Final draft **EN 301 361-1** V1.1.1 (1999-06)

European Standard (Telecommunications series)

Digital Enhanced Cordless Telecommunications (DECT);
Integrated Services Digital Network (ISDN);
ISDN Mobility protocol Interworking specification Profile (IMIP);
Part 1: DECT/ISDN interworking for Cordless Terminal Mobility (CTM) support

ETSI

Reference
DEN/DECT-030126 (clo90ico.PDF)

Keywords
CTM, DECT, DSS1, interworking, ISDN, mobility

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

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

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

ETSI

Contents

Intellectual Property Rights

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

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

Foreword

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

The present document is part 1 of a multi-part EN covering the ISDN Mobility protocol Interworking specification Profile (IMIP), as identified below:

> **Part 1:** **"DECT/ISDN interworking for Cordless Terminal Mobility (CTM) support";**
>
> Part 2: "DECT/ISDN interworking for Global System for Mobile communications (GSM) support".

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

Introduction

This two-part EN defines a profile for interworking between a DECT system and an Integrated Services Digital Network (ISDN) using the enhanced Digital Subscriber Signalling No. 1 (DSS1) protocol defined in EN 301 144-1 [8]. This ISDN protocol enables cordless terminals to have access to an ISDN infrastructure.

Part one defines the DECT/DSS1+ interworking for the CTM support.

Part two considers the DECT/DSS1+ interworking for the GSM support.

The present document specifies how DSS1+ procedures and information are mapped over the DECT air interface, and how they are provided and used by the DECT Fixed Part.

1 Scope

The present document specifies a set of technical requirements for Digital Enhanced Cordless Telecommunications (DECT) Fixed Parts (FP) supporting connection, via an ISDN interface, to a network supporting terminal mobility.

The standard covers the requirements necessary for the support of Cordless Terminal Mobility (CTM) Phase 1 (Part 1) and for the support of the DECT access to GSM via ISDN interfaces (Part 2). In both of these scenarios, the FT is connected to the network via the alpha interface, as specified in EN 301 144-1 [8].

> NOTE: For CTM phase 1, the Portable Part (PP) requirements are specified in EN 300 444 [6].

The present document specifies the interworking procedures between the Digital Enhanced Cordless Telecommunications (DECT) air interface and the mobility management protocols defined for Integrated Services Digital Network (ISDN) interfaces.

The ISDN Access Profile (IAP), ETS 300 434-2 [12], specifies the requirements for the support of ISDN services. Apart from the mobility management procedures, that are covered in the present document, the IAP includes interworking specifications for the support of basic call.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

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

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

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

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

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

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

[7]   EN 300 403-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[8]   EN 301 144-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) and Signalling System No.7 (SS7); Signalling application for the mobility management service on the alpha interface; Part 1: Protocol specification".

[9]   ISO/IEC 9646-7 (1995): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[10]   ITU-T Recommendation X.219 (1988): "Remote operation: Model, notation and service definition".

[11]   EN 301 061-1 (1.2.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Generic functional protocol for the support of supplementary services at the "b" service entry point for Virtual Private Network (VPN) applications; Part 1: Protocol specification".

[12]   ETS 300 434-2: "Digital Enhanced Cordless Telecommunications (DECT); Integrated Services Digital Network (ISDN); DECT/ISDN interworking for end system configuration; Part 2: Access profile".

[13]   CCITT Recommendation I.411 (1988): "ISDN user-network interfaces; Reference configurations".

[14]   ETS 300 402-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Data link layer; Part 1: General aspects [ITU-T Recommendation Q.920 (1993), modified]".

[15]   ETS 300 011-1: "Integrated Services Digital Network (ISDN); Primary rate user-network interface; Layer 1 specification and test principles; Part 1: Layer 1 specification".

[16]   ETS 300 012-1: "Integrated Services Digital Network (ISDN); Basic user-network interface; Layer 1 specification and test principles; Part 1: Layer 1 specification".

[17]   EN 301 175: "Cordless Terminal Mobility (CTM); Phase 1; Service description".

3   Definitions, symbols and abbreviations

3.1   Definitions

For the purposes of the present document, the following definitions in addition to all terms defined in EN 300 444 [6] apply.

supplementary service: service that modifies or supplements a basic telecommunications service

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

3.2   Symbols

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

NOTE 1: The symbols defined in this subclause are applied for procedures, features, services in the present document if not explicitly otherwise stated. The interpretation of status columns in all tables is as follows:

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

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

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

NOTE 2: The used notation is based on the notation proposed in ISO/IEC 9646-7 [9].

3.3   Abbreviations

For the purposes of the present document, the following abbreviations in addition to all abbreviations defined in EN 300 444 [6] apply:

BRA	Basic Rate Access
CI	Common Interface
CLIP	Calling Line Identification Presentation
IAP	ISDN Access Profile [12]
IE	Information Element
NCIC	Network Call-Independent Connection
NCICs	Network Call-Independent Connection Oriented Signalling
NT	Network Termination
PRA	Primary Rate Access
ROSE	Remote Operation Service Element

4   Feature definitions

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

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

4.1   Network (NWK) features

See EN 300 444 [6].

4.1.1   Application features

The application features defined in the present document concern the interworking of the corresponding network layer features. Hence no new definitions are required.

5   General requirements

5.1   Architecture

5.1.1   Reference configuration

Reference configurations describe functional groupings by using reference points, as described in ITU Recommendation I.411 [13] for ISDN. For CTM, the reference configurations are shown in the alpha interface specification [8].

An overview of standard ISDN and CTM specific reference configurations is shown in the following figure.
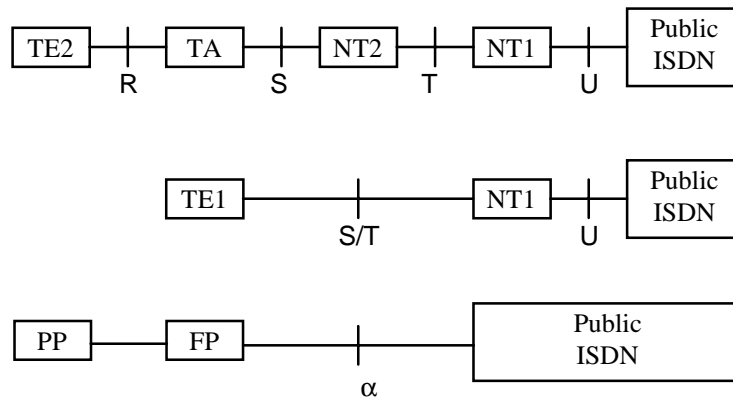
Figure 1: Standard ISDN and CTM specific reference configurations

The present document is applicable for the Fixed Parts attached to the alpha reference point. The interface protocols for the alpha interface are based upon the protocols defined for the T or the coincident S and T reference points.

5.1.2   Interfaces

This interworking profile is based on the alpha interface standard, which applies to public CTM networks.

   NOTE: The beta interface standard, which applies to private CTM networks, is not considered.

The present document covers both basic rate and primary rate access (BRA, PRA). Point-to-multipoint as well as point to point configurations are applicable.

5.2   Protocol model

The following figure provides an overview of the protocol model used to describe the protocol interworking within the FT. The present document is mainly concerned with the interworking between DECT mobility management procedures (invoked by means of messages and information elements at the air interface) and the CTM mobility management procedures on the alpha interface (invoked by means of Remote Operations).
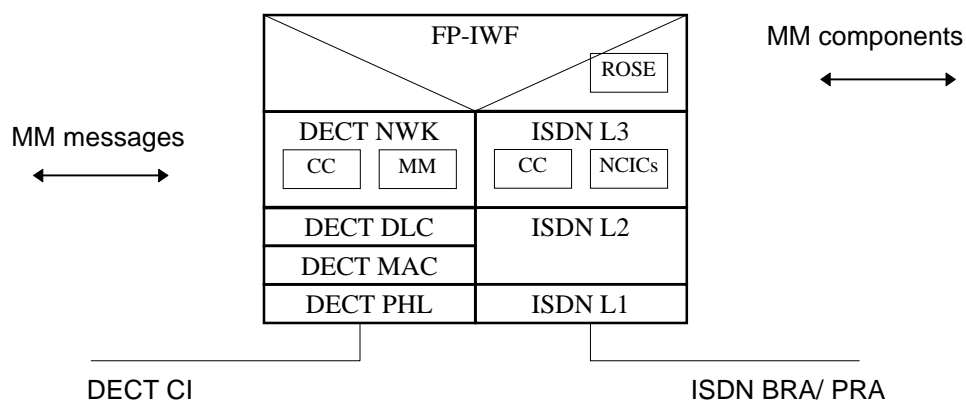
Figure 2: Protocol model

Table 1: Description of DECT and ISDN layers

Layers	DECT	ISDN
L4 to 6		EN 301 144-1 (CTM signalling application) [8] ITU-T Recommendation X.219 (ROSE) [10]
L3	EN 300 175-5 (NWK) [5]	EN 300 403-1 (CC) [7] EN 301 061-1 (NCICs) [11]
L2	EN 300 175-4 (DLC) [4] EN 300 175-3 (MAC) [3]	ETS 300 402-1 [14]
L1	EN 300 175-2 [2]	ETS 300 011-1 (PRA) [15] ETS 300 012-1 (BRA) [16]

5.3   Identity usage

5.3.1   CTM identity

At the alpha interface, the CTM identity is used to uniquely identify a CTM user. At the air interface however, the DECT PP- identity is used to identify the user. The FT provides the mapping between the PP- identity and the CTM- Identity.

The present document assumes the following:

-    there is a one to one relation between the CTM identity and the PP- identity (IPUI);

-    there are no restrictions concerning the PP- identity to be used at the air interface.

NOTE 1: The FT need not reject a PP- initiated request containing an identity type or length that may not be supported by the CTM network.

NOTE 2: The use of non-CTM identities (e.g. residential identities) for roaming to/from the residential area is outside the scope of the present document.

5.3.2   CTM number

The CTM number is the E.164 number that is dialled to call a CTM user.

In case CLIP is subscribed to, the network may provide the CTM number within the <<calling party number>> to the called user (public ISDN $\rightarrow$ FP).

5.3.3   FP- address

The FP- address is a globally unique E.164 number and corresponds to the address of the FT via which the PT is connected to the ISDN access. The FP address is required only in case of a point to multipoint configuration.

In case of an incoming call, the FP- address is conveyed inside the <<called party number>> (public ISDN -> FP). In case of an outgoing call, the FP- address is transferred within a <<calling party number>> (FP -> public ISDN).

6   Interoperability requirements

6.1   General

In order to achieve interoperability, this clause defines the status of features and the associated interworking requirements in a similar manner as done in EN 300 444 (GAP) [6].

The interworking requirements specified in the present document concern the application layer and the network layer.

The application layer requirements are specified in the present document. The ISDN network layer requirements are fully specified in EN 301 144-1 [8]. For the DECT network layer, all FT requirements specified in EN 300 444 (GAP) [6] apply unless explicitly stated otherwise. This means that only additions/modifications to EN 300 444 (GAP) [6] are included in this clause.

6.2   DECT NWK features

All requirements specified in subclause 6.2 of EN 300 444 [6] apply with the following modifications:

Table 2: NWK features status

Feature supported					
			Status		
Item no.	Name of feature	GAP Ref.	FT		
			R	B	P
N.13	Identification of portable	4.1	M	M	M
N.26	Authentication of network	4.1	M	M	M
N.9	Authentication of portable	4.1	M	M	M
N.11	Location registration	4.1	M	M	M
N.18	Subscription registration	4.1	O	O	O
N.12	Key allocation	4.1	M	M	M
N.17	Network initiated ciphering	4.1	M	M	M
NOTE 1: The above table indicates the status of feature from a CTM service perspective. Features that are required by GAP may not be required for supporting the CTM service, in which case the feature will be optional in the above table.					
NOTE 2: The CTM service should be uniform across different application areas. As a result, the status of features is the same in all environments.					

6.3   Application features

This subclause concerns the FT's application layer which mainly handles the interworking between the DECT and the alpha interface protocols.

Table 3: Application features status

Feature supported					
			Status		
Item no.	Name of feature	GAP Ref.	FT		
			R	B	P
IMIP-A.1	General	4.1.1	M	M	M
IMIP-A.2	Identification of portable	4.1.1	M	M	M
IMIP-A.3	Authentication of network	4.1.1	M	M	M
IMIP-A.4	Authentication of portable	4.1.1	M	M	M
IMIP-A.5	Location registration	4.1.1	M	M	M
IMIP-A.6	Location cancellation	4.1.1	M	M	M
IMIP-A.7	Location registration suggest	4.1.1	M	M	M
IMIP-A.8	Subscription registration	4.1.1	O	O	O
IMIP-A.9	Key allocation	4.1.1	M	M	M
IMIP-A.10	Subscription deregistration	4.1.1	O	O	O
IMIP-A.11	Network initiated ciphering	4.1.1	M	M	M
IMIP-A.12	Portable initiated ciphering	4.1.1	O	O	O
IMIP-A.13	Outgoing call	4.1.1	M	M	M
IMIP-A.14	Incoming call	4.1.1	M	M	M
IMIP-A.15	Supplementary service activation	4.1.1	O	O	O
IMIP-A.16	DTMF generation	4.1.1	O	O	O

6.4   NWK feature to procedure mapping

All requirements specified in EN 300 444 [6] apply with the following modifications:

Table 4: NWK feature to procedure mapping

Feature/Procedure mapping					
			Status		
Feature	Procedure	CAP Ref. GAP Ref.	PT FT		
			R	B	P
Location registration			M	M	M
	Location update	8.29	M	M	M
Outgoing call			M	M	M
	Overlap sending	8.3	M	M	M
	Outgoing call proceeding	8.4	M	M	M
	Outgoing call confirmation	8.5	M	M	M
	Flexible U-plane connection		O	O	O
NOTE: For the listed features, only those procedures are specified for which the requirements are different as compared to EN 300 444 (GAP) [6]; for feature location registration, the requirements for the location registration procedure are as specified in EN 300 444 (GAP) [6].					

