ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 011

October 1993

Source: ETSI TC-BT

Reference: DTR/BT-01005

ICS: 33.080

Key words: BT, PTN, mobility

Business Telecommunications (BT); Private Telecommunication Network (PTN) internal mobility Private user mobility and cordless terminal mobility General principles and service aspects

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

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

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

Contents

Foreword

This Technical Committee Reference Technical Report (TCR-TR) was prepared by the Business Telecommunications (BT) Technical Committee of the European Telecommunications Standards Institute (ETSI).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI TC or STC studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilised by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

Blank page

1 Scope

The aim of standardisation work based on this TCR-TR is to support Cordless Terminal Mobility (CTM) and Private User Mobility (PUM) in a multivendor environment.

This TCR-TR identifies and describes the functions required to support mobility within a single Private Telecommunication Network (PTN). Incoming and outgoing calls both internal and external to the PTN are covered. The aim is to cover both "private user mobility" and "cordless terminal mobility".

Cordless terminal mobility is closely related to a technology in which the radio interface capabilities determine the mobility functions (coverage area, handover, etc.). Private user mobility is a functionality offered to PTN users to or from any terminal. Private user mobility and cordless terminal mobility are dealt with separately in this TCR-TR.

This TCR-TR does not cover the case of a mobile Private Telecommunication Network Exchange (PTNX).

The first part of the TCR-TR deals with private user mobility and covers:

- registration procedures for incoming and/or outgoing calls;
- procedures for incoming and outgoing calls;
- access security procedures (identification and authentication);
- requirements for signalling protocols enhancements;
- new services.

Interworking with the Universal Personal Telecommunications (UPT) service is outside the scope of this TCR-TR. However, some of the procedures for providing private user mobility within a PTN could be similar to UPT procedures.

The second part of the TCR-TR deals with cordless terminal mobility and covers:

- procedures to support mobility (roaming, handover etc.) according to the mobility functions of each radio technology;
- procedures for incoming and outgoing calls;
- access security procedures (identification, authentication, encryption);
- requirements for signalling enhancements;
- new services.

However, features which are relevant only to the radio interface are outside the scope of this TCR-TR.

It is intended that this TCR-TR be used as a basis for the identification of ETSs and ETRs which may be required for the specification of mobility within a PTN, and which may apply to both private user mobility and cordless terminal mobility.

2 References

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

[1] NA-TR 004 (1992): "Universal Personal Telecommunications (UPT); Phase 1, Service aspects: Guidelines".

[2] ETR 055-1 (1992): "Universal Personal Telecommunications (UPT); The service concept, Part 1: Principles and objectives".

[3] ETR 055-2 (1992): "Universal Personal Telecommunications (UPT); The service concept, Part 2: General service description".

[4] ETS 300 175-6 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT), Common interface; Part 6: Identities and addressing".

[5] I-ETS 300 131 (1992): "Radio Equipment and Systems (RES); Common air interface specification to be used for the interworking between cordless telephone apparatus in the frequency band 864,1 MHz to 868,1 MHz, including public access".

[6] ETS 300 189 (1992): "Private Telecommunications Network (PTN), Addressing".

[7] ETS 300 175-5 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT), Common Interface; Part 5: Network layer".

[8] ETR 043 (1992): "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT), Service and facilities requirements specification".

[9] Proposal for a Council Directive: "The protection of personal data and privacy in the context of public digital telecommunications networks, in particular Integrated Services Digital Networks (ISDN) and private digital mobile networks (SYN 288)".

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

[11] ISO 2022 (1986): "Information processing - ISO 7-bit and 8-bit coded character set - coded extension techniques".

[12] ETS 300 192 (1992): "Private Telecommunication Network (PTN); Signalling protocol at the S reference point; Circuit mode basic services".

[13] ETS 300 172 (1992): "Private Telecommunication Network (PTN); Inter-exchange signalling protocol; Circuit mode basic services".

[14] ENV 41007-1: "Definition of terms in private telecommunications networks, Part 1: Definition of general terms".

[15] ETR 079 (1993): "Private Telecommunication Network (PTN); Supplementary services and additional network features".

[16] ECMA TR/57 (1991): "Private Telecommunication Networks".

[17] ETSI-GSM Technical Report 01.04 (version 3.0.1): "Vocabulary in a GSM PLMN".

[18] CCITT Recommendation E.163 (1988): "Numbering plan for the international telephone service".

[19] CCITT Recommendation E.164 (1988): "Numbering plan for the ISDN era".

[20] ETS 300 062 (1991): "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service, service description".

[21] ETS 300 063 (1991): "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service, functional capabilities and information flows".

[22] ETS 300 050 (1991): "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service, service description".

[23] ETS 300 051 (1991): "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service, functional capabilities and information flows".

[24] CCITT Recommendation I.112 (1988): "Vocabulary of terms for ISDNs".

[25] CCITT Recommendation X.219 (1988): "Remote operations: Model, notation and service definition".

[26] ETS 300 239 (1993): "Private Telecommunication Network (PTN); Inter-exchange signalling protocol; Generic functional protocol for the support of supplementary services".

[27] ETS 300 171 (1992): "Private Telecommunication Network (PTN); Specification, functional models and information flows; Control aspects of circuit mode basic services".

3 Terminology

3.1 Definitions

For the purposes of this TCR-TR, the following definitions apply. The sources of the definitions are given in square brackets.

Address [6]: formalised information used to indicate unambiguously an identifiable entity. Within the context of this TCR-TR, identifiable entities are those which use telecommunication services.

Additional Network Feature (ANF) [15]: a capability, over and above that of a basic service, provided by a PTN, but not directly to a PTN user.

Attendant [15]: a PTN user whose prime task is to provide assistance and support to the users.

Authentication:

a) To verify the identity of a user, terminal or both of these entities, often as a prerequisite to allowing access to resources in the PTN;
b) To verify the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorised modification.

Cell: the coverage area of one RBS.

Cordless Terminal: a physical entity that provides access to the telecommunications services of a PTN via a radio interface.

NOTE: A user in DECT terminology is equivalent to a cordless terminal in this TCR-TR.

Cordless Terminal Mobility (CTM): Cordless Terminal Mobility involves the ability of a cordless terminal to be in continuous motion whilst accessing and using the telecommunication services offered by the PTN, as well as the capability of the network to keep track of the location of the cordless terminal throughout the entire network.

Coverage area: the area over which reliable communication can be established and maintained.

Dialling Plan [6]: a plan according to which a user can identify addressable entities by means of numbers and, if applicable, of prefixes indicating the (sub)-domain to which the addressable entity belongs.

Domain [6]: the range of responsibility of an authority for setting up numbering and/or addressing plans. The boundaries of a domain need not coincide with the physical boundaries of a given network.

Dynamic Registration: the procedure performed by a PUM user which informs the PTN of which PTN number should be utilised for locating the user.

Explicit Numbering Plan: a numbering plan in which each number is accompanied by an indication to which (sub)-domain it applies.

Fixed Part: a physical grouping of some or all of the fixed component parts of a mobile radio system. These would include one or more pieces of radio equipment attached to an antenna system. It could also include common control functions and interfaces to the PTNX.

Fixed Radio Part (FRP): a functional group containing all of the radio systems functions on the PTN side of an air interface.

Function: a set of processes defined for the purpose of achieving a specified objective.

Handover: the process of switching a call in progress from one physical channel to another physical channel. These processes can be internal or external with respect to a FRP.

NOTE: Only the external handover, i.e. the handover between two different FRPs, is relevant for this TCR-TR.

Home Data Base (HDB): the data base in which the current location and all associated parameters of a cordless terminal or a user are stored.

Identification Address/Number [6]: an address or a number which is used for the identification of an entity.

NOTE: This term also applies to addresses in general, i.e. also to subaddresses.

Implicit Numbering Plan [6]: a numbering plan in which each number is not accompanied by an indication to which (sub)-domain it applies. Instead the identification has to be determined from the number digits themselves.

Integrated Services Digital Network (ISDN) [24]: an integrated services network that provides digital connections between user-network interfaces.

ISDN Numbering Plan (ISDN NP) [6]: the numbering plan explicitly relating to the global ISDN domain, as defined in CCITT Recommendation E.164 [19].

Integrated Services Centrex (ISCTX) [14]: an implementation of a private telecommunication network exchange that is not located on the premises of a private network operator. It may be co-located with or physically part of a public ISDN local exchange.

Integrated Services Private Branch Exchange (ISPBX) [14]: an implementation of a private telecommunication network exchange located on the premises of a private network operator.

Location Area (LA): the coverage area in which a cordless terminal may receive and initiate calls as a result of a single location registration.

Location Registration: the process whereby the position of a cordless terminal is determined at the level of one location area, and the process of updating the position of this cordless terminal in one or more databases.

Multiple Subscriber Number (MSN) [6]: a full or a partial number assigned to a user-to-network access for which an arrangement has been established in the context of the MSN supplementary service ("MSN arrangement").

Native Numbering Plan [6]: a numbering plan employed by a given domain in a way that it unambiguously identifies the addressable entities of that domain.

Number [6]: an address restricted to containing numerical values, as defined by a numbering plan.

Numbering Plan Identifier (NPI) [6]: an indication of the numbering plan to which a number belongs; it is separate from the number itself.

Partial Number [6]: the subset of a number which is at least significant at a particular access of the network concerned for distinguishing addressable entities beyond that access.

Private [14]: an attribute indicating that the application of the so qualified item, e.g. a network, a unit of equipment, a service, is offered to or is in the interest of a determined set of users.

NOTE: The term does not include legal or regulatory aspects, nor does it indicate any aspects of ownership.

Private Numbering Plan (PNP) [6]: the numbering plan explicitly relating to a particular private numbering domain, defined by the Authority of that domain.

PNP Number [6]: a number belonging to a PNP.

Private Telecommunication Network (PTN) [16]: a network comprising one or more interconnected PTNXs. The PTN provides PTN services to its users which are based on those provided by its PTNXs. The PTN may comprise more than one PTNX spread over more than one user premises. In this case,

inter-PTNX connections between the PTNXs serving the individual premises are required. The inter-PTNX connections are considered part of the PTN.

In the context of this TCR-TR a PTN is considered a private ISDN.

Private Telecommunication Network Exchange (PTNX) [16]: a nodal entity in a PTN which provides autonomous and automatic switching and call handling functions used for the provision of telecommunications services which are based on those specified for public ISDNs.

NOTE: If applicable, a PTNX provides:

- telecommunication services within its own area; and/or
- telecommunication services from the public ISDN; and/or
- telecommunication services from other public or private networks; and/or
- within the context of a PTN, telecommunication services from other PTNXs;

to users of the same and/or other PTNX.

A PTNX may be represented by an ISPBX, or by equipment which is physically part of the equipment of, for example, a public ISDN local exchange.

Private Telecommunications Network Numbering Plans (PTN NP) [6]: the generic designation for the numbering plan(s) chosen as native by a PTN authority for its particular PTN.

Private User Mobility (PUM): Private User Mobility (PUM) is conferred through the provision of flexible user access to the PTN telecommunication services available at any terminal. PUM enables the user to participate in a user-defined set of services and to initiate and receive calls on the basis of a unique, personal PUM number throughout his PTN at any terminal, fixed, movable or mobile, irrespective of geographic location. PUM is limited only by terminal and network capabilities and the restrictions imposed by the PTN. PUM also allows the user to move between terminals during a call.

PTN Number [6]: a number of the domain covered by a PTN Numbering Plan.

PTN User [16]: a user of the network layer service provided by a PTN.

Public [14]: an attribute indicating that the application of the so qualified item, e.g. a network, a unit of equipment, a service, is offered to the general public.

NOTE: The term does not include legal or regulatory aspects, nor does it indicate any aspects of ownership.

PUM Number: a number which uniquely identifies a PUM user. This is the number used by the caller to reach the PUM user.

Radio Base Station (RBS): a physical grouping that contains all of the radio equipment on the PTN side of the air interface directly connected to a single antennae system.

Radio Exchange (RE): a physical grouping between the RBSs and the PTNX.

Region [6]: the entire domain or a defined sub-domain of a PNP.

NOTE: A region does not necessarily correspond to a geographical area of a PTN.

Registration: a term that should be used with a qualifier, e.g. location registration or dynamic registration.

Roaming: the movement between calls of a cordless terminal from one Fixed Radio Part (FRP) coverage area to another FRP coverage area, where the capabilities of the PTN enable the cordless terminal to access PTN services.

NOTE 1: Roaming requires the FRP and the cordless terminals to be interoperable.

NOTE 2: See also the definition of handover.

Selection Address/Number [6]: an address or a number used to select an addressable entity with which a call is to be established.

NOTE: This term also applies to addresses in general, i.e. also to subaddresses.

Sub-domain [6]: a part of a domain where the responsibility for administering numbering and/or addressing plans is delegated to a subordinate authority.

PTN Network Supervisor (SUP): the entity which is allowed to execute a PTN management task.

Telecommunication Network [14]: all the means of providing telecommunication services between a number of locations where the services are accessed via equipment attached to the network.

Terminal equipment; terminal [6]: an item of equipment attached to a telecommunication network to provide access for a user to one or more services.

Terminal Swapping (TSW): the capability for a PUM user to switch a call from one terminal to another terminal during an active call.

Type of Number (TON): an indication which distinguishes the various complete and shortened forms of number; it is separate from the number itself.

Universal Personal Telecommunication (UPT) [3]: Universal Personal Telecommunication (UPT) is a telecommunication service which enables access to telecommunication services by allowing personal mobility. It enables each UPT Users to participate in a user defined set of subscribed services, and to initiate and receive calls on the basis of a unique, personal, network independent UPT Number across multiple networks at any terminal, fixed or mobile, irrespective of geographical location, limited only by terminal and network capabilities and restrictions imposed by the network provider. Calls to UPT Users may also be made by non-UPT users.

NOTE: Mobile terminal meaning a terminal using any type of radio access.

Unknown Numbering Plan (Unknown NP) [6]: the numbering plan reflecting a dialling plan which is implicitly based on a particular private numbering domain as defined by the authority.

Visitor Data Base (VDB): the database in which all relevant parameters concerning a cordless terminal and a PUM user are stored for as long as they are located in an area controlled by this database.

ZAP [8]: the ability to re-program the account data held in the portable part so that access rights are suspended subject to the other conditions being met, coupled with the ability to re-program the account data again to reinstate access rights once these conditions have been met. There are two categories, ZAP Suspend and ZAP Terminate.

3.2 Symbols and abbreviations

ANF	Additional Network Feature
ARC	Access Rights Class
ARD	Access Rights Details
ARI	Access Rights Identity
CC	Call Control entity
CCA	Call Control Agent
CNT	Cordless Network Terminator
CSTA	Computer Supported Telephony Application
CT	Cordless Terminal
CTI	Cordless Terminal Identity
CTM	Cordless Terminal Mobility
CT2	Cordless Telephone generation 2
DAP	Directory Access Protocol
DCT	Dedicated Cordless Terminal
DECT	Digital European Cordless Telecommunications
DIT	Directory Information Tree
DN	Dialling Number

DSA	Directory System Agent
DSP	Directory System Protocol
DTMF	Dual Tone Multiple Frequencies
DUA	Directory User Agent
EIC	Equipment Installer's Code
EMC	Equipment Manufacturer Code
FPN	Fixed Part Number
FPS	Fixed Part Subnumber
FRP	Fixed Radio Part
GSM	Global System for Mobile communications
HDB	Home Data Base
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
ISCTX	Integrated Services Centrex
ISDN	Integrated Services Digital Network
ISDN NP	ISDN Numbering Plan
ISPBX	Integrated Services Private automatic Branch Exchange
LA	Location Area
LAI	Location Area Identity
LAN	Local Area Network
MAP	Mobile Application Part
MSN	Multiple Subscriber Number
NPI	Numbering Plan Identifier
PARK	Portable Access Rights Key
PID	Portable Identification Code
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PNP	Private Numbering Plan
PSN	Portable Equipment Serial Number
PTN	Private Telecommunications Network
PTN NP	Private Telecommunications Network Numbering Plans
PTNX	Private Telecommunications Network Exchange
PUM	Private User Mobility
PUMN	Private User Mobility Number
PUN	Portable User Number
PUT	Portable User Type
RBS	Radio Base Station
RC	Region Code
RE	Radio Exchange
RFPI	Radio Fixed Part Identity
RMN	Roaming Number
RN	Regional Number
RPN	Radio Fixed Part Number
SS	Supplementary Services
SUP	PTN Network Supervisor
TE	ISDN Terminal Equipment
TM	Terminal Mobility
TON	Type of Number
TP	Terminal Portability
TPUI	Temporary Portable User Identity
TSW	Terminal Swapping
UPT	Universal Personal Telecommunications
VA	Visitor Area
VAI	Visitor Area Identity
VDB	Visitor Data Base
WTM	Wired Terminal Mobility

4 General framework

This Clause provides some background and gives an overview of the concepts covered in this TCR-TR by describing the basic structure of a PTN and explaining the key areas related to mobile users and terminals.

