internally.

If timer <LCE.04> is already running, it shall not be restarted.

NOTE: If the transfer mode of the call is circuit-mode, the LCE may nonetheless choose to clear the call. If the transfer mode of the call is packet mode and the MAC layer is recognised as normal in spite of the data link failure, the LCE should not clear the call and should request data link re-establishment.

When informed of a successful DLC link re-establishment by means of the DL_ESTABLISH-cfm primitive, the LCE shall stop timer <LCE.04>.

If timer <LCE.04> expires prior to DLC link re-establishment, the LCE shall clear all of the associated calls.

Annex A (normative): System parameters

A.1 CC timers

All CC running timers except <CC.02> shall in addition to the conditions defined below be stopped upon following events:

- the <CC.02> timer is started;

- a {CC-RELEASE-COM} message is received or sent;

- the LCE is notified by the DLC via the DLC-RELEASE-ind primitive that there is a data link failure.

When a timer is restarted by the means of a {CC-NOTIFY} message indicating "Timer restart" the timer shall be stopped and started from its initial value.

<CC.01>	Overlap sending timer.
FT value:	20 seconds.
PT value:	Not used.
Start:	An incomplete called party number is received.
Stop:	A complete called party number is received.

<CC.02>	CC release timer.
FT value:	36 seconds.
PT value:	36 seconds.
Start:	A {CC-RELEASE} message is sent.
Stop:	A {CC-RELEASE-COM} message is received.

<CC.03>	CC set-up timer.
FT value:	20 seconds.
PT value:	20 seconds.
Start:	A {CC-SETUP} message has been sent.
Stop:	An response message has been received.

<CC.04>	CC completion timer.
FT value:	100 seconds.
PT value:	100 seconds.
Start:	Refer to subclause 9.3.
Stop:	Refer to subclause 9.3.

<CC.05>	CC connect timer.
FT value:	Not used.
PT value:	10 seconds.
Start:	A {CC-CONNECT} message has been sent.
Stop:	A {CC-CONNECT-ACK} message is received.

A.2 SS timers

No timers defined.

A.3 COMS timers

<COMS.00> COMS storage timer.
FT value: 5 seconds.
PT value: 5 seconds.
Start: The first segment of a segmented message is received.
Stop: The last segment is received.

<COMS.01> COMS information acknowledge.
FT value: 2 seconds.
PT value: 2 seconds.
Start: A {COMS-INFO} message is sent.
Stop: A {COMS-ACK} message is received.

<COMS.02> COMS release timer.
FT value: 10 seconds.
PT value: 10 seconds.
Start: A {COMS-RELEASE} message is sent.
Stop: A {COMS-RELEASE-COM} message is received.

<COMS.03> COMS set-up timer.
FT value: 10 seconds.
PT value: 10 seconds.
Start: A {COMS-SETUP} message has been sent.
Stop: An response message has been received.

A.4 CLMS timer

<CLMS.00> CLMS storage timer.
FT value: 5 seconds.
PT value: 5 seconds.
Start: The first segment of a segmented message has been received.
Stop: The last segment is received.

A.5 MM timers

In addition to the conditions defined below an MM running timer except <MM_wait> shall also be stopped upon following events:

- a valid MM message has been received initiating a higher priority MM procedure, see subclause 15.5;

- the LCE is notified by the DLC via the DLC-RELEASE-ind primitive that there is a data link failure;

- applicable to PT only: PT sends an {AUTHENTICATION-REQUEST} message initiating the FT authentication procedure when another PT initiated MM procedure different from authentication of FT is still running.

In the case of a higher priority MM procedure interrupting a lower priority one the timer of the lower priority procedure shall be restarted on completion of the higher priority procedure starting from its initial value.

<MM_access.1> Access rights timer.
FT value: None.
PT value: 60 seconds.
Start: An {ACCESS-RIGHTS-REQUEST} message is sent.
Stop: An {ACCESS-RIGHTS-ACCEPT} message or an {ACCESS-RIGHTS-REJECT} message is received.

<MM_access.2> Access rights termination timer.
FT value: 10 seconds.
PT value: 20 seconds.
Start: An {ACCESS-RIGHTS-TERMINATE-REQUEST} message is sent.
Stop: An {ACCESS-RIGHTS-TERMINATE-ACCEPT} message or an {ACCESS-RIGHTS-TERMINATE-REJECT} message is received.

<MM_auth.1> PT or FT authentication timer.
FT value: 10 seconds.
PT value: 10 seconds.
Start: An {AUTHENTICATION-REQUEST} message is sent.
Stop: An {AUTHENTICATION-REPLY} message or an {AUTHENTICATION-REJECT} message is received.

<MM_auth.2> User authentication timer.
FT value: 100 seconds.
PT value: 100 seconds.
Start: An {AUTHENTICATION-REQUEST} message is sent.
Stop: An {AUTHENTICATION-REPLY} message or an {AUTHENTICATION-REJECT} message is received.

<MM_cipher.1> FT cipher-switching timer.
FT value: 10 seconds.
PT value: None.
Start: A {CIPHER-REQUEST} message is sent.
Stop: A {CIPHER-REJECT} message or a DL_ENC_KEY-ind primitive is received.

<MM_cipher.2> PT cipher-switching timer.
FT value: None.
PT value: 10 seconds.
Start: A {CIPHER-SUGGEST} message is sent.
Stop: A {CIPHER-REQUEST} message or a {CIPHER-REJECT} message is received.