6.5   Application feature to procedure mapping

Table 5: Application feature to procedure mapping

Feature/Procedure mapping					
			Status		
Feature	Procedure	Ref.	FT		
			R	B	P
General			M	M	M
	Connection establishment and release	7.1	M	M	M
	Generic mobility management interworking procedures	7.2 to 7.2.4	M	M	M
	Generic message mapping	8 to 8.2.2	M	M	M
	Generic information element	8.4	M	M	M
Identification of portable			O	O	O
	Identification of PP	7.2.5	M	M	M
Authentication of network			M	M	M
	Authentication of network	7.2.6	M	M	M
Authentication of portable			M	M	M
	Authentication of PT	7.2.7	M	M	M
Location registration			M	M	M
	Location registration	7.2.8	M	M	M
Location cancellation			M	M	M
	Location cancellation	7.3.1	M	M	M
Location registration suggest			M	M	M
	Location update	7.2.9	M	M	M
Subscription registration			O	O	O
	Obtaining access rights	7.2.10	M	M	M
Key allocation			M	M	M
	On air key allocation	7.2.11	M	M	M
Subscription deregistration			O	O	O
	FP terminating access rights	7.2.12	M	M	M
Network initiated ciphering			M	M	M
	Cipher switching initiated by network	7.2.13	M	M	M
Portable initiated ciphering			O	O	O
	Cipher switching initiated by PT	7.2.14	M	M	M
Outgoing call			M	M	M
	Outgoing call	7.3.2	M	M	M
	Call progress information transfer	7.3.4	O	O	O
	Call release	7.3.5	M	M	M
Incoming call			M	M	M
	Incoming call	7.3.3	M	M	M
	Call progress information transfer	7.3.4	O	O	O
	Call release	7.3.5	M	M	M
Supplementary service activation			O	O	O
	Keypad information transfer	7.3.6	M	M	M
DTMF generation			O	O	O
	Keypad information transfer	7.3.6	M	M	M
NOTE: In order to simplify the specification, a feature "General" has been introduced. This is used to specify the status of clauses specifying interworking requirements/principles that are not related to a specific feature.					

7   Procedure descriptions

This clause specifies the interworking requirements for the mobility management procedures as required for CTM phase 1. Furthermore, this clause specifies additions/modifications to the interworking requirements for call control as specified in the ISDN Access Profile [12].

NOTE: The interworking requirements may include requirements concerning the interaction between interworking and non-interworking procedures.

7.1 Connection establishment and release

This subclause describes the co-ordination between the radio connection establishment/release and the establishment/release of the mobility management transport mechanism used at the alpha interface.

There are requirements concerning co-ordination during connection establishment, but not for connection release.

7.1.1 NCICs connection control

The NCICs connection establishment and release procedures are described in EN 301 144-1 [8]. The radio link establishment and release procedures are specified in subclauses 8.35 to 8.39 of EN 300 444 [6].

There is co-ordination between NCICs and radio link control procedures during connection establishment and data transfer, as specified in the following.

7.1.2 Connection establishment co-ordination

7.1.2.1 PT initiated mobility management transaction

In case the FT receives a PT- initiated mobility management request concerning a PT for which an NCICs connection already exists, it shall use this connection to transfer the mobility management request.

In case the FT receives a PT- initiated mobility management request concerning a PT for which no NCICs connection exists, the FT shall initiate the establishment of such a NCICS connection.

> NOTE: Across the alpha interface the NCICs connection establishment request shall include a CTM Identity. In case the PT- initiated transaction request does not include a <<PP- identity>>, the FT may need to derive or retrieve the IPUI.
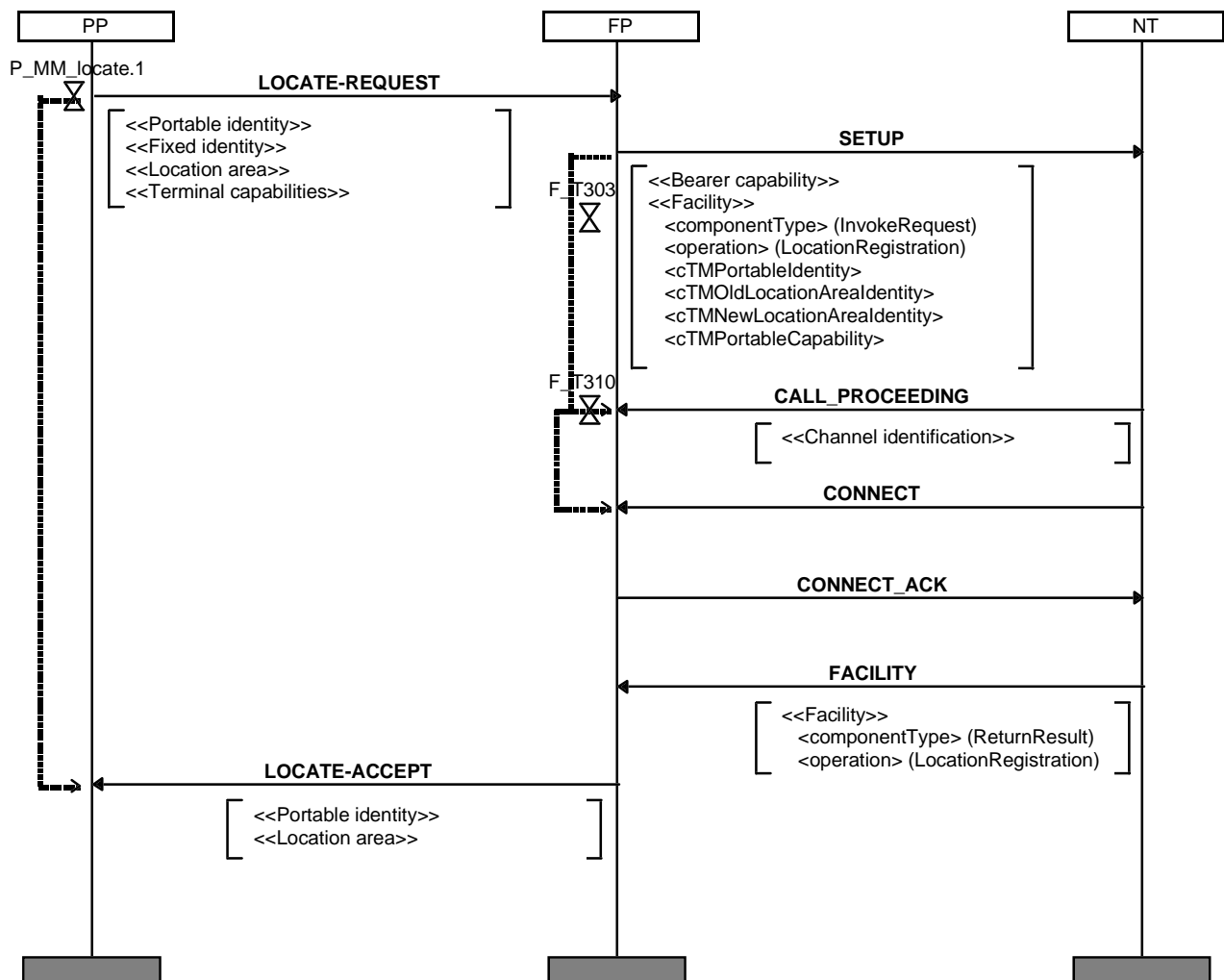
NOTE: This is the normal terminal initiated NCICs connection establishment. The Location Registration operation is given as an example.

Figure 3: NCIC terminal initiated connection establishment

7.1.2.2   Network initiated mobility management transaction

The FT need not delay acceptance of the NCICs- connection establishment request until radio connection establishment has been completed successfully and/or a response has been received from the PT for the associated MM- transaction.

The FT shall not reject an NCICs connection establishment request concerning a PT for which another NCICs connection has already been established.

NOTE: Although in most cases the network re- uses an existing NCICs connection for the concerned PT, this may not always be possible. In the latter case, multiple simultaneous NCICs connections may be used for a PT.
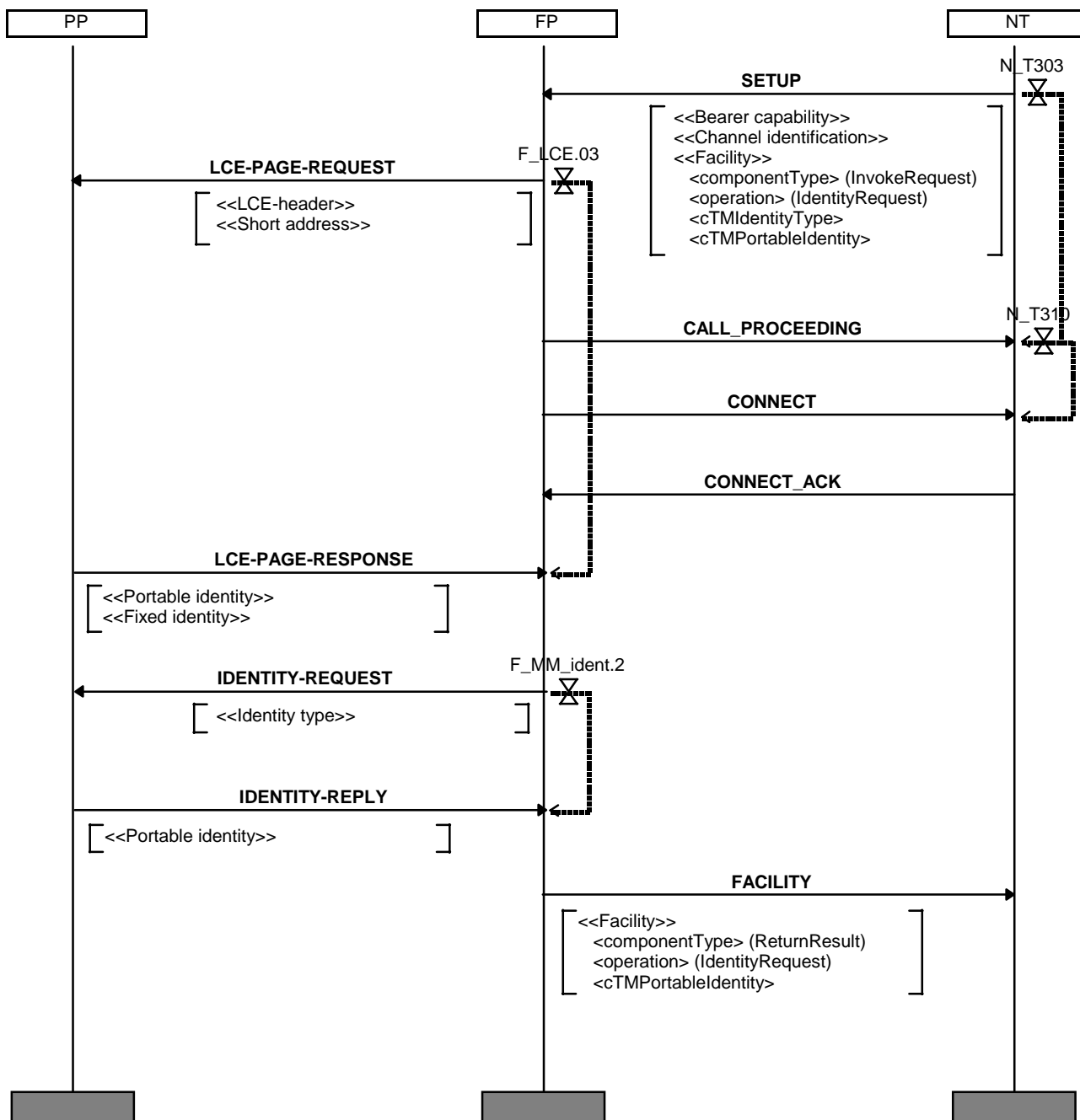
NOTE: This is the normal network initiated NCICs connection establishment. IdentifyRequest operation is given as an example.

Figure 4: NCIC network initiated connection establishment

7.1.3 Connection oriented data transfer co-ordination

In case more than one NCICs connection exists for the connected PT, the FT shall apply the following rules:

- a return result/error shall be transferred across the same NCICs connection as used to transfer the invoke;

- a request concerning an embedded procedure, e.g. authentication of network, shall be returned across the same NCICs connection as used to transfer the initial request that triggered the embedded procedure (e.g. terminate access rights, network initiated).

NOTE: Within the CTM network, more than one node may initiate mobility management transactions. Due to this, the CTM network may be unable to ensure that only one NCICs connection is established per PT.

7.1.4   Connection release co-ordination

The FT need not co-ordinate release of the radio link connection and the NCICs connection as illustrated in the following sequence diagrams.
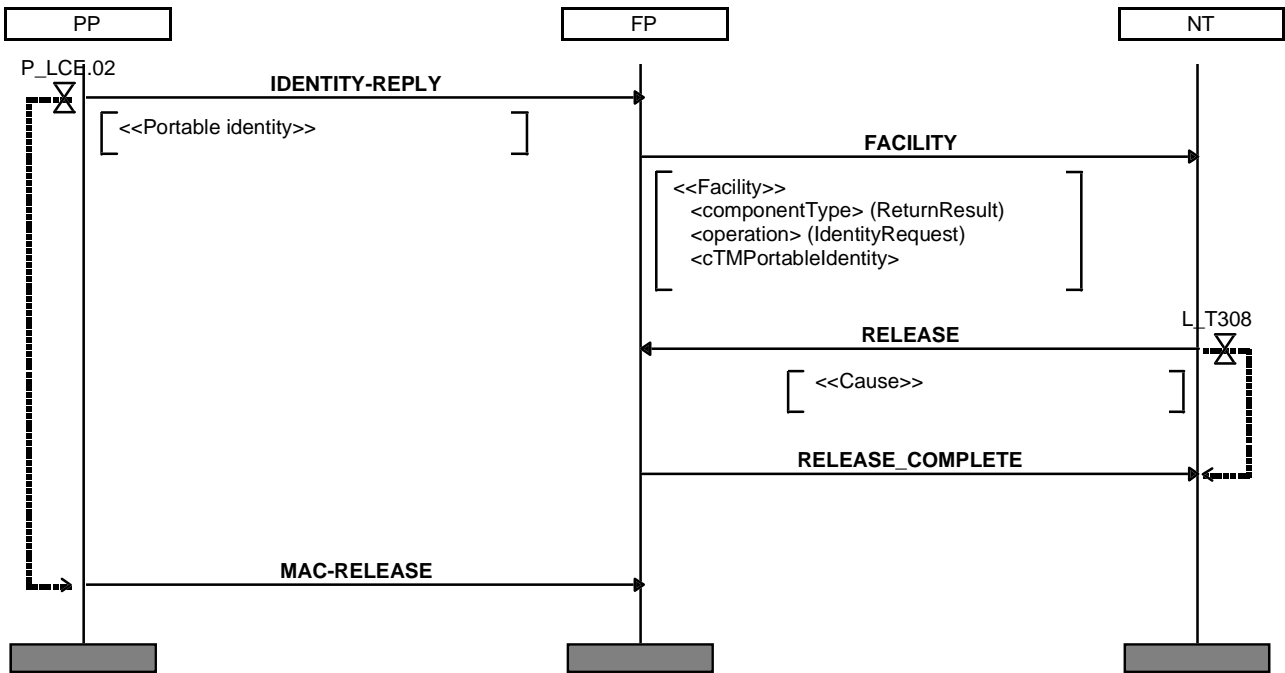
NOTE: Identity request is given as an example. Partial release applies at the air interface.

