ETSI EN 300 444 V2.5.1 (2017-10)

Digital Enhanced Cordless Telecommunications (DECT);
Generic Access Profile (GAP)

Reference
REN/DECT-00309

Keywords
access, DECT, generic, IMT-2000, mobility,
profile, radio, synchronization, TDD, TDMA

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

The present document is based on ETSI EN 300 175, parts 1 [1] to 8 [8]. General attachment requirements and speech attachment requirements are based on ETSI EN 301 406 [11] (replacing ETSI TBR 006 [i.1]) and ETSI EN 300 176-2 [10] (previously covered by ETSI TBR 010 [i.2]).

The present document has been developed in accordance to the rules of documenting a profile specification as described in ISO/IEC 9646-6 [i.4].

National transposition dates	
Date of adoption of this EN:	9 October 2017
Date of latest announcement of this EN (doa):	31 January 2018
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2018
Date of withdrawal of any conflicting National Standard (dow):	31 July 2019

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies that set of technical requirements for Digital Enhanced Cordless Telecommunications (DECT) Fixed Part (FP) and DECT Portable Part (PP) necessary for the support of the Generic Access Profile (GAP).

The GAP is applicable to all DECT Portable radio Terminations (PT) and Fixed radio Terminations (FT) which under the scope of ETSI EN 300 176-2 [10] (i.e. 3,1 kHz telephony teleservice) and specifies the minimum functionality that is supported by all other 3,1 kHz voice profiles.

The objective of the present document is to ensure the Air Interface (AI) inter-operability of DECT equipment capable of 3,1 kHz telephony applications, in such a way that any DECT PT conforming to the procedures described in the present document is inter-operable with any DECT FT conforming to the procedures described in the present document.

The profile consists of the minimum mandatory requirements that allow a 3,1 kHz teleservice connection to be established, maintained and released between a FT and a PT with the appropriate access rights, irrespective of whether the FP provides residential, business or public access services.

In addition, the present document defines the features, services, procedures etc. for both the FT and the PT, which are provision mandatory either in the PT or in the FT, as well as some elements that are provision optional but still process mandatory.

Mobility Management (MM) procedures at the DECT AI to support incoming calls and outgoing calls are included.

Inter-working between the FT and the attached network is outside the scope of the present document.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

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

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

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

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

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

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

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

[9] ETSI EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 1: Radio".

[10] ETSI EN 300 176-2: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 2: Audio and speech".

[11] ETSI EN 301 406: "Digital Enhanced Cordless Telecommunications (DECT); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU".

[12] ETSI EN 300 700: "Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)".

2.2 Informative references

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

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

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

[i.1] ETSI TBR 006: "Digital Enhanced Cordless Telecommunications (DECT); General terminal attachment requirements".

[i.2] ETSI TBR 010: "Digital Enhanced Cordless Telecommunications (DECT); General Terminal Attachment Requirements; Telephony Applications".

[i.3] ETSI TS 102 527-3: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 3: Extended wideband speech services".

[i.4] ISO/IEC 9646-6: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 6: Protocol profile test specification".

[i.5] ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[i.6] ISO/IEC 8073 (1997): "Information technology - Open Systems Interconnection - Protocol for providing the connection-mode transport service".

[i.7] Recommendation ITU-T G.726: "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

attach: process whereby a PP within the coverage area of a FP to which it has access rights, notifies this FP that it is operative

NOTE 1: The reverse process is detach, which reports the PP as inoperative.

NOTE 2: An operative PP is assumed to be ready to receive calls.

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

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

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

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

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

DECT network: network that uses the DECT 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: 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) (FP): physical grouping that contains all of the elements in the DECT network between the local network and the DECT AI

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

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

NOTE: 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: related to FP identities, PARIs and RFPIs, it indicates that two systems with the same PARI, or respectively two RFPs with the same RFPI, cannot be reached or listened to at the same geographical position

NOTE: For PARI and RFPI, see abbreviations clause.

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

NOTE: 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: identity is unique within DECT (without geographical or other restrictions)

handover: process of switching a call in progress from one physical channel to another physical channel

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

incoming call: call received at a PP

inter-cell handover: switching of a call in progress from one cell to another cell

internal general call: internal call setup by a PP to ring all other PPs (i.e. excluding the initiator) and FP (when capable of)

NOTE: This is typically useful in residential environments when transferring a call.

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: 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: capability of FPs and PPs, that enables 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)

inter-operator roaming: roaming between FP coverage areas of different operators (different service providers)

InterWorking Unit (IWU): unit that is used to interconnect sub networks

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

intra-cell handover: 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)

list access service: ability to store information on the DECT system in a set of lists on the FP and manage these lists from the PP (see ETSI TS 102 527-3 [i.3], feature [NG1.N.16])

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

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

Location Area (LA): domain in which a PP may receive (and/or make) calls as a result of a single location registration

location registration: 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: These databases are not included within a DECT FT.

MAC connection (connection): association between one source MAC Multiple Bearer Control (MBC) entity and one destination MAC MBC entity

NOTE: 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: call originating from a PP

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

NOTE: 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): physical grouping that contains all elements between the user and the DECT AI

NOTE 1: PP is a generic term that may describe one or several physical pieces.

NOTE 2: A DECT PP is logically divided into one PT plus one or more PAs.

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

NOTE: 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 (RFP): 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: ambiguous term that should always be qualified. See either location registration or subscription registration

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

RS: value used to establish authentication session keys

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

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

3.2 Symbols

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

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

Provision mandatory, process mandatory means that the indicated feature service or procedure is to 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 is to 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 [i.5].

3.3 Abbreviations

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

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
AES	Advanced Encryption Standard
AI	Air Interface
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity
ARQ	Automatic Repeat reQuest
BCD	Binary Coded Decimal
B_S	Slow Broadcast channel
CC	Call Control
CHO	Connection HandOver
CI	Common Interface
CISS	Call Independent Supplementary Service
CLIP	Calling Line Identification Presentation
CLMS	ConnectionLess Message Service
CN	Carrier Number
CNIP	Calling Name Identification Presentation
CRC	Cyclic Redundancy Check
CRFP	Cordless Radio Fixed Part
C_S	higher layer signalling Channel (slow)
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DLC	Data Link Control
DLEI	Data Link Endpoint Identifier

DSAA	DECT Standard Authentication Algorithm
DSAA2	DECT Standard Authentication Algorithm #2
DSC	DECT Standard Cipher (algorithm)
DSC2	DECT Standard Cipher (algorithm) #2
DTMF	Dual Tone Multi-Frequency
EMC	Equipment Manufacturer's Code
ESC	ESCape
FLEN	Frame LENgth
FMID	Fixed part MAC IDentity
FP	Fixed Part
FT	Fixed radio Termination
GAP	Generic Access Profile
GPS	Global Positioning System
HATS	Head And Torso Simulator
IE	Information Element
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication standardization sector
IUT	Implementation Under Test
IWU	InterWorking Unit
KS'	FP authentication Session Key
KS	PP authentication Session Key
KSG	Key Stream Generator
LA	Location Area
LAL	Location Area Level
LAPC	DLC layer C-plane protocol entity
LCE	Link Control Entity
LiA	List Access
LLME	Lower Layer Management Entity
LLN	Logical Link Number
LNW	Local NetWork
LSB	Least Significant Bit
LSIG	Link SIGnature
MAC	Medium Access Control
MAP	MAPping
MBC	Multiple Bearer Control
MCEI	MAC Connection Endpoint Identifier
ME	Management Entity
MM	Mobility Management
MMI	Man-Machine Interface
MSB	Most Significant Bit
M_T	MAC control channel on A-tail field, or one message on such channel
MUX	MUltipleXer
NLF	New Link Flag
NR	Normal-Reverse
N_T	identities information channel or one message in such channel
NTP	Normal Transmit Power
NWK	NetWorK
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
PSCN	Primary Scan Carrier Number
PSN	Portable equipment Serial Number
PSTN	Public Switched Telephone Network
PT	Portable radio Termination

PUN	Portable User Number
PUT	Portable User Type
Q_H	4 bit Header in the Q_T channel
Q_T	system information and multiframe marker (MAC logical channel)
R/B	Residential/Business (environment)
RAND	RANDom challenge issued by a FP
RES	RESponse calculated by a PP
RF	Radio Frequency
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RLRH	Receiving Loudness Rating of the Handset
RPN	Radio fixed Part Number
RR	Receive Ready
RS	a cryptographic parameter used in the calculation of authentication session keys
SAP	Service Access Point
SAPI	Service Access Point Identifier
SARI	Secondary Access Rights Identity
SC	Speech Coding
SDU	Service Data Unit
SN	Slot Number
SP	Start Position
SPR	Spare Bits
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
WRS	Wireless Relay Station
ZAP	ability first to assign and then to re-program the account data held in the PP

4 Feature definitions

4.0 General

For the purposes of the present document the feature definitions in the following clauses 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]: call initiated at a DECT PP.

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

on-hook (FULL Release) [N.3]: 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]: capability to dial digits 0 to 9, *, #.

register recall [N.5]: 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.

go to DTMF signalling (defined tone length) [N.6]: go to DTMF signalling with defined tone length.

pause (dialling pause) [N.7]: ability to generate or indicate a dialling pause, e.g. to await further dial tone.

incoming call [N.8]: call received at a DECT PP.

authentication of PP [N.9]: process by which the identity of a DECT PP is checked by the FP.

authentication of user [N.10]: 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.11]: 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.12]: capability to transform Authentication Code (AC) into User Authentication Key (UAK) using the key allocation procedure.

identification of PP [N.13]: ability for the FP to request and PP to provide specific identification parameters.

service class indication/assignment [N.14]: 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.15]: activates or deactivates alerting at the PP using any appropriate indication.

ZAP [N.16]: 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.17]: activation of the encryption process requested by FT.

subscription registration procedure on-air [N.18]: standardized procedure for loading subscription registration data into a PP in real time over the air-interface.

link control [N.19]: ability to request, accept, maintain and release a data link for the purposes of a NWK layer procedure.

terminate access rights FT initiated [N.20]: ability of the FP to delete a subscription in the PP.

partial release [N.21]: ability to release an established or in progress Call Control (CC) call whilst retaining the radio resource for the purpose of accessing further services.

go to DTMF (infinite tone length) [N.22]: go to DTMF signalling, indicating infinite DTMF tone duration.

go to pulse [N.23]: go to pulse (decadic) signalling.

signalling of display characters [N.24]: transmission to the PP of characters to be displayed on the user's PP display (if provided).

display control characters [N.25]: 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.26]: process by which the identity of a FP is checked by the PP.

encryption activation PT initiated [N.27]: 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.28]: 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.29]: 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.30]: ability to provide the calling party number to the called party before accepting the call.

internal call [N.31]: call between 2 users that does not make use of the local network resources. This is typically useful in residential environments.

service call [N.32]: 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.

Enhanced U- plane connection [N.33]: ability of the FT to initiate connection of the U- plane during call establishment or release e.g. to facilitate the provision of in band tones or announcements.

Calling Name Identification Presentation (CNIP) [N.34]: ability to provide the calling party name to the called party before accepting the call.

Enhanced Security [N.35]: mechanism to enhance DECT security by introduction of early encryption and the possibility of re-keying during an ongoing call.

AES/DSAA2 authentication [N.36]: authentication using the DECT Authentication Algorithm #2 (DSAA2), based on AES, and including type 2 (see ETSI EN 300 175-7 [7]) air i/f procedures.

4.2 Speech coding and audio features

For the purposes of the present document the following definitions shall apply:

G.726 32 kbit/s ADPCM [SC.1]: Recommendation ITU-T G.726 [i.7] narrow band codec as defined by ETSI EN 300 175-8 [8] clause 5.1.

PP audio type 1a ("classic GAP" handset) [SC.2]: audio specification for a general purpose 3,1 kHz telephony handset as defined by ETSI EN 300 175-8 [8], clause 7.2.3.

PP audio type 1b ("improved GAP" handset) [SC.3]: audio specification for a general purpose 3,1 kHz telephony handset with improved TCLw, as defined by ETSI EN 300 175-8 [8], clause 7.2.4. It is compatible with VoIP and long delay networks.

PP audio type 1c (HATS tested, 3,1 kHz handset) [SC.4]: audio specification for a general purpose 3,1 kHz telephony handset based on the new HATS methodology, as defined by ETSI EN 300 175-8 [8], clause 7.2.5. It includes strong echo suppression (TCLw) requirements and is compatible with VoIP and long delay networks.

PP audio type 1d (HATS tested, 3,1 kHz "improved" handset) [SC.5]: audio specification for a general purpose 3,1 kHz telephony handset based on the new HATS methodology with improved quality, as defined by ETSI EN 300 175-8 [8], clause 7.2.6. It includes strong echo suppression (TCLw) requirements and is compatible with VoIP and long delay networks. This type has a more demanding acoustic specification, providing superior subjective quality. In practice, this means better electro-acoustic components (speaker, microphone), electronics and signal processing.

PP audio type 3a (HATS tested, 3,1 kHz handsfree) [SC.6]: audio specification for a Narrowband (3,1 kHz) handsfree device as defined by ETSI EN 300 175-8 [8], clause 7.2.7. This type applies to handsfree devices operating with an open loudspeaker and microphone. The type applies to either:

1) specific PPs designed to operate in handsfree mode;

2) standard handset implementing types 1a, 1b, 1c or 1d, but with the option to operate in handsfree mode; and

3) handsfree accessory devices connected to a handset by any wired or wireless technology.

It provides (300 Hz to 3,4 kHz) frequency range, and it is defined based on HATS methodology.

PP audio type 3b (HATS tested, 3,1 kHz "improved" handsfree) [SC.7]: audio specification for a Narrowband (3,1 kHz) handsfree device, improved quality version, as defined by ETSI EN 300 175-8 [8], clause 7.2.8. This type applies to handsfree devices operating with an open loudspeaker and microphone. The type applies to either:

1) specific PPs designed to operate in handsfree mode;

2) standard handset implementing types 1a, 1b, 1c or 1d, but with the option to operate in handsfree mode; and

3) handsfree accessory devices connected to a handset by any wired or wireless technology.

It provides (300 Hz to 3,4 kHz) frequency range, and it is defined based on HATS methodology. This type has a more demanding acoustic specification, providing superior subjective quality. In practice, this means better electro-acoustic components (speaker, microphone), electronics and signal processing.

FP audio type 1a ("classic ISDN" 3,1 kHz) [SC.8]: audio specification for a DECT FP supporting narrowband service and providing a digital 64 kbit/s G.711 interface, typically (but not necessarily) an ISDN connection, classic specification, as defined by ETSI EN 300 175-8 [8], clause 7.3.2. It is recommended to use FP type 1b instead of type 1a.

FP audio type 1b ("new ISDN" 3,1 kHz) [SC.9]: audio specification for a DECT FP supporting narrowband service and providing a digital 64 kbit/s G.711 interface, typically (but not necessarily) an ISDN connection, new specification, as defined by ETSI EN 300 175-8 [8], clause 7.3.3. It is recommended to use FP type 1b instead of type 1a.

PP echo canceller for FP [SC.10]: auxiliary feature for FPs consisting on echo canceller for handling the echo generated by PPs type 1a. As defined by ETSI EN 300 175-8 [8], clause 7.4.2. Only narrowband echo cancellation capability is required.

PP echo suppressor for FP [SC.11]: auxiliary feature for FPs consisting on echo suppressor for handling the echo generated by PPs type 1a. As defined by ETSI EN 300 175-8 [8], clause 7.4.3. Only narrowband capability is required.

FP audio type 2 (analogue PSTN 3,1 kHz) [SC.12]: audio specification for a DECT FP supporting narrowband service and providing an analogue 2-wire PSTN interface. As defined by ETSI EN 300 175-8 [8], clause 7.3.4.

FP audio type 3 (VoIP 3,1 kHz) [SC.13]: audio specification for a DECT FP supporting narrowband service and providing a VoIP interface, with codecs G.711 (typically) or G.726 on top of it. As defined by ETSI EN 300 175-8 [8], clause 7.3.5.

FP audio type 6a (internal call) [SC.14]: this type of audio specification applies to the case of internal call inside a DECT FP or a DECT system without any external interface. This type applies to any service. As defined by ETSI EN 300 175-8 [8], clause 7.3.8.

FP audio type 6b (internal conference) [SC.15]: this type of audio specification applies to the case of 3-party or multi-party conference inside a DECT FP or a DECT system with or without an external interface. Applies to any service. As defined by ETSI EN 300 175-8 [8], clause 7.3.9.

Adaptive volume control for FP [SC.16]: accessory feature for FPs consisting on an adaptive volume control depending on the level of environmental noise at the PP. The gain variation shall be symmetrical. As described in ETSI EN 300 175-8 [8], (detailed descriptions for each type of FP in clause 7.6, and examples of settings in informative annex D).

4.3 Application features

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

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

manual entry of the Portable Access Rights Key (PARK) [A.3]: 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.

terminal identity number assignment in mono-cell system [A.4]: ability to assign to each PT a terminal identity number.

5 Service definitions

5.0 General

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]: 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.

C_S channel fragmentation and recombination [D.2]: 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 C_S logical channel) and recombination (by means of joining several service units received from the MAC layer C_S logical channel into a LAPC data unit).

broadcast Lb service [D.3]: 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.

LU1 TRansparent UnProtected service (TRUP) class 0/min_delay [D.7]: transparent unprotected service introducing minimum delay between the higher layers and the MAC layer. May be used for speech and non-speech applications. Speech transmission shall only use the class 0/min_delay operation over a single bearer MAC connection. Data integrity is not guaranteed. No error protection is applied, and octets may be lost, erroneous or duplicated. The continuous higher layer data is fragmented for delivery to the I_N logical channel in the transmission direction, and recombined from the I_N logical channel in the receiving direction.

FU1 [D.8]: offers a defined fixed length frame structure and buffering functions for transmission of U-plane data to the MAC layer (at the transmit side) or accept of data from the MAC layer (at the receiving side) on demand and with minimum delay. Used for speech but may be used for more general data purposes.

encryption deactivation [D.9]: transporting the NWK layer encryption deactivation request to the MAC layer, thereby disabling the encryption process in the MAC layer.

5.2 MAC service definitions

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

continuous broadcast [M.2]: 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.3]: 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.

basic connection [M.4]: service providing connection between FT and PT consisting of one full slot duplex bearer supporting the In_minimum_delay data service (i.e. speech). Only one basic connection may exist between a FT and particular PT (except during connection handover). The service includes the means for setting-up and releasing the required bearer(s).

C_S higher layer signalling [M.5]: low rate connection oriented data service with ARQ using the C_S channel to transfer higher layer signalling data.

quality control [M.6]: provides means for monitoring and controlling the radio link quality.

encryption activation [M.7]: 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.

extended frequency allocation [M.8]: service which allows a FT to support frequencies in addition to the standard DECT frequencies.

bearer handover - intra-cell [M.9]: 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.10]: 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.11]: 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.12]: 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.

Secondary Access Rights Identity (SARI) support [M.13]: ability to support, in addition to the primary Access Rights Identity (ARI), secondary ARIs that the FT broadcasts less frequently than PARIs. These may be used to reflect an inter-operators agreement allowing a portable to access more than one operator or services through FT.

encryption deactivation [M.14]: 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).

Re-keying [M.15]: mechanism to change the cipher key during an ongoing call.

Early encryption [M.16]: mechanism to activate encryption immediately after connection establishment.

AES/DSC2 encryption [M.17]: encryption using the DSC2 algorithm, based on AES, with Cipher Key of 128 bits.

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 clause 3.3 for the GAP FP and PP. All optional elements shall be process mandatory according to the procedures described in the present document.

Protocol elements defined as mandatory, optional or conditional in this clause are further defined in clauses 8 to 14 in detail, either explicitly and/or as references to the DECT base standard ETSI EN 300 175-2 [2] to ETSI EN 300 175-8 [8], ETSI EN 300 176-1 [9] and ETSI EN 300 176-2 [10].

NOTE: Annexes A and B are informative and may be used as additional information, but do not mandate requirements.

The requirements of ETSI EN 301 406 [11] and ETSI EN 300 176-2 [10] shall be met by all equipment conforming to the present document.

6.2 NWK features

Table 1: NWK features status

Feature supported					
			Status		
Item no.	Name of feature	Reference	PT	FT	
				R/B	P
N.1	Outgoing call	4.1	M	M	M
N.2	Off hook	4.1	M	M	M
N.3	On hook (full release)	4.1	M	M	M
N.4	Dialled digits (basic)	4.1	M	M	M
N.5	Register recall (see notes 4 and 5)	4.1	M	O	O
N.6	Go to DTMF signalling (defined tone length) (see note 1)	4.1	M	O	M
N.7	Pause (dialling pause) (see note 3)	4.1	M	O	O
N.8	Incoming call	4.1	M	M	M
N.9	Authentication of PP	4.1	M	C101	M
N.10	Authentication of user (see note 2)	4.1	M	O	O
N.11	Location registration	4.1	M	O	M
N.12	On air key allocation (see note 2)	4.1	M	C101	O
N.13	Identification of PP	4.1	M	O	O
N.14	Service class indication/assignment	4.1	M	O	M
N.15	Alerting	4.1	M	M	M
N.16	ZAP (see note 2)	4.1	M	O	O
N.17	Encryption activation FT initiated	4.1	M	C101	M
N.18	Subscription registration procedure on-air	4.1	M	M	M
N.19	Link control	4.1	M	M	M
N.20	Terminate access rights FT initiated (see note 2)	4.1	M	O	O
N.21	Partial release	4.1	O	O	O
N.22	Go to DTMF (infinite tone length)	4.1	O	O	O
N.23	Go to Pulse	4.1	O	O	O
N.24	Signalling of display characters	4.1	O	O	O
N.25	Display control characters	4.1	O	O	O
N.26	Authentication of FT	4.1	O	O	O
N.27	Encryption activation PT initiated	4.1	O	O	O
N.28	Encryption deactivation FT initiated	4.1	O	O	O
N.29	Encryption deactivation PT initiated	4.1	O	O	O
N.30	Calling Line Identification Presentation (CLIP)	4.1	O	O	O
N.31	Internal call	4.1	O	O	O
N.32	Service call	4.1	O	O	O
N.33	Enhanced U- plane connection	4.1	O	O	O
N.34	Calling Name Identification Presentation (CNIP)	4.1	O	O	O
N.35	Enhanced security	4.1	O	O	O
N.36	AES/DSAA2 authentication	4.1	C102	C102	C102
NOTE 1: The PT is only required to be able to send the <<MULTI-KEYPAD>> information element containing the DECT standard 8-bit character (ETSI EN 300 175-5 [5], annex D) codings "Go to DTMF", defined tone length and the FT is required to be able to understand it in the public environment. NOTE 2: This feature is required to be supported in the PT to guarantee the same level of security among all the handsets that operates in a system. The invocation of the feature is however optional to the operator. NOTE 3: The PT is required to be able to send the <<MULTI-KEYPAD>> information element containing the DECT standard 8-bit character (ETSI EN 300 175-5 [5], annex D) codings "Dialling Pause". This guarantees automatic access to secondary or alternative networks. NOTE 4: This feature uses keypad code 15 hex. NOTE 5: The FT is not mandated to receive and understand the register recall DECT character. However, if a FT supports it there may be no corresponding action that the FT can take with the local network as a result of this function.					
C101: IF feature N.35 THEN M ELSE O. C102: IF MAC service M.17 THEN M ELSE O.					

6.3 DLC services

Table 2: DLC services status

Service supported					
			Status		
Item no.	Name of service	Reference	PT	FT	
				R/B	P
D.1	LAPC class A service and Lc	5.1	M	M	M
D.2	C_S channel fragmentation and recombination	5.1	M	M	M
D.3	Broadcast Lb service	5.1	M	M	M
D.4	Intra-cell voluntary connection handover	5.1	M	C201	C201
D.5	Intercell voluntary connection handover (see note)	5.1	M	O	O
D.6	Encryption activation	5.1	M	C203	M
D.7	LU1 TRUP Class 0/min_delay	5.1	M	M	M
D.8	FU1	5.1	M	M	M
D.9	Encryption deactivation	5.1	C202	C202	C202
NOTE:	The PT is required to be able to support handover between RFPs. The invocation of the feature is however optional to the operator.				
C201:	IF service M.9 THEN O ELSE M.				
C202:	IF feature N.29 OR N.28 THEN M ELSE I.				
C203:	IF feature N.17 OR N.27 THEN M ELSE I.				

6.4 MAC services

Table 3: MAC services status

Service supported					
			Status		
Item no.	Name of service	Reference	PT	FT	
				R/B	P
M.1	General	5.2	M	M	M
M.2	Continuous broadcast	5.2	M	M	M
M.3	Paging broadcast	5.2	M	M	M
M.4	Basic connections	5.2	M	M	M
M.5	C_S higher layer signalling	5.2	M	M	M
M.6	Quality control	5.2	M	M	M
M.7	Encryption activation	5.2	M	C304	M
M.8	Extended frequency allocation (see note 1)	5.2	M	O	O
M.9	Bearer Handover, intra-cell	5.2	M	C301	C301
M.10	Bearer Handover, inter-cell	5.2	M	O	O
M.11	Connection Handover, intra-cell	5.2	M	C302	C302
M.12	Connection Handover, inter-cell	5.2	M	O	O
M.13	SARI support	5.2	M	O	O
M.14	Encryption deactivation	5.2	C303	C303	C303
M.15	Re-keying	5.2	C305	C305	C305
M.16	Early encryption	5.2	C306	C306	C306
M.17	AES/DSC2 encryption (see note 2)	5.2	O	O	O
NOTE 1:	Handsets not supporting these extra frequencies need only adapt scanning to allow continued use of the standard DECT frequencies.				
NOTE 2:	IF implemented THEN NWK feature N.36 shall be implemented.				
C301:	IF service M.11 THEN O ELSE M.				
C302:	IF service M.9 THEN O ELSE M.				
C303:	IF feature N.29 OR N.28 THEN M ELSE I.				
C304:	IF feature N.17 OR N.27 THEN M ELSE I.				
C305:	IF feature N.35 and NWK layer procedure "Re-keying during a call" are implemented THEN M ELSE O.				
C306:	IF feature N.35 and NWK layer procedure "Early encryption" are implemented THEN M ELSE O.				

6.5 PHysical Layer (PHL) services

See PHL requirements, clause 11.

6.6 Application features

Table 4: Application features status

Feature supported					
			Status		
Item no.	Name of feature	Reference	PT	FT	
				R/B	P
A.1	AC_bitstring_mapping	4.3	M	C401	M
A.2	Multiple subscription registration	4.3	M	N/A	N/A
A.3	Manual entry of the PARK	4.3	O	N/A	N/A
A.4	Terminal identity number assignment in mono-cell system	4.3	O	O	N/A
C401: IF feature N.9 OR N.10 OR N.12 OR N.26 THEN M ELSE N/A.					

6.7 Speech coding and audio features

DECT Generic Access Profile (GAP) shall support the following Speech coding and audio related features.

Table 4a: Speech Coding and audio features

Feature/Service supported					
			Status		
Item no.	Name of service	Reference	PT	FT	
				R/B	P
SC.1	G.726 32 kbit/s ADPCM codec	4.2	M	M	M
SC.2	PP Audio type 1a (classic GAP handset)	4.2	C404	N/A	N/A
SC.3	PP Audio type 1b (improved GAP handset)	4.2	C404	N/A	N/A
SC.4	PP Audio type 1c (HATS 3,1 kHz handset)	4.2	C404	N/A	N/A
SC.5	PP Audio type 1d (HATS 3,1 kHz improved handset)	4.2	C404	N/A	N/A
SC.6	PP Audio type 3a (HATS 3,1 kHz handsfree)	4.2	O	N/A	N/A
SC.7	PP Audio type 3b (HATS 3,1 kHz improved handsfree)	4.2	O	N/A	N/A
SC.8	FP Audio type 1a (classic ISDN 3,1 kHz)	4.2	N/A	C405	C405
SC.9	FP Audio type 1b (new ISDN 3,1 kHz)	4.2	N/A	C405	C405
SC.10	PP echo cancellation feature for FP type 1b or 3	4.2	N/A	C406	C406
SC.11	PP echo suppressor feature for FP type 1b or 3	4.2	N/A	C406	C406
SC.12	FP Audio type 2 (analogue PSTN 3,1 kHz)	4.2	N/A	C405	C405
SC.13	FP Audio type 3 (VoIP 3,1 kHz)	4.2	N/A	C405	C405
SC.14	FP Audio type 6a (internal call)	4.2	N/A	C407	C407
SC.15	FP Audio type 6b (internal conference)	4.2	N/A	O	O
C404: At least one should be provided. Type 1a may introduce echo issues in combination with VoIP or long delay networks. Types 1b, 1c or 1d are recommended for this scenario. C405: At least one should be provided. FP type 1b (SC.9) is recommended instead of type 1a (SC.8). C406: IF feature SC.9 (FP type 1b) OR SC.13 (FP type 3) THEN O ELSE I. Either SC.10 or SC.11 may be provided, but not both at the same time. C407: IF feature N.31 THEN M ELSE I.					

NOTE 1: Testing specification for audio features, including handsfree, is provided in ETSI EN 300 176-2 [10].

NOTE 2: PP types 1c and 1d are based on HATS methodology. This methodology provides objective test results more consistent with subjective tests compared to artificial ear methodology.