<MM_ident.1> Temporary identity PUI assignment timer.
FT value: 10 seconds.
PT value: None.
Start: A {TEMPORARY-IDENTITY-ASSIGN} message is sent.
Stop: A {TEMPORARY-IDENTITY-ASSIGN-ACK} message is received.

<MM_ident.2> Identification timer.
FT value: 10 seconds.
PT value: None.
Start: An {IDENTITY-REQUEST} message is sent.
Stop: An {IDENTITY-REPLY} message is received.

<MM_key.1> Key allocation timer.
FT value: 10 seconds.
PT value: None.
Start: A {KEY-ALLOCATE} message is sent.
Stop: An {AUTHENTICATION-REQUEST} message is received.

<MM_locate.1> Location timer.
FT value: None.
PT value: 20 seconds.
Start: A {LOCATE-REQUEST} message is sent.
Stop: A {LOCATE-ACCEPT} message or a {LOCATE-REJECT} message is received.

<MM_wait> Re-attempt timer.
FT value: None.
PT value: 5 minutes.

A.6 LCE timers

<LCE.01>	Link release timer.
FT value:	5 seconds.
PT value:	5 seconds.
Start:	A DL_RELEASE-req primitive is sent.
Stop:	A DL_RELEASE-cfm primitive is received.

<LCE.02>	Link maintain timer.
FT value:	10 seconds maximum.
PT value:	10 seconds maximum.
Start:	A higher entity indicates partial release to the LCE.
Stop:	

<LCE.03>	{LCE-REQUEST-PAGE} message resubmission timer.
FT value:	3 seconds.
PT value:	None.
Start:	A {LCE-REQUEST-PAGE} message has been sent.
Stop:	A matching response is received.

<LCE.04>	Link suspend and resume timer.
FT value:	5 seconds.
PT value:	5 seconds.
Start:	A link suspend or a link resume has been requested.
Stop:	A matching response is received.

<LCE.05>	DLC establish without SDU timer.
FT value:	5 seconds.
PT value:	None.
Start:	A DLC data link has been established after reception of a DL_ESTABLISH-ind without an SDU.
Stop:	A new higher entity message or a DL_DATA-ind with an SDU is received.

A.7 NWK layer constants

N300: resubmission of an indirect link establish message.
N300 is an application specific value.
Recommended value for voice applications is 3.

N400: external handover release pending value.
Mandated value is 5.

A.8 Restart

Restart of a timer means restart from its initial value.

Annex B (normative): CC state transition tables

B.1 CC state transitions at PT side

B.1.1 CC state table at PT side

Table B.1: CC state table at PT side

EVENT (CC message)		STARTING STATE										END STATE
		T00	T01	T02	T03	T04	T06	T07	T08	T10	T19	
{CC-SETUP}	sent	P01										T01
{CC-SETUP}	rcvd	P08										T06
{CC-SETUP-ACK}	rcvd		P03									T02
{CC-CALL-PROC}	rcvd		P05	P05								T03
{CC-ALERTING}	rcvd		P06	P06	P06							T04
{CC-CONNECT}	rcvd		P07	P07	P07	P07						T10
{CC-CONNECT-ACK}	rcvd								P11			T10
{CC-SETUP}	accept						P09					T07
{CC-CONNECT}	sent						P10	P10				T08
{CC-INFO}	rcvd			P12	P12	P12		P12	P12	P12	P19	*
{CC-INFO}	sent			P04	P12	P12		P12	P12	P12		*
{CC-RELEASE}	sent		P13	P13	P13	P13		P13	P13	P13		T19
{CC-RELEASE}	rcvd			P20	P20	P20	P20	P20	P20	P20	P22	* T00
{CC-RELEASE-COM}	rcvd		P14	P14	P14	P14	P14	P14	P14	P14	P22	T00
{CC-RELEASE-COM} (reject)	sent						P16					T00
{CC-RELEASE-COM} (response)	sent			P21	P21	P21	P21	P21	P21	P21		T00
{CC-NOTIFY}	rcvd		P18	P18	P18	P18			P18			*
TIMEOUT				P17	P17	P17			P17			T19
RELEASE TIMEOUT											P15	T00
SETUP TIMEOUT			P27									T00

An entry "*" in the END STATE column indicates current state maintained. All unspecified events (blank entries in the above table) shall be treated according to the normal procedures given in clause 9 where defined. If not defined they shall be treated according to subclause 17.4 (handling of errors for unexpected messages).

NOTE 1: States T-22 and T-23 are for further study.

NOTE 2: The PT may send CRSS ({FACILITY}) messages when in the CC state F-19. This will allow the user and network to initiate (and correspondingly acknowledge) supplementary services during call release procedure (e.g. advice of charge requested at the termination of the call).

B.1.2 CC transition procedures at PT side

P01: MNCC_SETUP-req primitive received.
{CC-SETUP} message sent. Next state T-01.

P03: {CC-SETUP-ACK} message received. Next state T-02.
EITHER: start PT generated "dial" tone if provided;
install and connect the receive U-plane.

P04: Stop PT generated "dial" tone after first digit sent.
Send further digits. State T-02 maintained.

P05: {CC-CALL-PROC} message received. Next state T-03.

P06: {CC-ALERTING} message received. Next state T-04.
EITHER: start PT generated "called party alerting" tone;
continue to connect receive U-plane.

P07: {CC-CONNECT} message received.
Stop PT generated "called party alerting" tone.
Connect U-plane. Next state T-10.

