

ETSI EN 300 175-5 V2.5.1 (2013-08)



**Digital Enhanced Cordless Telecommunications (DECT);
Common Interface (CI);
Part 5: Network (NWK) layer**

Reference

REN/DECT-000268-5

Keywords

DECT, IMT-2000, mobility, radio, TDD, TDMA**ETSI**

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

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

© European Telecommunications Standards Institute 2013.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	16
Foreword.....	16
1 Scope	17
2 References	18
2.1 Normative references	18
2.2 Informative references.....	22
3 Definitions, symbols and abbreviations	23
3.1 Definitions.....	23
3.2 Symbols and abbreviations.....	23
4 Overview of the NWK layer	27
5 Overview of procedures	29
5.1 General	29
5.2 Overview of Call Control (CC)	29
5.2.1 General.....	29
5.2.2 Call establishment.....	30
5.2.2.1 Call setup	30
5.2.2.2 Service negotiation.....	30
5.2.3 Call connect	30
5.2.4 Call information.....	31
5.2.5 Service change	31
5.2.6 Call release.....	31
5.3 Overview of Supplementary Services (SS)	31
5.3.1 General.....	31
5.3.2 Keypad protocol.....	32
5.3.3 Feature key management protocol	32
5.3.4 Functional protocol.....	32
5.4 Overview of Connection Oriented Message Service (COMS).....	33
5.4.1 General.....	33
5.4.2 COMS establishment	33
5.4.3 Service negotiation	33
5.4.4 COMS connect.....	33
5.4.5 COMS data transfer	33
5.4.6 COMS suspend and resume	34
5.4.7 COMS release	34
5.5 Overview of ConnectionLess Message Service (CLMS)	34
5.5.1 Fixed length message service.....	34
5.5.2 Variable length message service.....	34
5.6 Overview of Mobility Management (MM)	35
5.6.1 General.....	35
5.6.2 Identity procedures	35
5.6.3 Authentication procedures	35
5.6.4 Location procedures.....	36
5.6.5 Access rights procedures	36
5.6.6 Key allocation procedure	37
5.6.7 Parameter retrieval procedure	37
5.6.8 Ciphering related procedure.....	37
5.6.9 External protocol information procedure.....	37
5.7 Overview of Link Control Entity (LCE)	37
5.7.1 General.....	37
5.7.2 Data Link Endpoint Identifier (DLEI)	38
5.7.3 Data link establishment.....	38
5.7.4 Data link re-establishment	38
5.7.5 Data link release	39

5.7.6	Data link suspend and resume.....	39
5.7.7	Queuing of messages	39
5.7.8	Request paging.....	39
6	Message functional definitions.....	40
6.1	Overview of message structures	40
6.1.1	Messages.....	40
6.1.2	Information elements	40
6.2	Message summaries.....	41
6.2.1	Summary of CC messages	41
6.2.2	Summary of CISS messages	41
6.2.3	Summary of COMS messages	42
6.2.4	Summary of CLMS messages.....	42
6.2.5	Summary of MM messages	43
6.2.6	Summary of LCE messages	43
6.3	S-FORMAT message functional contents.....	44
6.3.1	S-FORMAT message overview	44
6.3.2	CC-messages.....	44
6.3.2.1	{CC-SETUP}	44
6.3.2.2	{CC-INFO}	46
6.3.2.3	{CC-SETUP-ACK}	47
6.3.2.4	{CC-CALL-PROC}	48
6.3.2.5	{CC-ALERTING}	49
6.3.2.6	{CC-CONNECT}	50
6.3.2.7	{CC-CONNECT-ACK}	51
6.3.2.8	{CC-RELEASE}	51
6.3.2.9	{CC-RELEASE-COM}	53
6.3.2.10	{CC-SERVICE-CHANGE}	54
6.3.2.11	{CC-SERVICE-ACCEPT}	55
6.3.2.12	{CC-SERVICE-REJECT}	55
6.3.2.13	{CC-NOTIFY}	56
6.3.2.14	{IWU-INFO}	56
6.3.3	SS-messages (call related and call independent)	57
6.3.3.1	{FACILITY}	57
6.3.3.2	{HOLD}	58
6.3.3.3	{HOLD-ACK}	58
6.3.3.4	{HOLD-REJECT}	59
6.3.3.5	{RETRIEVE}	59
6.3.3.6	{RETRIEVE-ACK}	60
6.3.3.7	{RETRIEVE-REJECT}	60
6.3.3.8	{CISS-REGISTER}	61
6.3.3.9	{CISS-RELEASE-COM}	62
6.3.4	COMS-messages.....	62
6.3.4.1	{COMS-SETUP}	62
6.3.4.2	{COMS-INFO}	63
6.3.4.3	{COMS-ACK}	64
6.3.4.4	{COMS-CONNECT}	64
6.3.4.5	{COMS-RELEASE}	65
6.3.4.6	{COMS-RELEASE-COM}	65
6.3.4.7	{COMS-NOTIFY}	66
6.3.5	CLMS-message.....	66
6.3.5.1	{CLMS-VARIABLE}	66
6.3.6	MM-messages.....	67
6.3.6.1	{ACCESS-RIGHTS-ACCEPT}	67
6.3.6.2	{ACCESS-RIGHTS-REJECT}	67
6.3.6.3	{ACCESS-RIGHTS-REQUEST}	68
6.3.6.4	{ACCESS-RIGHTS-TERMINATE-ACCEPT}	68
6.3.6.5	{ACCESS-RIGHTS-TERMINATE-REJECT}	69
6.3.6.6	{ACCESS-RIGHTS-TERMINATE-REQUEST}	69
6.3.6.7	{AUTHENTICATION-REJECT}	70
6.3.6.8	{AUTHENTICATION-REPLY}	71
6.3.6.9	{AUTHENTICATION-REQUEST}	72

6.3.6.10	{CIPHER-REJECT}	72
6.3.6.11	{CIPHER-REQUEST}	73
6.3.6.12	{CIPHER-SUGGEST}	73
6.3.6.13	{DETACH}	73
6.3.6.14	{IDENTITY-REPLY}	74
6.3.6.15	{IDENTITY-REQUEST}	75
6.3.6.16	{KEY-ALLOCATE}	75
6.3.6.17	{LOCATE-ACCEPT}	76
6.3.6.18	{LOCATE-REJECT}	76
6.3.6.19	{LOCATE-REQUEST}	77
6.3.6.20	{MM-INFO-ACCEPT}	78
6.3.6.21	{MM-INFO-REJECT}	78
6.3.6.22	{MM-INFO-REQUEST}	79
6.3.6.23	{MM-INFO-SUGGEST}	80
6.3.6.24	{TEMPORARY-IDENTITY-ASSIGN}	80
6.3.6.25	{TEMPORARY-IDENTITY-ASSIGN-ACK}	81
6.3.6.26	{TEMPORARY-IDENTITY-ASSIGN-REJ}	81
6.3.6.27	{MM-IWU}	82
6.3.6.28	{MM-NOTIFY}	82
6.3.7	LCE-messages	83
6.3.7.1	{LCE-PAGE-RESPONSE}	83
6.3.7.2	{LCE-PAGE-REJECT}	83
6.4	B-FORMAT message functional contents	84
6.4.1	B-FORMAT message overview	84
6.4.2	{LCE-REQUEST-PAGE}	84
6.4.3	{CLMS-FIXED}	85
7	S-FORMAT message structures	85
7.1	Overview	85
7.2	Protocol Discrimination (PD) element	86
7.3	Transaction Identifier (TI) element	86
7.4	Message type element	87
7.4.1	Messages for CC	88
7.4.2	Messages for SS	88
7.4.3	Messages for COMS	88
7.4.4	Messages for CLMS	89
7.4.5	Messages for MM	89
7.4.6	Messages for LCE	89
7.5	Other information elements	90
7.5.1	Coding rules	90
7.5.2	Extensions of codesets	92
7.5.3	Locking shift procedure	92
7.5.4	Non-locking shift procedure	93
7.5.5	Display and keypad elements	93
7.5.6	Repeated elements	93
7.6	Fixed length information elements	94
7.6.1	Summary	94
7.6.2	Sending complete, delimiter request and use TPUI	94
7.6.3	Repeat indicator	95
7.6.4	Basic service	95
7.6.5	Single display	96
7.6.6	Single keypad	96
7.6.7	Release reason	97
7.6.8	Signal	98
7.6.9	Timer restart	99
7.6.10	Test hook control	99
7.7	Variable length information elements	99
7.7.1	Summary	99
7.7.2	Allocation type	101
7.7.3	Alphanumeric	101
7.7.4	Auth type	103
7.7.5	Call attributes	104

7.7.6	Call identity	108
7.7.7	Called party number.....	109
7.7.8	Called party subaddress	110
7.7.9	Calling party number	110
7.7.10	Cipher info	111
7.7.11	Connection attributes	112
7.7.12	Connection identity	116
7.7.13	Duration	117
7.7.14	End-to-end compatibility	118
7.7.15	Facility	121
7.7.16	Feature activate	121
7.7.17	Feature indicate.....	123
7.7.18	Fixed identity	125
7.7.19	Identity type.....	126
7.7.20	Info type.....	127
7.7.21	InterWorking Unit (IWU) attributes	128
7.7.22	IWU packet	133
7.7.23	IWU to IWU	134
7.7.24	Key.....	136
7.7.25	Location area	136
7.7.26	Multi-display.....	137
7.7.27	Multi-keypad.....	138
7.7.28	NetWorK (NWK) assigned identity.....	138
7.7.29	Network parameter	139
7.7.30	Portable identity	141
7.7.31	Progress indicator	145
7.7.32	RAND	146
7.7.33	Rate parameters	146
7.7.34	Reject reason.....	147
7.7.35	RES	148
7.7.36	RS	149
7.7.37	Segmented info	149
7.7.38	Service change info.....	150
7.7.39	Service class.....	151
7.7.40	Setup capability	152
7.7.41	Terminal capability	153
7.7.42	Transit delay	159
7.7.43	Window size	160
7.7.44	ZAP field	160
7.7.45	Escape to proprietary	161
7.7.46	Model identifier	161
7.7.47	MMS Generic Header.....	162
7.7.48	MMS Object Header.....	162
7.7.49	MMS Extended header	163
7.7.50	Time-Date	163
7.7.51	Ext h/o indicator	165
7.7.52	Called party Name	165
7.7.53	Calling party Name	166
7.7.54	Codec List.....	167
7.7.55	Events notification	168
7.7.55.1	General structure	168
7.7.55.2	Event types	170
7.7.56	Call information.....	174
7.7.57	List change details	177
7.7.58	ULE MAC Configuration Info.....	179
8	B-FORMAT message structures	180
8.1	General	180
8.2	LCE request paging messages	180
8.2.1	Short format message.....	180
8.2.2	Full format message.....	182
8.2.3	Long format message.....	183

8.2.4	Message elements	183
8.2.4.1	LCE paging header.....	183
8.2.4.2	Info fields (Full format)	185
8.2.4.3	Default setup behaviour	186
8.2.4.4	Address elements in collective or group ringing.....	187
8.3	CLMS-FIXED messages.....	187
8.3.1	General message structure	187
8.3.2	Message elements	188
8.3.3	Standard message structures	190
8.3.3.1	General	190
8.3.3.2	Messages using 4-bit characters	190
8.3.3.3	Messages using 8-bit characters	190
9	Call Control (CC) procedures.....	190
9.1	General	190
9.2	Call Control (CC) states	193
9.2.1	States at PT	193
9.2.1.1	State T-00: "NULL"	193
9.2.1.2	State T-19: "RELEASE PENDING"	193
9.2.1.3	State T-10: "ACTIVE"	193
9.2.1.4	State T-01: "CALL INITIATED"	193
9.2.1.5	State T-02: "OVERLAP SENDING"	193
9.2.1.6	State T-03: "CALL PROCEEDING"	193
9.2.1.7	State T-04: "CALL DELIVERED"	193
9.2.1.8	State T-06: "CALL PRESENT"	193
9.2.1.9	State T-07: "CALL RECEIVED"	193
9.2.1.10	State T-08: "CONNECT PENDING"	193
9.2.2	States at FT	194
9.2.2.1	State F-00: "NULL"	194
9.2.2.2	State F-19: "RELEASE PENDING"	194
9.2.2.3	State F-10: "ACTIVE"	194
9.2.2.4	State F-01: "CALL-INITIATED"	194
9.2.2.5	State F-02: "OVERLAP SENDING"	194
9.2.2.6	State F-03: "CALL PROCEEDING"	194
9.2.2.7	State F-04: "CALL DELIVERED"	194
9.2.2.8	State F-06: "CALL PRESENT"	194
9.2.2.9	State F-07: "CALL RECEIVED"	194
9.2.3	Optional states (PT and FT).....	195
9.2.3.1	States T-22 and F-22: "OVERLAP RECEIVING"	195
9.2.3.2	States T-23 and F-23: "INCOMING CALL PROCEEDING"	195
9.3	Call establishment procedures.....	195
9.3.1	PT initiated call establishment (outgoing call).....	195
9.3.1.1	Call request	195
9.3.1.2	Call accept or reject.....	196
9.3.1.3	Selection of lower layer resources	196
9.3.1.4	Connection of U-plane	197
9.3.1.5	Overlap sending	197
9.3.1.6	Call proceeding	198
9.3.1.7	Call confirmation	198
9.3.1.8	Call connection	199
9.3.1.9	Expiry of timer <CC.04>	199
9.3.2	FT initiated call establishment (incoming call).....	199
9.3.2.1	Call request	199
9.3.2.2	Call accept or reject.....	200
9.3.2.3	Selection of lower layer resources	200
9.3.2.4	Connection of U-plane	201
9.3.2.5	Overlap receiving.....	201
9.3.2.6	Call proceeding	201
9.3.2.7	Call confirmation	201
9.3.2.8	Call connection	202
9.3.2.9	Sending of <<TERMINAL-CAPABILITY>>	202
9.3.2.10	Expiry of timer <CC.04>	202

9.4	Call information procedures	202
9.5	Call release procedures	202
9.5.1	Normal call release	202
9.5.2	Abnormal call release	203
9.5.2.1	Definitions	203
9.5.2.2	Abnormal release general description (PT or FT)	203
9.5.2.3	Abnormal release in case of call setup collisions	205
9.5.3	Release collisions	208
9.6	Service change procedures	208
9.6.1	General	208
9.6.2	Change of Bandwidth parameters (including changes in connection type)	209
9.6.3	Service rerouting	209
9.6.4	NWK layer service suspension and resumption	209
9.6.5	Modulation scheme change	210
9.7	NWK layer Packet mode procedures	210
9.7.1	General	210
9.7.2	PT initiated access	211
9.7.3	FT initiated access	211
9.7.4	NWK layer suspend and resume	211
9.7.4.1	General	211
9.7.4.2	C-plane NWK layer suspend and resume	212
9.7.4.3	U-plane NWK layer suspend and resume	212
9.8	Emergency call procedure	212
9.9	Segmentation of information in CC procedures	213
10	Supplementary Services procedures	214
10.1	General	214
10.2	Keypad protocol	215
10.3	Feature key management protocol	215
10.4	Functional protocol	216
10.4.1	Separate messages approach	216
10.4.1.1	Hold procedures	216
10.4.1.2	Retrieve procedures	216
10.4.1.3	Auxiliary states for hold and retrieve	217
10.4.2	Common information element approach	217
10.4.2.1	Call Related Supplementary Services (CRSS) procedures	217
10.4.2.2	Call Independent Supplementary Services (CISS) procedures	217
10.4.2.2.1	Transport of CISS	217
10.4.2.3	Connectionless Supplementary Service (CLSS) procedure	218
10.5	Co-existence of multiple protocols	218
10.6	Application protocols	219
10.6.1	DECT standard functional supplementary services	219
10.6.2	DECT specific supplementary services	220
10.6.2.1	Queue management	220
10.6.2.2	Indication of subscriber number	220
10.6.2.3	Control of echo control functions	221
10.6.2.4	Cost information	221
11	Connection Oriented Message Service (COMS)	222
11.1	General	222
11.2	COMS states	222
11.2.1	States at PT	222
11.2.1.1	State TS-0: "NULL"	222
11.2.1.2	State TS-1: "CONNECT PENDING"	222
11.2.1.3	State TS-2: "RELEASE PENDING"	222
11.2.1.4	State TS-3: "ACTIVE"	222
11.2.2	States at FT	222
11.2.2.1	State FS-0: "NULL"	222
11.2.2.2	State FS-1: "CONNECT PENDING"	222
11.2.2.3	State FS-2: "RELEASE PENDING"	222
11.2.2.4	State FS-3: "ACTIVE"	223
11.3	COMS establishment procedures	223

11.3.1	PT initiated COMS establishment	223
11.3.1.1	COMS request.....	223
11.3.1.2	COMS connection.....	223
11.3.2	FT initiated COMS establishment	224
11.3.2.1	COMS request.....	224
11.3.2.2	COMS connection.....	224
11.4	COMS data transfer procedures	224
11.4.1	Procedure at the sending side.....	224
11.4.2	Procedure at the receiving side	225
11.5	COMS NWK layer suspend and resume procedures.....	226
11.6	COMS release procedures	226
11.6.1	Normal COMS release.....	226
11.6.2	Release collisions.....	226
12	ConnectionLess Message Service (CLMS).....	227
12.1	General	227
12.2	CLMS states	227
12.3	CLMS message transmission procedures	227
12.3.1	Fixed length messages	227
12.3.1.1	Procedure in the Fixed radio Termination (FT)	227
12.3.1.2	Procedure in the Portable radio Termination (PT)	228
12.3.2	Variable length messages.....	228
12.3.2.1	Procedure at the sending side	228
12.3.2.2	Procedure at the receiving side.....	228
12.3.2.3	Restrictions for portable side initiated messages.....	229
13	Mobility Management (MM) procedures.....	229
13.1	General	229
13.2	Identity procedures	230
13.2.1	Procedure for identification of PT	230
13.2.2	Procedure for temporary identity assignment	231
13.3	Authentication procedures.....	232
13.3.1	Authentication of a PT.....	232
13.3.2	Authentication of the user.....	234
13.3.3	Authentication of a FT.....	234
13.4	Location procedures	235
13.4.1	Location registration	236
13.4.2	Detach	237
13.4.3	Location update	238
13.5	Access rights procedure.....	238
13.5.1	Obtaining the access rights	238
13.5.2	Termination of access rights	239
13.5.3	Modification of access rights.....	241
13.6	Key allocation procedure.....	242
13.7	Parameter retrieval procedure.....	243
13.8	Ciphering related procedure	245
13.9	External protocol information procedure	247
13.9.1	Procedure for external protocol information initiated by the FT	247
13.9.2	Procedure for external protocol information initiated by the PT	247
13.9.3	Segmentation of information in MM procedures.....	248
14	Link Control Entity (LCE) procedures.....	249
14.1	General	249
14.2	Connection oriented link control procedures.....	250
14.2.1	Link establishment.....	250
14.2.2	Direct PT initiated link establishment.....	250
14.2.3	Indirect (paged) FT initiated link establishment	251
14.2.4	Direct FT initiated link establishment.....	252
14.2.5	Link maintenance.....	253
14.2.6	Link suspend and resume.....	253
14.2.6.1	Link suspend	253
14.2.6.2	Link resume.....	254
14.2.7	Link release.....	254

14.2.7.1	NLR notification without "partial release" as release reason	254
14.2.7.2	NLR notification with "partial release" as release reason	255
14.3	Connectionless link control procedures.....	255
14.3.1	Message routing.....	255
14.3.2	Broadcast announce procedure	255
14.3.3	LCE paging codes for connectionless service.....	256
14.4	Procedure for collective and group ringing	256
14.5	LCE paging procedures for DPRS	257
14.5.1	DPRS initial setup paging.....	257
14.5.1.1	Assumptions for Short paging format or for Full format with IPUI.....	257
14.5.1.2	Coding for Full paging format with TPUI.....	257
14.5.2	DPRS Resume paging.....	258
14.5.2.1	Assumptions for Short paging format or for Full format with IPUI.....	258
14.5.2.2	Coding for Full paging format with TPUI.....	258
14.5.2.3	LCE Resume Procedure description.....	259
14.5.3	Special cases	259
14.5.3.1	Rule for DPRS Class 1 devices	259
14.5.3.2	Rule for backcompatibility with former A/B 1 devices	259
15	Management procedures.....	260
15.1	Lower Layer Management Entity (LLME)	260
15.2	Service mapping and negotiation	260
15.2.1	General.....	260
15.2.2	Prioritized list negotiation.....	260
15.2.3	Exchanged attribute negotiation	261
15.2.4	Operating parameter negotiation.....	261
15.2.5	Peer attribute negotiation	262
15.3	Service modification procedures	262
15.4	Resource management.....	262
15.5	Management of MM procedures	262
15.6	Call ciphering management.....	264
15.7	External Handover.....	264
15.7.1	Handover candidate procedures	264
15.7.1.1	General	264
15.7.1.2	Handover candidate indication.....	265
15.7.1.3	Handover candidate retrieval	265
15.7.1.4	Target FP selection.....	266
15.7.2	Handover reference procedure.....	266
15.7.2.1	General	266
15.7.2.2	Handover reference indication	266
15.7.2.3	Handover reference retrieval	266
15.7.3	External handover suggested by FP	267
15.7.4	NWK layer set up procedure.....	267
15.7.4.1	Handover request	267
15.7.4.2	Handover confirm	267
15.7.4.3	Handover accept.....	267
15.7.4.4	Handover reject.....	267
15.7.4.5	Release of old connection	268
15.7.4.6	Handover Fall Back.....	268
15.7.5	U-plane handling	268
15.7.6	Ciphering procedure	269
15.7.7	Interaction with location registration	269
15.8	Test management procedures	270
15.8.1	Test call back procedure	270
15.8.2	Test hook control procedures.....	270
15.8.3	Upper tester procedure.....	271
15.9	Application assistance procedures.....	271
15.9.1	DECT Identity Resolution (Retrieval) Procedure	271
15.9.1.1	FT (or HyP) initiated Connectionless Identity Resolution procedure	271
15.9.1.2	PT initiated Connectionless Identity Resolution procedure	272
15.9.1.3	Connection oriented Identity Resolution procedure.....	272
15.9.2	Application Address Resolution (Retrieval) Procedure.....	272

15.9.3	Application Parameter Allocation Procedure.....	272
15.9.3.1	FT initiated application parameter allocation procedure.....	273
15.9.3.2	PT initiated application parameter allocation procedure.....	273
15.9.4	Application parameter information procedure.....	273
15.9.4.1	FT initiated connection oriented Application parameter information procedure	273
15.9.4.2	PT initiated connection oriented Application parameter information procedure	274
15.9.4.3	FT initiated connectionless Application parameter information procedure	274
15.9.4.4	PT initiated connectionless Application parameter information procedure	274
15.9.5	Application Parameter Indication procedure	275
16	Primitives	275
16.1	Primitive types.....	275
16.2	Primitives to lower layer (DLC layer).....	275
16.3	Primitives to IWU	276
16.3.1	Parameter definitions	276
16.3.2	MNCC primitives	276
16.3.2.1	MNCC_SETUP primitive	277
16.3.2.2	MNCC_SETUP_ACK primitive.....	277
16.3.2.3	MNCC_REJECT primitive	278
16.3.2.4	MNCC_CALL_PROC primitive.....	278
16.3.2.5	MNCC_ALERT primitive	279
16.3.2.6	MNCC_CONNECT primitive.....	279
16.3.2.7	MNCC_RELEASE primitive.....	280
16.3.2.8	MNCC_FACILITY primitive	280
16.3.2.9	MNCC_INFO primitive	281
16.3.2.10	MNCC_MODIFY primitive.....	281
16.3.2.11	MNCC_HOLD primitive	281
16.3.2.12	MNCC_RETRIEVE primitive	282
16.3.2.13	MNCC_IWU_INFO primitive	282
16.3.3	MNSS primitives	282
16.3.3.1	MNSS_SETUP primitive	282
16.3.3.2	MNSS_FACILITY primitive	283
16.3.3.3	MNSS_RELEASE primitive.....	283
16.3.4	MNCO primitives	283
16.3.4.1	MNCO_SETUP primitive	284
16.3.4.2	MNCO_CONNECT primitive	284
16.3.4.3	MNCO_INFO primitive.....	284
16.3.4.4	MNCO_ACK primitive.....	284
16.3.4.5	MNCO_RELEASE primitive.....	285
16.3.4.6	MNCO_REJECT primitive	285
16.3.5	MNCL primitives.....	285
16.3.5.1	MNCL_UNITDATA primitive	285
16.3.6	MM primitives	286
16.3.6.1	MM_IDENTITY primitive	286
16.3.6.2	MM_IDENTITY_ASSIGN primitive	286
16.3.6.3	MM_AUTHENTICATE primitive	287
16.3.6.4	MM_LOCATE primitive	287
16.3.6.5	MM_DETACH primitive.....	287
16.3.6.6	MM_ACCESS_RIGHTS primitive.....	288
16.3.6.7	MM_ACCESS_RIGHTS_TERMINATE primitive.....	288
16.3.6.8	MM_KEY_ALLOCATE primitive	288
16.3.6.9	MM_INFO primitive.....	289
16.3.6.10	MM_CIPHER primitive.....	289
16.3.6.11	MM_IWU primitive	289
17	Handling of error and exception conditions	290
17.1	Protocol discrimination error.....	290
17.2	Message too short.....	290
17.3	Transaction identifier error.....	290
17.3.1	Illegal and unsupported transaction identifier value	290
17.3.2	Transaction identifier procedural errors and exception conditions	290
17.3.2.1	Unknown active CC call	290

17.3.2.2	Unknown active CISS call	291
17.3.2.3	Unknown active COMS call	291
17.3.2.4	Unknown active CLMS call	291
17.3.2.5	Unknown active MM transaction	291
17.3.2.6	Unknown active LCE transaction	291
17.3.3	Call Resource Contention	291
17.4	Message type or message sequence errors	292
17.4.1	CC message error	292
17.4.2	CISS message error	292
17.4.3	COMS or CLMS message error	292
17.4.4	MM message error	292
17.4.5	LCE message error	292
17.5	General information element errors	292
17.5.1	Information element out of sequence	292
17.5.2	Duplicated information elements	293
17.6	Mandatory information element errors	293
17.6.1	Mandatory information element missing in CC messages	293
17.6.2	Mandatory information element content error in CC messages	293
17.6.3	Mandatory information element error in COMS or CLMS messages	293
17.6.4	Mandatory information element error in MM messages	294
17.6.5	Mandatory information element error in LCE messages	294
17.7	Non-mandatory information element errors	294
17.7.1	Unrecognized information element	294
17.7.2	Non-mandatory information element content error	294
17.8	Data link reset	295
17.9	Data link failure	295
Annex A (normative):	System parameters	296
A.1	CC timers	296
A.2	SS timers	297
A.3	COMS timers	297
A.4	CLMS timer	298
A.5	MM timers	298
A.6	LCE timers	301
A.7	NWK layer constants	302
A.8	Restart	302
Annex B (normative):	CC state transition tables	303
B.1	CC state transitions at PT side	303
B.1.1	CC state table at PT side	303
B.1.2	CC transition procedures at PT side	304
B.2	CC state transitions at FT side	306
B.2.1	CC state table at FT side	306
B.2.2	CC transition procedures at FT side	306
Annex C (informative):	DLC states as viewed by the LCE	309
Annex D (normative):	DECT standard character sets	310
D.1	General	310
D.2	DECT standard 8-bit characters	310
D.2.1	General	310
D.2.2	Control codes	311
D.2.3	Standard IA5 codes	312
D.2.4	extended codes and escape to alternative character sets	312

D.3	DECT standard 4-bit characters	312
Annex E (normative): Default coding of information elements.....		313
E.1	Default coding of <<IWU-ATTRIBUTES>> and <CALL-ATTRIBUTES>> information elements for basic speech	313
E.2	Default coding of <<IWU-ATTRIBUTES>>, <<CALL-ATTRIBUTES>> and <<CONNECTION-ATTRIBUTES>> information elements for wideband speech	313
E.2.1	Default setup attributes for basic service wideband speech	314
Annex F (normative): Broadcast attributes coding		315
F.1	Higher layer capabilities.....	315
F.2	Extended higher layer capabilities	316
F.3	Extended higher layer capabilities (part 2).....	316
Annex G (normative): Use of <<IWU-PACKET>> and <<IWU-TO-IWU>> information elements		318
G.1	General	318
G.2	Sending of <<IWU-PACKET>> elements.....	318
G.2.1	CC and MM use of <<IWU-PACKET>>	318
G.2.2	COMS and CLMS use of <<IWU-PACKET>>.....	318
G.2.3	Rejection of <<IWU-PACKET>> elements	318
G.3	Use of <<IWU-TO-IWU>> elements	319
G.3.1	Sending of <<IWU-TO-IWU>> elements.....	319
G.3.2	Rejection of <<IWU-TO-IWU>> elements	319
Annex H (normative): Transaction identifier flags (TIF) assignment in MM procedures.....		320
H.1	General	320
H.2	Nested procedures	320
H.3	Stand alone procedures.....	321
H.3.1	Location update procedure	321
H.3.2	Location registration procedure with temporary identity assignment	321
H.3.3	PT initiated cipher switching.....	322
H.3.4	Key allocation	322
H.4	External protocol information procedure	323
Annex I (normative): Distributed communications.....		324
I.1	Introduction	324
I.2	General requirements	324
I.2.1	DCDL-net.....	324
I.2.2	Subscription.....	324
I.2.3	Communication	325
I.3	Procedure description.....	326
I.3.1	HyP Identities	326
I.3.2	Membership Access Rights Allocation	326
I.3.3	Re-initialization of membership access rights.....	327
I.3.4	Members Data Transfer	327
I.3.5	Presence/Absence Indication.....	329
I.3.6	Bandwidth management	329
I.3.7	Direct Link Establishment.....	330
I.3.8	Indirect Link Establishment	331
I.3.9	MASTER management	332
I.3.9.1	MASTER assign	332

I.3.9.2	MASTER Change	332
I.3.9.3	DCDL-net System bearer management	332
I.3.10	Common Subscription Database management	333
I.3.10.1	IdN	333
I.3.10.2	RFPI, PARK and PLI	333
I.3.10.3	IPUI	334
I.3.10.4	TPUI and LAL	334
I.3.10.5	Keys	334
I.3.11	Handover issues	334
I.4	Elements of Messages/Information Elements	334
I.4.1	CLMS-FIXED	335
I.4.2	IWU-TO-IWU	335
I.4.3	Info-type	336
I.4.4	CLMS-VARIABLE	336
I.5	Examples	336
I.5.1	General	336
I.5.2	Example 1	337
I.5.3	Example 2	337
I.5.4	Example 3	338
I.5.5	Example 4	339
I.6	Usage of PPs or FPs in DCDL-net	340
I.6.1	General	340
I.6.2	Requirements to FPs	340
I.6.2.1	General	340
I.6.2.2	Members Data Transfer	341
I.6.2.3	Direct Link Establishment	341
I.6.3	Requirements to PPs	342
I.6.3.1	General	342
I.6.3.2	Membership Access Rights Allocation	342
I.6.3.3	Members Data Transfer	343
I.6.3.4	Direct Link Establishment	343
I.6.3.5	Indirect Link Establishment	343
Annex J (normative):	Scrolling Behaviour	344
Annex K (normative):	Additional information on Message Elements	346
K.1	Detailed description of the different connection types as defined by the IE <Connection Attributes>	346
K.1.1	General	346
K.1.1.1	Real number of bearers "on the air"	346
K.1.1.2	Definitions (applicable to all connection types)	346
K.1.2	Types of connection	347
K.1.2.1	Symmetric only connections	347
K.1.2.2	Asymmetric frozen connections	347
K.1.2.3	Asymmetric reversible connections	348
K.1.2.4	Asymmetric one-way-only connections	349
K.1.2.5	Asymmetric unrestricted connections	351
Annex L (informative):	Additional information on paging	352
L.1	List of "well-known" uses of LCE paging codes	352
L.1.1	Purpose of the list	352
L.1.2	List of "well-known" uses of LCE paging codes	353
L.2	Compatibility with historic DECT devices	353
L.2.1	Rule for compatibility with devices based on former data profile A/B 1 (historic)	353
Annex M (informative):	UTF-8 encoded character sets - Guidelines for implementation	355
M.1	General	355

M.2	Characters sets tables.....	355
M.3	Encoding of Western Europe languages.....	355
M.4	Encoding of Hebrew.....	359
M.5	Useful symbols.....	360
Annex N (informative):	Bibliography.....	362
Annex O (informative):	Change history	364
History		365

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT).

The present document is part 5 of a multi-part deliverable ([1] to [8]). Full details of the entire series can be found in part 1 [1].

Further details of the DECT system may be found in TR 101 178 [i.1] and ETR 043 [i.2].

National transposition dates	
Date of adoption of this EN:	20 August 2013
Date of latest announcement of this EN (doa):	30 November 2013
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2014
Date of withdrawal of any conflicting National Standard (dow):	31 May 2014

1 Scope

The present document is one of the parts of the specification of the Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

The present document specifies the Network (NWK) layer. The NWK layer is part 5 of the EN 300 175 and layer 3 of the DECT protocol stack.

Network layer	Network layer
C-plane (3)	U-plane
DLC layer	DLC layer
C-plane (2b)	U-plane
MAC layer	
(2a)	
Physical layer	
(1)	

Figure 1a

The present document 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).

The present document uses the layered model principles and terminology as described in Recommendations ITU-T X.200 [i.3] and X.210 [i.4].

The present document includes New Generation DECT, a further development of the DECT standard introducing wideband speech, improved data services, new slot types and other technical enhancements.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

- [1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".
- [2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".
- [3] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".
- [4] ETSI EN 300 175-4: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".
- [5] Void.
- [6] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".
- [7] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".
- [8] ETSI EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech and audio coding and transmission".
- [9] ETSI EN 300 403-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".
- [10] ETSI TS 144 018: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol (3GPP TS 44.018)".
- [11] ISO/IEC 2022: "Information technology - Character code structure and extension techniques".
- [12] ETSI ETS 300 133 (all parts): "ElectroMagnetic Compatibility and Radio Spectrum Matters (ERM); Enhanced Radio MESSage System (ERMES)".
- [13] ETSI EN 300 001: "Attachments to the Public Switched Telephone Network (PSTN); General technical requirements for equipment connected to an analogue subscriber interface in the PSTN".
- [14] ETSI EN 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; Part 1: Protocol specification".
- [15] ETSI 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".
- [16] Recommendation ITU-T T.71: "Link Access Protocol Balanced (LAPB) extended for half-duplex physical level facility".

- [17] ISO/IEC 8802-2: "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical link control".
- [18] ISO/IEC 8208: "Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment".
- [19] ISO/IEC 8348: "Information technology - Open Systems Interconnection - Network service definition".
- [20] ISO/IEC 8473 (all parts): "Information technology - Protocol for providing the connectionless-mode network service".
- [21] Recommendation ITU-T X.263: "Information technology - Protocol identification in the Network Layer".
- [22] ETSI EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [23] ETSI EN 300 207-1: "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. One (DSS1); Part 1: Protocol specification".
- [24] ETSI EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [25] ETSI EN 300 092-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [26] ETSI EN 300 093-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [27] ETSI EN 300 097-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [28] ETSI EN 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [29] ETSI EN 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; Part 1: Protocol specification".
- [30] ETSI EN 300 210-1: "Integrated Services Digital Network (ISDN); Freephone (FPH) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [31] ETSI EN 300 182-1: "Integrated Services Digital Network (ISDN); Advice of Charge (AOC) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [32] ETSI EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [33] ETSI EN 300 055-1: "Integrated Services Digital Network (ISDN); Terminal Portability (TP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

- [34] ETSI EN 300 058-1: "Integrated Services Digital Network (ISDN); Call Waiting (CW) supplementary service; Digital subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [35] ETSI EN 300 064-1: "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [36] ETSI EN 300 052-1: "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [37] ETSI EN 300 138-1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [38] ETSI EN 300 369-1: "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [39] ETSI EN 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".
- [40] ETSI EN 300 141-1: "Integrated Services Digital Network (ISDN); Call Hold (HOLD) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [41] ETSI EN 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".
- [42] Recommendation ITU-T E.182: "Application of tones and recorded announcements in telephone services".
- [43] ETSI TS 144 006: "Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Stations System (MS - BSS) Interface Data Link (DL) layer specification (3GPP TS 44.006)".
- [44] Recommendation ITU-T X.25: "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".
- [45] Recommendation ITU-T T.70: "Network-independent basic transport service for the telematic services".
- [46] ISO 1745: "Information processing - Basic mode control procedures for data communication systems".
- [47] ISO/IEC 8859-1: "Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1".
- [48] ETSI EN 300 757: "Digital Enhanced Cordless Telecommunications (DECT); Low Rate Messaging Service (LRMS); including Short Messaging Service (SMS)".
- [49] ETSI EN 300 370: "Digital Enhanced Cordless Telecommunications (DECT); Global System for Mobile communications (GSM); DECT/GSM Interworking Profile (IWP); Access and mapping (protocol/procedure description for 3,1 kHz speech service)".
- [50] ETSI EN 300 765-1: "Digital Enhanced Cordless Telecommunications (DECT); Radio in the Local Loop (RLL) Access Profile (RAP); Part 1: Basic telephony services".
- [51] ETSI EN 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".
- [52] ISO/IEC 8859-15: "Information technology - 8-bit single-byte coded graphic character sets - Part 15: Latin alphabet No. 9".

- [53] ISO/IEC 8859-7: "Information technology - 8-bit single-byte coded graphic character sets - Part 7: Latin/Greek alphabet".
- [54] ISO/IEC 8859-9: "Information technology - 8-bit single-byte coded graphic character sets - Part 9: Latin alphabet No. 5".
- [55] Recommendation ITU-T V.110: "Support by an ISDN of data terminal equipments with V-Series type interfaces".
- [56] Recommendation ITU-T V.120: "Support by an ISDN of data terminal equipment with V-Series type interfaces with provision for statistical multiplexing".
- [57] Recommendation ITU-T X.30: "Support of X.21, X.21 bis and X.20 bis based Data Terminal Equipments (DTEs) by an Integrated Services Digital Network (ISDN)".
- [58] ETSI EN 300 765-2: "Digital Enhanced Cordless Telecommunications (DECT); Radio in the Local Loop (RLL) Access Profile (RAP); Part 2: Advanced telephony services".
- [59] ISO/IEC 646: "Information technology - ISO 7-bit coded character set for information interchange".
- [60] Recommendation ITU-T X.400: "Message handling system and service overview".
- [61] ETSI TS 101 863 (all parts): "Digital Enhanced Cordless Telecommunications (DECT); DECT/UMTS Interworking Profile (IWP)".
- [62] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".
- [63] ETSI EN 300 700: "Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)".
- [64] IETF RFC 791 (STD5): "Internet Protocol".
- [65] IETF RFC 1661 (STD51): "The Point-to-Point Protocol (PPP)".
- [66] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".
- [67] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [68] Recommendation ITU-T V.42: "Error-correcting procedures for DCEs using asynchronous-to-synchronous conversion".
- [69] ETSI TS 102 265: "Digital Enhanced Cordless Telecommunications (DECT); DECT access to IP networks".
- [70] ETSI TS 102 342: "Digital Enhanced Cordless Telecommunications (DECT); Cordless multimedia communication system; Open Data Access Profile (ODAP)".
- [71] ETSI TS 102 379: "Digital Enhanced Cordless Telecommunications (DECT); Fixed network Multimedia Message Service (F-MMS) Interworking Profile".
- [72] ETSI EN 301 649: "Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Service (DPRS)".
- [73] ETSI TS 102 527-1: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 1: Wideband speech".
- [74] ETSI TS 102 527-2: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 2: Support of transparent IP packet data".
- [75] ETSI TS 102 527-3: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 3: Extended wideband speech services".

- [76] ETSI TS 102 527-4: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 4: Light Data Services; Software Update Over The Air (SUOTA), content downloading and HTTP based applications".
- [77] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".
- [78] ETSI TS 102 527-5: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 5: Additional feature set nr. 1 for extended wideband speech services".
- [79] ETSI TS 102 939-1: "Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1)".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TR 101 178: "Digital Enhanced Cordless Telecommunications (DECT); A High Level Guide to the DECT Standardization".
- [i.2] ETSI ETR 043: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Services and facilities requirements specification".
- [i.3] Recommendation ITU-T X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".
- [i.4] Recommendation ITU-T X.210: "Information technology - Open systems interconnection - Basic Reference Model: Conventions for the definition of OSI services".
- [i.5] Recommendation ITU-T T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".
- [i.6] ETSI I-ETS 300 022: "Digital cellular telecommunications system (Phase 1) (GSM); Mobile radio interface; Layer 3 specification".
- [i.7] Recommendation ITU-T E.163: "Numbering plan for the international telephone service".
- [i.8] Recommendation ITU-T E.164: "The international public telecommunication numbering plan".
- [i.9] Recommendation ITU-T X.121: "International numbering plan for public data networks".
- [i.10] Recommendation ITU-T I.460: "Multiplexing, rate adaption and support of existing interfaces".
- [i.11] IEEE 802.3: "IEEE 802.3 Systems Networking Guide: How to Optimize Your Network Using the ISO/IEC 8802-3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Standard".
- [i.12] Recommendation ITU-T Q.921: "ISDN user-network interface - Data link layer specification".
- [i.13] ETSI EN 301 238: "Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Isochronous data bearer services with roaming mobility (service type D, mobility class 2)".
- [i.14] ETSI ETS 300 435 (historical): "Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Base standard including interworking to connectionless networks (service types A and B, class 1)".
- [i.15] Recommendation ITU-T Q.931: "ISDN user-network interface layer 3 specification for basic call control".
- [i.16] Unicode <http://www.unicode.org/>.
- [i.17] ISO 8859 (all parts): "Information technology - 8-bit single-byte coded graphic character sets".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 175-1 [1], EN 300 175-7 [7], EN 300 175-8 [8] and the following apply:

active terminal/member: member of a DCDL-net that is powered-up, has locked to the MASTER and has announced itself as being present to the MASTER

DECT Local Network (DL-net): local network comprising number of DECT terminals capable of inter-communicating which may but need not be connected to an external network

LAPC: DLC layer C-plane protocol entity

MASTER: specially dedicated terminal determining the DCDL-net synchronization and providing means of intra DCDL-net control and exchange of information

NOTE: By definition a MASTER is always an Active terminal.

3.2 Symbols and abbreviations

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

3PTY	Three ParTY
AAC-LD	Advanced Audio Coding-Low Delay
AC	Authentication Code
ACC	ACCount number
ACK	ACKnowledgement
ADPCM	Adaptive Differential Pulse Code Modulation
AK	Authentication Key
AOC	Advice Of Charge
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity
ASCII	American Standard Code for Information Interchange
A-VOL	Adaptive - VOLUME
BA (bits)	B-field identification bits, a group of bits in the A-field header (MAC layer)
BACN	Bank ACcount Number
BCD	Binary Coded Decimal
BRAT	Basic Rate Adaption Service
B _S	Slow Broadcast channel
C/L	ConnectionLess mode
C/O	Connection Oriented mode
CACN	Credit card ACcount Number
CAI	Common Air Interface
CAP	CTM Access Profile
CBI	Collective Broadcast Identifier
CC	Call Control
CCBS	Completion of Calls to Busy Subscriber
CCEI	Call Control Endpoint Identifier
CD	Call Deflection
C _F	higher layer signalling Channel (fast)
CFB	Call Forwarding Busy
CFM	ConFirM
CFNR	Call Forwarding No Reply
CFU	Call Forwarding Unconditional
CH	Call Hold
CI	Cell Identity

CI	Common Interface
CISS	Call Independent Supplementary Services
CK	Cipher Key
CL	Connection Less
CL	higher layer ConnectionLess channel (protected; see CL _S and CL _F)
CLEI	CLMS Endpoint Identifier
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CLMS	ConnectionLess Message Service
CLSS	ConnectionLess Supplementary Service
CNIP	Calling Name Identification Presentation
COEI	COMS Endpoint Identifier
COLP	COConnected Line identification Presentation
COLR	COConnected Line identification Restriction
COMS	Connection Oriented Message Service
CONF	CONference call add-on
C-plane	Control plane
CRC	Cyclic Redundancy Check
CRSS	Call Related Supplementary Services
CSDb	Common System Database
C _S	higher layer signalling Channel (slow)
CS	Call Status
CT2	Cordless Telecommunication 2nd Generation
CTA	Cordless Terminal Adapter
CTM	Cordless Terminal Mobility
CUG	Closed User Group
CW	Call Waiting
D-CAM	Digital CAMera
DCDL-net	Distributed Communication DECT Local-network
DCK	Derived Cipher Key
DDI	Direct Dialling In
DefCK	Default Cipher Key
DLC	Data Link Control
DLEI	Data Link Endpoint Identifier (DLC layer)
DL-net	DECT Local-network
DMAP	DECT Multimedia Access Profile
DPRS	DECT Packet Radio Service
DSAA	DECT Standard Authentication Algorithm
DSAA2	DECT Standard Authentication Algorithm #2
DSC	DECT Standard Cipher (algorithm)
DSC2	DECT Standard Cipher (algorithm) #2
DTAM	Digital Telephone Answering Machine
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
ECN	Exchanged Connection Number (DLC/MAC layer)
ECT	Explicit Call Transfer
EIC	Equipment Installer's Code
ELI	Extended Location Information
EMC	Equipment Manufacturer Code
ER	Error Resilient
ERMES	European Radio MESSaging System
ETI	Extended Transaction Identifier
E+U type	B-field multiplexer mode when the slot carries U-plane data (channel I _{PF}) and signalling (channels G _F and M)
F	Flag
F-CC	FT side-Call Control
F-IWU	FT-InterWorking Unit
F-MMS	Fixed net-Multimedia Messaging Service
FP	Fixed Part
FPH	FreePHone
FREL	Frame RELay service

FT	Fixed radio Termination
FU	DECT DLC U-Plane Frame format
GAP	Generic Access Profile
GEA	GPRS encryption algorithm
G _F	higher layer information control channel (a logical channel to the MAC layer)
GMT	Greenwich Mean Time
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HyP	Hybrid Part
IA5	International Alphabet No.5 (see Recommendation ITU-T T.50 [i.5])
ID	IDentifier
IdN	Identity Number
IE	Information Element
IETF	Internet Engineering Task Force
IIP	Intermediate ISDN access Profile
IMSI	International Mobile Subscriber Identity
I _N	higher layer Information channel (unprotected), (logical channels to the MAC layer)
I _{NA}	higher layer Information channel (unprotected), minimum delay operation
I _{NB}	higher layer Information channel (unprotected), normal delay operation
IND	INDication
IP	Internet Protocol
I _P	higher layer Information channel (Protected), (logical channels to the MAC layer)
I _{PF}	higher layer Information channel (protected) transported multiplexed with signalling in the E+U type slots
I _{PM}	higher layer Information channel (protected) with multi subfield format
I _{PMR}	higher layer Information channel (protected) with multi subfield format, with error correction using MOD-2 retransmission mechanism
I _{PQ}	higher layer Information channel (protected) with single subfield format
I _{PQR}	higher layer Information channel (protected) with single subfield format, with error correction using MOD-2 retransmission mechanism
I _{PX}	higher layer Information channel, encodec protected, minimum delay operation
IPEI	International Portable Equipment Identity
IPIU	International Portable User Identity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRV	International Reference Version
ISDN	Integrated Services Digital Network
IWP	Interworking Profile
IWU	InterWorking Unit
KS'	FP authentication Session Key
KS	PP authentication Session Key
LA	Location Area
LAC	Location Area Code
LAL	Location Area Level
LAN	Local Area Network
LAPC	A reliable C-plane DLC link
LCE	Link Control Entity
LCN	Logical Connection Number
LF	Line Feed
LF	Length of called party First name
LI	Location Information
LiA	List Access
LLC	Logical Link Control
LLME	Lower Layer Management Entity
LLN	Logical Link Number
LN	Length of called party Name
LRMS	Low Rate Messaging Service
LS	Least Significant

LSB	Least Significant Bit
LU	DECT DLC U-Plane Service
MAC	Medium Access Control
MBC	Multi-Bearer Control
MCC	Mobile Country Code
MCE	Message Control Entity
MCID	Malicious Call IDentification
ME	Management Entity
MFPB	Multi-Frequency Push Button
MI	Message Identifier
MM	Mobility Management
MMI	Man-Machine Interface
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MRAP	Multimedia in Radio in the local loop Access Profile
MS	Mobile Station
MS	Most Significant
MSB	Most Significant Bit
MSN	Multiple Subscriber Number
M _T	MAC control channel on A-tail field, or one message on such channel
NDT	Network Delay Type
NG-DECT	New Generation DECT
NIC	Network Independent Clock
NLR	No Link Required
N-REJ	Noise Rejection
NWK	NetWoRK
NSAP (address)	Network Service Access Point (address)
OA&M	Operation Administration and Management
ODAP	Open Data Access Profile
OID	Other fixed part ID
OSI	Open Systems Interconnection
PARI	Primary Access Rights Identity
PARK	Portable Access Rights Key
PBX	Private Branch eXchange
P-CC	PT side-Call Control
PC	Personal Computer
PCM	Pulse Code Modulation
PD	Protocol Discriminator
PDU	Protocol Data Unit
PLI	Park Length Indicator
PLMN	Public Land Mobile Network
PMID	Portable part MAC IDentity (MAC layer)
POC	Public Operator Code
PP	Portable Part
PPP	Point-to-Point Protocol
PSCN	Primary receiver Scan Carrier Number
PSN	Portable equipment Serial Number
PSTN	Public Switched Telephone Network
PT	Portable radio Termination
P-TMSI	Packet-Temporary Mobile Subscriber Identity
PUI	Portable User Identity
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
RAP	Radio in the local loop Access Profile
REJ	REJect
REP	REpeater Part
RES	RESponse
RES1	a RESponse calculated by a PT
RES2	a RESponse calculated by a FT

RFC	Request For Comments
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RLL	Radio in the Local Loop
RPN	Radio fixed Part Number
RS	cryptographic parameter used in the calculation of authentication session keys
RSS	Radio Signal Strength
SAP	Service Access Point
SAPI	Service Access Point Identifier
SARI	Secondary Access Rights Identity
SCK	Static Cipher Key
SCT	Second Call Type
SDU	Service Data Unit
SIM	Subscriber Interface Module
SIP	Session Initiation Protocol
SI _{PF}	higher layer connectionless channel (protected) transported multiplexed with signalling in the E+U type slots
SMS	Short Message Service
SS	Supplementary Services
STD	STandarD
SUB	SUBaddressing
TA (bits)	Tail identification bits, a group of bits in the A-field header (MAC layer)
TARI	Tertiary Access Rights Identity
TBC	Traffic Bearer Control
TCL	Telephone Coupling Loss
TCL _w	weighted Terminal Coupling Loss
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TI	Transaction Identifier
TIF	Transaction Identifier Flag
TMSI	Temporary Mobile Subscriber Identity
TP	Terminal Portability
TPUI	Temporary Portable User Identity
TV	Transaction Value
TVX	Transaction Value (eXtended)
UAK	User Authentication Key
UCS	Universal Character Set
UI	User Interface
ULE	Ultra Low Energy
ULN	U-plane Link Number
UMTS	Universal Mobile Telecommunications System
UPI	User Personal Identification
U-plane	User plane
U-type	B-field multiplexer mode when the slot carries U-plane data only (channels I _N or I _P)
UTF-8	UCS Transformation Format—8-bit
UUS	User to User Signalling
WRS	Wireless Relay Station
ZAP	ability first to assign and then to re-program the account data held in the PP

4 Overview of the NWK layer

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

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 the Lower Layer Management Entity (LLME). This provides coordination 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 EN 300 403-1 [9]. Many of the alterations adopted in I-ETS 300 022 [i.6] have also been adopted here.

The other groups of procedures are also based on the similar groupings as defined in I-ETS 300 022 [i.6].

Neither of these source documents can serve as a detailed reference for the present document, 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.

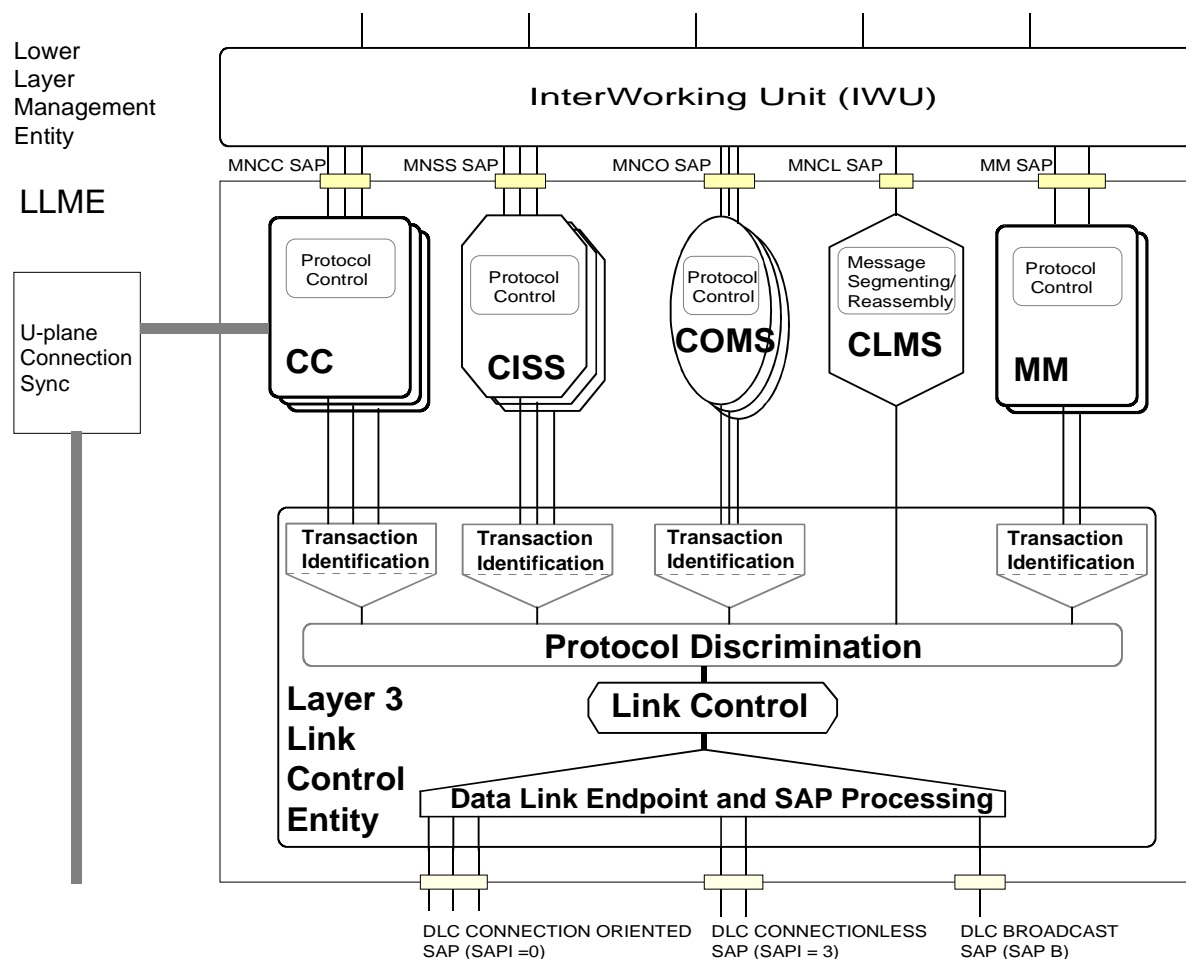


Figure 1b: C-plane model

The U-plane is completely null at the NWK layer. LUX (x = 1 to 15) is mapped to NUx (x = 1 to 15).

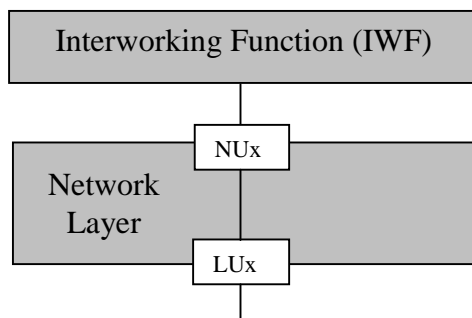


Figure 2: U-plane model

5 Overview of procedures

5.1 General

Each of the functional groupings (each entity) defined in clause 4 is described separately, and has 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 1b) 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.