6.8 Feature/service to procedure mapping

6.8.1 NWK feature to procedure mapping

Table 5: NWK feature to procedure mapping

Feature/Procedure mapping					
			Status		
Feature	Procedure	Reference	PT	FT	
				R/B	P
N.1 Outgoing call		4.1	M	M	M
	Outgoing call request	8.2	M	M	M
	Overlap sending	8.3	M	O	O
	Outgoing call proceeding	8.4	M	O	O
	Outgoing call confirmation	8.5	M	O	O
	Outgoing call connection	8.6	M	M	M
	Sending keypad information	8.10	M	M	M
N.2 Off Hook		4.1	M	M	M
	Outgoing call request	8.2	M	M	M
	Incoming call connection	8.15	M	M	M
N.3 On Hook (full release)		4.1	M	M	M
	Normal call release	8.7	M	M	M
	Abnormal call release	8.8	M	M	M
N.4 Dialled digits (basic)		4.1	M	M	M
	Sending keypad information	8.10	M	M	M
N.5 Register recall		4.1	M	O	O
	Sending keypad information	8.10	M	M	M
N.6 Go to DTMF signalling (defined tone length)		4.1	M	O	M
	Sending keypad information	8.10	M	M	M
N.7 Pause (dialling pause)		4.1	M	O	O
	Sending keypad information	8.10	M	M	M
N.8 Incoming call		4.1	M	M	M
	Incoming call request	8.12	M	M	M
	Incoming call confirmation	8.13	M	M	M
	PT alerting	8.14	M	M	M
	Incoming call connection	8.15	M	M	M
N.9 Authentication of the PP		4.1	M	C501	M
	Authentication of PP using DSAA	8.24	M	M	M
	Authentication of PP using DSAA2	8.45.7	C502	C502	C502
N10 Authentication of the user		4.1	M	O	O
	Authentication of user using DSAA	8.25	M	M	M
	Authentication of user using DSAA2	8.45.8	C502	C502	C502
N.11 Location registration		4.1	M	O	M
	Location registration	8.28	M	M	M
	Location update	8.29	M	O	O
	Terminal Capability indication	8.17	O	O	O
N.12 On air key allocation		4.1	M	C501	O
	Key allocation using DSAA	8.32	M	M	M
	Key allocation using DSAA2	8.45.9	C502	C502	C502
N.13 Identification of PP		4.1	M	O	O
	Identification of PT	8.22	M	M	M
N.14 Service class indication/assignment		4.1	M	O	M
	Obtaining access rights	8.30	M	M	M
	Terminal Capability indication	8.17	O	O	O
	Authentication of PP using DSAA	8.24	M	M	M
	Authentication of PP using DSAA2	8.45.7	C502	C502	C502
N.15 Alerting		4.1	M	M	M
	PT alerting	8.14	M	M	M

Feature/Procedure mapping					
			Status		
Feature	Procedure	Reference	PT	FT	
				R/B	P
N.16 ZAP		4.1	M	O	O
	Obtaining access rights	8.30	M	M	M
	Terminal Capability indication	8.17	O	O	O
	Incrementing the ZAP value	8.26	M	M	M
	Authentication of FT using DSAA	8.23	O	M	M
	Authentication of FT using DSAA2	8.45.6	C503	C502	C502
N.17 Encryption activation FT initiated		4.1	M	C501	M
	Cipher-switching initiated by FT using DSC	8.33	M	M	M
	Cipher-switching initiated by FT using DSC2	8.45.10	C504	C504	C504
	Storing the Derived Cipher Key (DCK)	8.27	M	M	M
N.18 Subscription registration user procedure on-air		4.1	M	M	M
	Obtaining access rights	8.30	M	M	M
	Terminal Capability indication	8.17	O	O	O
N.19 Link control		4.1	M	M	M
	Indirect FT initiated link establishment	8.35	M	M	M
	Direct PT initiated link establishment	8.36	M	M	M
	Link release "normal"	8.37	M	M	M
	Link release "abnormal"	8.38	M	M	M
	Link release "maintain"	8.39	M	M	M
N.20 Terminate access rights FT initiated		4.1	M	O	O
	FT terminating access rights	8.31	M	M	M
	Authentication of FT using DSAA	8.23	O	M	M
	Authentication of FT using DSAA2	8.45.6	C503	C502	C502
N.21 Partial release		4.1	O	O	O
	Partial release	8.9	M	M	M
N.22 Go to DTMF (infinite tone length)		4.1	O	O	O
	Sending keypad information	8.10	M	M	M
N.23 Go to Pulse		4.1	O	O	O
	Sending keypad information	8.10	M	M	M
N.24 Signalling of display characters		4.1	O	O	O
	Display	8.16	M	M	M
	Terminal capability indication	8.17	M	M	M
N.25 Display control characters		4.1	O	O	O
	Display	8.16	M	M	M
	Terminal capability indication	8.17	M	M	M
N.26 Authentication of FT		4.1	O	O	O
	Authentication of FT using DSAA	8.23	M	M	M
	Authentication of FT using DSAA2	8.45.6	C502	C502	C502
N.27 Encryption activation PT initiated		4.1	O	O	O
	Cipher-switching initiated by PT using DSC	8.34	M	M	M
	Cipher-switching initiated by PT using DSC2	8.45.11	C504	C504	C504
	Storing the DCK	8.27	M	M	M
N.28 Encryption deactivation FT initiated		4.1	O	O	O
	Cipher-switching initiated by FT using DSC	8.33	M	M	M
	Cipher-switching initiated by FT using DSC2	8.45.10	C504	C504	C504
N.29 Encryption deactivation PT initiated		4.1	O	O	O
	Cipher-switching initiated by PT using DSC	8.34	M	M	M
	Cipher-switching initiated by PT using DSC2	8.45.11	C504	C504	C504
N.30 Calling Line Identification Presentation (CLIP)		4.1	O	O	O
	Incoming call request	8.12	M	M	M
	Calling Line Identification Presentation	8.41	M	M	M

Feature/Procedure mapping					
			Status		
Feature	**Procedure**	**Reference**	**PT**	**FT**	
				R/B	**P**
N.31 Internal call		4.1	O	O	O
	Internal call setup	8.18	M	M	M
	Internal call keypad	8.19	M	O	O
	Internal call CLIP	8.43	O	O	O
	Internal call CNIP	8.44	O	O	O
N.32 Service call		4.1	O	O	O
	Service call setup	8.20	M	M	M
	Service call keypad	8.21	M	O	O
N.33 Enhanced U- plane connection		4.1	O	O	O
	Enhanced FT initiated U- plane connection	8.40	M	M	M
N.34 Calling Name Identification Presentation (CNIP)		4.1	O	O	O
	Calling Name Identification Presentation (CNIP) Indication	8.42	M	M	M
N.35 Enhanced security		4.1	O	O	O
	Encryption of all calls	8.45.1	M	M	M
	Re-keying during a call	8.45.2	O	O	O
	Early encryption	8.45.3	O	O	O
	Subscription requirements	8.45.4	M	M	M
	Behaviour against legacy devices	8.45.5	M	M	M
N.36 AES/DSAA2 authentication		4.1	C505	C505	C505
	Authentication of FT using DSAA2 (see note)	8.45.6	O	O	O
	Authentication of PP using DSAA2	8.45.7	M	M	M
	Authentication of user using DSAA2	8.45.8	M	M	M
	Key allocation using DSAA2	8.45.9	M	M	M
	Cipher-switching initiated by FT using DSC2	8.45.10	C506	C506	C506
	Cipher-switching initiated by PT using DSC2	8.45.11	C507	C507	C507

NOTE: The status of this procedure refers to its use as an standalone procedure. Note that the FT authentication is part of the Key Allocation procedure and, in this case, the status is M.

C501: IF feature N.35 THEN M ELSE O.
C502: IF feature N.36 THEN M ELSE I.
C503: IF feature N.36 THEN O ELSE I.
C504: IF feature N.36 and MAC service M.17 THEN M ELSE I.
C505: IF MAC service M.17 THEN M ELSE O.
C506: IF MAC service M.17 THEN M ELSE I.
C507: IF (feature N.27 or feature N.29) and MAC service M.17 THEN M ELSE I.

6.8.2 DLC service to procedure mapping

Table 6: DLC service to procedure mapping

Service/Procedure mapping					
			Status		
Service	**Procedure**	**Reference**	**PT**	**FT**	
				R/B	**P**
D.1 LAPC class A service and Lc		5.1	M	M	M
	Class A link establishment	9.1	M	M	M
	Class A acknowledged information transfer	9.2	M	M	M
	Class A link release	9.3	M	M	M
	Class A link re-establishment	9.4	M	M	M
D.2 C_S channel fragmentation and recombination		5.1	M	M	M
	C_S channel fragmentation and recombination	9.5	M	M	M
D.3 Broadcast Lb service		5.1	M	M	M
	Normal broadcast	9.6	M	M	M
D.4 Intra-cell voluntary connection handover		5.1	M	C601	C601
	Class A basic connection handover	9.7	M	M	M
D.5 Inter-cell voluntary connection handover		5.1	M	O	O
	Class A basic connection handover	9.7	M	M	M
D.6 Encryption activation		5.1	M	C603	M
	Encryption switching	9.8	M	M	M
D.7 LU1 TRUP Class 0/min_delay		5.1	M	M	M
	U-plane Class 0/min delay	9.9	M	M	M
D.8 FU1		5.1	M	M	M
	FU1 frame operation	9.10	M	M	M
D.9 Encryption deactivation		5.1	C602	C602	C602
	Encryption switching	9.8	M	M	M
C601: IF service M.9 THEN O ELSE M. C602: IF feature N.29 OR N.28 THEN M ELSE I. C603: IF feature N.17 OR N.27 THEN M ELSE I.					

6.8.3 MAC service to procedure mapping

Table 7: MAC service to procedure mapping

Service/Procedure mapping					
			Status		
Service	**Procedure**	**Reference**	**PT**	**FT**	
				R/B	**P**
M.1 General		5.2	M	M	M
	General	10.1	M	M	M
M.2 Continuous broadcast		5.2	M	M	M
	Downlink broadcast	10.2	M	M	M
	Higher Layer capability FP broadcast	13.6	M	M	M
M.3 Paging broadcast		5.2	M	M	M
	Paging broadcast	10.3	M	M	M
M.4 Basic connections		5.2	M	M	M
	Setup of basic connection, basic bearer setup (A-field)	10.4	M	M	M
	Connection/bearer release	10.5	M	M	M
M.5 C_S higher layer signalling		5.2	M	M	M
	C_S channel data	10.8	M	M	M
	Q2 bit setting	10.9	M	M	M
M.6 Quality control		5.2	M	M	M
	RFPI handshake	10.10	M	M	M
	Antenna diversity	10.11	M	O	O
	Sliding collision detection	10.12	O	M	M
M.7 Encryption activation		5.2	M	C704	M
	Encryption process - initialization and synchronization	10.13	M	M	M
	Encryption mode control	10.14	M	M	M
	Handover encryption process	10.15	M	M	M
M.8 Extended frequency allocation		5.2	M	O	O
	Extended frequency allocation	10.16	M	M	M
M.9 Bearer handover, intra-cell		5.2	M	C701	C701
	Bearer handover request	10.6	M	M	M
M.10 Bearer handover, inter-cell		5.2	M	O	O
	Bearer handover request	10.6	M	M	M
M.11 Connection handover, intra-cell		5.2	M	C702	C702
	Connection handover request	10.7	M	M	M
M.12 Connection handover, inter-cell		5.2	M	O	O
	Connection handover request	10.7	M	M	M
M.13 SARI support		5.2	M	O	O
	Downlink broadcast	10.2	M	M	M
	Higher Layer capability FP broadcast	13.6	M	M	M
M.14 Encryption deactivation		5.2	C703	C703	C703
	Encryption mode control	10.14	M	M	M
M.15 Re-keying		5.2	C705	C705	C705
	Re-keying	10.17	M	M	M
M.16 Early encryption		5.2	C706	C706	C706
	Early encryption	10.18	M	M	M
M.17 AES/DSC2 encryption (see note)		5.2	O	O	O
	AES/DSC2 encryption	10.19	M	M	M
	Additional procedures for devices supporting DSC2	8.45.12	M	M	M
NOTE: IF implemented THEN NWK feature N.36 shall be implemented.					
C701: IF service M.11 THEN O ELSE M. C702: IF service M.9 THEN O ELSE M. C703: IF feature N.29 OR N.28 THEN M ELSE I. C704: IF feature N.17 OR N.27 THEN M ELSE I. C705: IF feature N.35 and NWK layer procedure "Re-keying during a call" are implemented THEN M ELSE O. C706: IF feature N.35 and NWK layer procedure "Early encryption" are implemented THEN M ELSE O.					

6.8.4 Application feature to procedure mapping

Table 8: Application feature to procedure mapping

Feature/Procedure mapping					
			Status		
Feature	**Procedure**	**Reference**	**PT**	**FT**	
				R/B	**P**
A.1 AC to bitstring mapping		4.3	M	C801	M
	AC to bitstring mapping	14.2	M	M	M
A.2 Multiple subscription registration		4.3	M	N/A	N/A
	Subscription control	14.1	M	N/A	N/A
A.3 Manual entry of the PARK		4.3	O	N/A	N/A
	Manual entry of the PARK	14.3	M	N/A	N/A
A.4 Terminal identity number assignment in mono cell system		4.3	O	O	N/A
	Terminal identity number assignment	14.4	O	O	N/A
C801: IF feature N.9 OR N.10 OR N.12 OR N.26 THEN M ELSE N/A.					

6.8.5 Speech coding and audio feature to procedure mapping

Features listed in clause 6.7 of the present document shall be implemented as described in ETSI EN 300 175-8 [8], following the provisions stated for each feature in clause 4.2.

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, (see clause 9.2.3).

6.9.4 Handling of error and exception conditions

If a 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 unexpected CC message, except {CC-RELEASE} or {CC-RELEASE-COM}, or an unrecognized message is received in any CC state, the message shall be ignored.

When a message other than {CC-SETUP}, {CC-RELEASE} or {CC-RELEASE-COM} is received which has one or more mandatory information elements missing or with invalid content, the normal release procedure as described in clause 8.7 shall be invoked.

ETSI EN 300 175-5 [5], clause 17.6.4 shall also apply to mandatory information elements in MM messages with a length exceeding the allowed maximum value.

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.

In all other cases the rules and order of precedence specified in ETSI EN 300 175-5 [5], clause 17, shall be obeyed.

6.9.5 GAP default setup attributes

The <<IWU-ATTRIBUTES>> and <<CALL-ATTRIBUTES>> information elements are not required to be understood by a "GAP" equipment. The values, as stated in ETSI EN 300 175-5 [5], annex E shall be considered as default. The value "1" of the field <Network layer attributes> in <<CALL-ATTRIBUTES>> shall be interpreted as indicating "Generic Access Profile" (GAP).

6.9.6 Coexistence of MM and CC procedures

Table 9 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 9: 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

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.

6.9.7 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.

7 Procedure description

The following clauses define the process mandatory procedures which are in the scope of the GAP. 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 clause 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 clause 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

8.0 General

This clause specifies the NWK layer procedures, messages and information elements required in the GAP.

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 ETSI EN 300 175-5 [5], clause 17.

8.1 Summary of outgoing call messages, normal cases

Figures 1 to 4 show a summary of possible sequences of outgoing call related messages.

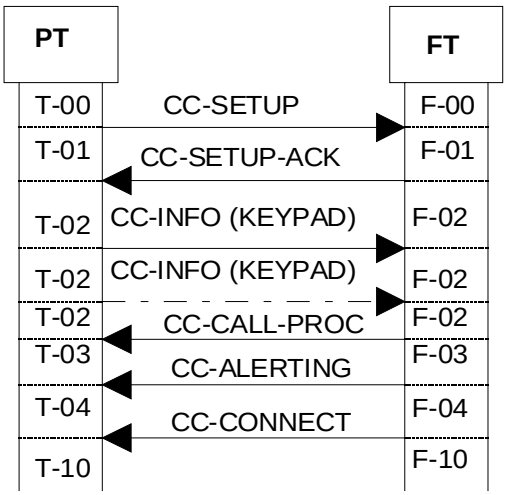


Figure 1

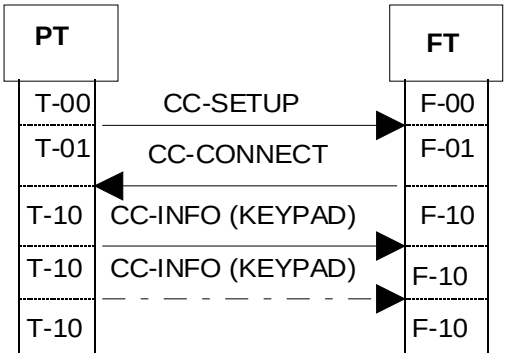


Figure 2

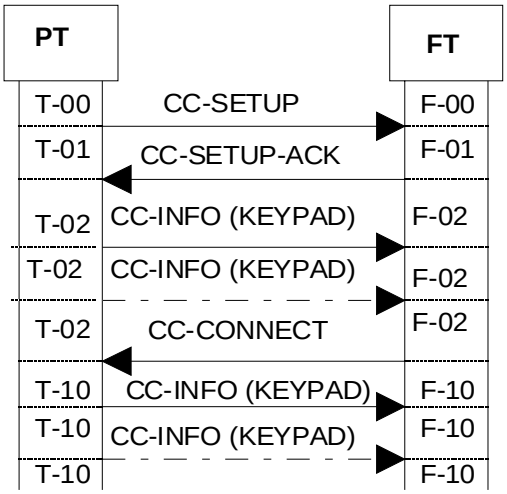


Figure 3

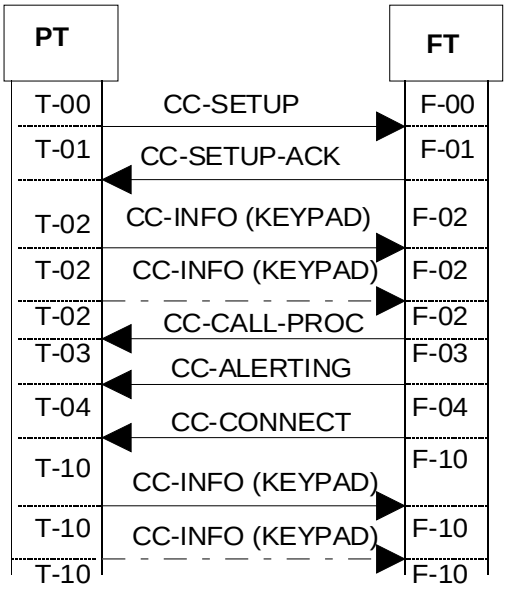


Figure 4

8.2 Outgoing call request

8.2.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.3.1, 9.3.1.1 and 9.3.1.2. Figure 5 and table 10 together with the associated clauses define the mandatory requirements with regard to the present document.

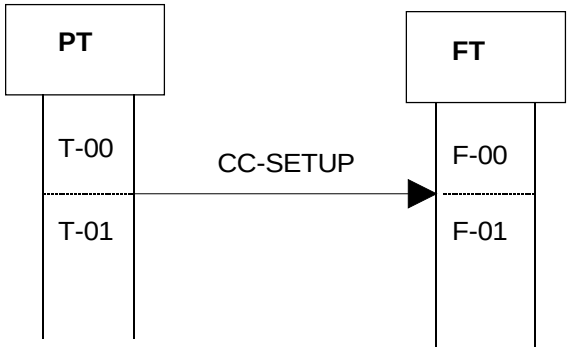


Figure 5: Outgoing call request

Table 10: 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 setup
		9	Optional, relates to feature internal call [N.31]. For the associated procedure (see clause 8.18)
		11	Optional, relates to feature service call [N.32]. For the associated procedure (see clause 8.20)
	<Basic service>	0	

8.2.1 Associated procedures

8.2.1.1 Timer P-<CC.03> management

<CC.03>: CC setup timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {CC-SETUP} message has been sent;

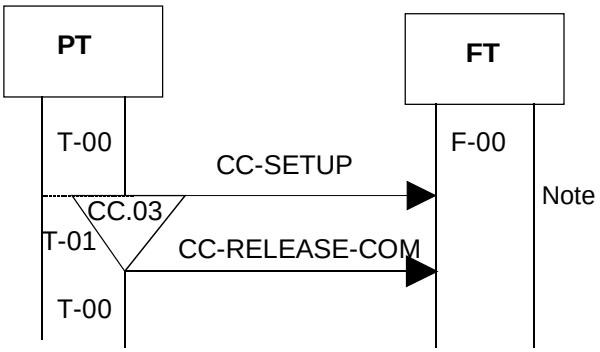
stop: an indication for release or reject from the IWU or for link release from the DLC layer is received. A {CC-SETUP-ACK}, {CC-CONNECT} or {CC-RELEASE-COM} message is received;

restart: FT may restart it at any time by sending a {CC-NOTIFY} message (see clause 6.9.6).

8.2.2 Exceptional cases

8.2.2.1 Timer P-<CC.03> expiry

The abnormal call release procedure shall be used (see clause 8.8).



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 6: Timer P<CC.03> expiry

For the values used within the {CC-SETUP} see table 10. For the contents of {CC-RELEASE-COM} message, see table 17.

8.2.2.2 PT releases the outgoing call request

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

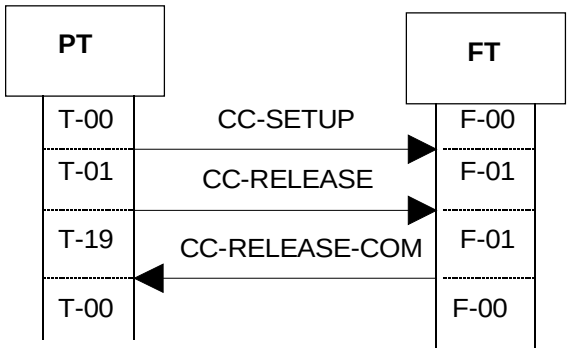
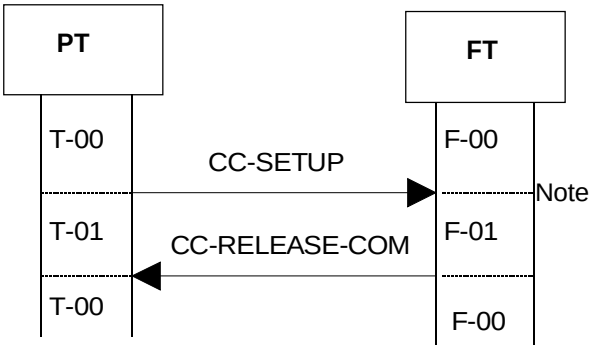


Figure 7: PT releases the outgoing call request

For the values used within {CC-SETUP} see table 10. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.2.2.3 FT rejects the outgoing call request

The abnormal call release procedure shall be used (see clause 8.8).



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

Figure 8: FT rejects the outgoing call request

For the contents of {CC-RELEASE-COM} see table 17.

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

8.3 Overlap sending

8.3.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.3.1.5 and 9.3.1.4. The following text together with the associated clauses 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.

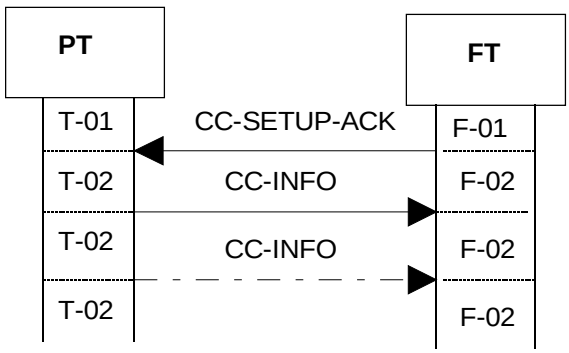


Figure 9: Overlap sending

Table 11: 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

For the values used in {CC-INFO} see table 20.

8.3.1 Associated procedure

8.3.1.1 Timer F-<CC.01> management

<CC.01>: overlap sending timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {CC-SETUP-ACK} has been sent;

stop: as soon as FT leaves "Overlap Sending" state;

restart: a {CC-INFO} message has been received.

8.3.2 Exceptional cases

8.3.2.1 PT releases the outgoing call request

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

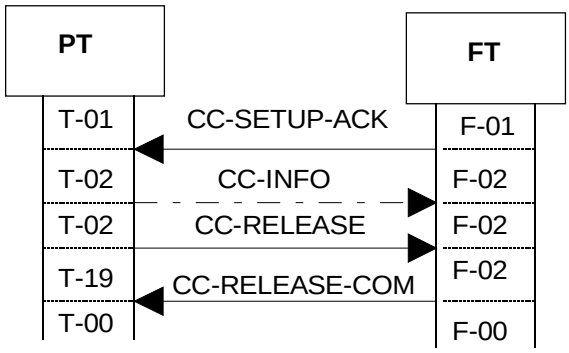
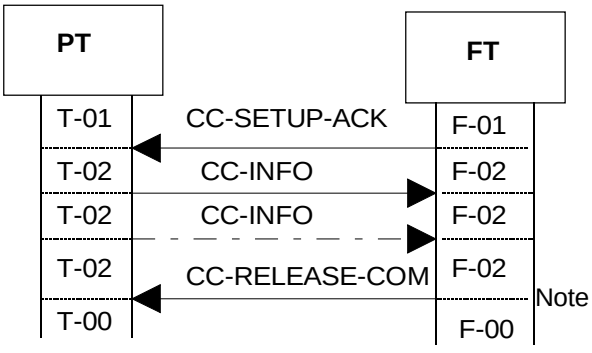


Figure 10: PT release the outgoing call request

For the values used within the {CC-SETUP-ACK} see table 11. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.3.2.2 FT rejects the outgoing call request

The abnormal release procedure shall be used (see clause 8.8).



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

Figure 11: FT rejects the outgoing call request

For the contents of {CC-SETUP-ACK} see table 11.

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

For the contents of {CC-RELEASE-COM} see table 17.

8.3.2.3 Timer F-<CC.01> expiry

The normal release procedure shall be used (see clause 8.7).

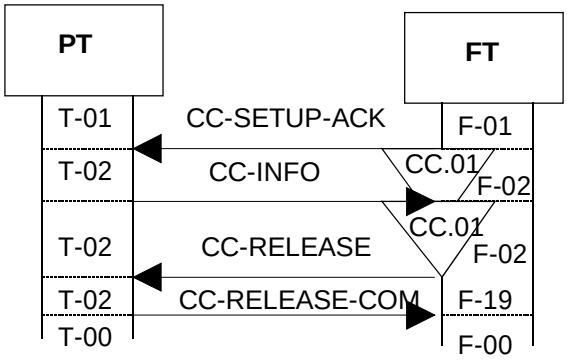


Figure 12: Timer F<CC.01> expiry

For the values used within the {CC-SETUP-ACK} see table 11. For {CC-INFO} (if any has been sent) see table 20. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.3.2.4 FT releases the outgoing call request

The normal release procedure shall be used (see clause 8.7).

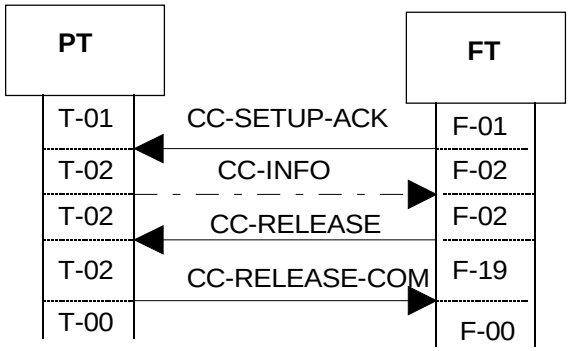


Figure 13: FT releases the outgoing call request

For the values used within the {CC-SETUP-ACK} see table 11. For {CC-INFO} (if any has been sent) see table 20. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.4 Outgoing call proceeding

8.4.0 Procedure

The procedure shall be performed as defined in clauses 9.3.1.6 and 9.3.1.4 of ETSI EN 300 175-5 [5]. Figure 14 and table 12 together with the associated clauses define the mandatory requirements with regard to the present document.

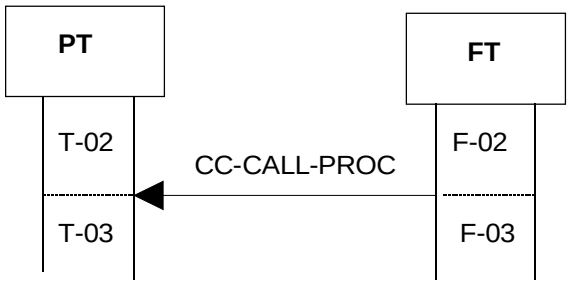


Figure 14: Outgoing call proceeding

Table 12: 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

8.4.1 Exceptional cases

8.4.1.1 PT releases the outgoing call request

The normal release procedure shall be used (see clause 8.7).

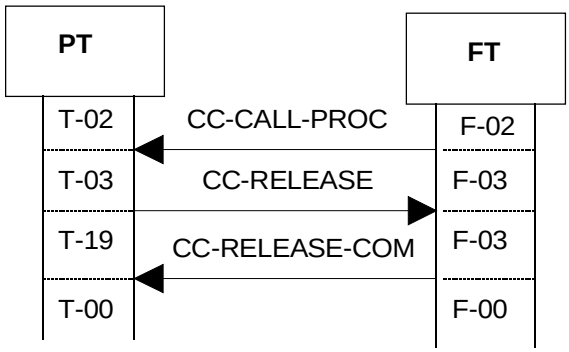


Figure 15: PT releases the outgoing call request

For the values used within the {CC-CALL-PROC} see clause 8.4, table 12. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see clause 8.7, tables 15 and 16.

8.4.1.2 FT releases the outgoing call request

The normal release procedure shall be used (see clause 8.7).

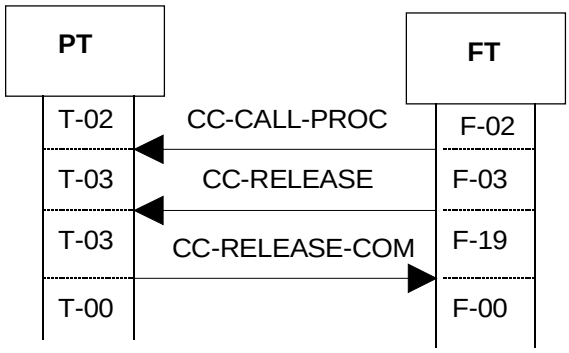


Figure 16: FT releases the outgoing call request

For the values used within the {CC-CALL-PROC} see clause 8.4, table 12. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see clause 8.7, tables 15 and 16.

8.5 Outgoing call confirmation

8.5.0 Procedure

The procedure shall be performed as defined in clauses 9.3.1.7 and 9.3.1.4 of ETSI EN 300 175-5 [5]. Figure 17 and table 13 together with the associated clauses define the mandatory requirements with regard to the present document.

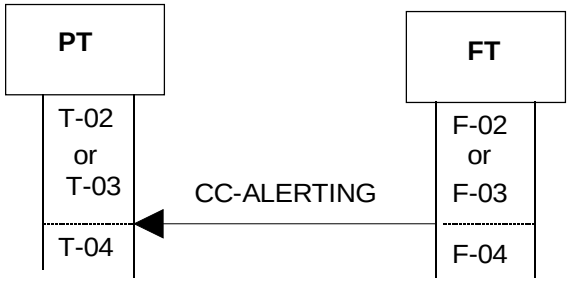


Figure 17: Outgoing call confirmation

Table 13: 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

8.5.1 Exceptional cases

8.5.1.1 PT releases the outgoing call request

The normal release procedure shall be used (see clause 8.7).

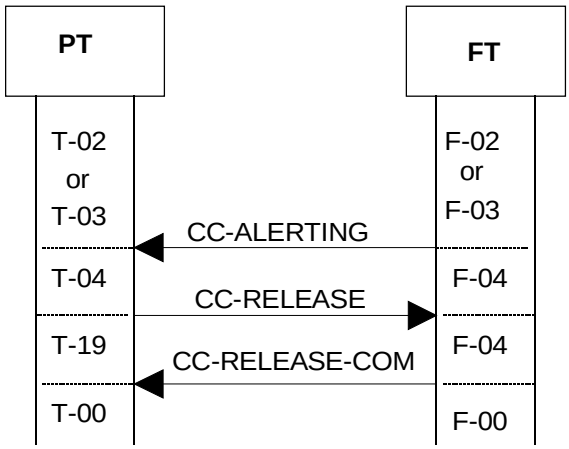


Figure 18: PT releases the outgoing call request

For the values used within the {CC-ALERTING} see table 13. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.5.1.2 FT releases the outgoing call request

The normal release procedure shall be used (see clause 8.7).

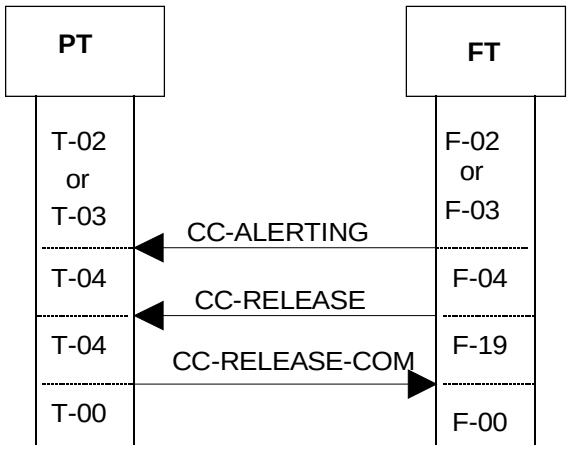


Figure 19: FT releases the outgoing call request

For the values used within the {CC-ALERTING} see table 13. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.6 Outgoing call connection

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.3.1.8 and 9.3.1.4. The following text together with the associated clauses 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.