P08: {CC-SETUP} message received.
Issue MNCC_SETUP-ind primitive. Next state T-06.

P09: MNCC_ALERT-req primitive received (user alerting has started).
Send {CC-ALERTING} message. Next state T-07.

P10: MNCC_CONNECT-req primitive received (e.g. user responds).
Send {CC-CONNECT} message. Next state T-08.

P11: {CC-CONNECT-ACK} message received. Connect U-plane (if not already connected).
Next state T-10.

P12: MNCC_INFO-req received; Send {CC-INFO} message.
or {CC-INFO} message received: issue MNCC_INFO-ind.
Current state maintained.

P13: MNCC_RELEASE-req primitive received.
{CC-RELEASE} message sent. Clear call.
Next state T-19.

P14: Receive {CC-RELEASE-COM} message.
Issue MNCC_REJECT-ind primitive. Clear call. Next state T-00.

P15: Release time-out. Send {CC-RELEASE-COM} message.
Issue MNCC_RELEASE-cfm primitive. Clear call. Next state T-00.

P16: Call rejected or MNCC_REJECT-req primitive received.
Send {CC-RELEASE-COM} message.
Clear call. Next state T-00.

P17: Send {CC-RELEASE} message. Reason = "timer expiry".
Next state T-19.

P18: {CC-NOTIFY} received. Issue MNCC-NOTIFY-ind primitive.
Current state maintained.

P19: {CC-INFO} received. Issue MNCC_INFO primitive. Next state T-19.

P20: {CC-RELEASE} message received. Issue MNCC_RELEASE-ind primitive.
Current state maintained.

P21: MNCC_RELEASE-res primitive received.
Send {CC-RELEASE-COM} message. Clear call. Next state T-00.

P22: {CC-RELEASE-COM} message or {CC-RELEASE} message received.
Issue MNCC_RELEASE-cfm primitive. Clear call. Next state T-00.

P23-P26: For further study.

P27: <CC.03> expires. Send {CC-RELEASE-COM} message.
Issue MNCC_REJECT-ind primitive. Clear call. Next state T-00.

ALL OTHER CASES: all unexpected messages shall be handled according to clause 9 (if described) or according to subclause 17.4 (if not described).

B.2 CC state transitions at FT side

B.2.1 CC state table at FT side

Table B.2: CC state table at FT side

EVENT (CC message)		STARTING STATE									END STATE
		F00	F01	F02	F03	F04	F06	F07	F10	F19	
{CC-SETUP}	sent	Q01									F06
{CC-SETUP}	rcvd	Q08									F01
{CC-SETUP-ACK}	sent		Q11								F02
{CC-CALL-PROC}	sent		Q09	Q09							F03
{CC-ALERTING}	sent		Q05	Q05	Q05						F04
{CC-ALERTING}	rcvd						Q06				F07
{CC-CONNECT}	sent		Q10	Q10	Q10	Q10					F10
{CC-CONNECT}	rcvd						Q07	Q07			F10
{CC-INFO}	sent			Q12	Q12	Q12		Q12	Q12	Q12	*
{CC-INFO}	rcvd			Q04	Q12	Q12		Q12	Q12	Q12	*
{CC-RELEASE}	sent			Q13	Q13	Q13	Q13	Q13	Q13		F19
{CC-RELEASE}	rcvd		Q20	Q20	Q20	Q20		Q20	Q20	Q22	* F00
{CC-RELEASE-COM}	rcvd		Q14	Q14	Q14	Q14	Q14	Q14	Q14	Q22	F00
{CC-RELEASE} (reject)	sent		Q16	Q16						Q16	F00
{CC-RELEASE-COM} (response)	sent		Q21	Q21	Q21	Q21		Q21	Q21		F00
{CC-NOTIFY}	sent		Q18	Q18	Q18	Q18					*
TIMEOUT				Q17	Q17	Q17		Q17			F19
RELEASE TIMEOUT									Q15		F00
SETUP TIMEOUT							Q27				F00

An entry "*" in the END STATE column indicates current state maintained. All unspecified events (blank entries in the above table) shall be treated according to the normal procedures given in clause 9 where defined. If not defined they shall be treated according to subclause 17.4 (handling of errors for unexpected messages).

NOTE 1: States F-22 and F-23 are for further study.

NOTE 2: The FT may send CRSS ({FACILITY}) messages when in the CC state F-19. This will allow the user and network to initiate (and correspondingly acknowledge) supplementary services during call release procedure (e.g. advice of charge requested at the termination of the call).

B.2.2 CC transition procedures at FT side

Q01: MNCC_SETUP-req primitive received.
Send {CC-SETUP} message to PT. Next state F-06.

Q04: {CC-INFO} message received.
Deliver <<KEYPAD>> element in MNCC_INFO-ind primitive.
State F-02 maintained.

Q05: MNCC_ALERT-req primitive received.
Send {CC-ALERTING} message. Next state F-04.

Q06: {CC-ALERTING} message received.
Issue MNCC_ALERT-ind primitive. Next state F-07.

Q07: {CC-CONNECT} message received.
Connect U-plane. Send {CC-CONNECT-ACK} message.
Issue MNCC_CONNECT-ind primitive. Next state F-10.

Q08: {CC-SETUP} message received from PT.
Issue MNCC_SETUP-ind primitive. Next state F-01.

Q09: MNCC_CALL_PROC-req primitive received.
Send {CC-CALL-PROC} message. Next state F-03.