The present document only considers the provision and coordination 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 the present document.

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 1b.

All of the procedures are based on the exchange of messages between peer entities. The present document uses two distinct formats of message:

- S-FORMAT messages; these messages have a similar structure to EN 300 403-1 [9] and I-ETS 300 022 [i.6];
- B-FORMAT messages; these messages are specially coded to meet the physical constraints of the broadcast service. They are not similar to EN 300 403-1 [9] 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 setup

Call setup involves the exchange of some of the following information between the originator and the responding side of the call:

- International Portable User Identity (IPUI), International Portable Equipment Identity (IPEI) or Temporary Portable User Identity (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 setup can be originated by either side (FT or PT or HyP).

NOTE 1: The HyP may initiate calls behaving as FT or PT, therefore the present document in general talks for communication between PT and FT assuming that this may be as well a HyP behaving as PT or FT. For the exact procedure related to HyP see annex I.

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

NOTE 2: One exception from this rule is e.g. the Collective Ringing described in clause 14.4. In this case in order to initiate a call setup, the IWU requests directly the LCE to page one or more PPs and the PP is expected to initiate a call setup which will be mapped to the call in the IWU.

This first call setup 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 setup message may not contain all of the setup 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 setup and shall respond with a positive message such as setup acknowledge. This reply, and all future replies, adopt the transaction identifier defined by the initial call setup message.

If the setup 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 setup 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

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

SS 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 SS, 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 clause 6.3.

This protocol applies to SS 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 clause 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 SS 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 SS. The first category, called the separate message approach, utilizes 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, utilizes the <<FACILITY>> information element and applies only to SS that do not require synchronization 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 setup 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 setup can be originated by either side (FT or PT).

The IWU can request a COMS entity to initiate a call setup at any time. The COMS then submits a call setup 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 setup 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 setup is successful, the complete setup 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 setup message.

If the COMS setup is unsuccessful, the originating entity will timeout. If the setup 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 setup 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 Recommendation ITU-T X.25 [44] 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 eight 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;
- h) external protocol information procedure.

These groups are briefly described in this clause. 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 clause 15.5.

5.6.2 Identity procedures

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

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.

The authentication procedures may be based on the DECT Standard Authentication Algorithm (DSAA), the DECT Standard Authentication Algorithm #2 (DSAA2) or proprietary algorithms.

See clause 13.3 for detailed description of the authentication procedures.

5.6.4 Location procedures

The location procedures are necessary for incoming call provision. They are designed to allow the FT to minimize 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

Three procedures are defined, one for obtaining the access rights, one for terminating the access rights and one for modifying 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 or/and at the base 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 another 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.

The procedure for modifying the access rights is used to change IPUI or PARK or PLI in the PT without user intervention.

5.6.6 Key allocation procedure

This procedure can be used to replace an Authentication Code (AC) by an UAK. For calculating the UAK the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) 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.

See clause 13.6 for detailed description of the procedure.

5.6.7 Parameter retrieval procedure

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

The procedure may be used for transmission of parameters needed in various other procedures, e.g. RPN for a WRS, DCCL-net active members specific information, dynamically assigned setup capabilities, etc.

5.6.8 Ciphering related procedure

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

5.6.9 External protocol information procedure

This procedure is used to provide means for exchange of external to the DECT protocol stack information.

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 (see note);
- 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 NWK layer instances to existing data link endpoints;
- i) reporting data link failures to all NWK layer instances that are using that link.

NOTE: A LCE-REQUEST-PAGE message may be transmitted over an existing link if it is used for resume paging.

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 create a single mapping, but the selection procedures are not defined in the present document.

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 shall determine the appropriate method of establishment. Two methods are defined:
 - direct establishment, for all PT initiations and for FT initiations where "fast DLC setup" is supported;
 - indirect establishment, for all other cases, including failure of FT initiated "fast DLC setup".

Indirect establishment uses the request paging procedures described in clause 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 EN 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 clause 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 clause 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 clause 5.7.7. The existence of queued messages for a suspended link should cause immediate resumption of that link.

NOTE: DECT standard provides two suspend/resume procedures. Data link suspend and resume which is described in the present document, and MAC suspend and resume described in EN 300 175-3 [3].

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 EN 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 clause 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 or the assigned individual TPUI of the responding PT (see clause 14.2.3).

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 clause 6.2. These summaries include both S-FORMAT messages and B-FORMAT messages.

Clauses 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 clause 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 clause 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)

	Direction	Clause
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

	Direction	Clause
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

	Direction	Clause
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

	Direction	Clause
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

	Direction	Clause
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
External protocol messages		
{MM-IWU}	Both	6.3.6.27
Internal protocol information message		
{MM-NOTIFY}	F=>P	6.3.6.28

6.2.6 Summary of LCE messages

Table 6: LCE message summary

	Direction	Clause
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 clause 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.
- c) further explanatory notes as required.

The fixed length information elements are always transmitted over the air in the order as they appear in the message tables, this order is mandatory for all instances of the message. The variable-length information elements are transmitted over the air in ascending numerical order, according to clause 7.5.1. Receiver implementations shall take account of the possibility that further information elements may be inserted in the messages in future editions of the present document.

6.3.2 CC-messages

6.3.2.1 {CC-SETUP}

This message is sent to initiate call establishment.

Table 7: {CC-SETUP}

Message Type		Format		Directions
{CC-SETUP}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	7 to 20
Fixed identity (see note 11)	7.7.18	M	M	5 to 20
NWK assigned identity	7.7.28	N	O	5 to 20
Basic service (see note 1)	7.6.4	M	M	2
Repeat Indicator (see note 3)	7.6.3	O	O	1
IWU attributes (see note 1)	7.7.21	M/N	M/N	6 to 12
Repeat Indicator (see note 2)	7.6.3	O	O	1
Call attributes (see notes 1 and 2)	7.7.5	O	O	6 to 8
Repeat Indicator (see note 3)	7.6.3	O	O	1
Connection attributes (see note 3)	7.7.11	O	O	7 to 12
Cipher info	7.7.10	O	O	4 to 5
Connection identity	7.7.12	O	O	≥ 3
Repeat indicator (see note 12)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Repeat indicator (see note 12)	7.6.3	O	N	1
Progress Indicator	7.7.31	O	N	4
Single-Display (see note 14)	7.6.5	O	N	2
Multi-Display (see note 14)	7.7.26	O	N	≥ 2
Single-Keypad (see notes 10 and 15)	7.6.6	N	O	2

Information Element	Clause	F to P message	P to F message	Length octets
Multi-Keypad (see notes 10 and 15)	7.7.27	N	O	≥ 2
Signal (see note 5)	7.6.8	O	N	2
Feature Activate	7.7.16	N	O	3 to 4
Feature Indicate	7.7.17	O	N	≥ 4
Network parameter (see note 8)	7.7.29	O	O	≥ 3
Ext h/o indicator	7.7.51	O	N	3
Terminal capability	7.7.41	N	O	6 to 19
End-to-end compatibility (see note 9)	7.7.14	O	O	3 to 6
Rate parameters (see note 7)	7.7.33	O	O	6 to 9
Transit Delay (see note 6)	7.7.42	O	O	3 to 6
Window size (see note 6)	7.7.43	O	O	4 to 10
Calling Party Number	7.7.9	O	O	≥ 3
Calling Party Name	7.7.53	O	O	≥ 2
Called Party Number (see note 10)	7.7.7	O	O	≥ 4
Called Party Subaddr	7.7.8	O	O	≥ 4
Sending Complete (see note 4)	7.6.2	O	O	1
Repeat indicator (see note 12)	7.6.3	O	O	1
Segmented info (see note 13)	7.7.37	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	≥ 4
Codec List	7.7.54	O	O	≥ 6
Call information	7.7.56	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 "prioritized list" for negotiation. Up to three versions of the <<CALL-ATTRIBUTES>> element may then follow (see clause 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-prioritized 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 setup of a rate adaption service (see EN 300 175-4 [4]).				
NOTE 8: Included only as part of external handover.				
NOTE 9: Mandatory for services using LU6 (Recommendations ITU-T V.110 [55] and X.30 [57] rate adaption).				
NOTE 10: Called party number information may be conveyed either in the <<CALLED-PARTY-NUMBER>> element or in the <<MULTI-KEYPAD>> element (but not in the <<SINGLE-KEYPAD>> element). When the <<CALLED-PARTY-NUMBER>> element is used, the <<SINGLE-KEYPAD>> or the <<MULTI-KEYPAD>> elements may also be included to convey other call establishment information (but not the called party number). See also informative note after the table.				
NOTE 11: This information element may contain zero length contents if the setup message is used in an ARI-D (GSM/UMTS) 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-prioritized list".				
NOTE 13: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				
NOTE 14: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				
NOTE 15: The message may contain either the <<SINGLE-KEYPAD>> element, or the <<MULTI-KEYPAD>> element, but not both.				

NOTE: Generic Access Profile (GAP) [51] does not transport the called party number in {CC-SETUP}. Instead of it, the <<MULTI-KEYPAD>> IE transported over a separate {CC-INFO} message is used.

6.3.2.2 {CC-INFO}

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

Table 8: {CC-INFO}

Message Type		Format		Directions
{CC-INFO}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Location area (see note 4)	7.7.25	N	O	≥ 3
NWK assigned identity (see note 4)	7.7.28	N	O	5 to 20
Repeat indicator (see note 5)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Repeat indicator (see note 5)	7.6.3	O	N	1
Progress Indicator	7.7.31	O	N	4
Single-Display (see note 6)	7.6.5	O	N	2
Multi-Display (see note 6)	7.7.26	O	N	≥ 2
Single-Keypad (see note 1)	7.6.6	O	O	2
Multi-Keypad (see note 1)	7.7.27	O	O	≥ 2
Signal	7.6.8	O	N	2
Feature Activate	7.7.16	N	O	3 to 4
Feature Indicate	7.7.17	O	N	≥ 4
Network parameter (see note 4)	7.7.29	O	O	≥ 3
Ext h/o indicator	7.7.51	O	N	3
Calling Party Number	7.7.9	O	O	≥ 3
Calling Party Name	7.7.53	O	O	≥ 2
Called Party Number (see notes 1 and 3)	7.7.7	O	O	≥ 4
Called Party Subaddr (see note 3)	7.7.8	O	O	≥ 4
Sending Complete (see note 2)	7.6.2	O	O	1
Test Hook Control	7.6.10	O	N	2
Called Party Name	7.7.52	O	N	≥ 5
Repeat indicator (see note 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	≥ 4
Codec List	7.7.54	O	O	≥ 6
Call information	7.7.56	O	O	≥ 2
M = Mandatory. N = Not allowed. O = Optional.				
NOTE 1: The message may contain either the <<CALLED-PARTY-NUMBER>> element, the <<SINGLE-KEYPAD>> element, or the <<MULTI-KEYPAD>> element, but only one of them. See also informative note after the table.				
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-prioritized list".				
NOTE 6: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

NOTE: Generic Access Profile (GAP) [51] does not allow the use of the <<CALLED-PARTY-NUMBER>> element in {CC-INFO} for carrying the called party number. Instead of it, the <<MULTI-KEYPAD>> IE is used.

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.

Table 9: {CC-SETUP-ACK}

Message Type		Format		Directions
{CC-SETUP-ACK}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Info type (see note 3)	7.7.20	O	-	≥ 3
Portable identity	7.7.30	O	-	7 to 20
Fixed identity	7.7.18	O	-	5 to 20
Location area	7.7.25	O	-	≥ 3
IWU attributes	7.7.21	O	-	6 to 12
Call Attributes (see note 4)	7.7.5	O	-	6 to 8
Connection attributes	7.7.11	O	-	7 to 12
Connection identity	7.7.12	O	-	≥ 3
Repeat indicator (see note 7)	7.6.3	O	-	1
Facility	7.7.15	O	-	≥ 4
Repeat indicator (see note 7)	7.6.3	O	-	1
Progress Indicator	7.7.31	O	-	4
Single-Display (see note 9)	7.6.5	O	-	2
Multi-Display (see note 9)	7.7.26	O	-	≥ 2
Signal (see note 2)	7.6.8	O	-	2
Feature Indicate	7.7.17	O	-	≥ 4
Network parameter (see note 8)	7.7.29	O	-	≥ 3
Ext h/o indicator	7.7.51	O	-	3
Transit Delay (see note 5)	7.7.42	O	-	3 to 6
Window size (see note 5)	7.7.43	O	-	4 to 10
Delimiter request (see note 6)	7.6.2	O	-	1
Repeat indicator (see note 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	-	≥ 4
Codec List	7.7.54	O	-	≥ 6
Call information	7.7.56	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 prioritized 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-prioritized list". NOTE 8: Included only as part of external handover. NOTE 9: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 10: {CC-CALL-PROC}

Message Type		Format		Directions
{CC-CALL-PROC}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	N	1/2
Transaction Identifier	7.3	M	N	1/2
Message Type	7.4	M	N	1
IWU attributes	7.7.21	O	N	5 to 12
Call Attributes (see note 3)	7.7.5	O	N	6 to 8
Connection attributes	7.7.11	O	N	7 to 12
Connection identity	7.7.12	O	N	≥ 3
Repeat indicator (see note 5)	7.6.3	O	N	1
Facility	7.7.15	O	N	≥ 4
Repeat indicator (see note 5)	7.6.3	O	N	1
Progress indicator	7.7.31	O	N	4
Single-Display (see note 6)	7.6.5	O	N	2
Multi-Display (see note 6)	7.7.26	O	N	≥ 2
Signal (see note 2)	7.6.8	O	N	2
Feature Indicate	7.7.17	O	N	≥ 4
Transit Delay (see note 4)	7.7.42	O	N	3 to 6
Window size (see note 4)	7.7.43	O	N	4 to 10
Called Party Number	7.7.7	O	N	≥ 4
Called Party Name	7.7.52	O	N	≥ 5
Repeat indicator (see note 5)	7.6.3	O	N	1
IWU-TO-IWU	7.7.23	O	N	≥ 4
IWU-PACKET	7.7.22	O	N	≥ 4
Escape to proprietary	7.7.45	O	N	≥ 4
Codec List	7.7.54	O	N	≥ 6
Call information	7.7.56	O	N	≥ 2
M = Mandatory.				
O = Optional.				
N = 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 prioritized 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-prioritized list".				
NOTE 6: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.2.5 {CC-ALERTING}

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

Table 11: {CC-ALERTING}

Message Type		Format		Directions
{CC-ALERTING}		S		Both

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
IWU attributes	7.7.21	O	O	6 to 12
Call Attributes (see note 2)	7.7.5	O	O	6 to 8
Connection attributes	7.7.11	O	O	7 to 12
Connection identity	7.7.12	O	O	≥ 3
Repeat indicator (see note 4)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Repeat indicator (see note 4)	7.6.3	O	N	1
Progress Indicator	7.7.31	O	N	4
Single-Display (see note 5)	7.6.5	O	N	2
Multi-Display (see note 5)	7.7.26	O	N	≥ 2
Signal (see note 1)	7.6.8	O	N	2
Feature Indicate	7.7.17	O	N	≥ 4
Terminal capability	7.7.41	N	O	6 to 19
Transit Delay (see note 3)	7.7.42	O	O	3 to 6
Window size (see note 3)	7.7.43	O	O	4 to 10
Called Party Number	7.7.7	O	N	≥ 4
Called Party Name	7.7.52	O	N	≥ 5
Repeat indicator (see note 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	≥ 4
Codec List	7.7.54	O	O	≥ 6
Call information	7.7.56	O	N	≥ 2

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

NOTE 1: Included if the FT optionally provides additional information describing tones.
NOTE 2: Included if prioritized 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-prioritized list".
NOTE 5: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.

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.

Table 12: {CC-CONNECT}

Message Type		Format		Directions
{CC-CONNECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
IWU attributes	7.7.21	O	O	6 to 12
Call Attributes (see note 2)	7.7.5	O	O	6 to 8
Connection attributes	7.7.11	O	O	7 to 12
Connection identity	7.7.12	O	O	≥ 3
Repeat indicator (see note 4)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Repeat indicator (see note 4)	7.6.3	O	N	1
Progress Indicator	7.7.31	O	N	4
Single-Display (see note 7)	7.6.5	O	N	2
Multi-Display (see note 7)	7.7.26	O	N	≥ 2
Signal (see note 1)	7.6.8	O	N	2
Feature Indicate	7.7.17	O	N	≥ 4
Network parameter (see note 5)	7.7.29	O	N	≥ 3
Ext h/o indicator	7.7.51	O	N	3
Terminal capability	7.7.41	N	O	6 to 19
Transit Delay (see note 3)	7.7.42	O	O	3 to 6
Window size (see note 3)	7.7.43	O	O	4 to 10
Called Party Number	7.7.7	O	N	≥ 4
Called Party Name	7.7.52	O	N	≥ 5
Repeat indicator (see note 4)	7.6.3	O	O	1
Segmented info (see note 6)	7.7.37	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	≥ 4
Codec List	7.7.54	O	O	≥ 6
Call information	7.7.56	O	N	≥ 2
M = Mandatory. N = Not allowed. O = Optional.				
NOTE 1: Included if the FT optionally provides additional information describing tones.				
NOTE 2: Included if prioritized 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-prioritized list".				
NOTE 5: Included only as part of external handover.				
NOTE 6: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				
NOTE 7: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 13: {CC-CONNECT-ACK}

Message Type		Format		Directions
{CC-CONNECT-ACK}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	O	N	≥ 2
Feature Indicate	7.7.17	O	N	≥ 4
Repeat indicator (see note 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	≥ 4
M = Mandatory.				
O = Optional.				
N = Not applicable.				
NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-to-IWU>> information elements indicating "non-prioritized list".				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 14: {CC-RELEASE}

Message Type		Format		Directions
{CC-RELEASE}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
Repeat indicator (see note 1)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Repeat indicator (see note 1)	7.6.3	O	O	1
Progress indicator	7.7.31	O	O	4
Single-Display (see note 3)	7.6.5	O	N	2
Multi-Display (see note 3)	7.7.26	O	N	≥ 2
Feature Indicate	7.7.17	O	N	≥ 4
Repeat indicator (see note 1)	7.6.3	O	N	1
Segmented info (see note 2)	7.7.37	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	≥ 4
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-prioritized list". NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages. NOTE 3: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 15: {CC-RELEASE-COM}

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

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
Identity type (see note 3)	7.7.19	O	N	4
Location area (see note 3)	7.7.25	O	N	≥ 3
IWU attributes (see note 1)	7.7.21	O	O	6 to 12
Connection attributes (see note 1)	7.7.11	O	O	7 to 12
Repeat indicator (see note 4)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Single-Display (see note 6)	7.6.5	O	N	2
Multi-Display (see note 6)	7.7.26	O	N	≥ 2
Feature Indicate	7.7.17	O	N	≥ 4
Network parameter (see note 2)	7.7.29	O	N	≥ 3
Repeat indicator (see note 4)	7.6.3	O	O	1
Segmented info (see note 5)	7.7.37	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	≥ 4

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

NOTE 1: The <<IWU-ATTRIBUTES>> and the <CONNECTION ATTRIBUTES> elements are only included if exchanged attribute negotiation is supported (see clause 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-prioritized list".
NOTE 5: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.
NOTE 6: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.

6.3.2.10 {CC-SERVICE-CHANGE}

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

Table 16: {CC-SERVICE-CHANGE}

Message Type		Format		Directions
{CC-SERVICE-CHANGE}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	7 to 20
IWU attributes	7.7.21	O	O	6 to 12
Call attributes	7.7.5	O	O	6 to 8
Service Change Info	7.7.38	M	M	4 to 5
Repeat Indicator (see note 1)	7.6.3	O	O	1
Connection Attributes (see note 1)	7.7.11	M/O	M/O	7 to 12
Connection identity (see note 2)	7.7.12	M/O	M/O	≥ 3
Transit delay	7.7.42	O	O	3 to 6
Window Size	7.7.43	O	O	4 to 10
ULE MAC Configuration Info	7.7.58	O	O	≥ 3
Repeat indicator (see note 3)	7.6.3	O	O	1
Segmented info (see note 4)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
Codec List	7.7.54	O	O	≥ 6
M = Mandatory.				
O = Optional.				
NOTE 1: The <<CONNECTION-ATTRIBUTES>> element is mandatory for certain service changes (see clause 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-prioritized list".				
NOTE 2: The <<CONNECTION-IDENTITY>> element is mandatory for certain service changes. See clause 9.6.				
NOTE 3: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-TO-IWU>> information elements indicating "non-prioritized list".				
NOTE 4: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

6.3.2.11 {CC-SERVICE-ACCEPT}

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

Table 17: {CC-SERVICE-ACCEPT}

Message Type		Format		Directions
{CC-SERVICE-ACCEPT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
IWU attributes	7.7.21	O	O	6 to 12
Call attributes	7.7.5	O	O	6 to 8
Connection identity (see note 1)	7.7.12	O	O	≥ 3
Transit delay	7.7.42	O	O	3 to 6
Window Size	7.7.43	O	O	4 to 10
ULE MAC Configuration Info	7.7.58	O	O	≥ 3
Repeat indicator (see note 2)	7.6.3	O	O	1
Segmented info (see note 3)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional.				
NOTE 1: The <<CONNECTION-IDENTITY>> element is mandatory for certain service changes (see clause 9.6.4).				
NOTE 2: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-TO-IWU>> information elements indicating "non-prioritized list".				
NOTE 3: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

6.3.2.12 {CC-SERVICE-REJECT}

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

Table 18: {CC-SERVICE-REJECT}

Message Type		Format		Directions
{CC-SERVICE-REJECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
IWU attributes	7.7.21	O	O	6 to 12
Connection attributes	7.7.11	O	O	7 to 12
Repeat indicator (see note 1)	7.6.3	O	O	1
Segmented info (see note 2)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional.				
NOTE 1: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<IWU-TO-IWU>> information elements indicating "non-prioritized list".				
NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

6.3.2.13 {CC-NOTIFY}

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

Table 19: {CC-NOTIFY}

Message Type		Format		Directions
{CC-NOTIFY}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	≥ 4
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.

Table 20: {IWU-INFO}

Message Type		Format		Directions
{IWU-INFO}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	O	O	7 to 20
MMS Generic Header	7.7.47	O	O	≥ 2
MMS Object Header	7.7.48	O	O	≥ 2
Repeat Indicator (see note 1)	7.6.3	O	O	1
MMS Extended Header	7.7.49	O	O	≥ 2
Repeat Indicator (see note 1)	7.6.3	O	O	1
Time-Date	7.7.50	O	O	6 to 10
ULE MAC Configuration Info	7.7.58	O	O	≥ 3
Repeat Indicator (see note 1)	7.6.3	O	O	1
Calling Party Number	7.7.9	O	O	≥ 3
Calling Party Name	7.7.53	O	O	≥ 2
Repeat Indicator (see note 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 (see note 1)	7.6.3	O	O	1
Segmented info (see note 2)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	O	≥ 4
Segmented info (see note 2)	7.7.37	O	O	4
IWU-PACKET	7.7.22	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
Codec List	7.7.54	O	O	≥ 6
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>>, and <<IWU-TO-IWU>> information elements indicating "non-prioritized list".

NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> or <<IWU-PACKET>> information element whenever the IE is segmented over a number of consecutive messages.

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.

Table 21: {FACILITY}

Message Type		Format		Directions
{FACILITY}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable Identity	7.6.30	N	M/O (see note 2)	7 to 20
Repeat indicator (see note 1)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Time-Date	7.7.50	O	O	6 to 10
Single-Display (see note 3)	7.6.5	O	N	2
Multi-Display (see note 3)	7.7.26	O	N	≥ 2
Single-Keypad (see note 4)	7.6.6	N	O	2
Multi-Keypad (see note 4)	7.7.27	N	O	≥ 2
Feature Activate	7.7.16	N	O	3 to 4
Feature Indicate	7.7.17	O	N	≥ 4
Repeat indicator (see note 1)	7.6.3	O	O	1
List change details	7.7.57	O	O	≥ 2
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
Events notification	7.7.55	O	O	≥ 4
Call information	7.7.56	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-prioritized list". NOTE 2: M for {FACILITY} used for CLSS, O otherwise. NOTE 3: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both. NOTE 4: The message may contain either the <<SINGLE-KEYPAD>> element, or the <<MULTI-KEYPAD>> element, but not both.				

6.3.3.2 {HOLD}

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

Table 22: {HOLD}

Message Type		Format		Directions
{HOLD}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	O	N	≥ 2
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory.				
N = Not allowed.				
O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 23: {HOLD-ACK}

Message Type		Format		Directions
{HOLD-ACK}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	O	N	≥ 2
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory.				
N = Not allowed.				
O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 24: {HOLD-REJECT}

Message Type		Format		Directions
{HOLD-REJECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	O	N	≥ 2
Reject Reason	7.7.34	O	O	3
Repeat indicator (see note 1)	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
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-prioritized list".				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.3.5 {RETRIEVE}

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

Table 25: {RETRIEVE}

Message Type		Format		Directions
{RETRIEVE}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	O	N	≥ 2
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 26: {RETRIEVE-ACK}

Message Type		Format		Directions
{RETRIEVE-ACK}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	O	N	≥ 2
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 27: {RETRIEVE-REJECT}

Message Type		Format		Directions
{RETRIEVE-REJECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	O	N	≥ 2
Reject Reason	7.7.34	O	O	3
Repeat indicator (see note 1)	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
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-prioritized list".				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 28: {CISS-REGISTER}

Message Type		Format		Directions
{CISS-REGISTER}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity (see note 1)	7.7.30	O	M	7 to 20
Repeat indicator (see note 2)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Single-Display (see note 3)	7.6.5	O	N	2
Multi-Display (see note 3)	7.7.26	O	N	≥ 2
Single-Keypad (see note 4)	7.6.6	N	O	2
Multi-Keypad (see note 4)	7.7.27	N	O	≥ 2
Feature Activate	7.7.16	N	O	3 to 4
Feature Indicate	7.7.17	O	N	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE 1: For Call Independent Supplementary Services the FP may not be able to derive the Portable Identity if this information element is not included. NOTE 2: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<FACILITY>> information elements indicating "non-prioritized list". NOTE 3: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both. NOTE 4: The message may contain either the <<SINGLE-KEYPAD>> element, or the <<MULTI-KEYPAD>> element, but not both.				

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.

Table 29: {CISS-RELEASE-COM}

Message Type		Format		Directions
{CISS-RELEASE-COM}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
Repeat indicator (see note 1)	7.6.3	O	O	1
Facility	7.7.15	O	O	≥ 4
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	O	N	≥ 2
Single-Keypad (see note 3)	7.6.6	N	O	2
Multi-Keypad (see note 3)	7.7.27	N	O	≥ 2
Feature Activate	7.7.16	N	O	3 to 4
Feature Indicate	7.7.17	O	N	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
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-prioritized list".				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				
NOTE 3: The message may contain either the <<SINGLE-KEYPAD>> element, or the <<MULTI-KEYPAD>> element, but not both.				

6.3.4 COMS-messages

6.3.4.1 {COMS-SETUP}

This message is used to initiate a COMS call.

Table 30: {COMS-SETUP}

Message Type		Format		Directions
{COMS-SETUP}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2.	M	M	1/2
Transaction Identifier	7.3.	M	M	1/2
Message Type	7.4.	M	M	1
Portable identity (see note 1)	7.7.30	M	M	7 to 20
Fixed identity (see note 1)	7.7.18	M	M	5 to 20
IWU attributes	7.7.21	M	M	6 to 12
Connection attributes	7.7.11	O	O	7 to 12
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	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	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE 1: <<Portable identity>> and <<Fixed identity>> are mandatory for direct data link establishment (see clause 14.2).				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.4.2 {COMS-INFO}

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

Table 31: {COMS-INFO}

Message Type		Format		Directions
{COMS-INFO}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note 2)	7.6.5	O	N	2
Multi-Display (see note 2)	7.7.26	O	N	≥ 2
Segmented info (see note 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	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE 1: The <<SEGMENTED-INFO>> element is used if the complete information cannot be fitted into one message.				
NOTE 2: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.4.3 {COMS-ACK}

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

Table 32: {COMS-ACK}

Message Type		Format		Directions
{COMS-ACK}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	O	N	≥ 2
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.4.4 {COMS-CONNECT}

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

Table 33: {COMS-CONNECT}

Message Type		Format		Directions
{COMS-CONNECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	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	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.4.5 {COMS-RELEASE}

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

Table 34: {COMS-RELEASE}

Message Type		Format		Directions
{COMS-RELEASE}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	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	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

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.

Table 35: {COMS-RELEASE-COM}

Message Type		Format		Directions
{COMS-RELEASE-COM}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Release Reason	7.6.7	O	O	2
Single-Display (see note)	7.6.5	O	N	2
Multi-Display (see note)	7.7.26	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	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: The message may contain either the <<SINGLE-DISPLAY>> element, or the <<MULTI-DISPLAY>> element, but not both.				

6.3.4.7 {COMS-NOTIFY}

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

Table 36: {COMS-NOTIFY}

Message Type		Format		Directions
{COMS-NOTIFY}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				

6.3.5 CLMS-message

6.3.5.1 {CLMS-VARIABLE}

Table 37: {CLMS-VARIABLE}

Message Type		Format		Directions
{CLMS-VARIABLE}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	7 to 20
MMS Generic Header	7.7.47	O	O	≥ 2
MMS Object Header	7.7.48	O	O	≥ 2
Repeat Indicator	7.6.3	O	O	1
MMS Extended Header	7.7.49	O	O	≥ 2
Repeat Indicator	7.6.3	O	O	1
Time-Date	7.7.50	O	O	6 to 10
Repeat Indicator	7.6.3	O	O	1
Calling Party Number	7.7.9	O	O	≥ 3
Calling Party Name	7.7.53	O	O	≥ 2
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 (see note)	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	≥ 4
M = Mandatory. O = Optional.				
NOTE: 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.

Table 38: {ACCESS-RIGHTS-ACCEPT}

Message Type		Format		Directions
{ACCESS-RIGHTS-ACCEPT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Portable identity	7.7.30	M	-	7 to 20
Repeat Indicator (see note)	7.6.3	O	-	1
Fixed identity(PARK) (see note)	7.7.18	M	-	5 to 20
Location area	7.7.25	O	-	≥ 3
AUTH-TYPE	7.7.4	O	-	5 to 6
Cipher info	7.7.10	O	-	4 to 5
ZAP field	7.7.44	O	-	3
Service class	7.7.39	O	-	3
Setup capability	7.7.40	O	-	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Model identifier	7.7.46	O	-	5 to 20
Escape to proprietary	7.7.45	O	-	≥ 4
Codec List	7.7.54	O	-	≥ 6
M = Mandatory. N = Not allowed. O = Optional. - = Not applicable.				
NOTE: More than one PARK can be transmitted by using the <<REPEAT-INDICATOR>> information elements. In this case the coding for "non-prioritized 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.

Table 39: {ACCESS-RIGHTS-REJECT}

Message Type		Format		Directions
{ACCESS-RIGHTS-REJECT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Reject Reason	7.7.34	O	-	3
Duration	7.7.13	O	-	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = 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.

Table 40: {ACCESS-RIGHTS-REQUEST}

Message Type		Format		Directions
{ACCESS-RIGHTS-REQUEST}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	7 to 20
AUTH-TYPE	7.7.4	-	O	5 to 6
Cipher info	7.7.10	-	O	4 to 5
Setup capability	7.7.40	-	O	4
Terminal capability	7.7.41	-	O	6 to 19
IWU-TO-IWU	7.7.23	-	O	≥ 4
Model identifier	7.7.46	-	O	5 to 20
Escape to proprietary	7.7.45	-	O	≥ 4
Codec List	7.7.54	-	O	≥ 6
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.

Table 41: {ACCESS-RIGHTS-TERMINATE-ACCEPT}

Message Type		Format		Directions
{ACCESS-RIGHTS-TERMINATE-ACCEPT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional.				

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.

Table 42: {ACCESS-RIGHTS-TERMINATE-REJECT}

Message Type		Format		Directions
{ACCESS-RIGHTS-TERMINATE-REJECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
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	≥ 4
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.

Table 43: {ACCESS-RIGHTS-TERMINATE-REQUEST}

Message Type		Format		Directions
{ACCESS-RIGHTS-TERMINATE-REQUEST}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	M	M	7 to 20
Repeat Indicator	7.6.3	O	O	1
Fixed identity (PARK)	7.7.18	O	O	5 to 20
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
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-prioritized 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.

Table 44: {AUTHENTICATION-REJECT}

Message Type		Format		Directions
{AUTHENTICATION-REJECT}		S		Both

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Repeat Indicator (see note)	7.6.3	O	O	1
AUTH-TYPE (see note)	7.7.4	O	O	5 to 6
Reject Reason	7.7.34	O	O	3
Repeat indicator	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional. N = Not allowed.				
NOTE: Instead of one <<AUTH-TYPE>> information element also a prioritized 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.

Table 45: {AUTHENTICATION-REPLY}

Message Type		Format		Directions
{AUTHENTICATION-REPLY}		S		Both

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
RAND (see notes 5, 6 and 7)	7.7.32	C	C	10
RES (see note 1)	7.7.35	M	M	6
RS (see notes 1, 2 and 8)	7.7.36	M/O	N	10 or 18
ZAP field (see note 3)	7.7.44	N	M/O	3
Service class (see note 4)	7.7.39	N	M/O	3
Key	7.7.24	N	O	≥ 4
Repeat indicator	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4

M = Mandatory.
N = Not allowed.
O = Optional.
C = Mandatory if DSAA2 and authentication type 2 is used (see EN 300 175-7 [7] clause 4.3), else Optional.

NOTE 1: The given length is when the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used.
NOTE 2: If this message is used in the FT authentication procedure and the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) 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 shall always be included if the DSAA2 algorithm is used and should not be included if DSAA algorithm is used.
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.
NOTE 5: The <<RAND>> IE shall be included when the DECT Standard Authentication Algorithm #2 (DSAA2) is used (authentication exchanges type 2). See EN 300 175-7 [7] clauses 4.3 and 6.3.
NOTE 6: In the case given in note 5, the <<RAND>> IE is used to carry the RAND_P parameter in the PT authentication type 2 procedure and the RAND_F parameter in the FT authentication type 2 procedure. See EN 300 175-7 [7] clauses 4.3 and 6.3.2.
NOTE 7: The given length is when the DECT Standard Authentication Algorithm #2 (DSAA2) is used
NOTE 8: RS has 64 bits and the total length of the IE is 10 octets when DSAA authentication is used. When DSAA2 is used, this IE carries the RS₁₂₈ (128 bits) and the total length of the IE is 18 octets.

6.3.6.9 {AUTHENTICATION-REQUEST}

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

Table 46: {AUTHENTICATION-REQUEST}

Message Type		Format		Directions
{AUTHENTICATION-REQUEST}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
AUTH-TYPE	7.7.4	M	M	5 to 6
RAND (see notes 1 and 4)	7.7.32	M	M	10
RES (see notes 1 and 3)	7.7.35	N	C	6
RS (see notes 1, 2 and 5)	7.7.36	M/O	N	10 or 18
Cipher info	7.7.10	O	O	4 to 5
Repeat indicator	7.6.3	O	O	1
IWU-TO-IWU	7.7.23	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. N = Not allowed. O = Optional. C = Mandatory If this message is used in the key allocation procedure (see clause 5.6.6), else Optional.				
NOTE 1: The given length is when the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used.				
NOTE 2: If a DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used, then the <<RS>> information element is mandatory in the direction FT to PT. Otherwise (proprietary algorithms) the IE is optional.				
NOTE 3: If this message is used in the key allocation procedure (see clause 5.6.6), then the <<RES>> information element is mandatory in the direction PT to FT.				
NOTE 4: The <<RAND>> IE is used to carry the RAND_F parameter in the PT authentication procedure (type 1 or 2) and the RAND_P parameter in the FT authentication procedure (type 1 or 2). See EN 300 175-7 [7] clause 6.3.2.				
NOTE 5: RS has 64 bits and the total length of the IE is 10 octets when DSAA authentication is used. When DSAA2 is used, this IE carries the RS ₁₂₈ (128 bits) and the total length of the IE is 18 octets.				

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.

Table 47: {CIPHER-REJECT}

Message Type		Format		Directions
{CIPHER-REJECT}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Repeat Indicator (see note)	7.6.3	O	O	1
Cipher info (see note)	7.7.10	O	O	4 to 5
Reject Reason	7.7.34	O	O	3
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional.				
NOTE: Instead of one <<CIPHER-INFO>> information element, also a prioritized 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.

Table 48: {CIPHER-REQUEST}

Message Type		Format		Directions
{CIPHER-REQUEST}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Cipher info	7.7.10	M	-	4 to 5
Call Identity	7.7.6	O	-	3 to 4
Connection Identity	7.7.12	O	-	≥ 3
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
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.

Table 49: {CIPHER-SUGGEST}

Message Type		Format		Directions
{CIPHER-SUGGEST}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Cipher info	7.7.10	-	M	4 to 5
Call Identity	7.7.6	-	O	3 to 4
Connection Identity	7.7.12	-	O	≥ 3
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4
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.

Table 50: {DETACH}

Message Type		Format		Directions
{DETACH}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	7 to 20
NWK assigned identity	7.7.28	-	O	5 to 20
Network parameter	7.7.29	-	O	≥ 3
Repeat indicator	7.6.3	-	O	1
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 51: {IDENTITY-REPLY}

Message Type		Format		Directions
{IDENTITY-REPLY}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Repeat Indicator (see note 1)	7.6.3	-	O	1
Portable identity (see note 1)	7.7.30	-	O	7 to 20
Repeat Indicator (see note 2)	7.6.3	-	O	1
Fixed identity (see note 2)	7.7.18	-	O	5 to 20
Repeat Indicator (see note 3)	7.6.3	-	O	1
NWK assigned identity (see note 3)	7.7.28	-	O	5 to 20
Network parameter	7.7.29	-	O	≥ 3
Repeat indicator	7.6.3	-	O	1
IWU-TO-IWU	7.7.23	-	O	≥ 4
Model Identifier	7.7.46	-	O	5 to 20
Escape to proprietary	7.7.45	-	O	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
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-prioritized 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-prioritized 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-prioritized 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.

Table 52: {IDENTITY-REQUEST}

Message Type		Format		Directions
{IDENTITY-REQUEST}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Repeat Indicator (see note)	7.6.3	M/N	-	1
Identity type (see note)	7.7.19	M	-	4
Network parameter	7.7.29	O	-	≥ 3
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. N = Not allowed. O = Optional.				
NOTE: More than one <<IDENTITY-TYPE>> information element can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritized 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 a User Authentication Key (UAK).

Table 53: {KEY-ALLOCATE}

Message Type		Format		Directions
{KEY-ALLOCATE}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Allocation type	7.7.2	M	-	4
RAND (see notes 1 and 3)	7.7.32	M	-	10
RS (see notes 2 and 4)	7.7.36	M	-	10 or 18
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory.				
NOTE 1: The length of 10 is when a DECT standard authentication algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used. NOTE 2: The length of 10 is when the DECT Standard Authentication Algorithm (DSAA) is used and the length of 18 is when the DECT Standard Authentication Algorithm #2 (DSAA2) is used. NOTE 3: The <<RAND>> IE carries the parameter RAND_F used in the PT authentication. NOTE 4: RS has 64 bits and the total length of the IE is 10 octets when DSAA authentication is used. When DSAA2 is used, this IE carries the RS ₁₂₈ (128 bits) and the total length of the IE is 18 octets.				

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.

Table 54: {LOCATE-ACCEPT}

Message Type		Format		Directions
{LOCATE-ACCEPT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Portable identity (see note 1)	7.7.30	M	-	2 to 20
Location area	7.7.25	M	-	≥ 3
Use TPUI	7.6.2	O	-	1
NWK assigned identity	7.7.28	O	-	5 to 20
Ext h/o indicator	7.7.51	O	-	3
Setup capability	7.7.40	O	-	4
ULE MAC Configuration Info	7.7.58	O	-	≥ 3
Duration	7.7.13	O	-	4
Repeat indicator	7.6.3	O	-	1
Segmented info (see note 2)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Model identifier	7.7.46	O	-	5 to 20
Escape to proprietary	7.7.45	O	-	≥ 4
Codec List	7.7.54	O	-	≥ 6
M = Mandatory. O = Optional. - = Not applicable.				
NOTE 1: This element may contain zero length contents if a new TPUI is not assigned. NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 55: {LOCATE-REJECT}

Message Type		Format		Directions
{LOCATE-REJECT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Reject Reason	7.7.34	O	-	3
Duration	7.7.13	O	-	4
Repeat indicator	7.6.3	O	-	1
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 56: {LOCATE-REQUEST}

Message Type		Format		Directions
{LOCATE-REQUEST}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	7 to 20
Fixed identity	7.7.18	-	O	5 to 20
Location area	7.7.25	-	O	≥ 3
NWK assigned identity	7.7.28	-	O	5 to 20
Cipher info	7.7.10	-	O	4 to 5
Network parameter	7.7.29	-	O	≥ 3
Setup capability	7.7.40	-	O	4
Terminal capability	7.7.41	-	O	6 to 19
Repeat indicator	7.6.3	-	O	1
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Model identifier	7.7.46	-	O	5 to 20
Escape to proprietary	7.7.45	-	O	≥ 4
Codec List	7.7.54	-	O	≥ 6
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 57: {MM-INFO-ACCEPT}

Message Type		Format		Directions
{MM-INFO-ACCEPT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
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 to 20
Location area	7.7.25	O	-	≥ 3
NWK assigned identity	7.7.28	O	-	5 to 20
Call Identity	7.7.6	O	-	3 to 4
Network parameter	7.7.29	O	-	≥ 3
Duration	7.7.13	O	-	4
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 58: {MM-INFO-REJECT}

Message Type		Format		Directions
{MM-INFO-REJECT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Call Identity	7.7.6	O	-	3 to 4
Reject Reason	7.7.34	O	-	3
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 59: {MM-INFO-REQUEST}

Message Type		Format		Directions
{MM-INFO-REQUEST}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Info type	7.7.20	-	M	≥ 3
Portable identity	7.7.30	-	O	7 to 20
Repeat indicator	7.6.3	-	O	1
Fixed identity	7.7.18	-	O	5 to 20
Location area	7.7.25	-	O	≥ 3
NWK assigned identity	7.7.28	-	O	5 to 20
Call Identity	7.7.6	-	O	3 to 4
Network parameter	7.7.29	-	O	≥ 3
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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 access rights modification or an external handover.

Table 60: {MM-INFO-SUGGEST}

Message Type		Format		Directions
{MM-INFO-SUGGEST}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Info type	7.7.20	M	-	≥ 3
Fixed identity	7.7.18	O	-	5 to 20
Location area	7.7.25	O	-	≥ 3
NWK assigned identity	7.7.28	O	-	5 to 20
Call Identity	7.7.6	O	-	3 to 4
Network parameter	7.7.29	O	-	≥ 3
Ext h/o indicator	7.7.51	O	-	3
KEY	7.7.24	O	-	≥ 4
Setup capability	7.7.40	O	-	4
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 61: {TEMPORARY-IDENTITY-ASSIGN}

Message Type		Format		Directions
{TEMPORARY-IDENTITY-ASSIGN}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Portable identity (see note)	7.7.30	O	-	7 to 20
Location area	7.7.25	O	-	≥ 3
NWK assigned identity (see note)	7.7.28	O	-	5 to 20
Network parameter	7.7.29	O	-	≥ 3
Duration	7.7.13	O	-	4
Repeat indicator	7.6.3	O	-	1
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: 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.

Table 62: {TEMPORARY-IDENTITY-ASSIGN-ACK}

Message Type		Format		Directions
{TEMPORARY-IDENTITY-ASSIGN-ACK}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

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.

Table 63: {TEMPORARY-IDENTITY-ASSIGN-REJ}

Message Type		Format		Directions
{TEMPORARY-IDENTITY-ASSIGN-REJ}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Reject Reason	7.7.34	-	O	3
Escape to proprietary	7.7.45	-	O	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				

6.3.6.27 {MM-IWU}

This message is used to exchange external protocol information in a transparent manner.

Table 63a: {MM-IWU}

Message Type		Format		Directions
{MM-IWU}		S		Both
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Repeat indicator (see note 1)	7.6.3	O	O	1
Segmented info (see note 2)	7.7.37	O	O	4
IWU-IWU	7.7.23	O	O	≥ 4
Segmented info (see note 2)	7.7.37	O	O	4
IWU-PACKET	7.7.22	O	O	≥ 4
Escape to proprietary	7.7.45	O	O	≥ 4
M = Mandatory. O = Optional.				
NOTE 1: The <<Repeat indicator>> information element may optionally be included in front of the <<IWU-TO-IWU>> information indicating "non prioritized" list.				
NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.				

6.3.6.28 {MM-NOTIFY}

This message is used to exchange internal protocol information.

Table 63b: {MM-NOTIFY}

Message Type		Format		Directions
{MM-NOTIFY}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	≥ 4
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.

Table 64: {LCE-PAGE-RESPONSE}

Message Type		Format		Directions
{LCE-PAGE-RESPONSE}		S		P=>F
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	7 to 20
Fixed identity	7.7.18	-	O	5 to 20
NWK assigned identity	7.7.28	-	O	5 to 20
Cipher info	7.7.10	-	O	4 to 5
Escape to proprietary	7.7.45	-	O	≥ 4
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.

Table 65: {LCE-PAGE-REJECT}

Message Type		Format		Directions
{LCE-PAGE-REJECT}		S		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Portable identity (see note)	7.7.30	M	-	7 to 20
Fixed identity	7.7.18	O	-	5 to 20
Reject Reason	7.7.34	O	-	3
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: 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 clause 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.
- 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 the present document.

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.

Table 66: {LCE-REQUEST-PAGE}

Message Type		Format		Directions
{LCE-REQUEST-PAGE}		B		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
LCE Header	8.2	M	-	1/2
Full address (see note)	8.2	O	-	4
Short address (see note)	8.2	O	-	2
M = Mandatory. O = Optional. - = Not applicable.				
NOTE: The message shall contain either a <<FULL-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.

Table 67: {CLMS-FIXED}

Message Type		Format		Directions
{CLMS-FIXED}		B		F=>P
Information Element	Clause	F to P message	P to F message	Length octets
CLMS Header (see note 1)	8.3.2	M	-	1/2
Short address (see note 2)	8.3.2	M	-	2
Protocol Discriminator (see note 2)	8.3.2	M	-	1
Length Indicator (see note 3)	8.3.2	M/N	-	1
Data	8.3.2	M	-	1 to 20
Fill4	8.3.2	O	-	0 to 3
M = Mandatory. N = Not allowed. O = Optional. - = Not applicable.				
NOTE 1: This message will be fragmented into message sections suitable for transmission by the MAC broadcast message control services.				
NOTE 2: This element appears in all message sections.				
NOTE 3: These elements are mandatory for all {CLMS-FIXED} messages. They are contained in the first message section. Refer to clause 12.3.1.				
NOTE 4: The <<LENGTH-INDICATOR>> is mandatory for multi-section messages. It is not allowed for single-section messages. Refer to clause 12.3.1.				
NOTE 5: The fill field is used to adjust the total message length to an integral number of sections. Refer to clause 8.3.				

7 S-FORMAT message structures

7.1 Overview

The S-FORMAT message structures are based on the principles adopted in EN 300 403-1 [9]. Similar modifications to those adopted in I-ETS 300 022 [i.6] have also been used. The detailed coding of all elements is unique to the present document.

Every message consists of the following parts:

- protocol discriminator;
- transaction identifier;
- message type;
- 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.

		Octet:
Transaction Identifier	Protocol Discriminator	1
Extended Transaction Value		1a
Message Type		2
Information elements		3
		N

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

Figure 3: S-FORMAT message structures

7.2 Protocol Discrimination (PD) element

Bit:	8	7	6	5	4	3	2	1	Octet:
	(see clause 7.3)				PROTOCOL DISCRIMINATOR				1

Figure 4: 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 (see note 2)
	0	1	0	0	Call Independent Supplementary Services (CISS) messages (see note 3)
	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.

NOTE 3: CISS messages may be transported over CLSS procedure (see clause 10.4.2.3).

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 IPU). 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 table 68.

Table 68: 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 clause 10.4.2.3.

Bit:	8	7	6	5	4	3	2	1	Octet:
	FLAG (F)	TRANSACTION VALUE (TV)			(see clause 7.2)				1

Figure 5: 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).

Bit:	8	7	6	5	4	3	2	1	Octet:
	FLAG (F)	TRANSACTION VALUE (TV)			(see clause 7.2)				1
	EXTENDED TRANSACTION VALUE (TVX)								1a

Figure 6: Extended Transaction Identifier (ETI) bits

7.4 Message type element

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

Figure 7: 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 69: 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 70: SS message type coding

CISS message types (call independent)	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)	Bits							
	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 71: 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 72: 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 73: 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
{MM-IWU}	0	1	0	1	1	0	1	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
{MM-NOTIFY}	0	1	1	0	1	1	1	0

7.4.6 Messages for LCE

Table 74: 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 EN 300 403-1 [9] has been used this should not be assumed. Most information elements have been redefined and reordered and EN 300 403-1 [9] 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 EN 300 403-1 [9].

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 clause 7.6.1. Octet 2 then contains a full octet of information.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Identifier			Contents				1

Figure 8: Single octet information element

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	1	1	0	2nd-Identifier				1
	Contents of element								2

Figure 9: Double octet information element

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

Variable length elements follow the principles defined in EN 300 403-1 [9].

The descriptions of the variable length information elements are in clause 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 defined in clause 7.7.1.
- The variable-length information elements are transmitted over the air according to the ascending numerical order of their identifiers. This allows receiving equipment to detect the presence or absence of a particular information element without scanning through an entire message.
- There is no specific rule for the <<Escape to proprietary>> information element (it respects also the ascending numerical order and is not always located as last position in the message).
- The only exception to the ascending numerical order is the <<Segmented Info>> information element that can be included just before some information elements whenever theses IEs are segmented over a number of consecutive messages (e.g. <<IWU-TO-IWU>>, <<IWU-PACKET>>, or <<Alphanumeric>>).
- The order of appearance of the variable length information element in the message tables is given for information, even if they should follow the numerical ascending order for the listed variable length information element identifiers.

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".

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	Element identifier							1
	Length of contents; L (octets)								2
									3
			Contents of element						
									L+2

Figure 10: 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 the present document 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 the present document;
 - an information element may be extended with additional octet groups in later versions of the present document, 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	most significant octet (n)								N
	least significant octet (1)								N+n-1

Figure 11: Structure of long fields

7.5.2 Extensions of codesets

The present document defines codeset "0". All elements listed in clauses 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 clauses 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 content 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 the present 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 clauses 7.5.2 to 7.5.4) shall be used. Other fixed length information elements may be different.

All equipment shall have the capability to recognize 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.

NOTE: Whenever an implementation receives an information element with an additional unexpected/undefined octet, it should not regard the information element to have invalid content/incorrect length. In order to accommodate future extension of the standards, the implementation should process the expected/defined/known octets and only discard the additional unexpected octets.

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 procedure 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:

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

Figure 12: Shift element (locking shift)

New (temporary) codeset identifier

Bits	3 2 1	Meaning
	0 0 0	Initial codeset (the present document)
	0 0 1 }	
	0 1 0 }	Reserved
	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 procedure 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:

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

Figure 13: Shift element (non-locking)

New (temporary) codeset identifier

As for locking shift: refer to clause 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

<<SINGLE-DISPLAY>>

<<SINGLE-KEYPAD>>

Variable Length

<<MULTI-DISPLAY>>

<<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 clause 17.5.2.

<<REPEAT-INDICATOR>>; coding 1.

The "non-prioritized 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 "prioritized 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 75: Fixed length information elements coding

Single Octet Elements	Bits								Reference
	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
Use TPUI	1	0	1	0	0	0	1	1	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, delimiter request and use TPUI

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

The purpose of the <<USE-TPUI>> element is to optionally indicate that a PT may use TPUI in the <<portable identity>> in {CC-SETUP} and in {LCE-PAGE-RESPONSE}.

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

Figure 14: SENDING-COMPLETE information element

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

Figure 15: DELIMITER-REQUEST information element

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

Figure 16: USE-TPUI 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 clause 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 indicator				1

Figure 17: REPEAT-INDICATOR information element

Repeat indicator coding (octet 1):

Bits	4 3 2 1	Meaning
0 0 0 1	Non prioritized list. See clause 7.5.6.	
0 0 1 0	Prioritized list. See clause 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 setup message.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	1	1	0	0	0	0	0	1
	<<BASIC-SERVICE>>								
	Call class				Basic Service				2

Figure 18: BASIC-SERVICE information element

Call class (octet 2):

Bits	8 7 6 5	Meaning
0 0 1 0	LiA service setup (see note 1)	
0 0 1 1	ULE service call setup	
0 1 0 0	Message call setup	
0 1 1 1	DECT/ISDN IIP	
1 0 0 0	Normal call setup	
1 0 0 1	Internal call setup (typically used in residential environments)	
1 0 1 0	Emergency call setup	
1 0 1 1	Service call setup	

- 1 1 0 0 External handover call setup (see clause 9.3.1.1)
 1 1 0 1 Supplementary service call setup
 1 1 1 0 OA&M call setup
 All other values reserved.

Basic service (octet 2):

Bits	4 3 2 1	Meaning
0 0 0 0		Basic speech default setup attributes (see note 2, clauses E.1 and 9.3.1.1)
0 1 0 0		DECT GSM IWP profile (Phase 2)
0 1 1 0		DECT UMTS IWP (TS 101 863 [61])
0 1 1 0		GSM IWP SMS
0 1 0 1		LRMS (E-profile) service (EN 300 757 [48])
1 0 0 0		Wideband speech default setup attributes (see note 3 and clause E.2)
1 0 0 1		Light data services: SUOTA (TS 102 527-4 [76]), Class 4 DPRS management, default setup attributes (see note 4)
1 0 1 0		Light data services: SUOTA (TS 102 527-4 [76]), Class 3 DPRS management, default setup attributes (see note 4)
1 0 1 1		DTAM Wideband speech default setup attributes (see note 3 and clause E.2)
1 1 1 1		Other (see clause 9.3.1.1)
All other values reserved.		

NOTE 1: Requires the support of the List access (LiA) service feature. See TS 102 527-3 [75] for description of List access service feature.

NOTE 2: The value of this field may be used in future standards to indicate "specific profile default setup attributes".

NOTE 3: Default wideband setup attributes are described in clause E.2. Codec negotiation mechanism is described in TS 102 527-1 [73].

NOTE 4: Default setup attributes for data services are defined in EN 301 649 (DPRS) [72], clause A.4.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<< SINGLE-DISPLAY >>							1
	Display Info (DECT character)								2

Figure 19: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<< SINGLE-KEYPAD >>							1
	Keypad Info (DECT character)								2

Figure 20: 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>> information 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<<RELEASE-REASON>>							1
	Release Reason Code								2

Figure 21: 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	Negotiation failed
0C	Collision
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	User call modify
17 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

Release reason coding: security related values

Value (hex)	Meaning (Reason)
40	Security attack assumed
41	Encryption activation failed
42	Re-Keying failed
43	No Cipher Key available

All other values reserved.

7.6.8 Signal

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<< SIGNAL >>							1
	Signal value								2

Figure 22: 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 (see note 3)
	0 0 0 0 0 0 0 1	Ring-back tone on (see note 4)
	0 0 0 0 0 0 1 0	Intercept tone on (see note 7)
	0 0 0 0 0 0 1 1	Network congestion tone on (see note 6)
	0 0 0 0 0 1 0 0	Busy tone on (see note 3)
	0 0 0 0 0 1 0 1	Confirm tone on (see note 5)
	0 0 0 0 0 1 1 0	Answer tone on (see note 5)
	0 0 0 0 0 1 1 1	Call waiting tone on (see note 3)
	0 0 0 0 1 0 0 0	Off-hook warning tone on (see note 5)
	0 0 0 0 1 0 0 1	Negative acknowledgement tone
	0 0 1 1 1 1 1 1	Tones off
	0 1 0 0 0 0 0 0	Alerting on - pattern 0 (see note 2)
	0 1 0 0 0 0 0 1	Alerting on - pattern 1 (see note 2)
	0 1 0 0 0 0 1 0	Alerting on - pattern 2 (see note 2)
	0 1 0 0 0 0 1 1	Alerting on - pattern 3 (see note 2)
	0 1 0 0 0 1 0 0	Alerting on - pattern 4 (see note 2)
	0 1 0 0 0 1 0 1	Alerting on - pattern 5 (see note 2)
	0 1 0 0 0 1 1 0	Alerting on - pattern 6 (see note 2)
	0 1 0 0 0 1 1 1	Alerting on - pattern 7 (see note 2)
	0 1 0 0 1 0 0 0	Alerting on - continuous (see 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 Recommendation ITU-T E.182 [42].

