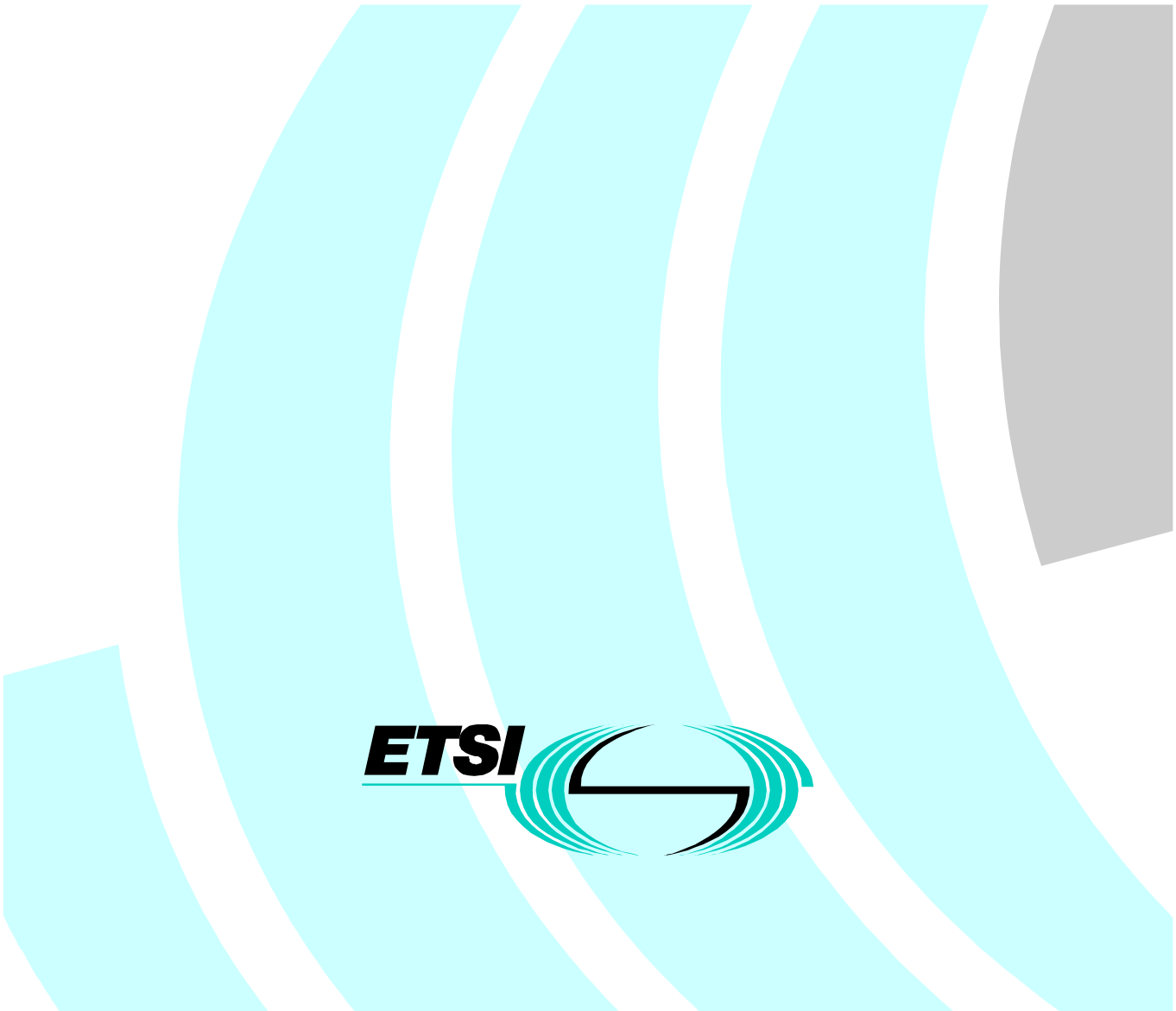
Draft EN 301 650 V0.5.1 (1999-03)

European Standard (Telecommunications series)

Digital Enhanced Cordless Telecommunications (DECT); Multimedia Access Profile (MMAP)



Reference
DEN/DECT-020138 (fa0001oo.PDF)

Keywords
DECT, access, DATA, MMAP, profile

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

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

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

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The scope of the present document is to define a very basic access profile mainly for home and small office and home office (SOHO) markets. This profile will combine a selection of the DECT data services with optional voice services offered by Generic Access Profile (GAP) allowing terminals to provide true integrated multimedia services comprising both voice and data.

The aim of the present document is to guarantee interoperability. The profile defines a selection of the relevant options available in the current data profiles and where necessary describes interworking scenarios.

The multimedia profile is based on existing profiles. It is an aim for the present documents to provide an easy route for development of DECT DATA applications, with the features of the present document being a common fall-back option available in all MMAP compliant equipment.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical layer (PHL)".

[2] EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[3] EN 300 175-4: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".

[4] EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[5] EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[6] EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[7] EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech coding and transmission".

[8] EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Approval test specification; Part 1: Radio".

[9] EN 300 176-2: "Digital Enhanced Cordless Telecommunications (DECT); Approval test specification; Part 2: Speech".

[10] EN 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[11] EN 300 651: "Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Generic data link service (service type C, class 2)".

[12] ISO/IEC 8073 (1992): "Information processing systems - Open System Interconnection - Connection oriented transport protocol specification".

[13] ISO/IEC 8802-3 (1996): "Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications".

[14] ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation conformance statement".

[15] TBR 22: "Attachment requirements for terminal equipment for Digital Enhanced Cordless Telecommunications (DECT) Generic Access Profile (GAP) applications".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

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

NOTE 1: Void.

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 (NWK) 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 NWK layer.

call: all of the NWK layer processes involved in one NWK 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: a network that uses the DECT Air Interface (AI) 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 NWK layer.

NOTE 6: A DECT network is a logical grouping that contains one or more FTs plus their associated PT. The boundaries of the DECT network are not physical boundaries.

fixed part (DECT Fixed Part): a physical grouping that contains all of the elements in the DECT network between the local network and the DECT AI.

NOTE 7: A DECT FP contains the logical elements of at least one FT, plus additional implementation specific elements.

fixed radio termination: a logical group of functions that contains all of the DECT processes and procedures on the fixed side of the DECT AI.

NOTE 8: A FT only includes elements that are defined in the DECT Common Interface (CI) standard. This includes radio transmission elements together with a selection of layer 2 and layer 3 elements.

geographically unique identity: this term relates to FP identities, PARIs and RFPIs. It indicates that two systems with the same Primary Access Rights Identity (PARI), or respectively two RFPs with the same Radio Fixed Part Identity (RFPI), can not be reached or listened to at the same geographical position.

NOTE 9: For PARI and RFPI, see abbreviations.

global network: a telecommunication network capable of offering a long distance telecommunication service.

NOTE 10: 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.

NOTE 11: There are two physical forms of handover, intra-cell handover and inter-cell handover.

HyP: a physical grouping that contains both Fixed Part (FT) and Portable Part (PP) functionality.

incoming call: a call received at a PP.

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 FT. Internal handover reconnects the call at the lower layers, while maintaining the call at the NWK layer.

NOTE 12: 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).

inter-operability: the capability of FPs and PPs, that enable a PP to obtain access to teleservices in more than one Location Area (LA) and/or from more than one operator (more than one service provider).

interworking unit: a unit that is used to interconnect sub networks.

NOTE 13: The IWU will contain the interworking functions necessary to support the required sub–network 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.

intra-operator roaming: roaming between different FP coverage areas of the same operator (same service provider).

local network: a telecommunication network capable of offering local telecommunication services.

NOTE 14: 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: a unique identity within one FP or LA, depending on application;

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

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

NOTE 15: These databases are not included within a DECT FT.

MAC connection (connection): an association between one source MAC Multiple 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 PP.

portable application: a logical grouping that contains all the elements that lie beyond the DECT network boundary on the portable side.

NOTE 16: The functions contained in the PA may be physically distributed, but any such distribution is invisible to the DECT network.

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

NOTE 17: A DECT PP is logically divided into one PT plus one or more PAs.

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 AI.

NOTE 18: A PT 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.

radio fixed part: one physical sub-group of a FP 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 PP from one FP coverage area to another FP coverage area, where the capabilities of the FPs enable the PP to make or receive calls in both areas.

NOTE 19: Roaming requires the relevant FPs and PP to be inter-operable.

subscription registration: the infrequent process whereby a subscriber obtains access rights to one or more FPs.

NOTE 20: Subscription registration is usually required before a user can make or receive calls.

3.2 Abbreviations

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

AC	Authentication Code
AI	Air Interface
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity
BCD	Binary Coded Decimal
CC	Call Control
CI	Common Interface
CISS	Call Independent Supplementary Service
CLMS	Connectionless Message Service
CR/LF	Carriage Return/Line Feed
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DLC	Data Link Control
DLEI	Data Link Endpoint Identifier
DSAA	DECT Standard Authentication Algorithm
DSCA	DECT Standard Cipher Algorithm
DTMF	Dual Tone Multi-Frequency
FLEN	Frame Length
FP	Fixed Part
FT	Fixed radio Termination
GAP	Generic Access Profile
GSM	Global System for Mobile communication
HyP	HYbrid Part
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity

ISDN	Integrated Services Digital Network
IUT	Implementation Under Test
IWU	Interworking Unit
KS	PP authentication Session Key
KS'	FP authentication Session Key
LA	Location Area
LAL	Location Area Level
LCE	Link Control Entity
LLME	Lower Layer Management Entity
LLN	Logical Link Number
LNW	Local Network
LSB	Least Significant Bit
LSIG	Link Signature
MAC	Medium Access Control
MBC	Multiple Bearer Control
ME	Management Entity
MM	Mobility Management
MSB	Most Significant Bit
NLF	New Link Flag
NTP	Normal Transmit Power
NWK	Network
Oct	Octet
P	Public (environment)
PA	Portable Application
PAP	Public Access Profile
PARI	Primary Access Rights Identity
PARK	Portable Access Rights Key
PHL	Physical layer
PLI	PARK Length Indicator
PMID	Portable part MAC Identity
PP	Portable Part
PSN	Portable equipment Serial Number
PT	Portable radio Termination
PUN	Portable User Number
PUT	Portable User Type
R/B	Residential/Business (environment)
RAND	A Random challenge issued by a FP
RES	A Response calculated by a PP
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RLR_H	Receiving Loudness Rating of the Handset
RPN	Radio fixed Part Number
RS	A value used to establish authentication session keys
SAP	Service Access Point
SAPI	Service Access Point Identifier
SARI	Secondary Access Rights Identity
SS	Supplementary Services
TARI	Tertiary Access Rights Identity
TBC	Traffic Bearer Control
TCL	Telephone Coupling Loss
TPUI	Temporary Portable User Identity
TRUP	Transparent Unprotected service
UAK	User Authentication Key
UPI	User Personal Identification

3.3 Symbols

The symbols defined in this subclause are applied for procedures, features, and services in the present document if not explicitly otherwise stated. The interpretation of status columns in all tables is as follows:

- M for mandatory to support (provision mandatory, process mandatory);
- O for optional to support (provision optional, process mandatory);
- I for out-of-scope (provision optional, process optional) not subject for testing;
- C for conditional to support (process mandatory);
- N/A for not-applicable (in the given context the specification makes it impossible to use this capability)
- X excluded, not allowed.

Provision mandatory, process mandatory means that the indicated feature service or procedure shall be implemented as described in the present document, and may be subject to testing.

Provision optional, process mandatory means that the indicated feature, service or procedure may be implemented, and if implemented, the feature, service or procedure shall be implemented as described in the present document, and may be subject to testing.

NOTE: The used notation is based on the notation proposed in ISO/IEC 9646-7 [14].

4 Feature definitions

For the purposes of the present document the feature definitions in the following subclauses apply.

The number given in square brackets after the name of a feature is the item number used in the tables of the present document.

4.1 Network (NWK) features

outgoing call [N.1]: a call initiated at a DECT PP.

off-hook [N.2]: the ability to indicate the action of going off-hook, e.g. to start call set-up or accept a call.

on-hook (FULL Release) [N.3]: the ability to indicate the action of going on-hook (e.g. to terminate a call) and fully release the radio resource.

dialled digits (basic) [N.4]: the capability to dial digits 0-9, *, #.

register recall [N.5]: the ability of the PP to request the invocation of the supplementary service "register recall" over the DECT interface and the ability of the FP to transmit the request to the local network. Register recall means to seize a register (with dial tone) to permit input of further digits or other action.

pause (dialling pause) [N.6]: the ability to generate or indicate an dialling pause, e.g. to await further dial tone.

incoming call [N.7]: a call received at a DECT PP.

authentication of PP [N.8]: the process by which the identity of a DECT PP is checked by the FP.

authentication of user [N.9]: the process by which the identity of a user of a DECT PP is checked by the FP. The User Personal Identification (UPI), a personal identification of 0 to 8 digits, manually entered by the user, is used for user authentication.

location registration [N.10]: a facility whereby a PP can be registered with a FP or a cluster of FPs such that incoming calls, radio pages or messages may be routed to it.

on-air key allocation [N.11]: the capability to transform Authentication Code (AC) into User Authentication Key (UAK) using the key allocation procedure.

identification of PP [N.12]: the ability for the FP to request and PP to provide specific identification parameters.

service class indication/assignment [N.13]: assignment by the FP to PP of the service class and indication to the FP by the PP of the contents of its service class.

alerting [N.14]: activates or deactivates alerting at the PP using any appropriate indication.

ZAP [N.15]: the ability first to assign and then to re-program the account data held in the PP so that access rights may be suspended subject to the conditions set by the service provider being met, coupled with the ability to re-program the account data again to reinstate access rights once these conditions have been met. One ZAP field shall be provided per account field. The PP has the right to authenticate the FP prior to the execution of ZAP suspend.

encryption activation FT initiated [N.16]: the activation of the encryption process requested by Fixed radio Termination (FT).

subscription registration procedure on-air [N.17]: a standardized procedure for loading subscription registration data into a PP in real time over the air-interface.

link control [N.18]: the ability to request, accept, maintain and release a data link for the purposes of a NWK layer procedure.

terminate access rights FT initiated [N.19]: the ability of the FP to delete a subscription in the PP.

partial release [N.20]: the ability to release an established or in progress Call Control (CC) call whilst retaining the radio resource for the purpose of accessing further services.

signalling of display characters [N.21]: the transmission to the PP of characters to be displayed on the user's PP display (if provided).

display control characters [N.22]: characters sent to the PP to control the user's display in the PP (if provided). Such characters include cursor control, clear screen, home, flash, inverse video etc.

authentication of FT [N.23]: the process by which the identity of a FP is checked by the PP.

encryption activation PT initiated [N.24]: the activation of the encryption process suggested by PT. The real time start of ciphering is done in the MAC layer and is always initiated by the PT.

encryption deactivation FT initiated [N.25]: the deactivation of the encryption process requested by FT. The real time stop of ciphering is done in the MAC layer and is always initiated by the PT.

encryption deactivation PT initiated [N.26]: the deactivation of the encryption process suggested by PT. The real time stop of ciphering is done in the MAC layer and is always initiated by the PT.

Calling Line Identification Presentation (CLIP) [N.27]: the ability to provide the calling party number to the called party before accepting the call.

internal call [N.28]: a call between 2 users that does not make use of the local network resources. This is typically useful in residential environments.

service call [N.29]: a call initiated by a DECT PT for entering of FT related service and adjustment procedures in a transparent way. After having sent the service call indication, the PT behaves according to the rules of a normal call.

in-call service change [N.30]: the ability to modify call parameters (e.g. bandwidth, IWU parameters etc.) while the call is maintained.

service suspension & resumption [N.31]: the ability to suspend a call due to inactivity of the connection, and to resume it when new activity is detected.

service negotiation [N.32]: the ability to negotiate call parameters during call set-up.

4.2 Application features

AC to bitstring mapping [A.1]: mapping of the AC into a bitstring.

multiple subscription registration [A.2]: the ability of PP to store more than one subscription.

manual entry of the Portable Access Rights Key (PARK) [A.3]: the ability of the PP to accept a manual entry of the PARK for ensuring attachment to the right FP in a physical area covered by many providers.

distributed communication [A.4]: the communication between a number of DECT terminals involving distributing of calls processing between a number of FPs and HyPs.

5 Service definitions

For the purposes of the present document the following service definitions apply.

5.1 DLC service definitions

LAPC class A service and Lc [D.1]: a single frame acknowledged C-plane data link service providing a single data link between one FT and one PT. The higher layer information is segmented (if necessary) and transmitted in numbered frames. The Lc provides frame delimiting, transparency and frame synchronization.

Cs channel fragmentation and recombination [D.2]: a Lc service providing channel dependant fragmentation (by means of dividing a LAPC data unit into more than one service data units for delivery to the MAC layer Cs logical channel) and recombination (by means of joining several service units received from the MAC layer Cs logical channel into a LAPC data unit).

broadcast Lb service [D.3]: a simplex point-to-multipoint transmission using simple fixed length DLC frames providing a restricted broadcast service in direction FP to PP(s).

intra-cell voluntary connection handover [D.4]: internal handover process provided and initiated by the DLC layer (e.g. as a result of continued poor quality of service from the MAC layer), whereby one set of DLC entities (C-plane and U-plane) can re-route data from one MAC connection to a second new MAC connection in the domain of the same cell, while maintaining the service provided to the NWK layer.

intercell voluntary connection handover [D.5]: internal handover process provided and initiated by the DLC layer (e.g. as a result of continued poor quality of service from the MAC layer), whereby one set of DLC entities (C-plane and U-plane) can re-route data from one MAC connection to a second new MAC connection not in the domain of the same cell, while maintaining the service provided to the NWK layer.

encryption activation [D.6]: transporting the NWK layer encryption request and the cipher key to the MAC layer, thereby enabling the encryption process in the MAC layer.

encryption deactivation [D.7]: transporting the NWK layer encryption deactivation request to the MAC layer, thereby disabling the encryption process in the MAC layer.

U-plane handling [D.8]: the LU2 Frame RELay service (FREL) introducing a protected data transfer including a retransmission scheme for the DLU. Only used for non-speech applications. The continuous higher layer data is fragmented for delivery to the Ip logical channel in the transmission direction, and recombined from the Ip logical channel in the receiving direction.

Cf channel fragmentation and recombination [D.9]: a Lc service providing channel dependant fragmentation (by means of dividing a LAPC data unit into more than one service data units for delivery to the MAC layer Cf logical channel) and recombination (by means of joining several service units received from the MAC layer Cf logical channel into a LAPC data unit).

selection of logical channel (C_S or C_F) [D.10]: selection of logical channel for Lc operation on a frame-by-frame basis.

U-plane peer to peer [D.11]: offers a connection oriented service.

U-plane point to multi-point [D.12]: offers a connection less point to multi-point service via the SIp channel.

5.2 MAC service definitions

general [M.1]: a set of basic requirements regarding data formats, multiplexing, CRC usage, scanning and locking, which are prerequisites to communication between peer MAC entities.

non-continuous broadcast [M.2]: the non-continuous broadcast service allows the PT to receive extended system information on request.

continuous broadcast [M.3]: a simplex service from FT to PT whereby the FT maintains at least one bearer with continuous transmissions. The PT can use the information carried in this bearer to lock to the FT and to obtain knowledge about the FT.

paging broadcast [M.4]: a service whereby the identities of specific PTs can be broadcast by the FT. This service is normally used by the FT to request a specific PT to set up a link to the FT.

higher layer connectionless U-plane point-to-multipoint service [M.5]: a simplex service from FT to PT whereby the FT transfers a single SDU of U-plane data from one source point to one (or more) destination points. The service uses the higher layer connectionless channel (protected) (SIP) logical channel: the SIP information is protected by MAC layer error detection procedure based on 16 bit CRCs.

advanced single bearer connection [M.6]: a service providing connection between FT and PT consisting of one duplex bearer. Advanced connections have a common connection number, called Exchanged Connection Number (ECN) which is assigned by the Management Entity (ME). Therefore, more than one advanced connection may exist between a PT and one FT. The service includes the means for setting-up and releasing the required bearer.

advanced multibearer connection [M.7]: a service providing connection between FT and PT consisting of one or more duplex bearers. Advanced connections have a common connection number, called ECN which is assigned by the ME. Therefore, more than one advanced connection may exist between a PT and one FT. The service includes the means for setting-up and releasing the required bearer(s).

advanced asymmetric connection [M.8]: a MAC connection that offers an asymmetric I-channel service to the DLC. An asymmetric MAC connection need to establish at least one double simplex bearer.

connection modification [M.9]: a service which allows to change the bandwidth of a connection (i.e. the number of required bearer):therefore a connection modification may switch the transmission direction of a double simplex bearer, a single bearer to a multibearer connection, an asymmetric connection to a symmetric connection and vice versa.

Ip_error_correction service [M.10]: the International Portable User Identity (IP) information is protected by MAC layer procedures based on a modulo 2 retransmission scheme. The DLC layer requests the maximum allowed transmission time. Due to the retransmission mechanism, the effective throughput is variable.

encryption activation [M.11]: a service providing means for enabling the encryption whereby on demand all higher layer data (including speech) is transferred across the AI in an encrypted form. Always initiated by the PT.

encryption deactivation [M.12]: a service providing means for disabling the encryption whereby on demand the process of transmitting higher layer data (including speech) across the AI in encrypted form is to be cancelled (a connection release automatically disables ciphering).

quality control [M.13]: provides means for monitoring and controlling the radio link quality.

physical channel selection [M.14]: defines the policy for the dynamic selection of a channel, caused by the fact that an old one has to be changed or a new one is needed. Detection of bad quality on the physical channel in use (i.e. due to weak signals or interference), detection of a Radio Fixed Part (RFP) with a stronger signal than the one of the own RFP, detection of local congestion are all criteria that can be used to select the channel.

fast connection set up [M.15]: a connection set-up initiated by a FT, without a previous paging attempt.

bearer replacement [M.16]: bearer replacement is defined to be the case where an old bearer is replaced with a new bearer that has a different Logical Bearer Number (LBN). For bearer replacement the new bearer contains independent packet numbering for IP MOD-2 protected data. The data on a new bearer may be different data or may (still) be a duplicate of the data on the old bearer.

MAC suspend [M.17]: internal MAC process where the connection are temporary suspended waiting for a MAC-resume command.

MAC resume [M.18]: internal MAC process where a suspended connection are returned to normal mode.

Cs higher layer signalling [M.19]: a low rate connection oriented data service with ARQ using the Cs channel to transfer higher layer signalling data.

extended frequency allocation [M.20]: a service which allows a FT to support frequencies in addition to the standard DECT frequencies.

bearer handover - intra-cell [M.21]: internal MAC process whereby data transfer (C channel and I channel) is switched from one duplex bearer to another in the domain of the same cell while maintaining the service to the DLC layer.

bearer handover - inter-cell [M.22]: internal MAC process whereby data transfer (C channel and I channel) is switched from one duplex bearer to another not in the domain of the same cell while maintaining the service to the DLC layer.

connection handover - intra-cell [M.23]: in the MAC layer, it is the process enabling setting up a new basic connection in the domain of the same cell to support connection handover at the DLC layer.

connection handover - inter-cell [M.24]: in the MAC layer, it is the process enabling setting up a new basic connection not in the domain of the same cell to support connection handover at the DLC layer.

Cf higher layer signalling [M.25]: provision of a fast duplex signalling channel for higher layer information with higher capacity than the Cs channel. Transmissions of CF channel data may reduce the throughput, or interrupt, the logical I channel.

6 Inter-operability requirements

6.1 General

The tables listed in this clause define all the protocol elements i.e. features, services, and procedures which are mandatory, optional, or conditional under the provision of another protocol element, or outside the scope of the present document, or in some context not applicable according to the status column designation as defined in subclause 3.3. All optional elements shall be process mandatory according to the procedures described in the present document. Based on the supported application FTs and PTs are divided into separate categories. The column HYbrid Part (HyP) is designated to the PPs that support the application feature "Distributed Communication" when they are switched in FT mode.

Protocol elements defined as mandatory, optional or conditional in this clause are further defined in clauses 8 to 15 in detail, either explicitly and/or as references to a relevant DECT standard.

A terminal that claims being compliant to MMAP shall indicate support to MMAP application(s) as defined in the following table:

Table 1: General Application support

Application	FP	PP
Voice	M	O
RS232	C100	O
WLAN	M	M

C100: IF capable of connection to voice networks THEN M ELSE O.

Annex B, D, E, F and H contain normative requirements for MMAP conformant equipment. Annexes C and G are informative and may be used as additional information, but do not mandate requirements.

In any case the requirements of EN 300 176-1 [8] shall apply. If GAP services are provided the requirements of EN 300 176-2 [9] and EN 300 444 [10] shall apply as well. If other profiles or interconnection to special networks are implemented other TBRs as appropriate may apply.

6.2 NWK features

Table 2: NWK features status

Feature supported							
Features			Status				
Item no.	Name of feature	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
N.1	Outgoing call	4.1	M	M	M	M	M
N.2	Off hook	4.1	M	M	M	M	M
N.3	On hook (full release)	4.1	M	M	M	M	M
N.4	Dialled digits (basic)	4.1	I	M	I	I	M
N.5	Register recall	4.1	I	O	O	I	O
N.6	Pause (dialling pause)	4.1	I	O	I	I	O
N.7	Incoming call	4.1	M	M	M	M	M
N.8	Authentication of PP	4.1	M	M	M	M	M
N.9	Authentication of user	4.1	M	M	M	M	M
N.10	Location registration	4.1	M	C201	C201	C201	C201
N.11	On air key allocation	4.1	M	O	O	O	O
N.12	Identification of PP	4.1	M	O	O	O	O
N.13	Service class indication/assignment	4.1	O	O	I	I	O
N.14	Alerting	4.1	M	M	M	M	M
N.15	ZAP	4.1	O	O	O	O	O
N.16	Encryption activation FT initiated	4.1	M	M	M	M	M
N.17	Subscription registration procedure on-air	4.1	M	M	M	M	M
N.18	Link control	4.1	M	M	M	M	M
N.19	Terminate access rights FT initiated	4.1	M	M	M	M	M
N.20	Partial release	4.1	O	O	O	O	O
N.21	Signalling of display characters	4.1	I	I	O	I	I
N.22	Display control characters	4.1	I	I	O	I	I
N.23	Authentication of FT	4.1	M	M	M	M	M
N.24	Encryption activation PT initiated	4.1	O	O	O	O	O
N.25	Encryption deactivation FT initiated	4.1	O	O	O	O	O
N.26	Encryption deactivation PT initiated	4.1	O	O	O	O	O
N.27	Calling Line Identification Presentation (CLIP)	4.1	O	O	O	O	O
N.28	Internal call	4.1	M	M	M	M	M
N.29	Service call	4.1	O	O	O	O	O
N.30	In call service change	4.1	M	M	M	M	M
N.31	Call Suspend & Resume	4.1	M	M	O	O	O
N.32	Service Negotiation	4.1	M	M	M	M	M

C201: IF service M.15 THEN M ELSE O.

6.3 DLC services

Table 3: DLC services status

Service supported							
Service			Status				
Item no.	Name of service	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
D.1	LAPC class A service and Lc	5.1	M	M	M	M	M
D.2	Cs channel fragmentation and recombination	5.1	M	M	M	M	M
D.3	Broadcast Lb service	5.1	M	M	M	M	M
D.4	Intra-cell voluntary connection handover	5.1	M	M	M	C301	C301
D.5	Intercell voluntary connection handover (note)	5.1	M	M	M	O	O
D.6	Encryption activation	5.1	M	M	M	M	M
D.7	Encryption deactivation	5.1	C302	C302	C302	C302	C302
D.8	U-plane handling	9.9	M	M	M	M	M
D.9	Cf channel fragmentation and recombination	5.1	M	M	M	M	M
D.10	Selection of logical channels (Cs and Cf)	5.1	M	M	M	M	M
D.11	U-plane peer to peer	9.10	M	M	M	M	M
D.12	U-plane point to multi-point	9.11	M		M	M	

C301: IF service M.9 THEN O ELSE M;
C302: IF feature N.25 OR N.26 THEN M ELSE I.

6.4 MAC services

Table 4: MAC services status

Service supported							
Service			Status				
Item no.	Name of service	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
M.1	General	5.2	M	M	M	M	M
M.2	Non continuous broadcast	5.2	O	O	O	O	O
M.3	Continuous broadcast	5.2	M	M	M	M	M
M.4	Paging broadcast	5.2	M	M	M	M	M
M.5	Higher layer connectionless U-plane point-to-multipoint service	5.2	C401	C401	C401	C401	C401
M.6	Advanced single bearer connections	5.2	M	M	M	M	M
M.7	Advanced multibearer connections	5.2	M	M	M	M	M
M.8	Advanced asymmetric connections	5.2	M	M	M	M	M
M.9	Connection modification	5.2	M	M	M	M	M
M.10	Ip_error_correction service	5.2	M	M	M	M	M
M.11	Encryption activation	5.2	M	M	M	M	M
M.12	Encryption deactivation	5.2	C402	C402	C402	C402	C402
M.13	Quality control	5.2	M	M	M	M	M
M.14	Physical channel selection	5.2	M	M	M	M	M
M.15	Fast connection set up	5.2	O	O	M	M	M
M.16	Bearer replacement	5.2	M	M	M	M	M
M.17	MAC suspend	5.2	M	M	M	M	M
M.18	MAC resume	5.2	M	M	M	M	M
M.19	Cs higher layer signalling	5.2	M	M	M	M	M
M.20	Extended frequency allocation (note)	5.2	M	M	M	O	O
M.21	Bearer Handover, intra-cell	5.2	M	M	M	C403	C403
M.22	Bearer Handover, inter-cell	5.2	M	M	M	O	O
M.23	Connection Handover, intra-cell	5.2	M	M	M	C404	C404
M.24	Connection Handover, inter-cell	5.2	M	M	M	O	O
M.25	Cf higher layer signalling	5.2	C402	C402	C402	C402	C402

C401: In case of wireless LAN M otherwise I;
C402: IF feature D.9 THEN M ELSE I;
C403: IF feature M.23 THEN M ELSE I;
C404: IF feature M.21 THEN M ELSE I;

6.5 Physical (PHL) layer services

See PHL layer requirements, clause 13.

6.6 Application features

Table 5: Application features status

Feature supported							
Feature			Status				
Item no.	Name of feature	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
A.1	AC_bitstring_mapping	4.2	M	M	M	M	M
A.2	Multiple subscription registration	4.2	M	M	M	N/A	N/A
A.3	Manual entry of the PARK	4.2	O	O	O	N/A	N/A
A.4	HyP (Distributed Communication)	4.2	M	O	M	M	O

6.7 NWK feature to procedure mapping

Table 6: NWK feature to procedure mapping

Feature/Procedure mapping							
Feature/Procedure			Status				
Feature Name	Procedure name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
N.1 Outgoing call		4.1	M	M	M	M	M
	Outgoing call request	8.2	M	M	M	M	M
	Overlap sending	8.3	M	M	O	O	O
	Outgoing call proceeding	8.4	M	M	O	O	O
	Outgoing call confirmation	8.5	M	M	O	O	O
	Outgoing call connection	8.6	M	M	M	M	M
	Sending keypad information	8.10	M	M	M	M	M
N.2 Off Hook		4.1	M	M	M	M	M
	Outgoing call request	8.2	M	M	M	M	M
	Incoming call connection	8.15	M	M	M	M	M
N.3 On Hook (full release)		4.1	M	M	M	M	M
	Normal call release	8.7	M	M	M	M	M
	Abnormal call release	8.8	M	M	M	M	M
N.4 Dialled digits (basic)		4.1	M	M	M	M	M
	Sending keypad information	8.10	M	M	M	M	M
N.5 Register recall		4.1	M	M	O	O	O
	Sending keypad information	8.10	M	M	M	M	M
N.6 Pause (dialling pause)		4.1	M	M	O	O	O
	Sending keypad information	8.10	M	M	M	M	M
N.7 Incoming call		4.1	M	M	M	M	M
	Incoming call request	8.12	M	M	M	M	M
	Incoming call confirmation	8.13	M	M	M	M	M
	PT alerting	8.14	M	M	M	M	M
	Incoming call connection	8.15	M	M	M	M	M
N.8 Authentication of the PP		4.1	M	M	M	M	M
	Authentication of PT	8.24	M	M	M	M	M
N.9 Authentication of the user		4.1	M	M	O	O	O
	Authentication of user	8.25	M	M	M	M	M
N.10 Location registration		4.1	M	M	M	M	M
	Location registration	8.28	M	M	M	M	M
	Location update	8.29	M	M	O	O	O
N.11 On air key allocation		4.1	M	M	O	O	O
	Key allocation	8.32	M	M	M	M	M
N.12 Identification of PP		4.1	M	M	O	O	O
	Identification of PT	8.22	M	M	M	M	M
N.13 Service class indication/assignment		4.1	M	M	O	O	M
	Obtaining access rights	8.30	M	M	M	M	M
	Authentication of PT	8.24	M	M	M	M	M
N.14 Alerting		4.1	M	M	M	M	M
	PT alerting	8.14	M	M	M	M	M
N.15 ZAP		4.1	M	M	O	O	O
	Obtaining access rights	8.30	M	M	M	M	M
	Incrementing the ZAP value	8.26	M	M	M	M	M
	Authentication of FT	8.23	O	O	M	M	M
N.16 Encryption activation FT initiated		4.1	M	M	M	M	M

Feature/Procedure mapping							
Feature/Procedure			Status				
Feature Name	Procedure name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
	Cipher-switching initiated by FT	8.33	M	M	M	M	M
	Storing the Derived Cipher Key (DCK)	8.27	M	M	M	M	M
N.17 Subscription registration user procedure on-air		4.1	M	M	M	M	M
	Obtaining access rights	8.30	M	M	M	M	M
N.18, Link control		4.1	M	M	M	M	M
	Indirect FT initiated link establishment	8.35	M	M	M	M	M
	Normal Paging		M	M	M	M	M
	Fast Paging		C601	C601	C602	C602	C602
	Direct FT initiated link establishment	8.35	M	M	M	M	M
	Direct PT initiated link establishment	8.36	M	M	M	M	M
	Link release "normal"	8.37	M	M	M	M	M
	Link release "abnormal"	8.38	M	M	M	M	M
	Link release "maintain"	8.39	M	M	M	M	M
	Link suspend		M	M	M	M	M
	Link resume		M	M	M	M	M
N.19 Terminate access rights FT initiated		4.1	M	M	O	O	O
	FT terminating access rights	8.31	M	M	M	M	M
	Authentication of FT	8.23	O	O	M	M	M
N.20, Partial release		4.1	O	O	O	O	O
	Partial release	8.9	M	M	M	M	M
N.21, Signalling of display characters		4.1	O	O	O	O	O
	Display	8.16	M	M	M	M	M
	Terminal capability indication	8.17	M	M	M	M	M
N.22, Display control characters		4.1	O	O	O	O	O
	Display	8.16	M	M	M	M	M
	Terminal capability indication	8.17	M	M	M	M	M
N.23, Authentication of FT		4.1	O	O	O	O	O
	Authentication of FT	8.23	M	M	M	M	M
N.24, Encryption activation PT initiated		4.1	O	O	O	O	O
	Cipher-switching initiated by PT	8.34	M	M	M	M	M
	Storing the DCK	8.27	M	M	M	M	M
N.25, Encryption deactivation FT initiated		4.1	O	O	O	O	O
	Cipher-switching initiated by FT	8.33	M	M	M	M	M
N.26, Encryption deactivation PT initiated		4.1	O	O	O	O	O
	Cipher-switching initiated by PT	8.34	M	M	M	M	M
N.27, Calling Line Identification Presentation (CLIP)		4.1	O	O	O	O	O
	Incoming call request	8.12	M	M	M	M	M
N.28, Internal call		4.1	O	O	O	O	O
	Internal call set-up	8.18	M	M	M	M	M
	Internal call keypad	8.19	O	O	O	O	O

Feature/Procedure mapping							
Feature/Procedure			Status				
Feature Name	Procedure name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
N.29, Service call		4.1	O	O	O	O	O
	Service call set-up	8.20	M	M	M	M	M
	Service call keypad	8.21	O	O	O	O	O
N.30, In call service change		4.1	M	M	M	M	M
	Bandwidth Change		M	M	M	M	M
	Connection Reversal						
N.31, Call Suspend and Resume		4.1	M	O	O	O	O
	Suspend		M	M	M	M	M
	Resume		M	M	M	M	M
N.32, Service Negotiation		4.1	M	M	M	M	M
	Selection of lower layer resources		M	M	M	M	M
	Peer attribute negotiation		M	M	M	M	M
	Operation parameter negotiation		O	O	O	O	O

C601: IF Fast paging at MAC THEN M ELSE X;
C602: IF PT Fast paging THEN O ELSE X;

6.8 Service to procedure mapping

6.8.1 DLC service to procedure mapping

Table 7: DLC service to procedure mapping

Service/Procedure mapping							
Service/Procedure			Status				
Service Name	Procedure Name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
D.1 LAPC class A service and Lc		5.1	M	M	M	M	M
	Class A PT initiated link establishment	9.1	M	M	M	M	M
	Class A FT initiated link establishment	9.2	M	M	M	M	M
	Class A acknowledged information transfer	9.2	M	M	M	M	M
	Class A link release	9.3	M	M	M	M	M
	Class A link re-establishment	9.4	M	M	M	M	M
	Connection modification		M	M	M	M	M
D.2 Cs channel fragmentation and recombination		5.1	M	M	M	M	M
	Cs channel fragmentation and recombination	9.5	M	M	M	M	M
D.3 Broadcast Lb service		5.1	M	M	M	M	M
	Normal broadcast	10.1	M	M	M	M	M
	Expedited broadcast	10.2	C703	C703	C704	C704	C704
D.4 Intra-cell voluntary connection handover		5.1	M	M	C701	C701	C701
	Class A basic connection handover	9.7	M	M	M	M	M

Service/Procedure mapping							
Service/Procedure			Status				
Service Name	Procedure Name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
D.5 Inter-cell voluntary connection handover		5.1	M	M	O	O	O
	Class A basic connection handover	9.7	M	M	M	M	M
D.6 Encryption activation		5.1	M	M	M	M	M
	Encryption switching	9.8	M	M	M	M	M
D.7 Encryption deactivation		5.1	C702	C702	C702	C702	C702
	Encryption switching	9.8	M	M	M	M	M
D.8 U-plane handling		9.9	M	M	M	M	M
	LU2 Frame RELay service		M	M	M	M	M
	Checksum operation		M	M	M	M	M
	Segmentation and transmission class		M	M	M	M	M
	Data transmission		M	M	M	M	M
	FU6		M	M	M	M	M
D.11 U-plane peer to peer		9.10					
	Ip_error_detection with selective retransmission protocol (SEL)		M	M	M	M	M
	Frame transmission		M	M	M	M	M
	Flow Control		M	M	M	M	M
D.12 U-plane point to multi-point		9.11					
	U-plane point to multi - point procedures		M		M	M	

C701: IF service M.9 THEN O ELSE M;
C702: IF feature N.29 OR N.28 THEN M ELSE I;
C703: IF Fast paging at MAC THEN M ELSE X;
C704: IF PT Fast paging THEN O ELSE X.

6.8.2 MAC service to procedure mapping

Table 8: MAC service to procedure mapping

Service/Procedure mapping							
Service/Procedure			Status				
Service Name	Procedure Name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
M.1 General							
	Bit MAPpings (MAP)	6.2.1	M	M	M	M	M
	Time multiplexes	6.2.2	M	M	M	M	M
	Scrambling	6.2.4	M	M	M	M	M
	Error control	6.2.5	M	M	M	M	M
	PP states and state transitions	11.3	M	M	M	M	M
	RFP idle receiver scan sequence	11.8	M	M	M	M	M
M.2 Non continuous broadcast							
	Request for specific Q-channel information	9.3.1.2	O	O	O	O	O
	Request for a new dummy	9.3.2	M	M	M	M	M
	Non continuous broadcast	9.3	M	M	M	M	M
	Extended system information	11.2	M	M	M	M	M
M.3 Continuous broadcast							
	Downlink broadcast	9.1.1	M	M	M	M	M

Service/Procedure mapping							
Service/Procedure			Status				
Service Name	Procedure Name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
M.4 Paging broadcast							
	Low duty cycle paging		O	O	O	O	O
	Normal paging	9.1.3	M	M	M	M	M
	Fast paging	9.1.3	O	O	M	M	M
M.5 Higher layer connectionless U-plane point-to-multipoint service							
	Downlink connectionless	9.1.2	M	M	M	M	M
M.6 Advanced single bearer connections							
	C/O connection set-up	10.2	M	M	M	M	M
	C/O connection release	10.4	M	M	M	M	M
	C/O bearer set-up	10.5	M	M	M	M	M
	C/O bearer release	10.7	M	M	M	M	M
M.7 Advanced multibearer connections							
	C/O connection set-up	10.2	M	M	M	M	M
	C/O connection release	10.4	M	M	M	M	M
	C/O bearer set-up	10.5	M	M	M	M	M
	C/O bearer release	10.7	M	M	M	M	M
M.8 Advanced asymmetric connections							
	C/O connection set-up	10.2	M	M	M	M	M
	C/O connection release	10.4	M	M	M	M	M
	C/O bearer set-up	10.5	M	M	M	M	M
	C/O bearer release	10.7	M	M	M	M	M
M.9 Connection modification							
	Connection modification	10.3	M	M	M	M	M
M.10 lp_error_correction service							
	MOD-2 protected I-channel operation (lp)	10.8.2	M	M	M	M	M
M.11 Encryption activation							
	Encryption process - initialization and synchronization		M	M	M	M	M
	Encryption mode control		M	M	M	M	M
	Encryption (features 33 and 34)		M	M	M	M	M
	Encryption mode control		M	M	M	M	M
M.13 Quality control							
	RFPI handshake		M	M	M	M	M
	PT frequency correction procedure		O	O	O	O	O
	Bearer and connection quality control		O	O	O	O	O
M.14 Physical channel selection			M	M	M	M	M
	Physical channel selection		M	M	M	M	M
M.15 Fast connection set-up							
	C/O connection set-up		M	M	M	M	M
	C/O connection release		M	M	M	M	M

Service/Procedure mapping							
Service/Procedure			Status				
Service Name	Procedure Name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
	C/O bearer set-up		M	M	M	M	M
	C/O bearer release		M	M	M	M	M
	PT fast set-up receiver scan sequence		M	M	M	M	M
M.16 Bearer replacement							
	Bearer replacement		M	M	M	M	M
M.17 MAC suspend							
	C/O connection release		M	M	M	M	M
M.18 MAC resume							
	C/O connection set-up		M	M	M	M	M
	C/O bearer set-up		M	M	M	M	M
M.19 Cs higher layer signalling							
	Cs channel data		M	M	M	M	M
	Q2 bit setting		M	M	M	M	M
M.20 Extended frequency allocation		5.2	M	M	O	O	O
	Extended frequency allocation		M	M	O	O	O
M.21 Bearer handover, intra-cell			M	M	C01	C01	C01
	Bearer handover request		M	M	M	M	M
M.22 Bearer handover, inter-cell			M	M	O	O	O
	Bearer handover request		M	M	M	M	M
M.23 Connection handover, intra-cell			M	M	C02	C02	C02
	Connection handover request		M	M	M	M	M
M.24 Connection handover, inter-cell			M	M	O	O	O
	Connection handover request		M	M	M	M	M
M.25 Cf higher layer signalling			M	M	M	M	M
	Cf channel data		M	M	M	M	M
	Q2 bit setting		M	M	M	M	M

C801: IF service M.23 THEN O ELSE M;

C802: IF service M.21 THEN O ELSE M;

6.8.3 Application feature to procedure mapping

Table 9: Application feature to procedure mapping

Feature/Procedure mapping							
Feature/Procedure			Status				
Feature Name	Procedure name	Ref.	PT		FT		
			WLAN	RS323	HyP	WLAN	RS232
A.1 AC to bitstring mapping		4.2	M	M	M	M	M
	AC to bitstring mapping	14.2	M	M	M	M	M
A.2 Multiple subscription registration		4.2	M	M	N/A	N/A	N/A
	Subscription control	14.1	M	M	N/A	N/A	N/A
A.3 Manual entry of the PARK		4.2	O	O	N/A	N/A	N/A
	Manual entry of the PARK	14.3	M	M	N/A	N/A	N/A
A.4 HyP							
	Voluntary distributed communication		M	M	M	M	M
	Involuntary distributed communication		M	M	M	M	M

6.8.4 Management procedures

Table 10: Application feature to procedure mapping

Feature/Procedure mapping						
Procedure		Status				
Procedure name	Ref.	PT		FT		
		WLAN	RS323	HyP	WLAN	RS232
Management of MM procedures	13.1	M	M	M	M	M
Location registration initiation management	13.2	M	M	M	M	M
Assigned individual TPUI management	13.4	M	M	M	M	M
PMID management	13.5	M	M	M	M	M
DCK management	13.6	M	M	M	M	M
Broadcast attributes management	13.7	M	M	M	M	M
Storage of subscription related data management	13.8	M	M	M	M	M
Link resource management	13.9	M	M	M	M	M
NWK layer Suspend and Resume management	13.10	M	M	M	M	M
MAC layer Suspend and Resume management	13.11	M	M	M	M	M

6.9 General requirements

6.9.1 NWK layer message contents

All reserved single bits shall be set to 0.

6.9.2 Transaction identifier

The transaction identifier value for a CC call shall always get assigned the lowest available free number.

6.9.3 Length of a NWK layer message

PP and the FP shall be capable of receiving and processing NWK layer messages of at least 63 octets long. All mandatory information elements as defined in the present document shall be included in the first 63 octets.

This requires only one DLC segment to be supported as mandatory. The DLC shall convey the first segment of a layer 3 message to the NWK layer. Additional segments of a layer 3 message may be discarded by the receiving side.

6.9.4 Handling of error and exception conditions

In general the requirements as specified in EN 300 175-5 [4] clause 17 shall apply.

If a Mobility Management (MM) message, requesting initiation of a MM procedure, is received in a CC state where the receiving entity is not required to support it and does not support it, this message shall be ignored.

Whenever an unrecognized message is received in any CC state, the message shall be ignored.

When normal release shall be initiated to handle error and exceptional condition, the normal release procedure as described in subclause 8.6 shall be invoked. The {CC-RELEASE} message may not include <<Release reason>> information element.

The usage of a reserved value in an information element field shall not by itself constitute an error. The receiver of such a value shall process the value if it understands it or shall ignore it otherwise.

6.9.5 Coexistence of MM and CC procedures

The following table describes whether an MM procedure is supported in any CC state or whether a restriction applies. The restriction has been made in order to limit the complexity of the receiving side so that it is not mandated to understand MM messages in all CC states for the purpose of achieving inter-operability.

Table 11: Support of MM procedures in CC states

Procedure	Mandatory support in CC state
Identification of PT	All states
Authentication of FT	All states
Authentication of PT	All states
Authentication of user	All states
Location registration	All states
Location update	All states
Obtaining access rights	T(F)-00
FT terminating access rights	F(T)-00, T-01, T-10
Key allocation	F(T)-00
Cipher-switching initiated by FT	All states
Cipher switching initiated by PT	All states
Detach	F(T)-00, Note
Temporary Identity Assign	F(T)-00, Note
NOTE: Detach and Temporary Identity Assign shall only be supported if HyP is supported.	

The CC and MM entities may work independently one from the other. If a FT decides to perform a MM procedure prior to proceeding with a PT initiated CC procedure, the FT has the rights to restart the CC timers in the PT to prevent the CC state machine from waiting on a response delayed because of the MM procedure execution. For this purpose the FT may send a {CC-NOTIFY} message. The support of this message is mandatory for the PT and optional for the FT. The {CC-NOTIFY} shall include the <<TIMER-RESTART>> information element. A MM procedure started when a call has been suspended shall lead to resumption of the call.

6.9.6 Coding rules for information elements

For mandatory information elements, at least the first octet within any octet group shall be present. It is not permitted to use the information element field <Length of Contents> to omit an octet group. However, if explicitly stated a mandatory information element may contain zero length contents.