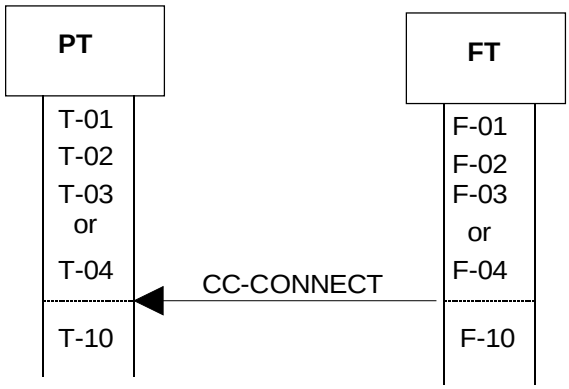


Figure 20: Outgoing call connection

Table 14: 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

8.7 Normal call release

8.7.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.5.1 and 9.5.3. Figures 21 and 22, and table 15 together with the associated clauses define the mandatory requirements with regard to the present document.

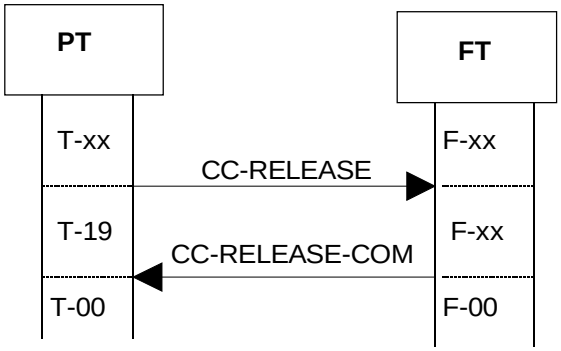


Figure 21: Normal call release, PT initiated

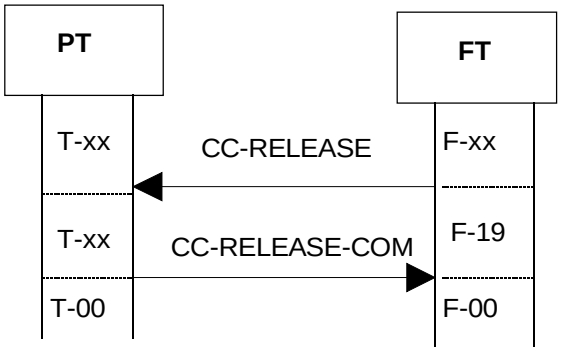


Figure 22: Normal call release, FT initiated

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 15: 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 16: 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

8.7.1 Associated procedures

8.7.1.1 Timer P-<CC.02> management

<CC.02>: CC release timer;

value: refer to ETSI EN 300 175-5 [5], 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 clause 6.9.6).

8.7.1.2 Timer F-<CC.02> management

<CC.02>: CC release timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.7.2 Exceptional cases

8.7.2.1 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.

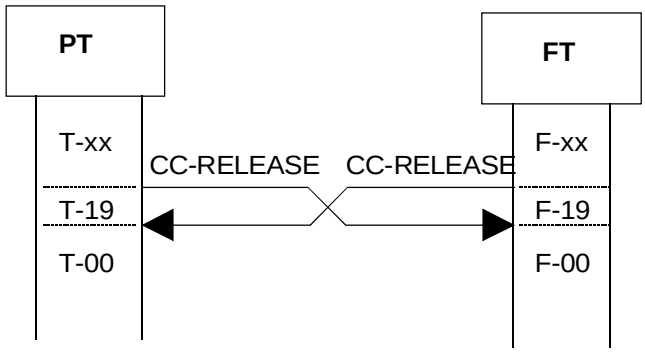


Figure 23: Both sides send {CC-RELEASE}

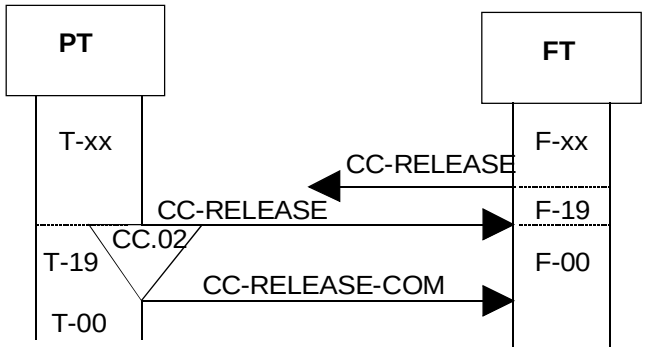
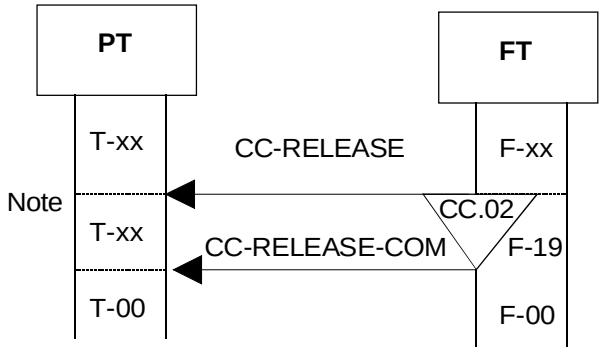


Figure 24: The {CC-RELEASE} sent by the FT has been lost

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} see tables 15 and 16.

8.7.2.2 Timer F-<CC.02> expiry

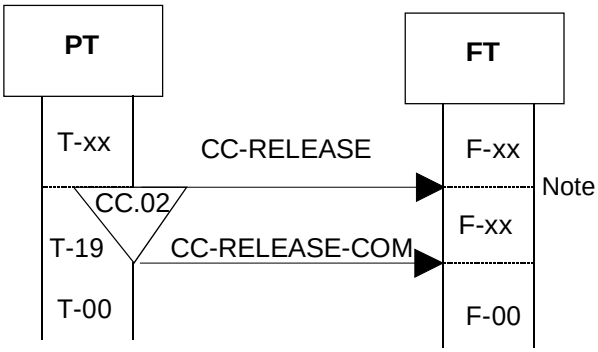


NOTE: PT may not be answering because of some PT problems or the {CC-RELEASE} sent by the FT or the eventual {CC-RELEASE-COM} message sent by the PT has been lost or corrupted.

Figure 25: Timer F<CC.02> expiry

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.7.2.3 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 26: Timer P<CC.02> expiry

For the values used within the {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.8 Abnormal call release

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 9.5.2. The following text together with the associated clauses 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.

In state T19 {CC-RELEASE-COM} may also be sent without expiry of <CC.02>.

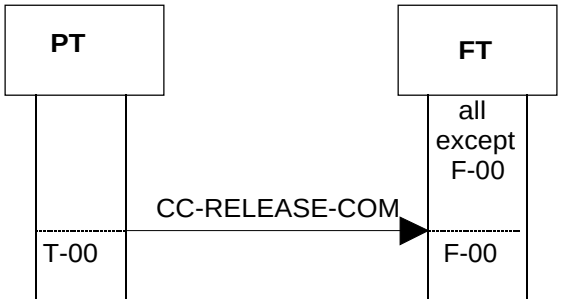


Figure 27: Abnormal call release, PT initiated

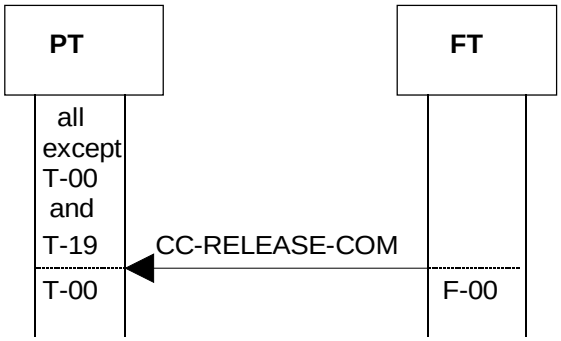


Figure 28: Abnormal call release, FT initiated

Table 17: 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>	All optional	All optional

In the case that the FT did not recognize the PT by its <<Portable identity>> IE, it is recommended that the FT includes the <<Release reason>> IE in its {CC-RELEASE-COM} message with the Release Reason code "Unknown identity" (value '0A'H).

8.9 Partial release

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 14.2.7. The following text together with the associated clauses 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 clause 8.39.

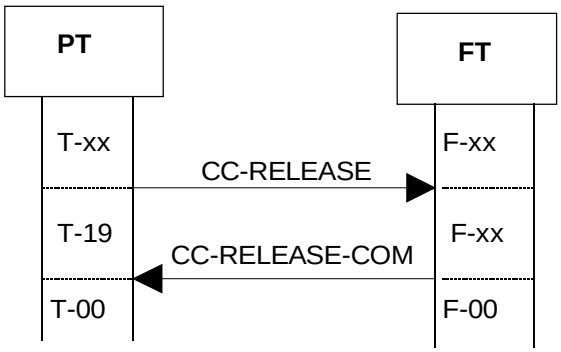


Figure 29: Partial release, PT initiated

Table 18: 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 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
<<Release reason>>	<Release reason code>	0EH	Always shall be included if the "partial release" has been requested, (see table 18), and if the requested side supports feature N.21

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

8.10 Sending keypad information

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.3.1.5, 9.4. and 10.2. The following text together with the associated clauses 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.

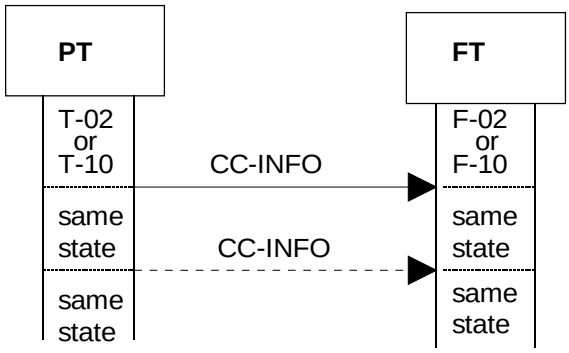


Figure 30: Sending keypad information

Table 20: 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.7]
		12H	Go to pulse. The support of this code is mandatory only if feature [N.23] is implemented
		14H	Relate to feature go to DTMF signalling (defined tone length) [N.6]
		15H	Relate to feature register recall [N.5]
		16H	Go to DTMF signalling (infinite tone length). The support of this code is mandatory only if feature [N.22] is implemented
		17H	Relates to feature internal call [N.31]. For the related procedure (see clause 8.19)
		18H	Relates to feature service call [N.32]. For the related procedure (see clause 8.21)
		23H, 2AH, 30H - 39H	#, *, 0 - 9. Relate to feature dialled digits (basic) [N.4] and outgoing call [N.1]

When en-bloc sending is used, a <<MULTI-KEYPAD>> information element shall be sent. The <<CALLED-PARTY-NUMBER>> information element shall not be used.

8.11 Summary of incoming call related messages, normal cases

Figures 31 and 32 show a summary of possible sequences of incoming call related messages.

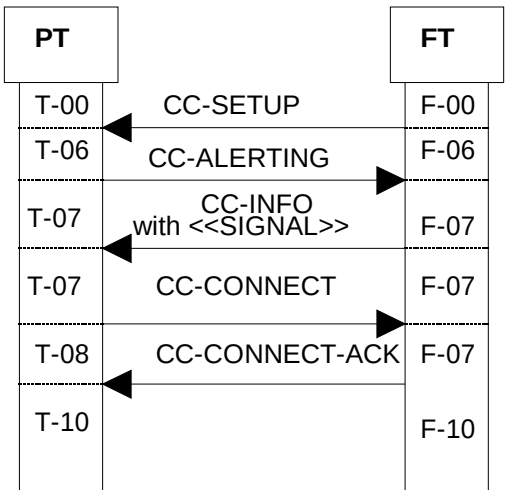


Figure 31

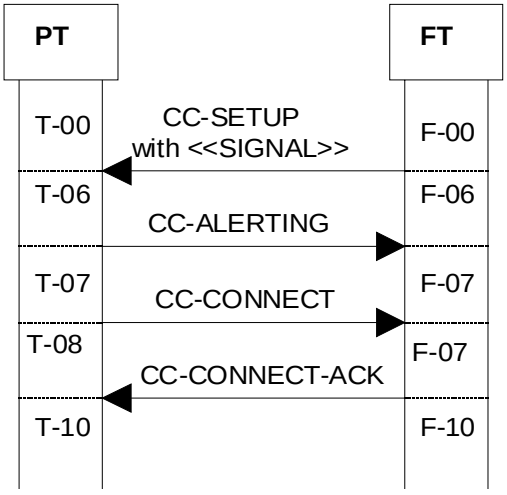


Figure 32

8.12 Incoming call request

8.12.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 9.3.2, 9.3.2.1 and 9.3.2.2. Figure 33 and table 21 together with the associated clauses define the mandatory requirements with regard to the present document.

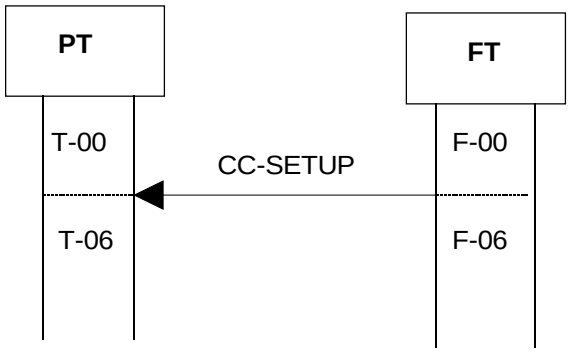


Figure 33: Incoming call request

Table 21: 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>	0	
<<Signal>>			Relates to procedure PT alerting (see clause 8.14)
	<Signal value>	40H - 47H, 48H, 4FH	
<<Calling party number>>			The support of this information element is only mandatory if feature [N.30] is implemented
	<Number type>	All	
	<Numbering plan id>	All	
	<Presentation indicator>	All	
	<Screening indicator>	All	
	<Calling party address>	All	

8.12.1 Associated procedure

8.12.1.1 Timer F-<CC.03> management

<CC.03>: CC setup timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.12.2 Exceptional cases

8.12.2.1 FT releases the incoming call request

The normal release procedure shall be used (see clause 8.7).

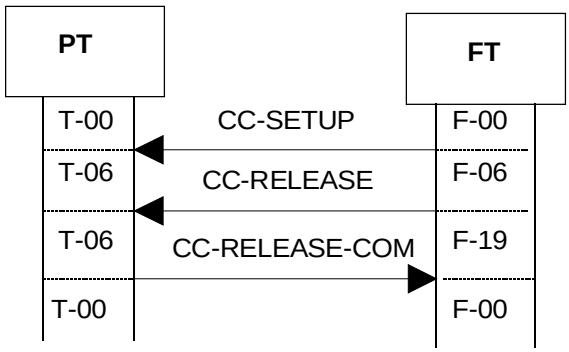
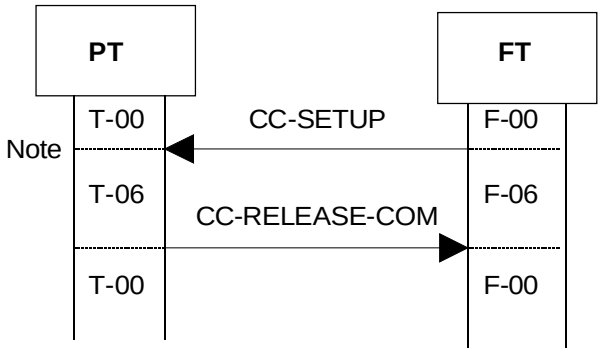


Figure 34: FT releases the incoming call request

For the values used within the {CC-SETUP} see table 21. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.12.2.2 PT rejects the incoming call request

The abnormal release procedure shall be used (see clause 8.8).



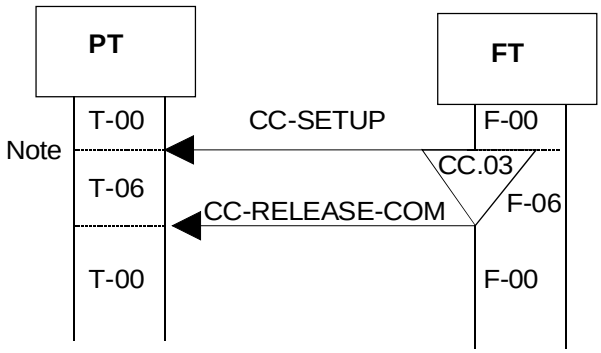
NOTE: Either PT-CC or PT-IWU may reject the call.

Figure 35: PT rejects the incoming call request

For the values used within the {CC-SETUP} see table 21. For the contents of {CC-RELEASE-COM} message see table 17.

8.12.2.3 Timer F-<CC.03> expiry

The abnormal release procedure shall be used (see clause 8.8).



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 36: Timer F<CC.03> expiry

For the values used within the {CC-SETUP} see table 21. For the contents of {CC-RELEASE-COM} see table 17.

8.12.3 Collective and group ringing

GAP equipment, which supports additionally to its GAP features collective and group ringing shall follow the procedures as specified in ETSI EN 300 175-5 [5], clause 14.4.

A PP that has already established a call, should interpret a collective or group ringing request as an unexpected message and shall not initiate ringing.

Similarly, when a PP receives a call setup request during collective or group ringing, should stop ringing and allow the call setup to proceed.

A FP which implements collective or group ringing during incoming call shall also implement all the incoming call mandatory procedures. Upon incoming call, after the collective and group ring, the FP shall additionally send a CC-SETUP message to each PP involved in the incoming call.

NOTE: The previous statement guarantees that:

1) the PP will always ring; and

2) CLIP and CNIP information elements can be sent in the CC-SETUP or in a CC-INFO message before the user picks up the call.

8.13 Incoming call confirmation

8.13.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 9.3.2.7. Figure 37 and table 22 together with the associated clauses define the mandatory requirements with regard to the present document.

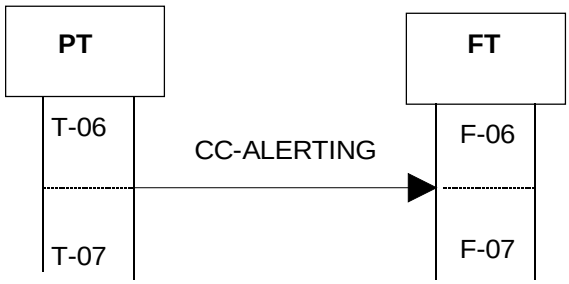


Figure 37: Incoming call confirmation

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

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

8.13.1 Exceptional cases

8.13.1.1 FT releases the incoming call transaction

The normal release procedure shall be used (see clause 8.7).

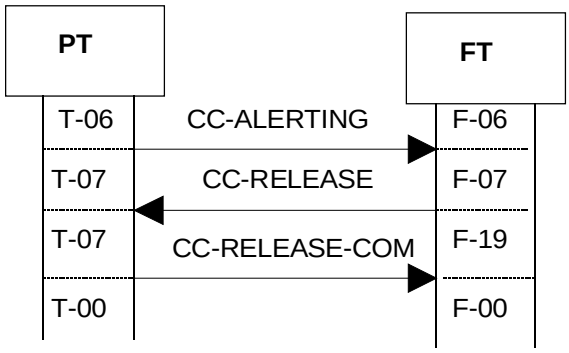


Figure 38: FT releases the incoming call transaction

For the values used within the {CC-ALERTING} see table 22. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.13.1.2 PT releases the incoming call transaction

The normal release procedure shall be used (see clause 8.7).

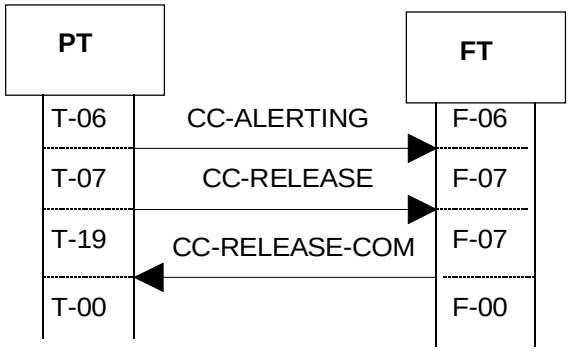


Figure 39: PT release the incoming call transaction

For the values used within the {CC-ALERTING} see table 22. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.14 PT alerting

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 9.3.2.7. The following text together with the associated clauses 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 21, with the following additions.

Table 23: 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.

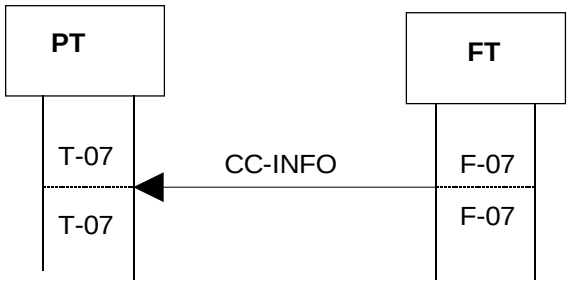


Figure 40: PT alerting in F-07

Table 24: 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

8.15 Incoming call connection

8.15.0 Procedure

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

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

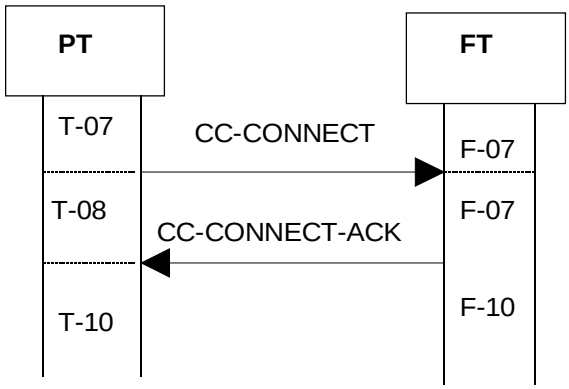


Figure 41: Incoming call connection

Table 25: 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 26: 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

8.15.1 Associated procedure

8.15.1.1 Timer P-<CC.05> management

<CC.05>: CC connect timer;

value: refer to ETSI EN 300 175-5 [5], 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 clause 6.9.6).

8.15.2 Exceptional cases

8.15.2.1 FT releases the incoming call transaction

The normal release procedure shall be used (see clause 8.7).

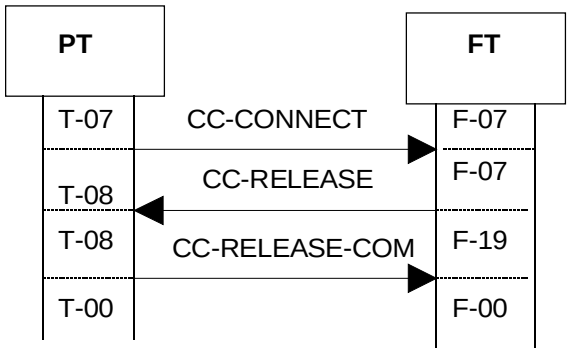


Figure 42: FT releases the incoming call transaction

For the values used within the {CC-CONNECT} see table 25. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.15.2.2 PT releases the incoming call transaction

The normal release procedure shall be used (see clause 8.7).

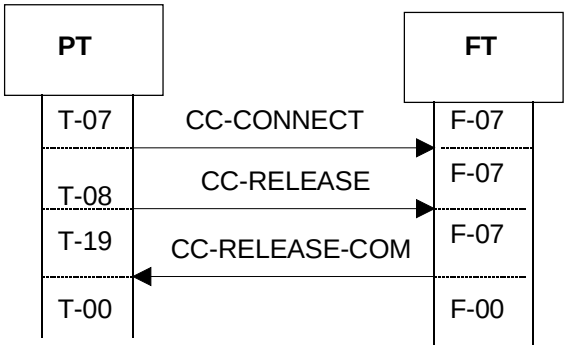
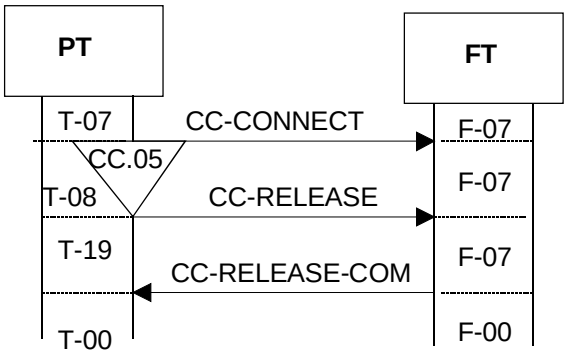


Figure 43: PT releases the incoming call transaction

For the values used within the {CC-CONNECT} see table 25. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.15.2.3 Timer P-<CC.05> expiry

The normal release procedure shall be used (see clause 8.7).



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 44: Timer P<CC.05> expiry

For the values used within the {CC-CONNECT} see table 25. For the contents of {CC-RELEASE} and {CC-RELEASE-COM} messages, see tables 15 and 16.

8.16 Display

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 10.2 and D.2.2. The following text together with the associated clauses 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 ETSI EN 300 175-5 [5], clause 6.3.2).

Table 27: 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>	0CH, 20H, 23H, 2AH, 30H - 39H	DECT standard characters = standard IA5 characters. The support of these codes is only mandatory if feature [N.24] is implemented. For the actual supported values see <<Terminal capability>> information element, clause 8.17
		08H - 0BH, 0DH	DECT control characters. The support of these codes is only mandatory if feature [N.25] is implemented. For the actual supported values see <<Terminal capability>> information element, clause 8.17

8.17 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 clauses define the mandatory requirements with regard to the present document.

Table 28: 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.24] it shall indicate in this field value which is equal to or higher than 2
	<Profile indicator_1> bit 2	"xxxxx1x"B	GAP and/or PAP supported
	<Profile indicator_7> bit 5	"xxXxxxx"B X = [0,1]	Support or no support of "Re-keying" and "default cipher key early encryption mechanism" (see note 1)
	DSAA2 (Octet 5)	[0,1]	Support (or not support) of the DSAA2 (see ETSI EN 300 175-7 [7] and note 2)
	DSC2 (Octet 5)	[0,1]	Support (or not support) of the DSC2 (see ETSI EN 300 175-7 [7] and note 3)
	<Control codes>	All	If PT supports feature [N.25] it shall indicate in this field value which is equal to or higher than 2
NOTE 1: This bit needs only to be understood by FTs supporting feature N.35 and NWK layer procedures "re-keying" or "early encryption". NOTE 2: This bit needs only to be understood by FTs supporting feature N.36. NOTE 3: This bit needs only to be understood by FTs supporting MAC service M.17.			

The capabilities in table 29 shall be assumed as default if the following fields in the <<TERMINAL CAPABILITY>> information element are not present.

Table 29: 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
	<Profile indicator_7>, bit 5	"xx0xxx"B	No support of "Re-keying" and "default cipher key early encryption mechanism"
	DSAA2 (Octet 5)	0	No support of the DSAA2
	DSC2 (Octet 5)	0	No support of the DSC2

No echoing of characters is allowed in the FT and therefore the PT would be responsible for displaying dialled digits (see figure 45). 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.

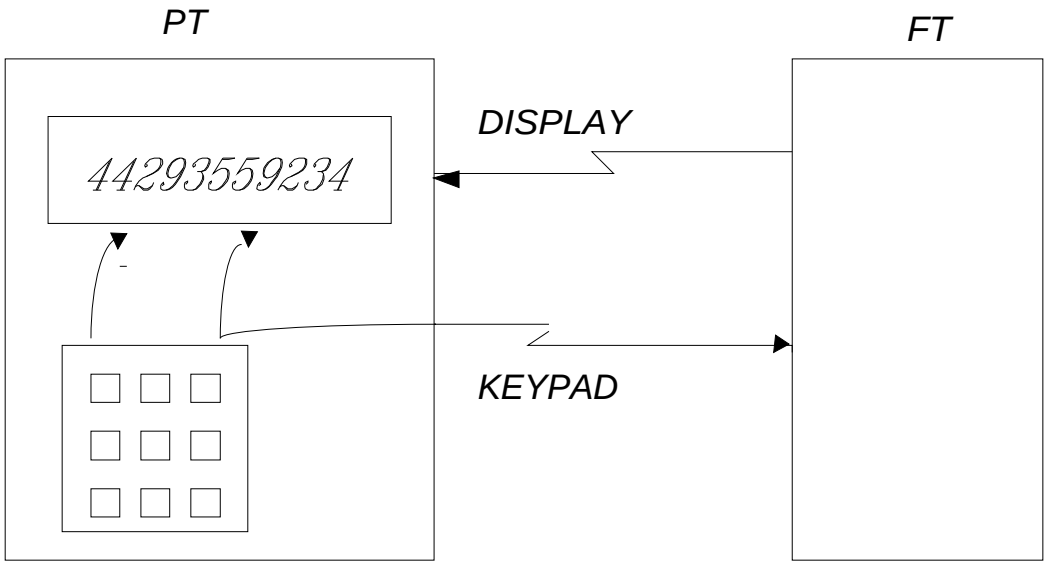


Figure 45: Terminal display

8.18 Internal call setup

The following text together with the associated clauses 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 clause 8.2) with the following replacement to the {CC-SETUP} message.

Table 30: 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

8.19 Internal call keypad

The following text together with the associated clauses 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 clause 8.10) with the following replacement to the {CC-INFO} message.

Table 31: 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

8.20 Service call setup

The following text together with the associated clauses 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 clause 8.2) with the following replacement to the {CC-SETUP} message.

Table 32: 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

8.21 Service call keypad

The following text together with the associated clauses 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 clause 8.10) with the following replacement to the {CC-INFO} message.

Table 33: 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

8.22 Identification of PP

8.22.0 Procedure

The procedure relates to feature Identification of PT [N.13] and shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.2.1. Figure 46 and tables 34 and 35, together with the associated clauses define the mandatory requirements with regard to the present document.

Figure 46: Identification of PT

Table 34: 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 35: 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.

8.22.1 Associated procedure

8.22.1.1 Timer F-<MM_ident.2> management

<MM_ident.2>: identification timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {IDENTITY-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.22.2 Exceptional cases

8.22.2.1 Identity not existing in the PT

This procedure is equivalent to the identification of PT procedure successful case defined in clause 8.22 except that the {IDENTITY-REPLY} message shall be sent without the identity information elements that have been requested but do not exist.

8.22.2.2 Timer F-<MM_ident.2> expiry

The timer F-<MM_ident.2> shall not be restarted by the FT. If a re-transmission 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.

8.23 Authentication of FT using DSAA

8.23.0 Procedure

The procedure relates to features ZAP [N.16] and Terminate access rights FT initiated [N.20], as well as to feature Authentication of FT [N.26] when the DECT Standard Authentication Algorithm (DSAA) is used.

NOTE: See also clause 8.45.6 describing the authentication of FT using the DECT Standard Authentication Algorithm #2 (DSAA2).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.3. Figure 47 and tables 36 and 37, together with the associated clauses define the mandatory requirements with regard to the present document.