NOTE 4: This tone should be used in accordance with the "Ringing" tone description given in Recommendation ITU-T E.182 [42].

NOTE 5: No description is provided for the use of this tone. This coding is included to provide alignment to the coding provided in EN 300 403-1 [9].

NOTE 6: This tone should be used in accordance with the "congestion tone" description given in Recommendation ITU-T E.182 [42].

NOTE 7: This tone should be used in accordance with the "intrusion tone" description given in Recommendation ITU-T E.182 [42].

7.6.9 Timer restart

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<< TIMER-RESTART >>							1
	Restart value								2

Figure 23: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	<< TEST-HOOK-CONTROL >>							1
	Hook value								2

Figure 24: 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

Table 76 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 clause where the detailed coding of the element shall be found.

Table 76: Variable length information element coding

Variable Length Elements	Bits								Reference
	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
Setup 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
ULE MAC Configuration Info	0	1	1	0	1	0	0	0	7.7.58
Calling Party Number	0	1	1	0	1	1	0	0	7.7.9
Calling Party Name	0	1	1	0	1	1	0	1	7.7.53
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
Called Party Name	0	1	1	1	0	0	1	1	7.7.52
List change details	0	1	1	1	0	1	0	0	7.7.57
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
Codec List	0	1	1	1	1	1	0	0	7.7.54
Events notification	0	1	1	1	1	1	0	1	7.7.55
Call information	0	1	1	1	1	1	1	0	7.7.56
Escape for extension	0	1	1	1	1	1	1	1	(see 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 figure 25.									

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<<ESCAPE-FOR-EXTENSION>>							1
	Length of Contents (L)								2
	1	info element identifier							3
	Contents of information element								4, etc.

Figure 25: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<<ALLOCATION-TYPE>>							1
	Length of Contents (L)								2
	Authentication algorithm identifier								3
	UAK number				AC number				4

Figure 26: 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 (DSAA)
	0	0	0	0	0	1	0		DECT standard authentication algorithm #2 (DSAA2)
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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<<ALPHANUMERIC>>							1
	Length of Contents (L)								2
	0	Character Type			O/E	Character Set			3
									4
	List of Characters								
									L+2

Figure 27: 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 (see annex D)
	0 1 0	IA5 characters (see Recommendation ITU-T T.50 [i.5])
	0 1 1	Reserved (see ISO/IEC 2022 [11])
	1 0 0	ERMES 7-bit characters (see ETS 300 133 [12], parts 1 to 7)
	1 0 1	Reserved [CT2/CAI characters]
	1 1 0	Standard ASCII (7 bit) characters (see ISO/IEC 646 [59])

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 (see annex D)
	1 0 0	ERMES 4-bit characters (see ETS 300 133 [12])
	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 identifier								3
	Proprietary algorithm identifier								3a
	Authentication key type				Authentication key number				4
	INC	DEF	TXC	UPC	Cipher key number				5
	Default Cipher Key Index (high byte)								5a
	Default Cipher Key Index (low byte)								5b

Figure 28: 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 (DSAA)
	0 0 0 0 0 0 1 0	DECT standard authentication algorithm #2 (DSAA2)
	0 1 0 0 0 0 0 0	GSM authentication algorithm
	0 0 1 0 0 0 0 0	UMTS 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 1: The User Personal Identity (UPI) is always used in combination with a 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

DEF bit coding (octet 5):

Bits	7	Meaning
	0	generated derived cipher key shall not be used as default cipher key for early encryption
	1	generated derived cipher key shall only be used as default cipher key stored under the given default cipher key index for early encryption (octet 5a,b)

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 2: 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.

Default cipher key index (octet 5a,b):

These octets shall be sent if and only if the DEF bit coding in octet 5 is set, indicating that the generated derived cipher key shall be used as default cipher key for early encryption. When sent, these octets shall contain the index of the default cipher key.

NOTE 3: Two octets are used for this purpose, in order to allow that even in office/public environments each PP has a default cipher key with a system wide unique index.

The index shall be system wide unique so that the related MAC procedures can rely on this uniqueness to identify the requested default cipher key index.

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 setup 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 standard		NWK Layer Attributes					3
	1	C-plane class			C-plane routing				4
	0/1	LU identification							5
	1	0	0	LU identification					5a
		spare		F=>P direction					
	0/1	U-plane class			U-plane frame type and options				6
	1	U-plane class F=>P			U-plane frame type and options; F=>P				6a

Figure 29: 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 0 0 1 0	DPRS Class 2 Management (see EN 301 649 [72], DPRS-ME.2)
	0 0 0 1 1	DPRS Class 3 Management (see EN 301 649 [72], DPRS-ME.3)
	0 0 1 1 0	DPRS Class 4 Management (see EN 301 649 [72], DPRS-ME.4)
	0 1 0 0 0	DECT GSM IWP profile phase 2
	0 0 1 0 0	DECT UMTS IWP
	0 0 1 0 1	ODAP basic data
	0 1 0 0 0	ULE part 1 (see TS 102 939-1 [79])
		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
	1 1 1	No C-plane (see note 2)
		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 (see note 1)
	1 1 1 1	No C-plane routing (see note 2)
		All other values reserved.

NOTE 1: 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 EN 300 175-4 [4], clause 9.5.1.2 for details of dedicated bearer operation).

NOTE 2: "No C-plane" and "no -plane routing" refer to the case when there is no DLC C-plane (LAPC) over the MBC associated to the call.

U-plane symmetry (bit 8 of octet 5):

Bits	8	Meaning
	1	Symmetric
	0	Asymmetric

If symmetric, only octet 5 shall appear with bit 8 coded to "1". The LU type coded by octet 5 shall refer to both directions. If asymmetric, bit 8 in octet 5 shall be coded to "0". Octet 5 shall only refer to the direction P=>F and octet 5a shall refer to the direction F=>P.

NOTE 3: bit 8 of octet 6 will be usually coded in the same way as bit 8 of octet 5.

LU identification (octet 5 and 5a):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 1	LU1
	0 0 0 0 0 1 0	LU2
	0 0 0 0 0 1 1	LU3
	0 0 0 0 1 0 0	LU4
	0 0 0 0 1 0 1	LU5
	0 0 0 0 1 1 0	LU6
	0 0 0 0 1 1 1	LU7
	0 0 0 1 0 0 0	LU8
	0 0 0 1 0 0 1	LU9
	0 0 0 1 0 1 0	LU10
	0 0 0 1 0 1 1	LU11
	0 0 0 1 1 0 0	LU12
	0 0 0 1 1 0 1	LU13
	0 0 0 1 1 1 0	LU14
	0 0 0 1 1 1 1	reserved for LU15
	0 0 1 0 0 0 0	LU16
	All other values reserved.	

U-plane class (octets 6 and 6a) (see note 4):

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.	

NOTE 4: "U-plane class" refers to DLC transmission class. See EN 300 175-4 [4].

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

Bits 1 to 4 in octet 6 (and in octet 6a, if included) are used to code the frame type and other options for each LU service.

FU-type symmetry (bit 8 of octet 6):

Bits	8	Meaning
	1	Symmetric (same FU type and options in both directions)
	0	Asymmetric (different FU type or options in both directions)

If symmetric, only octet 6 shall appear with bit 8 coded to "1". The FU type and options coded by octet 6 shall refer to both directions. If asymmetric, bit 8 in octet 6 shall be coded to "0". Octet 6 shall only refer to the direction P=>F and octet 6a shall refer to the direction F=>P.

NOTE 5: bit 8 of octet 6 will be usually coded in the same way as bit 8 of octet 5.

For service type LU 1

Bits	4 3 2 1	Meaning
	0 0 0 1	FU1
	All other values reserved.	

For service type LU 2

Bits	4 3 2 1	Meaning
	0 1 0 0	FU4
	0 1 0 1	FU5a/b
	0 1 1 0	FU6a/b

All other values reserved.

For service type LU 3

Bits	4 3 2 1	Meaning
	0 1 0 0	FU4
	0 1 0 1	FU5a/b
	0 1 1 0	FU6a/b
	All other values reserved.	

For service type LU 5

Bits	4 3 2 1	Meaning
	0 0 0 1	FU1
	0 1 0 1	FU5
	All other values reserved.	

For service type LU 6

Bits	4 3 2 1	Meaning
	0 0 0 1	FU1
	0 1 0 1	FU5
	All other values reserved.	

For service type LU 16

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
	1 0 0 0	FU8
	1 0 0 1	FU9
	1 0 1 0	FU10a/c
	1 0 1 1	FU10b
	1 1 0 0	FU12
	All other values reserved.	

For service type LU 7

Bits	4 3 2 1	Meaning
	0 1 1 1	FU7
	All other values reserved.	

For service type LU 8

Bits	4 3 2 1	Meaning
	1 0 0 0	FU8
	All other values reserved.	

For service type LU 9

Bits	4 3 2 1	Meaning
	1 0 0 1	FU9
	All other values reserved.	

For service type LU 10

Bits	4 3 2 1	Meaning
	1 0 0 1	FU10a/d

1 0 1 0 FU10a/c
 1 0 1 1 FU10b
 All other values reserved.

For service type LU 11

Bits **4 3 2 1** **Meaning**
 0 0 0 1 FU11
 All other values reserved.

For service type LU 12

Bits **4 3 2 1** **Meaning**
 1 1 0 0 FU12
 All other values reserved.

For service type LU 13

Bits **4 3 2 1** **Meaning**
 0 0 0 1 FU10a/d, Checksum 16 bit
 0 0 1 0 FU10a/c, Checksum 16 bit
 0 0 1 1 FU10b, Checksum 16 bit
 1 0 0 1 FU10a/d, CRC 32 bit
 1 0 1 0 FU10a/c, CRC 32 bit
 1 0 1 1 FU10b, CRC 32 bit
 All other values reserved.

For service type LU 14

Bits **4 3 2 1** **Meaning**
 1 0 0 1 FU10a/d
 1 0 1 0 FU10a/c
 1 0 1 1 FU10b
 All other values reserved.

7.7.6 Call identity

The purpose of the <<CALL-IDENTITY>> information element is to identify the call to which the message/procedure applies, e.g. to initiate ciphering of calls, to retrieve call related parameters.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALL-IDENTITY >>							1
	Length of Contents (L)								2
	F	TV			PD				3a
	Extended Transaction Value								3b

Figure 30: 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 clause 7.3;
- for protocol discriminator coding (octet 3a) see clause 7.2;
- for extended transaction value coding (octet 3b) see clause 7.3.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALLED-PARTY-NUMBER >>							1
	Length of Contents (L)								2
	1	Number Type			Numbering plan identification				3
									4
	Called Party Address								
	(List of DECT characters)								L+2

Figure 31: 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 Recommendation ITU-Ts E.164 [i.8]/E.163 [i.7] (see note 1)
	0 0 1 1	Data plan Recommendation ITU-T X.121 [i.9] (see note 1)
	0 1 1 1	TCP/IP address (see note 2)
	1 0 0 0	National standard plan (see note 1)
	1 0 0 1	Private plan (see note 1)
	1 0 1 0	SIP addressing scheme, "To:" field (see RFC 3261 [67])
	1 0 1 1	Internet character format address (see note 1)
	1 1 0 0	LAN MAC address (see note 1)
	1 1 0 1	Recommendation ITU-T X.400 [60] address (see note 1)
	1 1 1 0	Profile service specific alphanumeric identifier (see note 3)
	1 1 1 1	Reserved for extension
	All other values reserved.	

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

NOTE 2: The address will 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALLED-PARTY-SUBADDR >>							1
	Length of Contents (L)								2
	1	Subaddress			O/E	0	0	0	3
		Type			ind	spare			
									4
	List of Subaddress Information								
									L+2

Figure 32: CALLED-PARTY-SUBADDRESS information element

Subaddress type (octet 3):

Bits	7 6 5	Meaning
	0 0 0	NSAP; ISO/IEC 8348 [19]
	0 1 0	User specified
	1 0 0	Profile service specific alphanumeric identifier (see note 1)
	All other values reserved.	

NOTE 1: 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 2: 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

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALLING-PARTY-NUMBER >>							1
	Length of Contents (L)								2
	0/1	Number type			Numbering plan identification			3	
	1	Present		0	0	0	Screening		3a
		indicator		Spare			indicator		
									4
	Calling Party Address								
	(List of DECT characters)								L+2

Figure 33: 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 Recommendations ITU-T E.164 [i.8]/E.163 [i.7] (see note 1)
	0 0 1 1	Data plan Recommendation ITU-T X.121 [i.9] (see note 1)
	0 1 1 1	TCP/IP address (see note 2)
	1 0 0 0	National standard plan (see note 1)
	1 0 0 1	Private plan (see note 1)
	1 0 1 0	SIP addressing scheme, "From:" field (RFC 3261 [67])
	1 0 1 1	Internet character format address (see note 1)
	1 1 0 0	LAN MAC address (see note 1)
	1 1 0 1	Recommendation ITU-T X.400 [60] address (see note 1)
	1 1 1 0	Profile service specific alphanumeric identifier (see 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 (see note 4)
	1 0	Number not available (see note 4)
	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 clause D.2.3) are used. Bit number 8 will be set to zero.

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

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

NOTE 4: When Presentation is restricted or Number is not available the <Calling party address> may contain a default number or the octet group may be missing.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CIPHER-INFO >>							1
	Length of Contents (L)								2
	Y/N	Cipher algorithm identifier							3
	Proprietary algorithm identifier								3a
	Cipher key type				Cipher key number				4

Figure 34: 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 (DSC)
	0 0 0 0 0 1 0	DECT Standard Cipher algorithm #2 (DSC2)
	0 1 0 1 0 0 0	GPRS ciphering not used
	0 1 0 1 0 0 1	GPRS encryption algorithm GEA/1
	0 1 0 1 0 1 0	GPRS encryption algorithm GEA/2
	0 1 0 1 0 1 1	GPRS encryption algorithm GEA/3
	0 1 0 1 1 0 0	GPRS encryption algorithm GEA/4
	0 1 0 1 1 0 1	GPRS encryption algorithm GEA/5
	0 1 0 1 1 1 0	GPRS encryption algorithm GEA/6
	0 1 0 1 1 1 1	GPRS encryption algorithm GEA/7
	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 Contents (L)								2
	1	Type			Connection identity				3
	0/1	0	0	Maximum bearers P=>F direction					4
	0/1	0	1	Minimum bearers P=>F direction					4a
	0/1	1	0	maximum bearers F=>P direction					4b
	0/1	1	1	Minimum bearers F=>P direction					4c
	0/1	Slot type			MAC service				5
	1	0	0	0	MAC service F=>P				5a
	0/1	CF channel attributes			MAC packet lifetime				6
	1	CF channel attributes F=>P			MAC packet lifetime F=>P				6a
	0/1 ext	A attributes			spare	B attributes			7

Figure 35: CONNECTION-ATTRIBUTES information element

Type (octet 3):

Bits	7 6 5	Meaning
	0 0 1	Symmetric only connection
	1 0 0	Asymmetric frozen connection
	0 1 0	Asymmetric reversible connection
	1 0 1	Asymmetric one-way-only connection
	1 1 0	Asymmetric unrestricted connection
	All other values reserved.	

Definition of the different types of connection: (See also clause K.1 for detailed description of the properties of each connection type).

Symmetric only: the connection can use duplex bearers only. The maximum and minimum number of bearers P=>F are identical to F=>P. Octets 4b and 4c shall be ignored.

See clause K.1.2.1 for detailed properties.

NOTE 1: Symmetric only connections can be used with DPRS and other profiles.

Asymmetric frozen connection: Octets 4b and 4c shall be provided. The connection can use duplex and double simplex bearers in one direction only, which is defined by the values of the maximum number of bearers. In this type of connection, the MAC layer bandwidth negotiation parameters shall be fixed and identical to the maximum and minimum number of bearers P=>F and F=>P negotiated at NWK layer in this IE.

See clause K.1.2 for detailed properties.

NOTE 2: Asymmetric frozen connections are intended for circuit mode profiles and are not compatible with DPRS or any other profile that changes the Bandwidth at MAC layer.

Asymmetric reversible connection: the connection can use duplex bearers and double simplex bearers in any direction (but not at the same time). In this connection maximum and minimum number of bearers in both directions are identical. Octets 4b and 4c are ignored. The MAC layer could set or change the bandwidth at any time to any combination of values placed within the limits set by this IE. See clause K.1.3 for detailed description.

Asymmetric one-way-only connection: in this connection, only double simplex bearers in one direction, plus duplex bearers, are allowed. Octets 4b and 4c shall be provided. The connection can be either downstream or upstream depending on the values of number of bearers. See clause K.1.4 for detailed description and possible settings.

Asymmetric unrestricted connection: the connection can use duplex bearers and double simplex bearers in any direction (but not at the same time). In this connection maximum and minimum number of bearers $P \Rightarrow F$ and $F \Rightarrow P$ are different. Octets 4b and 4c shall be provided. See clause K.1.5 for detailed description, properties and possible settings.

NOTE 3: All connection types, except asymmetric frozen, are compatible with DPRS.

NOTE 4: (Applicable to all connection types). The values of all number of bearers parameters should take into account the intrinsic limitations of DECT, in particular, that the total number of simplex bearers should be even.

NOTE 5: (Applicable to all connection types except Asymmetric frozen). When used in DPRS, the bandwidth combination (0,0), -also known "suspend" state- is also allowed to the MAC layer.

NOTE 6: (Applicable to all asymmetric connection types). A minimum of 1 duplex bearer is required for all asymmetric connections to provide the "special" bearer functions. Refer to EN 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 7: If already established, the (advanced) connection is identified using the Logical Connection Number (LCN) placed in position NNN. The coding of the LCN is identical to the MAC layer ECN.

Bearer definition coding (octets 4, 4a, 4b, 4c):

Bits	7 6	Meaning
	0 0	Maximum number of bearers; $P \Rightarrow F$ direction
	0 1	Minimum number of bearers; $P \Rightarrow F$ direction
	1 0	Maximum number of bearers; $F \Rightarrow P$ direction
	1 1	Minimum number of bearers; $F \Rightarrow P$ 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 ($1 \leq \text{Number} \leq 31$)

NOTE 8: 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".

The Maximum 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 as described for each type of connection. If operation within the specified limits cannot be accomplished the call should be released.

Octets 4a, 4b and 4c are not mandatory for all types of connections. If present they shall appear in order shown. The following rules shall apply:

- If "symmetric only" or "asymmetric reversible" are indicated in the type indicator (octet 3), octets 4b and 4c shall be omitted and octets 4 and 4a shall refer to both directions. If any other type is indicated in octet 3, then octets 4 and 4a shall only refer to the direction $P \Rightarrow F$ and octets 4b and 4c shall refer to the direction $F \Rightarrow P$.
- Octets 4a and 4c (if applicable) may be omitted for all connection types. If omitted, they shall be defaulted to:
 - "1" for DPRS and packet mode profiles;

- the value given in octets 4 and 4b for circuit mode profiles.

In all of these fields the "number of bearers" coding refers to the total number of individual (simplex) bearers.

MAC slot type (octet 5):

Bits	7 6 5	Meaning
	0 0 0	Half slot; $j = 80$
	0 0 1	Long slot; $j = 640$
	0 1 0	Long slot; $j = 672$
	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_{NA} ; (I_N minimum delay)
	0 0 0 1	I_{NB} ; (I_N normal delay)
	0 0 1 0	I_{PM} ; (I_P error detect, multisubfield)
	0 0 1 1	I_{PMR} ; (I_P Mod-2 correct, multisubfield)
	0 1 0 0	I_{PX} ; (encoded protected)
	0 1 1 0	I_{PQ} ; (I_P error detect, singlesubfield)
	0 1 1 1	I_{PQR} ; (I_P Mod-2 correct, single subfield)
	All other values reserved.	

C_F channel attributes (octets 6 and 6a):

Bits	7 6 5	Meaning for circuit-mode connections	Meaning for packet-mode connections
	0 0 0	C_F never (C_S only)	C_F never (C_S only)
	0 1 0	C_F Demand/1 bearer (interrupting)	C_F priority D (lowest)
	0 1 1	C_F Demand/2 bearers (interrupting)	C_F priority C
	1 0 0	C_F Reserved/1 bearer (non-interrupting)	C_F priority B
	1 0 1	C_F Reserved/2 bearers (non-interrupting)	C_F priority A (highest)
	All other values reserved.		

NOTE 9: Handling of C_F priority modes for packet mode connections are described in EN 301 649 [72], clause 10.14.2.1.

NOTE 10: 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 BA bits in the A-field header (see EN 300 175-3 [3]).

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 (I_P ; Mod-2 operation only)
	All other values reserved.	

NOTE 11: The maximum packet lifetime (nnn) is only defined if the MAC service uses MOD-2 retransmission (I_{PMR} or I_{PQR} , octet 5 or 5a as appropriate). The value "nnn" defines the allowed values of maximum packet lifetime using the coding given in clause 7.2.5.3.8 of EN 300 175-3 [3]. In all other cases the "Not applicable" coding is used.

NOTE 12: 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 EN 300 175-3 [3], clause 7.2.5.3.8 for the use of this attribute.

The octets 5a and 6a are optional and can only be used if octets 4b and 4c have been provided. If octets 5a and 6a are not provided, it means that the MAC service, C_F channel attributes and MAC packet lifetime are the same in both directions.

A-field modulation scheme coding (octet 7):

Bits	7 6 5	Meaning
	0 0 0	2-level
	0 0 1	4-level
	0 1 0	8-level

All other values reserved.

(B+Z)-fields modulation scheme coding (octet 7):

Bits	3 2 1	Meaning
	0 0 0	2-level
	0 0 1	4-level
	0 1 0	8-level
	0 1 1	16-level
	1 0 1	64-level

All other values reserved.

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), to allocate ECN for connections associated with a Broadband data link or to identify an existing connection (or connections) in certain procedures (e.g. Cipher related procedures or Service change procedures).

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CONNECTION-IDENTITY >>							1
	Length of Contents (L)								2
	U-plane link identity				Connection identity				3
	List of other U-plane/connection associations								3a

Figure 36: CONNECTION-IDENTITY information element

Each octet identifies a connection or defines an association between one U-plane link and one MAC connection (for the case of Broadband links see the end of this clause). 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. The coding of the LCN is identical to the MAC layer ECN.

Link identity coding:

Bits	8 7 6 5	Meaning
	0 0 0 0	U-plane Unnumbered link
	0 1 1 1	Broadband data link
	1 N N N	U-plane 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 EN 300 175-4 [4], clause 13.2, for details of U-plane link number coding.

Format of <<CONNECTION-IDENTITY>> element if the coding "Broadband data link" is used:

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CONNECTION-IDENTITY >>							1
	Length of Contents (L)								2
	Broadband data link = 0111				Connection identity 1				3
	Connection identity 2				Connection identity 3				3a

Figure 36a

Connection identity coding (octet 3 and 3a):

Bits	4	3	2	1	Meaning
	1	N	N	N	Logical connection number (LCN) NNN
	All other values reserved.				

The <Connection identity 1> indicates the LCN of the first established connection of a Broadband data link; the <Connection identity 2> and <Connection identity 3> indicate the LCN of up to two additional connections that can be associated with the same data link. A value "0000" in one of the fields of octet 3a indicates that only one additional LCN is allocated for additional connections associations.

7.7.13 Duration

The purpose of the <<DURATION>> information element is to indicate a time duration.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< Duration >>							1
	Length of Contents (L)								2
	0/1	Lock Limits			Time Limits				3
	Time duration								3a

Figure 37: DURATION information element

Lock limits coding (octet 3):

Bits	7	6	5	Meaning
	1	1	0	Temporary user limit (see note 1)
	1	1	1	No limits
	1	0	1	Temporary user limits 2 (see note 1)

NOTE 1: "Temporary user limit" indicates that a time limit applies when the PP leaves the locked state with the relevant FP (see EN 300 175-6 [6]).

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 (see 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 EN 300 175-3 [3].

Defined time limit 1: 1 unit = 2^8 multiframes.

Defined time limit 2: 1 unit = 2^{16} multiframes (see note 3).

NOTE 3: This unit corresponds to the most significant octet of the multiframe number that may be transmitted by FPs (see EN 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< END-TO-END-COMPATIB >>							1
	Length of Contents (L)								2
	0/1	S/A	Neg	User rate					3
	0/1	Intermediate rate		NIC tx	NIC rx	F-C tx	F-C rx	0 spr	3a (see note 2)
	0/1	Stop bits		Data bits		Parity			3b
	1	Dup	Modem type						3c

Figure 38: 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 Recommendation ITU-Ts V.110 [55]/X.30 [57] 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 (see note 4)

NOTE 4: "In band negotiation possible" is only used in the context of Recommendation ITU-Ts V.110 [55] and X.30 [57] 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. (See note 5)
1 1 0 0 0	1,2/0,075 kbit/s;	V.6 and X.1. (See 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 PT => FT direction of the call. The second rate is the transmit rate in the FT => PT direction of the call.

NOTE 6: See ITU-T Series V Recommendations.
See ITU-T Series X Recommendations.
See Recommendation ITU-T I.460 [i.10].

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 Recommendations ITU-T V.110 [55] and X.30 [57].

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 Recommendations ITU-T V.110 [55] and X.30 [57].

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 1 1 1 1 1 1	} Reserved for national use
	All other values reserved.	

NOTE 13: See ITU-T Series V Recommendations.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< FACILITY >>							1
	Length of Contents (L)								2
	1	0	0	Service discriminator					3
	Component(s)								4

Figure 39: 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 EN 300 196-1 [14].

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

Figure 40: FEATURE-ACTIVATE information element

Feature coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning	Parameter
	0 0 0 0 0 0 1	Register recall	no
	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 $01 \leq nn \leq 7F$

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 $01 \leq nn \leq 7F$

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 $01 \leq nn \leq 7F$

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 (see note 1)
	0 1	Only option a) connected (see note 1)
	1 0	Only option b) connected (see note 1)
	1 1	No change (see note 1)
Bits	4 3	Meaning
	0 0	Disconnect for requirement 2 (see note 2)
	0 1	Connect ≥ 9 dB for requirement 2 (see note 2)
	1 0	Connect reduced loss for requirement 2 (see note 2)
	1 1	No change for requirement 2 (see note 2)
Bits	2 1	Meaning
	0 0	Disconnect for requirement 1 (see note 2)
	0 1	Connect for requirement 1 (see note 2)
	1 0	Reserved for requirement 1 (see note 2)
	1 1	No change for requirement 1 (see note 2)

NOTE 1: Refer to EN 300 175-8 [8], clause 7.4.1.2.

NOTE 2: Refer to EN 300 175-8 [8], clause 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 clause 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 clause 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< FEATURE-INDICATE >>							1
	Length of Contents (L)								2
	0/1	Feature							3
	1	Parameter							3a
	Status indicator								4
	Component(s)								5 to L+2

Figure 41: FEATURE-INDICATE information element**Feature coding (octet 3):**

Bits	7 6 5 4 3 2 1	Meaning	Parameter
	0 0 0 0 0 0 1	Register recall	no
	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.

	0	Subscriber number							
	0	(List of DECT characters)							L+2

Figure 42: Subscriber number indication coding

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:

Bit:	8	7	6	5	4	3	2	1	
	Charging component					Length			
	Value								

Figure 43: Cost information coding

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 to c23	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 unitization 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 unitization.

Component c7: this component defines the initial time interval for unitization.

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 EN 300 175-6 [6], describing identities and addressing.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< FIXED-IDENTITY >>							1
	Length of Contents (L)								2
	1	Type							3
	1	Length of identity value							4
	0	ARC			ARD				5
									6
	ARD (and RPN)								
									L+2

Figure 44: 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 0 0 0 0 1 0	Access rights identity plus radio fixed part number for WRS
	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 EN 300 175-6 [6].

Access Rights Details (ARD) coding (octet 5 to L+2): refer to EN 300 175-6 [6]. 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. For Identity type "ARI + RPN for WRS" the RPN shall be the RPN of the WRS.

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 EN 300 175-6 [6].

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

Figure 45: 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 0 0 0	Application assigned
	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 Temporary mobile subscriber identity
 1 1 1 1 1 1 1 Proprietary (application specific)
 All other values reserved.

Type coding for identity group "application assigned" (octet 4):

Bits 7 6 5 4 3 2 1 Meaning
 0 1 1 0 0 0 0 Ethernet (IEEE 802.3 [i.11]) Address
 0 1 1 0 0 0 1 Token Ring Address
 0 1 1 0 0 1 0 Internet Protocol Version 4 Address (IPv4), RFC 791 [64]
 0 1 1 0 0 1 1 Internet Protocol Version 6 Address (IPv6), RFC 2460 [66]
 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< INFO-TYPE >>							1
	Length of Contents (L)								2
	0/1	List of one or more							3
	ext	parameter types							

Figure 46: 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 0 0 1	Access rights modify suggest
	0 0 0 0 1 0 0	Authentication of PP failure
	0 0 0 0 1 1 0	Dynamic parameters allocation
	0 0 0 1 0 0 0	External handover parameters (see 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 synchronized external handover candidate
	0 0 0 1 1 0 0	External handover candidate
	0 0 0 1 1 0 1	Multiframe synchronized external handover candidate
	0 0 0 1 1 1 0	Non synchronized external handover candidate
	0 0 0 1 1 1 1	Multiframe, PSCN and multiframe number synchronized 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
	0 1 0 0 1 0 0	OA&M call
	0 1 0 0 1 0 1	Distributed Communication Download
	0 1 1 0 0 0 0	Ethernet (IEEE 802.3 [i.11]) Address
	0 1 1 0 0 0 1	Token Ring Address
	0 1 1 0 0 1 0	Internet Protocol Version 4 Address (IPv4), RFC 791 [64]
	0 1 1 0 0 1 1	Internet Protocol Version 6 Address (IPv6), RFC 2460 [66]
	0 1 1 0 1 0 0	Identity allocation
	All other values reserved.	

NOTE: External handover parameters include 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 Standard							3
									etc.

Figure 47: 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	Information Transfer Capability					3
	1	Negotiation indicator			External Connection Type				4
	0/1	Transfer mode		Information transfer rate					5
	0/1	Unit rate		Rate Multiplier					5a
	0/1	Structure			Configuration		Estab.		5b
	0/1	Symmetry		Information transfer 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

Figure 48: 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	2×64 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	Recommendations ITU-T V.110 [55]/X.30 [57] rate adaption (see 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.726 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 [56] 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 [55]/X.30 [57] rate adaption", the setup 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	EN 300 403-1 [9]
	0 0 1 1 0	Recommendation ITU-T X.25 [44] packet layer
	0 0 1 1 1	ISO/IEC 8208 [18] (Recommendation ITU-T X.25 [44] packet level for DTE)
	0 1 0 0 0	ISO/IEC 8348 [19] (OSI C/O protocol)
	0 1 0 0 1	ISO/IEC 8473 [20] (OSI C/L service)
	0 1 0 1 0	Recommendation ITU-T T.70 [45], minimum network layer
	1 0 0 1 0	GSM TS 144 018 [10]
	1 0 0 1 1	UMTS TS 124 008 [62]
		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 1745 [46]
	0	0	0	1	0	Recommendation ITU-T Q.921 [i.12]/I.441 (LAP.D)/ETS 300 125 [15]
	0	0	1	1	0	Recommendation ITU-T X.25 [44]; link layer (LAP.B)
	0	0	1	1	1	Recommendation ITU-T X.25 [44] multilink
	0	1	0	0	0	Extended LAP.BN Recommendation ITU-T T.71 [16]
	0	1	1	0	0	ISO/IEC 8802-2 [17] (LAN LLC)
	1	0	0	0	1	ISO/IEC 8802-2 [17] (see note 7)
	1	0	0	1	0	GSM TS 144 006 [43]
	1	0	0	1	1	TS 124 008 [62]
	1	0	1	1	0	Recommendation ITU-T V.42 [68] (LAP.M)

All other values reserved.

NOTE 4: ISO/IEC 8802-2 [17] refers to LAN operation with a null layer 2 protocol (LLC not implemented).

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	1	Profile					3
	1	Negotiation indicator			Profile subtype				4
									5
	IWU Attribute(s) information								
									L+2

Figure 49: IWU-ATTRIBUTES information element for Profile defined coding standard

Profile (octet 3):

Bits	5	4	3	2	1	Meaning
	0	0	0	0	0	DPRS FREL
	0	0	0	0	1	DPRS Stream
	0	0	0	1	0	D data profile
	0	0	0	1	1	LRMS (E-profile) service (EN 300 757 [48])
	0	0	1	0	0	F data profile (historical)
	0	0	1	0	1	ODAP basic data
	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
	0	1	1	0	1	CTM FP1 32 kbit/s
	0	1	1	1	0	DMAP
	0	1	1	1	1	MRAP
	1	0	0	0	0	ULE part 1 (TS 102 939-1 [79])

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, MM, 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< IWU-PACKET >>							1
	Length of Contents (L)								2
	0/1	S/R	0 spr	L2 protocol ID					3
	1	1	1	L3 protocol ID					3a
									4
	IWU PACKET INFORMATION								
									L+2

Figure 50: 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 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).

L2 protocol ID coding (octet 3):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User Specific (see note 4)
	0 0 0 0 1	Basic mode ISO 1745 [46]
	0 0 0 1 0	Recommendation ITU-T Q.921 [i.12]/I.441 (LAP.D)/ETS 300 125 [15]
	0 0 1 1 0	Recommendation ITU-T X.25 [44] link layer (LAP.B)
	0 0 1 1 1	Recommendation ITU-T X.25 [44] multilink
	0 1 0 0 0	Extended LAP.B
	0 1 0 0 1	IPv4 (Internet Protocol version 4) RFC 791 [64]
	0 1 0 1 0	IPv6 (Internet Protocol version 6) RFC 2460 [66]
	0 1 0 1 1	PPP (Point-to-Point Protocol) RFC 1661 [65]
	0 1 1 0 0	ISO/IEC 8802-2 [17] (LAN LLC)
	1 0 0 0 1	ISO/IEC 8802-2 [17] (see note 3)
	1 0 0 1 0	GSM TS 144 006 [43]
	1 0 1 1 0	Recommendation ITU-T V.42 (LAP.M) [68]
		All other values reserved.

L3 protocol ID coding (octet 3a):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (see note 4)
	0 0 0 1 0	EN 300 403-1 [9]
	0 0 1 1 0	Recommendation ITU-T X.25 [44], packet layer
	0 0 1 1 1	ISO/IEC 8208 [18] (X.25 [44] packet level for DTE)
	0 1 0 0 0	ISO/IEC 8348 [19] (OSI C/O protocol)
	0 1 0 0 1	ISO/IEC 8473 [20] (OSI C/L service)
	0 1 0 1 0	Recommendation ITU-T T.70 [45] (minimum NWK layer)
	1 0 0 1 0	GSM TS 144 018 [10]
	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 clause 7.7.21.

NOTE 3: ISO/IEC 8802-2 [17] 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) or to exchange DECT Profile specific information between the peer interworking units.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< IWU-TO-IWU >>							1
	Length of Contents (L)								2
	1	S/R	Protocol Discriminator						3
									4
	IWU-TO-IWU INFORMATION								
									L+2

Figure 51: 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 (see note 2)
0 0 0 0 0 1		OSI high layer protocols
0 0 0 0 1 0		Recommendation ITU-T X.263 [21] (see note 3)
0 0 0 0 1 1		List Access
0 0 0 1 0 0		IA5 characters
0 0 0 1 0 1		ULE Configuration and Control (see TS 102 939-1 [79])
0 0 0 1 1 0		Light data service, Software Upgrade Over The Air (SUOTA) (see TS 102 527-4 [76])
0 0 0 1 1 1		Recommendation ITU-T V.120 [56] Rate adaption
0 0 1 0 0 0		Recommendation ITU-T Q.931 [i.15] (I.451), message
0 0 1 0 0 1		Recommendation ITU-T Q.931 [i.15] (I.451), information element(s) (see note 4)
0 0 1 0 1 0		Recommendation ITU-T Q.931 [i.15] (I.451), partial message. (see note 5)
0 0 1 1 1 1		Digital Telephone Answering Machine (DTAM)
0 1 0 0 0 0		GSM, message/TS 144 018 [10]
0 1 0 0 0 1		GSM, information element(s)/TS 144 018 [10] (see note 4)
0 1 0 0 1 0		UMTS/GPRS information element(s) (note 4)/TS 124 008 [62]
0 1 0 0 1 1		UMTS/GPRS, messages/TS 124 008 [62]
0 1 0 1 0 0		LRMS (EN 300 757 [48])
0 1 0 1 0 1		RLL Access Profile (RLL access profile, EN 300 765-1 [50])
0 1 0 1 1 0		WRS (EN 300 700 [63])
1 0 0 0 0 0		DECT/ISDN Intermediate System C-plane specific
1 0 0 0 0 1		DECT/ISDN Intermediate System U-plane specific
1 0 0 0 1 0		DECT/ISDN Intermediate System Operation and Maintenance
1 0 0 0 1 1		Terminal Data (see note 6)
1 0 0 1 0 0		DECT access to IP Networks specific, TS 102 265 [69]
1 0 0 1 0 1		MPEG-4 ER AAC-LD Configuration Description, TS 102 527-1 [73]
1 1 1 1 1 1		Unknown
All other values reserved.		

NOTE 2: The IWU information is structured as shown in figure 52.

IWU-to-IWU information field (octets 4 to L+2) for Protocol Discriminator value "user specific".

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Discriminator type							4
									5
	User specific contents								
									L+2

Figure 52

NOTE 3: The IWU information is structured according to Recommendation ITU-T X.263 [21] (Recommendation ITU-T X.25 [44] call user data).

NOTE 4: If more than one element is included, they are interpreted in the order of appearance.

NOTE 5: The Recommendation ITU-T Q.931 [i.15] (I.451) partial message excludes the protocol discriminator and the call reference.

NOTE 6: If the protocol discriminator indicates the value "Terminal data" for the content of the information element see annex I.

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"

Bit:	8	7	6	5	4	3	2	1	Octet:
	Discriminator								5
	Discriminator (continued)								6
									7
	Proprietary contents								
									L+2

Figure 53

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< KEY >>							1
	Length of Contents (L)								2
	Key type								3
									4
	Key								
									L+2

Figure 54: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< LOCATION-AREA >>							1
	Length of Contents (L)								2
	LI-Type		Location area level						3
	ELI-Type								3a
	Extended Location Information								
									L+2

Figure 55: 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 PARI + RPN are relevant for this location area. The bit count starts with the MSB of the PARI + RPN.

Extended Location Information (ELI) type coding (octet 3a):

Bits	8 7 6 5	Meaning
	0 1 1 1	Location information is requested and not included; bits 1 to 4 of octet 3a should be set to 1
	1 1 1 1	Location information
		All other values reserved.

Location information coding:

Bit:	8	7	6	5	4	3	2	1	Octet:
	MCC digit 2				MCC digit 1				4
	1	1	1	1	MCC digit 3				5
	MNC digit 2				MNC digit 1				6
	LAC								7
	LAC (continued)								8
	CI								9
	CI (continued)								10

MCC: Mobile Country Code;
MNC: Mobile Network Code;
LAC: Location Area Code;
CI: Cell Identity.

Figure 56

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MULTI-DISPLAY >>							1
	Length of Contents (L)								2
									3
	List of Display Information (DECT characters)								
									L+2

Figure 57: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MULTI-KEYPAD >>							1
	Length of Contents (L)								2
									3
	List of Keypad Information (DECT characters)								
									L+2

Figure 58: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< NWK-ASSIGNED-IDENTITY >>							1
	Length of Contents (L)								2
	1	Type							3
	1	Length of identity value							4
									5
	Identity value								
									L+2

Figure 59: 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 Temporary Mobile Subscriber Identity (TMSI, P-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 TMSI:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of identity value							4
									5
	TMSI value								
									L+2

Figure 60

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< NETWORK-Parameter >>							1
	Length of Element (L)								2
	Discriminator								3
									4
	Data (see note)								
									L+2

NOTE: The <data> field is not structured because information is passed transparently.

Figure 61a: NETWORK Parameter information element

Discriminator coding (octet 3):

Bits	8	7	6	5	4	3	2	1	Meaning
	0	0	0	0	1	0	0	0	Application assigned
	0	0	0	1	0	0	0	0	Device name
	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
	1	1	1	0	1	0	1	1	Handover reference, UMTS network
	1	1	1	0	1	1	0	0	Handover reference request, UMTS network
All other values reserved.									

Data field coding for device name (octet 4):

The purpose of the device name element is to convey the name of the FP that may be displayed by the PT and may be used by the user to select the FP among those in subscription mode.

Data field coding for Device name (octet 4+):

Bit:	8	7	6	5	4	3	2	1	Octet:
									4
	Device name								
	(List of DECT characters)								L+2

Figure 61b

The length of the device name shall be chosen to fit in a {CLMS-FIXED} message.

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

Data field coding for handover reference (octet 4):

The handover reference is coded using binary representation.

Data field coding for Application assigned (octet 4+):

Bit:	8	7	6	5	4	3	2	1	Octet:
	0/1	Application type_1							4
	Parameter_1								4a

	Parameter_n								4n
								
	0/1	Application type_k							k
	Parameter_1								ka

	Parameter n								kn

Figure 61c

A number of octet groups related to different applications may be included where each group should be defined as follows. The extension bit should be used to indicate whether more than one octet group is included following the DECT rules.

Application type (octet group 4):**Bits 7 6 5 4 3 2 1 Meaning**

0 1 1 0 0 0 0 Ethernet (IEEE 802.3 [i.11]) Address

0 1 1 0 0 0 1 Token Ring Address

0 1 1 0 0 1 0 Internet Protocol Version 4 Address (IPv4), RFC 791 [64]

0 1 1 0 0 1 1 Internet Protocol Version 6 Address (IPv6), RFC 2460 [66]

All other values reserved.

Each parameter has structure and is coded as follows:

Bit:	8	7	6	5	4	3	2	1	Octet:
	M	Type of parameter							k
	0/1	Length of parameter							k+1
	...								
	1	Length of parameter							
	Parameter value								
								k+p	

Figure 61d: Parameters fields' general structure**Type of parameter (octet k):****Bits 7 6 5 4 3 2 1 Meaning**

0 0 0 0 0 0 1 Address

0 0 0 0 0 1 0 Other parameter

All other values reserved.

M bit (octet k):**Bits 8 Meaning**

0 No more parameters

1 More parameters

Length of parameter (octet k+1 ...): 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 of the last octet containing the length. Multiple octets comprising the length are identified by the setting of the extension bit.

Parameter value coding: the Parameter value is provided in format according to the format defined in the relevant standard specifying the relevant application.

7.7.30 Portable identity

The purpose of the <<PORTABLE-IDENTITY>> information element is to transport a DECT portable identity. Refer to EN 300 175-6 [6], describing identities and addressing.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< PORTABLE-IDENTITY >>							1
	Length of Element (L)								2
	1	Type							3
	1	Length of identity value							4
									5
	Identity value								
									L+2

Figure 62: 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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	PUT				PUN				5
	PUN (continued)							6	
								L+2	

Figure 63

Length of identity value coding (octet 4): defines the number of valid IPUI bits.

Portable User Type (PUT) coding (octet 5): refer to EN 300 175-6 [6]. The most significant bit is in bit position 8 in octet 5.

Portable User Number (PUN) coding (octet 5 to L+2): refer to EN 300 175-6 [6]. 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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	1	0	1	digit 1				5
	digit 2				digit 3				6
	digit p-1				digit p				L+2

Figure 64

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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	0	0	1	Number				5
	Number								6
	Number								L+2

Figure 65

Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals $4 + (0 \text{ to } 60)$.

Private number coding number (octet 5 to L+2): the number is binary coded and shall not exceed 60 bits. 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 T containing the equipment installer's code and private extended number:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	1	1	0	EIC				5
	EIC								6
	EIC				digit 1				7
	digit 2				digit 3				8
	digit p-1				digit p				L+2

Figure 66

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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	0	1	0	POC				5
	POC								6
	POC				ACC				7
	ACC								8
	ACC								L+2

Figure 67

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. 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 Q containing the bank account number:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	0	1	1	digit 1				5
	digit 2				digit 3				6
	digit p-1				digit p				L+2

Figure 68

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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	1	1	1	digit 1				5
	digit 2				digit 3				6
	diait p-1				digit p				L+2

Figure 69

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 IMSI:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Length of Identity Value							4
	0	1	0	0	digit 1				5
	digit 2				digit 3				6
	digit p-1				digit p				L+2

Figure 70

Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to $4 + 4 \times p$.

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):

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	1	0	1	0	0	0	4
	0	0	0	0	EMC				5
					EMC				6
	EMC				PSN				7
					PSN				8
					PSN				9

Figure 71

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 EN 300 175-6 [6]. 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 EN 300 175-6 [6]. 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:

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	0	1	0	1	0	0	4
	Assignment type				TPUI value				5
					TPUI value				6
					TPUI value				7

Figure 72

Length of identity value coding (octet 4): the number of valid bits for a TPUI is 20.

Assignment Type coding (octet 5):

Bits	8 7 6 5	Meaning
	0 0 0 0	TPUI
	0 0 0 1	TPUI with number assigned (see note)
		All other values reserved.

Temporary Portable User Identity (TPUI) coding (octet 5 to 7): Refer to EN 300 175-6 [6]. The most significant bit is in bit position 4 in octet 5. The order of bit values progressively decreases as the octet number increases.

NOTE: The last part of assigned value may be used to convey the terminal identity number, extension number, or last part of the BCD coded telephone number.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< PROGRESS-INDICATOR >>							1
	Length of Contents (L)								2
	1	Coding standard	0	Location					3
	1	Progress description							4

Figure 73: PROGRESS-INDICATOR information element

Coding standard coding (octet 3):

Bits	7 6	Meaning
	0 0	ITU-T standardized 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
									3
	RAND Field								
									L+2

Figure 74: RAND information element

NOTE 1: 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 and message.

NOTE 2: For either the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2), the <<RAND>> IE is used to carry in the {AUTHENTICATION-REQUEST} message the RAND_F parameter in the PT authentication procedure and the RAND_P parameter in the FT authentication procedure (see EN 300 175-7 [7] clauses 4.3 and 6.3).

NOTE 3: For the DECT Standard Authentication Algorithm #2 (DSAA2), and using type 2 authentication exchanges (see EN 300 175-7 [7], clauses 4.3 and 6.3), the <<RAND>> IE is used to carry in the {AUTHENTICATION-REPLY} message the RAND_P parameter in the PT authentication procedure and the RAND_F parameter in the FT authentication procedure.

NOTE 4: For either the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2), the <<RAND>> IE is used to carry in the {KEY-ALLOCATE} message the RAND_F parameter used in the PT authentication procedure (see EN 300 175-7 [7] clause 6.5.6).

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 Contents (L)								2
	1	Symmetry		I	Class of service				3
	0/1	Channel 1 user rate P=>F			Channel 1 arrangement P=>F				4
	1	Channel 1 user rate F=>P			Channel 1 arrangement F=>P				4a
	0/1	Channel 2 user rate P=>F			Channel 2 arrangement P=>F				5
	1	Channel 2 user rate F=>P			Channel 2 arrangement F=>P				5a
	0/1	Channel 3 user rate P=>F			Channel 3 arrangement P=>F				6
	1	Channel 3 user rate F=>P			Channel 3 arrangement F=>P				6a

Figure 75: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< REJECT-REASON >>							1
	Length of Contents (L)								2
	Reject reason code								3

Figure 76: 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 (see 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 another 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< RES >>							1
	Length of Contents (L)								2
									3
	RES Field								
									L+2

Figure 77: RES information element

NOTE 1: 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 L+2);
- 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.

NOTE 2: For authentication using either, the DSAA or the DSAA2 algorithms, the RES field consist of 4 octets and the total length of the IE is 6 octets.

NOTE 3: The <<RES>> IE is used in the {AUTHENTICATION-REPLY} message. It carries the RES1 parameter in the PT authentication procedure and the RES2 parameter in the FT authentication procedure.

NOTE 4: In the procedure "Key-allocation" (see clause 5.6.6), the <<RES>> IE is also used in the {AUTHENTICATION-REQUEST} message, carrying the RES1 parameter used in the PT authentication procedure.

7.7.36 RS

The purpose of the authentication parameter <<RS>> information element is to transport the security parameter RS (or RS₁₂₈ if DSAA2 algorithm is used). This parameter is used together with <<RAND>> and the authentication key to calculate the authentication response signature.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< RS >>							1
	Length of Contents (L)								2
									3
	RS Field								
									L+2

Figure 78: 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.

NOTE 1: The <<RS>> IE is used in either, the {AUTHENTICATION-REQUEST} and the {AUTHENTICATION-REPLY} messages when transmitted in FT > PT direction, and in the {KEY-ALLOCATE} message.

NOTE 2: The size of the <<RS>> IE is 10 octets when DSAA is used (RS of 64 bits) and 18 octets when DSAA2 is used (RS₁₂₈ of 128 bits).

7.7.37 Segmented info

The purpose of the <<SEGMENTED-INFO>> element is to indicate that the message in which it 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	Number of segments remaining							3
	0	Segmented element type							4

Figure 79: 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 standard	M	Change Mode					3
	1	Extended change mode							3a
	1	A attributes			R	B attributes			4

Figure 80: 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 clause 9.6)
	0 0 1 1	Modulation scheme change (see clause 9.6)
	0 1 0 0	Rerouting (of U-plane links) (see clause 9.6)
	0 1 0 1	Bandwidth plus modulation scheme change (see clause 9.6)
	0 1 1 0	Rerouting plus bandwidth change (see clause 9.6)
	0 1 1 1	Bandwidth or modulation scheme change (see clause 9.6)
	1 0 0 0	Suspend
	1 0 0 1	Resume
	1 0 1 0	Voice/data change to data (see note 1)
	1 0 1 1	Voice/data change to voice (see note 1)
	1 1 0 0	IWU attribute change
	1 1 0 1	Audio Codec change
	1 1 1 0	Profile/Basic service and IWU attributes change (see notes 1 and 2)
	1 1 1 1	Reserved for extension (see 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":

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	0	0	0	Coded as bits 4-1 of				3a
		spare			<<Basic service>>				

Figure 81

Figure 82: Void

Extended change mode for "reserved" is reserved for further standardization.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< SERVICE-CLASS >>							1
	Length of Contents (L)								2
	Service class field								3

Figure 83: 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 Setup capability

The purpose of the <<SETUP-CAPABILITY>> element is to convey some aspects of the PP call setup capabilities to the FP during location registration.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< SETUP-CAPABILITY >>							1
	Length of Contents (L)								2
	0/1	Protocol Discriminator			Setup		Page		3
	1	0	0	0	0	0	0	0	3a
	Spare (see note)								

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. Exact coding may be defined in relevant profiles.

Figure 84: SETUP-CAPABILITY information element

Page capability coding (octet 3):

Bits	2 1	Meaning
	0 1	Normal paging only (normal duty cycle paging detection, see note 4)
	1 0	Fast paging and normal paging (high duty cycle paging detection, see note 4)
		All other values reserved.

Setup capability coding (octet 3):

Bits	4 3	Meaning
	0 0	Selective fast setup (SEL1, SEL2 or SEL2b) supported (see note 5)
	0 1	No fast setup supported (only indirect setup is supported)
	1 0	Complete fast setup mode supported (see note 5)
	1 1	Complete and selective (SEL1, SEL2 or SEL2b) fast setup modes supported (see note 5)

Protocol Discriminator (octet 3):

Bits	7 6 5	Meaning
	0 0 0	Shall not be used (see note 1)
	0 0 1	DPRS (see note 2)
	0 1 0	ODAP (see note 3)
		All other values reserved.

NOTE 1: For backwards compatibility with terminals already using this information element complying with versions of the standard before ed4.

NOTE 2: The exact coding of the octets to follow is to be defined in the DPRS profile (EN 301 649 [72]).

NOTE 3: The exact coding of the octets to follow is to be defined in the ODAP profile (TS 102 342 [70]).

NOTE 4: See EN 300 175-3 [3], clause 11.3.3.1, for the description of the different modes of paging detection.

NOTE 5: See EN 300 175-3 [3], clause 11.3.3.2, for the description of the different modes of listening for setup.

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 capabilities			display capabilities				3
	0/1	echo parameter			N-REJ		A-VOL		3b (see note 1)
	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							4
	0/1	Profile indicator_2							4a
	0/1	Profile indicator_3							4b
	0/1	Profile indicator_4							4c
	0/1	Profile indicator_5							4d
	0/1	Profile indicator_6							4e
	0/1	Profile indicator_7							4f
	0/1	Profile indicator_8							4g
	0/1	Profile indicator_9							4h
	0/1 ext	Profile indicator_10							4i
	0/1	DSAA2	DSC2	0	0	control codes			5
				spare					
	0/1 ext	escape to 8 bit character sets_1 (see note 12)							5a
	0/1	Blind slot indication		sp0	sp1	sp2	sp3	sp4	6
	1	sp5	sp6	sp7	sp8	sp9	sp10	sp11	6a

Figure 85: TERMINAL-CAPABILITY information element

Display capability coding (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	0 0 0 1	No display (see note 8)
	0 0 1 0	Numeric (see note 12)
	0 0 1 1	Numeric-plus (see note 12)
	0 1 0 0	Alphanumeric (see note 13)
	0 1 0 1	Full display (see note 14)
	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 (see note 8)
	0 1 0	dial tone only
	0 1 1	Recommendation ITU-T E.182 [42] tones supported (see note 15)
	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 TCLw (see notes 8, 9, 10, 11 and 27)
	0 1 0	TCLw > 46 dB (Full TCLw, see notes 9, 10 and 11)
	0 1 1	TCLw > 55 dB (VoIP compatible TCLw, see notes 9, 10 and 11)
		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 (see notes 8 and 9)
	1 0	Noise rejection provided (see note 9)
	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 (see notes 8 and 9)
	1 0	PP adaptive volume control used (see note 9)
	1 1	Disable FP adaptive volume control (see note 9)

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 = 80
Bit 2:	Long slot; j = 640
Bit 3:	Long slot; j = 672
Bit 4:	Full slot; (see 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 16 383.

