ETSI TS 102 265 V1.1.1 (2003-10)

Technical Specification

Digital Enhanced Cordless Telecommunications (DECT); DECT access to IP networks

Reference

DTS/DECT-A0181

Keywords

DECT, access, IP, network

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

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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

Foreword

This Technical Specification (TS) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT).

The present document is based on DECT Common Interface (CI) specification EN 300 175, parts 1 [1] to 8 [8] to enable DECT terminals to interwork in the public and private environment when connected to an IP network.

In addition, for the purpose of interoperability and wherever it is found appropriate, the present document takes into consideration the requirements of:

- the DECT Generic Access Profile (GAP), EN 300 444 [13] to enable the same DECT portable part (PT) to interwork with a DECT fixed part (FP) complying to the GAP requirements, irrespective of whether this FP provides residential, business or public access services;

- the DECT Packet Radio Service (DPRS), EN 301 469 [16] to enable DECT data terminals to interwork with a DECT FP complying to the DPRS requirements, irrespective of whether this FP provides residential, business or public access services.

General attachment requirements are based on EN 301 406 [15].

Further details on the DECT system may be found in TR 101 178 [11], EN 300 176-1 [9] and EN 300 176-2 [10].

1 Scope

The present document specifies additional requirements for DECT Internet Protocol (IP) applications including networking aspects, Voice over IP (VoIP), mobility and quality of service properties.

It provides an end system, i.e. termination of IP into the DECT Fixed Termination (FT).

NOTE: Transparent IP packet service is described in EN 301 469 [16], DPRS standard.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

[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 coding and transmission".

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

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

[11] ETSI TR 101 178: "Digital Enhanced Cordless Telecommunications (DECT); A High Level Guide to the DECT Standardization".

[12] ETSI TR 102 010: "Digital Enhanced Cordless Telecommunications (DECT); DECT access to IP networks".

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

[14] ETSI EN 300 824: "Digital Enhanced Cordless Telecommunications (DECT); Cordless Terminal Mobility (CTM); CTM Access Profile (CAP)".

[15] ETSI EN 301 406: "Digital Enhanced Cordless Telecommunications (DECT); Harmonized EN for Digital Enhanced Cordless Telecommunications (DECT) covering essential requirements under article 3.2 of the R&TTE Directive; Generic radio".

[16] ETSI EN 301 469 (all parts): "Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Service (DPRS) Test Case Library (TCL)".

[17] IETF RFC 3344: "IP Mobility Support for IPv4".

[18] IETF RFC 3261: "SIP: Session Initiation Protocol".

[19] IETF RFC 2327: "SDP: Session Description Protocol".

[20] IETF RFC 2030: "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI".

[21] IETF RFC 1305: "Network Time Protocol (Version 3) Specification, Implementation and Analysis".

[22] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[23] IETF RFC 2806: "URLs for Telephone Calls".

[24] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[25] IETF RFC 2794: "Mobile IP Network Access Identifier Extension for IPv4".

[26] IETF RFC 2003: "IP Encapsulation within IP".

[27] IETF RFC 2821: "Simple Mail Transfer Protocol".

[28] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[29] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

3 Definitions, symbols and abbreviations

Generic DECT definitions, symbols and abbreviations can be found in the base standard EN 300 175-1 [1].

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 175-1 [1], RFC 3344 [17], RFC 3261 [18] and the following apply:

DECT User Agent (UA): a logical entity comprising the SIP functionality provided by the DECT Fixed Termination User Agent (FT-UA) and DECT Portable Termination User Agent (PT-UA). Physically it includes one DECT FP and one or more DECT PPs.

3.2 Symbols

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

M	mandatory to support (provision mandatory, process mandatory)
O	optional to support (provision optional, process mandatory)
I	out-of-scope (provision optional, process optional) not subject for testing
C	conditional to support (process mandatory)
N/A	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.

3.3 Abbreviations

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

AC	Access Code
ACK	ACKnowledge
ADPCM	Adaptive Differential Pulse Code Modulation
AOR	Address-Of-Record
AP	Access Point
CAP	CTM Access Profile
CI	Common Interface
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DIMS	DECT IP Mobility signature
DLC	Data Link Control
DPRS	DECT Packet Radio Service
EN	European Norm
FA	Foreign Agent
FP	Fixed Part
FT	Fixed Termination
FT-UA	Fixed Termination User Agent
GAP	Generic Access Profile
HA	Home Agent
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPUI	International Portable User Identity
IPv4	IP version 4
IPv6	IP version 6
IWU	Inter Working Unit
MAC	Medium Access Control
MM	Mobility Management
MN	Mobile Node
MPEG	Moving Picture Experts Group
MSA	Mobility Security Association
NAI	Network Access Identifier
NTP	Network Time Protocol
NWK	NetWorK
PP	Portable Part
PPP	Point to Point Protocol
PT	Portable Termination
PT-UA	Portable Termination User Agent
QoS	Quality of Service
RFC	Request For Comment
RSVP	ReSerVation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-Time Streaming Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure

SPI	Security Parameter Index
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
VoIP	Voice over IP

4 General

The main focus of the present document is on provision of speech services. This however should not preclude implementers of using it for other services too. IP mobility and Session Initiation Protocol (SIP) interworking for example are applicable to any DECT device that provides access to an IP network.

Some of the requirements specified in the present document are relevant only to IP version 4 (IPv4). Support of IPv6, as well as, non speech services may be added in future versions of the document.

Clause 6 provides the reference configuration of the protocols and services relevant for the present document. Clause 7 specifies the requirements in regard to the services provision. The annexes provide additional information.

NOTE: The interworking specification between the FT and the IP is out of the scope of the present document and is left to the implementer's choice. Any excerpts form the IP protocols shown in the present document are used only as examples.

5 Overview

DECT is a standard for short range, low power, digital cordless communications which provides access to a great variety of external (to DECT) networks.

DECT access to IP networks is already described in the DPRS standard, EN 301 469 [16]. DPRS provides a transparent mechanism for exchange of data between an IP network and an IP terminal, or an IP application in a terminal, where DECT is used as a cordless carrier for the transport of the data.

A general introduction to the issues related to DECT access to IP networks is provided in TR 102 010 [12].

The present document provides requirements aimed at solving some issues identified in TR 102 010 [12] with specific focus on Voice over IP, e.g. mobility, QoS, interworking with SIP, etc.

6 Reference configuration

In figures 1 and 2 are shown 2 possible reference configurations in regard to interaction between DECT FP and PP.

Configuration 1 is related to the termination of the IP protocol in the PP (which is out of the scope of the present document). Such configuration may be useful in case the applications attached to the DECT PT are more general. The DPRS standard provides requirements for this case, see EN 301 469 [16].

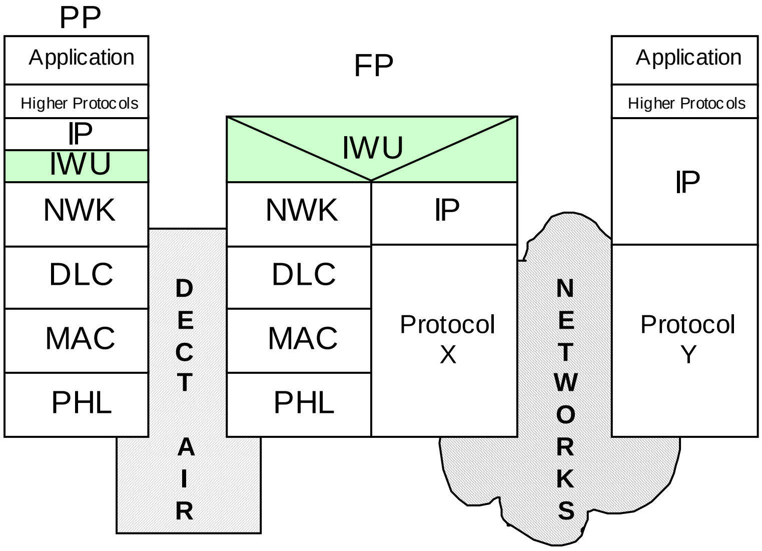

Figure 1: Reference configuration 1 (IP terminated at the PP)

Configuration 2, figure 2, describes the case when the IP protocol is terminated in the FP (which is into the scope of the present document). This configuration may be preferable especially in the case of a DECT voice IP telephone (this does not exclude messaging or other data only services). To provide interoperability between FPs and PPs issues here are, e.g. unified way of transmitting the voice samples to the PP and interaction with the signalling protocol use by the VoIP (e.g. SIP).

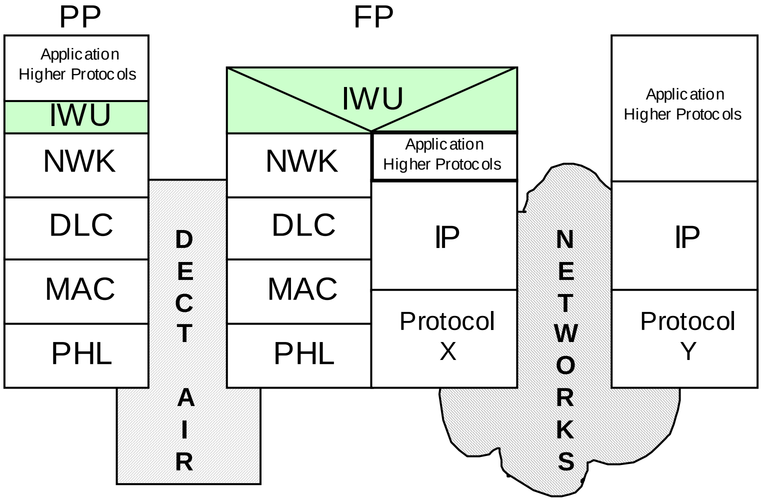

Figure 2: Reference configuration 2 (IP terminated at the FP)

7 Requirements

7.1 Requirements Table

Table 1 lists the requirements that have fallen into the scope of the present document. Details are provided in the clauses that follow.

Table 1: DECT access to IP networks requirements

Item	Name of service	Procedure	Reference	Support status	
				PT	FT
DAIP-F.1	PP IP Roaming IPv4		7.2.1.2	C1	C1
		Set up of DECT IP supporting environment	7.2.1.2.2	M	M
		DECT attachment/IP roaming registration FT handled IP mobility authentication	7.2.1.2.3	M	M
		DECT attachment/IP roaming registration PT handled IP mobility authentication	7.2.1.2.4	O	O
DAIP-F.2	FP IP Roaming IPv4		7.2.1.3	-	C1
		FP IP Roaming	7.2.1.3	-	M
DAIP-F.3	Roaming without IP Mobility		7.2.1.4	C1	C1
		Roaming without IP Mobility	7.2.1.4	M	M
DAIP-F.4	User Roaming		7.2.1.5	C1	C1
		User IP Roaming	7.2.1.5	M	M
DAIP-F.5	Handover		7.2.2	C1	C1
		Basic requirements	7.2.2.1	M	M
		Automatic assignment of external handover related Identities	7.2.2.2	O	O
		External handover call setup	7.2.2.3	M	M
		FP Synchronisation over the IP network	7.2.2.4	O	O
DAIP-F.6	SIP interworking		7.3	C1	C1
		Registration - Procedure mapping	7.3.2.1	M	M
		Registration - Adding/Modifying bindings	7.3.2.1.1	M	M
		Registration - Fetching bindings	7.3.2.1.2	O	O
		Registration - Refreshing bindings	7.3.2.1.3	M	M
		Call Control	7.3.3	M	M
		Service Attributes negotiation/modification	7.3.4	C3	C3
		Security	7.3.5	M	M
		Query for Capabilities	7.3.6	O	O
DAIP-F.7	QoS		7.4	-	C2
		QoS	7.4	-	M
C1: At least one shall be supported. C2: M if service is VoIP. C3: I for the present document.					

7.2 Mobility

Figure 3 provides a reference model for DECT-IP mobility with a number of DECT base stations (FPs) connected to different IP networks.

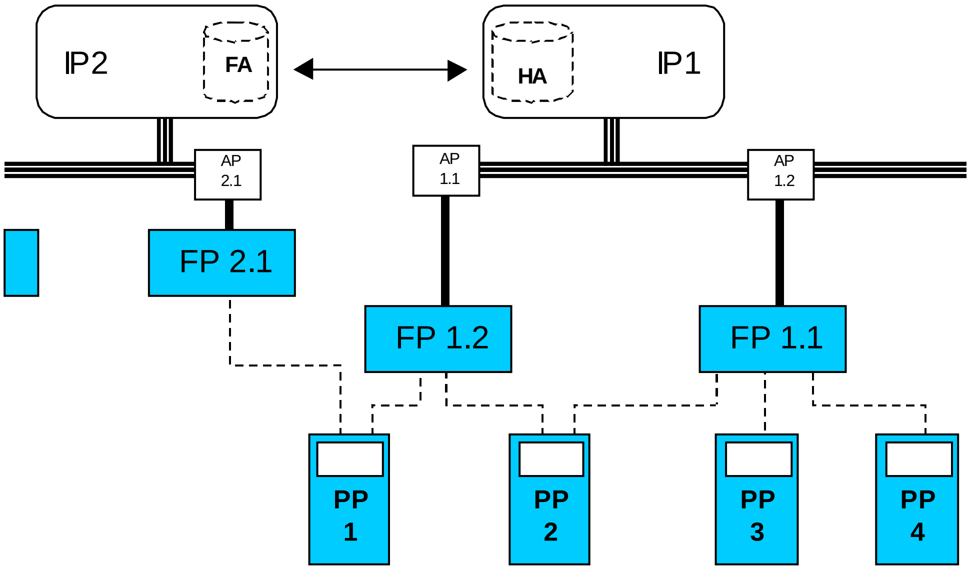

Figure 3: Mobility reference model

Basic assumptions:

1) A PP may move from one FP to another FP when both FPs are connected to one and the same IP network, or when each FP is connected to a different IP network.

2) A FP may move from one Access Point (AP) to another when the access points belong to the same or to different IP networks.

3) An end user may move from one PP to another PP, when each PP is logged on to different FPs, carrying on an external media her/his user profile data and providing it to the new PP.

4) IP is terminated in the FP. Optionally, for some services or special terminals, FP may be transparent in which case the DPRS standard shall be used. The mechanism for distinction and utilisation of such duality is out of the scope of the present document and left to manufacturers own implementation.

5) How configuration and address allocation is implemented on the boundary between the IP network and the FP is out of the scope of the present document, it is assumed that standard, common, procedures and requirements (e.g. DHCP, BOOTP, IPCP, Auto configuration, etc.) will be obeyed.

6) Mapping between assigned IP address(es) and PTs' DECT identities, if needed, shall be managed by the DECT FT. The possibility of single terminal maintaining a number of different addresses should be taken into account (e.g. *global address*, *link-local address*, *site-local address*, *multicast address*, *care-of-address*, etc.).

7) Depending on the contract initially signed one or more IP addresses may be assigned to be handled at one access point, i.e. by one FP. These addresses may be allocated to different PPs or a number of PPs may have been allocated a single IP address. The latter case needs special consideration if one of the PPs is to be allowed to move to another location.

8) Each FP may maintain a service record comprising location and service characteristics offered by the accessed IP network; for each PP attached to the FP applicability of each of those needs to be indicated, a general mechanism for providing the PP with all necessary information may need to be defined.

9) The IP mobility protocols/solutions differ in regard to the IP version supported, i.e. IPv4 or IPv6. The IPv4 protocol is described in RFC 3344 [17]. The IPv6 is currently described into an Internet draft (see annex B) which is expected to be completed by the end of 2003 and therefore is not taken into consideration of the present document.

7.2.1 Roaming

7.2.1.1 General IPv4

Due to the fact that the present document implies that the IP protocol is terminated in the FT for the basic DECT operation the PT needs not be aware of the kind of network the FT is connected to. Therefore, any PP that complies with the
EN 300 444, GAP [13] shall be capable of operating with an FT that complies with the requirements in this clause. However, in order to provide all the services described in this clause PPs may need to comply with additional requirements as specified in the present document.

This clause deals with the requirements which an IP enabled DECT terminal needs to satisfy when moving (i.e. roaming) between different IP access points. The term adopted in the IP world for such a terminal is "Mobile Node (MN)". According to RFC 3344 [17], a Mobile Node is "a host or router that changes its point of attachment from one network or subnetwork to another without changing its IP address and still being capable to communicate with other Internet nodes, assuming link-layer connectivity to a point of attachment is available".

The term "roaming" in DECT is normally related to a PP moving between different FPs, this clause extends the scope of the term to include FPs moving between different network access points.

Due to the fact that the IP protocol is terminated in the DECT FT, whereas the PP can move between different FPs, the term Mobile Node (MN) requires a special interpretation. The bases for such a special interpretation are depicted into figure 4.

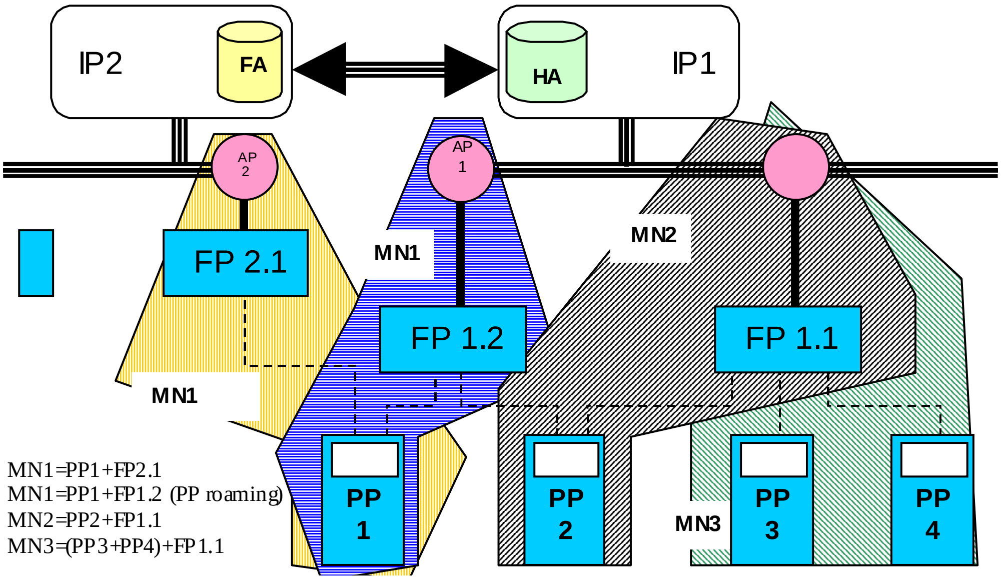

Figure 4: Mobility reference model

Accordingly a DECT Mobile Node (DECT MN) is an association between a DECT FP connected to an IP network and a DECT PP attached to that FP, where an IP address has been allocated to this tandem. Consequently as shown on figure 4 the tandems <PP1-FP1.2> and <PP1-FP2.1> represent one and the same mobile node - MN1. When PP1 is attached to FP 1.2 (tandem <PP1-FP1.2>), MN1 will be present at access point 1 (AN 1) and connected to IP network 1 (IP1), whereas, when PP1 is attached to FP 2.1 (tandem <PP1-FP2.1>), MN1 will be present at access point 1 (AP 2) and connected to IP network 2 (IP2).