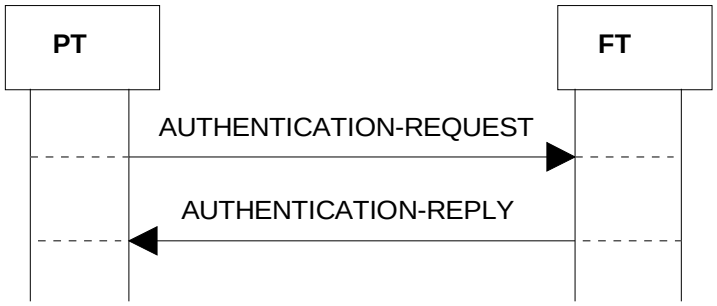


Figure 47: Authentication of FT using DSAA

Table 36: 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>>			
	Length of Contents (L)	8	Length of RAND_P (64 bits)
	<RAND Field>	All	Authentication parameter RAND_P (see ETSI EN 300 175-7 [7])

Table 37: 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>>			
	Length of Contents (L)	4	Length of RES2 (32 bits)
	<RES Field>	All	Authentication parameter RES2 (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	8	Length of RS (64 bits)
	<RS Field>	All	Authentication parameter RS (see ETSI EN 300 175-7 [7])

8.23.1 Associated procedure

8.23.1.1 Timer P-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.23.2 Exceptional cases

8.23.2.1 Authentication algorithm/key not supported

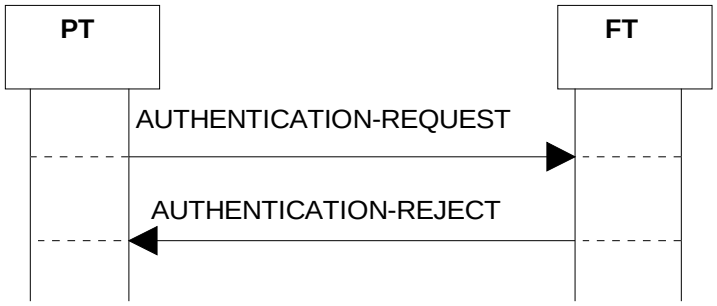


Figure 48: Authentication algorithm/key not supported by the FT

Table 38: 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.

8.23.2.2 FT Authentication failure (authentication challenge RES2 has wrong value)

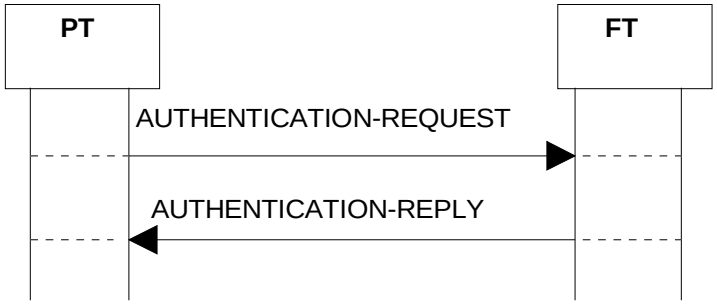


Figure 49: Authentication challenge RES2 has wrong value

Any failure of the procedure (FT authentication failure) shall result on the interruption of any call in progress between both peers. Either, the normal call release procedure (clause 8.7) PT initiated (figure 21) or the abnormal call release procedure (clause 8.8), PT initiated (figure 27) may be used. The release reason IE may be optionally included in the {CC-RELEASE} or {CC-RELEASE-COM} messages.

NOTE: If included, the recommended value is "Authentication failed".

In case the FT authentication has been performed using proprietary or non-DECT algorithms, the handling of the case is out of the scope of the present document.

8.23.2.3 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.

8.24 Authentication of PP using DSAA

8.24.0 Procedure

The procedure relates to the feature Authentication of PP [N.9] when the DECT Standard Authentication Algorithm (DSAA) is used.

NOTE 1: See also clause 8.45.7 describing the authentication of PP using the DECT Standard Authentication Algorithm #2 (DSAA2).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.1. Figure 50 and tables 39 and 40, together with the associated clauses define the mandatory requirements with regard to the present document.

Figure 50: Authentication of PT

Table 39: 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 clause 8.26)
	<DEF>	0,1	Value 1 only allowed in case PP indicated support of 'Re-keying' and 'early encryption' in terminal capabilities
	<TXC>	0	
	<UPC>	0	Value 1 used in storing the DCK procedure, (see clause 8.27)
	<Cipher key number>	0	Value 8 used in storing the DCK procedure, (see clause 8.27)
	< Default Cipher Key Index>	all	Contains default cipher key index in case DEF bit is set
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	8	Length of RS (64 bits)
	<RS Field>	All	Authentication parameter RS (see ETSI EN 300 175-7 [7])

Table 40: 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>>			
	Length of Contents (L)	4	Length of RES1 (32 bits)
	<RES Field>	All	Authentication parameter RES1 (see ETSI EN 300 175-7 [7])
<<ZAP field>>			
	<Contents field>	0-15	M if stored else O. Associated to feature [N.16]
<<Service class>>			
	<Service class field>	1-6	M if stored else O. Associated to feature [N.14]

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.

NOTE 2: The ciphering key generated by DSAA has a length of 64 bits.

8.24.1 Associated procedure

8.24.1.1 Timer F-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.24.2 Exceptional cases

8.24.2.1 Authentication algorithm/key not supported

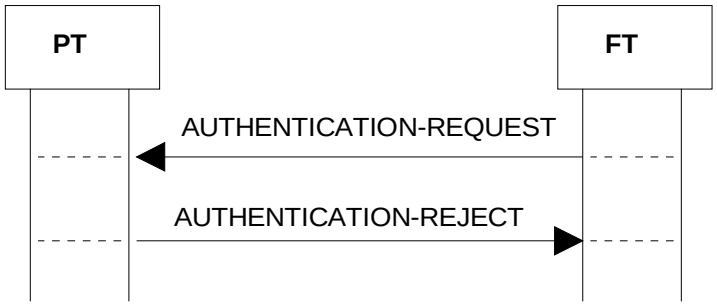


Figure 51: Authentication algorithm/key not supported by the PT

For the contents of the {AUTHENTICATION-REJECT} message see table 38.

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

8.24.2.2 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.

8.23.2.3 PP Authentication failure (authentication challenge RES1 has wrong value)

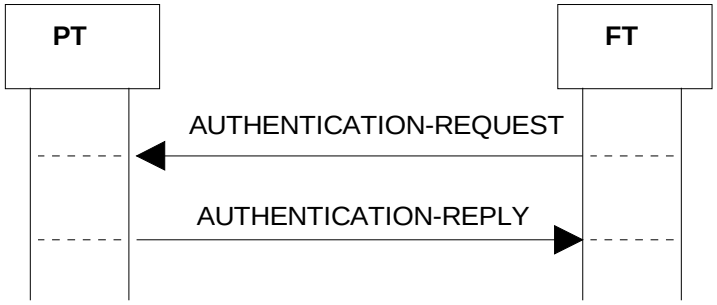


Figure 52: Authentication challenge RES1 has wrong value

Any failure of the procedure (PP authentication failure) shall result on the interruption of any call in progress between both peers. Either, the normal call release procedure (clause 8.7) FT initiated (figure 22) or the abnormal call release procedure (clause 8.8), FT initiated (figure 28) may be used. The release reason IE may be optionally included in the {CC-RELEASE} or {CC-RELEASE-COM} messages.

NOTE: If included, the recommended values are either "Authentication failed" or "Encryption Activation Failed".

In case the FT authentication has been performed using proprietary or non-DECT algorithms, the handling of the case is out of the scope of the present document.

8.25 Authentication of user using DSAA

8.25.0 Procedure

The procedure relates to the feature Authentication of user [N.10] when the DECT Standard Authentication Algorithm (DSAA) is used.

NOTE: See also clause 8.45.8 describing the authentication of the user using the DECT Standard Authentication Algorithm #2 (DSAA2).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.2. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

This procedure is equivalent to the authentication of PT procedure defined in clause 8.24 with the following replacement to the {AUTHENTICATION-REQUEST} message.

Table 41: 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".

8.25.1 Associated procedure

8.25.1.1 Timer F-<MM_auth.2> management

<MM_auth.2>: authentication of user timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.25.2 Exceptional cases

8.25.2.1 Authentication algorithm/key not supported

This procedure is equivalent to the procedure defined in clause 8.24.2.1.

8.25.2.2 Timer F-<MM_auth.2> expiry

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

8.26 Incrementing the ZAP value

The procedure relates to the feature ZAP [N.16]. This procedure may be executed using either DSAA or DSAA2 algorithms.

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.3. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

This procedure is equivalent to the authentication of PT procedure defined in clause 8.24 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.

The procedure for authentication of PT shall be executed as described in clause 8.24 when DSAA is used or as described in clause 8.45.7 when DSAA2 is used.

The procedure for authentication of FT shall be executed as described in clause 8.23 when DSAA is used or as described in clause 8.45.6 when DSAA2 is used.

For both procedures, the authentication algorithm shall be the same in use for the execution of other FT or PT authentication procedures.

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.

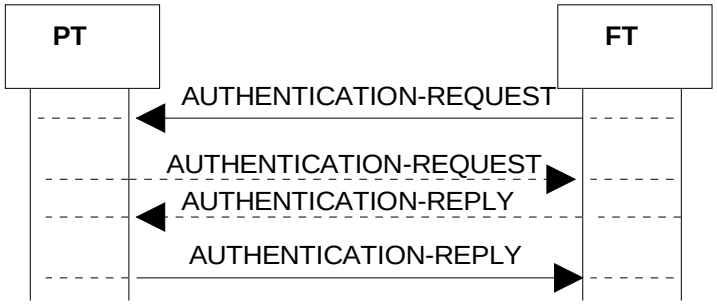


Figure 53: ZAP increment

Table 42: 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 {AUTHENTICATE REPLY} sent by FT see tables 36 and 37 if DSAA is used or tables 79 and 80 if DSAA2 is used.

For the contents of {AUTHENTICATION-REPLY} sent by the PT see table 40 if DSAA is used or table 83 if DSAA2 is used.

8.27 Storing the DCK

This procedure relates to the feature encryption activation FT initiated [N.17] as well as to feature encryption activation PT initiated [N.27] and is equivalent to the authentication of PT procedure with the modification described in table 43 to the {AUTHENTICATION-REQUEST} message.

This procedure may be executed using either DSAA or DSAA2 algorithms. The procedure for authentication of PT shall be executed as described in clause 8.24 when DSAA is used or as described in clause 8.45.7 when DSAA2 is used.

The authentication algorithm shall be the same in use for the execution of the FT authentication procedures.

The following modification shall apply in the message {AUTHENTICATION-REQUEST} sent by the FT.

Table 43: 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	

For the other contents of the {AUTHENTICATION-REQUEST} message, refer to table 39 if DSAA is used or to table 82 if DSAA2 is used.

8.28 Location registration

8.28.0 Procedure

The procedure relates to the feature location registration [N.11] and shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.4.1. The following text together with the associated clauses 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.

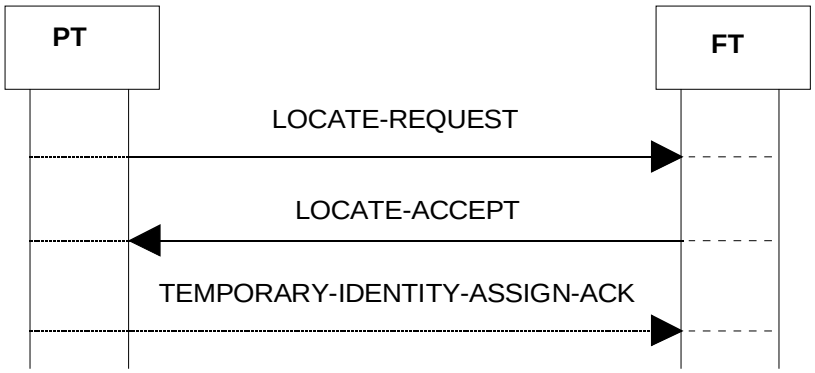


Figure 54: Location registration

Table 44: 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 128)
	<Type>	1	
	<ARC>	All	
	<ARD+RPN>	All	
<<Location-area>>			This information element shall contain the old Location Area Level (LAL) (see table 128)
	<LI-type>	1	
	<LAL>	All	
<<Terminal capability>>			(see clause 8.17)
	<Tone capability>	All	
	<Display capability>	All	
	<Profile indicator_1> bit 2	"xxxxx1x"B	GAP and/or PAP supported
	<Profile indicator_7> bit 5	"xxXxxxx"B X = [0,1]	Support or no support of "Re-keying" and "default cipher key early encryption mechanism" (see note 1)
	DSAA2 (Octet 5)	[0,1]	Support (or not support) of the DSAA2 (see ETSI EN 300 175-7 [7] and note 2)
	DSC2 (Octet 5)	[0,1]	Support (or not support) of the DSC2 (see ETSI EN 300 175-7 [7] and note 3)
	<Control codes>	All	
NOTE 1: This bit needs only to be understood by FTs supporting feature N.35 and NWK layer procedures "re-keying" or "early encryption". NOTE 2: This bit needs only to be understood by FTs supporting feature N.36. NOTE 3: This bit needs only to be understood by FTs supporting MAC service M.17.			

Table 45: 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
	<Type>	32	TPUI
	<Length of id value>	20	
	<Identity-value>	Values in ETSI EN 300 175-6 [6] clause 6.3.1 are allowed	Only assigned individual TPUIs are allowed
<<Location-area>>			
	<LI-type>	1	
	<LAL>	0-39	Even if default LAL

Table 46: 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 clause 13.7 (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.

8.28.1 Associated procedures

8.28.1.1 Timer P-<MM_locate.1> management

<MM_locate.1>: location timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: {LOCATE-REQUEST} message is sent or an 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.

8.28.1.2 Timer F-<MM_ident.1> management

<MM_ident.1>: TPUI assignment timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.28.2 Exceptional cases

8.28.2.1 FT rejects the location registration procedure

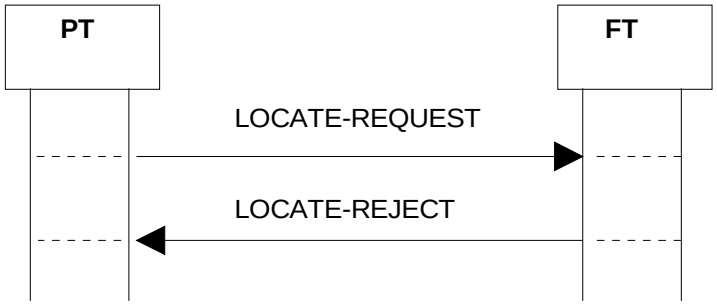


Figure 55: Location registration not supported by the FT

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

Table 47: Values used within the {LOCATE-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Reject Reason>>	<Reject Reason Code>	All optional	All optional

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

In the case that the FT did not recognize the PT by its <<Portable identity>> IE, it is recommended that the FT includes the <<Reject reason>> IE in its {LOCATE-REJECT} message with the Reject Reason code "IPUI unknown" (value '02'H).

In the case of a rejection by the FT, the PT should not initiate a location registration procedure until the conditions for location registration initiation are met as defined in clause 13.2.

8.28.2.2 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 re-transmit 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.

8.28.2.3 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, the PT shall send back a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message.

NOTE: For the requirements in regard to FT sending the {LOCATE-ACCEPT} message, the requirements as stated in table 46, clause 8.28 apply.

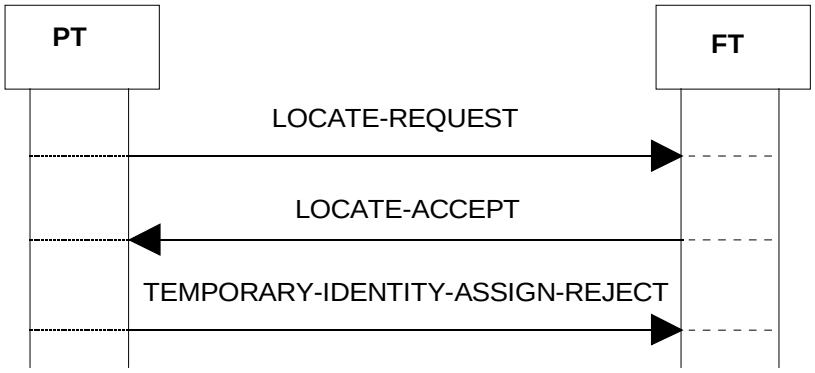


Figure 56: Rejection of identity assignment

Table 48: 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

8.28.2.4 Timer F-<MM_identity.1> expiry

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

8.29 Location update

The procedure relates to the feature Location registration [N.11] and shall be performed with regard to clause 13.4.3 of ETSI EN 300 175-5 [5]. The following text together with the associated clauses 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.

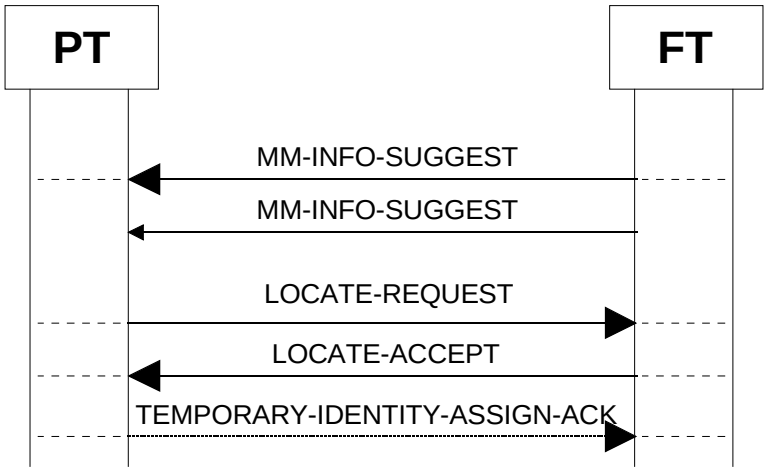
The FT shall send two consecutive {MM-INFO-SUGGEST} messages, each contains an <<INFO-TYPE>> information element with only the parameter type "locate suggest"; the <ext> parameter associated to this parameter type shall be set to 0 in the first {MM-INFO-SUGGEST} and to 1 in the second {MM-INFO-SUGGEST}.

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 clause 8.28.

Even if the bit a38, see clause 13.6, table 126, 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 57: Location update

Table 49: 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

8.30 Obtaining access rights

8.30.0 Procedure

The procedure relates to the features Subscription registration user procedure on-air [N.18], Service class indication/assignment [N.14], and, ZAP [N.16] and shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.5.1. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

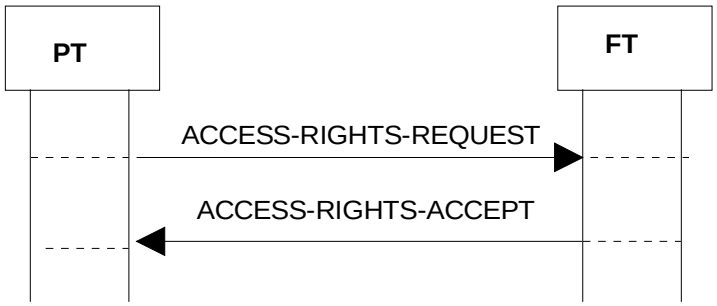


Figure 58: Obtain access rights

Table 50: 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, 2	DSAA, DSAA2 (see note 1)
	<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
<<Terminal capability>>			(see clause 8.17)
	<Tone capability>	All	
	<Display capability>	All	
	<Profile indicator_1> bit 2	"xxxxx1x"B	GAP and/or PAP supported
	<Profile indicator_7> bit 5	"xxXxxxx"B X = [0,1]	Support or no support of "Re-keying" and "default cipher key early encryption mechanism" (see note 2)
	DSAA2 (octet 5)	[0,1]	Support (or not support) of the DSAA2 (see ETSI EN 300 175-7 [7] and note 3)
	DSC2 (octet 5)	[0,1]	Support (or not support) of the DSC2 (see ETSI EN 300 175-7 [7] and note 4)
	<Control codes>	All	

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
NOTE 1: The value DSAA2 is only applicable if feature N.36 is supported. NOTE 2: This bit needs only to be understood by FTs supporting feature N.35 and NWK layer procedures "re-keying" or "early encryption". NOTE 3: This bit needs only to be understood by FTs supporting feature N.36. NOTE 4: This bit needs only to be understood by FTs supporting MAC service M.17.			

Table 51: 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.16]
	<Contents-field>	All	
<<Service-class>>			Relates to feature [N.14]
	<Service-class-field>	All	

8.30.1 Associated procedure

8.30.1.1 Timer P-<MM_access.1> management

<MM_access.1>:access rights timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {ACCESS-RIGHTS-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.30.2 Exceptional cases

8.30.2.1 FT rejects the access rights

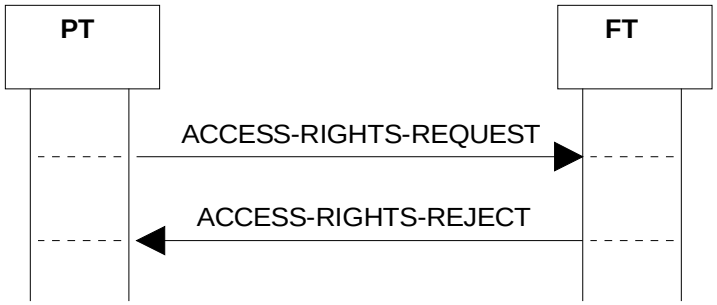


Figure 59: FT rejects access rights request

Table 52: 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.

8.30.2.2 Timer P-<MM_access.1> expiry

Upon expiry of P-<MM_access.1> PT shall consider the procedure as failed. PT shall not re-transmit 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.

8.31 FT terminating access rights

8.31.0 Procedure

The procedure relates to the feature FT terminate access rights [N.20] and shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.5.2. The following text together with the associated clauses 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.

An FP may request termination of a subscription assigned to an IPUI/PARK pair which has not been used for the establishment of the current link however it is optional for the PP to accept it.

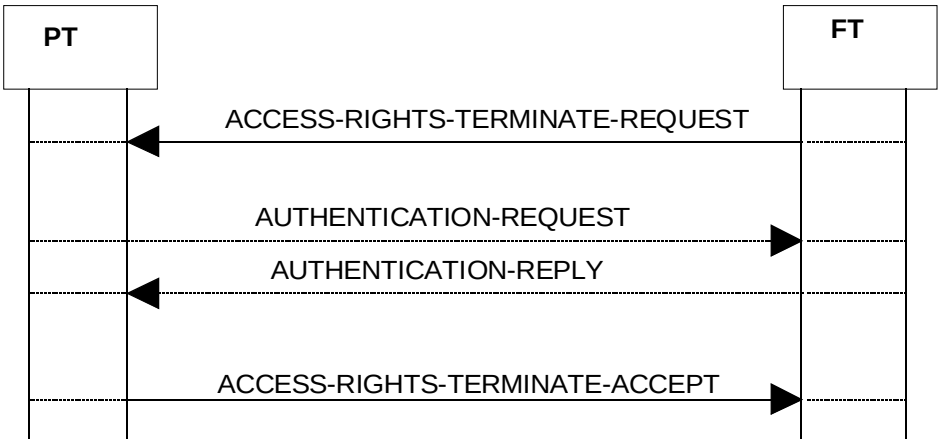


Figure 60: Termination of access rights

Table 53: 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 {AUTHENTICATE-REQUEST} and {AUTHENTICATE-REPLY} see tables 36 and 37.

Table 54: 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.

8.31.1 Associated procedure

8.31.1.1 Timer F-<MM_access.2> management

<MM_access.2> access rights termination timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {ACCESS-RIGHTS-TERMINATE-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.31.2 Exceptional cases

8.31.2.1 PT rejects the termination request

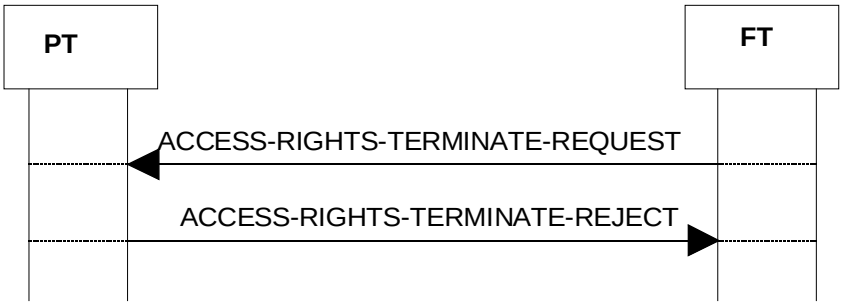


Figure 61: PT rejects

Table 55: 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

8.31.2.2 Timer F-<MM_access.2> expiry

Upon expiry of F-<MM_access.2> FT shall consider the procedure as failed. FT shall not re-transmit 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.

8.32 Key allocation

8.32.0 Procedure

The procedure relates to the feature On air key allocation [N.12] when the DECT Standard Authentication Algorithm (DSAA) is used.

NOTE: See also clause 8.45.9 describing the Key allocation using the DECT Standard Authentication Algorithm #2 (DSAA2).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.6. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

The PT shall support the key allocation procedure prior to the completion of the obtaining access rights procedure even if the IPUI/PARK pair may not have been provided yet.

The key allocation procedure consists of only one MM transaction.

See clause 6.9.6 for coexistence rules between MM procedures and CC states.

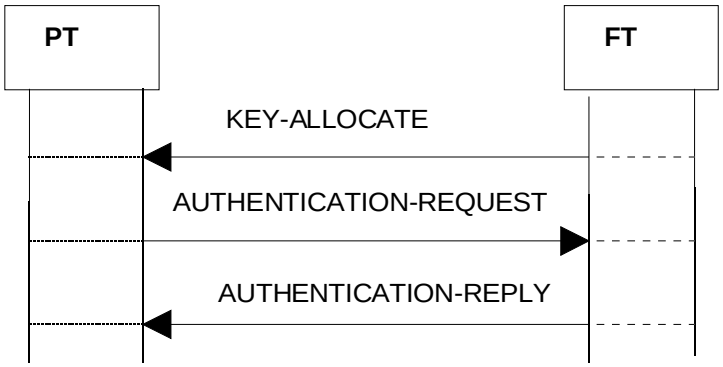


Figure 62: Key allocation

Table 56: 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, if available
	<AC number>	8	Keys relate to IPUI/PARK pair, if available
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	8	Length of RS (64 bits)
	<RS Field>	All	Authentication parameter RS (see ETSI EN 300 175-7 [7])

Table 57: 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>>			
	Length of Contents (L)	8	Length of RAND_P (64 bits)
	<RAND Field>	All	Authentication parameter RAND_P (see ETSI EN 300 175-7 [7])
<<RES>>			
	Length of Contents (L)	4	Length of RES1 (32 bits)
	<RES Field>	All	Authentication parameter RES1 (see ETSI EN 300 175-7 [7])

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 58: 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>>			
	Length of Contents (L)	4	Length of RES2 (32 bits)
	<RES Field>	All	Authentication parameter RES2 (see ETSI EN 300 175-7 [7])

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.

8.32.1 Associated procedures

8.32.1.1 Timer F-<MM_key.1> management

<MM_key.1>: key allocation timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {KEY-ALLOCATE} message is sent or an 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.

8.32.1.2 Timer P-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.32.2 Exceptional cases

8.32.2.1 Timer F-<MM_key.1> expiry

Upon expiry of F-<MM_key.1> FT shall consider the procedure as failed. FT shall not re-transmit 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.

8.32.2.2 Timer P-<MM_auth.1> expiry

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

8.32.2.3 Allocation-type element is unacceptable

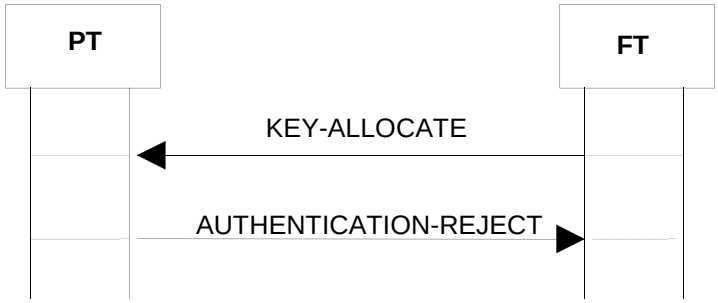


Figure 63: Allocation-type unacceptable for PT

Table 59: Standard 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

8.32.2.4 Authentication of PT fails

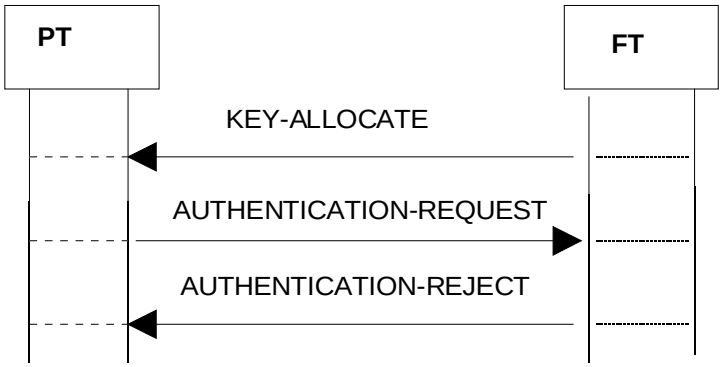


Figure 64: Authentication of PT fails

Table 60: Standard values used within the {AUTHENTICATION-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Comments	Normative actions
			All optional	

8.32.2.5 Authentication of FT fails

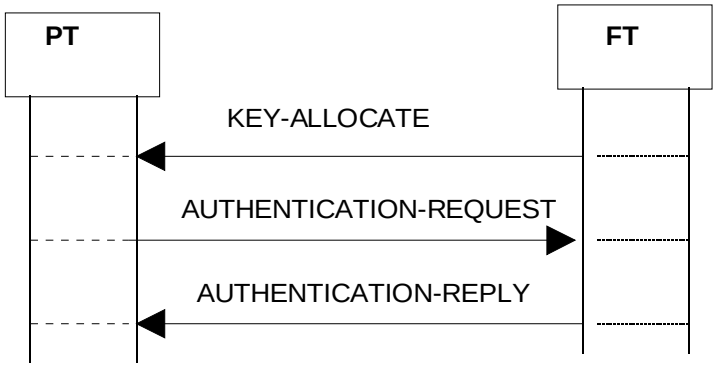


Figure 65: Authentication of FT fails

If the Authentication of FT fails, as XRES2 ≠ RES2, the KS' shall not be 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.

8.33 Cipher-switching initiated by FT using DSC

8.33.0 Procedure

This procedure relates to the feature Encryption activation FT initiated [N.17] and Enhanced Security [N.35] as well as to feature Encryption deactivation FT initiated [N.28] when the DECT Standard Cipher (DSC) is used.

NOTE: See also clause 8.45.10 describing the Cipher-switching initiated by FT when the DECT Standard Cipher #2 (DSC2) is used.

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.8 and ETSI EN 300 175-7 [7], clause 6.5.3. Figure 66 and table 61 together with the associated clauses define the mandatory requirements with regard to the present document.

Figure 66: Cipher - switching initiated by FT

Table 61: 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.28]
		1	Enable ciphering respectively performing re-keying
	<Cipher-algorithm-id>	1	DECT Standard Cipher algorithm 1
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= subscription)

In case the encryption is disabled, the {CIPHER-REQUEST} shall be sent before the transfer of any C-plane data intended to be encrypted (e.g. dialled number).

{CIPHER-REQUEST} may also be sent in case early encryption is active (clause 8.45.3), or in case the encryption key of an already encrypted connection shall be changed by means of re-keying (clause 8.45.2).

The DCK shall be produced and stored in advance using the storing the DCK procedure (see clause 8.27). In order for the encryption mechanism to be activated (respectively switched to a new DCK) 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, unless a re-keying is initiated by sending DL_ENC_KEY-req primitive to the DLC layer.

In order to generate the DCK, the authentication of the PT may be performed using either the DSAA or the DSAA2 algorithms according to the procedures described in clauses 8.24 or 8.45.7 respectively.

When the authentication of PT has been performed based on DSAA2 (clause 8.45.7), only the 64 less significant bits of the cipher key generated by DSAA2 shall be used.

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. Respectively, the re-keying shall be invoked at MAC layer.

8.33.1 Associated procedure

8.33.1.1 Timer F-<MM_cipher.1> management

<MM_cipher.1>: cipher-switching timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {CIPHER-REQUEST} message is sent;

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

8.33.2 Exceptional cases

8.33.2.1 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.