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 1	CAP supported
	x x x x x 1 x	GAP supported (EN 300 444 [51])
	x x x x 1 x x	DECT/GSM interworking profile supported
	x x x 1 x x x	ISDN End-system supported
	x x 1 x x x x	LRMS (EN 300 757 [48]) supported
	x 1 x x x x x	DPRS Stream supported (EN 301 649 [72])
	1 x x x x x x	DPRS asymmetric bearers supported (EN 301 649 [72])

Profile Indicator_2 Coding (Octet 4a):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	DPRS Class 2 management and B-field procedures (DPRS-M.5) supported (see EN 301 649 [72] and note 25)
	x x x x x 1 x	Data Services Profile D, Class 2 supported (EN 301 238 [i.13])
	x x x x 1 x x	ISDN Intermediate Access Profile supported
	x x x 1 x x x	DECT/UMTS-GSM interworking - UMTS-GSM Bearer service supported
	x x 1 x x x x	DECT/UMTS-GSM interworking - UMTS-GSM SMS service supported
	x 1 x x x x x	DECT/UMTS-GSM interworking - UMTS-GSM Facsimile service supported
	1 x x x x x x	RAP 1 Profile (EN 300 765-1 [50]) supported

Profile/Application Indicator_3 Coding (Octet 4b):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	DECT/GSM dual mode terminal
	x x x x x 1 x	WRS supported
	x x x x 1 x x	SMS over LRMS(EN 300 757 [48]) supported
	x x x 1 x x x	DMAp supported
	x x 1 x x x x	Multiport CTA (EN 300 765-1 [50])
	x 1 x x x x x	Ethernet supported
	1 x x x x x x	Token Ring supported

Profile/Application Indicator_4 Coding (Octet 4c):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	IP supported
	x x x x x 1 x	PPP supported
	x x x x 1 x x	V.24 supported
	x x x 1 x x x	C _F supported
	x x 1 x x x x	I _{PQ} services supported (note 2)
	x 1 x x x x x	RAP 2 Profile supported (EN 300 765-2 [58])
	1 x x x x x x	Generic Media Encapsulation transport (DPRS) supported (EN 301 649 [72])

Profile/Application Indicator_5 Coding (Octet 4d):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	2-level modulation scheme supported (B+Z field) (see note 3)
	x x x x x 1 x	4-level modulation scheme supported (B+Z field)
	x x x x 1 x x	8-level modulation scheme supported (B+Z field)
	x x x 1 x x x	16-level modulation scheme supported (B+Z field)
	x x 1 x x x x	2-level modulation scheme supported (A field)
	x 1 x x x x x	4-level modulation scheme supported (A field)
	1 x x x x x x	8-level modulation scheme supported (A field)

Profile/Application Indicator_6 Coding (Octet 4e):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	DECT/UMTS interworking profile supported (TS 101 863 [61])
	x x x x x 1 x	DECT/UMTS interworking - GPRS services supported (TS 101 863 [61])
	x x x x 1 x x	Basic ODAP supported (TS 102 342 [70])
	x x x 1 x x x	F-MMS Interworking profile supported (TS 102 379 [71])
	x x 1 x x x x	Channel G _F supported (see note 20)
	x 1 x x x x x	PT with fast hopping radio (see notes 21 and 22)
	1 x x x x x x	Capability to support "no emission" mode (see EN 300 175-3 [3], clause 9.4)

Profile/Application Indicator_7 Coding (Octet 4f):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	64-level modulation scheme supported (B+Z field)
	x x x x x 1 x	NG-DECT Part 1: Wideband voice supported (TS 102 527-1 [73])
	x x x x 1 0 x	Shall not be used (see note 23)
	x x x x 1 1 x	Support of NG-DECT Part 3 (TS 102 527-3 [75]) (see note 23)
	x x x 1 x x x	Support of the "Headset management" feature (see note 24).
	x x 1 x x x x	Support of "Re-keying" and "default cipher key early encryption mechanism"
	x 1 x x x x x	Support of 'associated melody' per contact (TS 102 527-3 [75]) (see note 28)
	1 x x x x x x	Support of NG-DECT Part 5 (TS 102 527-5 [78]) (see note 29)

Profile/Application Indicator_8 Coding (Octet 4g):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	E+U-type mux and channel I _{PF} basic procedures supported (see note 17)
	x x x x x 1 x	Channel I _{PF} advanced procedures supported (see note 17)
	x x x x 1 x x	Channel SI _{PF} supported (see notes 17 and 18)
	0 0 0 0 x x x	DPRS/NG-DECT Packet Data: No packet data supported or non categorized system (see note 19)
	0 0 0 1 x x x	DPRS/NG-DECT Packet Data Category: Cat 1 (low-end data devices, see note 19)
	0 0 1 0 x x x	DPRS/NG-DECT Packet Data Category: Cat 2 (mid-end data devices, see note 19)
	0 0 1 1 x x x	DPRS/NG-DECT Packet Data Category: Cat 3 (high-end data devices, see note 19)
	0 1 0 0 x x x	DPRS/NG-DECT Packet Data Category: Cat 4 (high-level modulation up to 8PSK, see note 19)
	0 1 0 1 x x x	DPRS/NG-DECT Packet Data Category: Cat 4 (high-level modulation up to 64QAM, see note 19)
	0 1 1 x x x x	Reserved for future Data Categories
	1 0 x x x x x	Reserved for future Data Categories
	1 1 x x x x x	Reserved for future Data Categories

Profile/Application Indicator_9 Coding (Octet 4h):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	DPRS Class 3 management and A-field procedures (DPRS-M.30) supported (see EN 301 649 [72] and note 26)
	x x x x x 1 x	DPRS Class 4 management and A-field procedures (DPRS-M.30) supported (see EN 301 649 [72])
	x x x x 1 x x	Support for DECT ULE Phase 1 (see TS 102 939-1 [79])
	x x x 1 x x x	Reserved for DECT ULE (see note 30)
	x x 1 x x x x	Reserved for DECT ULE (see note 30)
	x 1 x x x x x	Support of Light data services (TS 102 527-4 [76])
	1 x x x x x x	Reserved

Profile/Application Indicator_10 Coding (Octet 4i):

Bits	7 6 5 4 3 2 1	Meaning
	x x x x x 1	Support of "Date and Time recovery" procedure in NG-DECT Part 5 (TS 102 527-5 [78])
	x x x x x 1 x	Support of "Extended list change indication" procedure (see TS 102 527-5 [78])
	x x x x 1 x x	Support of "Screening" feature (see TS 102 527-5 [78])
	All other values	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.

Authentication and Ciphering Algorithms (octet 5):

These bits define the support of certain algorithms for authentication and ciphering. See EN 300 175-7 [7] for the meaning of DSAA2 and DSC2.

DSAA2:

Bits	7	Meaning
	0	DSAA2 not supported
	1	DSAA2 supported

DSC2:

Bits	6	Meaning
	0	DSC2 not supported
	1	DSC2 supported

Bits 4 and 5 of octet 5 are reserved for further standardization and shall be set to "0".

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) (note 4):

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.	

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 ISO/IEC 2022 [11]. A "1" indicates support for the specified character set and that the PT correctly interprets ISO/IEC 2022 [11] escape sequences, see clause 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/IEC 8859-1 [47]
	x x x x x 1 x	Latin alphabet no 9 supported ISO/IEC 8859-15 [52]
	x x x x 1 x x	Latin alphabet no 5 supported ISO/IEC 8859-9 [54]
	x x x 1 x x x	Greek alphabet supported ISO/IEC 8859-7 [53]
	x x 1 x x x x	reserved
	x 1 x x x x x	reserved
	1 x x x x x x	reserved

Blind slot indication (octets 6 and 6a) (see notes 6 and 7):

Bits	7 6	Meaning
	0 0	No blind slots
	0 1	Setup is not possible on both slots adjacent to an active slot
	1 0	Setup is not possible on every second slot
	1 1	Limitations indicated in the following bits (octet 6 and 6a)

sp_x (octet 6 and octet 6a):

For sp_x with $0 \leq x \leq 11$:

if $sp_x = 1$: then full slot pair $\{(x), (x + 12)\}$ is not "blind", i.e. available;

else ($sp_x = 0$) full slot pair $\{(x), (x + 12)\}$ is "blind", i.e. not available.

NOTE 1: Octet 3a is intentionally absent.

NOTE 2: For the definition of the I_{PQ} services see EN 300 175-4 [4] and EN 300 175-3 [3].

NOTE 3: For definition of the modulation schemes see annex D of EN 300 175-2 [2].

NOTE 4: The display behaviour in response to some control codes may be dependent on the scrolling behaviour of the display.

NOTE 5: Void.

NOTE 6: The blind slot information applies to the same slot number of all available carriers.

NOTE 7: Older equipment might not include octet group 6. In this case one should assume that the blind slot information is unknown.

NOTE 8: This capability is assumed as the default value unless otherwise specified by a service profile, if the <<TERMINAL-CAPABILITY>> information element is omitted.

NOTE 9: Refer to EN 300 175-8 [8] for a definition of TCLw, PP Adaptive Volume (A-VOL) control, PP ambient Noise Rejection (N-REJ) and the usage of these parameters.

NOTE 10: For PPs implementing regular (handset) and handsfree modes, the value refers to the handset mode.

NOTE 11: For PPs implementing narrowband and wideband modes, it is strongly recommended to implement similar values of TCLw for both modes. In case of differences, the bit setting will be done as for the narrowband mode.

NOTE 12: "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 13: "Alphanumeric" indicates support for at least the following characters: space, 0-9, *, #, a-z and A-Z.

NOTE 14: "Full display" indicates support for the full DECT character set. (i.e. displayable characters with character codes up to 7F).

NOTE 15: "E.182 tones supported" indicates support of all of the E.182 compatible tones identified in clause 7.6.8.

NOTE 16: More octets may follow for the indication of further profiles or character sets.

NOTE 17: See EN 300 175-3 [3] for description of the I_{PF} channel and the E+U-type mux.

NOTE 18: Requires the support of the SI_P channel. See EN 300 175-3 [3] for description of SI_{PF} channel.

NOTE 19: See EN 301 649 [72] or TS 102 527-2 [74] for exact definition of Packet data Categories (bits 4 to 7 of Octet 4g). Packet data Categories are incremental: Cat 3 systems also support Cat 1 and Cat 2; Cat 2 systems also support Cat 1; Cat 4 and Cat 5 systems also support Cat 1, Cat 2 and Cat 3.

NOTE 20: This bit indicates that the PT has the ability to receive the G_F channel.

NOTE 21: This bit set to 1 indicates that the PT that has not blind slots due to radio transceiver implementation, even if the slots in use are full of double.

NOTE 22: If bit 1 is set to zero, it is assumed that the PT needs a blind slot after any full or double slot in use, however, it does not require a blind slot after a long $j=640$ or a long $j=672$ slot.

NOTE 23: Bit 2 for TS 102 527-1 [73] should also be set.

NOTE 24: This bit indicates that the PT supports the "Headset management" feature (see TS 102 527-3 [75], feature NG1.N.21).

NOTE 25: Implies the support of MAC suspend/resume (see EN 301 649 [72]).

NOTE 26: Implies the support of some procedures of MAC suspend resume (see EN 301 649 [72]).

NOTE 27: For PPs implementing NG-DECT Part 1 (TS 102 527-1 [73]) or NG-DECT Part 3 (TS 102 527-3 [75]) the coding "001" has the meaning of $TCLw > 42$ dB for all other PPs this coding has the meaning of $TCLw > 34$ dB.

NOTE 28: This bit indicates that the PT supports the 'Associated melody' per contact requirements (see TS 102 527-3 [75], procedure 'PT Alerting using pattern signalling').

NOTE 29: Bit 2 for TS 102 527-1 [73] and Bit 3 for TS 102 527-3 [75] should also be set since NG-DECT Part 5 includes all mandatory features of NG-DECT Part 1 and Part 3.

NOTE 30: Reserved DECT ULE bits will be set to '0' for transmission and may not be checked by the receiving party.

7.7.42 Transit delay

The purpose of the <<TRANSIT-DELAY>> element is to indicate the maximum allowable delay that shall be imposed for data transmitting the DECT subnetwork. It may also be used to indicate the maximum allowable delay allowed in the MAC layer.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< TRANSIT-DELAY >>							1
	Length of Contents (L)								2
	0/1	Upstream (PT => FT) overall DECT system maximum delay							3
	1	Downstream (FT => PT) overall DECT system maximum delay							3a
	0/1	Upstream (PT => FT) overall MAC layer maximum lifetime							4
	1	Downstream (FT => PT) overall MAC layer maximum lifetime							4a

Figure 86: TRANSIT-DELAY information element

Overall DECT system PT => FT maximum delay (FT => PT maximum delay) octet 3 (and 3a): the maximum allowable delay over the DECT subnetwork shall be coded as given below, and the result placed in the octet with the least significant bit in position 1. Delay may be calculated in steps of 1 TDMA frame (10 ms) or in steps of 1 Multiframe (160 ms).

Allowable values are coded as follows:

- When bit 7 = 0, bits 6-1 indicate the value in frames (10 ms). The range is "1" to "63" frames.
- Bit 7 = 0 and bits 6-1 coded to "0" indicate infinite (no limit for the transit delay).
- When bit 7 = 1, bits 6-1 indicate the value in Multiframe (160 ms). The range is "1" to "63" Multiframe.
- Bit 7 = 1 and bits 6-1 coded to "0" is reserved for further standardization.

If octet 3a is not included, it means that the value is for downstream direction is the same as the value for upstream direction.

Overall MAC layer PT => FT maximum lifetime (FT => PT maximum lifetime) octet 4 (and 4a): the maximum lifetime allowable in the MAC layer shall be coded as given below, and the result placed in the octet with the least significant bit in position 1. Delay may be calculated in steps of 1 TDMA frame (10 ms) or in steps of 1 Multiframe (160 ms).

Allowable values are coded in the same way as the Overall DECT system maximum delay.

If octet 4a is not included, it means that the value is for downstream direction is the same as the value for upstream direction.

7.7.43 Window size

The purpose of the <<DLC-U-plane-parameters>> element is to indicate (and optionally to negotiate) the window size to be used for frame transmission. replace current content with the following:

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< WINDOW SIZE >>							1
	Length of Contents (L)								2
	0	Window size value (PT => FT)							3
	0/1 ext	Window size value (PT => FT), continue							3a
	0/1 ext	Maximum PDU length (PT => FT)							3b
	1	SDU LAPU timer (PT => FT)							3c
	0	Window size value (FT => PT)							4
	0/1 ext	Window size value (FT => PT), continue							4a
	0/1 ext	Maximum PDU length (FT => PT)							4b
	1	SDU LAPU timer (FT => PT)							4c

Figure 87: WINDOW SIZE information element

If octet group 4 is omitted, the FT => PT values shall be understood to be equal to the PT => FT values.

Window size value (PT => FT and FT => PT) octets 3 and 3a (and 4 and 4a): the <<WINDOW-SIZE>> shall be coded with the natural binary value, and the result placed starting in octet 3a (4a) with the least significant bit in position 1 of octet 3a (4a).

The value "0" shall be used to indicate "not applicable" in the event that no window size is defined for the PT => FT (FT => PT) direction.

Maximum (PT => FT and FT => PT) PDU length (octets 3b, 4b) 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.

SDU LAPU timer (PT => FT and FT => PT) (octet 3c, 4c) value is coded as natural binary value.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< ZAP-FIELD >>							1
	Length of Contents (L)								2
	0	0	0	0	Contents field				3

NOTE 1: Contents field (octet 3).

NOTE 2: Contains the 4 bit ZAP value.

Figure 88: ZAP-FIELD information element

7.7.45 Escape to proprietary

The purpose of the <<ESCAPE-TO-PROPRIETARY>> information element is to send non-standardized information inside a DECT message.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<<ESCAPE-TO-PROPRIETARY>>							1
	Length of Contents (L)								2
	1	Discriminator type							3
	User specific contents								4
									L+2

Figure 89: 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":

Bit:	8	7	6	5	4	3	2	1	Octet:
	Discriminator								4
	Discriminator (continued)								5
									6
	Proprietary contents								
									L+2

Figure 90

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 or vice versa.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MODEL-IDENTIFIER >>							1
	Length of Contents (L)								2
									3
	Model value								
									L+2

Figure 91: MODEL IDENTIFIER information element

NOTE: Model value can represent DECT MANIC+MODIC or IMEISV model identifier types. Distinction is taken based on the Length of Contents (L) information.

Model value coding for DECT MANIC +MODIC containing the EMC code and the model code:

Bit:	8	7	6	5	4	3	2	1	Octet:
	MANIC								3
									4
	MODIC								5

Figure 92

MANIC coding (octets 3 and 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/FT. The combination of MANIC and MODIC should be unique for each hardware/software variant of a PT/FT. The most significant bit of MODIC is in octet 5 bit 8. 0 shall have the meaning of "model number not supported".

Model value for IMEISV containing the IMEISV code:

Bit:	8	7	6	5	4	3	2	1	Octet:
									3
	IMEISV								:
									20

Figure 93

IMEISV coding (octets from 3 to 20): the field contents is specified in EN 300 370 [49].

7.7.47 MMS Generic Header

The usage and coding of the <<MMS Generic Header>> information element is defined in the LRMS profile EN 300 757 [48].

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MMS GENERIC HEADER >>							1
	Length of Contents (L)								2
									3
									L+2

Figure 94: 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 LRMS profile EN 300 757 [48].

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MMS Object Header >>							1
	Length of Contents (L)								2
									3
									L+2

Figure 95: 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 LRMS profile EN 300 757 [48].

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< MMS EXTENDED HEADER >>							1
	Length of Contents (L)								2
									3
									L+2

Figure 96: 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< TIME-DATE >>							1
	Length of Contents (L)								2
	Coding		Interpretation					3	
									4
									L+2

Figure 97: 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 octet 4 contains <Hour>, octet 5 <Minute>, octet 6 <Second> and octet 7 <Time Zone> thus only contains the time information.

The coding value 1 0 "Date" indicates that octets 7 - 10 are omitted and the element only contains 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)
0 0 0 1 0 0		Request to send current time/date (note 2)
0 0 0 1 0 1		No valid time/date available (note 2)
1 0 0 0 0 0		The time/date at which to start forwarding/delivering the MMS message (see note 1)
1 0 0 0 0 1		The time/date the MMS user data was created (see note 1)
1 0 0 0 1 0		The time/date the MMS user data was last modified (see note 1)
1 0 0 0 1 1		The time/date the message was received by the MCE (see note 1)
1 0 0 1 0 0		The time/date the message was delivered/accessed by the End Entity (see note 1)
1 0 1 0 0 0		The time/date stamp for use as an identifier (see note 1)

All other values are reserved.

NOTE 1: These interpretations have specific meanings within the context of profiles.

NOTE 2: This interpretation is used with coding "Time and Date" ('11'B). See NG-DECT Part 3 (TS 102 527-3 [75]) "Date and Time recovery" procedure (clause 7.4.20) If this interpretation is used, octets 4 to L+2 are omitted.

Octets 4 to 6 coding (Time/Date element coding = 1 1 or 1 0):**Table 77**

Octet field	Digits (Semi octets)	Octet
Year	2	4
Month	2	5
Day	2	6

Year, month and day shall be coded in BCD format with the nibble carrying the most significant digit transmitted in bits 8-5 of each octet. Only the last 2 digits of the year shall be used.

EXAMPLE 1: Date 14/01/2009 shall be coded with Octet 4 = 09H (year), Octet 5 = 01H (month), Octet 6 = 14H.

Octets 4 to 7 coding (Time/Date element coding = 0 1):**Table 78**

Octet field	Digits (Semi octets)	Octet
Hour	2	4
Minute	2	5
Second	2	6
Time Zone	2	7

Hour, minutes and seconds shall be coded in BCD format with the nibble carrying the most significant digit transmitted in bits 8-5 of each octet. Hour shall use the 24 hours format (18h stands for 6 p.m.).

EXAMPLE 2: Time 18h58min54sec shall be coded with Octet 4 = 18H (hour), Octet 5 = 58H (minute), Octet 6 = 54H.

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.

Octets 7 to 10 coding (Time/Date element coding = 1 1):

Table 79

Octet field	Digits (Semi octets)	Octet
Hour	2	7
Minute	2	8
Second	2	9
Time Zone	2	10

The same rules defined for octets 4 to 7 with Time/Date element coding = 0 1 shall apply.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< EXT H/O INDICATOR >>							1
	Length of Contents (L)								2
	OID	SYNC		length indicator				3	

Figure 98: EXT H/O INDICATOR information element

length indicator coding (octet 3):

Value	Meaning
0	no handover candidates available via the <<ext. h/o indicator>>
1 to 31	1+ ext h/o length indicator

NOTE: In case value 0 is applied, handover candidates may still be available via the handover retrieval procedure.

The ext h/o length indicator defines how many bits of the PARI 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 synchronization, or no information provided
0 1		Indicates that all identified FPs are multiframe synchronized
1 0		Indicates that all identified FPs are multiframe and PSCN synchronized
1 1		Indicates that all identified FPs are multiframe, multiframe number and PSCN synchronized

7.7.52 Called party Name

The purpose of the << CALLED-PARTY-NAME >> information element is to convey the name of the called party when this name exists in the FP contact list (service defined in NG-DECT Part3: Extended Wideband speech services (TS 102 527-3[75])) or is provided by the network.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALLED-PARTY-NAME >>							1
	Length of Contents (L)								2
	0	spare		Used Alphabet			Screening indicator		3
	1	Length of Called Party Name (LN)							4
	Called Party Name								
	(List of characters)								
	1	Length of Called Party First Name (LF)							LN+5
	Called Party First Name								
	(List of characters)								L+2

Figure 98a: CALLED-PARTY-NAME information element

Used Alphabet (octet 3):

Bits	5 4 3	Meaning
	0 0 0	DECT standard (as described in annex D)
	0 0 1	UTF-8 (see notes 1 and 2)
	All other values reserved.	

Screening indicator (octet 3):

Bits	2 1	Meaning
	0 0	User-provided
	1 1	Network provided.
	All other values reserved.	

NOTE 1: UTF-8 is defined in RFC 3629 [77].

NOTE 2: Some guidelines are given in annex M of the present document.

7.7.53 Calling party Name

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CALLING-PARTY-NAME >>							1
	Length of Contents (L)								2
	0	Presentation indicator	Used Alphabet				Screening indicator	3	
									4
	Calling Party Name								
	(List of characters)								L+1

Figure 98b: CALLING-PARTY-NAME information element

Presentation indicator (octet 3):

Bits	7 6	Meaning
	0 0	Presentation allowed (see notes 1 and 2)
	0 1	Presentation restricted (see note 2)
	1 0	Name not available (see note 3)
	1 1	Handset locator

Used Alphabet (octet 3):

Bits	5 4 3	Meaning
	0 0 0	DECT standard (as described in annex D)
	0 0 1	UTF-8 (see notes 4 and 5)
	1 1 1	Network specific
	All other values reserved.	

Screening indicator (octet 3):

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: No matter network service provision or CNIP content, if the associated CLIP provided by the network has a Calling Party Address which matches an entry in the FP contact list (service defined in NG-DECT Part 3: Extended Wideband speech services (TS 102 527-3 [75])), the name from the contact list should be sent in the Calling-Party-Name information element. In that case, the Screening indicator is set to "User-provided, verified and passed".

NOTE 2: The presentation indicator should match the indications given by the network for the CNIP service.

NOTE 3: When no CNIP indication is provided by the network (if no CNIP service is provisioned by the network), the complete information element should not be used (except if note 1 applies). The "Name not available" presentation indicator should not be used to cover this case.

NOTE 4: UTF-8 is defined in RFC 3629 [77].

NOTE 5: Some guidelines are given in annex M of the present document.

7.7.54 Codec List

This information element is used in New Generation DECT, wideband speech. The purpose of <<CODEC-LIST>> is the indication of a prioritized list of "speech services". Each item in the list contains a speech codec, the supported MAC service, supported C_F channel attributes and supported slot size. The information element contains a negotiation indicator, used for codec negotiation.

The information element is used in several procedures described in TS 102 527-1 [73].

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< CODEC-LIST >>							1
	Length of Contents (L)								2
	1	Negotiation indicator			Reserved				3
	0	1 st Codec Identifier (highest priority)							4
	0	Reserved			MAC and DLC service				4a
	0/1	C-plane routing			Slot size				4b
	0	...							
	0	...							
	0	Last Codec Identifier (lowest priority)							k
	0	Reserved			MAC and DLC service				ka
	1	C-plane routing			Slot size				kb

Figure 98c: CODEC LIST information element

Negotiation indicator (octet 3):

Bits	7 6 5	Meaning
	0 0 0	Negotiation not possible
	0 0 1	Codec negotiation
	All other values reserved.	

Codec identifier: (octets 4, 5...k):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 1	user specific, information transfer rate 32 kbit/s
	0 0 0 0 0 1 0	G.726 ADPCM, information transfer rate 32 kbit/s
	0 0 0 0 0 1 1	G.722, information transfer rate 64 kbit/s
	0 0 0 0 1 0 0	G.711 A law PCM, information transfer rate 64 kbit/s
	0 0 0 0 1 0 1	G.711 μ law PCM, information transfer rate 64 kbit/s
	0 0 0 0 1 1 0	G.729.1, information transfer rate 32 kbit/s
	0 0 0 0 1 1 1	MPEG-4 ER AAC-LD, information transfer rate 32 kbit/s
	0 0 0 1 0 0 0	MPEG-4 ER AAC-LD, information transfer rate 64 kbit/s
	0 0 0 1 0 0 1	user specific, information transfer rate 64 kbit/s
	All other values reserved.	

MAC and DLC service: (octets 4a, 5a...ka):

Bits	4 3 2 1	Meaning
	0 0 0 0	DLC service LU1, MAC service: I_{NA} ($I_{N_minimum_delay}$)
	0 0 0 1	DLC service LU1, MAC service: I_{NB} ($I_{N_normal_delay}$)
	0 0 1 0	DLC service LU1, MAC service: I_{PM} ($I_{P_error_detect}$)
	0 0 1 1	DLC service LU1, MAC service: I_{PQ} ($I_{PQ_error_detect}$)
	0 1 0 0	DLC service LU7, MAC service: I_{NB} ($I_{N_normal_delay}$)
	0 1 0 1	DLC service LU12, MAC service: I_{NB} ($I_{N_normal_delay}$), encapsulation as EN 300 175-4 [4], clause E.1
	All other values reserved.	

Slot size: (octets 4b, 5b...kb):

Bits	4 3 2 1	Meaning
	0 0 0 0	Half slot; $j = 0$.
	0 0 0 1	Long slot; $j = 640$
	0 0 1 0	Long slot; $j = 672$
	0 1 0 0	Full slot
	0 1 0 1	Double slot
	All other values reserved.	

C plane routing: (octets 4b, 5b...kb):

Bits	7 6 5	Meaning
	0 0 0	C_S only
	0 0 1	C_S preferred/ C_F accepted
	0 1 0	C_F preferred/ C_S accepted
	1 0 0	C_F only
	All other values reserved.	

7.7.55 Events notification

7.7.55.1 General structure

The purpose of the <<EVENTS-NOTIFICATION>> information element is to convey events notification to the user regarding the state of one or several resources.

Events may be standard or proprietary.

- A **standard event** coding comprises an event type octet (with proprietary flag unset), an optional event subtype field, and a one or two octet event multiplicity field.
- A **proprietary event** coding comprises an event type octet (with proprietary flag set), a two-octet discriminator field, a one-octet length field (length in octet of the next field), and a proprietary event value (one or several octets).

An event notification IE comprises:

- An Event notification IE discriminator octet with the code 0x7d.
- A Length of Contents octet (octet 2) indicating the number of octets in the IE starting from octet 3.
- One or several events, of any of the two defined types (standard or proprietary) in any order.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< Events-Notification >> (0x7d)							1
	Length of Contents (L)								2
	0/1	prop=0	Standard Event type value						3
	0/1	Event sub type							3a
	0/1	Event multiplicity							4
	1	Event multiplicity							4a
	...								
	0/1	prop=0	Standard Event type value						K
	0/1	Event sub type							Ka
	0/1	Event multiplicity							K+1
	1	Event multiplicity							(K+1)a
	...								

NOTE: Figure 98d only shows standard events notifications. However there can be also proprietary event notifications. Proprietary event notifications have the structure shown in figure 98e that replaces octet groups 3 and 4 (or K and K+1) of figure 98d. Standard and proprietary notifications may be combined in any order.

Figure 98d: Structure of the <<EVENTS-NOTIFICATION>> information element

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	prop=1	Proprietary event type value						P
	Discriminator								P+1
	Discriminator (continued)								P+2
	Length of proprietary event (Le)								P+3
	Proprietary event								P+4
	...								
	Proprietary event								P+Le+3
	...								

NOTE: This group replaces octet groups 3 and 4 (or K and K+1) of figure 98d.

Figure 98e: Proprietary notification structure within an <<EVENTS-NOTIFICATION>> information element

Length of Contents (L, octet 2):

This field shall contain the number of octets in the IE from octet 3 to the end of the IE. It allows the PP to know, when reading an event, if it is the last event of the IE, or if there is an additional event afterwards.

7.7.55.2 Event types

Event type octet: coding for standard (octet groups 3 or K) and proprietary (octet group P) notifications:

Bit 8 (extension bit) - Presence of event subtype octet (3a or Ka):

In case of standard event, bit 8 of the "Event type" octet set to 0 indicates the presence of a following "Event sub type" in the following octet.

In case of proprietary event, bit 8 of the "Event type" octet shall always be set to 0.

Bit 1 to 7 - Proprietary event type flag (prop bit) and event type value:

Bit 7 of the "Event type" octet set to '1' indicates that the event is a proprietary event. Otherwise the event is a standard event.

There are 64 possible values for standard event types.

There are 64 possible values for proprietary event types.

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	Message waiting
	0 0 0 0 0 0 1	Missed call
	0 0 0 0 0 1 0	Web content
	0 0 0 0 0 1 1	List change indication
	0 0 0 0 1 0 0	Software upgrade indication
	0 0 0 0 1 0 1	Line use status indication
	0 0 0 0 1 1 0	Handset use status indication
	0 0 0 0 1 1 1	Diagnostic indication 0 0 0 1 0 0 0 SMS message
	1 x x x x x x	Proprietary notification
	All other values reserved.	

7.7.55.3 Event subtypes

Event sub type field coding for standard event types (octet 3a, Ka):

The "Event subtype" field is an optional (see bit 8 of octet 3 or K above) extensible field of one or more octets.

For most uses of the "Event sub type" field, a single octet is used. In that case, bit 8 of the "Event subtype" octet shall be set to 1 (end of octet group 3).

EXAMPLE 1: For the list change indication event type, the "Event subtype" field may use more than one octet. See the dedicated subsection below.

Bits 1 to 7 of the used octets shall contain the "Event subtype" value. The "Event subtype" value interpretation depends on the "Event type" value. The set of possible values for the event subtype is described below.

Event sub type field coding for standard event type "Message waiting" (octet 3a, Ka):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 0 0 0 0 0	Unknown
	1 0 0 0 0 0 0 1	Voice message
	All other values reserved.	

Event sub type field coding for standard event type "Missed call" (octet 3a, Ka):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 0 0 0 0 0	Unknown
	1 0 0 0 0 0 0 1	A new external missed voice call just arrived (see note 1).
	1 0 0 0 0 0 1 0	No new missed call arrived, but the number of "unread" external missed voice calls has -or may have- changed (see note 2).
All other values reserved.		

NOTE 1: The purpose of this notification is to allow the PP to warn the user that a missed call just arrived in the missed call list. The total number of "unread" entries in the missed call list for the indicated line is provided with the notification. As it is allowed to send a single notification for several close events, this total number may actually not have changed in some cases (see in TS 102 527-3 [75], clauses 7.4.1.3 and C.2.6).

NOTE 2: The purpose of this notification is to allow the PP to update the total number of "unread" missed calls, if it changed although there was no new missed call (most notably when one of the PPs reads an entry). The PP receiving the notification does not need to consult the list. In some cases this total number, although notified, may actually not have changed (see in TS 102 527-3 [75], clause 7.4.1.3, example 2).

Event sub type field coding for standard event type "Web content" (octet 3a, Ka):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 0 0 0 0 0	Unknown
	1 0 0 0 0 0 0 1	RSS description
All other values reserved.		

Event sub type field coding for standard event type "List change indication" (octet subgroup 3a, Ka):

The "Event sub type" field indicates a list identifier.

NOTE 3: The list change indication event notification for a proprietary list requires the use of a two-octet "Event subtype" field.

EXAMPLE 2: Event subtype coding for proprietary list identifier 0x80 is: 0x0180.

NOTE 4: See TS 102 527-3 [75] for use of "List change indication".

Event sub type field coding for Event type "Software upgrade indication" (octet 3a, Ka):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 0 0 0 0 0	Unknown
	1 0 0 0 0 0 0 1	Firmware upgrade
	1 1 x x x x x x	Reserved for proprietary upgrade codes
All other values reserved.		

Event sub type field coding for Event type "Line use status indication" (octet 3a or Ka):

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Event subtype value = 'Line use status value'							3a

Line use status coding (octet 3a or Ka)

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	Line is idle (no active call at all)
	0 0 0 0 0 0 1	Line is in-use (but additional calls can be placed)
	0 0 0 0 0 1 1	Line or system is busy
All other values reserved.		

NOTE 5: For more information on the meaning of the status values, see 102 527-5 [78], clause 7.4.34.3.3.

Event sub type field coding for Event type "Handset use status indication" (octet 3a or Ka):

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Event subtype value = '0000000'B							3a

NOTE 6: For the event type 'handset use status indication', the event subtype is not used.

Event sub type field coding for Event type "Diagnostic indication" (octet 3a or Ka):

Bit:	8	7	6	5	4	3	2	1	Octet:
	1	Event subtype value = 1H, 2H							3a

Event subtype value (octet 3a or Ka):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 1	Line related change (see note 7)
	0 0 0 0 0 1 0	Non line related change (see note 8)
	All other values reserved.	

NOTE 7: The concerned line is indicated in the accompanying <Event multiplicity> field.

NOTE 8: In that case the <Event multiplicity> field holds a *don't care* value.

Event sub type field coding for standard event type "SMS message" (octet 3a, Ka):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 0 0 0 0 0	Unknown
	1 0 0 0 0 0 0 1	A new SMS message just arrived (see note 9)
	1 0 0 0 0 0 1 0	No new SMS message arrived, but some other list change(s) triggered the notification (see note 10)
	All other values reserved.	

NOTE 9: This value is used for notifying the PP (and end user) of a change (or set of changes close in time) in the incoming SMS list (and concerning the indicated SMS service). The change or set of changes notified includes one single SMS arrival for that SMS service. Conversely, a single notification with this subtype value can be used for any given SMS. This notification is always sent with a list change indication. The total number of "unread" entries (at the time of sending) in the incoming SMS list for the indicated SMS service is provided with the notification (see in TS 102 527-5 [78], clause 7.4.1.6).

NOTE 10: This value is used for notifying a change (or set of changes close in time) in the incoming SMS list that does not include any new SMS arrival. This notification is always sent with a list change indication (see TS 102 527-5 [78], clause 7.4.1.6).

7.7.55.4 Event multiplicity

Event multiplicity for standard event types (octet 4, K+1): the total number of events notified.

The event multiplicity field is mandatory and shall have a length of one or two octets.

Allowable values: 0 to 127 if the Event multiplicity field is coded with one octet. 0 to 16383 if event multiplicity is coded with several octets.

The extension bit allows to code the Event multiplicity field with several octets. Extension bit set to 0 indicates that there is an additional octet after the current one for coding the "Event multiplicity" field value. Extension bit set to 1 indicates that the current octet is the last one.

If event multiplicity includes only 1 octet, "event multiplicity = 1" is coded as (octet k+1)= 0x81,

If event multiplicity includes several octets, most significant bit appear first (with leading zeros before if needed); e.g. "event multiplicity = 128" is coded as (octet K+1 = 0x01), following and last octet = 0x80.

Event multiplicity for standard event type "Message waiting" (octet 4, K+1):

The "Event multiplicity" field indicates the total number of unread messages for the line indicated in the accompanying <<CALL INFORMATION>> IE (see clause 7.4.1.2 in both TS 102 527-3 [75] and TS 102 527-5 [78] for more details).

NOTE 1: If the 'DTAM incoming call list' is implemented (see TS 102 527-5[78], clause 6.10) this total number corresponds to the number of entries in this list that have a 'Read status' field value of 'unread'.

Event multiplicity for standard event type "Missed call" (octet 4, K+1):

The "Event multiplicity" field indicates the total number of unread messages in the missed calls list for the line indicated in the accompanying <<CALL INFORMATION>> IE (see TS 102 527-3 [75], clause 7.4.1.3).

Event multiplicity for standard event type "List change indication" (octet 4, K+1):

If the accompanying <<CALL INFORMATION>> IE contains a line id, the "Event multiplicity" field indicates the total number of elements in the list for the corresponding line.

If the accompanying <<CALL INFORMATION>> IE contains a service id, the "Event multiplicity" field indicates the total number of elements in the list for the corresponding service.

Event multiplicity for standard event type "Software upgrade indication" (octet 4, K+1):

The "Event multiplicity" field is not used and shall be one octet long with a value of '0'.

Event multiplicity for standard event type "Line use status indication" (octet 4, K+1):

The "Event multiplicity" field shall contain the line id of the concerned line.

Event multiplicity for standard event type "Handset use status indication" (octet 4, K+1):

The "Event multiplicity" field shall contain the line id of the concerned line.

Event multiplicity for standard event type "Diagnostic indication" (octet 4, K+1):

In case the diagnostic is line related, the "Event multiplicity" field shall contain the line id of the concerned line. Otherwise, it shall contain a value of '0'.

NOTE 2: Whether the diagnostic is line related or not is indicated in the event subtype value of the diagnostic indication.

Event multiplicity for standard event type "SMS message" (octet 4, K+1):

The "Event multiplicity" field indicates the total number of unread messages in the 'incoming SMS' list for the SMS service indicated in the accompanying <<CALL INFORMATION>> IE (see TS 102 527-5 [78], clause 7.4.1.6).

7.7.55.5 Proprietary events**Event notification format for proprietary events (see figure 98e):**

The proprietary event type value shall be coded in octet P. Bit 7 of octet P shall be set to '1'.

Bit 8 of octet P has no special meaning and shall be set to '0'.

NOTE: Value '1' is reserved for further standardization and should not be used.

Discriminator (octets P+1 and P+2):

The discriminator field comprises 2 octets, and shall contain the EMC. Octet P+1 is EMC value high byte, octet P+2 is EMC value low byte.

Length of proprietary event coding (Le, octet P+3):

This field represents the number of octets following the length field itself (octets P+4 to P+Le+3). It is coded as a natural binary value (least significant bit is bit 1)

Proprietary event (octets P+4 to P+Le+3):

The proprietary event value.

7.7.56 Call information

The purpose of the << CALL-INFORMATION >> information element is to convey line identifiers in various contexts, call identifiers, and call statuses.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< Call information >> (0x7e)							1
	Length of Contents (L)								2
	Identifier type								3
	Identifier subtype								3a
	0/1	Identifier value							4
							
	1	Identifier value							
	Identifier type								3
	Identifier subtype								3a
	0/1	Identifier value							4
							
	1	Identifier value							

Figure 98f: CALL INFORMATION information element

Identifier type (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	Line identifier
	0 0 0 0 0 0 0 1	Call identifier
	0 0 0 0 0 0 1 0	Call status
	0 0 0 0 0 0 1 1	Service identifier

The meaning of the identifier subtype is depending on the value of the "Identifier type".

A party (PP or FP) receiving an identifier with an "Identifier type" that it does not understand, shall ignore this identifier, and proceed further with the next one (i.e. it shall not ignore the whole <<CALL-INFORMATION>> information element as a result).

Line identifier subtype (octet 3a):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	Line identifier for external call (see note 1)
	0 0 0 0 0 0 0 1	Source line identifier for internal call (see note 2)
	0 0 0 0 0 0 1 0	Target line identifier for internal call (see note 2)
	0 0 0 0 0 0 1 1	"Relating-to" line identifier (see note 3)
	0 0 0 0 0 1 0 0	"All lines" (see note 4)
	0 0 0 0 0 1 0 1	Line type information (see note 5)
	All other values	reserved.

NOTE 1: Subtype '00'H is used to specify the line id value used for an external call, or to specify that this line id value is not yet known (see the "None" special identifier value defined in the "Identifier value" subsection).

NOTE 2: Use of the "Source line identifier for internal call" value, or of the "Target line identifier for internal call" value indicates that the line id is used as a shorthand for the group of PPs attached to the external line (seen as a possible source or target of an internal call). Either one of these values or both values may be used in the same message.

NOTE 3: A "relating-to" line identifier indicates that the current exchange is relating to this line.

NOTE 4: An "All lines" line identifier indicates that the current exchange or information is relating to all the lines of the DECT system.

NOTE 5: A "Line type information" line identifier indicates that the following identifier value contains further information on the type of the line which is identified through the line identifier of subtype "Line identifier for external call" present in the same <<CALL-INFORMATION>> information element.

If one line identifier subtype is equal to "All lines" in the IE, the corresponding identifier value shall not be present in the IE.

Call identifier subtype (octet 3a):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	Call identifier
	0 0 0 0 0 0 0 1	Updated call identifier
	All other values	reserved.

Call status subtype (octet 3a):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 1	Call status
	0 0 0 0 0 0 1 0	Call status reason
	All other values	reserved.

Service identifier subtype (octet 3a):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 0	SMS service identifier (see note 1)
	All other values	reserved.

NOTE 5a: Subtype '00'H is used to specify the SMS service concerned by the notification. See TS 102 527-5 [78], clauses 7.4.1.6 and 7.4.35.4.2.1 (octet 4 of 'SMS service id' field).

Identifier value (from octet 4):

- If the identifier type is "Line identifier", and the line identifier subtype is "Line identifier for external call", the identifier value indicates the "number" of the line used for incoming or outgoing external calls in the DECT system when the "Line identification" feature is supported by the system. This shall not apply to the special identifier value "None" as explained below:
 - The special value '7F'H (called "None") shall be used to indicate that the line id for the external call is not yet known (FP managed line selection). See example 3 for the corresponding coding.
- If the identifier type is "Line identifier", and the line identifier subtype is "Line type information", the identifier value contains further information on the type of the line identified through the line identifier of subtype "Line identifier for external call" present in the same <<CALL-INFORMATION>> information element.

NOTE 6: The line identifier is present when the "Line identification" feature is implemented, in messages that support the <<CALL-INFORMATION>> information element.

- If the identifier type is "Call identifier" and the call identifier subtype is "Call identifier", the identifier value indicates the "number" of the current call (incoming or outgoing, external or internal), or of another call (depending on the context, see note 9), when the "Call identification" feature is supported by the system. Call identifiers are system-wide, and FP-defined (they are neither PP specific, nor line specific).

NOTE 7: The call identifier is present when the "Call identification" feature is implemented, in messages that support the <<CALL-INFORMATION>> information element.

NOTE 8: Bit 8 of any identifier value octet set to 0 indicates that there is an additional identifier value octet after the current one; bit 8 of any identifier value octet set to 1 indicates that the current octet is the last one.

NOTE 9: The call identifier may not be that of the current call. Following is a non-limitating list of examples: the call identifier specified within a call waiting indication/acceptation/rejection is that of the waiting call, not of the current call; the call identifier specified within a call toggle is that of the targeted call, not of the current call.

- If the identifier type is "Call identifier", and the call identifier subtype is "Updated call identifier", the identifier value indicates a new value for the call identified within the same <<CALL INFORMATION>> information element using call identifier subtype "Call identifier".

NOTE 10: As a consequence, a call identifier with subtype "Updated call identifier" can never be conveyed alone in a <<CALL-IDENTIFICATION>> information element.

Identifier value (from octet 4) for line identifier subtype "Line type information":

Bit:	8	7	6	5	4	3	2	1	Octet:
	0/1						SCT	NDT	4
	0/1	...							
	1								

Figure 98g: Identifier value for the line identifier subtype "Line type information"

"Network delay type" value (NDT, bit 1 of octet 4):

Bits	1	Meaning
	0	connected to a network with low delay (e.g. PSTN/ISDN)
	1	connected to a network with significant delay (e.g. VoIP)

NOTE 11: The "Network delay type" flag indicates the delay type of the network connected to the line. Either the line is connected to a network with low delay (e.g. PSTN/ISDN) or with significant delay (e.g. VoIP). The "Network delay type" flag is only sent from the FP to the PP.

"Second call type" value (SCT, bit 2 of octet 4):

Bits	2	Meaning
	0	Second calls are handled with "common parallel call procedures" (e.g. VoIP lines)
	1	Second calls are handled with in-band signalling (e.g. PSTN lines)

NOTE 12: The "Second call type" flag indicates whether on this line second calls are handled with the "common parallel call procedures" or with "in-band" signalling (see TS 102 527-3 [75], clause 7.4.3.10 for more details). Although a PSTN line is usually an "in-band second call" line, an enhanced FP may choose to handle a given PSTN line with the "common parallel call procedures" if it is possible (e.g. by using a tone detector). The "Second call type" flag is only sent from the FP to the PP.

Identifier value (from octet 4, bit 3) for line identifier subtype = "Line type information":

Bits	7 6 5 4 3	Meaning
		All values reserved

Identifier value (from octet 4) for call status subtype = "Call status":

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	CS idle
	0 0 0 0 0 0 1	CS call setup
	0 0 0 0 0 1 0	CS call setup ack
	0 0 0 0 0 1 1	CS call proc
	0 0 0 0 1 0 0	CS call alerting
	0 0 0 0 1 0 1	CS call connect (note 13)
	0 0 0 0 1 1 0	CS call disconnecting
	0 0 0 1 0 0 1	CS call hold
	0 0 0 1 0 1 0	CS call intercepted
	0 0 0 1 0 1 1	CS conference connect
	0 0 0 1 1 0 0	CS call under transfer

0 0 0 1 1 0 1	CS call remote hold (note 14)
0 0 0 1 1 1 0	CS call remote connect (note 14)
0 0 0 1 1 1 1	CS screening setup (note 15)
0 0 1 0 0 0 0	CS screening connect (note 15)
All other values reserved	

NOTE 13: 'CS call connect' call status indicates end to end connection of the call. However, the connection may be active from local PP to remote system only (the call may be either active or on hold on remote PP side). This also applies for internal call (but in that case the local system is equal to the remote system).

NOTE 14: See TS 102 527-3 [75] 'CS call remote hold' and 'CS call remote connect' call statuses indicate to the local PP the call status of the call on remote party side. It is always available in case of internal call, but availability in case of external call depends on the type of line used.

NOTE 15: See TS 102 527-5 [78] 'CS screening setup' and 'CS screening connect' call statuses indicate external incoming call presentation of a call in call screening mode. See clause 7.4.36 (Screening feature) of TS 102 527-5 [78].

Identifier value (from octet 4) for call status subtype = "Call status reason":

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	system busy
	0 0 0 0 0 0 1	line in use
	0 0 0 0 0 1 0	control code not supported
	0 0 0 0 0 1 1	control code failed
	0 0 1 0 0 0 0	user busy
	0 0 1 0 0 0 1	number not available
All other values reserved		

Identifier value (from octet 4) for service identifier subtype = "SMS service identifier":

SMS service id value as described in TS 102 527-5 [78], clause 7.4.35.4.2.1 (octet 4 of 'SMS service id' field).

Examples:

Taking into account octets 3, 3a and 4, the following examples apply:

EXAMPLE 1: call-id=2 is coded as follows: '01'H, '00'H, '82'H;

EXAMPLE 2: line-id=2 for external call is coded as follows: '00'H, '00'H, '82'H;

EXAMPLE 3: line-id=127 ("None") for external call is coded as follows: '00'H, '00'H, 'FF'H;

EXAMPLE 4: relating-to line-id=2 is coded as follows: '00'H, '03'H, '82'H;

EXAMPLE 5: "all lines" is coded as follows: '00'H, '04'H.

7.7.57 List change details

The purpose of the << LIST-CHANGE-DETAILS >> information element is to convey detailed change information to the PP for caching purpose. It shall be sent together with an IE <<events notification>> containing a list change indication in the same {FACILITY} (or other) message.

NOTE 1: The corresponding list identifier is indicated in the accompanying list change indication.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< List change details >> (0x74)							1
		Length of Contents (L)							2
	0/1	Originating PP (if common)							3
		Length of added or modified entry ids (L1)							4
	0/1	Entry id (added or modified)							5
		...							
	0/1	Entry id (added or modified)							
		Length of deleted entry ids (L2)							6
	0/1	Entry id (deleted)							7
	0/1	...							
	0/1	Entry id (deleted)							

Figure 98h: LIST CHANGE DETAILS information element

Originating PP (octet 3):

This field contains the change origin device identifier. It shall only be non-zero if all changes specified in the IE originate from one single PP.

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0	Change origin is FP OR Change origin is not common to all entry ids specified.
	x x x x x x	terminal id number (≥ 1) of originating PP (if smaller than 127). See note 2.
		All other values reserved.

NOTE 2: It is extensible to the next octet if the value exceeds 127.

Case of a single originating PP. In case all changes since the previous notification were made by a single PP through a LiA session, this PP terminal id number shall be specified in the 'Originating PP' subfield.

NOTE 3: This allows the change originating PP maintaining a local copy of the list to avoid accessing the list for requesting the corresponding entries, as it already knows their contents.

Case of several originating PPs. In case changes made since the previous notification originated from several PPs, or if at least one of the changes was made by the FP, the 'Originating PP' subfield shall be set to '0'. In case a PP receives a notification with an 'Originating PP' subfield set to '0', it should access the list for the purpose of updating its local copy of the list (if any).

NOTE 4: This means there is no optimization in this case. All PPs are invited to consult the list for all changes, including their own changes (if any).

Entry ids for added and/or modified entries (octets 4, 5, etc.):

A <<list change details>> IE shall contain a first series of entry ids, for which an addition and/or modification took place in the list

NOTE 5: Addition and modification of an entry are not distinguished because the consequence is the same for the PP: it should access the list in order to know the entry contents and copy it locally if it supports caching for that list (whether it already held this entry id locally or not).

The length of added or modified entry ids (L1) shall always be present, even if there is no such entry ids in the IE (i.e. if its value is '0')

Entry ids for deleted entries (octets 6, 7, etc.):

A <<list change details>> IE shall contain a second series of entry ids, which were deleted in the list

The length of deleted entry ids (L2) shall always be present, even if there is no such entry ids in the IE (i.e. if its value is '0')

Merging. The same entry id shall not be present more than once in the <<LIST CHANGE DETAILS>> IE, as all changes concerning a single entry shall be merged in the notification.

EXAMPLE: An addition/modification followed by a deletion are notified as a deletion only. See TS 102 527-5 [78] for detailed merging rules.

Overflow. The FP should put as many entry ids in the IE as possible (e.g. a {FACILITY} message (if used) has a length up to 63 bytes); If too many entries have been modified, the FP shall either use several list change indications, or use a single list change indication with NO associated <<List change details>> IE. For a PP caching the list, this indicates a need for a full resynchronization of the list. See TS 102 527-5 [78] for more details.

Entry id coding. The entry id value shall be in the interval [1..16383], and shall be coded with the usual DECT extension mechanism, on one or two octets:

- For entry ids in the range [1..127], the entry id shall be coded on one octet, with bit 8 set to 1B (indicating that there is no further octet), followed by the 7 bits of the entry id value.
- For entry ids in the range [128..16383], the entry id shall be coded on two octets:
 - In the first octet: bit 8 set to 0B, followed by the 7 most significant bits of entry id
 - In the second octet: bit 8 set to 1B, followed by the 7 least significant bits of entry id

7.7.58 ULE MAC Configuration Info

The purpose of the <<ULE-MAC-CONFIGURATION-INFO>> element is to transmit MAC configuration parameters, generally (but not necessarily) in FT => PT direction, for different DECT applications. The detailed coding shall be defined in the applicable Application Profile.

Bit:	8	7	6	5	4	3	2	1	Octet:
	<< ULE-MAC-CONFIGURATION-INFO >>								1
	Length of Contents (L)								2
	1	Coding standard							3
	MAC CONFIGURATION INFORMATION								...
									L+2

Figure 98i: LIST CHANGE DETAILS information element

Reserved bit (octet 3):

Bits	8	Meaning
	1	shall be set to '1'

The value '0' is reserved for further expansion and shall not be used

Coding standard (octet 3):

Bits	7 6	Meaning
	0 0	DECT ULE TS part 1 (TS 102 939-1 [79])
	all others	reserved

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 B_S logical channel). Refer to EN 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
full format	5 octets
extended format	5 octets, 10 octets, 15 octets, 20 octets, 25 octets 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 EN 300 175-3 [3].

8.2 LCE request paging messages

Request paging messages shall use one of the following formats:

- a) short format;
- b) full format with TPUI;
- c) full format with IPUI.

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

Bit:	8	7	6	5	4	3	2	1	Octet:
	X	X	X	X	W	LCE Header			1
	Information								2
	Information (continued)								3

Figure 99: 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 is a conventional value or three bits used to identify the application or service reason of the paging message. The use and meanings of the LCE paging code are described in clause 8.2.4.1.

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.

Table 80: format for address field in short paging messages

W	LCE Header	Octet 2 bits 5 to 8	Octet 2 bits 1 to 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	X	X	X	X	W	LCE Header			1
	ring pattern				Address/Group Mask				2
	Address/Group Mask (continued)								3

Figure 100: Short format message for collective or group ringing request

The meaning of the special address elements used in collective or group ringing request is described in clause 8.2.4.4.

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

Figure 101: 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 EN 300 175-6 [6] for details of IPUI and TPUI.

For the address fields the order of bit values shall progressively decrease as the octet number increases.

Response to a short paging format regarding setup and slot type

When receiving a short paging, the PP shall use the setup method and the slot type as indicated in clause 8.2.4.3, table 80b (default behaviour table).

8.2.2 Full format message

The full format message shall contain 36 bits of information, placed into a 5 octet frame. There are two structures for the full 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
	Info Field 1 (slot type)				TPUI Address				2
	TPUI Address (cont)								3
	TPUI Address (cont)								4
	Info Field 2 (set up info)				Info Field 3 (Reserved or LCN)				5

Figure 102: Full format, 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

Figure 103: Full format, IPUI address structure

Address elements (TPUI or IPUI address fields):

The address structure depends on the value of "W" bit and LCE header.

a) LCE code different of 001, W = "1": TPUI address element:

- Message structure as defined in figure 102.
- TPUI address = complete TPUI (20 bits).
- Info field 1, Info field 2 and Info field 3, as described in clause 8.2.4.2.

For the TPUI address field, the order of bit values shall progressively decrease as the octet number increases.

b) LCE code different of 001, W = "0": IPUI address element:

- Message structure as defined in figure 103.
- class = IPUI Class.
- IPUI address = lowest 28 bits of IPUI.
- There are no fields info 1, info 2 and info 3.

For the IPUI address field, the order of bit values shall progressively decrease as the octet number increases.

c) LCE code = 001: (unknown and collective ringing):

No format with IPUI is allowed, and format with TPUI (message structure as defined in figure 102) is used with the following modifications:

- The W bit could set either to "0" or "1" (keeping in both cases the format of figure 102).
- The address field (octet 2, bits 1 to 4, octet 3 and octet 4) shall carry the information described in table 80a.
- Info field 1, Info field 2 and Info field 3, as described in clause 8.2.4.2.

Table 80a: special format for address field in full paging messages when LCE = 001

W	LCE Header	Octet 2 bits 1 to 4	Octet 3	Octet 4
1	001	Ring pattern	group mask = sequence of "1s" or/and "0s"	
0	001	Ring pattern	lowest 16 bits of the assigned connectionless group TPUI or CBI	

See description of the ring pattern, group mask and assigned connectionless group TPUI or CBI in clause 8.2.4.4.

Info fields 1, 2 and 3:

The fields info 1, info 2, and info 3 are used in the general TPUI structure (figure 102) and are described in clause 8.2.4.2.

Response to a full paging format regarding setup and slot type:

When receiving a full paging message with TPUI structure and a value different from zero (\neq "0000"B) in the info field 2 (setup info), the PP shall use the setup method and the slot type indicated in the paging message.

When receiving a full paging message with IPUI structure, or a full paging with TPUI structure and the default ("0000"B) value in info field 2, the PP shall use the setup method and the slot type as indicated in clause 8.2.4.3, table 80b (default behaviour table).

8.2.3 Long format message

Long paging format is defined as the format of paging messages longer than 36 bits.

The long format paging is for further study.

8.2.4 Message elements

8.2.4.1 LCE paging header

LCE header coding

The LCE header is a conventional value or three bits used to identify the application or service that should be initiated as result of the paging message.

Although there is no need to define at this stage the MAC service to be used (this may be done later, during the bearer setup), by historic reasons some of the LCE codes have the name and are associated to specific MAC services. However, this is just a convention.

The LCE headers have the nature of "well-known" codes. The LCE code to be used by any DECT application should be defined in the Application Profile specification. The definition should take into account the possible cases of implementation of multiple DECT profiles in the same equipment.

For applications not covered by any application profile, the basic rules described in this clause should be used.

The list of current "well-known" uses of LCE paging codes is included in clause L.1.

LCE headers codes

Bits	3 2 1	Name/recommended application
	0 0 0	no U-plane
	0 0 1	Unknown (MAC service type) and Ringing
	0 1 0	Escape
	0 1 1	General purpose code (former unknown)
	1 0 0	General code for voice service (former I _{N_min_delay})
	1 0 1	Auxiliary code (former I _{N_normal_delay})
	1 1 0	DPRS initial set-up code (former IP_error_detect)
	1 1 1	DPRS resume code (former IP_error_correct)

Description of the LCE header codes

The coding "000" = "**no U-plane**" indicates that no U-plane service is required. This code should be used to indicate services that only require a C-plane (e.g. MM procedures).

