EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 175-5

October 1992

Source: ETSI TC-RES

Reference: DE/RES 3001-5

ICS: 33.060

Key words: DECT

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

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

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

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

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI), and was adopted, having passed through the ETSI standards approval procedure (Public Enquiry 23: 1991-09-02 to 1991-12-27, Vote 22: 1992-05-25 to 1992-07-17).

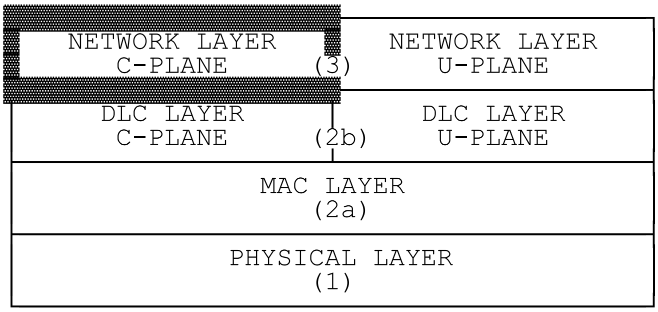
Annex C to this ETS is informative, and Annexes A, B, D, E, and F are normative.

Further details of the DECT system may be found in the ETSI Technical Reports, ETR 015 [16], and ETR 043 [15], and also in the draft ETSI Technical Report: "Digital European Cordless Telecommunications system description document" [17].

Blank page

1 Scope

This part of the Digital European Cordless Telecommunications (DECT) Common Interface specifies the network layer. The network layer is Part 5 of the DECT Common Interface standard and layer 3 of the DECT protocol stack.



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

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

- call control;
- supplementary services;
- connection oriented message service;
- connectionless message service;
- mobility management;
- link control entity.

This part uses the layered model principles and terminology as described in CCITT Recommendations X.200 [23] and X.210 [24].

2 Normative references

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

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

[2] ETS 300 175-2: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Part 2: Physical layer".

[3] ETS 300 175-3: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Part 3: Medium access control layer".

[4] ETS 300 175-4: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Part 4: Data link control layer".

[5] ETS 300 175-5: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Part 5: Network layer".

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

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

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

[9] ETS 300 175-9: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Part 9: Public access profile".

[10] Reserved.

[11] Reserved.

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

[13] Reserved for future ETS version of [12].

[14] CEPT Recommendation T/SGT SF2 (89) 6/0: "Draft Recommendation T/SF Services and Facilities of Digital European Cordless Telecommunications".

[15] ETR 043: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common Interface Services and Facilities requirements specification".

[16] ETR 015: "Digital European Cordless Telecommunications Reference document".

[17] Draft ETSI Technical Report: "Digital European Cordless Telecommunications System description document".

[18] ETR 042: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT). A Guide to the DECT features that influence the traffic capacity and the maintenance of high radio link transmission quality, including the results of simulations".

[19] Reserved for future DECT related document.

[20] Reserved.

[21a] ETS 300 102-1 (1991): "Integrated Services Digital Network (ISDN); User-network interface layer 3 Specification for basic call control".

[21b] ETS 300 102-2 (1991): "Integrated Services Digital Network (ISDN); User-network interface layer 3 Specification Description Language (SDL) diagrams".

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

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

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

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

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

[27] ETS 300 133-1 to -7: "Paging Systems (PS); European Radio Message System (ERMES)".

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

[29] prETS 300 196 (draft ETS T/S 46-32B): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol".

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

[31] CCITT Recommendation Q.921 (1988): "Digital Subscriber Signalling System No.1; Data Link Layer".

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

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

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

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

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

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

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

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

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

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

[42] Draft ETS T/S 46-33R1: "Integrated Services Digital Network (ISDN); Call Forwarding Busy (CFB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[43] Draft ETS T/S 46-33R3: "Integrated Services Digital Network (ISDN); Call Forwarding Unconditional (CFU) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[44] Draft ETS T/S 46-33T: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

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

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

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

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

[49] Draft ETS T/S 46-33G: "Integrated Services Digital Network (ISDN); Completion of Calls to Busy Subscriber (CCBS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[50] Draft ETS T/S 46-33P: "Integrated Services Digital Network (ISDN); Freephone (FPH) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

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

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

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

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

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

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

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

[58] Draft ETS T/S 46-33Q1: "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[59] Draft ETS T/S 46-33Q2: "Integrated Services Digital Network (ISDN); Single Step Call Transfer (SCT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[60] Draft ETS T/S 46-33R2: "Integrated Services Digital Network (ISDN); Call Forwarding No Reply (CFNR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[61] Draft ETS T/S 46-33R4: "Integrated Services Digital Network (ISDN); Call Deflection (CD) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol".

[62] prETS 300 185: "Integrated Services Digital Network (ISDN); Conference Call add-on (CONF) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol (T/S 46-33K)".

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

[64] prETS 300 188: "Integrated Services Digital Network (ISDN); Three Party (3PTY) supplementary service Digital Subscriber Signalling System No. one (DSS1) protocol".

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

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

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

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

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

3 Definitions, symbols and abbreviations

Refer to ETS 300 175-1 [1] for a complete list of definitions, symbols and abbreviations.

3.1 Network layer definitions

Attach: the process whereby a portable part within the coverage area of a fixed part to which it has access rights, notifies this fixed part that it is operative. The reverse process is detach, which reports the portable part as inoperative.

NOTE 1: An operative portable part is assumed to be ready to receive calls.

Authentication: the process whereby a Digital European Cordless Telecommunications (DECT) subscriber is positively verified to be a legitimate user of a particular fixed part.

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

Bearer service: a type of telecommunication service that provides a defined capability for the transmission of signals between user-network interfaces.

NOTE 3: The DECT user-network interface corresponds to the top of the network layer (layer 3).

C-plane: the Control plane of the DECT protocol stacks, which contains all of the internal DECT protocol control, but may also include some external user information.

NOTE 4: The C-plane stack always contains protocol entities up to and including the network layer.

Call: all of the NetWorK (NWK) layer processes involved in one network layer peer-to-peer association.

NOTE 5: Call may sometimes be used to refer to processes of all layers, since lower layer processes are implicitly required.

DECT NetWork (DNW): a network that uses the DECT air interface to interconnect a local network to one or more portable applications. The logical boundaries of the DECT network are defined to be at the top of the DECT network layer.

NOTE 6: A DECT network is a logical grouping that contains one or more fixed radio terminations plus their associated portable radio termination . The boundaries of the DECT network are not physical boundaries.

End System (ES): a logical grouping that contains application processes and supports telecommunication services.

NOTE 7: From the Open System Interconnection (OSI) point of view, end systems are considered as sources and sinks of information.

External handover: the process of switching a call in progress from one fixed radio termination to another fixed radio termination.

Fixed Part (DECT Fixed Part) (FP): a physical grouping that contains all of the elements in the DECT network between the local network and the DECT air interface.

NOTE 8: A DECT fixed part contains the logical elements of at least one fixed radio termination, plus additional implementation specific elements.

Fixed radio Termination (FT): a logical group of functions that contains all of the DECT processes and procedures on the fixed side of the DECT air interface.

NOTE 9: A fixed radio termination only includes elements that are defined in the DECT Common Interface standard (DECT CI). This includes radio transmission elements together with a selection of layer 2 and layer 3 elements.

Geographically unique identity: this term relates to fixed part identities, PARIs and RFPIs. It indicates that two systems with the same PARI, or respectively two RFPs with the same RFPI, can not be reached or listened to at the same geographical position.

NOTE 10: PARI stands for Primary Access Rights Identifier; RFPI stands for Radio Fixed Part Identifier.

Global NetWork (GNW): a telecommunication network capable of offering a long distance telecommunication service.

NOTE 11: The term does not include legal or regulatory aspects, nor does it indicate if the network is a public or a private network.

Globally unique identity: the identity is unique within DECT (without geographical or other restrictions).

Handover: the process of switching a call in progress from one physical channel to another physical channel. These processes can be internal (see internal handover) or external (see external handover).

NOTE 12: There are two physical forms of handover, intra-cell handover and inter-cell handover. Intra-cell handover is always internal. Inter-cell handover can be internal or external.

Incoming call: a call received at a portable part.

Inter-cell handover: the switching of a call in progress from one cell to another cell.

Internal handover: handover processes that are completely internal to one fixed radio termination. Internal handover reconnects the call at the lower layers, while maintaining the call at the NWK layer.

NOTE 13: The lower layer reconnection can either be at the Data Link Control (DLC) layer (connection handover) or at the Medium Access Control (MAC) layer (bearer handover).

Interoperability: the capability of fixed parts and portable parts, that enable a portable part to obtain access to teleservices in more than one location area and/or from more than one operator (more than one service provider).

Interoperator roaming: roaming between fixed part coverage areas of different operators (different service providers).

InterWorking Unit (IWU): a unit that is used to interconnect subnetworks.

NOTE 14: The IWU will contain the interworking functions necessary to support the required subnetwork interworking.

Intra-cell handover: the switching of a call in progress from one physical channel of one cell to another physical channel of the same cell.

Intraoperator roaming: roaming between different fixed part coverage areas of the same operator (same service provider).

Local NetWork (LNW): a telecommunication network capable of offering local telecommunication services.

NOTE 15: The term does not include legal or regulatory aspects, nor does it indicate if the network is a public network or a private network.

Locally unique identity: the identity is unique within one FP or location area, depending on application.

Location area: the domain in which a portable part may receive (and/or make) calls as a result of a single location registration.

Location registration: the process whereby the position of a DECT portable termination is determined to the level of one location area, and this position is updated in one or more databases.

NOTE 16: These databases are not included within the DECT fixed radio termination .

Lower Layer Management Entity (LLME): a management entity that spans a number of lower layers, and is used to describe all control activities which do not follow the rules of layering.

NOTE 17: The DECT LLME spans the network layer, the DLC layer, the MAC layer and the physical layer.

MAC connection (connection): an association between one source MAC Multi-Bearer Control (MBC) entity and one destination MAC MBC entity. This provides a set of related MAC services (a set of logical channels), and it can involve one or more underlying MAC bearers.

Outgoing call: a call originating from a portable part.

Paging: the process of broadcasting a message from a DECT fixed part to one or more DECT portable parts.

NOTE 18: Different types of paging message are possible. For example, the {REQUEST-PAGING} message orders the recipient to respond with a call set-up attempt.

Paging area: the domain in which the portable part will be paged as a part of incoming call establishment.

NOTE 19: In general, the paging area will be equal to the Temporary Portable User Identity (TPUI) domain, since the TPUI is used for paging.

Portable Application (PA): a logical grouping that contains all the elements that lie beyond the DECT network boundary on the portable side.

NOTE 20: The functions contained in the portable application may be physically distributed, but any such distribution is invisible to the DECT network.

Portable Part (PP) (DECT Portable Part): a physical grouping that contains all elements between the user and the DECT air interface. Portable part is a generic term that may describe one or several physical pieces.

NOTE 21: A DECT portable part is logically divided into one portable termination plus one or more portable applications.

Portable radio Termination (PT): a logical group of functions that contains all of the DECT processes and procedures on the portable side of the DECT air interface.

NOTE 22: A portable radio termination only includes elements that are defined in the DECT CI standard. This includes radio transmission elements (layer 1) together with a selection of layer 2 and layer 3 elements.

Public Access Profile (PAP): a defined part of the DECT Common Interface standard (DECT CI) that ensures interoperability between fixed parts and portable parts for public access services.

Radio End Point (REP): a physical grouping that contains one radio transceiver (transmitter/receiver), fixed or portable.

NOTE 23: A REP may operate only as a receiver or only as a transmitter.

Radio Fixed Part (RFP): one physical sub-group of a fixed part that contains all the radio end points (one or more) that are connected to a single system of antennas.

Registration: an ambiguous term, that should always be qualified. See either location registration or subscription registration.

Roaming: the movement of a portable part from one fixed part coverage area to another fixed part coverage area, where the capabilities of the fixed parts enable the portable part to make or receive calls in both areas.

NOTE 24: Roaming requires the relevant fixed parts and portable part to be interoperable.

Roaming service: a service which can be used in more than one fixed part coverage area.

Segment: one of the pieces of data that is produced by the process of segmentation.

NOTE 25: In general, one segment only represents a portion of a complete message.

Segmentation: the process of partitioning one Service Data Unit (SDU) from a higher layer into more than one Protocol Data Unit (PDU). The reverse process is assembly.

Service provider (telecommunications service provider): the individual or entity who or which interfaces to the customer in providing telecommunications service.

NOTE 26: The term does not imply any legal or regulatory conditions, nor does it indicate whether public service or private service is provided.

NOTE 27: The term service provider is also used with a different meaning in the ISO/OSI layered model.

Sequencing (sequence numbering): the process of adding a sequence number to a set of data packets so that the packets can be reassembled in the correct order, regardless of the order they are received. See also segmentation.

Subscriber (customer): the natural person or the juristic person who has subscribed to telecommunication services, and is therefore responsible for payment.

Subscription registration: the infrequent process whereby a subscriber obtains access rights to one or more fixed parts.

NOTE 28: Subscription registration is usually required before a user can make or receive calls.

Supplementary service: a service that modifies or supplements a basic telecommunications service.

NOTE 29: Three functional groups of supplementary services are defined for DECT:

1) DECT TRANSPARENT supplementary services:

- the service elements are unspecified within the DECT ETS 300 175.

2) DECT STANDARD supplementary services:

- the service elements are specified within the DECT ETS 300 175, by reference to other standards.

3) DECT SPECIFIC supplementary services:

- the service elements are fully specified within the DECT ETS 300 175.

Teleservice: a type of telecommunications service that provides the complete capability, including terminal equipment functions, for communication between users, according to protocols that are established by agreement.

TPUI domain: the domain over which every Temporary Portable User Identity (TPUI) is (locally) unique.

NOTE 30: In general, the TPUI domain will be equal to the paging area and thereby equal to the location area.

U-plane: the user plane of the DECT protocol stacks. This plane contains most of the end-to-end (external) user information and user control.

NOTE 31: The U-plane protocols do not include any internal DECT protocol control, and it may be null at the network layer and at the DLC layers for some services.

User (of a telecommunication network): A person or machine delegated by a subscriber (by a customer) to use the services and/or facilities of a telecommunication network.

3.2 Network layer abbreviations

For the purpose of this ETS, the following abbreviations apply:

AC	Authentication Code
ACK	ACKnowledgement
ADPCM	Adaptive Differential Pulse Code Modulation
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity. There are three categories of ARIs: - PARI = Primary ARI; - SARI = Secondary ARI; - TARI = Tertiary ARI.
ARQ	Automatic Repeat reQuest
BCD	Binary Coded Decimal
CC	Call Control
CCITT	(the) International Telegraph and Telephone Consultative Committee
CI	Common Interface (standard)
CISS	Call Independent Supplementary Services
CK	Cipher Key
CODEC	COder-DECoder
CLMS	ConnectionLess Message Service
COMS	Connection Oriented Message Service
CRC	Cyclic Redundancy Check
CRSS	Call Related Supplementary Services
CSPDN	Circuit Switched Public Data Network
C-Plane	Control Plane. See definitions
C/L	ConnectionLess mode
C/O	Connection Orientated mode
DAM	DECT Authentication Module
DCK	Derived Cipher Key
DECT	Digital European Cordless Telecommunications
DLC	Data Link Control. Layer 2b of the DECT protocol stack

DLEI	Data Link Endpoint Identifier (DLC layer)
DNW	DECT NetWork. See definitions
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DTMF	Dual Tone Multi-Frequency
ES	End System
FP	Fixed Part. See definitions
FT	Fixed radio Termination. See definitions
HDB	Home Data Base
IA5	International Alphabet No.5 as defined by CCITT
IFEI	International Fixed Equipment Identity
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
ISDN	Integrated Services Digital Network
IWU	InterWorking Unit. See definitions
K	authentication Key
KS	PP authentication Session Key
KS'	FP authentication Session Key
KSG	Key Stream Generator
KSS	Key Stream Segment
LAPC	a DLC layer C-plane protocol entity
LAN	Local Area Network
LCE	Link Control Entity
LCN	Logical Connection Number
LLME	Lower Layer Management Entity
LLN	Logical Link Number
LSB	Least Significant Bit
MAC	Medium Access Control. Layer 2a of the DECT protocol stack
MM	Mobility Management. A NWK layer functional grouping
MSB	Most Significant Bit

NWK	NetWorK. Layer 3 of the DECT protocol stack (this layer)
PAP	Public Access Profile
PARI	Primary Access Rights Identity
PARK	Portable Access Rights Key
PBX(PABX)	Private (Automatic) Branch eXchange
PLI	Park Length Indicator
PMID	Portable part MAC IDentity (MAC layer)
PP	Portable Part
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
PT	Portable radio Termination. See definitions
PUN	Portable User Number
PUT	Portable User Type
RAND-F	a RANdom challenge issued by a FT
RAND-P	a RANdom challenge issued by a PT
REP	Radio End Point. See definitions
RES1	a RESponse calculated by a PT
RES2	a RESponse calculated by a FT
RFP	Radio Fixed Part. See definitions
RFPI	Radio Fixed Part Identity
RS	a value used to establish authentication session keys
SAP	Service Access Point
SARI	Secondary Access Rights Identity
SCK	Static Cipher Key
SS	Supplementary Services
TARI	Tertiary Access Rights Identity
TCL	Telephone Coupling Loss
TDMA	Time Division Multiple Access
TI	Transaction Identifier
TPUI	Temporary Portable User Identity

UAK	User Authentication Key
UPI	User Personal Identification
U-Plane	User Pane. See definitions
VDB	Visitors Data Base
XRES1	an eXpected RESponse calculated by a FT
XRES2	an eXpected RESponse calculated by a PT

4 Overview of the network layer

The DECT network layer (layer 3) protocol contains the following groups of functions. Refer to figure 1.

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

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

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

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

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

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

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

The call control procedures and messages used in this protocol are based on the layer 3 procedures and messages defined in ETS 300 102-1 [21a]. Many of the alterations adopted in prI-ETS 300 022 [22] have also been adopted here.

The other groups of procedures are also based on the similar groupings as defined in prI-ETS 300 022 [22].

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

a) the link control entity, that provides a coordinated use of the layer 2 resources, including management of the broadcast services;

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

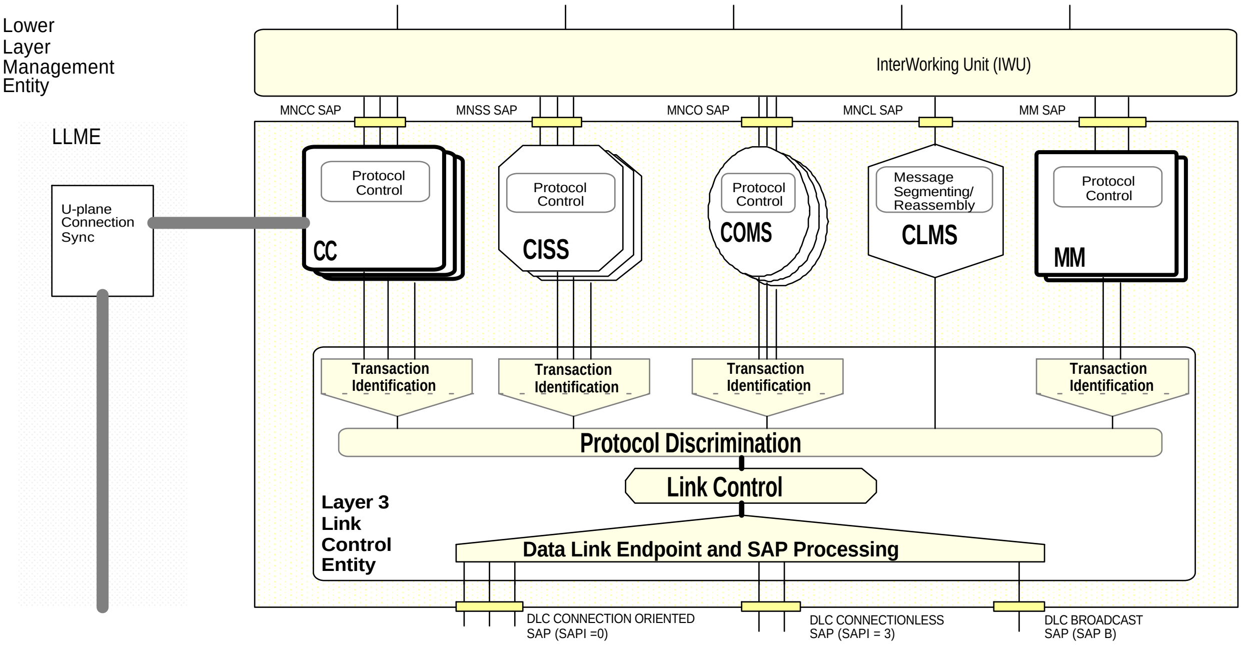
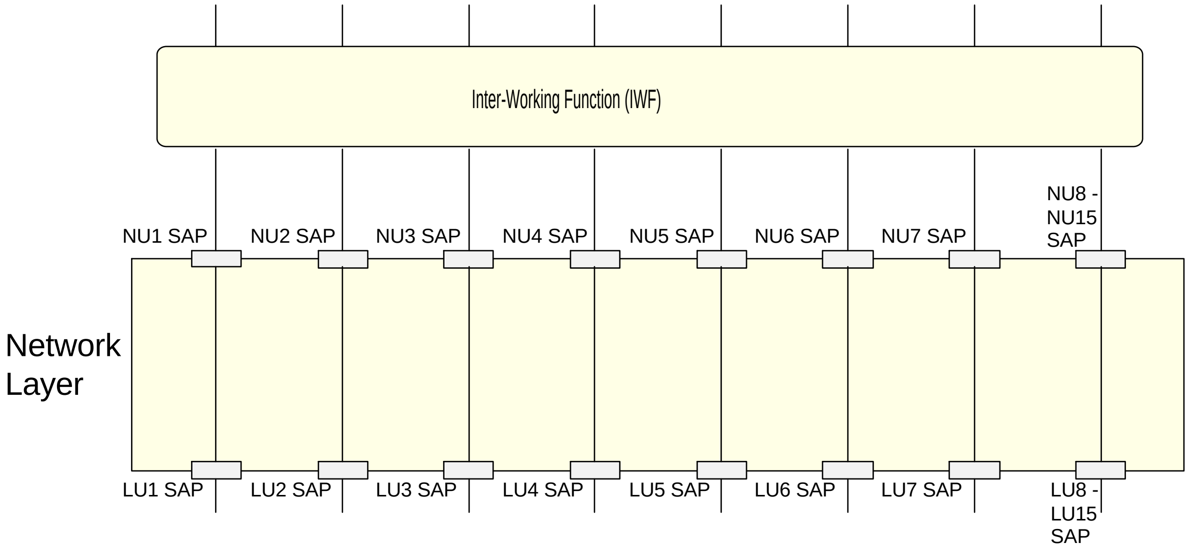


Figure 1: C-Plane Model



The U-Plane is completely null at Network Layer

Figure 2: U-Plane Model

5 Overview of procedures

5.1 General

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

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

As shown in the C-plane model (figure 1, Clause 4) the link control entity shall provide a common foundation for all the other "higher entities". The Call Control (CC), Call Independent Supplementary Services (CISS), Connection Oriented Message Service (COMS), ConnectionLess Message Service (CLMS) and Mobility Management (MM) are collectively described as "higher entities". The Link Control Entity (LCE) shall provide a message routing service to these "higher entities", using the combination of the Data Link Control (DLC) layer DLEI and the higher entity protocol discriminator element.

This ETS shall only consider the provision and coordination of services to a single portable radio termination. The provision of services to multiple PTs by one FT shall be understood to be based on independent operation, and shall not be considered further within this ETS.

Within one PT, multiple instances of the CC, CISS and COMS entities may exist but there may be only two instances of the MM and one instance of the CLMS entities as shown in figure 1, Clause 4.

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

- S-FORMAT messages; these messages have a similar structure to ETS 300 102-1 [21a] and prI-ETS 300 022 [22];

- B-FORMAT messages; these messages are specially coded to meet the physical constraints of the broadcast service. They are not similar to ETS 300 102-1 [21a] 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

Call Control (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 Lower Layer Management Entity (LLME). Both the CC service and this associated U-plane service are required to provide the complete service to a user.

5.2.2 Call establishment

5.2.2.1 Call set-up

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

- International Portable User Identity (IPUI) (or group TPUI) (portable identity);
- Access Rights Identity (ARI) (fixed identity);
- called party number;
- interworking attributes;
- call attributes:
    * C-plane attributes (network layer and DLC layer);
    * U-plane attributes (DLC and MAC layers).

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

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

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

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

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

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

5.2.2.2 Service negotiation

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

5.2.3 Call connect

The call connect procedures are used to signal that the peer-to-peer U-plane communication has been enabled. These procedures provide signalling to/from the interworking units 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 must 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 network 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

5.3.1 General

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

Supplementary services are divided into two types:

- Call Related Supplementary Services (CRSS);

- Call Independent Supplementary Services (CISS).

Call Related Supplementary Services (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.

Call Independent Supplementary Services (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 Call Independent Supplementary Service (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 supplementary services, two of which are stimulus, the third being functional. These protocols are:

- the keypad protocol;

- the feature key management protocol;

- the functional protocol.

The keypad protocol can only be used for Call Related Supplementary Services, the feature key management protocol and the functional protocol may be used for call related or call independent supplementary services.

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-INFORMATION} messages and in the CISS messages. The <<DISPLAY>> information element may be included in various messages sent by the network to the user, as defined in subclause 6.3.

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

The protocol is stimulus in the sense that it does not require any knowledge about the invoked supplementary service 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 Call Control (CC) messages or CISS messages as specified in subclause 6.3, message in the user-to-network direction. The <<FEATURE-INDICATE>> information element may be included in various basic Call Control (CC) messages or CISS messages in the network-to-user direction.

This protocol typically applies to supplementary services operation during calls but also allows for Call Independent Supplementary Services (CISS) control. Call Independent Supplementary Services (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 supplementary services. The first category, called the separate message approach, utilises separate message types to indicate a desired function. The hold and retrieve family of messages are identified for this category.

The second category, called the common information element procedure, utilises the <<FACILITY>> information element and applies only to supplementary services that do not require synchronisation of resources between the user and the network. A {FACILITY}, a {CISS-REGISTER} or an existing call control 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 supplementary service by the portable or fixed radio termination supporting it. This protocol, therefore, allows for autonomous operation by the DECT network, with no user (human) intervention. The protocol does not define the man-machine-interface.

5.4 Overview of Connection Oriented Message Service (COMS)

5.4.1 General

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

5.4.2 COMS establishment

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

- TPUI or IPUI portable identity;
- ARI fixed identity;
- interworking attributes;
- COMS attributes (C-plane attributes for network layer and DLC layer).

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

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

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

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

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

5.4.3 Service negotiation

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

5.4.4 COMS connect

The COMS connect procedures are used to signal that the interworking-to-interworking communication (C-plane) has been enabled. These procedures provide signalling to/from the interworking units 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 interworking unit. Long packets may be segmented, and are only delivered and acknowledged if all segments are received correctly.

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

5.4.6 COMS suspend and resume

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

NOTE: This service is intended to support virtual data circuits such as for CCITT Recommendation X.25 [67] 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 ConnectionLess Message Service (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 Mobility Management (MM) entity handles functions necessary for the secure provision of DECT services and supports in particular incoming calls. These functions are necessary due to the mobile nature of the DECT user and due to highly probable fraudulent attacks upon the radio interface.

MM procedures are described in seven groups:

a) identity procedures;

b) authentication procedures;

c) location procedures;

d) access rights procedures;

e) key allocation procedure;

f) parameter retrieval procedure;

g) ciphering related procedure.

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

5.6.2 Identity procedures

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

The identity procedures serve two 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 fixed radio terminations 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.

The authentication procedures serve two purposes:

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

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

5.6.4 Location procedures

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

The location procedures are concerned with two levels of location:

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

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

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

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

Three location procedures are defined:

- location registration procedure for locating and attaching;

- detach procedure for detaching;

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

5.6.5 Access rights procedures

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

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

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

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

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

5.6.6 Key allocation procedure

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

5.6.7 Parameter retrieval procedure

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

5.6.8 Ciphering related procedure

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

5.7 Overview of Link Control Entity (LCE)

5.7.1 General

The LCE is the lowest entity in the network 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-PAGING} messages, and submitting them to the B-SAP;

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

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

h) assignment of new layer 3 instances to existing data link endpoints;

i) reporting data link failures to all layer 3 instances that are using that link.

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

5.7.2 Data Link Endpoint Identifier (DLEI)

Every message submitted to the LCE must 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 shall create a single mapping, but the selection procedures are not defined in this ETS.

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

5.7.3 Data link establishment

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

The LCE shall request a suitable DLEI from the LLME in response to this request, using both the IPUI (or individual assigned TPUI) and the originating entity (CC, CISS, COMS, CLMS or MM).

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

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

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

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

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

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

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

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

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

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

5.7.4 Data link re-establishment

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

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

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

5.7.5 Data link release

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

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

5.7.6 Data link suspend and resume

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

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

5.7.7 Queuing of messages

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

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

5.7.8 Request paging

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

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

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

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

NOTE: A reserved coding of the {LCE-REQUEST-PAGE} message may be used to announce the CLMS. This differs from all other codings because it refers to a connectionless service, therefore it does not require the receiving PT to generate a reply. Refer to subclause 8.2.

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.

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

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

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

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

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

6.1.2 Information elements

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

- DECT specific information elements;

- DECT standard information elements;

- DECT transparent information elements.

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

DECT standard information elements are those elements that relate to the interaction of the DECT protocol with the interworking units 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 mechanisms 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: Call Control (CC) message summary (includes call related supplementary services)

	Dir.	Subclause
Call establishment messages		
CC-SETUP	Both	6.3.2.1
CC-INFOrmation	Both	6.3.2.2
CC-SETUP-ACKnowledge	F=>P	6.3.2.3
CC-CALL-PROCeeding	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-ACKnowledge	F=>P	6.3.2.7
Call information phase messages		
CC-INFOrmation	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-INFOrmation	Both	6.3.2.14
Call related supplementary services		
FACILITY	Both	6.3.3.1
HOLD	Both	6.3.3.2
HOLD-ACKnowledge	Both	6.3.3.3
HOLD-REJECT	Both	6.3.3.4
RETRIEVE	Both	6.3.3.5
RETRIEVE-ACKnowledge	Both	6.3.3.6
RETRIEVE-REJECT	Both	6.3.3.7
Call release messages		
CC-INFOrmation	Both	6.3.2.2
CC-RELEASE	Both	6.3.2.8
CC-RELEASE-COMplete	Both	6.3.2.9

NOTE: Call information phase messages shall only be sent while in the "ACTIVE" state.

6.2.2 Summary of CISS messages

Table 2: Call Independent Supplementary Services (CISS) message summary

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

6.2.3 Summary of COMS messages

Table 3: Connection Oriented Message Service (COMS) message summary

	Dir.	Subclause
COMS establishment messages		
COMS-SETUP	Both	6.3.4.1
COMS-CONNECT	Both	6.3.4.4
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-COMplete	Both	6.3.4.6

6.2.4 Summary of CLMS messages

Table 4: Connectionless Message Service (CLMS) message summary

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

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

6.2.5 Summary of MM messages

Table 5: Mobility Management (MM) message summary

	Dir.	Subclause
Identity messages		
TEMPORARY-IDENTITY-ASSIGN	F=>P	6.3.6.24
TEMPORARY-IDENTITY-ASSIGN-ACK	P=>F	6.3.6.25
TEMPORARY-IDENTITY-ASSIGN-REJ	P=>F	6.3.6.26
IDENTity-REQUEST	F=>P	6.3.6.15
IDENTity-REPLY	P=>F	6.3.6.14
Authentication messages		
AUTHenticate-REQUEST	Both	6.3.6.9
AUTHenticate-REPLY	Both	6.3.6.8
AUTHenticate-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	P=>F	6.3.6.10

6.2.6 Summary of LCE messages

Table 6: Link Control Entity (LCE) message summary

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

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

6.3 S-FORMAT message functional contents

6.3.1 S-FORMAT message overview

Each of the S-FORMAT message definitions includes:

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

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

   1) the name of the information element;

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

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

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

c) further explanatory notes as required.

The information elements are always listed in their order of appearance; this order is mandatory for all instances of the message. Mandatory elements always appear before optional elements.

6.3.2 CC-messages

6.3.2.1 CC-SETUP

This message is sent to initiate call establishment.

Message Type	Format	Directions
CC-SETUP	S	Both

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

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

NOTE 1: The use of a <<PORTABLE-IDENTITY>> and a <<FIXED-IDENTITY>> are mandatory for both indirect and direct data link establishment. The portable identities used are defined in Clause 9.

NOTE 2: The <<CALL-ATTRIBUTES>> and <<INTERWORKING-ATTRIBUTES>> are mandatory if the <<BASIC-SERVICE>> element indicates "other". They are not allowed if the <<BASIC-SERVICE>> element indicates "default attributes".

NOTE 3: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<CALL-ATTRIBUTES>> indicating "prioritised list" for negotiation. Up to three versions of the <<CALL-ATTRIBUTES>> element may then follow. See subclause 15.2.

NOTE 4: If more than one connection is required, a list of <<CONNECTION-ATTRIBUTES>> may be included preceded by the <<REPEAT-INDICATOR>> element indicating "non-prioritised list". If the <<CONNECTION-ATTRIBUTES>> element is omitted, the attributes shall be indirectly defined by reference to the connection(s) indicated by the <<CONNECTION-IDENTITY>> element.

NOTE 5: Included if the PT or the FT optionally indicates that all information necessary for call establishment is included in the {CC-SETUP} message.

NOTE 6: Optionally included if the FT optionally provides additional information describing tones.

NOTE 7: Optionally included for data services whenever these parameters are applicable.

NOTE 8: Mandatory for call set-up of a rate adaption service. Refer to ETS 300 175-4 [4].

NOTE 9: Included only as part of external handover.

NOTE 10: Mandatory for services using LU6 (V.110/X.30 rate adaption).

NOTE 11: Called party number information may only be conveyed in the <<CALLED-PARTY-NUMBER>> element. The <<"KEYPAD">> element may only be included to convey other call establishment information.

6.3.2.2 CC-INFOrmation

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

Message Type	Format	Directions
CC-INFOrmation	S	Both

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

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

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

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

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

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

6.3.2.3 CC-SETUP-ACKnowledge

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

Message Type	Format	Directions
CC-SETUP-ACKnowledge	S	F=>P

Information Element		Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator		7.2	M	-	½
Transaction Identifier		7.3	M	-	½
Message Type		7.4	M	-	1
Info type	3	7.7.20	O	-	3-*
Portable identity		7.7.30	O	-	5-20
Fixed identity		7.7.18	O	-	5-20
Location area		7.7.25	O	-	3-*
Call Attributes	4	7.7.11	O	-	6-11
Connection identity		7.7.12	O	-	3-*
Facility		7.7.15	O	-	2-*
Progress Indicator		7.7.31	O	-	4
Display		7.5.5	O	-	2-*
Signal	2	7.6.8	O	-	2
Feature Indicate		7.7.17	O	-	4-*
Transit Delay	5	7.7.42	O	-	4
Window size	5	7.7.43	O	-	4
Delimiter request	6	7.6.2	O	-	1
IWU-TO-IWU		7.7.23	O	-	4-*
IWU-PACKET		7.7.22	O	-	4-*

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

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

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

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

NOTE 4: Included if prioritised list negotiation is used.

NOTE 5: Included if operational parameter negotiation is used.

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

6.3.2.4 CC-CALL-PROCeeding

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

Message Type	Format	Directions
CC-CALL-PROCeeding	S	F=>P

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

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

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

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

NOTE 3: Included if prioritised list negotiation is used.

NOTE 4: Included if operational parameter negotiation is used.

6.3.2.5 CC-ALERTING

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

Message Type	Format	Directions
CC-ALERTING	S	Both

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

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

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

NOTE 2: Included if prioritised list negotiation is used.

NOTE 3: Included if operational parameter negotiation is used.

6.3.2.6 CC-CONNECT

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

Message Type	Format	Directions
CC-CONNECT	S	Both

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

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

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

NOTE 2: Included if prioritised list negotiation is used.

NOTE 3: Included if operational parameter negotiation is used.

6.3.2.7 CC-CONNECT-ACKnowledge

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.

Message Type	Format	Directions
CC-CONNECT-ACKnowledge	S	F=>P

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

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

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 and then return a {CC-RELEASE-COM} message.

Message Type	Format	Directions
CC-RELEASE	S	Both

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

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

6.3.2.9 CC-RELEASE-COMplete

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

Message Type	Format	Directions
CC-RELEASE-COMplete	S	Both

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

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

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

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

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

6.3.2.10 CC-SERVICE-CHANGE

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

Message Type	Format	Directions
CC-SERVICE-CHANGE	S	Both

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

M = Mandatory;
O = Optional;

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

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

6.3.2.11 CC-SERVICE-ACCEPT

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

Message Type	Format	Directions
CC-SERVICE-ACCEPT	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Connection identity	7.7.12	O	O	3-*

M = Mandatory;
O = Optional;

6.3.2.12 CC-SERVICE-REJECT

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

Message Type	Format	Directions
CC-SERVICE-REJECT	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1

M = Mandatory;

6.3.2.13 CC-NOTIFY

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

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

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

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

6.3.2.14 IWU-INFOrmation

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

Message Type	Format	Directions
IWU INFOrmation	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Segmented info	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-*

M = Mandatory;
O = Optional;

6.3.3 Supplementary services messages (call related and call independent)

6.3.3.1 FACILITY

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

Message Type	Format	Directions
FACILITY	S	Both

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

M = Mandatory;

N = Not allowed;

O = Optional;

6.3.3.2 HOLD

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

Message Type	Format	Directions
HOLD	S	Both

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

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

6.3.3.3 HOLD-ACKnowledge

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

Message Type	Format	Directions
HOLD-ACKnowledge	S	Both

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

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

6.3.3.4 HOLD-REJECT

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

Message Type	Format	Directions
HOLD-REJECT	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Display	7.5.5	O	N	2-*
Reject Reason	7.7.34	O	0	3

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

6.3.3.5 RETRIEVE

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

Message Type	Format	Directions
RETRIEVE	S	Both

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

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

6.3.3.6 RETRIEVE-ACKnowledge

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

Message Type	Format	Directions
RETRIEVE-ACKnowledge	S	Both

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

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

6.3.3.7 RETRIEVE-REJECT

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

Message Type	Format	Directions
RETRIEVE-REJECT	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Display	7.5.5	O	N	2-*
Reject Reason	7.7.34	O	O	3

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

6.3.3.8 CISS-REGISTER

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

Message Type	Format	Directions
CISS-REGISTER	S	Both

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

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

6.3.3.9 CISS-RELEASE-COMplete

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

Message Type	Format	Directions
CISS-RELEASE-COMplete	S	Both

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

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

6.3.4 COMS-messages

6.3.4.1 COMS-SETUP

This message is used to initiate a COMS call.