Q10: MNCC_CONNECT-req primitive received. Connect U-plane.
Send {CC-CONNECT} message. Next state F-10.

Q11: MNCC_SETUP_ACK-req primitive received.
Send {CC-SETUP-ACK} message. Next state F-02.

Q12: MNCC_INFO-req received; Send {CC-INFO} message.
or {CC-INFO} message received: issue MNCC_INFO-ind.
Current state maintained.

Q13: MNCC_RELEASE-req primitive received. Clear call.
Send {CC-RELEASE} message. Next state F-19.

Q14: Receive {CC-RELEASE-COM} message.
Issue MNCC_REJECT-ind primitive. Clear call. Next state F-00.

Q15: Release time-out. Send {CC-RELEASE-COM} message.
Issue MNCC_RELEASE-cfm primitive. Clear call. Next state F-00.

Q16: Call rejected, or MNCC_REJECT-req primitive received.
Send {CC-RELEASE-COM} message. Clear call.
Next state F-00.

Q17: Timer Expires. Send {CC-RELEASE} message.
Reason = "timer expiry". Next state F-19.

Q18: MNCC-NOTIFY-req primitive received.
Send {CC-NOTIFY} message. Current state maintained.

Q20: {CC-RELEASE} message received. Issue MNCC_RELEASE-ind primitive.
Current state maintained.

Q21: MNCC_RELEASE-res primitive received.
Send {CC-RELEASE-COM} message. Clear call. Next state F-00.

Q22: {CC-RELEASE-COM} message or {CC-RELEASE} message received.
Issue MNCC_RELEASE-cfm primitive. Clear call. Next state F-00.

Q23-Q26: For further study.

Q27: <CC.03> expires. Send {CC-RELEASE-COM} message.
Issue MNCC_REJECT-ind primitive. Clear call. Next state F-00.

ALL OTHER CASES: all unexpected messages shall be handled according to clause 9 (if described) or according to subclause 17.4 (if not described).

Annex C (informative): DLC states as viewed by the LCE

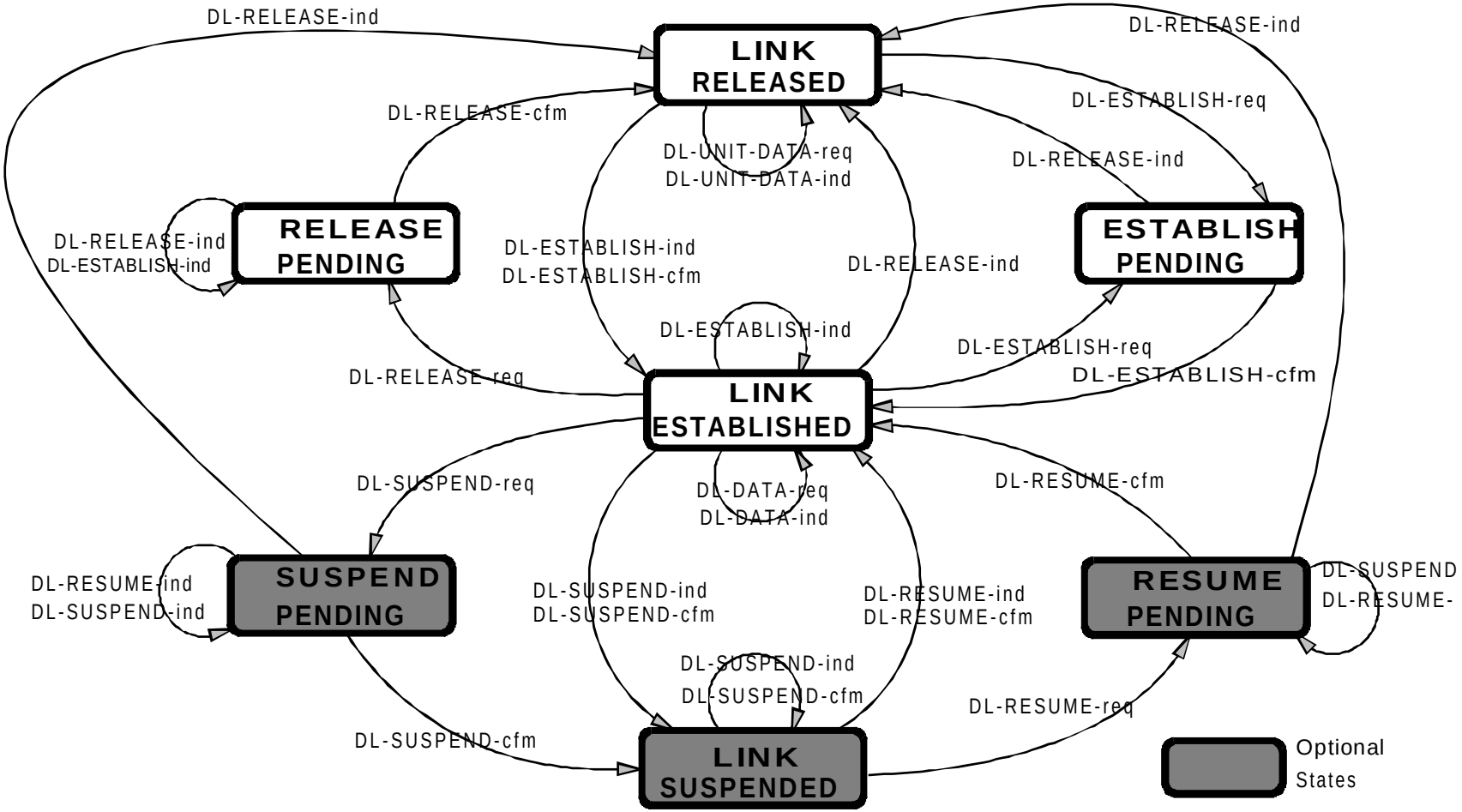


Figure C.1: DLC Link states as viewed by the LCE

Annex D (normative): DECT standard character sets

D.1 General

Two standard character sets are defined:

- DECT standard 8-bit characters;
- DECT standard 4-bit characters.