Figure 5: NCIC network initiated call release
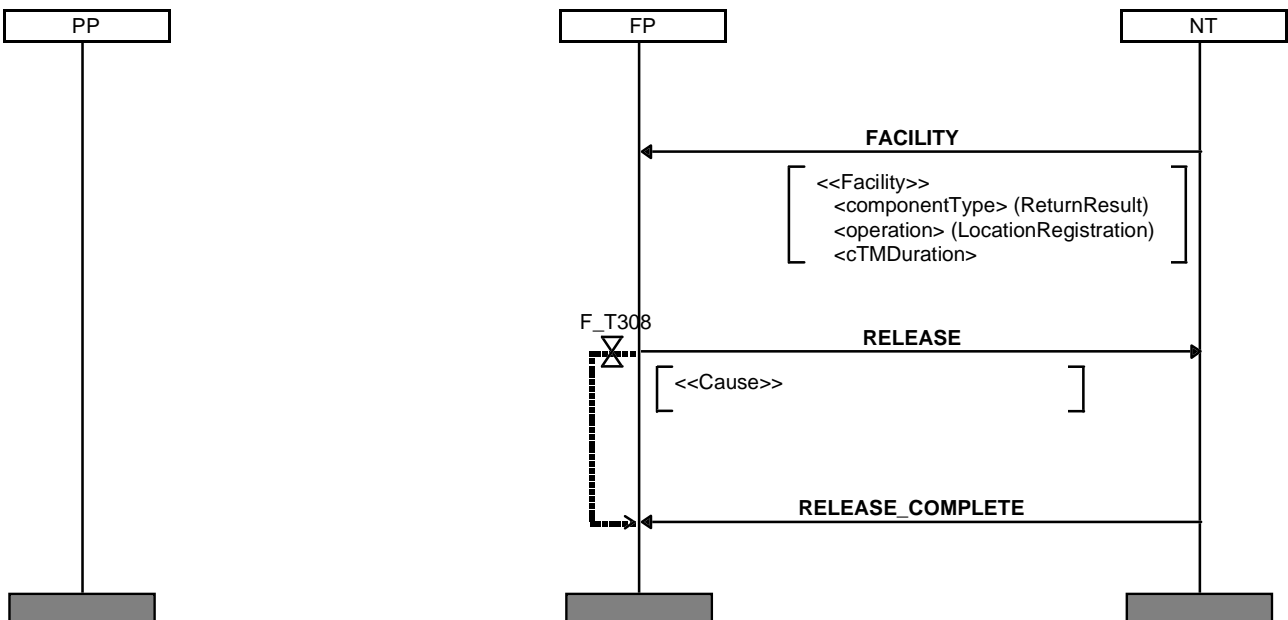
NOTE: Terminal initiated MM- signalling connection release. Only used in exceptional cases e.g. maintenance action.

Figure 6: NCIC terminal initiated call release

7.2   Mobility management procedures

The following table provides an overview of the mobility management procedures and their status in CTM phase 1 as specified in EN 301 144-1 [8].

Table 6: Overview of the mobility management procedures

Procedure	DECT messages	MM operation	Note
Identification of PP	IDENTITY-REQUEST IDENTITY-REPLY	identityRequest	
Authentication of network	AUTHENTICATION-REQUEST AUTHENTICATION-REPLY AUTHENTICATION-REJECT	networkAuthentication	
Authentication of PP	AUTHENTICATION- REQUEST AUTHENTICATION-REPLY AUTHENTICATION-REJECT	terminalAuthentication	
Location registration	LOCATE-REQUEST LOCATE-ACCEPT LOCATE-REJECT TEMPORARY-IDENTITY-ASSIGN-ACK TEMPORARY-IDENTITY-ASSIGN-REJECT	locationRegistration	1
Location update	MM-INFO-SUGGEST	locationRegistrationSuggest	2
Obtaining access rights	ACCESS-RIGHTS-REQUEST ACCESS-RIGHTS-ACCEPT ACCESS-RIGHTS-REJECT	accessRightsRequest	
Network terminating access rights	ACCESS-RIGHTS-TERMINATE-REQUEST ACCESS-RIGHTS- TERMINATE-ACCEPT ACCESS-RIGHTS- TERMINATE-REJECT	accessRightsTerminate	
On air key allocation	KEY-ALLOCATE AUTHENTICATION-REQUEST AUTHENTICATION-REPLY AUTHENTICATION-REJECT	keyAllocate, networkAuthentication	
Cipher switching initiated by network	CIPHER-REQUEST CIPHER-REJECT (DL_ENCRYPT.IND)	ciphering	3
Cipher switching initiated by PP	CIPHER-SUGGEST	cipheringSuggest	4
NOTE 1: This procedure includes an additional information transfer related to the assignment of a temporary identity. NOTE 2: This procedure applies two subsequent transactions. NOTE 3: For this procedure the return result is triggered by a local primitive rather than by a network layer message received across air interface. NOTE 4: At the air interface, the PT initiated ciphering and the subsequent network initiated ciphering are consider as a single transaction.			

The following sublauses only describe the generic interworking procedures. Additional requirements, if applicable, are included in the sublause providing the interworking procedure specific for the corresponding MM- procedure.

The feature specific sublauses also include message interworking specifications, for which the general principles are described in subclause 8.1.

7.2.1   Generic interworking procedures, network initiated transaction, explicit acknowledgement

7.2.1.1   FT accepts mobility management request

Upon reception of a MM invoke component concerning a network initiated mobility management request, the FT shall initiate the corresponding mobility management transaction towards the PT. This involves the starting of the related FP- timer as described in EN 300 175-5 [5] and the interworking of the MM component as specified within the applicable feature specific procedure description.

7.2.1.2   FT receives response from PT

Upon reception of the response, either positive or negative, the FP shall stop the applicable timer as described in
EN 300 175-5 [5] and interwork the received DECT message to the corresponding MM return result or return error
component.

7.2.1.3   FT rejects mobility management request

In case the FT rejects the network initiated mobility management request, it shall send a MM return error component
towards the network, including an error value indicating the reason of rejection.

> NOTE: The FT may reject the network initiated mobility management request in case of resource contention, no
> response to paging, expiry of the applicable DECT timer, loss of the radio link connection.
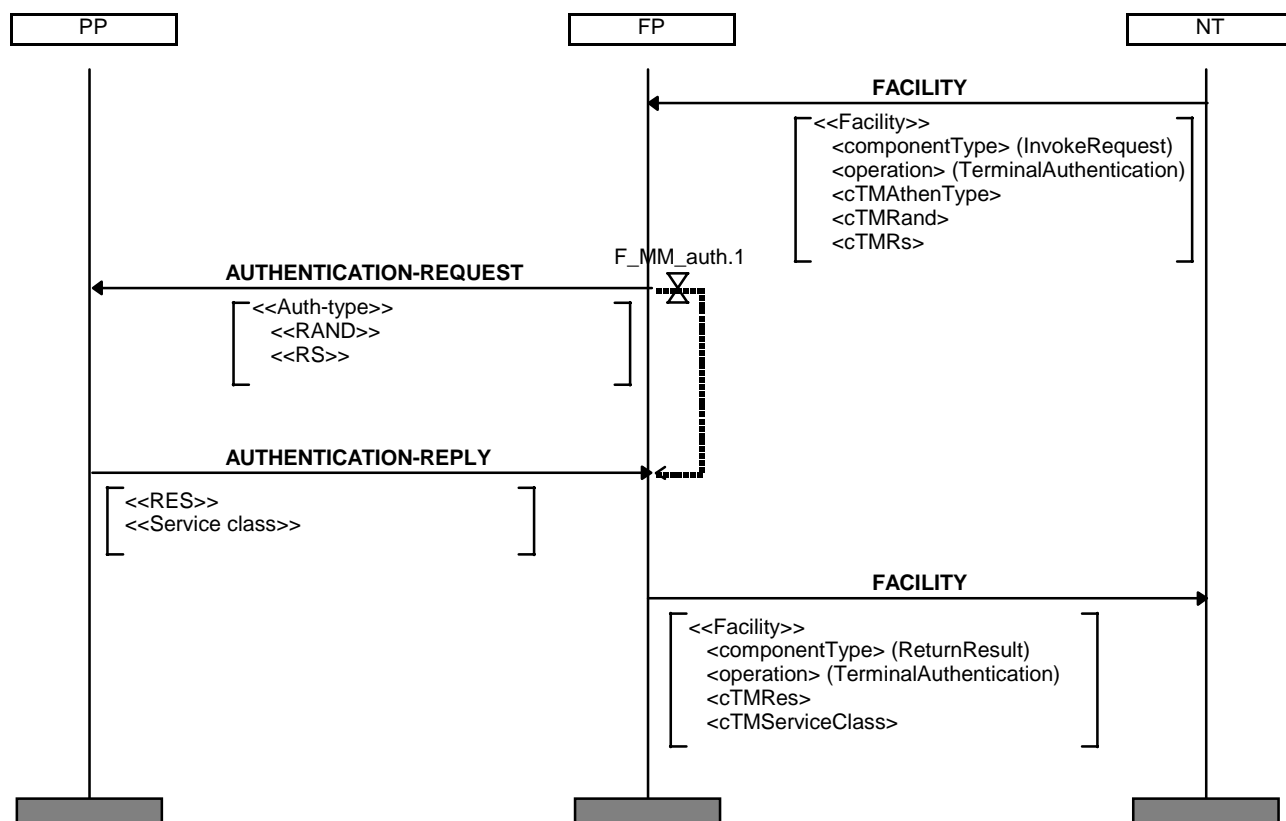
> NOTE: Terminal authentication is shown as an example. FACILITY is shown as a possible NCICs data transport
> message.

Figure 7: Network initiated MM transaction with explicit acknowledgement

7.2.2   Generic interworking procedures, network initiated transaction, no explicit acknowledgement

7.2.2.1   FT accepts mobility management request

Upon reception of a MM invoke component concerning a network initiated mobility management request, the FT shall
initiate the corresponding mobility management transaction towards the PT. This involves the interworking of the
received MM component as specified within the applicable feature specific procedure description.

In response to the network initiated procedure, the PT may start a mobility management procedure. This is considered as
another transaction/operation e.g. the location registration following the location update procedure.

7.2.2.2   FT rejects mobility management request

In case the FT rejects the network initiated mobility management request, it shall send a MM return error component towards the network, including an error value indicating the reason of rejection.

> NOTE: The FT may reject the network initiated mobility management request in case of resource contention, no response to paging, expiry of the applicable DECT timer, loss of the radio link connection.
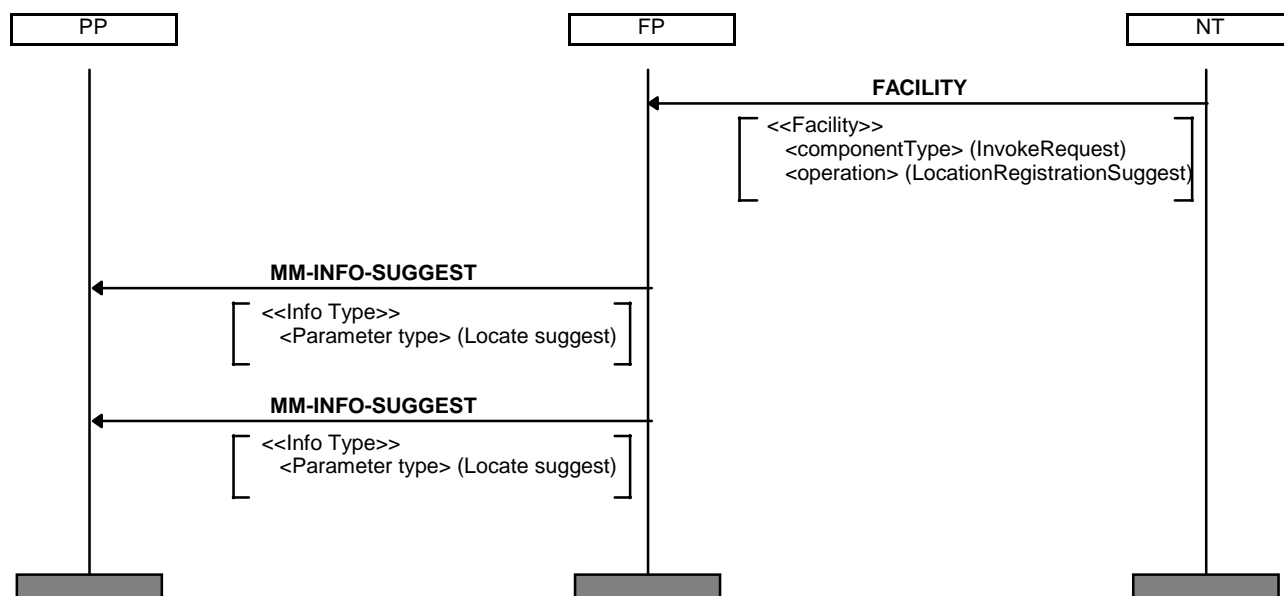
> NOTE: Location Update is shown as an example. FACILITY is shown as possible NCICs transport message. Locate Suggest needs to be sent twice.

Figure 8: Network initiated MM transaction with no explicit acknowledgement

7.2.3   Generic interworking procedures, PT initiated transaction, explicit acknowledgement

7.2.3.1   FT accepts mobility management request

Upon reception of a DECT mobility management message, the FT shall initiate the corresponding MM invoke component towards the network. This involves the interworking of the message as described in clause 8.

7.2.3.2   FT receives response from network

Upon reception of the MM return response or return error component from the network, the FT shall interwork the received component to the corresponding DECT mobility management message as specified in clause 8.

7.2.3.3   FT rejects mobility management request

In case the FT rejects the PT- initiated mobility management request, it shall apply the reject procedure as defined in EN 300 175-5 [5] for the concerned DECT mobility management procedure.