The code is "011" = "**General purpose/unknown**" is the general use code. This code may be used with any MAC service (including I_p services). This code forces the bearer setup process to negotiate the MAC service type (message "Attributes"), unless the MAC service is clear by the application or context. Refer to EN 300 175-3 [3], clause 10.2.4.3 for more details of service modification.

NOTE 1: 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).

NOTE 2: The "011" = "unknown" is suggested as the default choice for new applications not covered by an application profile, or by other definition provided in this clause.

Code "001" = "Unknown (MAC service type) and Ringing"

If the coding "Unknown (MAC service type) and Ringing" is used this shall be interpreted as request for ringing according to Collective/Group ringing procedure clause 14.4 and the PP should request any suitable MAC service when it attempts to establish a link upon the outgoing call.

Code "100" = **Voice Service code (former I_{N_min_delay})** is the traditional code used in GAP [51] voice devices. When used as short paging, this code shall cause a Basic connection M_T bearer setup with full slot and MAC service I_{N_min_delay}. Compared to "010" this code does not force an immediate Attributes negotiation (however, it is still possible). This code is the standard code for Wideband voice (DECT New Generation [73] and [75]), but full paging format is mandatory if the slot is different of a full slot.

Code "101" = **Auxiliary code (former I_{N_normal_delay})** may be used by applications profiles requiring differentiation with the 100. The default response to a short paging is similar to the "100" with the difference that the MAC service is I_{N_min_delay}.

Codes "110" and "111" are reserved for data applications. Code "110" is used in **DPRS initial call setup** and code "111" in **DPRS resume** process. The use of the codes in DPRS is described in clause 14.5.

The codes "110" and "111" can be also used by other data applications.

- If the applications never coexist with DPRS, the codes could be used without any special remark.
- The traditional practice was using code "110" if MAC service was going to be I_{p_error_detect} and "111" if MAC service was I_{p_error_correct}.

The advisable practice for new data non-DPRS applications is:

- use only code "110", nevertheless of the MAC service, and to avoid the use of code "111";
- use short page only if B-field setup is used. Otherwise use full paging with the setup type coded in Field 2;
- take into account the possibility of coexistence with DPRS applications in the same equipment.

8.2.4.2 Info fields (Full format)

This clause applies to full paging format with TPUI address structure (bit W = "1").

The meaning of the three info fields is the following:

Field 1: Slot type (octet 2):

Indicates the type of slot that the PT shall use in the setup attempt.

Bits	8 7 6 5	Meaning
	0 0 0 0	Half slot; j = 80
	0 0 0 1	Long slot; j = 640
	0 0 1 0	Long slot; j = 672
	0 1 0 0	Full slot
	0 1 0 1	Double slot
	All other values reserved	

For backcompatibility reasons, if bit 8 of slot type = 1, it shall be understood as slot type="full slot". However, this coding should be avoided in new developments.

Field 2: Setup info (octet 5):

Indicates the type of setup procedure that the PT shall use.

Bits	8 7 6 5	Meaning
	0 0 0 0	No setup info (see clause 8.2.4.3 for indication about the PT behaviour in this case)
	0 0 0 1	Use M _T signalling Basic Connection, Attributes_T negotiation optional
	0 0 1 0	Use M _T signalling Basic Connection, Attributes_T negotiation mandatory
	0 0 1 1	Use M _T signalling Advanced Connection, Attributes_T negotiation mandatory
	0 1 0 0	Use B-field signalling. (no info about C _F support)
	0 1 0 1	Use B-field signalling, and may use C _F for NWK layer set up
	All other values reserved	

Info Field 3 (octet 5):

For LCE = 111 (Data/DPRS Resume code)

This field carries the LCN of the DPRS connection to be resumed.

Field 3 (octet 5): Connection identity if LCE = 111

Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	1 n n n	LCE = n n n

For any other LCE

The field is reserved and can be used by application profiles as an additional discriminator. Otherwise it shall be set to "0000".

Field 3 (octet 5): Additional discriminator if LCE ≠ 111

Bits	4 3 2 1	Meaning
	0 0 0 0	Default value
All other values		Reserved for additional discriminators (defined in an application profile)

8.2.4.3 Default setup behaviour

This clause applies to short paging, full paging with IPUI and full paging with TPUI.

In the cases where there is no information about the setup method in the paging message, the PT shall use the default behaviour as described in this clause.

The lack of setup information happens in short paging and full paging with IPUI messages (in all cases), and in full paging with TPUI if the default code "0000"B is transmitted in info field 2.

In such cases, the PT access behaviour shall be as follows:

NOTE 1: The default behaviour depends on the value of the LCE code.

NOTE 2: This default behaviour applies unless the applicable application profile provides different instructions.

Table 80b: default setup behaviour

LCE codes	Type of paging and slot type field (if full paging with TPUI)	Default behaviour regarding setup
000	Short paging, Full paging with IPUI or full paging with TPUI and full slot	M _T basic connection setup on full slot, PP does not initiate attributes negotiation. MAC service = no MAC service
000	Full paging with TPUI, any other slot	M _T advanced connection setup on the requested slot, PP does not initiate attributes negotiation. MAC service = no MAC service
001	Short paging special structure (figure 100 and table 80) or Full paging special structure (figure 102 modified according to table 80a) and full slot	M _T basic connection setup on full slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
001	Full paging special structure (figure 102 modified according to table 80a), any other slot	M _T advanced connection setup on requested slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
011, 010	Short paging Full paging with IPUI or full paging with TPUI and full slot	M _T basic connection setup on full slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
011, 010	Full paging with TPUI, any other slot	M _T advanced connection setup on requested slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
100	Short paging Full paging with IPUI or full paging with TPUI and full slot	M _T basic connection setup on full slot, PP does not initiate attributes negotiation. Initial MAC service = I _{N_min_delay}
100	Full paging with TPUI, any other slot	M _T advanced connection setup on requested slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
101	Short paging Full paging with IPUI or full paging with TPUI and full slot	M _T advanced connection setup on full slot, PP does not initiate attributes negotiation. MAC service = I _{N_normal_delay}
101	Full paging with TPUI, any other slot	M _T advanced connection setup on requested slot, PP does initiate attributes negotiation. MAC service = as negotiated in attributes
110	Short paging or full paging with IPUI	B-field advanced setup on longest supported slot (see clause 14.5.1.1). MAC service = as negotiated in the setup
111	Short paging or full paging with IPUI	B-field advanced setup on the same slot used by the connection before suspension (see clause 14.5.2.1). MAC service = as negotiated in the setup (it should be the same service used by the connection before suspension)
110, 111	Full paging with TPUI, any slot type	B-field advanced setup on the requested slot type. MAC service = as negotiated in the setup (if resume (111), it should be the same service used by the connection before suspension)

8.2.4.4 Address elements in collective or group ringing

The following special address elements are used when LCE code is "001" (Collective/group Ringing).

Ring pattern

Bits	8 7 6 5	Meaning
	0 0 0 0	alerting on - pattern 0 (see note 1)
	0 0 0 1	alerting on - pattern 1 (see note 1)
	0 0 1 0	alerting on - pattern 2 (see note 1)
	0 0 1 1	alerting on - pattern 3 (see note 1)
	0 1 0 0	alerting on - pattern 4 (see note 1)
	0 1 0 1	alerting on - pattern 5 (see note 1)
	0 1 1 0	alerting on - pattern 6 (see note 1)
	0 1 1 1	alerting on - pattern 7 (see note 1)
	1 0 0 0	alerting on - continuous
	1 0 1 0	incoming call released by the FP (see note 2)
	1 0 1 1	incoming call has been answered (see note 2)
	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: The use of alerting patterns is FT dependent; the resulting sound is PT dependent.

NOTE 2: The value does not represent a ring pattern but indicates stop of ringing.

Address/Group Mask (short paging)

When used for group mask ringing this field shall include a sequence of 12 bits as group mask, see clause 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 EN 300 175-6 [6] clause 6.3.1.

Address/Group Mask (full paging)

When used for group mask ringing this field shall include a sequence of 16 bits as group mask, see clause 14.4.

When used for group ringing this field shall include the lowest 16 bits of the assigned connectionless group TPUI.

When used for Collective ringing this field shall include the last 16 bits of the CBI, see EN 300 175-6 [6] clause 6.3.1.

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 carry information equivalent to that contained in the <<ALPHANUMERIC>> information element (see clause 7.7.3) or other specific information. {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 clause 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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	X	X	X	X	A = 1	CLMS Header			1
	Address								2
	Address (cont)								3
	Protocol Discriminator								4
	Length Indicator/Data								5

Figure 104: CLMS-FIXED message structure: address section

NOTE 2: The content of octets 5 is determined by the header coding.

Bit:	8	7	6	5	4	3	2	1	Octet:
	X	X	X	X	A = 0	CLMS Header			1
	Data/Fill								2
	Data/Fill (cont)								3
	Data/Fill (cont)								4
	Data/Fill (cont)								5

Figure 105: 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 three types of message to be defined, a DECT standard message, or, a general alphanumeric message, or, a general bit stream message. The basic structure of the first two 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
	0 1 1	One section:	Bit stream	Data
	1 0 0	Multi-section:	Bit stream	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: The CLMS service requires the use of assigned TPUIs. Refer to EN 300 175-6 [6].

Protocol discriminator (octet 4 of address section):

Coding as for octet 3 of <<Bit stream>>

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

Figure 106: Format of Protocol Discriminator (PD)**Bits 7 6 5 4 3 2 1 Meaning**

0 0 0 0 0 0 1 DECT Information elements coding

0 0 1 x x x x Distributed Communications

All other values reserved. The Distributed Communications in fact occupies more than one code.

When the value "DECT Information Element Coding" is used the data field shall contain only DECT information elements as coded in the present document. Multiple information elements may be included.

When the value "Distributed Communications" is used the coding of the octets is defined in annex I.

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.

Bit:	8	7	6	5	4	3	2	1	Octet:
	L8	L7	L6	L5	L4	L3	L2	L1	5

Figure 107: Format of Length Indicator (LI)

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):

Bit:	8	7	6	5	4	3	2	1	Octet:
	Data or Fill				Data or Fill				*

Figure 108: 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 positions 5, 6, 7 and 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 81: Messages using 4-bit characters

Message Type	1st character	2nd character	Other characters
Tone alert	0	0 to 9	not allowed
Other messages are for further standardization			

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 is not defined in the present document.

8.3.3.3 Messages using 8-bit characters

Table 82: Messages using 8-bit characters

Message Type	1st character	2nd character	Other characters
8-bit messages are for further standardization			

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 109 illustrates the states and transitions on the PT side.

Figure 110 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. Annex B is included as a shortform summary. In the event of any discrepancy, the main text (the following clauses) takes 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.



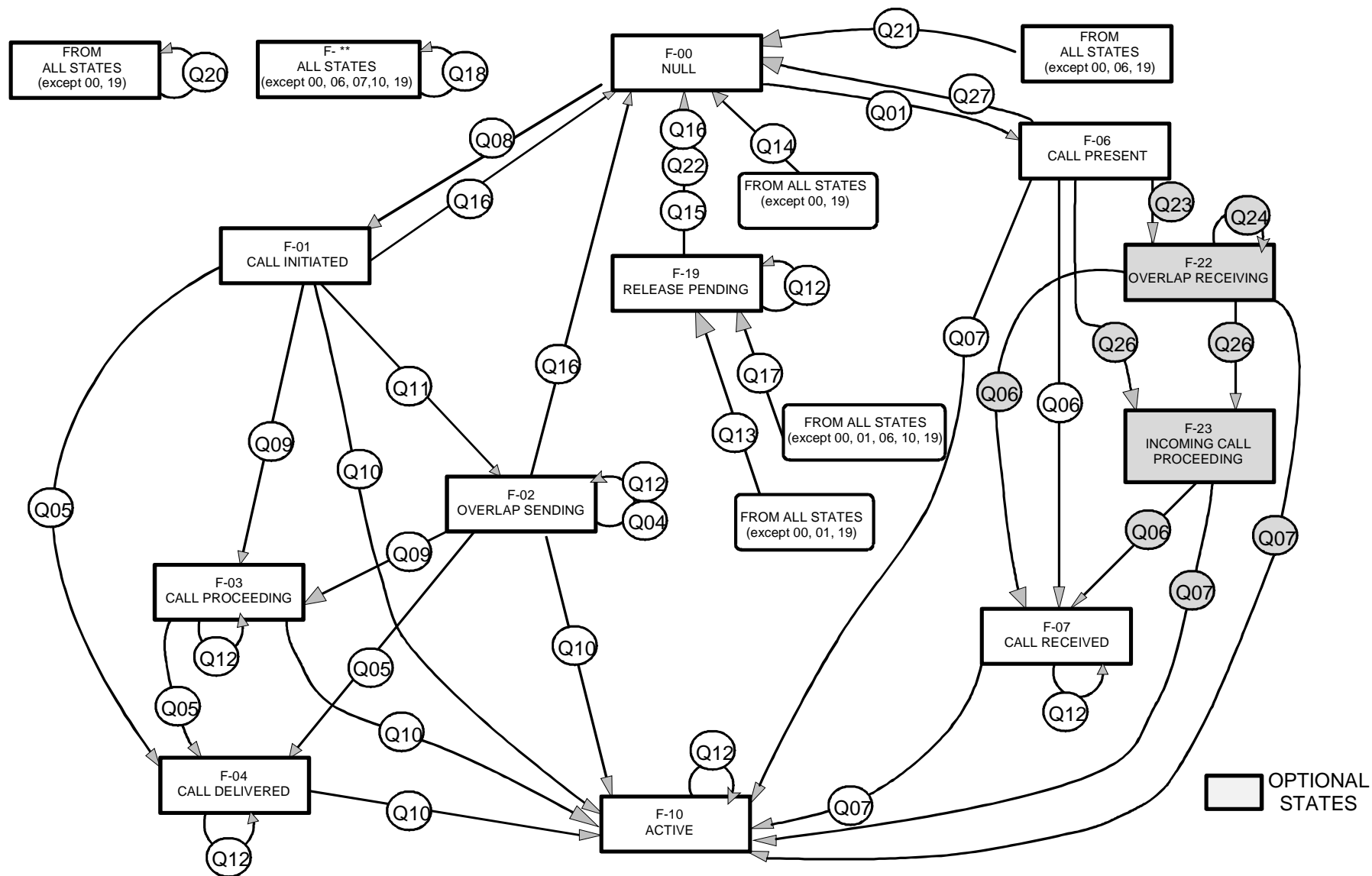


Figure 110: Call control states in the FT

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 setup 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 setup 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 setup 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 setup has been started. The FT has received a setup 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 setup 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 setup 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 setup 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

The P-CC entity starts the call establishment by sending a {CC-SETUP} message to its peer entity at the FT side (F-CC). This message is submitted to the LCE in the PT, and the P-CC enters "CALL INITIATED" state and starts timer P<CC.03>.

The {CC-SETUP} message shall carry a portable part identity plus a full fixed part identity (the relevant ARI) according to the identity rules given in EN 300 175-6 [6]. The portable part identity used is by default the IPUI, however, the assigned individual TPUI may be used if the FT has indicated that this is allowed. This indication is provided by the <<USE-TPUI>> information element in the {LOCATE-ACCEPT} message.

The {CC-SETUP} message shall contain the <<BASIC-SERVICE>> information element. If this element indicates "default setup attributes" 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 setup 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 FT and the interworking unit at the FT side (F-IWU).

NOTE 1: The setup message may contain a list of attribute elements when using prioritized list negotiation. Refer to clause 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 the present document. They should be defined in the relevant profiles specifications based on DECT CI.

Emergency call establishment is described in detail in clause 9.8.

NOTE 3: 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 clauses 9.3.1.3 to 9.3.1.9.

Call reject:

If the F-CC cannot meet any of the setup 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 setup by sending a {CC-RELEASE-COM} message, and shall enter the "NULL" state.

The MNCC_REJECT-req may include a release reason (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Call reject of an outgoing call at call establishment is a special case of abnormal release (see clause 9.5.2.2) performed by the FT. Upon receipt of the {CC-RELEASE-COM} message, the PT shall also act according to clause 9.5.2.2.

NOTE 2: Call rejection may also occur as part of exchanged attribute service negotiation. Refer to clause 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 clause 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. The <<CONNECTION-IDENTITY>> element may be used as well to allocate a number of MAC connection identifiers for connections that are associated with one Broadband data link (see clause 9.4 as well). 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 setup is accepted (e.g. if the PT is attempting to setup 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 EN 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 setup, 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.

After the lower resources are identified the NWK layers at both sides should inform the DLC for the result sending a DL_SERVICE_MOD primitive.

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 clause 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 setup 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: The present document 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 setup 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 setup 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.

Call reject of an outgoing call at overlap sending is a special case of abnormal release (see clause 9.5.2.2) performed by the FT. Upon receipt of the {CC-RELEASE-COM} message, the PT shall also act according to clause 9.5.2.2.

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 clause 9.5.1. The {CC-RELEASE} message should contain the reason "TIMER-EXPIRY".

9.3.1.6 Call proceeding

Upon receipt of the MNCC_CALL_PROC-req primitive, the F-CC shall stop timer F<CC.01> (if running), 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 clause 10.6.2.

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_ALERT-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 clause 9.5.1.

Equally, if timer F<CC.04> expires, the F-CC shall immediately release the call using the procedures described in clause 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 portable part identity plus a full fixed part identity (the relevant ARI) according to the identity rules given in EN 300 175-6 [6]. The portable part identity used is by default the IPUI, however, the assigned individual TPUI may be used if the PT used the assigned individual TPUI in the {LCE-PAGE-RESPONSE} message.

For group calls the {CC-SETUP} message shall carry either one portable part identity (IPUI or individual TPUI according to the same rules as for individual calls) 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. If this element indicates "default service attributes" 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 setup 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.

The following call classes are not applicable for incoming call: emergency call, external handover, LiA service call and service call.

NOTE: The setup message may contain a list of attribute elements when using prioritized list negotiation. Refer to clause 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 fulfil 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 examines 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 accepts 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 clauses 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 setup 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.

Call reject of an incoming call at call establishment is a special case of abnormal release (see clause 9.5.2.2) performed by the PT. Upon receipt of the {CC-RELEASE-COM} message, the FT shall also act according to clause 9.5.2.2.

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. The <<CONNECTION-IDENTITY>> element may be used as well to allocate a number of MAC connection identifiers for connections that are associated with one Broadband data link (see clause 9.4 as well). 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.

After the lower resources are identified the NWK layers at both sides should inform the DLC for the result sending a DL_SERVICE_MOD primitive.

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 clause 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 setup 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 clause 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 the present document. 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 clause 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.

If the call requires usage of a Broadband data link and the <<CONNECTION-IDENTITY>> element to allocate a number of MAC connection identifiers for connections that are associated with this Broadband data link was not sent with the {CC-SETUP} it shall be sent here. As the call information procedure takes place when a first connection has already been established, the sending entity shall include the assigned to this connection LCN as <Connection identity 1> and shall allocate one or two additional LCNs to be used for one or two additional connections respectively depending on the service requirements for the Broadband link. The receiving site shall indicate the acceptance of the allocated connection identities by submitting the same <<CONNECTION-IDENTITY>> element in opposite direction.

Service change procedures during the call information phase are described in clause 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 clause 9.3.

NOTE 1: A MNCC_RELEASE-req primitive is an illegal response to a call setup. The following normal call release procedure is not followed when responding to a call setup. A FT in the "CALL INITIATED" or "OVERLAP SENDING" state responds as though rejecting the call setup and should follow the procedures defined in clauses 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 setup and should follow the procedures defined in clause 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 EN 300 403-1 [9] 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 clause 14.2.7.

9.5.2 Abnormal call release

9.5.2.1 Definitions

Sending side. Side (PT or FT) that triggers abnormal release by sending a {CC-RELEASE-COM} message.

Receiving side. Side (PT or FT) that receives the {CC-RELEASE-COM} message.

9.5.2.2 Abnormal release general description (PT or FT).

Abnormal release at sending side. Abnormal release is triggered at sending side by the rejection of the call either at CC level or at IWU level. If rejected at IWU level, a MNCC_REJECT-req primitive is used to inform the CC layer. In both cases, the receiving side is informed by the sending of a {CC-RELEASE-COM} message.

NOTE 1: In case of abnormal release, a {CC-RELEASE} message cannot be used, as the call has not yet been accepted.

NOTE 2: 'Call reject' described in clauses 9.3.1.2 (outgoing call) and 9.3.2.2 (incoming call) are a particular case with abnormal release performed at call establishment.

NOTE 3: 'Call reject' described in clauses 9.3.1.5 (outgoing call) is a particular case of abnormal release performed at OVERLAP SENDING.

NOTE 4: EN 300 444 [51] (GAP), clause 8.45.5.2 (Behaviour of PPs regarding legacy FPs) uses abnormal release possibly after {CC-CONNECT}.

The <<RELEASE-REASON>> IE of the {CC-RELEASE-COM} message contains the release reason originating from CC (and possibly forwarded from IWU level if IWU rejected the call).

More specifically, abnormal release may occur at sending side in the following cases:

- **Main case:** the sending side is in any state except for the NULL and RELEASE_PENDING states. In this case the {CC-RELEASE-COM} message is sent without prior receipt of a {CC-RELEASE} message.
- **Special case:** the sending side has sent or received a {CC-RELEASE} message and entered the RELEASE_PENDING state. Then the sending side receives from IWU an MNCC_REJECT-req primitive (e.g. the FT receives a "RELEASE" message from the local network) and sends a {CC-RELEASE-COM} to the other side.

NOTE 5: When release is pending, the IWU should issue the MNCC-REJECT-req primitive only in exceptional cases.

NOTE 6: If the receiving side sent the {CC-RELEASE} message, it already expects a {CC-RELEASE-COM} message in return, and is therefore only informed of abnormal release thanks to the <<RELEASE-REASON>> IE that should transmit the IWU level call rejection reason.

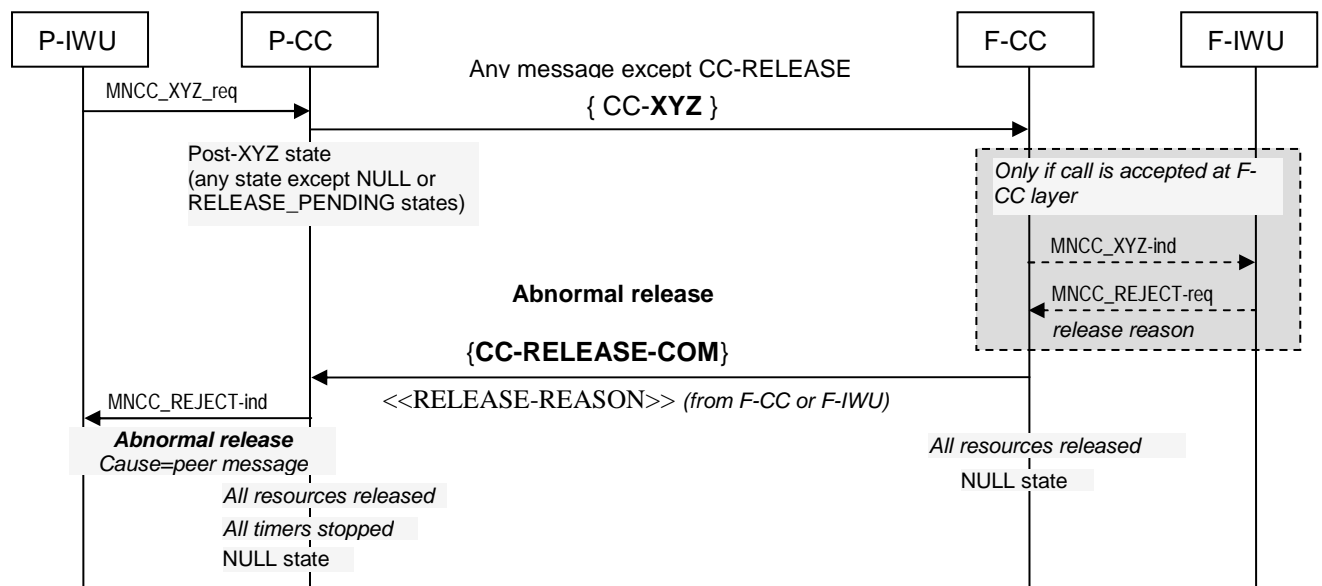


Figure 110A: Abnormal release (main case) when triggered by FT

At sending side, when the call is rejected at IWU level, and upon receipt of the MNCC_REJECT-req primitive, the CC entity shall:

- (special case only) if {CC-RELEASE} was sent by the sending side, stop timer <CC.02>.
- (all cases) send a {CC-RELEASE-COM} message, release all resources and enter the "NULL" state.

Abnormal release at receiving side. Abnormal release is indicated at receiving side 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" state).

NOTE 7: If the receiving side is in the RELEASE_PENDING state, only the *special case* of abnormal release can occur.

Upon receipt of the unexpected {CC-RELEASE-COM} message at receiving side 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.

LCE notification. Both sides shall report the completion of the release of the call to their respective LCEs by the use of an NLR notification (see clause 14.2.7). 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.

9.5.2.3 Abnormal release in case of call setup collisions

This clause applies to the PT and FT establishing simultaneously outgoing and incoming calls on the same link ({CC-SETUP} collision). The outgoing call is not limited to a voice call, but may be e.g. an LiA service call, or a DTAM call.

NOTE 1: Abnormal release in case of call setup collisions is a special case of the *main case* of abnormal call release described in clause 9.5.2.2.

The PT and FT shall both solve the conflict by initiating abnormal release (as described in clause 9.5.2.2, *main case*) of the call initiated by the opposite side.

In order to release the call initiated by the opposite side, the PT and FT shall use the correct transaction identifier in the sent {CC-RELEASE-COM}.

NOTE 2: A call is a special case of transaction as defined in clause 7.3. All CC messages exchanged during the call from PT to FT and FT to PT belong to the same transaction.

NOTE 3: A given CC transaction uses two transaction identifiers. All messages sent from the transaction initiating side (i.e. from the side sending the {CC-SETUP}) use transaction id (0, TV), while all messages sent from the opposite side use transaction id (1,TV), where TV is the common transaction value of all messages in the transaction.

NOTE 4: The transaction value could be used by two different CC transactions (initiated by PT and FT respectively).

More specifically:

PT requirements.

As soon as the PT detects a {CC-SETUP} collision, the PT shall start the CC setup crossing resolving timer P-<CC.06>. Within P-<CC.06> timeout:

- The PT shall perform abnormal release of the FT-initiated call (incoming call), by sending a {CC-RELEASE-COM}:
 - with transaction identifier (F, TV) = (1, TV1), where TV1 is the transaction value of the FT-initiated call;
 - using release reason 'Insufficient resources'.
- The PT shall immediately notify the LCE of the release by use of a 'No link required' (NLR) notification, using release reason 'partial release' (see clause 14.2.7.2).
- If the PT receives a {CC-RELEASE-COM} from FT releasing the outgoing call, it shall wait for the re-presentation of the incoming voice call from the FT, and not setup any new outgoing call:
 - if the incoming call is restarted by the FT, the PT shall stop timer P-<CC-06>.

After P-<CC.06> timer expiry, if the incoming call was not restarted by FT within timeout, the PP may restart the outgoing call.

FT requirements.

As soon as the FT detects a {CC-SETUP} collision:

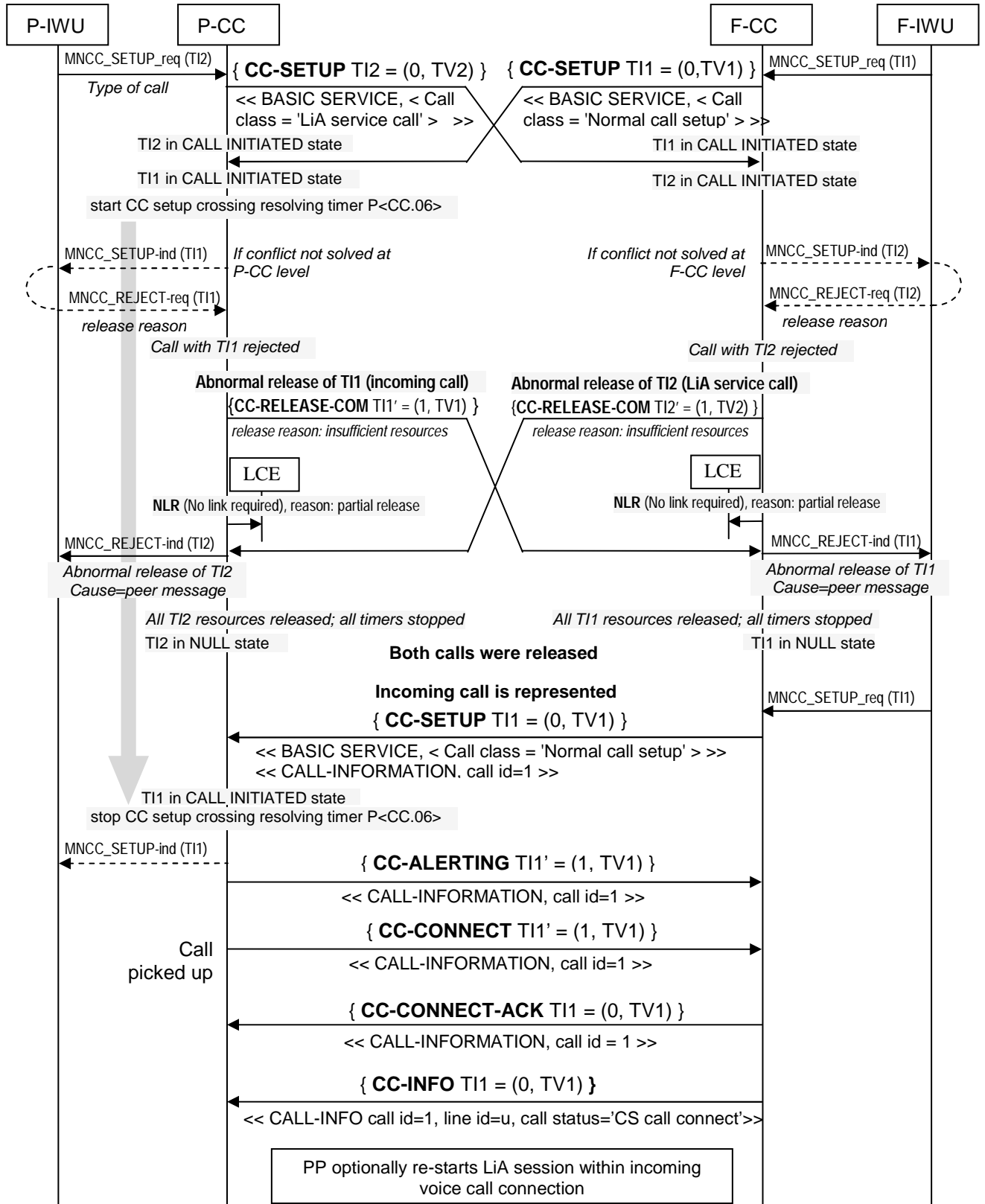
- The FT shall perform abnormal release of the PT-initiated call (outgoing call) by sending a {CC-RELEASE-COM}:
 - with transaction identifier (F, TV) = (1, TV2), where TV2 is the transaction value of the PT-initiated call;

- using release reason 'Insufficient resources'.
- The FT shall immediately notify the LCE of the release by use of a 'No link required' (NLR) notification, using release reason 'partial release' (see clause 14.2.7.2).
- If the FT receives a {CC-RELEASE-COM} releasing the incoming call, the FT may re-present the incoming call if it was not cancelled in the mean time. If the FT does re-present it, it shall do so immediately.

NOTE 5: If for any reason the link could not be maintained, the FT needs to re-establish it first.

NOTE 6: In order to avoid any new collision, the FT should not wait before re-presenting the incoming call, so that the incoming {CC-SETUP} arrives on PT side before P-<CC.06> timer expiry.

NOTE 7: TV1 and TV2 may be equal or different. When they are equal, only the flag F allows the receiving side to know which call the received {CC-RELEASE-COM} message belongs to (and therefore which call it releases).



NOTE: Crossing arrows indicate that messages are sent independently of each other (hence in any order).

Figure 110B: Crossing {CC-SETUP}'s of LiA service call and incoming call (example): abnormal release of both calls. FT represents incoming call

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 and/or IWU attributes.

A service change may be indicated by the receipt of a MNCC-MODIFY-req primitive. Upon receipt of this primitive, the initiating CC entity sends a {CC-SERVICE-CHANGE} message to request the change and starts timer <CC.06>. The {CC-SERVICE-CHANGE} 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 NWK layer suspend and resume.

Upon receipt of the {CC-SERVICE-CHANGE} message, the receiving CC entity shall attempt to meet the revised proposal. If the change is possible, and if no change of the IWU attributes is requested, 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 changes required may concern the IWU in which case upon receipt of the {CC-SERVICE-CHANGE} message, the accepting side shall issue a MNCC_MODIFY-ind primitive to the IWU. Acceptance of the change by the IWU is indicated by a MNCC_MODIFY-res primitive. Upon receipt of this response, the CC shall send a {CC-SERVICE-ACCEPT} if the change was accepted by the IWU or {CC-SERVICE-REJECT} message if the service change was rejected.

Either the CC or the IWU may reject the call. The CC examines the <<CALL-ATTRIBUTES>> and the <<CONNECTION-ATTRIBUTES>> elements, and the IWU examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the IWU after it has been accepted by the CC, i.e. changes not relevant to IWU are possible.

Upon receipt of the {CC-SERVICE-ACCEPT} or the {CC-SERVICE-REJECT} message the initiating CC entity shall stop timer <CC.06>. If timer <CC.06> expires before the receipt of a {CC-SERVICE-ACCEPT} or a {CC-SERVICE-REJECT} message, the initiating side shall consider the service change procedure as failed and issue a MNCC-MODIFY-cfm primitive indicating failure.

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 or change of the modulation scheme can only be initiated, at MAC layer, from one side. In these cases the master side is defined in EN 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-MODIFY-cfm primitive indicating success and the receiving entity shall issue a MNCC-MODIFY-ind primitive.

NOTE 3: Changes undertaken by the receiving CC without the knowledge of the IWU may result in the need for changes to the IWU attributes. After receiving the MNCC-MODIFY-ind the IWU may initiate a new service change procedure.

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-MODIFY-cfm primitive indicating failure.

After the lower resources are agreed the NWK layers at both sides should inform the DLC for the result sending a DL_SERVICE_MOD primitive.

9.6.2 Change of Bandwidth parameters (including changes in connection type)

NOTE: See clauses 7.7.11 and K.1 for better understanding of the meaning of the bandwidth parameters defined at NWK layer and their relationship to the bandwidth parameters at MAC layer.

The following procedures shall only be used for advanced connections.

Bandwidth changes shall be defined as changes that may be realized by modification of the NWK layer attributes that define the connection bandwidth properties. 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 clause 9.6.3.

Both the <<CONNECTION-ATTRIBUTES>> element and the <<CONNECTION-IDENTITY>> elements may be included to specify the new connection bandwidths and/or associations. If the <<CONNECTION-IDENTITY>> element is omitted, the bandwidth change shall be understood to apply to the connection which LCN is specified in octet 3 of <<CONNECTION-ATTRIBUTES>>.

The special case of change in the connection type (i.e. from symmetric to asymmetric or vice versa) shall be identified by using the target connection type in octet 3 of <<CONNECTION-ATTRIBUTES>>.

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 or remove allocated connection identities in the case of broadband data links. 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 clause 9.6.2.

9.6.4 NWK layer 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.

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. When the <<CONNECTION-IDENTITY>> is specified, then only those DLC-U plane elements specified will be suspended.

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 setup procedures defined in clauses 9.3.1.3 (PT initiated) or 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 clauses 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.

9.6.5 Modulation scheme change

A {CC-SERVICE-CHANGE} message may request change into the modulation scheme used at the Physical layer. This should only be used for packet services.

The <<SERVICE-CHANGE-INFO>> element shall indicate "Modulation scheme change" and the <<CONNECTION-ATTRIBUTES>> information element shall be included to identify the exact details of the new modulation to be used.

The modulation scheme change can be combined with Bandwidth modification, see clause 9.6.2.

9.7 NWK layer Packet mode procedures

9.7.1 General

The following procedures shall only be used for advanced connections.

DECT Packet mode calls are defined at NWK layer by the use of a DPRS code in octet 3 "NWK layer attributes" of the IE <<Call Attributes>>. The IE <<Connection Attributes>> is usually included in the same operation, which is usually a call setup, but may also be a CC_SERVICE_CHANGE. The call acquires the packet mode properties after completion of the setup or service change operation. There is also the option of defining permanent packet mode connections by configuration. See DPRS (EN 301 649 [72]) for further details.

Once the call is defined as packet mode, the ME (Management Entity) together with the MAC layer may dynamically suspend, resume or change the bandwidth of the call according to DPRS (EN 301 649 [72]) rules, and within the limits defined by the NWK layer attributes. The point of action of the DPRS suspend/resume mechanism is the MAC MBC (Multibearer control).

Packet mode calls are named "virtual calls". See EN 301 649 [72] for terminology.

The NWK layer sees a permanent connection during the whole duration of the DPRS call and no further NWK layer signalling activity is generally needed (with the exception of LCE activity in certain paging operations).

DECT DPRS calls are regular connection oriented services at NWK layer. The NWK layer is aware of the packet mode nature of the call and of the value of all parameters defined at NWK layer. However it is generally not aware of the packet activity and the dynamic state (suspended/resumed/allocated bandwidth) of the lower MAC and physical connection.

DLC link is also permanently connected during the whole duration of the virtual call, with the exception of Class 1 operation, that also releases DLC layer resources in each suspend operation.

In addition to the general DECT Packet mode procedures, that operate at MAC layer, there also exist the possibility of suspending and resuming a call at NWK layer by means of the NWK layer suspend/resume procedure defined in clause 9.7.4. The NWK layer suspend/resume procedure allows the releasing of all DLC and MAC layer, and part of the NWK layer resources allocated to the call. Nevertheless, NWK layer suspend/resume is not needed for DECT packet mode operation and not used in DPRS (EN 301 649 [72]).

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, the normal procedures defined in clause 9.3 shall apply. The <<IWU-ATTRIBUTES>> information element shall be set appropriately.

If packet switched access is required, the procedures defined in EN 301 649 (DPRS) [72] shall apply.

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, the normal procedures defined in clause 9.3 shall apply. The <<IWU-ATTRIBUTES>> information element shall be set appropriately.

If packet switched access is required, the procedures defined in EN 301 649 (DPRS) [72] shall apply.

9.7.4 NWK layer suspend and resume

NWK layer suspend/resume is a CC_SERVICE-CHANGE procedure that allows to suspend or resume a call at NWK layer by means of a NWK layer signalling operation. The NWK layer suspend releases all resources allocated to the call at DLC and MAC (TBC and MBC) layers.

NWK layer suspend/resume may be, in principle, applied to both packet mode (DPRS) and circuit mode calls. In packet mode calls, such procedure may be of some interest when there is no activity in the call during a long time. However it is not fundamental for the packet mode operation.

NOTE 1: The use of NWK layer suspend/resume in packet mode calls is for further study and is not contemplated in current revision of DPRS [72].

NWK layer suspend/resume may be used in circuit mode calls carrying occasional traffic and interworked to services supporting a similar feature at NWK interface. In such a case, the use of NWK layer suspend/resume allows to free DECT resources without interrupting the call.

The NWK layer suspend/resume may be seen as a kind of slow speed pseudo-packet mode procedure. However it has to be taken into account that the NWK layer suspend/resume is inherently slow and heavy in signalling operations (requires the exchange of NWK layer signalling at each suspend/resume operation), and is, in general, not seen as a valid approach to implement a true packet handling mechanism.

NOTE 2: To avoid confusion, the terminology "packet mode" is reserved in DECT for services using the MAC layer suspend resume procedures according to DPRS [72], and identified as a DPRS call at NWK layer by the IE <<CALL ATTRIBUTES>>.

9.7.4.1 General

A DECT call may optionally be suspended at NWK layer. The suspend procedure allows the service attributes to be reserved such that the call can be resumed more rapidly.

A NWK layer suspension releases all resources allocated to the call at DLC and MAC (TBC and MBC) layers.

The NWK layer 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 NWK layer 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 NWK layer suspend and resume

U-plane NWK layer suspend and resume shall use the service change procedures as described in clause 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.

9.8 Emergency call procedure

The procedure is initiated by a special manual interworking at the MMI of a DECT-Portable Part PP. This may be the dialling of "112" as known for GSM/UMTS handsets, pressing of a special "emergency call button", selecting a menu-item, dialling an emergency number, etc.

For emergency call normal outgoing call control procedures apply unless explicitly stated otherwise in this clause.

After recognition of this manual interworking the PP can decide whether:

- a) to setup a normal outgoing call and dial automatically a (preconfigured) emergency call number; or
- b) to initiate an emergency call.

Case a) is allowed only, when the handset is locked to a DECT-Fixed Part FP where it has access-rights to. Since normal outgoing call procedures as defined in clause 9.3.1 apply for this case, this clause only specifies case b) in further detail.

Case b) if the PP is not synchronized to a basestation which supports emergency calls, the PP starts to search for a DECT basestation which supports emergency calls. The PP recognizes this by reading the extended higher layer capabilities of the FP which are broadcasted by the RFPs (Radio Fixed Parts). Because it is most likely that a public DECT FP supports emergency calls, the PP tries first to synchronize to a public DECT-FP. It identifies the system being "public" using the identity ARC (Access Rights Class) which is broadcast more often than the "emergency call supported" message by the RFPs. If there is no public FP supporting emergency calls available, the handset tries to search also for private FPs supporting emergency calls.

If a PP which offers emergency calls is not in range of an FP where it has access rights to, the PP is allowed to lock to every FP in range which supports emergency calls even when no emergency call is initiated. This will shorten the time for setting up emergency calls and makes it possible to indicate the availability of the emergency call to the user.

If the PP is locked to an FP, to which it does not have access rights to, because it wants to offer the possibility of emergency calls, the PP shall not initiate any other procedure than emergency call setup towards this FP.

After having found a suitable FP or if the handset was already locked to an FP supporting emergency calls the PP tries to setup a connection using the basic bearer setup procedure as defined in EN 300 175-3 [3], clause 10.5.1.1. The bearer_request message for this procedure shall contain the emergency call PMID (Portable MAC Identity). By receiving this special PMID the FP can distinguish between normal and emergency calls from the first message received from the PP.

Emergency call requests shall only be supported for PT initiated call.

NOTE 1: If the MAC layer at the FP identifies a call being an emergency call it can forward this call to the higher layers and the Lower Layer Management Entity (LLME) may initiate the reservation of a free speech path in case of trunk limitation (e.g. if there are only 8 speech paths possible per basestation, but all of them are settled). This reservation may lead into a release of another call in case of trunk limitation. Other emergency calls should not be dropped because of this reason.

NOTE 2: This special PMID can also be used if an RFP wants to reserve its last timeslot(s) for emergency calls only.

The NWK-layer CC_SETUP Message which follows the MAC layer setup shall carry the IE <<BASIC-SERVICE>> indicating "default service attributes" (i.e. single bearer speech call only) within <basic-service> and "emergency call" within <call class>.

The NWK-layer CC_SETUP Message which follows the MAC layer setup shall carry the IE <<BASIC-SERVICE>> indicating <call class> "Emergency call" and indicate the "default service attributes" (i.e. shall only request a single bearer speech call). The IE <<Portable_ID>> should contain the IPEI of the handset or the IPUI in case the PT has access based upon an active subscription. The IE <<Fixed_ID>> shall be empty (length of contents 0).

The FP shall accept this CC_SETUP message regardless of the contents of <<FIXED_ID>> and <<PORTABLE_ID>> and proceed with the NWK layer setup-procedure.

NOTE 3: After establishment of this call, the call can, if possible, be routed to an emergency line of the local emergency centre. This can even be done by a residential or business FP by automatically dialling an emergency call number.

Once this call is established, it can only be released by the FP and not by the PP. The connection is held to be able to retrieve the location of the PP and to avoid an unwanted release of the call by accident.

If the emergency call setup procedure leads into an abnormal call release or if the FP rejects the outgoing call request the handset may search for another FP supporting emergency calls.

9.9 Segmentation of information in CC procedures

For the completion of any CC procedure the exchange of large amount of IWU information may be required. To avoid the need for DLC segmentation of the NWK layer's PDU carrying the CC message the IWU information may be segmented into a number of CC messages.

Segmentation may be applied if the CC message that is to carry the IWU information exceeds the following limits:

DOWNLINK: 58 octets;

UPLINK: 58 octets for full slot operation.

NOTE 1: These lower limits are chosen because the maximum information length of a LAPC UI frame, see EN 300 175-4 [4] is 63 octets.

Segmentation may be used in any CC procedure. The service data shall be segmented into two or more messages, and these messages shall be transmitted independently. The first segment should be carried by a CC message belonging to the procedure, whereas the second and following segments shall be carried in one or more {IWU-INFO} messages. The TI and PD determined by the running CC procedure shall be used.

If the service data is segmented, each message shall contain the <<SEGMENTED-INFO>> information element. Each message should contain the maximum amount of service data (of IWU/user information).

The CC shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery. Sending/reception of a {IWU-INFO} message carrying a segmented information shall trigger restart of the running CC procedure's timer.

Upon receipt of a CC message that contains the <<SEGMENTED-INFO>> element the CC (identified by the TI+PD) shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <CC_segment.1> seconds. Whenever a new segmented message is received, the CC shall attempt to construct a complete message using all stored segmented messages. Any duplicated 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 CC shall map the elements into the parameters of the relevant to the CC procedure message primitive. Duplicated mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<IWU-TO-IWU>> and/or <<IWU-PACKET>> elements shall be concatenated into a single message unit parameter. The primitive shall be delivered to the IWU and the CC may change its state.

NOTE 2: 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.

An example of segmentation used in an Outgoing call setup procedure is provided on figure 110a:

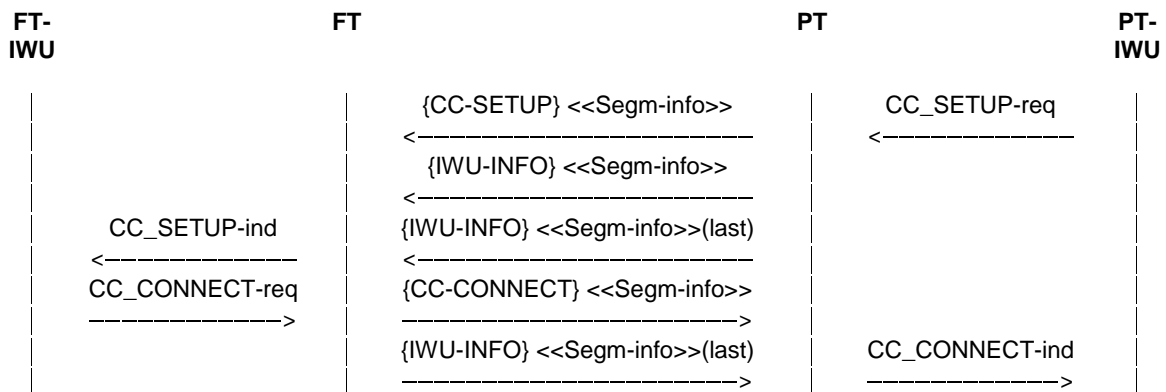


Figure 110a: Call setup with segmentation

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:

- 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;
- 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>> } <<"KEYPAD">>
 or <<MULTI-KEYPAD>> }
- <<SINGLE-DISPLAY>> } <<"DISPLAY">>
 or <<MULTI-DISPLAY>> }

The CRSS and CISS use 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.

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, utilizes the hold and retrieve set of messages. The second category, called the common information element approach, utilizes the <<FACILITY>> information element and applies only to supplementary services that do not require synchronization of resources between the user and the network.

10.4.1 Separate messages approach

The messages defined in this clause 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 Supplementary Services (CRSS) 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 Supplementary Services (CISS) 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.

10.4.2.2.1 Transport of CISS

CISS messages may be transported over the following mechanisms:

- Using any already established data link used by any C/O service.
- Using the Connectionless Supplementary Service (CLSS) procedure (see clause 10.4.2.3).

In both cases, the Protocol Discriminator (PD) "0100"B corresponding to CISS shall be used. When using any established link used by a C/O service, multiple instances of CISS identified by different values of the TV are allowed. When using the CLSS procedure, the TV value "6" shall be used and only one instance is allowed.

10.4.2.3 Connectionless Supplementary Service (CLSS) procedure

Normal operation

If a point-to-point DECT link is known not to exist, a connectionless transport mechanism can be used using a reliable data link connection.

NOTE 1: For the moment this procedure (CLSS) is restricted to the {FACILITY} message. Transport of other CISS messages is for further study.

The connectionless transport mechanism is based on {FACILITY} messages. The CLSS procedure shall only use the dummy TI value 6 and only one instance of CISS is allowed at the same time.

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 EN 300 175-4 [4]. Completion of establishment of this connection is indicated by a DL_ESTABLISH-cfm primitive.

The {FACILITY} message is used to convey one of the following information:

- "user" information, i.e. the component structures in the <<FACILITY>> information element;
- events notification to the user in <<EVENTS-NOTIFICATION>> information element;
- line identifiers in <<CALL INFORMATION >> information element;
- time and date information to the user in <<TIME-DATE>> information element.
- Light Data Services C-Plane commands (see TS 102 527-4 [76]) in <<IWU-TO-IWU>> information element.

NOTE 2: In the current procedure, the CALL INFORMATION information element is allowed to be sent along with <<EVENTS-NOTIFICATION>>. IE.

For the <<FACILITY>> information element, structure and principals of coding and the procedures upon the components are described in EN 300 196-1 [14], clauses 8.1 and 8.2. Service specific coding is defined in the respective clauses 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>> nor <<EVENTS-NOTIFICATION>> nor <<TIME-DATE>> nor <<IWU-TO-IWU>> 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 the present document.

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 EN 300 196-1 [14]):

- Malicious Call Identification (MCID), see EN 300 130-1 [22].
- Call Forwarding Busy (CFB), see EN 300 207-1 [23].
- Call Forwarding Unconditional (CFU), see EN 300 207-1 [23].
- User to User Signalling (UUS), see EN 300 286-1 [24].
- Calling Line Identification Presentation (CLIP), see EN 300 092-1 [25].
- Calling Line Identification Restriction (CLIR), see EN 300 093-1 [26].
- COnnected Line identification Presentation (COLP), see EN 300 097-1 [27].
- COnnected Line identification Restriction (COLR), see EN 300 098-1 [28].
- Completion of Calls to Busy Subscriber (CCBS), see EN 300 359-1 [29].
- FreePHone (FPH), see EN 300 210-1 [30].
- Advice Of Charge (AOC), see EN 300 182-1 [31].
- SUBaddressing (SUB), see EN 300 061-1 [32].
- Terminal Portability (TP), see EN 300 055-1 [33].
- Call Waiting (CW), see EN 300 058-1 [34].
- Direct Dialling In (DDI), see EN 300 064-1 [35].
- Multiple Subscriber Number (MSN), see EN 300 052-1 [36].
- Closed User Group (CUG), see EN 300 138-1 [37].
- Explicit Call Transfer (ECT), see EN 300 369-1 [38].
- Call Forwarding No Reply (CFNR), see EN 300 207-1 [23].
- Call Deflection (CD), see EN 300 207-1 [23].
- COnterence call add-on (CONF), see EN 300 185-1 [39].
- Call Hold (CH), see EN 300 141-1 [40].
- Three ParTY (3PTY), see EN 300 188-1 [41].

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 EN 300 175-8 [8]. This service provides messages to control four FP echo control functions.

Requirement 1 and requirement 2:

(clause 7.10 of EN 300 175-8 [8]).

Option a) and option b):

(clause 7.4.1.2 of EN 300 175-8 [8]).

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/UMTS 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 optimize 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 clause 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 setup 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 setup 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 fulfil 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 setup 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.

Setup 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 fulfil 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 setup 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.

Setup 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 F-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 EN 300 175-4 [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 clause 11.6.

11.4.2 Procedure at the receiving side

Upon receipt of a {COMS-INFO} message, the COMS shall act as follows:

- 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 <<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 NWK layer suspend and resume procedures

A COMS call may optionally be suspended at NWK layer. 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 clause 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 setup 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 shall 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 clauses 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 are the responsibility of the LCE and are 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 clause 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.

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: 63 octets;

UPLINK: 63 octets for full slot operation.

NOTE: These lower limits are chosen because the maximum information length of a LAPC UI frame, see EN 300 175-4 [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 EN 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 eight groups:

- identity procedures;
- authentication procedures;
- location procedures;
- access rights procedures;
- key allocation procedure;
- parameter retrieval procedure;
- ciphering related procedure;
- external protocol information 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 clause 15.5 which describes the management of MM procedures.

If large amount of IWU information needs to be transmitted as part of a MM procedure the information may be segmented. For the requirements in regard of segmenting MM messages see clause 13.9.3.

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

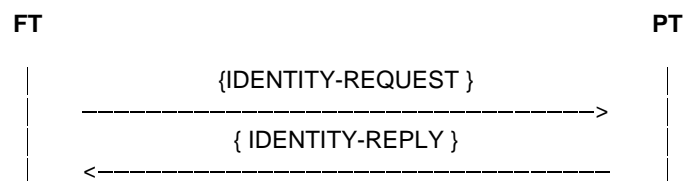
The identification procedure is used by the FT to request a PT to provide specific identification parameters to the FT e.g. the international portable user identity or the international portable equipment identity.

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.

Figure 111: Procedure for identification of PT

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 clause or by the procedure for location registration, described in clause 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 clause 7.7.13. Refer also to EN 300 175-6 [6] 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.

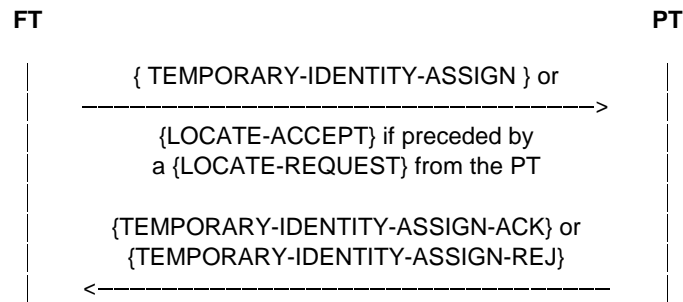


Figure 112: Temporary identity assignment

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 <<RAND>> IE shall be used for transporting the parameter RAND_F (a Random Number generated by the FT and used only once, see EN 300 175-7 [7], clause 6.3).
- The <<RS>> information element is only mandatory when the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) 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 clause H.2. If the authentication of the FT fails, the ZAP field may not be incremented.

NOTE: 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 DECT Standard Authentication Algorithm #2 (DSAA2) is used (see EN 300 175-7 [7], clause 6.3), then the <<RAND>> IE shall be also included in the response carrying the RAND_P parameter.
- If the PP has stored a ZAP field that is related to the current active IPUI, then 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 prioritized 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/UMTS) 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 at FT side by calculating it independently as function of K, RS, RAND_F and, if DSAA2 is used, RAND_P.

- 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 DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) 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.

If the DECT Standard Authentication Algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used and the DEF-bit in the <<AUTH-TYPE>> information element is set, the newly generated ciphering key shall be stored by PT and FT as default cipher key for early encryption with the default cipher key index as indicated in the <<AUTH-TYPE>> information element. The DEF-bit shall only be set in case the PP indicated support of the default cipher mechanism in the <<TERMINAL CAPABILITY>> information element.

- 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.

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.

The procedure shall follow the provisions given in EN 300 175-7 [7], and specifically the security procedure descriptions given in clause 6.3.3.1 for authentications based on DSAA algorithm and clause 6.3.3.3 for authentications based on DSAA2 algorithm.

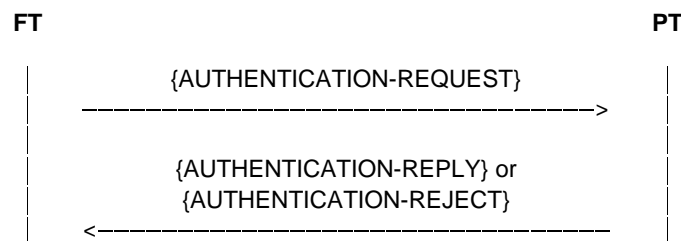


Figure 113: Authentication of the PT

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 clause 13.3.1. 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 clause 13.3.1. 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 clause 15.5.