This definition allows four (4) different DECT-IP roaming scenarios: (A) **PP IP Roaming**, FPs do not move and the PP roams between fixed FPs taking with it the IP address assigned to the initial tandem; (B) **FP IP roaming**, FP moves from one access point to another taking with it the IP address assigned to the initial tandem (and the subscribed PPs); (C) **Non IP assisted roaming**, FPs do not move and the PP roams between fixed FPs NOT taking with it the IP address assigned to the initial tandem; (D) **User Roaming**, the user moves carrying the IP mobility information, i.e. the user profile data, on some kind of external media and provides it into a suitable terminal at the new location.

For scenario (A), when a DECT MN roams, it is only the PP part, and not the FP part, of a DECT Mobile Node that does move. Consequently:

- one and the same FP may be part of different DECT MNs;
- one and the same PP, when roaming, may form associations with different FPs however representing one and the same DECT MN identified by the IP address assigned to this PP.

For scenario (B), when a DECT MN roams, it is the FP part of a DECT Mobile Node that does move, whereas the PP part may move but needs not. At the new access location it is possible that different PPs are in use. It is the FP having assigned an IP address and carrying it.

For scenario (C) from the point of view of IP mobility and our definition of DECT MN there is no move of the DECT Mobile Node. It is the FP having been assigned an IP address which from the IP network point of view does not move.

Scenario (D) may be considered as a variation of either scenario (A) - when, depending on the particular terminal implementation, at the new location the IP mobility related data is input into a DECT PP, or scenario (B) - if the input is to a DECT FP.

The following clauses specify the requirements relevant for each of these scenarios.

7.2.1.2 PP IP roaming IPv4

7.2.1.2.1 General

DECT PP IP roaming concept is based on, and comprises, a number of interactions as detailed below.

DECT Mobile Node establishment:

- A PP is DECT registered to a Home FP (HFP).
- The user has registered with a service provider or network operator and has received one or more IP addresses, User name(s) and password(s). In addition the service provider or network operator provides a netmask, a Mobility Security Association (MSA), and a Security Parameter Index (SPI) identifying a particular security context within the mobile security association (there may be more than one set of parameters belonging to the MSA). The MSA includes: a shared key or appropriate public/private key pair, identification of the authentication algorithm and mode and the style of Reply protection in use.
- The user assigns one of the received IP addresses to a PP and by making the FP aware of this assignment the user creates a virtual Mobile Node (MN) comprising the PP and the FP. The content of the Mobility Security Association and the SPI shall be made available to the MN and may be stored in the PP or/and in the FP. Having completed these configurations the user can consider its MN as being registered to the HA or an explicit registration procedure may be required.
- The same operation may be done with one or more additional PPs. Each of these PPs identified by its IPUI, its IP address, SPI and the relevant Mobility Security Association parameters' values define a virtual Mobile Node. It is the FT responsibility to differentiate the MNs it is engaged with and behave proper.

DECT Mobile Node operation:

- Before roaming a mobile node shall be configured at least with a netmask (subnet-directed broadcast address of the mobile node's home network) and a mobility security association for the home agent. In addition, a mobile node may be configured with its home address, and/or the IP address of one or more of its home agents. The means of configuration are not standardised and manual user input may be required. Alternatively, the user may carry all this information on an external media.
- When PP moves to a FP that support IP roaming, the PT shall DECT attach to the FT and make the FT aware that it supports Mobile IP and would like to engage the FT in a virtual MN. Although each time this DECT MN will include a new FP, from IP point of view, it is the same MN because it can be identified (and authenticated) with the same set of parameters. Consequently all necessary parameters for correct Mobile IP operation need to be made available to the MN (if they are not yet stored in the PT).

- An FP may be part of DECT MNs that consider the IP network to which the FP is attached as the home network, as well as, part of DECT MNs that consider the same IP network as a visited network. A DECT MN shall be capable of recognising that it is attached to a foreign network. The FT shall be capable of discovering the address of the local Mobile Agent and obtaining a care-of-address or alternatively obtaining a co-located care-of address. (The FT may have already information about the Mobile agents and procedures applied into the network as it has been in operation on this network.)

- If the Home agent address of the DECT MN is not known the FT shall use the netmask to discover it. If the MN home address is not provided, the FT shall use the Mobile Node NAI extension RFC 2794 [25] for the discovery of the address - to identify itself user shall provide its user name. Optionally, the PT part of the virtual MN or the user may provide this information upon the establishment of the virtual MN. Having obtained all necessary information the FT shall register with the Home Agent providing its new address.

- When PP is returning to its home, the home FP shall be capable of recognising that it is indeed a return to home and de-register with the HA.

- During the registration procedure the MN will be authenticated by the HA. The authentication is part of the registration, i.e. the data needed for the authentication is provided into the messages exchanged during the registration. There are two alternative ways of accomplishing this authentication. The input parameters needed for the calculation of the authentication parameters are made available at the FT part and the FT performs the necessary calculation, or, the calculation of the authentication parameters is performed into the PT part of the virtual MN and the result is submitted to the FT. The former solution is associated with some security risks as the visiting user is not in control of the visited FP and by providing to the FT its security information the user is vulnerable to this information being misused. Furthermore, the former alternative requires, if the parameters are not manually entered into the FT but e.g. sent from the PT, usage of encrypted DECT connection for their provision on air.

- Additionally, a MN may have mobility security association(s) as well with a Foreign Agent. In this case the FA may authenticate the MN in similar manner as the HA and hence the same issues that was raised in regard to HA authentication apply in this case too.

- Virtual MNs (i.e. the FT or/and the PT part depending on the implementation) shall be able to perform authentication as defined in RFC 3344 [17]. The default algorithm is HMAC-MD5, with a key size of 128 bits as specified in RFC 2104 [24]. It computes a 128-bit "message digest" of the registration message. The data over it is computed is the UDP payload (that is, the Registration Request or Registration Reply data), all prior Extensions in their entirety (i.e. if any Optional Non-Auth Extensions for HA), and the Type, Length, and SPI of the MN-HA Authentication Extension.

- In addition to the addresses discovery and the authentication issues the user should be provided with the possibility to indicate that she/he would like to keep its previously registered mobile addresses (setting the "S" bit in the Register message) or delete a particular mobile binding (setting the life time to zero), and/or, that the HA shall forward to it a copy of broadcast datagrams received by its home agent from the home network (setting the "B" bit in the Register message), and/or indicate a desired life time for the binding (registration). Re-registration for the active binding is the responsibility of the FT part of the virtual MN.

- A registration may be rejected. Some errors may be solved by the user, e.g. spelling errors in regard to information entered manually and should be therefore indicated to the user.

- After registration the normal operation of the virtual MN (in regard to IP interworking) shall be in the responsibility of the FT part.

DECT private use:

- The PP attachment to a FP usually requires that either the PP is subscribed to that FP (e.g. GAP [13]) or that the visited FP has a roaming agreement with the PP's home FP or home DECT network where the PT is subscribed (e.g. CAP [14]). When DECT Mobile IP is used in a DECT Public or business network which is managed centrally it is very likely that a combination of GAP and CAP like roaming rules will be applied. However, when DECT private users are involved care shall be taken to avoid FPs being overloaded with requests for IP roaming from visiting PPs, or/and, PPs being unable to provide services when constantly trying to attach to FPs.

The following clauses describe the DECT specific procedures that a DECT PT and/or FT should implement to satisfy the DECT IP mobility requirements and perform the interactions described in this clause.

7.2.1.2.2 Set up of DECT IP roaming supporting environment

DECT FPs that comply with the present document shall provide the user (owner) with the possibility to set the FP in one of the following IP mobility related modes:

- IP roaming not allowed (default);
- IP roaming Personal OR/AND IP Roaming Managed group;
- IP roaming unrestricted.

The mode "**IP roaming not allowed**" is the default mode. It does not require any IP mobility related settings or indications. Terminals that do not provide IP mobility, e.g. straight GAP terminals, are considered as being set to "IP roaming not allowed". Terminals that allow IP roaming only if a valid subscription is available are considered, from the point of vie of a roaming PP without subscription, as being set to "IP roaming not allowed".

The mode "**IP roaming Personal**" allows for the owner of a DECT base station to permit on case by case bases the IP roaming of portables (PPs) that are not subscribed to the base station. For the support of this service the following provisions shall be implemented:

- The Base station owner shall be capable of "reading" and providing to the visiting PP the RFPI transmitted by the FT. In addition an IP roaming AC shall be set and made known to the FT and to the visiting PT; the GAP [13] procedure AC to bitstring mapping shall be supported. A PT subscribed to the FT should be used for these purposes. The setting of the IP roaming AC may be used to set the FT in "IP roaming Personal" mode. In this mode the FT shall be prepared to handle IP roaming registrations from PTs that know the IP roaming AC; no other FT actions are required.
- The visiting PT shall support the GAP [13] procedures Manual entry of the Park and AC to bitstring mapping. PTs shall be able to store at least one pare of IP roaming RFPI/AC.
- A PT is allowed to lock to an FT and register for the purpose of IP roaming if it has stored the FP RFPI/AC. The AC shall be used for PT authentication. During the Authentication procedure a DCK should be stored. The DCK shall be used for link encryption if IP confidentiality parameters are to be sent over the DECT air (e.g. as defined in clause 7.2.1.2.3).

The mode "**IP roaming managed group**" allows for a business or public DECT system to assign a common SARI dedicated for IP roaming which may be transmitted by a number of DECT FTs. For the support of this service the following provisions shall be implemented:

- For the IP roaming SARI any DECT identity with the exception of ARI class A and D may be used (see EN 300 175-6 [6]). For the SARI provision proprietary configuration means may be used. The SARI value shall be given to any PP that is allowed IP roaming to the FTs transmitting the SARI. In addition an IP roaming AC shall be set and made known to the FT(s) and to the visiting PT(s); the GAP [13] procedure AC to bitstring mapping shall be supported. The setting of the IP roaming AC may be used to set the FT in "IP roaming managed group" mode. In this mode the FT shall broadcast the IP roaming SARI and shall be prepared to handle IP roaming registrations from PTs that know the IP roaming AC; no other FT actions are required.
- The visiting PT shall support the GAP [13] procedures Manual entry of the Park (used for SARI) and AC to bitstring mapping. PTs shall be able to store at least one pare of IP roaming SARI/AC.
- A PT is allowed to lock to an FT and register for the purpose of IP roaming if it has stored the FP SARI/AC. The AC shall be used for PT authentication. During the Authentication procedure a DCK should be stored. The DCK shall be used for link encryption if IP confidentiality parameters are to be sent over the DECT air (e.g. as defined in clause 7.2.1.2.3).

The mode "**IP roaming unrestricted**" allows for the owner of a DECT base station to permit any PP to attach for the purpose of IP roaming. For the support of this service the user shall be capable of setting the FT to start broadcasting "IP roaming unrestricted" in the Extended Fixed Part Higher layer Capabilities MAC message (see EN 300 175-3 [3] and EN 300 175-5 [5]). In this mode the FT shall allow bearer setup and IP mobility attach procedure initiated by any PP and shall not authenticate the PT.

NOTE 1: The FP owner of such a FP should be allowed to set up priority handling or restrictions among visiting and home MN. The means of setting up such schemes are out of the scope of the present document.

NOTE 2: The provision of the broadcast requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

In addition to the requirements related to setting up the environment to allow a PP to roam each such a PP requires the availability of a number of parameters that will be used during the IP Mobility Registration (described in the following clauses). For this purpose a PT should implement an IP mobility data information structure in which all parameters needed and supported for a correct IP mobility operation are stored. The exact implementation of this data structure, called in the present document as the "DECT IP Mobility signature (DIMS)", is left to the implementer's choice. Table 2 identifies the relevant parameters and the status of their provision.

Table 2: DECT IP Mobility Signature (DIMS)

Nr.	Data	Nr. of bits	Status	Comment
1	Mobile IP bindings properties.Settings	8	M	Notes 1, 5, 6
2	Mobile IP bindings properties.Lifetime	16	M	Notes 5, 6
3	Home Address (IPv4)	32	O	Note 6
4	Care-off address (IPv4)	32	O	
6.1	Netmask	nx8	M	Note 2
6.2	Agent address (IPv4)	32	O	Note 6
6.3	Security Parameter Index (SPI) MN-HA	32	M	
6.4	Mobility Security Association.Auth algorithm	4	M	Notes 3, 5
6.5	Mobility Security Association.Reply protection	4	M	Notes 3, 5
6.6	Mobility Security Association.Secret Authentication Key	128	M	
6.7	Username	nx8	C	Notes 4, 6

NOTE 1: This field represents the S|B|D|M|G|r|T|x|, see RFC 3344 [17] bits. User shall be allowed to set the values of bits "S" and "B".
NOTE 2: The provision of one set of the fields 6.1 to 6.7 is mandatory to cover the data related to one Home Agent. An implementation may allow provision of multiple sets to cover multiple Home Agents and Foreign Agents authentication.
NOTE 3: To indicate the exact option chosen.
NOTE 4: "Username" is required if no Home Address is provided.
NOTE 5: A default setting needs not be indicated.
NOTE 6: An implementer may choose to request this information dynamically from the user rather than storing it.

The means for establishing all necessary information to be included into the DIMS on the first place is out of the scope of the present document. Some of the information may be provided to the Home FT (HFT) over the IP network where proper IP configuration protocols may be implemented. Some information, if not all, may require manual input. Implementers shall provide means for manual input at the PP - those are out of the scope of the present document.

The minimum set of parameters from those indicated in table 2 that need to be available at the PT side for IP roaming are:

6.1	Netmask
6.3	Security Parameter Index (SPI) MN-HA
6.4	Mobility Security Association.Auth algorithm
6.5	Mobility Security Association.Reply protection
6.6	Mobility Security Association.Secret Authentication Key
6.7	Username

All PPs that claim support of IP Mobility as described in the present document shall be capable of accepting manual input and over the DECT-air interface input for establishing of its DIMS. FPs that support configuration over the IP or other "direct" means (e.g. wired interface) shall be capable of providing the established information to the PT over the DECT-air interface; FPs that do not support such configuration shall be capable of accepting and configuring such information over the DECT-air interface provided from a suitable PT.

It is PT responsibility to establish the DIMS. If the user has been provided with some DIMS parameters on external media those shall be entered to the PP manually.

If some of the parameters are missing and those needs to be downloaded from the FT over the air the DECT Parameter retrieval procedure as specified in EN 300 175-5 [5], clause 13.7 shall be used. The <<Info Type>> information element in the {MM-INFO-REQUEST} message shall be set to "Dynamic Parameters Allocation" and "IP Mobility DIMS" shall be indicated in a <<IWU-TO-IWU>>. If a "Username" and/or "Netmask" have been allocated this shall be included in the <<IWU-TO-IWU>> as well.

Upon the receipt of the request FT shall provide back any parameter available using the <<IWU-TO-IWU>> in a {MM-INFO-ACCEPT} message. Depending on the implementation the FT may try to obtain some parameters from external sources. If the FT is not capable of providing any parameter but supports IP Mobility it shall send back a {MM-INFO-ACCEPT} without parameters. If the FT does not support IP mobility it shall reject the request with a {MM-INFO-REJECT} message. At the PT side if a {MM-INFO-REJECT} is received or timer <MM-info.1> expires without an answer being received from the FT the PT should consider that the FT does not support IP roaming and inform the user respectively. If the Secret Authentication Key is to be transmitted over the air the DECT link shall be ciphered before hand - the FT initiated Ciphering as specified in GAP [13] shall be used.

For the structure of the <<IWU-TO-IWU>> information element in regard to IP mobility see clause 7.2.1.2.5. If the inclusion of the <<IWU-TO-IWU>> will result in a message longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented in one or more {MM-IWU} messages. PT shall restart timer <MM_info.1> after sending every {MM-IWU} message. To allow sending/reception of {MM-IWU} messages after the last message of a MM procedure has been sent/received the MM entity shall indicate "partial release" in the NLR notification as specified in EN 300 175-5 [5], clause 14.2.7.2.

Table 3: Values used within a MM message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Segmented Info>>			Note 2
	<Segmented element type>	1110111	<<IWU-TO-IWU>>
<<IWU-TO-IWU>>		All	Note 1
NOTE 1: For the content of the <<IWU-TO-IWU>> information element see clause 7.2.1.2.5. NOTE 2: Mandatory only if the message will exceed 63 octets or when <<IWU-TO-IWU>> was segmented.			

7.2.1.2.3 DECT attachment/IP roaming registration FT handled IP mobility authentication

All terminals complying with the present document shall support the "FT handled IP mobility authentication" and the related procedures as described in this clause. Optionally terminals may support PT handled IP mobility authentication and the related procedures as described in clause 7.2.1.2.4. The user shall be informed for the possible security issues as indicated in clause 7.2.1.2.1.

All FPs shall support in full the requirements of the Mobile IP Mobile Node as specified in RFC 3344 [17]. For the PP implementation the requirements of the RFC 3344 [17] are not applicable.

The IP roaming registration procedure shall be mapped to DECT Location registration and possibly DECT location update procedures as defined in GAP [13] with the modification specified in this clause.

The FT handled IP mobility authentication implies, as indicated in clause 7.2.1.2.1, that all parameters involved into the authentication procedure during the IP mobility registration with a HA or FA shall be made available into the FT prior to the construction of the IP Mobility Registration message.

For the provision of the DIMS to a visited FP (which can be used with HFP also) there are three alternatives identified: Direct (manual) input to the FP, Local PP-to-FP provision (manual entry into the local PP), and Visiting PP-to-FP provision (automatic).

A designer may choose to implement a kind of direct input to the FT. This implementation is out of the scope of the present document.

If direct input to the FT is not provided a DECT on-air exchange between the FT and a PT shall be used. The transmission should be made over an encrypted DECT link.

The designer may choose to implement such exchange to be assisted (performed) by a local PP already subscribed to the FT and the user will be expected to provide the information to be keyed into the PP.

To support manual entry of parameters, either directly into the FT or into the local PT, all PPs that claim support to the present document shall be capable on user's request to display the PP's IP mobility parameters allowing for the user to read them from the visiting PP and key them into the local PP that will transmit them to the FP. If such procedure is implemented the designer should take care that the provision of the information is guarded by local to the PT PIN (user password).