If the feature N.35 and the NWK layer procedure "Encryption of all calls" is supported, then the FT shall release the call on reception of a CIPHER-REJECT message as described in clause 8.45.1.

In any other case, the FT should not release the call on reception of a CIPHER-REJECT message.

If a non-DECT cipher algorithm was requested and the ciphering has been rejected, the handling of the case is out of the scope of the present document.

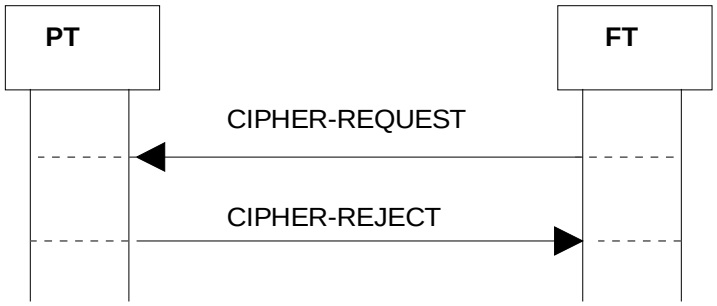


Figure 67: PT rejects the cipher request

Table 62: 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	

8.33.2.2 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 re-transmit 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.

The FT should not release the call on Timer F-<MM_cipher.1> expiry.

8.34 Cipher-switching initiated by PT using DSC

8.34.0 Procedure

The procedure relates to the feature Encryption activation PT initiated [N.27] and Encryption deactivation PT initiated [N.29] when the DECT Standard Cipher (DSC) is used.

NOTE: See also clause 8.45.11 describing the Cipher-switching initiated by PT when the DECT Standard Cipher #2 (DSC2) is used.

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.8 and ETSI EN 300 175-7 [7], clause 6.5.3. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

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

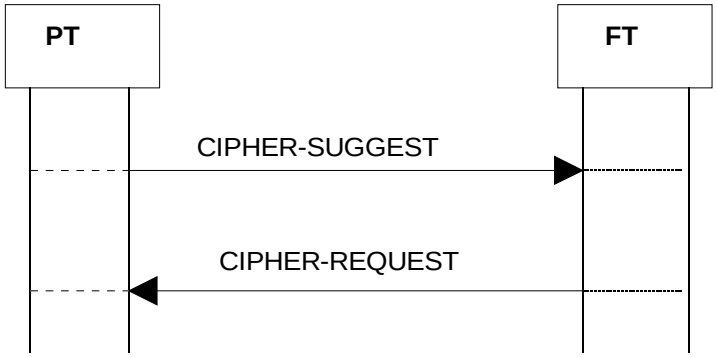


Figure 68: Ciphering, PT initiated

Table 63: 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.29]
		1	Enable ciphering. Relates to feature [N.27]
	<Cipher-algorithm-id>	1	DSC
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= Subscription)

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. Relates to feature [N.29]
		1	Enable ciphering. Relates to feature [N.27]
	<Cipher-algorithm-id>	1	DSC
	<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 clause 8.27). 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.

In order to generate the DCK, the authentication of the PT may be performed using either the DSAA or the DSAA2 algorithms according to the procedures described in clauses 8.24 or 8.45.7 respectively.

When the authentication of PT has been performed based on DSAA2 (clause 8.45.7), only the 64 less significant bits of the cipher key generated by DSAA2 shall be used.

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 clause 8.33 and the associated clauses).

8.34.1 Associated procedure

8.34.1.1 Timer P-<MM_cipher.2> management

<MM_cipher.1>:cipher-switching timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.34.2 Exceptional cases

8.34.2.1 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.

If the feature N.35 and the NWK layer procedure "Encryption of all calls" is supported, then the PT shall release the call on reception of a CIPHER-REJECT message as described in clause 8.45.1.

In any other case, the PT should not release the call on reception of a CIPHER-REJECT message.

If a non-DECT cipher algorithm was requested and the ciphering has been rejected, the handling of the case is out of the scope of the present document.

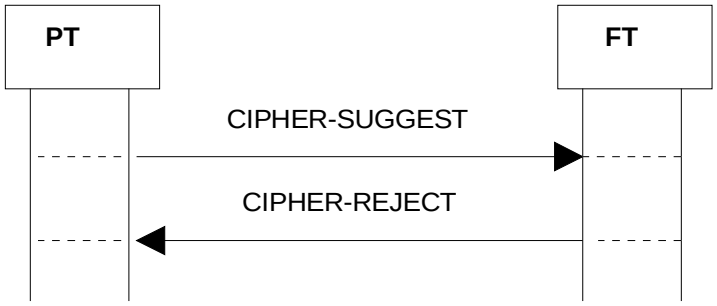


Figure 69: FT rejects the cipher requests

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	

8.34.2.2 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 re-transmit 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.

8.35 Indirect FT initiated link establishment

8.35.0 Procedure

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

FT and PT shall only support short format for the {LCE-REQUEST-PAGE} message. When the FT request for a link establishment is successfully received by the intended PT, the PT shall initiate direct PT link establishment (see clause 8.36).

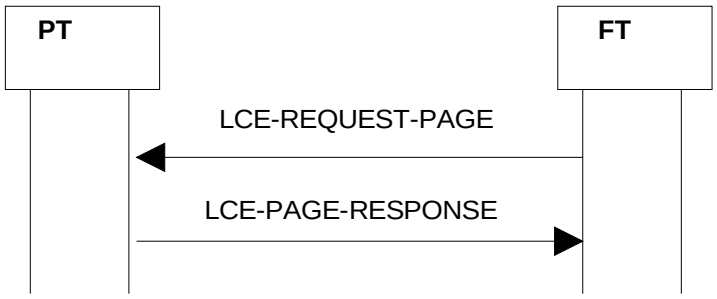


Figure 70: Indirect FT initiated link establishment

Table 66: 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	
	<LCE-header>	0,4	Indicates the U-plane services (MAC) required. The "0" value shall be used when only C-plane is required (e.g. MM procedures). The PT shall support a follow on call on the same link even if value "0" was used during initial paging
<<Short address>>			
	<TPUI Address>	All	The lowest 16 bits from the actual TPUI value

Table 67: 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 depend upon subscription records
	<Type>	32	PARK
	<Length of identity value>	All	PLI+1
	<ARC+ARD>	All	

8.35.1 Associated procedure

8.35.1.1 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 ETSI EN 300 175-5 [5], 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.

8.35.2 Exceptional cases

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

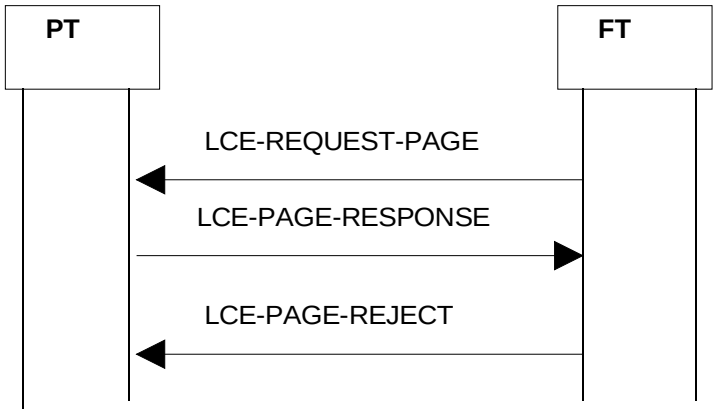


Figure 71: The IPUI received in the {LCE-PAGE-RESPONSE} does not match

Table 68: 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 clause 8.37).

The {LCE-PAGE-REJECT} message shall be sent by a DL_DATA-req primitive via the S-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.

8.35.2.2 Timer <LCE.03> expiry

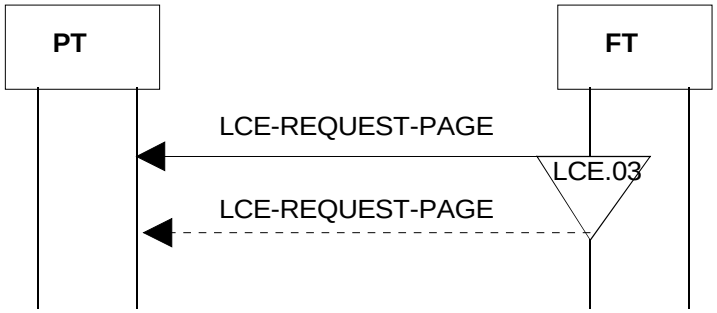


Figure 72: Timer <LCE.03> expiry

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).

8.35.2.3 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>.

8.36 Direct PT initiated link establishment

8.36.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clauses 14.2.1 and 14.2.2. The following text together with the associated clauses 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.

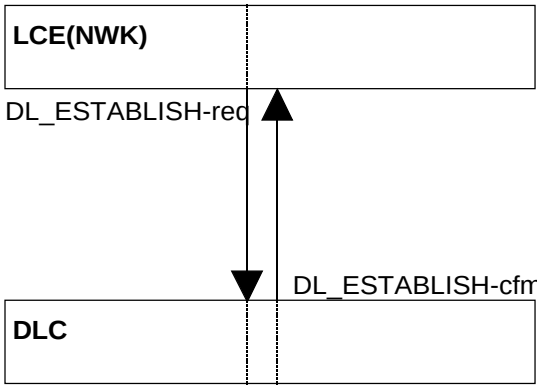


Figure 73: Direct PT initiated link establishment, initiating side

Table 69: Values used within the DL_ESTABLISH-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Establish mode>>		
	Class A 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 clause 8.35) otherwise it shall be empty

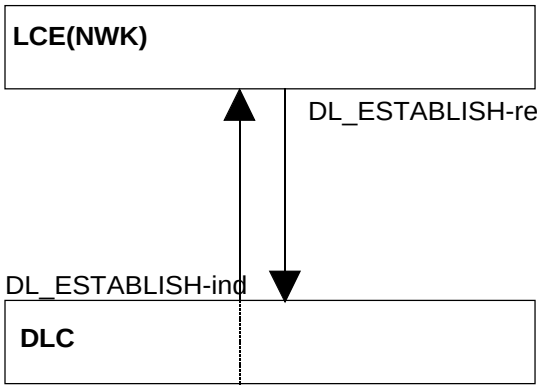


Figure 74: Direct PT initiated link establishment, receiving side

Table 70: Values used within the DL_ESTABLISH-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Establish mode>>		
	Class A 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 clause 8.35) otherwise it shall be empty

8.36.1 Exceptional case

8.36.1.1 Link establishment failure

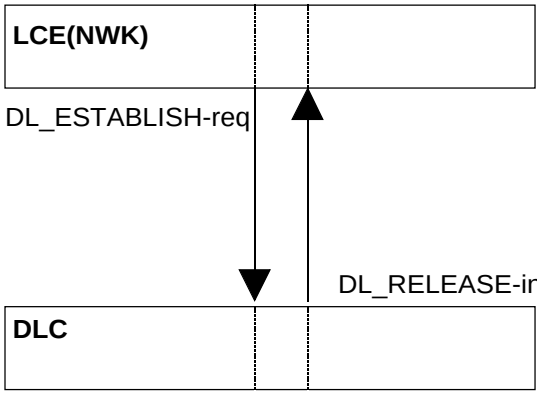


Figure 75: Direct PT initiated link establishment failure

Table 71: Values used within the DL_RELEASE-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 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.		

8.37 Link release "normal"

8.37.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 14.2.7. The following text together with the associated clauses 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.

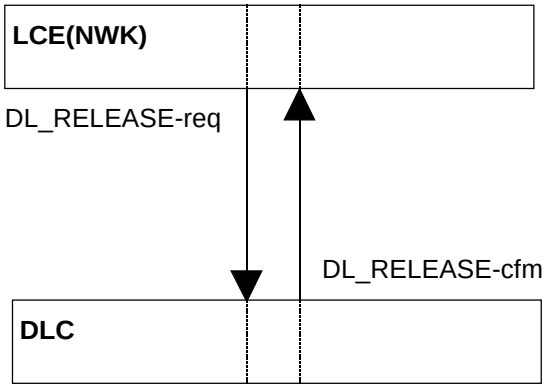


Figure 76: Link release "normal", initiating side

Table 72: Values used within the DL_RELEASE-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Release mode>>		
	Normal	

Table 73: Values used within the DL_RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Release mode>>		
	Normal	

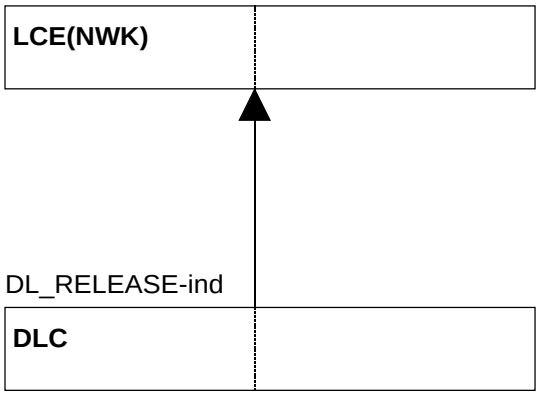


Figure 77: Link release "normal", receiving side

Table 74: Values used within the DL_RELEASE-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 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.		

8.37.1 Associated procedure

8.37.1.1 Timer <LCE.01> management

<LCE.01>: link release timer;

value: Refer to ETSI EN 300 175-5 [5], annex A;

start: A DL_RELEASE-req primitive is sent;

stop: A DL_RELEASE-cfm primitive is received.

8.37.2 Exceptional cases

8.37.2.1 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".

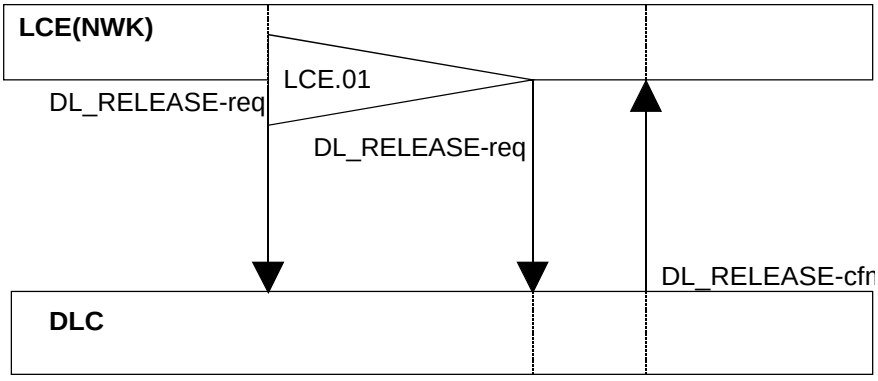


Figure 78: Timer <LCE.01> expiry

Table 75: Values used within the DL_RELEASE-req primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Release mode>>		
	Abnormal	

Table 76: Values used within the DL_RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Release mode>>		
	Normal or Abnormal	

8.37.2.2 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 77: Values used within the DL_RELEASE-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<DLEI>>		
	Data Link Endpoint Identifier	(see ETSI EN 300 175-4 [4], clause 7.3.6)
<<Release mode>>		
	Abnormal	

8.38 Link release "abnormal"

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 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 clause 8.37) only in the release mode identification which here shall be set to "Abnormal". Clauses 8.37.1 and 8.37.2 are not relevant to link release "abnormal" procedure.

8.39 Link release "maintain"

8.39.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 14.2.7. The following text together with the associated clauses 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 clause 8.38). 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 or after an obtaining access rights procedure), Call Independent Supplementary Service (CISS) and Connection Less 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 clause 8.9) the support of this procedure is optional.

8.39.1 Associated procedure

8.39.1.1 Timer <LCE.02> management

<LCE.02>: link maintain timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.40 Enhanced FT initiated U- plane connection

The procedure shall be performed as defined in clauses 9.3.1.4 and 9.3.2.4 of ETSI EN 300 175-5 [5]. Figure 79 and table 78 together with the associated clauses define the mandatory requirements with regard to the present document.

The PT shall support the call connection procedures defined in this clause in the following call states: T02, T03, T04 (outgoing call), T07, T08 (incoming call), T19 (call release).

The call connection procedures apply the <<Progress Indicator>> within the {CC-INFO} message as follows:

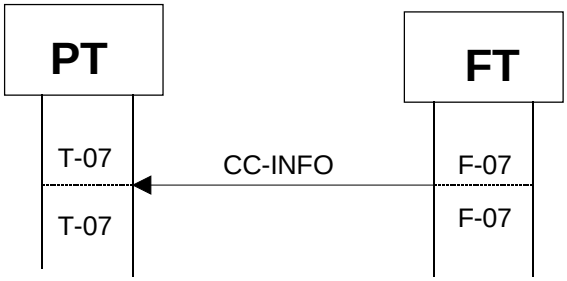


Figure 79: Call connection example, in F-07

Table 78: Values used within the {CC-INFO} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Progress indicator>>			
	<Progress description>	8H	In band information or appropriate pattern now available The PT shall connect the U-plane

8.41 Calling Line Identification Presentation (CLIP) Indication

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

Calling Line Presentation Indication may be sent either by including the <<CALLING-PARTY-NUMBER>> information element in the {CC-SETUP} message or in a {CC-INFO} message. The FT is required to support one of the methods, the PT is required to support both methods.

For CLIP indication through the {CC-SETUP}message, see clause 8.12, table 21 "values used within the {CC-SETUP} message".

CNIP or CLIP (especially when sent together) might not fit into the {CC-SETUP}message or into a single {CC-INFO}message, in that case an additional {CC-INFO}message shall be used.

For CLIP indication through {CC-INFO} consider the following:

Table 79: Values used within the {CC-INFO} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Calling party number>>			
	<Number type>	All	
	<Numbering plan id>	All	
	<Presentation indicator>	All	
	<Screening indicator>	All	
	<Calling party address>	All	

NOTE 1: To support the feature in the PP, it is sufficient that the PP is capable to display the IA5 characters given in the field <Calling party address> according to its display capabilities without consideration of the contents of octets 3 and 3a.

NOTE 2: In case both CLIP and CNIP are sent to the PP, it is sufficient to display CNIP. It is optional to display both.

8.42 Calling Name Identification Presentation (CNIP) Indication

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

Calling Name Presentation Indication may be sent either by including the <<CALLING-PARTY-NAME>> information element in the {CC-SETUP} message or in a {CC-INFO} message. FT is required to support at least one of the methods, PT is required to support both.

CNIP or CLIP (especially when sent together) might not fit into the {CC-SETUP}message or into a single {CC-INFO}message, in that case an additional {CC-INFO}message shall be used.

For CNIP indication through the {CC-SETUP} see clause 8.12, table 21, with the following additions:

Table 80: Values added within the {CC-SETUP} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Calling party name>>			
	<Presentation indicator>	All	
	<Screening indicator>	All	
	<Calling party name>	All	

For CNIP indication through {CC-INFO} consider the following:

Table 81: Values used within the {CC-INFO} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Calling party name>>			
	<Presentation indicator>	All	
	<Screening indicator>	All	
	<Calling party name>	All	

NOTE 1: To support the feature in the PP, it is sufficient that the PP is capable to display the IA5 characters given in the field <Calling party name> according to its display capabilities without consideration of the contents of octet 3.

NOTE 2: In case both CLIP and CNIP are sent to the PP, it is sufficient to display CNIP. It is optional to display both.

8.43 Internal Call Calling Line Identification Presentation (CLIP)

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

Calling Line Identification Presentation (CLIP), shall be implemented for internal calls.

The general procedure for CLIP is described in clause 8.41 "Calling Line Identification Presentation (CLIP) Indication" and it shall be used also for internal calls.

NOTE 1: The internal call CLIP indication can be used to convey internal handset number or any other number. External calling number could be used in case of call transfer.

NOTE 2: If internal call CLIP indication is used to indicate the handset number the following values for information element <<Calling Party Number>> should be used.

Table 82: Suggested values for <<Calling Party Number>> IE for internal calls

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Calling party number>>			
	<Number type>	3	Network specific number
	<Numbering plan id>	9	Private plan
	<Presentation indicator>	All	Presentation allowed
	<Screening indicator>	All	User-provided, verified and passed
	<Calling party address>	IA5 coding of Terminal Identity Number in decimal representation	Terminal Identity Number of the calling part: - 0 for FP - 1 to n for PP

NOTE 3: See clause 14.4 for a description of the Terminal Identity Number and its use.

NOTE 4: To support the feature in the PP, it is sufficient that the PP is capable to display the IA5 characters given in the field <Calling party address> according to its display capabilities without consideration of the contents of octets 3 and 3a.

NOTE 5: In case both CLIP and CNIP are sent to the PP, it is sufficient to display CNIP. It is optional to display both.

8.44 Internal Call Calling Name Identification Presentation (CNIP)

The following text and table 83 together with the associated clauses define the mandatory requirements with regard to the present document.

Calling Name Identification Presentation (CNIP), shall be implemented for internal calls. The internal call setup procedure (see clause 8.18) shall be used.

For internal calls, the calling PT name shall be used. This name should be configurable by the user. It is an easy-to-memorize alias for the terminal identity number, allowing users to clearly identify the handset within the DECT system. For example, in a residential environment, this name could be a room name ("kitchen", "living room"), a person name, etc.

Handset names may be stored in the PT or in the FT. However, the storage of the handset name in the FT is strongly recommended. The mechanism for storing and accessing the name is out of the scope of the current procedure.

A PT may send a <<CALLING PARTY NAME>> information element at call establishment. In that case, it shall be included in the {CC-SETUP} message or in the {CC-INFO} message. FT is required to support at least one of the methods; PT is required to support both.

Table 83: Values used within the {CC-SETUP} or {CC-INFO} message for internal call CNIP

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Calling party name>>			
	<Presentation indicator>	00B	Presentation allowed
	<Used Alphabet>	000B	DECT standard
	<Screening indicator>	01B	User-provided, verified and passed
	<Calling party name>	All	Name of the calling party PT

At internal call establishment, the FT shall send to the destination PT the name of the calling PT in an <<CALLING PARTY NAME>> information element. The following priority scheme shall be used by the FT to fill this information element:

1) If a <<CALLING PARTY NAME>> information element is received from the originating PT, the FT shall re-use it.

2) If a name for the originating PT is stored in the FT, the FT shall use it to fill the <<CALLING PARTY NAME>>.

3) Otherwise, the FT shall fill the <<CALLING PARTY NAME>> with a default string. For example "DECT n" default string can be used where n stands for the IA5 coding of the terminal identity number of the calling party PT in decimal representation.

For sending the name of the calling PT, from the FT to the called PT, the general procedure for CNIP shall be used. This procedure is described in clause 8.42 "Calling Name Identification Presentation (CNIP) Indication". The <<CALLING PARTY NAME>> information element received from the calling party handset shall be sent to the called party handset by the FT in the {CC-SETUP}or the {CC-INFO}message.

As a consequence of the priority scheme defined for the FT, the PT should not send its handset name at call establishment if the name is already stored in the FT. This would be useless.

NOTE 1: The originating PT could send temporary or application specific names. For example, a dual mode GSM/DECT PT could send the remote party name in the CNIP. This case is not a call transfer from DECT system point of view as only one DECT call is involved.

NOTE 2: In the current procedure, the called PT may receive successively two <<CALLING PARTY NAME>> information element to display.

Figures 80, 81, 82 and 83 show possible sequences of internal call CNIP using {CC-SETUP} or {CC-INFO} messages.

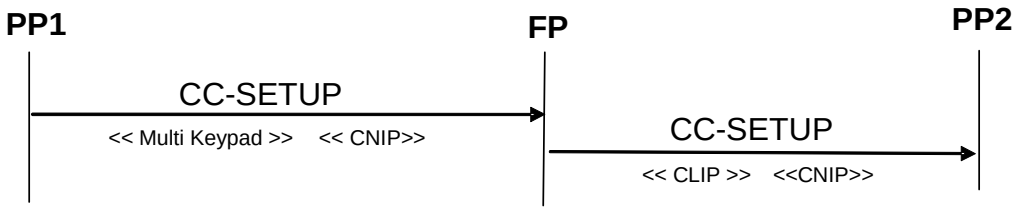


Figure 80: Internal call using <<CNIP>> from originating PP

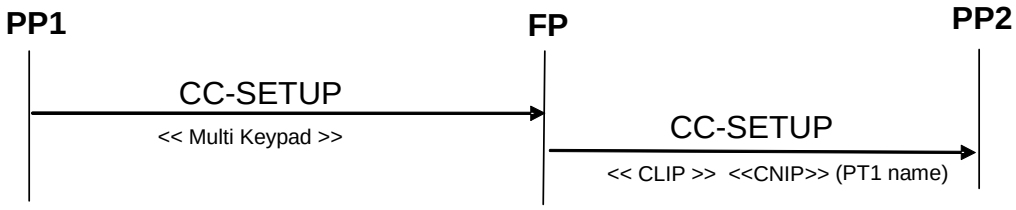


Figure 81: Internal call using <<CNIP>> from FP

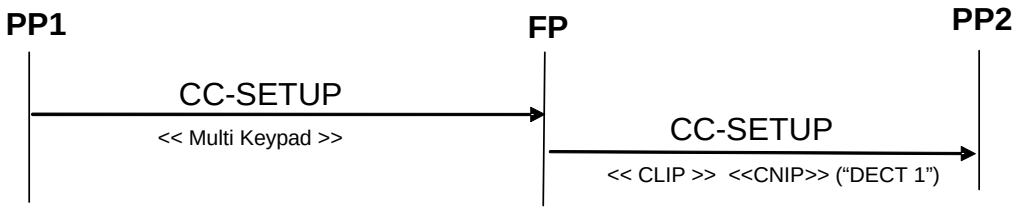


Figure 82: Internal call using default CNIP from FP

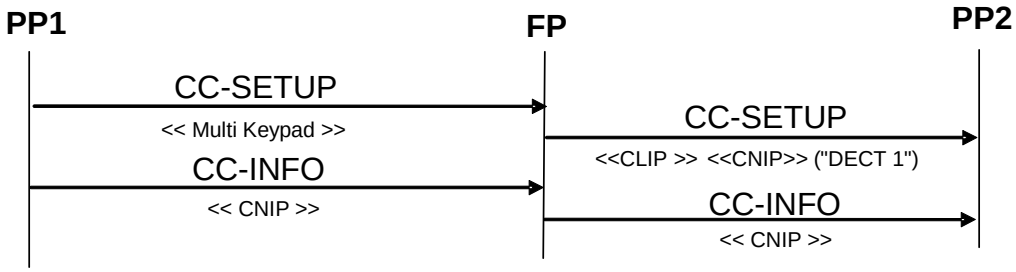


Figure 83: Internal call using default CNIP from FP, followed by <<CNIP>> from originating PP

8.45 Enhanced security procedures

8.45.0 General

These procedures relate to the feature Enhanced security [N.35] as well as to the feature Encryption activation FT initiated [N.17] and shall be performed as defined in ETSI EN 300 175-3 [3], ETSI EN 300 175-5 [5], and ETSI EN 300 175-7 [7]. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

It is recommended to implement the feature [N.35] as each procedure brings additional guarantee on security.

Features [N.17] "Encryption activation FT initiated", [N.9] "Authentication of PP" and [N.12] "On air key allocation" shall be supported by PT and FT in case feature [N.35] is supported.

The procedure "Enhanced security regarding legacy devices" of clause 8.45.5 defines exceptions to the requirements of clauses 8.45.1 to 8.45.4 in order to allow the use of legacy devices. Using this procedure for legacy devices does not prevent fulfilling the requirements of clauses 8.45.1 to 8.45.4 completely for other devices.

8.45.1 Encryption of all calls

FP shall initiate the encryption as described in procedure 8.33 (cipher switching FT initiated) for all calls, so that all calls are encrypted, i.e. voice calls as well as service calls and List Access (LiA) service calls (when supported). Encryption shall be initiated within timer <MM_encryption_check.1>.

Refer to ETSI EN 300 175-7 [7] clause I.1 for the value of timer <MM_encryption_check.1>.

The timer <MM_encryption_check.1> shall be started:

- for incoming calls, after receiving the first NWK message, after a {CC_SETUP} message has been sent;
- for outgoing calls, after receiving a {CC_SETUP} message.

FP shall perform abnormal call release as defined in clause 8.8 if the PP rejects 'cipher switching FT initiated', or if the encryption activation fails. The FP shall indicate the release reason [Encryption activation failed] within the information element <<Release Reason>> in the message {CC-RELEASE-COM}.

A new derived cipher key shall be generated on every call by use of the 'Storing the DCK' procedure as described in clause 8.27. This key shall only be used for encryption of a currently established call, unless it is a default cipher key. A default cipher key may be used for early encryption in several calls.

8.45.2 Re-keying during a call

This procedure consists on the periodic modification of the cipher key used for encryption during an ongoing call and thus improving the security of the call.

When implementing the procedure, the FP shall set bit a_{42} of the "Extended higher layer capabilities (part 2)" (see ETSI EN 300 175-5 [5], clause F.3).

The PP shall support the re-keying and indicate this in the <<Terminal Capability>> information element both in the {ACCESS-RIGHTS-REQUEST} message and in the {LOCATE-REQUEST} message. It is, however, allowed not to indicate this capability in case the FP does not itself indicate the same capability in the extended FP Capabilities part 2.

NOTE 1: This exception is allowed with respect to existing GAP Protocol test equipment which is not able to test PPs indicating newly defined terminal capability bits.

This procedure shall be used as described in ETSI EN 300 175-7 [7], clause 6.4 and ETSI EN 300 175-5 [5], clause 13.8 for each call, i.e. voice calls as well as service calls and List Access service calls (when supported).

The FP shall periodically perform 'authentication of PP' procedures with generation and storage of a new DCK (clause 8.27) followed by Cipher switching (clause 8.33) procedures, in a way that between the generation and the last use of such DCK there is never a longer time than timer <MM_re-keying.1>.

For the purposes of the timer <MM_re-keying.1>, the generation of the key is assumed to happen at the FT sending of the {AUTHENTICATION-REQUEST} message, and the last use of the key is assumed to happen at the FT sending of a {CIPHER-REQUEST} message that is confirmed by the reception of a MAC START.GRANT message.

The authentication procedure shall be executed using either DSAA (as clause 8.24) or DSAA2 (as clause 8.45.7) algorithms. DSAA2 procedure (clause 8.45.7) shall be used if DSAA2 is supported by both peers.

The encryption algorithm may be either DSC (see ETSI EN 300 175-7 [7], annex J) or DSC2 (see service M.17 and ETSI EN 300 175-7 [7], annex M).

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_re-keying.1>.

After receiving the {AUTHENTICATION-REPLY} message, the FP shall immediately perform the Cipher switching initiated by FT as described in clause 8.33.

The FP may retry the messages {AUTHENTICATION-REQUEST} and {CIPHER-REQUEST} in case of no proper answers from the PP (reception of {AUTHENTICATION-REPLY} and MAC START messages respectively).

In case of expiration of the timer associated to the authentication procedure (timer -<MM_auth.1> defined in ETSI EN 300 175-5 [5], clause A.5) or if the PP rejects the authentication, or answers with a wrong authentication result, the FP shall perform abnormal release of the call and shall indicate the release reason [Re-keying failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM} message.

In case of no completion of the re-keying procedure (reception of the START.GRANT after switching to the new key), the FP shall perform abnormal release of the call and shall indicate the release reason [Re-keying failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM} message.

In case the re-keying fails on MAC layer, the connection shall be released on MAC layer as specified in ETSI EN 300 175-7 [7], clause 6.4.6.