> NOTE: The FT may reject the network initiated mobility management request e.g. in case of resource contention, NCICs connection (establishment) failure.
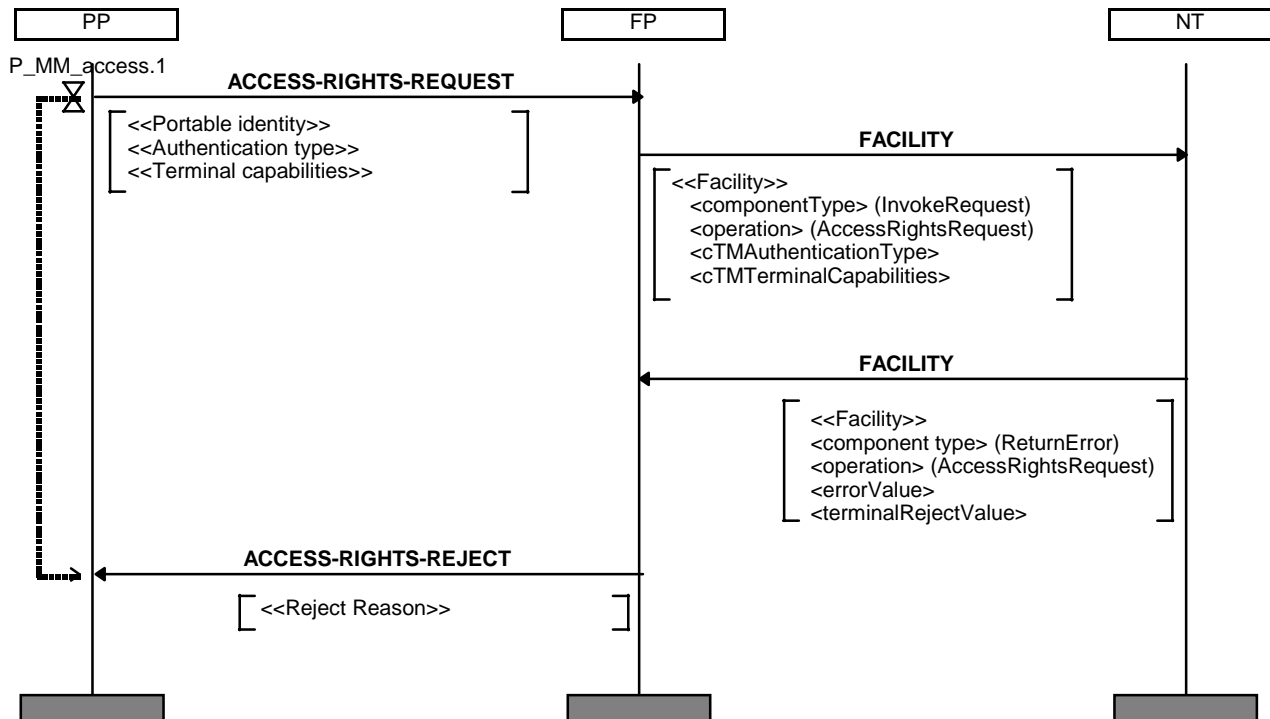
NOTE: Obtaining access rights request is shown as an example. FACILITY is shown as possible NCICs data transport message.

Figure 9: PT initiated MM transaction with explicit acknowledgement

7.2.4   Generic interworking procedures, PT initiated transaction with no explicit acknowledgement

7.2.4.1   FT accepts mobility management request

Upon reception of a DECT mobility management message, the FT shall initiate the corresponding MM invoke component towards the network. This involves the interworking of the DECT message as specified within the applicable feature specific procedure description.

In response to the PT- initiated procedure, the network may start a mobility management procedure. This may be considered as part of the same transaction e.g. the network initiated ciphering following the cipher switching initiated by PT.

NOTE: At the alpha interface the network initiated ciphering is not considered to be part of the same operation.

7.2.4.2   FT rejects mobility management request

In case the FT rejects the PT- initiated mobility management request, it shall apply the reject procedure if defined in EN 300 175-5 [5] for the concerned DECT mobility management procedure.

NOTE: The FT may reject the network initiated mobility management request e.g. in case of resource.
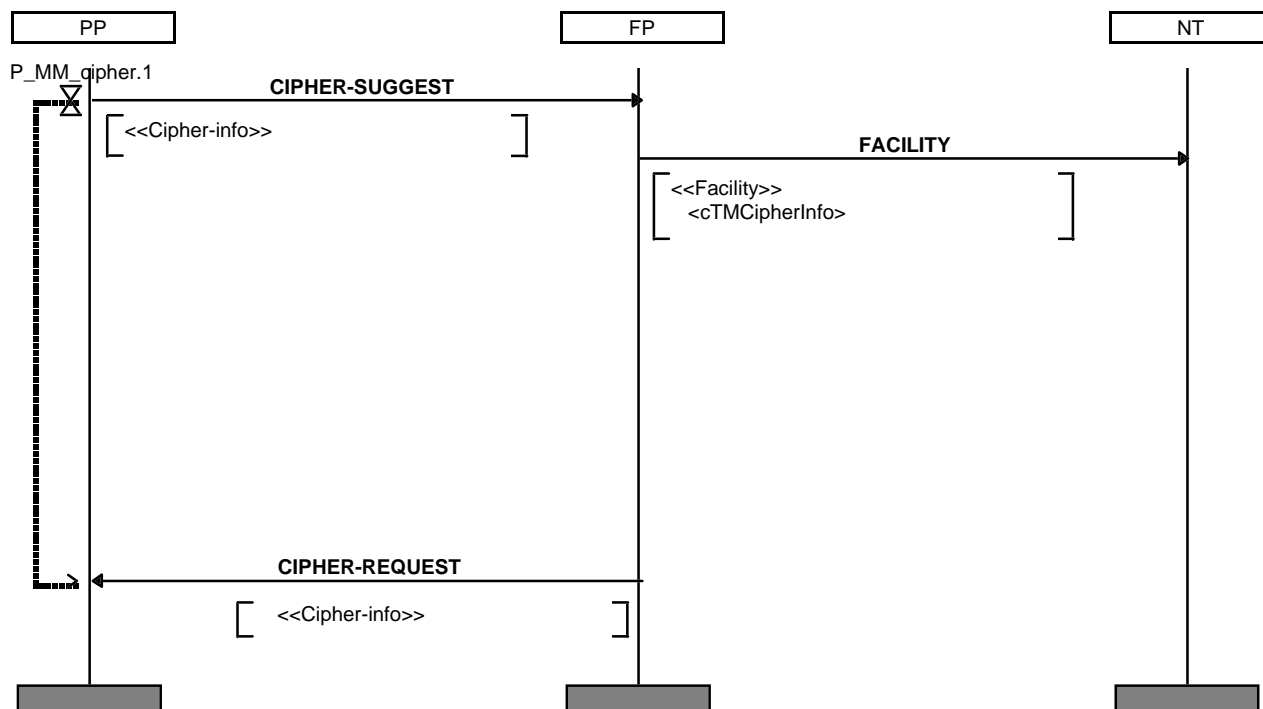
NOTE: Terminal initiated ciphering is shown as an example. FACILITY is shown as possible NCICs data transport message. Please note that at the air interface the follow on cipher request from the FT is considered to be part of the same transaction, while at the alpha interface there are two independent CTM ROSE operations.

Figure 10: PT initiated MM transaction with no explicit acknowledgement

7.2.5 Identification of PT

The network may use this procedure to retrieve the PP's IPUI or IPEI as defined in subclause 9.3.8 of EN 300 175-1 [1].

In addition to the requirements specified in subclause 7.2.1, generic interworking procedures for network initiated mobility management transactions with explicit acknowledgement, the following applies.

In case the PT does not include an identity within the {IDENTITY-RESULT}, the FT shall map this to a MM return error component. The FT shall include an appropriate indication (identityNotAvailable or portableIdentityUnknown) in the errorValue parameter.

Table 7: Mapping of IdentityRequest Invoke - IDENTITY-REQUEST

	MM component	DECT message			
Item No	IdentityRequest Invoke	IDENTITY-REQUEST	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMIdentityType	identity type	8.4.1	M	
5	cTMPortableIdentity		8.4.1	X	note 1
NOTE 1: The NT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.					
NOTE 2: Identity requests other than the network initiated request for a PP- identity (IPEI/IPUI) are outside the scope of the present document.					

Table 8: Mapping of IDENTITY-REPLY - IdentityRequest Return Result

Item No	DECT message	MM component	Ref.	Map status	NOTE
	IDENTITY-REPLY	IdentityRequest Return Result			
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	portable identity	cTMPortableIdentity	8.4.2	M	note 1
NOTE 1:	This interworking applies only in case the case the <<portable identity>> is included in the {IDENTITY-REPLY} message.				
NOTE 2:	Identity requests other than the network initiated request for a PP- identity (IPEI/IPUI) are outside the scope of the present document.				

Table 9: Mapping of IDENTITY-REPLY - IdentityRequest Return Error

Item No	DECT message	MM component	Ref.	Map status	NOTE
	IDENTITY-REPLY	IdentityRequest Return Error			
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4		errorValue		X	
5	reject reason	RejectReason	8.4.2	O	
NOTE:	This interworking applies in case no identity is included in the {IDENTITY-REPLY} message.				

7.2.6   Authentication of network

The PT may use this procedure to authenticate the network, e.g. during subscription termination, as defined in EN 301 144-1 [8], subclause 9.3.3.

There are no requirements in addition to the ones specified in subclause 7.2.3, generic interworking procedures for PT initiated mobility management transactions with explicit acknowledgement.

NOTE: This sublause does not cover requirements concerning the network authentication that is performed during key allocation. These requirements are specified in the key allocation procedure description.

Table 10: Mapping of AUTHENTICATION-REQUEST - NetworkAuthentication Invoke

Item No	DECT message	MM component	Ref.	Map status	NOTE
	AUTHENTICATION-REQUEST	NetworkAuthentication Invoke			
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	auth type	cTMAuthenticationType	8.4.2	M	
5	RAND	cTMRand	8.4.2	M	
6		cTMPortableIdentity		X	note
NOTE:	The FT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.				

Table 11: Mapping of NetworkAuthentication Return Result - AUTHENTICATION-REPLY

	MM component	DECT message			
Item No	NetworkAuthentication Return Result	AUTHENTICATION-REPLY	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMRes	RES	8.4.1	M	
5	cTMRs	RS	8.4.1	M	note
NOTE: Not applicable in case of key allocation.					

Table 12: Mapping of NetworkAuthentication Return Error - AUTHENTICATION-REJECT

	MM component	DECT message			
Item No	NetworkAuthentication Return Error	AUTHENTICATION-REJECT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	errorValue			X	
5	RejectReason	reject reason		O	

7.2.7   Authentication of PT

The network may use this procedure to authenticate the PT as defined in EN 301 144-1 [8], subclause 9.3.2.

There are no requirements in addition to the ones specified in subclause 7.2.1, generic interworking procedures for network initiated mobility management transactions with explicit acknowledgement.

Table 13: Mapping of TerminalAuthentication Invoke - AUTHENTICATION-REQUEST

	MM component	DECT message			
Item No	TerminalAuthentication Invoke	AUTHENTICATION-REQUEST	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMAuthenticationType	Auth type	8.4.1	M	
5	cTMRand	RAND	8.4.1	M	
6	cTMRs	RS	8.4.1	M	
7	cTMPortableIdentity			X	note
NOTE: The NT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.					

Table 14: Mapping of AUTHENTICATION-REPLY - TerminalAuthentication Return Result

	DECT message	MM component			
Item No	AUTHENTICATION-REPLY	TerminalAuthentication Return Result	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	RES	cTMRes	8.4.2	M	
6	service class	cTMServiceClass		O	

Table 15: Mapping of AUTHENTICATION-REJECT - TerminalAuthentication Return Error

Item No	DECT message AUTHENTICATION-REJECT	MM component TerminalAuthentication Return Error	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4		errorValue		X	
5	reject reason	RejectReason	8.4.2	O	

7.2.8   Location registration

The PT may use this procedure to inform the network about its location, as defined in EN 301 144-1 [8], subclause 9.2.1.

In addition to the requirements specified in subclause 7.2.3, generic interworking procedures for PT initiated mobility management transactions with explicit acknowledgement, the following applies.

Table 16: Mapping of LOCATE-REQUEST - LocationRegistration Invoke

Item No	DECT message LOCATE-REQUEST	MM component LocationRegistration Invoke	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	portable identity	cTMPortableIdentity	8.4.2	M	
5	fixed identity	cTMOldLocationAreaIdentity	8.4.2	M	
6	location area				
7		cTMNewLocationAreaIdentity		X	
8	terminal capability	cTMPortableCapabilities	8.4.2	M	

7.2.8.1   FT initiates temporary identity assignment

Upon reception of a positive response from the network, the FT may assign a TPUI to the PT by including a <<PP- identity>> with a non- zero length in the LOCATE-ACCEPT message as specified in EN 300 444 [6], subclause 8.28.

Although the temporary identity assignment procedure is part of the location registration and applies the same transaction identity, the handling of the TEMP-IDENTITY-ASSIGN-ACK is specified in EN 300 444 [6], subclause 8.28 and hence outside the scope of the present document.

Table 17: Mapping of LocationRegistration Return Result - LOCATE-ACCEPT

Item No	MM component LocationRegistration Return Result	DECT message LOCATE-ACCEPT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4		portable identity		X	
5		location area		X	

7.2.8.2 FT receives temporary reject from network

In case the response received from the network concerns a temporary rejection, the FT should clear the transaction internally, that is without sending a LOCATE-REJECT message to the PT.

NOTE: The network may indicate the temporary rejection by means a special value within the <errorValue> e.g. congestion or within <cTMTerminalRejectValue> e.g. overload.

Table 18: Mapping of LocationRegistration Return Error - LOCATE-REJECT

Item No	MM component LocationRegistration Return Error	DECT message LOCATE-REJECT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	errorValue			X	
5	RejectReason	reject reason		O	

7.2.9 Location update

The network may use this procedure to initiate location registration as defined in EN 301 144-1 [8], subclause 9.3.1.

There are no requirements in addition to the ones specified in subclause 7.2.2, generic interworking procedures for network initiated mobility management transactions with no explicit acknowledgement.

Table 19: Mapping of LocationRegistrationSuggest Invoke - MM-INFO-SUGGEST

Item No	MM component LocationRegistrationSugg est Invoke	DECT message MM-INFO-SUGGEST	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMPortableIdentity			X	
5		info type		X	
NOTE 1: The NT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.					
NOTE 2: As specified in subclause 8.29 of EN 300 444 [6], this procedure requires the FT to send two MM–INFO–SUGGEST messages.					

7.2.10 Obtaining access rights

The PT may use this procedure to obtain access rights as defined in subclause 9.1.1 of EN 301 144-1 [8].

There are no requirements in addition to the ones specified in subclause 7.2.3, generic interworking procedures for PT initiated mobility management transactions with explicit acknowledgement.