Message Type	Format	Directions
COMS-SETUP	S	Both

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

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

NOTE 1: Portable identity and fixed identity are mandatory for direct data link establishment (see subclause 5.7.3).

6.3.4.2 COMS-INFOrmation

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

Message Type	Format	Directions
COMS-INFOrmation	S	Both

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

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

6.3.4.3 COMS-ACKnowledge

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

Message Type	Format	Directions
COMS-ACKnowledge	S	Both

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

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

6.3.4.4 COMS-CONNECT

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

Message Type	Format	Directions
COMS-CONNECT	S	Both

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

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

6.3.4.5 COMS-RELEASE

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

Message Type	Format	Directions
COMS-RELEASE	S	Both

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

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

6.3.4.6 COMS-RELEASE-COMplete

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

Message Type	Format	Directions
COMS-RELEASE-COMplete	S	Both

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

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

6.3.5 CLMS-message

6.3.5.1 CLMS-VARIABLE

Message Type	Format	Directions
CLMS-VARIABLE	S	Both

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1
Portable identity	7.7.30	O	O	5-20
Segmented-Info (NOTE 3)	7.7.37	O	O	4
Alphanumeric (NOTE 2)	7.7.3	O	O	4-*
IWU-TO-IWU (NOTE 2)	7.7.23	O	O	4-*
IWU-PACKET (NOTE 2)	7.7.22	O	O	4-*

M = Mandatory;
O = Optional;

NOTE 1: The maximum message shall not exceed 63 octets, so that it may be transported in a single DLC frame.

NOTE 2: The message shall either contain one <<ALPHANUMERIC>> element or one <<IWU-TO-IWU>> element or one <<IWU-PACKET>> element.

NOTE 3: The <<SEGMENTED-INFO>> element shall be used if the complete information cannot be fitted into one message.

6.3.6 MM-messages

6.3.6.1 ACCESS-RIGHTS-ACCEPT

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

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

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

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

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

6.3.6.2 ACCESS-RIGHTS-REJECT

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

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

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

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

6.3.6.3 ACCESS-RIGHTS-REQUEST

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

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

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

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

6.3.6.4 ACCESS-RIGHTS-TERMINATE-ACCEPT

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

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

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	½
Transaction Identifier	7.3	M	M	½
Message Type	7.4	M	M	1

M = Mandatory;

6.3.6.5 ACCESS-RIGHTS-TERMINATE-REJECT

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

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

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

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

6.3.6.6 ACCESS-RIGHTS-TERMINATE-REQUEST

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

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

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

M = Mandatory;
O = Optional;

NOTE 1: A list of <<FIXED-IDENTITY>> information elements (PARKs) can be included by using the <<REPEAT-INDICATOR>> information element. In this case the coding for "non-prioritised list" shall be used. Not more then 3 PARKs should be included.

6.3.6.7 AUTHentication-REJECT

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

Message Type	Format	Directions
AUTHentication-REJECT	S	Both

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

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

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

6.3.6.8 AUTHentication-REPLY

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

Message Type	Format	Directions
AUTHentication-REPLY	S	Both

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

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

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

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

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

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

6.3.6.9 AUTHentication-REQUEST

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

Message Type	Format	Directions
AUTHentication-REQUEST	S	Both

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

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

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

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

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

6.3.6.10 CIPHER-REJECT

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

Message Type	Format	Directions
CIPHER-REJECT	S	Both

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

M = Mandatory;
O = Optional;

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

6.3.6.11 CIPHER-REQUEST

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

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

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

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

6.3.6.12 CIPHER-SUGGEST

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

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

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

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

6.3.6.13 DETACH

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

Message Type	Format	Directions
DETACH	S	P=>F

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

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

6.3.6.14 IDENTITY-REPLY

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

Message Type	Format	Directions
IDENTity-REPLY	S	P=>F

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

M = Mandatory;
O = Optional;

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

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

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

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

6.3.6.15 IDENTITY-REQUEST

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

Message Type	Format	Directions
IDENTity-REQUEST	S	F=>P

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

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

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

6.3.6.16 KEY-ALLOCATE

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

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

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

M = Mandatory;

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

6.3.6.17 LOCATE-ACCEPT

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

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

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

M = Mandatory;
O = Optional;

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

6.3.6.18 LOCATE-REJECT

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

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

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

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

6.3.6.19 LOCATE-REQUEST

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

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

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	5-20
Fixed identity	7.7.18	-	O	5-20
Location area	7.7.25	-	O	3-*
NWK assigned identity	7.7.28	-	O	5-20
Cipher info	7.7.10	-	O	4-5
Set-up capability	7.7.40	-	O	3-4
Terminal capability	7.7.10	-	O	3-6
IWU-TO-IWU	7.7.23	-	O	4-*

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

6.3.6.20 MM-INFO-ACCEPT

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

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

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

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

6.3.6.21 MM-INFO-REJECT

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

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

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

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

6.3.6.22 MM-INFO-REQUEST

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

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

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

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

6.3.6.23 MM-INFO-SUGGEST

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

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

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

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

6.3.6.24 TEMPORARY-IDENTITY-ASSIGN

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

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

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

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

NOTE: At least one <<IDENTITY>> information element shall be included in a {TEMPORARY-IDENTITY-ASSIGN} message.

6.3.6.25 TEMPORARY-IDENTITY-ASSIGN-ACKnowledge

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

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

Information Element	Sub-clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	½
Transaction Identifier	7.3	-	M	½
Message Type	7.4	-	M	1

M = Mandatory;
- = not applicable.

6.3.6.26 TEMPORARY-IDENTITY-ASSIGN-REJect

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

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

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

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

6.3.7 LCE-messages

6.3.7.1 LCE-PAGE-RESPONSE

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

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

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

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-PAGING} message.

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

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

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

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

6.4 B-FORMAT message functional contents

6.4.1 B-FORMAT message overview

Each of the B-FORMAT message definitions includes:

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

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

1) the name of the information element;

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

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

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

c) further explanatory notes as required.

The information elements are always listed in their order of appearance, this order is mandatory for all instances of the message. Mandatory elements always appear before optional elements.

6.4.2 LCE-REQUEST-PAGE

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

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

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

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

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

6.4.3 CLMS-FIXED

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

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

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

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

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

NOTE 1: This element appears in all message sections.

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

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

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

7 S-FORMAT message structures

7.1 Overview

The S-FORMAT message structures are based on the principles adopted in ETS 300 102-1 [21a]. Similar modifications to those adopted in prI-ETS 300 022 [22] have also been used. The detailed coding of all elements is unique to this ETS.

Every message consists of the following parts:

a) protocol discriminator;

b) transaction identifier;

c) message type;

d) mandatory elements;

e) optional elements.

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

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

```
                                   Octet:
┌────────────────┬────────────────┐
│ Transaction    │ Protocol       │  1
│ Identifier     │ Discriminator  │
├────────────────┴────────────────┤
│  Extended Transaction Value     │  1a
│                                 │
├─────────────────────────────────┤
│  Message Type                   │  2
│                                 │
├─────────────────────────────────┤
│                                 │  3
:-- Mandatory elements ---------:
:                               :
:-------------------------------:
│                                 │
├─────────────────────────────────┤
│                                 │
:-- Optional elements ----------:
:                               :
:-------------------------------:
│                                 │  N
└─────────────────────────────────┘
```

S-FORMAT message structures

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

7.2 Protocol Discrimination (PD) element

```
Bit: | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
     ┌--------------┌────────────────┐  Octet:
     :              │ PROTOCOL       │   1
     :(see subcl 7.3)│ DISCRIMINATOR  │
     └--------------└────────────────┘
```

Protocol Discriminator (PD) bits

Protocol Discriminator (PD):

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

All other values reserved.

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

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

7.3 Transaction Identifier (TI) element

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

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

Table 7: Allowable range of Transaction Identifiers (TIs)

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

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

```
Bit: | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
     ┌────┬────────────┬ - - - - - - -┐   Octet:
     FLAG │TRANSACTION │              :   1
     │(F) │ VALUE (TV) │(see subcl 7.2):
     └────┴────────────┴ - - - - - - -┘
```

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│ 1   1   1│                 :  1
     │(F) │TV extend │(see subcl 7.2)  :
     ├────┴─────────┴──────────────────┤
     │  EXTENDED TRANSACTION VALUE     │  1a
     │            (TVX)                │
     └─────────────────────────────────┘
```

Extended Transaction Identifier (ETI) bits

7.4 Message type element

```
Bit: | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
     ┌────┬────────────────────────────┐  Octet:
     │ 0  │      MESSAGE TYPE          │   2
     │    │                            │
     └────┴────────────────────────────┘
```

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 Call Control (CC)

Table 8: CC message type coding

	Bits							
CC message types	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-PROCeeding	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-ACKnowledge	0	0	0	0	1	1	0	1
CC-CONNECT-ACKnowledge	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-COMplete	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-INFOrmation	0	1	1	1	1	0	1	1

7.4.2 Messages for Supplementary Services (SS)

Table 9: SS message type coding

	Bits							
CISS message types (call independ.)	8	7	6	5	4	3	2	1
CISS-RELEASE-COMplete	0	1	0	1	1	0	1	0
FACILITY	0	1	1	0	0	0	1	0
CISS-REGISTER	0	1	1	0	0	1	0	0
CRSS message types (call related)	8	7	6	5	4	3	2	1
HOLD	0	0	1	0	0	1	0	0
HOLD-ACKnowledge	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-ACKnowledge	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 Connection Oriented Message Service (COMS)

Table 10: COMS message type coding

	Bits							
COMS message types	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-RELEASE	0	1	0	0	1	1	0	1
COMS-RELEASE-COMplete	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 ConnectionLess Message Service

Table 11: CLMS message type coding

	Bits							
CLMS message types	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 Mobility Management (MM)

Table 12: MM message type coding

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

7.4.6 Messages for Link Control Entity

Table 13: LCE message type coding

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

7.5 Other information elements

7.5.1 Coding rules

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

NOTE: Although similar coding to ETS 300 102-1 [21a] has been used this should not be assumed. Most information elements have been redefined and recoded and ETS 300 102-1 [21a] should not be used as a detailed reference.

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

The primary set of the fixed length information elements are single octet elements, where bits {4..1} contain the information. This corresponds to ETS 300 102-1 [21a].

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 16 double octet elements. Octet 2 then contains a full octet of information.

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

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

Double octet information element

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

Variable length elements follow the principles defined in ETS 300 102-1 [21a].

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

NOTE: Fixed length elements may appear at any place in a message.

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

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

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

```
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
     └─────────────────────────────────┘
```

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, bit 8 is shown as "0/1 ext" if another octet may follow. Bit 8 is shown as "1" if this is the last octet of that group.

   Additional octets may be added to each group in later versions of this ETS, and equipment should be prepared to receive such additional octets although the equipment need not be able to act upon the content of these octets;

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
     ├─────────────────────────────────┤
```

Structure of long fields

7.5.2 Extensions of codesets

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

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

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

The coding rules specified in subclause 7.5.1 shall apply to every codeset. All equipment shall have the capability to recognise the shift element and to determine the length of the following information element(s). This shall enable the equipment to determine the start of a subsequent element. Equipment is not required to interpret any codesets except for codeset "0", elements from alternative codesets may be discarded without further action.

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

7.5.3 Locking shift procedure

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

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

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

Shift element (locking shift)

New (temporary) codeset identifier

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

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

7.5.4 Non-locking shift procedure

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

A locking shift element shall not be transmitted directly after a non-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

Shift element (non-locking)

New (temporary) codeset identifier:
as for locking shift: refer to subclause 7.5.3.

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

7.5.5 Display and keypad elements

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

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

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

All <<"KEYPAD">> and <<"DISPLAY">> elements shall contain one 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 as follows:

Exception 1; <<REPEAT-INDICATOR>>; coding 1:

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

Exception 2; <<REPEAT-INDICATOR>>; coding 2:

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

7.6 Fixed length information elements

7.6.1 Summary

Table 14: Fixed length information elements coding

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

7.6.2 Sending complete and delimiter request

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

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

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

SENDING-COMPLETE information element

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

DELIMITER-REQUEST information element

7.6.3 Repeat indicator

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

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

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

REPEAT-INDICATOR information element

Repeat indicator coding (octet 1)

Bits 4 3 2 1	Meaning
0 0 0 1	Non prioritised list. See subclause 7.5.6
0 0 1 0	Prioritised list. See subclause 7.5.6
All other values reserved.	

7.6.4 Basic service

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

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

BASIC-SERVICE information element

Call class (octet 2)

Bits 7 6 5	Meaning
0 0 0	Normal call set-up
0 1 0	Emergency call set-up
1 0 0	External handover call set-up (NOTE 3)
All other values reserved.	

Basic service (octet 2)

Bits 4 3 2 1	Meaning
0 0 0 0	Default set-up attributes (NOTE 1)
1 1 1 1	Other (NOTE 2)
All other values reserved.	

NOTE 1: The coding "default set-up attributes" may be used to indicate a basic speech service. In this case, the <<CALL-ATTRIBUTES>> and <<IWU-ATTRIBUTES>> shall be omitted from the set-up message and the coding values given in Annex E shall be assumed by the receiving entity.

NOTE 2: The coding "other" shall indicate that the set-up attributes shall be defined by <<CALL-ATTRIBUTES>> and <<IWU-ATTRIBUTES>> elements included in the message.

NOTE 3: The coding "External handover call set-up" shall indicate a request for external handover. This shall invoke the procedures described in subclause 15.7.

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

SINGLE-DISPLAY information element

NOTE 1: The <<SINGLE-DISPLAY>> information element shall only be sent in the direction FT to PT.

NOTE 2: 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
     +-----------------------------------+
```

SINGLE-KEYPAD information element

NOTE 1: The <<SINGLE-KEYPAD>> information element shall only be sent in the direction PT to FT.

NOTE 2: DECT characters are specified in Annex D. These are based on IA5 characters.

7.6.7 Release reason

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

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

RELEASE-REASON information element

Release reason coding: general values

Value	Meaning
(hex)	(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 to 0C	Reserved
0D	Timer expiry
0E	Partial release
0F	Unknown

Release reason coding: user values

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

Release reason coding: external handover values

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

Release reason coding: temporary overload values

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

All other values reserved.

7.6.8 Signal

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

SIGNAL information element

Signal value coding (octet 2):

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

All other values reserved.

NOTE 1: A PT shall respond to all alerting patterns, but these may all produce the same sound.

NOTE 2: 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 3: The use of alerting patterns is FT dependent,; the resulting sound is PT dependent.

NOTE 4: This tone should be used in accordance with the description given in CCITT Recommendation E.182 [65].

NOTE 5: This tone should be used in accordance with the "Ringing" tone description given in CCITT Recommendation E.182 [65].

NOTE 6: No description is provided for the use of this tone. This coding is included to provide alignment to the coding provided in ETS 300 102-1 [21a].

NOTE 7: This tone should be used in accordance with the "congestion tone" description given in CCITT Recommendation E.182 [65].

NOTE 8: This tone should be used in accordance with the "intrusion tone" description given in CCITT Recommendation E.182 [65].

7.6.9 Timer restart

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

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

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
```

TEST-HOOK-CONTROL information element

Hook value coding (octet 2):

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

All other values reserved.

7.7 Variable length information elements

7.7.1 Summary

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

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

Table 15: Variable length information element coding

	Bits								Reference
Variable Length Elements	8	7	6	5	4	3	2	1	
Info Type	0	0	0	0	0	0	0	1	7.7.20
Identity type	0	0	0	0	0	0	1	0	7.7.19
Portable identity	0	0	0	0	0	1	0	1	7.7.30
Fixed identity	0	0	0	0	0	1	1	0	7.7.18
Location area	0	0	0	0	0	1	1	1	7.7.25
NWK assigned identity	0	0	0	0	1	0	0	1	7.7.28
AUTH-TYPE	0	0	0	0	1	0	1	0	7.7.4
Allocation type	0	0	0	0	1	0	1	1	7.7.2
RAND	0	0	0	0	1	1	0	0	7.7.32
RES	0	0	0	0	1	1	0	1	7.7.35
RS	0	0	0	0	1	1	1	0	7.7.36
IWU attributes	0	0	0	1	0	0	1	0	7.7.21
Call attributes	0	0	0	1	0	0	1	1	7.7.5
Service change info	0	0	0	1	0	1	1	0	7.7.38
Connection attributes	0	0	0	1	0	1	1	1	7.7.11
Cipher info	0	0	0	1	1	0	0	1	7.7.10
Call identity	0	0	0	1	1	0	1	0	7.7.6
Connection identity	0	0	0	1	1	0	1	1	7.7.12
Facility	0	0	0	1	1	1	0	0	7.7.15
Progress indicator	0	0	0	1	1	1	1	0	7.7.31
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
ZAP field	0	1	0	1	0	0	1	0	7.7.44
Service class	0	1	0	1	0	1	0	0	7.7.39
Key	0	1	0	1	0	1	1	0	7.7.24
Reject Reason	0	1	1	0	0	0	0	0	7.7.34
Set-up capability	0	1	1	0	0	0	1	0	7.7.40
Terminal capability	0	1	1	0	0	0	1	1	7.7.41
End-to-End compatibility	0	1	1	0	0	1	0	0	7.7.14
Rate parameters	0	1	1	0	0	1	0	1	7.7.33
Transit Delay	0	1	1	0	0	1	1	0	7.7.42
Window size	0	1	1	0	0	1	1	1	7.7.43
Calling Party Number	0	1	1	0	1	1	0	0	7.7.9
Called Party Number	0	1	1	1	0	0	0	0	7.7.7
Called Party Subaddr	0	1	1	1	0	0	0	1	7.7.8
Duration	0	1	1	1	0	0	1	0	7.7.13
Segmented info	0	1	1	1	0	1	0	1	7.7.37
Alphanumeric	0	1	1	1	0	1	1	0	7.7.3
IWU-to-IWU	0	1	1	1	0	1	1	1	7.7.23
IWU-PACKET	0	1	1	1	1	0	1	0	7.7.22
Escape to proprietary	0	1	1	1	1	0	1	1	(NOTE 1)
Escape for extension	0	1	1	1	1	1	1	1	(NOTE 1)
All other values are reserved									

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

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

Information element format using ESCAPE

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 ident. |    3
     +----------------+---------------+
     |   UAK number   |   AC number   |    4
     +----------------+---------------+
```

ALLOCATION-TYPE information element

Authentication algorithm identifier coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 1	DECT standard authentication algorithm 1

All other values reserved.

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

Bits 8 7 6 5 Meaning

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

Authentication Code (AC) number (octet 4):

Bits 4 3 2 1 Meaning

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

7.7.3 Alphanumeric

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

NOTE: 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 | Char. Type|O/E| Char. Set  |    3
     +---+-----------+---+------------+
     |                                |    4
     |--------------------------------|
     |    List of Characters          |
     |--------------------------------|
     |                                |    L+2
     +--------------------------------+
```

ALPHANUMERIC information element

Character type coding:

	Value	Meaning
Bits	7 6 5	(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 shall only be 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:

	Value	Meaning
Bits	3 2 1	(Character set)
	0 0 0	Reserved
	0 0 1	DECT standard 8-bit characters (Annex D)
	0 1 0	IA5 characters (CCITT Recommendation T.50 [25])
	0 1 1	Reserved (ISO Publication 2022 [26])
	1 0 0	ERMES 7-bit characters (ETS 300 133-1 to -7 [27])
	1 0 1	Reserved [CT2/CAI characters]
	1 1 0	Standard ASCII (7 bit) characters (ANSI X 3.4-1986)

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

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

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

Standard 4-bit character set coding
Character set coding:

	Value	Meaning
Bits	3 2 1	(Character set)
	0 0 0	Reserved
	0 0 1	DECT standard 4-bit characters (Annex D)
	1 0 0	ERMES 4-bit characters (ETS 300 133-1 to -7 [27])
	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, to indicate if the cipher key shall be updated and to allow to send a ZAP increment command.

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

AUTH-TYPE information element

Authentication algorithm identifier coding (octet 3):

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

All other values reserved.

Proprietary algorithm identifier (octet 3a):

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

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

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

All other values reserved.

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

Authentication Key (AK) number (octet 4):

Bits 4 3 2 1 Meaning

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

INC bit coding (octet 5):

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

TXC bit coding (octet 5):

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

UPC bit coding (octet 5):

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

Cipher key number (octet 5):

Bits 4 3 2 1 Meaning

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

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

7.7.5 Call attributes

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

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

CALL-ATTRIBUTES information element

Coding standard (octet 3):

Bits 7 6	Meaning
0 0	DECT standard coding
All other values reserved.	

Network layer attributes (octet 3):

Bits 5 4 3 2 1	Meaning
0 0 0 0 0	Undefined
0 0 0 0 1	Public Access Profile
For further study.	
All other values reserved.	

C-plane class (octet 4):

Bits 7 6 5	Meaning
0 0 0	Class U link; shared
0 1 0	Class A link; shared
1 0 0	Class B link; shared
1 0 1	Class B link; independent
All other values reserved.	

C-plane routing (octet 4):

Bits 4 3 2 1	Meaning
0 0 0 0	C_S only
0 0 0 1	C_S preferred / C_F accepted
0 0 1 0	C_F preferred / C_S accepted
0 1 0 0	C_F only
1 1 0 0	C_F only; dedicated bearer (NOTE 1)
All other values reserved.	

NOTE 1: When "dedicated bearer" is indicated, at least one bearer of the MAC connection must be reserved for the C_F channel (i.e. must not 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). Refer to ETS 300 175-4 [4] (subclause 9.5.1.2) for details of dedicated bearer operation.

U-plane symmetry (octet 5):

Bits 7 6	Meaning
0 0	Symmetric
1 0	Asymmetric

All other values reserved.

NOTE 2: If symmetric, only octet 5 shall appear and this shall refer to both directions. If asymmetric octet 5 shall only refer to the direction P=>F and octet 5a shall refer to the direction F=>P.

LU identification (octet 5 and 5a):

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

All other values reserved.

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

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

All other values reserved.

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

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

All other values reserved.

NOTE 3: If symmetric is indicated in octet 5, only octet 6 shall appear and this shall refer to both directions. If asymmetric is indicated in octet 5, then octet 6 shall only refer to the direction P=>F and octet 6a shall refer to the direction F=>P.

7.7.6 Call identity

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

```
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
     |_______________________________|
```

CALL-IDENTITY information element

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

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

For flag and transaction value coding (octet 3a) see subclause 7.3 (transaction identifier element).

for protocol discriminator coding (octet 3a) see subclause 7.2 (protocol discriminator element).

For extended transaction value coding (octet 3b) see subclause 7.3 (transaction identifier element).

7.7.7 Called party number

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

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

CALLED-PARTY-NUMBER information element

Number type (octet 3):

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

All other values reserved.

Numbering plan identification (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	Unknown
	0 0 0 1	ISDN/telephony plan Rec. E.164/E.163
	0 0 1 1	Data plan Rec. X.121
	1 0 0 0	National standard plan
	1 0 0 1	Private plan
	1 1 1 1	Reserved for extension

All other values reserved.

NOTE: DECT characters are specified in Annex D. They are based on IA5 characters.

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
```

CALLED-PARTY-SUBADDRESS information element

Subaddress type (octet 3):

Bits	7 6 5	Meaning
	0 0 0	NSAP; CCITT Recommendation X.213/ISO Publication 8348 [35]
	0 1 0	User specified

All other values reserved.

Odd/even (octet 3):

Bits	4	Meaning
	0	Even number of address signals
	1	Odd number of address signals

NOTE: The odd/even flag is used when the type of subaddress is "user specified" and the coding is Binary Coded Decimal (BCD). In all other cases it should be set to "even".

7.7.9 Calling party number

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

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

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 Recommendation E.164/E.163
	0 0 1 1	Data plan Recommendation X.121
	1 0 0 0	National standard plan
	1 0 0 1	Private plan
	1 1 1 1	Reserved for extension

All other values reserved.

Presentation indicator (octet 3a):

Bits	7 6	Meaning
	0 0	Presentation allowed
	0 1	Presentation restricted
	1 0	Number not available
	1 1	Reserved.

Screening indicator (octet 3a):

Bits	2 1	Meaning
	0 0	User-provided, not screened
	0 1	User-provided, verified and passed
	1 0	User-provided, verified and failed
	1 1	Network provided.

NOTE: DECT characters are specified in Annex D.

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 ident.								3a
Cipher key type				Cipher key nr.				4

CIPHER-INFO information element

Y/N bit coding (octet 3):

Bits 8	Meaning
0	Disable ciphering
1	Enable ciphering.

Cipher algorithm identifier coding (octet 3):

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

All other values reserved.

Proprietary algorithm identifier (octet 3a):

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

Cipher key type coding (octet 4):

Bits 8 7 6 5	Meaning
1 0 0 1	Derived cipher key
1 0 1 0	Static cipher key

All other values reserved.

Cipher key number (octet 4):

Bits 4 3 2 1 Meaning

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

NOTE: Different sets of static cipher keys could be used in different systems.

7.7.11 Connection attributes

The purpose of the <<CONNECTION-ATTRIBUTES>> element is to describe the connections that are required for the requested service.

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>0</td><td colspan="7"><< CONNECTION-ATTRIBUTES >></td><td>1</td></tr>
<tr><td></td><td colspan="8">Length of Content (L)</td><td>2</td></tr>
<tr><td></td><td>1</td><td colspan="3">Symmetry</td><td colspan="4">Connection identity</td><td>3</td></tr>
<tr><td></td><td>0/1 ext</td><td>0</td><td>0</td><td colspan="5">Target bearers P=>F direction</td><td>4</td></tr>
<tr><td></td><td>0/1 ext</td><td>0</td><td>1</td><td colspan="5">Minimum bearers P=>F direction</td><td>4a</td></tr>
<tr><td></td><td>0/1 ext</td><td>1</td><td>0</td><td colspan="5">Target bearers F=>P direction</td><td>4b</td></tr>
<tr><td></td><td>1</td><td>1</td><td>1</td><td colspan="5">Minimum bearers F=>P direction</td><td>4c</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="3">Slot size</td><td colspan="4">MAC service</td><td>5</td></tr>
<tr><td></td><td>1</td><td>0</td><td>0</td><td>0</td><td colspan="4">MAC service F=>P</td><td>5a</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="3">C_F chan. attributes</td><td colspan="4">MAC packet lifetime</td><td>6</td></tr>
<tr><td></td><td>1</td><td colspan="3">C_F chan. atts F=>P</td><td colspan="4">MAC packet lifetime F=>P</td><td>6a</td></tr>
</table>

CONNECTION-ATTRIBUTES information element

Symmetry:

Bits 7 6 5	Meaning
0 0 1	Symmetric connection
1 0 0	Asymmetric F to P with 1 duplex bearer
1 0 1	Asymmetric F to P with 2 target duplex bearers
1 1 0	Asymmetric P to F with 1 duplex bearer
1 1 1	Asymmetric P to F with 2 target duplex bearers

All other values reserved.

NOTE 1: A minimum of 1 duplex bearer is required for all asymmetric connections to provide the "pilot" bearer functions. Refer to ETS 300 175-3 [3].

Connection identity coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Unknown (not yet numbered)
1 N N N	Advanced connection number NNN

All other values reserved.

NOTE 2: If already established, the (advanced) connection shall be identified using the Logical Connection Number (LCN) placed in position NNN.

NOTE 3: Octets 4a, 4b and 4c are optional, but if present they shall appear in order shown. The following rules shall apply:

- if octet 4a is omitted, it shall be defaulted to the value given in octet 4;
- octets 4b and 4c shall be omitted if octet 3 indicates "symmetric";
- if octet 4c is omitted, it shall be defaulted to the value given in octet 4b.

NOTE 4: The meaning of octets 4, 4a, 4b and 4c is identified by the "bearer definition" coding in bits 7 and 6 as follows.

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

Bits	7 6	Meaning
	0 0	Target number of bearers; P=>F direction
	0 1	Minimum number of bearers; P=>F direction
	1 0	Target number of bearers; F=>P direction
	1 1	Minimum number of bearers; F=>P direction

Number of bearers coding (octets 4, 4a, 4b, 4c):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	No U-plane
	n n n n n	Number of bearers (1 µ Number µ 31)

NOTE 5: 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".

NOTE 6: If symmetric is indicated in octet 3, only octet 5 and 6 shall appear and these shall refer to both directions. If asymmetric is indicated in octet 3, then octet 5 and 6 shall only refer to the direction P=>F and octets 5a and 6a shall refer to the direction F=>P.

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

MAC slot size (octet 5):

Bits	7 6 5	Meaning
	0 0 0	Half slot; j = 0.
	1 0 0	full slot
	1 0 1	double slot

All other values reserved.

MAC service (octets 5 and 5a):

Bits	4 3 2 1	Meaning
	0 0 0 0	I_N; minimum delay
	0 0 0 1	I_N; normal delay
	0 0 1 0	I_P; detect only
	0 0 1 1	I_P; Mod-2 correct

All other values reserved.

CF channel attributes (octets 6 and 6a):

Bits	7 6 5	Meaning
	0 0 0	C_F never (CS only)
	0 1 0	C_F Demand/1 bearer (interrupting)
	0 1 1	C_F Demand/2 bearers (interrupting)
	1 0 0	C_F Reserved/1 bearer (non-interrupting)
	1 0 1	C_F Reserved/2 bearers (non-interrupting)

All other values reserved.

NOTE 7: The C_F channel attributes indicate the intended usage of the C_F channel. In all cases the actual C_F usage is defined on a slot-by-slot basis for each connection by the DLC layer.

NOTE 8: The maximum packet lifetime (nnn) shall only be defined if the MAC service (octet 5 or 5a as appropriate) indicates IP error_correct. The value "nnn" defines the allowed values of maximum packet lifetime using the coding given in subclause 7.2.5.3.8 of ETS 300 175-3 [3]. In this coding nnn = (0) indicates unlimited lifetime, and nnn = (1..7) indicates the maximum lifetime in TDMA frames. In all other cases the "Not applicable" coding shall be used.

MAC packet lifetime (octets 6 and 6a):

Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	1 n n n	Maximum packet lifetime (IP; Mod-2 operation only)

All other values reserved.

NOTE 9: The maximum packet lifetime (nnn) is coded with the natural binary value with the least significant bit in bit position "1". The allowable values are "0" to "7". The value "0" shall be interpreted as unlimited (i.e. infinite). The values "1" to "7" define the maximum lifetime in TDMA frames. Refer to ETS 300 175-3 [3] for the use of this attribute.

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).

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

CONNECTION-IDENTITY information element

Each octet defines an association between one U-plane link and one MAC connection. All associations refer to one call as identified by the transaction identifier (transaction identifier information element at the start of the message).

Connection identity coding (octet 3):

Bits	4 3 2 1	Meaning
	0 0 0 0	Unknown (not yet numbered)
	1 N N N	Advanced connection number NNN

All other values reserved.

NOTE 1: If already established, the (advanced) connection shall be identified using the Logical Connection Number (LCN) placed in position NNN.

U-plane link identity coding:

Bits	8 7 6 5	Meaning
	0 0 0 0	Unnumbered link
	1 N N N	Numbered link

For further study

All other values reserved.

NOTE 2: Most calls only contain 1 unnumbered U-plane link. Numbered links shall use the 3-bit U-plane Link Number (ULN) placed in position NNN. Refer to ETS 300 175-4 [4], subclause 13.2, for details of U-plane link number coding.

7.7.13 Duration

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

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>0</td><td colspan="7">&lt;&lt; Duration &gt;&gt;</td><td>1</td></tr>
<tr><td></td><td colspan="8">Length of Contents (L)</td><td>2</td></tr>
<tr><td></td><td>0/1
ext</td><td colspan="3">Lock
Limits</td><td colspan="4">Time
Limits</td><td>3</td></tr>
<tr><td></td><td colspan="8">Time duration</td><td>3a</td></tr>
</table>

DURATION information element

Lock limits coding (octet 3):

Bits	7 6 5	Meaning
	1 1 0	Temporary user limit (NOTE 1)
	1 1 1	No limits

NOTE 1: "Temporary user limit" indicates that a time limit applies when the PP leaves the locked state with the relevant FP. Refer to ETS 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 1 0	Defined time limit (NOTE 2)
	0 1 0 0	Standard time limit (NOTE 3)
	1 1 1 1	Infinite

NOTE 2: If a defined time limit is indicated, octet 3a shall follow.

NOTE 3: If a standard time limit is indicated, the standard time limit for the relevant procedure shall apply.

Time duration (octet 3a)
The time duration is binary coded (bit 1 being the least significant bit). The time duration defines time in units based on the MAC layer multiframes. Multiframes are defined in ETS 300 175-3 [3].

1 unit = 2E16 multiframes.

NOTE 4: This unit corresponds to the most significant octet of the multiframe counter that may be transmitted by FPs. Refer to ETS 300 175-3 [3].

7.7.14 End-to-end compatibility

The purpose of the <<END-TO-END-COMPATIBILITY>> element is to exchange some aspects of the end-to-end data terminal capabilities between PT and FT during call establishment.

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>0</td><td colspan="7">&lt;&lt; END-TO-END-COMPATIB &gt;&gt;</td><td>1</td></tr>
<tr><td></td><td colspan="8">Length of Contents (L)</td><td>2</td></tr>
<tr><td></td><td>0/1
ext</td><td>S/A</td><td>Neg</td><td colspan="5">User rate</td><td>3</td></tr>
<tr><td></td><td>0/1
ext</td><td colspan="2">Interm.
rate</td><td>NIC
tx</td><td>NIC
rx</td><td>F-C
tx</td><td>F-C
rx</td><td>0
spr</td><td>3a (NOTE 2)</td></tr>
<tr><td></td><td>0/1
ext</td><td colspan="2">Stop
bits</td><td colspan="2">Data
Bits</td><td colspan="3">Parity</td><td>3b</td></tr>
<tr><td></td><td>1</td><td>Dup</td><td colspan="6">Modem type</td><td>3c</td></tr>
</table>

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 shall be included if the service V.110/X.30 rate adaption is indicated in the <<IWU-ATTRIBUTES>>. Octet 3a may be included in other cases to extend into octets 3b and 3c but octet 3a should be ignored in these other cases.

Synchronous/Asynchronous (S/A) (octet 3):

Bits	7	Meaning
	0	Synchronous
	1	Asynchronous

NOTE 3: Octets 3a, 3b, 3c may be omitted if octet 3 indicates "synchronous" user rates.

Negotiation (Neg) (octet 3):

Bits	6	Meaning
	0	In-band negotiation not possible
	1	In band negotiation possible (NOTE 4)

NOTE 4: "In band negotiation possible" shall only be used in the context of V.110/X.30 rate adaption.

User rate coding (octet 3):

Bits	5 4 3 2 1	Meaning	
	0 0 0 0 1	0,6 kbps;	V.6 and X.1.
	0 0 0 1 0	1,2 kbps;	V.6.
	0 0 0 1 1	2,4 kbps;	V.6 and X.1.
	0 0 1 0 0	3,6 kbps;	V.6.
	0 0 1 0 1	4,8 kbps;	V.6 and X.1.
	0 0 1 1 0	7,2 kbps;	V.6.
	0 0 1 1 1	8,0 kbps;	I.460.
	0 1 0 0 0	9,6 kbps;	V.6 and X.1.
	0 1 0 0 1	14,4 kbps;	V.6.
	0 1 0 1 0	16 kbps;	I.460.
	0 1 0 1 1	19,2 kbps;	V.6.
	0 1 1 0 0	32 kbps;	I.460.
	0 1 1 1 0	48 kbps;	V.6 and X.1.
	0 1 1 1 1	56 kbps;	V.6.
	1 0 0 0 0	64 kbps;	X.1.
	1 0 1 0 1	0,1345 kbps;	X.1.
	1 0 1 1 0	0,1 kbps;	X.1.
	1 0 1 1 1	0,075/1,2 kbps;	V.6 and X.1. (NOTE 5)
	1 1 0 0 0	1,2/0,075 kbps;	V.6 and X.1. (NOTE 5)
	1 1 0 0 1	0,050 kbps;	V.6 and X.1.
	1 1 0 1 0	0,075 kbps;	V.6 and X.1.
	1 1 0 1 1	0,110 kbps;	V.6 and X.1.
	1 1 1 0 0	0,150 kbps;	V.6 and X.1.
	1 1 1 0 1	0,200 kbps;	V.6 and X.1.
	1 1 1 1 0	0,300 kbps;	V.6 and X.1.
	1 1 1 1 1	12 kbps;	V.6.

All other values reserved.

NOTE 5: The first rate is the transmit rate in the forward direction of the call. The second rate is the transmit rate in the backward direction of the call.

NOTE 6: For CCITT V-series Recommendations see [38].

For CCITT X-series Recommendations see [39].

For CCITT I.460 Recommendation see [40].

Intermediate rate (interm rate) (octet 3a):

Bits	7 6	Meaning
	0 0	Not used
	0 1	8 kbps
	1 0	16 kbps
	1 1	32 kbps

Network Independent Clock on transmission (NIC tx) (octet 3a):

Bits	5	Meaning
	0	Not required to send data with network independent clock
	1	Required to send data with network independent clock

NOTE 7: NIC tx refers to transmission in the forward direction of the call.

NOTE 8: See CCITT Recommendations V.110 [38] and X.30 [39].

Network Independent Clock on reception (NIC rx) (octet 3a):

Bits	4	Meaning
	0	Cannot accept data with Network independent clock
	1	Required to send data with Network independent clock

NOTE 9: NIC rx refers to transmission in the backward direction of the call.

NOTE 10: See CCITT Recommendations V.110 [38] and X.30 [39].

Flow-Control on transmission (F-C tx) (octet 3a):

Bits 3	Meaning
0	Not required to send data with flow control mechanism
1	Required to send data with flow control mechanism

NOTE 11: F-C tx refers to transmission in the forward direction of the call.

Flow-Control on reception (F-C rx) (octet 3a):

Bits 2	Meaning
0	Cannot accept data with flow control mechanism (i.e. sender does not support this optional procedure);
1	Can accept data with flow control mechanism (i.e. sender does support this optional procedure);

NOTE 12: F-C rx refers to transmission in the backward direction of the call.

Stop bits coding (octet 3b):

Bits 7 6	Meaning
0 0	Not used
0 1	1 bit
1 0	1,5 bits
1 1	2 bits

Data bits coding (octet 3b):

Bits 5 4	Meaning
0 0	Not used
0 1	5 bits
1 0	7 bits
1 1	8 bits

Parity coding (octet 3b):

Bits 3 2 1	Meaning
0 0 0	Odd
0 1 0	Even
0 1 1	None
1 0 0	Forced to 0
1 0 1	Forced to 1

All other values reserved.

Duplex mode (Dup) (octet 3c):

Bits 7	Meaning
0	Half duplex
1	Full duplex

Modem type (octet 3c):

Bits	6 5 4 3 2 1	Meaning
	0 0 0 0 0 0	Reserved
	0 0 0 0 0 1	V.21
	0 0 0 0 1 0	V.22
	0 0 0 0 1 1	V.22 bis
	0 0 0 1 0 0	V.23
	0 0 0 1 0 1	V.26
	0 0 0 1 1 0	V.26 bis
	0 0 0 1 1 1	V.26 ter
	0 0 1 0 0 0	V.27
	0 0 1 0 0 1	V.27 bis
	0 0 1 0 1 0	V.27 ter
	0 0 1 0 1 1	V.29
	0 0 1 1 0 0	V.32
	0 0 1 1 0 1	V.35
	1 0 0 0 0 0 to	} Reserved for national use
	1 1 1 1 1 1	}

All other values reserved.

NOTE 13: CCITT V-series Recommendations appear in [38].

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 discrimin.					3
Component(s)								4

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 prETS 300 196 (T/S 46-32B) [29].

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:
Length of Contents (L)								2
0/1	Feature							3
1	Parameter							3a

FEATURE-ACTIVATE information element

Feature coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning	Parameter
	0 0 0 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.

Register recall: to hold existing call and seize a register (with dial tone) to permit input of further digits or other action. Subsequent use of the same code causes retrieval of the original call.

NOTE 1: Since the feature key protocol is stimulus, the call state of the handset is not changed. The transfer of dial digits towards the register should be done using the keypad protocol. To avoid interference with the original call, use of this feature should also be restricted to those cases where only one call can be put on hold.

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 µ nn µ 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 µ nn µ 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 µ nn µ 7F

Control of echo control functions: the ability to connect or disconnect FP echo control functions, depending on e.g. the type of service and call routing information.

Parameter coding (octet 3a)

Bit 7 is reserved.

Bits	6 5	Meaning
	0 0	option a) and b) disconnected (NOTE 2)
	0 1	only option a) connected (NOTE 2)
	1 0	only option b) connected (NOTE 2)
	1 1	no change (NOTE 2)

Bits	4 3	Meaning
	0 0	Disconnect for requirement 2 (NOTE 3)
	0 1	Connect · 9 dB for requirement 2 (NOTE 3)
	1 0	Connect reduced loss for requirement 2 (NOTE 3)
	1 1	No change for requirement 2 (NOTE 3)

Bits	2 1	Meaning
	0 0	Disconnect for requirement 1 (NOTE 3)
	0 1	Connect for requirement 1 (NOTE 3)
	1 0	Reserved for requirement 1 (NOTE 3)
	1 1	No change for requirement 1 (NOTE 3)

NOTE 2: Refer to ETS 300 175-8, subclause 7.4.1.2 [8].

NOTE 3: Refer to ETS 300 175-8, subclause 7.10 [8].

Cost information: indication to the user of the call charge or call tariff. It may be used to invoke activation of this feature for all calls or on call-by-call basis. In the first case it is a Call Independent Supplementary Service (CISS) and the information element is placed in one of the CISS messages (see subclause 6.2.2). In the second case it is a Call Related Supplementary Service (CRSS) and the information element is placed in an allowed CC message as specified in subclause 6.3.

Parameter (octet 3a):

Bits	7 6 5	Meaning
	0 0 1	DECT internal cost information
	0 1 1	cost information for the complete connection

All other values reserved.

Parameter (octet 3a):

Bits	4 3 2 1	Meaning
	0 0 0 0	tariff information
	0 0 0 1	charging pulses during the call
	0 0 1 0	calculated amount of charge at the end of the call

All other values reserved.

7.7.17 Feature indicate

The purpose of the <<FEATURE-INDICATE>> information element is to allow the FT to convey feature indications to the user regarding the status of an activated feature.

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

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
└─────────────────────────────────┘
```