4.1 Private Telecommunications Network environment

As seen in this TCR-TR, the telecommunications environment of a PTN consists of PTNXs (ISPBXs and ISCTXs), radio exchanges (RE), radio base stations (RBS), wired terminals, cordless terminals and users of these terminals. See figure 1 for an illustration.

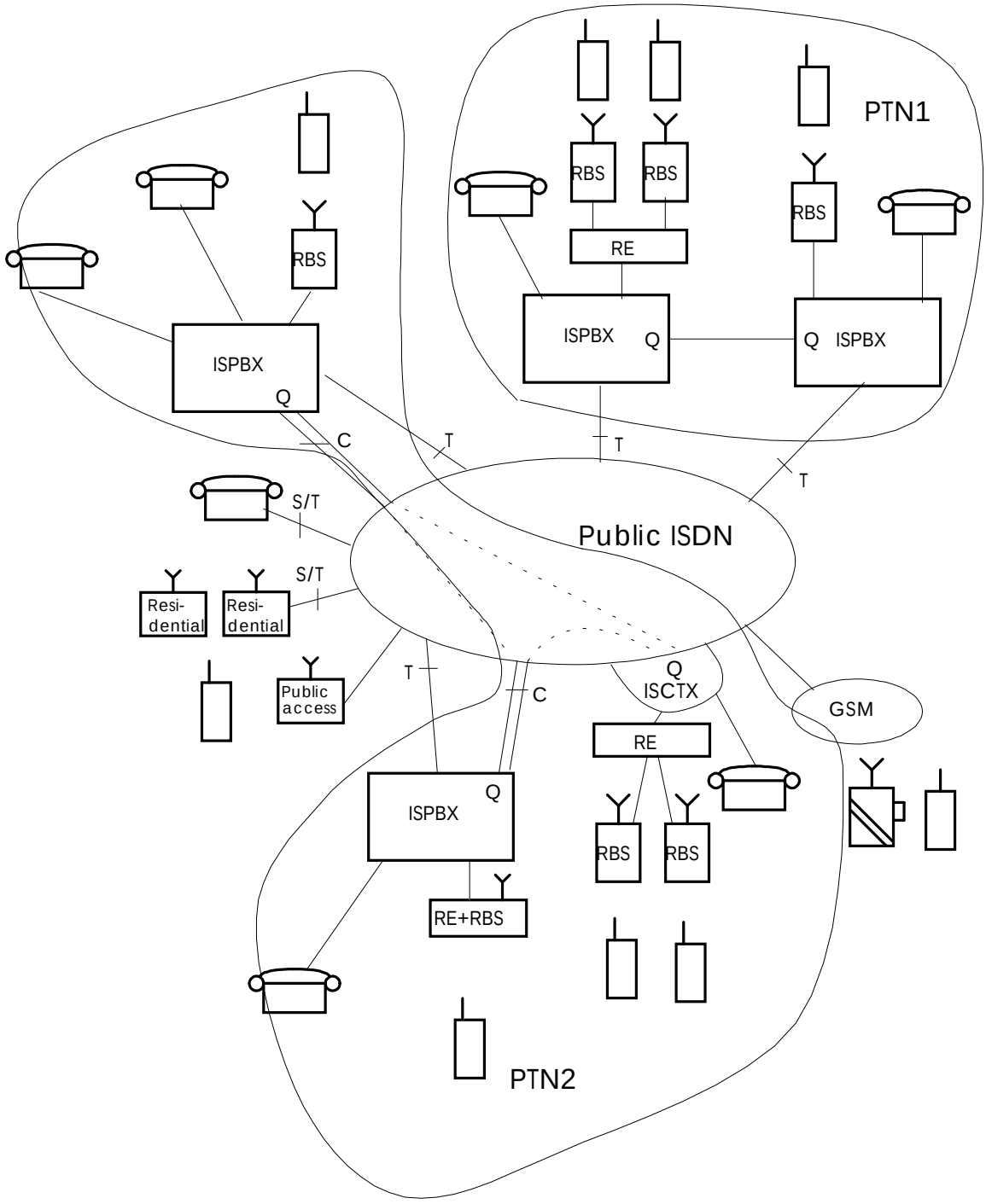


Figure 1: Example of a PTN environment

4.2 PTN mobility concept

As the PTNX itself is not mobile, mobility with respect to the access side of the PTNX can apply to the terminal, to the user of the terminal, or to both. This means that the relationship can be dynamic either between the access point and the terminal, or between the terminal and the user. See figure 2 for an illustration.

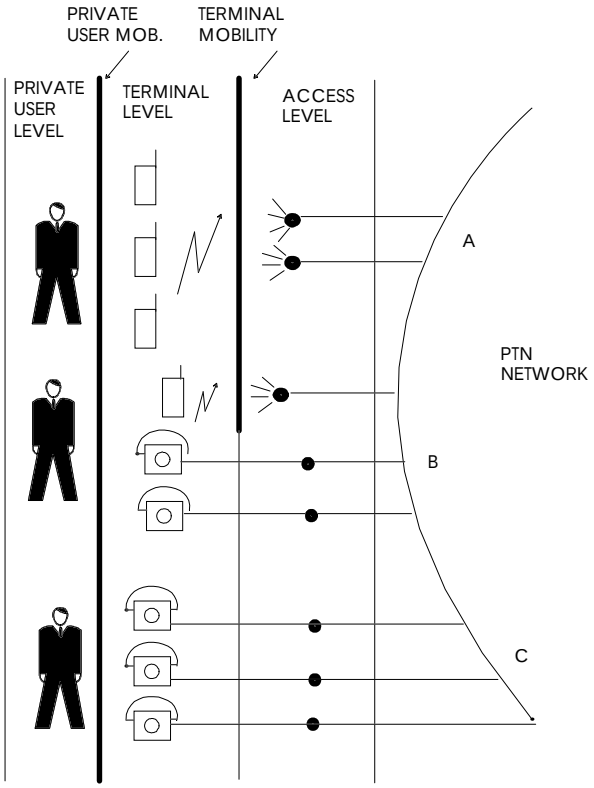


Figure 2: PTN mobility

As shown in figure 2, CTM is applicable only to cordless terminals (as considered in this TCR-TR). PUM is applicable both to wired and cordless terminals, as well as to a mixed environment utilising both terminal types.

Three different levels are identified in order to describe a PTN mobility model for this study:

- access level;
- terminal level;
- user level.

The use of a 3 level approach makes it possible to study terminal mobility independently from Private User Mobility (PUM), as well to study Cordless Terminal Mobility (CTM) separately from Wired Terminal Mobility (WTM).

Two mobility concepts are identified and generally described in this subclause. The two concepts are at this stage considered to be independent. This means that one of the concepts may be standardised/implemented without the other. The concepts are called "Private User Mobility" and "Cordless Terminal Mobility" and are briefly described below.

Mobility for users and terminals is limited to within a single PTN. Referring to figure 1, the mobility of a user/terminal is either within PTN1 or PTN2. Mobility between PTNs is outside the scope of this TCR-TR.

4.2.1 Private User Mobility (PUM)

With PUM, the static relationship between the user and the terminal providing his telecommunications services is abandoned.

In PUM it is possible for the user to change terminal, wired or cordless, while retaining his telecommunications services. This change of terminal may take place between calls or during an established call.

The intent of PUM is to associate services with users and not terminals. However, the services provided may be limited by the capabilities of the particular terminal at which the user registers.

The update of the users location shall be performed or initiated by the user. This can be done by the user manually (e.g. a key sequence), but, if the terminal permits, it can also be accomplished through more advanced and automatic means (e.g. use of smart cards).

4.2.2 Terminal Mobility (TM)

With terminal mobility (TM), the static relation between terminal and physical network access no longer exists. TM refers to the ability of the terminal to change its relationship to access point. This change of access point can occur between calls or during an established call. This ability may be limited, however, by the capabilities of the terminal and the access point. The capabilities of the terminal and access point shall match each other. Services are related to the terminal itself and are limited only by the characteristics of the terminal and access point.

4.2.2.1 Cordless Terminal Mobility (CTM)

With CTM, there is no fixed relation between the cordless terminal and the PTN access. The terminal can change access points as it is moving. This can occur between calls or during an established call.

Wherever possible, services should be provided to a cordless terminal in the same way as to a wired terminal. All existing services may need modification and new services may be required. From the users point of view, the same level of service quality is desired from cordless terminals as from wired terminals.

Location information concerning the cordless terminal may be available in the network and used for call handling (e.g. routeing, charging, etc.). This location information may be updated automatically by the cordless terminal or manually by the user of the cordless terminal.

4.2.2.2 Wired Terminal Mobility (WTM)

Wired Terminal Mobility (WTM) is the ability to move a wired terminal between different access points between calls and during an established call. This requires built-in terminal identities. A limited form of Wired Terminal Mobility is provided by the ISDN supplementary service Terminal Portability (TP). In this case the mobility is limited within one basic access.

WTM is out of scope for this TCR-TR.

4.3 Database architecture

An architecture with Home Data Base/Visitor Data Base (HDB/VDB) and procedures derived from Global System for Mobile communications/Mobile Application Part (GSM/MAP) are used for mobility management in this TCR-TR. This architecture is considered mature for telecommunication applications and available in the time frame of the present standardisation work. Furthermore the introduction of mobility based upon this approach is considered to minimise the impact on the current standards applicable to PTNs.

One consequence of the choice of the HDB/VDB concept is that the practical application of mobility with multiple HDBs in a PTN which allows a user to permanently change his location without changing his number (free numbering), is left for further study.

It is recognised that other approaches may be applicable, e.g. X.500, IN and CSTA. The applicability of these approaches for mobility supported in PTNs are for further study. Annex B gives a short description of the X.500 approach.

4.4 Relation between PUM and CTM

4.4.1 Mobility seen as a dynamic linking of identities

Private user mobility gives the user freedom to use any terminal in the PTN. Cordless terminal mobility allows a CT to be used at any compatible PTN radio access.

Each form of mobility requires a dynamic linking of two identities. PUM requires a dynamic linking between the PUM number and the terminal (access address in the case of a wired terminal). CTM requires a dynamic linking between the CT address and a PTN access address.

To the extent that each of these dynamic linkings are similar - in each of them one identity represents the mobile entity and the other identity represents its "location" - it should be possible to use the same addressing and routeing principles for both PUM and CTM.

It should then be possible to use the same HDB and VDB concept for both PUM and CTM, though different data structures may be required for the two forms of mobility.

There is no intention to standardise an interface between the PTNX and the databases (HDB/VDB).

4.4.2 Similarities of procedures

The following procedures:

- registration;
- identification;
- authentication,

should be defined as generically as possible for both PUM and CTM. This would minimise the differences between the procedures for PUM and CTM while allowing the specific characteristics of each to be taken into account.

a) CTM
Terminals can perform actions automatically.

b) PUM
The private user mobility concept involves actions performed by the users using either various procedures or key-pad messages. These procedures differ from the terminal procedures in that they have to be adapted to human actions.

4.4.3 Example of procedure

Specific procedures, based on the same generic procedure, may differ for terminals and private users, e.g. authentication:

- successful identification;
- mobile entity (terminal and user) requests an authentication word;
- initiate proper authentication algorithm;
- process request;
- pick up response procedure;
- pack response data;
- initiate response;
- respond.

This simple example shows that it is possible to define a generic procedure while still retaining these specific differences for PUM and CTM. The individual steps in the procedure described above may differ for PUM and CTM.

4.4.4 Location Area

The definition of Location Area (LA) shall only be used in relation with CTM and shall not be used in the PUM case.

4.4.5 The use of PUM and CTM together

CTM is independent of PUM in the sense that CTM and PUM together shall allow mobility of the terminal while maintaining the PUM user's registration on the terminal. This can be accomplished by means of a suitably independent structure for the databases. This does not hinder the implementation of the two logical databases as one physical database.

4.5 Mobility between calls and during an established call

Two fundamental situations should be covered when discussing mobility; the ability to change access/terminal between calls, and the ability to change access/terminal during an established call. As shown in figure 3, this applies to cordless terminal mobility as well to private user mobility.

		Wired terminals	**Cordless terminals**
User Mobility	During call	1. Terminal Swapping	1. Terminal Swapping
User Mobility	Outside call	2. User Moving	2. User Moving
Terminal Mobility	During call	3. Out of scope	5. Handover
Terminal Mobility	Outside call	4. Out of scope	6. Roaming

Figure 3: Mobility matrix

Hybrid terminals, i.e. terminals that can change from using radio to wired transmission, are identified, but not considered as being technically possible at this time.

4.5.1 Examples

This subclause explains the terminology used in figure 3 and gives examples for the purpose of clarification.

A general observation is that "user moving" can comprise two sets of procedures, i.e. registration for outgoing calls and registration for incoming calls.

Case 1: "Terminal Swapping (TSW)" - terminal independent

This means that the user can switch during an established call:

a) from one wired terminal to another wired terminal;
b) from one cordless terminal to another cordless terminal;
c) from wired terminal to cordless terminal or vice versa.

EXAMPLE: A user is engaged in a telephone conversation, and, at a certain point in time, wants to go to the adjacent room and to be able to continue the conversation from the terminal in that room. Therefore he/she performs an appropriate procedure and switches to another terminal.

Case 2: "User moving" - terminal independent

This means that the user can make/receive calls from different wired or cordless terminals at different points in time.

EXAMPLE: A user is in an office other than his own, and wants to use a terminal in that office to make calls which should be charged on his account, and/or receive all calls directed to him. To do this, he performs the appropriate procedure(s) and the network will charge outgoing calls to him and/or redirect calls to his own office to his new terminal, irrespective of whether it is wired or cordless.

Case 3: Wired terminal mobility during an active call

There may be a case where a limited form of mobility is provided via the terminal portability supplementary service (in ISDN).

This case is outside the scope of this TCR-TR.

Case 4: Wired terminal mobility outside an active call

There is a case where a limited form of mobility is given via the terminal portability supplementary service (in ISDN).

This case is outside the scope of the TCR-TR.

Case 5: Cordless Terminal Mobility - handover

Handover is the process of switching a call in progress from one physical channel to another physical channel. These processes can be internal or external with respect to the Fixed Radio Part (FRP).

EXAMPLE: A person is engaged in a conversation and moves from the coverage area of one FRP to another FRP. Therefore at a particular moment the call path is switched from one FRP to the other.

Case 6: Cordless Terminal Mobility - roaming

Roaming is the movement of a cordless terminal between calls from one FRP coverage area to another FRP coverage area, where the capabilities of the PTN enable the cordless terminal to access PTN services.

EXAMPLE: A person with a CT moves from the coverage area of one FRP to the coverage area of another FRP. With CTM roaming the person can still make and receive calls with the CT.

4.6 Services to be supported

The services that users find convenient to use shall be supported when mobility is introduced, with the same quality of service where ever possible. Various supplementary services that are available in PTNs shall be modified if necessary to be available to mobile users.

4.6.1 Bearer services and Teleservices

Circuit Mode 64 kbit/s bearer services:

- 64 kbit/s unrestricted;
- 3,1 KHz audio;
- speech,

supporting data and telephony services shall be offered.

Telephony:

The basic service handled by PTNs supporting mobility is two-way telephony. Users should be able to receive and initiate calls whilst mobile within a PTN.

4.6.2 Supplementary Services

All supplementary services defined for PTNs should be considered and made applicable if this can be done without undue difficulty. In addition there might be a need to standardise supplementary services which are specific to mobility.

4.6.3 Additional Network Features

The following additional network features (ANFs) for support of mobility have been identified:

- CTM roaming;
- PUM dynamic registration;
- handover.

5 Private user mobility

5.1 Introduction

This Clause aims to describe service requirements for Private User Mobility (PUM). From a PTN user's point of view, Private user mobility may be considered as a service which should be described in ETSs in 3 stages according to CCITT methodology.

5.1.1 Basic concept of private user mobility

Private user mobility is conferred by the flexibility of the user's access to PTN telecommunication service provision which is available at any PTN terminal. It enables each PUM user to participate in a user-defined set of services and to initiate and receive calls on the basis of a unique, personal PUM number throughout the PTN at any terminal, wired or cordless, irrespective of geographic location, limited only by terminal and network capabilities and restrictions imposed by the PTN. PUM also allows users to move between terminals during a call.

5.1.2 General description

Private user mobility will provide PTN users with personal mobility services irrespective of the terminal used within the PTN.

For a long time some facilities of personal mobility have been available to private users with solutions based on the services like Call Diversion, Follow Me, Substitution, Paging, Call Pick up, Call Park and so on. Each of these provide distinct services related to the availability and the temporary movement of the PTN user. However, PUM provides a homogeneous concept that supports mobile users with their telecommunications services.