Table 20: Mapping of ACCESS-RIGHTS-REQUEST - AccessRightsRequest Invoke

	DECT message	MM component			
Item No	ACCESS-RIGHTS-REQUEST	AccessRightsRequest Invoke	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	portable identity	cTMPortableIdentity	8.4.2	M	
5	auth type	cTMAuthenticationType	8.4.2	M	
6	terminal capability	cTMPortableCapabilities	8.4.2	M	

Table 21: Mapping of AccessRightsRequest Return Result - ACCESS-RIGHTS-ACCEPT

	MM component	DECT message			
Item No	AccessRightsRequest Return Result	ACCESS-RIGHTS-ACCEPT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMPortableIdentity	portable identity	8.4.1	M	
5	cTMFixedIdentity	fixed identity	8.4.1	M	
6	cTMServiceClass	service class		O	

Table 22: Mapping of AccessRightsRequest Return Error - ACCESS-RIGHTS-REJECT

	MM component	DECT message			
Item No	AccessRightsRequest Return Error	ACCESS-RIGHTS-REJECT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	errorValue			X	
5	RejectReason	reject reason		O	

7.2.11 On air key allocation

The network may use this procedure to replace the PP's Authentication Code (AC) by a more secure User Authentication Code (UAK) as defined in subclause 9.3.7 of EN 301 144-1 [8].

7.2.11.1 FT accepts or rejects mobility management request

Upon reception of a keyAllocate invoke component, the FT shall start timer F<MM_key.1> as described in EN 300 444 [6], subclause 8.32 and interwork the MM component as specified in subclause 7.2.1.1, generic procedures for network mobility management, FT accepts mobility management request or subclause 7.2.1.3, generic procedures for network mobility management, FT rejects mobility management request.

Table 23: Mapping of KeyAllocate Invoke - KEY-ALLOCATE

	MM component	DECT message			
Item No	**KeyAllocate Invoke**	**KEY-ALLOCATE**	**Ref.**	**Map status**	**NOTE**
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMAllocType	allocation type	8.4.1	M	
5	cTMRand	RAND	8.4.1	M	
6	cTMRs	RS	8.4.1	M	
7	cTMPortableIdentity			X	note
NOTE:	The NT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.				

7.2.11.2   FT receives positive response from PT

Upon reception of an AUTHENTICATION-REQUEST from the PT, the FT shall stop timer F<MM_key.1> as described in EN 300 444 [6], subclause 8.32 and interwork the received message to a MM keyAllocate return result component and a MM networkAuthentication invoke component as specified in subclause 7.2.1.2.

Table 24: Mapping of AUTHENTICATION-REQUEST - KeyAllocate Return Result

	DECT message	MM component			
Item No	**AUTHENTICATION-REQUEST**	**KeyAllocate Return Result**	**Ref.**	**Map status**	**NOTE**
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	auth type			X	note
5	RAND			X	note
6	RES	cTMRes	8.4.2	M	
NOTE:	As part of the key allocation procedure, the FT interworks the AUTHENTICATION-REQUEST message to two MM components at the alpha interface: the KeyAllocate Return Result component and the Network Authentication Invoke component. The indicated parameters of the AUTHENTICATION-REQUEST message are inteworked to the Network Authentication Invoke component.				

The interworking of the AUTHENTICATION-REQUEST message to the Network Authentication Invoke component is specified in subclause 7.2.6.

7.2.11.3   FT receives negative response from PT

Upon reception of a AUTHENTICATION-REJECT from the PT, the FT shall stop timer F<MM_key.1> as described in EN 300 444 [6] and interwork the received message to a keyAllocate return error component as specified in subclause 7.2.1.2 and the following. The FT shall indicate value terminalRejected within the <errorValue> parameter and a <cTMTerminalRejectValue> including the <<reject reason>> if provided by the PT.

Table 25: Mapping of AUTHENTICATION-REJECT - KeyAllocate Return Error

	DECT message	MM component			
Item No	**AUTHENTICATION-REJECT**	**KeyAllocate Return Error**	**Ref.**	**Map status**	**NOTE**
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4		errorValue		X	
5	reject reason	RejectReason		O	

7.2.11.4   FT receives authentication response from network

Upon reception of the authentication result component from the network, either positive or negative, the FT shall interwork the received message to the corresponding DECT mobility management message as specified in subclause 7.2.6.

7.2.12   FT terminating access rights

The network may use this procedure to terminate the access rights of the PT as defined in subclause 9.1.2 of EN 301 144-1 [8].

There are no requirements in addition to the ones specified in subclause 7.2.1, generic interworking procedures for network initiated mobility management transactions with explicit acknowledgement.

Table 26: Mapping of AccessRightsTerminate Invoke - ACCESS-RIGHTS-TERMINATE-REQUEST

	MM component	DECT message			
Item No	AccessRightsTerminate Invoke	ACCESS-RIGHTS-TERMINATE-REQUEST	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMPortableIdentity	portable identity	8.4.1	M	
5	cTMFixedIdentity	fixed identity	8.4.1	M	

Table 27: Mapping of ACCESS-RIGHTS-TERMINATE-ACCEPT - AccessRightsTerminate Return Result

	DECT message	MM component			
Item No	ACCESS-RIGHTS-TERMINATE-ACCEPT	AccessRightsTerminate Return Result	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	

Table 28: Mapping of ACCESS-RIGHTS-TERMINATE-REJECT - AccessRightsTerminate Return Error

	DECT message	MM component			
Item No	ACCESS-RIGHTS-TERMINATE-REJECT	AccessRightsTerminate Return Error	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4		errorValue		X	
5	reject reason	RejectReason	8.4.2	O	

7.2.13   Network initiated ciphering

The network may use this procedure to initiate encryption of the radio connection as defined in subclause 9.3.4 of EN 301 144–1 [8].

There are no requirements in addition to the ones specified in subclause 7.2.1, generic interworking procedures for network initiated mobility management transactions with explicit acknowledgement.

NOTE: It should be noted that in this case the FT initiates the result component upon reception of a local primitive rather than upon reception of a DECT network layer message.

Table 29: Mapping of Ciphering Invoke - CIPHER-REQUEST

	MM component	DECT message			
Item No	Ciphering Invoke	CIPHER-REQUEST	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	cTMCipherInfo	cipher info	8.4.1	M	
5	cTMCipherKey			X	note 1
6	cTMPortableIdentity			X	note 2
NOTE 1:	The NT derives the cipher key during authentication and provides it to the FT in every CIPHER–REQUEST message. The key is to be used by the FT and need not be passed to the PT, that derives the cipher key itself.				
NOTE 2:	The NT provides the cTMPortableIdentity in case the component is transferred within an NCICs connection establishment message.				

Table 30: Mapping of CIPHER- REJECT - Ciphering Return Error

	DECT message	MM component			
Item No	CIPHER-REJECT	Ciphering Return Error	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4		errorValue		X	
5	reject reason	RejectReason	8.4.2	O	

7.2.14   Portable initiated ciphering

The PT may use this procedure to initiate encryption of the radio connection as defined in subclause 9.3.5 of EN 301 144-1 [8].

There are no requirements in addition to the ones specified in subclause 7.2.4, generic interworking procedures for PT initiated mobility management transactions with no explicit acknowledgement.

NOTE 1:   Upon receiving the MM cipheringSuggest invoke component, the network should start the procedure for cipher switching initiated by the network.

NOTE 2:   At the alpha interface the network initiated ciphering is not considered to be part of the same operation, hence the network applies a new invoke identifier. At the DECT air interface however, the following FT- initiated cipher request is considered part of the same procedure, using the same transaction identity.

NOTE 3:   The FT need not implement special interworking to ensure that the following FT- initiated cipher request apples the same transaction identity as used for the PT- initiated transaction. Since the FT- initiated ciphering has a higher priority, the procedure succeeds.

Table 31: Mapping of CIPHER-SUGGEST - CipheringSuggest Invoke

	DECT message	MM component			
Item No	CIPHER-SUGGEST	CipheringSuggest Invoke	Ref.	Map status	NOTE
1	protocol discriminator			X	
2	transaction identifier	invokeIdentifier	8.4.2	M	
3	message type	componentType operation	8.4.2	M	
4	cipher info	cTMCipherInfo	8.4.2	M	
NOTE:	According to the Alpha interface specification [8], it is not allowed to include this operation in an NCICs connection establishment message. Hence, the cTMPortableIdentity is not included.				

Table 32: Mapping of CipheringSuggest Return Error - CIPHER-REJECT

Item No	MM component CipheringSuggest Return Error	DECT message CIPHER-REJECT	Ref.	Map status	NOTE
1		protocol discriminator		X	
2	invokeIdentifier	transaction identifier	8.4.1	M	
3	componentType operation	message type	8.4.1	M	
4	errorValue			X	
5	RejectReason	reject reason		O	

7.3 Call control procedures

7.3.1 General

The FT does not need to support IAP (see ETS 300 434-2 [12]) options exceeding the CTM phase 1 requirements as defined in EN 301 175 [17] and EN 300 444 [6].

Unless specified otherwise, the call control interworking requirements as defined in ETS 300 434-2 [12] apply; the requirements described in this chapter only concern additions and/or modifications to IAP.

7.3.2 Outgoing call

The interworking procedures as defined in subclause 5.2.1.1.1 of ETS 300 434-2 [12] apply with the following modifications.

The FT does not need to support the DECT en-block dialling procedures. This includes both the transfer of the complete destination number within a <<Called party number>> either carried within a {CC-SETUP} or a {CC-INFO} message.

The FT shall apply case a) as defined in subclause 5.2.1.1.1 of ETS 300 434-2 [12], it shall not delay the transfer of the SETUP message to the network until it has collected further dialling information.

  NOTE 1: An early transfer of the SETUP to the network is required to facilitate an early start of ciphering, which may be used for the encryption of the dialling information.

In case of a point-to-multipoint configuration, the FT shall provide the FT- address within the <<Calling party number>> information element. The FT should not transfer the <<Calling party number>>, if received from the PT, towards the network as specified in subclauses 5.2.4.2.4 and 5.2.4.2.11 of ETS 300 434-2 [12].

FT shall transfer <<Portable identity>> (IPUI), <<Fixed identity>> (PARK) and <<Basic service>> (normal) as parameters within a MM MobilityManagementInfo invoke component, as described in the following.

  NOTE 2: For CTM phase 1, the support of service negotiation/fallback procedures is not required across the air interface. Therefore, for outgoing calls the fall back procedures towards the NT are outside the scope of the present document.

  NOTE 3: The network may delay the sending of the {SETUP-ACK} message until the completion of network initiated ciphering procedure (in order to cipher dialling information).
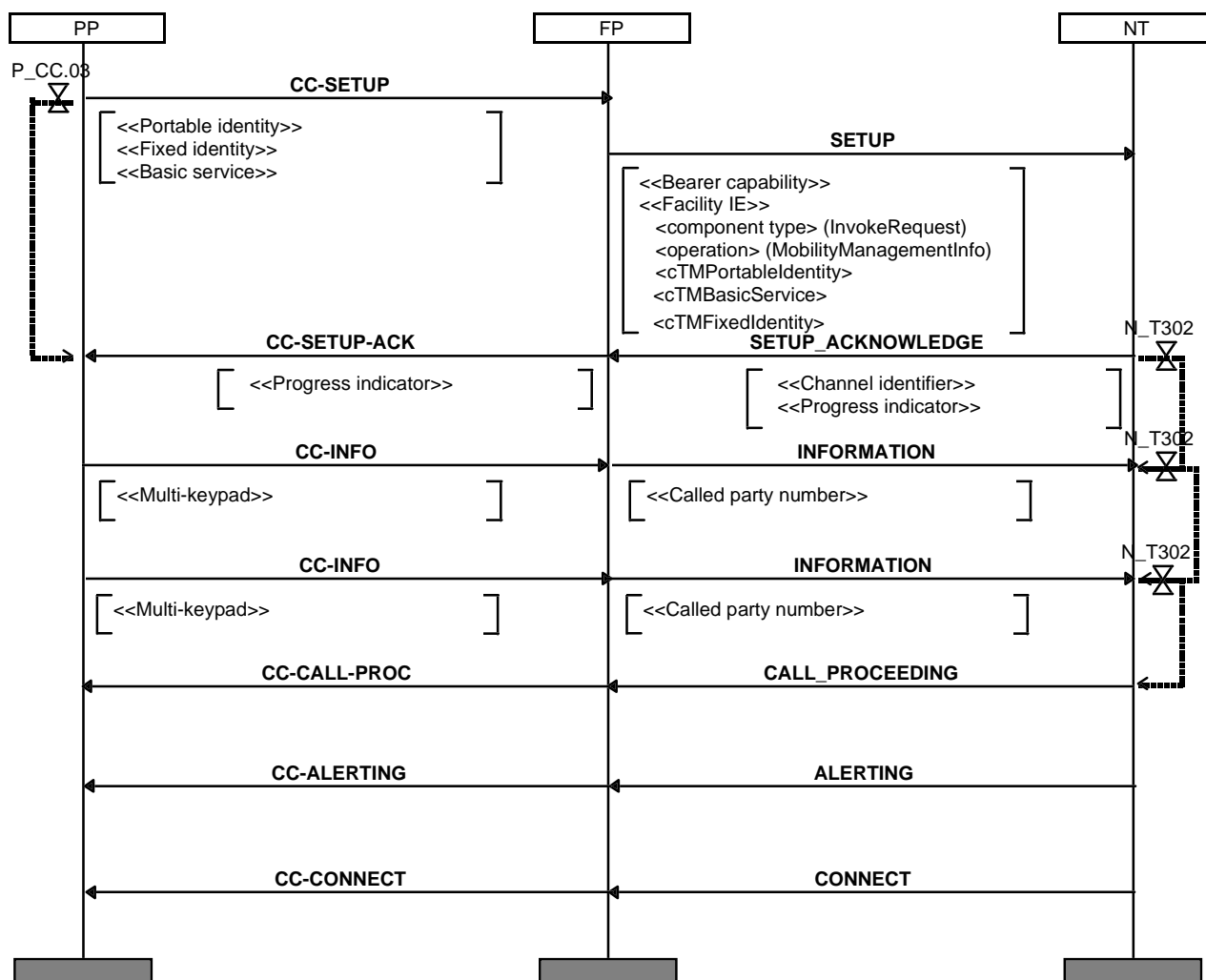
NOTE: Authentication and ciphering may be done in parallel to call establishment. The network may delay
         sending of SETUP_ACK until completion of ciphering.