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              │
      │-------------------------------│
      │                               │
      └───────────────────────────────┘
```

Charging component coding:

Bits	8 7 6 5 4	Name	Meaning
	0 0 0 0 0	c0	reserved
	0 0 0 0 1	c1	units per interval
	0 0 0 1 0	c2	seconds per time interval
	0 0 0 1 1	c3	scaling factor
	0 0 1 0 0	c4	unit increment
	0 0 1 0 1	c5	units per data interval
	0 0 1 1 0	c6	segments per data interval
	0 0 1 1 1	c7	initial seconds per time interval
	0 1 0 0 0	c8	reserved
	0 1 0 0 1	c9	reserved
	0 1 0 1 0	c10	fixed cost for access to a specific network
	0 1 0 1 1	c11	calculated charged amount
	0 1 1 0 0	c12	fixed supplementary service cost
	0 1 1 0 1	c13	supplementary service cost per time interval
	0 1 1 1 0	c14	pulse
	0 1 1 1 1	c15	reserved
	1 0 - - -	c16-23	network proprietary components
	All other values reserved.		

Component c1: this component defines the number of unit increments per interval. It is set in terms of visited location area units per interval.

Component c2: this component defines the time interval for unitisation and is specified in seconds.

Component c3: this component defines the scaling factor to convert from visited location area units to home location area units. It is a dimensionless multiplier.

Component c4: this component defines the number of unit increments on receipt of the message containing the cost information. It is specified in units of the visited location area.

Component c5: this component defines the number of unit increments per data interval. It is set in terms of visited location area units per interval.

Component c6: this component defines the data usage interval for unitisation.

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

Component c10: this component defines a fixed cost for access to a specific network.

Component c11: this component defines the calculated cost in either the currency of the home location area or the visited location area.

Component c12: this component defines a fixed cost for a specific supplementary service.

Component c13: this component defines the cost per time interval for a specific supplementary service.

Component c14: this component represents one pulse.

Length coding: this 3 bit number defines the length of the value field in octets and is coded with the natural binary value.

Value coding: this field contains the value of the charging components and is coded with the natural binary value.

Component	Resolution of the value
c1	0,1
c2	0,1
c3	0,01
c4	0,1
c5	0,1
c6	1,0
c7	0,1
c10	0,1
c11	0,1
c12	0,1
c13	0,1
c14	0,1

7.7.18 Fixed identity

The purpose of the <<FIXED-IDENTITY>> information element is to transport a DECT fixed identity or a Portable Access Rights Key (PARK). Refer to ETS 300 175-6 [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 indicator      |    4
     | 0 |    ARC    |      ARD      |    5
     |                               |    6
     |-------------------------------|
     |        ARD (and RPN)          |
     |-------------------------------|
     |                               |    L+2
```

FIXED-IDENTITY information element

Type coding (octet 3):

Bits	7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0	Access rights identity
	0 0 0 0 0 0 1	Access rights identity plus radio fixed part number
	0 1 0 0 0 0 0	Portable access rights key

All other values reserved.

Length indicator 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 indicator coding for identity type "ARI".
Length indicator = 1 + (number of ARI bits).

Length indicator 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 indicator coding for identity type "PARK"
Length of identity value = 1 + PARK length indicator
In this case the length indicator defines the "PARK length indicator".

Access rights class coding (octet 5): refer to ETS 300 175-6 [6].

Access Rights Details (ARD) coding (octet 5 to L+2): refer to ETS 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.

7.7.19 Identity type

The purpose of the <<IDENTITY-TYPE>> information element is to indicate a specific identity type, e.g. used by the FT when requesting for a specific PT identity. Refer to ETS 300 175-6 [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

IDENTITY-TYPE information element

Identity group coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Portable identity
0 0 0 1	Network assigned identity
0 1 0 0	Fixed identity (also including the Portable Access Rights Key PARK)
1 1 1 1	Proprietary (application specific)

All other values reserved.

Type coding for identity group "portable identity" (octet 4):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	International Portable User Identity (IPUI)
0 0 1 0 0 0 0	International Portable Equipment Identity (IPUI)
0 1 0 0 0 0 0	Temporary Portable User Identity (TPUI)

All other values reserved.

Type coding for identity group "fixed identity" (also including PARK) (octet 4):

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Access rights identity
0 0 0 0 0 0 1	Access rights identity plus radio fixed part number
0 1 0 0 0 0 0	Portable Access Rights Key (PARK)

All other values reserved.

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

Bits 7 6 5 4 3 2 1	Meaning
1 1 1 0 1 0 0	GSM temporary mobile subscriber identity
1 1 1 1 1 1 1	Proprietary (application specific)

All other values reserved.

7.7.20 Info type

The purpose of the <<INFO-TYPE>> information element is to indicate the type (or types) of requested or transmitted information.

```
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       |
     ---------------------------------
```

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 1 0 0 0	external handover parameters
	0 0 0 1 0 0 1	location area
	0 0 0 1 0 1 0	hand over reference
	0 0 0 1 1 0 0	external handover candidate
	0 0 0 1 1 0 1	synchronised external handover candidate
	0 0 0 1 1 1 0	non synchronised external handover candidate
	0 0 1 0 0 0 0	old fixed part identity
	0 0 1 0 0 0 1	old network assigned identity
	0 0 1 0 0 1 0	old network assigned location area
	0 0 1 0 0 1 1	old network assigned handover reference
	0 1 0 0 0 0 0	billing
	0 1 0 0 0 0 1	debiting

All other values reserved.

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.

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>0</td><td colspan="7">&lt;&lt; IWU-ATTRIBUTES &gt;&gt;</td><td>1</td></tr>
<tr><td></td><td colspan="8">Length of Contents (L)</td><td>2</td></tr>
<tr><td></td><td>1</td><td colspan="2">Coding Std.</td><td colspan="5">Info. Transfer Capability</td><td>3</td></tr>
<tr><td></td><td>1</td><td colspan="3">Negotiation indicator</td><td colspan="4">External Con-nection Type</td><td>4</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">Trans mode</td><td colspan="5">Information Transfer rate</td><td>5</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">Unit rate</td><td colspan="5">Rate Multiplier</td><td>5a</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="3">Structure</td><td colspan="2">Config</td><td colspan="2">Estab.</td><td>5b</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">Symm</td><td colspan="5">Info. Trans. Rate. (Dest=>Originator)</td><td>5c</td></tr>
<tr><td></td><td>1</td><td colspan="2">Unit rate</td><td colspan="5">Rate Multiplier (Dest=>Originator)</td><td>5d</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">0 0
NOTE 5</td><td colspan="5">User protocol ID</td><td>6</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">1 1
NOTE 5</td><td colspan="5">L3 protocol ID</td><td>7</td></tr>
<tr><td></td><td>0/1 ext</td><td colspan="2">1 0
NOTE 5</td><td colspan="5">L2 protocol ID</td><td>8</td></tr>
</table>

IWU-ATTRIBUTES information element

Coding standard (octet 3):

Bits	7 6	Meaning
	0 0	DECT standard coding

All other values reserved.

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

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	0 0 0 0 0	Packet mode calls
	0 1 0 1 0	16 kbps
	0 1 0 1 1	32 kbps
	1 0 0 0 0	64 kbps
	1 0 0 0 1	2 x 64 kbps
	1 0 0 1 1	384 kbps
	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.

NOTE 2: 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)

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.

NOTE 3: 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 kbps steps
	1 0	32 kbps steps
	1 1	64 kbps 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 4: 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.

NOTE 5: All of the user protocol identifier (octets 6, 7, 8) 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, 7, 8):

Bits	7 6	Meaning
	0 0	User protocol IDentifier (ID)
	1 1	L3 protocol ID
	1 0	L2 protocol ID

All other values reserved.

User protocol ID (octet 6):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (escape)
	0 0 0 0 1	V.110/X.30 rate adaption (NOTE 6)
	0 0 0 1 0	G.711 µ-law PCM
	0 0 0 1 1	G.711 A-law PCM
	0 0 1 0 0	G.721 ADPCM
	0 0 1 0 1	G.722 and G.725 7,0 kHz audio
	0 0 1 1 0	H.261 Video
	0 0 1 1 1	Non-standard rate adaption
	0 1 0 0 0	V.120 rate adaption
	0 1 0 0 1	X.31 rate adaption
	1 0 0 0 0	Group 3 fax
	1 0 0 0 1	Group 4 fax
	1 1 0 0 0	X.28/X.29

All other values reserved.

NOTE 6: If octet 6 indicates "V.110/X.30 rate adaption", the set-up message shall also contain the <<END-TO-END-COMPATIBILITY>> element to define the attributes of the rate adaption service.

L3 protocol ID (octet 7):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (escape)
	0 0 0 1 0	ETS 300 102 [21]
	0 0 1 1 0	CCITT Recommendation X.25 packet layer [67]
	0 0 1 1 1	ISO Publication 8208 [34] (CCITT Recommendation X.25 packet level for DTE [67])
	0 1 0 0 0	ISO Publication 8348 [35] (OSI C/O protocol)
	0 1 0 0 1	ISO Publication 8473 [36] (OSI C/L service)
	0 1 0 1 0	CCITT Recommendation T.70 [68], minimum network layer
	1 0 0 1 0	GSM Recommendation 04.08 [22]

All other values reserved.

L2 protocol ID (octet 8):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (escape)
	0 0 0 0 1	Basic mode ISO Publication 1745 [69]
	0 0 0 1 0	CCITT Recommendation Q.921/I.441 (LAP.D) [31]
	0 0 1 1 0	CCITT Recommendation X.25; link layer (LAP.B) [67]
	0 0 1 1 1	CCITT Recommendation X.25 [67] multilink
	0 1 0 0 0	Extended LAP.B [32]
	0 1 1 0 0	ISO Publication 8802/2 (LAN LLC)[33]
	1 0 0 0 1	ISO Publication 8802/x [33] (NOTE 7)
	1 0 0 1 0	GSM Recommendation 04.06) [66]
	1 0 1 1 0	CCITT Recommendation V.42 [38] (LAP.M)

All other values reserved.

NOTE 7: ISO Publication 8802/x refers to LAN operation with a null Layer 2 protocol (LLC not implemented).

7.7.22 IWU packet

The purpose of the <<IWU-PACKET>> information element is to encapsulate any external frame or unstructured data such that it can be transported inside one or more CC, COMS or CLMS messages.

This element may be used to encapsulate octet structured frames (e.g. frames that have an original octet structure or have had all zero insertions and flag octets removed). If the frame (or data) is too large to fit into a single <<IWU-PACKET>> element, it shall be segmented into a series of <<IWU-PACKET>> elements that are associated using the <<SEGMENTED-INFO>> element.

Refer to Annex G for more details on the use of this element.

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

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 shall be used to distinguish between the sending of a new messages (e.g. sent in the direction A=>B) and the rejection of a received message (e.g. message received by B can be rejected by sending "reject" code in direction B=>A).

L2 protocol ID coding (octet 3):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User Specific (NOTE 5)
	0 0 0 0 1	Basic mode ISO Publication 1745 [69]
	0 0 0 1 0	CCITT Recommendation Q.921/I.441 (LAP.D) [31]
	0 0 1 1 0	CCITT Recommendation X.25 [67] link layer (LAP.B) [67]
	0 0 1 1 1	CCITT Recommendation X.25 [67] multilink
	0 1 0 0 0	Extended LAP.B [32]
	0 1 1 0 0	ISO Publication 8802/2 (LAN LLC) [33]
	1 0 0 0 1	ISO Publication 8802/x [33] (NOTE 4)
	1 0 0 1 0	GSM Recommendation 04.06 [66]
	1 0 1 1 0	CCITT Recommendation V.42 (LAP.M) [38]

All other values reserved.

L3 protocol ID coding (octet 3a):

Bits	5 4 3 2 1	Meaning
	0 0 0 0 0	User specific (NOTE 5)
	0 0 0 1 0	ETS 300 102 [21]
	0 0 1 1 0	CCITT Recommendation X.25, packet layer [67]
	0 0 1 1 1	ISO Publication 8208 [34] (X.25 packet level for DTE [67])
	0 1 0 0 0	ISO Publication 8348 [35] (OSI C/O protocol)
	0 1 0 0 1	ISO Publication 8473 [36] (OSI C/L service)
	0 1 0 1 0	CCITT Recommendation T.70 [68] (minimum network layer)
	1 0 0 1 0	GSM Recommendation 04.08 [22]

All other values reserved.

NOTE 3: All the L2 protocol ID and L3 protocol ID codings are the same as the codings used in the <<IWU-ATTRIBUTES>> element. See subclause 7.7.21.

NOTE 4: ISO Publication 8802/x [33] refers to LAN operation with a null Layer 2 protocol (LLC not implemented).

NOTE 5: The <<IWU-PACKET>> is structured according to the user needs.

7.7.23 IWU to IWU

The purpose of the <<IWU-TO-IWU>> element is to encapsulate any message or information element that cannot be interworked into one or more other DECT information element(s).

If the message or element is too large to fit into a single <<IWU-TO-IWU>> element, it shall be segmented into a series of <<IWU-TO-IWU>> elements that are associated using the <<SEGMENTED-INFO>> element.

Refer to Annex G for more details on the use of this element.

```
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
    +--------------------------------+
```

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 shall be used to distinguish between the sending of a new message (e.g. sent in the direction A=>B) and the rejection of a received message (e.g. message received by B can be rejected by sending "reject" code in direction B=>A).

Protocol Discriminator (PD):

Bits	6 5 4 3 2 1	Meaning
	0 0 0 0 0 0	User Specific (NOTE 2)
	0 0 0 0 0 1	OSI high layer protocols
	0 0 0 0 1 0	CCITT Recommendation X.244 [37] (NOTE 3)
	0 0 0 1 0 0	IA5 characters [25]
	0 0 0 1 1 1	CCITT Recommendation V.120 Rate adaption
	0 0 1 0 0 0	CCITT Recommendation Q.931 (I.451), message [30]
	0 0 1 0 0 1	CCITT Recommendation Q.931 (I.451), element(s) [30] (NOTE 4)
	0 1 0 0 0 0	GSM Recommendation 04.08, message [22]
	0 1 0 0 0 1	GSM Recommendation 04.08, element(s) [22] (NOTE 4)
	1 1 1 1 1 1	Unknown

All other values reserved.

NOTE 2: The IWU information is structured according to the user needs.

NOTE 3: The IWU information is structured according to CCITT Recommendation X.244 [37] (CCITT Recommendation X.25 [67] call user data).

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

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
     ---------------------------------
```

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 modulo L2), 0 µ i µ 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
     ---------------------------------
```

LOCATION-AREA information element

Location Information (LI) type coding (octet 3):

Bits	8 7	Meaning
	0 0	Reserved
	0 1	Location area level is included (octet 3) but no extended location information is included
	1 0	Only extended location information (octet 3a to octet L+2) is included the value of the location area level (octet 3) is not a valid one
	1 1	Location area level (octet 3) as well as extended location information (octet 3a to octet L+2) are included

Location area level for LA type 01 and 11 (octet 3):
Contains a number which identifies how many bits of the RFPI are relevant for this location area. The bit count starts with the MSB of the RFPI.

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

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

GSM location information coding:

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

MCC: is the Mobile Country Code.
MNC: is the GSM Mobile Network Code.
LAC: is the GSM Location Area Code.
CI: is the GSM Cell Identity.

NOTE: The Cell Identity (CI) is needed for external handover.

7.7.26 Multi-display

The purpose of the <<MULTI-DISPLAY>> element is to supply a list of display information that may be displayed by the PT. Multi-display elements shall only contain DECT standard characters. Multiple characters shall be interpreted in the order of ascending octet numbers.

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

MULTI-DISPLAY information element

NOTE 1: <<MULTI-DISPLAY>> information elements shall only be sent in the direction FT to PT.

NOTE 2: 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 IA5 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
```

MULTI-KEYPAD information element

NOTE 1: <<MULTI-KEYPAD>> information elements shall only be sent in the direction PT to FT.

NOTE 2: 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
```

NWK-ASSIGNED-IDENTITY information element

Type coding (octet 3):

Bits 7 6 5 4 3 2 1	Meaning
1 1 1 0 1 0 0	GSM Temporary Mobile Subscriber Identity (TMSI)
1 1 1 1 1 1 1	Proprietary (application specific)

All other values reserved.

Length of identity value coding (octet 4): the length is defined in bits, and this is coded with the natural binary value. The least significant bit of the coding appears in bit position 1. Allowable values: 0 to 127.

Identity value coding for GSM-TMSI:

```
Bit: | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
     ________________________________     Octet:
     | 1 | Length of identity value  |      4
     |_______________________________|
     |                               |      5
     |-------------------------------|
     :          TMSI value           :
     |-------------------------------|
     |                               |      L+2
     |_______________________________|
```

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 field           |
     |-------------------------------|
     |                               |      L+2
     |_______________________________|
```

NETWORK PARAMETER information element

Discriminator coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 1 1 0 1 0 1 0	GSM handover reference
	0 1 1 1 1 1 1 1	Proprietary
	1 1 1 0 1 0 1 0	GSM handover reference requested (no data field included)
	All other values reserved.	

Data field coding for GSM handover reference (octet 4):
The handover reference is coded using binary representation.
Range: 0 to 255.

7.7.30 Portable identity

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

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

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 (cont.)          |  6
     |-------------------------------|
     |                               |
     |-------------------------------|
     |                               |  L+2
```

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

Portable User Type (PUT) coding (octet 5): refer to ETS 300 175-6 [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 ETS 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

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

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

Private number coding number (octet 5 to L+2): the number is binary coded and shall not exceed 60 bits.

Identity value coding for IPUI T containing the equipment installer's code and private extended number:

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

th 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 octect 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

Length of identity value coding (octet 4): defines the number of valid IPUI bits. The value equals to 20 + (0 to 80).

Public Operator Code (POC) (octet 5 to 7): the code is binary coded and is 16 bits.

ACCount number (ACC) coding (octet 7 to L+2): the number is binary coded and shall not exceed 80 bits.

Identity value coding for IPUI Q containing the bank account number

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

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
	:				:				
	digit p-1				digit p				L+2

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

Credit Card ACcount Number (CACN) coding (octet 5 to L+2): the number is BCD coded and shall not exceed 20 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

Identity value coding for IPUI R containing the GSM-IMSI:

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

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

International Mobile Subscriber Identity (IMSI) coding (octet 5 to L+2): the number is BCD coded and shall not exceed 15 digits. If the number of identity digits is even then bits 1 to 4 of the last octet shall be coded as "1111".

Identity value coding for the IPEI (same as for IPUI N):

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

Length of identity value coding (octet 4): the number of valid bits for IPUI N containing the IPEI is 40.

Equipment Manufacturer Code (EMC) coding (octets 5 to 7): refer to ETS 300 175-6 [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 ETS 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
	0	0	0	0	TPUI value				5
	TPUI value								6
	TPUI value								7

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

Temporary Portable User Identity (TPUI) coding (octet 5 to 7): Refer to ETS 300 175-6 [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.

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 |Cod.st.| 0 |   Location     |    3
     | 1 |  Progress description      |    4
```

PROGRESS-INDICATOR information element

Coding standard coding (octet 3):

Bits 7 6	Meaning
0 0	CCITT standardised coding, as described below
0 1	reserved for other international standards
1 0	national standard
1 1	standard specific to identified location

Location coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	user
0 0 0 1	private network serving the local user
0 0 1 0	public network serving the local user
0 1 0 0	public network serving the remote user
0 1 0 1	private network serving the remote user
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 1 0 0 0	In-band information or appropriate pattern now available
0 0 0 1 0 0 1	In-band information not available

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
```

RAND information element

NOTE: This information element is used for either the RAND-P or the RAND-F information. The actual contents are determined by the direction of transmission.

RAND field coding (octet 3 to L+2)
RAND shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

7.7.33 Rate parameters

The purpose of the <<RATE-PARAMETERS>> element is to indicate the requested attributes for the Basic Rate Adaption Service (BRAT).

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< RATE-PARAMETERS >>							1
Length of Content (L)								2
1	Symm		I	Class of service				3
0/1 ext	Ch 1 user rate P=>F			Ch 1. arrang. P=>F				4
1	Ch 1 user rate F=>P			Ch 1. arrang. F=>P				4a
0/1 ext	Ch 2 user rate P=>F			Ch 2. arrang. P=>F				5
1	Ch 2 user rate F=>P			Ch 2. arrang. F=>P				5a
0/1 ext	Ch 3 user rate P=>F			Ch 3. arrang. P=>F				6
1	Ch 3 user rate F=>P			Ch 3. arrang. F=>P				6a

RATE-PARAMETERS information element

Symmetry (octet 3):

Bits 7 6	Meaning
0 0	Symmetric
1 0	Asymmetric

All other values reserved.

NOTE 1: 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.

NOTE 2: If octets 5 or 6 is omitted the channel 2 rate and/or channel 3 rate shall be understood to be 0 kbps.

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 3: The excess capacity indicated for the Class 3 services are target figures only. The actual excess capacity shall be 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 kbps (channel off)
0 0 1	08 kbps
0 1 0	16 kbps
0 1 1	32 kbps
1 0 0	64 kbps

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

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
10	authentication failed
11	no authentication algorithm
12	authentication algorithm not supported
13	authentication key not supported
14	UPI not entered
17	no cipher algorithm
18	cipher algorithm not supported
19	cipher key not supported
20	incompatible service
21	false LCE reply (no corresponding service)
22	late LCE reply (service already taken)
23	invalid TPUI
24	TPUI assignment limits unacceptable
2F	insufficient memory
30	overload (NOTE)
40	test call back: normal, en-bloc
41	test call back: normal, piecewise
42	test call back: emergency, en-bloc
43	test call back: emergency, piecewise
5F	invalid message
60	information element error
64	invalid information element contents
70	timer expiry

All other values are reserved.

NOTE: If a {LCE-PAGE-REJECT} message with the <<REJECT-REASON>> "overload" is received, the portable part should try to access an other radio fixed part belonging to the same paging area.

7.7.35 RES

The purpose of the authentication parameter <<RES>> information element is to provide the calculated authentication response signature.

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

RES information element

NOTE: This information element is used for either the RES1 or the RES2 information. The actual contents are determined by the direction of transmission.

RES field coding (octet 3 to 6)
RES shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

7.7.36 RS

The purpose of the authentication parameter <<RS>> information element is to provide a number to be used together with <<RAND>> and the authentication key to calculate the authentication response signature.

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

RS information element

RS field coding (octet 3 to L+2)
RS shall be coded with the natural binary value with the least significant bit in position 1 of octet L+2.

7.7.37 Segmented info

The purpose of the <<SEGMENTED-INFO>> element is to indicate that the message in which is occurs contains only part of a segmented information element. When used, this element shall always appear immediately before the segmented element to which it refers.

```
Bit: | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
     _________________________________      Octet:
     | 0 |   << SEGMENTED-INFO >>      |      1
     |_________________________________|
     |     Length of Contents (L)      |      2
     |_________________________________|
     | F | No. of segments remaining   |      3
     |___|_____________________________|
     | 0 | Segmented element type      |      4
     |___|_____________________________|
```

SEGMENTED-INFO information element

F bit coding:

Bit	8	Meaning
	1	First segment follows
	0	Subsequent segment follows

No of segments remaining: the number of remaining segments (including the following segment) that are still to be sent. This is coded with the natural binary value, with the least significant bit in position 1.

Segmented element type: the normal coding of the <<SEGMENTED-INFO>> element (shall only refer to a variable length information element).

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 ext	Coding std.		M	Change Mode				3
	1	Extended change mode							3a
	1	A attributes			R	B attributes			4

SERVICE-CHANGE-INFO information element

Coding standard:

Bits	7 6	Meaning
	0 0	DECT standard coding
	All other values reserved.	

M (Master) coding:

Bits	5	Meaning
	0	Initiating side is master
	1	Receiving side is master

Change mode coding:

Bits	4 3 2 1	Meaning
	0 0 0 0	None
	0 0 0 1	Connection Reversal
	0 0 1 0	Bandwidth change (NOTE 1)
	0 1 0 0	Rerouting (of U-plane links) (NOTE 1)
	0 1 1 0	Rerouting plus bandwidth change (NOTE 1)
	1 0 0 0	Suspend
	1 0 0 1	Resume
	1 1 1 1	Reserved for extension (NOTE 2)
	All other values reserved.	

NOTE 1: Additional information elements shall be included in the message when indicating "bandwidth change" or "rerouting". Refer to subclause 9.6.

NOTE 2: When using the reserved value, octet 3a shall follow containing extended coding of the service change.

NOTE 3: Octet 4 shall only appear for "suspend" and "resume" codings.

Extended change mode:
Extended change mode is reserved for further standardisation.

A attributes coding:

Bits 7 6 5	Meaning
0 0 0	Not applicable
0 1 0	Maintain old connection(s)
0 1 1	Release old connection(s)

Reset (R) coding:

Bits 4	Meaning
0	Do not reset state variables
1	Reset state variables

B attributes coding:

Bits 3 2 1	Meaning
0 0 0	Not applicable
0 1 0	Interrupt data transfer
0 1 1	Maintain data transfer

7.7.39 Service class

The purpose of the <<SERVICE-CLASS>> information element is to identify services which a PT is allowed to use.

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

SERVICE-CLASS information element

Service class field coding (octet 3a):

Bits 8 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0 1	One nominated number only may be called
0 0 0 0 0 0 1 0	As above and local calls are allowed
0 0 0 0 0 0 1 1	As above and national calls are allowed
0 0 0 0 0 1 0 0	As above and mobile and premium service calls are allowed
0 0 0 0 0 1 0 1	As above and international calls are allowed
0 0 0 0 0 1 1 0	As above and satellite services are allowed

7.7.40 Set-up capability

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

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

SETUP-CAPABILITY information element

Page capability coding (octet 3):

Bits 2 1	Meaning
0 1	Normal paging
1 0	Fast paging

All other values reserved.

Set-up capability coding (octet 3):

Bits 4 3	Meaning
0 1	Normal set-up
1 0	Fast set-up

All other values reserved.

NOTE: Explicit provision for extension of this element is provided. Implementors should use the 0/1 ext flag (bit 8) to detect the use of additional octets in future versions.

7.7.41 Terminal capability

The purpose of the <<TERMINAL-CAPABILITY>> element is to convey some aspects of the PP capabilities to the FP during call establishment.

Bit: 8	7	6	5	4	3	2	1	Octet:
0	<< TERMINAL-CAPABILITY >>							1
Length of Contents (L)								2
0/1	tone capab.			display capab.				3
0/1	extended character sets							3a (NOTE 1)
0/1	echo param			N-REJ		A-VOL		3b
0/1	slot type capability							3c
1	0 Spare (NOTE 9)	0	0	0	0	0	0	3d

TERMINAL-CAPABILITY information element

NOTE 1: Octet 3a shall only appear if "extended display" is indicated in octet 3.

Display capability coding (octet 3):

Bits 4 3 2 1	Meaning
0 0 0 0	Not applicable
0 0 0 1	No display; (NOTE 3)
0 0 1 0	Numeric (NOTE 5)
0 0 1 1	Numeric-plus (NOTE 5)
0 1 0 0	Alphanumeric (NOTE 6)
0 1 0 1	Full display (NOTE 5)
1 1 1 1	Extended display capability (octet 3a shall follow)

All other values reserved.

Tone capability coding (octet 3):

Bits 7 6 5	Meaning
0 0 0	Not applicable
0 0 1	No tone capability (NOTE 3)
0 1 0	dial tone only
0 1 1	E.182 tones supported (NOTE 10)
1 0 0	Complete DECT tones supported

All other values reserved.

Extended character sets (octet 3a)
This is a bit pattern indicating capability in one or more character sets. A "1" in a bit position means full capability in the indicated character set; a "0" means incomplete capability (any capability less than full capability).

Bit 1:	DECT character set
Bit 2:	IA5 character set
Bit 3:	ERMES character set
Bit 4:	ASCII character set

All other bits are reserved, and should be set to "0".

NOTE 2: Refer to <<ALPHANUMERIC>> information element for details of these extended character sets. The default capability is no extended character set capability.

Echo parameters (octet 3b):

Bits	7 6 5	Meaning
	0 0 0	Not applicable
	0 0 1	Minimum TCL (>34 dB); (NOTE 3, NOTE 4)
	0 1 0	Full TCL (>46 dB); (NOTE 4)

All other values reserved.

Portable part ambient Noise REJection capability (N-REJ) (octet 3b):

Bits	4 3	Meaning
	0 0	Not applicable
	0 1	No noise rejection; (NOTE 3, NOTE 4)
	1 0	Noise rejection provided (NOTE 4)
	1 1	Reserved

Adaptive VOLume control provision (A-VOL) (octet 3b):

Bits	2 1	Meaning
	0 0	Not applicable
	0 1	No PP adaptive volume control; (NOTE 2)(NOTE 3)
	1 0	PP adaptive volume control used (NOTE 3)
	1 1	Disable FP adaptive volume control (NOTE 3)

Slot type capability (octet 3c)
This is a bit pattern indicating the slot type capabilities. A "1" in a bit position indicates capability of the indicated slot type; a "0" indicates no capability.

Bit 1:	Half slot; j = 0
Bit 4:	Full slot; (Note 3)
Bit 5:	Double slot

All other bits are reserved, and should be set to "0".

NOTE 3: This capability shall be assumed as the default value unless otherwise specified by a service profile, if the <<TERMINAL-CAPABILITY>> information element is omitted.

NOTE 4: Refer to ETS 300 175-8 [8] for a definition of TCL, PP Adaptive VOLume (A-VOL) control, PP ambient Noise REJection (N-REJ) and the usage of these parameters.

NOTE 5: Numeric displays shall display at least the following characters: space, 0-9. Numeric-plus displays shall also display the following characters: *, #, a, b, c, d.

NOTE 6: Alphanumeric displays shall display at least the following characters: space, 0-9, *, #, a-z and A-Z.

NOTE 7: Full displays shall display the full DECT character set (including graphics characters).

NOTE 8: All displays should support all of the DECT cursor control characters. The "clear display" code shall always be supported.

NOTE 9: Explicit provision for extension of this element is provided. Implementors should use the 0/1 extended flag (bit 8) to detect the use of additional octets in future versions.

NOTE 10: "E.182 tones supported" indicates support of all of the E.182 compatible tones identified in subclause 7.6.8.

7.7.42 Transit delay

The purpose of the <<TRANSIT-DELAY>> element is to indicate the allowable delay that shall be imposed for data transmitting the DECT subnetwork.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< TRANSIT-DELAY >>							1
	Length of Content (L)								2
	1	0	Forward Delay						3
	1	0	Backward Delay						4

TRANSIT-DELAY information element

Forward delay (backward delay) octet 3 (and 4): the <<TRANSIT-DELAY>> shall be coded with the natural binary value, and the result placed in the octet with the least significant bit in position 1. Delay shall be calculated in steps of 1 TDMA frame (10 ms).

Allowable values are "1" to "63".

7.7.43 Window size

The purpose of the <<WINDOW-SIZE>> element is to indicate (and optionally to negotiate) the window size to be used for frame transmission.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< WINDOW-SIZE >>							1
	Length of Content (L)								2
	1	Forward Value (NOTE 1)							3
	1	Backward Value (NOTE 2)							4

WINDOW-SIZE information element

Forward value (backward value) octet 3 (and 4): the <<WINDOW-SIZE>> shall be coded with the natural binary value, and the result placed in the octet with the least significant bit in position 1. Allowable values are "1" to "127".

NOTE 1: The value "0" shall be used to indicate "not applicable" in the event that no window size is defined for the forward direction.

NOTE 2: Octet 4 may be omitted, in which case the backward value shall be understood to be equal to the forward 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

ZAP-FIELD information element

Contents field (octet 3)
Contains the 4 bit ZAP value.

8 B-FORMAT message structures

8.1 General

The B-FORMAT messages shall only be originated by (and supplied to) either the LCE or the CLMS entity:

Message type	Originator
{LCE-REQUEST-PAGE}	LCE
{CLMS-FIXED}	CLMS

All the messages shall be fixed length, in order to allow simple mapping of the messages on to the lower layer broadcast channels (the MAC layer BS logical channel). Refer to ETS 300 175-3 [3].

All messages shall be sent to the B-SAP using the DL-BROADCAST-req or DL-EXPEDITED-req primitive. This shall use the broadcast service of the DLC.

The following formats are defined:

	Format	Frame length (octets)
-	short format	3 octets
-	long format	5 octets
-	extended format	5, 10, 15, 20, 25 or 30 octets

NOTE: Extended format messages shall be sent in a single primitive. Fragmentation of the message (into slot size pieces) is performed by the MAC layer. Refer to ETS 300 175-3 [3].