In fixed networks, users are associated with the point of attachment of the terminal to the network (i.e. line identification). In mobile networks, users are associated with the terminal (i.e. terminal identification). In order to provide a complete mobility within a PTN, the static relationship between terminal or line identity and user identity should be abandoned and replaced with a dynamic association.

Private user mobility applies to a user whatever terminal (wired or cordless) he uses and it is not likely that cordless terminal mobility has influence on this description of private user mobility.

Private user mobility extends mobility throughout the PTN irrespective of possible cordless system implementations and of their different radio features or coverage areas, and offers PTN users a larger degree of mobility. PUM service can be offered with or without cordless terminal mobility.

There is neither limitation in PUM applicability (speech, data, video, etc.) nor restriction in PUM evolution. Some technological and market developments in the future may influence implementation phases and service enrichment. At first, a minimum set of features should meet basic ideas of private user mobility.

The relation between PUM and UPT is described in subclause 5.3.1.

5.2 Feature description

PUM provides user mobility within a PTN, offering a range of features to be defined as follows.

5.2.1 Core features

5.2.1.1 Identification

PUM number:

The objective is to get a decoupling between user identity and identity/address/nature of the PTN port/terminal.

A PUM number uniquely identifies each PUM user and is used by the caller to reach that user. A PUM user may have more than one PUM number according to his business activities.

Each PUM number has a global meaning within the PTN according to rules of the Private Numbering Plan.

PUM numbers applicability does not extend beyond the PTN.

5.2.1.2 Registration

Dynamic registration for incoming calls:

The PUM user can specify a terminal access to which some or all incoming calls to the PUM user will be presented.

A different terminal access may be specified for each service type (e.g. voice, telefax).

The PUM user will be able to determine the desired "service profile" attached to this new registration, i.e.: depending on calling party's identity, call importance indication, for "no answer" and "busy" conditions, and other possible criteria.

Several PUM users may register for incoming calls at the same terminal access simultaneously.

In addition to new facilities brought by PUM service, the supplementary services, usually offered to any PTN user, should be made available to PUM users.

Registration for outgoing calls:

The ability for a PUM user to initiate one or more outgoing calls and to make use of the basic and supplementary services to which he has access.

This feature can be used to reserve a terminal for a single call or for a session of specified duration or of indefinite duration for one or more service types (e.g. voice or telefax), from one or more terminals. During a session, the user may initiate any number of outgoing calls without having to perform authentication.

At a given time, only one PUM user may be registered for an outgoing call session at a given terminal, i.e. different sessions can not overlap each other with the exception of registration for a single call.

Registration for incoming and outgoing calls or AllCall feature:

The ability for a PUM user to reserve a terminal for a session of outgoing calls and to register the same terminal for receiving incoming calls, using one procedure, and to make use of basic and supplementary services to which he has access. This combination is called an AllCall session.

The AllCall feature can be used to initiate one or more AllCall sessions of specified duration or of indefinite duration for one or more service type, from one or more terminals. However, only one terminal may be specified for the same service type (e.g. voice, telefax).

The following issues are for further study:

- Is it possible for a PUM registration session to exist on a terminal while the non-PUM user of this terminal has the ability to make outgoing calls at the same time?

- If a PUM user initiates a registration session on one terminal connected to a multi-point access, what happens to the other compatible terminals? Are they automatically part of the same registration session? If they are excluded from that session, may they have the possibility to make non-PUM outgoing calls or initiate other sessions?

- If MSN is used on the access, does a session on one number apply only to that number, and not to the other numbers on the access?

- What kind of signalling mechanisms can be used to support the session concept?

- Is it possible to achieve the session concept on a terminal not designed for PUM?

5.2.1.3 Terminal Swapping (TSW)

The ability for a PUM user to change terminals during a call. The call is held and may be retrieved at another terminal. This feature applies whatever the kind of terminal: wired or cordless. It is recognised that this feature overrides the current registration. When a call is retrieved the PUM user shall be identified.

5.2.1.4 Authentication

Various degrees of security of authentication may be considered, which depend on the PTN user's requirements. Several types of "PUM access device" (e.g. smart card, DTMF generator) may be considered, which contain varying degrees of information.

In the most simple implementation of PUM, the authentication procedure could be carried out manually by the PUM user with a Personal Identification Number (PIN), i.e. a user password.

In more complex implementations, depending on possible PUM access devices, complex authentication algorithms could be carried out.

5.2.2 Additional features

PUM will enable access to additional features, limited by terminal and network capabilities and restrictions imposed by the PTN.

5.2.2.1 Managed registration for incoming calls

The ability to set up a matrix of terminal identities so that incoming calls can be terminated and handled differently depending on time of day, day of week, calling party's identity, service type, call importance indication, for "no answer" and "busy" conditions, and other possible criteria.

This matrix can be modified by the user.

This feature enables a user with a regular schedule to set up a "timetable" matrix.

At the time of PUM number allocation, the new PUM user or PTN administrator shall set up a simplified time table with a set of default terminal accesses.

In addition to new facilities brought by PUM service, the supplementary services, usually offered to any PTN user, should be made available to PUM users.

A dynamic registration temporarily overrides any or all default terminal accesses which have been specified in the time table matrix, thus the duration of the override should be defined by PUM user.

Any or all of these overrides may be cancelled before the end of the duration by a new dynamic registration or by an appropriate procedure.

5.2.2.2 Status interrogation

The ability of the PUM user to obtain information of the status of PUM facilities (i.e. current registrations) from the user's own PUM service profile.

5.2.2.3 Mailbox announcement

The ability to inform the user, at the time of any registration, of waiting stored messages in his mailbox.

5.2.2.4 Abbreviated dialling

The ability for the PUM user to use a limited list of personalised short numbers.

5.2.2.5 Accounting on the basis of a PUM Number

The PUM users own number is used as the basis for accounting, independent of any terminal or PTNX used by the PUM user.

5.2.2.6 Terminal substitution

The ability of a user to use the same terminal configuration on any terminal.

5.3 Interaction considerations

5.3.1 Relation to UPT

As one person may be both a PUM user and a UPT user it seems desirable for user friendly reasons to offer the same procedures. Initially this could be achieved by having a common core for essential features and by using as far as possible the same identification devices. The level of co-ordination with UPT is dependant on the time planning for the respective standardisation project.

Since the UPT service documentation (references [1] to [3]) has split UPT features into one part of core features considered as essential or fundamental and another part of additional features, it would be desirable that PUM core features match as far as possible UPT core features in order to provide users the same perception of service.

In other words, it seems feasible, at first sight, to define most of PUM core features in line with UPT core features except those not appropriate to a private environment (e.g. billing). This compatibility does not prevent from defining other specific PUM features considered as essential for PTN users (see subclause 5.2.2) which might be included in UPT additional features in the future.

It is possible for PTN user who travel outside their own PTN, to have a UPT subscription. This would enable calls to those PUM users to be redirected to the UPT number by means of call forwarding. It will form a kind of external Follow me. Nevertheless, this can not be seen as a interworking between UPT and PUM because outside his PTN a PUM user becomes a UPT user with a UPT number and a different service profile and he can not have any means for remote PUM registration by means of UPT procedures.

Subsequently, it would be needed to conceive an extension of PUM service across different PTNs or public networks where each of them would provide PUM. This extension of PUM across public networks would be made easier if both UPT and PUM descriptions do not diverge. That might mainly concern PUM number structure, registration procedures, information exchange between databases and, of course, harmonisation of services.

At that further stage one can imagine that some of the essential features of PUM (if any) have been included in the UPT features and that these two services have been merged.

A PTN user roaming in public networks could benefit from most of the PUM services and could reach his home database (located in PTN) from a public access.

In turn, that would ease roaming of UPT users in a PTN by avoiding the risks of tromboning for instance. In this case, from UPT user's point of view the PUM database would act as the visitor UPT database.

In essence, the relationships between UPT and PUM should be considered within the framework of interworking between public and private ISDNs.

5.3.2 Interaction with existing services

The requirements for interaction between existing services (e.g. supplementary services) and PUM shall be identified within the frame of the PUM description. The requirements will then be forwarded to the relevant bodies. This is for further study.

5.4 Services

The basic services offered to extension users in a PTN should be made available also to PUM users. The same principle applies for supplementary services. However, the applicability and relevance of each supplementary service should be investigated (see "Interaction with existing services"). Also PUM users shall be supported by attendant.

5.5 Security aspects

Generally the PUM users may be exposed to various forms of misuse. These forms of misuse will concern for example:

- Fraudulent use: misuse of a user's resources by unauthorised persons who impersonate the user;

- Fraudulent access to data: access to a PUM service profile data by unauthorised means;

- Eavesdropping: unauthorised listening or recording of information during the communication;

- Malicious behaviour: malicious use of PUM procedures by a third party in order to interfere with or degrade the service offered to a PUM user.

PUM security shall be provided even if CTM security is not provided.

5.5.1 General requirements on security mechanisms

The security mechanisms provided by PUM to support mobility services, should at least be as good as for existing services. These security mechanisms, irrespective of their strength of protection, should not appear as complicated procedures to the PUM users, but they should be a part of the general PUM procedures.

5.5.2 Types of security mechanisms

Possible security mechanisms protecting the user may include:

- data access control;
- PUM user action authorisation;
- PUM user event protection;
- PUM user identity confidentiality;
- PUM user identity authentication;
- PUM service provider authentication.

NOTE 1: The proposed security features below are generally applicable to the long-term PUM scenarios.

NOTE 2: User data confidentiality is the property that the user information carried on traffic channels during communication is not made available or disclosed to unauthorised individuals, entities or processes. User data confidentiality will depend on the terminals, services and networks used.

5.5.2.1 Data access control

Data access control is the property that the PUM user's service profile data is protected against unauthorised access.

Only the PUM user and the PUM service provider should be authorised for operations on a PUM user's service profile. Any unauthorised access attempts should be rejected and possibly recorded.

5.5.2.2 User action authorisation

User action authorisation is the property that a PUM user's actions are:

- verified on request of an action;
- admitted when the PUM user is authorised for this action; and
- rejected otherwise.

It should be set up a list of authorised actions in the PUM service profile (like access parameters for service management procedures, interrogations or modifications, a list of services and facilities actually subscribed to, etc.).

5.5.2.3 User event protection

User event protection is the property that the PUM user has a certain control over the events he may be exposed to by the network or by other users.

User event protection may comprise various actions, including:

- protection against unexpected charges (e.g. negotiation procedures in case of unexpected charges, possibilities for advice of charge etc.);
- protection against unwanted incoming calls;
- protection against disclosure of physical location during normal procedures (e.g. connected with certain number identification supplementary services);
- protection against fraudulent outgoing calls. If the terminal where the PUM user is registered is left unattended, the PUM user may want to restrict outgoing calls from this terminal by requesting that authentication should be performed for each call setup;
- blocking of PUM account if the number of consecutive unsuccessful authentication attempts for this account exceeds a predefined limit;
- blocking the use of the PUM service from a terminal if the number of unsuccessful authentication attempts originating from this terminal exceeds a threshold (this threshold could be a number of attempts per time period).

User event protection may be provided by PUM specific supplementary services or through features of the PUM service profile.

5.5.2.4 User identity confidentiality

User identity confidentiality is the property that the user's identity is not made available or disclosed to unauthorised individuals, entities or processes.

User identity confidentiality protects the PUM user's general privacy, and protects the user against tracing of his physical location by illegal means. It implies that the PUM user should use another identity than the PUM number to identify himself to the network. The use of this identity should be optional for PUM users and PUM service providers.

5.5.2.5 User identity authentication

User identity authentication is the property that the user's identity is verified to be the one claimed.

User identity authentication protects the user and the network against unauthorised and fraudulent use. It may imply that the PUM user will have to authenticate himself during each of the PUM procedures. The authentication mechanisms used may vary according to the procedures requested by the PUM user and the current user-state. One example is when the PUM user has registered for outgoing calls, requesting that each outgoing call setup should be authenticated. In this case the authentication procedure should be simple for the PUM user, as he has already authenticated himself during the registration procedure.

5.5.2.6 PUM service provider authentication

PUM service provider authentication is the property that the PUM user can verify that the PUM service entity is the one claimed.

PUM service provider authentication protects the PUM user against unauthorised and fraudulent use as well as his general privacy. PUM service provider authentication may imply various actions:

- a specific authentication procedure is defined for the purpose of the PUM service provider authentication;
- an authentication procedure is used which authenticates both the PUM user and the service provider simultaneously.

PUM service provider authentication may in the first case be provided as an option. In the second case, however, it should be provided automatically together with the user identity authentication.

5.5.3 Security measures and devices

There are different aspects that influence the levels of security for the PUM user:

- the level of security provided by the PUM service provider and the agreement between this service provider and the PUM user;
- the level of security provided by the terminal currently used;
- the ability to provide PUM user security independently of the terminal security.

A high level of security on all these aspects and a combination of them would increase the overall security.

One example of this could be that the information to the terminal could be encrypted and the PUM user information is also encrypted. The PUM user information is sent encapsulated in the encryption structure understandable by the terminal. The PUM user information is deciphered either in the terminal, if it has the capability, or by measures (e.g. a device) of the PUM user.

The user and the terminal are totally independent and the securities are managed differently. Anyway, the user security needs more investigation and is for further study.

Parameters influencing the PUM security levels could be:

- the choice and use of security mechanisms;
- the choice of security equipment for PUM access;
- the security management applied by the PUM service provider.

Security mechanisms:
As a consequence of the types of security mechanisms, a PUM user may be offered a set of possible optional security mechanisms to decide upon. Security mechanisms especially relevant for PUM include:

- authentication mechanisms;
- access control mechanisms.

Security equipment for PUM access:
The levels of protection in the security mechanisms, depend also heavily on the realisation of the PUM equipment. The security equipment used for the PUM access concerns both PUM terminals and PUM access devices.

Security management:
The security management have to be supplied with a security management policy. It includes the following topics:

- how to handle cryptological keys and user-related data (key management, personalisation of security devices);
- how to react in case of misuse (security audit trail, event handling);
- what information and announcements have to be transmitted to PUM users and third parties (information policy).

Security management concerns indirectly the PUM user in the relations with his PUM service provider.

5.5.4 Multiple security levels

Each PUM service provider will have his own security policy, based on a minimum standardised security level and using a choice of security mechanisms, types of PUM access devices, and security management procedures. Various security levels will coexist for the PUM service. When PUM service providers with different security policies are involved, special procedures for interdomain security are required.

The capabilities of the terminals and networks will also influence the security level which can be guarantied for the PUM user. For example the high level of security provided by the use of smart cards is available only from a terminal with a card reader. A PUM user with a high level of security should not be precluded to use ordinary terminals. This case could have some limitations on the use of PUM features.

5.6 Signalling aspects

5.6.1 Signalling between a wired terminal and the PTNX.

The signalling system to be used between the PTNX and the wired terminal will be based on SSIG, ETS 300 192 [12]. It is, however, expected that some enhancements of the SSIG will be required.

5.6.2 Signalling between PTNXs

The signalling system to be used between the PTNXs will be based on QSIG, ETS 300 172 [13]. It is, however, expected that some enhancements of the QSIG will be required.

5.6.3 Signalling between public networks and PTNX

The signalling across the interface towards public networks are outside the scope of this TCR-TR.

5.6.4 Character sets

The standards should support the use of standardised character sets by adapting existing procedures to the need of mobile services.

5.7 Management

For further study.

6 Cordless terminal mobility

6.1 Introduction

This Clause describes the functions required to support mobility of Cordless Terminals (CT) within a single Private Telecommunication Network (PTN).

The main issues that are addressed are:

- identification of the mobility support procedures;
- location of the mobility support procedures;
- the protocols for the information flow between the fixed radio part and the PTNX; and
- the protocols for the information flow between the PTNXs.

6.1.1 General description

CTM provides a cordless terminal with the capability to access telecommunications services regardless of its geographical location by abandoning the "normal" fixed relation between the terminal and its physical connection to the network. Because of the mobile nature of a CT it will continuously change its PTN access point. This may happen during and between calls. In order for a PTN to support telecommunication services for continuously mobile CTs, the PTN (including the fixed radio parts) shall provide automatic functions which keep track of the CT's present and previous location as well as securing the communication with the terminal.

NOTE: This TCR-TR does not deal with any radio technical aspects. For information on such subjects, references should be made to the relevant standards for the applicable cordless systems.

In order to describe the CT's ability to freely move within the area covered by the PTN, this TCR-TR uses the term Cordless Terminal Mobility (CTM). CTM is not to be considered as a single function, but as a "collection" of all new and modified functions and procedures required to support mobility of cordless terminals. In this TCR-TR these functions have been gathered into two main groups which are:

- roaming; and
- handover.