6.9.7 Mode of operation

Portable Part and Fixed Part CC entities shall use circuit switched mode procedures.

7 Procedure description

The following clauses define the process mandatory procedures which are in the scope of the MMAP. Each procedure (if appropriate) is divided into three parts:

a) normal (i.e. successful) case(s). This part defines the functions and respective protocol element values in normal operation;

b) associated procedure(s). This is an integral part of the actual procedure (if defined in the present document) i.e. if a procedure is being declared to be supported, the respective entity shall also support the associated procedures, e.g. timer management, in the subclause following the description of the normal case;

c) exceptional case(s). This is an integral part of the actual procedure (if defined in the present document) i.e. if a procedure is being declared to be supported, the respective entity shall also support the exception handling defined in the subclause following the description of the normal case.

All protocol elements listed in the following clauses are process mandatory i.e. the FT and PT depending on their role in the procedure shall send or shall receive and process the relevant protocol elements as listed in the respective tables if not explicitly stated as being optional.

The primitives used in procedure descriptions are defined only for the purpose of describing layer-to-layer interactions. The primitives are defined as an abstract list of parameters, and their concrete realization may vary between implementations. No formal testing of primitives is intended. The primitive definitions have no normative significance.

8 NWK layer procedures

This clause specifies the NWK layer procedures, messages and information elements required in MMAP. When an MMAP device is used for 3,1 kHz telephony applications the requirements as specified in EN 300 444 [10] and other relevant standards shall apply.

This profile does not prevent any PT or FT from transmitting or receiving and processing any other NWK layer message or information element not specified in the profile. A PT or FT receiving an unsupported NWK layer message or information element which it does not recognize shall ignore it, as specified in EN 300 175-5 [4], clause 17.

8.1 Outgoing call request

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 9.3.1, 9.3.1.1, 9.3.1.2, 9.3.1.3 and 15.2.5. Figure 1 and table 12 together with the associated subclauses define the mandatory requirements with regard to the present document.

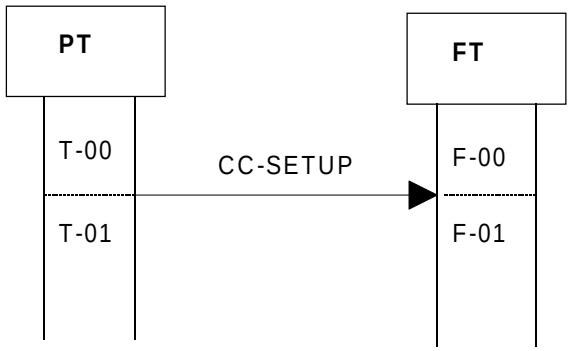


Figure 1: Outgoing call request

Table 12: Values used within the {CC-SETUP} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable identity>>			
	<Type>	0	International Portable User Identity (IPUI)
	<PUT>	All	Area dependent
	<PUN>	All	Area dependent
<<Fixed Identity>>			Shall always include the whole PARK including the non significant bits.
	<Type>	32	PARK
	<Length of identity value>	All	PARK Length Indicator (PLI)+1
	<ARC+ARD>	All	Area dependent
<<Basic service>>			
	<Call class>	8	Normal call set-up
		9	Relates to feature internal call N.28. For the associated procedure (see subclause 8.16).
		11	Relates to feature service call N.29. For the associated procedure (see subclause 8.18).
	<Basic service>	"1111"	Other
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

8.1.1 Associated procedures

8.1.1.1 Timer P-<CC.03> management

<CC.03>: CC set-up timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-SETUP} message has been sent;

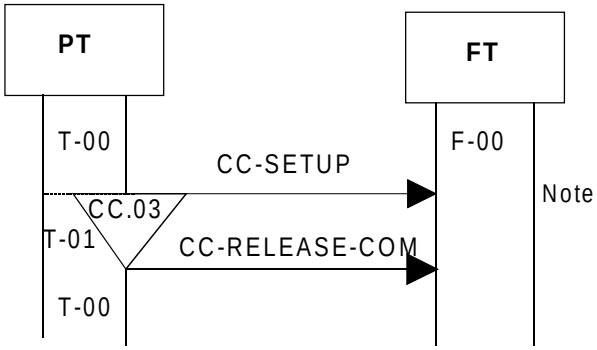
Stop: An indication for release or reject from the IWU or for link release from the DLC layer is received. A {CC-SETUP-ACK}, {CC-CONNECT} or {CC-RELEASE-COM} message is received;

Restart: FT may restart it at any time by sending a {CC-NOTIFY} message, (see subclause 6.9.5).

8.1.2 Exceptional cases

8.1.2.1 Timer P-<CC.03> expiry

The abnormal call release procedure shall be used, (see subclause 8.7).



NOTE: FT may not be answering because of some FT problems or because the {CC-SETUP} message has been lost or corrupted. The same result will occur if the eventual FT answer has been lost or corrupted.

Figure 2: Timer P<CC.03> expiry

For the values used within the {CC-SETUP} see table 12. For the contents of {CC-RELEASE-COM} message, see table 19.

8.1.2.2 PT releases the outgoing call request

The normal call release procedure shall be used, (see subclause 8.6).

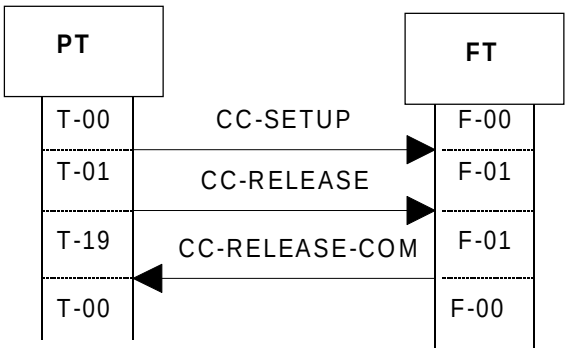
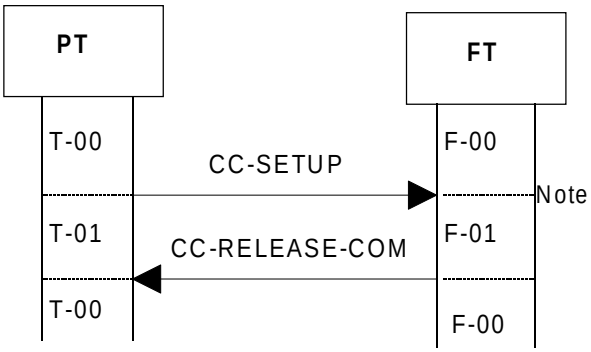


Figure 3: PT releases the outgoing call request

For the values used within {CC-SETUP} see table 12. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.1.2.3 FT rejects the outgoing call request

The abnormal call release procedure shall be used, (see subclause 8.7).



NOTE: Either F-CC or the F-IWU may reject the call.

Figure 4: FT rejects the outgoing call request

For the contents of {CC-RELEASE-COM} see table 19.

The contents of an unacceptable {CC-SETUP} is outside the scope of the present document.

8.2 Overlap sending

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 9.3.1.5, 9.3.1.4 and 15.2.5. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Both PT and FT shall support piecewise dialling using the <<MULTI-KEYPAD>> information element.

NOTE: A single <<MULTI-KEYPAD>> information element may contain the complete dialling information.

PP shall ensure that dialling information is sent after the {CC-SETUP-ACK} has been received to prevent expiry of timer F-<CC.01> at the FT side. The interpretation of the dialling information depends on the type of FT and the local network it is connected to.

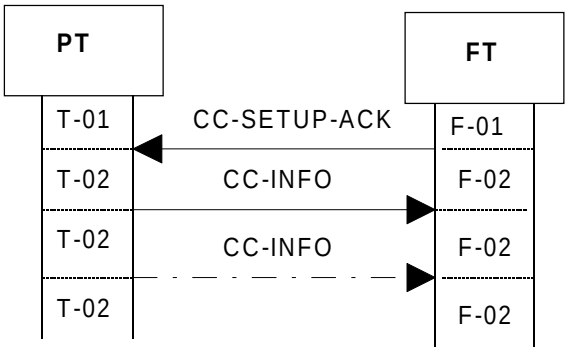


Figure 5: Overlap sending

Table 13: Values used within the {CC-SETUP-ACK} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Progress indicator>>			
	<Progress description>	8H	"In band information or appropriate pattern now available". Inclusion of this information element is optional, but if it is present, PT shall connect the U-plane
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

For the values used in {CC-INFO} see table 22.

8.2.1 Associated procedure

8.2.1.1 Timer F-<CC.01> management

<CC.01>: Overlap sending timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-SETUP-ACK} has been sent;

Stop: Change of the CC state occurs;

Restart: A {CC-INFO} message has been received.

8.2.2 Exceptional cases

8.2.2.1 PT releases the outgoing call request

The normal call release procedure shall be used, (see subclause 8.7).

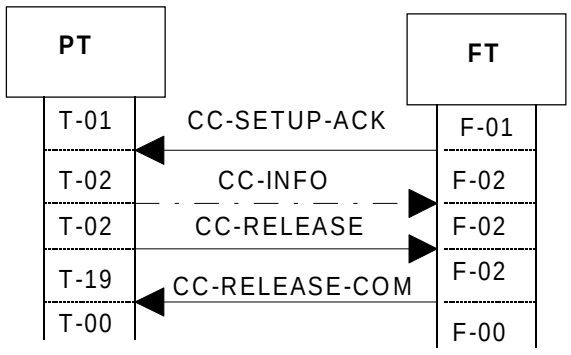
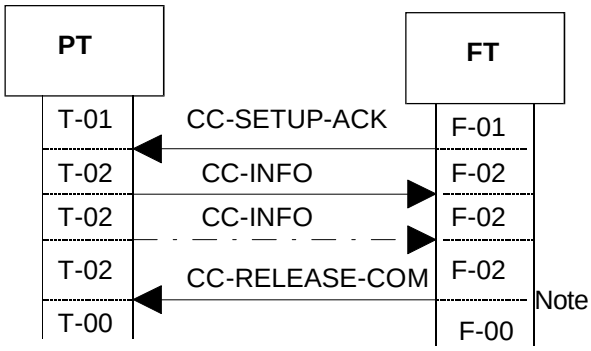


Figure 6: PT release the outgoing call request

For the values used within the {CC-SETUP-ACK} see table 13. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.2.2.2 FT rejects the outgoing call request

The abnormal release procedure shall be used, (see subclause 8.7).



NOTE: Either F-CC or F-IWU may reject the call.

Figure 7: FT rejects the outgoing call request

For the contents of {CC-SETUP-ACK} see table 13.

The contents of an unacceptable {CC-INFO} message is outside the scope of the present document.

For the contents of {CC-RELEASE-COM} see table 19.

8.2.2.3 Timer F-<CC.01> expiry

The normal release procedure shall be used, (see subclause 8.6).

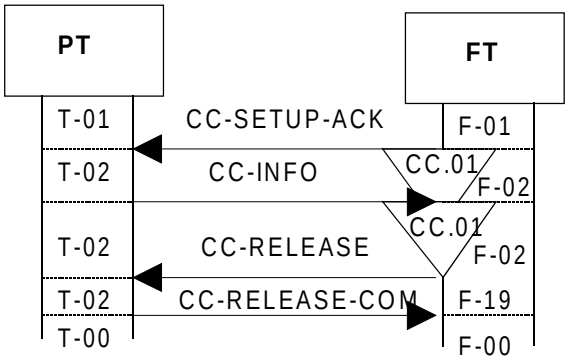


Figure 8: Timer F<CC.01> expiry

For the values used within the {CC-SETUP-ACK} see table 13. For {CC-INFO} (if any has been sent) see table 22. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.2.2.4 FT releases the outgoing call request

The normal release procedure shall be used, (see subclause 8.6).

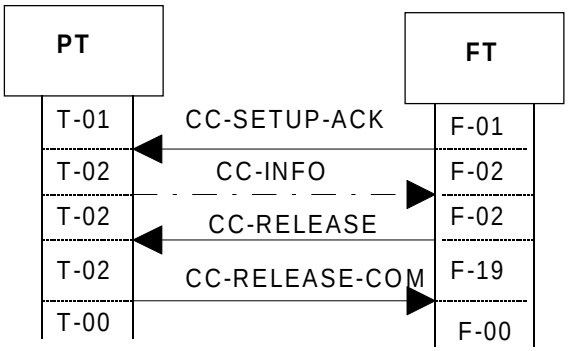


Figure 9: FT releases the outgoing call request

For the values used within the {CC-SETUP-ACK} see table 13. For {CC-INFO} (if any has been sent) see table 22. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.3 Outgoing call proceeding

The procedure shall be performed as defined in subclauses 9.3.1.6 and 9.3.1.4 of EN 300 175-5 [4]. Figure 10 and table 14 together with the associated subclauses define the mandatory requirements with regard to the present document.

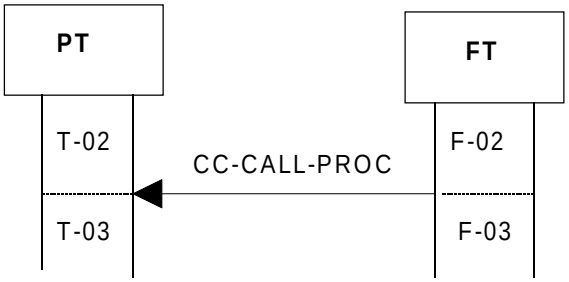


Figure 10: Outgoing call proceeding

Table 14: Values used within the {CC-CALL-PROC} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Progress indicator>>			
	<Progress description>	8H	"In band information or appropriate pattern now available". Inclusion of this information element is optional, but if it is present, PT shall connect the U-plane
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

8.3.1 Exceptional cases

8.3.1.1 PT releases the outgoing call request

The normal release procedure shall be used, (see subclause 8.6).

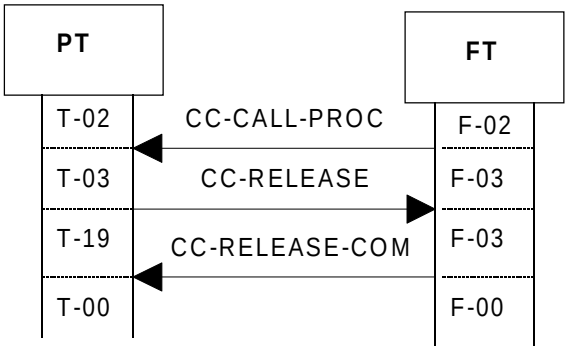


Figure 11: PT releases the outgoing call request

For the values used within the {CC-CALL-PROC} see subclause 8.3, table 14. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see subclause 8.6, tables 17 and 18.

8.3.1.2 FT releases the outgoing call request

The normal release procedure shall be used, (see subclause 8.6).

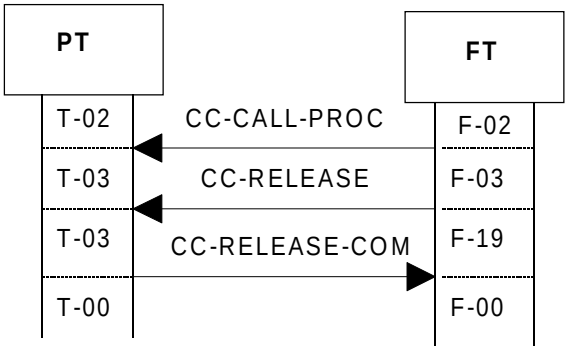


Figure 12: FT releases the outgoing call request

For the values used within the {CC-CALL-PROC} see subclause 8.3, table 14. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see subclause 8.6, tables 17 and 18.

8.4 Outgoing call confirmation

The procedure shall be performed as defined in subclauses 9.3.1.7 and 9.3.1.4 of EN 300 175-5 [4]. Figure 13 and table 15 together with the associated subclauses define the mandatory requirements with regard to the present document.

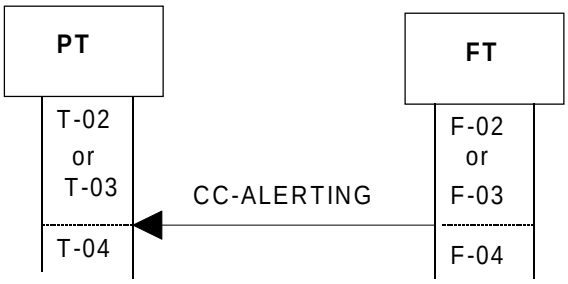


Figure 13: Outgoing call confirmation

Table 15: Values used within the {CC-ALERTING} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Progress indicator>>			
	<Progress description>	8H	"In band information or appropriate pattern now available". Inclusion of this information element is optional, but if it is present, PT shall connect the U-plane
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

8.4.1 Exceptional cases

8.4.1.1 PT releases the outgoing call request

The normal release procedure shall be used, (see subclause 8.6).

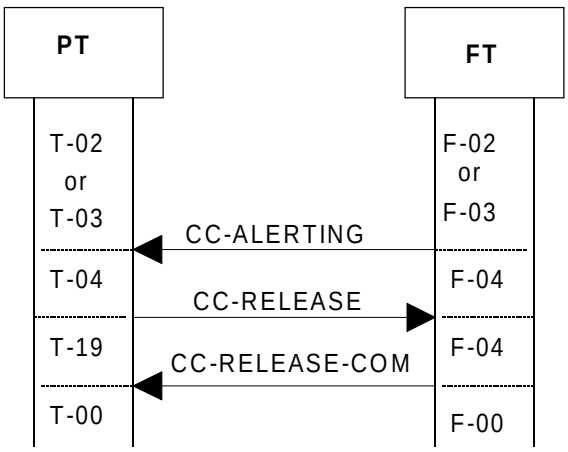


Figure 14: PT releases the outgoing call request

For the values used within the {CC-ALERTING} see table 15. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.4.1.2 FT releases the outgoing call request

The normal release procedure shall be used, (see subclause 8.6).

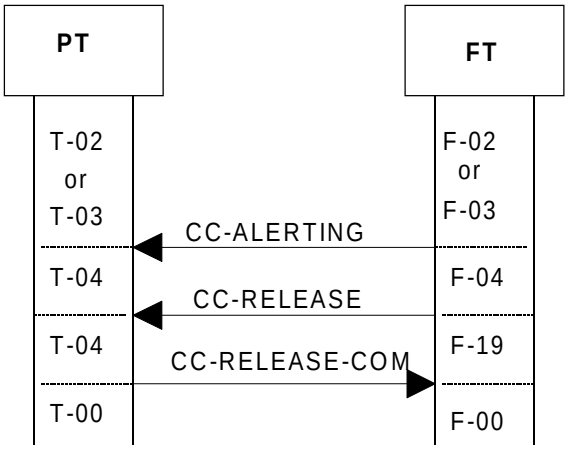


Figure 15: FT releases the outgoing call request

For the values used within the {CC-ALERTING} see table 15. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.5 Outgoing call connection

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 9.3.1.8 and 9.3.1.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Before sending the {CC-CONNECT} message the FT shall connect the U-plane. On receipt of {CC-CONNECT} message the PT shall connect the U-plane.

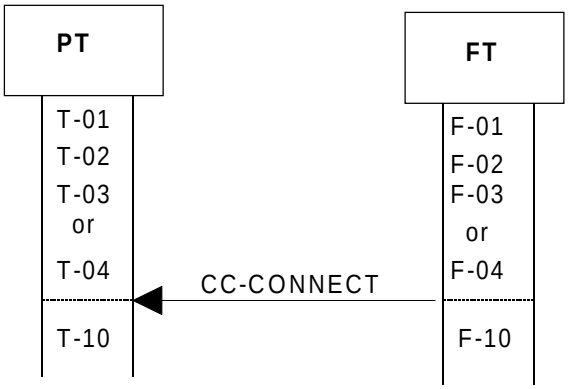


Figure 16: Outgoing call connection

Table 16: Values used within the {CC-CONNECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

8.6 Normal call release

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 9.5.1 and 9.5.3. Figures 17 and 18, and table 17 together with the associated subclauses define the mandatory requirements with regard to the present document.

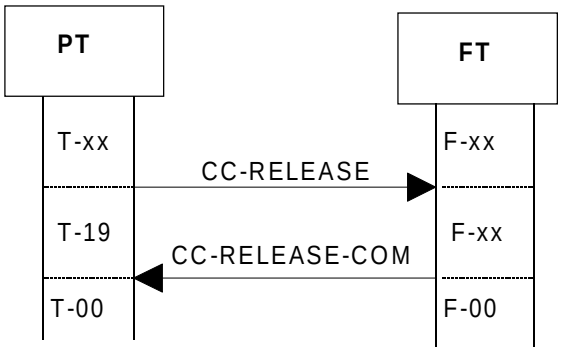


Figure 17: Normal call release, PT initiated

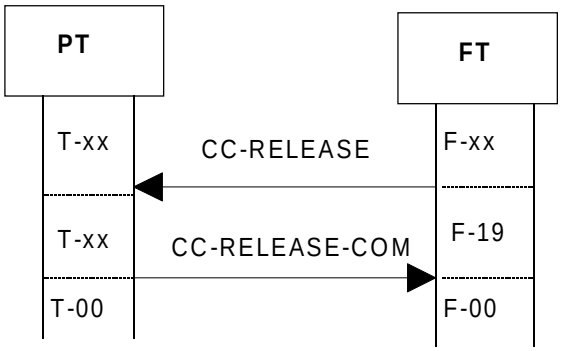


Figure 18: Normal call release, FT initiated

The PT is allowed to initiate this procedure in any state except T-00, T-06 and T-19.

The FT is allowed to initiate this procedure in any state except F-00, F-01 and F-19.

Table 17: Values used within the {CC-RELEASE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

Table 18: Values used within the {CC-RELEASE-COM} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

8.6.1 Associated procedures

8.6.1.1 Timer P-<CC.02> management

<CC.02>: CC release timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-RELEASE} message has been sent;

Stop: An indication for link release from the DLC layer is received.
A {CC-RELEASE-COM} or a {CC-RELEASE} message is received;

Restart: FT may restart it at any time by sending a {CC-NOTIFY} message, (see subclause 6.9.5).

8.6.1.2 Timer F-<CC.02> management

<CC.02>: CC release timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-RELEASE} message has been sent;

Stop: An indication for link release from the DLC layer is received.
A {CC-RELEASE-COM} or a {CC-RELEASE} message is received.

8.6.2 Exceptional cases

8.6.2.1 Release collisions

A release collision occurs when both sides send {CC-RELEASE} at the same time or a {CC-RELEASE} message has been received when the receiver is in "RELEASE PENDING" state due to loss of the first sent {CC-RELEASE} message.

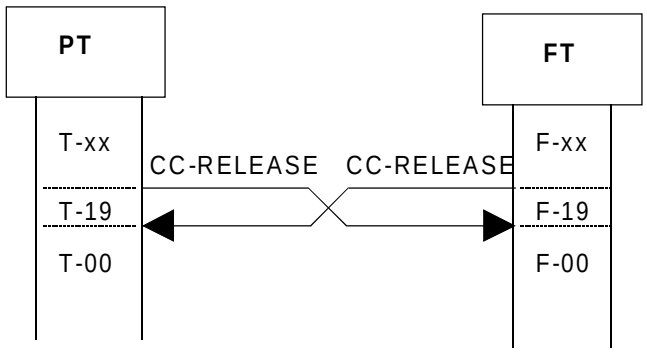


Figure 19: Both sides send {CC-RELEASE}

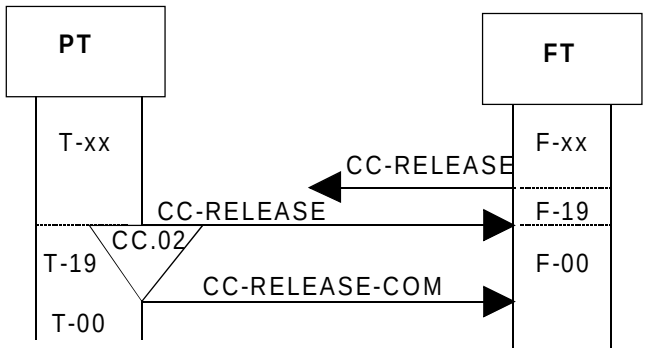
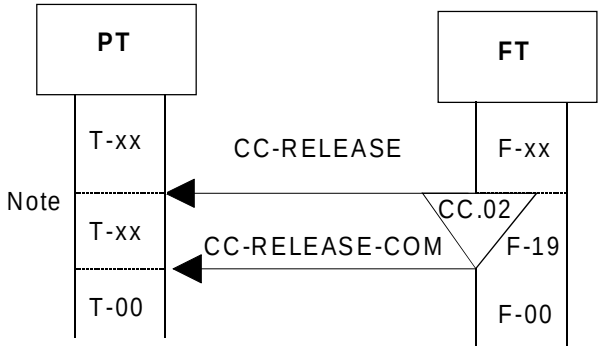


Figure 20: The {CC-RELEASE} sent by the FT has been lost

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} see tables 17 and 18.

8.6.2.2 Timer F-<CC.02> expiry

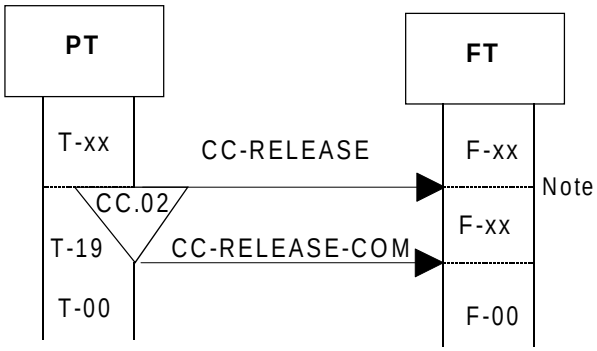


NOTE: PT may not be answering because of some PT problems or the {CC-RELEASE} sent by the FT or the eventual {CC-RELEASE-COM} message sent by the PT has been lost or corrupted.

Figure 21: Timer F<CC.02> expiry

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.6.2.3 Timer P-<CC.02> expiry



NOTE: FT may not be answering because of some FT problems or the {CC-RELEASE} sent by the PT or the eventual {CC-RELEASE-COM} message sent by the FT has been lost or corrupted.

Figure 22: Timer P<CC.02> expiry

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.7 Abnormal call release

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 9.5.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The abnormal release is indicated by the unexpected receipt of a {CC-RELEASE-COM} message without a prior transmission of a {CC-RELEASE} message.

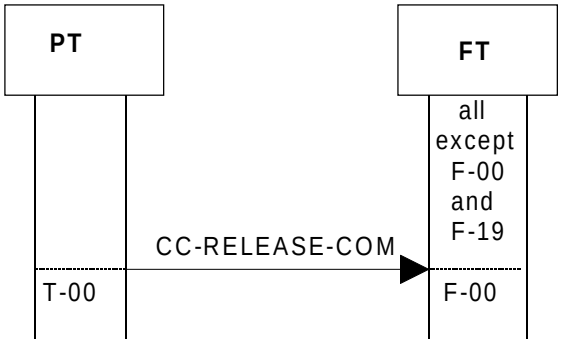


Figure 23: Abnormal call release, PT initiated

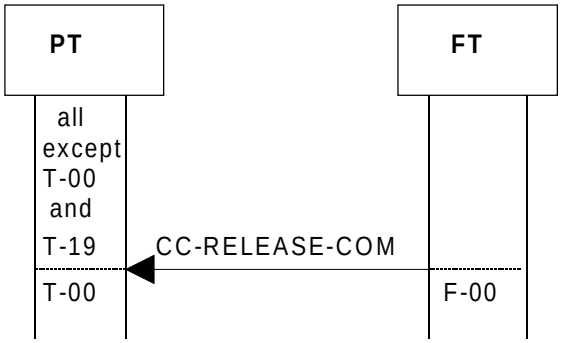


Figure 24: Abnormal call release, FT initiated

Table 19: Values used within the {CC-RELEASE-COM} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

8.8 Partial release

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 14.2.7. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If a "partial release" has been indicated in the <<Release reason>> information element in the {CC-RELEASE} message (implying that a follow-on call activities are expected), both the requesting and the requested CC (if the requested CC supports the feature N.21 as well) shall request a delayed link release from the Link Control Entity (LCE). In this event the link shall be retained for a few seconds (timer <LCE.02>) as it is described in subclause 8.39.

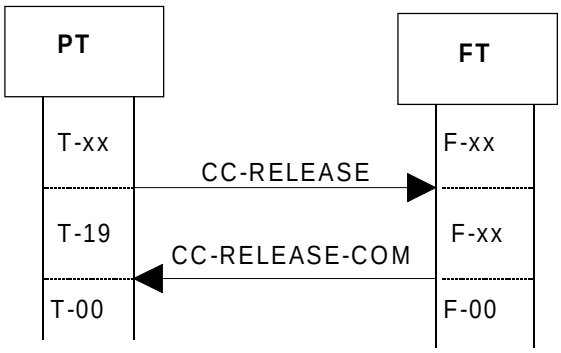


Figure 25: Partial release, PT initiated

Table 20: Values used within the {CC-RELEASE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Release reason>>	<Release reason code>	0EH	Partial release.

Table 21: Values used within the {CC-RELEASE-COM} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Release reason>>	<Release reason code>	0EH	Always shall be included if the "partial release" has been requested, (see table 20), and if the requested side supports feature N.21.

The case when the FT initiates this procedure differs only in the notation.

8.9 Sending keypad information

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 10.2, 9.3.1.5 and 9.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The PT shall be capable of sending keypad information which shall be included in the <<MULTI-KEYPAD>> information element in one or several {CC-INFO} messages. The PT and the FT are mandated to be able to perform this procedure in states T-02 and T-10.

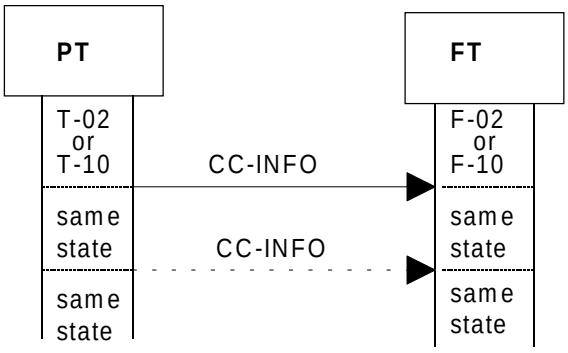


Figure 26: Sending keypad information

Table 22: Values used within the {CC-INFO} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Multi keypad>>			
	<Keypad information>	05H	Relate to feature pause (dialling pause) [N.6].
		15H	Relate to feature register recall N.5.
		17H	Relates to feature internal call N.28. For the related procedure (see subclause 8.16).
		18H	Relates to feature service call N.29. For the related procedure (see subclause 8.18).
		23H, 2AH, 30H - 39H	#, *, 0 - 9. Relate to feature dialled digits(basic) N.4 and outgoing call N.1.

8.10 Incoming call request

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 9.3.2, 9.3.2.1 and 9.3.2.2. Figure 27 and table 23 together with the associated subclauses define the mandatory requirements with regard to the present document.

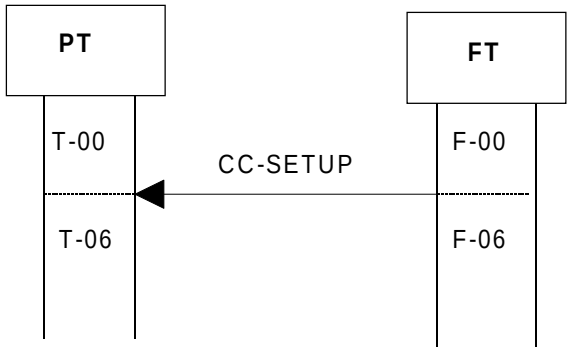


Figure 27: Incoming call request

Table 23: Values used within the {CC-SETUP} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable identity>>			
	<Type>	0	IPUI
	<PUT>	All	Area dependent
	<PUN>	All	Area dependent
<<Fixed Identity>>			Shall always include the whole PARK including the non significant bits.
	<Type>	32	PARK
	<Length of identity value>	All	PLI+1
	<ARC+ARD>	All	Area dependent
<<Basic service>>			
	<Call class>	8	
	<Basic service>	"1111"	Other
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Signal>>			Relates to procedure PT alerting, (see subclause 8.12).
	<Signal value>	40H - 47H, 48H, 4FH	
<<Calling party number>>			The support of this information element is only mandatory if feature N.27 is implemented.
	<Number type>	All	
	<Numbering plan id>	All	
	<Presentation indicator>	All	
	<Screening indicator>	All	
	<Calling party address>	All	

8.10.1 Associated procedure

8.10.1.1 Timer F-<CC.03> management

<CC.03>: CC set-up timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-SETUP} message has been sent;

Stop: An indication for release from the IWU or for link release from the DLC layer is received.
A {CC-ALERTING} or {CC-RELEASE-COM} message is received.

8.10.2 Exceptional cases

8.10.2.1 FT releases the incoming call request

The normal release procedure shall be used, (see subclause 8.6).

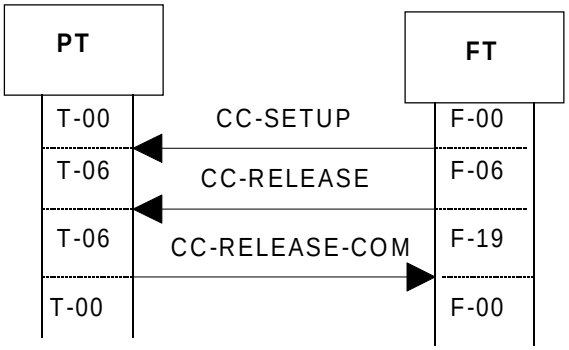
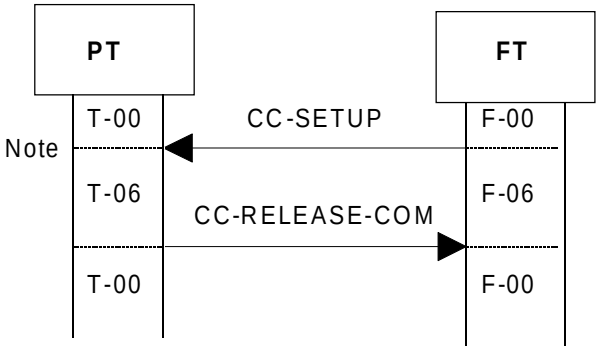


Figure 28: FT releases the incoming call request

For the values used within the {CC-SETUP} see table 23. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.10.2.2 PT rejects the incoming call request

The abnormal release procedure shall be used, (see subclause 8.7).



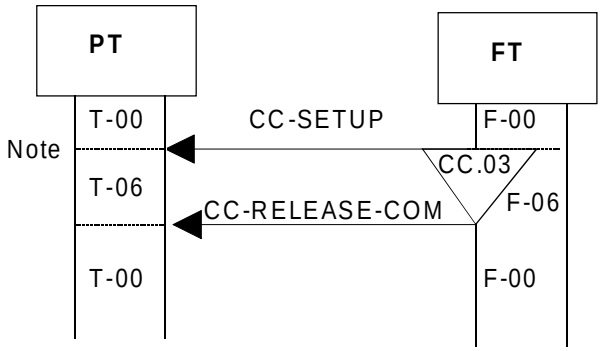
NOTE: Either PT-CC or PT-IWU may reject the call.

Figure 29: PT rejects the incoming call request

For the values used within the {CC-SETUP} see table 23. For the contents of {CC-RELEASE-COM} message see table 19.

8.10.2.3 Timer F-<CC.03> expiry

The abnormal release procedure shall be used, (see subclause 8.7).



NOTE: PT may not be answering because of some PT problems or because the {CC-SETUP} message has been lost or corrupted. The same result will occur if the eventual answer from the PT has been lost or corrupted.

Figure 30: Timer F<CC.03> expiry

For the values used within the {CC-SETUP} see table 23. For the contents of {CC-RELEASE-COM} see table 19.

8.11 Incoming call confirmation

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 9.3.2.7. Figure 31 and table 24 together with the associated subclauses define the mandatory requirements with regard to the present document.

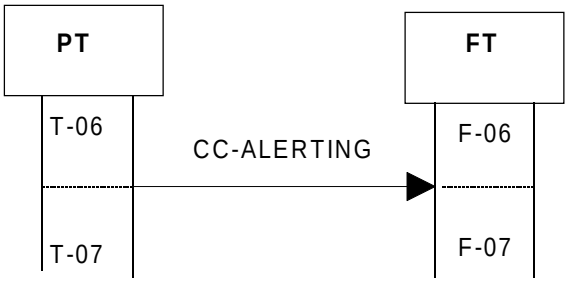


Figure 31: Incoming call confirmation

Table 24: Values used within the {CC-ALERTING} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<IWU attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection attributes>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.
<<Connection identity>>			Relates to feature Service Negotiation N.32. For the associated procedure see subclause 8.22.

8.11.1 Exceptional cases

8.11.1.1 FT releases the incoming call transaction

The normal release procedure shall be used, (see subclause 8.6).

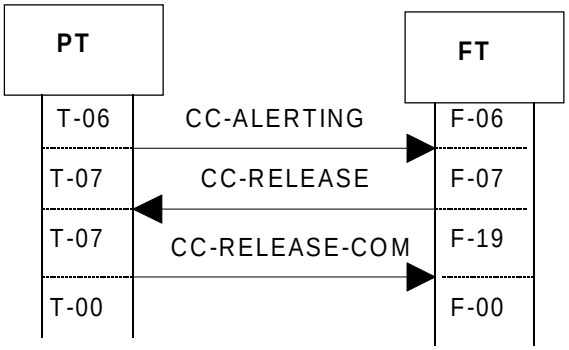


Figure 32: FT releases the incoming call transaction

For the values used within the {CC-ALERTING} see table 24. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.11.1.2 PT releases the incoming call transaction

The normal release procedure shall be used, (see subclause 8.6).

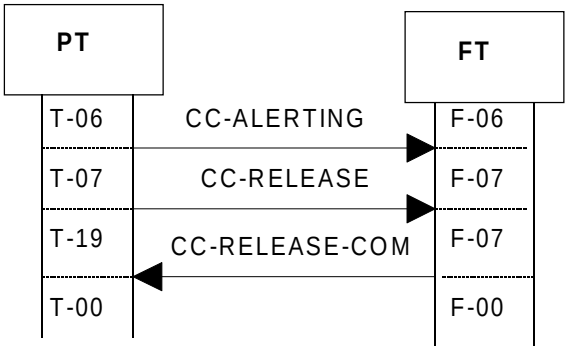


Figure 33: PT release the incoming call transaction

For the values used within the {CC-ALERTING} see table 24. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.12 PT alerting

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 9.3.2.7. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

PT alerting may be initiated either by including the <<SIGNAL>> information element in the {CC-SETUP} message or in a {CC-INFO} message in state F-07. FT is required to support one of the methods, PT is required to support both.

For PT alerting through the {CC-SETUP} see table 23, with the following additions:

Table 25: Values added within the {CC-SETUP} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Signal>>			
	<Signal value>	40H - 47H, 48H, 4FH	40H - internal, 41H - external

For PT alerting through {CC-INFO} in state F(T)-07 consider the following:

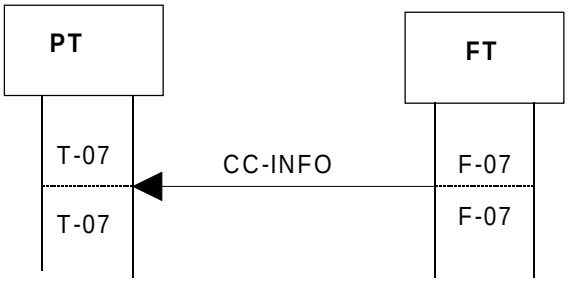


Figure 34: PT alerting in F-07

Table 26: Values used within the {CC-INFO} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Signal>>			
	<Signal value>	40H - 47H, 48H, 4FH	40H - internal, 41H - external

8.13 Incoming call connection

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 9.3.2.8. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

When the PT leaves the T-07 it shall stop alerting.

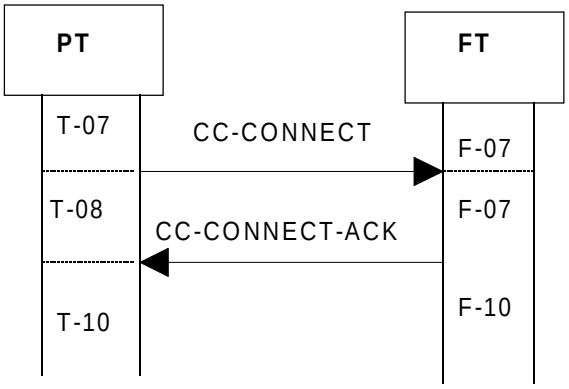


Figure 35: Incoming call connection

Table 27: Values used within the {CC-CONNECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

Table 28: Values used within the {CC-CONNECT-ACK} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

8.13.1 Associated procedure

8.13.1.1 Timer P-<CC.05> management

<CC.05>: CC connect timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CC-CONNECT} message has been sent;

Stop: An indication for release from the IWU or for link release from the DLC layer is received. A {CC-CONNECT-ACK} or {CC-RELEASE} message is received;

Restart: FT may restart it at any time by sending a {CC-NOTIFY} message, (see subclause 6.9.5).

8.13.2 Exceptional cases

8.13.2.1 FT releases the incoming call transaction

The normal release procedure shall be used, (see subclause 8.6).

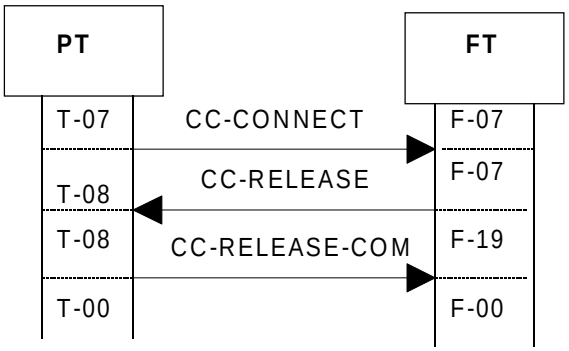


Figure 36: FT releases the incoming call transaction

For the values used within the {CC-CONNECT} see table 27. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.13.2.2 PT releases the incoming call transaction

The normal release procedure shall be used, (see subclause 8.6).

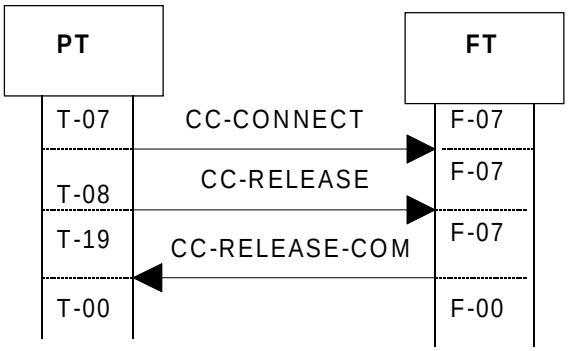
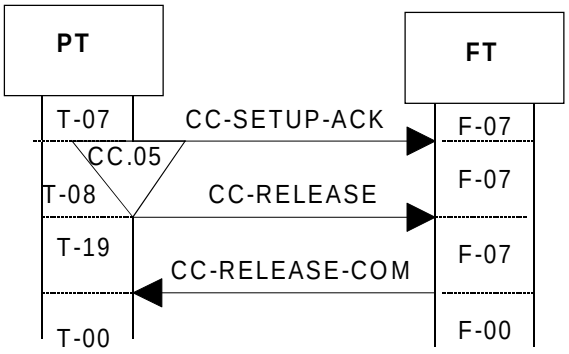


Figure 37: PT releases the incoming call transaction

For the values used within the {CC-CONNECT} see table 27. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.13.2.3 Timer P-<CC.05> expiry

The normal release procedure shall be used, (see subclause 8.6).



NOTE: FT may not be answering because of some FT problems or because the {CC-CONNECT} message has been lost or corrupted. The same result will occur if the eventual answer from FT has been lost or corrupted.

Figure 38: Timer P<CC.05> expiry

For the values used within the {CC-CONNECT} see table 27. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 17 and 18.

8.14 Display

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 10.2 and D.2.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

A <<DISPLAY>> information element may be included in any CC messages in the FT =>PT direction except in {CC-NOTIFY} and {IWU-INFORMATION}, (see EN 300 175-5 [4], subclause 6.3.2).

When included the information element is required to be handled only if the PP supports physical display.

Table 29: Values used within the <<DISPLAY>> information element in any message that includes it

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Multi display>>			
	<Display information>	DECT standard characters = standard IA5 characters	The support of these codes is only mandatory if feature N.21 is implemented. For the actual supported values see <<Terminal capability>> information element, subclause 8.15.
		08H - 0BH, 0DH	DECT control characters. The support of these codes is only mandatory if feature N.22 is implemented. For the actual supported values see <<Terminal capability>> information element, subclause 8.15.

8.15 Terminal capability indication

The PP shall be able to send the <<Terminal capability>> information element and the FP shall be able to receive it at least in {ACCESS-RIGHTS-REQUEST} and when location registration is supported in the {LOCATE-REQUEST}. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The capability indicated shall relate only to the terminal itself but not to the application that may be connected through.

Table 30: Values used within the <<TERMINAL CAPABILITY>> information element

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Terminal capability>>			
	<Tone capability>	All	
	<Display capability>	All	If PT supports feature N.21 it shall indicate in this field value which is equal to or higher than 2.
	<Profile indicator_1>	"xxxxx1x"B	GAP supported
	<Profile indicator_1>	"x1xxxxx"B	Data Services Profile A/B, Class 2 supported. This is mandatory if the PP supports RS232 services.
	<Profile indicator_1>	"1xxxxxx"B	Multi-bearers supported.
	<Profile indicator_2>	"xxxxxx1"B	Data Services Profile C, Class 2 supported. This is mandatory if the PP supports WLAN services.
	<Profile indicator_2>	"1xxxxxx"B	MMAP supported Always shall be indicated. Note: This new code need to be included into EN 300 175-5 [4] subclause 7.7.41
	<Control codes>	All	If PT supports feature N.22 it shall indicate in this field value which is equal to or higher than 2.
	<Slot type capability>	8	Full slot

The capabilities in table 31 shall be assumed as default if the following fields in the <<TERMINAL CAPABILITY>> information element are not present.

Table 31: Values assumed as terminal capabilities

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Terminal capability>>			
	<Echo parameters>	1	Minimum Telephone Coupling Loss (TCL) (>34 dB)
	<N-REJ>	1	No noise rejection
	<A-VOL>	1	No PP adaptive volume control
	<Slot type capability>	8	Full slot

No echoing of characters is allowed in the FT and therefore the PT would be responsible for displaying dialled digits (see figure 39). All display information from the FT would be assumed to be additional information that the PT shall display in addition. The PT shall logically separate display information originating at the FT and PT. This could be achieved, for example, by one physical display and two logical displays or two physical displays and two logical displays. The key point is that display characters from the PT and FT shall not be simultaneously interleaved/mixed on the same physical display.

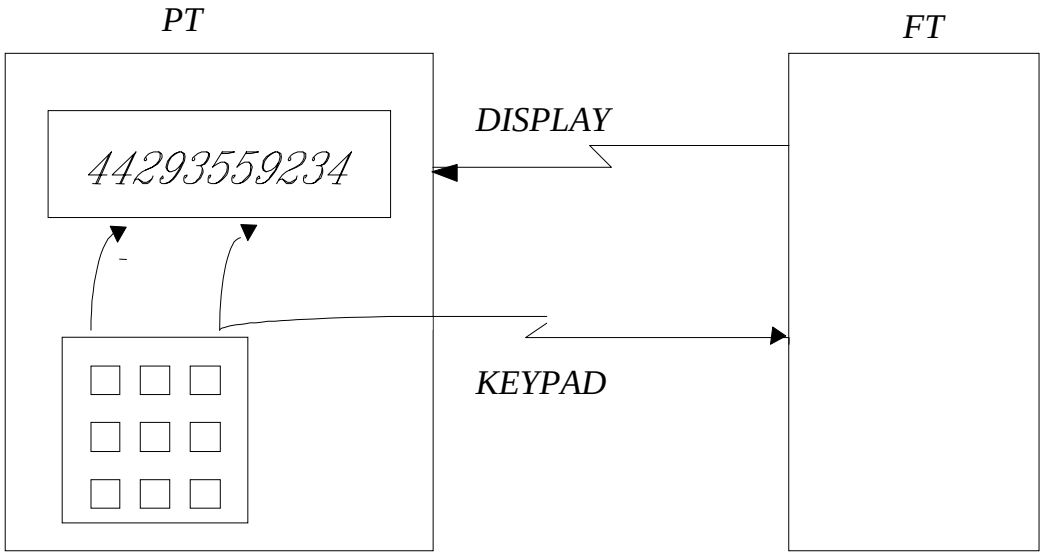


Figure 39: Terminal display

8.16 Internal call set-up

The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

For the initiation of this procedure the outgoing call request procedure shall be used, (see subclause 8.1) with the following replacement to the {CC-SETUP} message.