Figure 11: Successful outgoing call, typical sequence

Table 33: Mapping of CC-SETUP - SETUP

Item No	DECTmessage CC-SETUP	CTM message SETUP	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	basic service	bearer capability	8.4.2	M	note 1
5	-	channel identification		X	note 2
6	-	facility		X	
6.1	-	invokeIdentifier		X	
6.2	-	componentType		X	
6.3	-	operation		X	
6.4	portable identity	cTMPortableIdentity	8.4.2	M	
6.5	fixed identity	cTMFixedIdentity	8.4.2	M	
6.6	basic service	cTMBasicService	8.4.2	M	note 1
7	-	calling party number		X	note 3
NOTE 1: The <<basic service>> is mapped to both the <<bearer capability>> and the <cTMBasicService>.					
NOTE 2: It is optional for the FT to include this information element.					
NOTE 3: The FT may include its FT- address (E.164 number) within the <<calling party number>>.					

Table 34: Mapping of SETUP-ACKNOWLEDGE - CC-SETUP-ACK

	CTM message	DECT message			
Item No	SETUP-ACKNOWLEDGE	CC-SETUP-ACK	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	progress indicator	progress indicator	8.4.1	M	

Table 35: Mapping of CC-INFO - INFORMATION

	DECTmessage	CTM message			
Item No	CC-INFO	INFORMATION	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	multi- keypad	called party number	8.4.2	C1	

C1:   This mapping is required (in overlap sending state) in case the information contained in <<multi- keypad>>
        concerns dialling information (and DTMF generation, which shall be performed by the FT, has not been
        activated).

Table 36: Mapping of CALL PROCEEDING - CC-CALL-PROC

	CTM message	DECT message			
Item No	CALL PROCEEDING	CC-CALL-PROC	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	channel identification	-		X	
5	progress indicator	progress indicator	8.4.1	M	
NOTE: For outgoing calls fall back procedures are outside the scope of the standard. Therefore, in this message support of <<bearer capability>> is not required.					

Table 37: Mapping of ALERTING - CC-ALERTING

	CTM message	DECT message			
Item No	ALERTING	CC-ALERTING	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	channel identification	-		X	
5	progress indicator	progress indicator	8.4.1	M	
NOTE: For outgoing calls fall back procedures are outside the scope of the standard. Therefore, in this message support of <<bearer capability>> is not required.					

Table 38: Mapping of CONNECT - CC-CONNECT

Item No	CTM message CONNECT	DECT message CC-CONNECT	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	channel identification	-		X	
5	progress indicator	progress indicator	8.4.1	M	
NOTE:	For outgoing calls fall back procedures are outside the scope of the standard. Therefore, in this message support of <<bearer capability>> is not required.				

Figure 12: Outgoing call failure, e.g. no resources in network.

7.3.3   Incoming call

The interworking procedures as defined in subclause 5.2.1.1.2 of ETS 300 434-2 [12] apply with the following modifications.

The FT does not need to support the overlap receiving procedures.

   NOTE 1: Within CTM, the complete destination address is retrieved from a database, and hence procedures for the piece wise transfer of the destination address are not required.

In order to check if it is a compatible destination, the FT shall check the <<Bearer capability>> and the <<Progress indicator>> information elements if present in the SETUP message received from the network. The FT shall accept the call in case one of the following conditions is met: the <<Bearer capability>> is set to «speech» OR to «3,1 kHz audio».

NOTE 2: GAP [6] does not include requirements for the support of voice band data. In case the speech service is used for voice band data, the quality of service may be limited due to the application of speech processing techniques e.g. muting/echo control.

In case of a point to multi-point configuration, the FT shall accept the call if the destination provided within the <<Called party number>> information element corresponds to its FT- address.

The FT should not interwork the <<Called party number>> information element across the air interface as specified in subclause 5.2.4.1.22 of ETS 300 434-2 [12].

The FT shall transfer the <cTMPortableIdentity> and the <cTMSignal> parameters received within a MM MobilityManagementInfo invoke component to the corresponding DECT information elements (<<Portable identity>> (IPUI), <<Signal>>) as described in the following.

Upon reception of an incoming call request, the FT may have to retrieve the PARK of the PT by initiating the Identification of PT procedure as defined in subclause 8.22 of EN 300 444 [6].

For incoming calls the FT shall apply fall back to a service compatible with [6].

NOTE 3: For CTM phase 1, the support of service negotiation/fallback procedures is not required across the air interface.
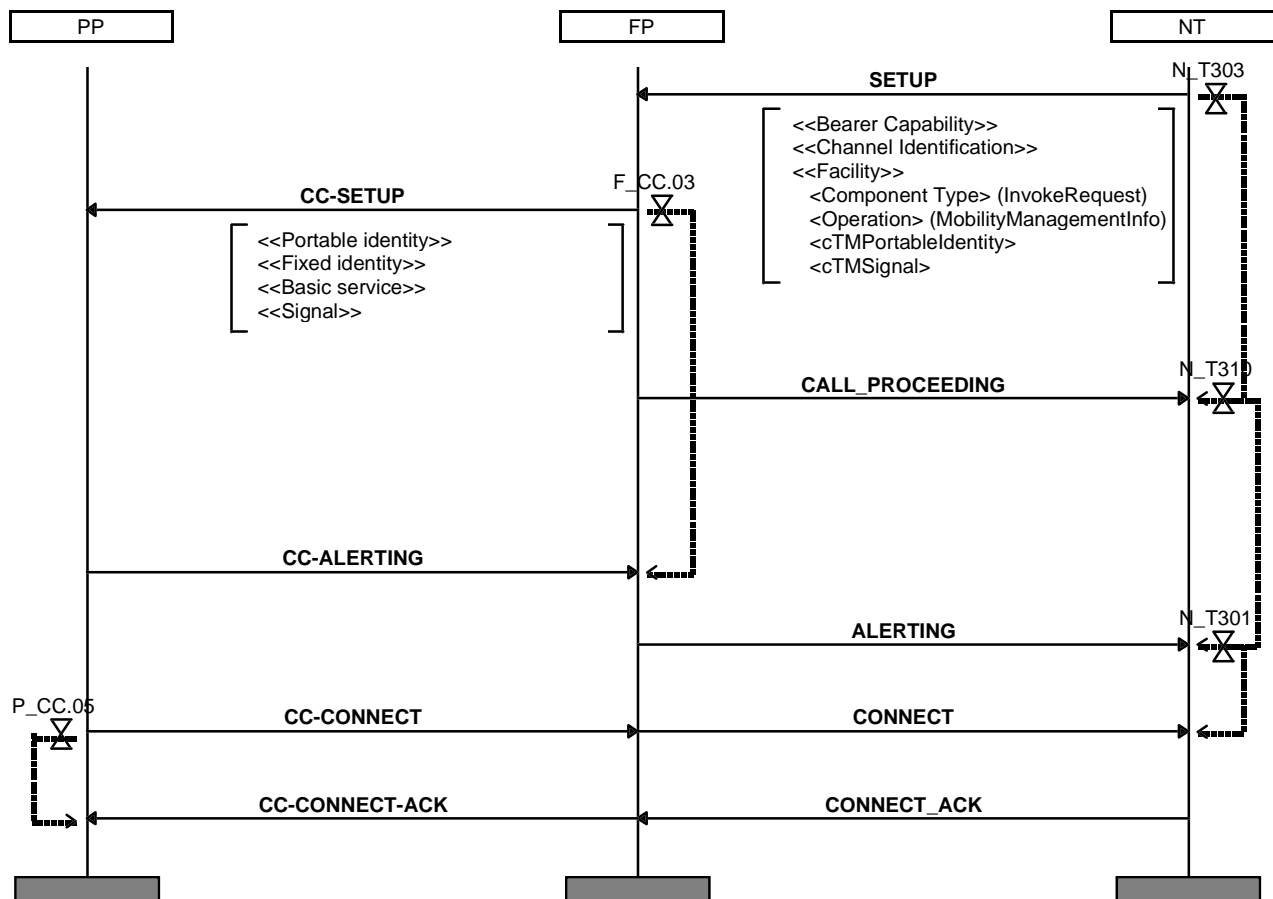
NOTE: Authentication and ciphering may be done prior or in parallel to call establishment.

Figure 13: Successful incoming call, typical scenario

Table 39: Mapping of SETUP - CC-SETUP

Item No	CTM message SETUP	DECT message CC-SETUP	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	bearer capability	basic service	8.4.1	M	
5	channel identification	-		X	
6	facility			X	
6.1	invokeIdentifier			X	
6.2	componentType			X	
6.3	operation			X	
6.4	cTMPortableIdentity	portable identity	8.4.1	M	
6.5	cTMSignal	signal	8.4.1	M	
7	calling party number	calling party number	8.4.1	M	
8	called party number	-		X	note
9	-	fixed identity		X	
NOTE: The called party number may include the FT- address (E.164 number); hence it is not relevant to map this information to the PT.					

Table 40: Mapping of CC-ALERTING - ALERTING

Item No	DECTmessage CC-ALERTING	CTM message ALERTING	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	-	bearer capability		X	
5	-	channel identification		X	

Table 41: Mapping of CC-CONNECT - CONNECT

Item No	DECTmessage CC-CONNECT	CTM message CONNECT	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	-	bearer capability		X	
5	-	channel identification		X	

Table 42: Mapping of CONNECT-ACKNOWLEDGE - CC-CONNECT-ACK

Item No	CTM message CONNECT-ACKNOWLEDGE	DECT message CC-CONNECT-ACK	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
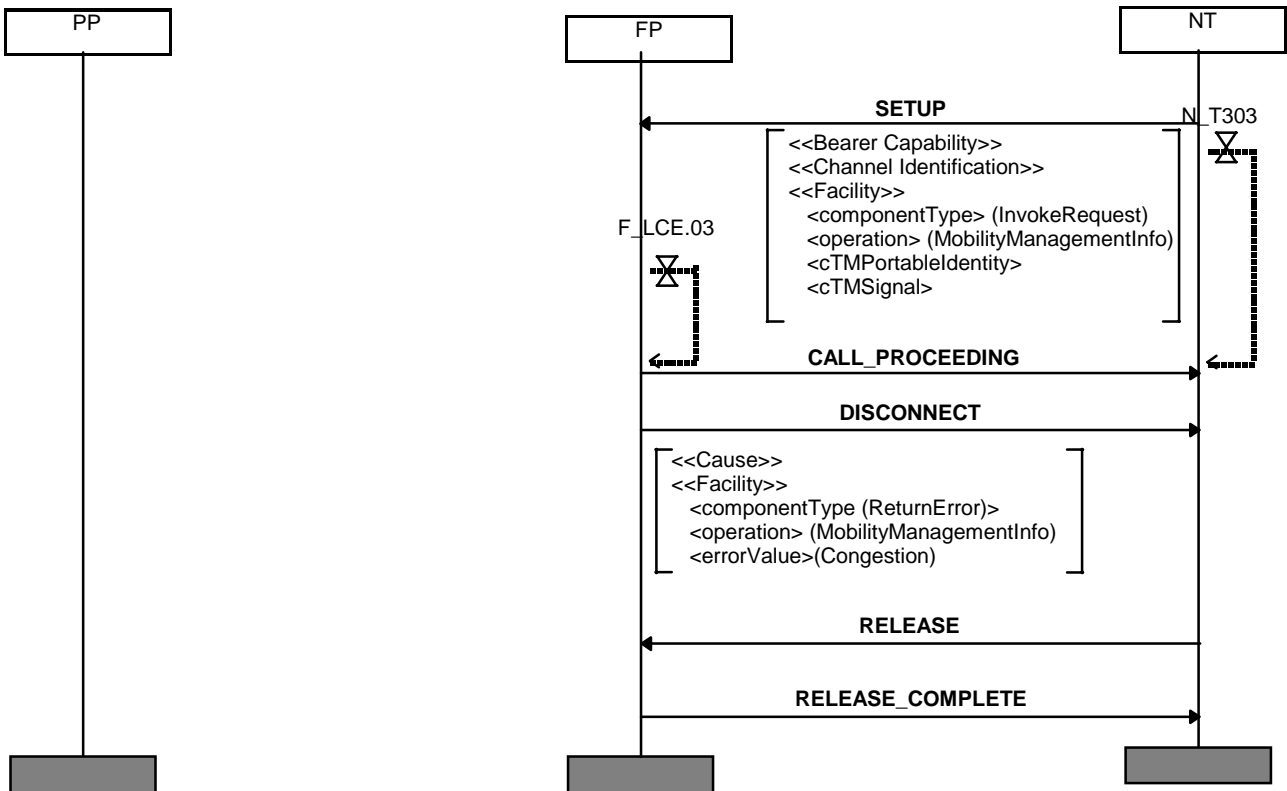
Figure 14: Incoming call failure, FT resources unavailable
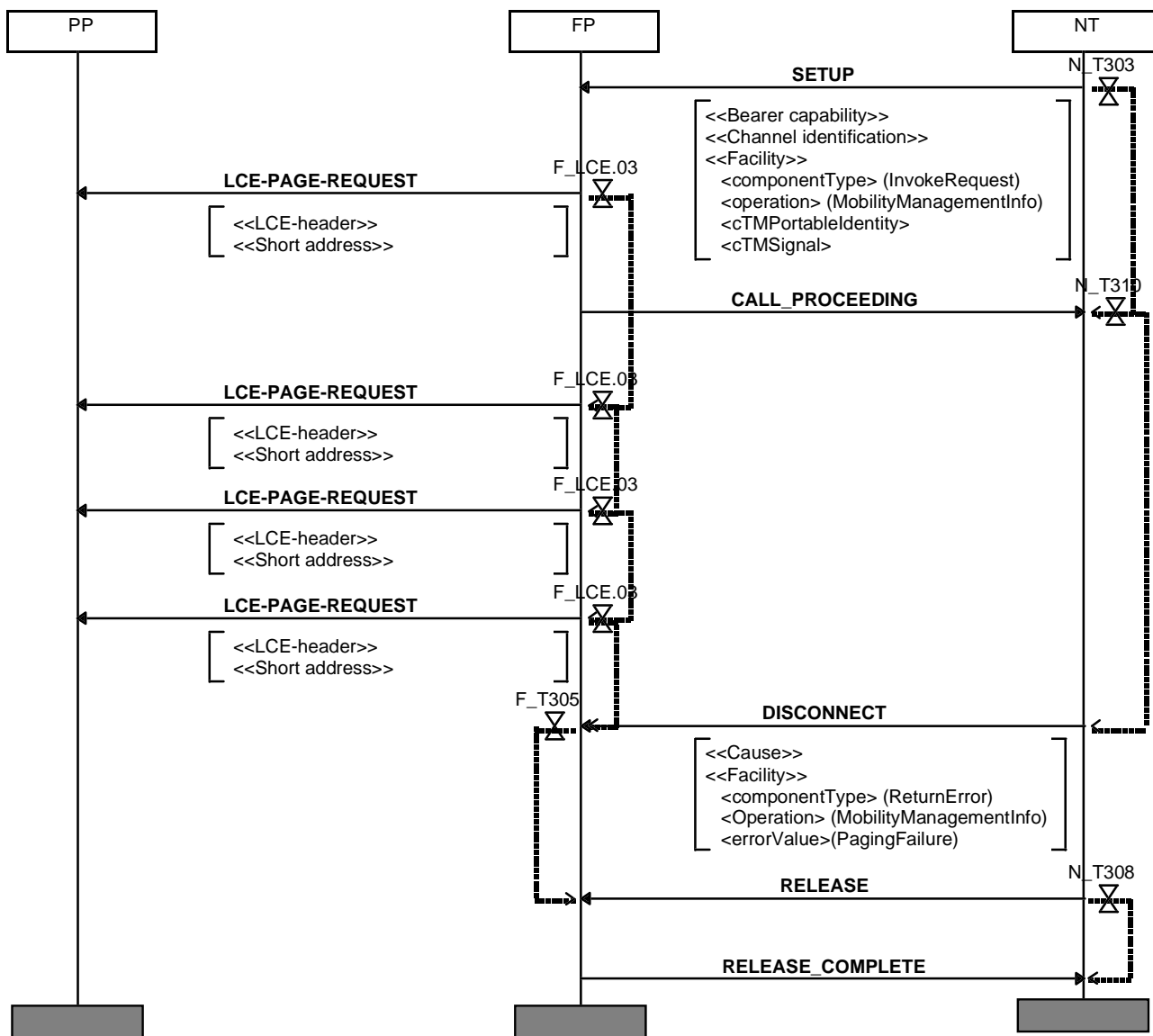
Figure 15: Incoming call failure, no response to paging request

7.3.4 Call progress information transfer

In case the network want to inform the user about the progress of a call without changing the call state, it may send a PROGRESS message. The FT shall interworking this message as specified in the following.