Independent of whether a manual entry to the FT is supported, to ensure interoperability among terminals from different vendors every PT that claims support to the present document shall support the Local PP-to-FP provision procedure.

Alternatively, the visiting PT may itself provide the parameters to the FT. The support of this procedure is optional. It should be noted however that this is the only way that a PP may roam without user intervention into already set up IP mobility environment for which the PT knows the setting parameters.

Whichever of these three options is implemented the user shall be provided with the capability to request IP mobility registration. Optionally a roaming PT may prompt the user to start the registration upon entering an IP mobility allowed area. Automatic registration may be implemented as well allowing fro the PT to start registration as soon as it recognizes an area in which the IP mobility for this PT is allowed.

The PT shall initiate an attach (roaming registration) procedure using the GAP Location registration procedure as defined in [13] providing at least its netmask address and optionally its IP home-address and/or HA address. If Home address is not provided the User shall provide its User name. Mobile IP bindings properties may be provided as well (see DECT IP Mobility Signature (DIMS) above).

Upon receipt of the {LOCATE-REQUEST} message the FT shall behave depending on the information available:

1) If the visited FT (VFT) does not have a record of the PT's IP mobility authentication parameters and if a roaming security key is available the FT shall initiate a DECT authentication procedure using the AC (the roaming security key) indicating that DCK shall be stored. If the authentication is successful the FT shall initiate FT initiated ciphering procedure as defined in GAP [13]. After the link is ciphered the FT shall request transmission of IP mobility authentication parameters and PT shall provide them in a <<IWU-TO-IWU>> information element included in a {MM-IWU} messages which shall not exceed the length of 63 octets or the <<IWU-TO-IWU>> shall be segmented in a number of {MM-IWU} messages. If HA address has not been provided the FT shall perform as soon as possible HA address discovery as specified in RFC 3344 [17]. The FT shall proceed with step 4.

2) If the visited FT (VFT) does not have a record of the PT's IP mobility authentication parameters and if a roaming security key is not available the FT shall reject the Location registration procedure providing indication to the user for the reason. The procedure shall be rejected as well if not sufficient address information has been provided.

3) If the visited FT (VFT) does have a record of the PT's IP mobility authentication parameters it shall proceed with step 4. If HA address has not been provided the FT shall perform as soon as possible HA address discovery as specified in RFC 3344 [17].

4) After the VFT obtains all information needed it shall initiate a Mobile IP registration procedure as defined in the RFC 3344 [17]. If User name was provided instead of a Home address the FT shall follow the requirements specified in RFC 3344 [17] and RFC 2794 [25] for the construction of the Registration message. When the registration is completed the VFT shall confirm this to the PT by sending back a {LOCATE-ACCEPT} message. Any not provided by the visiting PT but discovered by the FT address should be stored for future use.

If the completion of the procedures on the IP side is taking time longer than the time allowed for the completion of the DECT Location registration procedure the VFT shall used the {MM-NOTIFY} to restart the running at the PT timer associated with the attach procedure.

NOTE: The format and the usage of the {MM-NOTIFY} message requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C in the present document. All changes are backwards compatible.

Figure 5 shows an example of a complete PP IP roaming registration procedure. It assumes that: Roaming has been enabled at the FT (i.e. Roaming RFPI and Roaming security key available at the FT and at the PT).

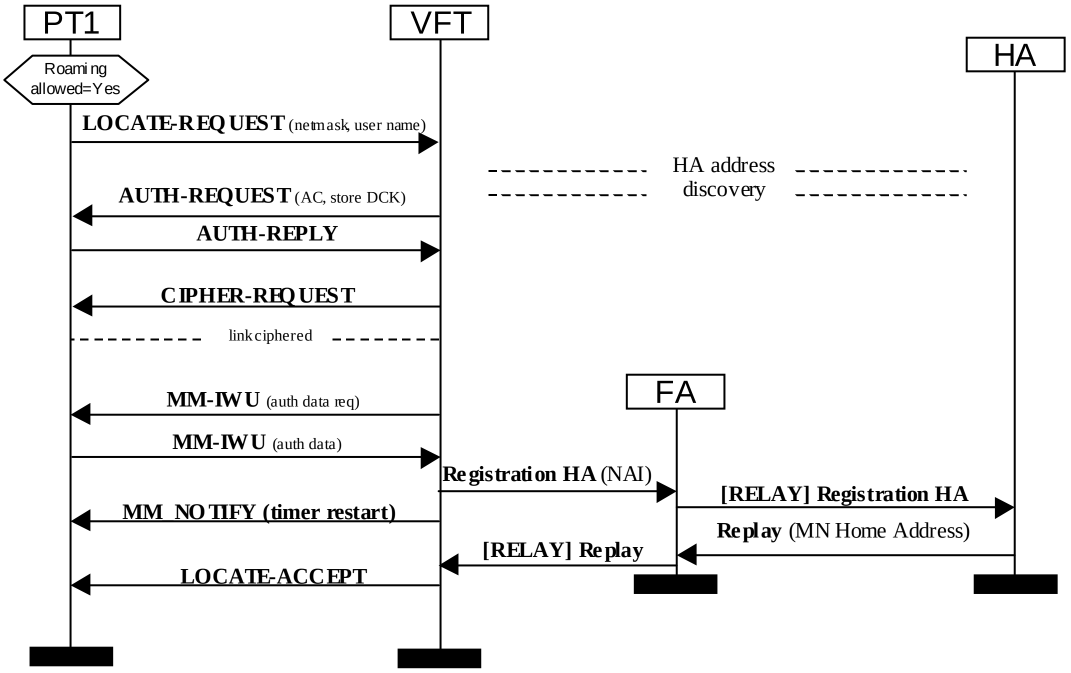

Figure 5: Successful PP mobile IP roaming registration (FT auth)

The DECT message/information elements support required in addition to the requirements of GAP is indicated into clause 7.2.1.2.5.

7.2.1.2.4 DECT attachment/IP roaming registration PT handled IP mobility authentication

All terminals complying with the present document may optionally, in addition to the requirements provided in clause 7.2.1.2.3, support PT handled IP mobility authentication and the related procedures as described in this clause.

NOTE 1: The main target of the requirements in this clause is to provide a solution for some security concerns indicated in clause 7.2.1.2.1.

IP mobility authentication as specified in RFC 3344 [17] is based on the performing of calculations (using the Mobility Security Association parameters) applied over parts of the Registration message and including the result of this calculation together with the SPI in the message before sending it to the HA (FA). Consequently, the PT handled IP mobility authentication does not require full implementation of the RFC 3344 [17] into the PT rather it is based on the requirements that all IP mobility handling is done into the FT except that the calculations over information available in the PT and such provided by the FT to the PT are done into the PT and the result is provided back to FT for construction of the Registration message. In the same manner authentication verification is performed in the PT upon provision of parts of the receipt by the FT Reply message.

NOTE 2: The IP handled IP mobility authentication may be seen as moving the Authentication module, which normally will be a part of the FT RFC 3344 [17] protocol software, from the FT to the PT and standardising the exchange between the FT's RFC 3344 protocol and the PT's Authentication module.

In this regard, all PPs that claim support of this clause shall support the requirements for IP mobility authentication calculation as specified in RFC 3344 [17] and the authentication algorithm as specified in RFC 2104 [24].

In regard to the requirements of this clause the IP roaming registration procedure shall be mapped to DECT Location registration and possibly DECT location update procedures as defined in GAP [13] with the modification specified in this clause.

The user shall be provided with the capability to request IP mobility registration. Optionally a roaming PT may prompt the user to start the registration upon entering an IP mobility allowed area. Automatic registration may be implemented as well allowing for the PT to start registration as soon as it recognizes an area in which the IP mobility for this PT is allowed (Roaming RFPI is available and matches the one transmitted by the FT).

NOTE 3: The provision of roaming security key for this procedure is optional, although the implementers should consider provision of encryption on the DECT air interface in any case (see GAP [13]) which could not be otherwise ensured as the visiting PT will not have a standard DECT subscription.

The PT shall initiate an attach (roaming registration) procedure using the GAP Location registration procedure as defined in [13] providing at least its netmask address and its SPI, and, optionally its IP home-address and/or HA address. If Home address is not provided the User shall provide its User name in which case the FT shall follow the requirements specified in RFC 3344 [17] and RFC 2794 [25] for the construction of the Registration message. If HA address has not been provided the FT shall perform HA address discovery as specified in RFC 3344 [17]. Mobile IP bindings properties may be provided as well (see DECT IP Mobility Signature (DIMS) table earlier).

Having obtained the provided information, the FT shall construct an IP mobility Registration message. The value of the Identification field shall be calculated by the FT - the timestamps method shall be used (see RFC 3344 [17]). The FT shall take into account that the calculation of the Authenticator value will consume some time therefore a time tolerance value shall be added to the actual timestamp relevant to the construction of the message. Addition of 2 sec is suggested. The FT shall send the message part over which the Authenticator shall be computed to the PT. The FT shall use the <<IWU-TO-IWU>> information element if necessary segmented in one or more {MM-IWU} messages.

On figure 6 an example of a Registration message is shown. It is assumed that the PT has not provided Home Address and has provided Username therefore the MN-NAI extension is included. The relevant for authentication part is highlighted with colour and this is the data the FT shall send to the PT for authentication.

Table 4: Registration request message

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="8">Type = 1</td><td>S</td><td>B</td><td>D</td><td>M</td><td>G</td><td>r</td><td>T</td><td>x</td><td colspan="16">Lifetime</td></tr>
<tr><td colspan="32">Home Address = 0.0.0.0</td></tr>
<tr><td colspan="32">Home Agent</td></tr>
<tr><td colspan="32">Care-off address</td></tr>
<tr><td colspan="32">Identification</td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="8">Type = 131</td><td colspan="8">Length</td><td colspan="16">MN-NAI</td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="8">Type = 32</td><td colspan="8">Length</td><td colspan="16">Security Parameter Index (SPI)</td></tr>
<tr><td colspan="16">SPI (cont..)</td><td colspan="16"></td></tr>
<tr><td colspan="32">MN-HA Authenticator (variable length)</td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="32">Optional Non-Auth Extensions for FA ....</td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="32"></td></tr>
<tr><td colspan="32">Optional MN-FA Authentication Extension...</td></tr>
<tr><td colspan="32"></td></tr>
</table>

Having received the registration data the PT shall provide it as input, together with the relevant parameters from the Mobility Security Association to the authentication algorithm (HMAC-MD5 as specified in RFC 2104 [24]) and compute a 128-bit "message digest" of the provided data. If the SPI was not known to the FT before calculating the result the PT shall add it to the received information from the FT.

The PT shall communicate back to the FT the result, i.e. the Authenticator value. The PT shall use the <<IWU-TO-IWU>> information element if necessary segmented in one or more {MM-IWU} messages. If the SPI was not known to the FT before calculating the result the PT shall provide the SPI to the FT. To reduce the exchange PT is not required to send back the whole Registration message.

Finally the FT shall complete the Registration message and send it to the FA.

After a successful Reply message is received the FT shall provide the Message part over which the HA has performed authentication calculation to PT. PT shall calculate Authenticator and return it to the FT. FT shall compare the received Authenticator and the one included into the Reply to verify the authenticity of the Reply. For this exchange again the <<IWU-TO-IWU>> IEs and the {MM-IWU} messages shall be used.

If the completion of the procedures on the IP side is taking time longer than the time allowed for the completion of the DECT Location registration procedure the VFT shall used the {MM-NOTIFY} to restart the running at the PT timer associated with the attach procedure.

NOTE 4: The format and the usage of the {MM-NOTIFY} message requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

Figure 6 shows an example of a complete PP IP roaming registration procedure. It assumes that: Roaming has been enabled at the FT (i.e. Roaming RFPI is available at the FT and at the PT). Compare to the case in the previous clause here there is no need for DECT authentication and ciphering.

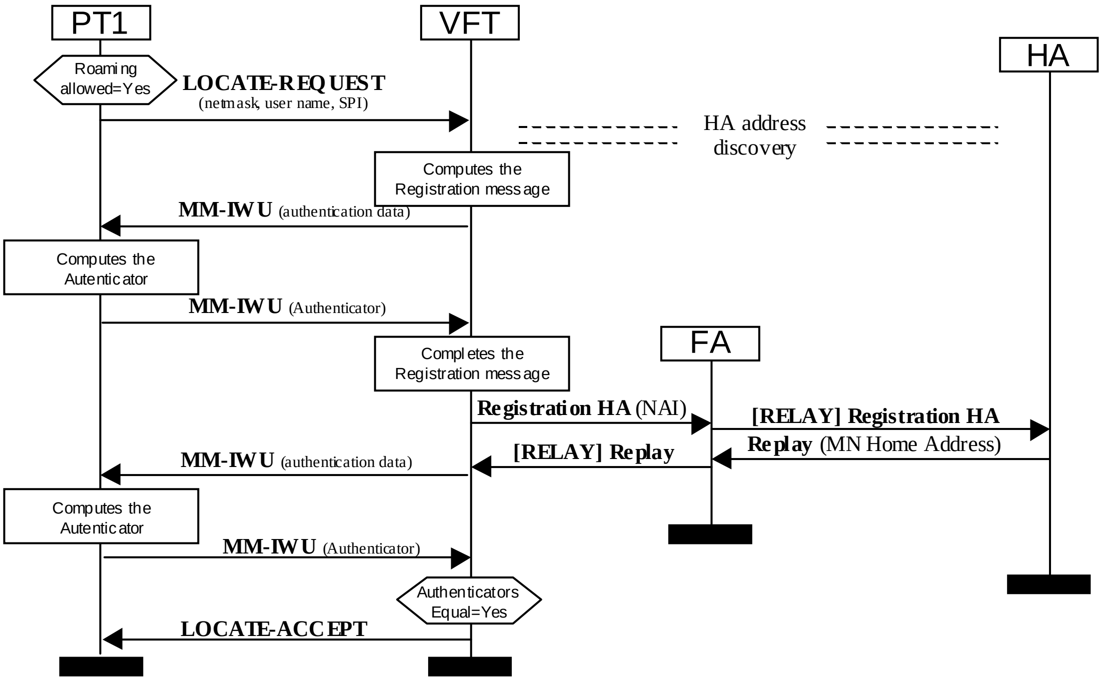

Figure 6: Successful PP mobile IP roaming registration (PT auth)

The DECT message/information elements support required in addition to the requirements of GAP is indicated into clause 7.2.1.2.5.

7.2.1.2.5 Message/Information elements specification

For the content of messages/information elements the requirements specified in EN 300 444 GAP [13] and/or in EN 300 175-5 [5] whenever relevant apply. For the structure of the <<IWU-TO-IWU>> information element the requirements in EN 300 175-5 [5] and annex A of the present document apply. This clause lists only the differences/additions.

As a general rule if the inclusion of the <<IWU-TO-IWU>> in a message will result in message being longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and provided in one or more additional {MM-IWU} messages. Consequently for the messages that carry the <<IWU-TO-IWU>> information element in addition to any mandatory information element the following basic structure shall apply.

Table 5: Values used within an IP mobility MM message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Segmented Info>>			Note
	<Segmented element type>	1110111	<<IWU-TO-IWU>>
<<IWU-TO-IWU>>		All	
NOTE: Mandatory if the message will exceed 63 octets or when carrying the last segment from a segmented <<IWU-TO-IWU>>.			

NOTE: The inclusion of the <<Segmented Info>> into the MM messages requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

Table 6 specifies the structure and content of the <<IWU-TO-IWU>> information element in regard to IP mobility. Which and when a filed shall be included is indicated into the clauses that describe the procedures.

Table 6: <<IWU-TO-IWU>> Action field

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1000001	IP Mobility: DIMS
		1000110	IP Mobility: Authentication Payload
		1000100	IP Mobility: Authenticator
Body	All	All	The content of this field depends on the settings of the Action Value and is described in the tables that follow.

Table 7: <<IWU-TO-IWU>> Action field = Authentication payload

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1000110	IP Mobility: Authentication Payload
Body	Auth Payload	All	Note
NOTE: RFC 3344 [17] specifies the part of the Registration/Reply messages over which Authentication is calculated and this shall be included here - the format shall be preserved.			

Table 8: <<IWU-TO-IWU>> Action field = Authenticator

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1000100	IP Mobility: Authenticator
Body	Authenticator	All	Note
NOTE: RFC 3344 [17] specifies how the value of the Authenticator field is calculated - the format shall be preserved.			

Table 9: <<IWU-TO-IWU>> Action field = DIMS

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1000001	IP Mobility: DIMS
Body	Fields_presence_indicator.ext	1	Multi octet extension - last
		0	Multi octet extension - more
	Fields_presence_indicator.value	xxxxxxx	Identifies which field is present in the rest of the Body. A bit set to "1" shall be understood as "field present"
		xxxxxx1	Mobile IP bindings properties.Settings
		xxxxx1x	Mobile IP bindings properties.Lifetime
		xxxx1xx	Home Address
		xxx1xxx	Care-off address
		xx1xxxx	Home Agent sets
		x1xxxxx	Foreign Agent sets
		1xxxxxx	Not assigned yet
	Mobile IP bindings properties.Settings	All	1 octet setting according to |S|B|D|M|G|r|T|x| defined in RFC 3344 [17]
	Mobile IP bindings properties.Lifetime	All	2 octets as defined in RFC 3344 [17]
	Home Address		4 octets
	Care-off address		4 octets
	Home Agent set fields indicator.ext	1	One Home set
		0	More Home sets
	Home Agent set fields indicator.value	xxxxxxx	Identifies which field is present in the Home set. A bit set to "1" shall be understood as "field present"
	Netmask	All	4 octets
	Agent address	All	4 octets
	Security Parameter Index (SPI) MN-HA	>255	4 octets
	MSA.Auth algorithm+Reply protection	0001 0001	Auth. algorithm HMAC-MD5; Reply protection Timestamps
		0001 0010	HMAC-MD5; Nonces (optional)
		0010 0001	Keyed MD5; Timestamps (optional)
		0010 0010	Keyed MD5; Nonces (optional)
	MSA.Secret Authentication Key.Length	All	Number of bits (at least 128 bits long keys shall be supported)
	MSA.Secret Authentication Key.Value	All	
	Username.Length	1-255	Number of octets
	Username.Value	All	IA5 characters (maximum 255 characters long)
	Foreign Agent Set fields indicator.ext	1	One Foreign set
		0	More Foreign sets
	Foreign Agent Set fields indicator.value	xxxxxxx	Identifies which field is present in the Foreign set. A bit set to "1" shall be understood as "field present"
	Netmask.Value	All	4 octets
	Agent address	All	4 octets
	Security Parameter Index (SPI) MN-HA	>255	4 octets
	MSA.Auth algorithm+Reply protection	All	See same field for Home agent set
	MSA.Secret Authentication Key.Length	All	Number of bits (at least 128 bits long keys shall be supported)
	MSA.Secret Authentication Key.Value	All	
	Username.Length	1-255	Number of octets
	Username.Value	All	IA5 characters

7.2.1.3 FP IP roaming IPv4

A User may move (roam with) its entire DECT system which may include one FP and a number of PPs from one IP access point to another. The DECT system may comprises one or more DECT MN if multiple IP home addresses were assigned and different associations between the FT and different PTs were given different IP addresses.