The DECT standard 8-bit characters shall be used for both dialling and display functions when contained in the following information elements:

- <<"KEYPAD">>;
- <<"DISPLAY">>;
- <<CALLED-PARTY-NUMBER>>;
- <<CALLING-PARTY-NUMBER>>.

Both the 8-bit and 4-bit DECT standard character sets may be carried in the <<ALPHANUMERIC>> information element or in the {CLMS-FIXED} message.

All of these elements may contain one or several characters.

D.2 DECT standard 8-bit characters

D.2.1 General

The first 128 characters shall use the standard IA5 characters, except for the first 32 (control) characters which are redefined as DECT "control codes".

NOTE 1: Refer to CCITT Recommendation T.50 [14] for details of IA5 characters.

The second 128 characters are called DECT "extended codes".

NOTE 2: The <<ALPHANUMERIC>> element allows for alternative character sets, including the complete standard IA5 character coding.

D.2.2 Control codes

Character codes 00 Hex to 1F Hex are specific to the DECT character set. They are not used in the standard IA5 sense. The following values are defined for cursor control (display purposes only) and dialling control:

Code(Hex)	Control character
00	Null/cancel DTMF tone;
02	Return home;
03	Return end;
05	Dialling pause (note 3);
06	Move forward to next column tab position (note 1);
07	Move backward to next column tab position (note 1);
08	Move backward one column;
09	Move forward one column;
0A	Move down one row;
0B	Move up one row;
0C	Clear display (and return home);
0D	Return (to start of current row);
0E	Flash off (note 2);
0F	Flash on (note 2);
11	XON (resume transmission);
12	Go to pulse dialling;

13 XOFF (stop transmission);
14 Go to DTMF dialling; defined tone length;
15 Register recall (note 4)
16 Go to DTMF dialling; infinite tone length;
17 Internal call (note 5)
18 Service
19 Clear to end of display (maintain cursor position);
1A Clear to end of line (maintain cursor position);
1B ESC. ESCape in the IA5 sense;
All other values reserved.

NOTE 1: Column tabs should be set at 10 column intervals.

NOTE 2: Flash on/Flash off is a toggle action, that applies to all subsequent display characters.

NOTE 3: The duration of the dialling pause is determined by the FT.

The dialling characteristics (pulse duration and DTMF defined tone length) are determined by the FT. DTMF tones shall conform to Multi-Frequency Push Button (MFPB) tones as defined in ETS 300 001 [17].

PT controlled DTMF pulse duration is supported by using "go to DTMF; infinite tone length" following by the selected digit. The tone shall be stopped upon receipt of any other character (e.g. another digit). To terminate an infinite tone with no other action the "null" character shall be used.

NOTE 4 Register recall: to seize a register (with dial tone) to permit input of further digits or other action. The transfer of dial digits towards the register should be done using the keypad protocol.

NOTE 5: A call from one user to another user within the domain of 1 FP. This is typically useful in residential environments.

D.2.3 Standard IA5 codes

Character codes 20 Hex to 7F Hex shall be used in the standard IA5 sense as defined in CCITT Recommendation T.50 [14]. The International Reference Version (IRV) characters shall be used.

D.2.4 extended codes and escape to alternative character sets

Character codes 80 Hex to FF Hex may be used for extended character sets. Extended character sets shall be designated and invoked by use of escape sequences in accordance with ISO 2022 [15] for 8-bit environments. The following requirements shall apply to ensure compatibility.

To allow independent operation of different CC/COMS/CISS instances, escape sequences in display information elements shall only affect the CC/COMS/CISS instance to which the information element relates.

Additional character sets (for which the PT indicates support in <<TERMINAL-CAPABILITY>> information element) may be designated to the G0, G1, G2 or G3 set. The DECT standard character set (IA5) shall by default be designated to the G0 set. If the PT indicates support of only one additional character set this character set shall by default be designated to the G1 set. The G0 set shall by default be invoked at the lower part of the address space and the G1 set at the upper part of the address space. Default designations and invocations shall always be used when a new CC/COMS/CISS instance is created.

A PT indicating support of more than one additional character set should be able to correctly interpret the escape sequences for designation of all supported character sets to the G1, G2 and G3 sets. Furthermore it should at least be able to correctly interpret the escape sequences for the locking-shift functions LS1R, LS2R and LS3R plus the single-shift functions SS2 and SS3. The SS2 and SS3 functions should by default be assigned to the relevant codings in the C1 control character set.

If proprietary character sets are needed they should be designated to the G3 set.

D.3 DECT standard 4-bit characters

Code(Hex)	Character:
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
B	(space)

All other values reserved.