Table 43: Mapping of PROGRESS - CC-INFO

Item No	CTM message PROGRESS	DECT message CC-INFO	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	progress indicator	progress indicator	8.4.1	M	

7.3.5 Call release

The interworking procedures as defined in subclause 5.2.1.1.3 of ETS 300 434-2 [12] apply with the following modifications.

7.3.5.1   Network initiated release

In case of call release initiated by the NT with in band tones or announcements provided, the FT shall interwork the received DISCONNECT message including a <<Progress indicator>> information element to a {CC-INFO} message as described in the following message specifications.

The FT may transfer the <<Release reason>> information element received within a {CC-RELEASE} message to the <rejectReason> parameter within a MM MobilityManagementInfo return error component as described in the following message specifications.
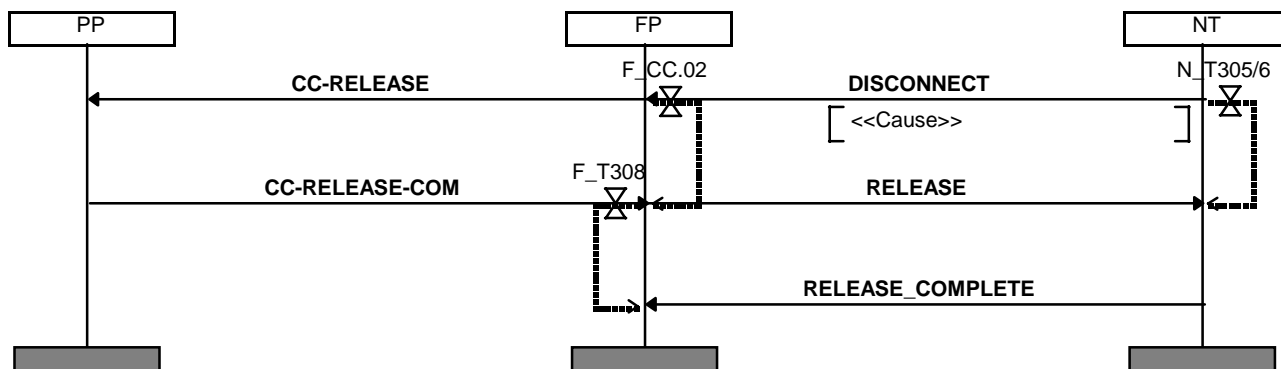
Figure 16: Normal call release, network initiated.

Table 44: Mapping of DISCONNECT - CC-INFO

	CTM message	DECT message			
Item No	DISCONNECT	CC-INFO	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
4	progress indicator	progress indicator	8.4.1	M	
NOTE:	This mapping is required due to the (conditional) rejection of CR.24. It requires approval of CR.22.				

Table 45: Mapping of DISCONNECT - CC-RELEASE

	CTM message	DECT message			
Item No	DISCONNECT	CC-RELEASE	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	
6	facility			X	
6.1	invokeIdentifier			X	
6.2	componentType			X	
6.3	operation			X	
6.4	errorValue			X	
6.5	RejectReason	release reason	8.4.1	O	

Table 46: Mapping of CC-RELEASE-COM - RELEASE

	DECTmessage	CTM message			
Item No	CC-RELEASE-COM	RELEASE	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	

7.3.5.2   PT initiated release
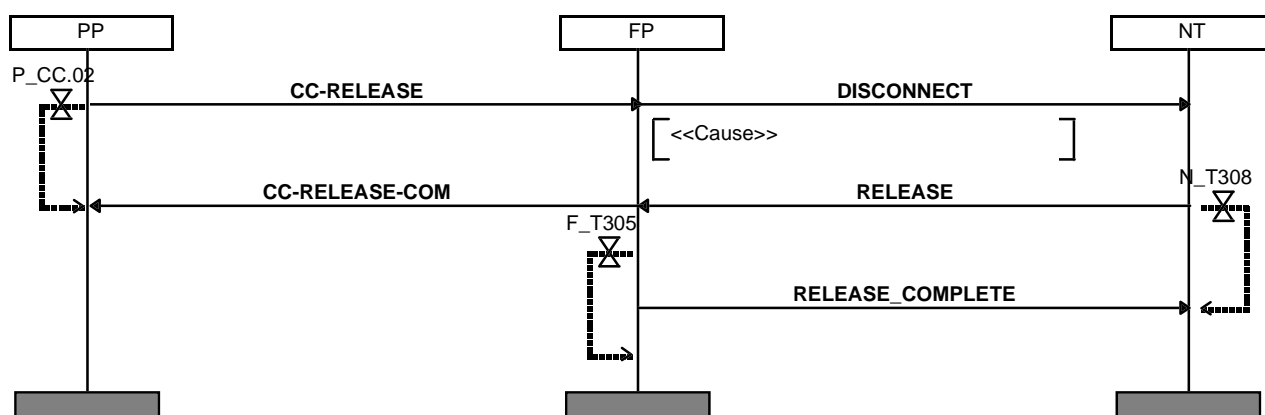
Figure 17: Normal call release, terminal initiated

Table 47: Mapping of CC-RELEASE - DISCONNECT

| Item No | DECTmessage | CTM message | | | |
	CC-RELEASE	DISCONNECT	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	-	cause			

Table 48: Mapping of RELEASE - CC-RELEASE-COM

| Item No | CTM message | DECT message | | | |
	RELEASE	CC-RELEASE-COM	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	

7.3.5.3   Other release cases

Table 49: Mapping of RELEASE - CC-RELEASE

| Item No | CTM message | DECT message | | | |
	RELEASE	CC-RELEASE	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	

Table 50: Mapping of RELEASE-COMPLETE - CC-RELEASE-COM

| Item No | CTM message | DECT message | | | |
	RELEASE-COMPLETE	CC-RELEASE-COM	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.1	M	

Table 51: Mapping of CC-RELEASE-COM - DISCONNECT

Item No	DECTmessage CC-RELEASE-COM	CTM message DISCONNECT	Ref.	Map status	NOTE
1	protocol discriminator	protocol discriminator		M	
2	transaction identifier	transaction identifier		M	
3	message type	message type	8.3.2	M	
4	-	cause		X	
5	-	facility		X	
5.1	-	invokeIdentifier		X	
5.2	-	componentType		X	
5.3	-	operation		X	
5.4		errorValue		X	
5.5	release reason	RejectReason	8.4.2	O	note
NOTE:	The MM return error component applies in case of an incoming call failure, rejected by the PT. In this case the release reason, if provided, may be mapped to the <RejectReason>.				

7.3.6 Keypad information transfer

The interworking procedures as defined in subclause 5.2.2.1 of ETS 300 434-2 [12] apply with the following modifications.

Upon reception of a request for "go to DTMF dialling, defined tone length", the FT shall start the generation of DTMF tones. The handling of supplementary service related keypad information signalling is outside the scope of the present document.

7.4 Other interworking procedures

7.4.1 Interaction in-between MM transactions

The FT shall apply the priority rules as described in subclause 15.5 of EN 300 175-5 [5]. These priority rules imply that only one MM transaction may be initiated towards the PT at a time.

NOTE 1: The priority rules shall also take into account non-interworked procedures e.g. an FT- initiated identity request procedure.

The FT shall queue a network initiated MM invoke request that is received while another FT-initiated mobility management transaction is active. The FT may either queue or reject a network initiated MM invoke request that is received while another network initiated mobility management transaction is active.

In case the FT rejects the MM invoke component, is shall apply the procedures as defined in subclause 7.2.1 generic interworking procedures, network initiated transaction, explicit acknowledgement. In this case, the FT shall apply error value «priority rule violation».

NOTE 2: Within the CTM network, more than one nodes may initiate mobility management transactions. This is one of the reasons why the CTM network is not required to provide co-ordination between mobility transactions.

NOTE 3: There are no limitations to the number of parallel MM- transactions the CTM network may initiate. However, considering that larger queue sizes result in MM- timer problems, there seems no justification to mandate the FT to support queuing of network initiated MM- transactions.

7.4.2 Interactions between MM- and CC- transactions

Subclause 6.9.6 of EN 300 444 (GAP) [6] defines the FT requirements concerning the states in which the MM procedures shall be supported.

7.4.3   Other interactions between local and interworked procedures

EN 300 444 [6] and EN 301 144-1 [8] specify procedures for which there is no interworking procedure defined in the present document; these procedures are local to the interface. However, some of these procedure may interact with procedures for which interworking is defined. The following cases have been identified: upon reception of a STATUS or RESTART message, the FT may have to initiate clearing of call control and or mobility management transactions.

NOTE: There are no requirements concerning the interactions required upon reception of a locate cancel; the FT need not initiate clearing of ongoing transactions upon receiving a locate cancel invoke component.

7.4.4   Error handling

There are no requirements regarding error handling.

NOTE: The above implies that upon NCICs connection (establishment) failure, the FT need not immediately reject the associated MM- transaction. Likewise, in case of a radio connection failure, the FT need not immediately initiate clearing of the related transactions towards the NT. There are no requirements specified since this is not required to achieve interoperability. However, the drawback is that that radio resources may be occupied longer than required.

8   Message mappings

8.1   General

Within this specification, the following approach/conventions are used:

1) The mapping status is based on table 1 of EN 301 144-1 [8] (and not on GAP [6]).

2) The message mapping specifications only cover messages/information elements that are relevant for the CTM application. The handling of other (optional) messages/information elements is outside the scope of the present document.

3) For informative reasons, the mapping interworking specifications include information elements that are not mapped but required on one of the interfaces.

4) The mapping of information elements and its fields/values as specified in ETS 300 434-2 (IAP) [12] applies unless explicitly stated otherwise; the present document only defines additions and/or modifications.

5) MM information is transferred within NCICs messages. However, for the mapping of MM information it is irrelevant which NCICs message was used to transfer the information. Therefore, for MM- messages the mapping tables only show the mapping between the MM components and the DECT MM- messages.

6) The MM mapping tables do not include addressing parameters which are never mapped. The handling of these parameters is clarified by means of an example.

7) The order of information elements within the message interworking specifications need not be in accordance to the requirements of the DECT and/or alpha interface specifications.

8) All fields/parameters are mapped transparently unless explicitly specified otherwise.

NOTE: The reasons for specifying call control message/information mapping are as follows:

- the status of message/information mappings and or interworking procedures differs from IAP [12];

- the message/information mapping or interworking procedures is different from IAP e.g. to overcome the limitations of a GAP terminal. For <<called/called party number party number>> and the <<release reason>> information elements, the present document specifies requirements that conflict with the requirements specified in IAP.

8.2   Mobility management message/component mapping

8.2.1   MM component to DECT message

NOTE 1:   No requirements are specified concerning PT- initiated transactions that are not required for CTM, e.g. PT- initiated termination of access rights; whether FT or LE should reject this transaction.

NOTE 2:   The status corresponds with the user side status for the corresponding feature as specified in table 1 of EN 301 144-1 [8].

Table 52: MM component to DECT message mapping

Item No	CTM component	DECT message	Ref.	Map Status
1	AccessRightsRequest Return Result	ACCESS-RIGHTS-ACCEPT	7.2.10	O
2	AccessRightsRequest Return Error	ACCESS-RIGHTS-REJECT	7.2.10	O
3	AccessRightsTerminate Invoke	TERMINATE-ACCESS-RIGHTS-REQUEST	7.2.12	O
4	Ciphering Invoke	CIPHER_REQUEST	7.2.13	M
5	CipheringSuggest Return Error	CIPHER_REJECT	7.2.14	O
6	IdentityRequest Invoke	IDENTITY_REQUEST	7.2.5	M
7	KeyAllocate Invoke	KEY_ALLOCCATE	7.2.11	M
8	LocationRegistration Return Result	LOCATE_ACCEPT	7.2.8	M
9	LocationRegistration Return Error	LOCATE_REJECT	7.2.8	M
10	LocationRegistrationSuggest Invoke	MM_INFO_SUGGEST	7.2.9	M
11	NetworkAuthentication Return Result	AUTHENTICATION_REPLY	7.2.6	M
12	NetworkAuthentication Return Error	AUTHENTICATION_REJECT	7.2.6	M
13	TerminalAuthentication Invoke	AUTHENTICATION_REQUEST	7.2.7	M
NOTE:	The handling of non- interworked messages is outside the scope of the present document.			

8.2.2   DECT message to MM component

NOTE 1:   No requirements are specified concerning PT- initiated transactions that are not required for CTM e.g. PT- initiated termination of access rights; whether FT or LE should reject this transaction.

NOTE 2:   The status is based on the alpha interface standard [8] and not on GAP [6].