In such a case it is the responsibility of the FT to obtain care-off addresses and register all DECT MN at the new access as from the point of the PTs no change will occur. After obtaining all necessary information the FT shall update the PTs' DIMS as described in the previous clause.

7.2.1.4 Roaming without IP mobility (IPv4 and IPv6)

This clause describes an alternative method of providing PP mobility between different FPs connected to IP networks without relying upon IP mobility protocols being implemented on the network. It is based on the assumption that when PP moves it does not take the assigned Home IP address. The address is kept with the FT and since the FP does not move it is always accessible on the assigned (home) IP address.

7.2.1.4.1 General IP issues

When a FP is connected to an IP network it will obtain one or more IP addresses. The User may associate these IP addresses with one or another PP subscribed to the FP. From this moment on the particular FP becomes the Home FP (HFP) for this PP. A home FP shall maintain a Home Data Base for each of the PPs it has associated IP addresses.

When a PP moves to another FP its IP address shall remain associated with the Home FP. At the new Visited FP (VFP) the visiting PT shall provide its home address and as soon as a new IP address is obtained at the new location this shall be associated with the visiting PP and the VFT shall communicate to the HFT (over IP) the new address of the PP.

After the new address of the PP has become known to the HFT the communication handling depends on the implementation. Two alternatives are identified:

- **Tunnelling:** the Home FP shall act as a router (or a Home Agent) for communication to and from the PP, i.e. whenever data arrives with destination address the IP address associated with the PP, the Home FT shall route (tunnel) the data to the new address of the PP; likewise, when the PP wants to send out data the Visited FT shall send it (reverse tunnel) to the Home FT which in turn shall send it to the right destination (the original home IP address shall be used as source address). Both HFT and VFT shall support tunnelling datagrams using IP in IP encapsulation (RFC 2003 [26]).

- **SIP mix:** the Home FT shall act as a mixer for a SIP based 3PTY conference like call. Although handled as a SIP 3pty call this call will have only 2 parties and 2 call legs, i.e. the VFT (the Party at the PP visited location) and the Called/Calling Party (the Party which was called or initiated the call), and consequently, a call leg from the VFT (PP's visited location) to the HFT and from the HFT to the location of the Called/Calling Party.

DECT specific signalling information (see the clause 7.2.1.4.2) exchanged between the VFT and the HFT shall be included into the body of internet messages formatted according to the RFC 2045 [28] and RFC 2046 [29] MIME specification using Content-type: application/octet-stream and Content-Transfer-Encoding: binary; the "Subject" field shall provide in text the DECT message type code for the message carried in. For example if the included message is the {AUTHENTICATE-REQUEST}, the "Subject" field shall indicate "01000000" as specified in clause 7.4 of EN 300 175-5 [5]. The messages shall be transmitted in the case of tunnelling using the SMTP as specified in RFC 2821 [27] and in the SIP messages Message body for the case of SIP mix (see RFC 3261 [18]).

7.2.1.4.2 General DECT issues

From DECT point of view roaming between different FPs will require a solution in regard to subscription and security which allows the PT to attach a Visited FT.

To avoid a FT to be overloaded with undesirable requests for roaming from PTs and visa versa PTs getting into dead circles by trying to access FTs that does not offer the roaming service, each FT and PT that claims support to the present document shall comply to the requirements defined in clause 7.2.1.2.2 in regard to setting up of a Roaming RFPI or alternatively, DECT business or Public networks can use the EN 300 824 [14], DECT CAP profile.

This clause specifies requirements only related to the communication between the VFT and the HFT.

7.2.1.4.3 The tunnelling method

For terminals that support the tunnelling method the requirements specified in this clause apply.

After a PT establishes that it is allowed to roam to a particular FT it shall attempt roaming registration. In such a case the PT, VFT and HFT shall comply with the following:

- PP tries to attach to a VFT indicating Roaming registration and providing the HFT address - sends {LOCATE-REQUEST}.
- VFT stores temporarily the HFT address, adds its own address, constructs an internet message incorporates the {LOCATE-REQUEST} into the body and sends the message to the HFT.
- HFT extracts the DECT messages from the Internet message, stores temporarily the VFT address and Authenticates the PP by constructing a {AUTH-REQ}, incorporating it in an Internet message and sending the message to the VFT.
- VFT extracts the {AUTH-REQ} and sends it to the PT.
- PT sends {AUTH-REPLY} to VFT.
- VFT constructs an internet message incorporates the {AUTH-REPLY} into the body and sends the message to the HFT.
- If authentication is successful the HFT stores PT bindings and sends back the {LOCATE-ACCEPT}.
- VFT extracts the {LOCATE-ACCEPT}, stores PT bindings, and sends it to the PT.

An example of a message carrying the {AUTHENTICATE-REQUEST} message is provided in table 10.

Table 10: AUTH-REQUEST example

```
From: main@etsi.org
To: einstein@etsi.org
Subject: 01000000
Date: Fri, 25 Jul 2003 09:55:06 -0600
MIME-Version: 1.0
Content-type: application/octet-stream
Content-Transfer-Encoding: binary

05 40 0a 03 01 10 10 0c 08 90 18 03 a1 83 01 70 0a
```

After a PT has registered to a particular FT normal operation can resume, e.g. outgoing/incoming calls can be handled. In such a case the PT, VFT and HFT shall comply with the following:

Outgoing Calls Tunnelling

- PT Provides Calling party To address indicating "IP Mobility: Call establishment". VFT shall construct an internet message, include the CC-SETUP in the message body and forward the message to the HFT. Mapping between DECT signalling messages and IP shall be made in the HFT. Any run in parallel DECT procedures shall be made between the HFT and VPT and the transport mechanism as described above shall be used (SMTP and MIME messages).

Incoming calls Tunnelling

- On receipt of a call dedicated to the PT, HFT shall initiate a DECT incoming call as described GAP. DECT messages shall be transferred to the VFT incorporated into Internet message as describe above. The Calling party number shall be sent using IWU-TO-IWU information element.
- The VFT shall recover the DECT message and received from the HFT and send them to the PT, and shall incorporate DECT messages received from the VPT into Internet message as describe above and send them to the HFT.

7.2.1.4.4 The SIP mix method

For terminals that support the SIP mix method the requirements specified in this clause apply.

After a PT establishes that it is allowed to roam to a particular FT it shall attempt roaming registration. In such a case the PT, VFT and HFT shall comply with the following:

Registration

For the Registration in this case the same exchange of DECT messages as in the Case of the Tunnelling method shall be used. The method for transport, however should be based on establishing of a SIP session between the VFT and the HFT and carrying the DECT messages as Message bodies into the relevant SIP messages (Messages specified in SIP extensions may be used as well if supported by the SIP protocols at both sides):

- {LOCATE-REQUEST} into the {INVITE}.
- {AUTH-REQUEST} into the {200 OK}.
- {AUTH-REPLY} into the {ACK}.
- {LOCATE-ACCEPT} into the {BYE}.

Outgoing/Incoming calls

- Te rules for SIP conference sessions shall apply (RFC 3261 [18]).

7.2.1.4.5 DECT elements of messages/procedures

DECT procedures relevant for this clause shall be implemented as described in GAP, EN 300 444 [13], or if not included there as described in DECT Common Interface (CI), EN 300 175-5 [5], Network (NWK) layer. Modifications, additions specified in this clause apply as well.

Specific IP related information shall be included into IWU-TO-IWU information element. If necessary the IWU-TO-IWU shall be segmented to avoid messages exceeding 63 octets of length.

Table 11: <<IWU-TO-IWU>> Action field = Registration/Call establishment

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1001000	IP Mobility: Registration
Body		1001001	IP Mobility: Call establishment
	Fields_presence_indicator.ext	1	Multi octet extension - last
		0	Multi octet extension - more
	Fields_presence_indicator.value	xxxxxxx	Identifies which field is present in the rest of the Body. A bit set to "1" shall be understood as "field present"
		xxxx1xx	To address
		xxx1xxx	From address
	To	All	4 octets
	From	All	4 octets

Due to the fact that the transmission of DECT messages over the IP may take longer time, the use of the {CC-NOTIFY} and {MM-NOTIFY} is required to avoid timing out at the initiating side. The VFT shall be responsible for sending the messages to the VPT and the HFT IWU shall take care of it at the HFT side.

NOTE: The format of the {MM-NOTIFY} message and its usage in MM procedures require additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

7.2.1.5 User roaming IP roaming IPv4

The User roaming is a feature that allows a User to be accessible on its Home address as defined by RFC 3344 [17] when the user moves from one DECT PP terminal to another DECT PP terminal.

For the provision of this feature:

- The user shall be capable of carrying on external media all mandatory IP mobility parameters.
- The DECT terminals shall support setting up of multiple user profiles allowing for a visiting user to configure its own MN profile on a visited terminal.

The support of multiple user profiles adds to the concept of DECT MN defined in the previous clauses the possibility that one and the same tandem of a PP and FP may represent more than one DECT mobile nodes.

For the provision of multiple user profiles the following requirements apply:

- A DECT PP shall be capable of establishing and storing more than one DIMS as defined in clause 7.2.1.2.2 distinguishable by the Username. All actions related to IP mobility registration and call handling shall be distinguished by Username/DIMS. This may require either pre-setting of the PP in user X mode, or upon user request for action the user X shall provide her username.
- A DECT FP shall be capable of establishing different user records based on the PP's IPUI and the Username. All actions related to IP mobility registration and call handling shall be distinguished by IPUI/Username. For incoming actions, e.g. incoming calls provision at the Portable terminal of an indication for which user the call is related is required.
- In regard to IP mobility the requirements as stated in all relevant previous clauses parts of clause 7.2.1 shall apply, e.g. in addition to the requirements specific for User roaming a designer needs to implement the requirements for PP IP Mobility for example.

For User Identification the User name shall always be included:

- For Registration into the {LOCATE-REQUEST} message even if Home Address is provided (see clause 7.2.1.2.3).
- For Call handling in a <<IWU-TO-IWU>> information element indicating "IP Mobility: DIMS" and providing the User name (see clause 7.2.1.2.5). The <<IWU-TO-IWU>> shall be included into the {CC-SETUP} message.

7.2.2 Handover

IP handover is not currently specified in the IETF - IP roaming is. An IP handover includes IP roaming and consequently all IP roaming requirements in the case of IPv4 as specified in RFC 3344 [17] shall apply (the case of IPv6 is left for further study). Compliance with the Registration procedure defined for the IPv4 Mobility will result in unpredictable time interruption and will make DECT seamless handover impossible.

The IPv4 Roaming without IP Mobility feature specified in clause 7.2.1.4, however, does not require such registration and hence can provide handover capabilities to terminals that support it. The requirements needed for the provision of external handover in addition to the requirements specified in clause 7.2.1.4 are described in this clause.

7.2.2.1 Basic requirements

DECT External handover is currently defined in the EN 300 824 CAP [14] and EN 300 175-5 [5], Network (NWK) layer. The DECT CAP standard does not specify the backbone network that interconnects the separate DECT base stations (FTs) or/and DECT sub-networks.

There are two basic pre-requisites defined in CAP for the correct external handover operation:

- The provision of FT identities that allow a PT to handover from one FT to another without the need to register at the time of handover. Such Identity is assumed to be provided and set up by the network operator.
- The provision, by the FT to which the PT is locked, of handover candidates from which the PT may choose.

For the case of large systems, e.g. CTM or PBXs, a centralised provision and management of the identities and access rights is feasible and such capabilities are usually foreseen and provided by the manufacturer. Therefore, for such DECT systems the requirements specified in CAP [14] or other suitable DECT standards still can apply.

For smaller, a kind of a self-made plug-and-play, DECT systems based on an IP network backbone and e.g. a number of DECT residential FPs, an easier manageable solution is desirable. The present document specifies two alternatives.

- Alternative one (1) is based on the requirements specified in clause 7.2.1.2.2 and mandates a manual, set by the user, SARI which shall solve both problems: provision of access rights and handover candidate indication. The combination of a common Roaming ARI plus the indication of "External Handover allowed" broadcasted by the FT shall provide a PT with the bases for taking of a decision to attempt external handover to a FT. This solution avoids the use of Handover Candidate/Reference procedures as specified in CAP.

- Alternative two (2) is based on automatic assignment of a Roaming ARI and is suitable for FTs that are connected to one and the same IP network. The procedure is defined in clause 7.2.2.2. This solution provides as an option the usage of Handover Candidate/Reference procedures as specified in CAP.

After a PT has established that an external handover to a particular FT is allowed it shall initiate an External Handover call setup procedure as defined in clause 7.2.2.3.

7.2.2.2 Automatic assignment of a external handover related identities

Upon connection to the IP NWK a FT shall listen for T_roaming time whether a Roaming RFPI is being broadcasted on the net. The FT shall repeat the procedure up to N_roaming times if no Roaming RFPI broadcast has been detected.

If no Roaming RFPI is received the FT shall allocate a Roaming RFPI for this network and shall start periodically broadcasting it on the IP network for every FT that may connect to the same network.

For the allocation of a Roaming RFPI the FT shall use the procedures defined in clause 7.2.1.2.2 with the following modification. If the FT's PARI contains ARI of class A, the FT should request the PT to assist in the allocation of the Roaming RFPI FPN number. In this case the PT shall listen for a Roaming RFPI possibly transmitted by FTs connected to another closely allocated IP network, shall then determine the FPN number and send it back to the FT. If the FT's PARI contains ARI not of class A it shall use its own RFPI for the allocation of the Roaming RFPI. The FT initiated parameter retrieval procedure shall be used. The <<Info Type>> information element in the {MM-INFO-SUGGEST} message shall be set to "Identity allocation". At the PT side the procedure defined in clause 7.2.1.2.2 shall apply.

For the broadcast on the IP network the FT shall use the {MM-INFO-SUGGEST} message included into the body of internet messages formatted according to the RFC 2045 [28] and RFC 2046 [29] MIME specification using Content-type: application/octet-stream and Content-Transfer-Encoding: binary and "Subject" field set to "01010010", i.e. the message type code for {MM-INFO-SUGGEST}. The {MM-INFO-SUGGEST} message shall contain a <<Info type>> indicating "External handover parameters" and a <<Network parameter>> information element indicating Handover reference, e.g. "Handover reference, private network" and providing the Roaming ARI.

If a Roaming RFPI is received the FT shall accept it and shall start broadcasting it on the DECT air interface as a SARI (see clause 7.2.1.2.2) together with the indication "External Handover Supported".

7.2.2.3 External handover call setup

For the External Handover call establishment the requirements as specified in CAP [14], clauses 9.1.4 and 9.1.5 shall apply with the following modifications.

The support of External handover candidates related procedures/requirements is optional. The choice of FT suitable for external handover shall be based on the common knowledge of the Roaming ARI broadcasted.

For the external handover call setup in addition to indicating "External handover" into the <<Basic Service>> information element included into the {CC-SETUP} message, the PT shall provide its current IP address, i.e. the address on which the PT is engaged in the call which the PT attempts to handover. The IWU-TO-IWU information element shall be used indicating "IP Mobility: Call establishment" and the address shall be provided into the "To" field of the <Body>.

Table 12: <<IWU-TO-IWU>> Action field = Registration/Call establishment

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1001000	IP Mobility: Registration
Body		1001001	IP Mobility: Call establishment
	Fields_presence_indicator.ext	1	Multi octet extension - last
		0	Multi octet extension - more
	Fields_presence_indicator.value	xxxxxxx	Identifies which field is present in the rest of the Body. A bit set to "1" shall be understood as "field present"
		xxxx1xx	To address
	To	All	4 octets

Having the address of the FT that is currently handling the call (HFT) the VFT should proceed depending on the implementation of the IP network:

- If SIP is supported on the NWK, the VFT may attempt to establish a "3 party conference" session with the HFT which should mix the current call leg and the new call leg. A DECT LOCATE-REQUEST message providing the PT's identity should be included into the INVITE message body to be used as indication that this is an attempt of external handover. The HFT may perform authentication towards the VFT-PT to ensure that the PT is indeed the one engaged in the call.

- If SIP is not supported, the VFT should incorporate the received from the PT {CC-SETUP} message into the body of an internet message formatted according to the RFC 2045 [28] and RFC 2046 [29] MIME specification as specified in clause 7.2.1.4 and send it to the HFT. Upon reception of the message the HFT should attempt establishing of a VoIP call to the VFT and if successful should connect the two paths. The HFT may perform authentication towards the VFT-PT to ensure that the PT is indeed the one engaged in the call.

7.2.2.4 FP synchronisation over the IP network

For handover purposes synchronisation between FTs may be desirable.

NOTE: There may be PTs that support handover between non synchronised FTs. However, due to the fact that such an implementation requires support of two reference clocks there are not many terminals on the market supporting it. Furthermore, handover between unsynchronised FTs reduces the overall DECT capacity.

In the IP world time synchronization across network servers, routers and network devices with accuracy to the order of a microseconds may be achieved using the well-established Network Time Protocol (NTP, RFC 1305 [21]). Most users of the Internet NTP synchronization use a relatively big and complex software package which may not be appropriate for all applications. The Simple Network Time Protocol (SNTP, RFC 2030 [20]) has been designed to target wide variety of "simpler" applications, however, SNTP provide accuracy only in the order of milliseconds.

The DECT specification requires that the difference between reference timers of synchronized RFPs shall be less than 4 microseconds. Consequently if a system would like to provide DECT base stations synchronisation over the IP it shall implement the NTP [21].

If the cost of such implementation is not feasible DECT base station synchronisation over separate wire or the DECT air interface may be more applicable. The implementation of such solutions is out of the scope of the present document.

7.3 SIP interworking

7.3.1 General

This clause specifies the requirements in regard to the mapping between SIP and DECT relevant procedures and messages.

The IP procedures, and, messages format and content mapped to DECT procedures/messages are based on the requirements found into the following IETF RFCs:

RFC 3261 [18]: "SIP: Session Initiation Protocol".
RFC 2327 [19]: "Session Description Protocol (SDP)".
RFC 2617 [22]: "HTTP Authentication: Basic and Digest Access Authentication".
RFC 2806 [23]: "URLs for Telephone Calls".