The authentication of the user may be performed using either DSAA, DSAA2 or a proprietary algorithm. The PT authentication procedure shall follow the provisions given in EN 300 175-7 [7], clause 6.3.3.1 for authentications based on DSAA algorithm and clause 6.3.3.3 for authentications based on DSAA2 algorithm.

13.3.3 Authentication of a FT

This authentication procedure is activated by the PT, typically (but not necessarily) when the FT is sending a ZAP-command. The procedure is also part of the "Key allocation" procedure.

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.

- The <<RAND>> IE shall be used for carrying the authentication parameter RAND_P (a random number generated by the PT necessary for calculating the response parameter, see EN 300 175-7 [7]).
- 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 the DECT standard authentication algorithm (DSAA) or the DECT Standard Authentication Algorithm #2 (DSAA2) is used, for other algorithms it can be optional.
- If the DECT Standard Authentication Algorithm #2 (DSAA2) is used, (see EN 300 175-7 [7]), then the <<RAND>> IE shall be also included in the response carrying the RAND_F parameter.
- 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 prioritized 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 by the PT by calculating it independently as function of K, RS, RAND_P and, in the case of DSAA2, RAND_F. 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.

The procedure shall follow the provisions given in EN 300 175-7 [7], and specifically the security procedure descriptions given in clause 6.3.3.2 for authentications based on DSAA algorithm and clause 6.3.3.4 for authentications based on DSAA2 algorithm.

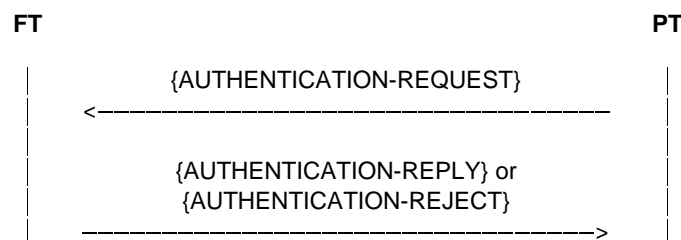


Figure 114: Authentication of a FT

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 clause 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 clause.

The location registration procedure is used as follows:

Upon receiving a MM_LOCATE-req primitive the PT sends a {LOCATE-REQUEST} message containing the following information elements:

- A <<PORTABLE-IDENTITY>> information element. The portable identity may be either the IPUI or, if the extended higher layer capabilities bit a39 is set to 1, then an assigned individual TPUI may be used. A TPUI may also be used when sending a {LOCATE-REQUEST} in the same location area as a result of expiry of validity of previous location registration if indicated by <<USE-TPUI>> in the previous {LOCATE-ACCEPT}.

NOTE 2: Extended higher layer capabilities bit a39 indicates that at least one of the networks to which an FT may provide access can support access based on TPUIs. It does not indicate that all networks accessible via the FT can support TPUI access.

- If an assigned individual TPUI is used, the FT and/or an associated network, may be unable to determine the identity of the PT, resulting in a {LOCATE-REJECT} message. In this situation the PT shall re-attempt the location registration procedure using the IPUI unless there is a <<reject reason>> indicating that location registration failed for a different reason.

NOTE 3: In some situations there may be more than one PT with the same TPUI. Further procedures to determine the PT identity are required in these situations (e.g. authentication, followed by identity request if authentication fails).

- 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 an optional <<SETUP-CAPABILITY>> information element and an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity. If the FT is capable of dealing with call setup attempts using temporary identities, it should also include the <<USE TPUI>> information element. A <<USE TPUI>> information element only applies to the active IPUI/PARK pair.

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 clause 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 clause 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 clause 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 clause 13.2.2. On receipt of a {TEMPORARY-IDENTITY-ASSIGN-ACK} message or a {TEMPORARY-IDENTITY-ASSIGN-REJ} message as described in clause 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 clause 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. Timer <MM_locate.1> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {MM-NOTIFY} message.

NOTE 4: Restarting of the timer may be required if the Location registration procedure involves communication with external networks or protocols before accepting or rejecting it.

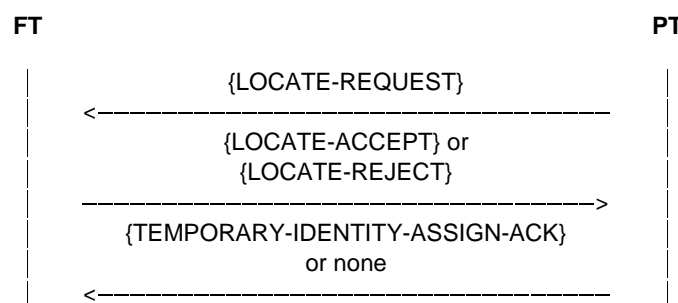


Figure 115: Location registration

NOTE 5: 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 clause 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.

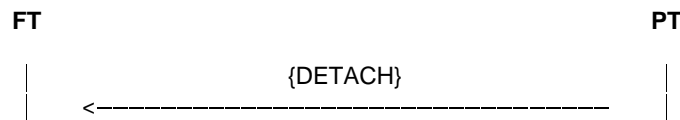


Figure 116: Detach

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 clause 13.4.1.

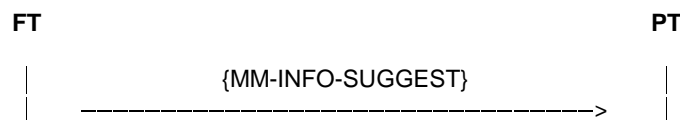


Figure 117: Location update

The locate suggest and the following location registration procedure shall be treated as two different transactions, see clause 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;
- recognize the system in order to receive calls.

The FT can then use the knowledge to:

- validate service requests from the PT;
- allow certain classes of service; and

- recognize 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, then 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 <<SETUP-CAPABILITY>> 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 <<SETUP-CAPABILITY>> information element which communicates some dynamic parameters, 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.

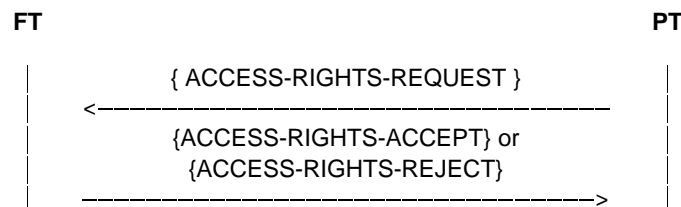


Figure 118: Obtaining of Access Rights

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;

- recognize 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;
- recognize 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 procedure 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 clause 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.

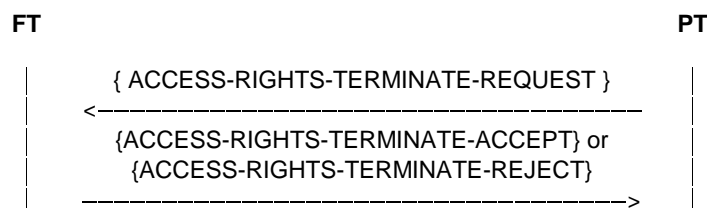


Figure 119: PT termination of access rights

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 clause 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.

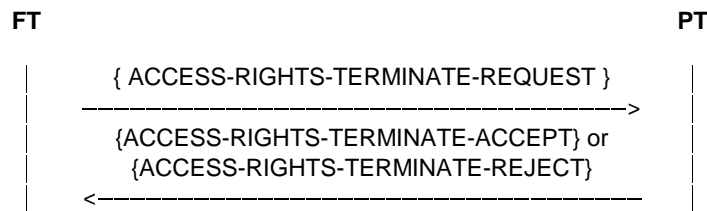


Figure 120: FT termination of access rights

13.5.3 Modification of access rights

Modification of access rights procedure is used by the FT to modify access rights stored in the PT without user intervention.

Procedure for modification of access rights:

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 "access rights modify suggest".

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues a MM_INFO-ind primitive. If the parameter type "access rights modify suggest" is indicated in the <<INFO-TYPE>> information element, the PT shall initiate the obtaining of access rights procedure as described in clause 13.5.1. Prior to this the PT should perform authentication of a FT as described in clause 13.3.3.

If obtaining the access rights procedure fails, the PT shall leave the access rights parameters unchanged.

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 (DSAA algorithm) or with the 128-bit number RS₁₂₈ (DSAA2 algorithm). 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 (DSAA). If DSAA2 is used, the PT shall generate a further random parameter RAND_P and use it in the calculation. 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 (used in the calculation of RES1 if DSAA2 is used). 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, RS and, if DSAA2 is used, RAND_P. The authentication of PT is considered as successful if RES1 = XRES1. If it is successful the FT shall use the original RS (if DSAA is used), or a freshly generated RS₁₂₈ (if DSAA2 is used), together with the AC, the received random number RAND-P and, if DSAA2 is used, a freshly generated RAND_F, 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 DSAA2 is used, the message shall also contain the RS₁₂₈ and the RAND_F used in the calculation of 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, original RS (if DSAA) or received RS₁₂₈ (if DSAA2) plus received RAND_F (if DSAA2). 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 <<ALLOCATION-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 reject the key allocation and retain the AC..

NOTE 2: The reverse Session authentication Key, KS', is an intermediate result during the calculation of RES2. Refer also to EN 300 175-7 [7].

NOTE 3: Further actions may be taken upon an authentication failure, depending of the application. For voice profiles such as GAP, the expected behaviour is dropping any call in progress.

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.

The procedure shall follow the provisions given in EN 300 175-7 [7], and specifically the security procedure descriptions given in clause 6.5.6.

Successful case:

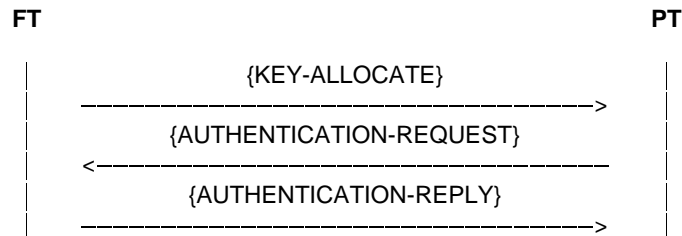


Figure 121: Successful key allocation procedure

Unsuccessful case:

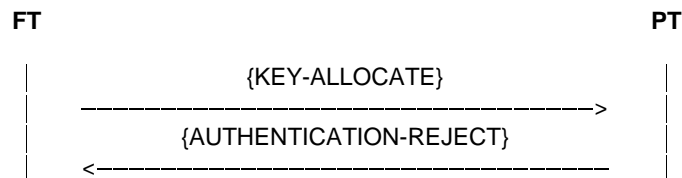


Figure 122: Unsuccessful key allocation procedure

This procedure shall not be used for roaming key allocation in a visited network.

NOTE 4: 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 EN 300 175-7 [7].

The complete key allocation procedure shall be treated as a single transaction, see clause 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 example 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 clause. 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 clause 13.4.3. One of the codings "external handover parameters", "location area", "hand over reference", "external handover candidate", "synchronized external handover candidate" and "non synchronized external handover candidate" is used for the external handover procedure which is described in clause 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);

<<SETUP-CAPABILITY>>	communicating some dynamic parameters;
<<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.

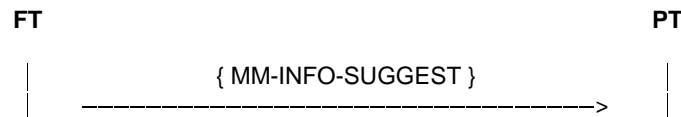


Figure 123: FT parameter retrieval procedure

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.

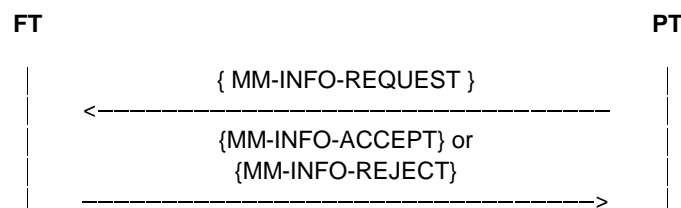


Figure 124: PT parameter retrieval procedure

The parameter retrieval procedure is supervised by the timer <MM_info.1> in the PT. At the first expiry of the timer <MM_info.1> the PT should retransmit the {MM-INFO-REQUEST} message. If the timer <MM_info.1> expires a second time, the PT shall abort the procedure and release the transaction. Timer <MM_info.1> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {MM-NOTIFY} message.

NOTE: Restarting of the timer may be required if the Parameter retrieval procedure involves communication with external networks or protocols before accepting or rejecting it.

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: 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 table 83.

Table 83: 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 a DL_ENCRYPT req primitive is issued to the DLC 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 (see note)
NOTE: 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 prioritized 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:

- release the call; or
- proceed in the existing mode.

In the case, that switching from clear to ciphered was requested, the FT has the following additional two options:

- 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;

- b) 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.

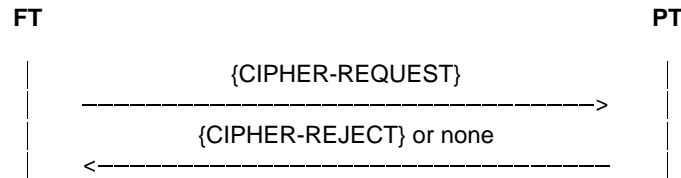


Figure 125: FT cipher switching

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 84: 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 (see note)
NOTE: 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, then 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.

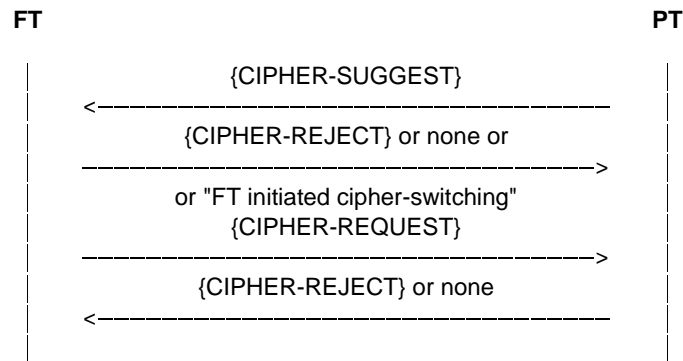


Figure 126: PT cipher switching

The complete procedure for cipher-switching initiated by the PT shall be treated as a single transaction, see clause H.3.3.

Procedure for re-keying:

Re-keying is the action of changing of the active cipher key during an ongoing encrypted call. The FP shall only trigger a re-keying procedure in case the PP indicated support of the re-keying mechanism in the <<TERMINAL CAPABILITY>> information element. For re-keying during an encrypted call, the FP uses the "Authentication of a PT" procedure to generate a new derived cipher key and then triggers the cipher-switching initiated by FT procedure.

Procedure for early encryption with the default cipher key:

After assignment of a default cipher key by means of the "Authentication of a PT" procedure, there is no cipher switching on NWK layer required for activation of encryption with the default cipher key. In the following, MAC layer can activate encryption with the default cipher key by itself, e.g. directly after connection establishment.

13.9 External protocol information procedure

This is used to exchange information between the FT and the PT.

The procedure can be initiated by the FT or by the PT.

13.9.1 Procedure for external protocol information initiated by the FT

Upon receiving a MM_IWU-req primitive the FT initiates the procedures by sending a {MM-IWU} message. This message may contain the optional information elements <<Repeat Indicator>>, <<IWU-TO-IWU>>, <<IWU-PACKET>> and <<Escape to Proprietary>>.

Upon receipt of the {MM-IWU} message the PT issues this information directly to the IWU by issuing a MM_IWU-ind primitive.

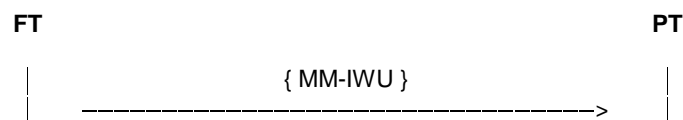


Figure 126a: FT external protocol information procedure

13.9.2 Procedure for external protocol information initiated by the PT

Upon receiving a MM_IWU-req primitive the PT initiates the procedure by sending a {MM-IWU} message. This message may contain the optional information elements <<Repeat Indicator>>, <<IWU-TO-IWU>>, <<IWU-PACKET>> and <<Escape to Proprietary>>.

Upon receiving a {MM-IWU} message the FT issues a MM_IWU-ind primitive.

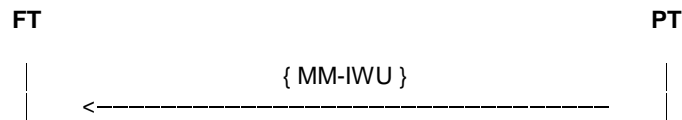


Figure 126b: PT external protocol information procedure

13.9.3 Segmentation of information in MM procedures

For the completion of any MM procedure the exchange of large amount of IWU information may be required. To avoid the need for DLC segmentation of the NWK layer's PDU carrying the MM message the IWU information may be segmented into a number of MM messages.

Segmentation may be applied if the MM message that is to carry the IWU information exceeds the following limits:

DOWNLINK: 58 octets;

UPLINK: 58 octets for full slot operation.

NOTE 1: These lower limits are chosen because the maximum information length of a LAPC UI frame, see EN 300 175-4 [4] is 63 octets.

Segmentation may be used in any MM procedure. The service data shall be segmented into two or more messages, and these messages shall be transmitted independently. The first segment shall be carried by a MM message belonging to the procedure, whereas the second and following segments shall be carried in one or more {MM-IWU} messages. In this case the External protocol information procedure shall be considered as part of the running MM procedure. The {MM-IWU} messages shall use the TI as the message that carries the first segment (see annex H for more information).

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 IWU/user information).

The MM shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery. Sending/reception of a {MM-IWU} message carrying a segmented information shall trigger restart of the running MM procedure's timer.

Upon receipt of a MM message that contains the <<SEGMENTED-INFO>> element the MM shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <MM_segment.1> seconds. Whenever a new segmented message is received, the MM shall attempt to construct a complete message using all stored segmented messages. Any duplicated 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 MM shall map the elements into the parameters of the relevant to the MM procedure message primitive. Duplicated mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<IWU-TO-IWU>> and/or <<IWU-PACKET>> elements shall be concatenated into a single message unit parameter.

NOTE 2: 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.

An example of segmentation used in a Parameter retrieval procedure is provided on figure 126c.

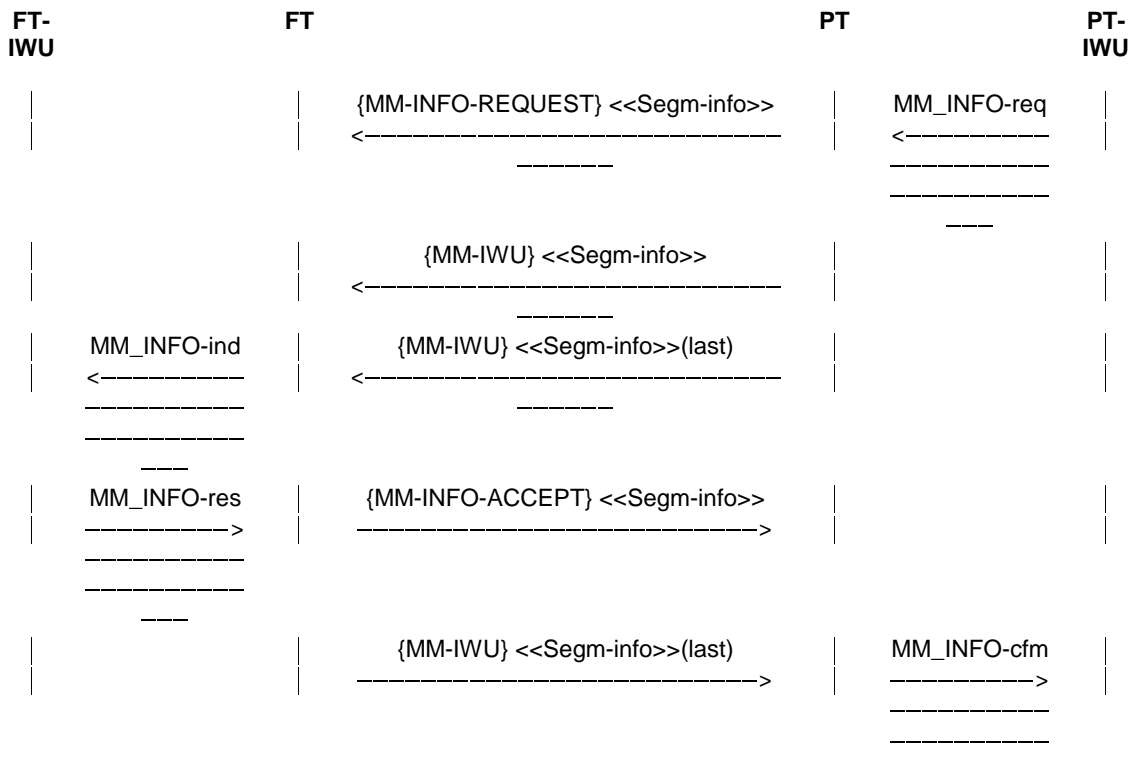


Figure 126c: External protocol information procedure used for segmentation

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 in the FT 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 the present document.

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 EN 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 clauses. The structure of this table is not defined in the present document.

Additional messages may be queued at the originating LCE during this setup 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 clause 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 full 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 full 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 EN 300 175-6 [6] for details of IPUI and TPUI. Refer to clause 8.2 of the present document, 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 clause 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 be used by default.
- the assigned individual TPUI may be used if the FT has indicated that this is allowed. This indication is provided by the <<USE-TPUI>> information element in the {LOCATE-ACCEPT} message.

NOTE 2: If an FT permits a PT to respond with TPUI, it has no mechanism to deal with multiple responses. There is an implicit requirement on the FT to ensure that TPUI assignments are unique.

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 clause 7.3.

The {LCE-REQUEST-PAGE} message may contain extended details of the required MAC layer service (see clause 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 3: 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 4: 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 5: 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 setup 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 an 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 clause 15.8.

This unwanted link shall be immediately released using the "normal" release procedures defined in clause 14.2.7.

NOTE 6: 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 7: 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 setup 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 8: The failure of one or more indirect establishment attempts may be used to update the LCE location table such that future setup requests are rejected. Any such action is not specified as part of the present document.

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

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 shall 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 the present document.

When the first message for a particular PT is passed to the LCE in the FT, the LCE queues (stores) the call setup 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 setup 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 setup 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 clause 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 the present document.

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 clause 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 clause 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 clause 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

Partial release NLR notification to LCE and timeout. 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>.

Partial release termination if link is not re-used within timeout (DLC level abnormal release). 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 clause 14.2.7.1.

Partial release if link is reused before timer expiry. 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.

CC initiated partial release (with normal CC level release). If CC wants to clear a call using "partial release", it shall first execute a normal call release procedure as specified in clause 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.

CC initiated partial release (with abnormal CC level release after {CC-SETUP} collision). If CC wants to clear a call after {CC-SETUP} collision, it shall first execute an abnormal call release procedure as specified in clause 9.5.2.3, using "insufficient resources" in the <<RELEASE-REASON>> information element in the {CC-RELEASE-COM} message. Thereafter it shall issue an NLR notification with "partial release" as reason parameter.

Partial release for other network level protocols. CISS and CLMS shall always indicate "partial release" in their NLR notifications. The use of partial release is not required for CLSS. MM should normally indicate "partial release" in the NLR notification, except when partial release is undesirable e.g. 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 clause 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").

CLMS-FIXED messages shall be sent to the B-SAP using the DL_BROADCAST-req or DL_EXPEDITED-req primitive.

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 clause 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 clause 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 setup attributes of the relevant portable. See also clause 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"), or, a DL_BROADCAST-req or DL_EXPEDITED-req primitive via the B-SAP depending on the type of CLMS message used.

14.3.3 LCE paging codes for connectionless service

If the paging message contains a connectionless TPUI, the LCE header may be used to indicate the expected service type. If the code LCE = "010" ("General/unknown") is used, the PP should accept any suitable service at the indicated transmission. If the code LCE = "000" ("no U-plane") is used, the PP should only accept C-plane connectionless services. The "no U-plane" coding is also used to announce CLMS messages.

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 connectionless 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 clause 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 "1 s" 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 "do not 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 "do not care" bits.)

NOTE 1: The P-IWU reaction in the event of another call being in progress when collective or group ringing occurs 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 clause 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 clause 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 seconds.

14.5 LCE paging procedures for DPRS

14.5.1 DPRS initial setup paging

The LCE code = "110" (DPRS S code) shall be used to setup a new DPRS virtual call.

NOTE: This code will be used nevertheless the MAC service to be used in the call.

Short and full paging formats may be used.

14.5.1.1 Assumptions for Short paging format or for Full format with IPUI

In the case of short format, or Full format with IPUI, the following assumptions shall apply:

Slot type: if the PP or FP supports only one slot type for DPRS, this slot shall be used in the setup.

If the PP and FP supports several slot types for DPRS, the slot used in the setup shall be the longest slot supported in the following sequence: double slot, long slot (j=640), full slot.

NOTE: If the slot required is not the result of this rule, then Full paging format with TPUI should be used.

Set up info: it will be assumed as "use B-field setup (no info about C_F support)".

14.5.1.2 Coding for Full paging format with TPUI

In the case of full paging format with TPUI the following rules shall be fulfilled.

Slot type: it indicates the slot required in the setup process.

Possible values:

0 0 0 1	Long slot; j = 640
0 0 1 0	Long slot; j = 672
0 1 0 0	Full slot
0 1 0 1	Double slot

Set up info: possible values:

0 0 0 0	No setup info (same assumption defined in clause 14.5.1.2 applies)
0 1 0 0	Use B-field signalling. (no info about C _F support)
0 1 0 1	Use B-field signalling, and may use C _F for NWK layer set up

NOTE: Other values may be used in non-DPRS applications.

The code "0101" allows the PP to initiate the network layer call setup using C_F without previous negotiation at MAC layer of C_F support.

14.5.2 DPRS Resume paging

The LCE code = "111" (DPRS R code) shall be used to resume an existing DPRS connection.

NOTE: This code will be used nevertheless the MAC service to be used in the call.

Short and full formats may be used.

Short format, or full format with IPUI, can be only used if there is only one DPRS logical connection between the pair PT-FT. In case of multiple connections, full format with TPUI is mandatory.

14.5.2.1 Assumptions for Short paging format or for Full format with IPUI

In the case of short format, or Full format with IPUI, the following assumptions shall apply:

Slot type: the slot type used in the existing DPRS logical connection shall be used.

Set up info: it will be assumed as "use B-field setup, (no info about C_F support)". However, the support of C_F shall be as previously negotiated before the suspension.

14.5.2.2 Coding for Full paging format with TPUI

In the case of full paging format with TPUI the following rules shall be fulfilled.

Slot type: it indicates the slot required in the setup process. It shall match with the used slot in the connection to be resumed.

Possible values:

0 0 0 1	Long slot; j = 640
0 0 1 0	Long slot; j = 672
0 1 0 0	Full slot
0 1 0 1	Double slot

Set up info: possible values:

0 0 0 0	No setup info
0 1 0 0	Use B-field signalling. (no info about C _F support). However, the support of C _F shall be as previously negotiated before the suspension.

The same assumption defined in clause 14.5.2.1 shall apply in the case of code "0000" no setup info. Therefore both codes are equivalent.

14.5.2.3 LCE Resume Procedure description

This procedure is closely related to MAC resume procedure as defined in EN 300 175-3 [3].

If MAC layer paging fails (e.g. PP has moved to another cluster) the FT LLME shall request the FT-NWK LCE for initiating a LCE resumption providing the ECN of the related link.

As result the LCE shall construct a Page message as defined in clause 14.5.2.

The LCE shall issue the {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 "RESUMPTION PENDING" state, and shall start timer <LCE.03>.

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. (N300 is an application specific value. Recommended value for voice applications is 3.)

If the {LCE-REQUEST-PAGE} message is successfully received by the intended PT, it shall check whether there is a link in ACTIVE state which belongs to a DPRS connection and can be identified by the received in the paging message Connection identity (or if there is only one when ECN is not transmitted). If such link exists the PT shall construct a LCE-PAGE-RESPONSE message following the rules as described in clause 14.2.3 and shall send it in a DL-DATA-req primitive over the existing link.

NOTE: The arrival of this message at PT MAC layer will consequently trigger a PT initiated connection resumption at MAC.

On receipt of the LCE-PAGE-RESPONSE (over the resumed connection) the FT-LCE shall check the identity contained in this response against a list of outstanding {LCE-REQUEST-PAGE} messages, and if the identity matches the identity associated with this link FT-LCE shall mark the link as "LINK ESTABLISHED"; it shall stop timer <LCE.03> and shall continue with normal operation (i.e. with the action that was the reason for the required resumption).

14.5.3 Special cases

14.5.3.1 Rule for DPRS Class 1 devices

In the case of DPRS Class 1 devices (devices without C plane), any of the codes may be used with equal result, since there is no difference between setup and resume. The use of code 110 is recommended for new products.

NOTE: The traditional practice has been using the S code (110) if the MAC service is Ip_error_detect, and the R code if the MAC service is Ip_error_correct. However this is not really needed since the MAC service is provided in the bearer setup message. In any case, the MAC service negotiated at bearer setup overrules the LCE header selection.

14.5.3.2 Rule for backcompatibility with former A/B 1 devices

If a FP wish to implement compatibility with former devices based on historic data profile A/B 1, it can implement the rule described in clause E.2 (informative).

In A/B devices there is no difference between setup and resume.

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 setup 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.

Application assistance: managing mapping, exchange and allocation of application related parameters.

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 prioritized 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 Prioritized list negotiation

Prioritized 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 "prioritized list"; followed by

- a prioritized 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 prioritized list negotiation. Exchanged attribute negotiation provides a mechanism for peer (receiving) entities to suggest alternative service attributes in response to an unacceptable setup 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 clause 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 prioritized 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 Prioritized 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 clause 9.6.

The LLME is required to map the new service demands (as indicated by the MNCC-MODIFY 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 clause 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 the present document, 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;
- the only exception to these two rules is the External protocol information procedure which can be initiated by any side at any time.

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.

The event of sending/reception of a {MM-IWU} message during an unfinished MM procedure shall restart the running MM timer.

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.

The External protocol information procedure is not put on the priority level list. It is allowed to be initiated at any time and by any side interrupting any MM procedure. However, the procedure is allowed to interrupt a running MM procedure only if it carries information needed for the completion of the running MM procedure. In all other cases the procedure shall be run outside of other MM procedures.

NOTE: When used to carry segments of information the External protocol information procedure is considered as a part of the running MM procedure (see clause 13.9.3).

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 clause 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 clause 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 clause 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 clause 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 clause 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 setup of a DECT connection to a new FP, and release of the old connection are defined in clause 15.7.4.

Procedures for ciphering during an external handover are described in clause 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 synchronization 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 (see clause 15.7.1.2), and, handover candidate retrieval (see clause 15.7.1.3).

Handover candidate information provided in a CC message should be regarded as call specific. Handover candidate information provided in {MM-LOCATE-ACCEPT} or {MM-INFO-SUGGEST} or {MM-INFO-ACCEPT} is valid until a change of FP.

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.

15.7.1.2 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.

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 synchronized external handover candidate", "multiframe, PSCN and multiframe number synchronized external handover candidate", "multiframe and PSCN synchronized external handover candidate" or "non-synchronized 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: The info types "multiframe synchronized external handover candidate", "multiframe, PSCN and multiframe number synchronized external handover candidate" and "multiframe and PSCN synchronized external handover candidate" are not mutually exclusive. For example, the FP response to a request for "multiframe synchronized external handover candidate" should include FPs from all of the above categories.

Upon receipt of an MM-INFO-REQUEST including a request for external handover parameters, the FP shall respond either with MM-INFO-ACCEPT or MM-INFO-REJECT, as described in the following.

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.

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 clauses 15.7.2.2 and/or 15.7.2.3.

Regardless of whether the Handover reference indication or the Handover reference retrieval procedure is used, the provided handover reference value is valid until the end of the call.

By default, the handover value remains valid after the successful completion of an external handover. In case updating of the handover reference value is desired upon external handover, FP-2 should indicate a new value within a CC-INFO message following the CC-CONNECT-ACK message.

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 clause 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.

Upon reception of a MM-INFO-REQUEST including a request for external handover parameters, FP shall respond either with MM-INFO-ACCEPT or MM-INFO-REJECT, as described in the following.

The FP should 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 clause 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.

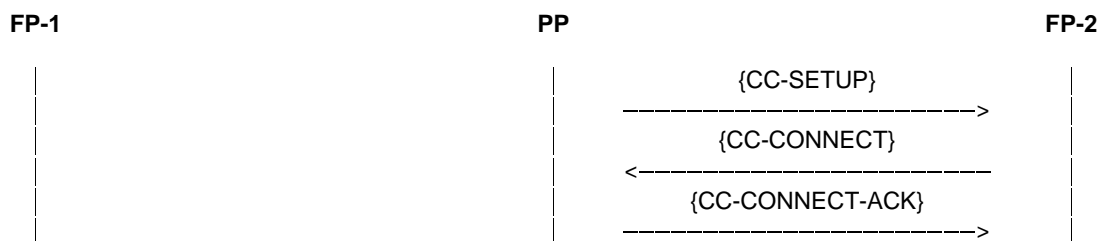


Figure 127: NWK layer set up procedure

NOTE: An entity receiving a release from its peer during external handover, should consider it to be only a release of the concerned connection (and therefore not of the associated call). Likewise, in case an entity wishes to release the entire call, it should initiate release of both network layer connections.

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 clause 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.

In this clause, the preferred radio connection to be used to transfer signalling information, is referred to as the primary signalling connection. During external handover, the primary signalling connection changes. Moreover, there may be another, secondary, connection that may be used to transfer signalling information.

If signalling information, e.g. keypad or display information, is transferred during external handover of the signalling connection should be as defined in table 85.

Table 85: Signalling information transferred during external handover

Step	Event	PP-Tx	PP-Rc	FP-Rc	FP-Tx
1	PP sends {CC-SETUP} to FP-2	FP-1	FP-1	FP-1	FP-1
2	FP-2 sends {CC-CONNECT}	FP-1	FP-1	FP-1 and FP-2	-
3	PP receives {CC-CONNECT} from FP-2	FP-1	FP-1	FP-1 and FP-2	-
4	PP sends {CC-CONNECT-ACK}	FP-2	FP-2	FP-1 and FP-2	-
5	FP-2 receives {CC-CONNECT-ACK}	FP-2	FP-2	FP-2	FP-2
6	PP receives {CC-RELEASE}	FP-2	FP-2	FP-2	FP-2

During step 2 to 4, the FP should not transfer signalling information as it may result in duplicated information being received by the PP, e.g. in case the transfer delay is not the same for both connections.

NOTE 3: Alternatively, the network and PP may queue signalling information during external handover.

15.7.5 U-plane handling

External handover also involves rerouting the U-plane. Table 86 shows the recommended receive and transmit path connections for PP and FPs.

Table 86: Recommended path connections

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.

In case the PP contains only a single cipher engine it shall delay the initiation of ciphering until the old connection is released; it shall not deactivate ciphering of the connection to FP-1 prior to initiating ciphering of the connection to FP-2.

In case the PP supports ciphering of two connections, the PP should at latest initiate ciphering upon reception of {CC-CONNECT}.

If the connection to FP-1 was ciphered, and the PP initiated ciphering fails, the PP shall re-attempt the PP-initiated ciphering procedure. This does not apply in case FP-initiated ciphering has succeeded in the mean time. The PP need not resume a PP-initiated ciphering attempt that is interrupted by a successfully completed FP-initiated ciphering procedure. The PP shall release the connection if the re-attempted PP-initiated ciphering fails.

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.

The PP shall not initiate deactivation of ciphering on the old connection unless upon reception of a CIPHER-REQUEST as indicated previously. This implies that, unless the PP supports ciphering on two connections, the PT shall not initiate ciphering prior to the release of the old connection.

NOTE 1: Deactivation of ciphering may result in loss of the call/connection which is likely to introduce an interruption of the speech service. 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.

NOTE 2: The above implies that during external handover, two cipher keys may need to be stored.

For the description of the procedure see clause 13.8.

15.7.7 Interaction with location registration

The PP which is performing an external handover should not initiate the location registration procedure until the handover is completed.

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 EN 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 in figure 128.

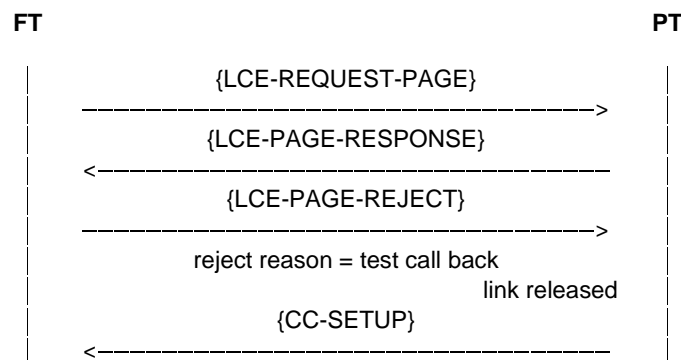


Figure 128: Test call back procedure

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 clause 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 clause 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 clause 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 cannot 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 EN 300 175-3 [3]. The coding of this message is defined in figure 129.

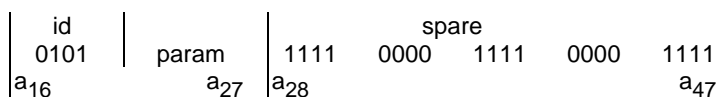


Figure 129: Upper tester procedure

Where:

- "id" indicates a NWK layer test message;
- "a_{ii}" indicates the bit positions in the MAC message.

Table 87: MM procedure parameters

Parameter		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.

15.9 Application assistance procedures

15.9.1 DECT Identity Resolution (Retrieval) Procedure

The DECT IDENTITY RESOLUTION procedure provides means for retrieving the IDENTITY of a DECT terminal, given an ADDRESS used by an application residing in or connected to this terminal.

The procedure may be used there is request for transmission of data from an application and the DECT terminal (e.g. a HyP) has knowledge for the application address of the desired recipient but does not know its DECT identity. Depending on the circumstances connectionless or connection oriented procedure may be used.

15.9.1.1 FT (or HyP) initiated Connectionless Identity Resolution procedure

The FT shall construct a Connectionless Identity Resolution REQUEST. The REQUEST shall include at least an "identity section" and an "address section". In the "identity section", the identity (or identities) of the terminals to which the REQUEST will be sent shall be included. Any identity allowed by the DECT protocol may be used and the request may be sent to all or group of terminals. In the "address section", the address (or addresses) of one or multiple applications for which the relevant DECT identities are inquired, shall be included.

Upon receipt of the REQUEST, the PTs shall check the provided with the REQUEST identity. If the identity matches to one of the PT identities, the PT shall compare the addresses provided with the REQUEST with its own application(s) addresses. If the PT finds addresses that match, the PT shall send back a Connectionless Identity Retrieval/Resolution RESPOND. The respond shall include the address (or addresses) that have been found to match and the PT's own identity.

If the identity received with the REQUEST does not match to one of the PT identities, or, if the addresses received with the REQUEST do not match to one of the PT application addresses, the PT shall ignore the request.

For the REQUEST and RESPOND the CLMS Fixed messages with <Protocol Discriminator> field set to "DECT Information Element coding" as defined in clause 8.3 should be used. For the Identity section the <<PortableIdentity>> or the <<Fixed Identity>> as defined in the present document shall be used as appropriate. For the address section, the <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" shall be used.

15.9.1.2 PT initiated Connectionless Identity Resolution procedure

The PT shall construct a Connectionless Identity Resolution REQUEST. The REQUEST shall include at least an "Address section". In the "Address section", the address (or addresses) of one or multiple applications for which the relevant DECT identities are inquired, shall be included. The PT shall send the REQUEST to the FT.

Upon receipt of the REQUEST, the FTs shall check the provided with the REQUEST addresses and shall determine whether there are addresses that match addresses of its own applications. If the FT finds addresses that match, the FT shall send back to the PT a Connectionless Identity Retrieval/Resolution RESPOND. The respond shall include the address (or addresses) that have been found to match, and the FT's own identity. Alternatively the FT may delay the RESPOND until it retrieves all identities.

If in the received REQUEST addresses are found that do not match the FT own applications addresses, the FT shall temporarily store those addresses and shall initiate a FT initiated Identity Retrieval/Resolution procedure for those addresses. When the procedure is completed and relevant identities are found the FT shall send back to the PT a Connectionless Identity Retrieval/Resolution RESPOND. The respond shall include the address (or addresses) that have been found to match, and the relevant identities.

For the REQUEST the CLMS Fixed messages with <Protocol Discriminator> field set to "DECT Information Element coding" as defined in clause 8.3 should be used. For the address section, the <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" shall be used.

15.9.1.3 Connection oriented Identity Resolution procedure

Alternatively to the connectionless procedure connection oriented procedures may be used as well. This procedure may be used for example by a HyP terminal to request address/identity mapping information which is assumed to be available at the Master.

If performed by a PP, the Parameter retrieval procedure as defined in the present document may be used. If performed by the FP, the PT Identification procedure defined in clause 13.2.1 may be used. Alternatively, exchange of {CC-INFO} messages during a call may be used. With the difference of replacing the connectionless messages with connection oriented, the procedure shall be as defined in the clauses for the connectionless case.

15.9.2 Application Address Resolution (Retrieval) Procedure

The APPLICATION AADDRESS RESOLUTION procedure provides means for retrieving the Address of an Application residing in or connected to a DECT terminal, given a DECT Identity of this terminal. An example for usage of this procedure is when the Distributed Communication is supported (see annex I) and a HyP needs to retrieve routing information for another members of the local DECT network.

The procedure implementation is similar to the described above Identity Resolution procedure with the only difference that the roles of the DECT Identity and Application addresses are replaced.

15.9.3 Application Parameter Allocation Procedure

The APPLICATION Parameter ALLOCATION PROCEDURE, provides means for allocating parameters (e.g. addresses) to of an Application residing in or connected to a DECT terminal.

15.9.3.1 FT initiated application parameter allocation procedure

The FT shall construct an APPLICATION-Parameter-ALLOCATION- REQUEST message. The REQUEST shall include at least a specially dedicated information element to indicate which application and which parameters are being assigned. The FT shall send the REQUEST to the PT.

Upon receipt of the REQUEST, the PTs shall check the provided with the REQUEST parameter and shall determine whether the parameter may be assigned to relevant application. If the indicated parameters can be assigned the PT shall send an APPLICATION-Parameter-ALLOCATION-ACCEPT message. If the assignment is not possible the PT shall send an APPLICATION-Parameter-ALLOCATION-REJECT message. The REJECT message may include a REJECT reason indicating the identified problem, and, may include one or more alternative proposals.

The Temporary Identity Assign procedure shall be used as specified in clause 13.2.2. The {TEMPORARY-IDENTITY-ASSIGN} message shall include a <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" indicating the relevant type of application and parameter.

15.9.3.2 PT initiated application parameter allocation procedure

The PT shall construct an APPLICATION-Parameter-ALLOCATION- REQUEST message. The REQUEST shall include at least a specially dedicated information element to indicate which application and which parameters are being assigned and in addition DECT Identity information to identify the DECT terminal to which the parameter is related. More than one identity and more than one application parameter may be provided. The PT shall send the REQUEST to the FT. IF the PT requests assignment for itself it shall include its own identity.

Upon receipt of the REQUEST, the FTs shall check the provided with the REQUEST identity and shall initiate the "FT initiated application parameter allocation procedure" (as described above) towards the terminal identified with the provided in the request identity. The outcome of this procedure the FT shall convey back to the initiating terminal by sending an APPLICATION-Parameter-ALLOCATION-ACCEPT or an APPLICATION-Parameter-ALLOCATION-REJECT message respectively.

The Parameter Retrieval procedure shall be used as specified in clause 13.7. The {MM-INFO-REQUEST} message shall include a <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" indicating the relevant type of application and parameter and a <<Portable Identity>> or <<Fixed Identity>> information element as appropriate.

15.9.4 Application parameter information procedure

The APPLICATION Parameter INFORMATION PROCEDURE, provides means to a DECT terminal participating in a local DECT network to request another DECT terminal to provide its application parameters, for example the address or the addresses of one or more application residing in or connected to another DECT terminal.

15.9.4.1 FT initiated connection oriented Application parameter information procedure

The FT shall construct an APPLICATION-Parameter-INFORMATION- REQUEST message. The REQUEST shall include at least a specially dedicated information element to indicate which application and which parameters are being requested. The FT shall send the REQUEST to the PT.

Upon receipt of the REQUEST, the PTs shall check the provided with the REQUEST parameter and shall send an APPLICATION-Parameter-INFORMATION-RESPOND message providing the requested parameters. If one or more of the requested parameters are not available the PT shall send APPLICATION-Parameter-INFORMATION-RESPOND with no application information.

The PT Identification procedure as defined in clause 13.2.1 may be used where the <<Identity Request>> message shall include an <<Identity type>> as defined in clause 7.7.19 information element and the <<Identity replay>> message shall include (when available) a <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned".

15.9.4.2 PT initiated connection oriented Application parameter information procedure

The PT shall construct an APPLICATION-Parameter-INFORMATION- REQUEST message. The REQUEST shall include at least a specially dedicated information element to indicate which application and which parameters are being requested, as well as an identity to identify the terminal for which the information is enquired. The PT shall send the REQUEST to the FT.

Upon receipt of the REQUEST, the FTs shall check the provided with the REQUEST identity and parameter and shall determine whether it has the requested information. If the FT has the information it shall provide it back. If the information is not available the FT shall start an FT initiated information procedure towards the terminal indicated in the request. The outcome of this procedure the FT shall convey back to the initiating terminal by sending an APPLICATION-Parameter-INFORMATION-RESPOND or an APPLICATION-Parameter-INFORMATION-REJECT message respectively.

The Parameter retrieval procedure as defined in clause 13.7 shall be used. The <<MM Info Request>> message should include <<Portable Identity>> or <<Fixed Identity>> information element as appropriate, and an <<Info type>> information element indicating the application type as defined in clause 7.7.20. The <<MM Info Accept>> message shall include (when available) a <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned".

15.9.4.3 FT initiated connectionless Application parameter information procedure

With this procedure the FT may request application parameters from group of terminals without establishing connections to each one of them. The FT shall construct a connectionless APPLICATION-Parameter-INFORMATION-REQUEST message. The REQUEST shall include an address section where for example group identity may be included when more than one terminal are requested to respond, as well as, at least a specially dedicated section to indicate which application and which parameters are being assigned. The FT shall send the REQUEST.

Upon receipt of the REQUEST, the PTs shall first check if the provided with the REQUEST address matches one of the terminals identities and if it does the terminal shall process the message and ignore it otherwise. IF the address matches, the PT shall check the provided application parameter indication and shall send a connectionless APPLICATION-Parameter-INFORMATION-RESPOND message providing the requested parameters. If one or more of the requested parameters are not available the PT shall send a connectionless APPLICATION-Parameter-INFORMATION-REJECT message. The REJECT message may include a REJECT reason indicating the identified problem.

For the REQUEST and RESPOND the CLMS Fixed messages with <Protocol Discriminator> field set to "DECT Information Element coding" as defined in clause 8.3 should be used. For the Identity section the <<PortableIdentity>> or the <<Fixed Identity>> as defined in the present document shall be used as appropriate. For the address section, the <<Identity type>> indicating the application type as defined in clause 7.7.19 and the <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" respectively shall be used.

15.9.4.4 PT initiated connectionless Application parameter information procedure

The PT shall construct a connectionless APPLICATION-Parameter-INFORMATION- REQUEST message. The REQUEST shall include at least a specially dedicated section to indicate which application and which parameters are being assigned, as well as, an Identity section to identify the terminal (or terminals) for which the information is enquired. The PT shall send the REQUEST to the FT.

Upon receipt of the REQUEST, the FTs shall check the provided with the REQUEST identity and parameter and shall determine whether it has the requested information. If the FT has the information it shall provide it back. If the information is not available the FT shall start an FT initiated information procedure towards the terminal (or terminals) indicated in the request. The outcome of this procedure the FT shall convey back to the initiating terminal by sending a connectionless APPLICATION-Parameter-INFORMATION-RESPOND or an APPLICATION-Parameter-INFORMATION-REJECT message respectively.

For the REQUEST and RESPOND the CLMS Fixed messages with <Protocol Discriminator> field set to "DECT Information Element coding" as defined in clause 8.3 should be used. For the Identity section the <<PortableIdentity>> or the <<Fixed Identity>> as defined in the present document shall be used as appropriate. For the address section, the <<Info type>> indicating the Application type and the <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" respectively shall be used.

15.9.5 Application Parameter Indication procedure

The APPLICATION Parameter INDICATION PROCEDURE provides means to a DECT terminal participating in a local DECT network to provide without request its application parameters for example the address or the addresses of one or more application residing in or connected to this terminal to another DECT terminal.

If a terminal wants to provide some of its application parameters to another DECT terminal it may either include the appropriate information element providing the application parameters in any DECT connection oriented message; or alternatively, the terminal may construct a special connectionless APPLICATION-Parameter-INDICATE message which includes at least a section with the identification of the application and the relevant parameters and submit it to one or more terminals using appropriate DECT identity address. The <<Network Parameter>> information element as defined in clause 7.7.29 with <Discriminator> set to "Application Assigned" respectively shall be used.

The procedure may be initiated by PT or by FT and may be used for update of the relevant entries in application/identity resolution tables. When used in a {DETACH} message the relevant entry may be deleted.

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 realization 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 EN 300 175-4 [4].

16.3 Primitives to IWU

This clause summarizes 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 the present document. 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, res | }; | |
| 7) | MNCC_RELEASE- | {req, cfm, ind, res | }; | |
| 8) | MNCC_FACILITY- | {req, | ind | }; |
| 9) | MNCC_INFO- | {req, | ind | }; |
| 10) | MNCC_MODIFY- | {req, cfm, ind, res | }; | |
| 11) | MNCC_HOLD- | {req, cfm, ind, res | }; | |
| 12) | MNCC_RETRIEVE- | {req, cfm, ind, res | }; | |
| 13) | MNCC_IWU_INFO- | {req, | ind | }; |

16.3.2.1 MNCC_SETUP primitive

Table 88: 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	-
Calling party name	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

Table 89: 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

Table 90: 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 the present document.

16.3.2.4 MNCC_CALL_PROC primitive

Table 91: MNCC_CALL_PROC primitive

Parameter	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
FacilityProgress indicator	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

Table 92: 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

Table 93: MNCC_CONNECT primitive

Parameter	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Message units (possible elements)				
Facility	O	N	O	N
Progress indicator	O	N	O	N
Display	O	O	O	O
Signal	O	N	O	N
Feature indicate	O	O	O	O
Terminal capability	O	N	O	N
Transit delay	O	N	O	N
Window size	O	N	O	N
IWU-to-IWU	O	O	O	O
IWU-packet	O	O	O	O
A = Always. O = Optional. "- " = Not applicable. N = Not allowed.				

16.3.2.7 MNCC_RELEASE primitive

Table 94: 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 the present document.

16.3.2.8 MNCC_FACILITY primitive

Table 95: MNCC_FACILITY 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	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-
A = Always. O = Optional. "-" = Not applicable.				

16.3.2.9 MNCC_INFO primitive

Table 96: 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	-
Calling party number	O	-	O	-
Calling party name	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

Table 97: 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	O
IWU attributes	O	O	O	O
IWU-TO-IWU	O	O	O	O
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

Table 98: 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

Table 99: 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

Table 100: 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

Table 101: MNSS_SETUP primitive

Parameter	REQ	CFM	IND	RES
Supplementary Services Endpoint Identifier	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

Table 102: MNSS_FACILITY primitive

Parameter	REQ	CFM	IND	RES
Supplementary Services Endpoint Identifier	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

Table 103: MNSS_RELEASE primitive

Parameter	REQ	CFM	IND	RES
Supplementary Services Endpoint Identifier	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 };
- 6) MNCO_REJECT- {req }.

16.3.4.1 MNCO_SETUP primitive

Table 104: 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

Table 105: 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

Table 106: 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

Table 107: 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

Table 108: 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.				

16.3.4.6 MNCO_REJECT primitive

Table 109: MNCO_REJECT primitive

Parameter	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	-	-
Message units (possible elements)				
Release reason	O	-	-	-
Display	O	-	-	-
IWU-to-IWU	O	-	-	-
IWU-packet	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

Table 110: MNCL_UNITDATA primitive

Parameter	REQ	CFM	IND	RES
CLMS Endpoint Identifier (CLEI)	A	-	A	-
CLMS Message type (see note 1)	A	-	A	-
Message units (possible elements)				
Alphanumeric	O	-	O	-
IWU-to-IWU (see note 2)	O	-	O	-
IWU-packet (see 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 }; |
| 11) MM_IWU | { req, ind }. |

16.3.6.1 MM_IDENTITY primitive

Table 111: 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
Model Identifier	N	O	N	O
A = Always. O = Optional. N = Not allowed.				

16.3.6.2 MM_IDENTITY_ASSIGN primitive

Table 112: MM_IDENTITY_ASSIGN primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see 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	O	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

Table 113: MM_AUTHENTICATE primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see note)	N	A	N	N
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

Table 114: MM_LOCATE primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see note)	N	A	N	N
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
Setup capability	O	N	O	N
Terminal capability	O	N	O	N
Duration	N	O	N	O
IWU-TO-IWU	O	O	O	O
Model Identifier	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

Table 115: 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

Table 116: MM_ACCESS_RIGHTS primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see 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
Model Identifier	O	N	O	N
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

Table 117: MM_ACCESS_RIGHTS_TERMINATE primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see 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

Table 118: 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

Table 119: MM_INFO primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see note)	N	A	N	A
Message units (possible elements)				
Info type	A	O	A	O
Call identity	O	O	O	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

Table 120: MM_CIPHER primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (see 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.				

16.3.6.11 MM_IWU primitive

Table 120a: MM_IWU primitive

Parameter	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	-	A	-
Accept/Reject flag (see note)	N	-	N	-
Message units (possible elements)				
IWU-TO-IWU	O	-	O	-
IWU-PACKET	O	-	O	-
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 the present document (see clause 7.2) are applicable only to those messages which pass the checks described in clauses 17.1 to 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 clause and shall be provided in each implementation.

Clauses 17.1 to 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 the present document.

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 clause 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

Unknown transaction identifier. Whenever any message except {CC-SETUP}, {CC-RELEASE}, {CC-RELEASE-COM} or (for FPs or PPs supporting the service change procedures of clause 9.6) {CC-SERVICE-CHANGE} is received specifying a transaction identifier which is not recognized 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 recognized as relating to an active call or to a call in progress, no action should be taken.

Incorrect {CC-SETUP} transaction identifier flag. When a {CC-SETUP} message is received specifying a transaction identifier flag incorrectly set to "1", this message shall be ignored.

Incorrect {CC-SERVICE-CHANGE} transaction identifier. When a {CC-SERVICE-CHANGE} message is received specifying a transaction identifier which is not recognized as relating to an active call, this message shall be ignored.

Repeated {CC-SETUP}. When a {CC-SETUP} message is received specifying a transaction identifier which is recognized 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 recognized 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 recognized 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 recognized 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 recognized 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

{CC-SETUP} received during active call or call in progress. When a {CC-SETUP} message is received specifying a transaction identifier which is not recognized as relating to an active call or to a call in progress (but with a transaction identifier flag correctly set to 0), one of two conditional actions shall be taken:

- If the call was in progress and at CALL INITIATED state ({CC-SETUP} just sent), then clause 9.5.2.3 ('Abnormal release in case of call setup collision') shall be applied by both sides.
- If the call was in progress but reached a state beyond CALL INITIATED, or was active, the call shall continue, and 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 unrecognized 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 clause 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 clause 9.5.2 shall be followed.

17.4.2 CISS message error

Whenever an unexpected message, or an unrecognized 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 unrecognized message is received in any state, the message should be ignored.

17.4.4 MM message error

Whenever an unexpected message, or an unrecognized message is received in any state, the message should be ignored.

17.4.5 LCE message error

Whenever an unrecognized 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 clause 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 clause 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 clause 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 clause 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 clause 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 clauses identify actions on information elements not recognized as mandatory.