8.2 LCE request paging messages

Request paging messages shall use one of the following formats:

a) short format;

b) long format.

When using short format messages, or long format messages with the IPUI address structure (see subclause 8.2.2), the following default values shall apply for the missing fields:

Target number of bearers:
default value = 1

Symmetry:
default value = symmetric connection

Slot type:
no default value is defined;
if missing, the PT may select any suitable slot type.

MAC connection type:
no default value is defined;
the PT may select any suitable connection type.

MAC packet lifetime:
default value = unlimited.

NOTE 1: The default values are chosen so that the short format message can be used to indicate most types of single bearer duplex connection. The only exception is I_p-error-correct services that require a different packet lifetime.

For multibearer connections, or for a single bearer connections with different attributes, the long format message with TPUI address structure should be used to supply the additional service attributes. The following default attributes shall apply to this messages:

Minimum number of bearers:
default value = target number of bearers

Otherwise, the LCE header coding "advanced - unknown" shall be used. In this event only a single bearer connection of unknown service type can be established and a subsequent service modification procedure is required. Refer to ETS 300 175-3 [3], subclause 10.2.4.3 for more details of service modification.

NOTE 2: A subsequent service modification is essential if the LCE header coding indicates "advanced - unknown" in order to define the wanted connection attributes. Service modification may also be used in other cases (e.g. to modify a known established connection).

8.2.1 Short format message

The short format message shall contain 20 bits of information, placed into a 3 octet frame:

Bit:	8	7	6	5	4	3	2	1	Octet:
	X	X	X	X	W	LCE Header			1
	TPUI Address								2
	TPUI Address (cont)								3

SHORT address structure

The TPUI address element shall be derived as follows:

W = "1": address derived from assigned TPUI:
address = lowest 16 bits of assigned TPUI

W = "0": address derived from default TPUI:
address = lowest 16 bits of default individual TPUI.

Refer to ETS 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.

LCE header coding
The LCE header coding shall indicate the U-plane service (MAC service type) required:

Bits 3 2 1	U-plane service (MAC service type)
0 0 0	None
0 0 1	Reserved
0 1 0	Reserved
0 1 1	Unknown
1 0 0	I_N-min_delay
1 0 1	I_N-normal_delay
1 1 0	I_p-error-detect
1 1 1	I_p-error-correct

NOTE 1: The coding "none" indicates that no U-plane service is required. This should be used to indicate services that only require a C-plane (e.g. MM procedures).

NOTE 2: If the paging message contains a connectionless TPUI, the U-plane coding may be used to indicate the expected service type. If the coding "unknown" is used, the PP should accept any suitable service at the indicated transmission. If the coding "none" is used, the PP should only accept C-plane connectionless services. The "none" coding shall also be used to announce CLMS messages.

8.2.2 Long format message

The long format message shall contain 36 bits of information, placed into a 5 octet frame. There are two structures for the long format message, and the chosen structure shall be indicated by the coding of the W bit:

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>W=1</td><td colspan="3">LCE Header</td><td>1</td></tr>
<tr><td></td><td colspan="4">Attributes</td><td colspan="4">TPUI Address</td><td>2</td></tr>
<tr><td></td><td colspan="8">TPUI Address (cont)</td><td>3</td></tr>
<tr><td></td><td colspan="8">TPUI Address (cont)</td><td>4</td></tr>
<tr><td></td><td colspan="4">Target bearers</td><td colspan="4">MAC pkt life</td><td>5</td></tr>
</table>

TPUI address structure

<table>
<tr><th>Bit:</th><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet:</th></tr>
<tr><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>W=0</td><td colspan="3">LCE Header</td><td>1</td></tr>
<tr><td></td><td colspan="4">IPUI Class</td><td colspan="4">IPUI Address</td><td>2</td></tr>
<tr><td></td><td colspan="8">IPUI Address (cont)</td><td>3</td></tr>
<tr><td></td><td colspan="8">IPUI Address (cont)</td><td>4</td></tr>
<tr><td></td><td colspan="8">IPUI Address (cont)</td><td>5</td></tr>
</table>

IPUI address structure

The address element shall be derived as follows:

W = "1": TPUI address element:
TPUI address = complete TPUI (20 bits)

W = "0": IPUI address element:
class = IPUI Class
IPUI address = lowest 28 bits of IPUI

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

LCE header coding:
refer to subclause 8.2.1.

Attributes coding:
The attributes field can contain two alternative codings, that are distinguished by the setting of bit 8. This means that a paging message can specify either the slot type for symmetric connections or the asymmetric parameter.

Slot type option:

Bits	8	7	6	5	Meaning
	0	0	0	0	Half slot; j = 0
	0	1	0	0	full slot
	0	1	0	1	double slot

Symmetry option:

Bits	8	7	6	5	Meaning
	1	0	0	1	Symmetric connection
	1	1	0	0	Asymmetric F to P with 1 duplex bearer
	1	1	0	1	Asymmetric F to P with 2 target duplex bearers
	1	1	1	0	Asymmetric P to F with 1 duplex bearer
	1	1	1	1	Asymmetric P to F with 2 target duplex bearers

All other values reserved.

NOTE 1: The default value shall be assumed for the missing option.

NOTE 2: A minimum of 1 duplex bearer is required for all asymmetric connections to provide the "pilot" bearer functions. Refer to ETS 300 175-3 [3].

Target bearers (advanced connections only):

Bits	8 7 6 5	Meaning
	0 0 0 0	Undefined: (pilot bearer only)
	N N N N	Target number of bearers required

NOTE 3: The target number of bearers (NNNN) is coded with the natural binary value with the least significant bit in bit position "5". The allowable values are "1" to "15".

The target number of bearers defines the total number of paired bearers to be used for the connection. For symmetric connections this refers to the total number of duplex bearers. For asymmetric connections this refers to the total number of duplex bearers PLUS the total number of double simplex bearers.

For asymmetric connections, the direction of the double simplex bearers, and the number of duplex bearers shall be defined by using the symmetry option for "attributes" field.

MAC packet life:

Bits	4 3 2 1	Meaning
	0 0 0 0	Not applicable
	1 n n n	Maximum packet lifetime (I_P; error_protect service only)

NOTE 4: The maximum packet lifetime (nnn) is coded with the natural binary value with the least significant bit in bit position "1". The allowable values are "0" to "7". The value "0" shall be interpreted as unlimited (i.e. infinite). The values "1" to "7" define the maximum lifetime in TDMA frames. Refer to ETS 300 175-3 [3] for the use of this attribute.

8.3 CLMS-FIXED messages

8.3.1 General message structure

Each {CLMS-FIXED} message shall contain 1 or more message sections, where each section shall contain 36 bits of information in a 5 octet frame. {CLMS-FIXED} messages can only carry information equivalent to that contained in the <<ALPHANUMERIC>> information element (see subclause 7.7.3). {CLMS-FIXED} messages shall use one of the following formats:

a) long format (single section message);

b) extended format (multi section message).

The first section of each message shall contain addressing and control information. The remaining sections shall contain any data. The contents of any given section shall be indicated by the A bit.

Each message shall only comprise complete sections, up to a maximum of 6 sections (i.e. one address section followed by up to 5 data sections). All of the sections for a complete message shall be delivered in a single primitive, and should be received in a single primitive. Refer to subclause 12.3.1.

NOTE 1: The received message may be incomplete. Missing sections may not be detected by the lower layers before delivery. Missing sections may be detected by examining the length indicator element and/or the data segment numbers.

The possible data structures are defined by the protocol discriminator field, this shall use the same coding as octet 3 of the <<ALPHANUMERIC>> information element. This allows for either 8 bit characters, 4 bit characters or application specific codings.

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

CLMS-FIXED message structure: address section

NOTE 2: The contents 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

CLMS-FIXED message structure: data section

8.3.2 Message elements

A-bit coding (octet 1):

A = "1"	address section
A = "0"	data section

CLMS header coding (octet 1):

The header coding is different for address sections and data sections. The address section allows two types of message to be defined, a DECT standard message or a general alphanumeric message. The basic structure of these messages is the same, but DECT standard messages provide standard codings for the message contents.

CLMS header coding for address section:

Bits	3 2 1	Message type	octet 4	octet 5
	0 0 1	One section:	Standard	Data
	0 1 0	Multi-section:	Standard	Length indicator
	1 0 1	One section:	Alphanumeric	Data
	1 1 0	Multi-section:	Alphanumeric	Length indicator

All other values reserved.

CLMS header coding for data section:

Bits	3 2 1	Meaning
	n n n	Data section number

The first data section shall be numbered 000. The following sections shall be numbered in ascending order.

Address (octets 2 and 3 of address section):

The address shall only be derived from a connectionless TPUI:

address = lowest 16 bits of connectionless TPUI.

NOTE 1: The CLMS service requires the use of assigned TPUIs. Refer to ETS 300 175-6 [6].

Protocol discriminator (octet 4 of address section):

Coding as for octet 3 of <<ALPHANUMERIC>>

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	Char. Type			O/E	Char. Set			4

Format of Protocol Discriminator (PD)

NOTE 2: DECT standard messages shall only use the DECT standard 8-bit or 4-bit characters.

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

Format of Length Indicator (LI)

NOTE 3: Each complete data segment shall contain 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				*

Format of Data/Fill

Each Data/Fill octet is used to carry the user information. This shall be formatted in accordance with the format indicated in the protocol discriminator octet.

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

- the original character is placed in the octet, with the least significant bit in bit position "1", and a unused bit positions are filled with "0".

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

Fill characters (8-bit or 4-bit as appropriate) shall then be inserted to fill up the final octets.

NOTE 4: A complete data segment that contains no valid data (i.e. fill only) shall not be transmitted.

8.3.3 Standard message structures

8.3.3.1 General

DECT standard messages shall only use one of the DECT standard character sets: either 4-bit characters or 8-bit characters. In both cases, the first character of the message shall be used as a message type identifier to define the meaning of the following characters.

8.3.3.2 Messages using 4-bit characters

Table 16: Messages using 4-bit characters

Message Type	1st char.	2nd char.	Other characters
Tone alert	0	0 to 9	not allowed
Other messages are for further standardisation			

Message type 0: tone alert: the second character identifies one of ten possible alerting tones. The use of tones by the FT, and the resulting sound at the PT shall not be defined in this ETS.

8.3.3.3 Messages using 8-bit characters

Table 17: Messages using 8-bit characters

Message Type	1st char.	2nd char.	Other characters
8-bit messages are for further standardisation			

9 Call Control (CC) procedures

9.1 General

The Call Control (CC) procedures provide mechanisms to support both circuit oriented and packet oriented services. Each independent service is called a "call" and this is controlled by an independent instance of CC. A CC always establishes circuit oriented lower resources to provide the service (i.e. uses the MAC layer connection oriented service). The CC represents a group of procedures covering all aspects of call establishment and release, and also covering a range of call related supplementary services (CRSS).

The protocol allows for multiple instances of a CC call at both the fixed termination and at the portable termination (for example, a PT may provide two or more simultaneous calls). These multiple instances are assumed to operate completely independently from each other. The possible existence of multiple instances is therefore ignored in the following clauses, which only describe the procedures for a single instance.

Figure 3 illustrates the states and transitions on the PT side.

Figure 4 illustrates the states and transitions on the FT side.

An alternative description of the CC state transitions is included in Annex B. This contains a state transition table, plus a summary of the transition procedures. This annex is included as a shortform summary. In the event of any discrepancy, the main text (the following clauses) take precedence.

A reliable C-plane DLC link (LAPC) must be available before any of these CC procedures can operate. The establishment and maintenance of this link is the responsibility of the LCE and is described in Clause 14.

NOTE: A "LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. If a CC timer expires whilst in this state, the resulting release should be handled locally.

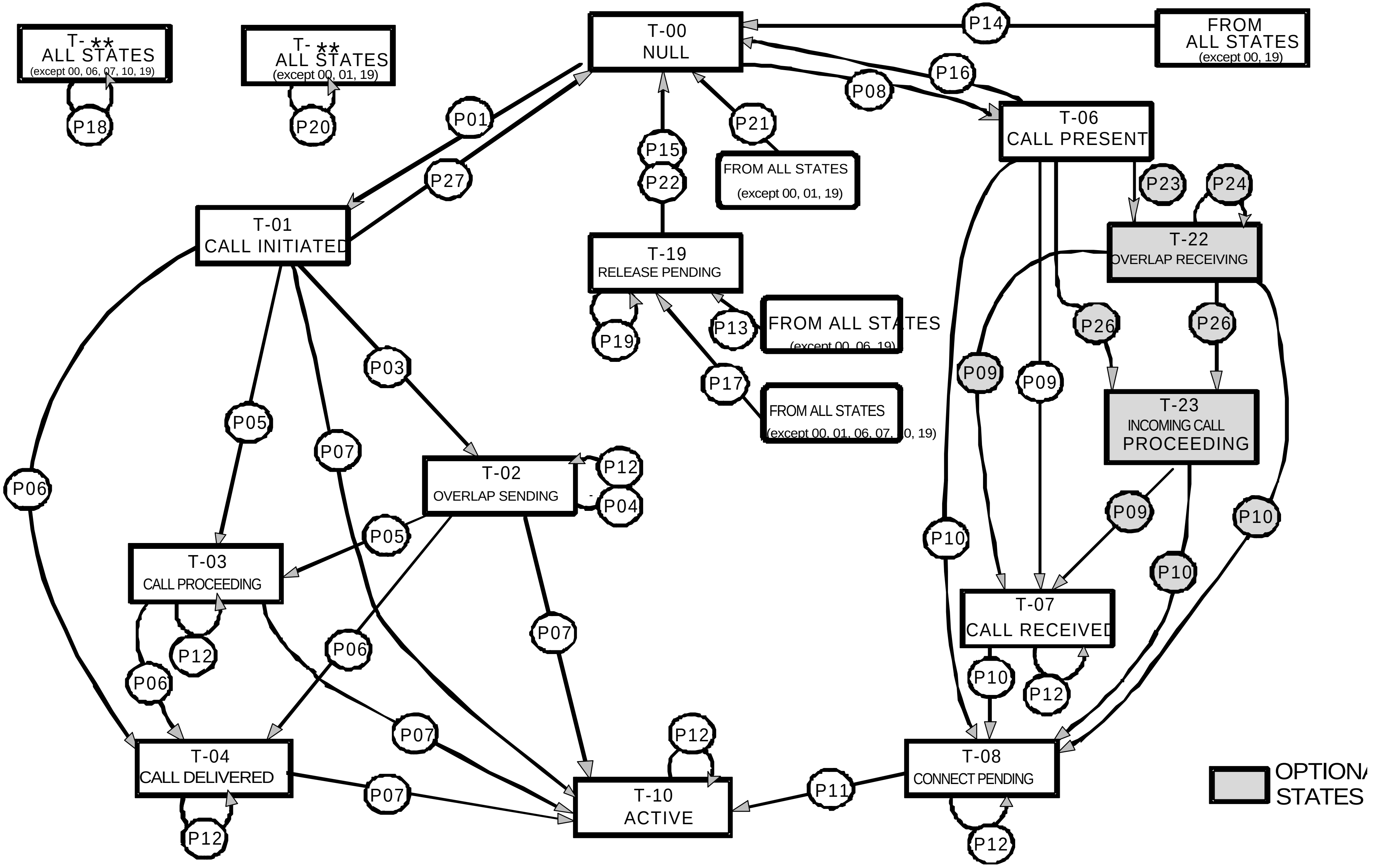


Figure 3: Call control states in the PT

]

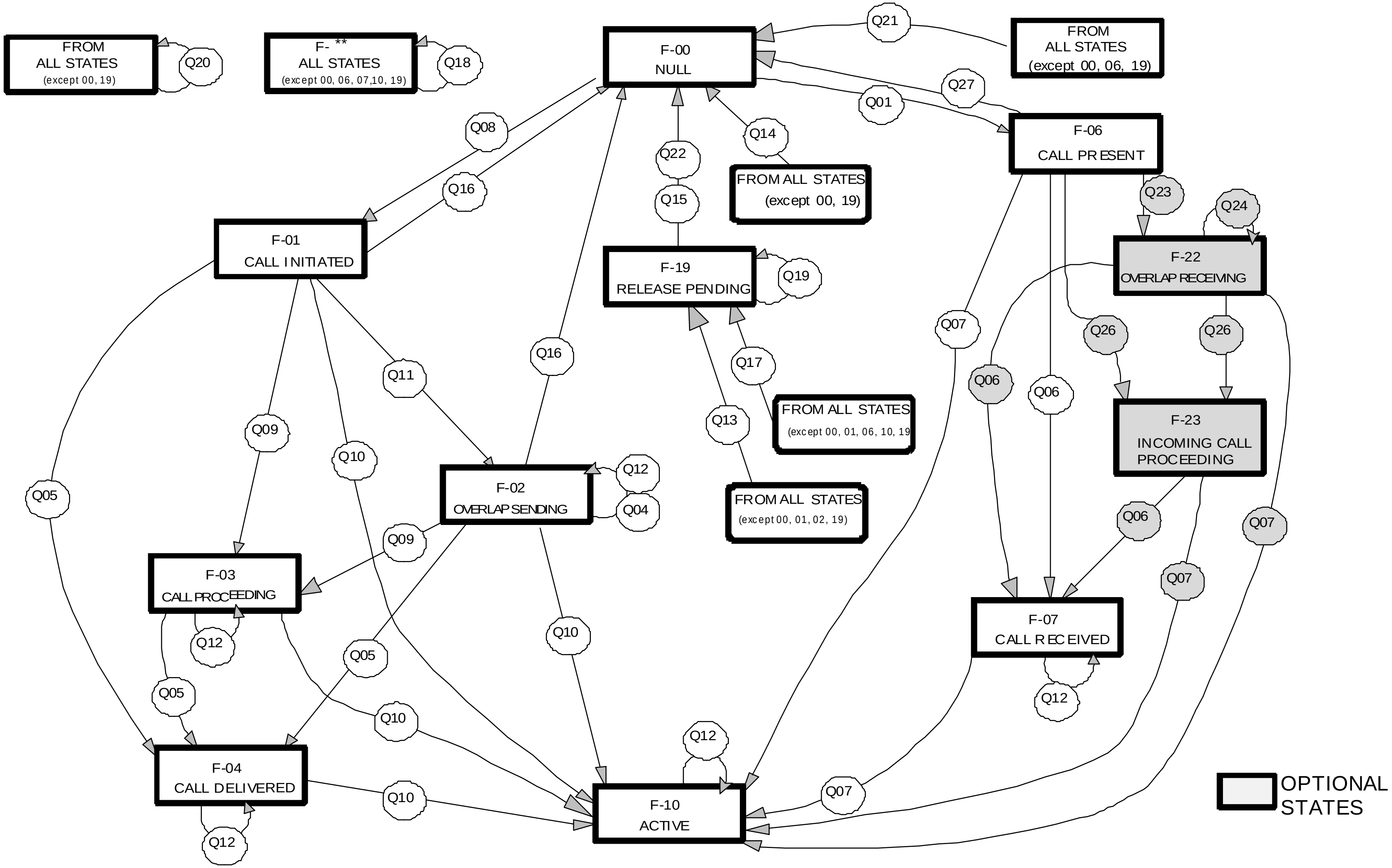


Figure 4: Call control states in the FT

9.2 Call Control (CC) states

9.2.1 States at PT

Central call states

9.2.1.1 State T-00: "NULL"

No call exists.

9.2.1.2 State T-19: "RELEASE PENDING"

The PT has sent a release message to the FT, but has not received a response.

9.2.1.3 State T-10: "ACTIVE"

a) The PT user has answered an incoming call;

b) the PT has received an indication that the FT has connected a PT outgoing call.

PT originated call states (outgoing call)

9.2.1.4 State T-01: "CALL INITIATED"

A PT initiated call has been started, by sending a set-up message to the FT.

9.2.1.5 State T-02: "OVERLAP SENDING"

An outgoing call is being established using "OVERLAP SENDING".

9.2.1.6 State T-03: "CALL PROCEEDING"

The PT has received a message from the FT to confirm that all set-up information has been received.

9.2.1.7 State T-04: "CALL DELIVERED"

The PT has received a message from the FT that indicates that called party alerting has been started.

PT terminated call states (incoming call)

9.2.1.8 State T-06: "CALL PRESENT"

The PT has received a set-up message from the FT, but has not yet responded.

9.2.1.9 State T-07: "CALL RECEIVED"

The PT has sent a message to the FT to report alerting of the user, but the user has not yet responded.

9.2.1.10 State T-08: "CONNECT PENDING"

The PT user has answered the call, but is waiting for a message from the FT giving confirmation of a U-plane connection (assumed to be an end-to-end connection).

9.2.2 States at FT

Central call states

9.2.2.1 State F-00: "NULL"

No call exists.

9.2.2.2 State F-19: "RELEASE PENDING"

The FT has sent a release message to the PT, but has not received a response.

9.2.2.3 State F-10: "ACTIVE"

a) The FT has allocated an incoming call to one PT;

b) the FT has sent a message to the PT reporting connection of an outgoing call (assumed to mean that the called party has answered the outgoing call).

PT originated call states (outgoing call)

9.2.2.4 State F-01: "CALL-INITIATED"

A PT initiated call set-up has been started. The FT has received a set-up message from the PT, but has not yet replied.

9.2.2.5 State F-02: "OVERLAP SENDING"

A PT initiated call is being established using "OVERLAP SENDING".

9.2.2.6 State F-03: "CALL PROCEEDING"

The FT has sent a message to the PT to confirm that all set-up information has been received.

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.

PT terminated call states (incoming call)

9.2.2.8 State F-06: "CALL PRESENT"

The FT has sent a set-up message to the PT, but has not yet received a satisfactory response.

9.2.2.9 State F-07: "CALL RECEIVED"

The FT has received a message from the PT to report that it is alerting the user (but the user has not yet responded).

9.2.3 Optional states (PT and FT)

The following states are optional. They are required for incoming calls, when DECT is being used as an intermediate network. In this case, the call is not terminated in the DECT portable termination, and these additional states are used to allow the call establishment procedures to interact with the attached network on the PT side.

9.2.3.1 States T-22 and F-22: "OVERLAP RECEIVING"

An incoming call is being established using "OVERLAP RECEIVING".

9.2.3.2 States T-23 and F-23: "INCOMING CALL PROCEEDING"

The PT has sent a message to the FT to confirm that all set-up information has been received.

9.3 Call establishment procedures

9.3.1 PT initiated call establishment (outgoing call)

PT initiated call establishment is started upon receipt of a MNCC-SETUP-req primitive by the CC entity at the PT side (P-CC). This primitive shall specify whether a normal or emergency call is required.

9.3.1.1 Call request

Case A: normal call request

The CC entity in the PT (P-CC) starts a normal call establishment by sending a {CC-SETUP} message to its peer CC entity in the FT (F-CC). This message is submitted to the LCE in the PT, and the P-CC entity enters the "CALL INITIATED" state and starts timer P<CC.03>.

The {CC-SETUP} message shall carry a full portable part identity (the IPUI) plus a full fixed part identity (the relevant ARI) according to the identity rules given in ETS 300 175-6 [6].

The {CC-SETUP} message shall contain the <<BASIC-SERVICE>> information element. This element shall indicate "normal set-up" and may optionally indicate "default service attributes", in which case the service shall be defined by the defined default codings given in Annex E and no further <<IWU-ATTRIBUTES>> or <<CALL-ATTRIBUTES>> elements shall be included. Alternatively, if the service is indicated as "other", the set-up message shall also contain both the <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> elements to fully define the required service, such that all the necessary resources can be reserved and installed by the FT and the interworking unit at the FT side (F-IWU).

NOTE 1: The set-up message may contain a list of attribute elements when using prioritised list negotiation. Refer to subclause 15.2.2.

The PT should include the <<TERMINAL-CAPABILITIES>> element in the set-up message. If omitted the default values shall be assumed.

NOTE 2: The action of a FT in response to an omitted <<TERMINAL-CAPABILITIES>> element is defined for the public access profile service in ETS 300 175-9 [9].

Case B: emergency call request

Emergency call establishment uses the same CC procedures as normal call establishment, except that the call shall be indicated as an "emergency call" in the <<BASIC-SERVICE>> information element.

The <<BASIC-SERVICE>> element for an emergency call request shall always indicate the "default service attributes" (i.e. shall only request a single bearer speech call).

NOTE 3: Emergency call requests shall only be supported for PT initiated calls.

Case C: external handover request

Call establishment for external handover uses the same CC procedures as normal call establishment, except that the call shall be indicated as an "external handover" in the <<BASIC-SERVICE>> information element.

NOTE 4: External handover requests shall only be supported for PT initiated calls.

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 fulfill 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.

If the F-IWU accepts the call it is expected to reply with one of the following primitives:

a) a MNCC-SETUP-ACK-req primitive;

b) a MNCC-CALL-PROC-req primitive;

c) a MNCC-ALERT-req primitive;

d) a MNCC-CONNECT-req primitive.

Upon receipt of one of these primitives, the F-CC shall act according to subclauses 9.3.1.3 to 9.3.1.9.

Call reject

If the F-CC cannot meet any of the set-up requests, or if the {CC-SETUP} message contains errors or inconsistencies, or if the F-IWU rejects the call by responding to the MNCC-SETUP-ind primitive with a MNCC-REJECT-req primitive, the FT shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the "NULL" state.

The MNCC-REJECT-req shall always include a <<RELEASE-REASON>> (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the PT shall act according to subclause 9.5.2.

NOTE 2: Call rejection may also occur as part of exchanged attribute service negotiation. Refer to subclause 15.2.3.

Expiry of timer <CC.03>

Timer P<CC.03> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {CC-NOTIFY} message. If timer P<CC.03> expires before a suitable reply (or a restart) is received, the P-CC shall immediately release the call by sending a {CC-RELEASE-COM} message, with the reason set to "timer expiry". It shall then issue a MNCC-REJECT-ind primitive indicating unacknowledged release (cause = local timer expiry) and shall enter the "NULL" state.

9.3.1.3 Selection of lower layer resources

The following procedures shall only be used when using advanced connections. The elements described in this subclause shall be omitted when using basic connections, and this omission shall be understood to indicate a basic connection.

The PT should indicate the lower layer resources (DLC U-plane link identifier and MAC connection identifier) by including a <<CONNECTION-IDENTITY>> element in the {CC-SETUP} message. If this element is included, the FT shall be obliged to use the indicated resources or shall reject the call.

NOTE 1: The attributes of the indicated connection may still be undefined (i.e. connection type "unknown") at this point. The attributes shall subsequently be defined by the MAC establishment procedures (PT initiated).

Alternatively <<CONNECTION-ATTRIBUTES>> elements may be used to postpone the establishment (or modification) of suitable connection(s) until the set-up is accepted (e.g. if the PT is attempting to set-up a second call using the C-plane resources of an existing call). In this event, the PT may include one or more <<CONNECTION-ATTRIBUTES>> elements in the {CC-SETUP} message; one element for each postponed connection. Each element shall contain a valid LCN assignment 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-ALERT} 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 shall indicate that this modification has been initiated.

NOTE 3: "Unknown" PT assignments are intended to allow FT choice when the indicated resources require FT modification of existing connections. "Unknown" assignments may also be used in other cases, provided that all possible associations are acceptable for the PT.

Upon receipt of the first message from the FT indicating acceptance of the set-up, the PT shall immediately establish all remaining connections (or modify existing connections) and shall associate all remaining U-plane links to complete the required service.

NOTE 4: In all cases, it is the responsibility of the PT to establish any new connections.

If any of the required resources are not available, the FT shall reject the call.

Both the <<CONNECTION-IDENTITY>> and the <<CONNECTION-ATTRIBUTES>> elements shall be omitted from all messages for a call establishment relating to a basic connection. If this basic connection is not already established when the {CC-SETUP} message is received, the call shall be rejected.

9.3.1.4 Connection of U-plane

The PT is not required to request the LLME to connect its receive U-plane unless it receives a message containing the <<PROGRESS-INDICATOR>> element indicating cause no. 8 ("In-band information or appropriate pattern is now available in band"). The FT should not assume that the PT has connected the U-plane unless this message has been sent.

NOTE: If this <<PROGRESS-INDICATOR>> element is not used, the PT may delay connection of the U-plane until receipt of the {CC-CONNECT} message. See subclause 9.3.1.7.

9.3.1.5 Overlap sending

"OVERLAP SENDING" is indicated if the F-CC receives a MNCC-SETUP-ACK-req primitive.

NOTE 1: This indicates that the set-up message contains either no called number information, or incomplete called number information, or called number information that cannot be determined to be complete.

Upon receipt of this primitive, the F-CC shall send a {CC-SETUP-ACK} message to the P-CC. It shall then start timer F<CC.01> and shall enter the "OVERLAP SENDING" state. In this state it is waiting for a {CC-INFO} message (or messages) from the P-CC.

Upon receipt of the {CC-SETUP-ACK} message, the P-CC shall stop timer P<CC.03>, shall optionally start timer P<CC.04>. It shall then issue a MNCC-SETUP-ACK-ind primitive and shall enter the "OVERLAP SENDING" state.

The remainder of the set-up information should now be supplied by the PP application in a series of one or more MNCC-INFO-req primitives. The P-CC shall send this information in one or more {CC-INFO} messages.

The called party number shall be supplied by the PP application in one of two ways:

- en-bloc sending, where the called party number is sent in a single variable length <<CALLED-PARTY-NUMBER>> information element;

- piecewise sending, where the called party number is sent in a series of fixed or variable length <<"KEYPAD">> information elements, contained in one or more messages (one <<"KEYPAD">> element per message).

Only one method of sending shall be used within any one call.

NOTE 2: This ETS allows piecewise sending to include more than one character in each <<"KEYPAD">> information element.

NOTE 3: The length of the called party number shall be defined by the length of the <<CALLED-PARTY-NUMBER>> information element when this is used. If <<"KEYPAD">> information elements are used the length definition is specific to the F-IWU: it may be undefined, or it may be defined by the <<SENDING-COMPLETE>> information element.

Upon receipt of a {CC-INFO} message, the F-CC shall immediately forward the contents to the F-IWU in a MNCC-INFO-ind primitive, and shall restart timer F<CC.01>.

Call reject

If the F-CC cannot meet any of the set-up requests whilst in the "OVERLAP SENDING" state, or if a {CC-INFO} message contains errors or inconsistencies, or if the F-IWU rejects the call by responding to a MNCC-INFO-ind primitive with a MNCC-REJECT-req primitive, the FT shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the NULL state.

The MNCC-REJECT-req shall always include a <<RELEASE-REASON>> (as provided by the F-IWU) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the PT shall act according to subclause 9.5.2.

9.3.1.6 Call proceeding

Upon receipt of a complete number, either in the {CC-SETUP} message or as a result of "OVERLAP SENDING", the F-IWU should respond with a MNCC-CALL-PROC-req primitive.

Upon receipt of the MNCC-CALL-PROC-req primitive, the F-CC shall stop timer F<CC.01>, shall enter the "CALL PROCEEDING" state and shall send a {CC-CALL-PROC} message to the P-CC. It shall then start timer F<CC.04>.

Upon receipt of the {CC-CALL-PROC} message, the P-CC shall stop timer P<CC.03> if running and shall optionally start timer P<CC.04>. It shall then issue a MNCC-CALL-PROC-ind primitive and shall enter the "CALL PROCEEDING" state.

NOTE: 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.

If timer F<CC.01> expires before a suitable primitive is received, the F-CC shall immediately release the call using the release procedures defined in subclause 9.5.1. The {CC-RELEASE} message shall contain the reason <<TIMER-EXPIRY>>.

9.3.1.7 Call confirmation

When the F-CC receives a MNCC-ALERT-req primitive (usually meaning that user alerting has been initiated at the called destination), the FCC 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>, shall optionally start timer P<CC.04>. It shall then issue a MNCC-ALERTING-ind primitive and shall enter the "CALL DELIVERED" state.

9.3.1.8 Call connection

Upon receiving a MNCC-CONNECT-req primitive (usually meaning that the call has been accepted by the destination), the F-CC shall request confirmation of the U-plane connection from the F-LLME. When the U-plane is confirmed, it shall stop timer F<CC.01> if running and shall send a {CC-CONNECT} message to the P-CC. It shall then enter the "ACTIVE" state.

On receipt of the {CC-CONNECT} message the P-CC shall request confirmation of the U-plane connection from the P-LLME. When the U-plane connection is confirmed, the P-CC shall stop timer P<CC.03> if running, stop timer P<CC.04> if used, and enter the "ACTIVE" state. It shall then issue a MNCC-CONNECT-ind primitive.

9.3.1.9 Expiry of timer <CC.04>

Timer P<CC.04> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {CC-NOTIFY} message. If timer P<CC.04> expires, the P-CC shall immediately release the call using the procedures described in subclause 9.5.

Equally, if timer F<CC.04> expires, the F-CC shall immediately release the call using the procedures described in subclause 9.5.

NOTE: The use of timer <CC.04> is optional for both PT and FT.

9.3.2 FT initiated call establishment (incoming call)

FT initiated call establishment is started upon receipt of a MNCC-SETUP-req primitive by the CC entity at the FT side (F-CC).

9.3.2.1 Call request

The F-CC entity starts the call establishment by sending a {CC-SETUP} message to its peer entity at the PT side (P-CC). This message is submitted to the LCE in the FT, and the F-CC enters "CALL PRESENT" state and starts timer F<CC.03>.

For individual calls, the {CC-SETUP} message shall carry a full portable part identity (the IPUI) plus a full fixed part identity (the relevant ARI) according to the identity rules given in ETS 300 175-5 [5]. For group calls the {CC-SETUP} message shall carry either one full portable part identity (one IPUI) or one group identity (one group TPUI) plus a full fixed part identity (the relevant ARI).

The {CC-SETUP} message shall contain the <<BASIC-SERVICE>> information element. This element shall indicate "normal set-up" and may optionally indicate "default service attributes", in which case the service shall be defined by the defined default codings given in Annex E and no further <<IWU-ATTRIBUTES>> or <<CALL-ATTRIBUTES>> elements shall be included. Alternatively, if the service is indicated as "other", the set-up message shall also contain both the <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> elements to fully define the required service, such that all the necessary resources can be reserved and installed by the PT.

NOTE: The set-up message may contain a list of attribute elements when using prioritised list negotiation. Refer to subclause 15.2.2.

9.3.2.2 Call accept or reject

Call accept

Upon receipt of a {CC-SETUP} message the P-CC shall enter the "CALL PRESENT" state. The P-CC entity shall examine the attributes defined in the {CC-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCC-SETUP-ind primitive.

NOTE: Either the P-CC or a PP higher layer application may reject the call. The P-CC examines the <<CALL-ATTRIBUTES>> and the <<CONNECTION-ATTRIBUTES>> elements, and the PP higher layers examine the <<IWU-ATTRIBUTES>> element. The call is only offered to the PP higher layers after it has been accepted by the P-CC.

If the PP higher layers accept the call, they are expected to respond to the P-CC with one of the following primitives:

For normal calls:

a) a MNCC-ALERT-req primitive;

b) a MNCC-CONNECT-req primitive.

For calls using "OVERLAP RECEIVING":

c) a MNCC-SETUP-ACK-req primitive;

d) a MNCC-CALL-PROC-req primitive.

Upon receipt of one of these primitives, the P-CC shall act according to subclauses 9.3.2.3 to 9.3.2.8.

Call reject

If the PT cannot meet any of the demands, or if the {CC-SETUP} message contains errors or inconsistencies, or if a MNCC-REJECT-req primitive is received in response to the MNCC-SETUP-ind primitive (thus indicating rejection by the PP higher layers), the P-CC entity shall reject the call set-up by sending a {CC-RELEASE-COM} message, and shall enter the "NULL" state.

The MNCC-REJECT-req shall always include a <<RELEASE-REASON>> (as provided by the PP higher layers) and this should be included in the {CC-RELEASE-COM} message.

Upon receipt of the {CC-RELEASE-COM} message, the FT shall act according to subclause 9.5.2.

Expiry of timer <CC.03>

If timer F<CC.03> expires before a suitable reply is received, the F-CC shall immediately release 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 when using advanced connections. These elements shall be omitted when using basic connections, and this omission shall be understood to indicate a basic connection.

The FT may indicate the lower layer resources (DLC U-plane link identifier and MAC connection identifier) by including a <<CONNECTION-IDENTITY>> element in the {CC-SETUP} message. If this element is included, the PT shall be obliged to use the indicated resources or shall reject the call. The FT may also include the <<CONNECTION-ATTRIBUTES>> element to indicate other needed connections.

NOTE 1: The attributes of the indicated connection may still be undefined (i.e. connection type "unknown") at this point. The attributes shall 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-ALERT} or {CC-CONNECT}). This element may be omitted if all associations have been defined by the FT in the {CC-SETUP} message.

If suitable resources are not available and cannot be established the PT shall reject the call.

Both the <<CONNECTION-IDENTITY>> and the <<CONNECTION-ATTRIBUTES>> elements shall be omitted from all messages for a call establishment relating to a basic connection. If this basic connection is not already established when the {CC-SETUP} message is received, the call shall be rejected.

9.3.2.4 Connection of U-plane

The PT is not required to request the LLME to connect its receive U-plane unless it receives a message containing the <<PROGRESS-INDICATOR>> element indicating cause no. 8 ("in-band information or appropriate pattern is now available in band"). The FT should not assume that the PT has connected the U-plane unless this message has been sent.

NOTE: If this <<PROGRESS-INDICATOR>> element is not used, the PT may delay connection of the U-plane until sending of the {CC-CONNECT} message. See subclause 9.3.2.7.

9.3.2.5 Overlap receiving

These procedures are optional, and shall only apply to PTs that implement this option.

Overlap receiving is for further study.