DECT procedures/messages requirements are based on those specified in:

DECT Common Interface (CI), EN 300 175-5 [5], Network (NWK) layer.
DECT Generic Access Profile (GAP), EN 300 444 [13].

SIP is an application-layer signalling protocol that can establish, modify, and terminate interactive multimedia sessions over IP between intelligent terminals with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. It is a clear text client/server protocol using Uniform Resource Locators (URL) for addressing (in this sense having a lot in common with HyperText Transfer Protocol (HTTP)).

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types (users may move between endpoints, they may be addressable by multiple names, and they may communicate in several different media - sometimes simultaneously). SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers.

SIP runs on top of several different transport protocols enabling Internet endpoints called user agents (UA) to discover one another and to agree on a characterization of a session they would like to share. For locating prospective session participants, and for other functions, SIP enables the creation of an infrastructure of network hosts (called proxy servers) to which user agents can send registrations, invitations to sessions, and other requests.

A user agent represents an end system. In the context of the present document a User Agent comprises a DECT FP and a DECT PP part and the UA activities may be provided either by the FP part (called FP-UA) or by the PP (called PP-UA). As a FP can serve a number of PPs, each tandem of the FP and a PP may, but need not, represent an independent UA, i.e. the FP may be engaged in a number of different UAs, whereas a PP may be engaged only in one UA.

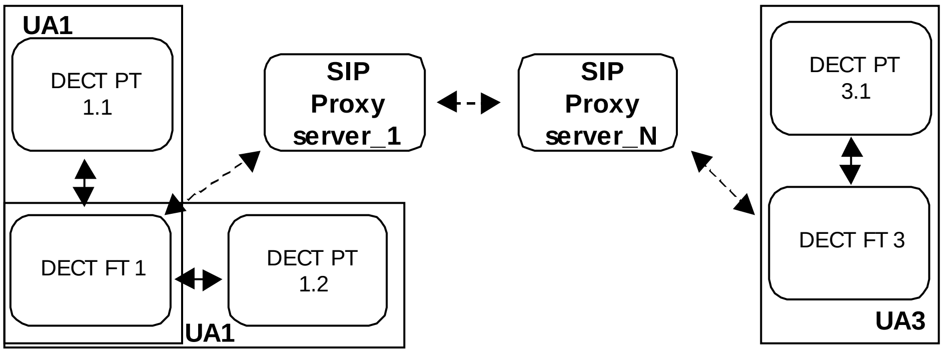

Figure 7: SIP elements reference model

Figure 8 shows the FT DECT - SIP protocol reference architecture for the scope of the present document. The Ethernet protocol, towards the external NWK, is shown only as an example.

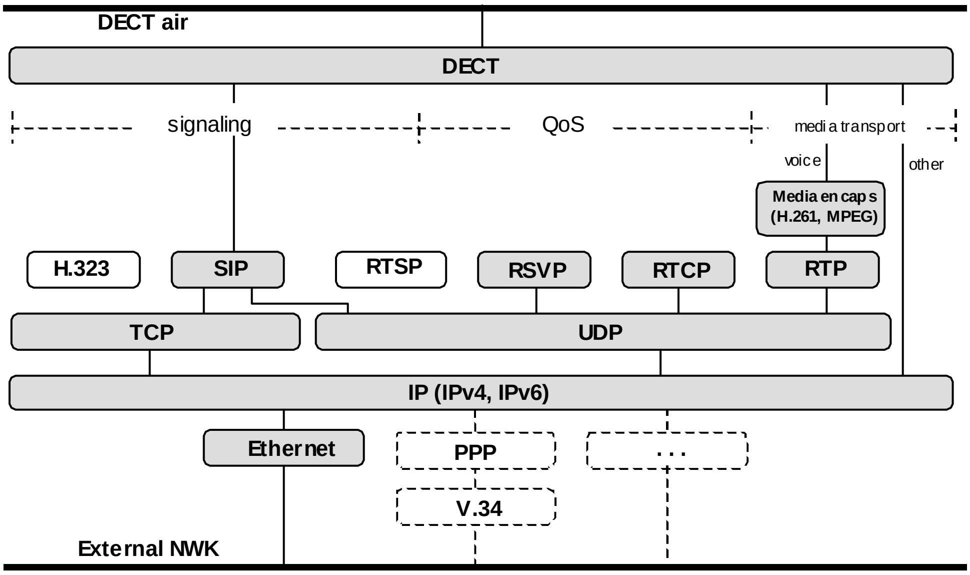

Figure 8: Protocols relation reference architecture FT

Generally speaking, a DECT PT may be seen as a special application that uses the DECT protocol to interwork with the residing into the FT SIP and related protocols. This application represents an interface to the user, thereby allowing for the user to actively interact with the network, and is responsible for the provision to the FT of all user information that the FT, in turn, needs to successfully implement and perform the SIP and related protocols requirements. In this regard, the aim of the present document is to specify a transport mechanism, whereas the local, at the PP, implementation of this communication is left to the designer.

The Procedures described in this clause are based on the exchange of SIP related information carried into one or a number of DECT <<IWU-TO-IWU>> information elements. Although other DECT information elements could have been used for different portions from the SIP messages content, the current approach has been chosen with the aim of facilitating the protocol implementation by separating and concentrating all relevant data into a single space. Furthermore the current approach requires a single information decoding/interpretation requirement: data shall be formatted/interpreted as specified in RFC 3261 [18]. Contrary to RFC 3261 however the present document mandates usage of IA5 character set (see EN 300 175-5 [5], clause D.2.3) on DECT air which requires the DECT FT to make the conversion IA5/UTF-8 (the latter mandated for usage in SIP).

In compliance to GAP the present document does not mandate the support of DECT messages of more than 63 octets length (see EN 300 444 [13], GAP, clause 6.9.3). SIP information is a character based which will inevitably result into longer DECT messages. Consequently, implementations that comply with the present document shall support DECT segmentation of information elements, i.e. whenever necessary the <<IWU-TO-IWU>> information element shall be segmented in a number of DECT messages. As a general rule in the case of a MM procedure the <<IWU-TO-IWU>> segments from the second on shall be carried in {MM-IWU} messages and in the case of the CC procedure into {IWU-INFO} messages. To allow sending/reception of {MM-IWU} messages after the last message of a MM procedure has been sent/received the MM entity shall indicate "partial release" in the NLR notification as specified in EN 300 175-5 [5], clause 14.2.7.2.

NOTE: Segmentation of <<IWU-TO-IWU>> and the usage of {MM-IWU} together with other MM procedures require additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

7.3.2 Registration

7.3.2.1 Procedure mapping

The SIP Registration procedures (RFC 3261 [18]) create explicitly bindings in a location service for a particular domain that associates an User Agent's (UA's) Address-Of-Record (AOR), i.e. a URI (Unified Resource Indicator), with one or more contact addresses. An AOR is a SIP or SIPS URI that points to a domain with a location service that can map the AOR to a contact address (another URI) where the user might be available. An AOR is frequently thought of as the "public address" of the user whereas a contact address is an address on which the user may be found at a particular moment of time. The AOR is normally given to the user from a service provider. In addition for security reasons a user name and password will normally be given to the user too.

NOTE 1: There are many ways by which the contents of a location service can be established. One way is administratively. These are out of the scope of the present document.

SIP registration entails the UA sending a REGISTER request to a special type of UA known as a registrar which acts as the front end to the location service for a domain, reading and writing mappings based on the contents of REGISTER requests. This location service is then typically consulted by a proxy server that is responsible for routing requests for that domain.

NOTE 2: The registrar and proxy server are logical roles that can be played by a single device in a network.

SIP distinguishes a number of UA registration related procedures which for the purpose of the present document are grouped in three sets:

- Adding/Modifying bindings including: Adding bindings, Setting the Expiration Interval of Contact Addresses, Setting Preferences among Contact Addresses and Removing Bindings.
- Fetching Bindings.
- Refreshing Bindings.

The Adding/Modifying bindings procedures shall be mapped to the DECT Attach (Location registration) procedure as specified in GAP, EN 300 444 [13] and modifications/additions specified in the present document. The fetching bindings shall be mapped to a Parameter retrieval procedure as specified in EN 300 175-5 [5] and modifications/additions specified in the present document. The Refreshing Bindings is not mapped to a DECT procedure.

NOTE 3: It is possible that the manufacturer of a DECT FP offers some proprietary means at the FP for configuration of all necessary parameters allowing for the DECT FT to be fully in control and perform all necessary tasks in regard to SIP registration. Such implementation is out of the scope of the present document.

7.3.2.1.1 Adding/Modifying bindings

All SIP procedures falling in this group can be run separately or in combination and shall be started upon the User's request.

Upon procedure initiation the user shall provide at least its AOR (<To> field of the REGISTER message) and the relevant authentication data (password, realm and user name). In addition the user may optionally provide contact details (<Contact> field of the REGISTER message), i.e. one or more contact addresses with associated parameters, e.g. preferences ("q" value in the <Contact> field) and expiration time ("expires" value in the <Contact> field). All information shall be provided via a suitable PP user interface (see notes 2 and 3 later on in this clause).

The minimum information provision required for support at the PT is the user's AOR, password, realm and user name. In this case the FT shall be capable of establishing the contact address in regard to the access point it is attached to and go for default contact details according to registrar administration polices. This minimum requirement does not allow the user to be able to choose contacts and details, to request more than one binding registration, nor to register bindings for a third party. For the provision of these services the user (and the PT) should be capable of supplying additional information:

- A contact address for registering a binding.

- A contact address AND contact parameters ("q" and "expire") for registering a binding with preferred parameters, as well as, removing a binding (expiration = 0) and removing all bindings (Contact = *).
- More contact addresses and parameters for registering more than one binding at a time.
- Differentiation between addresses provided for the "To" and "From" field for registering a third party.

Using the submitted by the user information the PT shall start a DECT Attach procedure providing the information in the <<IWU-TO-IWU>> information element of a {LOCATE-REQUEST} message. The PT is not required to store any of the provided information. The Attach procedure, in addition, shall be used by the PT to indicate its media capabilities provided into the <<Terminal capability>> information element. The default media type support is "voice" which needs not be explicitly indicated. If other media types are supported these shall be indicated. If the information to be included into the <<IWU-TO-IWU>> information element will result in a {LOCATE-REQUEST} message longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and segments shall be included in one or more {MM-IWU} messages being sent after the {LOCATE-REQUEST} message carrying the first segment. PT shall restart timer <MM_locate.1> after sending every {MM-IWU} message.

NOTE 1: Media types different than voice are left for further study.

Upon receipt of the {LOCATE-REQUEST} message the FT shall check for the presence of a <<IWU-TO-IWU>> and possibly a <<Segmented Info>> information elements. If <<IWU-TO-IWU>> has been segmented FT shall await reception of one ore more {MM-IWU} messages and attempt to re-assemble the complete information. When the information has been re-assembled the FT shall examine it, shall store it in a user record distinguished by the PT's IPUI and the user's authorisation data, and shall proceed with the desired procedure at the IP side depending on the content of the <<IWU-TO-IWU>> i.e. a SIP Registration related procedure.

If the procedure is successful at the FT-IP side the FT shall store the agreed details and send back to the PT a {LOCATE-ACCEPT} message. Any difference between the provided by the user and the approved by the registrar information shall be communicated to the user in the <<IWU-TO-IWU>> information element. If the user requested Adding bindings and did not provide a <Contact> into the request, the associated with the registration contact shall be provided by the FT into the {LOCATE-ACCEPT} message for user information. In the SIP 200 OK message normally all existing bindings of the user will be provided, including such made previously; these bindings may but need not be provided to the user at this moment and may but need not be stored in the user record in the FT (see the procedure for Fetching bindings later on in this clause).

If the information to be included into the <<IWU-TO-IWU>> information element will result in a {LOCATE-ACCEPT} messages longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and segments shall be included in one or more {MM-IWU} messages being sent after the {LOCATE-ACCEPT} message carrying the first segment. The MM entity shall use "partial release" to maintain the link open for these messages.

NOTE 2: The implementation of the interface and dialog with the user (possibly a combination of keypad and display) for providing the required information is left to the manufacturer. User may be provided with the opportunity of inputting the URI manually or selecting it from some sort of address book. User may be allowed to provide only partial information which will later on be correctly formatted by the PT before providing it to the FT, e.g. the user needs not enter a complete URI, but rather a string of digits or letters (for example, "sbaev" for sip:sbaev@etsi.org). Furthermore, the user needs not to be required to enter some field formatting characters, e.g. "<". It is at the discretion of the PT-UA to choose how to interpret this input and provide unambiguous data to the FT-UA (e.g. sip and sips need to be distinguished, etc.).

NOTE 3: In the case of the Setting the Expiration Interval of Contact Addresses SIP provides two ways in which a client can suggest an expiration interval for a binding: through an Expires header field or an "expires" Contact header parameter. The latter allows expiration intervals to be suggested on a per-binding basis when more than one binding is given in a single REGISTER request, whereas the former suggests an expiration interval for all Contact header field values that do not contain the "expires" parameter. The present document specifies that expiration, when provided by the user, will be provided per binding.

NOTE 4: It is assumed that a Location registration procedure may also take place under circumstances out of the scope of the present document where it may be regarded as a location registration in the normal DECT meaning and not as a SIP Registration. A manufacturer may for example chose to pre-register a PP with a FP and sale them together. At such point of time no SIP information will be available. In such cases no <<IWU-TO-IWU>> information element indicating a SIP action will be present in the {LOCATE-REQUEST} message.

NOTE 5: The maintenance of a User record at the FT side is mandated to allow faster SIP handling and reduced DECT on-air traffic.

If the completion of the procedure on the IP side takes longer time that the time guarding the Attach procedure duration in the PT the FT shall restart the PT timer sending a {MM-NOTIFY} message.

NOTE 6: The usage of {MM-NOTIFY} requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

Upon receiving the {LOCATE-ACCEPT} message the PT shall assess the presence and content of the <<IWU-TO-IWU>> and possibly the <<Segmented info>> information elements. If <<Segmented info>> is present the PT MM entity shall indicate "partial release" to the LSE to maintain the link open for the following up {MM-IWU} messages. After the complete information has been re-assembled the PT shall examine it and inform the user for any details.

NOTE 7: The presentation of the information to the user is left to the manufacturer's choice.

For security reasons if a SIP registration procedure has been requested the PT shall first cipher the link. The requirements for Cipher switching initiated by PT procedure as specified in GAP, EN 300 444 [13], clause 8.34 apply. Figure 9 provides an example of messages flow of a SIP Registration procedure.

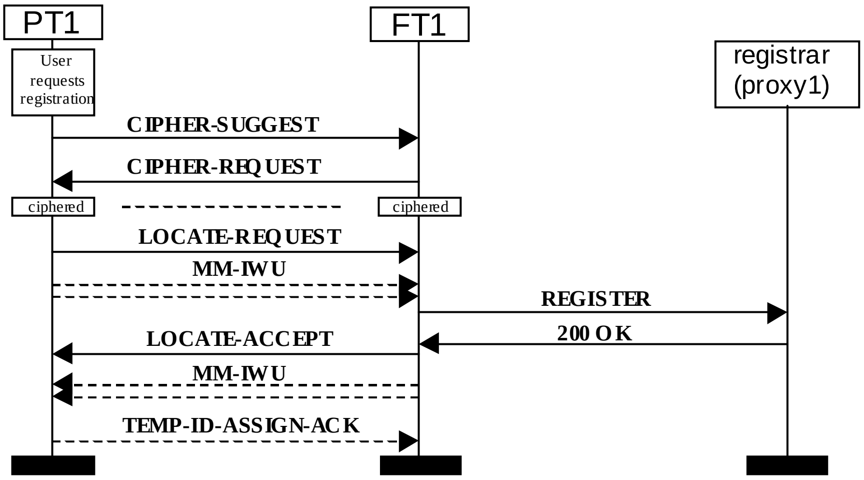

Figure 9: Successful SIP registration

If a SIP Registration related procedure fails the FT shall reject the Attach procedure providing the SIP response code and optionally the code word into the {LOCATE-REJECT} message if the reason for the failure could be attributed to the User's input, e.g. misspelled address. The user shall be informed, e.g. the problem should be displayed. The user may re-initiate the procedure. If the information to be included into the <<IWU-TO-IWU>> information element will result in a {LOCATE-REJECT} messages longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and segments shall be included in one or more {MM-IWU} messages being sent after the {LOCATE-REJECT} message carrying the first segment. The MM entity shall use "partial release" to maintain the link open for these messages.

In some cases the reason for failure at the SIP side may be attributed to technical problems not related to the user, e.g. timeout at the registrar due to delay on the IP network. If possible the FT shall try to solve the problem before completing the attach procedure and without engaging the PT and the user. If however this is not possible for the time required for response back to the PT, the FT shall reject the attach procedure providing the reason for the rejection. After rejecting the attach the FT may still try to register following the rules as specified in the SIP protocol RFC 3261 [18] and inform the user for the results. The user should be properly informed for such activities. If the user tries to register again when a registration procedure is still in progress at the FT-IP side, the FT shall examine the new {LOCATE-REQUEST} message and if there is no different address parameters provided shall continue with the on-going registration (new contact parameters shall be ignored). In any other case the FT should try to complete the ongoing procedure before taking any action.

7.3.2.1.2 Fetching bindings

The user shall be provided with the possibility to review its registration details. Upon procedure initiation the user shall provide the relevant authentication data (password, realm and user name).

Using the submitted by the user information the PT shall start a DECT Parameter retrieval procedure providing the information in a {MM-INFO-REQUEST} message. If the information to be included into the <<IWU-TO-IWU>> information element will result in a {MM-INFO-REQUEST} messages longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and segments shall be included in one or more {MM-IWU} messages being sent after the {MM-INFO-REQUEST} message carrying the first segment. The PT shall restart timer <MM_info.1> after each {MM-IWU} message sent.

Upon receipt of the request the FT shall examine the provided data and shall compare it with the data the FT has stored for that PT/user. If the data matches the FT shall provide full bindings details back into a {MM-INFO-ACCEPT} message or reject the request otherwise with a {MM-INFO-REJECT} message. The bindings details should be retrieved from the PT record maintained at the FT if FT maintains full bindings details, or otherwise the FT shall initiate SIP fetching bindings procedure towards the IP before sending the response. It is the responsibility of the FT to guarantee that up to date registration information is always available into the User's record.

If the completion of the procedure on the IP side takes longer time that the time guarding the Parameter retrieval procedure duration in the PT the FT shall restart the PT timer sending a {MM-NOTIFY} message.