Annex E (normative): Default coding of <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> information elements for basic speech

Table E.1: Default coding for <<IWU-ATTRIBUTES>> information element

Octet	Information element field	Field Value
3	Coding standard	DECT standard
	Info. transfer capability	Speech
4	Negotiation indicator	Not possible
	External connection Type	Connection oriented
5	Transfer mode	Circuit mode
	Info. transfer rate	32 kbit/s
6	Protocol identifier	User protocol ID
	User protocol ID	G.721 ADPCM

Table E.2: Default coding for <<CALL-ATTRIBUTES>> information element

Octet	Information element field	Field Value
3	Coding standard	DECT standard
	Network layer attributes	Basic speech
4	C-plane class	Class A; shared
	C-plane transfer rate	CS only
5	U-plane symmetry	Symmetric
	LU identification	LU1
6	U-plane class	Class 0 min_delay
	U-plane frame type	FU1

Annex F (normative): Broadcast attributes coding

F.1 Higher Layer Capabilities

The broadcast attributes are a small set of NWK layer and DLC layer capabilities (jointly known as "higher layer capabilities") that shall be broadcast regularly as part of the MAC layer broadcast service.

NOTE 1: These "higher layer" attributes comprise a total of 20 bits of information. These bits are combined with lower layer attributes in the MAC layer to form a single MAC layer broadcast message. Refer to ETS 300 175-3 [3].

Table F.1: Broadcast attributes coding

BIT NUMBER (note 2)	ATTRIBUTE ("1" means that service is available)
a32	ADPCM/G.721 Voice service
a33	GAP/PAP basic speech
a34	Non-voice circuit switched service
a35	Non-voice packet switched service
a36	Standard authentication required
a37	Standard ciphering supported
a38	Location registration supported
a39	SIM services available
a40	Non-static Fixed Part (FP)
a41	CISS services available
a42	CLMS service available
a43	COMS service available
a44	Access rights requests supported
a45	External handover supported
a46	Connection handover supported
a47	Reserved

NOTE 2: The bit numbers refer to the bit positions in the MAC message. Refer to subclause 7.2.3.4.2 in ETS 300 175-3 [3].

NOTE 3: The default setting for all bits is "0"; meaning "not available".

NOTE 4: The value of any bit might change during normal operation.

F.2 Extended Higher Layer Capabilities

If a profile is supported, then the bit corresponding to that profile is set to 1; otherwise (if profile is not supported) the bit is set to 0.

BIT NUMBER	Profile Supported
a47	ISDN Data Services
a46	Data Service Profile A/B
a45	Data Service Profile C
a44	Data Service Profile D
a43	Data Service Profile E
a42	Data Service Profile F
a41	Assymetric bearers supported

NOTE 1: The bit numbers refer to the bit positions in the MAC message. Refer to subclause 7.2.3.5 in ETS 300 175-3 [3].

NOTE 2: The default setting for all bits is "0"; meaning "not available".

Annex G (normative): Use of <<IWU-PACKET>> and <<IWU-TO-IWU>> information elements

G.1 General

The <<IWU-PACKET>> and <<IWU-TO-IWU>> are transparent information elements (refer to subclause 6.1.2). They are defined to provide two alternative mechanisms for the transparent transportation of external information (e.g. from a PP application to an FP interworking unit). The two elements correspond to two possible structures of external information.

NOTE: The <<IWU-TO-IWU>> element provides a capability equivalent to the <<USER-TO-USER>> information element defined in ETS 300 102-1 [10].

G.2 Sending of <<IWU-PACKET>> elements

G.2.1 CC and MM use of <<IWU-PACKET>>

An unsegmented <<IWU-PACKET>> may be carried in most CC and MM messages provided that each message contains at most one <<IWU-PACKET>> information element. A segmented <<IWU-PACKET>> shall only be sent in a series of {IWU-INFO} messages, and each {IWU-INFO} message shall contain one <<IWU-PACKET>> element preceded by a <<SEGMENTED-INFO>> element. A {IWU-INFO} message should be used if there are no suitable CC messages scheduled for transmission.

G.2.2 COMS and CLMS use of <<IWU-PACKET>>

An unsegmented or a segmented <<IWU-PACKET>> may be sent in a series of {COMS-INFO} or {CLMS-VARIABLE} messages. If segmented, each message shall contain one <<IWU-PACKET>> element preceded by a <<SEGMENTED-INFO>> element.

G.2.3 Rejection of <<IWU-PACKET>> elements

The <<IWU-PACKET>> element shall be used to reject any <<IWU-PACKET>> element that is received but cannot be understood (i.e. contains a protocol discriminator coding that is not supported). In this event the element shall indicate rejection (using the S/R bit) and shall contain a partial echo of the message that has been rejected. This echo shall only contain the L2 protocol discriminator and the following octet (i.e. in most cases the echoed information will be truncated). A rejection element shall be returned immediately after receiving the message containing the rejected element.

G.3 Use of <<IWU-TO-IWU>> elements

G.3.1 Sending of <<IWU-TO-IWU>> elements

An unsegmented <<IWU-TO-IWU>> may be carried in most CC or MM messages. An {IWU-INFO} message may be used for transmission of unsegmented <<IWU-TO-IWU>> elements, if there are no suitable messages scheduled for transmission.

A segmented <<IWU-to-IWU>> shall only be sent in a sequence of {IWU-INFO} messages, and each message shall carry only one <<IWU-TO-IWU>> element, and each of these <<IWU-TO-IWU>> elements shall be preceded by a <<SEGMENTED-INFO>> element.

Segmented or unsegmented <<IWU-TO-IWU>> elements may be carried in {COMS-INFO} or {CLMS-VARIABLE} messages.