Table 32: Values used within the {CC-SETUP} message for internal call

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Basic service>>	<Call class>	9	Internal call.

8.17 Internal call keypad

The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

For the initiation of this procedure the sending keypad information procedure shall be used, (see subclause 8.9) with the following replacement to the {CC-INFO} message.

This call may be set only if it does not require changes into the negotiated service parameters of the existing call.

Table 33: Values used within the {CC-INFO} message for internal call

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Multi keypad>>	<Keypad information>	17H	Internal call

8.18 Service call set-up

The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

For the initiation of this procedure the outgoing call request procedure shall be used, (see subclause 8.1) with the following replacement to the {CC-SETUP} message:

Table 34: Values used within the {CC-SETUP} message for service call

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Basic service>>	<Call class>	11	Service call.

8.19 Service call keypad

The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

For the initiation of this procedure the sending keypad information procedure shall be used, (see subclause 8.9) with the following replacement to the {CC-INFO} message:

Table 35: Values used within the {CC-INFO} message for service call

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Multi keypad>>	<Keypad information>	18H	Service call

8.20 Call Suspend and Resume

Invocation of the suspend and resume procedures is controlled by the Lower Layer Management Entity (LLME).

The LLME may for implementation specific reasons decide when to suspend the MAC connection, but shall do this at least when during the last 5/n seconds no I or C channel data has been sent or received by MBC. The parameter "n" represents the total number of active duplex and double simplex bearers in the MAC connection.

The LLME shall not resume the MAC connection until I or C channel data is presented to MBC for transfer, or expiration of timer T219.

8.21 Selection of lower layer resources

The procedure relates to feature Service Negotiation N.32 and shall be performed as defined in EN 300 175-5 [4], subclauses 9.2.1.3 and 9.3.1.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

To negotiate the exact parameters of the requested service the initiating side shall include into the {CC-SETUP} message, see EN 300 175-4 [3]:

- a <<IWU ATTRIBUTES>> information element used to indicate the type/characteristics of MMAP service requested;
- a <<CONNECTION ATTRIBUTES>> information element;
- a <<CONNECTION IDENTITY>> information elements to indicate the connection relevant to the requested service;
- a <<WINDOW SIZE>> information element to indicate the window size to be used for U-plane frame transmission and the value of DLU.04 timer.

The <<CONNECTION-ATTRIBUTES>> element shall conventionally signify the maximum capabilities of the sender for the requested call, and hence shall be subject to negotiation. The actual values of the connection attributes are continuously negotiated at the MAC layer. Octets 5, 5a, 6, 6a codings shall be used to indicate transmit and receive capabilities respectively.

Table 36: Values used within the {CC-SETUP} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<IWU attributes>>			
	<Coding standard>	01	
	<Profile>	00001	RS232 - Not full set of C.2 profile is required for support - For the mandatory coding in this case see below
		00000	WLAN - Not full set of A/B.2 profile is required for support - For the mandatory coding in this case see below
	<Negotiation Indicator>	000, 010	
	<Profile Subtype>	0000	Interworking to V.24 circuits (RS323)
		1000	B-Ethernet (WLAN)
<<Connection attributes>>			
	<Symmetry>	001,100,110	Symmetric FT to PT with 1 duplex bearer Asymmetric PT to FT with 1 duplex bearer
	<Connection identity>	0000	Not yet numbered
	<Target bearers (P => F direction)>	1-23	If "Symmetric" has been indicated max. value that need to be supported is 12
	<Minimum bearers (P => F direction)>	0	Shall be omitted if "Symmetric" has been indicated

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
	<Target bearers (F => P direction)>	1-23	Shall be omitted if "Symmetric" has been indicated
	<Minimum bearers (F => P direction)>	0	Shall be omitted if "Symmetric" has been indicated
	<MAC slot size>	100	Full slot
	<ext5>	1	Octet 5a not included
	<MAC service>	0011	Ip correction
	<Ext6>	1	Octet 6a not included
	<CF channel attributes>	000, 001	C_F never (CS only) C_F Demand/1 bearer (interrupting)
	<MAC packet life time>	0, 8-15	
<<Connection identity>>			
	U-plane link identity	"000“	Always in Class A link operation
	Connection identity	"000“	Always in Class A link operation
<<Window size>>			
	FFS		

8.22 Peer Attribute Negotiation

The procedure relates to feature Service Negotiation N.32 and shall be performed as defined in EN 300 175-5 [4], subclauses 15.2.5. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If attributes are not acceptable the receiving side shall attempt negotiation if different services are possible, otherwise the call shall be rejected as specified in EN 300 175-5 [4] subclauses 9.3.1.2 and 9.3.2.2.

Peer determined attribute negotiation shall only be invoked by the receiving side if support of this capability is indicated in the <<IWU-ATTRIBUTES>> element (as contained in the {CC-SETUP} message).

If SOME of the proposed services in the {CC-SETUP} message are not acceptable the peer entity shall continue the call set-up procedure by including one alternative service description returning the appropriate <<CALL-ATTRIBUTES>> and/or <<CONNECTION ATTRIBUTES>> and/or <<IWU-ATTRIBUTES>> elements in the first response message (i.e. {CC-SETUP-ACK} or {CC-CONNECT} for FT, {CC-ALERTING} for PT).

For the allowed values of these information elements see subclause 8.21. The values of <Coding standard> and <Profile> in the <<IWU-ATTRIBUTES>> cannot and shall not be changed; if these values are unacceptable the receiving side shall reject the call.

The initiating entity shall indicate its acceptance of these new attributes by proceeding with the normal call set-up procedures. If it cannot support the new attributes the call shall be released using the normal release procedures.

8.23 Operation parameter negotiation

The procedure relates to feature Service negotiation N.32 and shall be performed as defined in EN 300 175-5 [4], subclauses 15.2.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If the initiating side includes a <<Window size>> information element 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 by returning the modified elements in the first response message (i.e. {CC-SETUP-ACK} or {CC-CONNECT} for FT, {CC-ALERTING} for PT).

If the values are acceptable the receiving side shall 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.

8.24 Bandwidth Change

The procedure relates to feature In Call Service Change N.30 and shall be performed as defined in EN 300 175-5 [4], subclauses 9.6.1 and 9.6.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Bandwidth changes shall be defined as changes that may be realized by modification of the existing MAC connection. The <<CONNECTION-ATTRIBUTES>> element shall always be included to define the new connection bandwidths.

Table 37: Values used within the {CC-SERVICE-CHANGE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<< Service Change Info >>	<Ext3>	1	
	<Coding standard>	"00"B	DECT standard coding
	<M>	0/1	Initiating/Receiving side is master
	<Change Mode>	"0001"	Connection Reversal - the complete reversal of unidirectional connections
		0010	Bandwidth change
	<A attributes>	"000“	Not applicable
	<R>	"0"	Do not reset state variables
	<B attributes>	"011“	Maintain data transfer

Table 38: Values used within the {CC-SERVICE-ACCEPT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<< TI&PD>>	<Transaction Identifier>	1-6	The TI associated with the active CC call to be suspended
<<Connection Attributes>>			
	<Symmetry>	001,100,110	Symmetric – shall not be used with "Connection Reversal" Asymmetric FT to PT with 1 duplex bearer Asymmetric PT to FT with 1 duplex bearer
	<Connection identity>	0000	Not yet numbered
	<Target bearers (P => F direction)>	1-23	If "Symmetric" has been indicated max. value that need to be supported is 12
	<Minimum bearers (P => F direction)>	1-23	If this is omitted the default value shall be as defined in " Target bearers (P => F direction)" If "Symmetric" has been indicated max. value that need to be supported is 12

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
	<Target bearers (F => P direction)>	1-23	Shall be omitted if "Symmetric" has been indicated
	<Minimum bearers (F => P direction)>	1-23	Shall be omitted if "Symmetric" has been indicated If this is omitted the default value shall be as defined in " Target bearers (F => P direction)"
	<MAC slot size>	100	Full slot
	<ext5>	1	Octet 5a not included
	<MAC service>	0011	Ip correction
	<Ext6>	1	Octet 6a not included
	<CF channel attributes>	000, 001	C_F never (CS only) C_F Demand/1 bearer (interrupting)
	<MAC packet life time>	0, 8-15	
<<Connection Identity>>	U-plane link identity	"000“	Always in Class A link operation
	Connection identity	"000“	Always in Class A link operation

8.25 Identification of PP

The procedure relates to feature Identification of PP N.12 and shall be performed as defined in EN 300 175-5 [4], subclause 13.2.1. Figure 40, and tables 39 and 40, together with the associated subclauses define the mandatory requirements with regard to the present document.

Figure 40: Identification of PT

Table 39: Values used within the {IDENTITY-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Identity-type>>			
	<Identity-group>	0, 4	Portable identity, Fixed identity
	<Type>	0, 16, 32	Codings for identity-group = 0 IPUI, IPEI, TPUI required
		0, 1, 32	Codings for identity-group = 4 PARI, PARI plus RPN, PARK required

If an identity request is made for a Temporary Portable User Identity (TPUI), this implies a request for the assigned TPUI, but not the default TPUI.

Table 40: Values used within the {IDENTITY-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			The inclusion of this information element depends on what type identity has been requested in the {IDENTITY-REQUEST}. This identity relates to the active IPUI/PARK pair.
	<Type>	0, 16, 32	
	<Identity-value>	all PUT values, all PUN values	For <Type> = 0 The parameter depends upon subscription records.
		All EMC values, all PSN values	For <Type> = 16 The parameter depends upon subscription records.
		TPUI type: 0-B, all TPUI values	For <Type> = 32 The parameter depends upon subscription records.
<<Fixed-identity>>			The inclusion of this information element depends on what type identity has been requested in the {IDENTITY-REQUEST}. This identity relates to the active IPUI/PARK pair.
	<Type>	0, 1, 32	
	<Length indicator>	All	Depending on the type.
	<ARC+ARD (+RPN)>	All	Radio fixed Part Number (RPN) is needed only for type 1

The PARI or PARI + RPN sent in the {IDENTITY-REPLY} message shall be taken from the RFP to which the PT is currently locked.

8.25.1 Associated procedure

8.25.1.1 Timer F-<MM_ident.2> management

<MM_ident.2>: Identification timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {IDENTITY-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC layer is received. An {IDENTITY-REPLY} message is received or a interrupting higher priority transaction begins.

8.25.2 Exceptional cases

8.25.2.1 Identity not existing in the PP

This procedure is equivalent to the identification of PP procedure successful case defined in subclause 8.25 except that the {IDENTITY-REPLY} message shall be sent without the identity information elements that have been requested but do not exist.

8.25.2.2 Timer F-<MM_ident.2> expiry

The timer F-<MM_ident.2> shall not be restarted by the FT. If a retransmission of the {IDENTITY-REQUEST} message (and restarting of the timer F-<MM_ident.2>) is needed, it may be initiated by the interworking unit/application layer.

8.26 Authentication of FT

The procedure relates to features ZAP N.15 and Terminate access rights FT initiated N.19, as well as to feature Authentication of FT N.23 and shall be performed as defined in EN 300 175-5 [4], subclause 13.3.3. Figure 41, and tables 41 and 42, together with the associated subclauses define the mandatory requirements with regard to the present document.

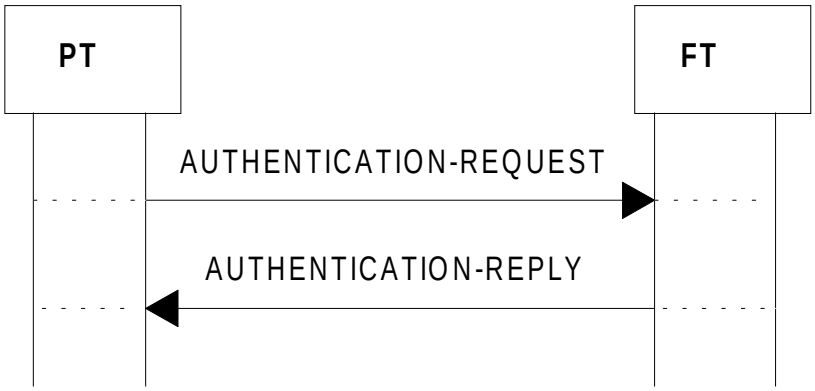


Figure 41: Authentication of FT

Table 41: Values used within the {AUTHENTICATION-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth-type>>			
	<Auth algorithm id>	1	DSAA.
	<Auth key type>	1	UAK
		4	AC. Length shall always be 32 bits
	<Auth Key number>	8	Always IPUI/PARK pair (= subscription)
	<INC>	0	Ignore
	<TXC>	0	Ignore
	<UPC>	0	Ignore
	<Cipher key number>	0	Ignore
<<RAND>>			
	<RAND Field>	All	DSAA length

Table 42: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RES>>	<RES Field>	All	DSAA length.
<<RS>>	<RS Field>	All	DSAA length.

8.26.1 Associated procedure

8.26.1.1 Timer P-<MM_auth.1> management

<MM_auth.1>: Authentication timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {AUTHENTICATION-REQUEST} message is sent;

Stop: An indication for link release from the DLC is received. An {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message is received.

8.26.2 Exceptional cases

8.26.2.1 Authentication algorithm/key not supported

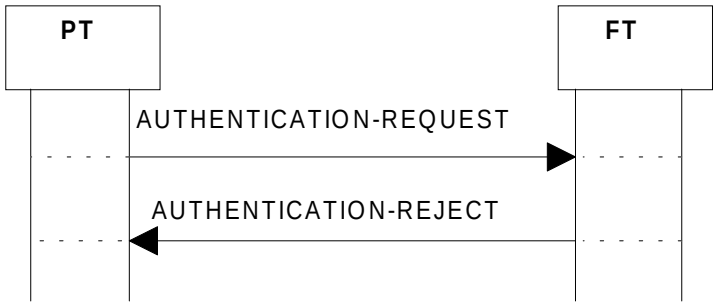


Figure 42: Authentication algorithm/key not supported by the FT

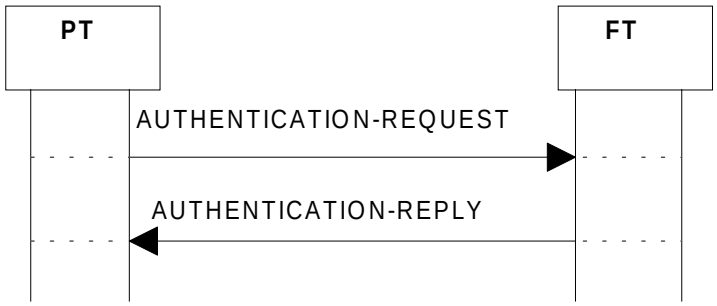
Table 43: Values used within the {AUTHENTICATION-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

The <<reject reason>> information element need not be sent by the FT and need not be understood by the PT.

In case the PT has made attempt with non DSAA algorithm indicated the PT shall re-attempt to authenticate the FT with DSAA.

8.26.2.2 Authentication challenge RES has wrong value



NOTE: If the received RES value in the {AUTHENTICATION REPLY} message is not equal to XRES1 further actions taken by the PT depend on the PP application.

Figure 43: Authentication challenge RES has wrong value

8.26.2.3 Timer P-<MM_auth.1> expiry

The timer P-<MM_auth.1> shall not be restarted by the PT. The inter-working unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.27 Authentication of PP

The p DECT Standard Authentication Algorithmrocedure relates to the feature Authentication of PP N.8 and shall be performed as defined in EN 300 175-5 [4], subclause 13.3.1. Figure 44, and tables 44 and 45, together with the associated subclauses define the mandatory requirements with regard to the present document.

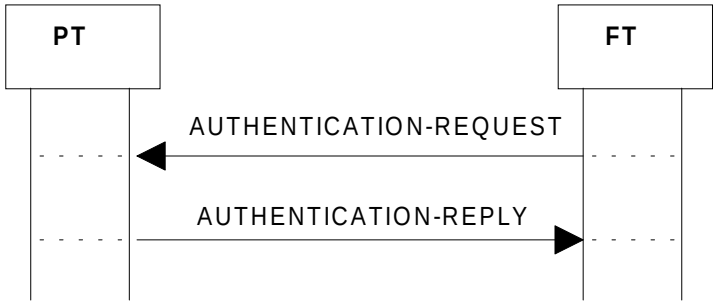


Figure 44: Authentication of PT

Table 44: Values used within the {AUTHENTICATION-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth-type>>			
	<Auth algorithm id>	1	DSAA
	<Auth key type>	1	UAK
		4	AC. Length shall always be 32 bits
	<Auth key number>	8	Always IPUI/PARK pair (= subscription)
	<INC>	0	Value 1 used in incrementing the ZAP value procedure, (see subclause 8.29).
	<TXC>	0	
	<UPC>	0	Value 1 used in storing the DCK procedure, (see subclause 8.30)
	<Cipher key number>	0	Value 8 used in storing the DCK procedure, (see subclause 8.30).
<<RAND>>			
	<RAND Field>	All	DSAA length
<<RS>>			
	<RS Field>	All	DSAA length

Table 45: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RES>>			
	<RES Field>	All	DSAA length. RES = XRES1
<<ZAP field>>			
	<Contents field>	0-15	M if stored else O. Associated to feature N.15.
<<Service class>>			
	<Service class field>	1-6	M if stored else O. Associated to feature N.13.

If the <UPC> field is set the PT shall store the new cipher key (even if ciphering is currently active) but the new key shall not be used until the next initiation of a ciphering procedure.

8.27.1 Associated procedure

8.27.1.1 Timer F-<MM_auth.1> management

<MM_auth.1>: Authentication timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {AUTHENTICATION-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message is received or a interrupting higher priority transaction begins.

8.27.2 Exceptional cases

8.27.2.1 Authentication algorithm/key not supported

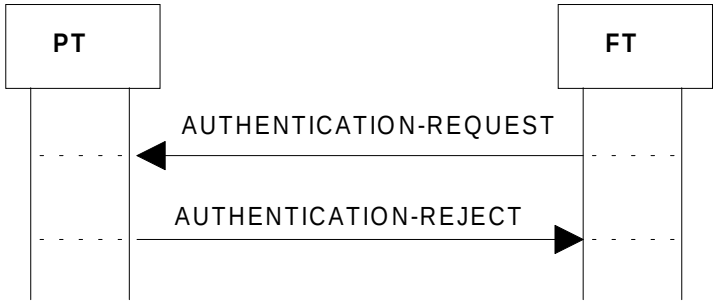


Figure 45: Authentication algorithm/key not supported by the PT

For the contents of the {AUTHENTICATION-REJECT} message see table 43.

The <<reject reason>> information element need not be sent by the PT and need not be understood by the FT.

In case the FT has made attempt with non DSAA algorithm indicated, the FT shall re-attempt to authenticate the PT with DSAA.

8.27.2.2 Timer F-<MM_auth.1> expiry

The timer F-<MM_auth.1> shall not be restarted by the FT. The interworking unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.28 Authentication of user

The procedure relates to the feature Authentication of user N.9 and shall be performed as defined in EN 300 175-5 [4], subclause 13.3.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

This procedure is equivalent to the authentication of PP procedure defined in subclause 8.27 with the following replacement to the {AUTHENTICATION-REQUEST} message:

Table 46: Additional coding to <<Auth Type>> for user authentication

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth type>>			
	<Auth key type>	3	UPI

The UPI shall be mapped to a bitstring in the following way:

- UPI shall always have a length of 32 bits;
- each decimal digit entered by the user, is translated into one semi-octet (BCD coded). The PT shall be capable to accept any UPI between 0 and 8 decimal digits (limits included);
- the resulting string of semi-octets is padded with a number of leading "all ones " semi octets to achieve a total of 8 semi octets;
- the result is a bitstring of 32 bits.

EXAMPLE: A value of "091" (3 decimal digits entered via keypad) is translated into a bitstring UPI of the following value:

"1111 1111 1111 1111 1111 0000 1001 0001".

8.28.1 Associated procedure

8.28.1.1 Timer F-<MM_auth.2> management

<MM_auth.2>: Authentication of user timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {AUTHENTICATION-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message is received or a interrupting higher priority transaction begins.

8.28.2 Exceptional cases

8.28.2.1 Authentication algorithm/key not supported

This procedure is equivalent to the procedure defined in subclause 8.27.2.1.

8.28.2.2 Timer F-<MM_auth.2> expiry

The timer F-<MM_auth.2> shall not be restarted by the FT. If a retransmission of the {AUTHENTICATION-REQUEST} message (and restarting of the timer <MM_auth.2>) is needed, it may be initiated by the interworking unit/application layer.

8.29 Incrementing the ZAP value

The procedure relates to the feature ZAP N.15 and shall be performed as defined in EN 300 175-5 [4], subclause 13.3.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

This procedure is equivalent to the authentication of PT procedure defined in subclause 8.27 with the following additions/replacements.

The procedure may consist of two nested MM transactions:

- one authentication of PT indicating "ZAP increment"; and
- authentication of the FT with its own independent transaction identifier.

Before incrementing the ZAP, PT may authenticate the FT and if this authentication fails, the PT shall not increment the ZAP field. The support of authentication of FT transaction in incrementing the ZAP value procedure is optional for the PT and mandatory for the FT.

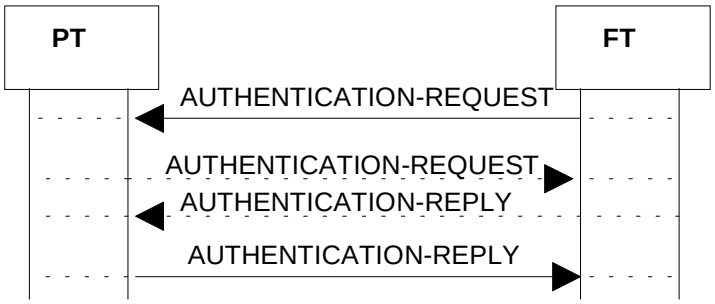


Figure 46: ZAP increment

Table 47: Replacement to {AUTHENTICATION-REQUEST} for incrementing the ZAP value

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth-type>>			
	<INC bit coding>	1	Increment

For the contents of {AUTHENTICATION-REQUEST} sent by PT and {AUTHENTICATION-REPLY} sent by FT see tables 41 and 42.

For the contents of {AUTHENTICATION-REPLY} sent by the PT see table 45.

8.30 Storing the DCK

This procedure relates to the feature encryption activation FT initiated N.16 as well as to feature encryption activation PT initiated N.24 and is equivalent to the authentication of PT procedure defined in subclause 8.27 with the replacement in table 48 to the {AUTHENTICATION-REQUEST} message.

Table 48: Replacement to {AUTHENTICATION-REQUEST} for storing the DCK

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth-type>>			
	<UPC>	1	Store the new DCK.
	<Cipher key number>	8	

8.31 Location registration

The procedure relates to the feature location registration N.10 and shall be performed as defined in EN 300 175-5 [4], subclause 13.4.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The location registration procedure consists of only one MM transaction regardless of whether an attempt for TPUI assignment has been made or has not.

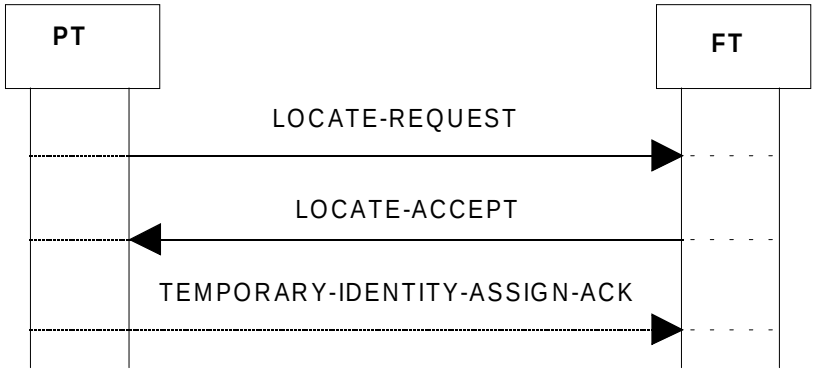


Figure 47: Location registration

Table 49: Values used within the {LOCATE-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			
	<Type>	0	IPUI
	<PUT>	All	Depends upon subscription records.
	<PUN>	All	Depends upon subscription records.
<<Fixed-identity>>			This information element shall contain the old PARI+RPN. (See table 140).
	<Type>	1	
	<ARC>	All	
	<ARD+RPN>	All	
<<Location-area>>			This information element shall contain the old Location Area Level (LAL) (see table 140).
	<LI-type>	1	
	<LAL>	All	
<<Set-up capability>>			
	<ext3>	1	
	<Set-up>	All	Setting and support depends on the relevant capability
	<Page>	All	Setting and support depends on the relevant capability
<<Terminal capability>>			(See subclause 8.15)

Table 50: Values used within the {LOCATE-ACCEPT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			Always mandatory. FT may use zero length contents if it does not wish to assign a TPUI. In this case PT maintains its current assigned TPUI if present or shall use default TPUI otherwise. An FT that supports "fast set-up" shall always assign TPUI.
	<Type>	32	TPUI
	<Length of id value>	20	
	<Identity-value>	Values in EN 300 175-6 [5] subclause 6.3.1 are allowed	Only assigned individual TPUIs are allowed.
<<Location-area>>			
	<LI-type>	1	
	<LAL>	0-39	Even if default LAL

Table 51: Values used within the {TEMPORARY-IDENTITY-ASSIGN-ACK} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

Upon reception of the {LOCATE-ACCEPT} message the PP shall store the PARI and the RPN derived from the RFPI. See subclause 14.7 (storage of subscription related data).

If a zero length contents of <<Portable identity>> information element is received by the PP, it shall not respond with a {TEMPORARY-IDENTITY-ASSIGN-ACK} message to the FP. If TPUI is to be assigned a {TEMPORARY-IDENTITY-ASSIGN-ACK} message shall follow.

8.31.1 Associated procedures

8.31.1.1 Timer P-<MM_locate.1> management

<MM_locate.1>: Location timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: {LOCATE-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. {LOCATE-ACCEPT} or {LOCATE-REJECT} message is received or interrupting higher priority transaction begins.

8.31.1.2 Timer F-<MM_ident.1> management

<MM_ident.1>: TPUI assignment timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: {LOCATE-ACCEPT} message assigning a TPUI is sent or an interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received.
A {TEMPORARY-IDENTITY-ASSIGN-ACK} or a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message is received, or, interrupting higher priority transaction begins.

8.31.2 Exceptional cases

8.31.2.1 FT rejects the location registration procedure

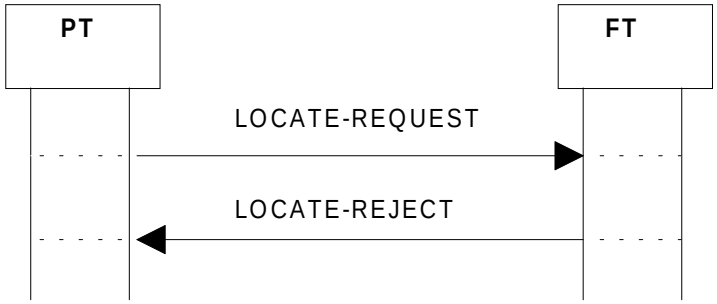


Figure 48: Location registration not supported by the FT

Upon receipt of a {LOCATE-REJECT} message the PP shall maintain the existing LAL value.

Table 52: Values used within the {LOCATE-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

The <<Reject reason>> information element need not be sent by the FT and need not be understood by the PT. In this case the PT should not initiate a location registration procedure until the conditions for location registration initiation are met as defined in subclause 14.2.

8.31.2.2 Failure of location registration procedure

Upon expiry of <MM_locate.1> or indication for link released is received from the DLC layer, PT shall consider the procedure as failed. The PP shall maintain the existing LAL value. PT shall not retransmit the {LOCATE-REQUEST} message. and shall not restart the timer <MM_locate.1> as part of the same procedure. The P-IWU should initiate a new location registration procedure.

8.31.2.3 PT rejects the identity assignment

PT shall be capable of storing an individual assigned TPUI. If the FT performs identity assignment and PT does not have the capability of storing the TPUI (excluding an assigned individual TPUI) or there is an error in the {LOCATE-ACCEPT} message it shall send back a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message.

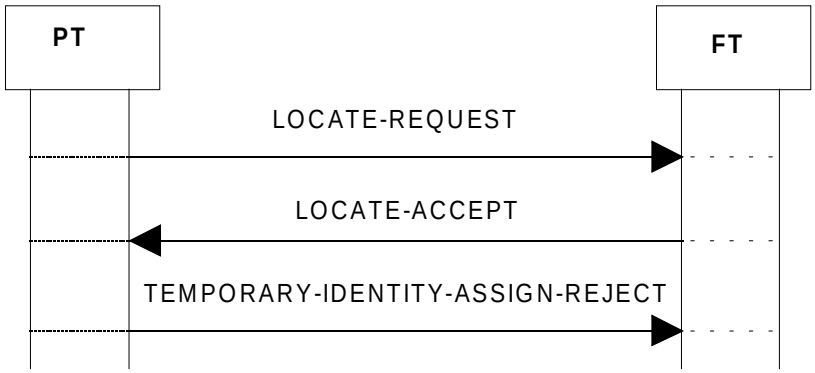


Figure 49: Rejection of identity assignment

Table 53: Values used within the {TEMPORARY-IDENTITY-ASSIGN-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

8.31.2.4 Timer F-<MM_identity.1> expiry

If timer F-<MM_identity.1> expires the FT shall consider the TPUI assignment as failed.

8.32 Location update

The procedure relates to the feature Location registration N.10 and shall be performed with regard to subclause 13.4.3 of EN 300 175-5 [4]. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Location update consists of two procedures (the location update procedure and the location registration procedure) each having its own transaction. It may be described as FT suggesting location registration and PT performing location registration.

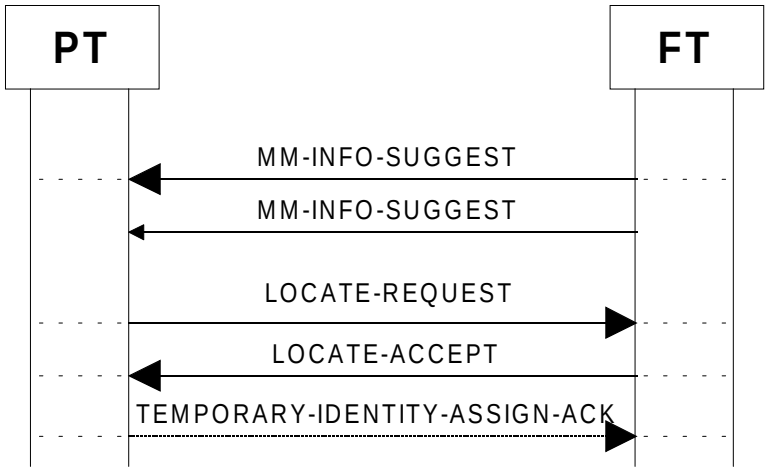
The FT shall send two consecutive {MM-INFO-SUGGEST} messages, each contains an <<INFO-TYPE>> information element with only the parameter type "locate suggest"; the <ext> parameter associated to this parameter type shall be set to 0 in the first {MM-INFO-SUGGEST} and to 1 in the second {MM-INFO-SUGGEST}.

Upon receipt of the {MM-INFO-SUGGEST} message the PT shall check the parameter type. If the parameter type "locate suggest" is indicated in the <<INFO-TYPE>> information element, the PT shall ignore bit 8 and the PT shall initiate the location registration procedure as described in subclause 8.31.

Even if the bit a38, see table 138, is not set to "1" the PT shall initiate location registration procedure on request of location update procedure. In the situation where the {MM-INFO-SUGGEST} sent by the FT interrupts a priority level 3 PT-initiated transaction the PT shall complete the interrupted one before initiating the location registration.

In the situation when the {MM-INFO-SUGGEST} interrupts a Location Registration procedure, the {MM-INFO-SUGGEST} shall be ignored.

NOTE: A PT implementation should take care that during the time the interrupting MM-INFO-SUGGEST message is processed a possible arriving LOCATE-ACCEPT or LOCATE-REJECT message does not get lost.



NOTE 1: The {LOCATE-REQUEST} message may be received by the FT before the second {MM-INFO-SUGGEST} message is sent by the FT.
NOTE 2: The requirement of sending two {MM-INFO-SUGGEST} instead of one has been introduced for backward compatibility with existing DECT equipment.

Figure 50: Location update

Table 54: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	1	
	<ext>	0/1	The first {MM-INFO-SUGGEST} message shall be sent using value 0, the second using value 1
	<Parameter type>	0	Locate suggest

8.33 Obtaining access rights

The procedure relates to the features Subscription registration user procedure on_air N.17, Service class indication/assignment N.13, and, ZAP N.15 and shall be performed as defined in EN 300 175-5 [4], subclause 13.5.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

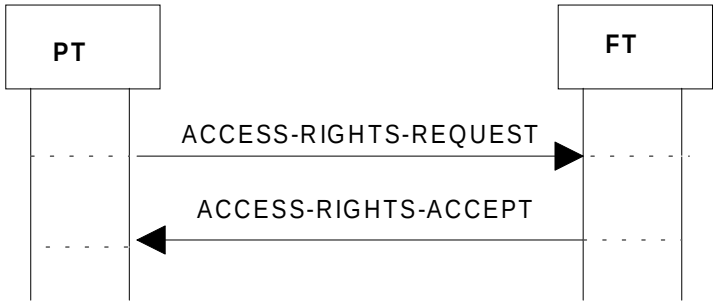


Figure 51: Obtain access rights

Table 55: Values used within the {ACCESS-RIGHTS-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			Default IPUI if not yet assigned.
	<Type>	0	IPUI
	<PUT>	All	Depends upon subscription records.
	<PUN>	All	Depends upon subscription records.
<<Auth-type>>			
	<Auth-algorithm-id>	1	DSAA
	<Auth key type>	1, 4	The PT shall set the value to 4 (AC) only if it does not have a UAK. If the PT sends value 1 (UAK), the FT assumes that the PT has a UAK. If FT has only AC for this PT, the FT shall assume that the AC-value has not been entered by the PP user. The FP shall not accept the access rights request.
	<Auth key number>	8	The keys are associated to IPUI/PARK pair (= subscription)
	<INC>	0	Ignore
	<TXC>	0	Ignore
	<UPC>	0	Ignore
	<Cipher key number>	0	Ignore
<<Set-up capability>>			
	<ext3>	1	
	<Set-up>	All	Setting and support depends on the relevant capability
	<Page>	All	Setting and support depends on the relevant capability
<<Terminal capability>>			(See subclause 8.15)

Table 56: Values used within the {ACCESS-RIGHTS-ACCEPT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			
	<Type>	0	IPUI. All ARI equipment classes other than Class A equipment, shall never send IPUI type N.
	<PUT>	All	Depends upon subscription records.
	<PUN>	All	Depends upon subscription records.
<<Fixed identity>>			Depends upon subscription records. Shall always include the whole PARK including the non significant bits.
	<Type >	32	PARK
	<Length of identity value>	All	PLI+1
	<ARC+ARD>	All	
<<Zap field>>			Relates to feature N.15
	<Contents-field>	All	
<<Service-class>>			Relates to feature N.13
	<Service-class-field>	All	

8.33.1 Associated procedure

8.33.1.1 Timer P-<MM_access.1> management

<MM_access.1>: Access rights timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {ACCESS-RIGHTS-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {ACCESS-RIGHTS-ACCEPT} or {ACCESS-RIGHTS-REJECT} message is received or a interrupting higher priority transaction begins.

8.33.2 Exceptional cases

8.33.2.1 FT rejects the access rights

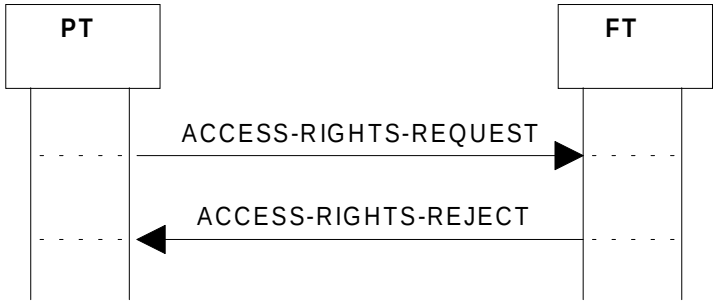


Figure 52: FT rejects access rights request

Table 57: Values used within the {ACCESS-RIGHTS-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

No actions are required by the portable.

If the PT has requested access rights identifying non DECT authentication or/and cipher algorithm, the PT shall initiate a new access rights request with DSAA or/and DCA.

8.33.2.2 Timer P-<MM_access.1> expiry

Upon expiry of P-<MM_access.1> PT shall consider the procedure as failed. PT shall not retransmit the {ACCESS-RIGHTS-REQUEST} message and shall not restart the timer P-<MM_access.1> as part of the same procedure. The interworking unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.34 FT terminating access rights

The procedure relates to the feature FT terminate access rights N.19 and shall be performed as defined in EN 300 175-5 [4], subclause 13.5.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The procedure consists of two nested MM transactions: one FT terminating access rights and other authentication of the FT with its own independent transaction identifier. Before terminating the access rights, PT may authenticate the FT and if this authentication fails, the PT shall not terminate the access rights. The support of authentication of FT transaction in FT terminating access rights procedure is optional for the PT and mandatory for the FT.

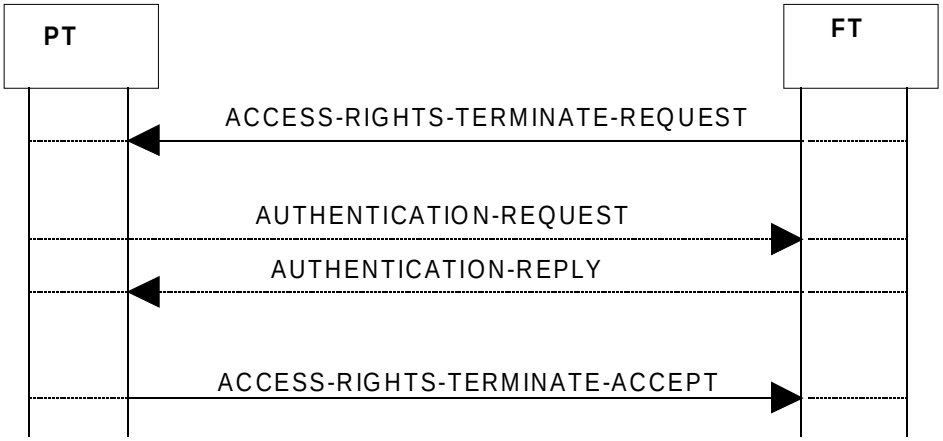


Figure 53: Termination of access rights

Table 58: Values used within the {ACCESS-RIGHTS-TERMINATE-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable-identity>>			
	<Type>	0	IPUI
	<PUT>	All	Depends upon subscription records.
	<PUN>	All	Depends upon subscription records.
<<Fixed identity>>			Depends upon subscription records. This procedure is only allowed for IPUI/PARK pair, therefore, <<Fixed-id>> shall always be included.
	<Type>	32	PARK
	<length of identity value>	All	PLI+1
	<ARC+ARD>	All	

For the values used within the {AUTHENTICATION-REQUEST} and {AUTHENTICATION-REPLY} see tables 41 and 42.

Table 59: Values used within the {ACCESS-RIGHTS-TERMINATE-ACCEPT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			No information elements

The reception of {ACCESS-RIGHTS-TERMINATE-ACCEPT} indicates to the FT that the PT has deleted the subscription data associated to the received IPUI/PARK.

8.34.1 Associated procedure

8.34.1.1 Timer F-<MM_access.2> management

<MM_access.2>: Access rights termination timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {ACCESS-RIGHTS-TERMINATE-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {ACCESS-RIGHTS-TERMINATE-ACCEPT} or {ACCESS-RIGHTS-TERMINATE-REJECT} message is received or a interrupting higher priority transaction begins.

8.34.2 Exceptional cases

8.34.2.1 PT rejects the termination request

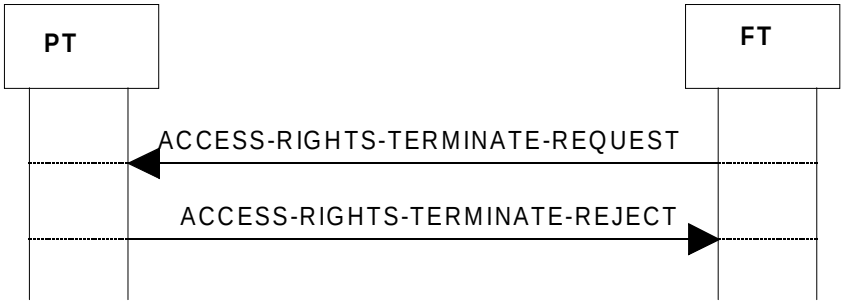


Figure 54: PT rejects

Table 60: Standard values used within the {ACCESS-RIGHTS-TERMINATE-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
			All optional

8.34.2.2 Timer F-<MM_access.2> expiry

Upon expiry of F-<MM_access.2> FT shall consider the procedure as failed. FT shall not retransmit the {ACCESS-RIGHTS-TERMINATE-REQUEST} message. and shall not restart the timer F-<MM_access.2> as part of the same procedure. However, the interworking unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.35 Key allocation

The procedure relates to the feature On air key allocation N.11 and shall be performed as defined in EN 300 175-5 [4], subclause 13.6. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The key allocation procedure consists of only one MM transaction.

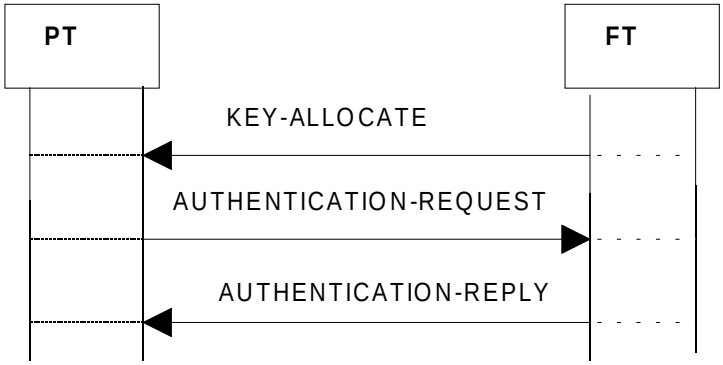


Figure 55: Key allocation

Table 61: Values used within the {KEY-ALLOCATE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Alloc-type>>			
	<Auth-algorithm-id>	1	DSAA
	<UAK number>	8	Keys relate to IPUI/PARK pair
	<AC number>	8	Keys relate to IPUI/PARK pair
<<RAND>>			
	<RAND Field>	All	DSAA length.RAND_F.
<<RS>>	<RS Field>	All	DSAA length

Table 62: Values used within the {AUTHENTICATION-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Auth-type>>			
	<Auth-algorithm-id>	1	DSAA
	<Auth key type>	4	AC, Length shall always be 32 bits
	<Auth key number>	8	Key relates to IPUI/PARK pair
	<INC>	0	ignore
	<TXC>	0	ignore
	<UPC>	0	ignore
	<Cipher key number>	0	ignore
<<RAND>>			
	<RAND Field>	All	DSAA length. RAND_P
<<RES>>			
	<RES Field>	All	DSAA length. RES1.

The value RES1 is computed by the PT from RAND_F and RS. FT possesses the value XRES1 which is the result from the same computation. The authentication of PT is considered as successful if RES1 = XRES1.

Table 63: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RES>>	<RES Field>	All	DSAA length. RES2.

The value RES2 is computed by the FT from RAND_P and RS. The FP authentication Session Key (KS') value, an intermediate result from this computing, shall be stored at FT as a new UAK under number 8. The FT marks the new UAK with "unconfirmed status" and shall retain both the AC and the UAK until the PT has been successfully authenticate using the UAK, then the AC shall be erased and the "unconfirmed status" marking shall be removed from the UAK.

The PT possesses the value XRES2 which is the result from the same computation. The authentication of FT is considered as successful if RES2 = XRES2. Then the PP authentication Session Key (KS) value, an intermediate result from the computing of XRES2 at PT, is stored at PT as a new UAK under number 8. The AC used for the UAK derivation shall be erased.

8.35.1 Associated procedures

8.35.1.1 Timer F-<MM_key.1> management

<MM_key.1>: Key allocation timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {KEY-ALLOCATE} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {AUTHENTICATION-REQUEST}, or {AUTHENTICATION-REJECT} message is received.

8.35.1.2 Timer P-<MM_auth.1> management

<MM_auth.1>: Authentication timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {AUTHENTICATION-REQUEST} message is sent or a interrupting higher priority transaction is completed;

Stop: An indication for link release from the DLC is received. An {AUTHENTICATION-REPLY} or {AUTHENTICATION-REJECT} message is received or a interrupting higher priority transaction begins.

8.35.2 Exceptional cases

8.35.2.1 Timer F-<MM_key.1> expiry

Upon expiry of F-<MM_key.1> FT shall consider the procedure as failed. FT shall not retransmit the {KEY-ALLOCATE} message and shall not restart the timer F-<MM_key.1> as part of the same procedure. However, the interworking unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.35.2.2 Timer P-<MM_auth.1> expiry

Upon expiry of P-<MM_auth.1> PT shall consider the procedure as failed and shall abort it.

8.35.2.3 Allocation-type element is unacceptable

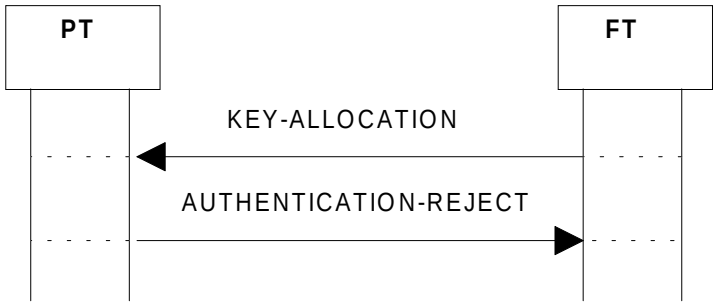


Figure 56: Allocation-type unacceptable for PT

8.35.2.4 Authentication of FT fails

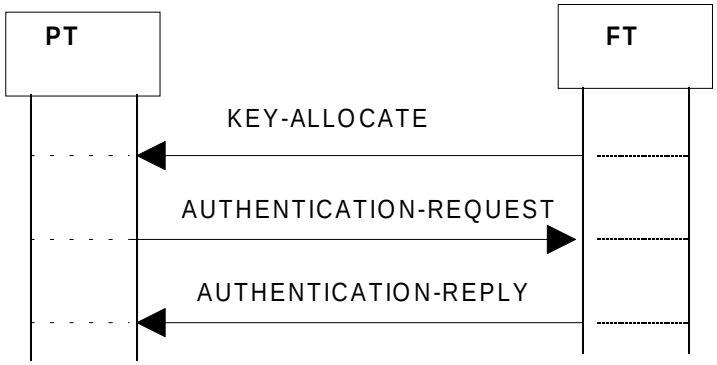


Figure 57: Authentication of FT fails

If the Authentication of FT fails, as XRES2><RES2, the KS shall be not stored, and the PT shall retain the AC. At the same time the FT has stored KS' as an eventual UAK with status "Unconfirmed", and the FT shall try to use this key in a future Authentication of PT procedure. In that case the PT shall reject because "authentication key not available" and the FT shall delete this UAK.