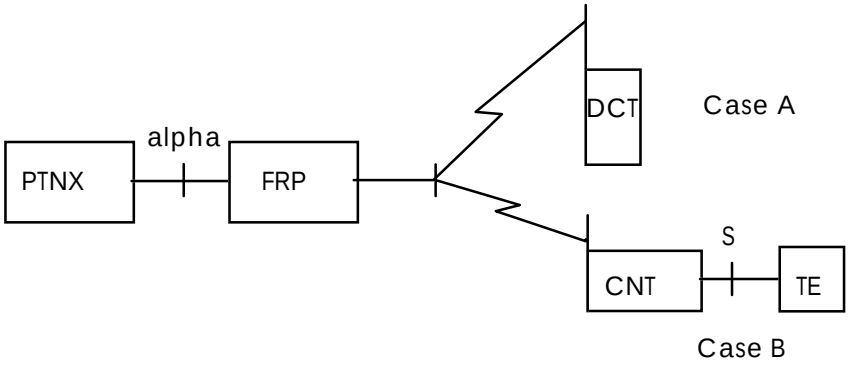
Subclause 6.2 covers these aspects in more detail.

NOTE: The CTM functions described are based on the perceived user requirements for CTM and are equally applicable to any air interface used for the cordless access. The main ones defined by ETSI are CT2 and DECT. It should be recognised that some forms of cordless access may not support all the services and procedures identified in this TCR-TR. However such limitations, where they do exist, do not invalidate the principles of this TCR-TR.

The mobility of cordless terminals is also supported by other systems (e.g. GSM). As there are many similar functions in GSM and PTN, it is expected that GSM will serve as a useful model in defining standards for mobility within a PTN.

6.1.2 Reference configuration

Figure 4 shows a possible reference configuration.



Legend: DCT means Dedicated Cordless Terminal;
CNT means Cordless Network Terminator;
TE is an ISDN terminal.

Figure 4: Reference configuration for CTM

The reference configuration shows two cases:

Case A: The cordless telephone systems acts as a terminal end system. A dedicated cordless terminal is used.

Case B: The cordless telephone system acts as an intermediate system. The cordless network terminator (CNT) provides a standardised wired interface to which a standardised ISDN terminal can be connected.

The reference configuration is not complete and requires further study however the following functional properties and limitations are recommended:

a) The FRP should not have any internal switching capabilities, i.e., the ability to interconnect two CTs.

b) The FRP may have more than one interface at the alpha reference point, but all such interfaces shall be connected to the same PTNX.

c) ETSI/ECMA should only produce standards at the alpha reference point, for interfaces that are based upon the ISDN basic and primary rate access standards.

d) The signalling protocol for the control of services and mobile functions should be based upon SSIG, ETS 300 192 [12]. The protocol shall support both case A and case B.

e) The allocation of functional entities and capabilities on either side of the alpha reference point requires further study.

f) The information flows across the Q reference point shall be independent of the allocation of functions across the Q reference point.

6.1.3 General information on roaming

The roaming function makes it possible for the user of a CTs to access PTN services between calls from different FRPs in the PTN.

NOTE: This TCR-TR covers the possibility to make and/or receive calls throughout the whole PTN within radio coverage areas 1 to 5 that are shown in figure 5.

The functions needed to support roaming include the following procedures:

- location registration (collection and storage of new location information);
- location deregistration (removal of location data);
- authentication (validation of the CT and/or FRP). This feature is optional.

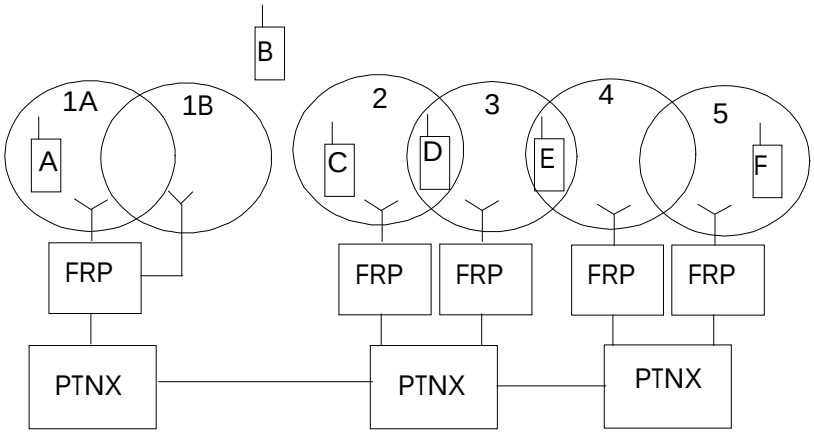


Figure 5: Logical block diagram of a simple PTN

6.1.4 General information on handover

The purpose of handover is to provide reliable and continuous telecommunication when a call is in progress to a terminal as it moves within and/or between the coverage areas of the FRPs in the PTN. The procedures used for performing the handover are basically the same as for roaming. The handover procedure includes the process of switching over to the new call path.

The procedures involved in a handover are:

- authentication (validation of CT and/or FRP), which should be optional;
- handover (change of communication path);
- location registration (if necessary).

Figure 5 shows a number of different handover situations. Basically these seen from the FRP can be classified as:

- internal; or
- external.

Internal handover means handover within one FRP, e.g. when moving between areas 1A and 1B of figure 5. This is an internal function of the FRP and does not require any cooperation from the PTN. Therefore, apart from identifying internal handover as a form of handover, it is not discussed any further in this TCR-TR.

External handover means handover between two different FRPs, e.g. when moving between areas 2 and 3 of figure 5. Because external handover involves two FRPs, the cooperation of the PTN is required. This form of handover is addressed in this TCR-TR. Therefore the unqualified term "handover" used in this TCR-TR always refers to the external form of handover.

NOTE 1: This use of the term handover corresponds to the term "external handover" used in DECT.

NOTE 2: Both types of handover may cause a location registration which requires communication with the PTNX.

Figure 5 shows cases of handover inside a PTN, of which only case a (below)is relevant to this TCR-TR:

a) handover between two FRPs in the same PTNX (e.g. between area 2 and 3);
b) handover between two FRPs in different PTNXs (e.g. between area 3 and 4);
c) handover between two FRPs in different PTNXs not directly interconnected (transit calls) e.g. between area 1 and 5.

6.2 Feature description

6.2.1 Core features

6.2.1.1 Identification

Generally the radio systems use four different identity categories for identification and addressing in the radio environment:

- connection related identities (radio internal);
- cordless terminal identities;
- fixed radio part identities;
- equipment related identities.

NOTE: Equipment related identities are normally used to derive a default identity coding for a cordless terminal prior to registration and/or for making some type(s) of special call(s), e.g. an emergency call, and to identify stolen terminals.

The identities of the fixed radio part and the cordless terminal are used to:

- to transfer access information from the fixed radio parts to the cordless terminals;
- to process access requests from cordless terminals;
- to identify the fixed radio parts and cordless terminals;
- for paging;
- for charging and billing.

The basic concept for the use of these identities is that every radio base station broadcasts a unique identity. This identity contains information about the service provider (PTN identity) and the capabilities of the base station. The cordless terminal has a corresponding "identification code". The "identities" of the fixed radio parts and the cordless terminals are then checked to see if they match each other. This mechanism allows only "valid" units to be interconnected in the case where several base stations and CTs exist in the same area. A CT may contain several such identities allowing the CT to connect to many base stations and/or networks.

The identity mechanism mentioned above support functions such as:

- use of the system for different environments (e.g. residential, public or private);
- provision of globally unique identities for manufacturers, installers and operators with a minimum of central administration;
- multiple access rights for the same CT;
- freedom to tailor access rights to groups of radio systems;
- roaming agreements between different networks;
- indication of handover domains;
- indication of location areas;
- indication of subscription areas;

NOTE: For detailed information about DECT and CT2 identities and addressing, see ETS 300 175-6 [4] and I-ETS 300 131 [5].

6.2.1.1.1 Identification of fixed radio part

The identity transmitted by the FRP is used by the CT to decide:

- if the fixed radio part belongs to the environment the CT wishes to access;
- whether or not that particular fixed radio part is the one the CT wishes to access.

6.2.1.1.2 Identification of Cordless Terminal (CT)

When a CT requests a service from the network, or if requested to by the fixed side, the terminal may supply its cordless terminal identity (e.g. for DECT the IPUI, TPUI or IPEI, and for CT2 the PID) which enables the fixed side and/or the PTN to:

- identify the user or user's equipment (CT);
- check if the request shall be allowed or rejected.

Before the CT and/or the request is accepted by the network or FRP, the PTN/FRP may decide to perform an authorisation check of the CT.

Functions for assignment and handling of these identities are required and should therefore be standardised.

Equipment related identities are used to identify the CT and are usually globally unique. The fixed part may be able to request the CT to transmit its equipment identity which could then be used by the PTN to for example, track stolen equipment. (In DECT the equipment identity is called IPEI. In CT2 the PID serves the same purpose.)

6.2.1.2 Roaming

Roaming is mainly provided by the following means:

1) identities and addressing;
2) location/registration and attachment;
3) authentication (optional).

Prior to providing services to an unknown CT, it is necessary first to check if the terminal has access rights to the system. The process should be as follows:

- firstly, the terminal reads the Fixed Radio Part Identity and uses this identity to check whether it has access rights to that system. Assuming it has access rights, the cordless terminal then proceeds to register with the system;
- secondly, the CT identifies itself to the system, after which an optional authentication of the terminal may take place. Upon successful completion of this authentication (which is optional), the terminal is added to the VDB and the terminal gets a temporary identity to use in the system.

The terminal can now make and receive calls.

The cordless terminal may deregister from the system by sending a request to the PTN If this request is successful, the terminal is deleted from the VDB.

6.2.1.2.1 Location registration related procedures

Four forms of location registration procedures have been identified:

- user initiated location updating. The user decides whether he wants to receive incoming calls in the radio system he is visiting (e.g. by pushing a special button);
- automatic location updating initiated by the CT. The cordless terminal initiates a location registration procedure; normally as soon as it detects having entered another location area;
- automatic location updating initiated by the fixed side. The fixed side instructs the CT to send a location registration request;
- the fixed side controls the location updating.

See Clause 8 (Scenarios) of this TCR-TR for further examples on registration procedures.

6.2.1.2.2 Attachment related procedures

When registered, the CT may inform the network whether it is active or not (e.g. in DECT marking IPUI active/inactive), by sending one of the following messages:

- attach;
- detach.

The intention of these messages is to minimise the load on the system by avoiding the initiation of unnecessary location registration and broadcast procedures.

6.2.1.3 Handover

Handover is the process of switching a call in progress from one physical channel to another physical channel. This process can be internal or external with respect to a FRP. A request for handover from one FRP to another FRP may come from:

- the FRP involved in a call;
- a new FRP; or
- the PTNX.

Special areas to be addressed regarding handover are:

a) identities;
b) registration;
c) authentication;
d) interruption during handover.

As a handover depends on a number of processes taking place, there may be an interruption in the communication path for the cordless terminal. This may cause a problem for some types of calls. For data communication even short interruptions in the communication path may corrupt the data.

6.2.1.4 Authentication

6.2.1.4.1 Authentication of cordless terminal

Authentication of a cordless terminal is necessary if the network operator wants to prevent "unauthorised " terminals access the PTN.

6.2.1.4.2 Authentication of the fixed part

In order to prevent a cordless terminal form logging onto an unauthorised fixed part, some form of authentication of the fixed part is also required. This is a function of the terminal, but exchange of information between the "network" and the CT may require the network to support some functions as well.

6.2.1.4.3 Mutual authentication

Mutual authentication means that both the CT and the fixed part require authentication of each other. This function is an optional function.

6.2.1.4.4 Proprietary authentication algorithms

Proprietary authentication algorithms may be required in some private networks and the standards should be able to support such functions.

6.2.2 Additional features

A general problem arises for active calls if the CT moves outside the coverage area of the current FRP or the CT is switched off. In this case the system should detect that the CT is no longer active and start a timer. If the timer expires a notification may be sent towards the network. During an active call when the CT temporarily moves outside the coverage of the current FRP, but returns within the time out value, a

temporary loss of communication may occur. The CT may also return to another FRP within the same PTNX.

In the case of a terminal being unreachable by the PTN, the PTN may decide to change or delete the location data.

6.3 Interaction considerations

6.3.1 Cordless systems

The standards to be developed should support ETSI standardised radio access systems that are applicable for use in a PTN.

6.3.2 Interworking with existing services

The standards shall support interworking with other services offered by other networks as if the CT was a "normal" wired terminal. Ideally the user should see no difference in the services that are offered to wired or cordless terminal.

6.3.3 Local area networks

This is outside the scope of this TCR-TR.

6.4 Services

Generally the services available to wired terminals should also be available to CTs. Initially, priority shall be given to the following basic services:

- telephony teleservice, and the following Circuit mode 64 kbit/s bearer services;
- 64 kbit/s unrestricted;
- 3,1 kHz audio;
- speech.

While the basic services supported in these standards are of the same form as those provided to users in the public ISDN, the situation regarding supplementary services (SS) for mobile CTs is more complicated because of the following factors:

- some SS may differ for wired terminals and mobile cordless terminals;
- some SS may not be possible to support from a particular mobile CT; and
- a CT may have new specific SS applicable only to CTM.

ECMA uses also the term Additional Network Feature (ANF) to describe special features which can be described as SS but, unlike supplementary services, they are not directly available to the end users. An ANF operates autonomously within a PTN and enhances the operation of the PTN for the benefit of all users. It is not the intention of this TCR-TR to describe supplementary services and/or ANFs in a PTN as these are described by the applicable standards and technical reports except where there is interaction with CT mobility.

6.4.1 Basic services

Initially the standards shall support the following teleservice:

- telephony.

Initially the standards shall support the following circuit mode bearer services:

- 64 kbit/s unrestricted;
- 3,1 kHz audio;
- speech.

6.4.2 Supplementary services

The supplementary services supported for a cordless terminal shall be those services that are specified in ETR 079 [15]. See also subclause 6.4.3 below.

As the PTN may have to interwork with the public ISDN, the cordless terminals connected to the PTN should also interwork with the relevant supplementary services of the public ISDN.

Supplementary services which have not been standardised can still be supported in a PTN as the signalling protocols at the "Q" reference point and the "alpha" reference point (i.e., between the FRP and the PTNX), shall provide escape mechanisms for the transfer of manufacturer specific information for the support of supplementary services which are not standardised, or for the support of non-standard extensions to standardised supplementary services.

6.4.3 ECMA-Supplementary Services and Additional Network Features in Private Telecommunication Networks

ETR 079 [15] lists supplementary services which have been identified as having applications in PTNs but, does not indicate which of the listed supplementary services that may be appropriate for standardisation. It is anticipated that as a general rule all supplementary services standardised either by ETSI or ECMA shall support roaming CTs.

The document lists the following groups of PTN services:

- supplementary services;
- additional network features;
- attendant services.

At present, it is not possible to provide a complete list of all services within each of these groups that shall be standardised and how each of these services may influence protocols at the Q reference point, and at the "alpha" reference point (i.e., between the FRP and the PTNX).

6.4.4 Additional services

For further study.

6.4.5 Radio specific supplementary services

It is expected that the CTs may require special SS not yet identified. This issue is for further study.

6.4.5.1 DECT

The standards should support the DECT specific supplementary services, see ETS 300 175-5 [7] and ETR 043 [8].

6.4.5.2 CT2 specific supplementary services

For information on CT2 specific supplementary services see the description of feature class 7 (Auxiliary function selection) in subclause 7.2.4 of I-ETS 300 131 [5].

6.4.5.3 Other radio systems

For further study.

6.4.6 Support by PTN attendant

CTs should be supported by the PTN attendant to the same extent as wired terminals. Possible additional requirements on attendant services due to CTs are for further study. The need for an attendant to be mobile is for further study.

6.5 Security aspects

In a PTN offering network wide mobility services, both the CTs and the PTN operator are vulnerable to unauthorised intrusion and misuse by third parties. In addition, special measures should be provided in order to protect the CTs integrity (e.g. location at a given time etc.). However, this subclause only addresses security aspects related to the use of the CT itself and not the security aspects associated with the user of the terminal.

6.5.1 Security related functions

The following two techniques may be used to protect the PTN, the CTs and the exchanged information:

- authentication;
- encryption.

NOTE 1: Protection of transmitted information is essential on the radio link, but may also be required on the links between the nodes within the PTN. However, this topic is outside the scope of this TCR-TR as this is a general PTN problem.

NOTE 2: The security aspects, seen from the protection of user's privacy, is addressed in the proposed CEC Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular Integrated Services Digital Networks (ISDN) and private digital mobile networks [9].