NOTE: The usage of {MM-NOTIFY} requires additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

If the information to be included into the <<IWU-TO-IWU>> information element will result in a {MM-INFO-ACCEPT/REJECT} messages longer than 63 octets, the <<IWU-TO-IWU>> shall be segmented and segments shall be included in one or more {MM-IWU} messages being sent after the {MM-INFO-ACCEPT/REJECT} message carrying the first segment. Both MM entities shall use "partial release" to maintain the link open for these messages.

For security reasons before initiating the Fetch bindings procedure the PT shall first cipher the link. The requirements for Cipher switching initiated by PT procedure as specified in GAP, EN 300 444 [13], clause 8.34 apply. Figure 10 provides an example of messages flow of a SIP Fetching bindings procedure when the FT did not have locally stored the requested information.

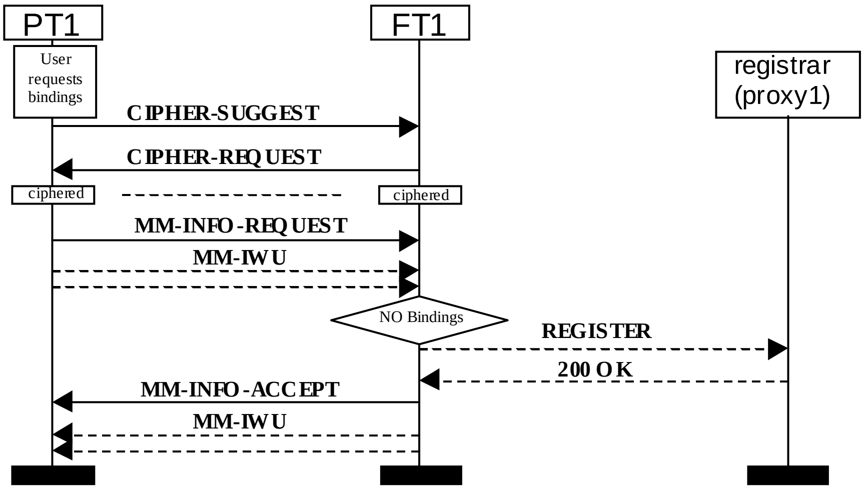

Figure 10: Fetching bindings

7.3.2.1.3 Refreshing bindings

The Refreshing bindings procedure relates to the refreshing of the bindings data stored into the FT for each user (PT). The procedure is specially related to the renewing bindings before their expiration interval has elapsed.

NOTE: Such renewing will be normally based on local network policies.

This procedure is not explicitly mapped to a DECT procedure because it is a matter to be handled between the FT and the IP.

It is assumed that it is the User's responsibility for an explicit change of her/his bindings. If however, after registration and without user intervention, a change in bindings occurs which has impact on the user's capability of receiving calls at that particular contact address, e.g. a binding was removed, this shall be indicated to the user with information provided in one or more {MM-IWU} messages.

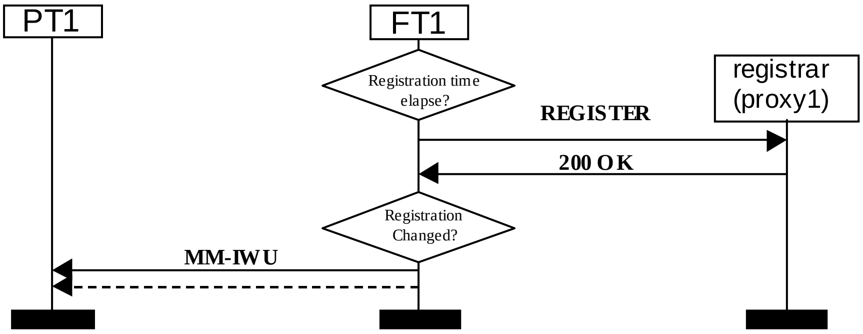

Figure 11: Information for bindings change

7.3.2.2 Message mapping

7.3.2.2.1 DECT-SIP message mapping

Table 13: SIP registration messages List DECT-to-SIP

Item No	DECT Message	SIP Message	Map status	Reference GAP
1	LOCATE-REQUEST	REGISTER	m	8.28
2	MM-INFO-REQUEST	REGISTER	m	-
3	MM-IWU	REGISTER	m	-

Table 14: SIP registration messages List SIP-to-DECT

Item No	SIP Message	DECT Message	Map status	Reference GAP
1	200 OK	LOCATE-ACCEPT	m	8.28
		MM-IWU	m	-
		MM-INFO-ACCEPT	m	-
2	3.xx, 4xx, 5xx	LOCATE-REJECT	m (note)	8.28
		MM-IWU	m	-
3	3.xx, 4xx, 5xx	MM-INFO-REJECT	m (note)	8.28
		MM-IWU	m	-
NOTE: The exact error indications possible during registration are specified in RFC 3261 [18].				

7.3.2.2.2 DECT messages/information elements mapping

For the content of messages/information elements the requirements specified in EN 300 444 GAP [13] and/or in EN 300 175-5 [5] whenever relevant apply. This clause lists only the differences/additions.

For the structure of the <<IWU-TO-IWU>> information element the requirements in EN 300 175-5 [5] and annex A of the present document apply. Here only the requirements in regard to SIP Registration are indicated.

NOTE: The segmentation of <<IWU-TO-IWU>> and its value of the <Protocol discriminator> require additions to the DECT CI standard, EN 300 175-5 [5]. Before these changes are implemented they are indicated in annex C of the present document. All changes are backwards compatible.

Table 15: <<IWU-TO-IWU>>

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	0000010	SIP REGISTER: Adding/Modifying bindings
		0000011	SIP REGISTER: Fetching bindings
		0000100	SIP REJECT
Body		All	Contains Fields from a SIP Message formatted according to RFC 3261 [18] using IA5 character set with the additions/modifications as specified in the present document.

Table 16: <<IWU-TO-IWU>> Body requirements

Field	Format/Comment	Support			
		PT to FT		FT to PT	
		PT	FT	FT	PT
Start Line	From the Start line only the Request URI portion needs to be supported in the format of "Request-URI: <name-addr>". The inclusion of the <Request-URI> field is optional. It is assumed that the FT shall have means to establish this address.	O	M	O	O
Status Line	Only the "Status-Code" portion needs to be supported for on-air transmission in which case the "Reason-Phrase" can be locally generated at the PT.	I	I	M	M
Message-Header	For the support of the different Headers see the table Message-Header fields support below.	M	M	M	M
Message body		I	I	I	I

Table 17: <<IWU-TO-IWU>> Body message-Header fields support

Field	Format/Comment	Support			
		PT to FT		FT to PT	
		PT	FT	FT	PT
Authorization	The format of this field is changed to include the user's password: Authorization: username = "name", realm = "realm", userpassword = "password"	M	M	-	-
Contact	Notes 2, 3, and 4	O	M	M	M
Error-Info	Optional to be used together with the Error status code	-	-	O	O
From	Support of "display name" is optional, only the provision of "name-addr" is mandatory, all other parameters are FT responsibility matter (note 5)	O	M	O	O
Proxy-Authorization	The format of this field is changed to include the user's password: Proxy-Authorization: username = "name", realm = "realm", userpassword = "password"	M	M	-	-
Retry-After	If included shall be used together with the Error status code	-	-	M	M
To	Support of "display name" is optional, only the provision of "name-addr" is mandatory, all other parameters are FT responsibility matter (note 5)	M	M	O	O

NOTE 1: Field's format and values, except otherwise stated in the present document, shall be provided according to the requirements specified in RFC 3261 [18]. To reduce the length of the DECT message the compact forms of the header field names shall always be used.

NOTE 2: The PT may provide none, one or more addresses into the <Contact> field if the user has requested so. It is assumed that the FT shall have knowledge as of its own address which shall be used for a contact address for registration, the user may provide more. The FT shall provide to the PT its contact address after registration if it differs to the name-addr provided in the <From> field.

NOTE 3: If the User would like to set preferences (priorities) among the addresses in the binding she/he shall provide the value of the "q" parameter into the contacts (see RFC 3261 [18]).

NOTE 4: If the user would like to set Expiration Interval for a binding she/he shall provide the value of the "expires" parameter into the contacts (see RFC 3261 [18]).

NOTE 5: Optionally a User may be provided with capability to SIP register a third party in which case different values for the <To> and <From> header fields need to be provided (see RFC 3261 [18]).

The <<IWU-TO-IWU>> information element may be included, with respect to the procedure performed, into the {LOCATE-REQUEST}, {LOCATE-ACCEPT}, {LOCATE-REJECT}, {MM-INFO-SUGGEST}, {MM-INFO-ACCEPT}, {MM-INFO-REJECT} or {MM-IWU} message. For the structure of those messages the requirements in EN 300 444 [13] or EN 300 175-5 [5] respectively apply with the following modifications.

Table 18: Values used within a MM message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Segmented Info>>			Note 2
	<Segmented element type>	1110111	<<IWU-TO-IWU>>
<<IWU-TO-IWU>>		All	Note 1
Note 1: For the content of the <<IWU-TO-IWU>> information element see above. Note 2: Mandatory only if the message will exceed 63 octets or when <<IWU-TO-IWU>> was segmented.			

Table 19: Values used within the {MM-INFO-REQUEST}

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Info type>>			
	<Parameter type Coding>	0000110	Dynamic parameters allocation (note 3)
<<Segmented Info>>			Note 2
	<Segmented element type>	1110111	<<IWU-TO-IWU>>
<<IWU-TO-IWU>>		All	Note 1
NOTE 1: For the content of the <<IWU-TO-IWU>> information element see above. NOTE 2: Mandatory only if the {MM-INFO-REQUEST} message will exceed 63 octets. NOTE 3: This coding may be used for other purposes as well therefore, implementations complying with the present document shall examine the content of the <<IWU-TO-IWU} information element, if present, before taking any action.			

The following tables provide examples of DECT information elements content in regard to the various registration procedures.

Table 20: <<IWU-TO-IWU>> Examples - default binding registration (minimum)

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000010	SIP REGISTER: Adding/Modifying bindings
Body		t: Stoyan <sip:sbaev@etsi.org> Authorization: username = baev, realm = etsi.org, password = dect03	The inclusion of the "display name" Stoyan is optional
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

Table 21: <<IWU-TO-IWU>> Examples - fetching bindings

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000011	SIP REGISTER: Fetching bindings
Body		t: Stoyan <sip:sbaev@etsi.org> Authorization: username = baev, realm = etsi.org, password = dect03	The inclusion of the "display name" Stoyan if the "t" is included is optional (note 2)
NOTE 1: Field values shall be formatted according to the requirements specified in RFC 3261 [18]. NOTE 2: The provision of the <To> field is optional for this procedure, FT shall have a record with the relevant information. However, the provision of the field would allow a user to fetch her bindings before registering for example when moving to a new FT.			

Table 22: <<IWU-TO-IWU>> Examples - registering 2 own contacts with parameters

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000010	SIP REGISTER: Adding/Modifying bindings
Body		t: Stoyan <sip:sbaev@etsi.org> m: "Stoyan" <sip:sbaev@einstein.etsi.org>;q = 0,7; expires = 3 600, "Stoyan_mail" <mailto:stoyan.baev@etsi.org> ;q = 0,1 Authorization: username = baev, realm = etsi.org, password = dect03	The inclusion of the "display names" optional
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

Table 23: <<IWU-TO-IWU>> Examples - removing binding from third party

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000010	SIP REGISTER: Adding/Modifying bindings
Body		t: Stoyan <sip:sbaev@etsi.org> f: Guenter <sip:guenter@viena.com> m: "Stoyan" <sip:sbaev@einstein.etsi.org> Authorization: username = guenterk, realm = etsi.org, password = epdectc	The inclusion of the "display names" optional
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

Table 24: <<IWU-TO-IWU>> Examples - Reject

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000100	SIP REJECT
Body		401 Unauthorized	The "Reason phrase" Unauthorized is optional
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

7.3.3 Call control

7.3.3.1 Procedure mapping

The main purpose of the SIP signalling protocol (RFC 3261 [18]) is the establishment, modification (if needed), and termination of interactive multimedia sessions. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. The SIP invitations used to create sessions carry contact information as well as session descriptions (RFC 2327 [19]) that allow participants to agree on a set of compatible media types (users may communicate in several different media - sometimes simultaneously).

NOTE 1: Voice media type sessions, as described in the QoS clause later on, will terminate the IP media transmission into the FT. For non voice media types the DECT U-plane interworking is left for further study. It is assumed that until such interworking is defined implementations may use for example the DPRS [16] IP interworking.

From DECT point of view a SIP session can be mapped to a DECT call and consequently a session establishment and termination can be mapped to a call establishment and termination. The call setup related procedures and the release procedure shall be performed in the case of a voice call as defined in GAP, EN 300 444 [13] with the modifications described in the present document.

If the user wants to communicate using different media simultaneously for each media type an independent DECT call shall be established. Modification of a session from one media type to another may use the same call or terminate the existing and establish a new one.

NOTE 2: For session modification see next clause.

NOTE 3: None voice media types communication is left for further study.

Upon user request for a call establishment the PT shall initiate an outgoing call setup procedure and provide all necessary information. The support of provision of the called party address information (the <To>) is mandatory. Optionally session description may be included. The SIP session related information shall be provided using the <<IWU-TO-IWU>> element segmented, if needed, into one or more consecutive {IWU-INFO} messages. The fragmentation is required if the message will exceed 63 octets if the complete <<IWU-TO-IWU>> information element is included. It is allowed that the <<IWU-TO-IWU>> is included already in the {CC-SETUP} message if sufficient information is available. FT shall re-assemble the received information, if segmented, in the order of arrival of the <<IWU-TO-IWU> fragments.

At the FT side, as soon as all necessary information is available the FT shall initiate towards the IP network a SIP session establishment.

Indication for the status of the session establishment may be mapped back to PT.

The agreed parameters of the session may be conveyed back to the PT in one or more {IWU-INFO} messages. After the SIP session is established the speech (audio) path will be connected and conversion between IP and DECT voice will occur at the FT side. An example of mapping between the DECT outgoing call establishment and release procedures and the SIP session establishment and termination procedures is provided on figure 12.

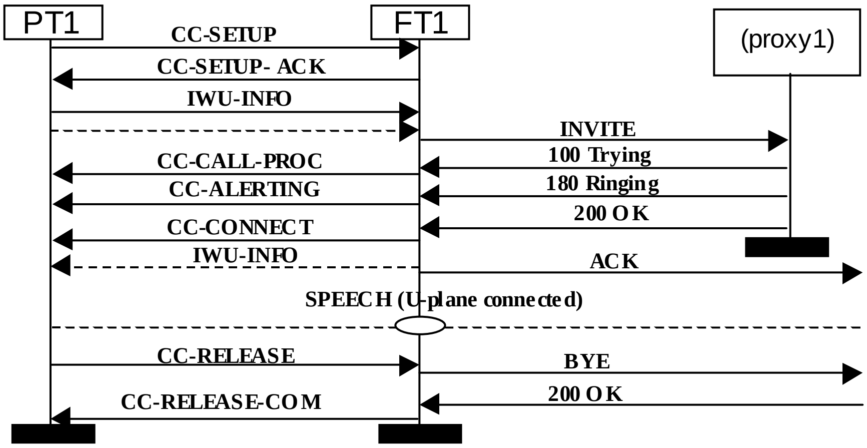

Figure 12: Successful SIP session establishment and termination Outgoing call - 1

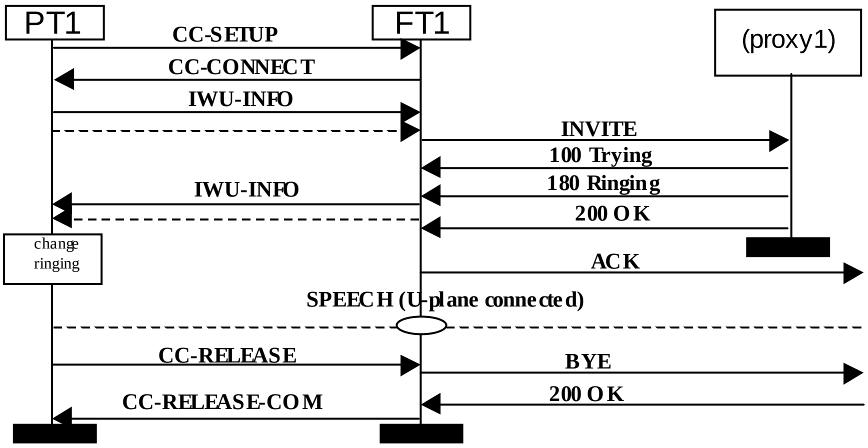

Figure 13: Successful SIP session establishment and termination Outgoing call - 2

In the case of an incoming call, the attempt of a SIP session establishment will be detected at the FT side. This, if the desired session is acceptable, will result into an incoming call establishment towards the PT.

The Caller address information (CLIP in GAP) and/or the Session description information, if supported, shall be provided into the <<IWU-TO-IWU>> information element included into the {CC-SETUP} message, segmented if necessary and in one or more consecutive {IWU-INFO} messages.

The mapping between the DECT incoming call establishment and release procedures and the SIP session establishment and termination procedures is provided on figure 14.

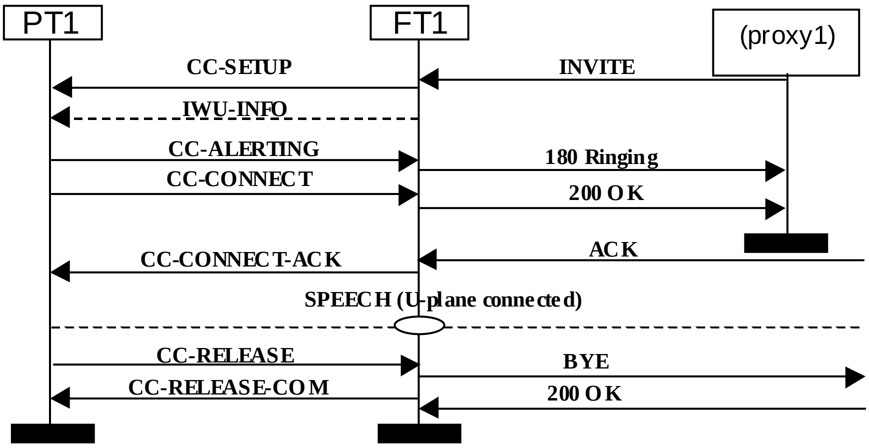

Figure 14: Successful SIP session establishment and termination Incoming call

An attempt for SIP session establishment may be unsuccessful. The reason will be indicated by the response type send to the FT from the Proxy. Some reasons may be handled at the FT whereas others may need a user action and shall be conveyed to the user. An example of unsuccessful SIP session establishment because the called party is not any longer available at the provided <To> address is shown on figure 15.