8.36 Cipher-switching initiated by FT

This procedure relates to the feature Encryption activation FT initiated N.16 as well as to feature Encryption deactivation FT initiated N.25 and shall be performed as defined in EN 300 175-5 [4], subclauses 13.8 and EN 300 175-7 [6], subclause 6.5.3. Figure 58 and table 64 together with the associated subclauses define the mandatory requirements with regard to the present document.

Figure 58: Cipher - switching initiated by FT

Table 64: Values used within the {CIPHER-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Cipher-info>>			
	<Y/N>	0	Disable ciphering. The support of this value is only mandatory if the procedure is used for feature N.25.
		1	Enable ciphering
	<Cipher-algorithm-id>	1	DECT standard cipher algorithm 1.
	<Cipher key type>	9	DCK.
	<Cipher key number>	8	Always IPUI/PARK pair (= subscription)

The {CIPHER-REQUEST} shall be sent before the transfer of any C-plane data intended to be encrypted (e.g. dialled number).

The DCK shall be produced and stored in advance using the storing the DCK procedure (see subclause 8.30). In order for the encryption mechanism to be activated at the MAC layer the NWK layer shall provide the encryption key by sending a DL-ENC_KEY.Req primitive to the DLC layer any time the encryption activation is requested. A new DCK may be produced and stored during the time a call is ciphered; this DCK shall not affect the current encryption mode.

Upon receipt, the <<Cipher-info>> shall be examined by the receiver. It is defined to be acceptable if the Y/N bit is consistent with the current cipher mode, the algorithm can be implemented, and the cipher key is available. Once this is accepted, Encryption activation/deactivation DLC and MAC services shall be invoked and ciphering shall be enabled/disabled at the MAC layer.

8.36.1 Associated procedure

8.36.1.1 Timer F-<MM_cipher.1> management

<MM_cipher.1>: Cipher-switching timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: An {CIPHER-REQUEST} message is sent;

Stop: An indication for link release from the DLC is received. An {CIPHER-REJECT} message or an indication from DLC layer for Y/N ciphering is received or an interrupting higher priority transaction begins.

8.36.2 Exceptional cases

8.36.2.1 PT rejects the cipher request

Possible reasons a cipher request to be rejected: Required Cipher algorithm is not supported; Required cipher key is not supported or is not available.

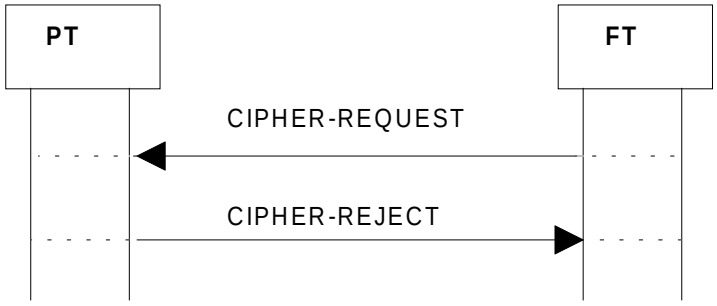


Figure 59: PT rejects the cipher request

Table 65: Standard values used within the {CIPHER-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Comments	Normative actions
			All optional	
Actions by the FT/PT: If a non-DECT cipher algorithm was requested and the ciphering has been rejected a new attempt shall be made requesting this time the DECT Standard Cipher Algorithm (DSCA).				

8.36.2.2 Timer F-<MM_cipher.1> expiry

Inconsistency of the Y/N bit with the current cipher mode is one of the possible reasons that shall not trigger an answer from the PT.

Upon expiry of F-<MM_cipher.1> the FT shall consider the procedure as failed. The FT shall not retransmit the {CIPHER-REQUEST} message and shall not restart the timer F-<MM_cipher.1> as part of the same procedure. However, the interworking unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.37 Cipher-switching initiated by PT

The procedure relates to the feature Encryption activation PT initiated N.24 and Encryption deactivation PT initiated N.26 and shall be performed as defined in EN 300 175-5 [4], subclause 13.8 and EN 300 175-7 [6], subclause 6.5.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The cipher-switching initiated by PT procedure consists of only one MM transaction.

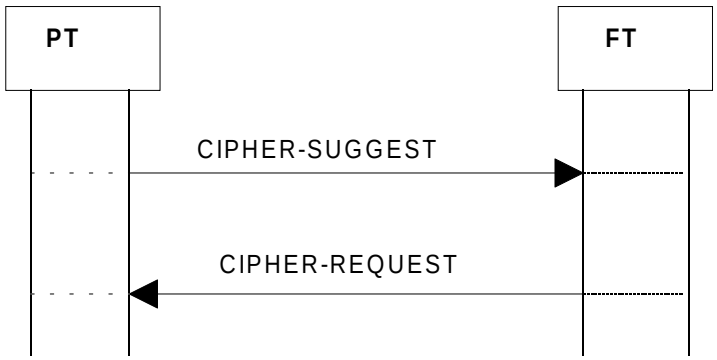


Figure 60: Ciphering, PT initiated

Table 66: Values used within the {CIPHER-SUGGEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Cipher-info>>			
	<Y/N>	0	Disable ciphering. Relates to feature N.26
		1	Enable ciphering. Relates to feature N.24
	<Cipher-algorithm-id>	1	DSCA
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= Subscription)

Table 67: Values used within the {CIPHER-REQUEST} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Cipher-info>>			
	<Y/N>	0	Disable ciphering. Relates to feature N.26
		1	Enable ciphering. Relates to feature N.24
	<Cipher-algorithm-id>	1	DSCA
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= Subscription)

The DCK shall be produced and stored in advance using the storing the DCK procedure (see subclause 8.30). In order for the encryption mechanism to be activated at the MAC layer, the NWK layer shall provide the encryption key by sending a DL-ENC_KEY.Req primitive to the DLC layer any time the encryption activation is requested. A new DCK may be produced and stored during the time a call is ciphered; this DCK shall not affect the current encryption mode.

Upon receipt, the <<Cipher-info>> shall be examined by the receiver. It is defined to be acceptable if the Y/N bit is consistent with the current cipher mode, the algorithm can be implemented and the cipher key is available. Once this is accepted the FT shall start the FT initiated cipher switching procedure, (see subclause 8.36 and the associated subclauses).

8.37.1 Associated procedure

8.37.1.1 Timer P-<MM_cipher.2> management

<MM_cipher.1>: Cipher-switching timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {CIPHER-SUGGEST} message is sent;

Stop: An indication for link release from the DLC is received. A {CIPHER-REJECT}or {CIPHER-REQUEST} message is received.

8.37.2 Exceptional cases

8.37.2.1 FT rejects the cipher request

Possible reasons a cipher request is rejected: required cipher algorithm is not supported; required cipher key is not supported or is not available.

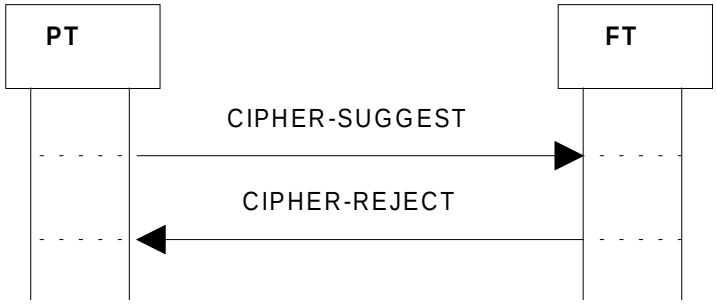


Figure 61: FT rejects the cipher requests

Table 68: Standard values used within the {CIPHER-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Comments	Normative actions
			All optional	
Actions by the FT/PT: If a non-DECT cipher algorithm was requested and the ciphering has been rejected a new attempt shall be made requesting this time the DSCA.				

8.37.2.2 Timer P-<MM_cipher.2> expiry

Inconsistency of the Y/N bit with the current cipher mode is one of the possible reasons that shall not trigger an answer from the FT.

Upon expiry of P-<MM_cipher.2> the PT shall consider the procedure as failed. The PT shall not retransmit the {CIPHER-SUGGEST} message and shall not re-start the timer P-<MM_cipher.2> as part of the same procedure. However, the inter-working unit/application layer may start the procedure again if necessary by sending the relevant primitive.

8.38 Indirect FT initiated link establishment

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 14.2.1 and 14.2.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

FT and PT shall only support short format for the {LCE-REQUEST-PAGE} message. Support of long format is not required as service attributes shall be negotiated and assigned during Call set-up or Call Resume that will follow the link establishment. When the FT request for a link establishment is successfully received by the intended PT, the PT shall initiate direct PT link establishment (see subclause 8.40).

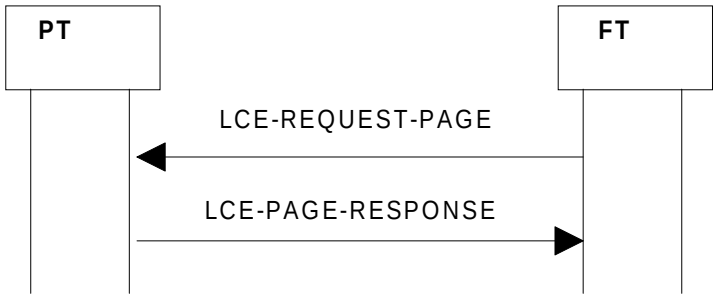


Figure 62: Indirect FT initiated link establishment

Table 69: Values used within the {LCE-REQUEST-PAGE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<LCE Header>>			
	<W>	All	For the relation between this field and the <LDE-header> field see EN 300 175-5 [4], subclause 8.2.1
	<LCE-header>	"001"	Unknown (MAC service type) & Ringing
<<Short address>>			
	<TPUI Address>	All	Part of the actual TPUI value or/and Ringing information, see EN 300 175-5 [4], subclause 8.2.1

Table 70: Values used within {LCE-PAGE-RESPONSE} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable identity>>			Depends upon subscription records.
	<Type>	0	IPUI
	<PUT>	All	
	<PUN>	All	
<<Fixed identity>>			Parameters depends upon subscription records.
	<Type>	32	PARK
	<Length of identity value>	All	PLI+1
	<ARC+ARD>	All	

8.38.1 Associated procedure

8.38.1.1 Timer F-<LCE.03> management

There shall be separate instances of a <LCE.03> timer corresponding to each IPUI identity that has been paged with {LCE-REQUEST-PAGE} message.

<LCE.03>: {LCE-REQUEST-PAGE} message re submission timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A {LCE-REQUEST-PAGE} message is sent;

Stop: A {LCE-PAGE-RESPONSE} message with a matching IPUI or a release from the higher entity is received.

8.38.1.2 Normal paging

The FP should transmit the {LCE-REQUEST-PAGE} to DLC included into a DL_BROADCAST_req primitive. At the receiving side the event shall be indicated to the LCE respectively with a DL_BROADCAST_ind primitive. For the possible contents of the related primitives see EN 300 175-4 [3], subclause 8.3.3.1.

8.38.1.3 Fast paging

FP shall always initiate "Fast paging" if the PP has indicated into the <Set-up-capability>, see subclauses 8.31 and 8.33, that it supports Fast Paging, otherwise the FP shall initiate "Normal Paging".

In case the PP has indicated as well "Fast set-up" capabilities the FP shall use the Direct link establishment procedure in precedence to the Indirect link establishment procedure.

The FP should transmit the {LCE-REQUEST-PAGE} to DLC included into a DL_EXPEDITED_req primitive. At the receiving side the event shall be indicated to the LCE respectively with a DL_EXPEDITED_ind primitive. For the possible contents of the related primitives see EN 300 175-4 [3], subclause 8.3.3.2.

8.38.2 Exceptional cases

8.38.2.1 The IPUI received in the {LCE-PAGE-RESPONSE} does not match

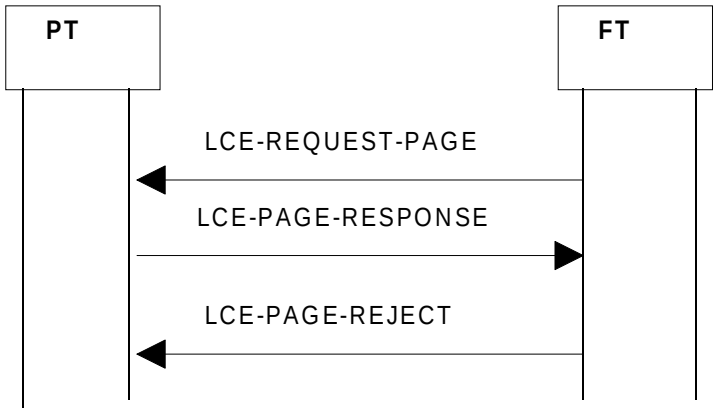


Figure 63: The IPUI received in the {LCE-PAGE-RESPONSE} does not match

Table 71: Values used within the short format {LCE-PAGE-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Portable identity>>			It shall be the full IPUI of the PT that is rejected
	<Type>	IPUI	
	<PUT>	All	
	<PUN>	All	

The unwanted link shall immediately be released using the Link release "normal" procedure (see subclause 8.41).

The {LCE-PAGE-REJECT} message shall be sent by a DL-DATA-req primitive via the Service Access Point (SAP) (SAP Identifier (SAPI) = "0") using the same Data Link Endpoint Identifier (DLEI) as indicated by the DL-ESTABLISH-ind carrying 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.

8.38.2.2 Timer <LCE.03> expiry

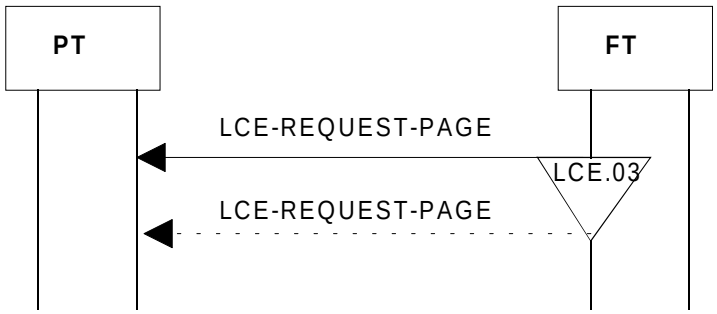


Figure 64: Timer <LCE.03> expiry

If timer <LCE.03> expires before the wanted link is established, the LCE may resubmit the {LCE-REQUEST-PAGE} message; in this case the link shall remain in the "ESTABLISH-PENDING" state. 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.

NOTE: N300 is an application specific value. Recommended value for voice applications is three (3).

8.38.2.3 Release from the higher entity

If the higher entity indicates that the link resources are no longer required the LCE shall immediately delete the outstanding IPUI and stop the corresponding timer <LCE.03>.

8.39 Direct FT initiated link establishment

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 14.2.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The FT shall always use this procedure if the relevant PT has indicated in its <<Set-up capability>>, see subclauses 8.31 and 8.33, that it supports "Fast Set-up". In this procedure there shall be no peer-to-peer NWK layers message exchange.

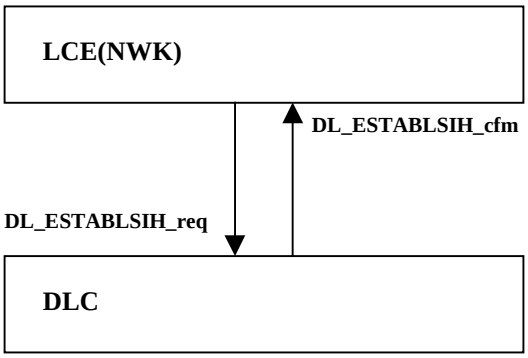


Figure 65: Direct FT initiated link establishment, initiating side

Table 72: Values used within the DL-ESTABLISH-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	see EN 300 175-4 [3], subclause 7.3.6
<<Establish mode>>		
	Class A operation	

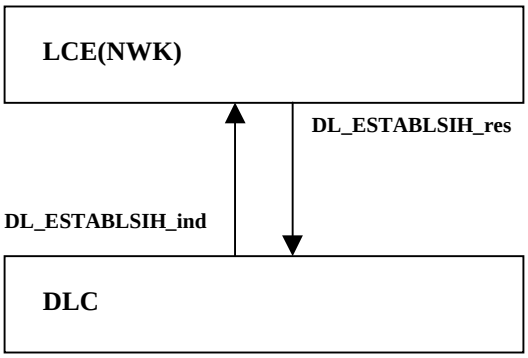


Figure 66: Direct FT initiated link establishment, receiving side

Table 73: Values used within the DL-ESTABLISH-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Establish mode>>		
	Class A operation	

8.39.1 Exceptional case

8.39.1.1 Link establishment failure

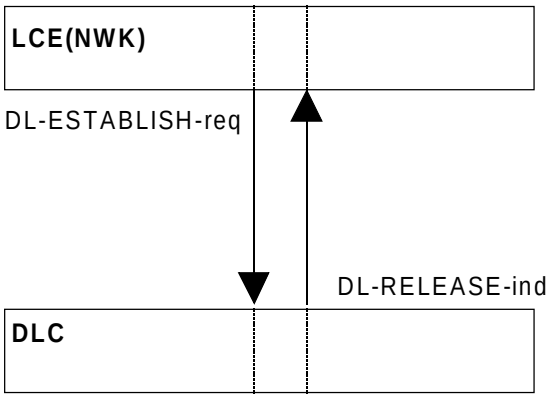


Figure 67: Direct FT initiated link establishment failure

Table 74: Values used within the DL-RELEASE-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Abnormal	
Actions by the FT/PT: The LCE shall inform all higher entities requesting the use of the link that the link establishment has failed and shall enter "LINK-RELEASED" state.		

8.40 Direct PT initiated link establishment

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 14.2.1 and 14.2.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Direct PT initiated link establishment shall occur when the first service requested is detected by the LCE in the PT. In this procedure there shall be no peer-to-peer NWK layers message exchange except if the procedure is used in an indirect FT link establishment procedure. In the latter case a {LCE-PAGE-RESPONSE} message shall be sent.

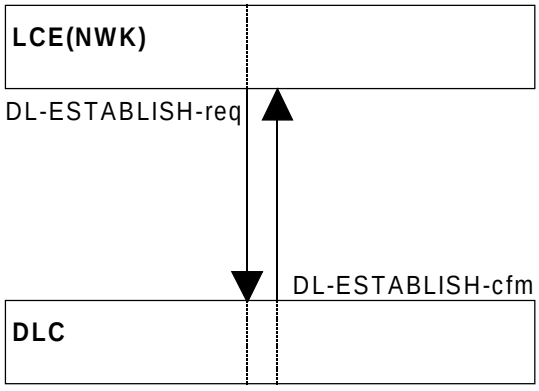


Figure 68: Direct PT initiated link establishment, initiating side

Table 75: Values used within the DL-ESTABLISH-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	see EN 300 175-4 [3], subclause 7.3.6
<<Establish mode>>		
	Class A operation	
	Class B operation	
<<Message unit length>>	The length of the higher layer information	Included only when the parameter <<Message unit>> follows.
<<Message unit>>	Higher layer information	The PT shall use the <<Message unit>> parameter to carry the {LCE-PAGE-RESPONSE} message when the procedure is used as a part of an indirect FT initiated link establishment (see subclause 8.38) otherwise it shall be empty.

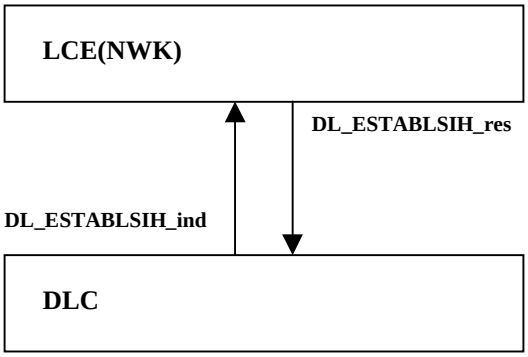


Figure 69: Direct PT initiated link establishment, receiving side

Table 76: Values used within the DL-ESTABLISH-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Establish mode>>		
	Class A operation	
	Class B operation	
<<Message unit length>>	The length of the higher layer information	Included only when the parameter <<Message unit>> follows.
<<Message unit>>	Higher layer information	The PT shall use the <<Message unit>> parameter to carry the {LCE-PAGE-RESPONSE} message when the procedure is used as a part of an indirect FT initiated link establishment (see subclause 8.38) otherwise it shall be empty.

8.40.1 Exceptional case

8.40.1.1 Link establishment failure

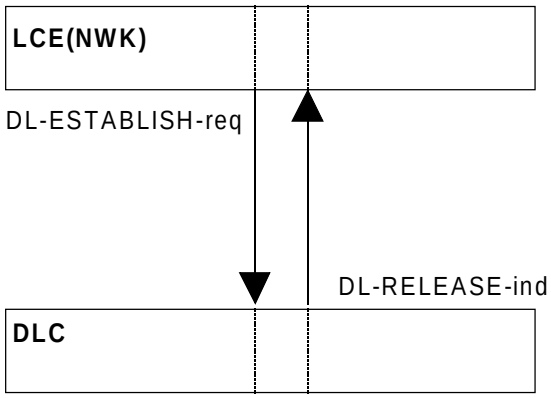


Figure 70: Direct PT initiated link establishment failure

Table 77: Values used within the DL-RELEASE-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Abnormal	
Actions by the FT/PT: The LCE shall inform all higher entities requesting the use of the link that the link establishment has failed and shall enter "LINK-RELEASED" state.		

8.41 Link release "normal"

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 14.2.7. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

In this procedure there is no peer-to-peer NWK layer message exchange, only NWK(LCE) to DLC layer information exchange thereby invoking services from the lower layers.

The "normal" release allows the DLC to complete transmission of any outstanding messages before releasing the link.

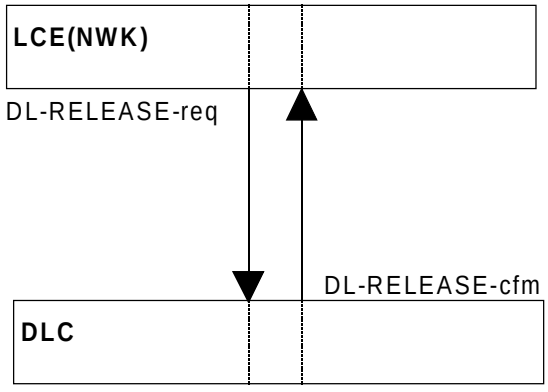


Figure 71: Link release "normal", initiating side

Table 78: Values used within the DL-RELEASE-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Normal	

Table 79: Values used within the DL-RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Normal	

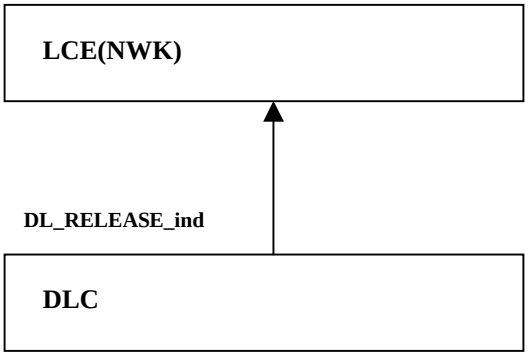


Figure 72: Link release "normal", receiving side

Table 80: Values used within the DL-RELEASE-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Normal or Abnormal	
Actions by the FT/PT: The LCE shall inform all higher entities using the link that the link has been released and shall enter "LINK-RELEASED" state.		

8.41.1 Associated procedure

8.41.1.1 Timer <LCE.01> management

<LCE.01>: Link release timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A DL-RELEASE-req primitive is sent;

Stop: A DL-RELEASE-cfm primitive is received.

8.41.2 Exceptional cases

8.41.2.1 Timer <LCE.01> expiry

If the <LCE.01> expires before a DL-RELEASE-cfm is received (e.g. the transmission of outstanding data needs more time) a new request for link release shall immediately be issued this time indicating release mode as "abnormal".

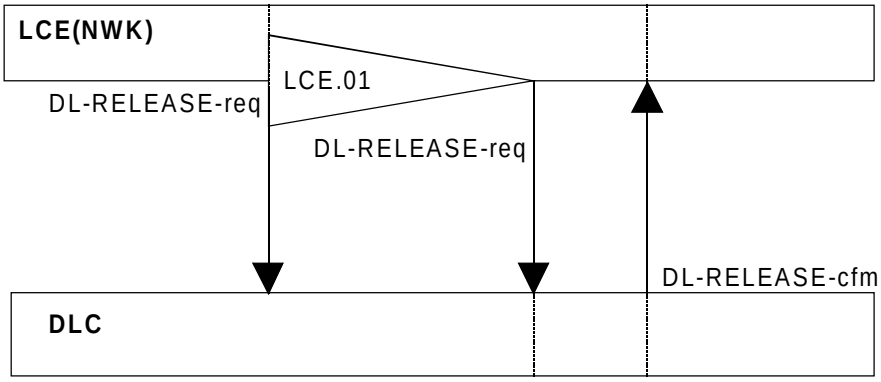


Figure 73: Timer <LCE.01> expiry

Table 81: Values used within the DL-RELEASE-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Abnormal	

Table 82: Values used within the DL-RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Normal or Abnormal	

8.41.2.2 Outstanding data has been discarded

Even if the requested release mode was "normal" the DL-RELEASE-cfm primitive may indicate "abnormal" release mode (e.g. if any DL-DATA-req or I-frames were discarded or were unacknowledged because of time-out or other problems at the lower layers).

The primitive's exchange is the same as in link release "normal", except the information that is to be carried back in the DL-RELEASE-cfm primitive.

Table 83: Values used within the DL-RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	See EN 300 175-4 [3], subclause 7.3.6
<<Release mode>>		
	Abnormal	

8.42 Link release "abnormal"

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 14.2. The following text defines the mandatory requirements with regard to the present document.

The "abnormal" release requires the DLC to release immediately the link without completing the transmission of any outstanding data.

The procedure description differs from the link release "normal" procedure description (see subclause 8.41) only in the release mode identification which here shall be set to "Abnormal". Subclauses 8.41.1 and 8.41.2 are not relevant to link release "abnormal" procedure.

8.43 Link release "maintain"

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 14.2.7. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Every higher entity shall provide an explicit notification to the LCE when it ceases to use a link. This notification shall indicate if the entity requires the link to be maintained. If the higher entity requires the link to be maintained then it shall indicate release reason "partial release" and the LCE shall start timer <LCE.02> (even if the timer is already running).

If the higher entity does not require the link to be maintained and no other higher entities are using it and no LCE timers are running then the LCE shall release the link.

On expiry of timer <LCE.02> when no higher entities are using the link and no other LCE timers are running the LCE shall release the link immediately using the "abnormal" release procedure (see subclause 8.42). No action shall be taken on expiry of timer <LCE.02> if any higher layer entity is still using the link or any other LCE timer is running.

The MM (except after a location registration procedure with TPUI assignment has been accomplished), Call Independent Supplementary Service (CISS) and ConnectionLess Message Service (CLMS) shall always indicate that the link shall be maintained using partial release. If CC wants to maintain the link it shall first initiate partial release procedure (see subclause 8.8) the support of this procedure is optional.

8.43.1 Associated procedure

8.43.1.1 Timer <LCE.02> management

<LCE.02>: Link maintain timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: A higher entity indicates partial release to the LCE;

Stop: An indication for link release from the DLC layer has been received.

8.44 Link Suspend

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 16.2.6 and 14.2.6.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If request for suspension of a link is received by the LCE and the link is a class A operation link the LCE shall initiate a normal link release procedure by issuing a DL_RELEASE-req primitive to the DLC layer indicating "normal". 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. Before releasing the link the DLC shall try to transmit all outstanding messages/frames.

At the receiving side, a request for suspension of a class A link is indicated with a DL_RELEASE-ind primitive indicating "normal" at the time when the LCE has knowledge that suspension has been initiated (suspension has been in advance agreed with higher layer messages exchanged). The LCE shall accept the suspension, shall immediately mark the link as "LINK SUSPENDED" and shall inform the CC entity for the success. No further messages shall then be submitted, without first invoking link resumption. The case that LCE has no knowledge for suspension shall be handled as a normal link release procedure as described in subclause 8.41.

The success of the suspension shall be indicated to the initiating LCE by a DL_RELEASE-cfm primitive indicating "normal". Upon this the initiating LCE shall stop timer <LCE.04>, shall mark the link as "LINK SUSPENDED" and shall inform the CC entity for the success.

NOTE: If there are any queued messages the link should be immediately resumed.

8.44.1 Associated procedures

8.44.1.1 Timer LCE.04 management

<LCE.04>: Link Suspend and Resume timer;

Value: Refer to EN 300 175-5 [4], annex A;

Start: LCE has taken action on request for link suspension/resumption from higher layer entity;

Stop: Action for suspension/resumption at LCE has been completed.

8.44.2 Exceptional cases

8.44.2.1 Abnormal release

Upon receipt of a DL_RELEASE-cfm primitive indicating "abnormal" (i.e. frames have been discarded, data has been lost), the initiating LCE shall stop timer <LCE.04>, shall mark the link as "LINK SUSPENDED" and shall inform the CC entity for the failure.

The CC shall initiate realize of the call submitting a {CC-RELEASE-COM} message to LCE (i.e. resume procedure shall be initiated).

8.44.2.2 Timer LCE.04 expires

If timer LCE.04 expires before DL_RELEASE-cfm primitive has been received the LCE shall inform the Management entity in which responsibility shall be the action in response.

NOTE: A reason of such a delay may be difficulties at DLC of transmitting outstanding frames.

8.45 Link Resume

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 16.2.6 and 14.2.6.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If request for resume of a link is received by the LCE when the state of the link is "LINK SUSUPENDED" and the link is a class A operation link the LCE shall initiate a proper link establishment procedure depending on the capabilities of the initiating and the receiving side, i.e. Fast or Normal paging, Direct or Indirect link establishment, see subclauses 8.44. With the following modifications: the link shall be then marked as "RESUME PENDING", timer <LCE.04> shall be started (for the handling of timer LCE.04 see subclause 8.44). All messages for this link shall be queued until a response is received from the DLC.

Successful establishment of the link shall lead to marking the link as "LINK ESTABLISHED". The initiating side shall stop timer <LCE.04>; any queued messages shall be immediately transmitted using DL_DATA-req primitives.

8.45.1 Exceptional cases

8.45.1.1 The receiving side cannot recognize whether this is a resumption

The receiving side may not be able to distinguish whether the request for a link is a request for resumption of a suspended link or a request for an independent new link related to the same FT/PT.

This should be at least established upon the receipt of the first higher layer message and appropriate action shall be taken. In any case the link shall be marked as "LINK ETSBLISHED".

In case it was not recognized whether the request was for link resumption, and the higher layer message received is a {CC-SETUP} message the receiving entity should react depending on the available resources. If it decides to reject the new CC call it shall send the {CC-RELEASE-COM} message, release the link "abnormal", and mark the link back to "LINK SUSPENDED".

8.45.1.2 Link failure

Rejection is indicated to both the receiving LCE and the initiating LCE with DL_RELEASE primitives. In this event, the initiating LCE shall stop timer <LCE.04> and shall inform the CC for the failure.

8.45.1.3 Timer LCE.04 expires

If timer LCE.04 expires before DL_ESTABLISH-cfm primitive has been received the LCE shall inform the Management entity in which responsibility shall be the action in response.

9 DLC layer procedures C-plane

9.1 Class A PT initiated link establishment

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 9.2.3.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

If, class B acknowledged transfer is requested but not supported (B acknowledged transfer is not required to be supported for GAP) by the receiving side, the I_frame requesting class B operation shall be treated as though it was a class A frame, see EN 300 175-4 [3], subclause 9.2.4.3.1 b).

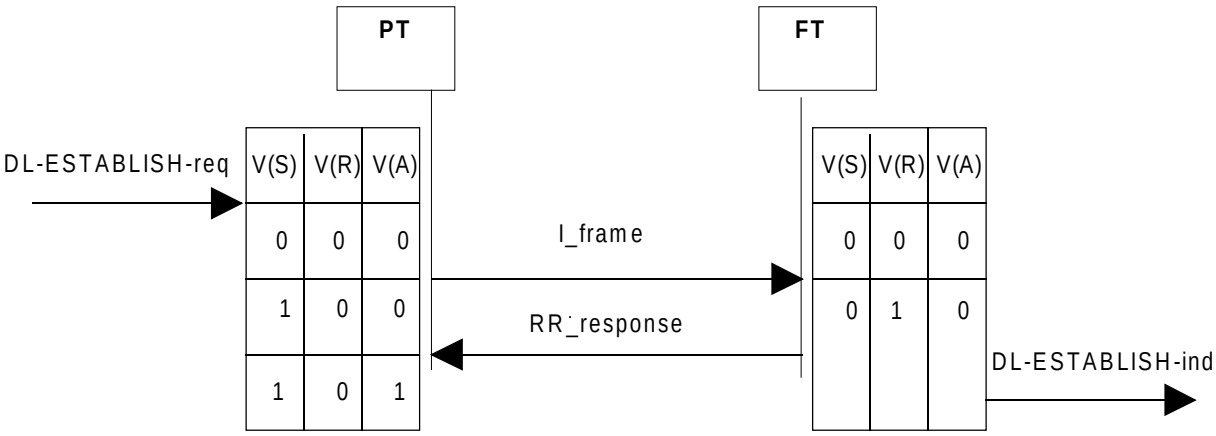


Figure 74: Class A link establishment

Table 84: Values used within the I-frame

Field	Parameter within the field	Standard values within the field/parameter	Normative action/comment
<<Address-field>>			
	<NLF>	1	New link
	<LLN>	1	Class A operation
	<SAPI>	0	Connection oriented
	<C/R>	0	PT command
	<RES>	1	
<<Control-field>>			
	<N(R)>	0	N(R)=V(R)
	<P>	0	Ignore
	<N(S)>	0	N(S)=V(S)
<<Length-indicator-field>>			
	<Li>	0	No higher layer information
		1..63	Higher layer info length
	<M>	All	
	<N>	1	No extended length field. If "0" the frame may be discarded
<<Information field>>		All appropriate	Higher layer information. If <Li> field indicates "0" shall be omitted. This field shall be used to carry the {LCE-PAGE-RESPONSE} message in case of FT initiated indirect link establishment.
<<Fill field>>		11110000B	Ignore. 0 to 4 such octets may be included in case for the Cs logical channel, as the Frame Length (FLEN) mod 5 = 0. If <Li> indicates "0", no <Fill filed> is required.
<<Checksum field1>>		All	The contents shall be calculated using two elements: LSIG see EN 300 175-4 [3] subclause 10.3.1; underlying checksum calculation based on ISO/IEC 8073 [12]
<<Checksum field2>>		All	See above

Table 85: Values used within the {RR-Frame} S-format message

Field	Parameter within the field	Standard values within the field/parameter	Normative action/comment
<<Address-field>>			
	<NLF>	1	New link
	<LLN>	1	Class A operation
	<SAPI>	0	Connection oriented
	<C/R>	0	FT response
	<RES>	1	
<<Control-field>>			
	<N(R)>	1	N(R) = V(R)
	<P/F>	0	Ignore
	<SS>	0	
	<***>	1	constant
<<Length-indicator-field>>			
	<Li>	0	No higher layer information
	<M>	0	
	<N>	1	No extended length field. If "0" the frame may be discarded
<<Checksum field1>>		All	
<<Checksum field2>>		All	

9.1.1 Associated procedures

9.1.1.1 Timer P<DL.07> management

<DL.07>: Class A establishment timer;

Value: Refer to EN 300 175-4 [3], annex A;

Start: A Class A link establishment I_frame is transmitted;

Stop: On receipt of: a Class A errorless RR_response with the New Link Flag (NLF) bit set to "1"; a DL-RELEASE-req primitive indicating "abnormal"; a MAC_DIS.Ind primitive.

9.1.1.2 Retransmission counter management

Refer to EN 300 175-4 [3], subclauses 9.2.3.1 and 9.2.3.6.

Each LAPC entity shall maintain an internal Retransmission count variable determining the maximum number of retransmissions of an I_frame. The default value shall be 3.

For Class A operations the Retransmission counter shall be reset any time a new I_frame has been sent.

9.1.1.3 Multiple frame operation variables management

Refer to EN 300 175-4 [3], subclause 7.5.2.

For the DLC layer acknowledged transfer to be performed the V(S), V(A), and V(R) operation variables together with their appropriate management shall be supported.

The allowed values of all state variables for a given class of operation shall always be defined by the modulus operation. For Class A operation, the modulus equals 2.

9.1.1.4 Lower Layer Management Entity (LLME) establishment of a MAC connection

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.2. and EN 300 175-3 [2], subclause 8.1.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

For a link to be established a suitable MAC connection is needed. If such one does not exist the LLME shall request it.

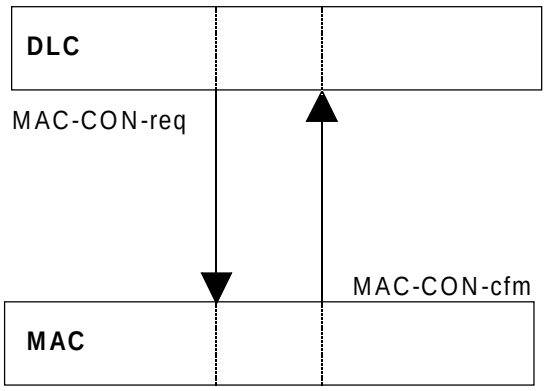


Figure 75: Establishment of a MAC connection initiating side

Table 86: Values used within the MAC_CON-req primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<PMID>>	Portable part MAC Identity (PMID)	See subclause 14.4.
<<CHO flag>>	Y/N	Y - if the connection is required for Connection handover
<<Old MCEI>>	All relevant	Only needed for Connection handover and Basic type connections
<<Cf required>>	No	
<<Slot type>>	full slot	
<<Service type>>	In_minimum_delay or C-channel only	
<<connection type>>	basic	

Table 87: Values used within the MAC_CON-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<Connection type>>	Basic	The type of the established connection

The receiving side shall be informed about the action that has taken place in case it was successful by a MAC_CON.Ind primitive.

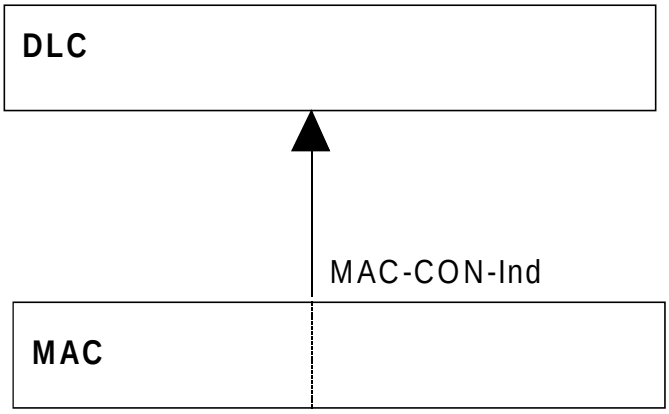


Figure 76: Establishment of a MAC connection receiving side

Table 88: Values used within the MAC_CON.Ind primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<PMID>>	PMID	(See subclause 13.4 14.4.
<<CHO flag>>	Y/N	Y - if the connection is required for Connection handover
<<Cf required>>	No	
<<Slot type>>	full slot	
<<Service type>>	In_minimum_delay or C-channel only	
<<connection type>>	basic	

9.1.2 Exceptional cases

9.1.2.1 Timer P<DL.07> expiry

If a RR response is received with the NLF bit set to "0" or containing errors the LAPC entity shall discard it. If the peer find errors in the I_frame, response shall not be generated. In both cases timer P<DL.07> shall expire. An action shall be taken according to EN 300 175-4 [3], subclause 9.2.3.1.

9.1.2.2 Receipt of a request for link release

If DL-RELEASE-req primitive is received timer P<DL.07> shall be stopped. Class A link release procedure shall be performed (see subclause 9.3).

9.1.2.3 Receipt of an indication for a connection release

Timer P<DL.07> shall be stopped, all outstanding data shall be discarded, and, the NWK layer shall be informed for the MAC failure by DL-RELEASE-ind primitive.

9.2 Class A FT initiated link establishment

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 9.2.3.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The procedure description is similar to the "Class A PT initiated link establishment" with the difference that frames and primitives indicated as PT initiated shall be FT initiated and vice versa.

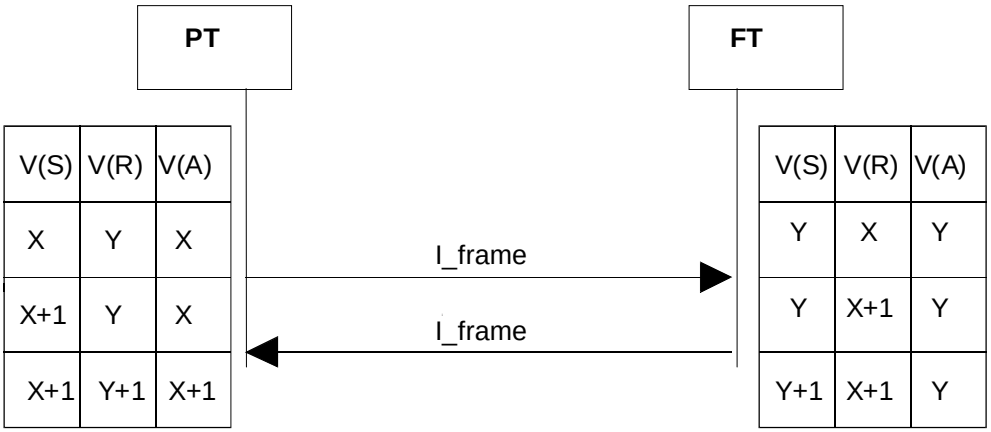
9.2.1 Class A Acknowledged Information transfer

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 9.2.3.2, 9.2.3.3, 9.2.3.4, 9.2.3.5, and 9.2.3.6. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The following cases, depending on the frame which confirms the reception of the frame-request, shall be supported:

- acknowledgement with an I_frame;
- acknowledgement with a RR_frame.

9.2.1.1 Acknowledgement with an I_frame



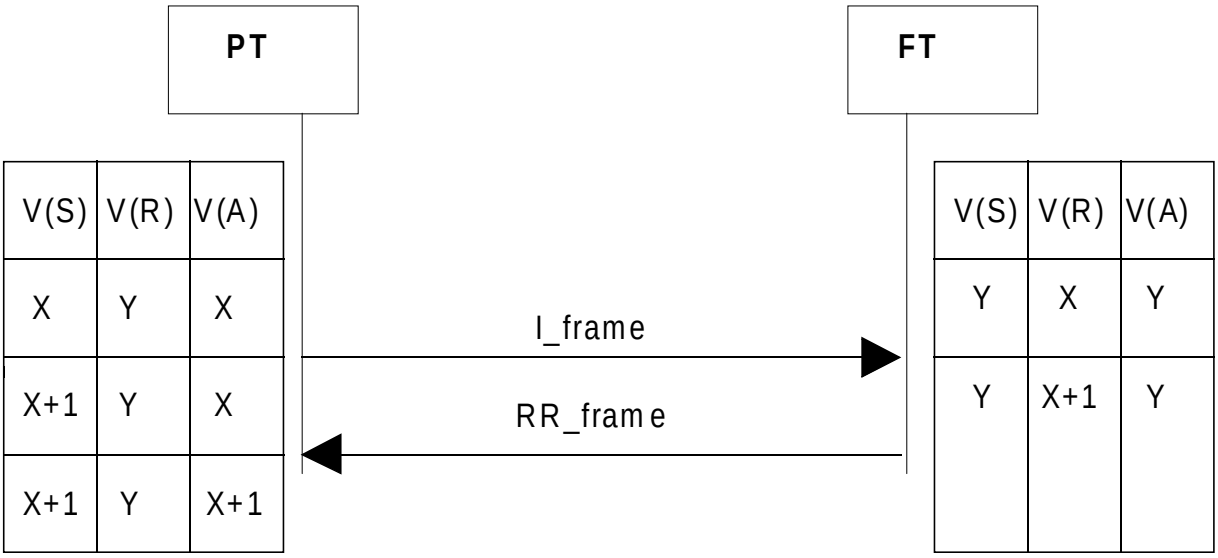
NOTE 1: During the calculation of the variable's values the assumptions have been made that the I_frame sent by PT is not used for acknowledgement of previous received I_frames and, both frames are not retransmission.
NOTE 2: A Class A acknowledged information transfer procedure is considered as successful for the Initiator when in case N(S) is sent and N(R) is received the next equation is valid: (N(S)+1)mod2=N(R).
NOTE 3: The I_frame sent by the FT is assumed to be acknowledged as well. (not indicated in the figure).
NOTE 4: The case when FT initiates differs only in the notations.

Figure 77: Class A acknowledge information transfer by I_frame, PT initiated

Table 89: Values used within the I-Frame sent by the PT(FT)

Field	Parameter within the field	Standard values within the field/parameter	Normative action/comment
<<Address-field>>			
	<NLF>	0	
	<LLN>	1	Class A operation
	<SAPI>	0	Connection oriented
	<C/R>	0	From PT
		1	From FT
	<RES>	1	
<<Control-field>>			
	<N(R)>	=V(R)	In I_frame transmitter
	<P>	0	Ignore
	<N(S)>	=V(S)	In I_frame transmitter
<<Length-indicator-field>>			
	<Li>	1..63	higher layer info length
	<M>	All	
	<N>	1	No extended length field. If "0" the frame may be discarded
<<Information field>>		All relevant	Higher layer information
<<Fill field>>		11110000B	Ignore. 0 to 4 such octets may be included in case for the Cs logical channel
<<Checksum field1>>		All	
<<Checksum field2>>		All	

9.2.1.2 Acknowledgement with a RR_frame



NOTE 1: During the calculation of the variable's values an assumption has been made that the I_frame sent by PT is not used for acknowledgement of previous received I_frames and is not a retransmission.
NOTE 2: A Class A acknowledged information transfer procedure is considered as successful for the Initiator when in case N(S) is sent and N(R) is received the next equation is valid: (N(S)+1)mod2=N(R).
NOTE 3: The case when FT initiates differs only in the notations.

Figure 78: Class A acknowledge information transfer by RR_frame

The values used within the {I-Frame} shall be the same as in the case Acknowledgement with an I_frame, (see table 89).

Table 90: Values used within the {RR-Frame} S-format message

Field	Parameter within the field	Standard values within the field/parameter	Normative action/comment
<<Address-field>>			
	<NLF>	0	
	<LLN>	1	Class A operation
	<SAPI>	0	Connection oriented
	<C/R>	0	From FT
		1	From PT
	<RES>	1	
<<Control-field>>			
	<N(R)>	=V(R)	In RR-frame transmitter
	<P/F>	0	Ignore
	<SS>	0	
	<***>	1	Constant
<<Length-indicator-field>>			
	<Li>	0	No higher layer information
	<M>	0	
	<N>	1	No extended length field. If "0" the frame may be discarded
<<Checksum field1>>		All	
<<Checksum field2>>		All	

9.2.1.3 Class A acknowledged information transfer with segment reassemble

As the required length of a NWK layer message to be supported is 63 octets (see subclause 6.9.3) the segmentation of NWK layer messages in the DLC layer is not required to be supported for implementations complying to GAP.

If an implementation supporting longer messages wants to access a GAP implementation which does not support segmentation, the last shall act as follows:

- acknowledge the receipt of each error free, in sequence segment;
- do not store any segment after the first;
- deliver to its own NWK layer only the first segment.

9.2.1.4 Associated procedures

9.2.1.4.1 Timer <DL.04> management

DL.04>: Re transmission timer;

Value: Refer to EN 300 175-4 [3], annex A;

Start: A I_frame is transmitted;

Stop: On receipt of: an acknowledgement for that frame; a DL-RELEASE-req primitive indicating "abnormal"; a MAC_DIS-ind primitive.

9.2.1.4.2 Re transmission timer management

Refer to subclause 9.1.1.2.

9.2.1.4.3 Multiple frame operation variables management

Refer to subclause 9.1.1.3.