9.3.2.6 Call proceeding

For FT initiated calls, the set-up message should normally contain sufficient information to complete the call. However the F-CC may also send any supplementary information (e.g. <<"DISPLAY">> information elements) in a subsequent {CC-INFO} message (or messages) in response to MNCC-INFO-req primitives from the F-IWU.

9.3.2.7 Call confirmation

Confirmation of the call is indicated when a MNCC-ALERT-req primitive is received at the P-CC (usually indicating that user altering has been initiated). Upon receipt of this primitive, the P-CC shall send a {CC-ALERTING} message to the F-CC and shall enter the "CALL RECEIVED" state.

The F-CC, upon receipt of the {CC-ALERTING} message shall stop timer F<CC.03> and shall start timer F<CC.04> (if implemented). It shall then issue a MNCC-ALERT-ind primitive and shall enter the "CALL RECEIVED" state.

Whilst in the "CALL-RECEIVED" state, the FT may send further information to the PT in one or more {CC-INFO} messages in response to further MNCC-INFO-req primitives. The PT should issue the contents of all these messages using MNCC-INFO-ind primitives.

NOTE: Cadence following of the PT alerting may be achieved by sending a sequence of <<SIGNAL>> elements in a series of {CC-INFO} messages.

9.3.2.8 Call connection

Connection of the call is indicated when a 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 shall request confirmation of the U-plane connection from the LLME and when confirmed it shall send a {CC-CONNECT} message to the F-CC. It shall then start timer P<CC.05> and enter the "CONNECT PENDING" state.

On receipt of the {CC-CONNECT} message the F-CC shall also request confirmation of the U-plane connection from the LLME, and when confirmed it shall stop timer F<CC.03> if running and shall stop timer F<CC.04> (if implemented). It shall then issue a MNCC-CONNECT-ind primitive to the F-IWU, 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 stop timer P<CC.05>. It shall then issue a MNCC-CONNECT-cfm primitive, and shall enter the "ACTIVE" state.

If timer P<CC.05> expires, the P-CC shall immediately release the call using the normal procedure described in subclause 9.5.

9.3.2.9 Sending of <<TERMINAL-CAPABILITIES>>

The PT should include the <<TERMINAL-CAPABILITIES>> element in its first response message. If omitted the default values shall be assumed.

NOTE: The action of a FT in response to an omitted <<TERMINAL-CAPABILITIES>> element is only defined for the public access profile service. Refer to ETS 300 175-9 [9].

9.3.2.10 Expiry of timer <CC.04>

If timer F<CC.04> expires, the F-CC shall immediately release the call using the procedures described in subclause 9.5.

NOTE: The use of timer <CC.04> is optional.

9.4 Call information procedures

While in the "ACTIVE" state, the P-CC and F-CC shall immediately transfer any information received in MNCC-INFO-req primitives, using a series of one or more {CC-INFO} messages. Upon receipt of a {CC-INFO} message, the peer CC entity shall immediately issue the contents in a MNCC-INFO-ind primitive.

Service change procedures during the call information phase are described in subclause 9.6.

9.5 Call release procedures

9.5.1 Normal call release

The call release procedures may be started by the CC entity at either side at any time, upon receipt of a MNCC-RELEASE-req primitive or as a result of timer expiry as described in subclause 9.3.

NOTE 1: A MNCC-RELEASE-req primitive is an illegal response to a call set-up. The following normal call release procedure shall not be followed when responding to a call set-up. A FT in the "CALL INITIATED" or "OVERLAP SENDING" state shall respond as though rejecting the call set-up and should follow the procedures defined in subclauses 9.3.1.2 and 9.3.1.5 for PT initiated calls. A PT in the "CALL PRESENT" state shall respond as though rejecting the call set-up and should follow the procedures defined in subclause 9.3.2.2 for FT initiated calls.

To initiate a normal release, the starting entity sends a {CC-RELEASE} message, starts timer <CC.02>, and enters the "RELEASE PENDING" state. The release message may include an information element giving the reason for the release, if no reason is given "normal" release should be assumed.

Upon receipt of the {CC-RELEASE} message, the accepting side shall issue a MNCC-RELEASE-ind primitive to the IWU. Acceptance of the release by the IWU is indicated by a MNCC-RELEASE-res primitive. Upon receipt of this response, the CC shall send a {CC-RELEASE-COM} message. It shall then release all resources associated with the call and enter the "NULL" state.

Upon receipt of the {CC-RELEASE-COM} reply the initiating side shall issue a MNCC-RELEASE-cfm primitive indicating normal acknowledged release (cause = peer message). It shall then release all resources, stop timer <CC.02>, and enter the "NULL" state.

If timer <CC.02> expires before the receipt of a {CC-RELEASE-COM} message, the initiating side shall immediately send a {CC-RELEASE-COM} message. It shall then issue a MNCC-RELEASE-cfm primitive indicating an unacknowledged release (cause = local timer expiry) and shall 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.

NOTE 2: The {DISCONNECT} message used by ETS 300 102-1 [21a] has not been introduced. However, the above procedure provides a similar function by allowing limited information transfer to the initiating entity.

Both sides shall report the completion of the release of the call to their respective LCEs. This report shall be given immediately after sending the last message, the LCE shall issue the final message to the DLC before releasing the lower layer resources.

NOTE 3: If a "partial" release has been indicated in the <<RELEASE-REASON>> information element (implying that a follow-on call is expected) the CC should request a delayed release from the LCE. In this event the link should be retained for a few seconds as described in subclause 14.2.7.

9.5.2 Abnormal call release

Abnormal release is indicated by the unexpected receipt of a {CC-RELEASE-COM} message (i.e. without a prior transmission of a {CC-RELEASE} message). This may occur in any state (except for the "NULL" or "RELEASE PENDING" states).

Upon receipt of the unexpected {CC-RELEASE-COM} message the CC entity shall issue a MNCC-REJECT-ind primitive to indicate abnormal release (cause = peer message). It shall then release all resources, stop all timers, and enter the "NULL" state.

Both sides shall report the completion of the release of the call to their respective LCEs. This report shall be given immediately after sending the last message, the LCE shall issue the final message to the DLC before releasing the lower layer resources.

9.5.3 Release collisions

A release collision occurs when both sides of a call issue a {CC-RELEASE} message at the same time, such that at least one of these messages is received by a CC entity that is already in the "RELEASE PENDING" state.

If either CC entity receives a {CC-RELEASE} message, while in the "RELEASE PENDING" state, the normal release procedure is not followed by that CC entity. In this event, the CC entity shall stop timer <CC.02> and shall issue a MNCC-RELEASE-cfm primitive indicating normal acknowledged release (cause = peer message). It shall report this release to the LCE, and enter the "NULL" state.

9.6 Service change procedures

9.6.1 General

When in the "ACTIVE" state, service change procedures may be used to modify some of the existing service characteristics. This may include modification of the existing MAC connection(s) and/or the association of the call to a new MAC connection.

A service change may be indicated by the receipt of a MNCC-MODIFY-req primitive. Upon receipt of this primitive, the initiating CC entity sends a {CC-SERVICE-CHANGE} message to request the change. This message shall contain a complete description of the new (requested) service using the <<SERVICE-CHANGE-INFO>>.

NOTE 1: The <<SERVICE-CHANGE-INFO>> provides codings for a set of standard service changes. Complex service changes (in particular, a switch between 2 different service mappings) may be achieved using a combination of the suspend and resume.

Upon receipt of the {CC-SERVICE-CHANGE} message, the receiving entity shall attempt to meet the revised proposal. If the change is possible, the receiving entity shall immediately return a {CC-SERVICE-ACCEPT}. If the change is not acceptable, the receiving entity shall respond with a {CC-SERVICE-REJECT} message.

The {CC-SERVICE-CHANGE} message may specify the master side for activation of the proposed change at the MAC layer. This shall only apply if the change may be initiated from either side, in some cases the choice of master is implicit in the change.

NOTE 2: Service changes that involve modification of an asymmetric MAC connection can only be initiated from one side. In these cases the master side shall be as defined in ETS 300 175-3 [3].

If the master is indicated as "receiving side", the receiving entity shall immediately activate the MAC layer changes after sending the {CC-SERVICE-ACCEPT} message. If the master is indicated as "sending side", the initiating entity shall activate the change immediately after receiving the {CC-SERVICE-ACCEPT} message.

All other changes shall be independently invoked immediately after sending or receiving the {SERVICE-CHANGE-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.

Service change rejection, as indicated by the sending and receipt of a {SERVICE-CHANGE-REJECT} message, shall cause no immediate action at either side. The initiating entity shall issue a MNCC-MODIFY-cfm primitive indicating failure.

9.6.2 Bandwidth changes (including reversals)

Bandwidth changes shall be defined as changes that may be realised by modification of the existing MAC connection or connections. The <<CONNECTION-ATTRIBUTES>> element (or a list of elements) shall always be included to define the new connection bandwidths.

Bandwidth changes may be combined with establishment of new connections and/or rerouting of links by also including the <<CONNECTION-IDENTITY>> element to define the new associations. See also subclause 9.6.3.

The special case of connection reversal shall be identified using the reserved coding. Both the <<CONNECTION-ATTRIBUTES>> element and the <<CONNECTION-IDENTITY>> elements may be included to specify the new connection bandwidths and/or associations. If these elements are omitted, the reversal shall be understood to apply to all relevant connections.

9.6.3 Service rerouting

A {CC-SERVICE-CHANGE} message may alternatively request a rerouting of the DLC U-plane elements. This should only be used for packet services. The <<CONNECTION-IDENTITY>> element shall always be included to indicate the proposed connections.

The old (dis-associated) MAC connection may be released or may be maintained following an agreed rerouting. This decision shall be indicated in the <<SERVICE-CHANGE-INFO>> element. A maintained connection shall be immediately available for reuse, following completion of the service change procedure.

This procedure may be combined with a bandwidth change as described in subclause 9.6.2.

9.6.4 Service suspension and resumption

A {CC-SERVICE-CHANGE} message may alternatively request a suspension or resumption of the DLC U-plane elements. This should only be used for packet services.

The <<CONNECTION-IDENTITY>> element may be omitted for a suspend request, in which case the suspend shall be understood to apply to all relevant U-plane elements.

The <<CONNECTION-IDENTITY>> element shall always be included in a resume request to indicate the proposed connections. The resume request may also include <<CONNECTION-ATTRIBUTES>> elements to request establishment of new connections or modification of existing connections according to the set-up procedures defined in subclause 9.3.1.3. (PT initiated) or subclause 9.3.2.3. (FT initiated). If new connections and/or associations are required as part of the resume, these shall be confirmed in the {CC-SERVICE-ACCEPT} message using the <<CONNECTION-IDENTITY>> element as defined in subclause 9.3.1.3. or 9.3.2.3.

The associated MAC connection may be released or may be maintained following an agreed suspension. This decision shall be indicated in the <<SERVICE-CHANGE-INFO>> element. A maintained connection shall be immediately available for reuse, following completion of the service change procedure.

9.7 Packet mode procedures

9.7.1 General

This Clause describes the use of the CC procedures to offer a packet mode service. This Clause shall apply to CC operations that invoke the LU2 or LU3 service.

The CC service may be accessed in one of two modes:

a) permanent access;

b) demand assigned access.

For permanent access, the resources of all layers remain allocated. For demand assigned access the lower layer resources (MAC and physical layers) may be released during periods of inactivity using the suspend and resume procedures.

9.7.2 PT initiated access

For outgoing data calls, the user shall decide whether a circuit switched or packet switched service is required. If circuit switched access is required (case A) the normal procedures defined in subclause 9.3. shall apply. The <<IWU-ATTRIBUTES>> information element shall be set to "unrestricted digital information" or "restricted digital information" as appropriate.

If packet switched access is required (case B) the procedures defined in this subclause shall apply.

NOTE: The service requested may not be available. The FT will clear a request for unsupported services by sending a {CC-RELEASE-COM} message, with the reason set to "service not implemented".

Packet switched PT initiated access shall use the standard CC procedures with the following exceptions:

a) the procedures for overlap sending shall not apply;

b) the procedures for call proceeding shall not apply;

c) the procedures for call confirmation apply as follows:

- upon accepting the service requested in the {CC-SETUP} message, the FT shall return a {CC-CONNECT} message to the PT and shall enter the "ACTIVE" state;

- the {CC-CONNECT} message shall confirm installation of the requested U-plane entity;

- upon receipt of the {CC-CONNECT} message the PT shall enter the "ACTIVE" state and shall issue a MNCC-CONNECT-ind primitive.

9.7.3 FT initiated access

For incoming data calls, the IWU shall decide whether a circuit switched or packet switched service is required. If circuit switched access is required (case A) the normal procedures defined in subclause 9.3 shall apply. The <<IWU-ATTRIBUTES>> information element shall be set to "unrestricted digital information" or "restricted digital information" as appropriate.

If packet switched access is required (case B) the procedures defined in this subclause shall apply.

NOTE: The requested service may not be available. The PT will clear a request for unsupported services by sending a {CC-RELEASE-COM} message, with the reason set to "service not implemented".

Packet switched FT initiated access shall use the standard CC procedures with the following exceptions:

a) the procedures for overlap receiving shall not apply;

b) the procedures for call alerting may apply, but the receipt of a {CC-ALERTING} message shall not cause the FT to issue a MNCC-ALERT-ind primitive.

9.7.4 Packet mode suspend and resume

9.7.4.1 General

A packet mode call may optionally be suspended. The suspend procedure allows the service attributes to be reserved such that the call can be resumed more rapidly.

The suspend and resume shall use two independent procedures:

- C-plane suspend and resume, under control of the LCE;

- U-plane suspend and resume, under control of the LLME.

These procedures may be invoked independently, once the relevant call is in the "ACTIVE" state.

9.7.4.2 C-plane suspend and resume

The CC entity may request the LCE to suspend a C-plane link at any time after reaching the "ACTIVE" state. No further messages should be submitted for that link as these will invoke an immediate resumption of the link.

NOTE: The DLC suspend and resume procedures are managed by the LCE. In the case of Class A operation, all resources associated with the link shall be released (i.e. suspension is equivalent to release). In the case of Class B operation, all MAC and physical layer resources shall be released, but the DLC C-plane resources shall be preserved. This allows for the link to be restarted with Class B operation.

9.7.4.3 U-plane suspend and resume

U-plane suspend and resume shall use the service change procedures as described in subclause 9.5.3. Any U-plane DLC instance may be suspended, provided that all network layer resources (in particular the CC transaction identifier are preserved. A suspension shall always suspend all of the U-plane resources associated with the indicated CC instance (all resources related to the indicated TI).

Following acceptance of a service change indicating suspension of a service, all of the relevant U-plane resources shall be immediately suspended, all resources shall be preserved and all timers shall be stopped. Any associations to MAC connections shall then be removed.

Following acceptance of a service change indicating resumption of a service, the relevant U-plane resources shall be reassociated to a suitable open MAC connection. The U-plane operations shall then be resumed and all timers shall be restarted (and reset).

NOTE: The state variables of the U-plane link may be reset as part of link resumption.

10 Supplementary Services procedures

10.1 General

This Clause describes the generic procedures for the control of all supplementary services at the user-network interface. The procedures may be used for the invocation and operation of supplementary services as part of either the CC or CISS protocol entities:

a) Call Related Supplementary Services (CRSS); that operate in association with an existing CC call(s), but do not influence the states at either side of the call;

b) Call Independent Supplementary Services (CISS); that operate outside of any CC calls.

Three generic protocols are defined for supplementary services:

	GENERIC NAME	PROTOCOL TYPE
1)	Keypad	Stimulus
2)	Feature key management	Stimulus
3)	Functional	Functional

10.2 Keypad protocol

The keypad protocol is based on the use of the following information elements:

- <<SINGLE-KEYPAD>> } <<"KEYPAD">>
  or <<MULTI-KEYPAD>> }

- <<SINGLE-DISPLAY>> } <<"DISPLAY">>
  or <<MULTI-DISPLAY>> }

The CRSS and CISS uses the generic keypad protocol as follows:

- the PT sends a <<"KEYPAD">> information element to invoke a service. This element contains network dependent access codes;

- the FT sends a <<"DISPLAY">> information element that gives an indication to the PT user about the service.

These elementary steps may be repeated several times, with the FT <<"DISPLAY">> element providing a prompt for the PT user. The semantics of this dialogue are not specified.

The CRSS keypad protocol can be invoked at any phase of the associated CC call. During the establishment phase, a <<"KEYPAD">> element may only be included in the {CC-SETUP} message or a {CC-INFO} message. Subsequent elements shall always be sent in a {CC-INFO} message. A <<"DISPLAY">> element may be included in any CC message in the F=>P direction except {CC-NOTIFY} and {IWU-INFORMATION}.

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 must be agreed in advance, and may either adopt a common set of access codes (specified elsewhere) or may be network dependent.

10.3 Feature key management protocol

The feature key management protocol is based on the use of the following information elements:

- <<FEATURE-ACTIVATE>>

- <<FEATURE-INDICATE>>

These elements may be included in various CC messages or CISS messages, as defined in Clause 6 of this ETS.

The PT may send a <<FEATURE-ACTIVATE>> element at any time. The CRSS uses the generic feature protocol 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.

The <<FEATURE-INDICATE>> element may be included in any CC message or any CISS message in the F=>P direction.

10.4 Functional protocol

Two categories of procedures are defined for the functional signalling for supplementary services. The first category, called the separate message approach, utilises the hold and retrieve set of messages. The second category, called the common information element procedure, utilises the <<FACILITY>> information element and applies only to supplementary services that do not require synchronisation of resources between the user and the network.

10.4.1 Separate messages category

The messages defined in this subclause are specified as separate functional messages for invoking specific functions which require changes of the resources. The following messages are defined:

- {HOLD};
- {HOLD-ACKNOWLEDGE};
- {HOLD-REJECT};
- {RETRIEVE};
- {RETRIEVE-ACKNOWLEDGE};
- {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 by sending the {HOLD} message. It will place the auxiliary state in the "HOLD REQUEST" state. The responding entity will acknowledge this request with a {HOLD-ACKNOWLEDGE} message if this operation was successful. This will result in the auxiliary state being put in the "CALL HELD" state. If 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.

10.4.1.2 Retrieve procedures

The retrieve function is requested 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.

If the "RETRIEVE-REQUEST" is successful, the {RETRIEVE-ACKNOWLEDGE} message will be returned. The auxiliary state would then return to the "IDLE" state.

If the "RETRIEVE REQUEST" is not successful, the {RETRIEVE-REJECT} message will be returned. The auxiliary state would then remain in the "CALL HELD" state.

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 category

The common information element category is based on the use of the information element:

- <<FACILITY>>.

10.4.2.1 Call related procedures

The CRSS uses the generic functional protocol as follows:

- either side (PT or FT) sends a <<FACILITY>> information element to invoke a service;

- the responding side replies by returning the same <<FACILITY>> element. This reply can either accept or reject the service.

If appropriate, either side can respond to a rejection of the service by releasing the CC call, using the procedures defined in Clause 9.

The facility protocol can be invoked at any phase of the associated CC call. During the establishment phase, a <<FACILITY>> element in the P=>F direction may only be included in the {CC-SETUP} message or a {CC-INFO} message. A <<FACILITY>> element in the F=>P direction may be included in any CC message.

10.4.2.2 Call independent procedures

The functional protocol is invoked by either side, 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.

All subsequent exchanges shall use the {FACILITY} message containing a single <<FACILITY>> information element.

All messages in the direction P=>F may include a <<"KEYPAD">> element, to invoke a service.

All messages in the direction F=>P may include a <<"DISPLAY">> element, that provides an indication to the user of the progress of the service.

Each instance of the CISS is released using a single unacknowledged {CISS-RELEASE-COM} message.

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. This is contained in draft ETS T/S 46-32B, and defines the supplementary services which are detailed in the following draft of finalised ETSs. This protocol defines the following services:

- Malicious Call Identification (MCID) (ETS 300 130 [41]);
- Call Forwarding Busy (CFB) (ETSI T/S 46-33R1 [42]);
- Call Forwarding Unconditional (CFU) (ETSI T/S 46-33R3 [43]);
- User to User Signalling (UUS) (ETSI T/S 46-33T [44]);
- Calling Line Identification Presentation (CLIP) (ETS 300 092 [45]);
- Calling Line Identification Restriction (CLIR) (ETS 300 093 [46]);
- COnnected Line identification Presentation (COLP) (ETS 300 097 [47]);
- COnnected Line identification Restriction (COLR) (ETS 300 098 [48]);
- Completion of Calls to Busy Subscriber (CCBS) (ETSI T/S 46-33G [49]);
- FreePHone (FPH) (ETSI T/S 46-33P [50]);
- Advice Of Charge (AOC) (prETS 300 182 [51]);
- SUBaddressing (SUB) (ETS 300 061 [52]);
- Terminal Portability (TP) (ETS 300 055 [53]);
- Call Waiting (CW) (ETS 300 058 [54]);
- Direct Dialling In (DDI) (ETS 300 064 [55]);
- Multiple Subscriber Number (MSN) (ETS 300 052 [56]);
- Closed User Group (CUG) (ETS 300 138 [57]);
- Explicit Call Transfer (ECT) (ETSI T/S 46-33Q1 [58]);
- Single step Call Transfer (SCT) (ETSI T/S 46-33Q2 [59]);
- Call Forwarding No Reply (CFNR) (ETSI T/S 46-33R2 [60]);
- Call Deflection (CD) (ETSI T/S 46-33R4 [61]);
- CONFerence call add-on (CONF) (prETS 300 185 [62]);
- Call Hold (CH) (ETS 300 141 [63]);
- Three ParTY (3PTY) (prETS 300 188 [64]).

NOTE: For the keypad protocol no specific application protocol is identified.

10.6.2 DECT specific supplementary services

For DECT specific supplementary services the feature key management protocol is used.

The following supplementary services are defined:

- queue management;
- indication of subscriber number;
- control of echo control functions;
- cost information.

10.6.2.1 Queue management

This service can be used to register a PP in a queue for outgoing calls, e.g. in the case of a network congestion.

If an outgoing call is requested by a PT by sending a {CC-SETUP} message and no external line is available, then the FT can respond with an allowed CC-message, which can include <<"DISPLAY">> information and/or a <<PROGRESS-INDICATOR>> information element indicating cause no. 8 ("in-band information or appropriate pattern now available") to request the PT to connect the U-plane. Upon receipt of this element, the PT should request its LLME to connect the receive U-plane, so that the user can receive verbal information.

In response to the displayed and/or verbal information about the outgoing call queue, the user can request to enter the queue or release the call.

To enter the queue the PT shall send a <<FEATURE-ACTIVATE>> information element containing a "queue entry request" e.g. in a {CC-INFO} message.

Upon receipt of the "queue entry request" the FT shall respond with a <<FEATURE-INDICATE>> information element e.g. in a {CC-INFO} message to tell if the service request has been accepted and to indicate the position in the queue.

NOTE: The FT might have to send a <<TIMER-RESTART>> with a {CC-NOTIFY} message to avoid that the CC completion timer <CC.04> in the PT expires.

If the queue position changes, then the FT shall send a new <<FEATURE-INDICATE>> information element containing the updated information about the position in the outgoing call queue. The FT can also send display and/or voice information.

The FT may send a <<PROGRESS-INDICATOR>> information element indicating cause No. 9 ("in-band information not available") to inform the PT that the verbal information has concluded. Upon receipt of this element, the PT may disable the received audio (in particular, the speech codec and audio circuits may be disabled) but the U-plane shall remain connected.

The PT may exit the queue at any time by releasing the call.

As soon as the external line is free the FT proceeds with the normal call set up procedure, by giving a dial tone or by sending a {CC-CALL-PROC} message or a {CC-ALERTING} message or a {CC-CONNECT} message, depending on the status of the call.

10.6.2.2 Indication of subscriber number

The subscriber number shall be requested by sending a <<FEATURE-ACTIVATE>> information element with the feature coding "indication of subscriber number".

Upon receipt of the <<FEATURE-ACTIVATE>> information element the FT shall respond with a <<FEATURE-INDICATE>> information element indicating if the service is accepted or rejected. If the service is accepted and activated, then the subscriber number shall be sent in a <<FEATURE-INDICATE>> information element.

10.6.2.3 Control of echo control functions

This service is used to connect or disconnect fixed part echo control functions, depending on e.g. the type of service and call routing information. See also ETS 300 175-8 [8]. This service provides messages to control four FP echo control functions:

Requirement 1 and requirement 2:
(subclause 7.10 of ETS 300 175-8 [8]).

Option a) and option b):
(subclause 7.4.1.2 of ETS 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 mobile or fixed network) to ensure that the effective TCL from the DECT network is always in excess of 46 dB.

The exact echo control function(s) to be used depend upon the type of interface and the type of local network to which DECT is connected. These echo control functions should be disconnected when not needed to optimise the speech quality. The connect/disconnect decision (for each function) depends upon the installation and/or routing information (on a per call basis).

Where possible, all echo control function should be fully controlled by the fixed part and in many cases may be preset at installation. For particular cases (e.g. disconnection of requirement 2 for internal PBX calls) this service allows the PP to over-ride the FP control.

NOTE: All possible PP control options are provided to allow for future developments, but most of these should not be required.

Control of echo functions on a per call basis is expected to use the call routing information. This can be provided by number analysis in the PP or FP. When number analysis is provided in the PP, the messages in subclause 7.7.16 may be used to transfer this information to the FP.

10.6.2.4 Cost information

This service can be used to obtain cost information such as tariffing, charging or charging pulses. It can furnish either DECT specific cost information or cost information for the complete connection including the DECT link.

The cost information shall be requested by sending a <<FEATURE-ACTIVATE>> information element with the feature coding "cost information".

The parameter in the <<FEATURE-ACTIVATE>> information element is used to request either DECT internal cost information or cost information for the complete connection and to choose between tariff information, charging pulses during the call or a calculated amount at the end of the call.

Upon receipt of the <<FEATURE-ACTIVATE>> information element the FT shall respond with a <<FEATURE-INDICATE>> information element indicating if the service is accepted or rejected. If the service is accepted and activated, then the cost information shall be sent in one or more <<FEATURE-INDICATE>> information elements containing charging components.

The support of this feature does not compel any specific tariffing principle.

11 Connection Oriented Message Service (COMS)

11.1 General

The connection oriented message service procedures only deal with packet switched connections. The COMS represents a group of procedures covering all aspects of packet mode call establishment, packet data transfer and release.

The protocol allows for multiple instances of a COMS call at both the fixed termination and at the portable termination. These multiple instances are assumed to operate completely independently from each other. The possible existence of multiple instances is therefore ignored in the following clauses, which only describe the procedures for a single instance.

A reliable C-plane DLC link (LAPC) must be available before any of these COMS procedures can operate. The establishment and maintenance of this link is the responsibility of the LCE and is described in Clause 14.

NOTE: A "LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. If a COMS timer expires whilst in this state, the resulting release should be handled locally.

11.2 COMS states

11.2.1 States at PT

11.2.1.1 State TS-0: "NULL"

No call exists.

11.2.1.2 State TS-1: "CONNECT PENDING"

The PT has sent a set-up message to the FT, but has not received a response.

11.2.1.3 State TS-2: "RELEASE PENDING"

The PT has sent a release message to the FT, but has not received a response.

11.2.1.4 State TS-3: "ACTIVE"

a) The PT has answered an incoming call;

b) the PT has received an indication that the FT has connected a PT outgoing call.

11.2.2 States at FT

11.2.2.1 State FS-0: NULL

No call exists.

11.2.2.2 State FS-1: "CONNECT PENDING"

The FT has sent a set-up message to the PT, but has not received a response.

11.2.2.3 State FS-2: "RELEASE PENDING"

The FT has sent a release message to the PT, but has not received a response.

11.2.2.4 State FS-3: "ACTIVE"

a) The FT has allocated an incoming call to one PT;

b) the FT has sent a message to the PT reporting connection of an outgoing call.

11.3 COMS establishment procedures

11.3.1 PT initiated COMS establishment

11.3.1.1 COMS request

PT initiated COMS establishment is started upon receipt of a MNCO-SETUP-req primitive from the interworking unit at the PT side.

The COMS entity (P-COMS) initiates COMS establishment by sending a {COMS-SETUP} message to its peer entity (F-COMS). This message is submitted to the LCE in the PT, and the P-COMS enters the "CONNECT PENDING" state and starts timer <COMS.03>.

The {COMS-SETUP} message shall carry all details of the interworking attributes such that all the necessary resources can be reserved and installed by the F-COMS and the F-IWU.

Call accept

The F-COMS entity shall examine the attributes defined in the {COMS-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCO-SETUP-ind primitive to the F-IWU. The F-IWU is expected to reply with a MNCO-CONNECT-req primitive, if the call is acceptable.

NOTE: Either the F-COMS or a F-IWU may reject the COMS call. The F-COMS examines the <<CONNECTION-ATTRIBUTES>> element and the F-IWU examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the F-IWU after it has been accepted by the F-COMS.

Call reject

If the F-COMS cannot meet any of the set-up requests, or if the {COMS-SETUP} message contains errors or inconsistencies, or if the F-IWU replies with a MNCO-REJECT-req primitive, the FT shall reject the request by sending a {COMS-RELEASE-COM} message.

Set-up release

If timer <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 <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 <COMS.03>.

The {COMS-SETUP} message should carry all details of the interworking attributes such that all the necessary resources can be reserved and installed by the PT.

Call accept

The P-COMS entity shall examine the attributes defined in the {COMS-SETUP} message and attempt to fulfill them. If it can meet the request, it shall issue a MNCO-SETUP-ind primitive. A MNCO-CONNECT-req primitive will then be received in reply if the call is acceptable.

NOTE: Either the P-COMS or the PP higher layer application may reject the COMS call. The P-COMS examines the <<CONNECTION-ATTRIBUTES>> element and the PP higher layer application examines the <<IWU-ATTRIBUTES>> element. The call is only offered to the PP higher layer application after it has been accepted by the P-COMS.

Call reject

If the P-COMS cannot meet any of the set-up requests, or if the {COMS-SETUP} message contains errors or inconsistencies, or if a MNCO-REJECT-req primitive is received, the P-COMS shall reject the request by sending a {COMS-RELEASE-COM} message.

Set-up release

If timer <COMS.03> expires before a suitable response is received, the F-COMS shall immediately release the call by sending a {COMS-RELEASE-COM} message, with the reason set to "timer expiry". It shall then issue a MNCO-RELEASE-ind primitive to the F-IWU and shall enter the "NULL" state.

11.3.2.2 COMS connection

Upon receiving a MNCO-CONNECT-req primitive, the P-COMS shall complete the C-plane connection and shall send a {COMS-CONNECT} message to the P-COMS. It shall then enter the "ACTIVE" state.

On receipt of this message the F-COMS shall complete the C-plane connection. The F-COMS shall then stop timer <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

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.

NOTE 1: This service shall only support structured service data, using any either the <<ALPHANUMERIC>> or the <<IWU-PACKET>> elements. Unstructured data shall not be supported.

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 2: The maximum information length of a LAPC UI frame is 63 octets. These lower limits are chosen to limit a message to 8 fragments (i.e. the complete UI frame shall be less than 64 octets).

If the service data is segmented, each message shall contain the <<SEGMENTED-INFO>> information element, together with a duplicate of all of the mandatory elements. Each message should contain the maximum amount of service data (of user information).

The COMS shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery via the connection oriented S-SAP (SAPI="0"). The messages shall be delivered using DL-UNITDATA-req primitives, indicating the use of a Class U (unacknowledged) link.

After sending a complete message (of one or more segments) the COMS shall start timer <COMS.01> and shall wait for the final acknowledgement to be received from the peer COMS entity. No further messages shall be submitted until this acknowledgement is received. Upon receipt of this acknowledge, the COMS shall issue a MNCO-ACK-ind primitive to the IWU to indicate successful delivery.

If timer <COMS.01> expires the COMS shall resubmit the complete message starting from the first segment. Timer <COMS.01> shall be restarted after transmission of the complete message. If timer <COMS.01> expires a second time the service shall be released using the procedures defined in subclause 11.6.

11.4.2 Procedure at the receiving side

Upon receipt of a {COMS-INFO} message, the COMS shall check the contained address. If the address does not match any of the PT identities the message shall be discarded. If the address is valid, the COMS shall:

a) if the message does not contain the <<SEGMENTED-INFO>> information element it shall map the elements into the parameters of a MNCO-INFO-ind primitive. It shall immediately issue the resulting primitive via the MNCO-SAP;

b) if the message does contain the <<SEGMENTED-INFO>> element the COMS shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <COMS.00> seconds. Whenever a new segmented message is received, the COMS shall attempt to construct a complete message using all stored segmented messages that contain the same <<SHORT-ADDRESS>> and <<PROTOCOL-DISCRIMINATOR>> element coding. Any duplicate segmented messages should be discarded.

A complete message shall be identified by the receipt of all of the segments as indicated in the <<SEGMENTED-INFO>> elements. Upon detection of a complete series of segments, the COMS shall map the elements into the parameters of a MNCO-INFO-ind primitive. Duplicate mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<ALPHANUMERIC>> and/or <<IWU-PACKET>> elements shall be concatenated into a single message unit parameter. The COMS shall immediately issue the resulting primitive via the MNCO-SAP.

NOTE: The <<SEGMENTED-INFO>> element in each segmented message indicates the total number of segments belonging to the complete message, plus the number of segments remaining. The latter field should be used to sequence the segments.

Upon issuing the complete message to the IWU, the COMS shall immediately return a {COMS-ACK} message to its peer entity using the same Class U link as used for {COMS-INFO} messages.

11.5 COMS suspend and resume procedures

A COMS call may optionally be suspended. The suspend procedure allows the service attributes to be reserved such that the call can be resumed more rapidly.

The suspend and resume shall use the standard C-plane suspend and resume procedure under control of the LCE. See subclause 14.2.6.

The COMS entity may request the LCE to suspend a C-plane link at any time after reaching the "ACTIVE" state. No further messages should be submitted for that link as these will invoke an immediate resumption of the link.

> NOTE: The DLC suspend and resume procedures are managed by the LCE. In the case of Class A operation, all resources associated with the link shall be released (i.e. suspension is equivalent to release). In the case of Class B operation, all MAC and physical layer resources shall be released, but the DLC C-plane resources shall be preserved. This allows for the link to be restarted with Class B operation.

The COMS service can be resumed by either side by submitting a new {COMS-INFO} message to the LCE. This resumption may use any suitable link.

A suspended COMS entity may be discarded without notification to the sender. Any subsequent resumption messages shall then be discarded without notification to the sender. A COMS entity may also be replaced with a new (re-established) COMS entity at any time (i.e. a COMS set-up that uses the transaction identifier of an existing entity) shall always take priority and shall over-write the existing values.

11.6 COMS release procedures

11.6.1 Normal COMS release

The COMS release procedures may be started by the COMS entity at either side at any time, upon receipt of a MNCO-RELEASE-req primitive. The starting entity sends a {COMS-RELEASE} message, starts timer <COMS.02>, and enters the "RELEASE PENDING" state. The release message may include an information element giving the reason for the release: if no reason is given "normal" release should be assumed.

Upon receipt of the {COMS-RELEASE} message, the accepting side shall immediately release all resources associated with the call. It then confirms completion of the release by sending a {COMS-RELEASE-COM} message, enters the "NULL" state, and issues a MNCO-RELEASE-ind primitive. The initiating side must wait for receipt of this {COMS-RELEASE-COM} message before it too can release all resources, stop timer <COMS.02>, and enter the "NULL" state. The initiating side shall then issue a MNCO-RELEASE-cfm primitive, indicating a normal (acknowledged) release. Both sides shall also record the release of the call in their respective LCEs.

If timer <COMS.02> expires before the receipt of a {COMS-RELEASE-COM} message, the initiating side shall release all resources, shall report the call as released to the LCE, and shall issue a MNCO-RELEASE-ind primitive indicating an abnormal time-out release.

11.6.2 Release collisions

A release collision occurs when both sides of a call issue a {COMS-RELEASE} message at the same time, such that at least one of these messages is received by a COMS entity that is already in the "RELEASE PENDING" state.

If either COMS entity receives a {COMS-RELEASE} message, while in the "RELEASE PENDING" state the normal release procedure is not followed by that COMS entity. In this event, the COMS entity immediately releases all the COMS resources, reports this release to the LCE and issues a MNCO-RELEASE-ind primitive indicating abnormal release.

12 ConnectionLess Message Service (CLMS)

12.1 General

The ConnectionLess Message Service procedures offer a connectionless packet service. The CLMS shall provide generic message formats that enable a single packet of differing types of user data to be transported. A single CLMS entity may handle messages from multiple applications.

All messages shall be handled sequentially, in the order of arrival, by a single CLMS entity. Each message shall be handled independently of all other messages. The following subclauses shall describe the procedures for the transmission and reception of one message.

There are two types of CLMS messages:

1) fixed length messages;

2) variable length messages.

Fixed length messages shall be routed via the broadcast service (B-SAP), and these messages shall conform to the fixed length operation specified for this service.

Variable length messages shall be routed via the LAPC services (S-SAP) where they may be routed via a connection oriented link (SAPI="0") or a connectionless link (SAPI="3"). In both cases unacknowledged link operation shall be used.

A connection oriented link shall only be used if a suitable link is already established. Otherwise a connectionless link should be used. The choice of link, and the establishment of these links is the responsibility of the LCE and is described in Clause 14.

NOTE: "LINK PENDING" state is included in the LCE definition which is used while the LCE is waiting for DLC link establishment to complete. A link in this state shall not be used for the transport of CLMS messages.

12.2 CLMS states

No states shall be defined for the CLMS entity, the CLMS shall always be ready to transmit or receive a message.

12.3 CLMS message transmission procedures

12.3.1 Fixed length messages

Fixed length CLMS messages shall use the B-FORMAT message structure.

12.3.1.1 Procedure in the Fixed radio Termination (FT)

Upon receipt of a MNCL-UNITDATA-req primitive indicating fixed length operation, the CLMS shall attempt to map the parameters into {CLMS-FIXED} message elements, using one or more message sections as appropriate. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

The CLMS shall only insert <<FILL>> elements into the final message section in order to fill that final section.