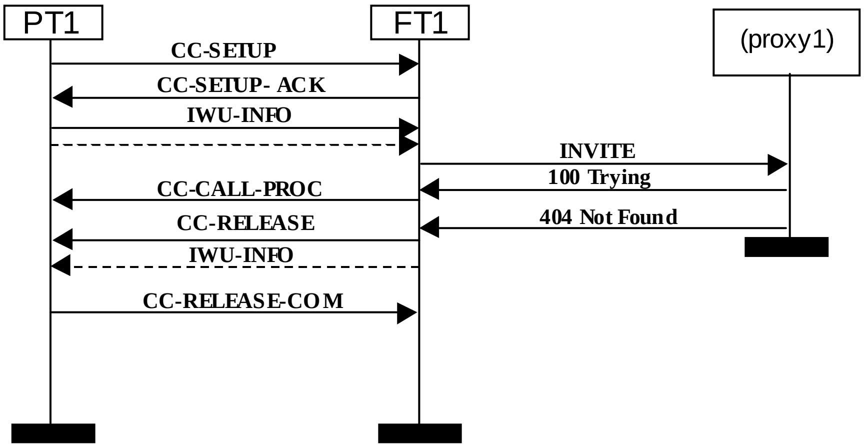

Figure 15: Unsuccessful SIP session establishment Outgoing call

If the initiating party decide to terminate its request before a call/session has been established the DECT abnormal/normal release procedure may be mapped to the SIP CANCEL or BYE procedures and may be delayed depending on the status of the SIP session establishment (see RFC 3261 [18]). An incoming SIP CANCEL shall be mapped to DECT abnormal/normal release procedure. An example of delayed mapping between a DECT release and SIP CANCEL is shown on figure 16.

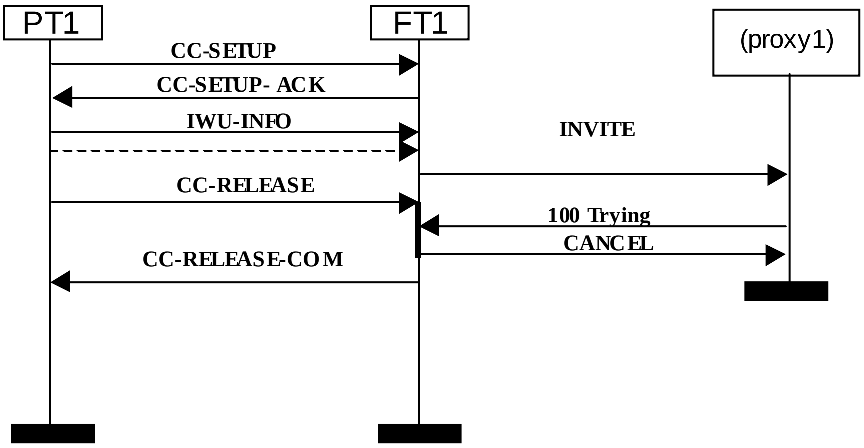

Figure 16: Calling party release before call establishment completed

By default a session shall be assumed to be a voice session in which case session description needs not be sent by the initiating side. It is the responsibility of the FT-UA to provide the correct relevant session description (audio type as defined in RFC 3261 [18] and RFC 2327 [19]) towards the IP network upon SIP session establishment. In all other cases session description information shall be provided to the receiving side into one or more {IWU-INFO} messages each of maximum length of 63 octets (see GAP [13], clause 6.9.3) included into the <<IWU-TO-IWU>> information element. When necessary this information element shall be segmented and included in consecutive {IWU-INFO} messages. If segmentation is used each message shall contain the <<SEGMENTED-INFO>> information element. Each message should contain the maximum amount of service data (of user information). On the receipt side the received information shall be re-assembled.

NOTE 4: Exact specification of session description information exchanged between the PT and the FT is left out of the scope of the present document. Further standardisation work will be required to define this exchange and a dedicated to each media transport interworking (not specified in DPRS).

A session establishment may be rejected. If a request for session establishment results not in a <200 OK> but in an error, certain error reasons shall be conveyed to the PT as corresponding reject reasons included into <<IWU-TO-IWU>> information element in a {CC-RELEASE} or {CC-RELEASE-COM} message as appropriate. If the <<IWU-TO-IWU>> was included into a {CC-RELEASE-COM} and segmented in one or more consecutive {IWU-INFO} messages, the receiving CC entity shall not request link release before all information was received.

FT shall distinguish the following general types of rejections:

a) A problem that can be solved at the FT-UA, e.g. problem related to IP. In this case FT-UA shall not reject the DECT call establishment and shall do whatever necessary to solve the problem. Optionally, FT may inform the PT for the problem providing the SIP reject coding information into a {IWU-INFO} message using the <<IWU-TO-IWU>> information element. PT shall inform the user for the outcome displaying parts or all of the information received into the <<IWU-TO-IWU>> information element. Additionally FT may need to restart the timer running at the PT and guarding the PT CC state.

b) A problem that can be solved at the FT-UA but it requires user agreement, e.g. call re-direction. In this case FT-UA shall not reject the DECT call establishment and shall inform the PT for the problem providing the SIP reject coding information and any additional information, e.g. suggested new addresses, into one or more {IWU-INFO} message using the <<IWU-TO-IWU>> information element (segmented if needed). PT shall inform the user for the outcome displaying parts or all of the information received into the <<IWU-TO-IWU>> information element. The FT shall not proceed with the IP action before the user gives OK to the FT to proceed in a {IWU-INFO} response message. The user may permit the FT to make choice on its own or the user may make the choice and provide it. FT may need to restart the timer running at the PT guarding the PT CC state.

c) A problem that was due to the user input, or user information. In this case FT-UA shall not reject the DECT call establishment and shall inform the PT for the problem providing the SIP reject coding information and any additional information, if available, into one or more {IWU-INFO} message using the <<IWU-TO-IWU>> information element (segmented if needed). PT shall inform the user for the outcome displaying parts or all of the information received into the <<IWU-TO-IWU>> information element. The User should re-submit the information required. For problems related to the users confidentiality parameters see clause Security later on.

d) All other problems, e.g. such that cannot be solved within the call establishment procedure, shall be rejected and reason code provided.

An example of reject type a) is provided on figure 17.

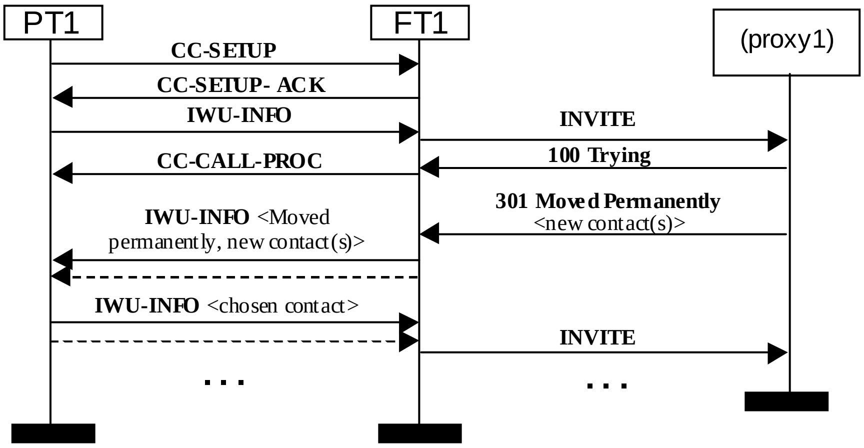
PT1
FT1
(proxy1)
CC-SETUP
CC-SETUP- ACK
IWU-INFO
INVITE
CC-CALL-PROC
100 Trying
301 Moved Permanently <new contact(s)>
IWU-INFO <Moved permanently, new contact(s)>
IWU-INFO <chosen contact>
INVITE
. . .
. . .

Figure 17: SIP session establishment after reject due to address related issue

7.3.3.2 Message mapping

7.3.3.2.1 DECT-SIP message mapping

Table 25: SIP session establishment messages List DECT-to-SIP

Item No	DECT Message	SIP Message	Map status	Reference GAP
1	CC-SETUP	INVITE	m	8.2
	IWU-INFO			-
2	CC-INFO	INVITE	m	8.2
	IWU-INFO			-
3	CC-RELEASE	BYE, CANCEL	o (note 1)	8.7
	IWU-INFO			-
4	CC-RELEASE-COM	BYE, CANCEL	o (note 1)	8.8
	IWU-INFO			-
5	CC-ALERTING	180	m (note 2)	8.14
	IWU-INFO			-
6	CC-CONNECT	200	m (note 2)	8.15
	IWU-INFO			-
7	IWU-INFO	INVITE, ACK	m	-
NOTE 1: It is left to the FT implementation to decide whether and how to map these DECT messages in relation to the SIP session establishment requirements. NOTE 2: Incoming call.				

Table 26: SIP session establishment messages List SIP-to-DECT

Item No	SIP Message	DECT Message	Map status	Reference GAP
1	INVITE	CC-SETUP	m	8.12
		IWU-INFO	m	-
2	BYE	CC-RELEASE	m	8.7
		IWU-INFO	m	-
3	ACK	CC-CONNECT-ACK	m	8.15
		IWU-INFO	m	-
4	CANCEL	CC-RELEASE, CC-RELEASE-COM	m	8.7, 8.8
		IWU-INFO	m	-
5	200	CC-CONNECT	m (note 1)	8.6
		IWU-INFO	o (note 3)	-
7	180	CC-ALERTING	c (note 2)	8.5
		IWU-INFO	m	-
8	100	CC-CALL-PROC	c (note 2)	8.4
9	181, 182, 301, 302	IWU-INFO	m	-
10	300, 400, 401, 403, 404, 408, 410, 480, 484, 485, 486, 5xx, 600, 603, 604	CC-RELEASE, CC-RELEASE-COM	m	8.7, 8.8
		IWU-INFO	m	-
NOTE 1: When answer to INVITE for outgoing call. NOTE 2: For Outgoing call a manufacturer may decide to skip some DECT CC states (see GAP [13]) - the FT-UA will generate/handle the relevant SIP messages as appropriate. NOTE 3: Used for session description. Session description is left for further study.				

7.3.3.2.2 DECT messages/information elements mapping

For the content of messages/information elements the requirements specified in EN 300 444 GAP [13] and/or in EN 300 175-5 [5] whenever relevant apply. This clause lists only the differences/additions.

For the structure of the <<IWU-TO-IWU>> information element the requirements in EN 300 175-5 [5] and annex A of the present document apply. Here only the requirements in regard to SIP Registration are indicated.

Table 27: <<IWU-TO-IWU>>

Field	Sub-field	Value	Comment
S/R		1	
Action	Ext	1	Multi octet extension
	Value	0001000	SIP SESSION ESTABLISHMENT
Body		All	Contains Fields from a SIP Message formatted according to RFC 3261 [18] using IA5 character set with the additions/modifications as specified in the present document.

The following tables indicate the SIP message fields that may be carried in the Body field of the <<IWU-TO-IWU>> SIP related information. Whether provision/understanding is required is indicated.

Table 28: <<IWU-TO-IWU>> Body

Field	Format/Comment	Support			
		PT to FT		FT to PT	
		PT	FT	FT	PT
Start Line	From the Start line only the Request URI portion needs to be supported in the format of "Request-URI: <name-addr>". The inclusion of the <Request-URI> field is optional. It is assumed that the FT shall have means to establish this address.	O	M	O	O
Status Line	Only the "Status-Code" portion needs to be supported for on-air transmission in which case the "Reason-Phrase" shall be locally generated at the PT. For the support of the different Status-Codes see the table Status-Codes field support below.	I	I	M	M
Message-Header	For the support of the different Headers see the table Message-Header fields support below.	M	M	M	M
Message body	The inclusion and understanding of Message body is optional (see the table Message-body fields support).	O	O	O	O

The provision and understanding of the following Status Codes shall be supported by FT and PT respectively.

Table 29: <<IWU-TO-IWU>> Body Status codes

Sautés Code	Reason phrase	Normative action/comment
181	Call Is Being Forwarded	The calling party User should be informed. User may release the call setup.
182	Queued	The calling party User shall be informed that the request has been queued rather than rejected. User may wait or release the call.
300	Multiple Choices	The calling party User shall be informed that the address in the request resolved to several choices, each with its own specific location. The locations shall be indicated as provided by the remote server. The calling user shall be capable of choosing location from those provided. The PT shall send the new contact address to the FT in a <To> field.
301	Moved Permanently	The provision of these status codes to the PT and user is optional - FT my process the new contacts provided with the response as specified in the RFC 3261 [18] without informing the user. Alternatively, the FT may provide the response code and the Contact details to the PT in which case the calling user shall be informed for the problem and provided with the possibility of choosing one new address from those indicated. The PT shall send the new contact address to the FT in a <To> field and this shall be used by the FT for a new INVITE.
302	Moved Temporarily	
400	Bad Request	The calling party User shall be informed. The user needs to resent the address
401	Unauthorized	If the FT is not able to retrieve credentials from the stored in the PT/user record it shall send this code to the PT together with the realm(s) causing the problem. The calling party User shall be informed and the realm(s) causing the problem provided. The user needs to send its credentials for each realm (if multiple): user name, password and realm. If the user does not have credential for a realm then user name = "anonymous" and password = "" shall be provided. If these are not accepted by the realm causing the problem the call shall be released and the reason indicated.
407	Proxy Authorization Required	
403	Forbidden	Call shall be released. The calling party User shall be informed for the reason (this may be received in result of a failed authorisation).
404	Not Found	Call shall be released. The calling party User shall be informed for the reason.
408	Request Timeout	The FT-UA has retried few times but still it does not work. The calling party User shall be informed for the reason.
410	Gone	Call shall be released. The calling party User shall be informed for the reason.
480	Temporarily Unavailable	Call shall be released. The calling party User shall be informed for the reason.
484	Address Incomplete	The calling party User shall be informed. User may retry to provide the address or release the call.
485	Ambiguous	
486	Busy Here	The calling party User shall be informed. User may retry another contact.
5xx	Server Failure	Call shall be released. The calling party User shall be informed for the reason.
600	Busy Everywhere	Busy tone.
603	Decline	Call shall be released. The calling party User shall be informed for the reason.
604	Does Not Exist Anywhere	Call shall be released. The calling party User shall be informed for the reason.

The requirements to FT and PT respectively of provision/understanding of the various SIP message header fields are indicated in table 30.

Table 30: <<IWU-TO-IWU>> Body message-Header fields support

Field	Format/Comment	Support			
		PT to FT		FT to PT	
		PT	FT	FT	PT
Accept	Note 5	I	I	I	I
Accept-Language	Default is English - FT needs not to support any other language. It is the PT's responsibility to convert to/from any other chosen by the user language for local presentation.	O	O	O	O
Alert-Info	Neither the FT nor the PT are required to be able to handle additional ringing tones. If they do not support a tone being requested, they shall map it to whatever tone appropriate.	O	O	O	O
Authorization	Not required to be provided, unless explicitly requested, see later the clause about Security.	O	O	-	-
Call-Info		O	O	O	O
Contact		O	O	O	O
Content-Disposition	Note 4	C1	C1	C1	C1
Content-Encoding	Note 4	C1	C1	C1	C1
Content-Language	Note 4	C1	C1	C1	C1
Content-Length	Note 4	C1	C1	C1	C1
Content-Type	Note 4	C1	C1	C1	C1
Error-Info		-	-	O	O
From	Note 3	O	O	O	O
Organization	Optional may be used for call incoming filtering	O	O	O	O
Priority	Mandatory, with default "normal"	O	M	O	M
Proxy-Authorization	Not required to be provided, unless explicitly requested, see later the clause about Security.	O	O	-	-
Reply-To	Note 3	O	O	O	O
Retry-After		-	-	M	M
Subject		O	O	O	O
To	Note 3	M	M	O	O

NOTE 1: Field's format and values, except otherwise stated in the present document, shall be provided according to the requirements specified in RFC 3261 [18]. To reduce the length of the DECT message the compact forms of the header field names shall always be used.
NOTE 2: The minimum requirements for support at the PT side are the provision of just its AOR into the <To> header field. Consequently it is required that the FT shall be capable of obtaining/computing all the rest necessary information for the construction of the REQUEST message.
NOTE 3: Support of "display name" is optional, only the provision of "name-addr" is mandatory, all other parameters are FT matter.
NOTE 4: Related to message body. The inclusion and understanding of Message body is optional (see the table Message-body fields support).
NOTE 5: In the present document due to the fact that only voice media type is covered this Field is set to be out of scope. In future versions it may be included to describe what types of message bodies the terminal could handle.

The requirements to FT and PT respectively of provision/understanding of SIP message bodies and related header fields are indicated in table 31.

Table 31: <<IWU-TO-IWU>> Body Message-body fields support

Field	Format/Comment	Support			
		PT to FT		FT to PT	
		PT	FT	FT	PT
Content-Type	application/sdp	C1	C1	C1	C1
Content-Length	Any	C1	C1	C1	C1
Message Body		C1	C1	C1	C1
NOTE 1: In the present document PT/user enabled support of sending/receiving of SIP Message bodies by the FT is not mandated. It is the responsibility of the FT to construct and use them in regard to the requirements of the SIP and SDP (RFC 2327 [19]) and on the assumption that the lack of information being provided by the PT shall be interpreted as message bodies of type "application/sdp" related to audio sessions was indicated. NOTE 2: (C1) For the present document neither the PT nor the FT are required to be able to decode those fields if they are included into the <<IWU-TO-IWU>> SIP related information.					

The <<IWU-TO-IWU>> information element may be included, with respect to the CC state and procedure performed, in any CC message that is relevant. If the inclusion of the <<IWU-TO-IWU>> into a message will result into the message length being higher than 63 octets, the <<IWU-TO-IWU>> shall be segmented. The second and following segments shall be included into one or more {IWU-INFO} messages. A first segment can be placed in a {IWU-INFO} message as well. The sending side shall not initiate transmission of a new <<IWU-TO-IWU>> information element before all segments of a previous one have been submitted. For the structure of the possible messages the requirements in EN 300 444 [13] or EN 300 175-5 [5] respectively apply with the following additions:

Table 32: Values used within a CC message

Information element	Field within the information element	Standard values within the field/information element	Normative action/comment
<<Segmented Info>>			Note 2
	<Segmented element type>	1110111	<<IWU-TO-IWU>>
<<IWU-TO-IWU>>		All	Note 1
NOTE 1: For the content of the <<IWU-TO-IWU>> information element see above. NOTE 2: Mandatory only if the CC message will exceed 63 octets or if the <<IWU-TO-IWU>> is segmented.			

7.3.4 Service attributes negotiation/modification

A session attributes, especially when a non voice media type is to be used, may be negotiated or modified. DECT protocol provides procedures for service negotiation and change which can be applied or adapted here. As the present document focuses only on voice media the specification of exact requirements and procedure/message mapping is left for future standardisation.