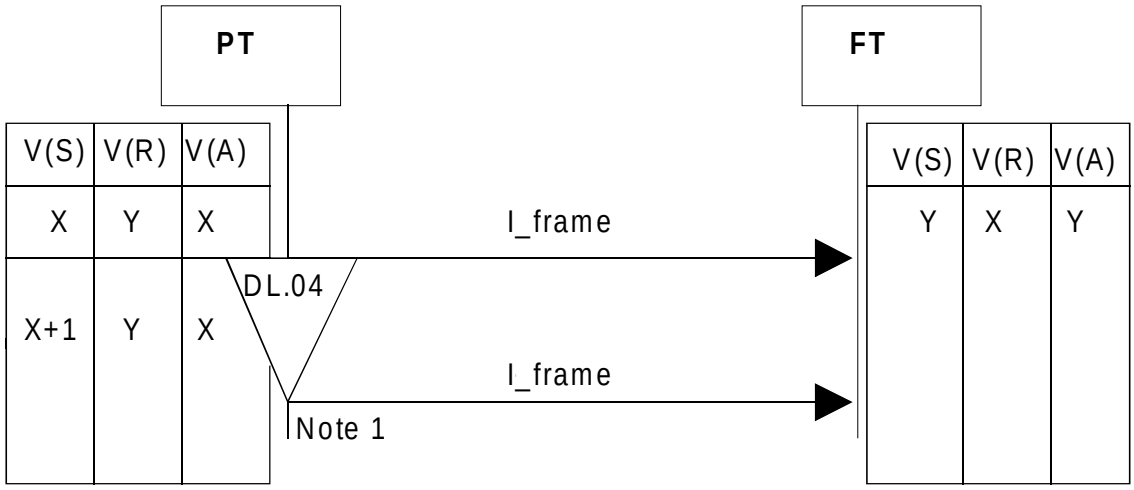
9.2.1.5 Exceptional cases

9.2.1.5.1 Timer <DL.04> expiry

Refer to EN 300 175-4 [3], subclause 9.2.3.6.

An erroneous I-frame shall be discarded and therefore shall not generate peer response.

An erroneous frame-acknowledgement shall be discarded and timer <DL.04> shall not be stopped.



NOTE 1: The I_frame is retransmitted only if N250<max.value.
NOTE 2: During the calculation of the variable's values an assumption has been made that the I_frames sent are not used for acknowledgement of previous received I_frames and the first one is not a retransmission.
NOTE 3: The case when FT initiates differs only in the notations.
NOTE 4: The contents of the retranslated frame shall be exactly the same as the first one.

Figure 79: Timer <DL.04> expiry

The values used within the {I-Frame} shall be the same as in the case acknowledgement with an I_frame, (see table 89).

9.2.1.5.2 Receipt of a request for link release

On receipt of a DL-RELEASE.req after a I-frame has been transmitted timer <DL.04> shall be stopped, and, class A link release procedure (see subclause 9.3) shall be performed.

9.2.1.5.3 Receipt of an indication for a connection release

On receipt of an indication from the MAC layer for a release meaning either a bearer release started by the MAC layer or a bearer release resulting from a link release initiated by the peer, the timer <DL.04> shall be stopped and class A Link release procedure (see subclause 9.3) shall be performed.

9.2.1.5.4 DLC wants to make a connection handover

See class A basic connection handover procedure given in subclause 12.7.

9.3 Class A link release

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 9.2.3.7, 9.2.7.1.2, 10.2.2, and 10.4.1, EN 300 175-3 [2], subclause 8.1.6, and EN 300 175-5 [4], subclause 17.9. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The procedure is initiated on receipt of a DL-RELEASE-req primitive (see subclause 8.41) or a MAC_DIS.Ind primitive.

On receipt of a MAC_DIS.Ind primitive DLC shall release the link.

A link release procedure is qualified as "normal" if no outstanding I-frames or outstanding DL-DATA-req primitives have been discarded before the link has been released.

Even if in the DL-RELEASE-req primitive a "normal" link release has been requested, the DLC layer might be unable to process all outstanding data. If any outstanding I-frames or DL-DATA-req primitives were or have to be discarded the release is qualified as "abnormal" and the resulting "abnormal" release mode shall be indicated in the DL-RELEASE-cfm and DL-RELEASE-ind primitives respectively.

9.3.1 Associated procedures

9.3.1.1 LLME U-plane release

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.4.2.

9.3.1.2 LLME release of a MAC connection

The procedure shall be performed as defined in of EN 300 175-4 [3], subclause 10.2 and EN 300 175-3 [2], subclause 8.1.6.

9.4 Class A link re-establishment

The procedure shall be performed as defined in of EN 300 175-4 [3], subclause 9.2.3.8 and EN 300 175-5 [4], subclause 17.8. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

A class A link may be re-established at any time using the procedure for class A link establishment, (see subclause 9.1). All outstanding DL-DATA primitives and I-frames shall be discarded, and all link variables shall be reset.

Alternatively an implementation is permitted to release the link after receipt of an I-frame with NLF flag set to "1".

A link shall not be re-established whilst in the "RELEASE-PENDING" state, see EN 300 175-5 [4], subclause 14.2.7.

9.5 Cs channel fragmentation and recombination

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 6.1.2, 6.1.3, 6.1.4, 6.1.4.2. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The complete frame shall be fragmented into 5 octet fragments.

9.6 Selection of logical channels

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.2.5. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

10 Connection modification

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.2.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

During the establishment of advanced connections, whenever the MAC_CON-req primitive has specified a multi-bearer connection or the connection type as "unknown" a MAC_MOD-req primitive shall be sent to identify the exact connection attributes. The primitive shall not be sent immediately after the MAC_CON-req primitive instead it shall be delayed in order to allow some higher layer exchanges to occur using a C_S only MAC service. These higher layer exchanges shall be used to agree the wanted service, which shall then be invoked at the MAC layer using the MAC_MOD primitives.

Connection modification may be used to modify service attributes of established advanced connections of known service type. This may be used by the LLME to optimize the use of the resources by changing the bandwidth of existing connections (including the complete reversal of unidirectional connections) in response to service demands or it may be used in response to a NWK layer request for changing the connection characteristics (i.e. slot type, service type). C_S service data integrity shall always be preserved during connection modification, but changes to connection bandwidth, service type and slot type may result in data sequencing errors and/or erasures for the I_P logical channel. If the "minimum bearers" parameter is changed to a value greater than the actual bandwidth, the connection will be released if the MAC cannot achieve the new requirement.

Connection modification may occur during connection handover as well.

Table 91: Values used within the MAC_MOD-req primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<ECN>>	All	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<Slot type>>	Full slot	
<<switching>>	non	
<<Service type>>	I_P_error_correction	
<<Max lifetime>>	All	As agreed by the higher layers
target number of uplink simplex bearers	All	As agreed by the higher layers
minimum acceptable uplink simplex bearers	All	As agreed by the higher layers
minimum acceptable downlink simplex bearers	All	As agreed by the higher layers

Table 92: Values used within the MAC_MOD-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<ECN>>	All	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<Slot type>>	Full slot	
<<switching>>	non	
<<Service type>>	I_P_error_correction	
<<Max lifetime>>	All	As agreed by the higher layers
result	accept/reject	

Table 93: Values used within the MAC_MOD-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to EN 300 175-4 [3], subclause 10.2.4.4
<<ECN>>		Refer to EN 300 175-4 [3], subclause 10.2.4.4
result	accept/reject	

10.1 Normal broadcast

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 6.2.1, 8.3.3.1, 9.4.1.1 and 9.4.1.2 and EN 300 175-3 [2], subclause 8.2.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Only short frame format (frame length = 3) is required to be supported.

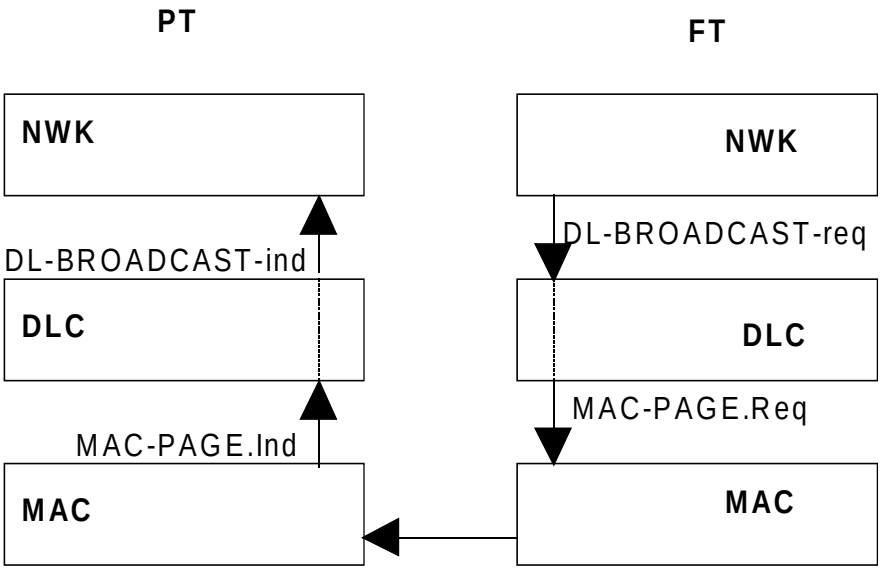


Figure 80: Normal broadcast

Table 94: Information used within the DL-BROADCAST-req primitive

Parameter	Information within the parameter	Normative action/comment
<<Cluster address list>>	all cluster / an integer	
<<Message unit length>>	3 octets	Only short frame format is required to be supported
<<Message unit>>	From the NWK layer	

Table 95: Information used within the MAC_PAGE.Req primitive

Parameter	Information within the parameter	Normative action/comment
<<cluster ID>>	all clusters / an integer	
<<page type>>	normal	"fast" is not required to be supported.
<<length of page field>>	0 or 20	
<<SDU>>	The data from the <<Message unit>> received in the DL-BROADCAST-req primitive	

Table 96: Information used within the MAC_PAGE.Ind primitive

Parameter	Information within the parameter	Normative action/comment
<<length of page field>>	20	
<<SDU>>		

Table 97: Information used within the DL-BROADCAST-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<Message unit length>>	3 octets	
<< Message unit>>	The data from the <<SDU>> from the MAC_PAGE.Ind primitive	

10.2 Expedited Broadcast

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 6.2.1, 8.3.3.1, 9.4.2.1 and 9.4.2.2 and EN 300 175-3 [2], subclause 8.2.1. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The primitive exchange and their contents is similar to the Normal Broadcast except that the DL_EXPEDITED primitives are used instead of the DL_BROADCAST and the type of broadcast is identified as "fast".

Only short frame format (frame length = 3) is required to be supported.

Table 98: Information used within the DL-EXPEDITED-req primitive

Parameter	Information within the parameter	Normative action/comment
<<Cluster address list>>	all cluster / an integer	
<<Message unit length>>	3 octets	Only short frame format is required to be supported
<<Message unit>>	From the NWK layer	

Table 99: Information used within the MAC_PAGE.Req primitive

Parameter	Information within the parameter	Normative action/comment
<<cluster ID>>	all clusters / an integer	
<<page type>>	fast	
<<length of page field>>	20	
<<SDU>>	The data from the <<Message unit>> received in the DL-EXPEDITED-req primitive	

Table 100: Information used within the MAC_PAGE.Ind primitive

Parameter	Information within the parameter	Normative action/comment
<<length of page field>>	20	
<<SDU>>		

Table 101: Information used within the DL-EXPEDITED-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<Message unit length>>	3 octets	
<< Message unit>>	The data from the <<SDU>> from the MAC_PAGE.Ind primitive	

10.3 Class A basic connection handover

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 9.2.7.3, 9.2.7.3.1, 9.2.7.3.3, 10.5 and 9.2.7.1.2. The following subclauses define the mandatory requirements with regard to the present document.

10.3.1 Voluntary handover

As a result of continued poor quality of service from the MAC layer, the LLME in the PT shall inform the PT LAPC entity, the LAPC entity shall enter the Handover pending condition, timer <DL.05> is not needed to be started, a new MAC connection shall be requested to be established.

The establishment of a new MAC connection shall be achieved by the LLME connection set-up procedure (see subclause 9.1.1.4). If a new MAC connection is successfully established the LAPC entity shall leave the Handover pending condition, and one of the two MAC connections shall be released by the PT using the LLME MAC connection release procedure (see subclause 9.3.1.2).

This implies that in case of unsuccessful handover the associated links shall not be released since the connection is still operational (even with bad quality).

NOTE: The involuntary handover is not required to be supported by a implementation complying to GAP. Any time an unexpected upward MAC_DIS.Ind primitive is received, the receiver of this primitive may assume that the connection and the far side of the link have been released.

10.3.2 Associated procedure

10.3.2.1 LLME connection handover management

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.5. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

Timer <DL.06> shall be started either after the connection handover is successfully completed or immediately after N251 successive "unsuccessful" connection handover attempts.

It shall be stopped upon an initiation of a link release "abnormal" (see subclause 8.42) or release indication from MAC layer (see subclause 9.3).

As long as <DL.06> is running, no connection handover attempts shall be initiated.

10.3.3 Exceptional case

10.3.3.1 Receipt of a request for link release

If while in the connection handover pending condition a link release request has been received from the own NWK layer the handover pending condition shall be cleared and class A link release procedure (see subclause 9.3) shall be performed.

The associated connection and the connection for which establishment is in progress shall also be released using the LLME release of the MAC connection procedures (see subclause 9.3.1.2).

10.4 Encryption switching

The procedure shall be performed as defined in EN 300 175-4 [3], subclause 10.6, EN 300 175-7 [6], subclauses 6.5.3 and 6.4.6 and EN 300 175-3 [2], subclause 6.2.3. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

The procedure for encryption deactivation is not required to be supported since a new connection is always established in clear mode. Therefore any connection or link release implies encryption deactivation.

The encryption deactivation is mandatory only if service D.6 is supported.

10.4.1 Associated procedure

10.4.1.1 Providing Encryption key to the MAC layer

On receipt of the DCK in a DL-ENC_KEY-req primitive the DLC shall transmit it to the MAC layer.

A record shall be kept for the active (the one used for the current encryption) DCK for use in case of connection handover.

10.4.2 Exceptional cases

10.4.2.1 Encryption fails

An encryption attempt which fails means the desired "Crypted" mode is not achieved. If the MAC fails to switch from clear to encrypted mode the connection is released and the DLC layer is informed by a MAC_DIS.Ind primitive. At the peer side this indication shall arrive as a result of the connection release.

10.4.2.2 Connection handover of ciphered connections

During a connection handover the new connection shall always be established in clear (encryption disabled). If the status of the old connection was "Crypted" then the LLME at the PT side shall command the DLC layer to enable ciphering on the new connection as soon as it is established by issuing a MAC_ENC_Key-req primitive to the MAC layer (to provide the cipher key) followed by a MAC_ENC_EKS-req primitive with the flag set to "Go Crypted".

NOTE: If during the time that data has been encrypted a new DCK has been produced and stored when a connection handover of ciphered connection is performed the new key is not available at the DLC layer. Therefore the ciphering is performed using the old DCK.

Notification of successful encryption of the new connection shall be indicated by receipt of a MAC_ENC_EKS-cfm at the initiating side and a MAC_ENC_EKS-ind at the peer side. In this event no indication shall be issued to the NWK layer.

If the encryption of the new connection fails, the connection is released and the DLC layer is informed using the MAC_DIS-ind primitive. No indication with a MAC_ENC_EKS.Ind or a MAC_ENC_EKS.Cfm primitive shall be provided.

10.5 Cf channel fragmentation and recombination

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 6.1.2, 6.1.3, 6.1.4, 6.1.4.2 and 10.2.5.

10.6 Selection of logical channels (Cs and Cf)

The procedure shall be performed as defined in EN 300 175-4 [3].

11 DLC layer procedures U-plane

11.1 U-plane handling

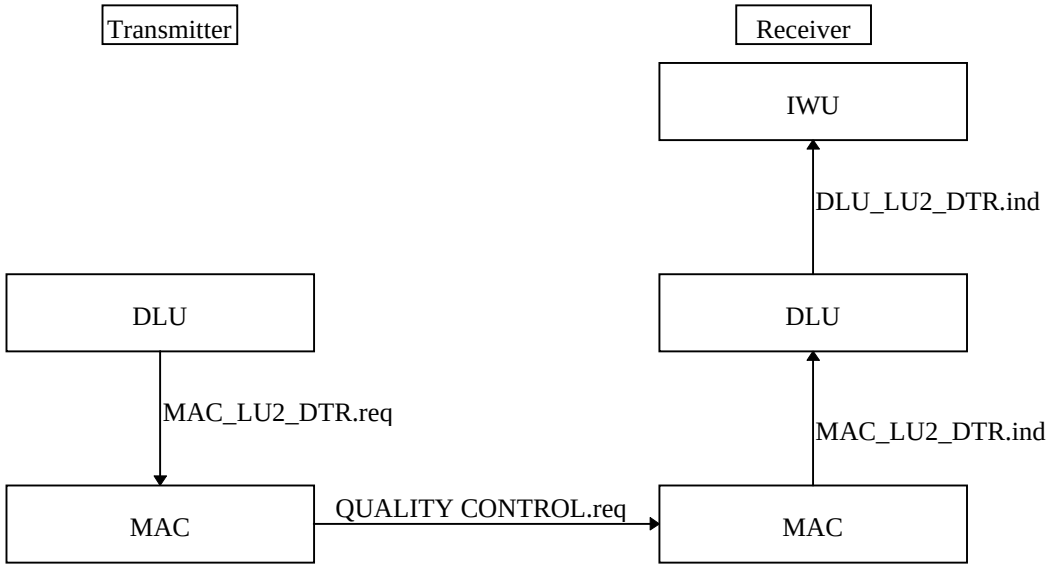


Figure 81: U-plane handling

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 11.3, 11.3.1 and 11.3.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

11.1.1 LU2 Frame RELay service (FREL)

The procedure shall be performed as defined in EN 300 175-4 [3] subclauses 11.3.1.

11.1.1.1 Data link service frame structure for LU2

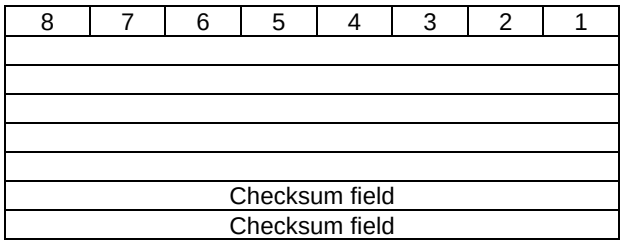


Figure 82: Frame format type

A type frame shall contain the following fields:

- a variable length information field of 0 to 2 046;
- a checksum field of 2 octets.

11.1.1.2 LU2 frame delimiting and transparency

Frame delimiting shall be provided by a combination of the MAC layer and the DLC layer LU2/FU6 entity.

The MAC layer shall always align LU2 PDUs to physical slot boundaries. This is described for LU2 in EN 300 175-2 [1]. This timing shall always be preserved. The LU2 shall additionally insert a send sequence number into each PDU. This number shall be incremented modulo 128 in successive PDUs and shall be independent of the higher layer frame boundaries.

A frame shall only start on a PDU boundary. The end of a multi-PDU frame should be identified by examining the FU6a length indicator octet, including the more data bit. Therefore the LU2 should process all frames in the order dictated by their send sequence numbers.

NOTE: The MAC layer is expected to provide a reliable connection-orientated service, with a residual PDU error rate better than 10^{-4}.

11.1.1.3 Transmission order

The physical transmission order shall be controlled by the MAC layer as defined in EN 300 175-3 [2]. This MAC layer ordering shall use the octet numbering and bit numbering shown above.

NOTE: The use of multibearer MAC connections will mean that PDU's will not necessarily be received in the order they were sent.

11.1.1.4 Invalid frames

An invalid data link frame shall be a frame that contains the following fault:

- contains a checksum error.

For the handling of erroneous frames, see 11.2.3 of this profile.

11.1.2 Checksum operation

The checksum shall provide an error detection capability for the reassembled segments (at the peer side) but there shall be no mechanism for the retransmission of a SDU that is found to be in error.

NOTE: The user should provide an external retransmission protocol, to protect against these infrequent erasures.

A 16-bit checksum is defined. The 16-bit checksum used shall be identical to that used in the C-plane (see subclauses 7.9 and 7.10) where the checksum shall be calculated over the complete SDU+checksum data field. Until there is no internal retransmission mechanism for a SDU defined, the result of the checksum calculation shall be neglected and the data shall be delivered to higher layers as if they are correct.

11.1.2A Segmentation and transmission class

The SDU + checksum shall be segmented into fixed length segments, where the segment length shall depend on the PDU structure chosen. LU 2 use the following combination of transmission class and PDU structure:

- Frame transmission bidirectional or unidirectional FU6 frame.

In all cases the original SDU boundaries shall be preserved (i.e. service data integrity shall be maintained) by use of a length indicator and More flag within each PDU, as defined in subclause 9.9.7.1.

11.1.3 Data transmission

11.1.3.1 Send side procedure

At the transmitting side a complete SDU shall be received in a DL_U_DATA-req primitive. The SDU shall be passed to the checksum function, where the checksum shall be calculated and appended to the end of the SDU.

Table 102: Values used within the { DL_U_DATA }.req primitive

Parameter	Information within the parameter	Normative action/comment
<<ULEI>>	U-plane Link Endpoint Identifier	See EN 300 175-4 [3], subclause 8.4.1
<<Message unit>>		See EN 300 175-4 [3], subclause 8.4.1
<<Message unit length>>		See EN 300 175-4 [3], subclause 8.4.1
<<Error flag>>	NOT allowed	

The resulting SDU + checksum shall be passed to the segmenting function and segmented into an integral number of segments. The last segment shall be filled with fill octets if necessary. The information content of each PDU shall be marked using the length indicator as described in subclause 9.9.7.1, and sequence numbers shall be added using the rules defined in subclauses 9.10.3.

The resulting PDUs shall be transmitted in ascending order of sequence number (i.e. the lowest numbered segment shall be transmitted first), using the procedures defined in subclause 9.10.3.1.

Several PDUs may be submitted once to the MAC layer in a single MAC_CO_DATA-req primitive in response to each MAC_CO_DTR-ind primitive. The number of PDUs shall be less than or equal to the maximum number requested in the MAC_CO_DTR-ind primitive.

Table 103: Values used within the { MAC_CO_DATA }.req primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	See EN 300 175-3 [2], subclause 5.6.1.3
<<transmit data channel type>>	Gf, Ip	
<<number of segments>>	0,1,...,30	
<<no. of bearers for control>>	0	
<<SDU>>		

Table 104: Values used within the { MAC_CO_DTR }.ind primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	See EN 300 175-3 [2], subclause 5.6.1.3
<<data channel type>>	Gf, Ip	
<<number of segments>>	0,1,...,30	
<<no. of duplex bearers>>	0	

11.1.3.2 Receive side procedure

Several PDUs may be received from the MAC layer in a single MAC_CO_DATA-ind primitive.

Table 105: Values used within the { MAC_CO_DATA }.ind primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	See EN 300 175-3 [2], subclause 5.6.1.3
<<receive data channel type>>	Gf, Ip	
<<number of segments>>	0,1,...,30	
<<SDU>>		

The receive side shall re-order the PDUs using the send sequence numbers as defined in subclauses 9.10.3. The receive side shall then search for SDU boundaries using the More data bit as defined in subclause 9.9.7.1.

A complete SDU shall be assumed to exist, and shall be passed to the checksum function when the following conditions are satisfied:

1) two successive boundaries have been identified using the More data bit (i.e. there are no intermediate boundaries);

2) PDUs have been successfully received for all of the sequence numbers that lie between those boundaries.

At the receiving side the checksum shall be tested on each reassembled SDU + checksum. If the checksum passes, the data shall be passed to the IWU using a DL_U_DATA-ind primitive. If the checksum fails, the data shall also be passed to the IWU using a DL_U_DATA-ind primitive. See also 9.9.2.

Table 106: Values used within the { DL_U_DATA }.ind primitive

Parameter	Information within the parameter	Normative action/comment
<<ULEI>>	U-plane Link Endpoint Identifier	See EN 300 175-4 [3], subclause 8.4.1
<<Message unit>>		See EN 300 175-4 [3], subclause 8.4.1
<<Message unit length>>		See EN 300 175-4 [3], subclause 8.4.1
<<Error flag>>	0,1	

11.1.4 FU6 frame structure

The procedure shall be performed as defined in EN 300 175-4 [3], subclauses 12.1, 12.6, 13.3.2 and 13.4. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

FU6 defines two fixed length frames. The total frame length shall always be equal to the segment size of the appropriate logical channel as detailed below.

8	7	6	5	4	3	2	1
Length indicator field							
Send sequence number							
Information field							
Fill fields							
Fill fields							

Figure 83: FU6a frame type

8	7	6	5	4	3	2	1
#1 receive sequence number							
#2 receive sequence number							
#3 receive sequence number							
#4 receive sequence number							
#5 receive sequence number							
#6 receive sequence number							
#7 receive sequence number							

Figure 84: FU6b frame type

Frame type FU6a is used for bidirectional links, and for the forward path of unidirectional links.

Frame type FU6b is used for the backward (control) path of bidirectional and unidirectional links. Type FU6b contains a list of receive sequence numbers for the forward link, i.e. for acknowledgement shall always FU6b be used. It shall use the GF logical channel, with a fixed fragment size of 7 octets.

Only one positive acknowledgement shall be used in the FU 6b framing for the receive sequence number. If a positive acknowledge is available, this receive sequence number has to be transmitted in the first octet of FU6b.

If more than one FU 6b frame is transmitted via the Gf channel, only one of these frames can have one receive sequence number with the A/N bit set to 1. All other sequence number are used for a request of the retransmission of the frames determined by the receive sequence number (ER7-ER1). So for these receive sequence numbers the A/N bit has set to 0.

FU6N is a function of the underlying connection type.

Table 107: FU6 connection type

Connection type	Slot type	FU6N
Ip_error_detection	Half slot	08 octets
Ip_error_detection	Full Slot	32 octets
Ip_error_detection	Double Slot	80 octets

11.1.5 FU6 buffering procedures

The FBP-frame buffering entity shall be used to provide a data buffering function, and is required to supply data (at the transmit side) or accept data (at the receive side) on demand and with minimum delay.

Transmit side: on receipt of a MAC_CO_DTR-ind primitive, one complete frame of data shall be submitted to the MAC layer in a MAC_CO_DATA-req primitive.

Receive side: each MAC_CO_DATA-ind primitive shall contain one complete frame of data from the MAC layer.

In all cases, the order of arrival of the higher layer information shall be preserved, and this shall be identical to the order of transmission.

11.1.6 Field formats for U-plane

11.1.6.1 Length indicator field

c	7	6	5	4	3	2	1
L7 - L1							M

Figure 85: Length indicator field

L7-L1: Length of information field;

More data bit M: the more data bit, M, is used to indicate segmentation of long messages into FU6 frames.

M = "1" indicates that the information field only contains part of a message - there is more to follow.

M = "0" indicates one of two things:

a) that the information field contains a complete message, provided that the M bit of the previous frame was also set to "0";

b) that the information field contains the last segment of a message, provided that the M bit of the previous frame was set to "1".

When the M bit is set to "1", the information field should contain the maximum number of octets.

NOTE 1: This rule only recommends that each frame contains the maximum amount of information. However, the Li field always defines the actual length.

11.1.6.2 Send sequence number format

8	7	6	5	4	3	2	1
I/R	ES7 - ES1						

Figure 86: Send sequence number format

ESi = Send Sequence Number (7-bits);

i of {7..1};

I/R = Initial/Retransmission bit.

Send sequence number parameters.

At the time that an in-sequence frame is designated for transmission, the value of ESi is set equal to the value of the send state variable SN. Refer to subclauses 9.10.3, 9.10.3.1and 9.10.3.2 of this profile.

The I/R bit shall define the meaning of the send sequence number contained in the same octet, using the following coding:

I/R = "1" First transmission (of this frame);

I/R = "0" Retransmission (of this frame).

11.1.6.3 Receive sequence number format

8	7	6	5	4	3	2	1
A/N	ER7 - ER1						

Figure 87: Receive sequence number format

ERi = Receive sequence number (7-bits);

i of {7..1};

A/N = ACK/NACK bit.

11.1.6.4 Receive sequence number parameters

At the time that a frame is designated for transmission, the value of ERi is set equal to the value of the receive state variable RN. Refer to subclauses 9.10.3, 9.10.3.1and 9.10.3.2 of this profile.

The A/N bit shall define the meaning of the Receive sequence number contained in the same octet, using the following coding:

A/N = "1" Positive acknowledge;

A/N = "0" Negative acknowledge.

11.1.6.5 Fill elements - Fill field format

Fill field format

8	7	6	5	4	3	2	1
1	1	1	1	0	0	0	0

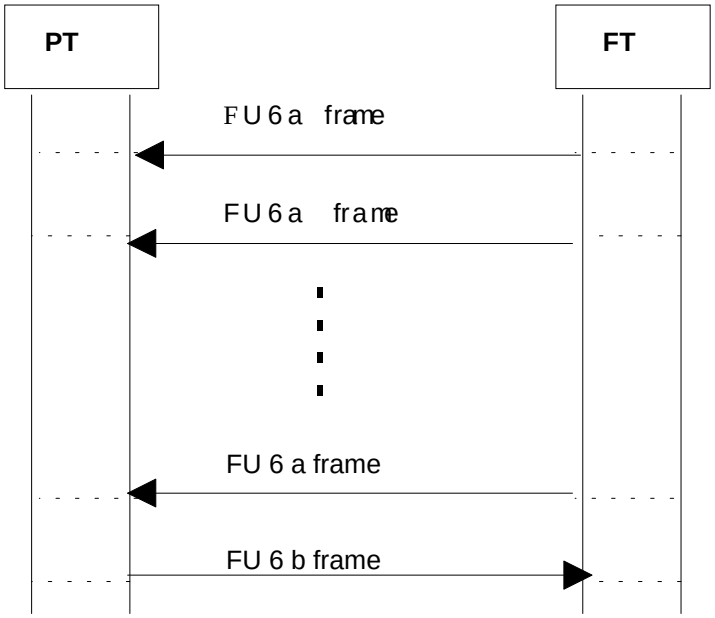
NOTE: Fill field octets are filled with balanced data.

Figure 88: Fill field format

11.2 U-plane peer to peer

The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

11.2.1 FU6 frame operation for the pilot bearer



NOTE: The case for uplink differs only in the notations.

Figure 89: Sending FU 6 frames

11.2.2 Ip_error_detection with SEL

The protected data service Ip_error_detection shall work with the selective retransmission protocol.

11.2.3 Frame transmission

The frame transmission uses both SNs and RNs. The RNs provide both window control to avoid possible sequencing errors, and also invoke automatic DLC retransmission. The DLC retransmission shall operate a selective retransmission protocol, combined with a lifetime limit on all packets to allow a guaranteed throughput.

11.2.3.1 Sending side procedure

The sending entity shall add SNs to all frames in the order specified by that entity. The I/R bit shall be set to "1" for the first transmission and to "0" for all retransmissions.

The resulting frames shall be submitted to the MAC layer in the order of ascending SN.

NOTE 1: This rule means that retransmissions always have priority relative to first transmissions.

The sending entity shall maintain a maximum window size between the SN and the last received RN. The maximum window size shall be equal to the (Modulus) of the SN used. A lower maximum value may be negotiated at call establishment (see EN 300 175-4 [3], subclause 14.2.4). A smaller operating window size may be unilaterally adopted by the sending entity at any time.

Due to the modulus operation, each SN may be re-used several times during the life of the link. The minimum interval between re-use shall meet the following requirements:

1) a SN shall not exceed the maximum window size;

2) a SN shall not be re-used within L(S) TDMA frames of the most recent previous use of that number.

The value of L(S) shall be equal to 2.

The maximum lifetime of each frame shall be limited to T(R) TDMA frames. This lifetime limit should be defined at call establishment, and shall not be subsequently changed. When this limit is exceeded for a given frame, the frame shall not be retransmitted (or transmitted) and the data should be discarded. If the lifetime limit is not specified at call establishment the following value shall apply:

T(R) default value shall be the maximum possible value, i.e. 63 TDMA frames.

NOTE 2: The value T(R) should normally be negotiated with the <<transit-delay>> element during call establishment (see EN 300 175-4 [3]).

The discarding of a frame shall not be treated as equivalent to acknowledgement of the SN. In all cases, the SN of that frame shall not be reused until the SN has been acknowledged by the peer. The peer entity maintains a corresponding lifetime limit, and should normally issue a (false) acknowledgement for expired frames when their lifetime limit is reached.

Whenever the window size limit is reached (thereby halting further transmissions) the sending side shall commence retransmission of all unexpired but outstanding frames, starting from the oldest unacknowledged frame. This automatic retransmission shall be stopped whenever a useably RN is received (i.e. an RN that acknowledges one or more outstanding frames), and normal transmission or retransmission procedures will be resumed.

Received RNs with the A/N bit set to "1" shall be treated as a positive acknowledgement for all frames up to and including the frame number RN. This positive acknowledgement shall cause an immediate stop to any redundant (unnecessary) retransmissions that may have been scheduled as a result of previously received negative acknowledgements.

Received RNs with the A/N bit set to "0" shall be treated as an negative acknowledgement for the single frame number RN. Receipt of a NACK shall cause a selective retransmission of the indicated frame(s).

If not all octets of the FU6b frame can be filled with acknowledge and negative acknowledge the last valid entry shall be copied to all the other octets.

Example: Acknowledge for frame 56 and negative acknowledge for frames 59, 61 and 64 have to be transmitted. So the first octet shall carry the acknowledge for frame 56, the second octet carries the negative acknowledge for frame 59, the third octet carries the negative acknowledge for frame 61 and the octets 4, 5, 6 and 7 carries the negative acknowledge for frame 64.

11.2.3.2 Receiving side procedure

The receiving entity shall accept data packets from the MAC layer in any order. Packets marked as type "unknown" and any packets that are indicated to contain errors in the first portion (MAC sub-field BO) shall be discarded. The remaining packets are assumed to contain valid frames, and shall be processed in their order of arrival.

In-sequence frames are defined as a series of one or more frames that contain no errors and that contain SN(s) that together form a continuous series of SNs when considered together with other received but undelivered frames. All in-sequence frames shall be immediately delivered to the higher functions.

NOTE 1: Most higher function users of this class retransmission are expected to provide frame buffering such that a continuous flow of data is produced. The buffer size should be greater than the product of connection bandwidth and maximum frame lifetime.

Out-of-sequence frames are defined as all other frames (i.e. a sequence of one or more frames that do not form a continuous series of SNs or contain some errors). These frames may only be delivered after they have been buffered for T(R) TDMA frames after their arrival. During this buffering period, out-of-sequence frames may become in-sequence frames due to the arrival of one or more missing frames. In this event, the frames shall be immediately delivered to the higher layer.

As an out-of-sequence frames is detected the receiving entity shall return a negative acknowledgement, by returning one frame containing the missing RNs and the A/N bit set to "0". If necessary, multiple RN values shall be returned; one for each missing frame. The return of a the negative acknowledgement shall be done at least every 6 TDMA frames. If no negative acknowledgement is necessary, a positive acknowledgement shall be done at least every 30 TDMA frames.

The transmission of the positive or negative acknowledgement shall be done with the Gf channel.

If no Cf data is carried in the same TDMA frame according to the C-Mux rules, no retransmission shall apply to this frame.

NOTE 2: So Gf channel data is only retransmitted, if the Gf channel is transmitted in combination with other data than Gf channel data.

NOTE 3: Out of sequence frames may be discarded before this time limit, in order to limit buffer sizes.

The value of T(R) shall be equal to the maximum frame lifetime. This lifetime limit should be defined at call establishment, and shall not be subsequently changed. If the lifetime limit is not specified at call establishment the following value shall apply:

T(R) default value shall be the maximum possible value, i.e. 63 TDMA frames.

NOTE 4: The value T(R) should normally be negotiated with the <<transit-delay>> element during call establishment (see EN 300 175-4 [3]).

During the total buffering period T(R) a frame may arrive that is a duplicate of one of the buffered frames. If the original buffered frame was correct, any such duplicates shall be discarded. If the original buffered frame contained errors, the duplicate may be used to correct those errors, using selective replacement of erroneous portions (replacement of MAC BN sub-fields).

NOTE 5: Selective replacement is only performed for frames with the same SN. This requires error free reception of the B0 sub-field (i.e. the sub-field containing the SN).

If after buffering for T(R) TDMA frames, out-of-sequence frames remain out-of-sequence, all of the valid frames shall nonetheless be delivered to higher functions, together with all missing frames. The receiving entity shall then act as though the frames had been received in sequence. In particular, the RN shall be updated to acknowledge acceptance of these frames.

Whenever frames are delivered to the higher functions, the RN for all positive acknowledgements shall be set equal to the highest delivered SN.

11.2.4 Flow Control

There are two different kinds of flow control depending on the availability of buffer space on the receiver and on the transmitter side.

Receiver side: If all current received PDUs are already acknowledged, but not yet delivered to higher layers and the receiving side has no more buffer for new receiving PDUs, a flow control mechanism has to be initiated by the receiver. The DLU shall send a MAC_LU2_DTR{req} primitive to the MAC with <<Stop/Go flag>>=0.

Table 108: Values used within the { MAC_LU2_DTR }.req primitive

Parameter	Information within the parameter	Normative action/comment
<<ULEI>>	U-plane Link Endpoint Identifier	See EN 300 175-4 [3], subclause 8.4.1
<<Stop/Go flag>>	0, 1	0 = Stop, 1 = Go

To inform the transmitter and to avoid unnecessary transmissions the MAC shall send the MAC message Bearer and quality control. The coding of the message depend on the transmission direction.

Table 109: Values used within bearer and quality control

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<bearer and quality control>>			
	<command>	See table 110	
	<FMID>	all	Fixed part MAC Identity
	< PMID>	all	Portable part MAC Identity
	<param_1>	See table 110	
	<param_2>	See table 110	
	0000 1111		

Table 110: Values used within the command/param fields in bearer and quality control

Field within the message	Standard values within the MAC message	Normative action/comment
<command>	1011	The FT informs the PT that transmission can start or transmission shall stop request FT→ PT confirm PT→ FT
<param_1>	RPN	
<param_2>	0000 0000, 1111 1111	0000 0000 request for Stop 1111 1111 request for Go

Table 111: Values used within the command/param fields in bearer and quality control

Field within the message	Standard values within the MAC message	Normative action/comment
<command>	1100	The PT informs the FT that transmission can start or transmission shall stop request PT→ FT confirm FT→ PT
<param_1>	0000 1111	
<param_2>	0000 0000, 1111 1111	0000 0000 request for Stop 1111 1111 request for Go

If the receiver gets again free buffer space, the DLU shall send a MAC_LU2_DTR{req} primitive to the MAC with <<Stop/Go flag>>=1. After the receive of a Go message, the MAC layer itself transmits the Bearer quality control message with a Go request.

Transmitter side: If the transmitter has no more free buffer space (one possible reason is, that he gets no positive acknowledgement from the receiver), the DLU shall send a DLU_LU2_DTR{ind} primitive to the IWU with <<<Stop/Go flag>>=0.

If the transmitter gets again free buffer space, the DLU shall send a DLU_LU2_DTR{ind} primitive to the IWU with <<Stop/Go flag>>=1.

Table 112: Values used within the { DLU_LU2_DTR }.ind primitive

Parameter	Information within the parameter	Normative action/comment
<<ULEI>>	U-plane Link Endpoint Identifier	See EN 300 175-4 [3], subclause 8.4.1
<<Stop/Go flag>>	0, 1	0 = Stop, 1 = Go

If the MAC receives a Bearer and quality control message, the MAC sends a MAC_LU2_DTR{ind} primitive to the DLU according to the <param_2> field.

Table 113: Values used within the { MAC_LU2_DTR }.ind primitive

Parameter	Information within the parameter	Normative action/comment
<<ULEI>>	U-plane Link Endpoint Identifier	See EN 300 175-4 [3], subclause 8.4.1
<<Stop/Go flag>>	0, 1	0 = Stop, 1 = Go

11.3 U-plane point to multi-point

If the FP-PP point-to-multipoint service is provided the DLC layer shall transmit and receive all FP-PP point-to-multipoint SDUs via LU2 (Class 1) and FU6a framing and segmentation and the PPs shall not send the FU6b acknowledge frames. Such DLC frames shall be transferred via the SIp service.

The SIp protected data connectionless downlink service is used by the FP-PP point-to-multipoint service to transfer the data frames after the LU2 (Class 1) framing and FU6a segmentation functions have been performed on the point-to-multipoint SDU. The SIp service is an application of the DECT MAC SIn service.

The SIp service shall code each data frame (which shall be 32 octets long) according to the protected B-field multiplex (as defined in EN 300 175-3 [2], subclause 6.2.1.3) and transmit the coded data as a single SDU via the DECT MAC SIn channel.

The FP shall only transmit SIp data starting at the start of a paging cycle. A PP shall understand the presence of SIp data to be indicated by the coding BA = SIn and the Pt MAC layer information = Dummy or C/L bearer. The TDMA frame immediately following the frame in which SIp data was received shall also be monitored to find out whether it contains SIp data. In this way SIp data shall be understood to be present in each subsequent TDMA frame until the BA and MAC layer information codings indicate that the SIp (SIn) data field is no longer present. No further SIp information shall then be available until the start of the next paging cycle.

The start of a paging cycle in this context shall be that time-slot in frame 0 of a multiframe that is carrying the start of a paging message. When paging repetition is supported by the fixed part, the number of this multiframe shall be 0 modulo 4.

12 MAC layer procedures

12.1 General

For voice services all MAC requirements are according to EN 300 444 [10] GAP.

For MAC requirements concerning data applications the following shall apply.

The minimum instance shall only require the capability to establish and maintain single-bearer connections. The provisions of EN 300 175-3 [2] shall be implemented with respect to the services, procedures, messages and information elements coding listed in annexes C to F. The provisions of EN 300 175-6 [5] shall be implemented with respect to the structure and use of identities.

If the FP $\Rightarrow$ PP point-to-multipoint service is implemented, the MAC layer shall in addition implement the protected data connectionless downlink service SI_P, as defined in annex A.

12.2 Downlink broadcast

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 9.1.1.

12.2.1 N_t message

The FT shall be capable of sending and the PT shall be capable of receiving and processing the N_t message as defined in EN 300 175-3 [2], subclause 7.2.2.

Table 114: Values used within N_t message

MAC message/broadcast element	Field within the message/broadcast element	Standard values within the MAC message	Normative action/comment
<<RFPI>>			
	<E-bit>	0	No SARI.
		1	SARI available. Relates to service SARI support .
	<PARI>	All	
	<RPN>	All	

12.2.2 Q_t - static system information

The FT shall be capable of sending and the PT shall be capable of receiving and processing the Q_t message as defined in EN 300 175-3 [2], subclause 7.2.3.2.

Table 115: Values used within static system info

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Static system info>>			
	<Qh>	0	
	<NR>	0	PT shall support all values in order to gain lock. Asymmetric connections are not required to be supported by the PT.
	<SN>	0 - 11	PT shall support all values.
	<SP>	0	PT shall support all values in order to gain lock. Half slot connections are not required to be supported by the PT.
	<ESC>	0	PT may ignore and assume the value to be 0.
	<Txs>	0	PT may ignore and assume the value to be 0.
	<Ext-car>	0, 1	PT shall support all values in order to keep in synchronization with the primary scan.
	<RF-car>	1 - 1 023	The PT shall not use carriers which are not supported.
	<SPR>	0	PT may ignore.
	<CN>	0 - 9	PT shall support all values.
	<SPR>	0	PT may ignore.
	<PSCN>	0 - N	PT shall support values 0 - 9.

12.2.3 Q_t - FP capabilities

12.2.3.1 Standard FP Capabilities

The FP shall indicate its standard capabilities using the Standard fixed part capabilities Qt message as described in EN 300 175-3 [2] subclause 7.2.3.4. The PT shall be able to receive and understand this message and react as described in this profile.

If an FT provides as well speech services, the settings in addition to those described below that are mandatory shall be compliant to those described in EN 300 444 [10] GAP.

Table 116: Values used within Standard FP capabilities

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<FP capabilities>>			
	<Qh>	3	
	<a15>	1	Double slot
	<a17>	1	Full slot
	<a25>	1	B-field set-up
	<a26>	0,1	CF messages
	<a30>	1	IP_error_correction
	<a31>	1	multibearer connections

Higher layer information: the management entity in the FP supplies the MAC layer with a 16 bit SDU via the Management Entity (ME) SAP. At the PT the MAC layer passes the 16 bits out through the ME SAP to the management entity.

For the setting of the higher layer information bits see subclause 12.2.3.2.

12.2.3.2 Extended FP Capabilities

The FP shall indicate its extended capabilities using the Extended fixed part capabilities Qt message as described in EN 300 175-3 [2] subclause 7.2.3.5. The PT shall be able to receive and understand this message and react as described in this profile.

Support of Wireless Relay Station is out of scope for this profile.

FT shall indicate to the PT whether it is supporting the MAC suspend/resume procedure described in subclauses 12.17.1 and 12.17.2 by setting bit a20 of the extended FP capabilities Qt message to "1". In this case FTs and PTs shall use only the MAC suspend and resume procedure. If bit a20 is set to "0" both FT and PT shall use the NWK layer suspend and resume procedures as described in subclauses 8.44 and 8.45.

Table 117: Values used within Extended FP capabilities

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<FP capabilities>>			
	<Qh>	4	
	<a20>	1	MAC suspend and resume procedure shall be used

For the settings of the extended higher layer capabilities see subclause 12.2.3.2. If the bit a40 in the extended higher layer capabilities is set to value "1", the PT may assume that the values of the Standard FP capabilities Qt message as indicated in table 116 are set to value "1". The FT shall set the respective values to "1".

12.2.4 Q_t - SARI list contents

The FT may send and the PT shall be capable of receiving and processing (if broadcast by the FT) the Q_t message as defined in EN 300 175-3 [2], subclause 7.2.3.6, and EN 300 175-6 [5], subclauses 5.5, 5.5.1, 5.5.3 and 5.5.4.

This is relevant if the Nt message indicates Secondary Access Rights Identity (SARI) support.

Table 118: Values used within SARI list contents

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<SARI list contents>>			
	<Qh>	5	
	<SARI list length>	All	
	<TARIs yes/no>	All	The PP may ignore it if Tertiary Access Rights Identity (TARI) request is not supported (support of TARI is not required in GAP)
	<Black yes/no>	All	The PP shall be able of distinguishing ARI from black ARI even if TARI is not supported.
	<ARI or black-ARI>	All	

12.3 Paging broadcast

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 9.1.3.

12.3.1 Short page, normal/extended paging

The following fields as defined in EN 300 175-3 [2], subclause 7.2.4 shall be supported by the PT and the FT.

Table 119: Values used within short page message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Short page message>>			
	<Extend flag>	0,1	PT shall support all values. Optional for the FT to support value 1.
	<B_S SDU length indication>	1	PT and FT shall support short page messages.
	<20 bits of BS channel data>	All	Higher layer information
	<Information type>	1, 2, 3, 4, 5, 8 and 9	The PT shall support values 1, 2, 5, and 9. FT shall support value 1 (see subclause 12.3.3) if blind slot information available. The FT shall support value 9 (see subclause 12.3.4) if bearer handover information available.
	<MAC layer information>	Corresponding information	Information type defined in the previous field

12.3.2 Zero page normal/extended paging

The following fields as defined in EN 300 175-3 [2], subclause 7.2.4 in the zero page message shall be supported by the PT and the FT.

Table 120: Values used within zero page message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Zero page message>>			
	<Extend flag>	0, 1	PT shall support all values. Optional for the FT to support value 1.
	<B_S SDU length indication>	0	PT shall support zero length page messages. The FT shall support if "Blind slot information" included.
	< 20 least significant bits of RFPI>	All	May be ignored by PT.
	<Information type>	1, 2, 3, 4, 5, 8 and 9	The PT shall support values 1, 2, 5 and 9. FT shall support value 1 (see subclause 12.3.3) if blind slot information available. The FT shall support value 9 (see subclause 12.3.4) if bearer handover information available.
	<MAC layer information>	Corresponding information	Information type defined in the previous field

12.3.3 MAC paging

The following fields as defined in EN 300 175-3 [2], subclause 7.2.4 shall be supported by the PT and the FT.