NOTE 1: The total message length is limited by the maximum number of data sections, as defined in subclause 8.3.

NOTE 2: If the data completely fills the last data sections, no <<FILL>> element shall be 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.

12.3.2.1 Procedure at the sending side

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.

NOTE 1: This service shall only support octet structured service data, using any one of the defined information elements. Unstructured data shall not be supported.

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 2: The maximum information length of a LAPC UI frame is 63 octets. These lower limits are chosen to limit a message to 8 fragments (i.e. the complete UI frame shall be less than 64 octets).

If the service data is segmented, each message shall contain the <<SEGMENTED-INFO>> information element, together with a duplicate of all of the mandatory elements. Each message should contain the maximum amount of service data (of user information).

The CLMS shall then deliver the resulting message (or series of messages) in sequence to the LCE for immediate delivery via the S-SAP.

12.3.2.2 Procedure at the receiving side

Upon receipt of a {CLMS-VARIABLE} message, the CLMS shall check the contained address. If the address does not match the message shall be discarded. If the address does match the CLMS shall:

a) if the message does not contain the <<SEGMENTED-INFO>> information element it shall map the elements into the parameters of a MNCL-UNITDATA-ind primitive. It shall immediately issue the resulting primitive via the MNCL-SAP;

b) if the message does contain the <<SEGMENTED-INFO>> element the CLMS shall store (buffer) the complete message. Each (segmented) message shall be stored for a maximum of <CLMS-00> seconds. Whenever a new segmented message is received, the CLMS shall attempt to construct a complete message using all stored segmented messages that contain the same

<<SHORT-ADDRESS>> and <<PROTOCOL-DISCRIMINATOR> element coding. Any duplicate segmented messages may be discarded.

A complete message shall be identified by the receipt of all of the segments as indicated in the <<SEGMENTED-INFO>> elements. Upon detection of a complete series of segments, the CLMS shall map the elements into the parameters of a MNCL-UNITDATA-ind primitive. Duplicate mandatory elements and all <<SEGMENTED-INFO>> elements shall be discarded, and the individual <<ALPHANUMERIC>>, <<IWU-TO-IWU>> or <<IWU-PACKET>> information elements shall be concatenated into a single message unit parameter. The CLMS shall immediately issue the resulting primitive via the MNCL-SAP.

NOTE: The <<SEGMENTED-INFO>> element in each segmented message indicates the total number of segments belonging to the complete message, plus the number of segments remaining. The latter field should be used to sequence the segments.

12.3.2.3 Restrictions for portable side initiated messages

CLMS messages initiated from the portable side are subject to the special transmission restrictions given in ETS 300 175-3 [3] when using connectionless MAC services. These restrictions introduce extra delays for messages in excess of two segments.

13 Mobility Management (MM) procedures

13.1 General

This Clause describes the procedures used for mobility management at the radio interface.

The main function of the Mobility Management (MM) is to support the mobility of portable parts, such as informing the network of its present location and providing user identity confidentiality.

The MM procedures are described in seven groups:

- identity procedures;
- authentication procedures;
- location procedures;
- access rights procedures;
- key allocation procedure;
- parameter retrieval procedure;
- ciphering related procedure.

Each of these procedures shall be treated as a separate transaction, with a single transaction identifier used for the whole procedure. The transaction identifier is assigned by the entity that initiates the procedure (the entity that sends the first message).

Two MM procedures are allowed at any one time, but they shall not both have been initiated by the same side. This limitation is enforced by the transaction identifiers, which allow only one value to be assigned by each side.

The priorities of the MM procedures are defined in subclause 15.5 which describes the management of MM procedures.

13.2 Identity procedures

The identity procedures can be used:

- to request a PT to provide specific identification parameters to the FT;
- to assign a temporary portable user identity to a PT;
- to delete a temporary portable user identity in a PT;
- to assign a network assigned identity to a PT;
- to delete a network assigned identity in a PT.

The identity procedures are initiated by the FT and can be used any time.

13.2.1 Procedure for identification of PT

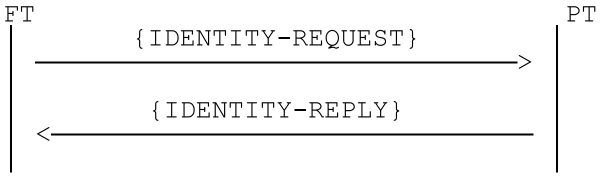
The identification procedure is used by the FT to request a PT to provide specific identification parameters to the FT e.g. the international portable user identity or the international portable equipment identity.

Upon receiving a MM-IDENTITY-req primitive the FT initiates the identification procedure by transferring an {IDENTITY-REQUEST} message to the PT and starts the timer <MM_ident.2>. The {IDENTITY-REQUEST} message specifies the type of the requested identity in the <<IDENTITY-TYPE>> information element. Optionally more than one <<IDENTITY-TYPE>> information element can be included by using the <<REPEAT-INDICATOR>> information element. Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {IDENTITY-REQUEST} message the PT issues a MM-IDENTITY-ind primitive and sends back an {IDENTITY-REPLY} message which contains the identification parameters as requested by the FT. If more than one identity has been requested and not all of them can be provided, then the available ones shall be included in the {IDENTITY-REPLY} message. If none of the requested identification parameters can be provided, then the {IDENTITY-REPLY} message will contain no identification information. Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {IDENTITY-REPLY} message the FT shall stop the timer <MM_ident.2>. The FT issues a MM-IDENTITY-cfm primitive.

The identification procedure is supervised by the timer <MM_ident.2> in the FT. At the first expiry of timer <MM_ident.2> the FT should retransmit the {IDENTITY-REQUEST} message. If the timer <MM_ident.2> expires a second time the FT shall abort the procedure and release the transaction.



NOTE: An {IDENTITY-REPLY} message without any information elements has the function of an identity reject.

13.2.2 Procedure for temporary identity assignment

Upon receiving a MM-IDENTITY-ASSIGN-req primitive the FT initiates the procedure by sending a {TEMPORARY-IDENTITY-ASSIGN} message to the PT or by implicitly incorporating a new TPUI and/or network assigned identity in a {LOCATE-ACCEPT} message. The FT starts the timer <MM_ident.1>.

The {TEMPORARY-IDENTITY-ASSIGN} message contains 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-

contain a defined time limit and/or a lock limit for the newly assigned TPUI. It may also contain an optional <<IWU-TO-IWU>> information element. If the <<DURATION>> element is omitted, the default values of "infinite" time limit and "no limits" lock limit shall be assumed.

NOTE 1: The detailed coding of the <<DURATION>> element appears in subclause 7.7.13. Refer also to ETS 300 175-6 [6] for details of the application of time limits and lock limits to assigned TPUIs.

Upon receipt of a new TPUI and/or network assigned identity the PT shall react in the following way:

If the PT has the capability of storing the received identities, then the PT shall consider the received identities as valid, store them and send a {TEMPORARY-IDENTITY-ASSIGN-ACKNOWLEDGE} message to the FT. If an individual TPUI has been received, then any previously assigned individual TPUI (for the relevant location area) shall be replaced by the new one. If a network assigned identity has been received, then an earlier stored NWK assigned identity shall be replaced by the new one.

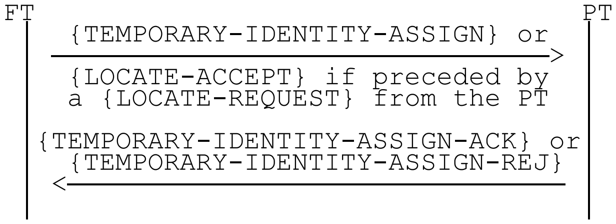
If the PT does not have the capability of storing all the received identities, or if the PT is unable to support any of the limits indicated in the <<DURATION>> element, then the PT shall not store any received identity and send a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message to the FT. The {TEMPORARY-IDENTITY-ASSIGN-REJECT} message can optionally contain the <<REJECT-REASON>> information element.

If a <<DURATION>> information element with the value "Erase" is contained in the received {TEMPORARY-IDENTITY-ASSIGN} message, or if the message contains a <<DURATION>> element that cannot be understood, then the PT shall erase the indicated identities and send a {TEMPORARY-IDENTITY-ASSIGN-ACKNOWLEDGE} message to the FT. If the PT has no record of the indicated identity (i.e. it is already erased) it shall nonetheless respond with a {TEMPORARY-IDENTITY-ASSIGN-ACKNOWLEDGE} message.

Upon receipt of a {TEMPORARY-IDENTITY-ASSIGN-ACKNOWLEDGE} message or a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message the FT shall stop the timer <MM_ident.1>. If a {TEMPORARY-IDENTITY-ASSIGN-ACKNOWLEDGE} message has been received the FT shall consider the assignment (or erasure) as successful. If a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message is received the FT shall consider the procedure to have failed. The FT shall issue 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 retransmit 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 shall then issue a MM-IDENTITY-ASSIGN-cfm primitive indicating failure of the procedure.


FT
PT
{TEMPORARY-IDENTITY-ASSIGN} or
{LOCATE-ACCEPT} if preceded by a {LOCATE-REQUEST} from the PT
{TEMPORARY-IDENTITY-ASSIGN-ACK} or {TEMPORARY-IDENTITY-ASSIGN-REJ}

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 can be initiated by the FT either when the PT requests for a call set-up or when there is an incoming call to the PT. Authentication can also be challenged during a call (in-call authentication).

Procedure for authenticating a PT:

Upon receiving a MM-AUTHENTICATE-req primitive the FT sends an {AUTHENTICATION-REQUEST} message which contains the <<AUTH-TYPE>> information element (defining the chosen authentication type and authentication key) and the <<RAND>> and <<RS>> information elements (two numbers necessary for calculating the response parameter). The <<RS>> information element is only mandatory, when a DECT standard authentication algorithm is used, for other algorithms it can be optional. The INC bit in the <<AUTH-TYPE>> information element can be used to ask the PT to increase its ZAP-register. The {AUTHENTICATION-REQUEST} message can also contain the optional <<CIPHER-INFO>> information element and an optional <<IWU-TO-IWU>> information element. The timer <MM_auth.1> is started.

Upon receipt of the {AUTHENTICATION-REQUEST} message the PT shall increment the relevant ZAP field, 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 PT should authenticate the FT. If the authentication of the FT fails, the PT may not increment the ZAP field. The PT issues a MM-AUTHENTICATE-ind primitive.

NOTE 1: A ZAP field is always related to one IPUI (subscription), as also an authentication key is always related to one IPUI. Therefore several ZAP fields can exist in the PT. In this procedure the relevant ZAP field is that, which is related to the same IPUI as the used authentication key.

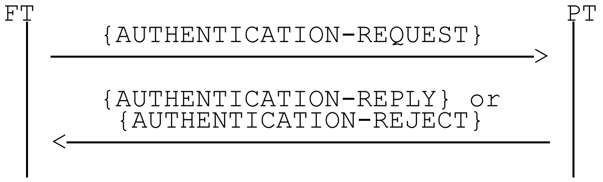
Upon receiving a MM-AUTHENTICATE-res primitive indicating "accept" the PT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result. If the PT has stored a ZAP field that is related to the current active IPUI, than also the <<ZAP-FIELD>> information element with the relevant ZAP value shall be included. If the PT has stored a "service class" that is related to the current active IPUI, then also the <<SERVICE-CLASS>> information element shall be included. If in the {AUTHENTICATION-REQUEST} message the TXC bit in the <<AUTH-TYPE>> information element was set, then the derived cipher key shall be sent using the <<KEY>> information element. An optional <<IWU-TO-IWU>> information element can also be included in the {AUTHENTICATION-REPLY} message. Upon receiving a MM-AUTHENTICATE-res primitive indicating "reject" the PT shall respond by sending an {AUTHENTICATION-REJECT} message containing the optional <<REJECT-REASON>> information element and one of a prioritised list of the optional <<AUTH-TYPE>> information element to propose an alternative algorithm or key.

NOTE 2: The FT shall only request to send a derived cipher key (e.g. for GSM) when the DECT link is already ciphered.

Upon receipt of the {AUTHENTICATION-REPLY} message or the {AUTHENTICATION-REJECT} message the FT shall stop the timer <MM_auth.1> and check the validity of the response. If the FT has received an {AUTHENTICATION-REPLY} message, where the <<RES>> information element contains the correct result the FT shall consider the PT authentication as successful. If the FT has received an {AUTHENTICATION-REPLY} message where the <<RES>> information element contains the wrong result, then in cases where the Temporary Portable User Identity (TPUI) has been used the FT may decide to initiate the identity procedure. In any case the FT may optionally communicate the failed authentication to the PT in a subsequent network layer message, using a <<RELEASE-REASON>> or <<REJECT-REASON>> information element. The FT issues a MM-AUTHENTICATE-cfm primitive.

If a DECT standard authentication algorithm is used, then together with the authentication result a new ciphering key is calculated. If in this case the UPC-bit in the <<AUTH-TYPE>> information element is set, this new ciphering key shall be stored and shall be given the cipher key number as indicated in the <<AUTH-TYPE>> information element.

The procedure for authenticating a PT is supervised by the timer <MM_auth.1> in the FT. At the first expiry of timer <MM_auth.1> the FT should retransmit the {AUTHENTICATION-REQUEST} message. If the timer <MM_auth.1> expires a second time the FT shall abort the procedure and release the transaction.



13.3.2 Authentication of the user

The authentication of the user is combined with the authentication of a PT. Therefore the information elements and messages are the same as in subclause 13.3.1 above. The only difference is that in the <<AUTH-TYPE>> information element the use of a different key is indicated. In this case part of the key is added by the user via the keypad. This keypad entry is not transmitted over the air, but locally used by the PT to calculate the authentication key, K.

The procedure is equivalent to that one described in subclause 13.3.1 above. The timer that is used by the FT is called <MM_auth.2>, which has a longer period in order to enable the user to enter the User Personal Identity (UPI).

If user authentication procedure is started during an unfinished PT initiated procedure of lower priority, then the PT shall stop the timer of the unfinished lower priority procedure and start the <MM_auth.2> timer. The

PT shall stop the <MM_auth.2> timer when it responds to the user authentication procedure by sending an {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message. If the <MM_auth.2> timer expires or is stopped and the lower priority procedure has not been finished in the meantime, then the timer of the interrupted lower priority procedure shall be restarted.

13.3.3 Authentication of a FT

This authentication procedure is activated by the PT, typically when the FT is sending a ZAP-command.

Procedure for authenticating a FT:

Upon receiving a MM-AUTHENTICATE-req primitive the PT sends an {AUTHENTICATION-REQUEST} message which contains the <<AUTH-TYPE>> information element (defining the chosen authentication type) and the <<RAND>> information elements (a random number necessary for calculating the response parameter). It can also contain the optional <<CIPHER INFO>> information element and an optional <<IWU-TO-IWU>> information element. The timer <MM_auth.1> is started.

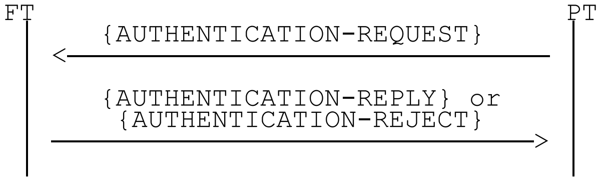
NOTE 1: The <<RES>> information element is only included when the {AUTHENTICATION-REQUEST} message is used for the key allocation procedure.

Upon receiving a MM-AUTHENTICATE-res primitive indicating "accept" the FT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result and the <<RS>> information element with a number necessary for calculating the response parameter. The <<RS>> information element is only mandatory when a DECT standard authentication algorithm is used, for other algorithms it can be optional. An optional <<IWU-TO-IWU>> information element can also be included in the {AUTHENTICATION-REPLY} message. Upon receiving a MM-AUTHENTICATE-res primitive indicating "reject" the FT shall respond by sending an {AUTHENTICATION-REJECT} message containing one or a prioritised list of the optional <<AUTH-TYPE>> information element to propose an alternative algorithm or key and an optional <<REJECT-REASON>> information element.

Upon receipt of the {AUTHENTICATION-REPLY} message or the {AUTHENTICATION-REJECT} message the PT shall stop the timer <MM_auth.1> and check the validity of the response. 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. The PT issues a MM-AUTHENTICATE-cfm primitive.

NOTE 2: A cipher key should not be generated during FT authentication. If generated, it shall not be used.

The procedure for authenticating a FT is supervised by the timer <MM_auth.1> in the PT. At the first expiry of timer <MM_auth.1> the PT should retransmit the {AUTHENTICATION-REQUEST} message. If the timer <MM_auth.1> expires a second time the PT shall abort the procedure and release the transaction.



NOTE 3: The procedure for authenticating a FT has the highest priority under the MM procedures and can therefore always be initiated. It restarts the MM timer in the FT of any FT initiated and yet unfinished MM procedure. See also subclause 15.5.

13.4 Location procedures

Three location related procedures are defined, location registration (attach), detach and location update.

13.4.1 Location registration

The location registration procedure is used to indicate to the FT where the PT is located in terms of location areas, where a location area consists of part of one or several DECT systems.

The location registration procedure is based on the International Portable User Identity (IPUI) and is only carried out with respect to the IPUI that is active at the time. The location information that has been stored in association with inactive IPUIs is not effected.

NOTE 1: Instead of the IPUI also, the individual assigned TPUI plus the identity of the old location area can be used.

The location registration procedure can only be initiated by the PT and it can be used when the present obtained location area is different from the stored one. The location area level identifies the part of the radio fixed part identity that is relevant for this location area.

NOTE 2: Within the same system the location area level has to be the same for the same IPUI.

NOTE 3: Location registration without changing the location area is referred to as attach, which is the process whereby a PT informs the FT that it is ready to receive incoming calls. Therefore the procedure for attach is the same as described in this subclause.

The location registration procedure is used as follows:

Upon receiving a MM-LOCATE-req primitive the PT sends a {LOCATE-REQUEST} message containing a <<PORTABLE-IDENTITY>> information element with its IPUI or a <<PORTABLE-IDENTITY>> information element with its individual assigned TPUI. 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 got Extended Location Information (ELI), then this shall also be included in the <<LOCATION-AREA>> information element (as LI-Type 11). If the PT has got 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.

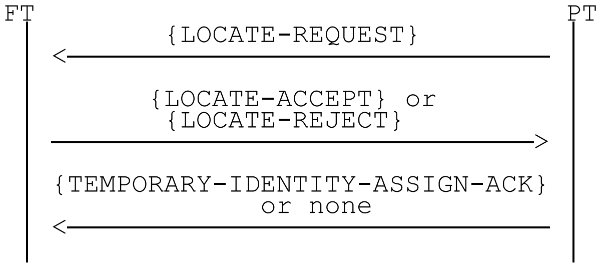
Upon receiving a {LOCATE-REQUEST} message the FT issues a MM-LOCATE-ind primitive. Upon receiving a MM-LOCATE-res primitive indicating "accept" the FT shall respond with a {LOCATE-ACCEPT} message containing the <<LOCATION-AREA>> information element with the location area level, an optional <<PORTABLE-IDENTITY>> information element with a new assigned individual TPUI of the PT and/or an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity. The message can also contain an optional <<DURATION>> information element, which may define for how long at least the location registration and the temporary identities, if provided, are valid. Optionally an <<IWU-TO-IWU>> information element can also be included in the {LOCATE-ACCEPT} message. If a TPUI or NWK assigned identity is included, then the {LOCATE-ACCEPT} message is used to start the procedure for temporary identity assignment as described in subclause 13.2.2. 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 PT 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 PT shall consider this as a temporary identity assignment, and shall respond according to the identity assignment criteria defined in subclause 13.2.2. If it can accept the assignment, it shall store the identities and send back a {TEMPORARY-IDENTITY-ASSIGN-ACKNOLWEDGE} message to the FT as described in subclause 13.2.2. If it cannot accept the assignment, it shall send back a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message as described in subclause 13.2.2.

NOTE 4: The complete location registration procedure shall be treated as a single transaction, even when it includes an identity assignment.

If a {LOCATE-REJECT} message has been received containing a <<DURATION>> information element, then the PT shall not initiate this procedure within this location area again before the defined time has passed. If the <<DURATION>> element indicates "Standard time limit" or cannot be understood, the PT shall wait a minimum of <MM_wait> minutes. The time starts with the reception of the {LOCATE-REJECT} message.

The location registration procedure is supervised by the timer <MM_locate.1> in the PT. At the first expiry of timer <MM_locate.1> the PT should retransmit the {LOCATE-REQUEST} message. If the timer <MM_locate.1> expires a second time the PT shall abort the procedure and release the transaction.



NOTE 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

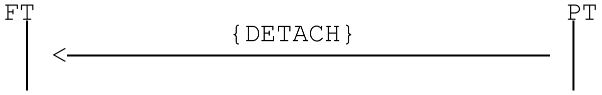
Detach is the process whereby a PT informs the FT that it is not ready to receive incoming calls.

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 subclause 13.4.1 for location registration.

The detach procedure is used as follows:

Upon receiving a MM-DETACH-req primitive the PT sends a {DETACH} message, containing the <<PORTABLE-IDENTITY>> information element with its IPUI or individual assigned TPUI. If the PT has got a network assigned identity, then this identity shall also be included, using a <<NWK-ASSIGNED-IDENTITY>> information element. Optionally an <<IWU-TO-IWU>> information element can also be included.

Upon receiving a {DETACH} message the FT issues a MM-DETACH-ind primitive.



NOTE 2: This message should have been preceded by a {LOCATE-REQUEST} message.

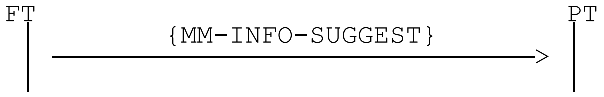
13.4.3 Location update

Location update is used by the FT to inform the PT of a modification of the location areas.

The location update procedure is used as follows:

Upon receiving a MM-INFO-req primitive the FT sends a {MM-INFO-SUGGEST} message, which contains an <<INFO-TYPE>> information element with the parameter type "locate suggest". Optionally an <<IWU-TO-IWU>> information element can be included.

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues a MM-INFO-ind primitive. If the parameter type "locate suggest" is indicated in the <<INFO-TYPE>> information element, the PT shall initiate the location registration procedure as described in subclause 13.4.1.



13.5 Access rights procedure

13.5.1 Obtaining the access rights

The procedure for obtaining the access rights is used to load the International Portable User Identity (IPUI), the Portable Access Rights Key (PARK) and other service specific information into the PT.

The PT can then use the knowledge to:

- gain access to the system and make calls;

- recognise the system in order to receive calls.

The FT can then use the knowledge to:

- validate service requests from the PT; and

- allow certain classes of service;

- recognise calls for valid PTs in order to route calls to them.

If the access rights procedure is not supported by the FT, as indicated in the broadcast attributes and as defined in Annex F, than the PT shall not initiate this procedure.

Procedure for obtaining the access rights:

Upon receiving a MM-ACCESS-RIGHTS-req primitive the PT initiates the procedure by sending an {ACCESS-RIGHTS-REQUEST} message and starts the timer <MM_access.1>. The {ACCESS-RIGHTS-REQUEST} message contains a <<PORTABLE-IDENTITY>> information element with an international portable user identity, e.g. IPUI type N with the portable's equipment number. The message can also contain an optional <<AUTH-TYPE>> information element, an optional <<CIPHER-INFO>> information element, an optional <<TERMINAL-CAPABILITY>> information element and an optional <<IWU-TO-IWU>> information element.

Upon receiving a {ACCESS-RIGHTS-REQUEST} message the FT issues a MM-ACCESS-RIGHTS-ind primitive. Upon receiving a MM-ACCESS-RIGHTS-res primitive indicating "accept" the FT shall respond by sending an {ACCESS-RIGHTS-ACCEPT} message containing a <<PORTABLE-IDENTITY>> information element with an international portable user identity and an <<FIXED-IDENTITY>> information element with the portable access rights key. Optionally a list of <<FIXED-IDENTITY>> information elements with further portable access rights keys can be included. Further optional information elements are the <<LOCATION-AREA>> information element with the location area level, the <<AUTH-TYPE>> information element which indicates the authentication algorithm and key, the <<CIPHER-INFO>> information element which indicates the cipher algorithm, the <<ZAP-FIELD>> information element with the ZAP value, the <<SERVICE-CLASS>> information element which defines the allowed service, and key and the <<IWU-TO-IWU>> information element with operator specific information.

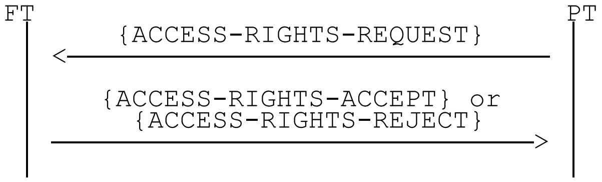
NOTE: For sending the user authentication key over the air the key allocation procedure can be used. That procedure needs a first key e.g. an authentication code which could be keyed in.

Upon receiving a MM-ACCESS-RIGHTS-res primitive indicating "reject" the FT shall respond by sending an {ACCESS-RIGHTS-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receipt of the {ACCESS-RIGHTS-ACCEPT} message or the {ACCESS-RIGHTS-REJECT} message the PT shall stop the timer <MM_access.1>. The PT issues a MM-ACCESS-RIGHTS-cfm primitive. If an {ACCESS-RIGHTS-ACCEPT} message has been received the PT shall store the received information.

If an {ACCESS-RIGHTS-REJECT} message has been received containing a <<DURATION>> information element, then the PT shall not initiate this procedure within this location area again before the defined time has passed. If the <<DURATION>> element cannot be understood or indicates "standard time limit" the PT shall wait a minimum of <MM_wait> minutes. The time starts with the reception of the {ACCESS-RIGHTS-REJECT} message.

The procedure for obtaining access rights is supervised by the timer <MM_access.1> in the PT. At the first expiry of timer <MM_access.1> the PT should retransmit the {ACCESS-RIGHTS-REQUEST} message. If the timer <MM_access.1> expires a second time the PT shall abort the procedure and release the transaction.



13.5.2 Termination of access rights

The procedure for terminating the access rights is used to remove a specific International Portable User Identity (IPUI) and all information which is related to this IPUI from the PT and FT.

The PT is then unable to:

- gain access to the system and make calls;

- recognise the system in order to receive calls.

The FT is then unable to:

- validate service requests from the PT and allow certain classes of service;

- recognise calls for valid PTs in order to route calls to them.

Procedure for terminating access rights initiated by the PT:

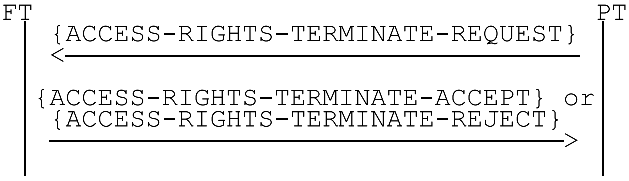
Upon receiving a MM-ACCESS-RIGHTS-TERMINATE-req primitive the PT initiates the procedure by sending an {ACCESS-RIGHTS-TERMINATE-REQUEST} message containing the <<PORTABLE-IDENTITY>> information element with the IPUI. The message can also contain an optional <<FIXED-IDENTITY>> information element with a portable access rights key and an optional <<IWU-TO-IWU>> information element. The timer <MM_access.2> is started.

Upon receipt of an {ACCESS-RIGHTS-TERMINATE-REQUEST} message the FT issues a MM-ACCESS-RIGHTS-TERMINATE-ind primitive. The FT should authenticate the PT. 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 erase the data as requested and 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 PT, that the former {ACCESS-RIGHTS-TERMINATE-REQUEST} message requested to be deleted in the FT.

If an {ACCESS-RIGHTS-TERMINATE-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 {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.


FT
PT
{ACCESS-RIGHTS-TERMINATE-REQUEST}
{ACCESS-RIGHTS-TERMINATE-ACCEPT} or
{ACCESS-RIGHTS-TERMINATE-REJECT}

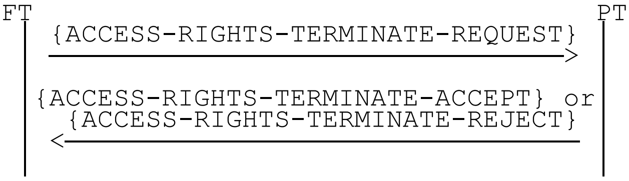
Procedure for termination of access rights initiated by the FT:

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 PT should authenticate the FT. If the authentication of the FT fails, then the PT should send an {ACCESS-RIGHTS-TERMINATE-REJECT} message containing the optional <<REJECT-REASON>> information element. Otherwise the PT 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 back an {ACCESS-RIGHTS-TERMINATE-ACCEPT} message.

Upon receipt of the {ACCESS-RIGHTS-TERMINATE-ACCEPT} message or the {ACCESS-RIGHTS-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.


FT
PT
{ACCESS-RIGHTS-TERMINATE-REQUEST}
{ACCESS-RIGHTS-TERMINATE-ACCEPT} or
{ACCESS-RIGHTS-TERMINATE-REJECT}

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 <<ALLOCATE-TYPE>> information element which indicates the authentication algorithm, the number of the used authentication code and the number which shall be given to the allocated user authentication key. The message shall also contain the <<RAND>> information element with the 64-bit random number RAND-F and the <<RS>> information element with the 64-bit number RS. The timer <MM_key.1> is started.

NOTE 1: The authentication code which is used in this procedure should be as long as possible, at least 32 bits, but better if 64 bits or more are used.

Upon receipt of the {KEY-ALLOCATE} message the PT issues a MM-KEY-ALLOCATE-ind primitive. The PT shall use the indicated authentication code and the received numbers RS and RAND-F to calculate the authentication result RES1. The PT shall respond by sending an {AUTHENTICATION-REQUEST} message including the <<AUTH-TYPE>> information element, with the same parameters (algorithm, type AC, 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. The timer <MM_auth.1> is started.

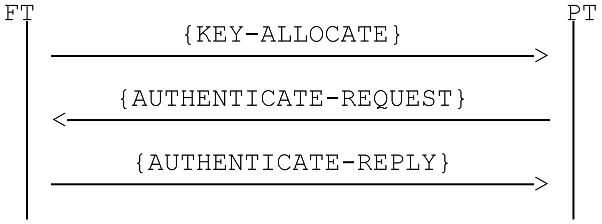
Upon receipt of the {AUTHENTICATION-REQUEST} message the FT shall stop the timer <MM_key.1> and use the received random number to calculate the authentication result RES2. The FT shall respond by sending an {AUTHENTICATION-REPLY} message which contains the <<RES>> information element with the calculated result RES2.

Upon receipt of the {AUTHENTICATION-REPLY} message the PT shall stop the timer <MM_auth.1> and check the received result RES2. If the received value is the correct one, then the PT shall store the reverse session authentication key KS' as new user authentication key under the UAK-number which was given in the <<ALLOCATE-TYPE>> information element in the {KEY-ALLOCATE} message and erase the used Authentication Code, AC.

NOTE 2: The reverse Session authentication Key KS' is an intermediate result during the calculation of RES2. Refer also to ETS 300 175-7 [7].

The FT shall also store the assigned user authentication key, but also keep the Authentication Code (AC) until the next successful PT authentication is performed, using the assigned UAK. Then also the FT shall erase the AC.

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 retransmit 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.



This procedure shall not be used for roaming key allocation in a visited network.

NOTE 3: A possibility for roaming key allocation is that the visited system obtains a Session Key KS with the corresponding value RS from the home system. It can then use this session key for the authentication procedures whereas the PT can use its standard user authentication key together with RS and RAND to calculate the authentication result as normal. Refer also to ETS 300 175-7 [7].

13.7 Parameter retrieval procedure

This procedure is used to exchange information between the FT and the PT. This information could be necessary for an external handover, where after having obtained this information the actual handover is done by the interworking unit via the call control entity and is not described in this subclause.

The procedure can be initiated by the FT or by the PT.

Procedure for parameter retrieval initiated by the FT:

Upon receiving a MM-INFO-req primitive the FT initiates the procedure by sending a {MM-INFO-SUGGEST} message. This message contains the <<INFO-TYPE>> information element which defines the suggested action. The coding "locate suggest" is used in the case of the location updating procedure which is described in subclause 13.4.3. One of the codings "external handover parameters", "location area", "hand over reference", "external handover candidate", "synchronised external handover candidate" and "non synchronised external handover candidate" is used for the external handover procedure which is described in subclause 15.7.

The {MM-INFO-SUGGEST} message can optionally also contain the following information elements:

<<FIXED-IDENTITY>> with the ARI or RFPI of a proposed new FT;

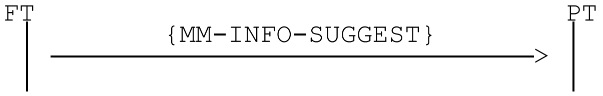
<<LOCATION-AREA>> with the identification of the current location area (extended location information);

<<NWK-ASSIGNED-IDENTITY>> with a network assigned identity;

<<NETWORK-PARAMETER>> with the value of a handover reference;

<<IWU-TO-IWU>> with application specific information.

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues this information directly to the IWU by issuing a MM-INFO-ind primitive.



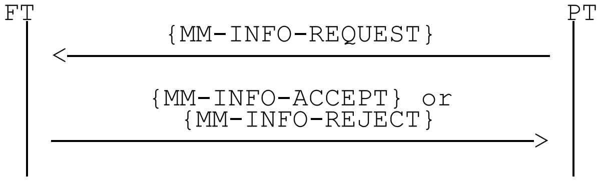
NOTE: If the {MM-INFO-SUGGEST} message included the <<FIXED-IDENTITY>> information element with the PARI of a proposed new FT and the <<LOCATION-AREA>> information element with the current location area code and cell identity, then IWU can perform a handover by using the call control entity.

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 with the ARI or RFPI of a new FT, 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 or RFPI 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-REQUEST} message or a {MM-INFO-REJECT} message the PT issues a MM-INFO-cfm primitive.



13.8 Ciphering related procedure

This procedure is initiated by the FT or PT and is used to engage or disengage ciphering and in the case of engaging ciphering to define the cipher parameters.

NOTE 1: The real time start and stop of ciphering is done in the MAC layer and is always initiated by the PT.

Procedure for cipher-switching initiated by the FT:

Upon receiving a MM-CIPHER-req primitive the FT initiates the procedure by sending a {CIPHER-REQUEST} message to the PT. The {CIPHER-REQUEST} message contains a <<CIPHER-INFO>> information element with the clear/cipher flag and the identification of the cipher algorithm and cipher key. The message can also contain an optional <<CALL-IDENTITY>> information element, which identifies the call for which ciphering shall be engaged or disengaged, and an optional <<CONNECTION-IDENTITY>> information element, which identifies the connection where ciphering shall be engaged or disengaged. If neither the <<CALL-IDENTITY>> information element nor the <<CONNECTION-IDENTITY>> information element is included, then cipher-switching shall relate to all existing calls/connections between the FT and PT. Optionally an <<IWU-TO-IWU>> information element can be included. The cipher key is transferred with a DL-ENC-KEY.req primitive to the lower layer and the timer <MM_cipher.1> is started.

Upon receipt of the {CIPHER-REQUEST} message the PT issues a MM-CIPHER-ind primitive. The PT checks the clear/cipher flag and if it supports the indicated cipher algorithm and cipher key. The response of the PT is as indicated in the following table:

Table 18: Response to cipher switching initiated by the FT

		Current state	
		clear	ciphered
Wanted state	clear	none	EITHER Ciphering is disabled at the MAC layer OR {CIPHER-REJ} message is sent to the FT (reject reason = incompatible service)
	ciphered	IF requested ciphering supported THEN ciphering is enabled at the MAC layer ELSE {CIPHER-REJ} message is sent to the FT (reject reason = "no cipher algorithm" or "cipher algorithm not supported" or "cipher key not supported"	none (NOTE 2)

NOTE 2: A change of the cipher parameters of an existing and already ciphered connection is not supported. It is however possible to switch, to clear, and to start ciphering with new parameters.

If the PT responds by sending an {CIPHER-REJECT} message, then this message may contain one or a prioritised list of the optional <<CIPHER-INFO>> information element to propose an alternative algorithm or key and an optional <<REJECT-REASON>> information element.

Upon receipt of a DL-ENCRYPT.ind primitive from the lower layer or a {CIPHER-REJ} message from the PT the FT shall stop the timer <MM_cipher.1>. The FT issues a MM-CIPHER-cfm primitive.

If a {CIPHER-REJ} message has been received the FT can:

a) release the call; or

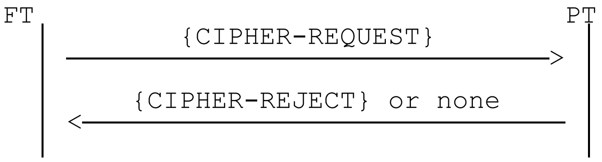
b) proceed in the existing mode;

In the case, that switching from clear to ciphered was requested, the FT has the following additional two options:

c) if the reject reason "cipher algorithm not supported" or the reject reason "cipher key not supported" was included, then the FT can send a new {CIPHER-REQ} message with a new <<CIPHER-TYPE>> information element. This element may have been received in the {CIPHER-REJ} message;

d) if the reject reason "cipher key not supported" was included, then the FT can perform "authentication of the PT" (and thereby establish a new cipher key) and then send a new {CIPHER-REQ} 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-REQ} message. If the timer <MM_cipher.1> expires a second time the FT shall abort the procedure and release the transaction.



Procedure for cipher-switching initiated by the PT:

Upon receiving a MM-CIPHER-req primitive the PT initiates the procedure by sending a {CIPHER-SUGGEST} message to the FT. The {CIPHER-SUGGEST} message contains a <<CIPHER-INFO>> information element with the clear/cipher flag and the identification of the cipher algorithm and cipher key. The message can also contain an optional <<CALL-IDENTITY>> information element, which identifies the call for which ciphering shall be engaged or disengaged, and an optional <<CONNECTION-IDENTITY>> information element, which identifies the connection where ciphering shall be engaged or disengaged. If neither the <<CALL-IDENTITY>> information element nor the <<CONNECTION-IDENTITY>> information element is included, then cipher-switching shall relate to all existing calls/connections between the FT and PT. Optionally an <<IWU-TO-IWU>> information element can be included. The timer <MM_cipher.2> is started.