6.5.1.1 Authentication of cordless terminal

Authentication is the process whereby a CT is positively verified to have the right to communicate. Authentication may be requested at any time. If a terminal has to be authenticated, and its specific parameters are unknown, the authentication process will require functions which support retrieval of authentication parameters from the network, i.e., the home data base. Authentication should be optional in a PTN.

NOTE: DECT and CT2 specify standard authentication algorithms which should be supported by the standards.

The use of proprietary authentication algorithms should also be possible.

The PTN may contain a list of stolen CT identities The PTN may disable CTs on this list by erasing data stored in the CT (ZAP register). After a ZAP, the CT can no longer be used and has to be taken to the network operators maintenance centre for re-programming.

6.5.1.2 Authentication of the fixed part

In order to prevent a CT from logging onto a "phoney" or incorrect fixed part, optional functions for the authentication of a Fixed Part are also required. The procedure for the authentication of a FRP is quite similar to the procedure for authentication of a cordless terminal. One example where it may be necessary to issue an authentication request of the FRP is when the FRP wants to "ZAP" a CT.

6.5.1.3 Mutual authentication

Mutual authentication allows a CT and a FRP, through which a call is connected, to authenticate each other. It is proposed that this is achieved by combining a number of other security services and thus does not require an explicit mutual authentication mechanism.

6.5.1.4 Proprietary authentication functions

Proprietary authentication algorithms may be required in some private networks and should be supported by the standards.

6.5.2 Support for encryption functions over the radio interface

Encryption functions over the radio interface may be required in certain applications. The encryption of both user information and signalling information might be required.

6.5.3 Functions to prevent unauthorised access

The following items are related to this area and are for further study:

- protection against use of unauthorised terminals;
- protection against unauthorised calls from sources outside the PTN;
- protection against unauthorised calls from sources within the PTN. The standards shall support functions whereby a CT can be verified to have the right to communicate via a particular FRP;
- protection against use of stolen equipment. The access rights for a CT can be temporarily and/or permanently withdrawn by sending a command to the CT which erases the memory in the CT. In addition the databases should also be updated such that the CT's Dialling Number (DN) is "black listed";
- authentication for access to user mobility data in network databases;
- authentication for secure answer;
- confidentiality of present location;
- confidentiality of identity;
- confidentiality of user data;
- data retrieval.

The following item is outside the scope of this TCR-TR:

- authentication of network operator's access to "subscription data".

6.6 Signalling aspects

6.6.1 Signalling between the cordless terminals and the fixed radio parts

The signalling on the air interface between the CT and the FRP is outside the scope of this TCR-TR.

6.6.2 Signalling between the fixed radio part and the PTNX

The signalling system to be used between the fixed radio part and the PTNX shall enable the use of SSIG [12] terminals at the S reference point to support the mobility requirements laid down in this TCR-TR, and taking into account the signalling system employed at the air interface.

6.6.3 Signalling between PTNXs

The signalling system to be used between the PTNXs shall be based on ETS 300 172 [13]. It is expected that some enhancements of QSIG will be required.

6.6.4 Signalling between public networks and PTNX

The signalling across the reference point T towards public networks is outside the scope of this TCR-TR.

6.6.5 Character sets

The "default" character set shall be IA5. Refer also to CCITT Recommendation T.50 [10]. Any translation to other character sets should take place in the FRP.

6.7 Management, administration and operation

6.7.1 Configuration management

NOTE: Configuration, as used in this TCR-TR, is called subscription registration in DECT.

It is anticipated that the management functions required for configuration and amendments that apply for wired terminals also apply to the cordless terminals. However, the radio systems may require some special functions related to the cordless terminals which may have an impact on the PTN and its functions.

6.7.1.1 Configuration management of cordless terminals

6.7.1.1.1 Configuration procedure (on-air)

Normally the CT has to be taken into a maintenance centre if the data kept in the terminal has to be modified. However, both from the user's as well as from the network operator's point of view, it would be desirable if this could be done remotely, i.e., "over the air interface". This does, however, require a standardised procedure for transmission of the configuration data to the FRP.

Examples of such types of data are:

- CT's identity;
- CT's visiting identity;
- information about authentication key/process;
- CT's class of service.

The method by which this configuration data is loaded into the CT over the air-interface is outside the scope of this TCR-TR.

6.7.1.1.2 Exchange of configuration data (on-air)

This function allows the exchange of subscription data between the network and the portable in real-time over the air interface. No subscriber/user actions are necessary.

6.7.1.1.3 Suspension/termination of access rights (on-air)

This function allows the fixed part to suspend or terminate the access rights of a CT. Normally the CT shall have the right to authenticate the fixed part before acting on the instructions received from the fixed side. The following variations of this function are foreseen:

- suspension/termination of all access rights;

- re-programming of some of the data (e.g. account data) held in the portable so that access rights are suspended subject to certain conditions being met, coupled with the ability to reprogram the data again in order to reinstate access rights once these conditions have been met;

- re-programming of data (e.g. account data) held in the portable so that access rights are terminated and such that it cannot be reinstated except by following a full a re-registration procedure.

Application of this procedure may e.g. be in the case of a portable being reported stolen or lost or after the subscription has been cancelled.

6.7.1.2 Management procedures for cordless terminals

6.7.1.2.1 Introduction

The procedures and features described in this subclause are recommended for use by the "PTN Network Supervisor (SUP)" in order to support mobility of cordless terminals.

The standards shall not specify how the supervisor accesses these functions, as this is a matter to be decided by the equipment manufacturer, but should address issues related to data structures, signalling systems and protocols, call state messages, updating of databases, transfer of information, fault recovery, unavailability of databases etc. Note that in this subclause, only the consequences for the cordless terminal are addressed in respect of the user service.

6.7.1.2.2 Network identity

Ideally the network identity of the CT shall be its directory number. Only the SUP shall have the ability to change and/or alter this identity. The SUP may specify several identities for a given CT in order that it can access more than one application. All CTs shall be able to read (only) the identities of all other CTs in the PTN. However, a feature should be available allowing "secret" identities which only can be read by CTs having authorisation to do so.

6.7.1.2.3 Access codes

The access codes needed to accept a registration shall be specified by the SUP. Access codes shall only be readable by the appropriate user(s) and the SUP.

6.7.1.3 Possible barring functions

6.7.1.3.1 Terminal access point barring

The SUP may have the ability to bar access to the network for terminals with specific addresses . This function may be applied on:

- outgoing calls;
- incoming calls;
- both in- and outgoing calls;
- on a service by service basis.

6.7.1.3.2 Network access point barring

This feature allows the SUP to block access to the network for all terminals connected to a network access point. This feature will also bar a valid CT access to the network if it attempts a network access from this point.

This function may be applied on:

- outgoing calls;
- incoming calls;
- both in- and outgoing calls;
- on a service by service basis.

6.7.1.3.3 Identity barring

The SUP may be able to bar access to the network for specific CT identities. This function may be applied on:

- outgoing calls;
- incoming calls;
- both in- and outgoing calls;
- on a service by service basis.

6.7.1.3.4 Call type barring

The SUP may be able to bar access to the network for special types of calls.

This function may be applied on:

- outgoing calls;
- incoming calls;
- both in- and outgoing calls;
- on a service by service basis.

6.7.1.3.5 Call barring exemption

A function may be available for the SUP to specify that some types of calls (e.g. emergency calls) can override the barring conditions.

6.7.1.4 Location registration and amendments

The SUP may be able to update the location registration databases for all users and terminals (he shall also be able to override data input by the user).

6.7.1.4.1 Incoming call

6.7.1.4.1.1 Registration

The SUP may be able to register a CT for incoming calls to any access point. It shall be possible to register:

- without restrictions;
- for a specified number of calls;
- for a specified period.

There shall be no limit to the number of users and/or terminals that can be registered for incoming calls to the same network access point.

6.7.1.4.1.2 De-registration

The SUP may be able to deregister a specified network identity for incoming calls at a given access point with or without alteration of his current location data.

6.7.1.4.2 Outgoing call

6.7.1.4.2.1 Registration

The SUP may have the possibility to register a CT for outgoing calls at any access point. It shall be possible to register:

- without restrictions;
- for a specified number of calls;
- for a specified period.

Registration for outgoing calls may require authentication of the CT (for each call or only once). There shall be no limit to the number of users and or terminals that may be registered by the SUP for outgoing calls from the same network access point at the same time. The SUP shall also be able to register a terminal for outgoing calls on more than one network access point at the same time.

6.7.1.4.2.2 De-registration

The SUP may be able to deregister a special access point for outgoing calls from a specific CT with or without alteration of his current location data.

6.7.1.5 Authentication code

The SUP may have the ability to specify and/or amend the authentication code for each CT at any time.

6.7.1.6 Basic announcements

Some information (which has to be clarified) about the various states of a call is provided to the user by the PTN. The method of informing the user depends on the characteristics of the terminal. However, for the case of tones these messages should fulfil national standards (e.g. frequencies, cadences, duration etc.).

6.7.1.7 Advanced announcements

The SUP may be able to assign special/additional information about the state of a call (advanced announcements), by providing more details than the basic announcements. This information may be verbal or text/graphical messages. The SUP shall have the ability to select from a set of messages as well as being able to specify new messages as and when required.

6.7.1.8 Global network access

Outside the scope of this TCR-TR.

6.7.1.9 Service profile

Each user/terminal may be allocated one or more fixed "profiles" which detail the communications and/or terminal options available when moving around in the PTN. The SUP shall have the ability to assign all, or some of these profiles to a user/terminal. Several profiles may be assigned to each user/terminal at the same time. However, the terminal can only use one of these profiles at any given time. The user is not allowed to alter a profile unless one or more fields contains user changeable data.

6.7.1.9.1 CT subscription identity

For some applications there may be a need to define a "User Profile" for the CT itself irrespective of the current user of the terminal. In this case the CT actually becomes the "owner" of the "subscription" and not the person using the terminal.

The application of this subscription profile is outside the scope of this TCR-TR, but it may be used to define the capabilities, or allowed functions, assigned to the CT (e.g. incoming calls only, barred for outgoing network calls etc.).

In order to change the subscription profile a "Subscription Identity" (together with an optional Authentication code) may be requested by the PTN. It is recommended that another identity other than the CT's DN is used for this purpose due to potential misuse by other terminals. The method by which this information is generated in/by the CT is a manufacturer implementation matter and therefore outside the scope of this TCR-TR.

6.7.1.9.2 CT identity code

In order to make it possible for the network to identify a legitimate CT, e.g. to prevent access from unauthorised CTs simulating another terminal, it is necessary to allocate a unique identity to each CT. On request, this identity should be sent by the CT towards the "fixed side" (e.g. during registration and handover). If the CT's DN is used for this purpose, then it is strongly recommended that an Authentication Code is added to the Identity Code to prevent fraudulent use of terminals simulating approved CTs.

The method by which this information is generated in the CT (e.g. smart cards, IC module, keypad etc.) is a manufacturer implementation option and is outside the scope of this TCR-TR.

The use of the radio specific identities inside the PTN is for further study.

NOTE: Annex A describes the applicable parts of the DECT identity structure, as well as an example of DECT addressing structure in a PTN.

6.7.1.10 Interrogation

The SUP may be able to interrogate the current status of a CT profile data (e.g. location registration, available services etc.) at any time.

6.7.1.11 Modification

The SUP may alter all or part of the CT profile(s) at any time.

6.7.1.12 Group registration

The SUP may be able to register a group of terminal access point for incoming and/or outgoing calls in one operation.

6.7.1.13 Specification of paging terminal

In order to reach a terminal not registered for incoming calls, a "paging" facility will be required. The SUP shall therefore have the ability to assign one or more terminal addresses as "paging terminals" addresses.

6.7.1.14 Specification of call pick-up addresses

The SUP may be able to specify one or more terminal addresses as answering positions for paged users.

6.7.1.15 Specification of terminal profiles

This feature provides the SUP with the ability to lay-out a user's terminal according to the user's own requirements (e.g. always to look like his home terminal).

6.7.1.16 Specification of user environment

This feature allows the SUP to design a particular user's "service environment" in a manner which suits the user (e.g. with service dialogues in a specific language etc.). This may be done either by providing a set of options or by specifying a fixed profile (or a menu of alternatives).

6.7.1.17 Specification of terminal matrix access profile

This feature allows the SUP to specify a "matrix" of allowed destinations so that calls can be routed and handled differently according to the type of service, time of day, time of week, calling parties identity etc. The matrix shall contain the possibility for the user to modify his own matrix. This feature may be valuable e.g. for a user which travels or move around according to a routine schedule.

6.7.1.18 Specification of alternative identities

The SUP may be provided with a feature allowing him to specify other type of address information other than numbers e.g. symbols, spoken messages, address, titles, company name, destination etc. or a combination of these.

6.7.1.19 Updating of databases

The following issues are for further study:

- update of identities;
- update of authentication/crypto keys;
- update of the ZAP register;
- data transfer rates.

The ZAP register is intended to keep information about CTs that are temporarily or permanently barred access to the PTN.

6.7.2 Fault management

The following issues are for further study:

- problem areas and fault recovery:
  - * authentication failure;
  - * link between PTNXs not available,
- fault recovery functions;
- cordless terminal moves out of range during handover;
- cancellation of handover.

6.7.3 Performance management

The following issues are for further study:

- Grade of service:
  the CTs ability to move freely within the network may cause some degradation of the grade of service if the PTN has a high density of CTs. Traditionally the routeing and the dimensioning of the trunk lines in a PTN has been calculated on an estimation of the traffic between each node. Dimensioning shall take mobility aspects into consideration;
- quality of service;
- service operability performance;
- serviceability performance;
- service integrity;
- capacity and timing requirements;
- statistics and traffic measurement;
- network management.

6.7.4 Security management

In a network supporting cordless terminals the need for security services are quite obvious as there is no "visible" evidence of:

- who is accessing the PTN;
- who is offering service to the terminals;
- who is listening to the communication on the air link;
- who is using the terminal;
- etc.

At least the following security services should be supported:

- authentication of the fixed radio part;
- authentication of the cordless terminal;
- mutual authentication of the fixed side and the CT;
- user authentication;
- data confidentiality.

Normally some of these services are provided by the appropriate radio systems. However, some of these services may require the definition of new ANFs, e.g. for providing network wide services.

6.7.4.1 User data security

The air-interface is literally open to everybody with suitable radio equipment and special considerations have been taken by the relevant radio systems to prevent eavesdropping and unauthorised access to information over the air-link. It is therefore not deemed necessary for the PTN to implement any extra security facilities above this for calls to/from CTs. However, the PTN should have the capability to store and handle encryption keys and any other information to ensure user data security over the air interface.

6.7.4.2 Encryption

The standards for CTM should support the use of appropriate standardised encryption keys for the applicable radio systems.

6.7.4.2.1 Encryption of user information

For further study.

6.7.4.2.2 Encryption of signalling information

Encryption of signalling information is only applicable over the air-interface. Management of the encryption keys is for further study.

6.7.4.2.3 Proprietary encryption keys

The use of proprietary encryption keys should be supported by the standards.

6.7.4.3 Authentication

Authentication of the fixed radio part:
This is a service initiated by the CT which allows a CT to check that it is communicating with a legitimate fixed radio part. This service is normally invoked at the beginning of a call, but may be requested at any time during a call.

Authentication of the cordless terminal:
This is service is normally initiated by the fixed radio part to check that it is communicating with a legitimate CT. Usually this service is invoked at the beginning of a call, but may be requested at any time during a call, e.g. to check that the FRP is communicating with a "legitimate" CT.

Mutual authentication:
This is a service which enables the FRP and CT to authenticate each other.

User Authentication:
This service allows the FRP to authenticate the user by checking the personal identity value associated with the user. Normally this value will be "input" by the user of the CT. It is, however, also possible to use it as a secondary authorisation code for the CT itself in order to increase the level of security. This TCR-TR does not intend to define or discriminate how this value is used nor does it attempt to describe how the value is generated in the CT (smartcard, PIN code via a key-pad, IC circuit etc.). This service is also applicable for wired extensions.

6.7.4.3.1 Authentication algorithms

It is outside the scope of this TCR-TR to define algorithms that may be used for authentication. However, the standards should support the standardised authentication algorithms or procedures for the applicable radio systems.

6.7.4.3.2 Proprietary algorithms

The standards should allow for use of proprietary algorithms.

6.7.4.4 Privacy

For further study.

6.7.5 Accounting management

6.7.5.1 Charging, billing and accounting

Due to cost sharing (e.g. between departments, logging of cost per user, different companies etc.) functions for "charging, billing and accounting" are considered as important functions also for private telecommunication networks. As billing and accounting are administrative functions, only the main charging aspects are addressed in this TCR-TR. Further studies are required on this subject.

6.7.5.1.1 Charging

Mechanisms should allow the possibility of applying various charging in relation to the mobility of terminals or users. The implementation of such mechanisms is a PTN operator's responsibility.