Specific for systems with Wireless Relay Stations (WRS)

In cases of systems with repeaters (Wireless Relay Station, see ETSI EN 300 700 [12]), the rules on aging of the key described in ETSI EN 300 175-7 [7], clause 6.7.2.3, shall apply. The requirement on re-keying shall be understood as that no key in use may have an age (in the meaning of ETSI EN 300 175-7 [7], clause 6.7.2.3.2) longer than timer <MM_re-keying.1>.

NOTE 2: Based on ETSI EN 300 175-7 [7], clause 6.7.2.3.2, the life of a key for a segment directly connected to the FP starts with its generation. The life of a key for any other segment inherits the previous age of the key used for protecting the message {MM-INFO-SUGGEST} that carries the key when it is provided to the WRS upper peer of the segment. The life of a key terminates when a Cipher Switching procedure is run and a new key is set in use.

NOTE 3: In general, the FP may control the re-keying rule by performing rekeying to both WRSs and PPs in the right sequence, and by starting a timer with the generation of the DCK in the segment directly connected to the FP and stopping it when it gets confirmation that key is replaced by a new one at the PP segment. Such timer should never exceed <MM_re-keying.1>.

Specific for DSC2

When the Cipher Algorithm in use is DSC2, the more relaxed timer <MM_re-keying.2> (defined in ETSI EN 300 175-7 [7], clause I.1) shall be used instead of <MM_re-keying.1>, allowing longer intervals between re-keying. In the case of systems with repeaters, DSC2 should be used in all segments of the connection. In any other case, the timer <MM_re-keying.1> shall apply.

NOTE 4: DSC2 is always used with Authentication Algorithm DSAA2.

8.45.3 Early encryption

This procedure allows to encrypt all CC messages in a call and thus, to protect the early stages of the signalling such as dialling or CLIP information sending, that may be sensitive.

This procedure shall be used for each call, i.e. voice calls, service calls and List Access service calls (when supported).

When implementing the procedure, the FP shall set bit a_{42} of the "Extended higher layer capabilities (part 2)" (see ETSI EN 300 175-5 [5], clause F.3).

The PP shall support the early encryption and indicate this in the <<Terminal Capability>> information element both in the {ACCESS-RIGHTS-REQUEST} message and in the {LOCATE-REQUEST} message. It is however allowed not to indicate this capability in case the FP does not itself indicate the same capability in the extended FP Capabilities part 2.

NOTE 1: This exception is allowed with respect to existing GAP Protocol test equipment which is not able to test PPs indicating newly defined terminal capability bits.

In case the PP indicated support of early encryption, the FP shall perform an 'Authentication of PP' procedure in order to generate a default cipher key after successful subscription registration. For this purpose the {AUTHENTICATION-REQUEST} message shall indicate that a default cipher key is being generated (DEF bit=1) and shall also contain a default cipher key index.

It is recommended that the FP should perform this 'Authentication of PP' procedure as soon as possible after successful subscription. In any case, this procedure shall be completed at the very latest before expiration of timer <MM_early_encryption.1> after start of encryption of the first call.

The FP may perform further 'Authentication of PP' procedures generating default cipher keys at any time. This may be done either to update a previous default cipher key, or to provision additional default cipher keys.

The authentication procedure shall be executed using either DSAA (as clause 8.24) or DSAA2 (as clause 8.45.7) algorithms. DSAA2 procedure (clause 8.45.7) shall be used if DSAA2 is supported by both peers.

The encryption algorithm may be either DSC (see ETSI EN 300 175-7 [7], annex J) or DSC2 (see service M.17 and ETSI EN 300 175-7 [7], annex M).

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_early_encryption.1>.

The generated default cipher key shall remain valid for the whole remaining validity of the current subscription or until the same default cipher key index is re-used in another 'Authentication of PP' procedure.

The FP may repeat the procedure in order to assign a new default cipher key at any time. It is recommended to do this not too often, since the default cipher key needs to be stored in non-volatile memory. The PP shall remember at least the last assigned default cipher key and the corresponding default cipher key index during the validity of the subscription. The FP shall remember all previously assigned default cipher keys and their corresponding default cipher key indices during the validity of the subscription.

When the FP assigns a DefCK, it may do so using a new default cipher key index, in which case it is considered as a new DefCK (i.e. requiring allocation of non-volatile storage). Alternatively, the FP may re-use an existing default cipher key index, in which case the new key shall over-write the old key.

NOTE 2: The FP is responsible for assigning the DefCKs, and so it is capable of managing the number of keys assigned to any device. For example, if non-volatile memory is limited it can re-use an existing default cipher key index, which will cause the old key to be over-written.

When a PP has multiple DefCK assigned, it may choose to use any of them that are appropriate. The PP algorithm for selecting the key to be used is left to the implementer.

As soon as a default cipher key is available, the PP shall activate encryption with one of the valid default cipher keys (as described in ETSI EN 300 175-7 [7], clause 6.4) immediately (at least before the first NWK C-Plane message is sent) after each MAC connection establishment. The PP shall indicate the chosen default cipher key by use of the corresponding default cipher key index. The PP shall not establish connections without immediately following early encryption activation as long as a valid default cipher key is available. The PP shall release the connection within 10 seconds from the start of the connection in case that the connection is not encrypted successfully (e.g. the FP repeatedly rejects early encryption activation attempts or the early encryption activation fails on MAC layer).

The PP shall encrypt the beginning of a call by using the default cipher key. The FP shall start the 'Authentication of PP' procedure in order to generate a new derived cipher key and shall use it for this call (as described in clauses 8.45.1 and 8.45.2) within timer <MM_re-keying.1>.

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_re-keying.1>.

The timer <MM_re-keying.1> shall be started:

- for incoming calls, after receiving the first NWK message, after a {CC_SETUP} message has been sent;
- for outgoing calls, after receiving a {CC_SETUP} message.

8.45.4 Subscription requirements

Possible risks regarding subscription are the FP staying permanently open for subscription, the registration of a wrong PP during subscription phase, and finally (of course) the use of the weak but usual AC (Authentication Code) value '0000'.

The FP shall not remain open for registration permanently. This shall be achieved through a dedicated MMI item that has to be activated manually by the user for having the FP enter the subscription mode. Example of such MMI items are a physical button (that might be combined with a paging button), a local menu or a remote access (e.g. via Web interface).

After the FP had entered the subscription mode following the use of the implemented MMI item, the FT shall remain in subscription mode (bit a44 set) for a maximum time equal to timer <MM_registration.1>.

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_registration.1>.

After successful registration of one single handset, the FT shall immediately re-set the bit a44 and exit the subscription mode.

The PT shall provide a feedback to the user (optical or acoustical) that the subscription has been successful.

It is recommended that the user manual informs the user that other PINs (AC) than "0000" or "1234" will give better security.

8.45.5 Enhanced security regarding legacy devices

8.45.5.0 General

In the following clause, procedures are defined which intend to enhance the security level against legacy devices. However, these procedures shall not only apply if the peer device is a legacy device, they shall apply in all cases and against all peer devices.

8.45.5.1 Behaviour of FPs regarding legacy PPs

FPs shall perform FT initiated encryption activation for every call against all PPs. In case the PP rejects the FT initiated cipher switching, the FP shall perform abnormal release of the call and indicate the release reason [encryption activation failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM} message.

In case the encryption is not activated within timer <MM_encryption_check.1>, with this timer being started:

- for incoming calls, after receiving the first NWK message, after a {CC_SETUP} message has been sent;
- for outgoing calls, after receiving a {CC_SETUP} message,

the FP shall perform abnormal release of the call, and indicate the release reason [encryption activation failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM} message, since the support of feature [N.17] "Encryption activation FT initiated" is mandatory for GAP PPs.

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_encryption_check.1>.

8.45.5.2 Behaviour of PPs regarding legacy FPs

Whether legacy FTs support encryption or not, and if so, at which points in time they start the FT initiated cipher switching, is not obvious in advance, but can only be determined by observation of the encryption status during previous calls.

At the start of a new observation period, the PP shall assume that the FP does not encrypt any calls.

A PP shall start a new observation period of the encryption status at the following points in time:

- the PP performs successfully the registration to an FP;
- the PP performs a reset;
- on user interaction (f.i. set back to factory defaults).

In case the PP detects that the FP disabled the FT capability bit for DECT Standard Cipher (DSC), the PP shall not suspend the observation automatically. Instead of this the PP should inform the user and shall only suspend the observation in case this is authorized by the user (e.g. switch on/off, re-registration, user menu).

NOTE 1: This exception allows the use of legacy repeater devices, which do not support encryption.

When an observation period of the encryption status is active (not suspended), the PP shall start (or restart if already running) the timer <MM_encryption_check.2> in the following situations:

- with sending of the {CC-ALERTING} message (in an incoming call);
- with sending of the {CC-CONNECT} message (in an incoming call);
- with receiving of the {CC-CALL-PROC} message (in an outgoing call);
- with receiving of the {CC-CONNECT} message (in an outgoing call).

Refer to ETSI EN 300 175-7 [7], clause I.1 for the value of timer <MM_encryption_check.2>.

After timeout, the PP shall check the encryption status of the call. The PP shall compare this encryption status with previous values of this status in the same situation and the same observation period:

- In case one of the previous calls in the same observation period and the same situation was encrypted whereas the current call is not, the PP shall assume that the peer side has been impersonated. As a result, it shall perform abnormal release of the call and indicate the release reason [Security attack assumed] within the information element <<Release Reason>> in the message {CC_RELEASE_COM}.

NOTE 2: If abnormal release is used once for an unencrypted call, all subsequent unencrypted calls (incoming and outgoing) within the same observation period necessarily also undergo abnormal release.

8.45.5.3 Behaviour regarding legacy 'repeater' devices

In order to allow interoperability with legacy 'repeater' devices, which do not support encryption, exceptions have to be defined for the procedures defined in clauses 8.45.1 to 8.45.5.

An FP of ARI Class A (see ETSI EN 300 175-6 [6]) may switch off the encryption support and broadcast a RPN > 0 in order to allow interoperability with legacy 'repeater' devices. In this case the FP shall not indicate the support of DECT Standard Cipher (DSC) in the higher layer capabilities (bit a_{37}) any longer.

In this case:

- the FP shall not initiate FT initiated cipher switching anymore;
- the FP shall not initiate re-keying;
- the PP shall not initiate early encryption;
- both FP and PP shall not delete valid default cipher keys;
- the FP may not initiate authentication of PP.

NOTE: It should be noted, that this reduces the security level of the whole system severely. It is recommended to switch off the repeater support if not needed. It is also recommended that the manual informs the user about these restrictions.

The PP shall react as described in clause 8.45.5.2.

As soon as the FP indicates the support of DECT Standard Cipher (DSC) in the higher layer capabilities (bit a_{37}) again:

- the FP shall initiate FT initiated cipher for following calls as described in clause 8.45.1;
- the FP shall initiate re-keying for following calls as described as described in clause 8.45.2;
- the FP shall start the 'Authentication of PP' procedure in order to generate a default cipher key in case there is no valid default cipher key available;
- the PP shall initiate early encryption for following connections as described in clause 8.45.3 as soon as a valid default cipher key is available;
- the PP shall resume the suspended observation of the encryption status.

8.45.6 Authentication of FT using DSAA2

8.45.6.0 Procedure

The procedure relates to features ZAP [N.16] and Terminate access rights FT initiated [N.20], as well as to feature Authentication of FT [N.26] when the feature N.36 (AES/DSAA2 authentication) is supported and the DECT Standard Authentication Algorithm #2 (DSAA2) is used.

NOTE: See also clause 8.23 describing the authentication of FT using the DECT Standard Authentication Algorithm (DSAA).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.3 and ETSI EN 300 175-7 [7], clause 6.5.2.4 with the following specific provisions:

- This procedure shall only be initiated by the PT if the FT has indicated the support of DSAA2 in Extended Higher Layer capabilities (part 2) FP broadcast.
- Authentication type 2 procedure, as defined by ETSI EN 300 175-7 [7], clauses 6.3.7, 6.3.3.4 and 6.5.2.4 shall be used.
- A algorithm, DSAA2 based, shall be used for all security processes as defined by ETSI EN 300 175-7 [7], clause 5.1.1.2.
- RAND_F parameter shall be used as input D3 of authentication process A22 and exchanged FT to PT during the authentication procedure.
- RS parameter shall have 128 bits (RS_{128}) and shall be used as input D2/D3 of authentication process A21.
- It is not required to run process A21 at every FT authentication. KS' may be reused and cached tagged by the RS_{128}' value used in its generation. The refresh timing or maximum number of reuses is up to the implementation. However the KS' should be refreshed from time to time. It is not allowed to use completely static KS'.

Figure 84 and tables 84 and 85, together with the associated clauses define the mandatory requirements with regard to the present document.

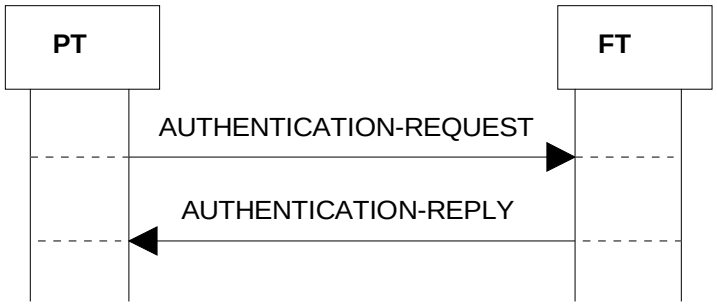


Figure 84: Authentication of FT using DSAA2

Table 84: 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>	2	DSAA2
	<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>>			
	Length of Contents (L)	8	Length of RAND_P (64 bits)
	<RAND Field>	All	Authentication parameter RAND_P (see ETSI EN 300 175-7 [7])

Table 85: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F (see ETSI EN 300 175-7 [7])
<<RES>>			
	Length of Contents (L)	4	Length of RES2 (32 bits)
	<RES Field>	All	Authentication parameter RES2 (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	16	Length of RS (128 bits)
	<RS Field>	All	Authentication parameter RS_{128} (see ETSI EN 300 175-7 [7])

8.45.6.1 Associated procedure

8.45.6.1.1 Timer P-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.45.6.2 Exceptional cases

8.45.6.2.1 Authentication algorithm/key not supported

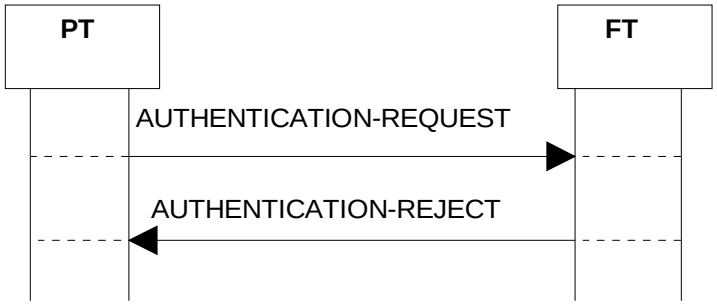


Figure 85: Authentication algorithm/key not supported by the FT

Table 86: 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.

8.45.6.2.2 FT Authentication failure (authentication challenge RES2 has wrong value)

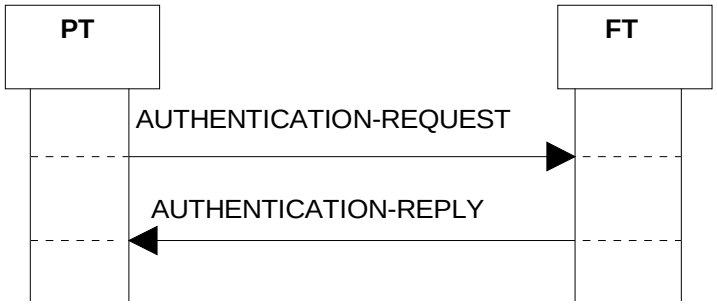


Figure 86: Authentication challenge RES2 has wrong value

Any failure of the procedure (FT authentication failure) shall result on the interruption of any call in progress between both peers. Either, the normal call release procedure (clause 8.7) PT initiated (figure 21) or the abnormal call release procedure (clause 8.8), PT initiated (figure 27) may be used. The release reason IE shall be included in the {CC-RELEASE} or in the {CC-RELEASE-COM} message with the value "Authentication failed".

8.45.6.2.3 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.

8.45.7 Authentication of PP using DSAA2

8.45.7.0 Procedure

The procedure relates to the feature Authentication of PP [N.9] when the feature N.36 (AES/DSAA2 authentication) is supported and the DECT Standard Authentication Algorithm #2 (DSAA2) is used.

NOTE 1: See also clause 8.24 describing the authentication of PP using the DECT Standard Authentication Algorithm (DSAA).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.1 and ETSI EN 300 175-7 [7], clause 6.5.2.3 with the following specific provisions:

- This procedure shall only be initiated by the FT if the PT has indicated the support of DSAA2 in Terminal Capability information.
- Authentication type 2 procedure, as defined by ETSI EN 300 175-7 [7], clauses 6.3.6, 6.3.3.3 and 6.5.2.3 shall be used.
- A algorithm, DSAA2 based, shall be used for all security processes as defined by ETSI EN 300 175-7 [7], clause 5.1.1.2.
- RAND_P parameter shall be used as input D3 of authentication process A12 and exchanged PT to FT during the authentication procedure.
- RS parameter shall have 128 bits (RS_{128}) and shall be used as input D2/D3 of authentication process A11.
- It is not required to run process A11 at every PT authentication. KS may be reused and cached tagged by the RS_{128} value used in its generation. The refresh timing or maximum number of reuses is up to the implementation. However the KS should be refreshed from time to time. It is not allowed to use completely static KS.

Figure 87 and tables 87 and 88, together with the associated clauses define the mandatory requirements with regard to the present document.

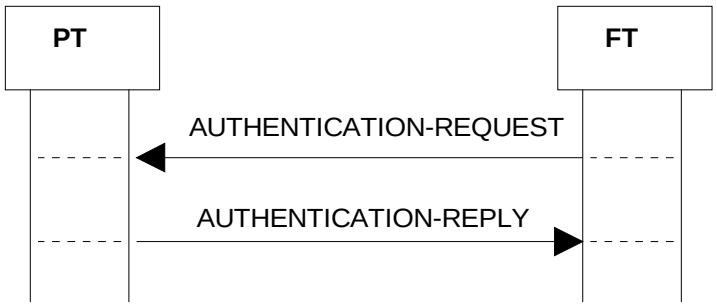


Figure 87: Authentication of PT using DSAA2

Table 87: 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>	2	DSAA2
	<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 clause 8.26)
	<DEF>	0,1	Value 1 only allowed in case PP indicated support of 'Re-keying' and 'early encryption' in terminal capabilities
	<TXC>	0	
	<UPC>	0	Value 1 used in storing the DCK procedure, (see clause 8.27)
	<Cipher key number>	0	Value 8 used in storing the DCK procedure, (see clause 8.27)
	< Default Cipher Key Index>	all	Contains default cipher key index in case DEF bit is set
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	16	Length of RS (128 bits)
	<RS Field>	All	Authentication parameter RS_{128} (see ETSI EN 300 175-7 [7])

Table 88: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_P (64 bits)
	<RAND Field>	All	Authentication parameter RAND_P (see ETSI EN 300 175-7 [7])
<<RES>>			
	Length of Contents (L)	4	Length of RES1 (32 bits)
	<RES Field>	All	Authentication parameter RES1 (see ETSI EN 300 175-7 [7])
<<ZAP field>>			
	<Contents field>	0-15	M if stored else O. Associated to feature [N.16]
<<Service class>>			
	<Service class field>	1-6	M if stored else O. Associated to feature [N.14]

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.

NOTE 2: The derived ciphering key when DSAA2 is used has a length of 128 bits.

8.45.7.1 Associated procedure

8.45.7.1.1 Timer F-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.45.7.2 Exceptional cases

8.45.7.2.1 Authentication algorithm/key not supported

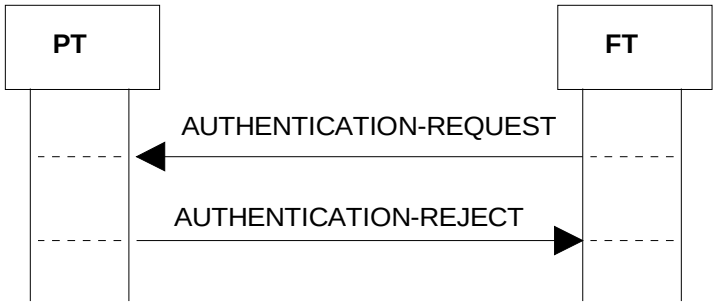


Figure 88: Authentication algorithm/key not supported by the PT

For the contents of the {AUTHENTICATION-REJECT} message see table 81.

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

8.45.7.2.2 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.

8.45.7.2.3 PP Authentication failure (authentication challenge RES1 has wrong value)

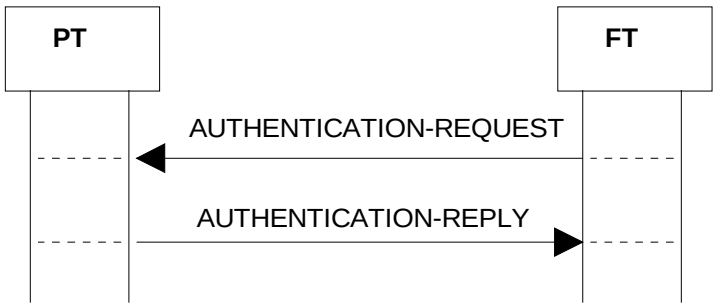


Figure 89: Authentication challenge RES1 has wrong value

Any failure of the procedure (PP authentication failure) shall result on the interruption of any call in progress between both peers. Either, the normal call release procedure (clause 8.7) FT initiated (figure 22) or the abnormal call release procedure (clause 8.8), FT initiated (figure 28) may be used. The release reason IE shall be included in the {CC-RELEASE} or {CC-RELEASE-COM} messages with the values either "Authentication failed" or "Encryption Activation Failed".

8.45.8 Authentication of user using DSAA2

8.45.8.0 Procedure

The procedure relates to the feature Authentication of user [N.10] when the feature N.36 (AES/DSAA2 authentication) is supported and the DECT Standard Authentication Algorithm #2 (DSAA2) is used.

NOTE: See also clause 8.25 describing the authentication of the user using the DECT Standard Authentication Algorithm (DSAA).

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.3.2 and ETSI EN 300 175-7 [7], clause 4.3.5.

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

This procedure is equivalent to the authentication of PT procedure defined in clause 8.45.7 with the following replacement to the {AUTHENTICATION-REQUEST} message.

Table 89: 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".

8.45.8.1 Associated procedure

8.45.8.1.1 Timer F-<MM_auth.2> management

<MM_auth.2>: authentication of user timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.45.8.2 Exceptional cases

8.45.8.2.1 Authentication algorithm/key not supported

This procedure is equivalent to the procedure defined in clause 8.24.2.1.

8.45.8.2.2 Timer F-<MM_auth.2> expiry

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

8.45.9 Key allocation using DSAA2

8.45.9.0 Procedure

The procedure relates to the feature On air key allocation [N.12] when the feature N.36 (AES/DSAA2 authentication) is supported and the DECT Standard Authentication Algorithm #2 (DSAA2) is used.

NOTE: See also clause 8.32 describing the Key allocation using the DECT Standard Authentication Algorithm (DSAA).

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

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.6 and ETSI EN 300 175-7 [7], clause 6.5.6.3 with the following specific provisions:

- The PT shall support the key allocation procedure prior to the completion of the obtaining access rights procedure even if the IPUI/PARK pair may not have been provided yet.
- The key allocation procedure consists of only one MM transaction.
- This procedure shall only be initiated by the FT if the PT has indicated the support of DSAA2 in Terminal Capability information.
- Authentication type 2 procedure, as defined by ETSI EN 300 175-7 [7], clauses 6.3.6, 6.3.7, 6.3.3.3, 6.3.3.4, 6.5.2.3 and 6.5.2.4 shall be used for both PT and FT authentications.
- A algorithm, DSAA2 based, shall be used for all security processes as defined by ETSI EN 300 175-7 [7], clause 5.1.1.2.
- RAND_F parameter shall be used as input D2 of authentication process A12 and exchanged FT to PT at the {KEY-ALLOCATE} message.
- A second RAND_F parameter shall be used as input D3 of authentication process A22 and exchanged FT to PT at the {AUTHENTICATION-REPLY} message.
- A single RAND_P parameter shall be exchanged PT to FT at the {AUTHENTICATION-REQUEST} message and used as input D3 of authentication process A12 and as input D2 of authentication process A22.
- RS parameter shall have 128 bits (RS_{128}). Two independent RS_{128} parameters shall be exchanged FT to PT for use by the PT authentication (process A11) and by the FT authentication (process A21).
- Authentication process A21 shall be necessarily run at both sides for the execution of the procedure.
- On the other hand, execution of process A11, or reusing of previously generated RS_{128} / KS pair for PT authentication is up to the implementation.
- Any PT or FT authentication failure shall result on the no acceptance of the allocated key. The procedure shall continue as indicated in clauses 8.45.9.2.4 (PT authentication fails) or 8.45.9.2.5 (FT authentication fails).
- See clause 6.9.6 for coexistence rules between MM procedures and CC states.

Figure 90 and tables 90, 91 and 92, together with the associated clauses define the mandatory requirements with regard to the present document.

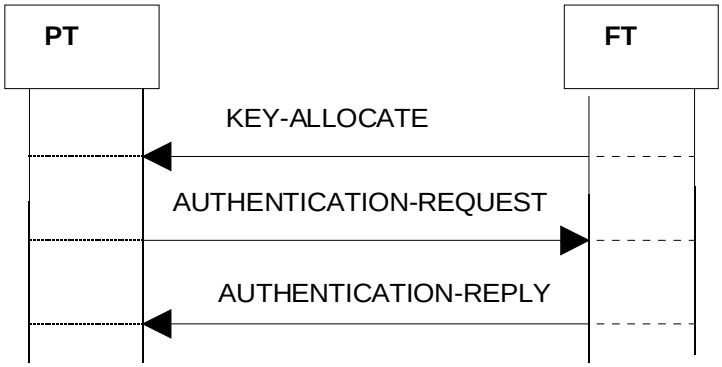


Figure 90: Key allocation using DSAA2

Table 90: 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>	2	DSAA2
	<UAK number>	8	Keys relate to IPUI/PARK pair, if available
	<AC number>	8	Keys relate to IPUI/PARK pair, if available
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	16	Length of RS (128 bits)
	<RS Field>	All	Authentication parameter RS_{128} (see ETSI EN 300 175-7 [7])

Table 91: 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>	2	DSAA2
	<Auth key type>	4	AC, Length shall 7always 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>>			
	Length of Contents (L)	8	Length of RAND_P (64 bits)
	<RAND Field>	All	Authentication parameter RAND_P used for both, PT and FT authentication. (see ETSI EN 300 175-7 [7])
<<RES>>			
	Length of Contents (L)	4	Length of RES1 (32 bits)
	<RES Field>	All	Authentication parameter RES1 (see ETSI EN 300 175-7 [7])

The value RES1 is computed by the PT from RAND_F and KS (computed from current K (AC) and RS_{128}). 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 92: Values used within the {AUTHENTICATION-REPLY} message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<RAND>>			
	Length of Contents (L)	8	Length of RAND_F (64 bits)
	<RAND Field>	All	Authentication parameter RAND_F used for the FT authentication (see ETSI EN 300 175-7 [7])
<<RES>>			
	Length of Contents (L)	4	Length of RES2 (32 bits)
	<RES Field>	All	Authentication parameter RES2 (see ETSI EN 300 175-7 [7])
<<RS>>			
	Length of Contents (L)	16	Length of RS (128 bits)
	<RS Field>	All	Authentication parameter RS_{128} used for the FT authentication (see ETSI EN 300 175-7 [7])

The value RES2 is computed by the FT from RAND_P, the second RAND_F and the second RS_{128}. 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.

8.45.9.1 Associated procedures

8.45.9.1.1 Timer F-<MM_key.1> management

<MM_key.1>: key allocation timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {KEY-ALLOCATE} message is sent or an 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.

8.45.9.1.2 Timer P-<MM_auth.1> management

<MM_auth.1>: authentication timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: an {AUTHENTICATION-REQUEST} message is sent or an 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 an interrupting higher priority transaction begins.

8.45.9.2 Exceptional cases

8.45.9.2.1 Timer F-<MM_key.1> expiry

Upon expiry of F-<MM_key.1> FT shall consider the procedure as failed. FT shall not re-transmit 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.

8.45.9.2.2 Timer P-<MM_auth.1> expiry

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

8.45.9.2.3 Allocation-type element is unacceptable

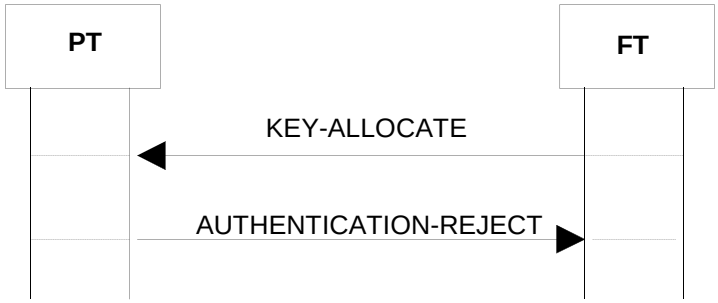


Figure 91: Allocation-type unacceptable for PT

Table 93: Standard 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

8.45.9.2.4 Authentication of PT fails

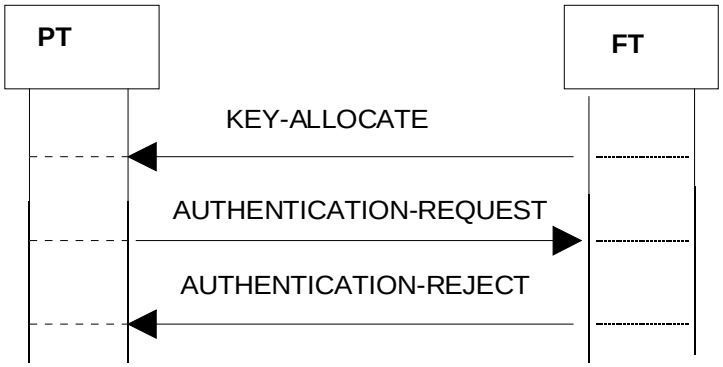


Figure 92: Authentication of PT fails

Table 94: Standard values used within the {AUTHENTICATION-REJECT} message

Information element	Field within the information element	Standard values within the field/information element	Comments	Normative actions
			All optional	

8.45.9.2.5 Authentication of FT fails

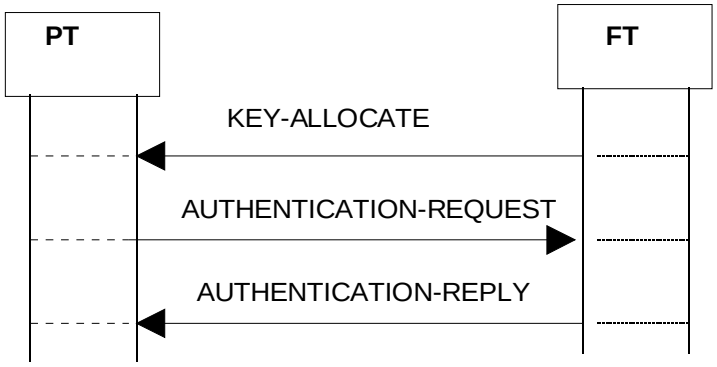


Figure 93: Authentication of FT fails

If the Authentication of FT fails, as XRES2 ≠ RES2, the KS' shall not be 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.