17.7.1 Unrecognized information element

Action shall only be taken on the message and those information elements which are recognized and have valid content.

Subsequent actions in the event of an unrecognized information element are therefore determined by the sender of the unrecognized 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 recognized and have valid content. All other elements shall be discarded.

This clause shall also apply to non-mandatory information elements with a length exceeding the maximum length (as given in clause 6).

There are two exceptions 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 clause 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 recognized 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> and <CC.06> 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 DL_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:	A {CC-SETUP -ACK} has been sent.
Stop:	as soon as FT leaves "Overlap Sending" state.
<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 setup timer.
FT value:	20 seconds.
PT value:	20 seconds.
Start:	A {CC-SETUP} message has been sent.
Stop:	A response message has been received.
<CC.04>	CC completion timer.
FT value:	100 seconds.
PT value:	100 seconds.
Start:	Refer to clause 9.3.
Stop:	Refer to clause 9.3.

<CC.05>	CC connect timer.
FT value:	10 seconds.
PT value:	10 seconds.
Start:	A {CC-CONNECT} message has been sent.
Stop:	A {CC-CONNECT-ACK} message is received.

In the direction FT-> PT {CC-CONNECT-ACK} applies only for external handover. Consequently, in the FP timer CC.05 only applies in case of external handover.

<CC.06>	CC setup crossing resolving timer.
FT value:	Not used.
PT value:	1500 milliseconds.
Start:	{CC-SETUP} crossing detection.
Stop:	new {CC-SETUP} received (incoming call restarted).
<CC_service>	Service Change timer.
value:	20 seconds.
Start:	{CC-SERVICE-CHANGE} message is sent.
Stop:	An indication for link release from the DLC is received; A {CC-SERVICE-ACCEPT} or a {CC-SERVICE-REJECT} message is received; {CC-RELEASE}, {CC-RELEASE-COM} messages are sent or received.
<CC_segment.1>	CC segments 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.

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 setup timer.
FT value:	10 seconds.
PT value:	10 seconds.
Start:	A {COMS-SETUP} message has been sent.
Stop:	A 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>, <MM_re-keying.1>, <MM_early_encryption.1>, <MM_encryption_check.1>, <MM_encryption_check.2> and <MM_registration.1> shall also be stopped upon following events:

- a valid MM message has been received initiating a higher priority MM procedure, see clause 15.5;
- the LCE is notified by the DLC via the DL_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.

When a timer is restarted by the means of a {MM-NOTIFY} message indicating "Timer restart" the timer shall be stopped and started 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.
<MM_info.1>	Parameter retrieval timer.
FT value:	None.
PT value:	5 seconds.
Start:	A {MM-INFO-REQUEST} message is sent.
Stop:	A {MM-INFO-ACCEPT} or a {MM-INFO-REJECT} message is received.
<MM_segment.1>	MM segments 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.
<MM_re-keying.1>	
Description:	FT re-keying timer.
FT value:	60 seconds.
Start:	A {AUTHENTICATION-REQUEST} message for re-keying is sent.
Stop:	Next { AUTHENTICATION-REQUEST } for re-keying message is sent. The timer is restarted.
<MM_early_encryption.1>	
Description:	FT early encryption timer within which a default cipher key has to be generated.
FT value:	30 seconds.

Start: Encryption activation of the first call after end of obtaining access rights procedure, in case no default cipher key was generated until this point in time.

Stop: Default cipher key is generated (Authentication of PP with DEF-bit = 1).

<MM_encryption_check.1>

Description: FT timer within which a call has to be encrypted.

FT value: 15 seconds.

Start: Send/receive of {CC-SETUP}.

Stop: Encryption is activated.

<MM_encryption_check.2>

Description: PT timer within which a call has to be encrypted.

PT value: 15 seconds.

Start: Send/receive of {CC-SETUP}, respectively {CC-CONNECT}.

Stop: Encryption is activated.

<MM_registration.1>

Description: FT timer within which the registration mode is active (Extended Fixed Part capability bit a44 = 1).

FT value: 120 seconds.

PT value: Not used.

Start: Subscription mode has been requested by the user: set a44 "access rights supported" bit.

Stop: As soon as on-air subscription procedure is successful, clear a44 "access rights supported".

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, 3 seconds minimum.

PT value: 10 seconds maximum, 3 seconds minimum.

Start: A higher entity indicates partial release to the LCE.

Stop: A new higher entity message or a DL_DATA-ind with an SDU is received.

<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}	sent									P28		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				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 clause 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).

NOTE 3: For segmentation purposes an {IWU-INFO} message can be sent/received in any state.

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.

Running timer restarted. 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 to P26: For further study.

P27: <CC.03> expires. Send {CC-RELEASE-COM} message.

Issue MNCC_REJECT-ind primitive. Clear call. Next state T-00.

P28: MNCC_CONNECT-res received.

Send {CC-CONNECT-ACK} message.

Current state maintained.

ALL OTHER CASES: all unexpected messages shall be handled according to clause 9 (if described) or according to clause 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
		F00	F01	F02	F03	F04	F06	F07	F10	F19	STATE
{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-CONNECT-ACK}	sent								Q28		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-COM} (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 table B.2) shall be treated according to the normal procedures given in clause 9 where defined. If not defined they shall be treated according to clause 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).

NOTE 3: For segmentation purposes an {IWU-INFO} message can be sent/received in any state.

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: Timer needs to be restarted.

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 to Q26: For further study.

Q27: <CC.03> expires. Send {CC-RELEASE-COM} message.

Issue MNCC_REJECT-ind primitive. Clear call. Next state F-00.

Q28: {CC-CONNECT-ACK} message received.

Issue MNCC_CONNECT-cfm primitive. Stop timer <CC.05> Next state F-10.

ALL OTHER CASES: all unexpected messages shall be handled according to clause 9 (if described) or according to clause 17.4 (if not described).

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

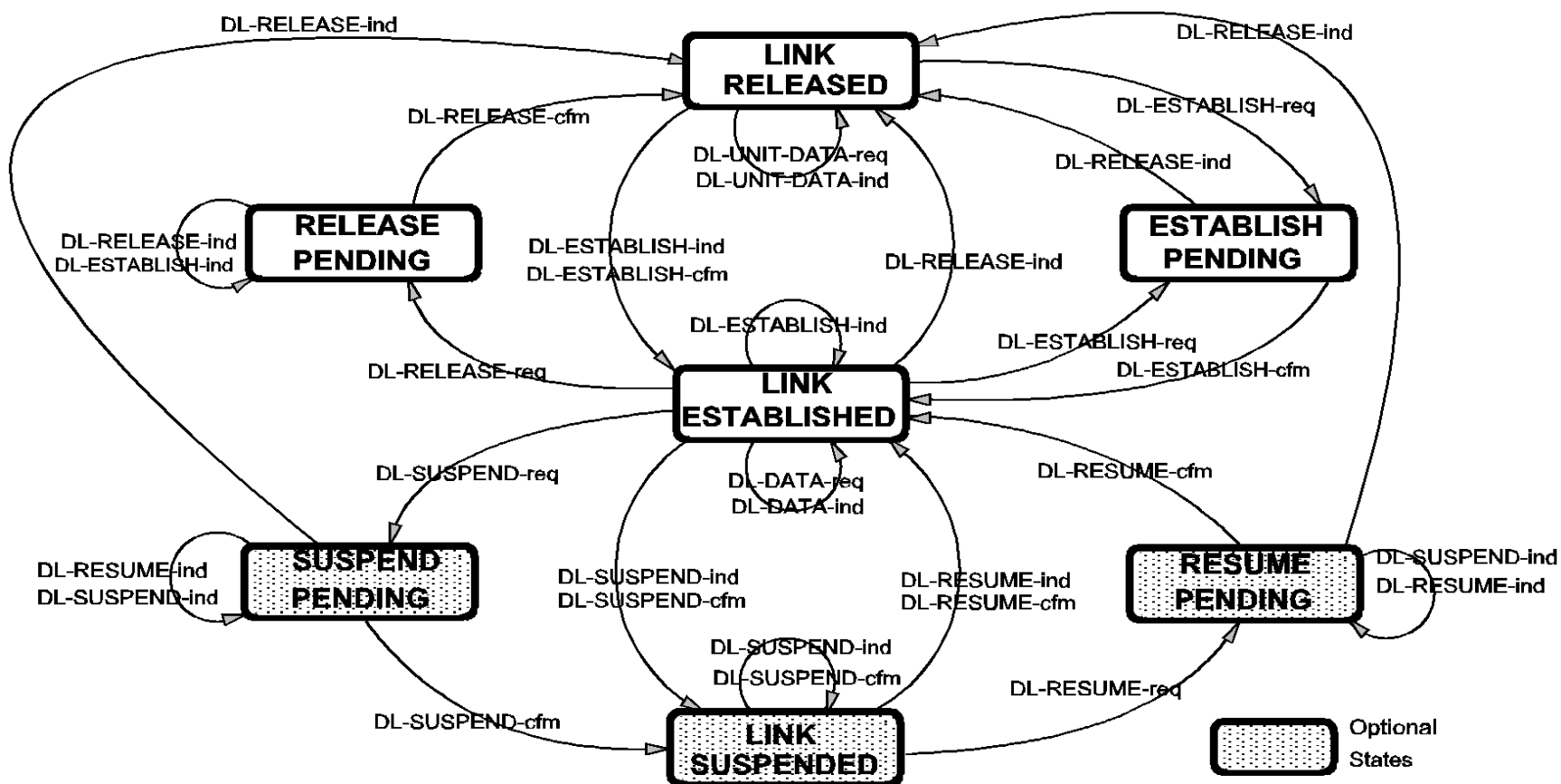


Figure C.1: DLC Link states as viewed by the LCE

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 Recommendation ITU-T T.50 [i.5] 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:

Table D.1

Code(Hex)	Control character
00	Null/cancel DTMF tone
02	Return home
03	Return end
05	Dialling pause (see note 3)
06	Move forward to next column tab position (see note 1)
07	Move backward to next column tab position (see 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 (see note 2)
0F	Flash on (see 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 (see note 4)
16	Go to DTMF dialling; infinite tone length
17	Internal call (see note 5)
18	Service call (see note 6)
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
1C	Supplementary service (see note 7)

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 EN 300 001 [13].

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.

NOTE 6: A call initiated by a DECT PT for entering of FT related service and adjustment procedures in a transparent way.

NOTE 7: To request a supplementary service as defined in NG-DECT Part 3: Extended Wideband speech services (TS 102 527-3 [75]).

D.2.3 Standard IA5 codes

Character codes 20 Hex to 7F Hex shall be used in the standard IA5 sense as defined in Recommendation ITU-T T.50 [i.5]. 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/IEC 2022 [11] 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

Table D.2

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 information elements

E.1 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
	Information transfer capability	Speech
4	Negotiation indicator	Not possible
	External connection Type	Connection oriented
5	Transfer mode	Circuit mode
	Information transfer rate	32 kbit/s
6	Protocol identifier	User protocol ID
	User protocol ID	G.726 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

E.2 Default coding of <<IWU-ATTRIBUTES>>, <<CALL-ATTRIBUTES>> and <<CONNECTION-ATTRIBUTES>> information elements for wideband speech

In case the basic service is indicated as wideband speech, the service negotiation shall be done via codec negotiation using the information element <<CODEC-LIST>>.

The setup attributes which are not covered by the information element <<CODEC-LIST>> shall have default values as given below.

E.2.1 Default setup attributes for basic service wideband speech

Table E.3: Default coding for <<IWU-ATTRIBUTES>> information element

Octet	Information element field	Field Value
3	Coding standard	DECT standard
	Information transfer capability	Speech
4	Negotiation indicator	According to IE <<CODEC-LIST>>
	External connection Type	Connection oriented
5	Transfer mode	Circuit mode
	Information transfer rate	According to IE <<CODEC-LIST>>
6	Protocol identifier	User protocol ID
	User protocol ID	According to IE <<CODEC-LIST>>

Table E.4: 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 routing	According to IE <<CODEC-LIST>>
5	U-plane symmetry	Symmetric
	LU identification	LU1
6	U-plane class	According to IE <<CODEC-LIST>>
	U-plane frame type	FU1

Table E.5: Default coding for <<CONNECTION-ATTRIBUTES>> information element for wideband speech

Octet	Information element field	Field Value
3	< Symmetry >	Symmetric
	< Connection identity >	Not yet numbered.
4	< Target bearers (P = > F direction) >	Number of target bearers always 1
5	< MAC slot size >	According to IE <<CODEC-LIST>>
	< MAC service P = > F >	According to IE <<CODEC-LIST>>
6	< CF-channel attributes P = > F >	According to IE <<CODEC-LIST>>
	< MAC packet life time P = > F >	Not applicable

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 EN 300 175-3 [3].

Table F.1: Broadcast attributes coding

Bit number (see note)	Attribute ("1" means that service is available)
a32	ADPCM/G.726 Voice service
a33	GAP basic speech
a34	Non-voice circuit switched service
a35	Non-voice packet switched service
a36	DECT Standard Authentication (DSAA) required
a37	DECT Standard Cipher (DSC) 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: The bit numbers refer to the bit positions in the MAC message. Refer to clause 7.2.3.4.2 in EN 300 175-3 [3].	

NOTE 2: The default setting for all bits is "0"; meaning "not available".

NOTE 3: The value of any bit might change during normal operation.

F.2 Extended higher layer capabilities

If a profile is supported or a capability provided, then the bit corresponding to that profile is set to 1; otherwise (if profile/capability is not supported) the bit is set to 0.

Table F.2: Extended higher layer capabilities

Bit number	Profile supported
a47	ISDN Data Services
a46	DPRS Class 2 management and B-field procedures supported (DPRS-M.5)
a45	DPRS Class 3 or Class 4 management and A-field procedures supported (DPRS-M.30), see note 3
a44	Data Service Profile D
a43	LRMS
a41	Asymmetric bearers supported
a40	Emergency call supported
a39	Location registration with TPUI allowed
a38	Synchronization to GPS achieved
a37	ISDN intermediate system
a36	RAP Part 1 Profile
a33	V.24
a32	PPP
a31	IP
a30	Token Ring
a29	Ethernet
a28	IP Roaming unrestricted supported
a27	Generic Media Encapsulation transport (DPRS) supported
a26	Basic ODAP supported
a25	F-MMS Interworking profile supported

NOTE 1: The bit numbers refer to the bit positions in the MAC message. Refer to EN 300 175-3 [3], clause 7.2.3.5.

NOTE 2: The default setting for all bits is "0"; meaning "not available".

NOTE 3: The supported management Class can be inferred from the state of bit a21 (MAC suspend/resume supported). If bit a21 = 1 then Class 3, if a21 is = 0, then Class 4.

F.3 Extended higher layer capabilities (part 2)

If a profile is supported or a capability provided, then the bit corresponding to that profile is set to 1; otherwise (if profile/capability is not supported) the bit is set to 0.

For DPRS [72] and New Generation DECT systems supporting packet data (TS 102 527-2 [74], the system category is indicated by bits a25 to a28.

For New Generation DECT systems supporting extended wideband speech services (TS 102 527-3 [75]), supported sets of services are indicated by bits a30 to a35.

Table F.3: Extended higher layer capabilities (part 2)

Bit number	Profile supported
a24	NG-DECT Wideband voice (see TS 102 527-1 [73])
a25 to a28	DPRS/NG-DECT Packet Data Category (see EN 301 649 [72] and TS 102 527-2 [74] and table F.3b)
a29	NG-DECT Extended wideband voice supported (TS 102 527-3 [75])
a30-a34	NG-DECT FP extended wideband voice (TS 102 527-3 [75]) specific sets of services (see table F.3c)
a35	"no emission" mode support (see EN 300 175-3 [3], TS 102 527-3 [75]) and note 4)
a36	Support of NG-DECT 5 (Additional feature set nr.1 for extended wideband voice, TS 102 527-5 [78])
a37	Reserved
a38	Reserved
a39	Support for DECT ULE Phase 1 (see TS 102 939-1 [79])
a40	Reserved for DECT ULE (see note 5)
a41	Reserved for DECT ULE (see note 5)
a42	Support of "Re-keying" and "early encryption" (see EN 300 175-7 [7])
a43	DSAA2 supported (see EN 300 175-7 [7])
a44	DSC2 supported (see EN 300 175-7 [7])
a45	Light data services (TS 102 527-4 [76]) supported
a46	Reserved
a47	Reserved

Table F.3b: NG-DECT [74]/DPRS [72] Packet Data Category (Cat)

Bits a25 to a28	DPRS/NG-DECT Packet Data Category
0000	No Packet data supported or non categorized system
0001	Cat 1: data Category 1 (see note 3)
0010	Cat 2: data Category 2 (see note 3)
0011	Cat 3: data Category 3 (see note 3)
0100	Cat 4: data Category 4 (see note 3)
0101	Cat 5: data Category 5 (see note 3)
All other values	Reserved for future standardization

Table F.3c: NG-DECT Extended voice [75] supported sets of services

Bits a30 - a34	Set of services and associated procedures	Related procedures
1xxxx	Permanent CLIR	7.4.12 [75]
x1xxx	Third party conference call (external or internal)	7.4.3.7 [75]
xx1xx	Intrusion call	7.4.3.8 [75]
xxx1x	Call deflection	7.4.4.1.1, 7.4.4.2 [75]
xxxx1	Multiple lines	7.4.7 [75]

NOTE 1: The bit numbers refer to the bit positions in the MAC message. Refer to EN 300 175-3 [3], clause 7.2.3.11.

NOTE 2: The default setting for all bits is "0"; meaning "not available".

NOTE 3: See the data profile specification for exact definition of Packet data Categories. Packet data Categories are incremental: Cat 3 systems also support Cat 1 and Cat 2; Cat 2 systems also support Cat 1; Cat 4 and Cat 5 systems also support Cat 1, Cat 2 and Cat 3.

NOTE 4: Bit a35 = "1" indicates, that the system may switch to "no emission" mode operation
Bit a35 = "0" indicates, that the system will not switch to "no emission" mode operation.

NOTE 5: Reserved DECT ULE bits will be set to "0" for transmission and may not be checked by the receiving party.

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 clause 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 1: The <<IWU-TO-IWU>> element provides a capability equivalent to the <<USER-TO-USER>> information element defined in EN 300 403-1 [9].

NOTE 2: The <<IWU-TO-IWU>> information element is used as well to exchange DECT profile specific information between the peer interworking units.

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} or {MM-IWU} messages, and each {IWU-INFO}/{MM-IWU} 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. A {MM-IWU} message should be used if there are no suitable MM 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 CC messages scheduled for transmission. A {MM-IWU} message should be used if there are no suitable MM messages scheduled for transmission.

A CC related 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. When sent during MM procedures the first segment of a segmented <<IWU-TO-IWU>> may be included in any valid MM message, whereas the following segment shall be sent in a sequence of <<MM-IWU>> messages each message carrying only one <<IWU-TO-IWU>> element, and each of these <<IWU-TO-IWU>> elements 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 annex H 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 clause 15.5) 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.

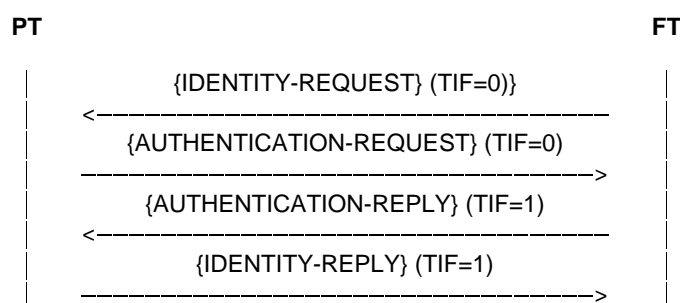


Figure H.1: Nested procedure, example 1

EXAMPLE 2: A PT initiated procedure for location registration is interrupted by a FT initiated authentication of PT procedure.

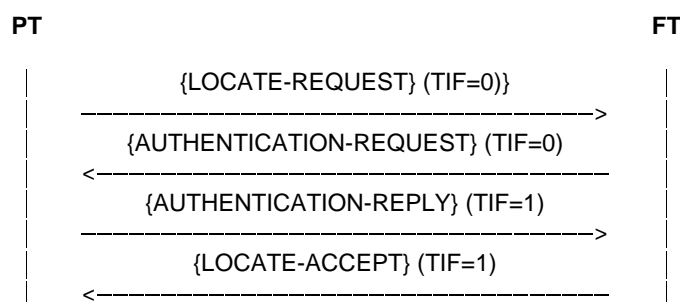


Figure H.2: Nested procedure, example 2

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.

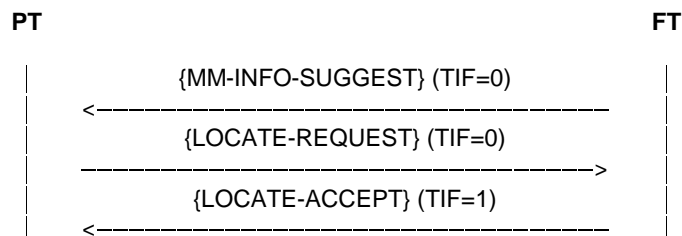


Figure H.3: Location update procedure

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:

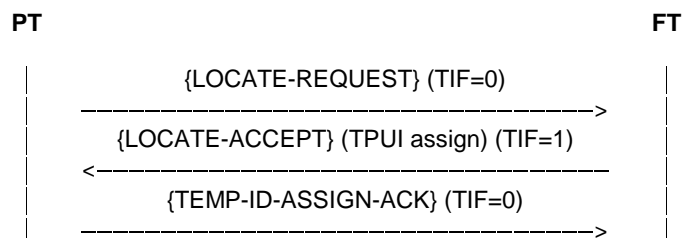


Figure H.4: TIF allocation, case 1

Case 2:

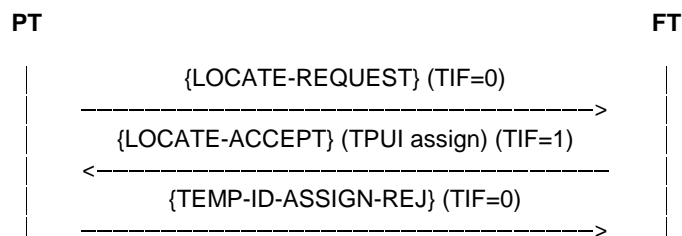


Figure H.5: TIF allocation, case 2

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:

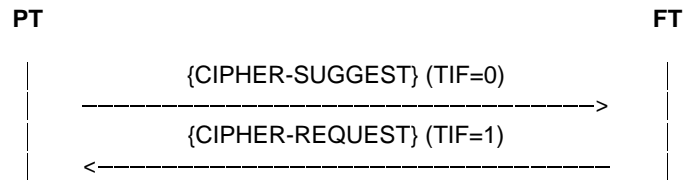


Figure H.6: PT initiated cipher switching, case 1

Case 2:

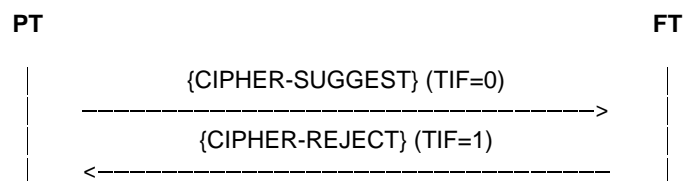


Figure H.7: PT initiated cipher switching, case 2

Case 3:

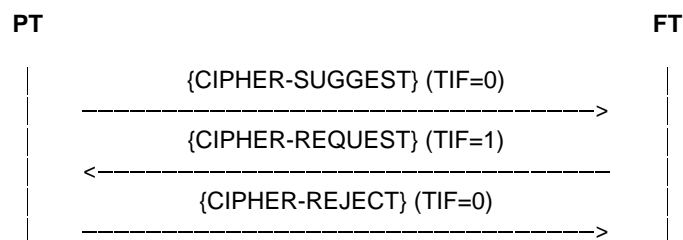


Figure H.8: PT initiated cipher switching, case 3

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.

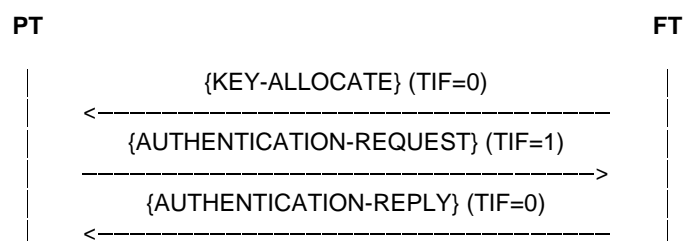


Figure H.9: Key allocation

H.4 External protocol information procedure

The External protocol information procedure represents a special case of an MM procedure that may be used as a standalone procedure as well as a part of a running MM procedure when used to carry additional segments of information needed for the successful completion of the MM procedure.

When used as a standalone procedure the rules specified in clause H.3 shall apply. If used for providing additional information to a running MM procedure the {MM-IWU} message shall have the same TI as the MM message carrying the first segment of the information.

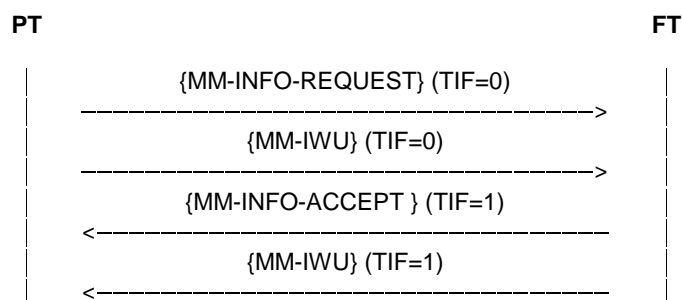


Figure H.10: Parameter retrieval procedure example

Annex I (normative): Distributed communications

I.1 Introduction

Annex I describes the DECT concept for Distributed communications to allow direct communication between two or more terminals without relaying the communications links via a FT or WRS.

The main goal is to provide more bandwidth for a set of terminals working together in a DECT system. Though the main target are DECT DATA local networking there are no limitations enforced by the concept on applying the idea on voice terminals as well.

Some of the requirements and procedures described in annex I later on are closely related to requirements specified in other parts of EN 300 175, e.g. Part 3 [3] - MAC. However, in order to ease the understanding the approach has been taken to keep the concept specific requirements together (i.e. in the present document) and not spread them over a number of documents.

I.2 General requirements

I.2.1 DCDL-net

A DL-net that supports Distributed communications (DCDL-net) shall:

- have allocated a MASTER terminal to determine the intra-network synchronization and provide common for the DCDL-net information and control. If there is a terminal that is intended for constant operation (e.g. the terminal that provides voice services to an external network and is not intended to be frequently powered-down) this should be allocated as MASTER;
- maintain for the whole time of its existence a DCDL-net System Control Bearer transmitted by the MASTER; if the MASTER is to switch-off or leave it should assign another active member as the new MASTER; the System Control Bearer should be a connectionless bearer and shall continuously provide information about the currently active members; all active DCDL-net members shall synchronize to the System Control Bearer, i.e. to the MASTER and shall continuously listen to it and retrieve the necessary information to maintain its communication within the DCDL-net;
- possess (meaning every member of the DCDL-net shall independently possess) a Common Subscription Database (CSDb) including: common to all members AC, DCK, PLI and LAL (provision of every single value depends on the support of a particular feature); List with all members distinguished by their identification number (IdN); Information for all member including RFPI, PARK, IPUI and TPUI, terminal capabilities, etc.;
- provide means of control of the usage of the resource throughout the DCDL-net by advising reduction of the number of used bearers (valid for multi-bearer connections).

I.2.2 Subscription

For establishment of the necessary values in the CSDb the following rules shall apply:

- a basic ARI should be assigned to particular DCDL-net at the DCDL-net initialization; this should be the ARI of the terminal assigned to be the DCDL-net MASTER at this time;
- to become a member of a DCDL-net a terminal shall subscribe to the MASTER;
- the obtain access rights procedure shall be used to provide the PARK, PLI and IPUI; RFPI, as well as, the IdN and the TPUIs may be derived from this information;

- the location registration procedure shall be used to provide LAL, it may be used to assign the TPUI but it can be as well automatically extracted from the IPUI instead; if TPUI is assigned during location registration this shall overwrite any derived TPUI;
- if provision of encryption is supported after, subscription is accomplished, both terminals shall establish a DCK, shall cipher the link and all common for the DCDL-net keys shall be after that provided by the master to the applicant over this ciphered link - parameter retrieval procedure shall be used; parameter retrieval procedure may be used for assignment of a RFPI as well in this case the assigned value shall overwrite any derived value;
- parameter retrieval procedure shall be used for provision to the applicant of information for all DCDL-net members. If encryption is provided this procedure shall be performed over an encrypted link;
- the DCDL-net's CSDB may be re-established on user request; the MASTER shall perform modification of user parameters procedure to all members; this action should be performed with care as not all members may be active at this moment and the change may make them implicitly excluded from the DCDL-net.

1.2.3 Communication

A Terminal that wants to participate in a DL-net that supports distributed communication shall behave as follows:

- only members of a DCDL-net can communicate within the DCDL-net;
- to become a member, a terminal (behaving as a PT) shall request access rights from the MASTER of the DCDL-net; during the assignment of the membership access rights the applicant shall be allocated all necessary subscription data; its own data shall become part of the CSDB; shall obtain information for all members of the DCDL-net (independent of whether they are currently active or not);
- if a terminal is a member of a DCDL-net when it is powered-up, or switched to search for a DCDL-net MASTER it shall synchronize to the current MASTER (frame and multiframe numbers, PSCN, etc.) and shall constantly from this point of time on update its information as which member is currently active and may be accessed;
- shall announce itself to the MASTER as being active and thereby accessible;
- shall start listening for Paging, and, may start listening to all slots for a direct link establishment;
- if a terminal recognizes a specific Paging message that contains its TPUI and the Id of another terminal, it shall initiate direct link establishment to that terminal behaving as a FT in a Direct FT initiated link establishment procedure as specified in clause 14.2.4;
- if the User of a terminal wants to initiate a call and the desired terminal is currently active the User's terminal shall attempt a direct link establishment if this fails it shall request the MASTER to transmit a Paging to the desired terminal; if the desired terminal is not currently active the user shall not initiate this procedure.

It should be preferable that every active HyP terminal constantly listen to all frames thereby direct link establishment towards this terminal shall always succeed. However to allow some terminal to be part of the DCDL-net which due to power consumption would favour low duty cycle mode a special paging procedure need to be applied when such terminals need to be accessed being in low duty cycle mode.

There may be cases when direct communication between two members will not be possible, e.g. though the distance between each of them to the MASTER is acceptable, the distance between them does not allow communication. In such case the only possible way for communication will be via the MASTER.

NOTE: See clause I.5 for graphic representation of some of the communications scenarios.

I.3 Procedure description

I.3.1 HyP Identities

A HyP shall be assigned by the manufacturer a RFPI and an IPEI which should represent the two sides of the HyP.

The IPUI-N (equal to IPEI) shall be used by the HyP to request membership access rights from the DCDL-net MASTER; the RFPI may be used by the HyP for the DCDL-net ARI if a new DCDL-net is to be established and this HyP is been allocated by the user to be the MASTER, see clause I.3.10.2.

I.3.2 Membership Access Rights Allocation

For the Membership Access Rights Allocation procedure the normal DECT Obtain access Rights procedure shall be used, see clause 13.5.

The applicant shall provide its capabilities description indicated in a <<Terminal capability>>, a <<Set-up capability>> and an <<IWU-TO-IWU>> information elements included into the {ACCESS-RIGHTS-REQUEST} message.

Table I.1: Values for capability description used within the {ACCESS-RIGHTS-REQUEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Set-up capability>>			As defined in the present document or an applicable profile
<<Terminal capability>>			As defined in the present document or an applicable profile
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
	<Command/Action>	0001	Capabilities
	<Length of Contents>>	All	
	<Terminal type>	Any relevant	See clause I.4.2
	<Extended capabilities>	Any	Any relevant, see clause I.4.2
	<Terminal data>	RFPI	If the subscribing terminal is a HyP terminal that can play the role of a MASTER it shall provide its RFPI which shall be later use in case this terminal is assigned as a new master. The information provided shall be in the form of complete <<Fixed Id>> information elements as specified in clause 7.7.18, see clause I.4.2 as well

With the {ACCESS-RIGHTS-ACCEPT} message the Applicant shall be assigned a DCDL-net related PARK, IPUI and PLI according to the values allocated for this DCDL-net. All other DCDL-net terminal specific values shall be extracted from these values. For the applicable rules see clause I.3.10.

Following immediately the Obtain access rights procedure a Location registration shall be performed and the terminal shall be assigned a LAL. This procedure shall indicate to the MASTER that the new member is accessible (i.e. the procedure shall be used with the meaning of an ATTACH procedure).

The procedure may be used to assign TPUI as well. If so used the TPUI shall be assigned according to the values allocated for this DCDL-net, see clause I.3.10.

If DCK (Encryption) is supported, a Store DCK procedure shall take place establishing a temporary (non DCDL-net) DCK. If this key was established for the first time in the DCDL-net life (i.e. the MASTER does not have a record for such key being ever established) this key should be used as a Static CK (SCK) for this DCDL-net for further ciphering procedures. Instead the MASTER may choose to derive a SCK based on some proprietary secure enough algorithm.

As soon as a SCK is available the MASTER shall provide it to the applicant always over a ciphered link (for encrypting this link the temporary DCK shall be used). The key shall be delivered to the applicant using the Parameter retrieval procedure described in clause I.3.4.

The DCDL-net system SCK may be recalculated on user request in order to provide sufficient system security - such procedure shall be MASTER originated.

I.3.3 Re-initialization of membership access rights

The DCDL-net membership access rights and hence the CSDB may be re-initialized at any time on user request or predefined periodic update procedure.

The MASTER should advice every member to initiate a new Membership Access Rights procedure during which the allocated DCDL-net related values can be assigned new. The FT initiated On air modification of user parameters by performing a FT initiated Parameter retrieval procedure as described in clause 13.7 and indicating in the <<Info type>> "access rights modify suggest".

I.3.4 Members Data Transfer

When membership access rights have been allocated to an applicant the MASTER shall provide the new member with information for the other members and their capabilities. The FT initiated parameter retrieval procedure shall be used as described in clause 13.7.

If encryption is provided the members data transfer procedures shall take place over a ciphered link.

The information related to every member shall include:

- the IdN of the member - all DCDL-net subscription related data for particular member may be derived from its IdN, see clause I.3.10;
- the member capability as provided in the {ACCESS-RIGHTS-REQUEST} message during the membership subscription including the <<Terminal capability>>, the <<Set-up>> capability and specific device information as provided in the <<iwu-to-iwu>>.

Table I.2: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	1	
	<ext>	1	
	<Parameter type>	0100101	Distributed communication download
<<Repeat indicator>>			Optional to use from the MASTER to provide information for number of members in one message. Mandatory to understand from the applicant/member
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
	<Command/Action>	0001	capabilities as provided by the <<iwu-to-iwu>>
	<Length of Contents>>	All	Determines whether the <Terminal data> field is included or not
	<Terminal type>	Any	Any relevant, see clause I.4.2
	<Extended capabilities>	Any	Any relevant, see clause I.4.2
	<Terminal Id>	All	IdN-Mean to distinguish different terminals
	<Terminal data>		
		<<Terminal Capability >>	The complete information element as received during subscription
		<<Set-up capability>>	The complete information element as received during subscription
		<<Fixed Id>>	If the subscribing terminal is a HyP terminal that can play the role of a MASTER its RFPI shall be provided and may later be used in case this terminals is assigned as a new master

This procedure may be used to provide as well RFPI or/and TPUIs by including the corresponding information elements <<Fixed Id>> or/and <<Portable Id>> as defined in clauses 7.7.18 and 7.7.30 respectively, into the <Terminal data> field. The values assigned shall be in accordance with the rules provided in clause I.3.10 and if assigned shall overwrite any derived value.

As a fall back the Members Data Transfer procedure may be used by all members to refresh their information on the available members by requesting update from the MASTER. For these purposes the PT initiated parameter retrieval procedure shall be used.

Table I.3: Values used within the {MM-INFO-REQUEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	00000001	
	<ext>	1	
	<Parameter type>	0100101	Distributed Communication download
<<IWU-TO-IWU>>			This information element need to be included only if information for particular member is required as indicated in the <Terminal Id> field If it is not included the request shall be understood as request for information for all DCDL-net members
	<S/R>	1	Transmission of message
	<Protocol discriminator>	0100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
	<Command/Action>	0001	capabilities
	<Length of Contents>>	All	Determines whether the <Terminal data> field is included or not
	<Terminal type>	Any	Any relevant, see clause I.4.2
	<Extended capabilities>	Any	Any relevant, see clause I.4.2
	<Terminal Id>	All	IdN - Mean to distinguish different terminals

I.3.5 Presence/Absence Indication

A member shall indicate the MASTER whether it is accessible or not.

To indicate that it is accessible the attach (location registration) procedure shall be used.

To indicate that it is inaccessible the detach procedure shall be used.

I.3.6 Bandwidth management

When a member would like to establish a call to another member all DCDL-net bandwidth may be in use from other members or may not be sufficient for satisfactory grade of service.

To acquire some bandwidth the member shall request assistance from the MASTER.

On receipt of a bandwidth management assistance request, the MASTER shall broadcast a connectionless message to all involved in communications terminals requiring bandwidth reduction and providing maximum time during which the freed bearers shall not be re-targeted. All communicating terminals, providing that sufficient bandwidth is available to maintain the communication, shall reduce the number of used bearers in number equivalent to a duplex bearer (a peer of bearers 12 slots apart). The freed bearers may be re-targeted for use after the allocated duration time expires.

During this time the member which intended to establish the call may do it using the freed slots.

To requests bandwidth management assistance from the MASTER the terminal in need shall send a {CLMS-VARIABLE} message to the MASTER utilizing the unused half of the double slot on which the System Control Bearer is transmitted according to the rules in EN 300 175-3 [3]. To reduce the time limits of transmission enforced by the MAC layer CL protocol, the usage of CLF channel is recommended.

Table I.4: Values used within the {CLMS-VARIABLE} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Portable Id>>			"0" length
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	0100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
	<Command/Action>	1001	Reduce number of bearers
	<Length of Contents>>	00000001	
	<Terminal type>	00000000	Unknown
	<Extended capabilities>	00000000	
	<Terminal Id>	All	IdN of the sender

After reception of this request the MASTER shall request all or a set of involved in communication members to reduced the number of used bearers by sending a {CLMS-FIXED} message.

Table I.5: Values used within the {CLMS-FIXED} message for bandwidth change

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		011	One section/Bit stream
<<Address>>		Any	Lowest 16 bits of connectionless TPUI when one HyP is addressed, or, the last 16 bits of the CBI, see EN 300 175-6 [6] clause 6.3.1 when all the HyPs are addressed
<<Protocol Discriminator>>	<Identifier>	0001	Distributed Communications
	<Command/Action>	1001	Reduce number of bearers
<<Data>>		Any	Time limit during which increase of number of used bearers is not allowed 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 EN 300 175-3 [3]. 1 unit = 28 multiframes

Whenever a terminal that is involved in communication receives this message, and, the received Connectionless TPUI matches one of the terminal's Connectionless TPUIs the Terminal shall try to reduce the number of bearers it is currently using.

At some cases however, reduction may not be possible - e.g. the lowest numbers of bearers necessary for maintaining the communication have been used. In such a case the terminal may decide to enforce a suspend procedure (if possible), or, need not to reduce the number of used bearers.

1.3.7 Direct Link Establishment

At any time an active member may initiate direct link establishment by a bearer establishment procedure as the bearer request may be placed in any slot.

For establishing a new link a HyP may use the PT initiated bearer establishment procedure as defined in EN 300 175-3 [3]. During the existence of a link the roles of the involved terminals shall be as allocated at the beginning of the link establishment.

A terminal should not attempt bearer establishment with a member that is not indicated as being currently active.

A bearer establishment may fail even the called terminal has been indicated as currently active, e.g. the called terminal is in low duty cycle mode. In such case the Indirect Link Establishment procedure should be used as described in clause I.3.8. In any case when a HyP is listening for direct link establishment it shall listen for request on any slot.

NOTE: It may happen that though 2 terminals have registered to the MASTER they still cannot establish direct communication, e.g. due to range problems when both are at opposite sides of the MASTER. In such case normally few failures of direct communication should lead to attempt of communication through the MASTER (internal call).

A MASTER may use paging for the purpose of establishing communication with another member of the DCDL-net.

I.3.8 Indirect Link Establishment

If a direct link establishment procedure to a particular terminal has failed the calling terminal shall request assistance from the MASTER by issuing a connectionless up-link request providing the IdN of the targeted terminal, as well as, its own Id.

Table I.6: Values used within the {CLMS-VARIABLE} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Portable Id>>			"0" length (see note)
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	0100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
	<Command/Action>	1010	Page assistance
	<Length of Contents>>	00000001	
	<Target Terminal Id>	All	IdN of the intended for connection terminal
	<Initiator Terminal Id>	All	IdN of the seeking connection terminal
NOTE: Inclusion of Portable Identity with length "0" is introduced in order to reduce the total length of the message. By this and adding the second Terminal Id the gain is 4 octets less length of the message compare to the case of providing the Caller Id in the portable identity information element.			

To reduce the time limits of transmission enforced by the MAC layer CL protocol, see EN 300 175-3 [3] the usage of CLF channel is recommended. The slot used for the transmission should be the reverse half of the DCDL-net System Control Bearer.

A terminal shall not initiate this procedure if the desired terminal is not indicated as currently available in the Active Members List distributed by the MASTER.

On receipt of the request the MASTER shall send a Connectionless message indication to the called terminal providing the IdN of the calling terminal. If the called terminal is not available the MASTER should ignore the request.

Table I.7: Values used within the {CLMS-FIXED} message one segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		011	One section/Bit stream
<<Address>>		Any	Lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Identifier>	0001	Distributed Communications
	<Command/Action>	1011	Direct link establishment
<<Data>>		Any	IdN of the terminal that requested the assistance - the receiver shall use this to identify to which terminal to initiate a direct link establishment

The called terminal should initiate direct link establishment to the calling terminal. As it may not be for whatever reason capable of doing this, the initiating terminal should not wait forever. It may repeat the procedure maximum 3 times and in case of all 3 attempts have failed the user should be informed for the call attempt failure.

I.3.9 MASTER management

I.3.9.1 MASTER assign

For setting up a DCDL-net a MASTER terminal is needed which shall transmit a System Control Bearer. The User shall ensure that a MASTER is available which MASTER shall start transmission of such a bearer on User request for setting-up a DCDL-net. The invocation of MASTER assign procedure is not specified and is left to the implementers assuming that User intervention shall be always required.

If a DCDL-net has been already set-up, however, during a reasonable time a member of a DCDL-net terminal cannot find the DCDL-net System Control Bearer proper indication shall be provided to the User of the terminal.

The DCDL-net System Control bearer shall be a connectionless bearer due to the fact that the DCDL-net system information it transmitted in connectionless messages.

If a member of DCDL-net has been assigned as MASTER this shall be responsible for the transmission of the Connectionless DCDL-net system bearer. This bearer shall be present if at least one member of a DCDL-net is active.

Establishment and maintenance of this bearer shall be done in accordance to the requirements of the EN 300 175-3 [3].

I.3.9.2 MASTER Change

If a MASTER is to leave the DCDL-net it should allocate any of the currently active members as its successor. Alternatively, complete re-initialization of the DCDL-net may be done, i.e. desubscribing and subscribing to a new MASTER.

For the MASTER assignment of new MASTER procedure, a connectionless message shall be sent.

Table I.8: Values used within the {CLMS-FIXED} message one segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		011	One section/Bit stream
<<Address>>		Any	Lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Identifier>	0001	Distributed Communications
	<Command/Action>	1100	master change
<<Data>>		Any	IdN of the terminal that is assign as new MASTER - the receiver shall use this to identify to which RFPI it needs to lock and shall modify the DCDL-net System ARI

The current MASTER shall start a timer and shall monitor the air for a new System Control Bearer establishment - a value of 4 seconds is recommended. When such is found the current MASTER shall inform all active members for the change of the bearer position and shall close its activities-"connectionless or dummy bearer position" shall be used.

If during this time no new System bearer is found the MASTER shall request another active member to undertake its responsibilities.

I.3.9.3 DCDL-net System bearer management

The System bearer shall be a connectionless bearer as defined in EN 300 175-3 [3].

In addition to the information normally transmitted when no additional dummy bearer is available, the MASTER shall transmit specific DCDL-net members related information in regular intervals - it is recommended that the first segment of this message occurs every 4 seconds.

Table I.9: Values used within the {CLMS-FIXED} message 1st segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		100	Multiple sections/Bit stream
<<Address>>		Any	Lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Identifier>	0001	Distributed Communications
	<Command/Action>	1101	active members list
<<Length Identifier>>		Any	Indicates implicitly the number of data sections to follow

Table I.10: Values used within the {CLMS-FIXED} message 2nd segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		0	Data section
<<CLMS header>>		000	Data section number - 0 (1st)
<<DATA/Fill>>		IN1	IdN number of an active terminal
		IN2/Fill	IdN number of an active terminal
		IN3/Fill	IdN number of an active terminal
		IN4/Fill	IdN number of an active terminal

Table I.11: Values used within the {CLMS-FIXED} message k segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		0	Data section
<<CLMS header>>		k	Data segment (k+1)
<<DATA/Fill>>		IN4k+1	IdN number of an active terminal
		IN4k+2/Fill	IdN number of an active terminal
		IN4k+3/Fill	IdN number of an active terminal
		IN4k+4/Fill	IdN number of an active terminal

I.3.10 Common Subscription Database management

I.3.10.1 IdN

Each member of a DCDL-net shall be assigned an Identity Number (IdN) which shall be of 8 bits length thereby providing 255 distinguishable numbers for 255 possible members of a DCDL-net.

I.3.10.2 RFPI, PARK and PLI

A DCDL-net is recognized by an ARI, a Common PARK and number of Members specific RFPIs.

For allocation of DCDL-net Common PARK and Members specific RFPIs, a DCDL-net System ARI shall be used. This shall be a unique ARI of this DCDL-net which shall be broadcasted by the MASTER and used for locking and obtaining system information. The ARI of the MASTER as assigned during manufacturing shall be used to guarantee its uniqueness.

For a given DCDL-net ARI the following rules in accordance to EN 300 175-6 [6] shall apply:

- the DCDL-net PARK should equal this ARI;
- for one cell systems or systems in which inter-cell handover is not foreseen the members specific RFPIs shall be based on an ARI that equals the DCDL-net ARI, the E bit should be set to 0 and the RPN shall equal the member's IdN (this means that if the RPN in use is only of 3 bits length the assignment of the IdN shall reflect this limitation and the unused MSB shall be set to 0);

- for multi-cell systems (determined by multi RFPs MASTER) with inter-cell handover care shall be taken during allocation providing that the MASTERS RFPs are assigned with IdNs allowing inter-cell handover and being still unique (e.g. not repeating a member IdN). See as well clause I.3.11.

NOTE: For further extension of the present document assignment of a per Member specific DCDL-net Cell Locator may be foreseen to allow Members to be multi-cell systems as well.

PLI should be assign to cover the PARI and to exclude the RPN.

I.3.10.3 IPUI

For the member specific IPUIs the IPUI type O as specified in EN 300 175-6 [6], clause 6.2.3 should be used.

Different Numbers shall be assigned to every member of the DCDL-net, these numbers shall be used to identify every particular member and provide means to derive all subscription related data.

For the assignment of these numbers the following rule apply: the 8 least significant bits shall be the IdN number and they shall be unique within the DCDL-net. The rest of the bits shall be set to "0".

I.3.10.4 TPUI and LAL

The LAL assigned during Location registration should be the same throughout the entire DCDL-net.

The individual assigned TPUI shall equal the IdN of the particular terminal with most significant bits following the rules of EN 300 175-6 [6] for individual assigned TPUI.

To perform all connectionless operations the MASTER shall assign Connectionless TPUIs to each member that equal the member's IdN with most significant bits following the rules of EN 300 175-6 [6].

I.3.10.5 Keys

A common AC shall be allocated to the DCDL-net by the user and shall be used during subscription and throughout the intra DCDL-net communication whenever authentication between two members is performed.

If encryption is supported a Static CK shall be allocated to the DCDL-net during the first subscription. Establishment of this key should be based on a Store DCK procedure performed using the AC, other proprietary establishment of this key may be applied by the MASTER as well. The resulted key shall be the SCK used by the DCDL-net for further communication.

I.3.11 Handover issues

The MASTER may decide to change the position of the System Control Bearer. The new position shall be announced. As the new position may overlap with a slot on which there is ongoing communication between two members of the DCDL-net, as soon as these members receive the new System Control Bearer slot position they should attempt to move their communication to another slot by performing bearer replacement or a bearer handover for the bearer(s) which will overlap.

I.4 Elements of Messages/Information Elements

This clause specifies in details the complete contents of the messages/information elements used by the Distributed Communication Protocol which are based on the general information elements description as specified earlier in clauses 7.7 and 8.3 and add specific Distributed Communication content.

I.4.1 CLMS-FIXED

Table I.12: Values used within the {CLMS-FIXED} message one segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		011	One section/Bit stream
<<Address>>		Any	Lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Identifier>	001	Distributed Communications
	<Command/Action>	1001	Reduce number of bearers
		1010	Page assistance
		1011	Direct link establishment
		1100	Master change
		1101	Active members list
<<Data>>		Any	Contents depends on the <Command/Action> field as described in relevant clause in the present document

For constructing a multi-section {CLMS-FIXED} message the rules as defined in clause 8.3 apply.

I.4.2 IWU-TO-IWU

Table I.13: Values used within the <<IWU-TO-IWU>> Information element for <Command/action> set to "capabilities"

information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			Preceding octets as defined in clause 7.7.23
	<ext3>	1	
	<S/R>	1/0	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
		0000	PP Information
		0010	FP Information
	<Command/Action>	0001	Capabilities
	<Length of Contents>>	All	
	<Terminal type>	00000000	Unknown
		00000001	PC
		00000010	Printer
		00000011	Scanner
		00000100	Digital Camera
		00000101	Modem
		00000110	Palmheld
		00001000	Voice
		00001001	External line connector (e.g. an ISDN base)
		***	More to be defined
	<Extended capability>		A bit mask
		xxxxxxx1	The device is able to perform internal calls
		xxxxxxx1x	The device is able to perform more than on simultaneous calls
		xxxxx1xx	The device provides access to external line
	<Terminal Id>	All	IdN of the concerned terminal - depends on the values indicated into the <Discriminator type> and the <Command/Action>
	<Terminal data>		The information provided shall be in the form of complete information elements as specified in clause 7.7, e.g. <<Terminal capability>>, <<Key>>, <<Portable Identity>>, <<Fixed Identity>>, etc.

Table I.14: Values used within the <<IWU-TO-IWU>> Information element for <Command/action> set to "Page Assistance"

information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	0100011	Terminal Data
	<Discriminator Type>	0001	HyP Information
		0000	PP Information
	<Command/Action>	1010	Page assistance
	<Length of Contents>>	00000001	
	<Target Terminal Id>	All	IdN of the intended for connection terminal
	<Initiator Terminal Id>	All	IdN of the seeking connection terminal

I.4.3 Info-type

Table I.15: Values used within the <<Info type>> Information element

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	00000001	
	<ext>	1	
	<Parameter type>	0100101	Distributed Communication download

I.4.4 CLMS-VARIABLE

The {CLMS-VARIABLE} shall be constructed in accordance to the requirements of clause 6.3.5.1. The mandatory information elements are indicated in table I.16.

Table I.16: Values used within the {CLMS-VARIABLE} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Portable Id>>			contents as specified in the related procedure
<<IWU-TO-IWU>>			contents as specified in the related procedure

I.5 Examples

I.5.1 General

To ease understanding this clause provides some examples.

For these examples the following basic user configuration is used:

- there are two PCs - PC_1 and PC_2 which are connected to a HyP terminals each;
- there is a Printer connected to a HyP terminal, here called "Print";
- there is a Scanner connected to a HyP terminal, here called "Scan";
- there is a Digital Camcorder connected to a HyP terminal, here called "D-Cam";

- there is a GAP voice Portable, here called "Handy";
- there is a Base Station called in here "Switch" (a HyP terminal from type External Line Connector) connected to an external line;
- there is Palmheld computer (organizer, etc.) connected to a HyP terminal, here called "PalmH".

A DCDL-net has been set-up comprising all the eight DECT terminals. The Switch has been assigned as the MASTER of this DCDL-net. Consequently the Switch is transmitting the DCDL-net System Control Bearer. When powered-on all terminals (except the Switch) locked to the MASTER, synchronize, obtain all information relevant to this DCDL-net (e.g. which are the present members, etc.) and are able to set-up connection directly to desired member of the DCDL-net.

1.5.2 Example 1

In this example all except the Handy and the Switch (MASTER) terminals are switched-off. The Handy is performing a voice session through the Switch and the External network to a far-end terminal.

Using the existing spectrum of 240 slots:

- the Master is transmitting the System Control Bearer occupying a connectionless bearer - 2 slots;
- the session between the Handy and the Switch is occupying 2 slots (a duplex channel).

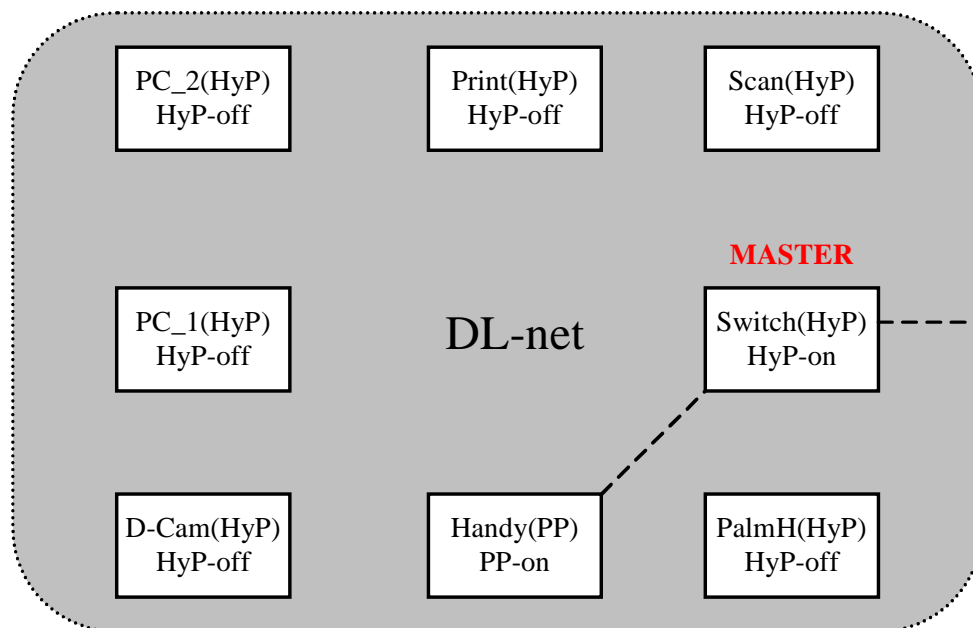


Figure I.1: DL-net - only voice communication enabled - Handy locked to Switch

1.5.3 Example 2

In this scenario the Handy is continuing its Voice session, and, all the rest of the terminals have been switched-on.

Using the existing spectrum of 240 slots:

- the Master is transmitting the System Control Bearer occupying a connectionless bearer - 2 slots;
- the session between the Handy and the Switch is occupying 2 slots (a duplex channel);
- PC_2 is printing having a direct communication with the Printer using let us say 1 duplex and 2 simplex bearers (4 slots);
- the D-Cam is uploading images to PC_1 using another 4 slots (1 duplex and 2 simplex bearers).

All in total 12 slots are in use. For comparison, if all the links had to be performed through the Switch (a FP) 20 slots should have been in used.