Upon receipt of the {CIPHER-SUGGEST} message the FT checks if the suggested service is supported. The FT issues a MM-CIPHER-ind primitive. The response of the FT is as indicated in the following table:

Table 19: Response to cipher switching initiated by the PT

		Current state	
		clear	ciphered

Wanted state	clear	none	IF clear is allowed
			THEN
			the "procedure for cipher-switching initiated by the FT" is started by sending {CIPHER-REQ} message
			ELSE
			{CIPHER-REJ} message is sent to the PT

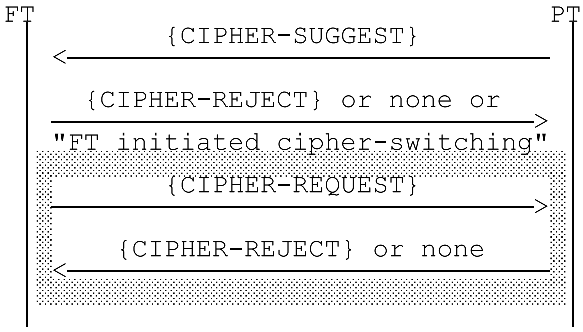
	ciphered	IF requested ciphering supported
		THEN
		the "procedure for ciphering-switching initiated by the FT" is started, sending {CIPHER-REQ} message
		ELSE
		{CIPHER-REJ} message is sent to the PT
			none (NOTE 3)

NOTE 3: A change of the cipher parameters of an existing and already ciphered connection is not supported. It is however possible to switch to clear and to start ciphering with new parameters.

Upon receipt of a {CIPHER-REQ} message or a {CIPHER-REJ} message from the FT the PT shall stop the timer <MM_cipher.2>. If a {CIPHER-REQ} message has been received, then the PT shall respond as described in the "procedure for cipher-switching initiated by the FT".

If a {CIPHER-REJ} message has been received, than the PT can either release the call or proceed in the existing mode. In this case the PT issues a MM-CIPHER-cfm primitive indicating "reject".

The procedure for PT initiated cipher-switching is supervised by the timer <MM_cipher.1> in the PT. At the first expiry of timer <MM_cipher.1> the PT should retransmit the {CIPHER-SUGGEST} message. If the timer <MM_cipher.1> expires a second time the PT shall abort the procedure and release the transaction.



14 Link Control Entity (LCE) procedures

14.1 General

The Link Control Entity (LCE) is the lowest entity in the network layer, and all messages to and from the higher entities pass through the LCE. There is a single LCE at both the FT and the PT.

The LCE controls independent links for each PT. The main function of this single LCE is the message routing task: there is no other interaction between the links. All the LCE procedures are described in terms of one link, and multiple instances of these procedures may be required for a complete FT implementation.

NOTE 1: The following procedures describe the message routing task in terms of two identities: IPUI and TPUI. This task implies a requirement for a local "LCE routing table" that contains the legal IPUI/TPUI associations. The procedures for the creation and management of this table is defined in this ETS.

Each connection oriented link (each Class U, Class A or Class B value of LLN for every PT) can exist in one of four states. A pictorial overview of these states is given in Annex C.

"LINK RELEASED": the link is fully released.

"LINK ESTABLISHED": the link is fully established, with a defined class of operation.

"ESTABLISH PENDING": link establishment has been requested, but has not yet been confirmed.

"RELEASE PENDING": link release has been requested, but has not yet been confirmed.

Each Class B link may support three additional states:

"LINK SUSPENDED": the link is fully suspended.

"SUSPEND PENDING": link suspend has been requested, but has not yet been confirmed.

"RESUME PENDING": link resume has been requested, but has not yet been confirmed.

Each connectionless link (Class U only) can only exist in one state.

NOTE 2: Refer to ETS 300 175-4 [4] for a description of Class U, Class A and Class B links.

The LCE operation is described in two groups of procedures:

a) connection orientated link control;

b) connectionless link control.

14.2 Connection oriented link control procedures

14.2.1 Link establishment

The connection oriented link control procedures are concerned with the establishment, the maintenance, the optional suspension/resumption and the release of one or more DLC C-plane links to each PT, whenever there is a demand from a higher network layer entity. The message from each higher layer instance shall only be routed via one link, but multiple instances may share a single link, or may use separate links.

Each C-plane link shall only be maintained while there are continued demands from the higher entities. When these demands cease (i.e. when all relevant calls are released), the LCE shall release the associated DLC link(s).

The LCE shall immediately (re) establish a DLC C-plane link, in response to the arrival of a message from any of the higher entities. This establishment of a C-plane link is the most complex part of the LCE operation. Three establishment procedures are described:

- direct PT initiated link establishment;

- indirect (paged) FT initiated link establishment;

- direct FT initiated link establishment.

NOTE: The operation of the link establishment procedures may be dependent on stored information relating to the capabilities of PTs. This information storage is described as a "LCE location table" in the following subclauses. The structure of this table is not defined in this ETS.

Additional messages may be queued at the originating LCE during this set-up phase.

If a higher entity releases a call, whilst the initial messages are still queued (i.e. if the link is in the "ESTABLISH PENDING" state), the queued messages shall be discarded, and the link establishment shall be immediately terminated by issuing a DL-RELEASE-req primitive to the DLC layer.

14.2.2 Direct PT initiated link establishment

Direct PT initiated link establishment shall occur when the first service request is detected by the LCE in the PT. The LCE queues (stores) the associated messages, and shall issue a DL-ESTABLISH-req primitive via the S-SAP (SAPI="0"). This primitive shall specify the class of link required and may optionally include a SDU containing the first message.

NOTE: 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").

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-PAGING} message using either a DL-BROADCAST-req primitive or a DL-EXPEDITED-req primitive via the B-SAP. It shall then mark the link as in the "ESTABLISH PENDING" state, and shall start timer <LCE.03>.

No further indirect link establishment messages shall be generated for a PT that has a link in the "ESTABLISH PENDING" state. New requests shall be queued until the pending link establishment is either successful or has failed (timer <LCE.03> has expired).

The DL-EXPEDITED-req primitive shall only be used if the wanted PT is recorded as having a "FAST-PAGE" capability in the LCE location table. Otherwise the DL-BROADCAST-req primitive shall be used.

For individual messages, the identity used in this message shall be decided as follows:

a) the assigned individual TPUI shall be used if available. This may be transmitted in either the short address format or the long address format;

b) if an assigned individual TPUI is not available the identity shall depend on the address format used:

either: the short address format shall be used. This shall contain the default individual TPUI;

or: the long address format shall be used. This shall contain part of the IPUI.

For group messages, an assigned value of TPUI shall always be used.

Refer to ETS 300 175-6 [6] for details of IPUI and TPUI. Refer to subclause 8.2 of this ETS, for details of the corresponding message formats.

NOTE 1: The use of a default individual TPUI or an IPUI means that the identity is not guaranteed to be unique. This allows the possibility of causing false responses from PTs. Therefore the use of assigned individual TPUIs is recommended.

If the {LCE-REQUEST-PAGING} message is successfully received by the intended PT, it shall respond with a PT initiated link establishment, using the procedure defined in subclause 14.2.2. The DL-ESTABLISH-req primitive used by the PT shall contain a {LCE-PAGE-RESPONSE} message which shall contain a complete portable identity. The identity used shall be decided as follows:

- the complete IPUI shall always be used.

This PT response shall be regarded as a new transaction, and the LCE in the PT shall set the transaction identifier to indicate a PT initiated transaction. See subclause 7.3.

The {LCE-REQUEST-PAGING} message may contain extended details of the required MAC layer service (see subclause 8.2). In this event the responding PT may use these service details to start immediate establishment of the required service at the MAC layer. In all other cases, the responding PT shall only establish the minimum MAC layer service needed for a single C-plane link (i.e. a single duplex bearer).

The PT may respond to {LCE-REQUEST-PAGING} messages that contain a correct identity, even if the DLC reports an error for the message, but in this event only a single C-plane link shall be established.

NOTE 2: The possibility to reply to an errored message is allowed to improve the probability of getting the wanted response (i.e. by allowing an error) even though it also means that some false responses may exist. False responses are already possible because the use of shortened IPUIs is allowed.

If this indirect link establishment is successful the DLC at the FT shall deliver a DL-ESTABLISH-ind primitive to the originating LCE containing the {LCE-PAGE-RESPONSE} message. The LCE shall then check the identity contained in this response against a list of outstanding {LCE-REQUEST-PAGING} messages, and if the identity matches it shall mark the link as "LINK ESTABLISHED"; it shall stop timer <LCE.03> and shall send all the queued messages using DL-DATA-req primitives via the S-SAP (SAPI="0").

NOTE 3: The MAC layer identity, PMID, is directly related to the assigned individual TPUI (if used). This identity should be available via the LLME, and may be used to identify the matching {LCE-REQUEST-PAGING} message.

NOTE 4: The LCE should only provide a consistency check of the portable identity. Further checks of identities (for validation or authentication) may occur in the higher entities.

If the identity does not match, the LCE shall immediately reject the set-up by sending a {LCE-PAGE-REJECT} message, using a DL-DATA-req primitive via the S-SAP (SAPI="0") using the same DLEI as indicated by the {LCE-PAGE-RESPONSE}. This FT reply shall also use the same transaction value as used by the PT in the {LCE-PAGE-RESPONSE} message.

The LCE may use the {LCE-PAGE-REJECT} to report a invalid assigned TPUI (individual or group TPUI), by using the <<REJECT-REASON>> information element to indicate "invalid TPUI". Upon receipt of this reason the PT should immediately erase the assigned TPUI.

The LCE may use the {LCE-PAGE-REJECT} to request an automatic test call back, by setting the <<REJECT-REASON>> to test call back: normal/emergency, en-bloc or test call back: normal/emergency, piecewise. See subclause 15.8.

This unwanted link shall be immediately released using the "normal" release procedures defined in subclause 14.2.7.

NOTE 5: The {LCE-PAGE-REJECT} message is only sent over the point-to-point link that has been established by the responding PT. It is not a broadcast message.

NOTE 6: The {LCE-REQUEST-PAGE} message may address more than one portable, when using a group identity. In this case the {LCE-PAGE-REJECT} message should be used to reject a second (and any subsequent) responses.

If timer <LCE.03> expires before the wanted link is established, the LCE should resubmit the {LCE-REQUEST-PAGING} message. Resubmitted messages shall only be issued at a lower priority than other outstanding B-FORMAT messages. A message may be resubmitted a maximum of N300 times, before it is discarded. The link shall remain in the "ESTABLISH PENDING" state until the {LCE-REQUEST-PAGE} message is discarded, thereby preventing any other set-up attempts to the same PT. Upon discarding the message, the link shall be immediately marked as "LINK RELEASED" and the LLME shall be notified of the failure. A new indirect establishment may be initiated immediately.

NOTE 7: The failure of one or more indirect establishment attempts may be used to update the LCE location table such that future set-up requests are rejected. Any such action is not specified as part of this ETS.

If the call is released by the higher entity (usually as a result of a time-out) the message shall be immediately discarded, such that any subsequent responses shall be appear as unwanted responses, thereby invoking the reject procedures described above.

14.2.4 Direct FT initiated link establishment (optional)

Direct FT initiated link establishment can be used as an alternative to indirect FT initiated link establishment only when the intended PT has a valid entry in a LCE location table. This table entry must specify one RFP as the likely location of the wanted PT.

NOTE: The definition of "valid entry" is a local matter and is not specified in this ETS.

When the first message for a particular PT is passed to the LCE in the FT, the LCE queues (stores) the call set-up message, and issues a DL-ESTABLISH-req primitive directly to the DLC layer via the S-SAP (SAPI="0"). This primitive shall contain the correct routing information (to identify a single RFP), and this is used by the DLC layer to address the RFP to use for the set-up attempt.

If link establishment is successful the DLC replies with a DL-ESTABLISH-cfm primitive. The LCE shall now mark the link as "LINK ESTABLISHED", and it shall send the original call set-up message using a DL-DATA-req primitive via the S-SAP (SAPI="0").

If this direct link establishment fails, the originating LCE may reattempt using the indirect procedures described in subclause 14.2.3.

14.2.5 Link maintenance

Active link maintenance is the responsibility of the DLC layer, and no additional maintenance procedures are defined for the LCE.

The LCE has a passive responsibility to report any link failures. An unexpected link failure may occur at any time, resulting in an unexpected DL-RELEASE-ind primitive. The LCE shall report this failure immediately to all active entities. Link re-establishment shall only be attempted upon receipt of service demands from a higher entity.

NOTE: The mechanism for such reporting is internal to the DLC layer, and is not specified in this ETS.

14.2.6 Link suspend and resume

A link may be suspended in response to a request from the CC or COMS entity. This request shall only activate the DLC layer suspend procedure if no other higher entities are using the link (this includes other CC or COMS entities).

A link should be resumed in response to a request from any higher entity. The arrival of a message from any higher entity shall be regarded as a request for link resumption.

Support of the suspend and resume procedures by the LCE is only required when using Class B links.

NOTE: A Class A link cannot be suspended. The LLME may command the release of the Class A link when suspending a call, this provides an equivalent function to Class B suspend.

14.2.6.1 Link suspend

The suspend procedure may be initiated by the LCE at either side (FT or PT) by issuing a DL-SUSPEND-req primitive to the DLC layer. The LCE shall then mark the link as "SUSPEND PENDING" and shall start timer <LCE.04>. Any subsequent messages for this link shall be queued until a response is received from the DLC.

At the receiving side, a request for suspension is indicated with a DL-SUSPEND-ind primitive. The receiving LCE may either accept or reject the suspension, and shall immediately indicate its' decision using a DL-SUSPEND-res primitive. If the suspension is accepted, the receiving LCE shall immediately mark the link as "LINK SUSPENDED". No further messages shall then be submitted, without first invoking link resumption. If the suspension is rejected the receiving LCE shall take no further action and may immediately continue with normal message transmission.

Acceptance or rejection of the suspension shall be indicated to the initiating LCE using a DL-SUSPEND-cfm primitive. Upon receipt of DL-SUSPEND-cfm primitive indicating acceptance, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK SUSPENDED".

NOTE: If there are any queued messages the link should be immediately resumed.

Upon receipt of a DL-SUSPEND-cfm primitive indicating rejection, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK ESTABLISHED". If there are any queued messages these shall be immediately transmitted using DL-DATA-req primitives.

14.2.6.2 Link resume

The resume procedure can be initiated by the LCE at either side (FT or PT) by issuing a DL-RESUME-req primitive to the DLC layer. The LCE shall then mark the link as "RESUME PENDING" and shall start timer <LCE.04>. All messages for this link shall be queued until a response is received from the DLC.

At the receiving side, a request for resumption is indicated with a DL-RESUME-ind primitive. The receiving LCE shall either accept the resumption or shall reject the resumption by immediately releasing the link using the "abnormal" release procedures described in subclause 14.2.7.

If the resumption is accepted, the receiving LCE shall immediately return a DL-RESUME-res primitive and shall mark the link as "LINK ESTABLISHED". Successful resumption shall be reported to the initiating LCE with a DL-RESUME-cfm primitive, and on receipt of this primitive, the initiating LCE shall stop timer <LCE.04> and shall mark the link as "LINK ESTABLISHED". Any queued messages shall be immediately transmitted using DL-DATA-req primitives.

Rejection is indicated to both the receiving LCE and the initiating LCE with DL-RELEASE primitives as described in subclause 14.2.7. In this event, the initiating LCE shall stop timer <LCE.04> and both entities shall mark the link as "LINK RELEASED".

NOTE: Either LCE may subsequently attempt to re-establish the link using the procedures defined in subclause 14.2.1.

14.2.7 Link release

Link release should be initiated automatically, when all higher entities have released their calls. Every higher entity shall provide an explicit notification to the LCE when it ceases to use a link. This notification shall be understood to mean that the link may be released.

NOTE 1: The mechanism for such reporting is internal to the DLC layer, and is not specified in this ETS.

When all relevant higher entities have notified the LCE that they no longer require a given link, the LCE may immediately release the link using either the "normal" release procedure or the "abnormal" release procedure.

NOTE 2: 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 shall be discarded without notification. Use of the "normal" release procedure is recommended in all cases.

Alternatively, if requested by the LLME, or by the initiating entity using the release reason "partial release", the LCE should maintain the link and start timer <LCE.02>. This allows for the possibility of a follow-on call. During this period, the link may be released by either side before <LCE.02> expires using the "abnormal" release procedure.

NOTE 3: The link will only be maintained if both sides independently adopt this option. Either side may elect to release the link before the expiry of <LCE.02>.

If timer <LCE.02> expires before a follow-on message is received, the link shall be immediately released using the "abnormal" release procedure.

NOTE 4: Timer <LCE.02> has a larger value than timer <LCE.01>. Therefore transmission of all outstanding messages should have been completed when <LCE.02> expires.

"Normal" release is 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 is 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".

NOTE 5: A link shall not be re-established whilst in the "RELEASE PENDING" state.

14.3 Connectionless link control procedures

14.3.1 Message routing

A single connectionless link may exist in the direction FT => PT or PT => FT. This link shall only be used by the CLMS entity.

No establishment or maintenance procedures shall be defined for this link, and the state of suitable lower resources shall be ignored by the LCE. CLMS messages shall be immediately submitted to the DLC unless the broadcast announcement procedure described in subclause 14.3.2 is used.

NOTE 1: The LLME is assumed to be responsible for establishing connectionless resources in all lower layers whenever required.

CLMS messages should be sent on the connectionless link using a DL-UNIT-DATA-req primitive via the connectionless S-SAP (SAPI="3"). However, if a suitable connection oriented link already exists in the "LINK ESTABLISHED" state, a CLMS message may be submitted over that link using a DL-UNIT-DATA-req primitive via the connection oriented S-SAP (SAPI="0").

NOTE 2: 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 3: There are restrictions on the maximum message lengths for all CLMS messages (refer to subclause 12.3.2.1). These restrictions apply directly to the CLMS operation, and no checking of message lengths is required in the LCE.

14.3.2 Broadcast announce procedure

CLMS messages in the direction FT to PT may optionally be queued in the LCE while an automatic announcement is broadcast.

NOTE 1: This procedure shall not be used if the CLMS message is being routed over a connection oriented link (SAPI="0").

Upon receipt of a message requiring an announcement, the LCE may queue the message. It shall then immediately issue a {LCE-REQUEST-PAGE} message indicating "none" (refer to message coding in subclause 8.2.1.) using a DL-BROADCAST-req or DL-EXPEDITED-req primitive via the B-SAP.

NOTE 2: The primitive shall be chosen according to the set-up attributes of the relevant portable. See also subclause 14.2.3.

The {LCE-REQUEST-PAGE} message shall contain the same value of connectionless TPUI as used in the CLMS message.

The LCE shall then start timer <LCE.03>, and upon expiry of this timer it shall submit the CLMS message using a DL-UNIT-DATA-req primitive via the S-SAP (SAPI="3")

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 network layer:

Service mapping and negotiation: mapping of the user service demands into information elements and procedures of the internal protocols. Exchange of information elements during call set-up to negotiate and agree the exact service details.

Service modification: management of service modifications (including suspension and resumption) in response to changing service demands.

Resource management: coordination of the installation and control of the lower layer resources in response to service demands.

Management of MM procedures: coordination of different Mobility Management (MM) procedures to avoid deadlock conditions.

Call ciphering management: coordination of ciphering functions between the Mobility Management (MM) entity and one or more Call Control (CC) entities.

External handover management: procedures to support the transfer of parameters related to external handover.

Test management: procedures to support testing of equipment.

15.2 Service mapping and negotiation

15.2.1 General

The LLME is required to map the external service demands (as indicated by the MNCC-SETUP primitive) into internal service instances. Negotiation of acceptable services may be performed at the same time using the following procedures the Call Control (CC) establishment phase.

The LLME shall map the interworking (user) service details into internal service demands and both the external attributes and the resulting internal attributes may be negotiated. If the negotiation is successful, only the agreed service details shall be passed to the lower layers (via the LLME) to invoke U-plane service installation.

Service negotiation may involve one or more of the following procedures:

a) the prioritised list procedure to negotiate the <<CALL-ATTRIBUTES>> element;

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.

15.2.2 Prioritised list negotiation

Prioritised list negotiation allows up to three choices of service mapping to be offered by the initiating entity by including repeated <<CALL-ATTRIBUTES>> information elements into the {CC-SETUP} message as follows:

- a <<REPEAT-INDICATOR>> element indicating "prioritised list"; followed by

- a prioritised list of up to 3 <<CALL-ATTRIBUTES>> 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>> element in the first response message (i.e. {CC-SETUP-ACK}, {CC-CALL-PROC}, {CC-ALERTING} or {CC-CONNECT}). If none of the offered mappings are acceptable, the call shall be released using the normal release procedures.

15.2.3 Exchanged attribute negotiation

Exchanged attribute negotiation may be supported by interworking units in addition to or instead of prioritised list negotiation. Exchanged attribute negotiation provides a mechanism for peer (receiving) entities to suggest alternative service attributes in response to an unacceptable set-up request. This response is designed to provide additional information to the initiating entity such that a subsequent reattempt (using modified service attributes) is more likely to succeed.

Exchanged attribute negotiation shall only be invoked by the receiving IWU if support of this capability is indicated in the <<IWU-ATTRIBUTES>> element (as contained in the {CC-SETUP} message), and if none of the proposed services in the {CC-SETUP} message are acceptable. In this event, the IWU shall reject the call by issuing a MNCC-REJECT-req primitive. It may include one alternative service description in this rejection using an <<IWU-ATTRIBUTES>> element indicating "exchanged parameter negotiation". This description shall indicate an alternative service from the services that are supported by that IWU.

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.

15.3 Service modification procedures

Service modification procedures provide for a restricted set of modifications to an existing "ACTIVE" call, as described in subclause 9.6.

The LLME is required to map the new service demands (as indicated by the MNCC-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 subclause shall only describe coordination of the resources associated with a single portable part. Any broader coordination (such as may be required in complex fixed parts) is not described.

C-plane resources are managed via the LCE, U-plane resources are managed directly via the LLME. In both cases, the detailed management procedures are not specified as part of this ETS, because of the need to allow considerable implementation flexibility.

15.5 Management of MM procedures

In order to avoid possible deadlocks between different Mobility Management (MM) procedures the following rules apply:

- two MM procedures are allowed at any one time, but they shall not both have been initiated by the same side;

  if a MM procedure has not yet been finished, then a second MM procedure may only be initiated if the second MM transaction has a higher priority than the first MM transaction.

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, the higher priority procedure restarts the timer of the lower priority procedure. If the higher priority procedure is a FT initiated user authentication procedure, then the PT shall stop the timer of an unfinished PT initiated lower priority procedure and start the <MM_auth.2> timer. The PT shall stop the <MM_auth.2> timer when it responds to the user authentication procedure by sending an {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message. If the <MM_auth.2> timer expires or is stopped and the lower priority procedure has not been finished in the meantime, then the timer of the interrupted lower priority procedure shall be restarted.

If a procedure with higher priority is invoked by the side which has already invoked a lower priority procedure, which is not yet finished, then the lower priority procedure shall be cancelled.

Priority level 1 (highest priority):

- authentication of a FT.

Priority level 2 (medium priority):

- access rights terminate, FT initiated;
- authentication of a PT;
- authentication of the user;
- ciphering related, FT initiated;
- identification of PT;
- key allocation;
- location update;
- temporary identity assignment.

Priority level 3 (lowest priority):

- access rights;
- access rights terminate, PT initiated;
- ciphering related, PT initiated;
- detach;
- location registration;
- parameter retrieval.

The procedures of priority level 1 and 3 are PT initiated. The procedures of priority level 2 are FT initiated.

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-SET-UP} message. These "interrupting" MM procedures might take more time than the expiry time of the running timers in the CC/COMS entity.

To prevent CC/COMS state machines from waiting on a response delayed by MM procedures, the FT has the possibility to restart the CC/COMS timers in the PT. To cause a timer restart, the LLME should request the CC (or COMS) entity at the FT side to send a {CC-NOTIFY} message containing the <<TIMER-RESTART>> information element.

15.6 Call ciphering management

Call ciphering shall be invoked using the MM procedures described in subclause 13.8. Each MM procedure may be used to enable or disable ciphering of one instance of CC or COMS.

When a cipher change is requested, the LLME shall relay the relevant call references (TI plus PD) from the CC to the MM for inclusion in the <<CALL-IDENTITY>> element.

Following successful reception of a cipher request, the receiving side LLME shall immediately invoke ciphering on all relevant MAC connections, and if successful shall mark the connection as ciphered.

The initiating entity shall take no direct action, but shall monitor the ciphering of all relevant MAC connections, and if successful shall mark the connection as ciphered.

NOTE: Once ciphered, the connection shall only be handed over to a second ciphered connection.

15.7 External handover management

15.7.1 General

External handover is the process of switching a call in progress from one Fixed radio Termination (FT-1) to another Fixed radio Termination (FT-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 terminations 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 an external handover.

15.7.2 External handover procedure

Normally the PT should decide to perform an external handover. Nevertheless the FT has the option to propose an external handover by using the FT initiated procedure for parameter retrieval as described in subclause 13.7.

To perform the handover from the old Fixed radio Termination (FT-1) to the new Fixed radio Termination (FT-2) the PT shall use the PT initiated CC call establishment procedure which is described in subclause 9.3.1. It shall indicate "external handover" in the <<BASIC-SERVICE>> element and shall include the <<NETWORK-PARAMETERS>> element if available. The PT shall only attempt to perform an external handover to a fixed termination which indicates the external handover capability within the broadcasted {FIXED-PART-CAPABILITIES}.

NOTE 1: The {FIXED-PART-CAPABILITIES} message is broadcast by the MAC layer. Refer to ETS 300 175-3 [3].

Upon deciding to attempt an external handover, the PT may either maintain or release the existing call to FT-1. If the call is maintained no further action is needed. If the call is released, the release message shall indicate "external handover release" in the <<RELEASE-REASON>> element. In this event FT-1 should supply at least the <<NETWORK-PARAMETER>> element in {CC-RELEASE-COM} message, unless these parameters have already been supplied by the MM parameter retrieval procedures. The FT-1 may also supply other parameters.

NOTE 2: FT-1 may also assume the external handover case if an existing call is lost without any message exchange. However, the ability to reconnect the call will be dependent soley on the capabilities of the local network.

The PT shall then attempt to establish a second (independent) call to the new FT-2. Depending on the reaction of FT-2 the following three cases are possible:

a) if the set-up to FT-2 has been successful then the call can be switched to the new link and the PT can release or drop the old link (if not already released);

b) if the FT-2 responds with a {CC-SETUP-ACK) message indicating that network parameters are missing, then the PT shall supply these parameters in one or more {CC-INFO} messages;

If a requested parameter is not available and the old call has been maintained, the PT shall request these parameters from FT-1 using the PT initiated procedure for parameter retrieval as described in subclause 13.7. It shall then immediately forward the missing parameters to FT-2.

If a requested parameter is not available and/or the old call has been released, the PT shall release the new call to FT-2, and shall then attempt to establish a MM call to FT-1. This MM call shall be used to request the missing parameters from FT-1 using the PT initiated procedure for parameter retrieval as described in subclause 13.7. If this MM procedure is successful, the PT should re-attempt a set-up to FT-2 and should then supply the missing parameters to FT-2 in the {CC-SETUP} message and/or when requested.

c) if the set-up to FT-2 fails, the call will be released using the normal {CC-RELEASE-COM} message. In this event, the external handover attempt has failed.

15.8 Test management procedures

The test management procedures are defined to allow for automatic testing of equipment without requiring manual intervention. These procedures shall be disabled during normal operation, but when provided they shall be active during the test standby mode.

> NOTE: The procedures for entering equipment into the test standby mode are defined in ETS 300 175-3 [3].

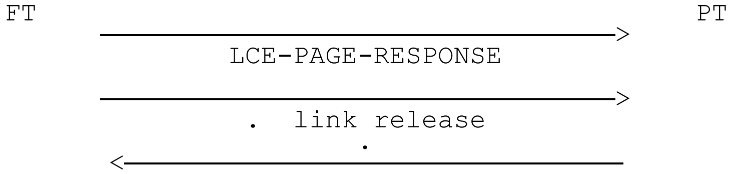
The following procedures are defined:

Test call back: the automatic generation of an outgoing call requested by the lower tester.

Test hook control: the remote control of the PTs hook switch by the lower tester. This allows automatic answering of incoming calls and automatic clearing of both incoming and outgoing calls.

Upper tester: the remote invocation of the FTs MM procedures by the lower tester.

15.8.1 Test call back procedure



Upon receipt of the {LCE-PAGE-REJECT} message including the <<REJECT-REASON>> element = test call back, the PT shall perform the link release procedure as per subclause 14.2.7, and then perform PT initiated call establishment as for a normal/emergency call request depending on the coding of reject reason.

The time taken for the PT to send {CC-SETUP} message upon receipt of the {LCE-PAGE-REJECT} message including the <<REJECT-REASON>> element = test call back shall be less than 10 seconds.

Dialling shall be initiated either as en-bloc or piecewise from the PT depending on the coding of reject reason and whether the PT implements piecewise dialling. Digits dialled shall be as per manufacturers declaration.

15.8.2 Test hook control procedures

Upon receipt of {CC-INFO} message during PT Call Control (CC) state T07 containing the <<TEST-HOOK-CONTROL>> element indicating hook value "off-hook", the PT shall act as though a MNCC-CONNECT-req primitive had been received and shall respond according to the procedures defined in subclause 9.3.2.8.

Upon receipt of a {CC-INFO} message during PT Call Control (CC) states T02, T03, T04, T10, T08 containing a <<TEST-HOOK-CONTROL>> element indicating hook value "on-hook", the PT shall act as though a MNCC-RELEASE-req primitive had been received and shall release the call according to the procedures defined in subclause 9.5.1.

15.8.3 Upper tester procedure

The upper tester procedure is used to invoke FT MM procedures as requested by the lower tester. This procedure should be implemented in the case where the MM procedures can not be invoked by other means at the test house (as declared by the manufacturer).

The LLME receives from the MAC layer the MAC test message {NETWORK-TEST}. Refer to ETS 300 175-3 [3]. The coding of this message is defined below:

```
╔═══════════════════════════════════════════════════════════╗
║  id  |              |    ||       spare      ||           ║
║ 0101 |    param     |1111||0000 1111||0000 1111           ║
╚═══════════════════════════════════════════════════════════╝
|a16                 |a28                                   |
|                 a27|                                   a47|
```

where: "id" indicates a network layer test message;
"a_{ij}" indicates the bit positions in the MAC message.

param	MM procedure invoked
0000 1100	Identification of PT
0000 1110	Temporary identity assignment
0000 0000	Authentication of PT
0000 0001	Authentication of user
0000 1010	Location update
0000 0100	Terminating access rights (FT initiated)
0000 0010	Key allocation
0000 1000	Parameter retrieval (info-suggest)
0000 0110	Ciphering (cipher-request)
other codes	reserved

Upon receipt of the MAC test message, the LLME shall unconditionally invoke the indicated MM procedure within 2 seconds, by proceding as though the equivalent MM primitive had been received. The MM procedure invoked shall use parameters as per manufacturers declaration.

16 Primitives

16.1 Primitive types

Four primitive types may be used:

-req (request)
for a higher layer to request service from a lower layer;

-cfm (confirm)
for the layer providing the service to confirm that the activity has been completed;

-ind (indication)
for a layer providing a service to notify the next higher layer of any specific service related activity;

-res (response)
for a layer to acknowledge receipt of an indication primitive from the next lower layer.

The defined types for each category of primitive are shown as a list in curly brackets. For example

7 MNCC-RELEASE- {req,cfm,ind }

In this example, the defined types are request, confirm and indicate (but not response).

NOTE: These primitives are defined only for the purpose of describing layer-to-layer interactions. The primitives are defined as an abstract list of parameters, and their concrete realisation may vary between implementations. No formal testing of primitives is intended. The following primitive definitions have no normative significance.

16.2 Primitives to lower layer (DLC layer)

The primitives used for communication to the DLC layer are described in ETS 300 175-4 [4].

16.3 Primitives to higher entity (IWU)

This subclause summarises the primitives between the interworking unit and the network layer together with the list of associated parameters.

16.3.1 Parameter definitions

Endpoint identifiers: all primitives shall contain an endpoint identifier. This identifier shall be used to distinguish primitives related to different instances of call. The coding and use of these identifiers is a local matter, and is not defined in this ETS. An identifier is defined for each entity as follows:

- Call Control Endpoint Identifier (CCEI);
- Supplementary Services Endpoint Identifier;
- COMS Endpoint Identifier (COEI);
- CLMS Endpoint Identifier (CLEI);
- Mobility Management Endpoint Identifier.

Message unit: each piece of higher layer (peer-to-peer) information that is included in the primitive is called a message unit. A series of one or more message units may be associated with each primitive where each separate unit is related to one information element in the corresponding network 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 shall be such that a layer sending a message can assume a temporal order of the bits within the message unit, and that the layer receiving the primitive can reconstruct the message with its assumed temporal order.

16.3.2 MNCC primitives

The following primitives are used:

1	MNCC-SETUP-	{req, ind }
2	MNCC-SETUP-ACK-	{req, ind }
3	MNCC-REJECT-	{req, ind }
4	MNCC-CALL-PROC-	{req, ind }
5	MNCC-ALERT-	{req, ind }
6	MNCC-CONNECT-	{req,cfm,ind }
7	MNCC-RELEASE-	{req,cfm,ind,res}
8	MNCC-FACILITY-	{req, ind }
9	MNCC-INFO-	{req, ind }
10	MNCC-MODIFY-	{req,cfm,ind }
11	MNCC-HOLD-	{req, ind }
12	MNCC-RETRIEVE-	{req, ind }
13	MNCC-IWU-INFO-	{req, ind }

16.3.2.1 MNCC-SETUP primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Basic Service	A	-	A	-
IWU attributes	O	-	O	-
Cipher info	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Signal	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
Terminal capability	O	-	O	-
End-to-end compatibility	O	-	O	-
Rate parameters	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
Calling party number	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
Sending complete	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A	= Always;
O	= Optional;
"-"	= not applicable

16.3.2.2 MNCC-SETUP-ACK primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Info type	O	-	O	-
Location area	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
Delimiter request	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A	= Always;
O	= Optional;
"-"	= not applicable

16.3.2.3 MNCC-REJECT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Cause	N	-	A	-
Message units (possible elements)		-		-
Release reason	A	-	A	-
Identity type	O	-	O	-
Location area	O	-	O	-
IWU attributes	O	-	O	-
Facility	O	-	O	-
Display	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A	= Always;
O	= Optional;
"-"	= not applicable

The "cause" parameter shall indicate one of the following values:

- peer message (a valid peer message was received);
- local timer expiry (a local timer has expired).

The coding of this parameter is a local matter and is not specified in this ETS.

16.3.2.4 MNCC-CALL-PROC primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A	= Always;
O	= Optional;
"-"	= not applicable

16.3.2.5 MNCC-ALERT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Signal	O	-	O	-
Feature indicate	O	-	O	-
Terminal capability	O	-	O	-
Transit delay	O	-	O	-
Window size	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A	= Always;
O	= Optional;
"-"	= not applicable

16.3.2.6 MNCC-CONNECT primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	-
Message units (possible elements)				
Facility	O	N	O	-
Progress indicator	O	N	O	-
Display	O	O	O	-
Signal	O	N	O	-
Feature indicate	O	O	O	-
Terminal capability	O	N	O	-
Transit delay	O	N	O	-
Window size	O	N	O	-
IWU-to-IWU	O	O	O	-
IWU-packet	O	O	O	-

A = Always;
O = Optional;
"-" = not applicable

N = Not allowed.

16.3.2.7 MNCC-RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Cause	N	A	N	N
Message units (possible elements)				
Release reason	O	O	O	O
Identity type	N	O	N	O
Location area	N	O	N	O
IWU attributes	N	O	N	O
Facility	O	O	O	O
Display	O	O	O	O
Feature indicate	O	O	O	O
Network parameter	N	O	N	O
IWU-to-IWU	O	O	O	O
IWU-packet	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

The "cause" parameter shall indicate one of the following values:

- peer message (a valid peer message was received);
- local timer expiry (a local timer has expired).

The coding of this parameter is a local matter and is not specified in this ETS.

16.3.2.8 MNCC-FACILITY primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Facility	O	-	O	-
Display	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.2.9 MNCC-INFO primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)		-		-
Location area	O	-	O	-
NWK assigned identity	O	-	O	-
Facility	O	-	O	-
Progress indicator	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Signal	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-
Network parameter	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
Sending complete	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.2.10 MNCC-MODIFY primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	-
Success/Failure flag	N	A	A	-
Message units (possible elements)				-
Service change info	A	O	A	-

A = Always;
O = Optional;
"-" = not applicable

The Success/Failure flag shall indicate the outcome of the service modification.

16.3.2.11 MNCC-HOLD primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Message units (possible elements)				
Display	O	O	O	O
Reject reason	N	O	N	O

A = Always;
O = Optional;
N = Not allowed.

16.3.2.12 MNCC-RETRIEVE primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	A	A	A
Message units (possible elements)				
Display	O	O	O	O
Reject reason	N	O	N	O

A = Always;
O = Optional;
N = Not allowed.