8.45.10 Cipher-switching initiated by FT using DSC2

8.45.10.0 Procedure

This procedure relates to the feature Encryption activation FT initiated [N.17] and Enhanced Security [N.35] as well as to feature Encryption deactivation FT initiated [N.28] when feature N.36 (AES/DSAA2 authentication) and service M.17 (AES/DSC2 encryption) are supported.

NOTE 1: The support of AES/DSAA2 authentication (feature N.36) is a prerequisite for the support of AES/DSC2 encryption (MAC service M.17) for devices compliant with the present document.

NOTE 2: See also clause 8.33 describing the Cipher-switching initiated by FT when the DECT Standard Cipher (DSC) is used.

This procedure shall only be initiated by the FT if the PT has indicated the support of DSC2 in Terminal Capability information.

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.8 and ETSI EN 300 175-7 [7], clause 6.5.3.

The following text together with figure 94, figure 95, table 95, table 96 and the associated clauses define the mandatory requirements with regard to the present document.

Figure 94: Cipher - switching initiated by FT

Table 95: 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.28]
		1	Enable ciphering respectively performing re-keying
	<Cipher-algorithm-id>	2	DECT Standard Cipher algorithm #2 (DSC2)
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= subscription)

In case the encryption is disabled, the {CIPHER-REQUEST} shall be sent before the transfer of any C-plane data intended to be encrypted (e.g. dialled number).

{CIPHER-REQUEST} may also be sent in case early encryption is active (clause 8.45.3), or in case the encryption key of an already encrypted connection shall be changed by means of re-keying (clause 8.45.2).

The DCK shall be produced and stored in advance using the storing the DCK procedure (see clause 8.27). In order for the encryption mechanism to be activated (respectively switched to a new DCK) 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, unless a re-keying is initiated by sending DL_ENC_KEY-req primitive to the DLC layer.

In order to use this procedure, the authentication of the PT shall have been performed using the DSAA2 procedure according to clause 8.45.7. The generated key has a length of 128 bits.

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. Respectively, the re-keying shall be invoked at MAC layer.

8.45.10.1 Associated procedure

8.45.10.1.1 Timer F-<MM_cipher.1> management

<MM_cipher.1>: cipher-switching timer;

value: refer to ETSI EN 300 175-5 [5], annex A;

start: a {CIPHER-REQUEST} message is sent;

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

8.45.10.2 Exceptional cases

8.45.10.2.1 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.

If the feature N.35 and the NWK layer procedure "Encryption of all calls" is supported, then the FT shall release the call on reception of a CIPHER-REJECT message as described in clause 8.45.1.

In any other case, the FT should not release the call on reception of a CIPHER-REJECT message.

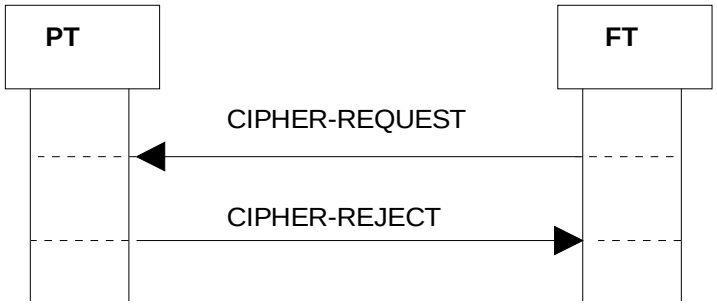


Figure 95: PT rejects the cipher request

Table 96: 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	

8.45.10.2.2 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 re-transmit 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.

The FT should not release the call on Timer F-<MM_cipher.1> expiry.

8.45.11 Cipher-switching initiated by PT using DSC2

8.45.11.0 Procedure

The procedure relates to the feature Encryption activation PT initiated [N.27] and Encryption deactivation PT initiated [N.29] when feature N.36 (AES/DSAA2 authentication) and service M.17 (AES/DSC2 encryption) are supported.

NOTE 1: The support of AES/DSAA2 authentication (feature N.36) is a prerequisite for the support of AES/DSC2 encryption (MAC service M.17) for devices compliant with the present document.

NOTE 2: See also clause 8.34 describing the Cipher-switching initiated by PT when the DECT Standard Cipher (DSC) is used.

This procedure shall only be initiated by the PT if the FT has indicated the support of DSC2 in Extended Higher Layer capabilities (part 2) FP broadcast.

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.8 and ETSI EN 300 175-7 [7], clause 6.5.3.

The following text together with figure 96, figure 97, table 97, table 98 and the associated clauses define the mandatory requirements with regard to the present document.

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

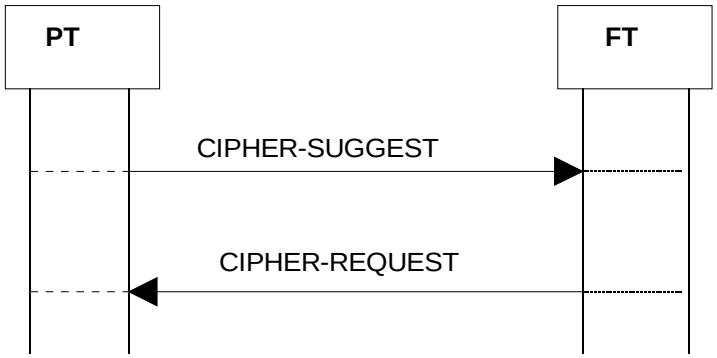


Figure 96: Ciphering, PT initiated

Table 97: 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.29]
		1	Enable ciphering. Relates to feature [N.27]
	<Cipher-algorithm-id>	2	DSC2
	<Cipher key type>	9	DCK
	<Cipher key number>	8	Always IPUI/PARK pair (= Subscription)

Table 98: 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.29]
		1	Enable ciphering. Relates to feature [N.27]
	<Cipher-algorithm-id>	2	DSC2
	<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 clause 8.27). 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.

In order to use this procedure, the authentication of the PT shall have been performed using the DSAA2 procedure according to clause 8.45.7. The derived ciphering key has a length of 128 bits.

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 clause 8.45.10 and the associated clauses).

8.45.11.1 Associated procedure

8.45.11.1.1 Timer P-<MM_cipher.2> management

<MM_cipher.1>:cipher-switching timer;

value: refer to ETSI EN 300 175-5 [5], 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.

8.45.11.2 Exceptional cases

8.45.11.2.1 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.

If the feature N.35 and the NWK layer procedure "Encryption of all calls" is supported, then the PT shall release the call on reception of a CIPHER-REJECT message as described in clause 8.45.1.

In any other case, the PT should not release the call on reception of a CIPHER-REJECT message.

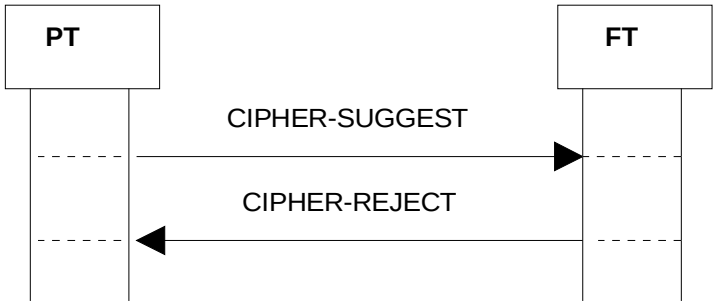


Figure 97: FT rejects the cipher requests

Table 99: 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	

8.45.11.2.2 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 re-transmit 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.

8.45.12 Additional procedures for devices supporting DSC2

8.45.12.1 General

Clause 8.45.12 describes the additional compatibility procedures to be supported by PP and FP implementing the encryption algorithm DSC2.

NOTE: See ETSI EN 300 700 [12] for the additional procedures for CRFPs.

8.45.12.2 Support of additional octet in <<AUTH-TYPE>>

PPs and FPs supporting DSC2 shall support the inclusion of the optional octet 5c in IE <<AUTH-TYPE>> as defined in ETSI EN 300 175-5 [5], clause 7.7.4. Such octet shall be inserted by the FP if the PP supports DSC2 and the authentication operation generates a Default Cipher Key.

FPs supporting DSC2 shall support the exchange and request of Default Cipher Keys by CRFPs using the <Key-type> "Default Cipher Key (DefCK) for DSC2" and the associated <<Key>> format as described in ETSI EN 300 175-5 [5], clause 7.7.24. This procedure is only used in operations between FPs and CRFP.

9 DLC layer procedures

9.1 Class A link establishment

9.1.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clause 9.2.3.1. The following text together with the associated clauses 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 ETSI EN 300 175-4 [4], clause 9.2.4.3.1 b).

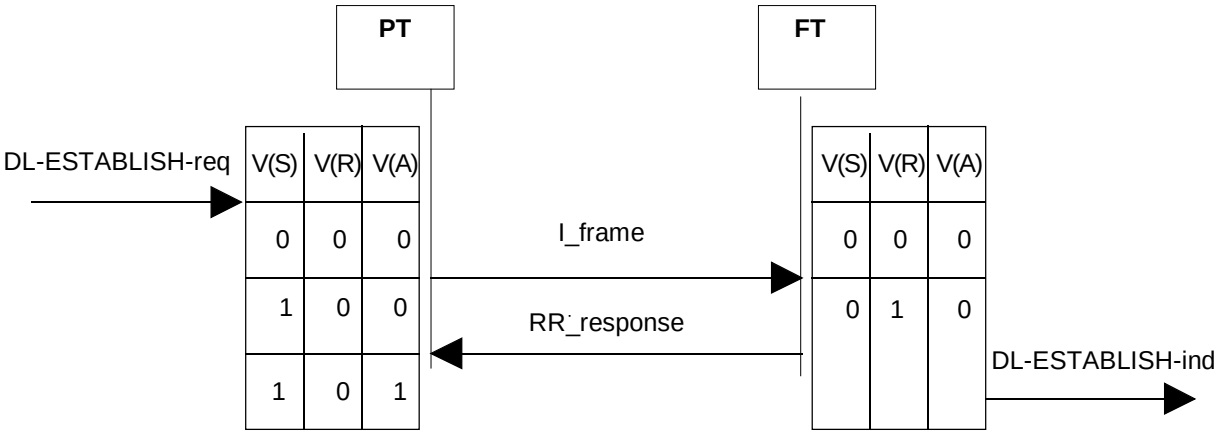


Figure 98: Class A link establishment

Table 100: 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 C_S 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 ETSI EN 300 175-4 [4], clause 10.3.1; underlying checksum calculation based on ISO/IEC 8073 [i.6]
<<Checksum field2>>		All	See above

Table 101: 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 ETSI EN 300 175-4 [4], 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 Re-transmission counter management

Refer to ETSI EN 300 175-4 [4], clauses 9.2.3.1 and 9.2.3.6.

Each LAPC entity shall maintain an internal Re-transmission count variable determining the maximum number of re-transmissions of an I_frame. The default value shall be 3.

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

9.1.1.3 Multiple frame operation variables management

Refer to ETSI EN 300 175-4 [4], clause 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 ETSI EN 300 175-4 [4], clause 10.2 and ETSI EN 300 175-3 [3], clause 8.1.1. The following text together with the associated clauses 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.

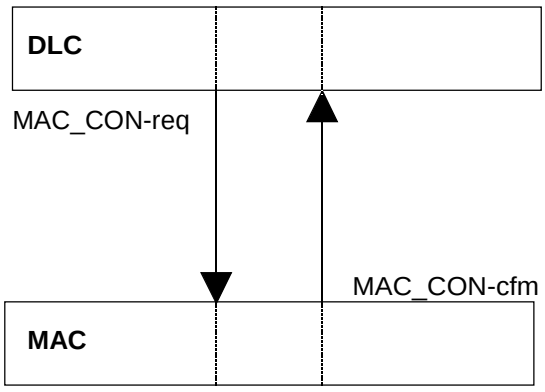


Figure 99: Establishment of a MAC connection initiating side

Table 102: Values used within the MAC_CON-req primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to ETSI EN 300 175-4 [4], clause 10.2.4.4
<<PMID>>	Portable part MAC Identity (PMID)	(see clause 13.4)
<<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 103: Values used within the MAC_CON-cfm primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to ETSI EN 300 175-4 [4], clause 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.

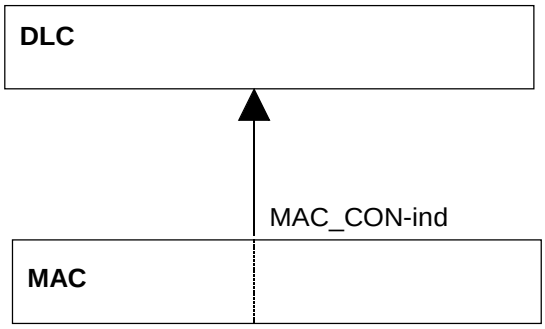


Figure 100: Establishment of a MAC connection receiving side

Table 104: Values used within the MAC_CON-ind primitive

Parameter	Information within the parameter	Normative action/comment
<<MCEI>>	MAC Connection Endpoint Identifier	Refer to ETSI EN 300 175-4 [4], clause 10.2.4.4
<<PMID>>	PMID	(see clause 13.4)
<<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 finds 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 ETSI EN 300 175-4 [4], clause 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 clause 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 Acknowledged Information transfer

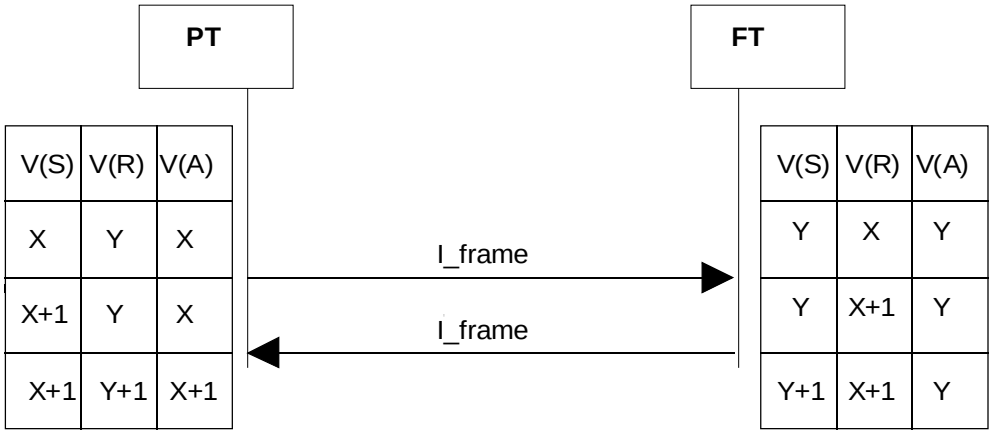
9.2.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clauses 9.2.3.2 to 9.2.3.6. The following text together with the associated clauses 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 an RR_frame.

9.2.1 Acknowledgement with an I_frame



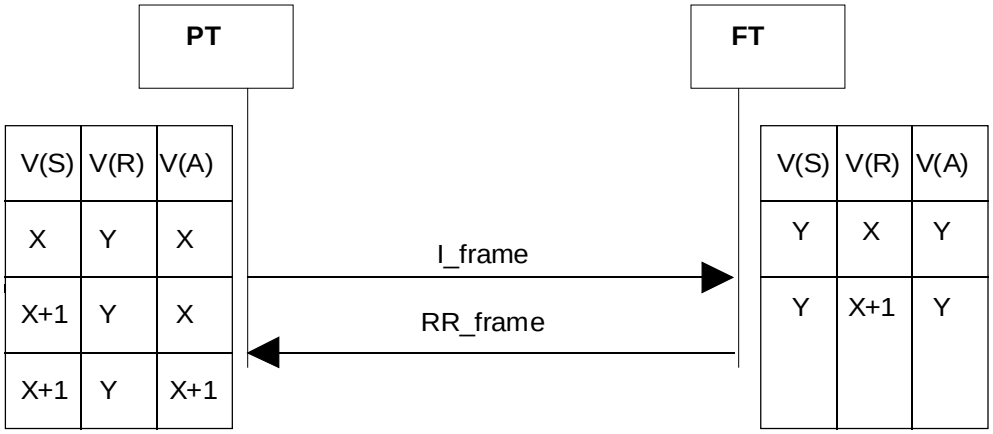
NOTE 1: During the calculation of the variable's values the assumptions have been made that the I_frame sent by PT is not used for acknowledgement of previous received I_frames and, both frames are not re-transmission.
NOTE 2: A Class A acknowledged information transfer procedure is considered as successful 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 101: Class A acknowledge information transfer by I_frame, PT initiated

Table 105: 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 C_S logical channel
<<Checksum field1>>		All	
<<Checksum field2>>		All	

9.2.2 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 re-transmission.
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 102: 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 105).

Table 106: 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	

9.2.3 Class A acknowledged information transfer with segment reassemble

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

9.2.4 Associated procedures

9.2.4.1 Timer <DL.04> management

DL.04>: re transmission timer;

value: refer to ETSI EN 300 175-4 [4], 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.

9.2.4.2 Re-transmission counter management

Refer to clause 9.1.1.2.

9.2.4.3 Multiple frame operation variables management

Refer to clause 9.1.1.3.

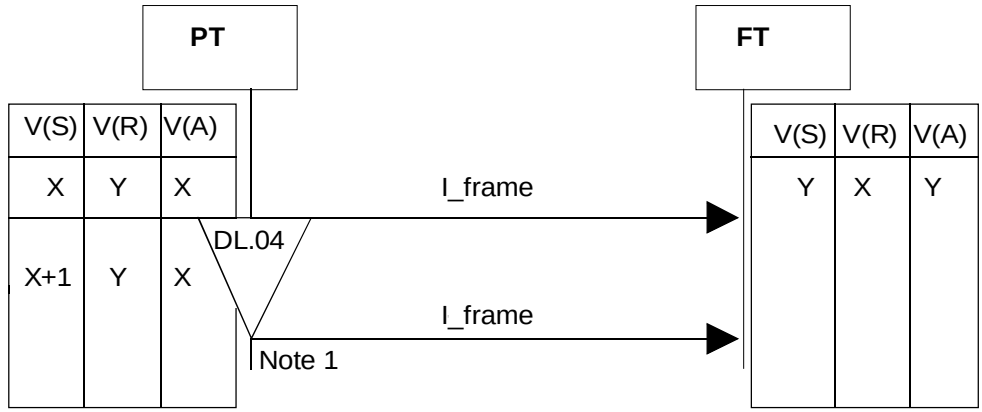
9.2.5 Exceptional cases

9.2.5.1 Timer <DL.04> expiry

Refer to ETSI EN 300 175-4 [4], clause 9.2.3.6.

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

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



NOTE 1: The I_frame is re-transmitted 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 re-transmission.
NOTE 3: The case when FT initiates differs only in the notations.
NOTE 4: The contents of the retranslated frame will be exactly the same as the first one.

Figure 103: 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 105).

9.2.5.2 Receipt of a request for link release

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

9.2.5.3 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 clause 9.3) shall be performed.

9.2.5.4 DLC wants to make a connection handover

See class A basic connection handover procedure given in clause 9.7.

9.3 Class A link release

9.3.0 Procedure

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

The procedure for Class A link release is initiated on receipt of a DL_RELEASE-req primitive (see clauses 8.37 and 8.38) 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 ETSI EN 300 175-4 [4], clause 10.4.2.

9.3.1.2 LLME release a MAC connection

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

9.4 Class A link re-establishment

The procedure shall be performed as defined in of ETSI EN 300 175-4 [4], clause 9.2.3.8 and ETSI EN 300 175-5 [5], clause 17.8. The following text together with the associated clauses 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 clause 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 ETSI EN 300 175-5 [5], clause 14.2.7.

9.5 C_S channel fragmentation and recombination

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clauses 6.1.2 to 6.1.4, 6.1.4.2 and 10.2.5. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

The complete frame shall be fragmented into 5 octet fragments.

9.6 Normal broadcast

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

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

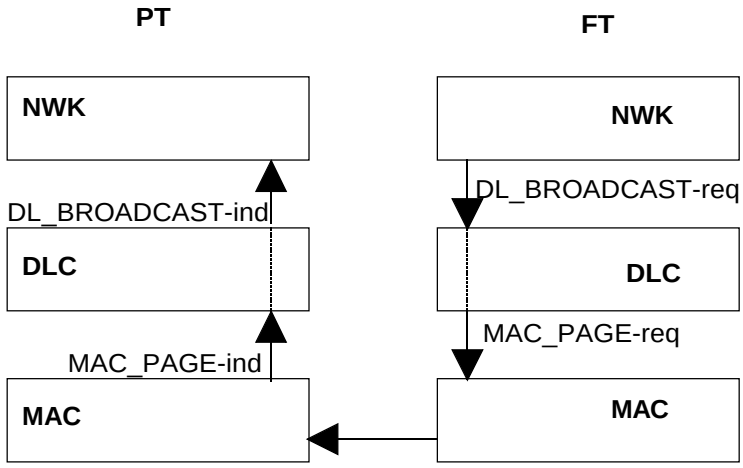


Figure 104: Normal broadcast

Table 107: 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 108: 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 109: Information used within the MAC_PAGE-ind primitive

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

Table 110: 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	

9.7 Class A basic connection handover

9.7.0 Procedure

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

9.7.1 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 setup procedure (see clause 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 clause 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 an implementation complying with 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.

9.7.2 Associated procedure

9.7.2.1 LLME connection handover management

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clause 10.5. The following text together with the associated clauses 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 clause 8.38) or release indication from MAC layer (see clause 9.3).

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

9.7.3 Exceptional case

9.7.3.1 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 clause 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 clause 9.3.1.2).

9.8 Encryption switching

9.8.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clause 10.6, ETSI EN 300 175-7 [7], clauses 6.5.3 and 6.4.6 and ETSI EN 300 175-3 [3], clause 6.2.3. The following text together with the associated clauses 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.9] is supported.

9.8.1 Associated procedure

9.8.1.1 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.

If the KSG supports several algorithms (i.e. DSC and DSC2), the DLC shall provide indication of the algorithm to be used.

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

9.8.2 Exceptional cases

9.8.2.1 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, or fails to switch the encryption key for the re-keying procedure, 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.

9.8.2.2 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 crypted 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.

9.9 U-plane class 0/min delay

9.9.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clauses 11.2, 14.2.3.1 and 14.3.2.

9.9.1 Associated procedure

9.9.1.1 LLME U-plane establishment

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clause 10.4.1. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

On demand from the NWK layer for the connection of the U-plane (see the NWK layer procedures in clauses 8.3 to 8.6 and 8.15) the LLME shall establish a suitable DLC entity and shall associate the DLC entity to the MAC connection already available for the C-plane. The NWK layer entity shall be informed by the LLME of the success of the procedure.

9.10 FU1 frame operation

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clauses 12.1 and 12.2. The following text together with the associated clauses define the mandatory requirements with regard to the present document.

NOTE: The case when FT initiates differs only in the notations.

Figure 105: Sending a FU1 frame

The length of a FU1 frame k = 40 octets (full slot).

One complete frame shall be submitted to/from MAC layer included in a MAC_CO_DATA-req(ind) primitive.

10 MAC layer procedures

10.1 General

The FT and PT shall support In_minimum_delay service as defined in ETSI EN 300 175-3 [3], clause 10.8.3.1.

The FT and PT shall support frame format as follows:

- full slot mode defined in ETSI EN 300 175-3 [3], clause 4.2.2;
- D-field mapping shall support the D-00 and D32 as defined in ETSI EN 300 175-3 [3], clause 6.2.1.1.

The FT and PT shall support A-field mapping A-MAP.

The FT and PT shall understand all A field tail identifications (a0, a1 and a2) in the header field as defined in ETSI EN 300 175-3 [3], clauses 6.2.1.2 and 7.1.2.

The FT and PT shall support the following B-field field identifications (a4, a5 and a6) as defined in ETSI EN 300 175-3 [3], clause 7.1.4:

- U-type: In, "000"B;
- no B-field, "111" B (shall only be used for dummy bearers).

The FT and PT shall support T-MUX as defined in ETSI EN 300 175-3 [3], clause 6.2.2.1.

The FT and PT shall support B-field multiplex E/U MUX type U32a.

The FT and PT shall support scrambling as defined in ETSI EN 300 175-3 [3], clause 6.2.4.

The FT and PT shall provide R-CRC generation and checking as defined in ETSI EN 300 175-3 [3], clause 6.2.5.2. The FT and PT shall provide X-CRC generation and checking as defined in ETSI EN 300 175-3 [3], clauses 6.2.5.3 and 6.2.5.4.

The PT shall support the normal duty cycle idle_locked mode as defined in ETSI EN 300 175-3 [3], clauses 4.3.1 and 11.3.

The FT and PT shall support primary scan procedure as defined in ETSI EN 300 175-3 [3], clause 11.8.

10.2 Downlink broadcast

10.2.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clause 9.1.1.

10.2.1 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 ETSI EN 300 175-3 [3], clause 7.2.2.

Table 111: 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 [M.13]
	<PARI>	All	
	<RPN>	All	

10.2.2 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 ETSI EN 300 175-3 [3], clause 7.2.3.2.

Table 112: 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 to 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 to 1 023	The PT shall not use carriers which are not supported
	<SPR>	0	PT may ignore
	<CN>	0 to 9	PT shall support all values
	<SPR>	0	PT may ignore
	<PSCN>	0 - N	PT shall support values 0 - 9

10.2.3 Q_T - FP capabilities

10.2.3.0 Q_T - FP capabilities

If the bit a33 in higher layer capabilities (see table 126) is set to value '1', the PT may assume the values of bits a17, a23 and a27 to be set to value '1'. The FT shall set the respective values to '1'.

Table 113: Values used within FP capabilities

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<FP capabilities>>			
	<Qh>	'3'H	
	<a12>	0,1	Extended FP Info (Q_H = 4). See notes 1 and 2
	<a17>	1	Full slot
	<a23>	1	Basic A-field setup
	<a27>	1	In minimum delay
NOTE 1: Bit a12 is only required to be set to '1' by FP implementations supporting the procedures in clause 8.45.2 "Re-keying during a call" and clause 8.45.3 "Early encryption". NOTE 2: Only PP implementations supporting the procedures in clause 8.45.2 "Re-keying during a call" and clause 8.45.3 "Early encryption" need to understand bit a12 set to '1'. All others may assume bit a12 as set to '0'.			

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 clause 13.6.1.

10.2.3.1 Q_T - Extended FP capabilities

If the bit a12 in FP capabilities (see table 113) is set to value '1', then, the FT shall set and the PT may assume "Extended higher layer capabilities" as shown in table 114. If the bit a12 in FP capabilities (see table 113) is set to value '0', then, the PT shall assume that "Extended higher layer capabilities" is not present.

NOTE: Only FP implementations supporting the procedures 8.45.2 "Re-keying during a call" and 8.45.3 "Early encryption" are required to broadcast the Q_T - Extended FP capabilities.

Table 114: 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'H	
	<a23>	1	Extended FP Info part 2

Higher layer information: no extended higher layer capabilities bits are is in use by the present document.

10.2.3.2 Q_T - Extended FP capabilities (part 2)

If the bit a12 in FP capabilities (see table 113) and the bit a23 in Extended FP capabilities (see table 114) are set to value '1', then, the FT shall set the "Extended FP capabilities (part 2)" as shown in table 115. If the bit a12 in FP capabilities (see table 113) is set to value '0', then, the PT shall assume that "Extended FP capabilities (part 2)" is not present.

NOTE 1: Only FP implementations supporting the procedures 8.45.2 "Re-keying during a call" and 8.45.3 "Early encryption" are required to broadcast the "Q_T - Extended FP capabilities (part 2)".

NOTE 2: Only PP implementations supporting the procedures 8.45.2 "Re-keying during a call" and 8.45.3 "Early encryption" need to understand "Q_T - Extended FP capabilities (part 2)".

Table 115: Values used within Extended FP capabilities (part 2)

MAC message	Field within the message	Standard values within the MAC message	Normative action/comment
<<FP capabilities>>			
	<Qh>	'C'H	

Higher layer information: for the setting of the extended higher layer information (part 2) bits see clause 13.6.3.

NOTE 3: Only the bits a42 (Support of "Re-keying" and "early encryption"), a43 (DSAA2 supported) and a44 (DSC2 supported) in extended higher layer capabilities (part 2) are used by the present document.

10.2.4 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 ETSI EN 300 175-3 [3], clause 7.2.3.6, and ETSI EN 300 175-6 [6], clauses 5.5, 5.5.1, 5.5.3 and 5.5.4.

This is relevant if the N_T message indicates SARI support.

Table 116: 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	

10.3 Paging broadcast

10.3.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clause 9.1.3.

10.3.1 Short page, normal/extended paging

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.4 shall be supported by the PT and the FT.

Table 117: 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, 5 and 9	The PT shall support values 1, 2, 5, and 9. FT shall support value 1 (see clause 10.3.3) if blind slot information available. The FT shall support value 9 (see clause 10.3.4) if bearer handover information available. Other values need not be supported by FT or PT
	<MAC layer information>	Corresponding information	Information type defined in the previous field

10.3.2 Zero page, normal/extended paging

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.4 in the zero page message shall be supported by the PT and the FT.

Table 118: 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, 5 and 9	The PT shall support values 1, 2, 5 and 9. FT shall support value 1 (see clause 10.3.3) if blind slot information available. The FT shall support value 9 (see clause 10.3.4) if bearer handover information available. Other values need not be supported by FT or PT
	<MAC layer information>	Corresponding information	Information type defined in the previous field

10.3.3 Blind slot information

It is mandatory for RFPs that have blind slots, due to non-duplex bearer operation on that slot (i.e. those RFPs that have technological limitations such as a slow synthesizer), 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 setup 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.

10.3.4 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 10 s).

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 117 and 118): "0000", "0001", "0010" and "0011".

10.4 Setup of basic connection, basic bearer setup (A-field)

10.4.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clauses 10.2.4.2 and 10.5.1.1.

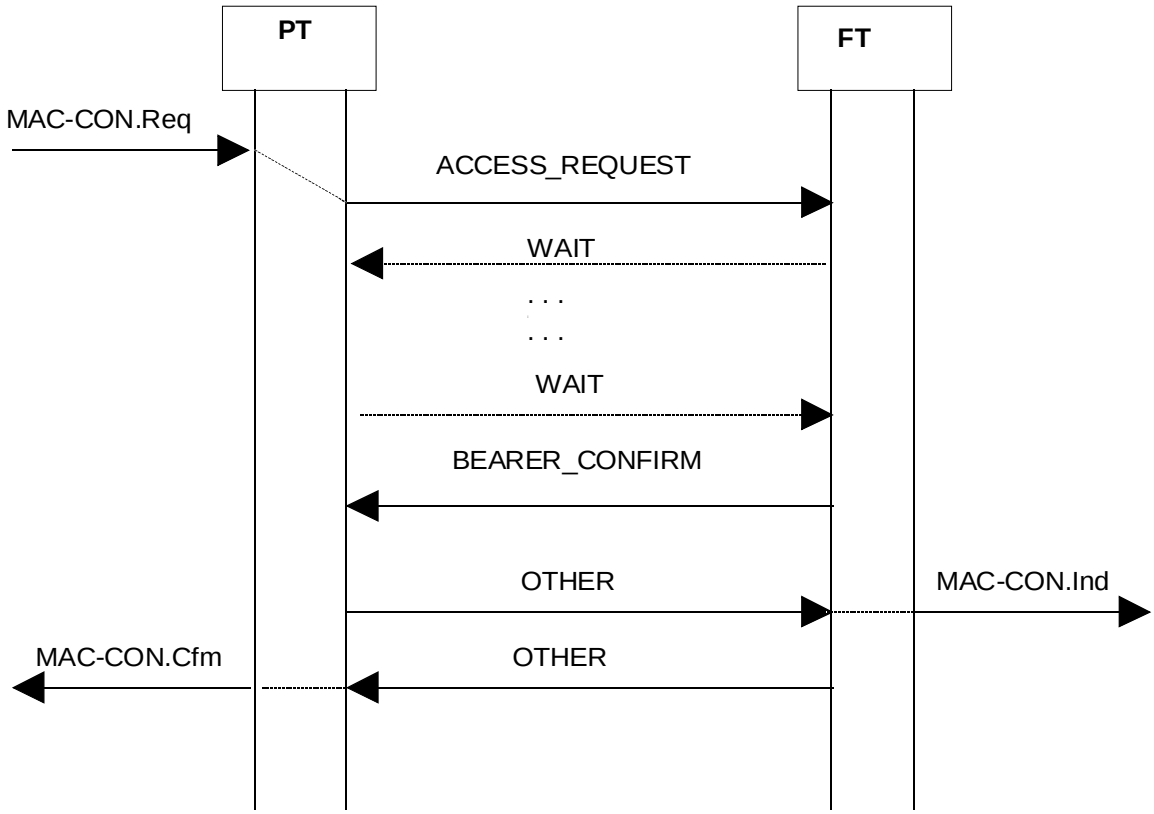


Figure 106: Setup of basic connection and bearer

10.4.1 M_T message

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.5.2 of in the MAC control (M_T) message shall be supported by the PT and the FT.