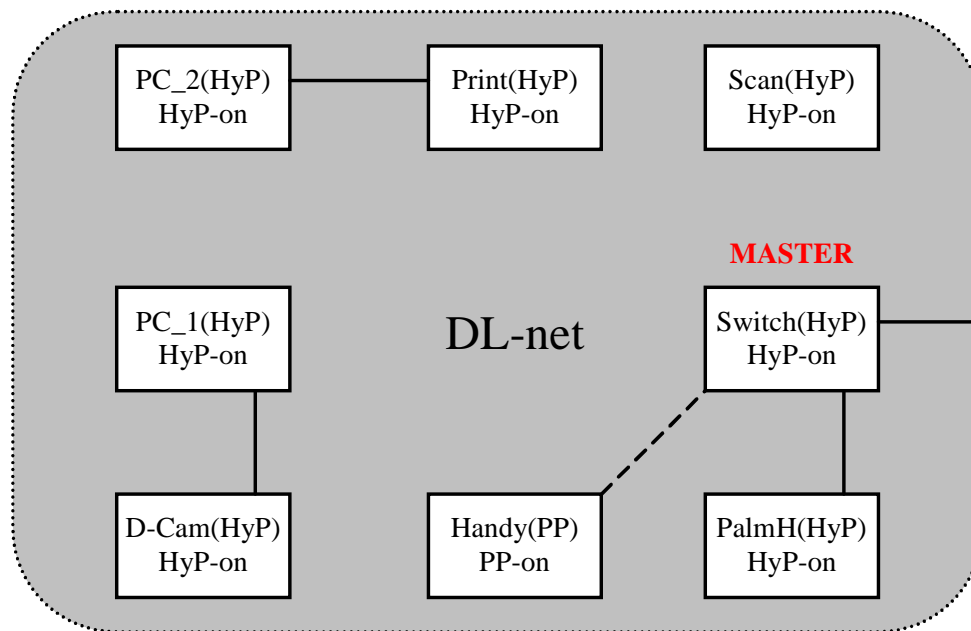


Figure I.2: DL-net communication - PC_2 prints; D-CAM uploads to PC_1; Handy locked to Switch; PalmH gets mails; Scan inactive

I.5.4 Example 3

In this scenario the Handy is continuing its Voice session, PC_2 is still printing, and, all the rest of the terminals have been switched-on.

PC_1 has established a direct link to the Print as well.

Using the existing spectrum of 240 slots:

- the Master is transmitting the System Control Bearer occupying a connectionless bearer - 2 slots;
- the session between the Handy and the Switch is occupying 2 slots (a duplex channel);
- a session between the PalmH and the Switch is occupying 2 slots (e.g. Internet session in parallel to a voice one for Switch connected to ISDN);
- PC_2 is printing having a direct communication with the Printer using let us say 1 duplex and 2 simplex bearers (4 slots);
- the PC_1 is printing using another 4 slots (1 duplex plus 2 simplex bearers);
- Print, as well as, Switch are handling two parallel links.

All in total 14 slots are in use. For comparison, if all the links had to be performed through the Switch (a FP) 22 slots should have been in used.

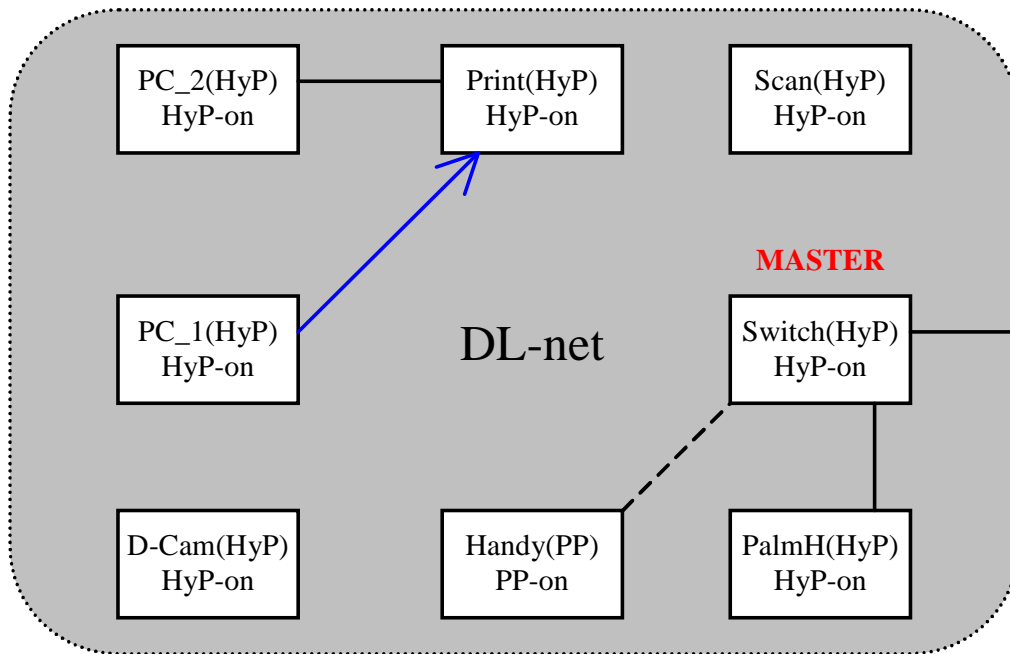


Figure I.3: DL-net communication - PC_2 prints; PC_1 prints (direct link establishment); D-CAM inactive; Handy locked to Switch; PalmH gets mails; Scan inactive

I.5.5 Example 4

In this scenario the Handy is continuing its Voice session, PC_2 is still printing and all the rest of the terminals have been switched-on.

In this special example PC_1 has not been able to successfully perform the direct link establishment procedure to Print (e.g. after being engaged with PC_2 Print does not listen to other bearer establishment attempts).

PC_1 has requested assistance from the MASTER in achieving the communication to the Print. The MASTER has sent a CL message to the Print requesting it to communicate to PC_1. Print has not miss it as it is required to listen to the System Control Bearer on which the indication was transmitted.

Finally, Print has establish link to PC_1 and PC_1 is able to print.

Using the existing spectrum of 240 slots:

- the Master is transmitting the System Control Bearer occupying a connectionless bearer - 2 slots;
- the session between the Handy and the Switch is occupying 2 slots (a duplex channel);
- a session between the PalmH and the Switch is occupying 2 slots (e.g. Internet session in parallel to a voice one for Switch connected to ISDN);
- PC_2 is printing having a direct communication with the Printer using let us say 1 duplex and 2 simplex bearers (4 slots);
- the PC_1 is printing using another 15 slots (1 duplex plus 13 simplex);
- Print as well as Switch are handling two parallel links.

All in total 25 slots are in use. In order to work this scenario requires from the involved terminals usage of some same slots on different frequencies which will be possible depending on the location of the terminals.

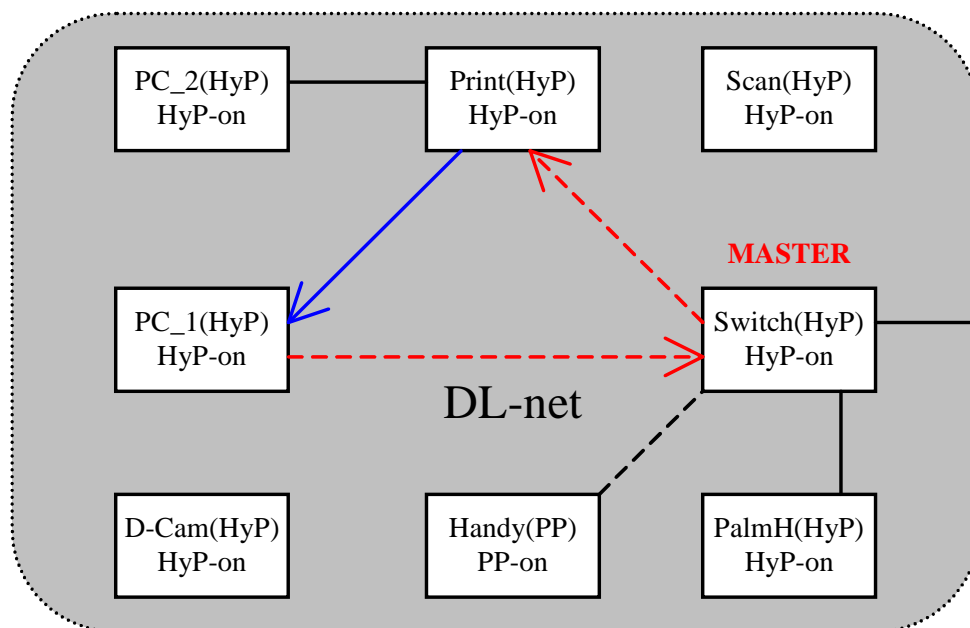


Figure I.4: DL-net communication - PC_2 prints; PC_1 prints (Indirect link establishment); D-CAM inactive; Handy locked to Switch; PalmH gets mails; Scan inactive

I.6 Usage of PPs or FPs in DCDL-net

I.6.1 General

Apart from HyPs terminals, normal PPs and FPs can become members of a DCDL-net.

Such terminals need to support some of the procedures described earlier in the present document. This clause describes the necessary requirements.

I.6.2 Requirements to FPs

I.6.2.1 General

A FP can be a member of a DCDL-net only in the role of a MASTER. To operate as MASTER a FP shall support the procedures as indicated in table I.17.

Table I.17: Support of DCDL-net procedures for a member of type FP

Procedure	Support	Comments
Membership Access Rights Allocation	YES	The MASTER related issues
Re-initialization of membership access rights	YES	The MASTER related issues
Members Data Transfer	YES	The MASTER related issues
Presence/Absence Indication	YES	To understand and handle initiation of this
Bandwidth management	YES	The MASTER related issues
Direct Link Establishment	OPTIONAL to initiate MANDATORY to response	The MASTER related issues
Indirect Link Establishment	YES	The MASTER related issues
MASTER management - MASTER assign	YES	The MASTER related issues
MASTER management - MASTER Change	YES	The MASTER related issues
MASTER management - DCDL-net System bearer management	YES	The MASTER related issues
Common Subscription Database management - RFPI, PARK and PLI	YES	The MASTER related issues
Common Subscription Database management - IPUI	YES	The MASTER related issues
Common Subscription Database management - TPUI and LAL	YES	The MASTER related issues
Common Subscription Database management - Keys	YES	The MASTER related issues

Modification to this procedure wherever required are described in the following clauses.

I.6.2.2 Members Data Transfer

The requirements as in clause I.3.4 shall apply with the following modification.

A FP can be distinguished from a HyP by the indication in the <Discriminator type>.

Table I.18: Discriminator type for PP

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			
	<Discriminator Type>	0010	FP Information

I.6.2.3 Direct Link Establishment

The requirements as in clause I.3.7 shall apply.

I.6.3 Requirements to PPs

I.6.3.1 General

A PP can be a member of a DCDL-net but not in the role of a MASTER. To operate as a member a PP shall support the procedures as indicated in table I.19.

Table I.19: Support of DCDL-net procedures for a member of type PP

Procedure	Support	Comments
Membership Access Rights Allocation	YES	The NON MASTER related issues
Re-initialization of membership access rights	YES	The NON MASTER related issues
Members Data Transfer	YES	The NON MASTER related issues
Presence/Absence Indication	YES	To be able to announce presence/absence
Bandwidth management	YES	The NON MASTER related issues
Direct Link Establishment	MANDATORY to initiate and response	The NON MASTER related issues
Indirect Link Establishment	YES	The NON MASTER related issues
MASTER management - MASTER assign	YES	The NON MASTER related issues, e.g. understanding and reacting properly to the MASTER behaviour
MASTER management - MASTER Change	YES	The NON MASTER related issues, e.g. understanding and reacting properly to the MASTER behaviour
MASTER management - DCDL-net System bearer management	YES	The NON MASTER related issues, e.g. understanding and reacting properly to the MASTER behaviour
Common Subscription Database management - RFPI, PARK and PLI	YES	The NON MASTER related issues, e.g. to manage the assignment/usage of related identities
Common Subscription Database management - IPUI	YES	The NON MASTER related issues, e.g. to manage the assignment/usage of related identities
Common Subscription Database management - TPUI and LAL	YES	The NON MASTER related issues, e.g. to manage the assignment/usage of related identities
Common Subscription Database management - Keys	YES	The NON MASTER related issues, e.g. to manage the assignment/usage of related keys

Modification to this procedure wherever required are described in the following clauses.

I.6.3.2 Membership Access Rights Allocation

The requirements as in clause I.3.2 shall apply with the following modification.

The PP shall indicate that this is a PP.

Table I.20: Values for capability description used within the {ACCESS-RIGHTS-REQUEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			
	<Discriminator Type>	0000	PP Information

I.6.3.3 Members Data Transfer

The requirements as in clause I.3.4 shall apply with the following modification.

A PP can be distinguished from a HyP by the indication in the <Discriminator type>:

Table I.21: Discriminator type for PP

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			
	<Discriminator Type>	0000	PP Information

I.6.3.4 Direct Link Establishment

The requirements as in clause I.3.7 shall apply with the following modification.

Normal PPs cannot initiate direct communication to another DCDL-net member. Such PTs may initiate call to another member either via the MASTER (internal call) or if they support the procedure for requesting assistance from the MASTER this can be used to indicate to the relevant terminal to start direct link to this PT.

I.6.3.5 Indirect Link Establishment

The requirements as in clause I.3.8 shall apply with the following modification.

A PP can be distinguished from a HyP by the indication in the <Discriminator type>.

Table I.22: Discriminator type for PP

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<IWU-TO-IWU>>			
	<Discriminator Type>	0000	PP Information

Annex J (normative): Scrolling Behaviour

Scrolling Behaviour Types 1 and 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.

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 summarized in table J.1.

Table J.1: Scrolling behaviour types

	Scrolling behaviour type = 1	Scrolling behaviour type = 2
Single line display	scroll by character	scroll by page (see above)
Multi line display	scroll by line	scroll by page

A PT display which scrolls may set its window origin as shown in table J.2. The first stored character is character 1.

Table J.2: PT display window origin settings

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 carried out 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 (normative): Additional information on Message Elements

K.1 Detailed description of the different connection types as defined by the IE <Connection Attributes>

K.1.1 General

The following clause describes the different connection types possible in DECT and that are relevant for the coding of the Information Element <Connection Attributes> (see clause 7.7.11).

The term "connection type" in the context of this IE refers to the number of bearers and type of them that may be used by the connection. It is a property of the connection defined at MBC (Multi Bearer Control) level and is represented by means of a connection type indicator and four parameters: maximum number of bearers downstream, minimum downstream, maximum upstream and minimum downstream. The connection type is negotiated by means of Network layer messages.

K.1.1.1 Real number of bearers "on the air"

The real number of bearers "on the air" depends on the connection type definition parameters, but may be also influenced by other factors:

- In packet-mode connections (DPRS), the number, type and direction of the bearers depend on dynamic ME decisions, that are also dependant on instantaneous traffic demands.
- In any case, it is influenced by the available resources (bearers) and the physical feasibility to setup and keep them active.

The connection type indicator defines a range or an area of allowable combinations for the instantaneous number of bearers "on the air".

K.1.1.2 Definitions (applicable to all connection types)

For the purpose of describing the different types of connections, the following notations are used:

- u: current value of the number of (simplex) bearers upstream;
- d: current value of the number of (simplex) bearers downstream;
- u₀: Minimum number of (simplex) bearers upstream (u₀ ≥ 1);
- d₀: Minimum number of (simplex) bearers downstream (d₀ ≥ 1);
- U₀: Maximum number of (simplex) bearers upstream (U₀ ≥ u₀);
- D₀: Maximum number of (simplex) bearers downstream (D₀ ≥ d₀);
- U₁: Maximum number of (simplex) bearers upstream when d = d₀ (U₀ ≥ U₁ ≥ u₀);
- D₁: Maximum number of (simplex) bearers downstream when u = u₀ (D₀ ≥ D₁ ≥ d₀).

NOTE 1: Parameters u₀, and d₀ always correspond to the fields defined in octets 4a and 4c, respectively. For some connection types, d₀ is not transmitted if equal to u₀ or equal to "1".

NOTE 2: According to connection type, octets 4 and 4b either correspond to (U_0 , D_0) or to (U_1 , D_1). For some connection types, $U_0 = U_1$ and/or $D_0 = D_1$.

NOTE 3: Parameters u and d always meet DECT system-wide conditions ($u+d$ even; $u+d \leq$ total number of slots for the given slot type).

For all connection types, the values of all number of bearers parameters shall take into account the intrinsic limitations of DECT; in particular, that the number of simplex bearers should be even.

K.1.2 Types of connection

K.1.2.1 Symmetric only connections

A **Symmetric only** connection shall only use duplex bearers. As a consequence, maximum (resp. minimum) number of (simplex) bearers upstream and downstream are identical ($U_0 = D_0$, $u_0 = d_0$).

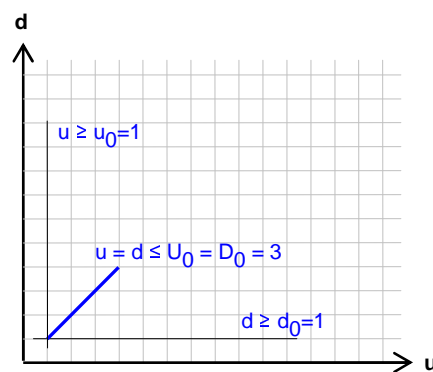


Figure K.1: Segment of authorized values for (u,d) in case of symmetric connection (example)

Octets 4, 4a shall be transmitted and shall contain (U_0 , u_0) respectively. Octets 4b and 4c shall not be transmitted.

NOTE: Symmetric only connections can be used with DPRS and other profiles.

K.1.2.2 Asymmetric frozen connections

An **Asymmetric frozen connection** can use:

- duplex bearers;
- double simplex bearers in one direction only (upstream or downstream).

Octets 4, 4a, 4b, and 4c shall all be transmitted and shall contain (U_0 , u_0 , D_0 , d_0) respectively.

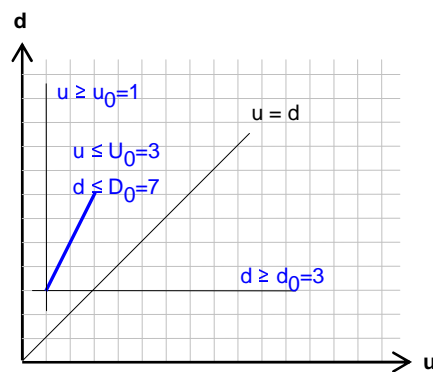


Figure K.2: Negotiated segment of values for (u,d) at NWK layer in case of asymmetric frozen connection (example)

In this type of connection, the MAC layer bandwidth negotiation parameters shall be fixed and identical to the maximum and minimum number of bearers upstream and downstream negotiated at NWK layer in this IE.

NOTE: Asymmetric frozen connection is intended for circuit mode profiles and is not compatible with DPRS or any other profile that change the Bandwidth at MAC layer.

K.1.2.3 Asymmetric reversible connections

Asymmetric reversible connections can use:

- duplex bearers;
- double simplex bearers in any direction (but not at the same time).

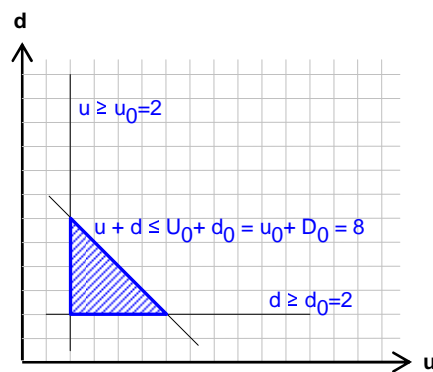
For *asymmetric reversible* connections, the following conditions apply:

- $U_0 = D_0 = U_1 = D_1$;
- $u_0 = d_0$.

meaning that maximum (resp. minimum) number of bearers upstream and downstream are identical. Octets 4, 4a shall be transmitted and shall contain (U_0 , u_0) respectively. Octets 4b and 4c shall not be transmitted.

The MAC layer can set or change the bandwidth at any time to any combination of values (u , d), such that the following conditions are met:

- $u \geq u_0$;
- $d \geq d_0$;
- $u + d \leq u_0 + D_1 = U_1 + d_0$;
- $u_0 + D_1 = U_1 + d_0$ is even.



**Figure K.3: Area of authorized values for (u,d)
in case of asymmetric reversible connection (example)**

NOTE 1: The third condition means that the total number of simplex bearers (upstream and downstream) cannot exceed the value $u_0 + D_1$. Consequently, the maximum number of bearers is reached in one direction when the opposite direction has the minimum number of bearers ($U_0 = U_1$ and $D_0 = D_1$).

NOTE 2: In the (u,d) plane, all conditions together draw a triangle of vertices (u_0, d_0) , (U_1, d_0) and (u_0, D_1) .

NOTE 3: This connection type is compatible with DPRS.

K.1.2.4 Asymmetric one-way-only connections

Asymmetric one-way-only connections can use:

- duplex bearers;
- double simplex bearers in one direction only (upstream or downstream).

NOTE 1: This connection type is compatible with DPRS.

The connection shall be either *asymmetric upstream only* (in that case, any existing double simplex bearer is upstream) or *asymmetric downstream only* (in that case, any existing double simplex bearer is downstream).

For *asymmetric one-way only* connections, octets 4, 4a, 4b, and 4c shall all be transmitted and shall contain (U_1, u_0, D_1, d_0) respectively.

For *asymmetric upstream only* connections, the following conditions shall apply and the transmitted values (U_1, u_0, D_1, d_0) shall be chosen accordingly:

- $u_0 \geq d_0$;
- $U_1 + d_0$ is even;
- $D_0 = (U_1 + d_0)/2$;
- $U_1 = U_0$;
- $D_1 = u_0$.

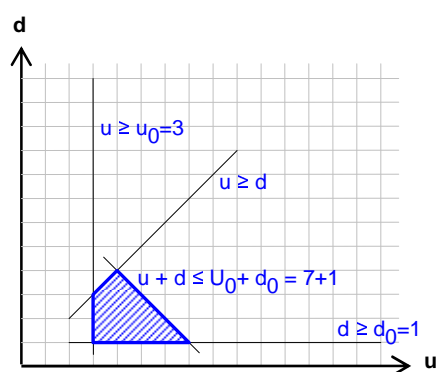
These conditions characterize upstream connections among one-way only connections.

NOTE 2: For *asymmetric upstream only* connections, D_0 (not transmitted) is also the maximum number of duplex bearers for the connection. It can only be reached when there is no double simplex bearer.

For *asymmetric upstream only* connections, the MAC layer can set or change the bandwidth at any time to any combination of values (u , d), such that the following four conditions are met:

- $u \geq u_0$;
- $d \geq d_0$;
- $u + d \leq U_1 + d_0$;
- $u \geq d$.

NOTE 3: In case $U_0 = u_0$, this area boils down to a single point (u_0 , d_0). In that case, u_0 and d_0 are different, otherwise, this would be a symmetric connection.



**Figure K.4: Area of authorized values for (u, d)
in case of asymmetric upstream-only connection (example)
(U_1, u_0, D_1, d_0) = (7, 3, 3, 1)**

For *asymmetric downstream only* connections, the following conditions shall apply and the transmitted values (U_1, u_0, D_1, d_0) shall be chosen accordingly:

- $u_0 \leq d_0$;
- $u_0 + D_1$ is even;
- $U_0 = (u_0 + D_1)/2$;
- $U_1 = d_0$;
- $D_1 = D_0$.

These conditions characterize downstream connections among one-way only connections.

For *asymmetric downstream only* connections, the MAC layer can set or change the bandwidth at any time to any combination of values (u , d), such that the following four conditions are met:

- $u \geq u_0$;
- $d \geq d_0$;
- $u + d \leq u_0 + D_1$;
- $u \leq d$.

NOTE 4: In case $D_0 = d_0$, this area boils down to a single point (u_0, d_0). In that case, u_0 and d_0 are different, otherwise, this would be a symmetric connection.

NOTE 5: For *asymmetric downstream only* connections, U_0 (not transmitted) also represents the maximum number of duplex bearers for the connection and can only be reached when there is no double simplex bearer.

K.1.2.5 Asymmetric unrestricted connections

Asymmetric unrestricted connections can use:

- duplex bearers;
- double simplex bearers in any direction (but not at the same time).

For *asymmetric unrestricted* connections, octets 4, 4a, 4b, and 4c shall all be transmitted and shall contain (U_1 , u_0 , D_1 , d_0) respectively.

NOTE 1: This connection type is compatible with DPRS.

For an *asymmetric unrestricted connection*, the MAC layer can set or change the bandwidth at any time to any combination of values (u , d) placed in the polygon limited by the vertices: (u_0 , d_0), (u_0 , D_1), (S , S) and (U_1 , d_0), where S stands for the maximum number of duplex bearers.

By definition of an *asymmetric unrestricted connection*, the maximum number of duplex bearers S shall be calculated as the maximum of $(u_0 + D_1)/2$ and $(U_1 + d_0)/2$.

NOTE 2: This maximum should be an integer in all cases (the value of octets 4, 4a, 4b and 4c should be chosen to fulfil this rule).

Examples of asymmetric unrestricted connections:

(U_1 , u_0 , D_1 , d_0) = (7, 1, 3, 3)
In this case, $D_1 < D_0 = 5$

(U_1 , u_0 , D_1 , d_0) = (7, 1, 4, 3)
Comment: here (u_0 , D_1) is never reached, but this still defines an acceptable area.

(U_1 , u_0 , D_1 , d_0) = (7, 1, 5, 3)
In this case, $D_1 = D_0 = 5$

(U_1 , u_0 , D_1 , d_0) = (7, 1, 7, 3)
In this case, $D_1 = D_0 = 7$

(U_1 , u_0 , D_1 , d_0) = (7, 1, 9, 3)
In this case, $D_1 = D_0 = 9$

(U_1 , u_0 , D_1 , d_0) = (7, 1, 11, 3)
In this case, $D_1 = D_0 = 9$
Max number of duplex bearer is now
 $(u_0 + D_1)/2 = 6$ which becomes
greater than $(U_1 + d_0)/2 = 5$.

**Figure K.5: Examples of authorized areas for (u , d)
in several asymmetric unrestricted connections
($U_1 = U_0$ applies in all examples)**

NOTE 3: In figure K.5, the vertices may be reachable or not, depending on if they fulfil the basic DECT rule requiring that total number of bearers have to be even. For instance the point (u_0 , D_1) = (1, 5) => (1+5 = even), in the third diagram is not reachable. On the other hand, the point (u_0 , D_1) = (1, 4) => (1+4 = odd) in the second diagram is not reachable.

Annex L (informative): Additional information on paging

L.1 List of "well-known" uses of LCE paging codes

L.1.1 Purpose of the list

This clause keeps a central record of all LCE paging codes used in DECT profiles and known applications.

The main purpose of the table is allowing designers of future DECT standards and applications checking easily the list of existing uses in order to avoid possible conflicts with previously used codes.

When designing a new DECT standard (i.e. an application profile), it is usually possible the use of several LCE codes to perform the paging. As a general rule, it is a good practice to avoid the repetition of the same code used by existing DECT applications that could coexist in the same FP or PP implementation.

Designers of DECT applications not covered by a specific application profile (based on the DECT CI), or when the application profile does not define uniquely the LCE code to be used, may also check the table to select the most convenient code.

The table is also useful for reporting the practical use convention for a DECT application.

This list is provided for informative purposes and is only updated when there is a new revision of the present document.

L.1.2 List of "well-known" uses of LCE paging codes

Table L.1: List of well-known uses of LCE paging codes

LCE code	Application	Application profile (if any)	Remarks and coding of fields	Expected PT response
001	G.726 voice service: paging with group mask and CBI	None (not covered by EN 300 444, [51] but allowed by EN 300 175-5)	short page format is used	Mt Basic Connection setup on full slot
100	GAP voice service G.726	EN 300 444 [51]	short page format is used	Mt Basic Connection setup on full slot. Default MAC service= I_N _min_delay
	DECT New Generation voice service G.726	TS 102 527-1 [73] TS 102 527-3 [75]		
	Standard paging for voice service			
100	DECT_New Generation Wideband speech (all voice services except G.726)	TS 102 527-1 [73] TS 102 527-3 [75]	Full page format is used. Info 1 = slot type (1, 2 or 4); Info 2 = 0; Info 3 = 0	Mt Advanced Connection setup on selected slot. MAC service negotiated in setup if needed. Default MAC service= I_N _min_delay
101	Data profile D2	EN 301 238 [i.13]	Short page format is used.	Mt_advanced connection setup on full slot. Default MAC service: I_N _normal_delay
110	DPRS Class 1 (setup or resume)	EN 301 649 [72]	Short or full format allowed Description in 14.5.3.1. Info 1 = slot type; Info 2 = 0 or 4; Info 3 = 0.	B-field Advanced Connection setup on specified or default slot. MAC service negotiated in setup (if resume, it should be as before the suspension)
110	DPRS Class 2, initial call setup	EN 301 649 [72]	Short or full format allowed Description in 14.5.1. Info 1 = slot type; Info 2 = 0, 4 or 5; Info 3 = 0.	B-field Advanced Connection setup on specified or default slot. MAC service negotiated in setup
111	DPRS Class 2, resume	EN 301 649 [72]	Short or full format allowed Description in 14.5.2. Info 1 = slot type; Info 2 = 0 or 4. Info 3 = LCN	B-field Advanced Connection setup on specified or suspended slot. MAC service negotiated in setup (it should be as before the suspension)
111	Former A/B 1 devices	ETS 300 435 [i.14]	Short page format.	Mt_advanced connection setup on full slot. See historic standard A/B 1

L.2 Compatibility with historic DECT devices

L.2.1 Rule for compatibility with devices based on former data profile A/B 1 (historic)

If a FP requires to implement compatibility with former data equipment based on historic profile A/B 1 (ETS 300 435 [i.14]) the following rule will be used (only when paging to a data profile A/B 1 PP).

- 1) **LCE code:** the S code (110) will be used either for setup or resume a connection if the MAC service is I_P _error_detect, and the R code will be used if the MAC service is I_P _error_correct.

NOTE 1: In A/B 1 devices, there were no difference between setup and resume.

2) **Field 1, slot indicator** will carry the following information:

Bits	8 7 6 5	Meaning
	1 0 0 1	Full slot, Symmetric connection
	1 1 0 0	Full slot, Asymmetric F to P with 1 duplex bearer
	1 1 0 1	Full slot, Asymmetric F to P with 2 target duplex bearers
	1 1 1 0	Full slot, Asymmetric P to F with 1 duplex bearer
	1 1 1 1	Full slot, Asymmetric P to F with 2 target duplex bearers
	All other values reserved.	

NOTE 2: Only full slot was used in former data profile A/B 1 devices.

3) **Field 2, set up indicator** will carry the following information instead of the set up type.

Bits	8 7 6 5	Meaning
	0 0 0 0	Number of bearers undefined (to be negotiated later)
	0 0 0 1	Number of bearers = 1 (single bearer device)
	0 N N N	Number of bearers = NNN (not recommended)

4) **Field 3**, will carry the Max packet lifetime, but only if the service is I_p _error_correct:

Bits	4 3 2 1	Meaning
	0 0 0 0	I_p error detect service
	1 n n n	Maximum packet lifetime if I_p ; error_protect service

NOTE 3: The FP should be aware that the A/B 1 PT device will answer the paging using A-field setup.

Annex M (informative): UTF-8 encoded character sets - Guidelines for implementation

M.1 General

The PP is not expected to support all Unicode characters. However, the PP should support UTF-8 encoding format for Unicode characters:

- to be able to display at least the characters the PP supports in any received UTF-8 encoded string or text;
- to avoid breaking a UTF8 string consistency if the user is allowed to edit it. Especially the user should be allowed to replace a UTF8 character not supported by this PP with another UTF8 character that this PP supports.

The list of characters that a PP should be able to display in addition to IA5 characters is given in the present annex as guidelines for implementation.

NOTE: Consistently with annex D which redefines IA5 characters (see [i.5]) below 0x1F as DECT control codes, values between 0x00 and 0x1F are not considered (and therefore could still be used as DECT control codes if applicable).

M.2 Characters sets tables

The following tables provide lists of Unicode characters a PP should be able to display when supporting the UTF-8 encoding format. It includes:

- Some language-related tables. Support is recommended if the PP supports UTF-8 and the corresponding language(s).
- A language-independent table of useful symbols. Support is recommended if the PP supports UTF-8.

NOTE 1: The present annex does not list all possible languages. Other languages could be added in further version of the present document.

The tables follow the Unicode standard [i.16]. For each character (logically identified in Unicode by its "code point", first column), a character glyph, the name, the UTF8 encoding are given. Membership to IA5 is indicated in the last column (otherwise a replacement character sequence is proposed when applicable).

NOTE 2: Some characters may be rendered in Unicode in several ways. For example "Ö" may be rendered either as code point U+00d6 (as shown in table M.1 of clause M.3), or as the base character U+004f ("O") followed by the combining character U+308 (COMBINING DIAERESIS). These alternate representations are not shown below. The PP is not requested to support them and the FP should therefore not use them.

M.3 Encoding of Western Europe languages

The following Western Europe character set is based on ISO/IEC 8859-1 [47] and is suitable for the following languages: Afrikaans, Albanian, Basque, Breton, Catalan, Danish, Dutch (NL&BE), English (UK&US), Faroese, Finnish, French, Gaelic, Galician, German, Icelandic, Irish, Italian, Kurdish, Latin, Leones, Luxembourgish, Norwegian, Occitan, Portuguese (PT&BR), Rhaeto-Romanic, Spanish and Swedish.

Table M.1: Encoding of Western Europe languages

Code point (hexa)	Character glyphe	Name	UTF8 encoding	Comment
U+0061	a	LATIN SMALL LETTER A	'61'H	IA5
U+0041	A	LATIN CAPITAL LETTER A	'41'H	IA5
U+00e4	ä	LATIN SMALL LETTER A WITH DIAERESIS	'c3a4'H	
U+00c4	Ä	LATIN CAPITAL LETTER A WITH DIAERESIS	'c384'H	
U+00e1	á	LATIN SMALL LETTER A WITH ACUTE	'c3a1'H	
U+00c1	Á	LATIN CAPITAL LETTER A WITH ACUTE	'c381'H	
U+00e0	à	LATIN SMALL LETTER A WITH GRAVE	'c3a0'H	
U+00c0	À	LATIN CAPITAL LETTER A WITH GRAVE	'c380'H	
U+00e2	â	LATIN SMALL LETTER A WITH CIRCUMFLEX	'c3a2'H	
U+00c2	Â	LATIN CAPITAL LETTER A WITH CIRCUMFLEX	'c382'H	
U+00e3	ã	LATIN SMALL LETTER A WITH TILDE	'c3a3'H	
U+00c3	Ã	LATIN CAPITAL LETTER A WITH TILDE	'c383'H	
U+0062	b	LATIN SMALL LETTER B	'62'H	IA5
U+0042	B	LATIN CAPITAL LETTER B	'42'H	IA5
U+0063	c	LATIN SMALL LETTER C	'63'H	IA5
U+0043	C	LATIN CAPITAL LETTER C	'43'H	IA5
U+00e7	ç	LATIN SMALL LETTER C WITH CEDILLA	'c3a7'H	
U+00c7	Ç	LATIN CAPITAL LETTER C WITH CEDILLA	'c387'H	
U+0064	d	LATIN SMALL LETTER D	'64'H	IA5
U+0044	D	LATIN CAPITAL LETTER D	'44'H	IA5
U+00f0	ð	LATIN SMALL LETTER ETH	'c3b0'H	
U+00d0	Ð	LATIN CAPITAL LETTER ETH	'c390'H	
U+0065	e	LATIN SMALL LETTER E	'65'H	IA5
U+0045	E	LATIN CAPITAL LETTER E	'45'H	IA5
U+00eb	ë	LATIN SMALL LETTER E WITH DIAERESIS	'c3ab'H	
U+00cb	Ë	LATIN CAPITAL LETTER E WITH DIAERESIS	'c38b'H	
U+00e9	é	LATIN SMALL LETTER E WITH ACUTE	'c3a9'H	
U+00c9	É	LATIN CAPITAL LETTER E WITH ACUTE	'c389'H	
U+00e8	è	LATIN SMALL LETTER E WITH GRAVE	'c3a8'H	
U+00c8	È	LATIN CAPITAL LETTER E WITH GRAVE	'c388'H	
U+00ea	ê	LATIN SMALL LETTER E WITH CIRCUMFLEX	'c3aa'H	
U+00ca	Ê	LATIN CAPITAL LETTER E WITH CIRCUMFLEX	'c38a'H	
U+0066	f	LATIN SMALL LETTER F	'66'H	IA5
U+0046	F	LATIN CAPITAL LETTER F	'46'H	IA5
U+0067	g	LATIN SMALL LETTER G	'67'H	IA5
U+0047	G	LATIN CAPITAL LETTER G	'47'H	IA5
U+0068	h	LATIN SMALL LETTER H	'68'H	IA5
U+0048	H	LATIN CAPITAL LETTER H	'48'H	IA5
U+0069	i	LATIN SMALL LETTER I	'69'H	IA5
U+0049	I	LATIN CAPITAL LETTER I	'49'H	IA5
U+00ef	ï	LATIN SMALL LETTER I WITH DIAERESIS	'c3af'H	
U+00cf	Ï	LATIN CAPITAL LETTER I WITH DIAERESIS	'c38f'H	
U+00ed	í	LATIN SMALL LETTER I WITH ACUTE	'c3ad'H	
U+00cd	Í	LATIN CAPITAL LETTER I WITH ACUTE	'c38d'H	
U+00ec	ì	LATIN SMALL LETTER I WITH GRAVE	'c3ac'H	
U+00cc	Ì	LATIN CAPITAL LETTER I WITH GRAVE	'c38c'H	
U+00ee	î	LATIN SMALL LETTER I WITH CIRCUMFLEX	'c3ae'H	
U+00ce	Î	LATIN CAPITAL LETTER I WITH CIRCUMFLEX	'c38e'H	
U+006a	j	LATIN SMALL LETTER J	'6a'H	IA5
U+004a	J	LATIN CAPITAL LETTER J	'4a'H	IA5
U+006b	k	LATIN SMALL LETTER K	'6b'H	IA5
U+004b	K	LATIN CAPITAL LETTER K	'4b'H	IA5
U+006c	l	LATIN SMALL LETTER L	'6c'H	IA5

Code point (hexa)	Character glyphe	Name	UTF8 encoding	Comment
U+004c	L	LATIN CAPITAL LETTER L	'4c'H	IA5
U+006d	m	LATIN SMALL LETTER M	'6d'H	IA5
U+004d	M	LATIN CAPITAL LETTER M	'4d'H	IA5
U+006e	n	LATIN SMALL LETTER N	'6e'H	IA5
U+004e	N	LATIN CAPITAL LETTER N	'4e'H	IA5
U+00f1	ñ	LATIN SMALL LETTER N WITH TILDE	'c3b1'H	
U+00d1	Ñ	LATIN CAPITAL LETTER N WITH TILDE	'c391'H	
U+006f	o	LATIN SMALL LETTER O	'6f'H	IA5
U+004f	O	LATIN CAPITAL LETTER O	'4f'H	IA5
U+00f6	ö	LATIN SMALL LETTER O WITH DIAERESIS	'c3b6'H	
U+00d6	Ö	LATIN CAPITAL LETTER O WITH DIAERESIS	'c396'H	
U+00f3	ó	LATIN SMALL LETTER O WITH ACUTE	'c3b3'H	
U+00d3	Ó	LATIN CAPITAL LETTER O WITH ACUTE	'c393'H	
U+00f2	ò	LATIN SMALL LETTER O WITH GRAVE	'c3b2'H	
U+00d2	Ò	LATIN CAPITAL LETTER O WITH GRAVE	'c392'H	
U+00f4	ô	LATIN SMALL LETTER O WITH CIRCUMFLEX	'c3b4'H	
U+00d4	Ô	LATIN CAPITAL LETTER O WITH CIRCUMFLEX	'c394'H	
U+00f5	õ	LATIN SMALL LETTER O WITH TILDE	'c3b5'H	
U+00d5	Õ	LATIN CAPITAL LETTER O WITH TILDE	'c395'H	
U+0070	p	LATIN SMALL LETTER P	'70'H	IA5
U+0050	P	LATIN CAPITAL LETTER P	'50'H	IA5
U+0071	q	LATIN SMALL LETTER Q	'71'H	IA5
U+0051	Q	LATIN CAPITAL LETTER Q	'51'H	IA5
U+0072	r	LATIN SMALL LETTER R	'72'H	IA5
U+0052	R	LATIN CAPITAL LETTER R	'52'H	IA5
U+0073	s	LATIN SMALL LETTER S	'73'H	IA5
U+0053	S	LATIN CAPITAL LETTER S	'53'H	IA5
U+00df	ß	LATIN SMALL LETTER SHARP S	'c39f'H	Or 'ss'
U+0074	t	LATIN SMALL LETTER T	'74'H	IA5
U+0054	T	LATIN CAPITAL LETTER T	'54'H	IA5
U+0075	u	LATIN SMALL LETTER U	'75'H	IA5
U+0055	U	LATIN CAPITAL LETTER U	'55'H	IA5
U+00fc	ü	LATIN SMALL LETTER U WITH DIAERESIS	'c3bc'H	
U+00dc	Ü	LATIN CAPITAL LETTER U WITH DIAERESIS	'c39c'H	
U+00fa	ú	LATIN SMALL LETTER U WITH ACUTE	'c3ba'H	
U+00da	Ú	LATIN CAPITAL LETTER U WITH ACUTE	'c39a'H	
U+00f9	ù	LATIN SMALL LETTER U WITH GRAVE	'c3b9'H	
U+00d9	Û	LATIN CAPITAL LETTER U WITH GRAVE	'c399'H	
U+00fb	û	LATIN SMALL LETTER U WITH CIRCUMFLEX	'c3bb'H	
U+00db	Û	LATIN CAPITAL LETTER U WITH CIRCUMFLEX	'c39b'H	
U+0076	v	LATIN SMALL LETTER V	'76'H	IA5
U+0056	V	LATIN CAPITAL LETTER V	'56'H	IA5
U+0077	w	LATIN SMALL LETTER W	'77'H	IA5
U+0057	W	LATIN CAPITAL LETTER W	'57'H	IA5
U+0078	x	LATIN SMALL LETTER X	'78'H	IA5
U+0058	X	LATIN CAPITAL LETTER X	'58'H	IA5
U+0079	y	LATIN SMALL LETTER Y	'79'H	IA5
U+0059	Y	LATIN CAPITAL LETTER Y	'59'H	IA5
U+00ff	ÿ	LATIN SMALL LETTER Y WITH DIAERESIS	'c3bf'H	
U+00fd	ý	LATIN SMALL LETTER Y WITH ACUTE	'c3bd'H	
U+00dd	Ý	LATIN CAPITAL LETTER Y WITH ACUTE	'c39d'H	
U+00fe	þ	LATIN SMALL LETTER THORN	'c3be'H	
U+00de	Ð	LATIN CAPITAL LETTER THORN	'c39e'H	
U+007a	z	LATIN SMALL LETTER Z	'7a'H	IA5

Code point (hexa)	Character glyphe	Name	UTF8 encoding	Comment
U+005a	Z	LATIN CAPITAL LETTER Z	'5a'H	IA5
U+00E5	å	LATIN SMALL LETTER A WITH RING ABOVE	'c3a5'H	
U+00C5	Å	LATIN CAPITAL LETTER A WITH RING ABOVE	'c385'H	
U+00e6	æ	LATIN SMALL LETTER AE	'c3a6'H	
U+00c6	Æ	LATIN CAPITAL LETTER AE	'c386'H	
U+00f8	ø	LATIN SMALL LETTER O WITH STROKE	'c3b8'H	
U+00d8	Ø	LATIN CAPITAL LETTER O WITH STROKE	'c398'H	

The following table lists other characters that are not included in the ISO/IEC 8859-1 [47] standard but might be useful for specific languages. The table also lists recommended ISO/IEC 8859-1 [47] substitutions for devices that are only capable of displaying ISO8859-1 characters.

Table M.2: Encoding of additional Western Europe characters

Code point (hexa)	Character glyphe	Name	UTF8 encoding	Comment	possible ISO/IEC 8859-1 [47] substitution
U+0153	œ	LATIN SMALL LIGATURE OE	'c593'H	French	'oe'
U+0152	Œ	LATIN CAPITAL LIGATURE OE	'c592'H	French	'OE' or 'Oe'
U+0178	ÿ	LATIN CAPITAL LETTER Y WITH DIAERESIS	'c5b8'H	French	'Y' or 'ÿ'

M.4 Encoding of Hebrew

Table M.3: Encoding of Hebrew

Code point (hexa)	Character	Name	UTF8 encoding	Comment
U+05d0	א	HEBREW LETTER ALEF	'd790'H	
U+05d1	ב	HEBREW LETTER BET	'd791'H	
U+05d2	ג	HEBREW LETTER GIMEL	'd792'H	
U+05d3	ד	HEBREW LETTER DALET	'd793'H	
U+05d4	ה	HEBREW LETTER HE	'd794'H	
U+05d5	ו	HEBREW LETTER VAV	'd795'H	
U+05d6	ז	HEBREW LETTER ZAYIN	'd796'H	
U+05d7	ח	HEBREW LETTER HET	'd797'H	
U+05d8	ט	HEBREW LETTER TET	'd798'H	
U+05d9	י	HEBREW LETTER YOD	'd799'H	
U+05da	ך	HEBREW LETTER FINAL KAF	'd79a'H	
U+05db	כ	HEBREW LETTER KAF	'd79b'H	
U+05dc	ל	HEBREW LETTER LAMED	'd79c'H	
U+05dd	ם	HEBREW LETTER FINAL MEM	'd79d'H	
U+05de	מ	HEBREW LETTER MEM	'd79e'H	
U+05df	נ	HEBREW LETTER FINAL NUN	'd79f'H	
U+05e0	נ	HEBREW LETTER NUN	'd7a0'H	
U+05e1	ס	HEBREW LETTER SAMEKH	'd7a1'H	
U+05e2	ע	HEBREW LETTER AYIN	'd7a2'H	
U+05e3	ף	HEBREW LETTER FINAL PE	'd7a3'H	
U+05e4	פ	HEBREW LETTER PE	'd7a4'H	
U+05e5	ץ	HEBREW LETTER FINAL TSADI	'd7a5'H	
U+05e6	צ	HEBREW LETTER TSADI	'd7a6'H	
U+05e7	ק	HEBREW LETTER QOF	'd7a7'H	
U+05e8	ר	HEBREW LETTER RESH	'd7a8'H	
U+05e9	ש	HEBREW LETTER SHIN	'd7a9'H	
U+05ea	ת	HEBREW LETTER TAV	'd7aa'H	

M.5 Useful symbols

Table M.4: Encoding of useful symbols

Code point (hexa)	Character	Name	UTF-8 encoding	Comment
U+0020		SPACE		IA5
U+0030	0	DIGIT ZERO		IA5
U+0031	1	DIGIT ONE		IA5
U+0032	2	DIGIT TWO		IA5
U+0033	3	DIGIT THREE		IA5
U+0034	4	DIGIT FOUR		IA5
U+0035	5	DIGIT FIVE		IA5
U+0036	6	DIGIT SIX		IA5
U+0037	7	DIGIT SEVEN		IA5
U+0038	8	DIGIT EIGHT		IA5
U+0039	9	DIGIT NINE		IA5
U+0027	'	APOSTROPHE		IA5
U+002B	+	PLUS SIGN		IA5
U+002D	-	HYPHEN-MINUS		IA5
U+002E	.	FULL STOP		IA5
U+002C	,	COMMA		IA5
U+003A	:	COLON		IA5
U+003F	?	QUESTION MARK		IA5
U+0021	!	EXCLAMATION MARK		IA5
U+0022	"	QUOTATION MARK		IA5
U+003B	;	SEMICOLON		IA5
U+005F	_	LOW LINE		IA5
U+002A	*	ASTERISK		IA5
U+002F	/	SOLIDUS		IA5
U+0028	(LEFT PARENTHESIS		IA5
U+0029)	RIGHT PARENTHESIS		IA5
U+003C	<	LESS-THAN SIGN		IA5
U+003D	=	EQUALS SIGN		IA5
U+003E	>	GREATER-THAN SIGN		IA5
U+0025	%	PERCENT SIGN		IA5
U+0023	#	NUMBER SIGN		IA5
U+0040	@	COMMERCIAL AT		IA5
U+005C	\	REVERSE SOLIDUS		IA5
U+0026	&	AMPERSAND		IA5
U+0024	\$	DOLLAR SIGN		IA5
U+005E	^	CIRCUMFLEX ACCENT		IA5
U+007E	~	TILDE		IA5
U+007C		VERTICAL LINE		IA5
U+005B	[LEFT SQUARE BRACKET		IA5
U+005D]	RIGHT SQUARE BRACKET		IA5
U+007D	}	RIGHT CURLY BRACKET		IA5
U+007B	{	LEFT CURLY BRACKET		IA5

Table M.5 lists other symbols that are not included in all parts of ISO 8859 [i.17] standards but might be useful for specific languages. The table also lists recommended IA5 substitutions.

Table M.5: Encoding of additional useful symbols

Code point (hexa)	Character	Name	UTF-8 encoding	Comment	possible IA5 substitution
U+2212	–	MINUS SIGN	'e28892'H		- (Hyphen-Minus)
U+2018	'	LEFT SINGLE QUOTATION MARK	'e28098'H		' (Apostrophe)
U+2019	'	RIGHT SINGLE QUOTATION MARK	'e28099'H		' (Apostrophe)
U+201c	"	LEFT DOUBLE QUOTATION MARK	'e2809c'H		" (Quotation Mark)
U+201d	"	RIGHT DOUBLE QUOTATION MARK	'e2809d'H		" (Quotation Mark)
U+20AC	€	EURO SIGN	'e282ac'H		EUR
U+00d7	×	MULTIPLICATION SIGN	'c397'H		"*" (Asterisk)
U+00f7	÷	DIVISION SIGN	'c3b7'H		"/" (Solidus)
U+00BF	¿	INVERTED QUESTION MARK	'c2bf'H		"?" (Question Mark)
U+00A1	¡	INVERTED EXCLAMATION MARK	'c2a1'H		"!" (Exclamation Mark)
U+00ab	«	LEFT-POINTING DOUBLE ANGLE QUOTATION MARK	'c2ab'H		" (Quotation Mark)
U+00bb	»	RIGHT-POINTING DOUBLE ANGLE QUOTATION MARK	'c2bb'H		" (Quotation Mark)
U+00A7	§	SECTION SIGN	'c2a7'H		? (Question Mark)
U+00A3	£	POUND SIGN	'c2a3'H		GBP
U+00A5	¥	YEN SIGN	'c2a5'H		JPY
U+00A4	¤	CURRENCY SIGN	'c2a4'H		CUR
U+00a9	©	COPYRIGHT SIGN	'c2a9'H		(C)
U+fffd	◆	REPLACEMENT CHARACTER	'efbffd'H		? (Question Mark)

Annex N (informative): Bibliography

- Recommendation ITU-T G.711: "Pulse Code Modulation (PCM) of voice frequencies".
- Recommendation ITU-T G.726: "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)".
- Recommendation ITU-T G.722: "7 kHz audio - coding within 64 kbit/s".
- Recommendation ITU-T G.729.1: "G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729".
- ISO/IEC 14496-3 (2005) Amd 1 (2007): "Low delay AAC profile".
- ISO/IEC 14496-3 (2005): "Information technology - Coding of audio-visual objects - Part 3: Audio".
- Recommendation ITU-T H.221: "Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices".
- Recommendation ITU-T H.242: "System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s".
- Recommendation ITU-T H.261: "Video codec for audiovisual services at p x 64 kbit/s".
- Recommendation ITU-T I.441: "ISDN user-network interface - Data link layer specification".
- Recommendations ITU-T Series V: "Data communication over the telephone network".
- Recommendation ITU-T V.6: "Standardization of data signalling rates for synchronous data transmission on leased telephone-type circuits".
- Recommendation ITU-T V.21: "300 bits per second duplex modem standardized for use in the general switched telephone network".
- Recommendation ITU-T V.22: "1200 bits per second duplex modem standardized for use in the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".
- Recommendation ITU-T V.22bis: "2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".
- Recommendation ITU-T V.23: "600/1200-baud modem standardized for use in the general switched telephone network".
- Recommendation ITU-T V.26: "2400 bits per second modem standardized for use on 4-wire leased telephone-type circuits".
- Recommendation ITU-T V.26bis: "2400/1200 bits per second modem standardized for use in the general switched telephone network".
- Recommendation ITU-T V.26ter: "2400 bits per second duplex modem using the echo cancellation technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".
- Recommendation ITU-T V.27: "4800 bits per second modem with manual equalizer standardized for use on leased telephone-type circuits".
- Recommendation ITU-T V.27bis: "4800/2400 bits per second modem with automatic equalizer standardized for use on leased telephone-type circuits".
- Recommendation ITU-T V.27ter: "4800/2400 bits per second modem standardized for use in the general switched telephone network".

- Recommendation ITU-T V.29: "9600 bits per second modem standardized for use on point-to-point 4-wire leased telephone-type circuits".
- Recommendation ITU-T V.32: "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits".
- Recommendation ITU-T V.35: "Data transmission at 48 kilobits per second using 60-108 kHz group band circuits".
- Recommendations ITU-T Series X: "Data networks and open system communication".
- Recommendation ITU-T X.28: "DTE/DCE interface for a start-stop mode Data Terminal Equipment accessing the Packet Assembly/Disassembly facility (PAD) in a public data network situated in the same country".
- Recommendation ITU-T X.29: "Procedures for the exchange of control information and user data between a Packet Assembly/Disassembly (PAD) facility and a packet mode DTE or another PAD".
- Recommendation ITU-T X.31: "Support of packet mode terminal equipment by an ISDN".
- ETSI TR 101 480: "Integrated Services Digital Network (ISDN); Public Switched Telephone Network (PSTN); Framework for the provision of calling party name information".
- TTC JT-H450.8: "Name Identification Supplementary Service for JT-H323".

Annex O (informative): Change history

The following table presents main changes from a published version to the next version (published or to be published).

Subject/Comment	Old	New
The enhancement of the DECT base standard to support higher data rates includes the 16 QAM/64 QAM modulation option and the Channel Coding based on the Turbo Code Principle.	1.6.1	1.7.1
The enhancement of the DECT base standard to support DECT Broadband service and backwards compatible changes for support of DECT access to IP networks (TS 102 265 [69] V1.1.1) and some minor editorial improvements.	1.7.1	1.8.1
Modifications required from the introduction of ODAP, Generic Multimedia encapsulation (DPRS) and F-MMS interworking profile included.	1.8.1	1.9.1
New Generation DECT: A major revision of the DECT base standard introducing wideband speech, improved data services, new slot types and other technical enhancements.	1.9.1	2.1.1
New Generation DECT: addition of flags and Information elements for new services. Technical enhancement of the IE <Connection Attributes> and LCE paging codes.	2.1.1	2.2.1
New Generation DECT: enhanced security; addition of flags and Information elements for new services; addition of UTF-8 character sets; review of NWK layer suspend/resume; technical and editorial review.	2.2.1	2.3.1
New authentication algorithm DSAA2 and new ciphering algorithm DSC2. New authentication procedures. Use of <<CALLED PARTY NUMBER>> aligned with GAP. Order of IEs in messages reviewed. Addition of RFP broadcast and Terminal Capability bits for new NG-DECT features. Removal of IE <<Authentication Reject Parameter>>. Editorial review.	2.3.1	2.4.1
New Generation DECT: Added diagnostic indication type (line-in-use) along with extended list change indication event types (and updated PT side capability bit for extended list change indication). Furthermore added two new remote call statuses. DECT ULE: Introduction of DECT Ultra Low Energy. <<Creation of the ULE MAC Configuration info>> IE. Expansion of usable codes for DLC LU Services. Updates in several other IEs.	2.4.1	2.5.1

History

Document history		
Edition 1	October 1992	Publication as ETS 300 175-5 (Historical)
Edition 2	September 1996	Publication as ETS 300 175-5 (Historical)
Edition 3	December 1997	Publication as ETS 300 175-5 (Historical)
V1.4.2	June 1999	Publication
V1.5.1	February 2001	Publication
V1.6.1	February 2002	Publication
V1.7.1	July 2003	Publication
V1.8.1	November 2004	Publication
V1.9.1	September 2005	Publication
V2.1.1	August 2007	Publication
V2.2.1	November 2008	Publication
V2.3.1	June 2010	Publication
V2.4.1	April 2012	Publication
V2.5.0	April 2013	EN Approval Procedure AP 20130820: 2013-04-22 to 2013-08-20
V2.5.1	August 2013	Publication