G.3.2 Rejection of <<IWU-TO-IWU>> elements

The <<IWU-TO-IWU>> element shall also be used to reject any <<IWU-TO-IWU>> element that is received but cannot be understood (i.e. contains a protocol discriminator coding that is not supported). In this event the element shall indicate rejection (using the S/R bit) and shall contain a partial echo of the message that has been rejected. This echo shall only contain the protocol discriminator and the first information octet of the rejected message (i.e. in most cases the echoed information will be truncated). A rejection element shall be returned immediately after receiving the message containing the rejected element.

Annex H (normative): Transaction identifier flags (TIF) assignment in MM procedures

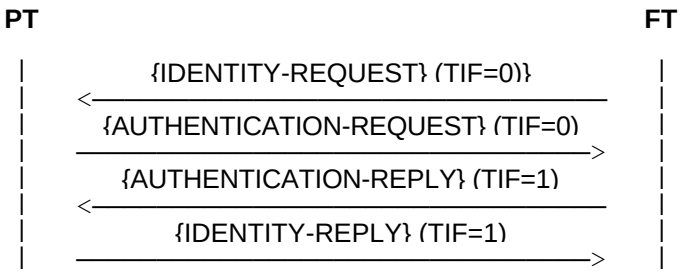
H.1 General

Implicit in this annex is the assumption that an MM procedure may consist of one or more transactions. Each transaction is owned by a single instance of an MM entity. Each instance of an MM entity may own only a single transaction. The priority level (as it is specified in subclause 15.5 of this ETS) relates to the transaction, and not to the procedure.

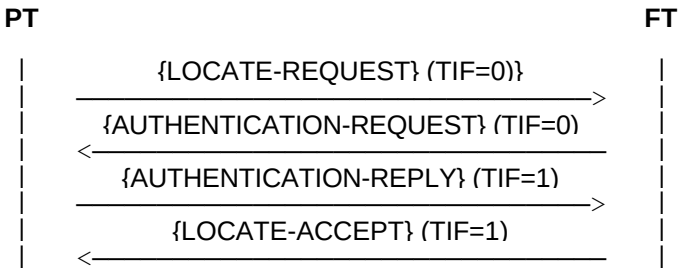
H.2 Nested procedures

TI-flags, in case of nested procedures (two procedures A and B are qualified as being nested if procedure B begin and is accomplished after procedure A has been started and before procedure A has been accomplished) shall be allocated independently.

EXAMPLE 1: A FT initiated procedure for identification of PT is interrupted by a PT initiated authentication of FT procedure.



EXAMPLE 2: A PT initiated procedure for location registration is interrupted by a FT initiated authentication of PT procedure.

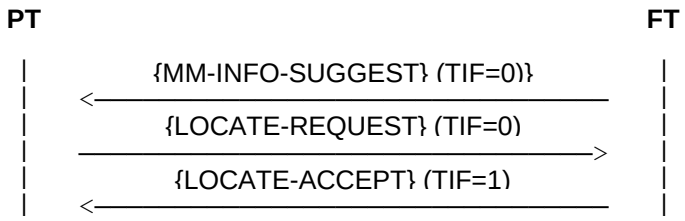


The setting of transaction flags shall be the same in any similar situation.

H.3 Stand alone procedures

H.3.1 Location update procedure

Location update procedure is a single procedure using two transactions that may be described as FT suggesting location registration and PT performing location registration. The TIF shall be allocated as follows:

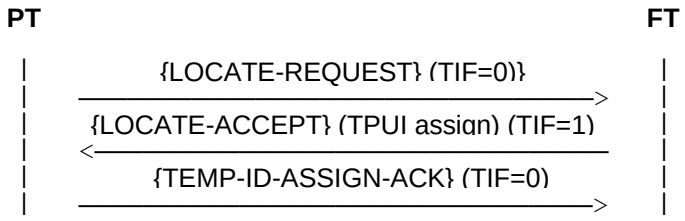


In the situation where the {MM-INFO-SUGGEST} interrupts a priority level 3 PT-initiated procedure the PT shall complete the interrupted procedure before initiating the location registration procedure.

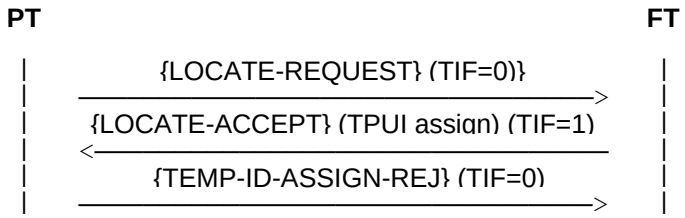
H.3.2 Location registration procedure with temporary identity assignment

Location registration procedure with temporary identity assignment consists of one transaction. This transaction has priority level 3. The PT shall not attempt to authenticate the FT during this procedure. The TIF shall be allocated as follows:

Case 1:



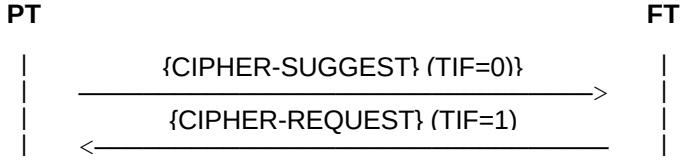
Case 2:



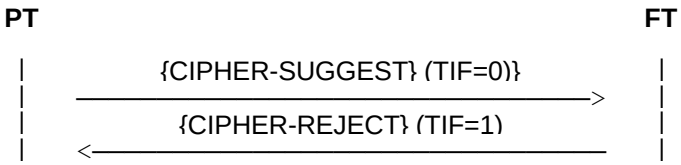
H.3.3 PT initiated cipher switching

Cipher switching initiated by PT procedure consists of one priority level 3 transaction. The TIF shall be allocated as follows:

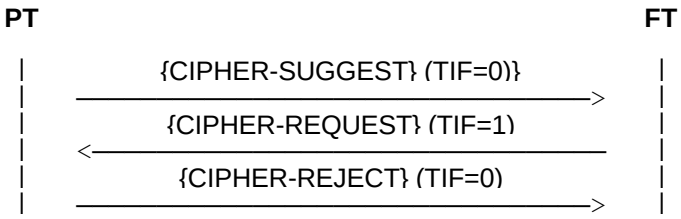
Case 1:



Case 2:

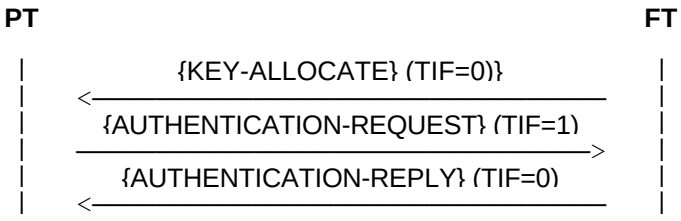


Case 3:



H.3.4 Key allocation

Key allocation procedure consists of one priority level 2 transaction. The PT shall not attempt to authenticate the FT during this procedure. The TIF shall be allocated as follows:



Annex J (normative): Scrolling Behaviour

Scrolling Behaviour Types 1,2

When the amount of stored display data exceeds the size of the physical display, the display shall be able to show sections (windows) of the stored data. If the window starts at character x in the stored display, the x^{th} character shall appear at the home position of the display and the (np -1) subsequent characters shall be mapped, line by line, sequentially to the rest of the display (where n is the number of lines in the display and p is the number of characters per line). The allowed window positions determine whether the display scrolls by character, by line or by page.

If the display has only one row and supports scrolling behaviour type = 1 then it shall scroll by character.

If the display has more than one row and supports scrolling behaviour type = 1 then it shall scroll by line.

If the display has only one row and supports scrolling behaviour type = 2 then it shall scroll by page.

NOTE: There is no distinction between line and page scrolling in a single line display. If the display has more than one row and supports display behaviour type = 2 then it shall scroll by page.

The scrolling behaviour is summarised in the following table:

	Scrolling behaviour type = 1	**Scrolling behaviour type = 2**
Single line display	scroll by character	scroll by page (see note above)
Multi line display	scroll by line	scroll by page

A PT display which scrolls may set its window origin as shown in the following table. The first stored character is character 1.

Scroll type	**Character**	**Line**	**Page**
Window origin	1	1	1
	2	p+1	np+1
	3	2p+1	2np+1
	.	.	.
	.	.	.
	etc.	etc.	etc.

where n is the number of lines in the display and p is the number of characters per line.

The effect of changing the display is to over-write existing characters. It is not possible to insert characters.

The action of the <<MULTI-DISPLAY>> information element 0CH shall be to clear the entire stored display and reset the display window and cursor to the first stored character.

The action of the <<MULTI-DISPLAY>> information element 02H shall be to reset the display window and cursor to the first stored character.

The action of the <<MULTI-DISPLAY>> information element 03H shall be to move the cursor to the end of the current display window. Any further displayable characters shall cause the display to scroll.

When a line is filled, further characters will be displayed at the beginning of a new line. A CR/LF sequence (<<MULTI-DISPLAY>> information element 0AH, 0DH) should not be sent unless a line is terminated before the end of the display line.

The cursor (indicating where the next displayable character will appear) should normally be within the visible window. However, when the display is filled, the displayed characters shall remain until a further display character is received, i.e. the cursor may not be within the visible window. When another display character is received, the PT shall move the window origin by one character, line or page as appropriate. (The character insert position within the stored display does not change.) The newly received characters are then displayed.

If the cursor is moved backwards or upwards through the display, the display shall scroll up (by character, line or page) when the cursor moves off the top of the screen. In upwards scrolling the cursor shall remain visible within the display window.

Manufacturers may incorporate automatic techniques to change display windows or may provide key sequences to allow the user to move the display windows In either case this action shall not affect the position in the stored display at which further characters are stored and the PT shall remember the window origin prior to the action. Immediately following the receipt of a further display character, the PT shall reset its display to the window position prior to the action and the display character shall be actioned as normal.

When the FT sends messages to the display, it should ensure that the capacity of the stored display is not exceeded. If the end of the stored display is reached, further characters shall be displayed but the subsequent scrolling behaviour of the display may be unpredictable.

Annex K (informative): Bibliography

1) ETR 043: "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Common Interface Services and Facilities requirements specification".

2) ETR 015: " Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); Reference document".

3) ETR 056: " Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); System description document".

4) ETR 042: "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT); A Guide to the DECT features that influence the traffic capacity and the maintenance of high radio link transmission quality, including the results of simulations".

History

Document history			
October 1992	First Edition		
July 1995	Public Enquiry	PE 90:	1995-08-21 to 1995-12-15
June 1996	Vote	V 106:	1996-06-24 to 1996-08-30
September 1996	Second Edition		

ISBN 2-7437-0949-9 - Edition complète - Edition 2
ISBN 2-7437-0954-5 - Partie 5 - Edition 2
Dépôt légal : Septembre 1996