Table 119: 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>	0	"Access_request"
		4	"Bearer_confirm"
		5	"Wait"
	<FMID>	All	
	<PMID>	All	(see clause 13.4)

10.4.2 Associated procedures

10.4.2.1 Timer T200 management

T200: connection setup timer;

value: refer to ETSI EN 300 175-3 [3], annex A;

start: at the creation of a MBC;

stop: the TBC reports "bearer_established" or on request for MAC connection release.

10.4.2.2 Counter N200 management

N200: max. number bearer setup re attempts during connection setup;

value: refer to ETSI EN 300 175-3 [3], annex A;

start: ACCESS_REQUEST is sent;

change: a new ACCESS_REQUEST within the same connection setup attempt is sent;

clear: the TBC reports "bearer_established" or on request for MAC connection release.

10.4.3 Exceptional cases

10.4.3.1 Bearer setup attempt fails N200+1 times

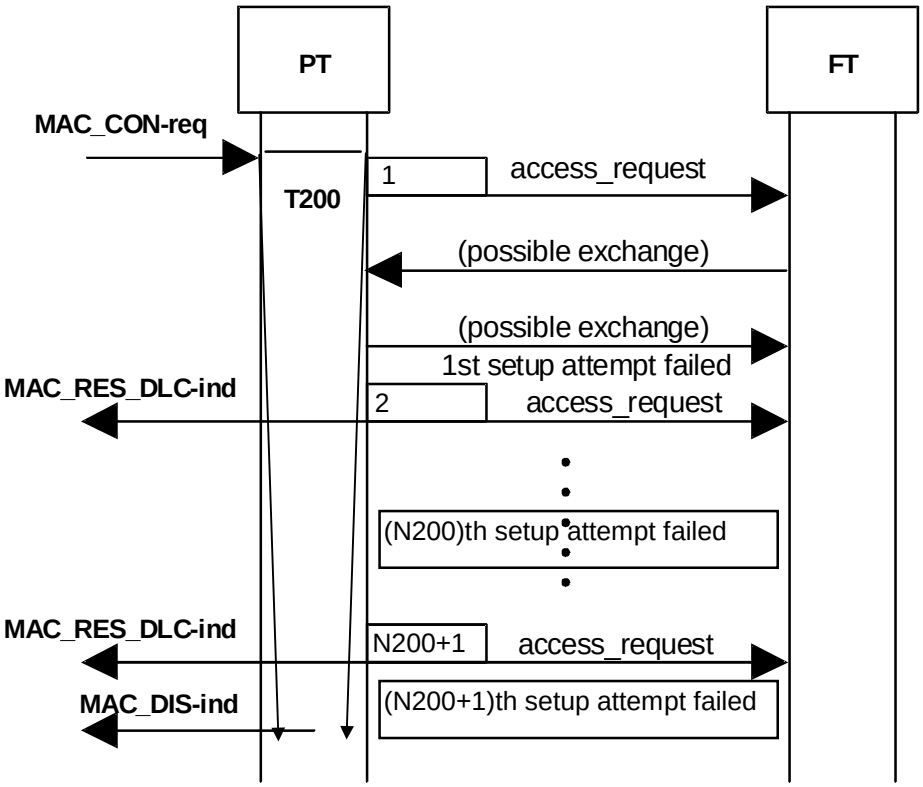


Figure 107: Bearer setup attempt fails N200+1 times

10.4.3.2 Timer T200 expiry

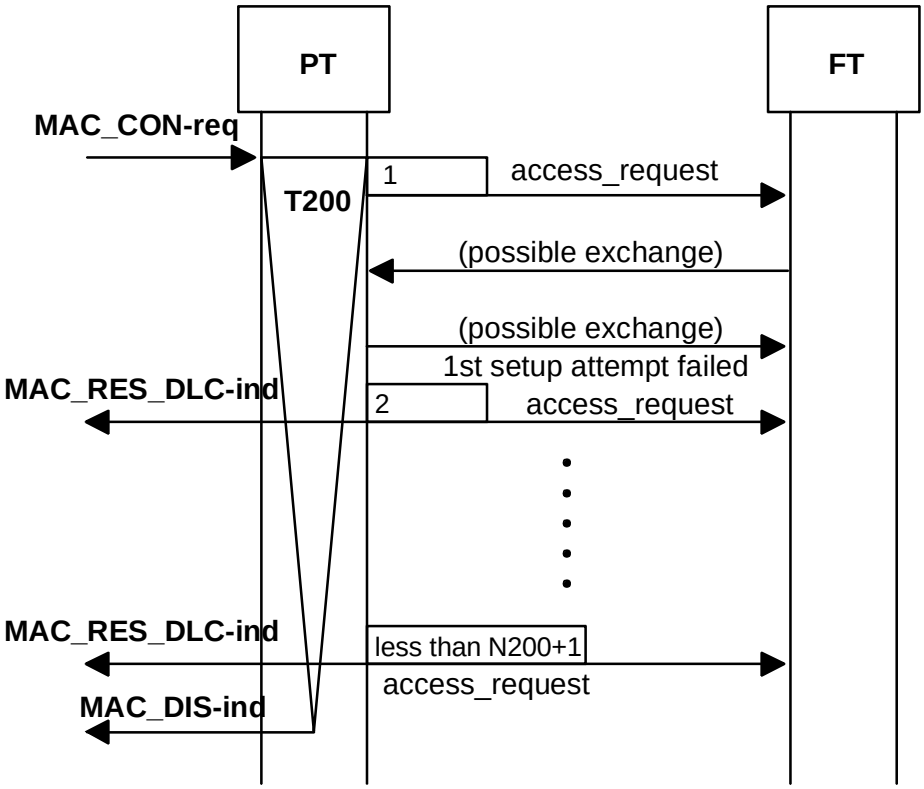


Figure 108: Timer T200 expiry

10.5 Connection/bearer release

10.5.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clauses 10.4 and 10.7.2.1.

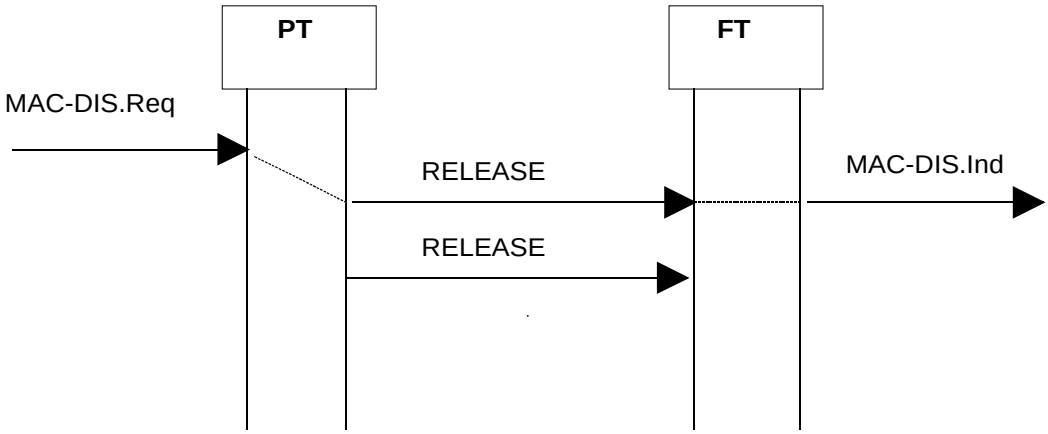


Figure 109: Bearer release

10.5.1 M_T message

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.5.2 in the MAC control (M_T) message shall be supported by the PT and the FT.

Table 120: 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 clause 13.4)

10.6 Bearer handover request

10.6.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clauses 10.6.2 and 10.5.1.1.

The procedure is equivalent for intra- and inter-cell handover.

The FT should not release the old bearer within 10 ms after the establishment of the new bearer.

10.6.1 M_T message

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.5.2 in the MAC control (M_T) message shall be supported by the PT and the FT.

Table 121: 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>	1	"Bearer_handover_request"
		4	"Bearer_confirm"
		5	"Wait"
	<FMID>	All	
	<PMID>	All	(see clause 13.4)

10.7 Connection handover request

10.7.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clauses 10.2.4.2 and 10.5.1.1.

The procedure is equivalent for intra- and inter-cell handover.

10.7.1 M_T message

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.5.2 in 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>	0	"Basic connection control"
	<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 clause 13.4)

10.8 C_S channel data

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clause 10.8.1.1.

10.9 Q2 bit setting

The procedure shall be performed for C_S channel as defined in ETSI EN 300 175-3 [3], clause 10.8.1.3.1.

10.10 RFPI handshake

The procedure shall be performed as defined in ETSI EN 300 175-3 [3], clause 11.5.1. The FT shall ignore the received E-bit.

10.11 Antenna diversity

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

10.12 Sliding collision

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

10.13 Encryption process - initialization and synchronization

The encryption procedure shall be performed as defined in ETSI EN 300 175-7 [7], clauses 6.4.4 and 6.4.5. The control procedures described in clause 6.4.6 of [7] shall be supported. The modifications described in clauses 6.4.8 to 6.4.11 of [7] shall be supported when applicable.

DSC or DSC2 (if service M.17 supported by both peers) algorithms may be used.

Encryption shall be applied for the logical C_S and I_N channels.

The FT shall (if encryption is provided by the FT) support broadcast of multiframe number as defined in ETSI EN 300 175-3 [3], clauses 7.2.3.7 and 9.1.1. The multiframe shall be synchronized between the RFPs in the whole FP area.

Table 123: Values used within Q_T 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}

10.14 Encryption mode control

10.14.0 Procedure

The procedure shall be performed as defined in ETSI EN 300 175-7 [7], clause 6.4.6.

10.14.1 M_T message

The following fields as defined in ETSI EN 300 175-3 [3], clause 7.2.5.7 in the MAC control (M_T) message shall be supported by the PT and the FT.

Table 124: 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.14] is implemented
		5	Stop Encryption Confirm. The support of this code is mandatory only if service [M.14] is implemented
		6	Stop Encryption Grant. The support of this code is mandatory only if service [M.14] is implemented
		8	Start encryption with cipher key-index request. The support of this code is mandatory if [M.16] is implemented
		9	Start encryption with cipher key-index confirm. The support of this code is mandatory if [M.16] is implemented
		'A'H	Start encryption with cipher key-index grant. The support of this code is mandatory if [M.16] is implemented
		'B'H	Start encryption with cipher key-index reject. The support of this code is mandatory if [M.16] is implemented

10.15 Handover encryption process

The procedure shall be performed as defined in ETSI EN 300 175-7 [7], clause 6.4.7.

10.16 Extended frequency allocation

This procedure shall be performed as defined in ETSI EN 300 175-3 [3], clauses 7.2.3.3 and 7.2.3.2.7.

Table 125: 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	
	<RF carriers>	All	
	<RF band>	All	
	<Spare>	0	
	<Number of RF carriers>	All	

10.17 Re-keying

The procedure shall be performed as specified in ETSI EN 300 175-7 [7], clause 6.4.6.5.

10.18 Early Encryption

The procedure shall be performed as specified in ETSI EN 300 175-7 [7], clause 6.4.6.

10.19 AES/DSC2 Encryption

The procedures specified in ETSI EN 300 175-7 [7], clause 6.4 shall apply with the following specific requirements:

- The DECT Standard Cipher #2 (DSC2) algorithm (see ETSI EN 300 175-7 [7], annex M) shall be used in the Key Stream Generator (KSG).
- The Cipher Key used by the KSG shall have 128 bits.

NOTE: This is the size of the DCK generated by DSAA2.

11 Physical Layer (PHL) requirements

11.1 General

As specified in ETSI EN 300 175-2 [2], and ETSI EN 301 406 [11] (replacing ETSI TBR 006 [i.1]).

To carry the speech information, full slots shall be used.

11.2 Minimum Normal Transmit Power (NTP)

The nominal NTP shall be greater than 80 mW per simultaneously active transmitter as shown by the test verdict criteria and declaration of ETSI EN 300 176-1 [9], clause 10.2.3.

11.3 Radio receiver sensitivity

The radio receiver sensitivity shall be -86 dBm, or better.

11.4 Z-field

The Z-field shall be transmitted by RFPs and PTs.

11.5 Sliding collision detection

PT and FT shall be able to detect sliding collision on received packets.

Minimum criteria for sliding collision are defined as S- or Z-field failure. Early sliding collision detection may be supported by other means e.g. signal strength measurements in the guard band.

The Z-field is defined to have failed if the received X- and Z-fields are not identical.

S-field failure is defined with some tolerance in order not to restrict the physical implementation of the word synchronization detector.

S-field failure may be indicated if there are 1 or more bit errors in bits s12 to s31 (errors in bits s0 to s11 shall be ignored). In all cases, S-field failure shall be indicated if 3 or more bit errors occur in bits s16 to s31.

11.6 Physical channel availability

A FP shall be able to receive and transmit on all DECT frequencies f0 to f9 and at least half of the slot pairs 0 to 11.

A PP shall be able to receive and transmit on all DECT frequencies f0 to f9, and shall be able to lock on any slot number 0 to 11, and receive and transmit at least on every slot pair that is not directly neighboured to the slot the PP is locked to, or to a slot on which a traffic bearer is active at the PP.

11.7 Synchronization window

Related to its reference timer, the PP synchronization window shall be at least ±4 bits for bearers to the RFP to which the reference timer is synchronized, and at least ±10 bits for other bearers.

12 Requirements regarding the speech transmission

12.1 General

The applicable requirements specified in ETSI EN 300 175-8 [8] and ETSI EN 300 176-2 [10] (previously covered by ETSI TBR 010 [i.2]) shall be applied.

12.2 User controlled volume control

A user-controlled volume control shall be provided in all GAP PP equipment, except where that equipment incorporates an adaptive volume control in the PP.

When adjusting the volume control from nominal to maximum setting, the decrease in RLRH shall not be less than 6 dB.

13 Management procedures

13.1 Management of MM procedures

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 15.5. The following text together with the associated clauses 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.

13.2 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 shall initiate 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 shall 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 clause 8.28 is always mandatory in the PT except when bit a38 in the broadcast attributes, see table 126, is set to 0.

Location registration shall be initiated immediately after a successful access rights procedure.

13.3 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 126.

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 than within LAs, see ETSI EN 300 175-6 [6], clause 6.3.1, note 2.

13.4 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 setup.

Within a link establishment procedure, the assigned PMID is recalculated for every connection setup attempt (during the connection setup procedure the assigned PMID shall not change); the arbitrary PMID is recalculated for every new bearer setup 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.

13.5 DCK management

The FT is responsible for initiating and storage of a DCK, (see clause 8.27) 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).

13.6 Broadcast attributes management

13.6.0 Procedure

RFPs belonging to the same LA shall broadcast the same values of higher layer attributes (see ETSI EN 300 175-5 [5], 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.

13.6.1 Higher layer capabilities

Table 126: Broadcast attributes interpretation by the Implementation Under Test (IUT) PP: Higher layer capabilities

Bit Number	Attribute	Value	Note
a32	ADPCM/G.726 Voice service	1	
a33	GAP and/or PAP basic speech	1	
a36	DECT Standard authentication (DSAA) required	0,1	
a37	DECT Standard Cipher (DSC) supported	0,1	
a38	Location registration supported	0,1	See location update procedure, clause 8.29 as an exception
a40	Non-static FP	0,1	A FP which is mounted on a moving vehicle
a44	Access Rights requests supported	0,1	The FP can toggle this bit to enable or disable on air subscription, (see annex A)
a46	Connection handover supported	0,1	

13.6.2 Extended higher layer capabilities

No Extended higher layer capabilities bits are used by the present document.

13.6.3 Extended higher layer capabilities (part 2)

Table 127: Broadcast attributes interpretation by the Implementation Under Test (IUT) PP: Extended Higher layer capabilities (part 2)

Bit Number	Attribute	Value	Note
a42	Support of "Re-keying" and "early encryption"	0,1	See clauses 8.45.2 and 8.45.3 in the present document and notes 1 and 2.
a43	DSAA2 supported	0,1	See ETSI EN 300 175-7 [7] and clause 8.45 in the present document.
a44	DSC2 supported	0,1	See ETSI EN 300 175-7 [7], clause 8.45 in the present document and note 3.
NOTE 1: Only FP implementations supporting the procedures 8.45.2 "Re-keying during a call" and 8.45.3 "Early encryption" or supporting the feature N.36 (AES/DSAA2 authentication) are required to broadcast the "Extended Higher layer capabilities (part 2)".			
NOTE 2: Only PP implementations supporting the procedures 8.45.2 "Re-keying during a call" and 8.45.3 "Early encryption" or supporting the feature N.36 (AES/DSAA2 authentication) need to understand the "Extended Higher layer capabilities (part 2)".			
NOTE 3: The support of DECT Standard Cipher #2 (DSC2) requires the support of the DECT Standard Authentication Algorithm #2 (DSAA2).			

13.7 Storage of subscription related data

The data as defined in table 128 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 128: 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	
9	<Service class> field	

The data as defined in table 129 shall be deleted in the PP upon power-down.

Table 129: 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. Last received value in regard to the active IPUI/PARK pair

14 Application procedures

14.1 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.

14.2 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 ETSI EN 300 175-7 [7], clause 4.5.2, AC[0] is defined as the least significant Bit (LSB) as defined above.

14.3 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

Figure 110

This is padded out to 15 bits, with two 0s, 101110010001100, which is 56 214 in octal.

Check is calculated as:

$$1 \times 1 + 2 \times 3 + 3 \times 5 + 4 \times 6 + 5 \times 2 + 6 \times 1 + 7 \times 4 = 1 + 6 + 15 + 24 + 10 + 6 + 28 = 90$$

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	#

Figure 111

14.4 Terminal Identity number assignment in mono cell system

14.4.1 General

In a mono cell system for residential and small office applications, the terminal identity number is the number that can be:

- used by the FT to identify the subscription data related to each PT (i.e. 1 to the maximum number of PT subscribed). The subscription data includes IPUI, PARK, terminal capabilities, etc.;
- displayed by each PP in Idle Locked mode (for example, "DECT 4" if the PP is the 4th PT on the FT);
- used to select the called DECT entity (PP or FP) when initiating Internal Call (for example, "Internal call to PP number 4");
- used to display the calling handset when receiving Internal Call (for example, "Internal call from PP number 4");
- used to select the suppressed PT when removing subscription data related on the FT.

NOTE: For FPs compliant with ETSI TS 102 527-3 [i.3] (NG-DECT Part 3), it is not recommended to use this feature since more advanced mechanisms (list access service) are defined for the same purpose in that specification (see ETSI TS 102 527-3 [i.3]).

14.4.2 Procedure description

At the FP side

The terminal identity number value for the FT shall be 0. The identity number value for a PT should correspond to its subscription records number and should be in the limit (1, maximum number of subscription data on FT).

The terminal identity number shall be assigned by the FT to each PT during the location registration procedure (see clause 8.28), and shall be of 8 bits length. The terminal identity number shall be the least significant bits part of the individual assigned TPUI. The most significant bits shall follow the rules of ETSI EN 300 175-6 [6], clause 6.3.1.

The location registration procedure shall be used, (see clause 8.28) with the following replacement to the {LOCATE-ACCEPT} message.

Table 130: 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>>			
	<Type>	32	TPUI
	<Length of id value>	20	
	<Assignment type>	1	TPUI with number assigned
	<Identity-value>	Values in ETSI EN 300 175-6 [6], clause 6.3.1 are allowed	Only assigned individual TPUIs are allowed

NOTE: According to clause 8.28.2.3 of the present document, PPs not implementing this feature will answer with a {TEMPORARY-IDENTITY-ASSIGN-REJECT} message. FPs implementing this feature (which is not recommended for NG-DECT Part 3 FPs, see note in clause 14.4.1) should be prepared to handle this reject message.

At the PP side

The Identity Number in the PT shall be derived from the individual assigned TPUI received during the location registration procedure (see clause 8.28).

14.4.3 Related Procedures

Internal call "called party"

To select the called DECT entity, the dialled digit including in the <<MULTI-KEYPAD>> information element in the {CC-SETUP} message or in a {CC-INFO} message can be used with the following replacement.

Table 131: Values used within the {CC-INFO} or {CC-SETUP} 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>	IA5 coding of terminal identity number in decimal (see note 2)	Terminal Identity Number of the called part - 0 for FP - 1 to n if PP
		2AH	Internal general call (see note 1)
NOTE 1: This value is used by the PP to request the FP to ring all other PPs and also the FP if capable of. NOTE 2: Example for coding of the Terminal Identity Number in IA5: - For terminal 1, terminal identity number is 0000 0001B, coded value is 31H. - For terminal 14, terminal identity number is 0000 1110B, coded value is 31H 34H.			

Calling Line Indication Presentation (CLIP) Indication

See clause 8.43, "Internal Call Calling line Identification Presentation" (CLIP). The terminal identity number can be used in <<CALLING-PARTY-NUMBER>> information element.

Annex A (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" Q_T 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 clause 13.6).

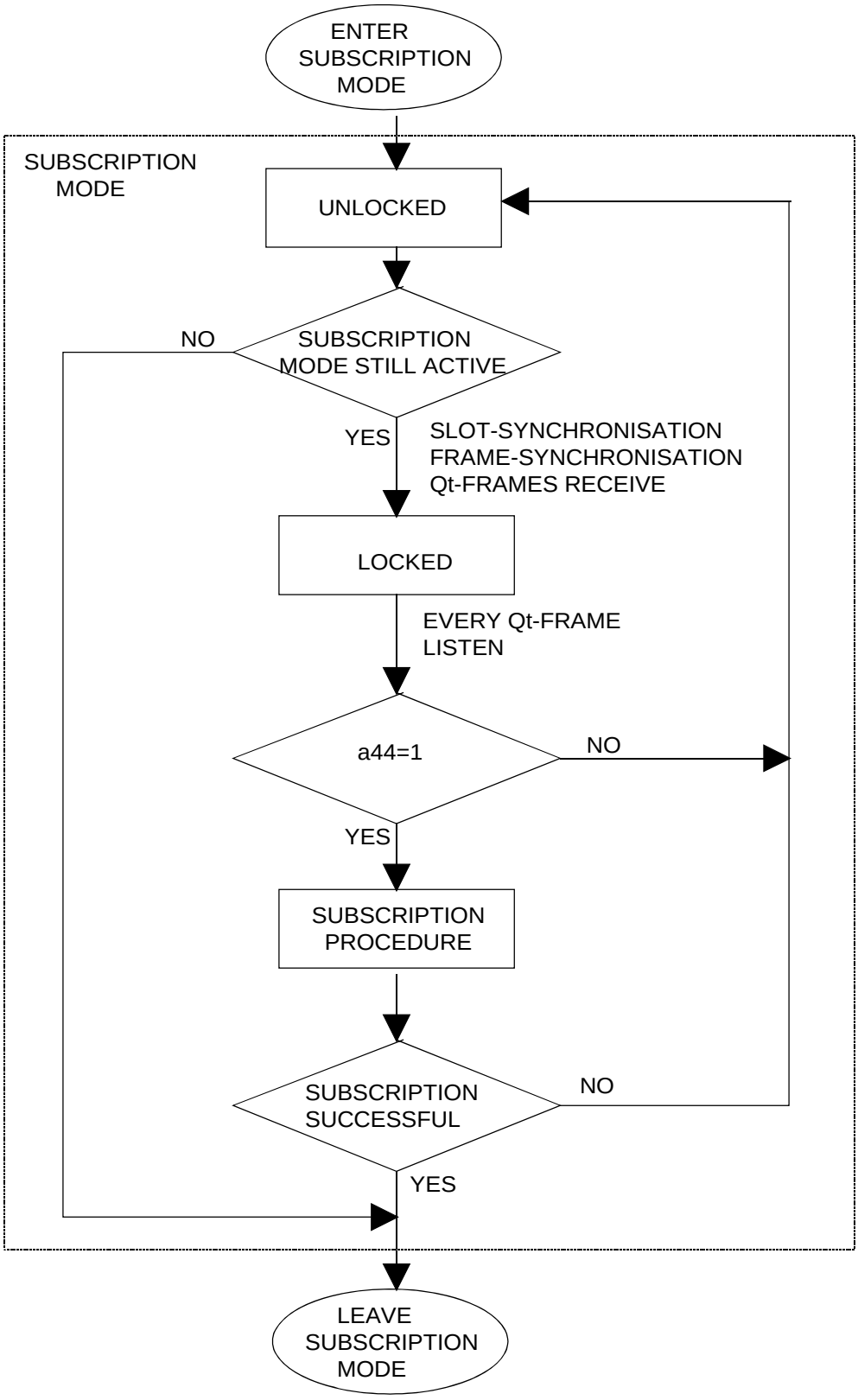


Figure A.1: PP "subscription mode" for MAC layer

Annex B (informative): Tones, progress indicator and U-plane connection

B.1 General

In order to prevent a possible misbehaviour upon receiving the <<Progress indicator>> information element, the connection of the U-plane, and the provision of tones to the GAP PP user, a GAP implementation manufacturer should consider that:

- there may be calls (external) leaving the FP (only the calling side belongs to the particular FP);
- there may be calls (internal) that do not leave the FP (calls between portables within the same FP);
- there may be a GAP FP without local tone provision;
- there may be a GAP PP without local tone provision;
- there may be a Local Network (LNW) without provision of in-band tones.

B.2 Connection of U-plane and provision of tones

A GAP PP will connect the U-plane either:

- Case A: upon receipt of the appropriate message that placed the PT in active state, (see clauses 8.6 or 8.15); or
- Case B: upon receipt of the <<Progress indicator>> information element indicating "In-band information or appropriate pattern now available" in an appropriate message beforehand, (see clauses 8.3 to 8.5).

When connection of the U-plane is the result of case B a PP may assume that the FP or the LNW provide a suitable in-band tone and may therefore not switch local tone (if provided) to the user.

B.3 Provision of tones before connection of the U-plane

For an outgoing call, in the case when a PP enters state T-02 (Overlap sending) and no dialling digit has been entered or available in the local dialling buffer, and the PP has not received the appropriate <<Progress indicator>> information element, that PP may indicate to its user that he should start to dial (invitation for dial) by providing local tones or another appropriate indication (e.g. by buzzer, display, etc.).

B.4 Provision of tones and <<Progress indicator>> information element

In the case where a LNW provides in-band tones a GAP FP may use this tones for calls that leaves the FP. The FP should indicate the provision of these in-band tones to the PP by transmitting the <<Progress indicator>> information element indicating "In-band information or appropriate pattern now available" in an appropriate message. This should imply that the FP has knowledge about the tone provision situation of the LNW. The PP should accept these in-band tones.

In the case where the LNW does not provide in-band tones or the FP has no knowledge about the tone provision situation of the LNW, the FP itself may supply in-band tones for calls that leave and that do not leave the FP indicating the provision of this tones by transmitting the <<Progress indicator>> information element indicating "In-band information or appropriate pattern now available" in an appropriate message. The PP should accept these in-band tones.

A GAP FP may be designed without local tone generator, therefore no in-band tones can be provided to the PP user. Such FP, if it has no knowledge about the tone provision situation of the LNW, should not transmit the <<Progress indicator>> information element indicating "In-band information or appropriate pattern now available".

B.5 Summary

Table B.1

	FP with local tone generator		**FP without local tone generator**	
	LNW provides in-band tones; FP knows	**LNW does not provide in-band tones or FP does not know**	**LNW provides in-band tones; FP knows**	**LNW does not provide in-band tones or FP does not know**
PP has a local tone generator; internal call	Use of FP local tone generator; convey <<Progress indicator>> to PP	Use of FP local tone generator; convey <<Progress indicator>> to PP	Use of PP local tone generator; do not convey <<Progress indicator>> to PP	Use of PP local tone generator; do not convey <<Progress indicator>> to PP
PP has a local tone generator; external call	Convey in-band tones from LNW; convey <<Progress indicator>> to PP	Use of FP local tone generator; convey <<Progress indicator>> to PP	Convey in-band tones from LNW; convey <<Progress indicator>> to PP	Use of PP local tone generator; do not convey <<Progress indicator>> to PP
PP has not a local tone generator; internal call	Use of FP local tone generator; convey <<Progress indicator>> to PP	Use of FP local tone generator; convey <<Progress indicator>> to PP	No tones available for the PP user; use other means to invite for dialling (e.g. display, buzzer, etc.)	No tones available for the PP user; use other means to invite for dialling (e.g. display, buzzer, etc.)
PP has not a local tone generator; external call	Convey in-band tones from LNW; convey <<Progress indicator>> to PP	Use of FP local tone generator; convey <<Progress indicator>> to PP	Convey in-band tones from LNW; convey <<Progress indicator>> to PP	No tones available for the PP user; use other means to invite for dialling (e.g. display, buzzer, etc.)

Annex C (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 D (informative): Change history

The following table presents main changes from a published version to the next version (published or to be published).

Subject/Comment	Old	New
New Generation DECT: A major revision of the DECT base standard introducing wideband speech, improved data services, new slot types and other technical enhancements. New audio type definitions. New application feature: Terminal identity number assignment in mono-cell system. New NWK feature: CNIP.	1.9.1	2.1.1
New Generation DECT; DECT: enhanced security features: re-keying and early encryption. Technical and editorial review.	2.1.1	2.2.1
New authentication and ciphering procedures based on new algorithms DSAA2 and DSC2. Additional security improvements. Technical and editorial review.	2.2.1	2.3.1
Clarify PP behaviour regarding legacy FPs. Technical and editorial review.	2.3.1	2.4.1
Security review; Technical and editorial review.	2.4.1	2.5.1

History

Document history		
Edition 1	December 1995	Publication as ETSI ETS 300 444
V1.2.2	August 1997	Publication
V1.3.3	May 1999	Publication
V1.4.1	September 2001	Publication
V1.4.2	February 2003	Publication
V2.1.1	October 2008	Publication
V2.2.1	June 2010	Publication
V2.3.1	April 2012	Publication
V2.4.1	July 2013	Publication
V2.4.8	July 2017	EN Approval Procedure AP 20171009: 2017-07-11 to 2017-10-09
V2.5.1	October 2017	Publication