For some PTNs these costs could be decomposed into the following cost elements:

- PTN network related cost elements;
- cordless/radio related cost elements.

These may again be split in:

- call related charging (duration of call, distance, time etc.);
- cost for the use of special resources (e.g. channels capacity, frequencies, conference units etc.);
- cost related to use of telecommunication services;
- non call related charging (registration costs, activation of services etc.).

6.7.5.1.2 Billing

Billing is to be understood as the process of transferring the collected charging information into an "invoice" for payment. This process is normally handled "off line" by the administrative staff and is outside the scope of this TCR-TR.

6.7.5.1.3 Accounting

Accounting is an administrative procedure between/by the network operator(s) for sharing the cost and/or revenue generated by internal and external traffic. This process is considered as an "off line" activity and is outside the scope of the TCR-TR.

6.7.5.2 Transferring of charging information

The need to transfer charging information depends on the structure of the network and location of databases. However, it is very likely that a PTN consisting of several PTNXs may need different data bases.

The exchange of call charging data may of course be handled "off line" as an administrative process.

Examples of the type of data that may be needed to be transferred between data bases are:

- identity of home PTNX;
- identity of visited PTNX;
- user identity;
- destination of the call (country, area etc.);
- telecommunication services used;
- chargeable time;
- identity of the terminal;
- date and time of the call;
- identity of "own" PTN (not addressed in this TCR-TR);
- identity of visited PTN (not addressed in this TCR-TR).

Further information on this subject can be found in subclause 6.7.4.

7 Numbering, addressing and routeing

7.1 General principles

The general principles of PTN addressing are described in ETS 300 189 [6] and these should also apply to PTNs which provide PUM and CTM. Though the scope of ETS 300 189 [6] does not exclude PTNs providing PUM and CTM, such features are not specifically considered either. Therefore, it is shown how ETS 300 189 [6] can be applied to PTNs providing PUM and CTM, and certain new aspects of addressing and numbering which are not covered in ETS 300 189 [6] are also identified.

Ideally the PTN numbering plan (PTN NP) should not be technology dependant, but should be of a generic nature. Therefore numbering for PUM should be independent of the type of terminal (wired or cordless) used and numbering for CTM should be independent of the cordless technology (CT2 or DECT).

As indicated in the ETS 300 189 [6] the authority of the private telecommunications network may use:

- the ISDN Numbering Plan according to CCITT Recommendation E.164 [19]; or
- a Private Numbering Plan; or
- an Implicit Numbering Plan; or
- any combination of these numbering plans,

as the native numbering plan in its PTN. These possibilities should be retained with the introduction of CTM and PUM.

7.1.1 Addresses in non-ISDN telecommunication networks

Non-ISDN telecommunication networks are usually dedicated networks providing single connections and, from an addressing point of view, there is a 1:1 relationship between the physical access of the PABX (point of access) and the terminal and thus between the user and the terminal (see figure6). Typically the addresses consist of decimal digits only, thus making addressing a question of numbering plans. Each user has his own dialling number (DN) which may be listed in a telephone directory. This DN is used by the other users for initiating calls and other services towards a particular user. In order to determine the routeing of the call and to control access to special services, etc. a conversion of a PTN number might be necessary.

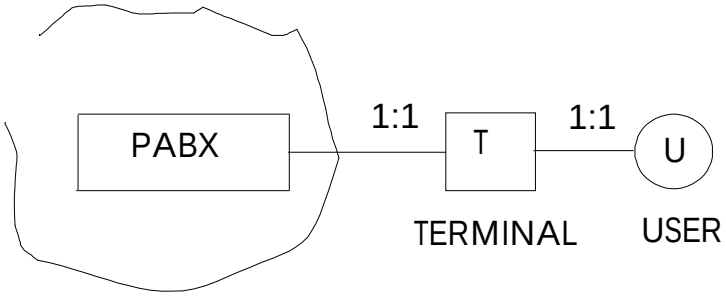


Figure 6: Addresses in non-ISDN telecommunication networks

The main characteristics of non-ISDN telecommunication networks are:

- the terminals are static (i.e. always connected to the same physical port in the exchange);
- the terminals normally do not have their own identity;
- it is actually the physical access of the PABX which is addressed (i.e. there is a 1:1 relationship between the terminal and the PABX access);
- a call normally follows a predetermined path through the network.

Owing to the static nature of such networks, the procedures for establishing calls (number analysis, routeing, etc.) could be kept simple. It was easy to plan the network architecture and routeing algorithms because the terminal could always be found at the same location. Furthermore, the DN could normally be used by the PBXs to determine the routeing through the network.

7.1.2 Access arrangement in public and private ISDNs

The ISDN (both public and private) allows accesses to be assigned more than one number. In addition the basic access allows a maximum of eight terminals to be attached simultaneously. In order to support the various arrangements of terminals and numbers at the network access, two supplementary services are applicable. They are:

- Direct Dial In (DDI);
- Multiple Subscriber Number (MSN),

and they are briefly described below.

7.1.2.1 DDI

The supplementary service DDI, ETS 300 062 [20] and ETS 300 063 [21], is applicable to both basic and primary accesses and only for incoming calls to a PTN. The DDI public network supplementary service enables a user to call direct a user on a PTN by use of a public ISDN numbering plan. The public ISDN achieves this by sending all or part of the destination ISDN number to the PTN.

In principle this service can also be applied to the terminal access of a private network, but at this time no ECMA or ETSI standards are under development.

7.1.2.2 MSN

The supplementary service MSN, ETS 300 050 [22] and ETS 300 051 [23], is applicable to both basic and primary accesses and for both incoming and outgoing calls. This service is explicitly defined for the public ISDN (see the references above). For a PTN, the procedures are included in the basic service specification ETS 300 171 [27]. The service allows multiple numbers to be assigned to the access such that each number has its own subscription profile.

For outgoing calls it is a requirement that the network user provides a user identification number (origination number). This number may be the whole or part of the ISDN number, a PTN number or a number that is specific to the access. The network will verify that the number provided is one of the numbers assigned to the access.

For incoming calls, the network (public or private) will provide a destination number that identifies the called user. The number provided by the network may be the whole or part of the ISDN number, a PTN number or a number specific to the access.

7.1.3 Addresses in PTNs supporting CTM

In networks supporting mobility via radio access systems, the correlation between the physical access in the PTNX and the terminal and the user is no longer a 1:1 relationship, as shown in figure 7. This figure also shows that the addressing mechanism needs to be enhanced in order to cater for one or more of the following situations related to the radio parts:

- more than one PUM user (e.g. W) may be logged on at the same terminal simultaneously, i.e. there is a 1:W relationship between the terminal and its users;

- there exists a 1:Z relationship between the CT and the FRP as one FRP can serve several CTs;

- a 1:X relationship exists between the PTNX and the FRP as it is very likely that a PTNX will serve more than one FRP;

- depending on how a specific FRP is connected to a PTNX, there may be many links between the two. The PTN addressing mechanism shall be designed such that the PTNX can determine which FRP to use for a specific call. However, the PTN addresses should not include any supplementary information for the selection of the physical link or timeslot between the PTNX and FRP.

The value of Z may be quite high since it corresponds to the number of CTs roaming in the coverage area of one FRP. It should be noted that an FRP may be implemented with several base stations. The estimation of the values of W, X and Z is for further study.

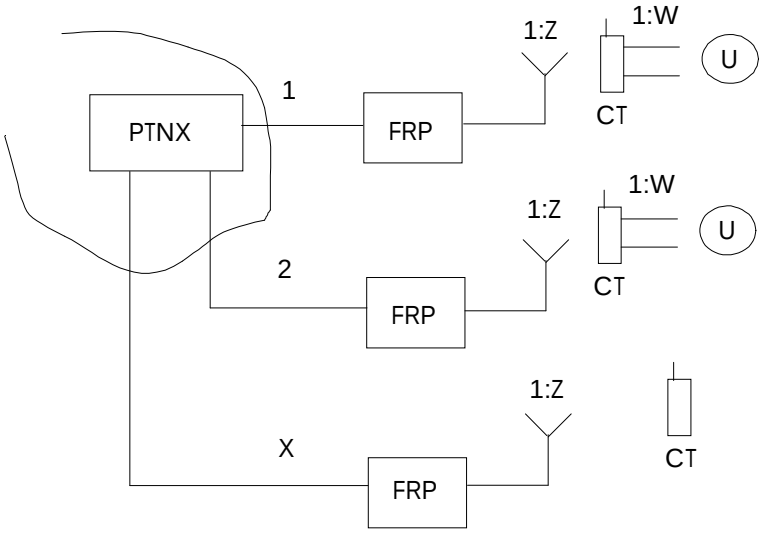


Figure 7: PTN supporting mobility

The following functional requirements may also have an impact on the addressing and routeing mechanisms of the PTN:

- any PUM user may log-on at a terminal anywhere in the network;

- a CT may appear at any FRP at any time. This is also possible during an active call, i.e. the CT's address changes and is not fixed to a particular geographical location;

- it is most likely that mobility will be implemented gradually in existing PTNs. From the network operator point of view, it may not be acceptable to totally rearrange or even change the existing PTN NP in order to provide this feature. This implies that a DN will be given to a CT as if it was a normal wired terminal of that PTNX and therefore calls to this CT will be initiated by dialling its DN;

- as the CT moves around in the network. the PTN number derived from the DN no longer reflects its current physical location. Therefore, unlike a call to a wired terminal, the routeing of a call to a CT cannot be decided entirely by the analysis of the dialled number. However, the PTN number should point to the PTNX where further information about the current location can be found. Therefore each call initiated in a PTNX to the same CT may follow a different route through the PTN.

The content of the PTN number is indicated in ETS 300 189 [6] subclause 7.1. In order to ease the reading of this TCR-TR, the relevant parts of this subclause have been copied into this TCR-TR.

Number information can be presented in two formats, the explicit and the implicit format. In both formats the number digits shall be accompanied by a Type of Number (TON) value, in accordance with table 1.

Table 1: TON values for the E.164, PNP and Unknown NP indications

Explicit Format NPI = E.164	**Explicit Format NPI = PNP**	**Implicit Format NPI = Unknown**
International Number	Level 2 Regional Number	
National Number	Level 1 Regional Number	
Subscriber Number	Local Number	
Partial Number (NOTE 1)	Partial Number (NOTE 1)	
Unknown (NOTE 1)	Unknown (NOTE 1)	Unknown (NOTE 2)
	PTN specific Number (NOTE 3)	
	Abbreviated Number (NOTE 3)	

NOTE 1: In the standard on the DSS1 of public and private ISDNs (ETS 300 102 and ETS 300 192), the TON values Unknown and Partial Number share the same code points. Distinction is made by the direction of number information flow:

At the boundary between the public ISDN and a PTNX the meaning for Selection Number is "Unknown" if the information flow is to the public ISDN, and the meaning is "Partial" if the information flow is from the public ISDN (i.e. in the context of DDI). For Identification Numbers the allocation of the meaning are reversed.

At the boundary between the private ISDN and its terminals the meaning for Selection Number is "Partial" if the information flow is from the private ISDN to the terminal (i.e. in the context of MSN), and the meaning is "Unknown" if the information flow is from the terminal to the PTNX. For Identification Numbers the allocation of the meanings are reversed.

NOTE 2: The number digits follow an implicit numbering plan and can include prefixes.

NOTE 3: The use of this type of number is under the control of the PTN authority and beyond the scope of this TCR-TR.

In the explicit format the Numbering Plan Identifier (NPI) shall have a value other than "UNKNOWN". The TON shall be set to either "UNKNOWN" or to any of the other values specified for the NPI concerned. Except where the TON is set to "UNKNOWN", the number digits shall not include prefixes.

In the implicit format the NPI shall have the value "UNKNOWN". The TON shall only take the value "UNKNOWN". If applicable, the number digits shall include prefixes, according to the implicit numbering plan employed.

7.2 User and network operator requirements

The CTM and PUM services should not impose any additional restrictions upon the numbering and addressing schemes of the PTN. The PTN extension user should have the possibility of retaining his or her extension number when changing between wired, CTM and PUM services. There should consequently be no need to allocate specific number series or prefixes for the CTM and PUM users and the related network entities. This should however not prevent a private network operator from arranging the PTN NP in such a way that CTM and PUM users are indicated by either a prefix or specific number series.

For the PUM service the possibility of registering several PUM users on one (cordless or wired) terminal should be allowed.

7.3 CTM numbering and addressing

7.3.1 General

The new entities required to support CTM are as follows:

- the cordless terminal (CT);
- the home data base (HDB);
- the visitor data base (VDB);
- the fixed radio part (FRP).

The purpose of the PTN NP is to make it possible to assign an unambiguous identity (i.e. address) to each of the entities which need to inter-communicate.

NOTE: It is not always necessary for communicating entities to have PTN numbers. For example an FRP does not need a PTN number if its PTNX uses internal addressing mechanisms to associate CTs with FRPs. However, for some applications it might be necessary to assign a PTN number to a functional entity which is contained within an FRP, e.g. an authentication entity. In such cases the FRP could be considered to have a PTN number.

It is, however, very likely that some additional information needs to be sent across the interface between the FRP and the PTNX. This additional information will only be used by the FRP and as such is irrelevant to the PTNX. However, the PTN may be required to store, retrieve and transport the information.

Basically two methods for addressing CTs beyond the PTNX access point are foreseen.

Firstly the CT's number can be sent over the interface between the FRP and the PTNX. This requires, however, that the radio parts (or the handsets) contain some sort of analysing function and a local data base which can relate the CT's number to the local radio identity. In this case the FRP can be considered similar to a PTNX from an addressing point of view (but not concerning the switching function). This method requires that both the CT's number and the PTNX access address are sent via the network.

Another method is to terminate the call to the CT at the FRP's access point in the PTNX and then to send the additional radio information across the PTNX-FRP interface. This method does not require an analysing functionality in the FRP, but does require the radio addresses to be sent over the PTN.

For both methods the CT's number is part of the PTN NP, but it will be necessary to develop functions which can associate the PTN number derived from the DN to the PTN number of the CT's current access.

7.3.2 Contents of the number digits in the PTN NP

The CT's PTN number should comprise a sequence of decimal digits as specified in ETS 300 189 [6]. Addressing of CTs should not make use of sub-addressing.

7.3.3 Structure of PTN NP

ETS 300 189 [6] allows a PTN NP to be hierarchically organised into regions by use of TON values (see table 1). It is for further study to identify how ETS 300 189 [6] can be used to identify the CTM entities (CT, HDB, VDB and FRP), e.g. by the use of TON values.

7.4 PUM numbering and addressing

The PUM number should comprise a sequence of decimal digits as specified in ETS 300 189 [6].

The following items have been identified as requiring further study:

- the entities needed for PUM in a PTN should be identified in order to see which of them need to have a PTN number;
- the PUM number shall be a number of the PTN NP. No special number series or prefixes should be required for PUM;
- the relation between the numbering of CTM and PUM should be investigated (i.e. similarities and differences should be identified);
- possible service interactions for PUM should be investigated (e.g. diversion).

7.5 Routeing

7.5.1 General principles

The general routeing principles of user and terminal mobility are based on the routeing principles described in ECMA TR/57 [16], but this document does not specifically cover the mobility aspects. For this reason, new concepts have been introduced, such as using the registration feature of the users and terminal as well as the location registration of the mobile terminals.

The routeing processes of mobility management use the concept of Home Data Bases and Visitor Data Bases for the storage of location information of users and terminals.

For the management of terminal mobility, the radio accesses of the PTN are grouped into Location Areas (LAs). A location area is a domain in which a CT may receive and/or make calls as a result of a single location registration by changing the location area. In a location area a CT can be searched for so that it can be informed of an incoming service, e.g. an incoming call. Several location areas may be combined into a Visitor Area (VA). A visitor area is related to a Visitor Data Base (VDB) which contains some information items (e.g. identity, access rights) of the CTs which are situated in this area, and the identity of the location area in which the CTs have to be searched for. The concept of VDB can also be used for user mobility.

The concept of Home Data Base (HDB) is used for both user and terminal mobility. An HDB contains the complete information set of all the terminals or the users belonging to this HDB (e.g. access rights, service profile etc.). The HDB also contains the current location of the users (e.g. the identity of the CTs on which the users are registered or the access addresses of the users) and the current location of the CTs (e.g. the access address or the identity of the VDB corresponding to the visitor area in which the CTs are located).

PTN routeing mechanisms should include the routeing of the call-related information as well as the routeing of the call-independent information, such as the registration of the users on a CT and location registration messages of the CTs.

7.5.2 Data Bases

If an update of the visiting CT's HDB is necessary, or the HDB needs to be accessed, then the CT shall provide its DN or any suitable identity that clearly identifies its HDB to the visited PTNX VDB. The PTNX shall then establish a connection with the HDB according to QSIG. The updating procedures of the HDB and VDB are for further study.