7.3.5 Security

7.3.5.1 Procedure mapping

The security issues in regard to DECT-SIP interworking can be divided into two groups:

- Those related to secure transmission over the DECT air interface of SIP related authorization parameters, e.g. user name, password and realm.
- Those related to security issues in regard to the SIP and related protocols.

To provide a secure transmission of SIP related authorization parameters over the DECT air interface every terminal that claims compliance with the present document shall prior to transmitting those parameters cipher the DECT link. It is the responsibility of the PT to ensure the secure transmission of the user's credentials. Consequently it is mandatory for both, the PT and the FT, to support the PT initiated Ciphering procedure as defined in GAP EN 300 444 [13].

During Registration phase, and during any procedure related to registration, the user shall provide its name, password and realm as specified in clause 7.3.2 earlier. The FT shall store the provided information into the user/PT record and shall use it for authentication/authorisation purposes during session establishment as specified into the RFC 3261 [18] (e.g. during session establishment the user is challenged by the realm for which credential information is stored).

If during a particular SIP procedure, e.g. session establishment, the FT needs to retrieve the user credentials, e.g. a Proxy Authorisation on the path challenge is received from a realm for which FT does not have a record, it shall provide to the PT the realm that requests the relevant authorisation parameters. The PT shall request the user to enter password and username for this realm and provide them back to the FT. The {IWU-INFO} messages shall be used during call establishment and {MM-IWU} during standalone MM procedures, e.g. registration. Prior to sending the response, if the link is in clear mode, the PT shall cipher the link.

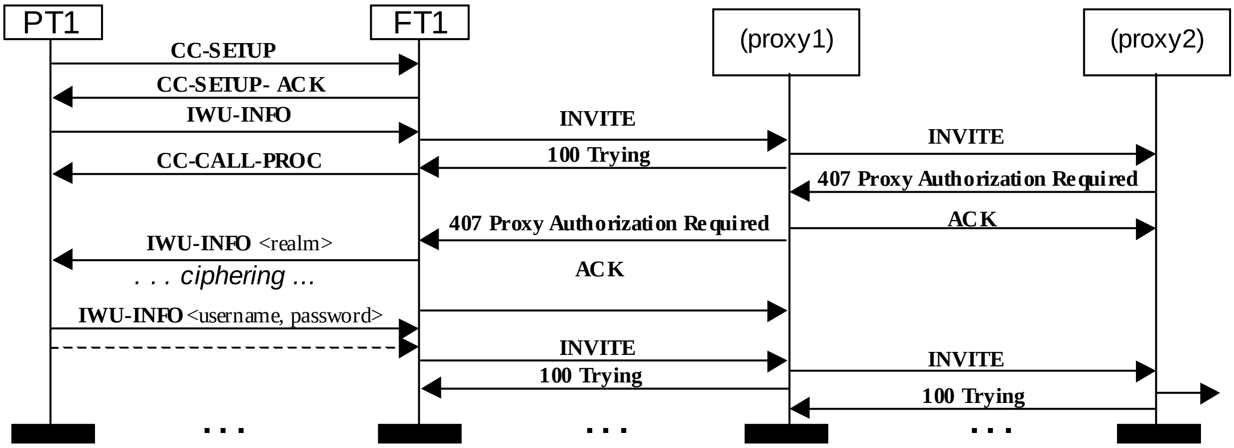

Figure 18: SIP session establishment credential retrieval example

For the message/information elements requirements and mapping see clause 7.3.3.2.

Table 33: <<IWU-TO-IWU>> Examples - Proxy authorisation request FT to PT

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000100	SIP REJECT
Body		407 Proxy Authorization Required Proxy-Authorisation: realm = viena.com	The reason phrase Proxy Authorization Required is optional but may be used to be displayed to the user
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

Table 34: <<IWU-TO-IWU>> Examples - Proxy authorisation response PT to FT

Field	Sub-field	Value	Comment
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	One octet with action values
	Value	0000100	SIP REJECT
Body		Authorization: username = stoyan, realm = viena.com, password = 123	
NOTE: Field values shall be formatted according to the requirements specified in RFC 3261 [18].			

The security at the IP side is left to the FT implementer and hence is out of the scope of the present document.

NOTE: Certain activities at the IP may need to be indicated to the user and in some cases a confirmation from the user may be expected before the FT proceeds further with the IP action. An example of such event is the possibility for redirection of a call from a sips address to a sip address (see RFC 3261 [18]), i.e. from a secure address to an insecure one. For handling of such cases see clause 7.3.2.

7.3.6 Query for capabilities

The SIP method OPTIONS allows a UA to inquire another UA or a proxy server for its capabilities. This procedure can normally be handled by the FT-UA without the PT being engaged because the FT would have already received all information related to the PT's capabilities during Attach.

The present document specifies requirements only in regard to voice media type sessions therefore no UA capabilities other than the FT capabilities need be indicated, nor there is a need for specification of User initiated procedure for query of capabilities. In future versions of the standard when other medias are addressed terminal's session capabilities may be provided during attach (location registration) or an explicit parameter retrieval. These are left for further study.

7.4 Quality of Service (QoS)

Implementations that comply with the present document shall implement code conversion in the DECT Fixed Part. This means that the DECT ADPCM speech service shall be used over the DECT air interface and DECT speech samples shall be transcoded to/from the voice-over-IP data to be sent out to the IP network or received in at the DECT FT from the IP network.

NOTE: The main advantages of this approach are that the IP overhead is removed and a minimum delay can be guaranteed.

From DECT point of view it shall be noticed that the exchange of SIP related information on the DECT air interface may result in long <<IWU-TO-IWU>> information elements and their segmentation. Future versions of the present document may consider SIP information compression mechanisms.

Annex A (normative): IWU-TO-IWU specification

A.1 General

This annex summarises the coding of <IWU-TO-IWU>> information element introduced into the present document and distinguished by the <Protocol Discriminator> indicating "DECT access to IP networks". For the general structure of the <<IWU-TO-IWU>> see EN 300 175-5 [5].

Table A.1: <<IWU-TO-IWU>>

Field	Sub-field	Value	Comment
S/R		1	
Protocol Discriminator		100100	DECT access to IP networks
Action	Ext	1	Multi octet extension
	Value	1000001	IP Mobility: DIMS
		1000110	IP Mobility: Authentication Payload
		1000100	IP Mobility: Authenticator
		1001000	IP Mobility: Registration
		1001001	IP Mobility: Call establishment
		0000010	SIP REGISTER: Adding/Modifying bindings
		0000011	SIP REGISTER: Fetching bindings
		0000100	SIP REJECT
		0001000	SIP SESSION ESTABLISHMENT
Body	All	All	The content of this field depends on the settings of the Action Value and is described in the relevant clauses of the present document.

Annex B (informative): Bibliography

IETF draft-ietf-mobileip-ipv6-24: "Mobility Support in IPv6".

IETF RFC 1144: "Compressing TCP/IP headers for low-speed serial links".

IETF RFC 2822: "Internet Message Format".

IETF RFC 3266: "Support for IPv6 in Session Description Protocol (SDP)".

IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

IETF RFC 2633: "S/MIME Version 3 Message Specification".

IETF RFC 2246: "The TLS Protocol Version 1.0".

IETF RFC 1847: "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted".

IETF RFC 3369: "Cryptographic Message Syntax (CMS)".

IETF RFC 2401: "Security Architecture for the Internet Protocol".

ITU-T Recommendation T.50 (1992): "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

Annex C (normative): Changes to EN 300 175

This annex describes changes that need to be introduced to EN 300 175 that have been called upon due to the requirements specified in the present document. This annex will be removed as soon as these changes are incorporated into the text of EN 300 175, therefore the annex is the last in the present document. All changes are backwards compatible.

C.1 EN 300 175-5 IWU-TO-IWU

As a result of the requirements specified in the present document the EN 300 175-5 [5], clause 7.7.23 "IWU TO IWU" shall be modified as follows (changes are underlined):

Protocol Discriminator (PD):

Bits	**6 5 4 3 2 1**	**Meaning**
	....	
	1 0 0 1 0 0	DECT access to IP Networks specific (see TS 101 XXX)
	....	

All other values reserved.

C.2 EN 300 175-5 MM-INFO-REQUEST

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 59 of clause 6.3.6.22 "MM-INFO-REQUEST" message shall be modified as follows (changes are underlined).

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

Information Element	**Clause**	**F to P message**	**P to F message**	**Length octets**
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Info type	7.7.20	-	M	3-*
Call Identity	7.7.6	-	O	3-4
Portable identity	7.7.30	-	O	7-20
Repeat indicator	7.6.3	-	O	1
Fixed identity	7.7.18	-	O	5-20
Location area	7.7.25	-	O	3-*
NWK assigned identity	7.7.28	-	O	5-20
Network parameter	7.7.29	-	O	3-*
Key	7.7.24	-	O	4-*
Segmented-Info (see note)	7.7.37	-	O	4
IWU-TO-IWU	7.7.23	-	O	4-*
Escape to proprietary	7.7.45	-	O	4-*

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

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

C.3 EN 300 175-5 Segmented Info

Segmentation of IWU-TO-IWU information element when included in any DECT message shall be allowed. This means that at least the messages included in EN 300 175-5 [5], clauses 6.3.2 and 6.3.6 need all to be updated. Some examples are listed in this clause (this is not an exhaustive list).

C.3.1 EN 300 175-5 MM-INFO-ACCEPT

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 57 of clause 6.3.6.20 "MM-INFO-ACCEPT" message shall be modified as follows (changes are underlined).

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

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Info type	7.7.20	O	-	3-*
Call Identity	7.7.6	O	-	3-4
Repeat Indicator	7.6.3	O	-	1
Fixed identity	7.7.18	O	-	5-20
Location area	7.7.25	O	-	3-*
NWK assigned identity	7.7.28	O	-	5-20
Network parameter	7.7.29	O	-	3-*
Duration	7.7.13	O	-	4
Segmented-Info (see note)	7.7.37	O	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
Escape to proprietary	7.7.45	O	-	4-*

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

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

C.3.2 EN 300 175-5 LOCATE-ACCEPT

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 54 of clause 6.3.6.17 "LOCATE-ACCEPT" message shall be modified as follows (changes are underlined).

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

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Portable identity (see note 1)	7.7.30	M	-	2-20
Location area	7.7.25	M	-	3-*
Use TPUI	7.6.2	O	-	1
NWK assigned identity	7.7.28	O	-	5-20
Ext h/o indicator	7.7.51	O	-	3
Setup capability	7.7.40	O	-	4
Duration	7.7.13	O	-	4
Repeat indicator	7.6.3	O	-	1
Segmented-Info (see note 2)	7.7.37	O	-	4
IWU-TO-IWU	7.7.23	O	-	4-*
Model identifier	7.7.46	O	-	5-20
Escape to proprietary	7.7.45	O	-	4-*

M = Mandatory;
O = Optional.				

NOTE 1: This element may contain zero length contents if a new TPUI is not assigned. NOTE 2: The <<SEGMENTED-INFO>> element is used if the complete information cannot be fitted into one message.				

C.3.3 EN 300 175-5 LOCATE-REQUEST

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 57 of clause 6.3.6.19 "LOCATE-REQUEST" message shall be modified as follows (changes are underlined).

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

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Portable identity	7.7.30	-	M	7-20
Fixed identity	7.7.18	-	O	5-20
Location area	7.7.25	-	O	3-*
NWK assigned identity	7.7.28	-	O	5-20
Cipher info	7.7.10	-	O	4-5
Setup capability	7.7.40	-	O	4
Terminal capability	7.7.41	-	O	6-19
Network parameter	7.7.29	-	O	3-*
Repeat indicator	7.6.3	-	O	1
Segmented-Info (see note)	7.7.37	-	O	4
IWU-TO-IWU	7.7.23	-	O	4-*
Model identifier	7.7.46	-	O	5-20
Escape to proprietary	7.7.45	-	O	4-*

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

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

C.3.4 EN 300 175-5 MM-IWU

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 63a of clause 6.3.6.27 "MM-IWU" message shall be modified as follows (changes are underlined).

Message Type	Format	Directions
{MM-IWU}	S	Both

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Repeat indicator	7.6.3	O	O	1
Segmented-Info (see note)	7.7.37	O	O	4
IWU-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	4-*

M = Mandatory;
O = Optional.				

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

C.3.5 EN 300 175-5 IWU-INFO

As a result of the requirements specified in the present document the EN 300 175-5 [5], table 20 of clause 6.3.2.14 "IWU-INFO" message shall be modified as follows (changes are underlined).

Message Type	Format	Directions
{IWU-INFO}	S	Both

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	M	1/2
Transaction Identifier	7.3	M	M	1/2
Message Type	7.4	M	M	1
Portable identity	7.7.30	O	O	7-20
MMS Generic Header	7.7.47	O	O	-*
MMS Object Header	7.7.48	O	O	-*
Repeat Indicator (see note)	7.6.3	O	O	1
MMS Extended Header	7.7.49	O	O	-*
Repeat Indicator (see note)	7.6.3	O	O	1
Time-Date	7.7.50	O	O	6-10
Repeat Indicator (see note)	7.6.3	O	O	1
Calling Party Number	7.7.9	O	O	3-*
Repeat Indicator (see note)	7.6.3	O	O	1
Called Party Number	7.7.7	O	O	4-*
Called Party Subaddr	7.7.8	O	O	4-*
Segmented info	7.7.37	O	O	4
Alphanumeric	7.7.3	O	O	4-*
Repeat Indicator (see note)	7.6.3	O	O	1
Segmented info	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	O	4-*
IWU-PACKET	7.7.22	O	O	4-*
Escape to proprietary	7.7.45	O	O	4-*

M = Mandatory;
O = Optional.				

NOTE: The <<REPEAT-INDICATOR>> information element may optionally be included in front of the <<MMS EXTENDED HEADER>>, <<TIME-DATE>> and <<CALLING PARTY NUMBER>> and <<CALLED PARTY NUMBER>> information elements indicating "non-prioritised list".				

C.3.6 EN 300 175-5 External protocol information procedure

As a result of the requirements specified in the present document the EN 300 175-5 [5], clause 13.9 "External protocol information procedure" shall be modified as follows (changes are underlined).

This is used to exchange information between the FT and the PT.

The procedure can be initiated by the FT or by the PT independently or in relation to another MM procedure, e.g. when additional information may be required. The latter may be the case if segmentation has occurred in the initial MM message for example.

C.4 EN 300 175-5 Extended higher layer capabilities

As a result of the requirements specified in the present document the EN 300 175-5 [5], table F.2 of clause F.2 "Extended higher layer capabilities", table F.2 shall be modified as follows (changes are underlined):

BIT NUMBER	Profile Supported
...	...
a28	IP Roaming unrestricted

C.5 EN 300 175-5 MM-NOTIFY

As a result of the requirements specified in the present document the EN 300 175-5 [5], clause 6.3.6 "MM-messages" shall be modified to add a new message {MM-NOTIFY}.

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

Message Type	Format	Directions
{MM-NOTIFY}	S	F=>P

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Timer Restart	7.6.9	O	-	2
Escape to proprietary	7.7.45	O	-	4-*

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

Other clauses may need modification to include reference for example in clause 7.4.5 "Messages for MM".

Table 73: MM message type coding

	Bits							
MM message types	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
{AUTHENTICATION-REQUEST}	0	1	0	0	0	0	0	0
{AUTHENTICATION-REPLY}	0	1	0	0	0	0	0	1
{KEY-ALLOCATE}	0	1	0	0	0	0	1	0
{AUTHENTICATION-REJECT}	0	1	0	0	0	0	1	1
{ACCESS-RIGHTS-REQUEST}	0	1	0	0	0	1	0	0
{ACCESS-RIGHTS-ACCEPT}	0	1	0	0	0	1	0	1
{ACCESS-RIGHTS-REJECT}	0	1	0	0	0	1	1	1
{ACCESS-RIGHTS-TERMINATE-REQUEST}	0	1	0	0	1	0	0	0
{ACCESS-RIGHTS-TERMINATE-ACCEPT}	0	1	0	0	1	0	0	1
{ACCESS-RIGHTS-TERMINATE-REJECT}	0	1	0	0	1	0	1	1
{CIPHER-REQUEST}	0	1	0	0	1	1	0	0
{CIPHER-SUGGEST}	0	1	0	0	1	1	1	0
{CIPHER-REJECT}	0	1	0	0	1	1	1	1

	Bits							
MM message types	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
{MM-INFO-REQUEST}	0	1	0	1	0	0	0	0
{MM-INFO-ACCEPT}	0	1	0	1	0	0	0	1
{MM-INFO-SUGGEST}	0	1	0	1	0	0	1	0
{MM-INFO-REJECT}	0	1	0	1	0	0	1	1
{LOCATE-REQUEST}	0	1	0	1	0	1	0	0
{LOCATE-ACCEPT}	0	1	0	1	0	1	0	1
{DETACH}	0	1	0	1	0	1	1	0
{LOCATE-REJECT}	0	1	0	1	0	1	1	1
{IDENTITY-REQUEST}	0	1	0	1	1	0	0	0
{IDENTITY-REPLY}	0	1	0	1	1	0	0	1
{MM-IWU}	0	1	0	1	1	0	1	1
{TEMPORARY-IDENTITY-ASSIGN}	0	1	0	1	1	1	0	0
{TEMPORARY-IDENTITY-ASSIGN-ACK}	0	1	0	1	1	1	0	1
{TEMPORARY-IDENTITY-ASSIGN-REJ}	0	1	0	1	1	1	1	1
{MM-NOTIFY}	0	1	1	0	1	1	1	0

C.6 EN 300 175-5 Info type

As a result of the requirements specified in the present document the EN 300 175-5 [5], clause 7.7.20 "Info Type" shall be modified as follows (changes are underlined).

Parameter type coding (octet 3):

Bits	**7 6 5 4 3 2 1**	**Meaning**
	.....	
	0 1 1 0 1 0 0	Identity allocation
	All other values reserved.	

C.7 EN 300 175-5 Management of MM procedures

As a result of the requirements specified in the present document the following text shall be added to the EN 300 175-5 [5], clause 15.5 "Management of MM procedures" (additions underlined).

In order to avoid possible deadlocks between different Mobility Management (MM) procedures the following rules apply:

- two MM procedures are allowed at any one time, but they shall not both have been initiated by the same side;
- if a MM procedure has not yet been finished, then a second MM procedure may only be initiated if the second MM procedure has a higher priority than the first MM procedure;
- the only exception to these two rules is the External protocol information procedure which can be initiated by any side at any time.

History

Document history		
V1.1.1	October 2003	Publication