MAC paging shall be used by the FT when it wants to re-establish (resume) a suspended connection and fast set-up is not supported by both ends. This shall not involve higher layer actions (for the description of MAC resume procedure see subclause 8.45).

NOTE: For the higher layers suspend and resume is invisible.

Table 121: Values used within MAC page message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Zero page message>>			
	<Extend flag>	0, 1	PT shall support all values. Optional for the FT to support value 1.
	<B_S SDU length indication>	3	
	< PMID>	All	
	<spare>	0	16 spare bits

12.3.4 Blind slot information

It is mandatory for RFP's that have blind slots, due to non-duplex bearer operation on that slot (i.e. those RFP's that have technological limitations such as a slow synthesiser), to periodically announce these blind slots (at least every 10 s). In the event the RFP announces blind slot information, such information may also include all blind slots due to an active bearer as well.

Not available (blind) slot means that the FP recommends the PP not to attempt a set-up on this slot.

If the PP receives blind slot information, it is mandatory for that PP to use it in the process of channel selection. The PP does not have to wait for the blind slot information before making the channel selection.

12.3.5 Bearer handover information

It is mandatory for FTs not supporting bearer handover within the whole FT to periodically send the bearer handover information (at least every 10s).

It is mandatory for PT to support the following values of field "Info type" (bits a36 to a39) for "Bearer handover information" (value "9" of <Information type> in the P_t message, see tables 119 and 120): "0000", "0001", "0010" and "0011".

12.4 Connectionless service

The SI_P protected data connectionless downlink service is used by the FP-PP point-to-multipoint service to transfer the data frames after the LU2 (class 1) framing and FU6a segmentation functions have been performed on the point-to-multipoint SDU (see clause 7).

The FP shall only transmit SI_P data starting at the start of a paging cycle. A PP shall understand the presence of SI_P data to be indicated by the coding BA = SI_N and the P_T MAC layer information = Dummy or (Connection Less) C/L bearer. The TDMA frame immediately following the frame in which SI_P data was received shall also be monitored to find out whether it contains SI_P data. In this way SI_P data shall be understood to be present in each subsequent TDMA frame until the BA and MAC layer information codings indicate that the SI_P data field is no longer present. No further SI_P information shall then be available until the start of the next paging cycle.

The start of a paging cycle in this context shall be that time-slot in frame 0 of a multiframe that is carrying the start of a paging message. When paging repetition is supported by the fixed part, the number of this multiframe shall be 0 modulo 4.

12.5 Connection oriented services

12.5.1 General

The PP or FP shall not establish a connection unless one or more DLC-PDU's are available for point-to-point transfer.

Even if the PP is known to support fast set-up it cannot assume that the PP will respond to fast set-up attempts.

NOTE: A PP that supports fast set-up does not need to support fast scanning all the time. A PP might decide after some time of inactivity to reduce scanning to support fast or even normal paging.

The connection establishment from the FP to the PP goes as follows:

- the FP shall try to establish the connection using the fast set-up procedure if the PP is known to support fast set-up;
- the fast set-up procedure should result in at least one set-up attempt;
- if the PP is known not to support the fast set-up procedure, then the fast set-up is not required;
- if the fast set-up fails or if the PP does not support fast set-up then;
- the FP shall try to establish the connection using a fast page, if the PP is known to support fast page;
- the paging should result in at least one paging attempt;
- if the fast paging fails or if the PP does not support fast paging then;
- the FP tries to establish a connection with normal paging.

In cases where both the PP and the FP are capable of diversity switching, the default operation in the absence of other user intervention shall be for the FP diversity to remain in operation and for the PP to disable its diversity function.

Encryption shall always be initiated immediately after service negotiation is ready and before additional bearers are added (so only the pilot exists). Enabling encryption is not necessary after suspension in case of resumption of MAC resources.

12.5.2 Set-up of PP initiated, single bearer, service type known

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.2.4.2 and 10.5.1.3.1.

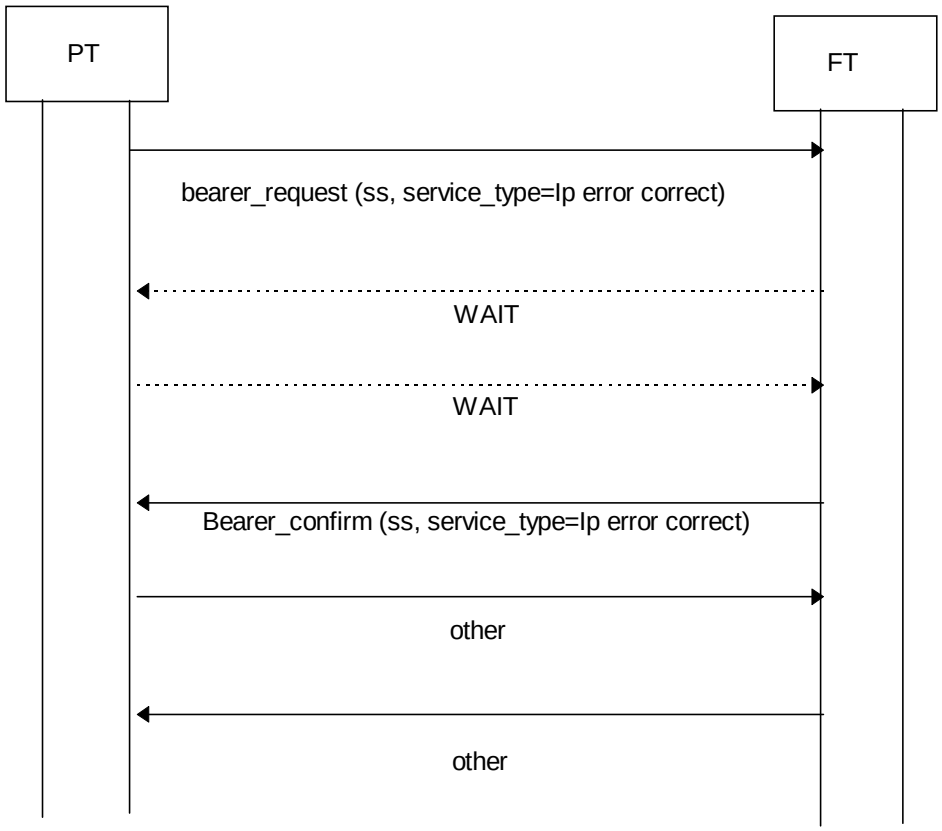


Figure 90: Set-up of PP initiated, single bearer, service type known

12.5.2.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT.

Table 122: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control"
	<Command>	0	"Access_request"
		4	"Bearer_confirm"
		5	"Wait"
	<FMID>	All	
	<PMID>	All	(See subclause 14.4)
	<ECN>	All	note 1
	<LBN>	All	note 1
	<up/down/ss/sm>	All	note 1
	<service type>	0, 3	note 1
	<max. lifetime>	0-7	note 1
	<slot type>	0	note 1
NOTE: For access_request, bearer_confirm.			

12.5.3 Multibearer connections

12.5.3.1 Set-up of pilot bearer, PT initiated

Independent of the type of multibearer connection, the set-up procedure starts with the set-up of a pilot bearer. This procedure shall be performed as defined in EN 300 175-3 [2], subclause 10.5.1.3.1.

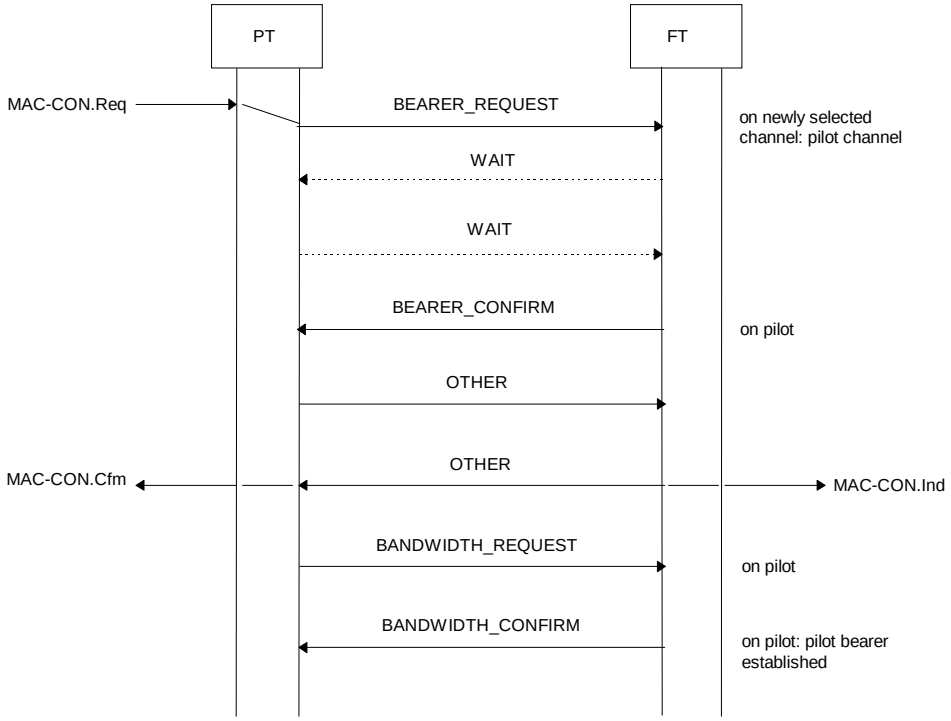


Figure 91: Set-up of pilot bearer, PT initiated

NOTE: BANDWIDTH request/confirm can also be used for OTHER. In most cases however network layer signalling is necessary before BANDWIDTH messages can be provided with meaningful content.

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT. For values used within BEARER_REQUEST and BEARER_CONFIRM see table.

Table 123: Values used within {BANDWIDTH(req,cfm)}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	8	“Bandwidth_B.request”
		9	“Bandwidth_B.confirm”
	<FMID>	All	
	<Mup, Mdown, Tup, Tdown>	1-23	

12.5.3.2 Set-up of pilot bearer, FP initiated, fast set-up

Item as in previous section, but reverse message directions.

12.5.3.3 Set-up of additional duplex bearer, PT initiated

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.2.4.3 and 10.5.1.3.1 and 10.5.1.3.2. The use of channel list messages in the way indicated in the figure below is mandatory. When possible, channel list messages may be combined with MAC control in order to optimize set-up times.

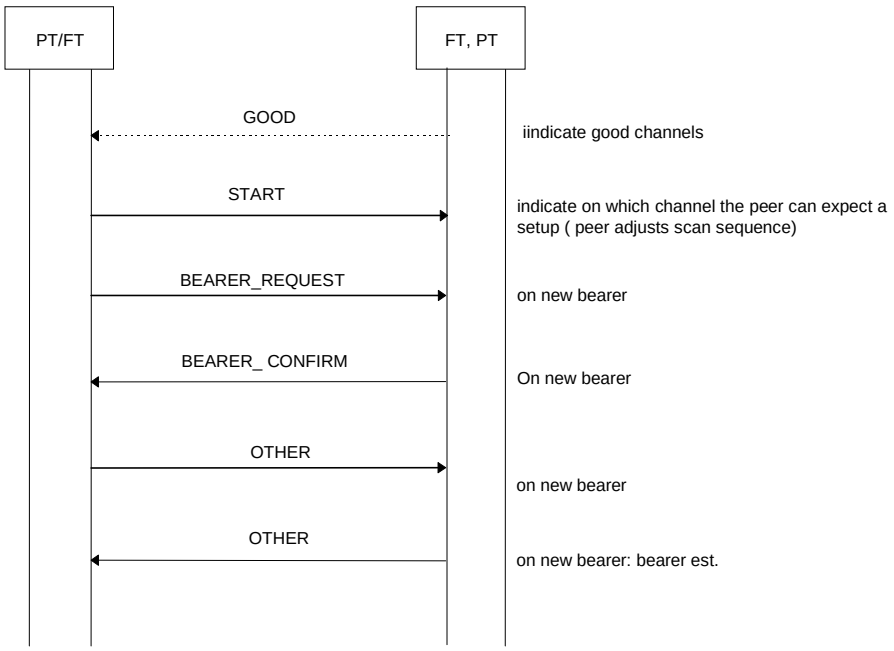


Figure 92: Set-up of additional duplex bearer, PT initiated

11.5.1.3.3.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT.

For values within {BEARER_REQUEST, BEARER_CONFIRM} see table 122.

For values within {START(req,cfm,grant) and STOP(req,cfm,grant)} see table 100 in EN 300 444 [10].

Table 124: Values used within {BANDWIDTH(req,cfm)}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	8	“Bandwidth_B.request”
		9	“Bandwidth_B.confirm”
		10	“Channel list”
	<FMID>	All	
	<Mup, Mdown, Tup, Tdown>	1-23	

Table 125: Values used within {CHANNEL_LIST}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	10	“Channel_list”
	<RPN>	All	
	<Command>	1,7	Sending of the GOOD message is optional. START is mandatory.
	S/D	All	
	SN	0-11	
	SP	0	
	CN	0-9	

12.5.3.4 FP initiated, asymmetric, FP->PP, indirect set-up

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.5.1.4.

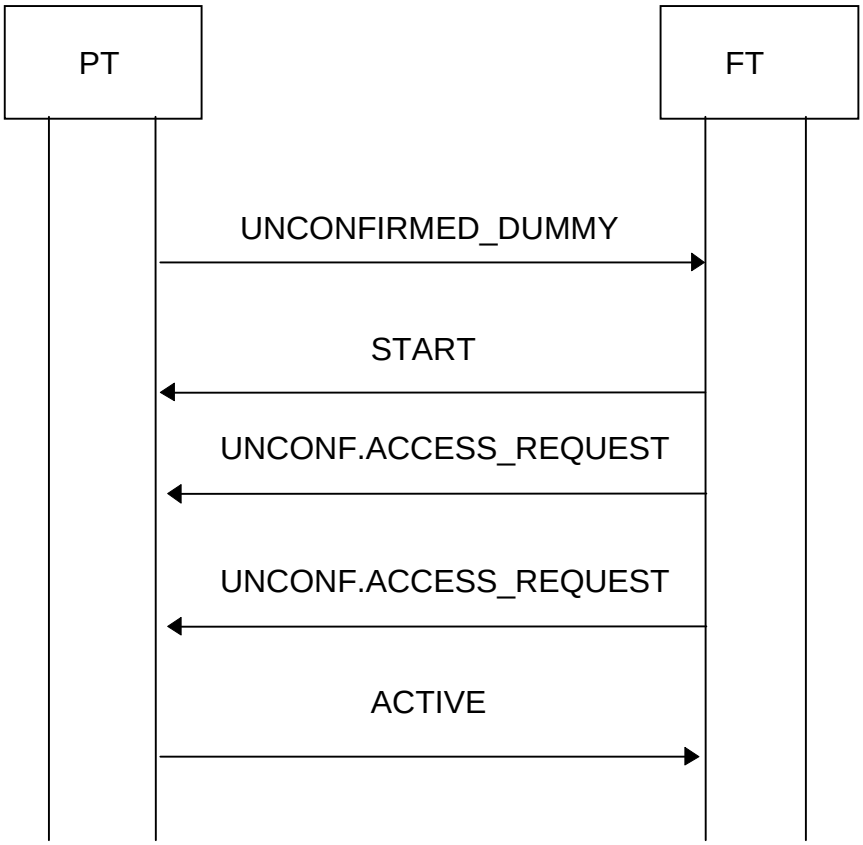


Figure 93: FP initiated, asymmetric, FP to PP, indirect set-up

12.5.3.4.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT.

Table 126: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	11	"Unconfirmed_dummy"
		3	"Unconfirmed_access_request"
		10	"Channel list"
	<FMID>	All	
	<PMID>	All	(See subclause 14.4)
	<ECN>	All	
	<LBN>	All	
	<up/down/ss/sm>	All	note
	<service type>	0, 3	note
	<max. lifetime>	0-7	note
	<slot type>	0	note
NOTE: Values shall be used that are currently valid for the connection.			

Table 127: Values used within {CHANNEL_LIST}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	10	"Channel_list"
	<RPN>	All	
	<Command>	0,7	
	S/D	All	
	SN	0-11	
	SP	0	
	CN	0-9	

12.5.3.5 FP initiated, asymmetric, FP->PP, direct set-up

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.5.1.4.

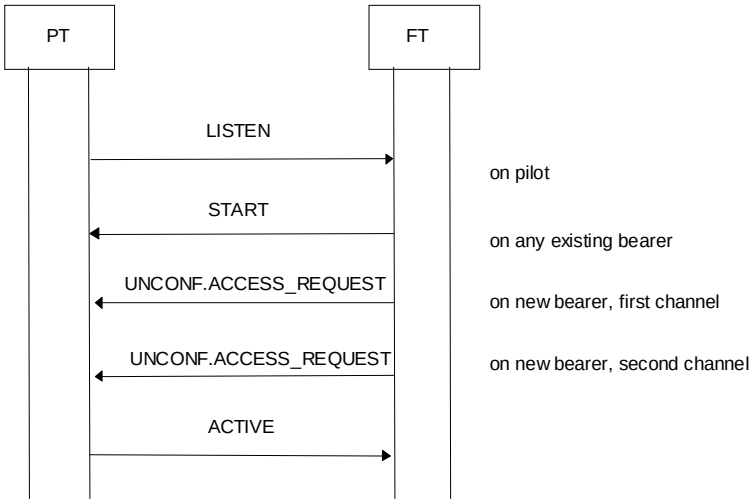


Figure 94: FP initiated, asymmetric, FP to PP direct set-up

12.5.3.5.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT.

Table 128: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	3	"Unconfirmed_access_request"
		10	"Channel list"
	<FMID>	All	
	<PMID>	All	(See subclause 14.4)
	<ECN>	All	
	<LBN>	All	
	<up/down/ss/sm>	All	note 1
	<service type>	0, 3	note 1
	<max. lifetime>	0-7	note 1
	<slot type>	0	note 1
NOTE: Values shall be used that are currently valid for the connection.			

Table 129: Values used within {CHANNEL_LIST}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	10	"Channel_list"
	<RPN>	All	
	<Command>	0,6,7	
	S/D	All	
	SN	0-11	
	SP	0	
	CN	0-9	

12.5.3.6 Connection set-up in case of resume

This section describes the start of the set-up of the single bearer or pilot bearer in case of connection re-establishment after suspension of the MAC resources.

The procedure shall be performed as defined in EN 300 175-3 [2], subclause (part of 10.2 connection set-up).

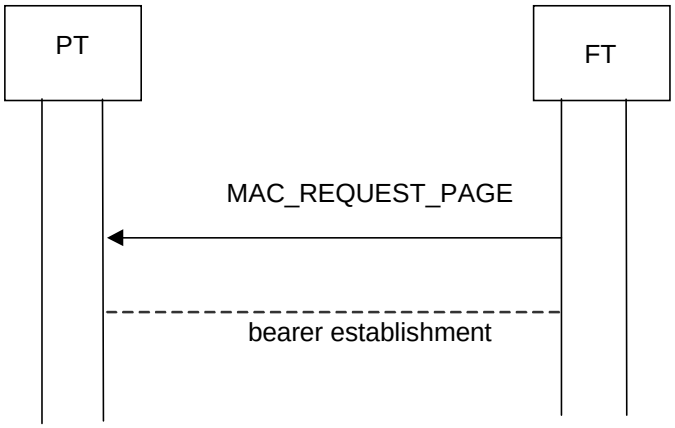


Figure 95: Connection set-up in case of resume

Values of the MAC_REQUEST_PAGE can be found in table 121 in section 'MAC page, normal/extended paging'.

12.5.3.7 Unacknowledged connection release

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.4 and 10.7.2.1.

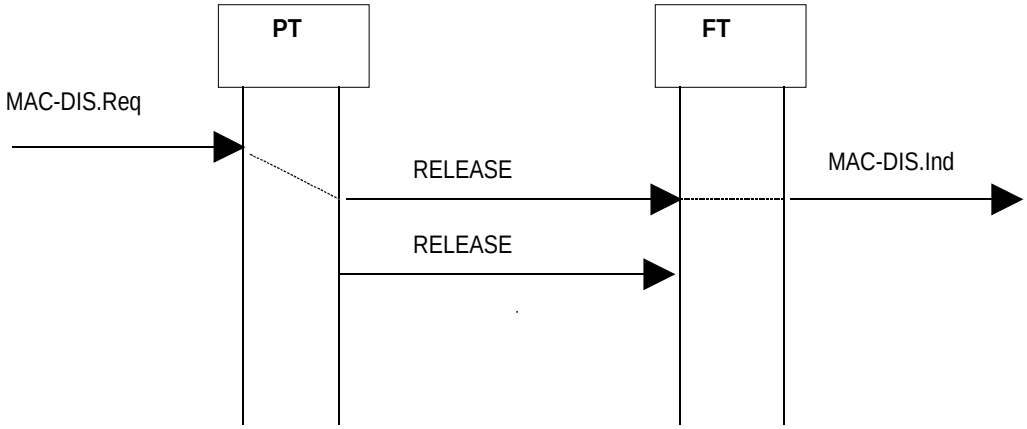


Figure 96: Bearer release

12.5.3.7.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.2.5.2 in the MAC control (M_t) message shall be supported by the PT and the FT.

Table 130: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	0	Basic connection control.
	<Command>	15	Release
	<FMID>	All	
	<PMID>	All	See subclause 14.4

12.5.3.8 Acknowledged connection release

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.7.2.2.

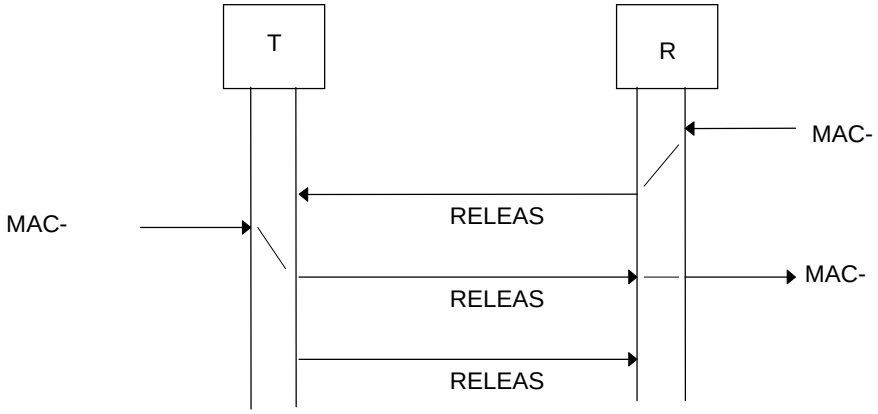


Figure 97: Acknowledged connection release

12.5.3.8.1 Exceptional case

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.7.2.2.

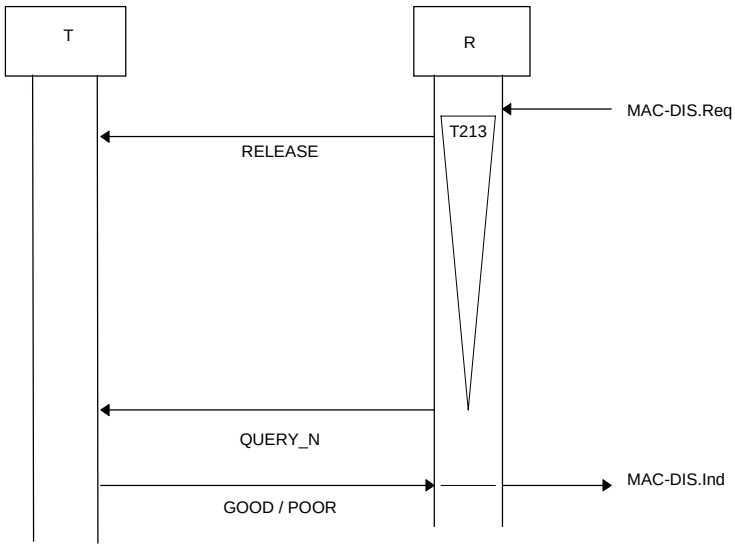


Figure 98: Acknowledged connection release, exceptional case

12.5.3.8.2 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.3.3 of the MAC control (M_t) message shall be supported by the PT and the FT.

Table 131: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	15	"Release"
	<FMID>	All	
	<PMID>	All	See subclause 14.4
	<LBN>	All	
	<reason>	0-13	

Table 132: Values used within {CHANNEL_LIST}

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	X001	"Advanced connection control".
	<Command>	10	“Channel_list”
	<RPN>	All	
	<Command>	1,2,4	
	S/D	All	
	SN	0-11	
	SP	0	
	CN	0-9	

12.5.3.9 Fast release

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.7.2.3.

12.5.3.10 Connection modification (informative)

The procedure shall be performed as defined in EN 300 175-3 [2], subclauses 10.7.2.3.

Suppose that the existing connection is asymmetric downlink consisting of two duplex bearers and two double simplex bearers and that the modified connection is asymmetric uplink consisting of one duplex bearers and one double simplex. The first release message releases the first double simplex bearer, the second release message enables fast reversal of the direction of the second double simplex bearer.

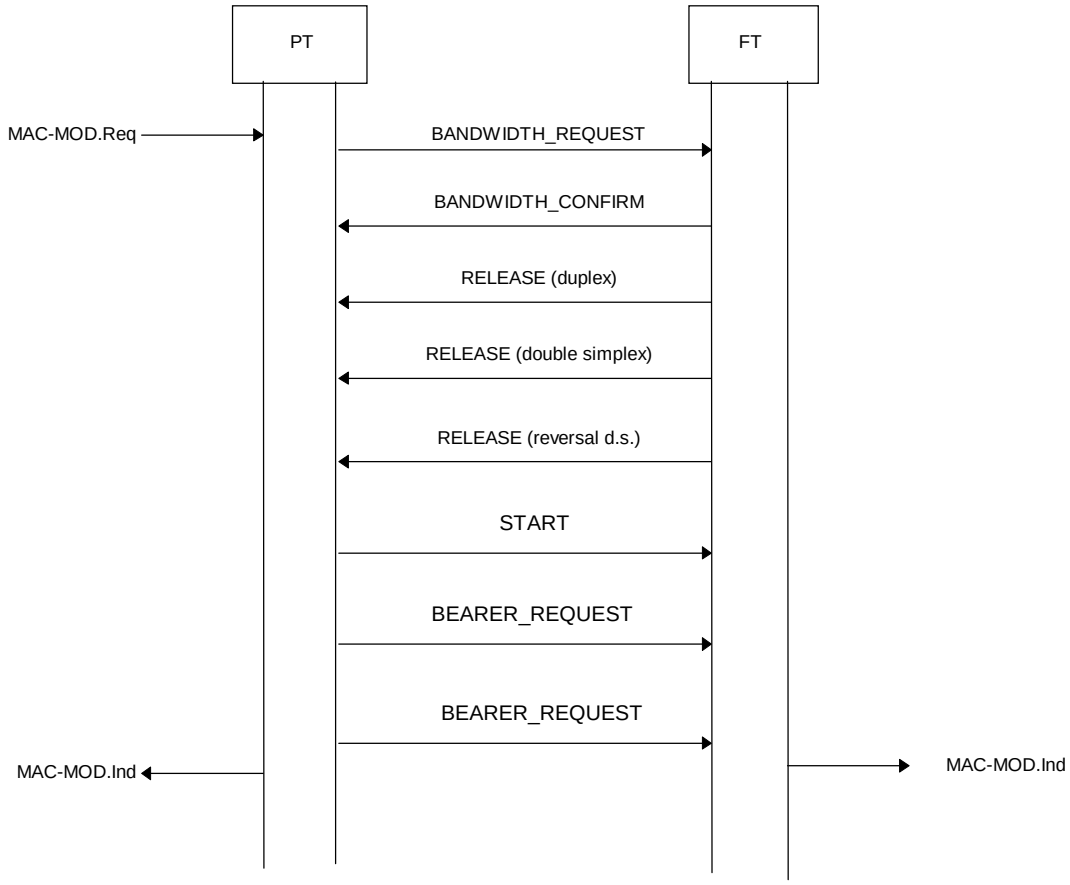


Figure 99: Connection modification

12.6 Bearer handover request

12.6.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.2.5.2 in the MAC control (M_t) message shall be supported by the PT and the FT.

Table 133: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>		
	<Command>	1	"Bearer_handover_request".
		4	"Bearer_confirm"
		5	"Wait"
	<FMID>	All	
	<PMID>	All	See subclause 14.4

12.7 Connection handover request

12.7.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.2.5.2 in the MAC control (M_t) message shall be supported by the PT and the FT.

Table 134: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	0	
	<Command>	2	"Connection_handover_request". PT shall capable to send. FT shall be capable to process.
		4	"Bearer_confirm"
		5	"Wait"
	<FMID>	All	
	<PMID>	All	See subclause 14.4

12.8 Cs channel data

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 10.8.1.1.

12.9 Q2 bit setting

The procedure shall be performed for Cs channel as defined in EN 300 175-3 [2], subclause 10.8.1.3.1.

12.10 RFPI handshake

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 11.5.1. The FT shall ignore the received E-bit.

12.11 Antenna diversity

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 10.8.1.3. The PT shall send and set Q1 bit accordingly. The FT may use the Q1 bit information to perform locally antenna diversity procedure.

12.12 Sliding collision

The procedure shall be performed as defined in EN 300 175-3 [2], subclause 10.8.1.3. The FT shall send and set Q1 bit accordingly when Q2 is set to "1". The PT may use the Q1 bit information to detect a sliding collision situation and act accordingly.

12.13 Encryption process - initialization and synchronization

The procedure shall use DSCA and shall be performed as defined in EN 300 175-7 [6], subclauses 6.4.4 and 6.4.5 of Encryption shall be applied for the logical Cs and In channels.

The FT shall (if encryption is provided by the FT) support broadcast of multiframe number as defined in EN 300 175-3 [2], subclauses 7.2.3.7 and 9.1.1. The multiframe shall be synchronized between the RFPs in the whole FP area.

Table 135: Values used within Qt multiframe number message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<multiframe number>>			
	<Q header>	6	
	<spare>	111100001111B	
	<multi frame number>	All	The number of the multiframe, modulo 2**24.

12.14 Encryption mode control

The procedure shall be performed as defined in EN 300 175-7 [6], subclause 6.4.6.

12.14.1 M_t message

The following fields as defined in EN 300 175-3 [2], subclause 7.2.5.7 in the MAC control (M_t) message shall be supported by the PT and the FT.

Table 136: Values used within M_t message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<M_t message>>			
	<M_t header>	5	Encryption control.
	<Command>	0	Start Encryption Request
		1	Start Encryption Confirm
		2	Start Encryption Grant
		4	Stop Encryption Request. The support of this code is mandatory only if service M.12 is implemented.
		5	Stop Encryption Confirm. The support of this code is mandatory only if service M.12 is implemented.
		6	Stop Encryption Grant. The support of this code is mandatory only if service M.12 is implemented.

12.15 Handover encryption process

The procedure shall be performed as defined in EN 300 175-7 [6], subclause 6.4.7.

12.16 Extended frequency allocation

This procedure shall be performed as defined in EN 300 175-3 [2], subclauses 7.2.3.3 and 7.2.3.2.7.

Table 137: Values used within extended RF carrier information message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Extended RF carrier information>>			
	<Q header>	2	
	<Reserved>	0	
	<Spare>	0	
	<Number of RF carriers>	All	

12.17 MAC suspend and resume

12.17.1 Suspend

The ME in the FP shall ensure that a connection is always released, together with all its bearers, if for a consecutive period of at most 5/n seconds, where n = the number of duplex plus double simplex bearers ($1 \leq n \leq 12$), no DLC-PDU has been received or sent successfully over it. The procedure is initiated by the FP and is build on the unacknowledged release procedure in case of duplex bearers and double simplex bearers in case the FP is the T-side. In case of double simplex bearers and the FP is the R-side, the acknowledged release procedure shall be used.

Higher layer information for a suspended connection are maintained. Therefore the encryption key shall be kept by the MAC ME.

12.17.2 Resume

The PP or FP shall not establish a connection unless one or more DLC-PDU's are available for point-to-point transfer. When MAC resources related to an already established higher layer connection are re-established, it is not necessary to enable encryption over the air. The ME in both FP and PP will start encryption after the second other message and/or for double simplex after the third frame boundary after the START message.

Resumption can be achieved by fast set-up or by MAC paging.

12.18 PP-to-PP ad-hoc communication

When in FP mode for the purpose of PP-to-PP ad-hock communication the PP_FP shall transmit intercell handover (bearer or connection) not allowed to prevent PPs from attempting handovers to PP_FPs in FP mode that are not in communication with that PP.

12.19 Cf channel data

The procedure shall be performed as defined in EN 300 175-3 [2].

13 PHL layer requirements

The physical layer shall conform to EN 300 175-2 [1] with tests specified in EN 300 176-1 [8], with the following constraints:

- full slots shall be used;
- the Portable radio Termination (PT) shall be capable of operating on any one, and no more than one, physical channel in each time slot;
- all Radio Fixed Parts (RFPs) shall be capable of operating on at least any one physical channel in each time slot;
- use of the Z-field is not required by this profile.

14 Management procedures

14.1 Management of MM procedures

The procedure shall be performed as defined in EN 300 175-5 [4], subclause 15.5. The following text together with the associated subclauses define the mandatory requirements with regard to the present document.

A MM procedure may consist of one or more transactions. Each transaction is owned by a single instance of a MM entity. Each instance of a MM entity may own only a single transaction. The priority level relates to the transaction, and not to the procedure.

14.2 Location registration initiation

The initiation of the location registration procedure (PT initiated) is dependent of the value of call attribute a38 broadcasted by the FT i.e. if set to "1" the PT initiates the location registration procedure in the following cases:

- upon change of LA; latest immediately after entering the CC null state (T-00);
- upon power-up and after the first lock to a system which the PT has access rights to.

Location registration shall be performed regardless if the system has been accessed via a PARI or SARI.

If call attribute a38 set to "0", the PT does not initiate the location registration procedure except upon receipt of "Locate suggest" in the parameter retrieval procedure initiated by the FT.

The FT may initiate and the PT may receive incoming calls without a location registration procedure. The initiation of the location registration procedure as defined in subclause 8.31 is always mandatory in the PT except when bit a38 in the broadcast attributes, see table 138, is set to 0.

Location registration is initiated immediately after a successful access rights procedure.

14.3 Assigned individual TPUI management

Only one individual assigned TPUI shall be stored per subscription i.e. any new assignments of an individual assigned TPUI overwrites an existing individual assigned TPUI.

The PT shall always delete the old individual assigned TPUI immediately when entering a new LA prior the initiation of location registration procedure. The PT shall always delete the old individual assigned TPUI immediately when entering a new LA even if the location registration is not being performed i.e. the broadcast attribute a38 is set to value "0", see table 138.

The default TPUI shall be derived from the allocated IPUI. If no IPUI has been allocated, the TPUI shall be derived from IPUI N i.e. the International Portable Equipment Identity (IPEI).

The LCE-PAGE-REJECT message shall not be used to delete an assigned TPUI.

NOTE: To avoid ambiguities of assigned TPUIs/PMIDs, assigned TPUIs should be unique within the entire FP rather then within LAs, see EN 300 175-6 [5], subclause 6.3.1, note 2.

14.4 PMID management

If the PP has a valid assigned individual TPUI, the PMID shall be this TPUI.

If the PP has not a valid assigned individual TPUI, the PMID shall be the arbitrary PMID. It may be derived from the IPUI used for the MAC connection set-up.

Within a link establishment procedure, the assigned PMID is recalculated for every connection set-up attempt (during the connection set-up procedure the assigned PMID shall not change); the arbitrary PMID is recalculated for every new bearer set-up attempt.

The PT shall not update its PMID until the current DLC link is released even if a connection or bearer handover has taken place or the individual assigned TPUI has changed, e.g. due to change of the LA.

14.5 DCK management

The FT is responsible for initiating and storage of a DCK, (see subclause 8.30) for the relevant procedure, and shall take into consideration that the PT may not have a DCK or may not have a valid DCK when entering a LA (or "SARI" area).

14.6 Broadcast attributes management

RFPs belonging to the same LA shall broadcast the same values of higher layer attributes (see EN 300 175-5 [4], annex F) at any given time.

The GAP PP shall be capable to read and interpret at least the following broadcast attributes codings during locking procedure. In the locked state the PP may assume them as static.

Table 138: Higher Layer Capabilities interpretation by the PP

BIT Number	Attribute	Value	Note
a32	ADPCM/G.726 Voice service	All	
a33	GAP and/or PAP basic speech	All	
a36	Standard authentication required	All	
a37	Standard ciphering supported	All	
a38	Location registration supported	All	See location update procedure, subclause 8.32 as an exception.
a40	Non-static FP	All	A FP which is mounted on a moving vehicle.
a44	Access Rights requests supported	All	The FP can toggle this bit to enable or disable on air subscription, (see annex G).
a46	Connection handover supported	All	

Table 139: Extended Higher Layer Capabilities interpretation by the PP

BIT Number	Attribute	Value	Note
a40	MMAP	All	Every MMAP compliant FP shall set this bit to 1
a41	Asymmetric Bearers Supported	All	
a45	Data Service Profile C	All	This bit shall further clarify what type of MMAP: shall be set to 1 for RS232
a46	Data Service Profile A/B	All	This bit shall further clarify what type of MMAP: shall be set to 1 for WLAN

14.7 Storage of subscription related data

The data as defined in table 140 shall be stored in the PP non-volatile memory as part of normal power-down routine of the PT. Removal of the battery whilst the PP is powered is not considered as a normal power-down. The PP shall be capable to retrieve the data upon power on and associate it to the subscription.

Table 140: Storage of identities/data

Item	Identity/Data	Normative comment
1	IPUI	Given at subscription.
2	PARK	Given at subscription. PARK shall be the complete PARK, including non significant bits.
3	PLI	Given at subscription.
4	LAL	Last received value.
5	ARI	Last received value. Implementations are not mandated to store PARI bits that are not covered by LAL.
6	RPN	Last received value. Implementations are not mandated to store PARI bits that are not covered by LAL.
7	UAK/AC	UAK and AC shall not co-exist within one subscription.
8	ZAP field	If supported
9	<Service class> field	If supported

The data as defined in table 141 shall be deleted in the PP upon power-down.

Table 141: Storage of identities/data

Item	Identity/Data	Normative comment
1	TPUI	Default TPUI shall be used upon power on.
2	DCK	Last value told to store.

14.8 Link resource management

The necessity to manage the use of radio resources in the most efficient manner, requires the participation of all the entities in the PP and FP. The higher layer entities are responsible for the presence or absence of the valid data at the MAC and LUx service boundaries upon which such lower layer resource management is based. The management entity shall consider that there is valid user data available to the lower layers, if a call transaction identifier exists and the call is active and not suspended, or if there are any valid LAP-C frames to transmit.

In all other cases, it shall consider that there is no valid user data available.

The request to suspend the call is issued by the Interworking Functions (IWF) to the DECT network layer through service primitives, but it shall be a management entity decision as to when to suspend or to resume a call.

The ME may choose at any time to suspend the call according to implementation-dependent specific algorithms. In any case, the ME shall suspend or release the call at least if all the following conditions are satisfied:

- the encapsulation entity in the IWF has not passed an user data packet for transmission to LAP-U for a period of 5/n, where n is the number of active duplex and double simplex MAC bearers related to LAP-U connection;
- the segmentation entity in the IWF contains no pending user data in its receiving packet assembly buffers;
- LAP-U is in an idle condition, as defined in annex A, subclause G.6.2;
- There are no peer-to-peer signalling procedures ongoing or pending and not a part from an active call.

The ME involving the PP and the FP shall not resume the call until either of the following conditions are met:

- There is data to be sent over the U-plane;
- There is a signalling message to be sent by a suspended C-plane entity.

LLME shall ensure that all responsible layers and processes are informed before a resources allocation/modification is to be made.

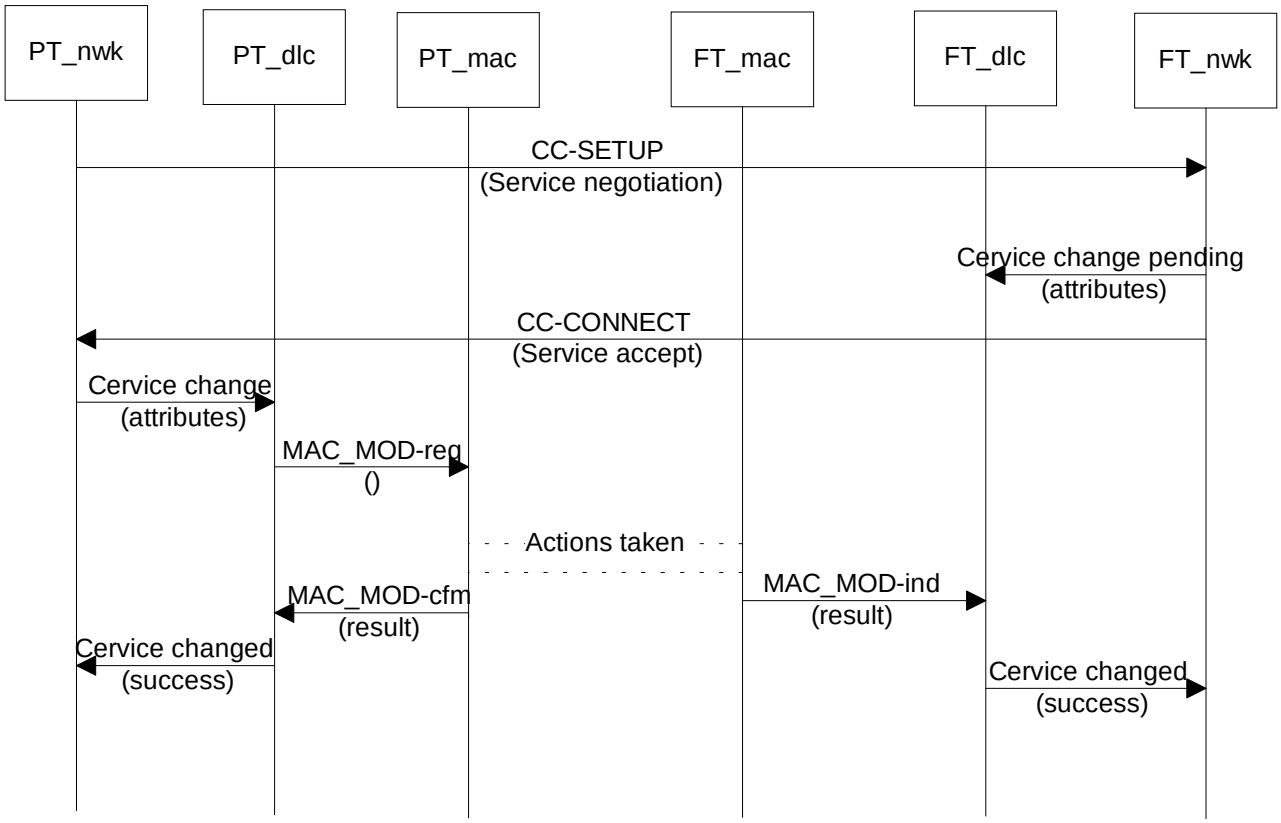


Figure 100: Example of service negotiation procedure with the initiating side initiating the resources allocation

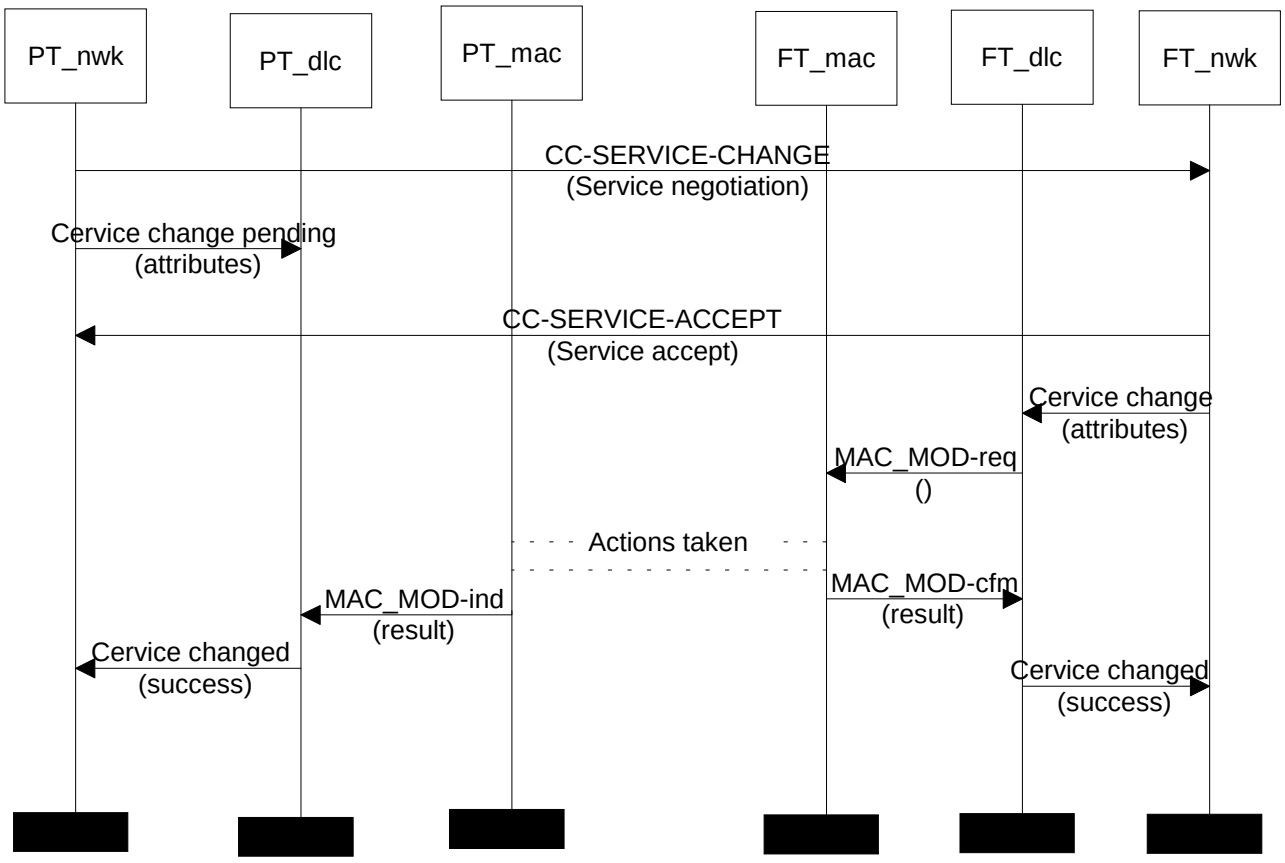


Figure 101: Example of service negotiation procedure with the receiving side initiating the resources allocation

14.9 NWK layer Suspend and Resume

If the link was previously ciphered the resumed link shall be ciphered as well if it was a U-plane resume procedure. Ciphering shall take place before the receiving side sends back the {CC-SERVICE-ACCEPT} message. If it was a CC resumption the link may remain un-ciphered.

During the suspension of a call a MM procedure may need to take place. The initiating entity shall establish a new link. If during the existence of the link a RESUME need to take place, the same link shall be used.

When the DL_ESTABLISH_cfm primitive is received the initiating side shall send the waiting message. When the peer side receives the message it shall check the TI whether there is a suspended call that matches and shall associate the link with it if there is such one otherwise the link shall be handled depending on the available resources. Than it shall react depending on the message received.

Establishment of new link for the purpose of call resumption may not be possible.

Suspended call may be cleared unnoticed. Whenever a {CC-SERVICE-CHANGE} message is received specifying a transaction identifier which is not recognized as relating to a suspended call clearing shall be initiated by sending a {CC-RELEASE-COM} message with release reason "unknown transaction identifier", using the same (unknown) transaction identifier in the returned message.

15 Application procedures

15.1 Subscription control

The PP shall be capable of accepting a new subscription for the active IPUI and PARK pair, in order to change the access rights (i.e. overwriting the active subscription).