The content of the HDBs and VDBs needs to be defined and this is for further study.

7.5.3 Example of routeing processes

7.5.3.1 Routeing of call-independent information

The registration of a user on a terminal, shall be activated by the user. The registration information is sent by the terminal to the corresponding HDB (and if necessary to the corresponding VDB). This requires that the network shall be able to determine the address of the HDB of a user by means of the user's PTN number.

For location registration of a CT, the CT shall send the location registration information either automatically or by a manual action by the user on the terminal. This information is sent at first to the VDB corresponding to the area in which the terminal is located. If the terminal is not already registered in this VDB the location registration information shall also be sent to the corresponding HDB. This process requires that the network shall be able to find the address of the HDB of a terminal by means of the terminal's PTN number.

7.5.3.2 Routeing of calls and call-related information

A user initiates a call towards another user by dialling the DN of this user. The terminal or the network analyses the DN and transforms it into the corresponding PTN number.

For an incoming call to a user, the network has at first to locate the terminal on which the called user is registered. The location enquiry may begin in the VDB corresponding to the network access from which the setup message accesses to the PTN. If the enquiry to the VDB is unsuccessful, the enquiry is sent to the HDB corresponding to the called user. If the called user is registered on a wired terminal, the usual routeing process is applied. For an incoming call to a CT, the CT has to be located by using the location information stored in the VDB and HDB. This process requires the network to be able to determine the address of the HDB of the user and the terminal from the PTN number of the user and of the terminal.

Two methods of routeing to CTs and PUM users have been identified: the rerouteing method and the forward switching method.

In the rerouteing method the network will perform a new routeing from the calling party to the destination after the current location has been retrieved from the HDB.

In the forward switching method the network's routeing algorithm joins the incoming call (at the PTNX containing the HDB) to an outgoing call path to the destination PTNX.

The rerouteing method seems to be more suitable for situations where a large number of CTs and PUM users are not located at their home PTNX.

8 Scenarios

8.1 Introduction

The provision of PUM and CTM requires extra functionality within the PTN. This Clause assumes that this extra functionality is provided by the FRP and HDB/VDB functional entities.

The purpose of this Clause is to describe various scenarios for the location of the functional entities in a PTN which supports either CTM or PUM or both. These scenarios are further examined to identify those which would benefit from standardisation. The aim is not to present an exhaustive study of all possible scenarios, but only to give some examples of the main procedures, e.g. registration of users, location registration of terminals and call setup.

There are a number of possibilities for the implementation of a PTN providing CTM and PUM. These are illustrated in figure 8 which shows a physical structure of a PTN with ISPBX/ISCTXs, radio exchanges (RE) and radio base stations (RBS).

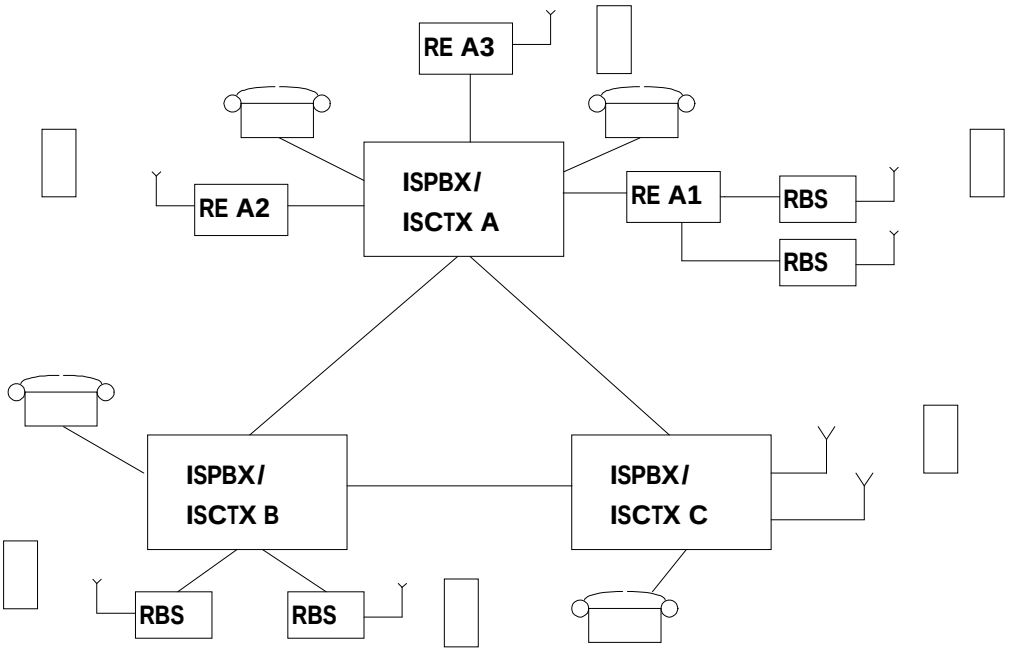


Figure 8: Example of physical structure of a PTN

ISPBX/ISCTX A is connected to RE A1 which in turn is connected to two RBSs. Here the ISPBX/ISCTX contains the PTNX functions and RE A1 and its RBSs together contain the FRP functions. In this case the interface between ISPBX A and RE A1 is a physical interface at the alpha reference point.

ISPBX/ISCTX A is also connected to RE A2. Here the ISPBX/ISCTX contains the PTNX functions and the RE contains the FRP functions. The interface between ISPBX/ISCTX A and RE A2 is also a physical interface at the alpha reference point.

ISPBX/ISCTX B is connected to two RBSs. Here the ISPBX/ISCTX contains the PTNX functions and also some of the FRP functions. The rest of the FRP functions are contained in the RBSs. In this case there is no physical interface at the alpha reference point.

ISPBX/ISCTX C is shown without any supporting REs or RBSs. Here the ISPBX/ISCTX contains the PTNX functions and the FRP functions. ISPBX/ISCTX C also has no physical interface at the alpha reference point.

Considering the standardisation of the signalling between the various PTN components two basic approaches have been identified:

- the mobility concept is defined by a fixed and well defined functional split between the various PTN components and as a consequence a specific protocol between the components is also defined;

- the functional split between the various PTN components is not uniquely defined. In this case the signalling protocol between the components should support different implementation variations.

The different possibilities for the distribution of the mobility related functions inside the PTN are given in subclause 8.2.

Subclause 8.3 gives examples of the location updating procedure of a CT, the registration procedure of a PUM user, and call setup procedures for PUM and CTM.

8.1.1 CTM

In the case of CTM, the coverage area of a PTN is logically divided into a number of Location Areas (LA). A location area is a part of the coverage area in which a cordless terminal may make or receive calls as a result of a single location registration. Each LA is identified by a LA Identifier (LAI).

A terminal initiates a location registration request when it has determined from the LAI that its location area has changed. In a location area a CT has to be located before it can be informed of an incoming service, e.g. an incoming call.

Several location areas may be combined into one Visitor Area (VA). Each VA is identified by a VA Identity (VAI).

The maximum size of a VA is one PTNX. The possibility that the VA exceeds the size of a PTNX is for further study.

The case that a LA is less than the coverage area of one FRP is not visible to the PTNX and is therefore not dealt within this TCR-TR.

For the case that one LA is identical with the coverage area of one FRP, the routeing of a call to a CT is performed by routeing the call to the indicated FRP. If however the physical size of the LA is small, a roaming CT will initiate frequent location registration requests.

For the case that one LA covers several FRPs, then the routeing of a call to a CT will require a search procedure (such as polling) which enables the PTNX to determine to which FRP the CT is connected.

Both of these cases have advantages and disadvantages, and it is left for further study to determine if both cases are to be included in CTM standards.

The minimum size of a LA is the coverage area of one FRP and the maximum size is one VA.

For the management of terminal mobility, the concept of HDB/VDB is applied. Each CT has a Home Data Base (HDB). The HDB contains all relevant information to provide PTN services to the CT. This information includes static information such as the CTs class of service and service profile, and dynamic information such as the CTs current location (i.e. the CT's VA). An HDB may hold information for a number of CTs belonging to the PTN.

A visitor area is related to a Visitor Data Base (VDB) which contains some information items (e.g. identity, access rights and current LA) of the terminals which are temporarily situated in this area.

The relationship between the HDB and VDB functional entities and the Visitor Area and Location Area concepts is shown in figure 9.

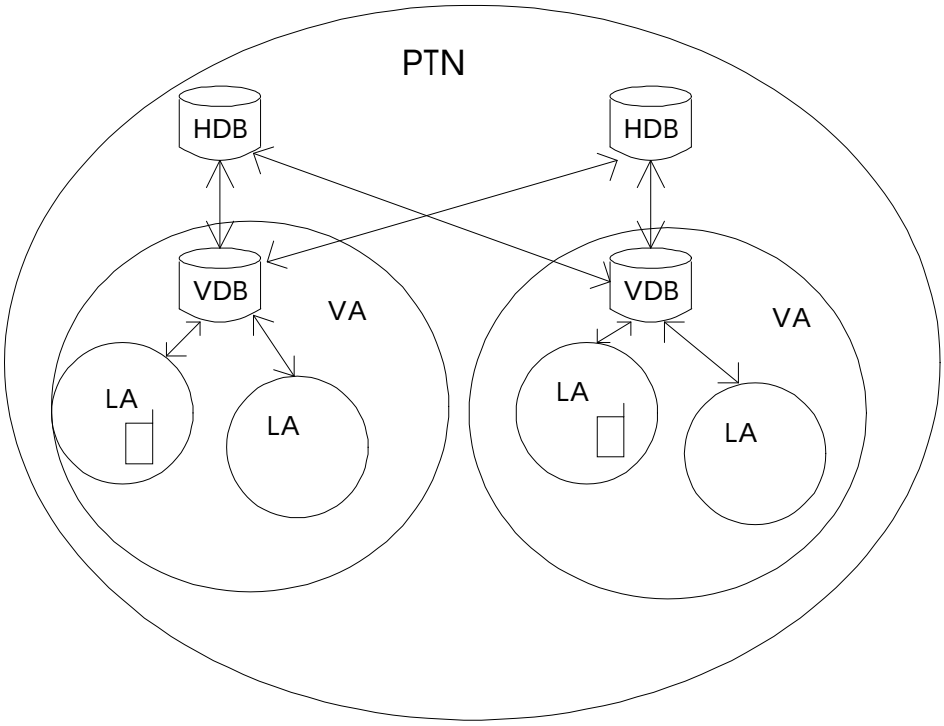


Figure 9: Example of relation between HDB, VDB, VA and LA in a PTN

8.1.2 PUM

For the management of PUM, the concept of HDB/VDB is applied. The use of location area is not necessary for PUM since a PUM user is located at one terminal.

In the case of PUM the terminals can be wired and cordless. For this reason a new term PTI (Private Terminal Identity) has to be introduced instead of the CTI (Cordless Terminal Identity). In the case of a cordless terminal the PTI is the same as the terminals CTI. In the case of a wired terminal the PTI is the same as the terminals PTN number.

8.2 Scenario criteria

The procedure for the realisation of the mobility features is one of the scenario criteria.

The other criteria are the allocation of the functions to the network components (e.g. FRP, PTNX, VDB, HDB) and the terminals.

Some capabilities of the network components, like the call handling, are also important criteria of the scenarios.

8.2.1 PUM features

For further study.

8.2.2 CTM features

8.2.2.1 Identification

- Identification of the FRP by the CT:
    - always realised in the CT.
- Identification of the CT. The identification can be done:
    - either decentral inside the FRPs (the identification of the terminals can be done directly inside the FRPs but the identity of every terminal has to be stored inside the FRPs); and/or
    - by the corresponding VDB entity of the Visitor Area (the identification information of the CT corresponding to this VDB is stored in the VDBs entity and a signalling procedure is necessary between the CT and the VDB entity via the FRP); or
    - by the HDB entity (the identification information is stored in the HDBs and a procedure has to be defined between the CT and the corresponding HDB entity via the FRP).

8.2.2.2 Automatic location registration / deregistration

Location registration may be performed by the CT and informs the network about the CT's current LA. The execution of the function by the CT also discloses that the CT is present in the network and may be accessible.

This function can be activated:

- either regularly by the CTs, i.e. the frequency spectrum has to support a considerable traffic load because of the messages sent by the CTs; or
- when the CTs change the location area, i.e. the CTs have to be searched inside the whole location area.

8.2.2.3 Terminal handover

Only external handover, that is handover between FRPs, is considered in this TCR-TR. FRP internal handover is invisible at the alpha reference point and is therefore not further considered. The FRPs could be in the same PTNX or in different PTNXs. Handover between FRPs in different PTNXs would require support by the inter-PTNX signalling protocol. Due to the limited need, the complexity of the signalling and the critical time issue, handover between FRPs at different PTNXs are excluded in this TCR-TR.

No scenario is given for handover. This is for further study.

8.2.2.4 Authentication functions

- Authentication of the FRP by the CT:
    - always in the CT.
- Authentication of the CT. The authentication of a CT can be done:
    - either in the FRPs, i.e. the information and algorithms necessary for the authentication have to be stored in the FRPs; or
    - by the corresponding VDB entity, i.e. an authentication procedure between the terminal and the VDB entity has to be defined and the signalling between the FRP and the VDB entity has to support this procedure; or
    - by the HDB entity, i.e. an authentication procedure between the terminal and the HDB entity has to be defined and the signalling between the FRP and the HDB entity has to support this procedure.

8.3 Signalling aspects

In this Clause some signalling aspects will be analysed on some examples. Because of the high numbers of possible solutions only the location registration and call setup are at first taken into consideration as mobility feature. Furthermore, in each scenario different solutions are possible for the realisation of the procedures. The described procedures are only given as examples.

In the scenarios the FRP, HDB and VDB are separate functional entities. It is assumed that the FRP is separated from any switching function.

The messages are only of illustrative character and may depend on the protocol which will be used later inside the PTN. It is expected that the protocols used inside a PTN will be based on SSIG, ETS 300 192 [12] and QSIG, ETS 300 172 [13].

8.3.1 Cordless terminal mobility

For the location registration (or location updating) of the cordless terminals two types of procedures are possible:

Scenario 1:

The FRPs broadcast periodically messages containing the location information, particularly the LAI. A CT activates a location updating procedure when it detects having entered a new LA (the received LAI' has changed).

Scenario 2:

In this scenario the PTN knows when the CT is not reachable. This can be done by e.g. the CTs sending periodically <<LOCATE-REQUEST>> messages via the FRP to the VDB of the VA, or by a polling of the CTs realised regularly by the FRPs. It is not necessary with a search procedure amongst the FRPs in the case of an incoming call. It has to be noted that a regularly sending of location updating messages produces a traffic load on the system.

8.3.1.1 Scenario 1

The FRPs transmit periodically broadcast messages containing location information, particularly the LAI (Location Area Identity), see figure 10.

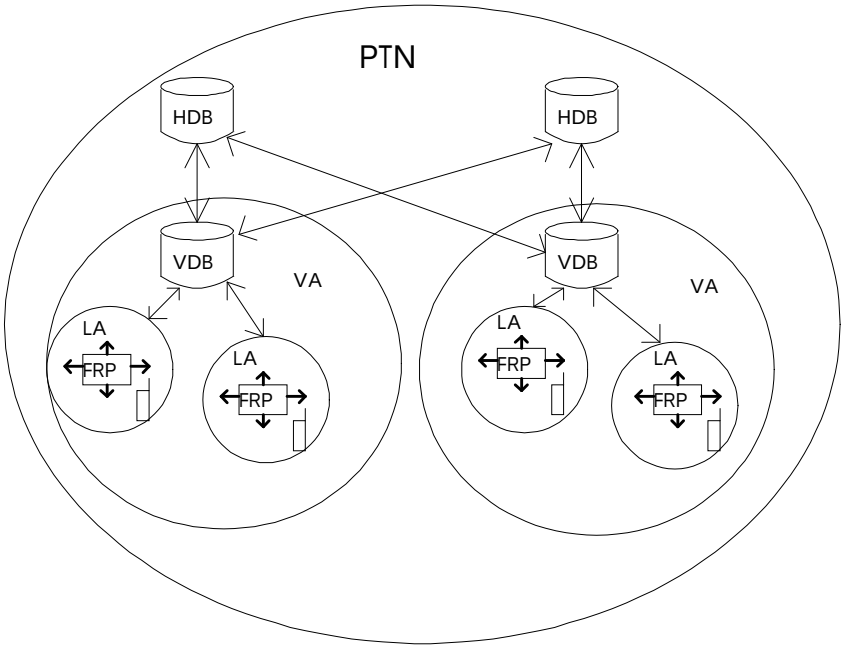


Figure 10: Scenario 1

8.3.1.1.1 Location updating procedure

The CT activates a location updating procedure (see figures 11 and 12) when it detects having entered a new LA (the received LAI' sent by the FRP has changed).