Table 53: DECT message to MM component mapping

Item No	DECT message	CTM component	Ref.	Map Status
1	ACCESS-RIGHTS- REQUEST	AccessRights Invoke	7.2.10	O
2	ACCESS-RIGHTS- TERMINATE-ACCEPT	AccessRightsTerminate Return Result	7.2.12	O
3	ACCESS-RIGHTS-TERMINATE-REJECT	AccessRightsTerminate Return Error	7.2.12	O
4	AUTHENTICATION_REQUEST	NetworkAuthentication Invoke	7.2.6	M
5	AUTHENTICATION_REQUEST	KeyAllocate Return Result	7.2.11	M
6	AUTHENTICATION_REPLY	TerminalAuthentication Return Result	7.2.7	M
7	AUTHENTICATION_REJECT	TerminalAuthentication Return Error	7.2.7	M
8	AUTHENTICATION_REJECT	KeyAllocate Return Error	7.2.11	M
9	CIPHER_SUGGEST	CipheringSuggest Invoke	7.2.14	M
10	CIPHER_REJECT	Ciphering Return Error	7.2.13	O
11	IDENTITY_REPLY	IdentityRequest Return Result	7.2.5	M
12	IDENTITY_REPLY	IdentityRequest Return Error	7.2.5	M
13	LOCATE_REQUEST	LocationRegistration Invoke	7.2.8	M
NOTE:	The handling of non- interworked messages is outside the scope of the present document.			

8.3   Call control message mapping

8.3.1   DSS1 message to DECT message

Table 54: DSS1 message to DECT message mapping

Item No	CTM message	DECT message	Ref.	Map Status
1	ALERTING	CC-ALERTING	7.3.2	M
2	CALL PROCEEDING	CC-CALL-PROC	7.3.2	M
3	CONNECT	CC-CONNECT	7.3.2	M
4	CONNECT-ACKNOWLEDGE	CC-CONNECT-ACK	7.3.3	M
5	PROGRESS	CC-INFO (note 1)	7.3.4	O
6	DISCONNECT	CC-INFO (note 1)	7.3.5	O
7	DISCONNECT	CC-RELEASE	7.3.5	M
8	RELEASE	CC-RELEASE-COM	7.3.5	M
9	RELEASE-COMPLETE	CC-RELEASE-COM	7.3.5	M
10	SETUP	CC-SETUP	7.3.3	M
11	SETUP-ACKNOWLEDGE	CC-SETUP-ACK	7.3.2	M
NOTE 1:	CTM phase 1 PP's need not support the handling of a <<Progress indicator>> contained within a CC-INFO message. Hence, it is not applicable to mandate the FT to supports this interworking.			
NOTE 2:	The handling of non-interworked messages is outside the scope of the present document.			

8.3.2   DECT message to DSS1 message

Table 55: DECT message to DSS1 message mapping

Item No	DECT message	CTM message	Ref.	Map Status
1	CC-ALERTING	ALERTING	7.3.3	M
2	CC-CONNECT	CONNECT	7.3.2	M
3	CC-INFO	INFORMATION	7.3.2	M
4	CC-RELEASE	DISCONNECT	7.3.5	M
5	CC-RELEASE-COM	DISCONNECT	7.3.5	M
6	CC-RELEASE-COM	RELEASE	7.3.5	M
7	CC-SETUP	SETUP	7.3.2	M
8	-	CALL PROCEEDING	7.3.3	X
NOTE 1:	Mapping of CC-INFO does not apply in case of FT- generated DTMF sending.			
NOTE 2:	In case the network indicates that fallback is possible, the FT shall indicate the selected <<bearer capability>> within {CALL PROCEEDING}.			
NOTE 3:	The handling of non- interworked messages is outside the scope of the present document.			

8.4 Information element/parameter mapping

8.4.1 CTM information element/parameter to DECT information element

Table 56: CTM information element/parameter to DECT information element mapping

Item No	CTM message	DECT message	Ref.	Map Status
1	bearer capability	basic service (note 3)	[12], 5.2.5.1.1	
2	calling party number	calling party number	[12], 5.2.5.1.2	
3	_componentType	message type	8.4.1.2	
4	_operation			
5	invoke identifier	transaction identifier	8.4.1.3	
6	_cTMAllocType	allocation type	8.4.1.1	
7	_cTMAuthenticationType	Auth type	8.4.1.1	
8	_cTMCipherInfo	cipher info	8.4.1.1	
9	_cTMFixedIdentity	fixed identity	8.4.1.1	
10	_cTMIdentityType	identity type	8.4.1.3	
11	_cTMPortableIdentity	portable identity	8.4.1.1	
12	_cTMRand	RAND	8.4.1.1	
13	_cTMRes	RES	8.4.1.1	
14	_cTMRs	RS	8.4.1.1	
15	_cTMServiceClass	service class	8.4.1.1	
16	_cTMSignal	signal	8.4.1.1	
17	_RejectReason	reject reason	8.4.1.1	
18	progress indicator	progress indicator (note 4)	[12], 5.2.5.1.15	
NOTE 1:	This table only specifies information elements/parameters that are not interworked/mapped; the handling of other information elements/parameters is defined by the respective interface protocol specifications (GAP, alpha interface).			
NOTE 2:	The mapping status is included in the message interworking/mapping specifications.			
NOTE 3:	The present document only requires support of the mapping for code value corresponding with "speech" and "3.1 kHz audio", see subclause 7.4.3.			
NOTE 4:	Since GAP only requires support of code value "0", value "8" should be interworked to value "0" to ensure that the U-plane is connected.			

8.4.1.1 General/transparent mapping

Across the alpha interface, the CTM mobility management parameters include the corresponding DECT information elements which are defined as octet strings. The octet string received from the NT is inserted without further processing into the DECT message; there is no real interworking. However, the FT has to ensure that across the air interface the information elements are in the correct order as defined in EN 300 175-5 [5].

NOTE 1: EN 301 144-1 [8] defines the order in which the parameters are transferred across the alpha interface.

NOTE 2: All off the following DECT IE's are defined as octet/bit strings: FixedIdentity, IPEI, IPUI, AuthType, AllocType, PortableCapabilities, CTMLocationAreaIdentity, CipherKey, CipherInfo, ServiceClass, BasicService, Rand, Res, Rs, RejectReason, Signal.

8.4.1.2   <_componentType>+ <_operation> - << message type>>

Table 57: <_componentType>+ <_operation> - << message type>> mapping

Item No	CTM information <_operation>	CTM information <_componentType>	DECT information << message type>>	Map status	NOTE
1	AccessRightsRequest	Return Result	ACCESS-RIGHTS-ACCEPT		
2	AccessRightsRequest	Return Error	ACCESS-RIGHTS-REJECT		
3	AccessRightsTerminate	Invoke	ACCESS-RIGHTS-TERMINATE-REQUEST		
4	Ciphering	Invoke	CIPHER_REQUEST		
5	CipheringSuggest	Return Error	CIPHER_REJECT		
6	IdentityRequest	Invoke	IDENTITY_REQUEST		
7	KeyAllocate	Invoke	KEY_ALLOCCATE		
8	LocationRegistration	Return Result	LOCATE_ACCEPT		
9	LocationRegistration	Return Error	LOCATE_REJECT		
10	LocationRegistrationSuggest	Invoke	MM_INFO_SUGGEST		
11	NetworkAuthentication	Return Result	AUTHENTICATION_REPLY		
12	NetworkAuthentication	Return Error	AUTHENTICATION_REJECT		
13	TerminalAuthentication	Invoke	AUTHENTICATION_REQUEST		

NOTE 1:   The <_componentType> defines whether the MM component concerns an invoke, a return result or reject component. The <_operation> on the other hand defines the nature of the operation e.g. location registration and/or network authentication. Across the DECT air interface, these two information fields are combined in the message type that indicated e.g. for a LOCATE-REQUEST the procedure is location registration and the type is an invoke.

NOTE 2:   Similar information is contained in subclause 8.2. Therefore, the mapping status is not repeated in this table.

8.4.1.3   <_cTMIdentityType> - <<identity type>>

The coding of <_cTMIdentityType> is specified as an enumerated type. The value of this enumerated type needs to be interworked to the <type> field of the <<Identity type>> as defined in the following.

Table 58: <_componentType>+ <_operation> - << message type>> mapping

Item No	CTM information <_cTMIdentityType>	DECT information < type>	Ref.	Map status	NOTE
1	ipui (4)	ipui (0)		M	
2	ipei (5)	ipei (16)		M	

NOTE: All other values are outside the scope of the present document.

8.4.1.4   <_invokeIdentifier> - << transaction identifier>>

The <_invokeIdentifier> and the << transaction identifier>> include a reference to a transaction/MM procedure. There is no fixed mapping between the references/values used at both interfaces. However, during an
MM- procedure/transaction there is an association/one to one relation between the value contained in the <_invokeIdentifier> and the << transaction identifier>>.

8.4.2   DECT information element to CTM information element/parameter

Table 59: DECT information element to CTM information element/parameter mapping

Item No	DECT message	CTM message	Ref.	Map Status
1	auth type	_cTMAuthenticationType	8.4.2.1	
2	basic service	_ctmBasicService	8.4.2.1	
3	basic service	bearer capability	[12], 5.2.5.1	
4	cipher info	_cTMCipherInfo	8.4.2.1	
5	fixed identity	_cTMFixedIdentity	8.4.2.1	
6	fixed identity	_cTMOldLocationAreaIdentity	8.4.2.2	
7	location area			
8	message type	_componentType	8.4.2.3	
9		_operation		
10	multi- keypad	called party number		
11	portable identity	_cTMPortableIdentity	8.4.2.1	
12	RAND	_cTMRand	8.4.2.1	
13	reject reason	_RejectReason	8.4.2.1	
14	RES	_cTMRes	8.4.2.1	
15	service class	_cTMServiceClass	8.4.2.1	
16	terminal capability	_cTMPortableCapabilities	8.4.2.1	
17	transaction identifier	_invokeIdentifier	8.4.2.4	
NOTE 1: This table only specifies information elements/parameters that are not interworked/mapped; the handling of other information elements/parameters is defined by the respective interface protocol specifications (GAP, alpha interface).				
NOTE 2: The mapping status is included in the message interworking/mapping specifications.				

8.4.2.1   General/transparent mapping

Across the alpha interface, the CTM mobility management parameters include the corresponding DECT information elements which are defined as octet strings. The octet string received from the NT is inserted without further processing into the DECT message; there is no real interworking. However, the FT has to ensure that across the air interface the information elements are in the correct order as defined in EN 300 175-5 [5].

   NOTE 1: EN 301 144-1 [8] defines the order in which the parameters are transferred across the alpha interface.

   NOTE 2: All off the following DECT IEEE's are defined as octet/bit strings: FixedIdentity, IPEI, IPUI, AuthType, AllocType, PortableCapabilities, CTMLocationAreaIdentity, CipherKey, CipherInfo, ServiceClass, BasicService, Rand, Res, Rs, RejectReason, Signal.

8.4.2.2   Fixed identity + location area - _cTMOldLocationAreaIdentity

Across the air interface the fixed identity and the location area length are transferred in two information elements. At the alpha interface however, the information is merged into one parameter; this parameter, the _cTMLocationAreaIdentity, shall contains the old PARI + RPN provided in the <<fixed identity>>, but truncated to the length corresponding to the LAL indicated in the <<location area>>.

8.4.2.3   Message type - _componentType+ _operation

Table 60: Message type - _componentType+ _operation mapping

	DECT information	CTM information	CTM information		
Item No	<< message type>>	<_operation>	<_componentType>	Map status	NOTE
1	ACCESS-RIGHTS-REQUEST	AccessRights	Invoke		
2	ACCESS-RIGHTS-TERMINATE-ACCEPT	AccessRightsTerminate	Return Result		
3	ACCESS-RIGHTS-TERMINATE-REJECT	AccessRightsTerminate	Return Error		
4	AUTHENTICATION_REQUEST	NetworkAuthentication	Invoke		
5	AUTHENTICATION_REQUEST	KeyAllocate Return	Result		
6	AUTHENTICATION_REPLY	TerminalAuthentication	Return Result		
7	AUTHENTICATION_REJECT	TerminalAuthentication	Return Error		
8	AUTHENTICATION_REJECT	KeyAllocate	Return Error		
9	CIPHER_SUGGEST	CipheringSuggest	Invoke		
10	CIPHER_REJECT	Ciphering	Return Error		
11	IDENTITY_REPLY	IdentityRequest	Return Result		
12	IDENTITY_REPLY	IdentityRequest	Return Error		
13	LOCATE_REQUEST	LocationRegistration	Invoke		
NOTE 1: The <_componentType> defines whether the MM component concerns an invoke, a return result or reject component. The <_operation> on the other hand defines the nature of the operation e.g. location registration and/or network authentication. Across the DECT air interface, these two information fields are combined in the message type that indicated e.g. for a LOCATE-REQUEST the procedure is location registration and the type is an invoke.					
NOTE 2: Similar information is contained in subclause 8.2. Therefore, the mapping status is not repeated in this table.					

8.4.2.4   Transaction identifier - _invokeIdentifier

The <_invokeIdentifier> and the << transaction identifier>> include a reference to a transaction/MM procedure. There is no fixed mapping between the references/values used at both interfaces. However, during an MM- procedure/transaction there is an association/one to one relation between the value contained in the <_invokeIdentifier> and the << transaction identifier>>.

Annex A (informative):
Open issues overview (temporary annex)

This annex provides an overview of the open issues as well as assumptions that need confirmation.

No	Description	Clause	Resp/involved
1	Alpha Interface specification does not allow cipher suggest as an NCICs establishment message. Is this correct?		SPS-5
2	In IAP the <<end to end compatibility>> shall be mapped if relevant for the network. Is it relevant for CTM/alpha interface.		SPS-5
3	Requirements concerning support of fallback procedures are unclear --> at air interface no support is required for fallback, hence FT will have to support it. FT could always select the highest provided option that is compatible with the CTM phase 1/GAP requirements. This may result in always selecting the lowest possible/fall back solution.		SPS-5
4	Applicability of call control requirements specified in IAP part 2 needs to be checked in detail and additions/modifications need to be specified as required.		
5	Add informative annex with coding example of MM component. Add informative annex showing mapping of MM- fields related to addressing that are not mapped addressing.		
6	Is it acceptable not to queue multiple simultaneous MM requests received from the CTM network.		SPS-3

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

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

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

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

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

History

Document history				
V1.1.1	August 1998	Public Enquiry	PE 9849:	1998-08-07 to 1998-12-04
V1.1.1	June 1999	Vote	V 9934:	1999-06-07 to 1999-08-20