The active IPUI/PARK pair is the stored IPUI/PARK value that the PT is using to seek to get locked or is locked to.

The PT shall be capable of storing at least two subscriptions i.e. 2 pairs of IPUI and PARK and associated subscription data.

15.2 AC to bitstring mapping

The mapping of AC shall be done as follows:

- the AC shall always have a length of 32 bits;
- each decimal digit entered by the user, is translated into one semi-octet (BCD coded). The PT shall be capable to accept any AC between 0 and 8 decimal digits (limits included);
- the resulting string of semi-octets is padded with a number of leading "all ones " semi octets to achieve a total of 8 semi octets;
- the result is a bitstring of 32 bits.

EXAMPLE: A value of "091" (3 decimal digits entered via keypad) is translated into a bitstring AC of the following value:

"1111 1111 1111 1111 1111 0000 1001 0001".

MSB: AC[31] LSB: AC[0]

NOTE: With regard to EN 300 175-7 [6], subclause 4.5.2, AC[0] is defined as the least significant Bit (LSB) as defined above.

15.3 Manual entry of the PARK

In order to allow proper inter-operation of GAP equipment it may be necessary to enter an initial PARK into a PP to allow it to correctly identify a FP to which to subscription register (e.g. in the telepoint or business environment the same physical area may be covered by different providers).

If manual entry of the PARK into the PP is provided, the key sequence shall be as follows:

!!LLP_____PC#

where:

!! is a manufacturer specific enabling key sequence;

LL is a two digit decimal representation of the PARK length;

P_____P is up to 12 octal digit representation of the PARK;

C is a check digit;

is the terminating digit.

The length indication specifies the number of bits in the PARK. The first digit is the most significant digit of the number, between 01 and 36.

The P_____P field is variable length, and the number of octal digits in this field shall be sufficient to define the number of bits indicated in LL; any unused bits shall be ignored by the PP. The first digit represents the most significant three bits of the PARK.

The check digit is calculated as the sum of each digit in the input stream multiplied by its position in the input stream, modulo 11; if the result is 10, this is represented by the digit "*".

EXAMPLE: PARK length is 13 bits; PARK is 101 110 010 001 1

MSB												LSB
1	0	1	1	1	0	0	1	0	0	0	1	1

This is padded out to 15 bits, with two 0's, 101110010001100, which is 56 214 in octal.

Check is calculated as:

1*1 + 2*3 + 3*5 + 4*6 + 5*2 + 6*1 + 7*4 = 1 + 6 + 15 + 24 + 10 + 6 + 28 = 90

90 modulo 11 = 2, hence C=2.

Thus the input key sequence is:

!	!	L	L	P	P	P	P	P	C	#
!	!	1	3	5	6	2	1	4	2	#

Annex A (normative): Changes to EN 300 175

A.1 Changes due to Suspend and Resume

A.1.1 Timers

Since the state of the MAC layer is invisible to higher layers, a timer is necessary to guard the MAC-suspended state. This timer prevents calls to hang in situations where a PT is lost while the connection is suspended.

Add the following line to EN 300 175-3 [2], clause A.1:

T219 = 600 seconds: MAC suspend state timer.

A.1.2 Messages

To inform the other side that a connection is released due to suspension, an extra release reason needs to be defined for the RELEASE message.

For resumption the normal access request messages can be used, because the other side knows that the connection is in suspended state.

A.1.2.1 A-tail advanced connection control messages

Change the following entry in the table in EN 300 175-3 [2], 7.2.5.3.13 (RELEASE):

1	1	1	1	connection suspend

A.1.2.2 B-field advanced connection control messages

Change the following entry in the table in EN 300 175-3 [2], 7.3.3.10 (RELEASE):

0	0	0	0	1	1	1	1	connection suspend
0	0	0	1	0	0	0	0	}

A.1.3 Primitives

Since suspend and resume procedures are controlled by the ME instead of the higher layers, extra primitives need to be defined for this purpose.

A.1.3.1 Management primitives

The ME should be informed of a resumed connection, like it is informed of a new connection. Change EN 300 175-3 [2], 8.3.1.1:

8.3.1.1 Connection set-up: MAC_ME_CON {ind}

Parameters:

- basic/advanced connection;
- ECN (if advanced connection);
- new connection/bearer handover/connection handover/connection resumption;
- old MCEI (if connection handover).

Also, to give ME the control over suspend and resume procedures, add to EN 300 175-3 [2]:

8.3.1.5 Connection suspend: MAC_ME_SUSPEND {req, cfm, ind}

Parameters:

- ECN;

8.3.1.6 Connection resume: MAC_ME_RESUME {req, cfm, ind}

Parameters:

- ECN;

A.1.4 Procedures

A.1.4.1 MAC layer

The MAC level suspend and resume procedures shall be added to the appropriate section of EN 300 175-3 [2].

Add to EN 300 175-3 [2]:

10.10 C/O connection suspend and resume

The following procedures provide means to suspend an advanced connection by only releasing the Traffic Bearer Control (TBC) instances, but leaving the MBC intact.

These procedures are used in situations where fast connection set-up and release is necessary, e.g. in packet data applications. In the normal case, the suspend and resume procedures are invisible for the higher layers.

10.10.1 C/O connection suspend

FT initiated:

The procedure is started upon receipt of a MAC_ME_SUSPEND.req from the LLME. The MBC initiates an unacknowledged bearer release on all associated TBCs, with reason "connection suspend", and disconnects the TBCs. After the last TBC has been disconnected, FT-MAC confirms the connection suspend to the LLME.

The PT-TBC instances controlling the released bearers indicate bearer release to the controlling MBC, with the reason field set to "connection suspend". When the last PT-TBC has been disconnected, the controlling MBC indicates a connection suspend to the LLME.

PT initiated:

The procedure is started upon receipt of a MAC_ME_SUSPEND.req from the LLME. The MBC initiates an unacknowledged bearer release on all associated TBCs, with reason "connection suspend", and disconnects the TBCs. After the last TBC has been disconnected, the PT-MAC confirms the connection suspend to the LLME.

The FT-TBC instances controlling the released bearers indicate bearer release to the controlling MBC, with the reason field set to "connection suspend". When the last FT-TBC has been disconnected, the controlling MBC indicates a connection suspend to the LLME.

In both cases, the LLME in the FT starts timer T219 as soon as the MAC connection is in suspended state. When time-out of T219 occurs, the FT LLME initiates a resume procedure to check whether the PT is still reachable. In case of success, the LLME may again suspend immediately.

While the MAC connection is in suspended state, the quality of service shall be maintained as if the connection were still active. This means that in suspended state the PP shall be able to detect fast set-up attempts from the FP, and that connection and external handovers are executed when necessary. For purpose of handover, the suspended connection first needs to be resumed.

10.10.2 C/O connection resume

FT initiated:

The procedure is started upon receipt of a MAC_ME_RESUME.req from the LLME. The resume procedure may be initiated from either side of the connection. The resumed connection shall have the same characteristics as it had before it was suspended. The connection may be modified after the resume operation has been finished.

The resume procedure itself is similar to a fast connection set-up procedure (see subclauses 10.2.4.2 and 10.2.4.3). In case of success, the MAC layer confirms this to the LLME. In case of failure, the higher layers are notified of this event with a MAC_DIS indication, with the result field set to "abnormal".

PT initiated:

This procedure is similar to the FT initiated connection resume procedure.

The specification of the conditions for connection release shall also be changed, so that an MBC without any associated active TBC survives if it is in suspended state. Therefore change the following in EN 300 1753 [2], subclause 10.4.1:

d) as a result of bearer release, no TBC controlling a duplex bearer exists and the MBC is not in suspended state;

A.2 Changes due to Distributed Communication

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				Key number				3
	Key								4 … L+2

Figure A.1: KEY information element

Key type coding (octet 3):

Bits 8 7 6 5 Meaning
0 0 0 1 User authentication key (UAK)
0 0 1 1 User personal identity (UPI)
0 1 0 0 Authentication code (AC)
1 0 0 1 Derived Cipher Key (DCK)
1 0 0 1 Static Cipher Key (SCK)
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).

Key number (octet 3):

Bits 4 3 2 1 Meaning
Contains the binary coded number of the selected 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

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 1: 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 ? i ? N-1.

NOTE 2: The length of a particular key is defined in EN 300 175-7 [6].

7.7.23 IWU to IWU

….

Protocol Discriminator (PD):

Bits 6 5 4 3 2 1 Meaning
1 0 0 0 1 1 Terminal data

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

Bit:	8	7	6	5	4	3	2	1	Octet:
	Discriminator type				Terminal Id				4
	Terminal Id								5
	Terminal Id								6
	Terminal Data								7
									L+2

Figure A.2

Discriminator type (octet 4):

Bits 8 7 6 5 Meaning
0 0 0 0 Portable Termination Information
0 0 0 1 Fixed Termination Information
0 0 1 0 HyP Information
All other values reserved

Terminal Id (octet 4 to 6):

Gives a number under which all related to particular PT data may be collected and when needed referenced. The value is binary coded value with LSB in bit position 1 of Octet 6.

Terminal Data (octets 7 to L+2)
Information about any of the following data derived from the subscription record of the particular terminal identified under the "Terminal Id" can be provided: PARK, PLI, IPUI, TPUI, LAL, UAK, UPI, AC, DCK and SCK, type of HyP or PP in regard to Distributed Communication

Any number of values can be provided within one <<IWU-to-IWU>> information element.

Each particular value shall be provided using the structure of the relevant information element that is used elsewhere in DECT, in this term:

PARK - the <<Fixed Identity>> information element shall be used, see 7.7.18;

IPUI, TPUI, etc. - the <<Portable Identity>> information element shall be used, see 7.7.30;

LAL - the <<Location Area>> information element shall be used, see 7.7.25;

UAK, UPI, AC, DCK and SCK - the <<Key>> information element shall be used, see 7.7.24;

type of HyP or PP in regard to Distributed Communication - <<Alphanumeric>>, see 7.7.3.

Additional Transparent Information about the Particular devise can be provided by including:

Transparent Information
Application specific

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>>							
	Call class				Basic Service				2

Figure A3: BASIC-SERVICE information element

Call class (octet 2):

Bits 8 7 6 5 Meaning

…

0 1 0 1 Direct call set-up

…

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 ext	List of one or more parameter types							3

Figure A4: INFO-TYPE information element

Parameter type coding (octet 3):

Bits 7 6 5 4 3 2 1 Meaning

…

0 1 0 0 1 0 1 Distributed Communication download

…

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	Subclause	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-*
Call Identity	7.7.6	O	-	3-*
Repeat Indicator	7.6.3	O	-	1
Fixed identity	7.7.18	O	-	5-20
Location area	7.7.25	O	-	3-*
NWK assigned identity	7.7.28	O	-	5-20
Network parameter	7.7.29	O	-	4-*
Duration	7.7.13	O	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
KEY	7.7.24	O	-	4-
Escape to proprietary	7.7.45	O	-	2-*

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

Figure A5

Annex B (normative): Distributed Communication

This is a proposal for introduction of DECT Distributed Communication feature. Though specially design for DATA communication this feature could be used for voice applications as well.

B.1 Types of Terminals

B.1.1 Groups of terminals

Three basic groups of DECT terminals may be identified:

- The FP group - all terminals that provide FP functionality but does not provide PP functionality;
- The PP group - all terminals that does not provide FP functionality but does provide PP functionality;
- The HyP group - all terminals that provide both FP functionality and PP functionality.

The FP and the PP groups shall provide a full set of FT/PT protocol features/services according to a particular Profile.

Each mode of the HyP group - FP or PP, may provide a full or a limited subset set of protocol features/services according to a profile.

Intra groups communication when one or more HyPs are involved requires additional protocol support. FPs and/or PPs may but need not to provide such a support. Intra DECT terminals communication including HyPs is referred hereafter as "distributed communication".

B.1.2 Classes of terminals

Every particular member of each group of terminals apart of providing different profile related features/services may claim different capabilities in relation to distributed communication.

In regard to the distributed communication the groups of terminals are here after divided further in subclasses based on the capabilities offered by the involved terminals, e.g. whether they can recognize from which of the groups identified above is the terminal they are in communication or intent to.

NOTE: Whether a PP is able to distinguish a FP from a HyP in FP mode is not considered as essential for the purpose of distributed communications. The provision of services to support the distributed communication is only of interest.

B.1.2.1 FPs that do not support distributed communication

There may be FPs that cannot distinguish a PP from a HyP in PP mode.

NOTE: Though this sub-group is not of interest to the distributed communication it is here considered in order to ease understanding and form a bases for the specification that follows.

For the purpose of the distributed communication such FPs are further divided based on the type of feature-services they provide to a PP as follows:

Table B.0

Class	provides means for accessing external telephone line	provides means for support of more than 1 PP simultaneous calls at a time	provide means for performing internal calls between 2 PPs
Class FP OS (Open-Simple)	YES	NO	NO
Class FP OL (Open-Limited)	YES	YES	NO
Class FP OB (Open-Basis)	YES	YES	YES
Class FP CS (Closed-Simple)	NO	NO	NO
Class FP CL (Closed-Limited)	NO	YES	NO
Class FP CB (Closed-Basic)	NO	YES	YES

B.1.2.2 FPs that support distributed communication

All such FPs can distinguish a PP from a HyP and provide support for distributed communications.

Based on the division made in subclause B.1.2.1 we can identify 6 classes of such FPs:

- Class FP OSD.
- Class FP OLD.
- Class FP OBD.
- Class FP CSD.
- Class FP CLD.
- Class FP CBD.

B.1.2.3 PPs that do not support distributed communication

For the purpose of the distributed communication there are 2 classes of PPs identified:

Table B.0.A

Class	Provides means for support of Outgoing call
Class PP A (Active)	YES
Class PP P (Passive)	NO

B.1.2.4 PPs that support distributed communication

All such PPs provides means of support to the distributed communication.

Based on the division made in subclause B.1.2.3 they are further divided in 32 classes:

- Class PP AD.
- Class PP PD.

B.1.2.5 Distributed communication subdivision

Every terminal that supports the Distributed Communication may support either:

- only Voluntary Distributed Communication;
- only Involuntary Distributed Communication;
- both Voluntary and Involuntary Distributed Communication.

NOTE: Voluntary and Involuntary distributed communication are described in clause B.2.

Table B.0.B

Class	Voluntary Distributed Communication	Involuntary Distributed Communication
Class FP OSD-VI	YES	YES
Class FP OSD-V	YES	NO
Class FP OSD-I	NO	YES
Class FP OLD-VI	YES	YES
Class FP OLD-V	YES	NO
Class FP OLD-I	NO	YES
Class FP OBD-VI	YES	YES
Class FP OBD-V	YES	NO
Class FP OBD-I	NO	YES
Class FP CSD-VI	YES	YES
Class FP CSD-V	YES	NO
Class FP CSD-I	NO	YES
Class FP CLD-VI	YES	YES
Class FP CLD-V	YES	NO
Class FP CLD-I	NO	YES
Class FP CBD-VI	YES	YES
Class FP CBD-V	YES	NO
Class FP CBD-I	NO	YES
Class PP AD-VI	YES	YES
Class PP AD-V	YES	NO
Class PP AD-I	NO	YES
Class PP PD-VI	YES	YES
Class PP PD-V	YES	NO
Class PP PD-I	NO	YES

B.1.2.6 The HyP group

The HyPs may be divided on the bases what type of FP they support when switched to FP mode and what type of PP - when switched to PP mode.

Every HyP, in each mode shall provide a full set of PT/FT protocol features/services according to a particular Profile. In addition procedures for support of Distributed communication may be provided.

A HyP may switch between modes on user requests, on request from an FP, or, on request from an PP.

B.2 Distributed communications protocol

B.2.1 General

Distributed communication may be requested by User intervention - this is called hereafter "Voluntary Distributed communication".

The Voluntary Distributed Communication comprises the cases when the User of a PP or a HyP requests direct communication (not trough the FP both terminals are subscribed and locked to) to another PP or HyP.

Distributed communication may be requested by the FP without User intervention - this is called hereafter "Involuntary Distributed communication".

Involuntary Distributed communication comprises the cases when two PPs; a PP and a HyP in PP mode; or, two HyPs in PP mode need to communicate to each other trough a FP they have subscription and are locked but the FP is not willing or is not capable of performing the operation. The FP may decide to re-direct (distribute) the communication by requesting the HyP (if a HyP is involved) to switch to FP mode for the purpose of direct communication with the PP; or, may request the PPs to connect to another FP trough which to perform the call (this may include request to a HyP to switch to FP mode to assist the communication between the PPs).

The procedures below are described from NWK layer point of view.

B.2.2 Voluntary Distributed communications

B.2.2.1 PP to HyP

A PP asks a FP to request a HyP to switch to FP mode for the purpose of direct communication between the PP and the HyP.

On User request the PP shall initiate the Distributed communication request procedure as described in subclause B.2.4.1 indicating " Distributed Communication REQUEST ", "Change Mode" and providing the connectionless TPUI of the desired HyP.

NOTE: This procedure may be used for HyP-to-HyP communication when the first HyP is to remain in PP mode.

If the procedure is successful (the related CLMS-FIXED message received from the FT indicates "Accept") the PP shall start searching for the new RFPI (as indicated in the CLMS-FIXED message received from the FT). If the RFPI is not found within a time of 100 sec, the PP shall lock back to the initial FP.

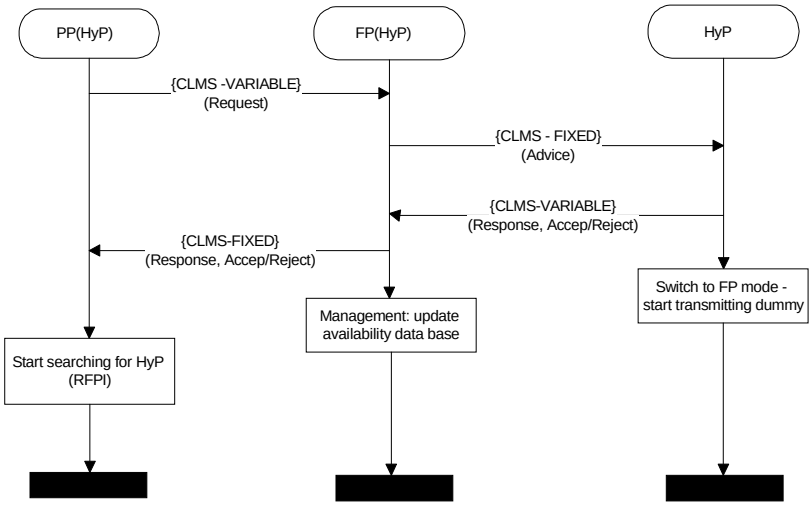


Figure B.1: Voluntary Distributed communication

B.2.2.2 HyP to PP

A HyP asks a FP to request a PP to attach to the HyP when the HyP in FP mode for the purpose of direct communication between the PP and the HyP.

On User request the HyP shall initiate the Distributed communication request procedure indicating "Distributed Communication REQUEST", "Attach" and providing the connectionless TPUI of the recommended HyP.

NOTE: This procedure may be used for HyP-to-HyP communication when the second HyP is to remain in PP mode.

If the procedure is successful (the related CLMS-FIXED message received from the FT indicates "Accept") the HyP shall switch to FP mode and after the PP attaches shall initiate a call. If the PP does not attach within a time of 100 sec, the HyP shall lock back to the initial FP.

B.2.2.3 PP to PP

A PP may ask a FP to request another PP to lock to another FP for the purpose of direct communications between the two PPs.

On user request the PP shall initiate the "Distributed communication request" procedure indicating "Distributed Communication REQUEST", "Attach" and providing the connectionless TPUI of the desired PP.

NOTE 1: The User may request this procedure e.g. if he tries to communicate to another PP but the system is busy.

NOTE 2: This procedure may be used for a HyP-to-HyP, HyP-to-PP or PP-to-HyP communication as well.

If the procedure is successful (the related CLMS-FIXED message received from the FT indicates "Accept" and provides the RFPI of the new FP) the PP shall start searching for the new RFPI. After successful lock to the new FT the PP shall attempt call to the desired PP. If the request is rejected due to the fact that the desired PP has not yet locked, the PP should repeat the call request after a reasonable time. If the RFPI is not found, or, the call initiation is not accepted within a time of 100 sec, the PP shall lock back to the initial FP.

B.2.3 Involuntary Distributed communications

B.2.3.1 A FP advice a HyP

A FP advice a HyP to switch to FP mode for the purpose of direct communications between the PP and the HyP.

On request (inquiry) from another terminal or on its own the FP shall initiate the Distributed communication advice procedure indicating "Change Mode".

If the procedure was initiated as result of the Distributed communication request procedure the FP shall communicate the result "Accept/Reject" as indicated in the received from HyP CLMS-VARIABLE message.

If the HyP accepts the advice it shall switch to FP mode. If the PP does not attach within a time of 100 sec, the HyP shall lock back to the initial FP. After the attach, in order to switch back to PP mode and lock to the initial FP the HyP shall be requested to do so by another terminal or may be forced by the User of the HyP.

B.2.3.2 A FP advice a PP

A FP advice a PP to search for another FP for the purpose of direct communications between the PP and the HyP.

On request (inquiry) from another terminal or on its own the FP shall initiate the Distributed communication advice procedure indicating "Attach" and shall provide the RFPI of the FP (HyP in FP mode) the PP shall search.

If the procedure was initiated as result of the Distributed communication request procedure the FP shall communicate the result "Accept/Reject" as indicated in the received from PP CLMS-VARIABLE message.

If the PP accepts the advice it shall start searching for the new RFPI (as indicated in the CLMS-FIXED message received from the FT). If it finds the FP it shall "Attach" by performing the Attach procedure as described in subclause B.2.4.6.5. If the RFPI is not found within a time of 100 sec, the PP shall lock back to the initial FP.

B.2.3.3 A FP advice a PP and a HyP

A FP advice a PP and a HyP to communicate directly.

A HyP may request Internal call as described in GAP or elsewhere. If the FP is unable or unwilling to perform the transaction it should attempt to advice the regarded PP (or HyP in PP mode) to lock directly to the HyP. If the advice is accepted, the FP shall advice the HyP to switch to FP mode to perform the direct communication. The HyP should accept the advice, shall release the call and should switch to FP mode.

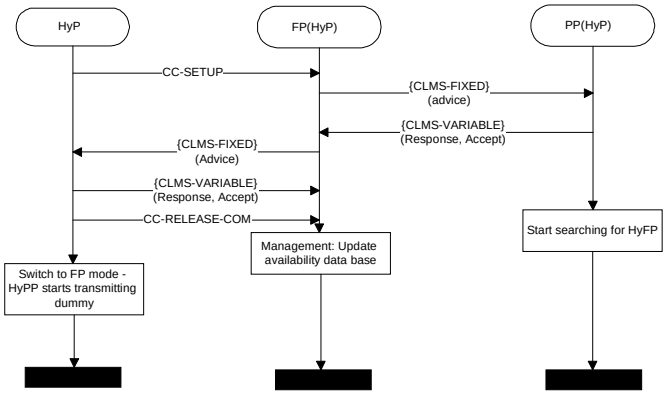


Figure B.2: Involuntary Distributed communication between a HyP and a PP

A PP may request Internal call to a HyP as described in GAP or elsewhere. If the FP is unable or unwilling to perform the transaction it should attempt to advice the regarded HyP to switch to FP mode for to be accessible directly by the PP. If the advice is accepted, the FP shall advice the PP to lock to the HyP for direct communication. The PP should accepts this and shall release the call. The HyP should switch to FP mode and the PP should lock to it.

In case of call resumption after call suspend the same procedure shall be used with the following modifications:

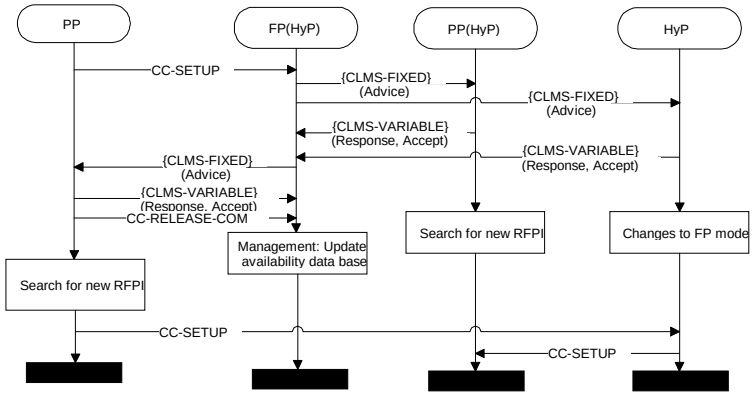
- Instead of {CC-SETUP} the {CC-SERVICE-CHANGE} indicating Call Resume shall be used.
- After successful completion of the procedure FP shall clear all association with the suspended call.
- When the PP attaches to the HyP the initiating side shall initiate the resume procedure and the receiving side shall accept it.

B.2.3.4 A FP advice 2 PPs

A FP advice 2 PPs (NWK Layer) to communicate directly.

A PP may request Internal call to a PP as described in GAP or elsewhere. If the FP is unable or unwilling to perform the transaction and if it knows a free HyP that is capable of performing internal calls when in FP mode the FP should attempt to advice the regarded PPs to lock directly to the HyP as at the same time shall advice the HyP to switch to FP mode to assist the call between the PPs. If the advises are accepted, the initiating PP shall release the call, the HyP shall switch to FP mode and both PPs shall lock to it.

NOTE: Instead of HyP a normal FP may be used, however such a FP need to posses all necessary data in order to perform the transaction.



NOTE: This procedure should be used with care because when in FP mode the HyP cannot be used for communication to the initial FP

Figure B.3: Involuntary Distributed communication between 2 PPs

B.2.3.5 Distributed Communication during active call

A HyP, a PP and a FP may provide capabilities to use the Distributed Communication during an active call between them trough the FP(or HyP in FP mode).

NOTE 1: This may be used by the FP when it cannot satisfy any more the required amount of traffic and big delay is occurring. The special requirement for the HyP is to be capable of communicating to the FP and transmitting dummy at the same time and listening for a PP attempt for communication.

To allow this to take place the FP shall use the distributed Communication advice procedure during the call to alert the PP to lock to the new RFPI and HyP to switch to FP mode and listen for the proper request.

Any of them may reject this if it does not support the procedure.

At the side that support the procedure this will lead to a short period of time (guarded by timer of 100 sec) during which direct communication is expected and the old communication is maintained. After the timer expires the side shall return to the previous condition.

NOTE 2: There is no need to announce whether any of the PP or HyP can support this procedure; upon unsuccessful result of the procedure FP my mark the devices as not supporting it and should not initiate it again.

While still connected to the FP the PP shall start searching for the new RFPI and when found the PP shall lock and initiate a direct call setup procedure to the HyP by sending a {CC-SETUP} message indicating in the <<BASIC-SERVICE>> <Call class> field the direct call setup.

The HyP shall send a {CC-CONNECT} message to the PP, to show confirmation of the switch-over and shall start timer <CC.05>.

The PP shall send a {CC-CONNECT-ACK} message to the HyP, to indicate that the switch-over was completed. On receipt of {CC-CONNECT-ACK} the HyP shall stop timer <CC.05>. If the timer <CC.05> expires before {CC-CONNECT-ACK} is received, the HyP shall immediately release the new connection.

NOTE 3: The receipt of {CC-CONNECT-ACK} is used to control the speech path see below.

The release procedure with the FP shall be initiated as soon as the connection between the PP and the HyP has been established. After the HyP has received the {CC-CONNECT-ACK} message, it shall initiate the release of the old connection by sending a {CC-RELEASE} message. The FP shall then, release the connection to the PP. If the PP has not received the {CC-RELEASE} message from FP N400 seconds after {CC-CONNECT-ACK} message has been sent, it shall release the old link by sending a {CC-RELEASE} message.

This switch-over also involves re-routing the U-plane. The table below shows the recommended receive and transmit path connections for PP.

Table B.0.C

Step	Event	Action	PP receive path	PP transmit path
1	PP sends {CC-SETUP}	PP starts transmission on new connection	FP	FP and HyP
2	HyP sends {CC-CONNECT}	HyP starts transmission	FP	FP and HyP
3	PP receives {CC-CONNECT}		FP	FP and HyP
4	PP sends {CC-CONNECT-ACK}	PP starts receiving on new connection	HyP	FP and HyP
5	HyP receives {CC-CONNECT-ACK}	HyP attaches to new connection.	HyP	FP and HyP
6	PP receives {CC-RELEASE}	PP releases old connection	HyP	HyP

If the connection trough the FP was ciphered, the connection to HyP shall also be ciphered.

The PP may initiate ciphering at MAC any time after it has been requested by the HyP but it should do it as soon as possible after receipt of {CC-CONNECT}.

NOTE: The HyP and the PP may have to delay the initiation of ciphering until the old connection is released if they have implemented only a single cipher engine. This will lead to having the link shortly un-ciphered.

B.2.4 Procedures

B.2.4.1 Distributed communication request

This procedure is based on the requirements specified in EN 300 175-5 [4], subclauses 12.3.1, 14.3.1, 6.3.5.1, 8.3.1 and clause D.3 with the following additions.

Either a HyP in PP mode or a PP may initiate this procedure.

Upon receipt of a MNCL_UNITDATA-req primitive indicating variable length operation, the CLMS at the initiating side 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.

The {CLMS-VARIABLE} as defined in EN 300 175-5 [4], 6.3.5.1 shall be used with the following additions:

Table B.1: Values used within the {CLMS-VARIABLE} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Alphanumeric>>			
	<Protocol Discriminator.Character type>	010	4 bits characters
	<Protocol Discriminator.O/E>	0	Even number of characters
	<Protocol Discriminator.Character set>	001	DECT standard 4-bit characters
	<List of Characters.Discrim>	1111 0000	Distributed communications REQUEST
	<List of Characters.Command>	0000 0001	Attach
		0000 0010	Change Mode
	<<List of Characters>>.Id	Any	CL TPUI of the desired PP(HyP in PP mode) BCD coded

The CLMS shall then deliver the resulting message to the LCE for immediate delivery via the S-SAP. LCE shall react as specified in Connectionless link control procedures- Message routing (see B.2.4.3).

On receipt of the message the FT-CLMS shall map the elements into the parameters of a MNCL_UNITDATA-ind primitive. It shall immediately issue the resulting primitive via the MNCL-SAP.

If the IWU accepts the procedure it shall initiate the Distributed communication advice procedure to the indicated in the received message terminal as specified in subclause B.2.3.2. The acceptance is local matter and should be based on the information that is available in the FT.

To convey the result of the Distributed communication advice procedure the FT-IWU shall send a MNCL_UNITDATA-req primitive indicating fixed length operation providing the CL TPUI of the initiator (PP or HyP) and the outcome "Accept" or "Reject". The FT shall send "Reject" as well if it does not accept the Distributed communication request procedure.

The CLMS entity in the NWK layer shall attempt to map the parameters into {CLMS-FIXED} message elements, using 2 message sections. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

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".

Table B.2: Values used within the {CLMS-FIXED} message 1st segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		010	Multi section/Standard
<<Address>>		Any	lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Character type>	010	4 bits characters
	<O/E>	0	Even number of characters
	<Character set>	001	DECT standard 4-bit characters
<<Length indicator>>		00100000	32 bits

Table B.3: Values used within the {CLMS-FIXED} message 2nd segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		0	Data section
<<CLMS header>>		000	Data section number - 0 (1st)
<<Data>>	<Discriminator>	1111 0001	Distributed communication response
	<Command>	0000 0001	Accept
		0000 0010	Reject
	<Identity>	Any	"don't care" bits if it is an answer to a HyP that shall switch to FP mode Otherwise the last 20 bits of the RFPI of the FP the terminal shall search

LCE shall react as specified in Connectionless link control procedures- Message routing see B.2.4.3.

At the procedure initiating side, 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 initiating side 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. It shall immediately issue the resulting primitive via the MNCL-SAP.

If the request was accepted the IWU shall react depending on the intention of the user reflected into the values indicated into the initial request (the CLMS-VARIABLE message).

B.2.4.2 Distributed communication advice

This procedure is based on the requirements specified in EN 300 175-5 [4], subclauses 12.3.1, 14.3.1, 6.3.5.1, 8.3.1 and clause D.3 with the following additions.

Either a FP or a HyP in FP mode may initiate this procedure. The procedure is applicable, e.g. when a terminal need to be advised to start looking for a new FP it can locked to, or, to change to FP mode.

The IWU at the initiating side shall initiate this procedure by sending a MNCL_UNITDATA-req primitive indicating fixed length operation providing the CL TPUI of the intended PP or HyP in PP mode and the last 20 bits from the RFPI of the HyP or FP the PP should search.

On receipt of the primitive the CLMS entity in the NWK layer shall attempt to map the parameters into {CLMS-FIXED} message elements, using 2 message sections. If no mapping is possible, the message unit shall be discarded, and no further action shall be required.

Table B.4: Values used within the {CLMS-FIXED} message 1st segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		1	Address section
<<CLMS header>>		010	Multi section/Standard
<<Address>>		Any	lowest 16 bits of connectionless TPUI
<<Protocol Discriminator>>	<Character type>	010	4 bits characters
	<O/E>	0	Even number of characters
	<Character set>	001	DECT standard 4-bit characters
<<Length indicator>>		00100000	32 bits

Table B.5: Values used within the {CLMS-FIXED} message 2nd segment

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<A>>		0	Data section
<<CLMS header>>		000	Data section number - 0 (1st)
<<Data>>	<Discriminator>	1111 0000	Distributed communication request
	<Command>	0000 0001	Attach
		0000 0010	Change Mode
	<Identity>	Any	If the code "Change mode is used these are "don't care" bits. Otherwise, these are the last 20 bits of the RFPI of the FP the terminal shall search

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". LCE shall react as specified in Connectionless link control procedures- Message routing, see later.

Upon receipt of a {CLMS-FIXED} message the receiving side 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. It shall immediately issue the resulting primitive via the MNCL-SAP.

If the IWU accepts/rejects the request it shall issue a MNCL_UNITDATA-req primitive indicating variable length operation indicating "Accept"/"Reject".

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.

The {CLMS-VARIABLE} as defined in EN 300 175-5 [4], 6.3.5.1 shall be used with the following additions:

Table B.6: Values used within the {CLMS-VARIABLE} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Alphanumeric>>			
	<Protocol Discriminator.Character type>	010	4 bits characters
	<Protocol Discriminator.O/E>	0	Even number of characters
	<Protocol Discriminator.Character set>	001	DECT standard 4-bit characters
	<List of Characters.Discrim>	1111 0001	Distributed communications RESPONSE
	<List of Characters.Command>	0000 0001	Accept
		0000 0010	Reject
	<<List of Characters>>.Id	Any	The last 20 bits of the RFPI of the FP the terminal will search, or, if the terminal was advised to switch to FP mode, the last 20 bits of the RFPI it will start transmitting

The CLMS shall map the parameters into the {CLMS-VARIABLE} message elements. The CLMS shall then deliver the resulting message to the LCE for immediate delivery via the S-SAP.

LCE shall react as specified in Connectionless link control procedures- Message routing see B.2.4.3.

After the message is successfully transmitted over the air and if it "Accept" was indicated the terminal shall initiate the action it has been advised to take.

On receipt of the message the FT 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.2.4.3 Connectionless link control procedures - 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.

CLMS messages shall be immediately submitted to the DLC - the state of suitable lower resources shall be ignored by the LCE. The LLME is assumed to be responsible for establishing connectionless resources in all lower layers whenever required.

{CLMS-VARIABLE} messages shall 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, the CLMS message shall be submitted over that link using a DL_UNIT_DATA-req primitive via the connection oriented S-SAP (SAPI="0").

A connection oriented link shall not be established to only carry CLMS messages.

{CLMS-VARIABLE} 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.

{CLMS-FIXED} messages shall be sent to the B-SAP using the DL_BROADCAST-req. This shall use the broadcast service of the DLC. {CLMS-FIXED} messages shall use the extended format and shall be sent in a single primitive.

B.2.4.4 DLC Layer Procedures

For to handle the CLMS-VARIABLE related procedures the requirements as specified in EN 300 175-4 [3], subclause 9.3 shall be followed.

For to handle the CLMS-FIXED related procedures the requirements as specified in EN 300 175-4 [3], subclause 9.4 shall be followed.

B.2.4.5 MAC Layer Procedures

For to handle the CLMS-VARIABLE related procedures the requirements as specified in EN 300 175-3 [2], subclause 9.2 shall be followed.

For to handle the CLMS-FIXED related procedures the requirements as specified in EN 300 175-3 [2], subclauses 9.1.3.1 and 9.1.3.2 shall be followed.

B.2.4.6 Distributed Communication Auxiliary Procedures

B.2.4.6.1 General

In any case for Distributed Communication to take place a FP or HyP in FP mode shall be available.

All devices that are able to communicate as PPs:

- shall subscribe to this FT (FP or HyP in FP mode) and shall announce their type in relation to distributed communication see subclause B.2.4.6.2. For this subscription the normal GAP subscription procedure shall be used;

- depending on their type they shall be provided with information related to the distributed communication e.g. Identities, Keys, Information for the type of the other devises connected to the base, etc.. In particular, a commonly known CK and UAK shall be established and distributed to all terminals allowing all procedures that are utilized in normal mode to be performed in distributed communication mode as well. These shall be assigned by the PPs and the HyPs to the IPU/PARK pair relevant to the active subscription to the particular FP (HyP in FP mode) by using different key numbers.

The FP shall provide a HyPs with a RFPI to be used when the HyP switches to FP mode. This RFPI should differ to the FP's RFPI only in the RPN number. To prevent attempts of the PP for handovers to the FP during direct communication with a HyP in FP mode the HyP should announce that inter cell handovers are not supported and shall reject any such attempt.

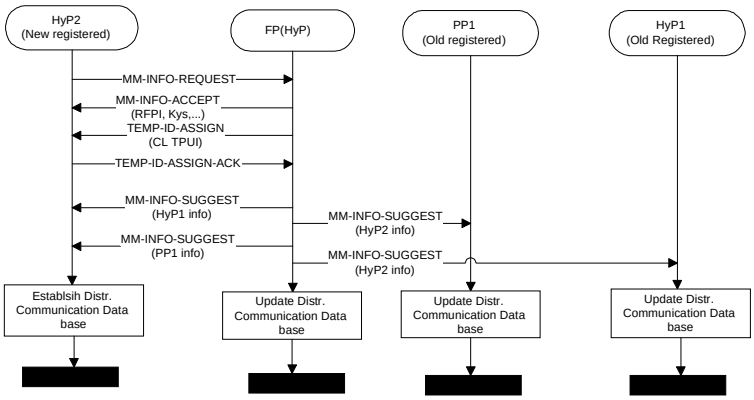


Figure B.4: Summary of Distributed communication download procedures

B.2.4.6.2 PT (HyP in PP mode) initiated Distributed communication download procedure

Every HyP and PP that support Distributed Communication shall be able to initiate on user request or automatically as part of the subscription procedure the Procedure described in this subclause.

NOTE: The User should be advised not initiate the procedure before all available terminals complete the normal subscription procedure as described in GAP to the FT (HyP in FP mode).

Before the essential information is passed over the air the link shall be ciphered.

The Parameter retrieval procedure as described in EN 300 175-5 [4], subclause 13.7 shall be used with the following additions/modifications.

The HyP or the PP shall indicate into the <<Info type>> information element as part of the {MM-INFO-REQUEST} message that the request is for "Distributed communication download" and shall indicate its type in regard to the Distributed Communication.

On receipt of the {MM-INFO-REQUEST} message the FT shall initiate Ciphering and when confirmation for the success of this operation is received FT shall send a {MM-INFO-SUGGESTACCEPT} message providing all or part of the available information:

- a RFPI that the HyP shall use when it switches to FP mode (relevant only for HyP initiated procedure);
- SCK or UAK to be used when the terminals are communicating directly without the assistance of the FP;
- IPUI, CL TPUI and specific direct communication terminal related information for all terminals that support distributed communication and have subscribed to the FP.

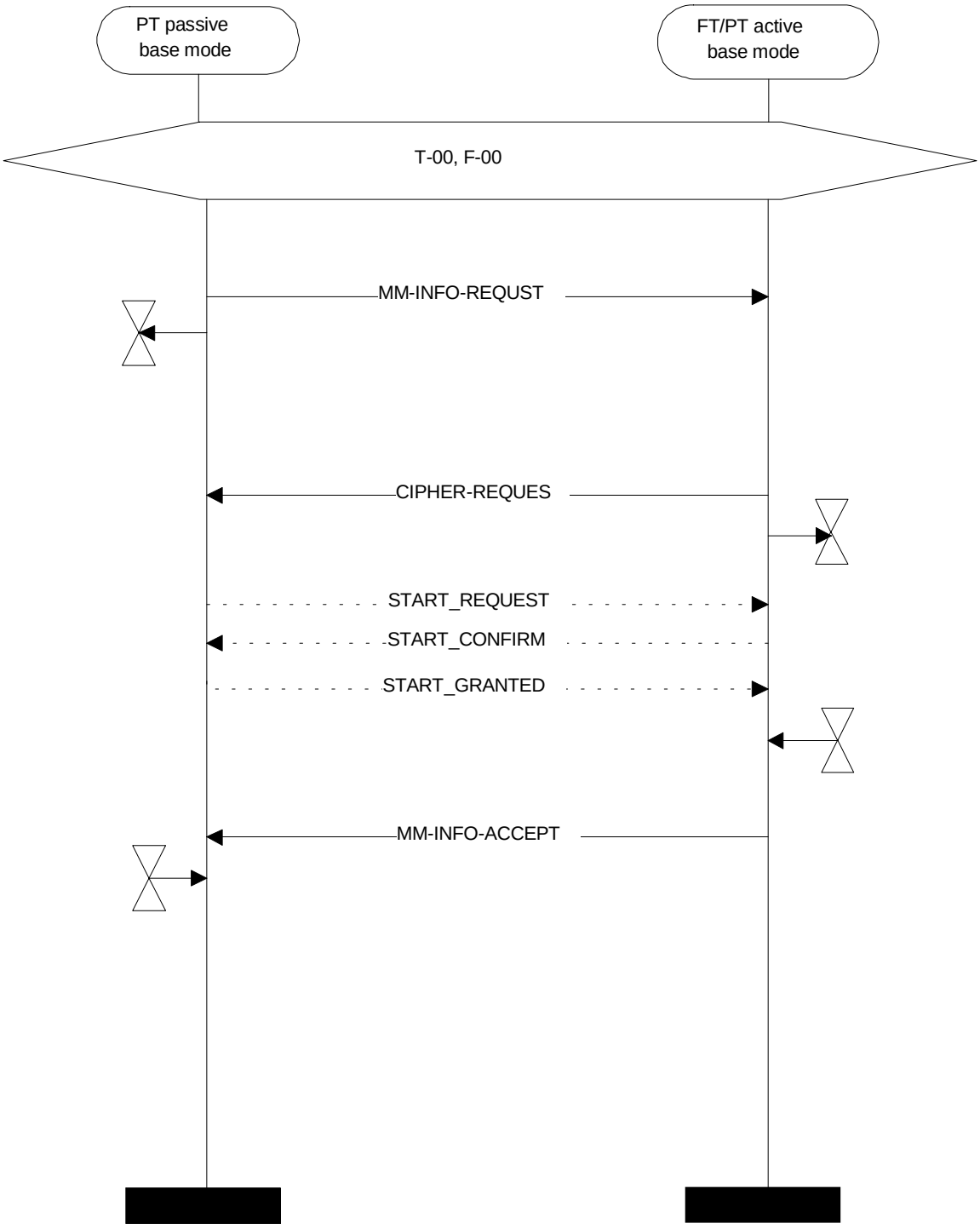


Figure B.5: PT initiated direct mode download procedure

Table B.7: Values used within the {MM-INFO-REQUEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	1	
	<ext>	1	
	<Parameter type>	0 1 0 0 1 0 1	Distributed Communication download
<<IWU-TO-IWU>>			
	<S/R>	1	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	0000	PT information
		0010	HyP Information
	<Terminal Id>	All	CL TPUI
	<Terminal data>. << Alphanumeric>>		<Character type> = 000 <List of Characters> 2 bytes of information the first byte to be used for the PP capabilities (as well the HyP PP capabilities) and the second byte for the HyP FP capabilities - for the values see below
		0000 0001	Class PP AD-VI
		0000 0010	Class PP AD-V
		0000 0011	Class PP AD-I
		0000 0100	Class PP PD-VI
		0000 0101	Class PP PD-V
		0000 0110	Class PP PD-I
		0000 0111	Class FP OSD-VI
		0000 1000	Class FP OSD-V
		0000 1001	Class FP OSD-I
		0000 1010	Class FP OLD-VI
		0000 1011	Class FP OLD-V
		0000 1100	Class FP OLD-I
		0000 1101	Class FP OBD-VI
		0000 1110	Class FP OBD-V
		0000 1111	Class FP OBD-I
		0001 0000	Class FP CSD-VI
		0001 0001	Class FP CSD-V
		0001 0010	Class FP CSD-I
		0001 0011	Class FP CLD-VI
		0001 0100	Class FP CLD-V
		0001 0101	Class FP CLD-I
		0001 0110	Class FP CBD-VI
		0001 0111	Class FP CBD-V
		0001 1000	Class FP CBD-I

Table B.8: Values used within the {MM-INFO-ACCEPT} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	1	
	<ext>	1	
	<Parameter type>	0100101	Distributed communication download
<<Fixed Identity>>			Included only to provide RFPI to a HyP
	<Type >	0000001	ARI+RPN
	<Length of identity value>	0101000	40 bits
	<ARC+ARD>	All	
<<Key>>			This is not required to be included in every message. The FP shall ensure that a SCK and a UAK are transmitted to all subscribed terminals.
	<Key type>	0001 or 1001	UAK or SCK
	<Key number>	1111	Associated with IPUI/PARK
	<Key>	All	UAK –128 bit value, SCK – 64 bits value, see EN 300 175-7 [6]
<<IWU-TO-IWU>>			Any valuable information may be provided by including the relevant DECT information element e.g. fixed identity, key information, or, Location area level related to the particular PP. This provision of additional is optional and not required for support by the PP.
	<S/R>	1	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	0000	PT information
		0010	HyP Information
	<Terminal Id>	All	CL TPUI - Mean to distinguish different terminals
	<Terminal data>		
		<<Repeat Indicator>>	
		<<Portable Id>>	IPUI
		<<Portable Id>>	TPUI
		<<Fixed Identity>>	Shall be sent if the discriminator type is set to "HyP information" to provide the complete RFPI that this HyP will transmit when in FP mode.
		<Transparent information>	Application dependant information, which shall be transparently offered to the application thereby allowing some configuration specific data (as related to drivers, etc.) to be transported between terminals.

The FT (HyP in FP mode) shall ensure that the 63 octets maximum length of a NWK message is preserved. In case of possible overload, data may be split and provided using the FT initiated direct mod download procedure, see B.2.4.6.3.

B.2.4.6.3 FT initiated distributed communication download procedure

The procedure shall be used (in addition to the PT initiated one) to provide the PTs and HyPs with information needed for direct communication in distributed communication environment.

It is the responsibility of the FT to ensure that:

- information about subscribed PPs and HyPs; and,
- direct communication related CK and UAK,

are passed to all subscribed PPs and HyPs.

For the purpose of this procedure the MM-INFO-SUGGEST message shall be used. Before any valuable information is passed over the air the lick shall be ciphered.