16.3.2.13 MNCC-IWU-INFO primitive

PARAMETER	REQ	CFM	IND	RES
Call Control Endpoint Identifier (CCEI)	A	-	A	-
Message units (possible elements)				
Alphanumeric	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.3 MNSS primitives

The following primitives are used:

1 MNSS-SETUP- {req, ind }
2 MNSS-FACILITY- {req, ind }
3 MNSS-RELEASE- {req, ind }

16.3.3.1 MNSS-SETUP primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)		-		-
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.3.2 MNSS-FACILITY primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)		-		-
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.3.3 MNSS-RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
Supplementary Services Endpoint Identif.	A	-	A	-
Message units (possible elements)		-		-
Release reason	O	-	O	-
Facility	O	-	O	-
Display	O	-	O	-
Keypad	O	-	O	-
Feature activate	O	-	O	-
Feature indicate	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.4 MNCO primitives

The following primitives are used:

1 MNCO-SETUP- {req, ,ind }
2 MNCO-CONNECT- {req, ,ind }
3 MNCO-INFO- {req, ind }
4 MNCO-ACK { , ind }
5 MNCO-RELEASE- {req,cfm,ind }

16.3.4.1 MNCO-SETUP primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)		-		-
IWU attributes	A	-	A	-
Display	O	-	O	-
Called party number	O	-	O	-
Called party subaddress	O	-	O	-
IWU-to-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.4.2 MNCO-CONNECT primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)		-		-
Display	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.4.3 MNCO-INFO primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	-	A	-
Message units (possible elements)		-		-
Display	O	-	O	-
Alphanumeric	O	-	O	-
IWU-TO-IWU	O	-	O	-
IWU-packet	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.4.4 MNCO-ACK primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	-	-	A	-
Message units (possible elements)		-		-
Display	-	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.4.5 MNCO-RELEASE primitive

PARAMETER	REQ	CFM	IND	RES
COMS Endpoint Identifier (COEI)	A	A	A	-
Message units (possible elements)		-		-
Release reason	O	O	O	-
Display	O	O	O	-
IWU-TO-IWU	O	O	O	-
IWU-packet	O	O	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.5 MNCL primitives

The following primitives are used:

1 MNCL-UNITDATA- {req, ind }

16.3.5.1 MNCL-UNITDATA primitive

PARAMETER	REQ	CFM	IND	RES
CLMS Endpoint Identifier (CLEI)	A	-	A	-
CLMS Message type (NOTE 1)	A	-	A	-
Message units (possible elements)		-		-
Alphanumeric	O	-	O	-
IWU-TO-IWU (NOTE 2)	O	-	O	-
IWU-packet (NOTE 2)	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

NOTE 1: The CLMS message type parameter shall specify the message format to be used, fixed or variable.

NOTE 2: If the CLMS message type is fixed, then only the Alphanumeric message unit shall be 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-TERMINATE	{req,cfm,ind,res}
8	MM-KEY-ALLOCATE	{req, ,ind, }
9	MM-INFO	{req,cfm,ind,res}
10	MM-CIPHER	{req,cfm,ind,res}

16.3.6.1 MM-IDENTITY primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Message units (possible elements)				
Identity type	A	N	A	N
Portable identity	N	O	N	O
Fixed identity	N	O	N	O
NWK assigned identity	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

16.3.6.2 MM-IDENTITY-ASSIGN primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	N
Message units (possible elements)				
Portable identity	O	N	O	N
NWK assigned identity	O	N	O	N
Duration	O	N	O	N
Reject reason	N	O	N	O
IWU-TO-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.3 MM-AUTHENTICATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
AUTH-TYPE	A	O	A	O
RAND	A	N	A	N
RES	O	O	O	O
RS	O	O	O	O
Cipher info	O	O	O	O
ZAP field	N	O	N	O
Service class	N	O	N	O
Key	N	O	N	O
Reject reason	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.4 MM-LOCATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
Portable identity	A	O	A	O
Fixed identity	O	N	O	N
Location area	O	O	O	O
NWK assigned identity	O	O	O	O
Cipher info	O	N	O	N
Reject reason	N	O	N	O
Set-up capability	O	N	O	N
Terminal capability	O	N	O	N
Duration	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.5 MM-DETACH primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	-	A	-
Message units (possible elements)				
Portable identity	A	-	A	-
NWK assigned identity	O	-	O	-
IWU-TO-IWU	O	-	O	-

A = Always;
O = Optional;
"-" = not applicable

16.3.6.6 MM-ACCESS-RIGHTS primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
Portable identity	A	O	A	O
Fixed identity	N	O	N	O
Location area	N	O	N	O
AUTH-TYPE	O	O	O	O
Cipher info	O	O	O	O
Terminal capability	O	N	O	N
ZAP field	N	O	N	O
Service class	N	O	N	O
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-TO-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.7 MM-ACCESS-RIGHTS-TERMINATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
Portable identity	A	N	A	N
Fixed identity	O	N	O	N
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-to-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.8 MM-KEY-ALLOCATE primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	-	A	-
Message units (possible elements)				
Allocate type	A	-	A	-
RAND	A	-	A	-
RS	A	-	A	-

A = Always;
"-" = not applicable

16.3.6.9 MM-INFO primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
Info type	A	O	A	O
Portable identity	O	N	O	N
Fixed identity	O	O	O	O
Location area	O	O	O	O
NWK assigned identity	O	O	O	O
Network parameter	O	O	O	O
Reject reason	N	O	N	O
Duration	N	O	N	O
IWU-to-IWU	O	O	O	O

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

16.3.6.10 MM-CIPHER primitive

PARAMETER	REQ	CFM	IND	RES
Mobility Management Endpoint Identifier	A	A	A	A
Accept/Reject flag (NOTE)	N	A	N	A
Message units (possible elements)				
Cipher info	A	O	A	O
Call identity	O	N	O	N
Connection identity	O	N	O	N
Reject reason	N	O	N	O
IWU-to-IWU	O	N	O	N

A = Always;
O = Optional;
N = Not allowed.

NOTE: The Accept/Reject flag indicates the outcome of the procedure.

17 Handling of error and exception conditions

All procedures transferring signalling information by using the values of protocol discriminators defined in this ETS (see subclause 7.2) are applicable only to those messages which pass the checks described in subclauses 17.1 through 17.7.

Detailed error and exception handling procedures are implementation dependent and may vary. However, capabilities facilitating the orderly treatment of error or/and exception conditions are provided for in this section and shall be provided in each implementation.

Subclauses 17.1 through 17.7 are listed in order of precedence.

17.1 Protocol discrimination error

When a message is received with a protocol discriminator value that indicates a service that is not supported by the receiving entity, or that is coded as "unknown protocol entity", that message shall be ignored. "Ignore" means to do nothing, as if the message had never been received.

NOTE: Messages using the protocol discriminator values "unknown protocol entity" are expected to be routed to external (application specific) protocols. However, such coding represents an exception with regard to the protocols defined in this ETS.

17.2 Message too short

When a message is received that is too short to contain a complete <<MESSAGE-TYPE>> information element, that message shall be ignored.

17.3 Transaction identifier error

17.3.1 Unsupported transaction identifier format

If the transaction identifier information element octet 1, bits 7 to 5 indicate an illegal value for the transaction value (i.e. a value that is not allowed in subclause 7.3), or if multiple transactions are not supported by the receiving equipment, 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

17.3.2.1 Unknown active CC call

Whenever any message except {CC-SETUP}, {CC-RELEASE}, {CC-RELEASE-COMPLETE} or (for FPs or PPs supporting the service change procedures of subclause 9.6) {CC-SERVICE-CHANGE} is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, clearing shall be initiated by sending a {CC-RELEASE-COMPLETE} 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-COMPLETE} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, no action should be taken.

When a {CC-SETUP} or {CC-SERVICE-CHANGE} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, and with a transaction identifier flag incorrectly set to "1", this message shall be ignored.

When a {CC-SETUP} message is received specifying a transaction identifier which is recognised as relating to an active call or to a call in progress, this {SETUP} message shall be ignored.

17.3.2.2 Unknown active CISS call

Whenever a CISS entity receives a {FACILITY} message specifying a transaction identifier which is not recognised as relating to an active CISS-call or to a call in progress, clearing is initiated by sending a {CISS-RELEASE-COMPLETE} 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-COMPLETE} is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, clearing shall be initiated by sending a {COMS-RELEASE-COMPLETE} 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-COMPLETE} message is received specifying a transaction identifier which is not recognised as relating to an active call or to a call in progress, no action should be taken.

17.3.2.4 Unknown active CLMS call

Not applicable (there is no "ACTIVE" state for a CLMS call).

17.3.2.5 Unknown active MM transaction

Whenever a MM message is received neither specifying a transaction identifier which is recognised as relating to an initiated MM procedure nor being an allowed messages initiating a new MM procedure, then this message should be ignored.

17.4 Message type or message sequence errors

17.4.1 CC message error

Whenever an unexpected message, except {CC-RELEASE} or {CC-RELEASE-COMPLETE}, or an unrecognised message is received in any state, the message should be ignored.

Alternatively, the abnormal release procedures described in subclause 9.5.2 may be initiated by sending a {CC-RELEASE-COMPLETE} message indicating the release reason as "unexpected message".

When an unexpected {CC-RELEASE} message is received (e.g. if a previous message was corrupted by undetected transmission errors), the message shall not be ignored, and the normal release procedures as specified in subclause 9.5.1 shall be followed.

When an unexpected {CC-RELEASE-COMPLETE} message is received, the message shall not be ignored, and the abnormal release procedures as specified in subclause 9.5.2 shall be followed.

17.4.2 CISS message error

Whenever an unexpected message is received, it should be ignored.

17.4.3 COMS or CLMS message error

Whenever an unexpected message is received, it should be ignored.

17.4.4 MM message error

Whenever an unexpected message is received, it should be ignored.

17.5 General information element errors

The general information element error procedures may also apply to information elements in codesets other than codeset "0". In that case, the release reason information element defined for codeset "0" may be used to indicate errors in information elements other than those in codeset "0" by applying the locking or non-locking shift procedures as described in subclause 7.5.4.

17.5.1 Information element out of sequence

A variable length information element which has a code value lower than the code value of the variable length information element preceding it shall be considered as an out of sequence information element.

If a message is received that contains an out of sequence information element, this information element may be ignored, and the receiving entity may continue to process the message. If this information is mandatory, and the receiving entity chooses to ignore this out of sequence information element, then the error handling procedure for missing mandatory information elements as described in subclause 17.6.1 shall be followed. If the ignored information element is non-mandatory, the receiving entity shall continue to process the message.

NOTE: An implementation may choose to process all the information elements received in a message regardless of the order in which they are placed.

17.5.2 Duplicated information elements

If an information element is repeated in a message in which repetition of the information element is not permitted, 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 COMPLETE} is received which has one or more mandatory information elements missing, the normal release procedure as described in subclause 9.5.1 should be invoked. In this case, the {CC-RELEASE} message shall 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-COMPLETE} message with release reason set to "mandatory information element missing" shall be returned.

When a {CC-RELEASE-COMPLETE} message is received with a <<RELEASE-REASON>> information element missing, it shall be assumed that a {CC-RELEASE-COMPLETE} 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-COMPLETE} is received which has one or more mandatory information elements with invalid content, the normal release procedure as described in subclause 9.5.1 should be invoked. In this case the {CC-RELEASE} message shall 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-COMPLETE} message with release reason "invalid information element contents" shall be returned.

When a {CC-RELEASE-COMPLETE} message is received with invalid content of the <<RELEASE-REASON>> information element, it will be assumed that a {CC-RELEASE-COMPLETE} message was received with release reason "normal".

This subclause shall also apply to mandatory information elements with a length exceeding the maximum length (as given in Clause 6).

17.6.3 Mandatory information element error in COMS or CLMS messages

When a message is received which has one or more mandatory information elements missing or has one or more mandatory information elements with invalid content, the message should be ignored.

Alternatively, when a {COMS-SETUP} message is received which has one or more mandatory information elements missing or with invalid content, a {COMS-RELEASE-COMPLETE} 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.

17.7 Non-mandatory information element errors

The following subclauses identify actions on information elements not recognised as mandatory.

17.7.1 Unrecognised information element

Action shall only be taken on the message and those information elements which are recognised and have valid content.

Subsequent actions in the event of an unrecognised information element are therefore determined by the sender of the unrecognised information elements.

17.7.2 Non-mandatory information element content error

When a message is received which has one or more non-mandatory information elements with invalid content, action shall only be taken on the message and those information elements which are recognised and have valid content. All other elements shall be discarded.

This subclause shall also apply to non-mandatory information elements with a length exceeding the maximum length (as given in Clause 6).

There are two exception to this treatment. The <<IWU-TO-IWU>> and <<IWU-PACKET>> information elements may be truncated and processed.

NOTE: The length of the <<IWU-TO-IWU>> and <<IWU-PACKET>> elements is variable up to several octets. These elements are deliberately placed at the end of all appropriate messages, such that they will be the first elements to suffer truncation in the event of buffer overflow.

17.8 Data link reset

Whenever the LCE is informed of a spontaneous data link layer reset by means of the DL-ESTABLISH-ind primitive, the following procedures apply:

a) for CC calls in the "OVERLAP SENDING" and "OVERLAP RECEIVING" states, the entity shall initiate the normal release procedures as given in subclause 9.5.1. with release reason "unknown";

b) for CC calls in the "ACTIVE", "RELEASE PENDING" or "NULL" states no action shall be taken;

c) for CC calls in the remaining establishment phase (states T-01, T-03, T-04, T-05, T-06, T-07, T-08, T-23 and F-01, F-03, F-04, F-06, F-07, F-23) and in any of the service change states, the call shall be maintained subject to the procedures contained in Clause 9;

d) for MM transactions, the transaction shall be maintained subject to the procedures contained in Clause 13.

17.9 Data link failure

Whenever a LCE is notified by its data link entity via the DL-RELEASE-ind primitive that there is a data link layer failure, the following procedure shall apply:

a) any calls not in the "ACTIVE" state shall be cleared internally;

b) if the DL-RELEASE-ind primitive indicates "normal" release, any calls in the "ACTIVE" state shall also be cleared internally;

c) if the DL-RELEASE-ind primitive indicates "abnormal" release, any calls in the "ACTIVE" state may be maintained, in which case the LCE should request link re-establishment from the DLC layer.

In case c), if the LCE requests DLC link re-establishment, it shall do this immediately by sending a DL-ESTABLISH-req primitive and shall start timer <LCE.04>. This shall only occur if at least one call is in the "ACTIVE" state. Otherwise, the LCE shall clear internally.

NOTE 1: If timer <LCE.04> is already running, it shall not be restarted.

NOTE 2: If the transfer mode of the call is circuit-mode, the LCE may nonetheless choose to clear the call. If the transfer mode of the call is packet mode and the MAC layer is recognised as normal in spite of the data link failure, the LCE should not clear the call and should request data link re-establishment.

When informed of a successful DLC link re-establishment by means of the DL-ESTABLISH-cfm primitive, the LCE shall stop timer <LCE.04>.

If timer <LCE.04> expires prior to DLC link re-establishment, the LCE shall clear all of the associated calls.

Annex A (normative): System parameters

A.1 CC timers

<CC.01>	Overlap sending timer.
FT value:	20 seconds
PT value:	Not used
Start:	An incomplete called party number is received.
Stop:	A complete called party number is received

<CC.02>	CC release timer.
FT value:	30 seconds
PT value:	30 seconds
Start:	A {CC-RELEASE} message is sent.
Stop:	A {CC-RELEASE-COM} message is received.

<CC.03>	CC set-up timer.
FT value:	20 seconds
PT value:	20 seconds
Start:	A {CC-SETUP} message has been sent.
Stop:	An response message has been received.

<CC.04>	CC completion timer.
FT value:	100 seconds
PT value:	100 seconds
Start:	Refer to subclause 9.3.
Stop:	Refer to subclause 9.3.

<CC.05>	CC connect timer.
FT value:	Not used
PT value:	10 seconds
Start:	A {CC-CONNECT} message has been sent.
Stop:	A {CC-CONNECT-ACK} message is received.

A.2 SS timers

No timers defined.

A.3 COMS timers

<COMS.00>	COMS storage timer.
FT value:	5 seconds
PT value:	5 seconds
Start:	The first segment of a segmented message is received.
Stop:	The last segment is received.

<COMS.01>	COMS information acknowledge.
FT value:	2 seconds
PT value:	2 seconds
Start:	A {COMS-INFO} message is sent.
Stop:	A {COMS-ACK} message is received.

<COMS.02>	COMS release timer.
FT value:	10 seconds
PT value:	10 seconds
Start:	A {COMS-RELEASE} message is sent.
Stop:	A {COMS-RELEASE-COM} message is received.

<COMS.03> COMS set-up timer.
FT value: 10 seconds
PT value: 10 seconds
Start: A {COMS-SETUP} message has been sent.
Stop: An response message has been received.

A.4 CLMS timer

<CLMS.00> CLMS storage timer.
FT value: 5 seconds
PT value: 5 seconds
Start: The first segment of a segmented message has been received.
Stop: The last segment is received.

A.5 MM timers

<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: A {ACCESS-RIGHTS-TERMINATE-REQUEST} message is sent.
Stop: A {ACCESS-RIGHTS-TERMINATE-ACCEPT} 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: A {KEY-ALLOCATE-ACKnowledge} message is received.

<MM_locate.1> Location timer.
FT value: None
PT value: 20 seconds
Start: A {LOCATE-REQUEST} message is sent.
Stop: A {LOCATE-ACCEPT} message or a {LOCATE-REJECT} message is received.

<MM_wait> Re-attempt timer.
FT value: None
PT value: 5 minutes

A.6 LCE timers

<LCE.01> Link release timer.
FT value: 5 seconds
PT value: 5 seconds
Start: A DL-RELEASE-req primitive is sent.
Stop: A DL-RELEASE-cfm primitive is received.

<LCE.02> Link maintain timer.
FT value: 10 seconds maximum
PT value: 10 seconds maximum
Start: All associated higher entities have been released.
Stop: A new higher entity message is received.

<LCE.03> {LCE-REQUEST-PAGE} message resubmission timer.
FT value: 3 seconds
PT value: 3 seconds
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.

A.7 Network layer constants

N300: resubmission of an indirect link establish message.
N300 is an application specific value.
Recommended value for voice applications is 3.

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 B1: CC state table at PT side

EVENT (CC message)	STARTING STATE										END STATE
	T00	T01	T02	T03	T04	T06	T07	T08	T10	T19	
{SETUP} sent	P01										TO1
{SETUP} rcvd	P08										TO6
{SET-ACK} rcvd		P03									T02
{CALL-PR} rcvd		P05	P05								TO3
{ALERTING}rcvd		P06	P06	P06							TO4
{CONNECT} rcvd		P07	P07	P07	P07						T10
{CON-ACK} rcvd								P11			T10
{SETUP} accept						P09					T07
{CONNECT} sent						P10	P10				T08
{INFO} rcvd			P12	P12	P12		P12	P12	P12	P19	*
{INFO} sent			P04	P12	P12		P12	P12	P12		*
{RELEASE} sent		P13	P13	P13	P13		P13	P13	P13		T19
{RELEASE} rcvd			P20	P20	P20	P20	P20	P20	P20	P22	* T00
{REL-COM} rcvd		P14	P14	P14	P14	P14	P14	P14	P14	P22	T00
{REL-COM} sent (reject)						P16					T00
{REL-COM} sent (response)			P21	P21	P21	P21	P21	P21	P21		T00
{NOTIFY} rcvd		P18	P18	P18	P18			P18			*
TIMEOUT			P17	P17	P17			P17			T19
REL TIMEOUT										P15	T00
SETUP TIMEOUT		P27									T00

NOTE 1: An entry "*" in the END STATE column indicates current state maintained.

NOTE 2: All unspecified events (blank entries in the above table) shall be treated according to the normal procedures given in Clause 9 where defined. If not defined they shall be treated according to subclause 17.4 (handling of errors for unexpected messages).

NOTE 3: States T-22 and T-23 are for further study.

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;
OR: 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.
OR: 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.
Next state T-10.

P12: MNCC-INFO-req received; Send {CC-INFO} message.
or {CC-INFO} message received: issue MNCC-INFO-ind.
Current state maintained.

P13: MNCC-RELEASE-req primitive received.
{CC-RELEASE} message sent. Clear call.
Next state T-19.

P14: Receive {CC-RELEASE-COM} message.
Issue MNCC-REJECT-ind primitive. Clear call. Next state T-00.

P15: Release time-out. Send {CC-RELEASE-COM} message.
Issue MNCC-RELEASE-cfm primitive. Clear call. Next state T-00.

P16: Call rejected or MNCC-REJECT-req primitive received.
Send {CC-RELEASE-COM} message.
Clear call. Next state T-00.

P17: Send {CC-RELEASE} message. Reason = "timer expiry".
Next state T-19.

P18: {CC-NOTIFY} received. Issue MNCC-NOTIFY-ind primitive.
Current state maintained.

P19: {CC-INFO} received. Issue MNCC-INFO primitive. Next state T-19.

P20: {CC-RELEASE} message received. Issue MNCC-RELEASE-ind primitive.
Current state maintained.

P21: MNCC-RELEASE-res primitive received.
Send {CC-RELEASE-COM} message. Clear call. Next state T-00.

P22: {CC-RELEASE-COM} message or {CC-RELEASE} message received.
Issue MNCC-RELEASE-cfm primitive. Clear call. Next state T-00.

P23-P26: For further study.

P27: <CC.03> expires. Send {CC-RELEASE-COM} message.
Issue MNCC-RELEASE-ind primitive. Clear call. Next state T-00.

ALL OTHER CASES: all unexpected messages shall be handled according to Clause 9 (if described) or according to subclause 17.4 (if not described).

B.2 CC state transitions at FT side

B.2.1 CC state table at FT side

Table B2: CC state table at FT side

EVENT (CC message)	STARTING STATE									END STATE
	F00	F01	F02	F03	F04	F06	F07	F10	F19	
{SETUP} sent	Q01									F06
{SETUP} rcvd	Q08									F01
{SETUP-ACK} sent		Q11								F02
{CALL-PROC} sent		Q09	Q09							F03
{ALERTING} sent		Q05	Q05	Q05						F04
{ALERTING} rcvd						Q06				F07
{CONNECT} sent		Q10	Q10	Q10	Q10					F10
{CONNECT} rcvd						Q07	Q07			F10
{INFO} sent			Q12	Q12	Q12		Q12	Q12		*
{INFO} rcvd			Q04	Q12	Q12		Q12	Q12	Q19	*
{RELEASE} sent				Q13	Q13	Q13	Q13	Q13		F19
{RELEASE} rcvd		Q20	Q20	Q20	Q20		Q20	Q20	Q22	* F00
{REL-COM} rcvd		Q14	Q14	Q14	Q14	Q14	Q14	Q14	Q22	F00
{REL-COM} sent (reject)		Q16	Q16							F00
{REL-COM} sent (response)		Q21	Q21	Q21	Q21		Q21	Q21		F00
{NOTIFY} sent		Q18	Q18	Q18	Q18					*
TIMEOUT			Q17	Q17	Q17		Q17			F19
REL TIMEOUT									Q15	F00
SETUP TIMEOUT						Q27				F00

NOTE 1: An entry "*" in the END STATE column indicates current state maintained.

NOTE 2: All unspecified events (blank entries in the above table) shall be treated according to the normal procedures given in Clause 9 where defined. If not defined they shall be treated according to subclause 17.4 (handling of errors for unexpected messages).

NOTE 3: States F-22 and F-23 are for further study.

B.2.2 CC transition procedures at FT side

Q01: MNCC-SETUP-req primitive received.
Send {CC-SETUP} message to PT. Next state F-06.

Q04: {CC-INFO} message received.
Deliver <<KEYPAD>> element in MNCC-INFO-ind primitive.
State F-02 maintained.

Q05: MNCC-ALERT-req primitive received.
Send {CC-ALERTING} message. Next state F-04.

Q06: {CC-ALERTING} message received.
Issue MNCC-ALERT-ind primitive. Next state F-07.

Q07: {CC-CONNECT} message received.
Connect U-plane. Send {CC-CONNECT-ACK} message.
Issue MNCC-CONNECT-ind primitive. Next state F-10.

Q08: {CC-SETUP} message received from PT.
Issue MNCC-SETUP-ind primitive. Next state F-01.

Q09: MNCC-CALL-PROC-req primitive received.
Send {CC-CALL-PROC} message. Next state F-03.

Q10: MNCC-CONNECT-req primitive received. Connect U-plane.
Send {CC-CONNECT} message. Next state F-10.

Q11: MNCC-SETUP-ACK-req primitive received.
Send {CC-SETUP-ACK} message. Next state F-02.

Q12: MNCC-INFO-req received; Send {CC-INFO} message.
or {CC-INFO} message received: issue MNCC-INFO-ind.
Current state maintained.

Q13: MNCC-RELEASE-req primitive received. Clear call.
Send {CC-RELEASE} message. Next state F-19.

Q14: Receive {CC-RELEASE-COM} message.
Issue MNCC-REJECT-ind primitive. Clear call. Next state F-00.

Q15: Release time-out. Send {CC-RELEASE-COM} message.
Issue MNCC-RELEASE-cfm primitive. Clear call. Next state F-00.

Q16: Call rejected, or MNCC-REJECT-req primitive received.
Send {CC-RELEASE-COM} message. Clear call.
Next state F-00.

Q17: Timer Expires. Send {CC-RELEASE} message.
Reason = "timer expiry". Next state F-19.

Q18: MNCC-NOTIFY-req primitive received.
Send {CC-NOTIFY} message. Current state maintained.
Q19: {CC-INFO} received. Issue MNCC-INFO primitive. Next state F-19.

Q20: {CC-RELEASE} message received. Issue MNCC-RELEASE-ind primitive.
Current state maintained.

Q21: MNCC-RELEASE-res primitive received.
Send {CC-RELEASE-COM} message. Clear call. Next state F-00.

Q22: {CC-RELEASE-COM} message or {CC-RELEASE} message received.
Issue MNCC-RELEASE-cfm primitive. Clear call. Next state F-00.

Q23-Q26: For further study.

Q27: <CC.03> expires. Send {CC-RELEASE-COM} message.
Issue MNCC-RELEASE-ind primitive. Clear call. Next state F-00.

ALL OTHER CASES: all unexpected messages shall be handled according to Clause 9 (if described) or according to subclause 17.4 (if not described).

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

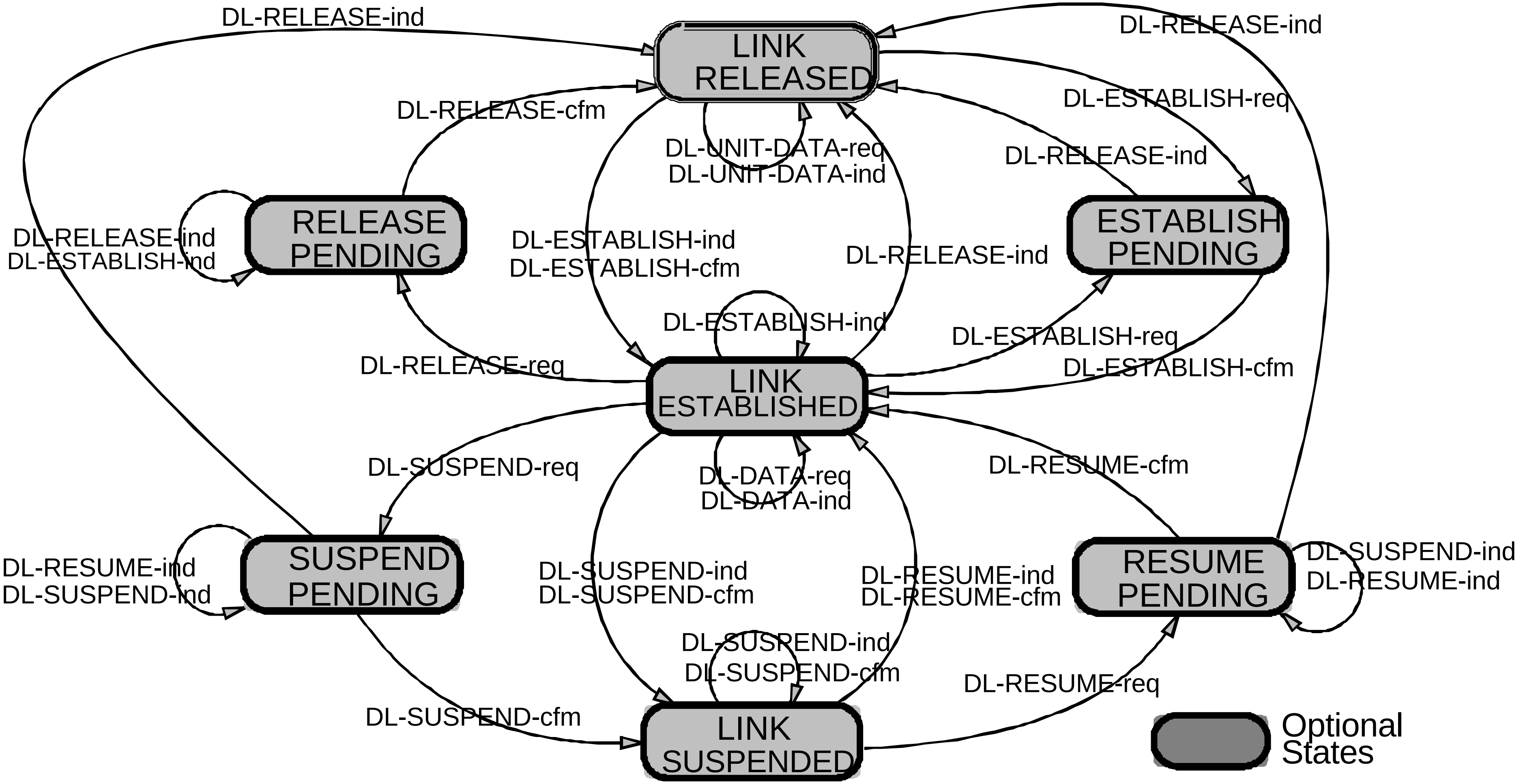


Figure C.1: DLC Link states as viewed by the cycle

Annex D (normative): DECT standard character sets

D.1 General

Two standard character sets are defined:

- DECT standard 8-bit characters;
- DECT standard 4-bit characters.

The DECT standard 8-bit characters shall be used for both dialling and display functions when contained in the following information elements:

- <<"KEYPAD">>;
- <<"DISPLAY">>;
- <<CALLED-PARTY-NUMBER>>;
- <<CALLING-PARTY-NUMBER>>.

Both the 8-bit and 4-bit DECT standard character sets may be carried in the <<ALPHANUMERIC>> information element or in the {CLMS-FIXED} message.

All of these elements may contain one or several characters.

D.2 DECT standard 8-bit characters

D.2.1 General

The first 128 characters shall use the standard IA5 characters, except for the first 32 (control) characters which are redefined as DECT "control codes".

NOTE 1: Refer to CCITT Recommendation T.50 [25] for details of IA5 characters.

The second 128 characters are called DECT "extended codes". These shall be reserved for DECT specific use.

NOTE 2: The <<ALPHANUMERIC>> element allows for alternative character sets, including the complete standard IA5 character coding.

D.2.2 Control codes

Character codes 00 Hex to 1F Hex are specific to the DECT character set. They are not used in the standard IA5 sense. The following values are defined for cursor control (display purposes only) and dialling control:

Code(Hex)	Control character
00	Null/cancel DTMF tone (NOTE 5);
02	Return home;
03	Return end;
05	Dialling pause (NOTE 3);
06	Move forward to next column tab position (NOTE 1);
07	Move backward to next column tab position (NOTE 1);
08	Move backward one column;
09	Move forward one column;
0A	Move down one row;
0B	Move up one row;
0C	Clear display (and return home);
0D	Return (to start of current row);
0E	Flash off (NOTE 2);
0F	Flash on (NOTE 2);
11	XON (resume transmission);
12	Go to pulse dialling (NOTE 4);
13	XOFF (stop transmission);
14	Go to DTMF dialling; defined tone length (NOTE 4);
16	Go to DTMF dialling; infinite tone length (NOTE 5);
19	Clear to end of display (maintain cursor position);
1A	Clear to end of line (maintain cursor position);
1B	ESC. ESCape in the IA5 sense;

All other values reserved.

NOTE 1: Column tabs should be set at 10 column intervals.

NOTE 2: Flash on/Flash off is a toggle action, that applies to all subsequent display characters.

NOTE 3: The duration of the dialling pause is determined by the FT.

NOTE 4: 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 prETS 300 001 [28].

NOTE 5: 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.

D.2.3 Standard IA5 codes

Character codes 20 Hex to 7F Hex shall be used in the standard IA5 sense as defined in CCITT Recommendation T.50 [25]. The International Reference Version (IRV) characters shall be used.

D.2.4 Extended codes

For further study.

D.2.5 Escape to alternative character sets

To be based on ISO Publication 2022 [26].

For further study.

D.3 DECT standard 4-bit characters

Code(Hex)	Character:
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
B	(space)

All other values reserved.

Annex E (normative): Default coding of <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> information elements

Table E1: Default coding for <<IWU-ATTRIBUTES>> information element

Octet	Information element field	Field Value
3	Coding standard	DECT standard
	Info. transfer capability	Speech
4	Negotiation indicator	Not possible
	External connection Type	Connection oriented
5	Transfer mode	Circuit mode
	Info. transfer rate	32 kbps
6	Protocol identifier	User protocol ID
	User protocol ID	G.721 ADPCM

Table E2: Default coding for <<CALL-ATTRIBUTES>> information element

Octet	Information element field	Field Value
3	Coding standard	DECT standard
	Network layer attributes	Public Acc. Profile
4	C-plane class	Class A; shared
	C-plane transfer rate	CS only
5	U-plane symmetry	Symmetric
	LU identification	LU1
6	U-plane class	Class 0 min_delay
	U-plane frame type	FU1

Annex F (normative): Broadcast attributes coding

The broadcast attributes are a small set of network layer and DLC layer capabilities (jointly known as "higher layer capabilities") that shall be broadcast regularly as part of the MAC layer broadcast service.

NOTE 1: These "higher layer" attributes comprise a total of 20 bits of information. These bits are combined with lower layer attributes in the MAC layer to form a single MAC layer broadcast message. Refer to ETS 300 175-3 [3].

Table F1: Broadcast attributes coding

BIT NUMBER (NOTE 2)	ATTRIBUTE ("1" means that service is available)
a32	ADPCM/G.721 Voice service
a33	Public Access Profile (PAP) supported
a34	Non-voice circuit switched service
a35	Non-voice packet switched service
a36	Standard authentication required
a37	Standard ciphering supported
a38	Location registration supported
a39	SIM services available
a40	Non-static Fixed Part (FP)
a41	CISS services available
a42	CLMS service available
a43	COMS service available
a44	Access rights requests supported
a45	External handover supported
a46	Connection handover supported
a47	Reserved

NOTE 2: The bit numbers refer to the bit positions in the MAC message. Refer to subclause 7.2.3.4.2 in ETS 300 175-3 [3].

NOTE 3: The default setting for all bits shall be "0"; meaning "not available".

NOTE 4: The value of any bit might change during normal operation.

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

G.1 General

The <<IWU-PACKET>> and <<IWU-TO-IWU>> are transparent information elements (refer to subclause 6.1.2). They are defined to provide two alternative mechanisms for the transparent transportation of external information (e.g. from a PP application to an FP interworking unit). The two elements correspond to two possible structures of external information.

NOTE: The <<IWU-TO-IWU>> element provides a capability equivalent to the <<USER-TO-USER>> information element defined in ETS 300 102 [21].

G.2 Sending of <<IWU-PACKET>> elements

G.2.1 CC and MM use of <<IWU-PACKET>>

An unsegmented <<IWU-PACKET>> may be carried in most CC and MM messages provided that each message contains at most one <<IWU-PACKET>> information element. A segmented <<IWU-PACKET>> shall only be sent in a series of {IWU-INFO} messages, and each {IWU-INFO} message shall contain one <<IWU-PACKET>> element preceded by a <<SEGMENTED-INFO>> element. A {IWU-INFO} message should be used if there are no suitable CC messages scheduled for transmission.

G.2.2 COMS and CLMS use of <<IWU-PACKET>>

An unsegmented or a segmented <<IWU-PACKET>> may be sent in a series of {COMS-INFO} or {CLMS-VARIABLE} messages. If segmented, each message shall contain one <<IWU-PACKET>> element preceded by a <<SEGMENTED-INFO>> element.

G.2.3 Rejection of <<IWU-PACKET>> elements

The <<IWU-PACKET>> element shall be used to reject any <<IWU-PACKET>> element that is received but cannot be understood (i.e. contains a protocol discriminator coding that is not supported). In this event the element shall indicate rejection (using the S/R bit) and shall contain a partial echo of the message that has been rejected. This echo shall only contain the L2 protocol discriminator and the following octet (i.e. in most cases the echoed information will be truncated). A rejection element shall be returned immediately after receiving the message containing the rejected element.

G.3 Use of <<IWU-TO-IWU>> elements

G.3.1 Sending of <<IWU-TO-IWU>> elements

An unsegmented <<IWU-TO-IWU>> may be carried in most CC or MM messages. Each message shall contain a maximum of one <<IWU-TO-IWU>> information element. An {IWU-INFO} message may be used for transmission of unsegmented <<IWU-TO-IWU>> elements, if there are no suitable messages scheduled for transmission.

A segmented <<IWU-to-IWU>> shall only be sent in a sequence of {IWU-INFO} messages, and each message shall carry only one <<IWU-TO-IWU>> element, and each of these <<IWU-TO-IWU>> elements shall be preceded by a <<SEGMENTED-INFO>> element.

Segmented or unsegmented <<IWU-TO-IWU>> elements may be carried in {COMS-INFO} or {CLMS-VARIABLE} messages.

G.3.2 Rejection of <<IWU-TO-IWU>> elements

The <<IWU-TO-IWU>> element shall also be used to reject any <<IWU-TO-IWU>> element that is received but cannot be understood (i.e. contains a protocol discriminator coding that is not supported). In this event the element shall indicate rejection (using the S/R bit) and shall contain a partial echo of the message that has been rejected. This echo shall only contain the protocol discriminator and the first information octet of the rejected message (i.e. in most cases the echoed information will be truncated). A rejection element shall be returned immediately after receiving the message containing the rejected element.

History

Document history	
October 1992	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)