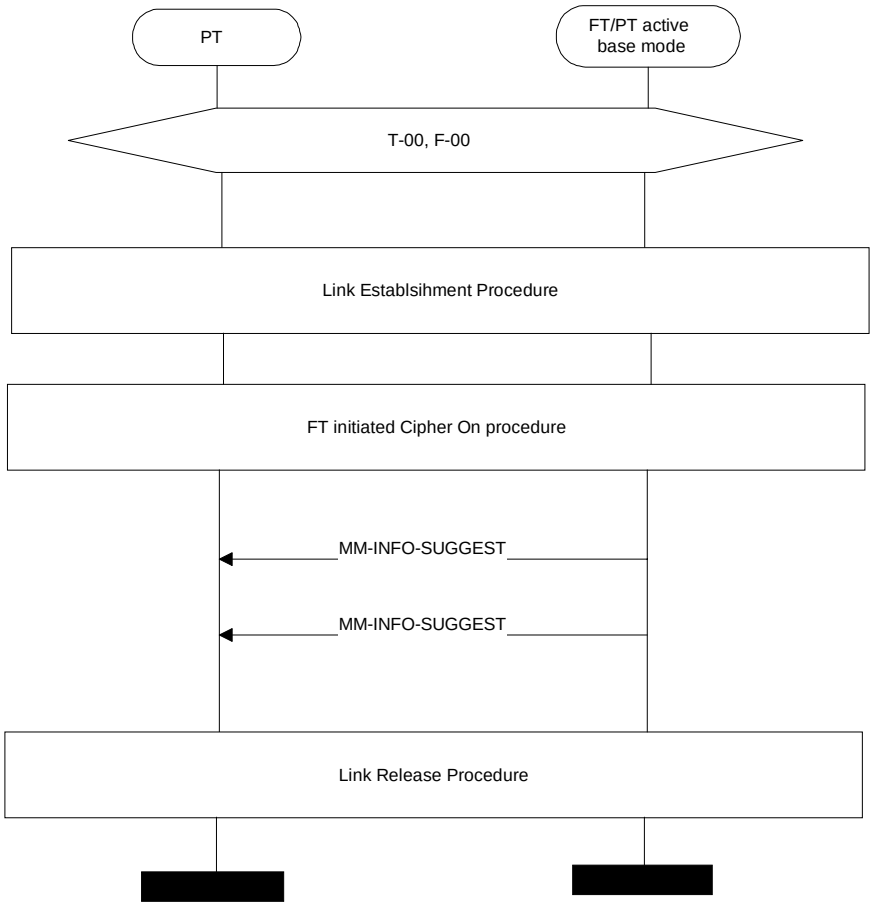


Figure B.6: FT initiated direct mode download procedure

Table B.9: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<Length of Contents >	1	
	<ext>	1	
	<Parameter type>	0100101	Distributed communication download
<<Fixed Identity>>			Included only to provide RFPI to a HyP
	<Type >	0000001	ARI+RPN
	<Length of identity value>	0101000	40 bits
	<ARC+ARD>	All	
<<Key>>			This is not required to be included in every message. The FP shall ensure that a SCK and a UAK are transmitted to all subscribed terminals at least once.
	<Key type>	0001 or 1001	UAK or SCK
	<Key number>	1111	Associated with IPUI/PARK
	<Key>	All	UAK –128 bit value, SCK – 64 bits value, see EN 300 175-7 [6]
<<IWU-TO-IWU>>			Any valuable information may be provided by including the relevant DECT information element e.g. fixed identity, key information, or, Location area level related to the particular PP. This provision of additional is optional and not required for support by the PP.
	<S/R>	1	Transmission of message
	<Protocol discriminator>	100011	Terminal Data
	<Discriminator Type>	000	PT information
		001	HyP Information
	<Terminal Id>	All	CL-TPUI Mean to distinguish different terminals
	<Terminal data>		
		<<Repeat Indicator>>	
		<<Portable Id>>	IPUI
		<<Portable Id>>	TPUI
		<<Fixed Identity>>	Shall be sent if the discriminator type is set to "HyP information" to provide the complete RFPI that this HyP will transmit when in FP mode.
		<<Alphanumeric>>	Type of HyP or PP in regard to distributed communication
		<Transparent information>	Application dependant information, which shall be transparently offered to the application thereby allowing some configuration specific data (as related to drivers, etc.) to be transported between terminals.

B.2.4.6.4 CL TPUI assignment

For assignment of Connectionless TPUI the Temporary Id assign procedure as specified in EN 300 175-5 [4], subclause 13.2.2 shall be used.

B.2.4.6.5 Attach

In order to Attach the PP (or HyP in PP mode) shall use the Location registration procedure, see subclause 8.31, applied without necessary change of location area.

B.2.4.6.6 Detach

The procedure shall be performed as defined in subclause 13.4.2 of EN 300 175-5 [4]. The following text defines the mandatory requirements with regard to this present document.

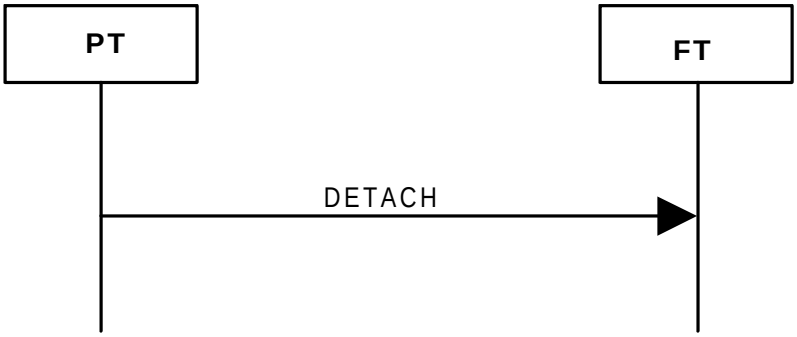


Figure B.7: Detach

Table B.10: Values used within the {DETACH} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Portable-identity>>			
	<Type>	0	IPUI
	<PUT>	All	
	<PUN>	All	
PUN: Portable User Number PUT: Portable User Type			

B.2.4.6.7 System Status Indication

RFPs shall periodically send the "RFP status" (at least every 10 seconds).

Table B.11: Values used within zero length page message

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<Zero length page message>>			
	<Extend flag>	0, 1	See subclause 10.3.2 of EN 300 444 [10]
	<BS SDU length indication>	0	See subclause 10.3.2 of EN 300 444 [10]
	<20 least significant bits of RFPI>	All	See subclause 10.3.2 of EN 300 444 [10]
	<Information type>	10	RFP status
	<MAC layer information>	Corresponding information	

RFP and PP shall support the following values of field "RFP status" (bits a36 to a39): "xx0x" (system clear) and "xx1x" (system busy).

"System busy" means that the FP recommends the PP to access another FP (or HyP in FP mode). In such a case the PP should try the voluntary distributed communication request procedure to get access directly. PP still can try to access the FP in normal way in which case the FP may initiate the Involuntary distributed communication advice procedure to re-direct the communication.

B.2.4.6.8 Distributed communications management

The FP (the initial FP) shall implement a special management procedure to handle the possible frequent change of the system configuration in regard to the distributed communication.

NOTE: It is recommended that a HyP requests Distributed Communication only if it really need to communicate to the desired PP.

To announce that it has locked to a FP (or HyP in FP mode) each terminal shall perform the Attach procedure, see subclause B.2.4.6.5. The FP (or HyP in FP mode) should periodically check for the presence of attached terminals by performing Location Update procedure, see subclause 8.32. In order to help the terminals in taking decision whether to request distributed communication the FP (or HyP in FP mode) shall transmit System status Indication as specified in subclause B.2.4.6.7.

When the User wants to communicate directly (without using the FP) to another terminal part from its system the User should know some kind of identifier which he can apply to distinguish the desired terminal among the others (the CL TPUI may be used). If this terminal is a HyP terminal the communication may be possible. The User terminal itself shall have knowledge of the desired terminal connectionless TPUI.

A suitable User procedure shall be implemented allowing the User to decide whether the terminals, after a successful communication is completed, shall return to the initial FP immediately or on user request. If a terminal wants to return back to the initial FP or do what ever that will prevent any immediate communication between the 2 terminals this terminal shall indicate to its partner explicitly that it shall go back to the initial FP utilizing one of the distributed communication procedures as specified in subclauses B.2.4.1 or B.2.4.2.

If a call is requested to a HyP that has switched to FP mode the FP may advice the calling side to try direct communication to the HyP.

In case of Involuntary Distributed Communication any of the requested for change sides may not be able to perform the request. If FP receives a "Reject" answer to the request for "Change mode" (to a HyP) or "Attach" (to a PP) the FP shall attempt to perform the original request (internal call) and shall react as described in relevant specification for implementation of this Internal call.

Detach shall be performed to the old FP (HyP in FP mode) any time a PP (HyP in PP mode) starts searching for a new RFPI. Detach shall be perform to the old FP (HyP in FP mode) any time a HyP changes to FP mode. Detach shall be performed immediately upon power-down of PT if the PT is still in range of the active subscription. In case of detach, MM may indicate that the normal link release procedures shall be used.

During Attach procedure the HyP in FP mode (or FP) shall not alter any terminal data, i.e. shall not assign new TPUI nor new LAL.

Annex C (informative): Scenarios for Distributed Communication Application

C.1 Basis

In this scenario it is assumed that the User has installed a FP which may as well be a HyP switched in FP mode.

In addition the User has a number of PPs and/or HyPs.

To put its system in operation, the User has to subscribe all available PPs and/or HyPs in PP mode to the FP. They shall announce themselves to the FP as what type of PP or HyP they are in regard to the Distributed communication using the PT initiated distributed communication download procedure, thereby the FP can establish all necessary information and provide back to the PPs and/or HyP all necessary information depending on their type needed for the Direct PP-to-PP communication.

In order further to clarify the requirements in the figure below one particular configuration is considered. The possible different types of FP are depicted under the common name "FP".

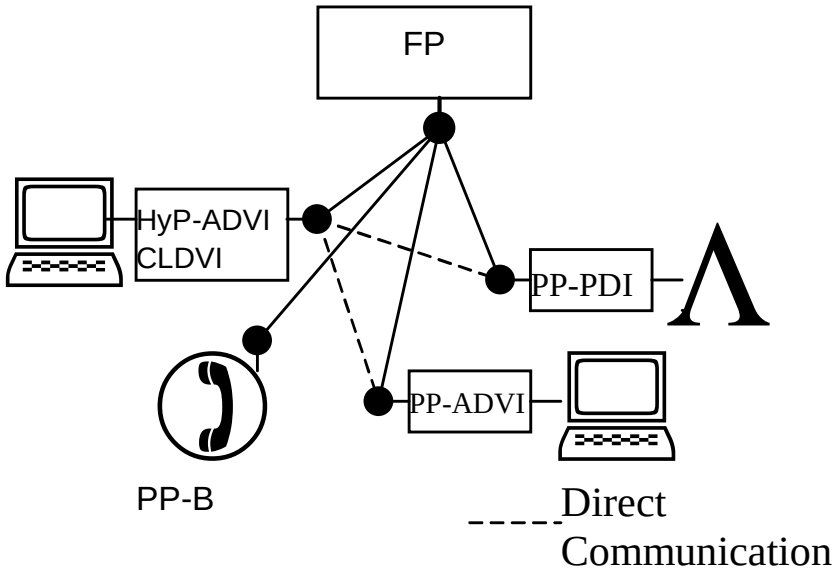


Figure C.1: Basic communication with 2 PCs, Printer and Voice Handset

In this case the FP:

- Shall posses a Subscription record for every PP.
- Shall posses information to facilitate the distributed communication

  SK and UAK.

  Data base for PP-ADVI: CL TPUI, Class PP ADVI, etc.

  Data base for PP-PDI: CL TPUI, Class PP PDI, etc.

  Data base for HyP- ADVI-CLDVI): CL TPUI, RFPI, Class FP CLD-VI, Class PP AVI, etc.

The HyP:

- Shall posses a Subscription record to operate in PP mode.
- Shall posses a RFPI to operate in FP mode.
- Shall posses information to perform Distributed communication.

  SK and UAK.

  Data base for PP-ADVI: CL TPUI, capabilities in regard to distributed communication, etc.

  Data base for PP-PDI: CL TPUI, capabilities in regard to distributed communication, etc.

  Its own CL TPUI.

NOTE: Subscription of all PPs to the HyP (see C.2) is not considered.

The PP-ADVI;

- Shall posses a Subscription record to the FP in order to operate in PP mode.
- Shall posses information to perform Distributed communication.

  SK and UAK.

  Data base for PP-PDI: CL TPUI, capabilities in regard to distributed communication, etc.

  Data base for HyP: CL TPUI, capabilities in regard to distributed communication, etc.

  Its own CL TPUI.

The PP-PDI:

- Shall posses a Subscription record to operate in PP mode.
- Shall posses information to perform distributed communication.

  SK and UAK.

  Its own CL TPUI.

In this configuration different possibilities are offered to the users of the PPs (HyP in PP mode).

The user of the HyP;

- could communicate with the FP on its or FP's request;
- could choose voluntary to communicate trough the FP with the PP-PDI or PP-ADVI;
- could choose voluntary to communicate directly to the PP-PDI or PP-ADVI;
- could involuntary (on advice from the FP) communicate directly to the PP-PDI or PP-ADVI.

The user of the PP-PDI;

- could communicate with the FP on FP's request;
- could communicate trough the FP with the PP-PDIHyP or PP-ADVI on their request;
- could involuntary (on advice form the FP) communicate directly to the HyP.

The user of the PP-ADVI;

- could communicate with the FP on its or FP's request;
- could communicate trough the FP with the PP-PDI or HyP on its or FP's request;
- could choose voluntary to communicate directly to the PP-PDI or HyP;
- could involuntary (on advice from the FP) communicate directly to the PP-PDI or HyP.

NOTE: If the HyP was of type CBDVI when in FP mode the PP-ADVI could communicate trough the HyP to the PP-PDI when the HyP and both PPs are advised from the FP to do so.

C.2 Ad Hoc

In this scenario it is assumed that a number of Users have come occasionally together and would like to perform an ad hoc communication session.

For this purpose at least one HyP (or a FP) is required to be available.

The HyP shall be switched in FP mode. All other terminals acting as PPs shall subscribe to the HyP when in FP mode. During the entire session the HyP shall stay in FP mode. All requirements as in the Basis scenario shall apply.

When more than one HyP is available the users may choose to operate as in the Basis scenario by agreeing one of the HyPs to operate as FP for the whole session and the rest to operate as PP and change dynamically on request.

Alternatively the Users may choose to have all HyPs being switched to FP mode for the most part of the session.

To do this the Users should perform the subscription registration operation (and direct PP-to-PP communication data allocation) as many times as HyPs are available - each time a particular HyP acting as FP and the rest of the HyPs acting as PPs. The non HyPs should be subscribed to only one of the HyPs. Following the completion of all procedures all HyPs should be switched to FP mode. The users of any of these HyPs may dynamically decide to go to PP mode and lock to a particular HyP by explicitly instructing their HyPs to do so.

In order to access the PPs (the non HyPs) every HyP shall:

- switch to PP mode;
- lock to the HyP in FP mode the PPs are subscribed to;
- request assistance in getting the particular PP locked.

NOTE: In this case, however, frequent manual user intervention will be required to communicate to any particular terminal and the role of the distributed communication is limited.

Annex D (normative): Specific requirements for RS323 service implementation

D.1 General

This annex describes specific requirements related to the implementation of DECT MMAP RS323 service implementation.

D.2 Reference configuration

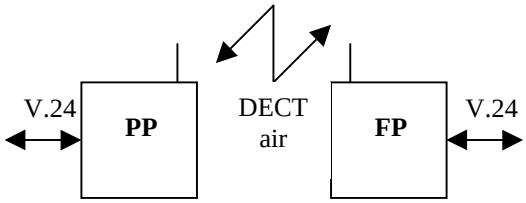


Figure D.1: Reference configuration showing the interworking to a V.24 interface

D.3 <<IWU-Attribute>> coding

Devices implementing the Interworking Units described in this annex shall use the following IWU-Attribute coding:

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< IWU-ATTRIBUTES >>							1
	Length of Contents (L)								2
	1	CodeStd		Profile					3
	1	Negotiation indicator		Profile subtype					4
	0	Stop bits		Data bits		Parity			5
	1	Data Rate							5a
	1	Maximum string length							6

Stop bits coding (octet 5):

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 5):

Bits 5 4 Meaning

0 0 6 bits

0 1 5 bits

1 0 7 bits

1 1 8 bits

Parity coding (octet 5):

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

1 1 1 BPAD operation

All other values reserved.

Data Rate (octet 5a):

Bits 7 6 5 4 3 2 1 Meaning

0 0 0 0 0 0 0 unspecified

0 0 0 0 1 x x (xx+1) * 50 bit/s. (50 - 200 bit/s.)

0 0 0 1 x x x (xxx+1) * 300 bit/s. (300 - 2400 bit/s.)

0 0 1 x x x x (xxxx+2) * 2400 bit/s. (4,8 - 40,8 kbit/s.)

0 1 x x x x x (xxxxx+1) * 8000 bit/s. (8 - 256 kbit/s.) (note 3)

1 0 x x x x x (xxxxx+6) * 9600 bit/s. (57,6 - 355,2 kbits/s.) (note 3)

1 1 0 x x x x (xxxx+11) * 24000 bit/s. (264 - 624 kbits/s.) (note 3)

1 1 1 0 0 0 0 75 bit/s.

1 1 1 0 0 0 1 110 bit/s.

1 1 1 0 0 1 0 134,5 bit/s.

1 1 1 0 0 1 1 75/1200 bit/s (note 2)

1 1 1 0 1 0 0 1200/75 bit/s (note 2)

All other values reserved.

NOTE 1: The first rate is the transmit rate in forward direction of the call. The second rate is the transmit rate in backward direction of the call.

NOTE 2: Some bitrates (24, 96, 144, 192, 240, 288, and 336 kbit/s.) can be coded in several different ways. These codings are all valid.

Examples:

Bits 7 6 5 4 3 2 1	Meaning	
0 0 0 0 1 0 0	50 bit/s	(V.6 and X.1)
0 0 0 0 1 0 1	100 bit/s	(V.6 and X.1)
0 0 0 0 1 1 0	150 bit/s	(V.6 and X.1)
0 0 0 0 1 1 1	200 bit/s	(V.6 and X.1)
0 0 0 1 0 0 0	300 bit/s	(V.6 and X.1)
0 0 0 1 0 0 1	600 bit/s	(V.6 and X.1)
0 0 0 1 0 1 1	1 200 bit/s	(V.6)
0 0 0 1 1 1 1	2 400 bit/s	(V.6 and X.1)
0 0 1 0 0 0 0	4 800 bit/s	(V.6 and X.1)
0 1 0 0 0 0 0	8 000 bit/s	(I.460)
0 0 1 0 0 1 0	9 600 bit/s	(V.6, X.1, GSM HSCSD)
0 0 1 0 0 1 1	12 000 bit/s	(V.6)
0 0 1 0 1 0 0	14 400 bit/s	(V.6, GSM HSCSD)
0 1 0 0 0 0 1	16 000 bit/s	(I.460)
0 0 1 0 1 1 0	19 200 bit/s	(V.6, GSM HSCSD)
0 0 1 1 0 0 0	24 000 bit/s	(1 C2-Bearer)
0 0 1 1 0 1 0	28 800 bit/s	(V.34, GSM HSCSD)
0 1 0 0 0 1 1	32 000 bit/s	(I.460, GSM HSCSD)
0 0 1 1 1 1 0	38 400 bit/s	(GSM HSCSD)
0 1 0 0 1 0 1	48 000 bit/s	(V.6, X.1, 2 C2-Bearers, GSM HSCSD)
0 1 0 0 1 1 0	56 000 bit/s	(V.6)
1 0 0 0 0 0 0	57 600 bit/s	(GSM HSCSD)
0 1 0 0 1 1 1	64 000 bit/s	(X.1, 1 ISDN B-Channel, GSM HSCSD)
1 0 0 0 0 0 1	67 200 bit/s	(GSM HSCSD)
1 0 0 0 0 1 0	76 800 bit/s	(GSM HSCSD)
0 1 0 1 0 0 0	72 000 bit/s	(3 C2-Bearers)
0 1 0 1 0 1 1	96 000 bit/s	(4 C2-Bearers, GSM HSCSD)
1 0 0 0 1 1 0	115 200 bit/s	(RS232 Data Rate)
0 1 0 1 1 1 0	120 000 bit/s	(5 C2-Bearers)
0 1 0 1 1 1 1	128 000 bit/s	(2 ISDN B-Channels)
1 0 0 1 0 0 1	144 000 bit/s	(6 C2-Bearers)
1 1 0 1 0 1 0	552 000 bit/s	(23 C2-Bearers)

Maximum string length (octet 6):

This 7 bit word represents the natural binary coding of the maximum string length used for data compression, with the least significant bit in position 1 (see ISO/IEC 8073 [12] annex A, parameter P2). It shall be coded with 0 when compression is not requested.

Table D.1: Values used within the IWU-ATTRIBUTES

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<IWU attributes>>			The values of Octet 3 and 4 mandated for support are indicated in subclause 8.22.
	<Stop bits>	All	
	<Data bits>	All	
	<Parity>	000, 010-101	
	<Data Rate>	All	
	<Maximum string length>	0000000	No data compression across the DECT-air-interface is to be used

Annex E (normative): Wireless LAN conventions

E.1 Reference configuration

This clause specifies the wireless LAN conventions applicable for a LAN implementation based on MMAP. The data encapsulation conventions are based on Ethernet LAN frames described in ISO 8802-3 [13].

The reference configuration for this interworking is shown in figure E.1.

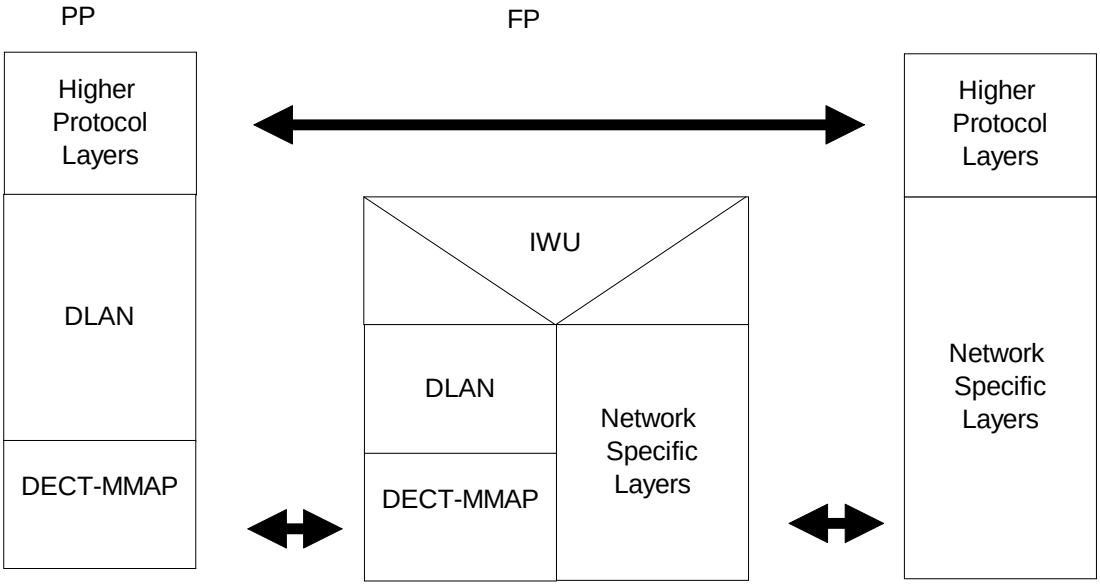


Figure E.1: Reference configuration for MMAP wireless LAN access

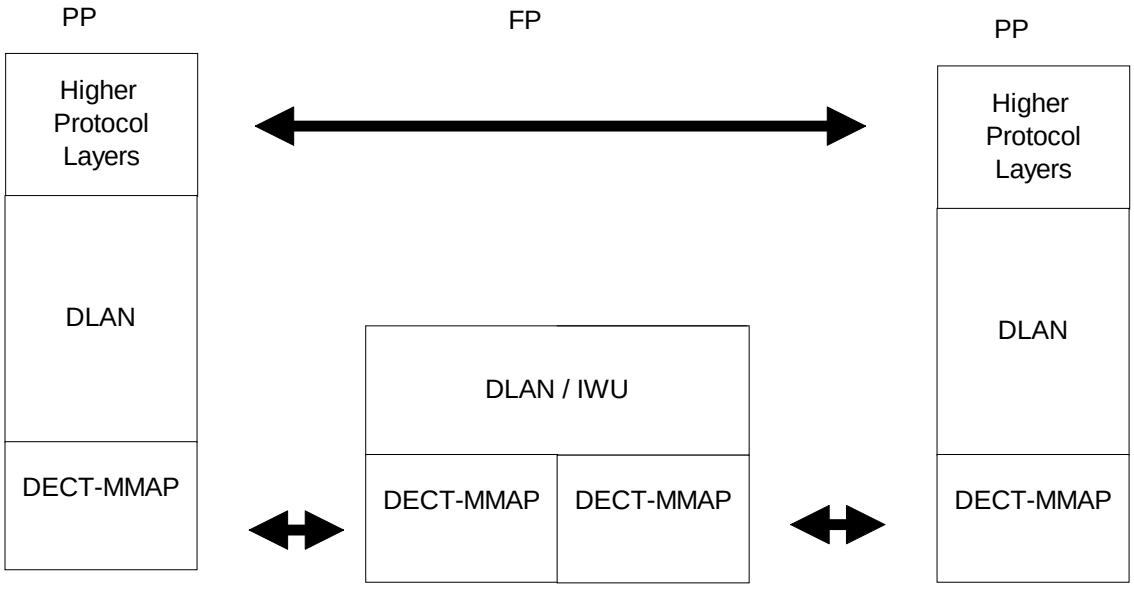


Figure E.2: The reference configuration for MMAP wireless LAN

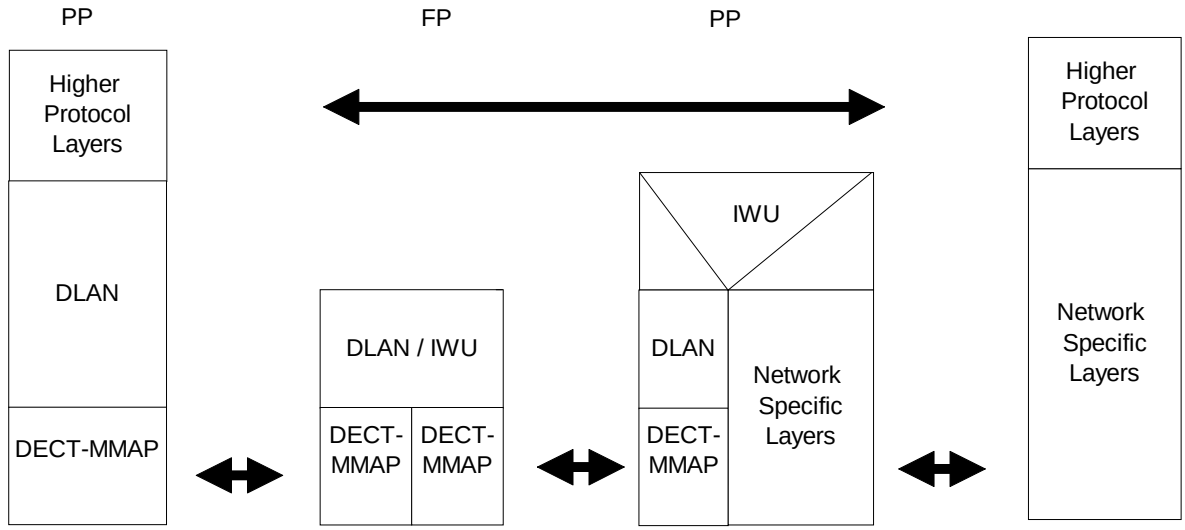
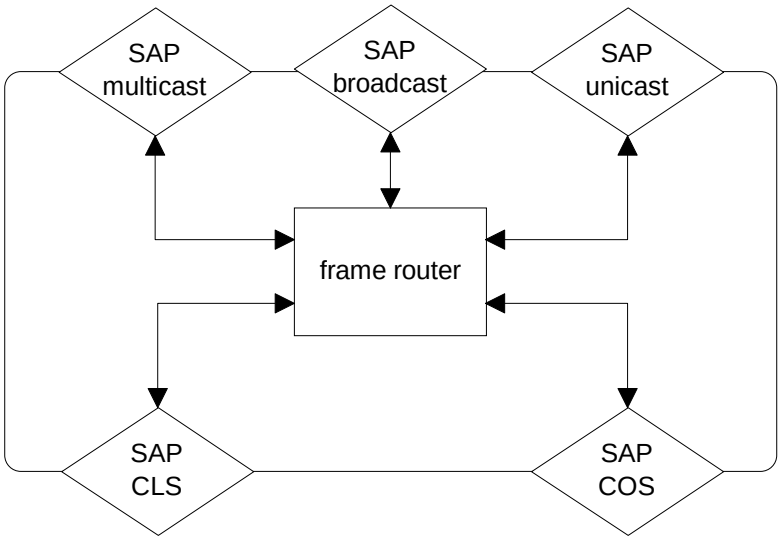


Figure E.3: Reference configuration for MMAP wireless LAN by PP network access

NOTE: DLAN includes a frame router and an interface like a wired ethernet card.

A typical configuration for this interworking is based upon the following principles interworking by an external network such as a gateway at the FP (figure E.1 interworking by a framerouter for internal networks (figure E.2) interworking by an external/internal network where a gateway is provided by a PP (figure E.3) This profile provides the data services (broadcast, multicast and unicast), as defined in ISO 8802-3 [13].

The higher layer protocol should be Internet Protocol, IPX/SPX, NDIS-driver, or other drivers of operation system. This Interface shall be specified by its standard or specification.



CLS ConnectionLess Service <=> MNCL-SAP
COS Connection Oriented Service <=> U-plane SAP

Figure E.4: DLAN block scheme

E.1.2 Ethernet and DECT-addresses

The Ethernet address of WLAN shall be used in a private network. Only a gateway on PP/FP, which is connected to wired ethernet network, such as router or bridge, needs an assigned Ethernet MAC address by the IEEE for the wired network adapter.

E.1.2.1 Ethernet Addresses Encoding

Network adapters are uniquely distinguished by their Ethernet address. The Ethernet address distinguishes a network adapter uniquely. For WLAN, a virtual Ethernet address(VEA) is formed by the following rules. The format of a Ethernet Address:

B1-B2-B3-B4-B5-B6

B1-B2-B3 ⇔ 00-00-02 BBN (was internal usage only, no longer used)

B4-B5-B6 ⇔ DP PP PP

D duplicate counter

P PP PP 20 bit Portable equipment Serial Number (PSN) of IPEI

All PP shall register at the FP. The FP verifies the uniqueness of each VEA. In case the VEA already exists, the D parameter is incremented until a uniqueness VEA exist.

If a MMAP PP/FP is used as a network adapter for a Ethernet LAN according to the IEEE organization, the adapter needs a global unique Ethernet MAC address including a manufacturer code distributed by the IEEE. These addresses have no relation with the identities used with DECT. It is up to a database functionality in the FP to build up a table of the relation between the DECT identity gained by the CC and the Ethernet MAC address gained from the source address in the ISO 8802-3 [13] frame.

E.1.2.2 Ethernet Broadcast Address

Broadcast is a point to multipoint service received by every station. To indicate an Ethernet Broadcast address, every bit of destination address of an Ethernet frame is set one, FF-FF-FF-FF-FF-FF. On a FP-side, this Ethernet frame shall be transmitted by connectionless services. On a PP-side the connection oriented service is used.

E.1.2.3 Ethernet Multicast Address

Multicast is a point to multipoint service where the different receivers have to subscribe to a multicast group. To indicate an Ethernet Multicast address the first byte should be odd, such as 01-xx-xx-yy-yy-yy. The 'xx ' shows the EVC and 'yy' is distributed by manufacturer. On a FP-side, this Ethernet frame shall be transmitted by connectionless service. On a PP-side the connection oriented service is used.

E.1.2.4 Ethernet Unicast Address

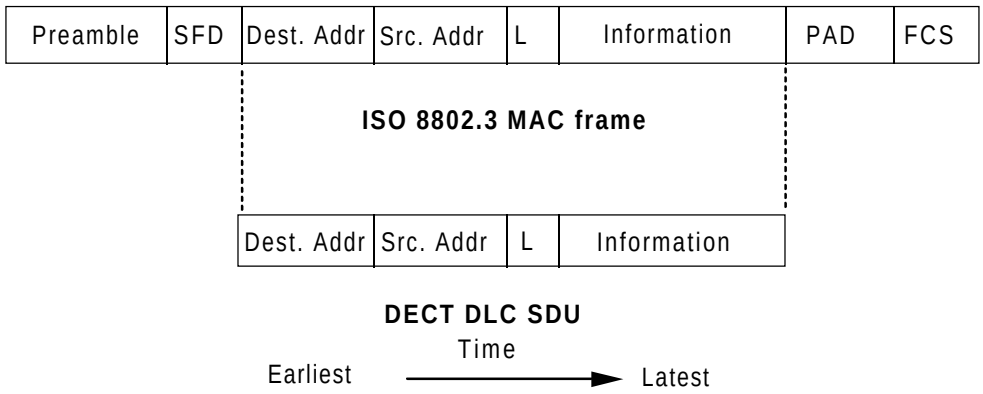
Unicast is a point to point service. To indicate an Ethernet Unicast, the destination Ethernet address is valid. This Ethernet frame shall be always transmitted by connection oriented service.

E.2 U-plane procedures

E.2.1A Encapsulation of Ethernet frames

- the ISO 8802-3 [13] MAC frame shall be transmitted as a single DECT DLC layer SDU beginning with the ISO 8802-3 [13] MAC Destination Address and ending with the MAC Information field;
- for MAC frames which are less than 64 octets in length, the PADding (PAD) field shall not be transmitted. This mapping is shown in figure E.6;

Figure E.5: Void



NOTE: The information (payload) can be compressed to increase bandwidth of the wireless LAN. Whether the information is compressed or not will be negotiated during call setup.

Figure E.6: Mapping of ISO 8802-3 [13] MAC frames into DECT DLC SDU

E.2.2 Mapping to different U-plane services

ISO 8802-3 [13] foresees different types of services: Broadcast, Multicast, Unicast. These services shall be mapped to the two different services offered by MMAP:

- connectionless downlink service; and
- connection oriented service.

Every control message shall always use connection oriented service.

E.2.2.1 PP U-plane service

For every transmission of each type of service (broadcast, multicast, unicast) the connection oriented service shall be used.

E.2.2.2 FP U-plane service

For transmission of multicast and broadcast, the connectionless service is used, whereas connection oriented service shall be used for unicast.

E.2.3 DECT specific Information elements

E.2.3.1 IWU-to-IWU IE

This IE shall be used by location registration procedure.

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
								…
								L+2

Figure E.7: IWU-TO-IWU information element

Send/Reject (S/R) bit:

Bits 7 Meaning

0 Rejection of message

1 Transmission of message

NOTE 1: This Send/Reject (S/R) bit is used to distinguish between the sending of a new message (e.g. sent in the direction A=>B) and the rejection of a received message (e.g. message received by B can be rejected by sending "reject" code in direction B=>A).

NOTE 2: The bit is always set to 1.

Protocol Discriminator (PD):

Bits 6 5 4 3 2 1 Meaning

0 0 0 0 0 0 User Specific (note 2)

0 1 0 0 1 0 MMAP WLAN

1 1 1 1 1 1 Unknown

NOTE 2: The IWU information is structured as shown below.

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

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

Figure E.8: Discriminator type

Discriminator type (octet 4):

Bits 7 6 5 4 3 2 1 Meaning

0 0 0 0 0 0 0 Unspecified

0 0 0 0 0 0 1 EMC

All other values reserved

User specific contents as defined in subclauses D.2.1.3.2 to D.2.1.3.5.

E.3 Connection oriented service procedures

E.3.1 Control information service

E.3.1.1 Procedure to register a VEA, a Ethernet MAC-address

To register a VEA or Ethernet MAC-address, the PP shall send a MM_LOCATE_REQUEST, as defined in ETS 300 175-5 [4], including the IWU-to-IWU IE. The procedure for location registration shall be done as defined in MMAP. If the location registration was successful, the VEA or Ethernet MAC-address shall be registered at DLAN. The MM_LOCATE_ACCEPT carries the DLAN response control message by containing in IWU-to-IWU IE.

If the response control message indicates 'duplication of VEA', the duplicate field shall be incremented and the procedure shall be restarted. After the duplicate field reaches 0xF, the procedure shall be stopped.

The PP stores the unique VEA to re-use it for the next WLAN session on this FP.

If location registration failed the register at DLAN fails, too.

E.3.1.2 Procedure to de-register a VEA, Ethernet MAC-address

The same procedure as defined in E.3.1.1. Every Ethernet MAC-address and VEA should be de-registered.

E.3.2 Link establishment

E.3.2.1 Initiated side of Link Establishment

If data of the Ethernet data services is available, DLAN shall issue a MMCC_SETUP.req primitive and change the state of DLAN to 'WLAN Link Requested'.

If DLAN receives a MMCC_REJECT.ind or a MMCC_RELEASE.ind primitive in the 'WLAN Link Requested' state, it shall flush the buffer, indicate to higher layer protocol that the connection is not available and shall return to 'WLAN No Link' .

If the DLAN receives an MNCC_CONNECT.ind primitive in the "WLAN Link Requested" state, it shall enter a "WLAN Link Active" state. Once in this state every data can be transmitted.

E.3.2.2 Initiated side of Link Release

For implementation-specific reasons the DLAN may choose to release the link at any time. In any case, the DLAN shall release the link if:

- the higher layer protocol indicates a failure;
- the peer shall be re-registered at the FP side.

To release the link, the DLAN shall issue a MNCC_RELEASE.req primitive, flush the buffer and indicate up to higher layer protocol and enter the 'WLAN No Link' state.

E.3.2.3 Initiated side of Link Suspend

The DLAN shall issue a MNCC_MODIFY.req primitive specifying a suspension and shall await a MNCC_MODIFY.cfm primitive. If this primitive notifies failure, it needs not take any action. If this primitive notifies success, it shall enter the "Link Suspended" state.

E.3.2.4 Initiated side of Link Resume

The IWF shall issue an MNCC_MODIFY.req primitive, specifying link resumption, and await a MNCC_MODIFY.cfm primitive. If this primitive notifies failure, it shall enter the "No Link" state and flush the buffer, indicate to higher layer protocol that the connection is not available. If the primitive notifies success, it shall enter the "Link Active" state and transmit the buffered data.

E.3.2.5 Destination side of Link Establishment

Upon receipt of a MNCC_SETUP.ind primitive, the DLAN shall determine that the service requested may be offered, and if so, it will issue a MNCC_CONNECT.ind primitive and enter the "Link Active" state. Once in this state, every provided data services are available and data shall pass by U-plane service. If the service cannot be supported, it will issue a MNCC_REJECT.req, indicating a release reason and will return to the "No Link" state.

E.3.2.6 Destination side of Link Release

If the DLAN receives a MNCC_RELEASE.ind primitive, it shall enter the "No Link" state, flush the buffer and indicate to higher layer protocol that the connection is released.

E.3.2.7 Destination side of Link Suspend

If the DLAN receives a MNCC_MODIFY.ind primitive, it shall wait until it has ceased to receive data from the U-plane then enter the "Link Suspended" state.

E.3.2.8 Destination side of Link Resume

If the DLAN receives a MNCC_MODIFY.ind primitive, it shall enter the "Link Active" state.

E.3.3 Data flow

The data flow control is handled as defined in MMAP. If a data flow stopped and the buffer are overloaded, incoming frames of higher layer protocol shall be discarded.

E.3.4 Data service

Ethernet frame shall only be transmitted if the DLAN has established the connection and has registered at the FP. Otherwise the Ethernet frame shall be buffered. If the buffer is overloaded, the incoming Ethernet frames shall be discarded.

E.4 Connectionless service procedures

E.4.1 General

The procedure shall be performed as defined in EN 300 175-5 [4], subclauses 12.3.2, 12.3.2.1 and 12.3.2.2. The following text together with the associated subclauses defines the mandatory requirements with regard to the present document.

Only the connectionless downlink service by using variable length message are mandatory.

E.4.2 Using of connectionless service

To Transmit the Ethernet Broadcast and Multicast services, the connectionless service of MMAP shall be used at the FP-side. All Ethernet Broadcast and Multicast services of PP-side, transmitting via COS shall be mapped to CLMS.

E.4.3 Coding

The contained message type is IWU-to-IWU infoelememt, as defined in MMAP, subclause E.2.3.1

Annex F (normative): Synchronization requirements for fixed parts

Public systems shall provide intersystem synchronization and shall have either Global Positioning System (GPS) synchronization and a Class 1 or Class 2 synchronization output port or a complete Class 1 or Class 2 synchronization port (input and output). This will allow absolute time synchronization via GPS or wired mutual synchronization if an operator requires local synchronization between fixed parts.

Annex G (informative): PP locking procedure for on-air subscription

This annex describes the locking procedure for PP on-air subscription:

1) invoke "subscription mode" manually;
2) listen and wait for the "FP capability" Qt message, read a44 "access rights supported" bit;
3) if bit a44 = 1 then try the subscription registration procedure;
4) if bit a44 = 0 then lock out and search for another FP;
5) leave subscription mode after finishing the subscription procedure. The PP may terminate this mode by means of e.g. a timer after some period of time;
6) the PP does not have to check if bit a44 goes off after having "seen" a44 on because the PP presumes the Q_t-info as static (see subclause 13.6).

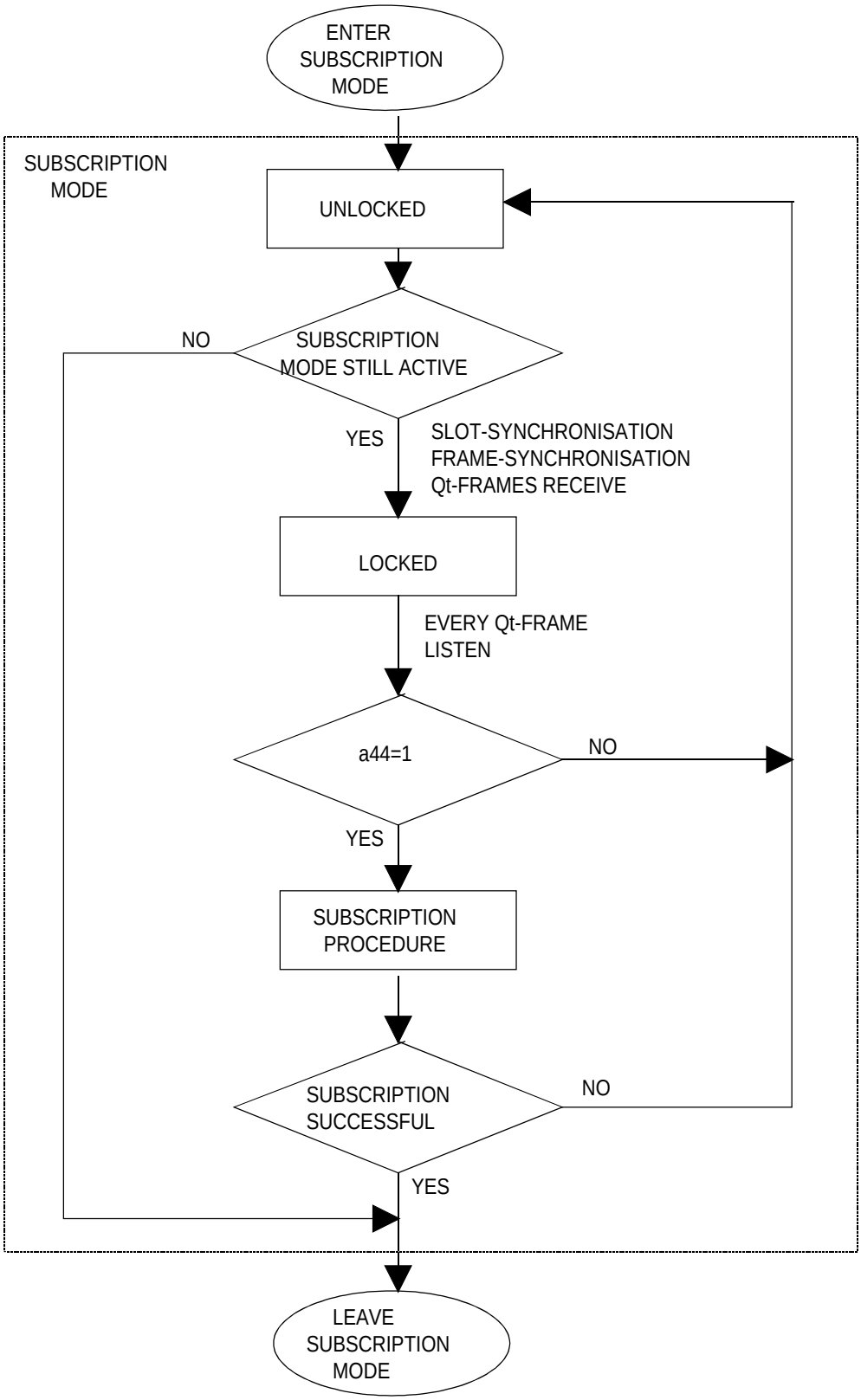


Figure G.1: PP "subscription mode" for MAC layer

Annex H (normative): Specific requirements for WLAN service implementation

H.1 General

This annex describes specific requirements related to the implementation of DECT MMAP WLAN service implementation.

H.2 Reference configuration

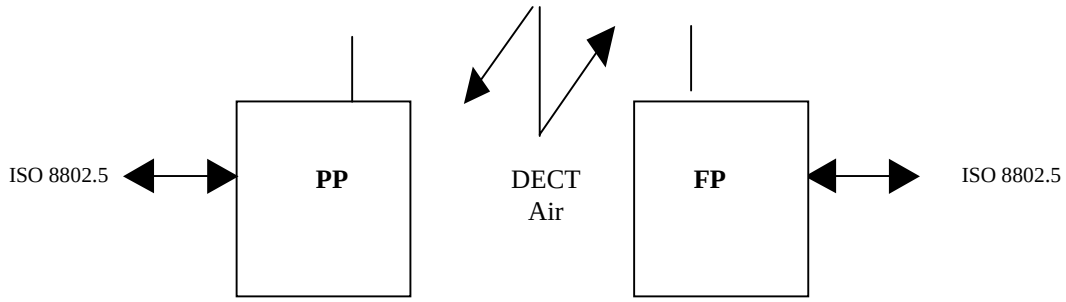


Figure H.1: Reference configuration showing the interworking to ISO 8802.5 (Ethernet)

H.3 <<IWU-Attribute>> coding

Devices implementing the Interworking Units described in this annex shall use the following IWU-Attribute coding:

NOTE: The values of Octet 3 and 4 mandated for support are indicated in subclause 8.22.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< IWU-ATTRIBUTES >>							1
	Length of Contents (L)								2
	1	CodeStd			Profile				3
	1	Negotiation indicator			Profile subtype				4
	0	Maximum SDU size (Most significant 7 bits)							5
	1	Maximum SDU size (Least significant 7 bits)							5a

Maximum SDU size (octets 5 and 5a):

This 14 bit word represents the natural binary coding of the maximum SDU length in units of eight octets used for data transmission, with the least significant bit in position 1 of octet 5a.

Table H.1: Values used within the IWU-ATTRIBUTES

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<IWU attributes>>			The values of Octet 3 and 4 mandated for support are indicated in subclause 8.22.
	<Maximum SDU size – MS 7 bits>	All	
	<Maximum SDU size – LS 7 bits	All	

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".
- ISO/IEC 9646-6: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 6: Protocol profile test specification".
- TBR 6: "Digital Enhanced Cordless Telecommunications (DECT); General terminal attachment requirements".
- TBR 10: "Digital Enhanced Cordless Telecommunications (DECT); General terminal attachment requirements; Telephony applications".
- ISO/IEC 2022 (1994): "Information Technology - Character code structure and extension techniques".
- ISO Publication 8859-1 (1987): "Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1".
- EN 300 435: "Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Base standard including interworking to connectionless networks (service types A and B, class 1)".
- EN 300 701: "Digital Enhanced Cordless Telecommunications (DECT); Data Services Profile (DSP); Generic frame relay service with mobility (service types A and B, class 2)".

History

Document history			
V0.5.1	March 1999	Public Enquiry	PE 9927: 1999-03-05 to 1999-07-02