Case 1: The two LAs are situated in the same VA (figure 11)

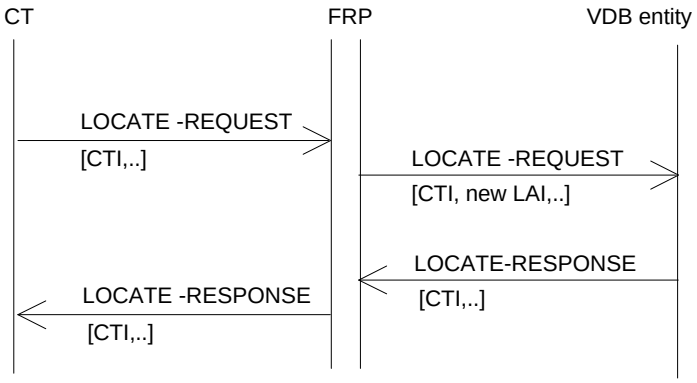


Figure 11: Case 1 of location updating of a cordless terminal

- A <<LOCATE-REQUEST>> message containing e.g. the CTI is sent to the FRP by the CT.
- This <<LOCATE-REQUEST>> message containing e.g. CTI and the new LAI, is sent to the VDB entity by the FRP. The VDB entity updates the location of the terminal.
- A <<LOCATE-RESPONSE>> message is sent to the FRP by the VDB entity.
- This <<LOCATE-RESPONSE>> message is sent to the CT by the FRP.

Case 2: The two LAs are situated in two different VAs (figure 12)

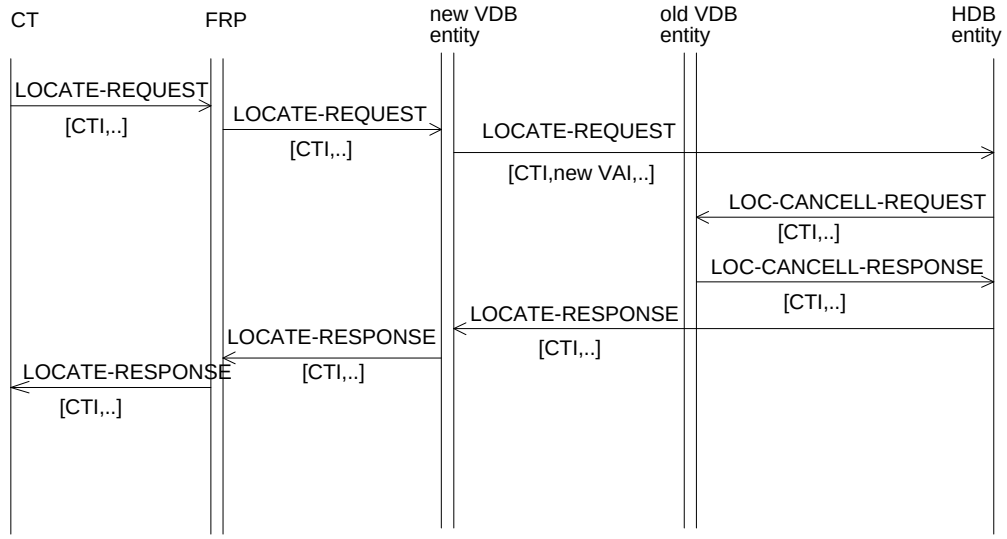


Figure 12: Case 2 of location updating of a cordless terminal

- A <<LOCATE-REQUEST>> message containing e.g. the CTI and the identity (or the address) of the corresponding HDB is sent to the FRP by the CT.
- This <<LOCATE-REQUEST>> message is sent to the VDB entity by the FRP.
- The new VDB informs the HDB of the new location (LAI') of the CT by sending a <<LOCATE-REQUEST>> message.
- The HDB sends a <<LOCATE-CANCELLATION-REQUEST>> message to the old VDB entity.
- The old VDB entity answers by sending a <<LOCATE-CANCELLATION-RESPONSE>> message to the HDB.
- The HDB entity answers to the new VDB entity by sending a <<LOCATE-RESPONSE>> message containing some data (e.g. access rights) on the CT to the new VDB entity.
- The new VDB entity sends a <<LOCATE-RESPONSE>> message to the FRP.
- The FRP sends a <<LOCATE-RESPONSE>> message to the CT.

8.3.1.1.2 Call setup procedures

When receiving a <<SETUP>> message, containing the identity of CT B, from the calling CT A via FRP A, the VDB entity checks if CT B is situated in its visitor area.

Case 1: The CTs are situated in the same VA

This case will not have any impact on the Q reference point, it is a PTNX internal case. This is due to the restriction that the maximum size of a visitor area is one PTNX.

Here it is assumed that the originating PTNX checks the local VDB before routeing the call to other PTNXs. The PTN number of the roaming CT is found in the VDB and the call may be established locally in the PTNX. If this local VDB check is not done, case 1 equals case 2 from an information flow point of view.

Case 2: The CTs are situated in two different VAs

In this case two different routeing procedures are considered:

- forward switching: the network routeing algorithm joins at the PTNX containing the HDB of the B-party the incoming call path with an outgoing call path to the destination PTNX;

- rerouteing: the network routeing algorithm will perform a new routeing from the A-party to the destination after the current location of the B-party has been retrieved from the HDB.

The call from the originating PTNX to the HDB may be established with or without a B channel. If the originating PTNX can not distinguish between a call to a normal "fixed" phone and a call to a CT, the call will be with a B channel ("normal call setup"). If the CTs can be identified from the dialled number the call to the HDB may be done as an location information retrieval procedure without a B channel.

Forward switching (figure 13):

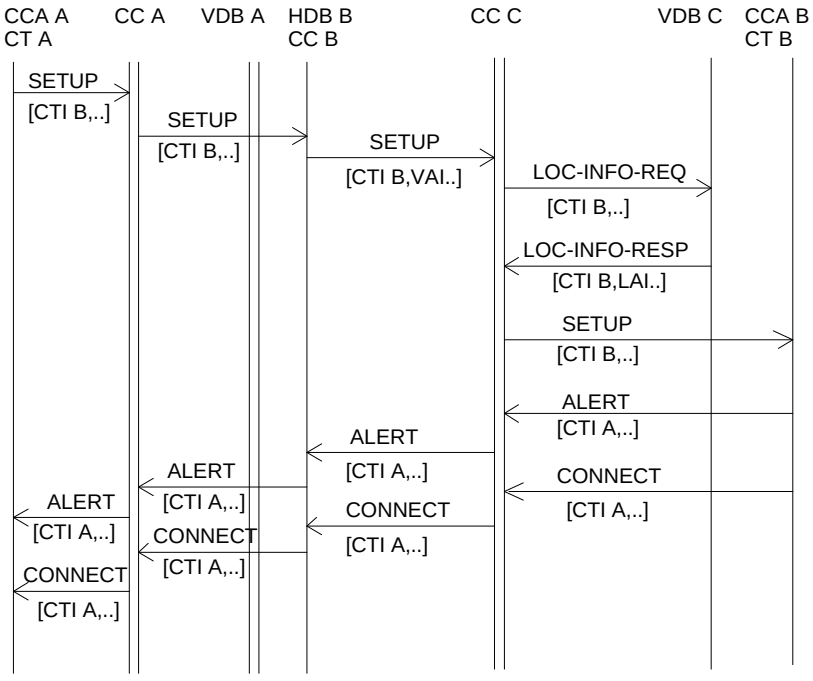


Figure 13: Scenario 1, call setup case 2: two CTs in different VAs, routeing mechanism is forward switching

- CCA A sends a <<SETUP>> message containing CTI B to CC A.
- CC A sends the <<SETUP>> message to the HDB corresponding to CT B.
- CC B sends the <<SETUP>> message containing CTI B and VAI C to CC C.
- CC C sends a <<LOC-INFO-REQ>> message to VDB C.
- VDB C answers with a <<LOC-INFO-RESP>> message containing a LAI, to CC C after having located CT B to one LA.
- CC C sends the <<SETUP>> message to CCA B.
- CCA B sends an <<ALERT>> message to CC C.
- CC C sends this <<ALERT>> message to CC B.
- CC B sends this <<ALERT>> message to CC A.
- CC A sends this <<ALERT>> message to CCA A.
- CCA B sends a <<CONNECT>> message to CC C.
- CC C sends this <<CONNECT>> message to CC B.
- CC B sends this <<CONNECT>> message to CC A.
- CC A sends this <<CONNECT>> message to CCA A.

Rerouteing (figure 14):

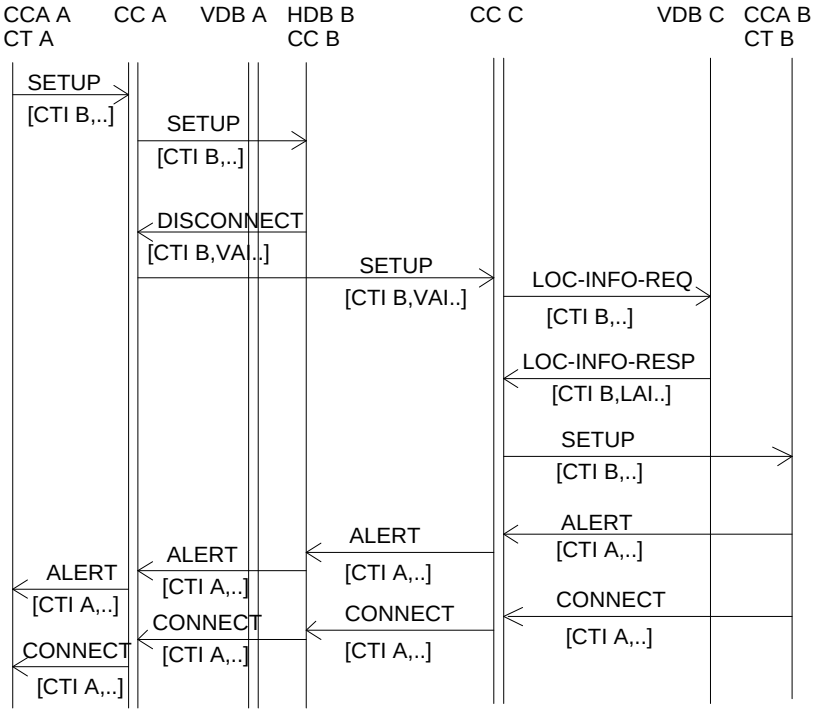


Figure 14: Scenario 1, call setup case 2: two CTs in different VAs, routeing mechanism is rerouteing

- CCA A sends a <<SETUP>> message containing CTI B to CC A.
- CC A sends the <<SETUP>> message to the HDB corresponding to CT B.
- HDB B returns the identity of the actual VDB where CT B is located (VAI) in a <<DISCONNECT>> message to CC A.
- CC A sends the <<SETUP>> message containing e.g. CTI B and VAI, directly to CC C.
- CC C sends a <<LOC-INFO-REQ>> message to VDB C to get information of the location of CT B.
- VDB C answers with a <<LOC-INFO-RESP>> message containing e.g. CTI B and LAI, to CC C after having located CT B.
- CC C sends the <<SETUP>> message to CCA B.
- CCA B sends an <<ALERT>> message to CC C.
- CC C sends this <<ALERT>> message to CC A.
- CC A sends this <<ALERT>> message to CCA A.
- CCA B sends a <<CONNECT>> message to CC C.
- CC C sends this <<CONNECT>> message to CC A.
- CC A sends this <<CONNECT>> message to CCA A.

8.3.1.2 Scenario 2

The PTN knows the location of the CTs.

The same location updating and call setup procedures as in scenario 1 can be applied, i.e.:

- the location updating is exactly the same (see figures 11 and 12);

- the call setup procedure is the same too (see figures 13 and 14), but a search of the CT inside a location area is no more necessary. The VDB or the HDB entity sends immediately the location address of the CT B to the call control entity of the PTNX.

8.3.2 Private user mobility

The case that a PUM user registers on a cordless terminal is for further study. No information diagrams are therefore given for this case.

The PTI might be provided (by different means) to the VDB in the case of a registration request either by the terminal itself, the network node or the PUM user of the terminal.

The described procedures are only examples.

The procedures for registration of a PUM user and call setup initiated by a PUM user, will depend on if only one VDB is involved or if different VDBs are involved. These two cases are described for PUM user registration and call setup.

8.3.2.1 Registration procedure

- The PUM user registers on a terminal.

- The terminal sends a <<REGISTRATION-REQUEST>> message to the PTN containing e.g. the PUM number of the PUM user, the PTI of the terminal, or the indication of the concerned PUM feature (e.g. registration for incoming or for outgoing calls).

- The VDB-entity of the area checks if the PUM user is already registered on a terminal of this area and registers the PUM user on the new terminal.

Case 1: Same VDB (figure 15)

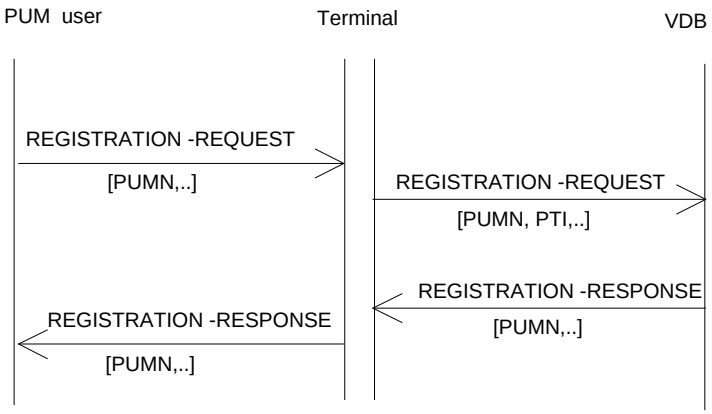


Figure 15: PUM user registration, case 1: same VDB

- The VDB sends a <<REGISTRATION-RESPONSE>> message to the terminal.
- The terminal informs the PUM user of the <<REGISTRATION-RESPONSE>>.

Case 2: Change of VDB (figure 16)

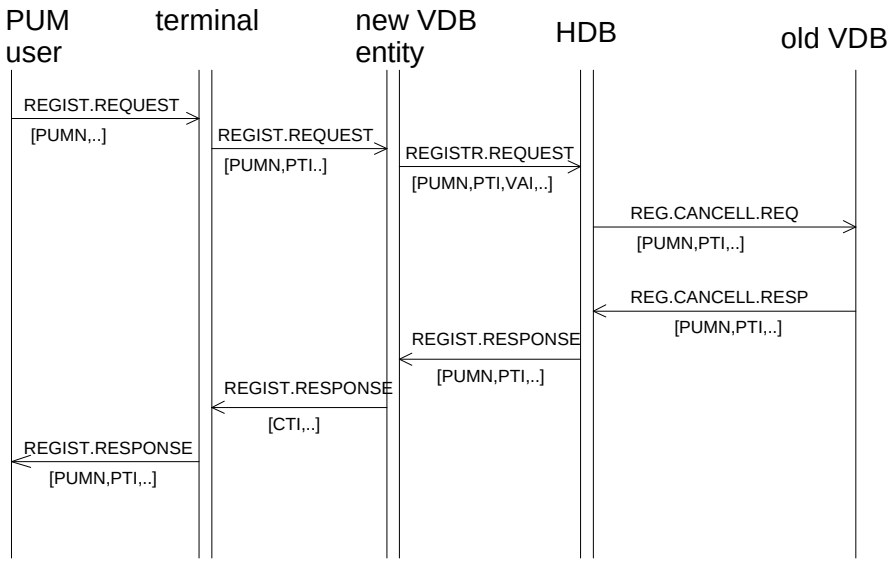


Figure 16: PUM user registration, case 2: change of VDB

- The new VDB sends a <<REGISTRATION-REQUEST>> message to the HDB.
- The HDB updates the registration of the PUM user, i.e. stores the identity of the visitor area in which the PUM user wants to be registered, and sends a <<REGISTRATION-CANCELL-REQUEST>> to the old VDB in which the PUM user is already registered for cancelling this registration.
- This old VDB cancels the registration of the PUM user and sends a <<REGISTRATION-CANCELL-RESPONSE>> to the HDB to confirm the cancellation.
- The HDB sends a <<REGISTRATION-RESPONSE>> to the new VDB.
- The new VDB sends a <<REGISTRATION-RESPONSE>> to the terminal.
- The terminal informs the PUM user of the <<REGISTRATION-RESPONSE>>.

8.3.2.2 Call setup procedures

- The calling PUM user A initiates a "SETUP" on terminal A.

- Terminal A sends a <<SETUP>> message containing e.g. the PUMN B of the called PUM user B, the identity of terminal A (PTI A) and some information like the required service to CC A.

Case 1: The PUM users are registered in the same VDB

In the case that PUM user A and PUM user B is registered in the same VDB-users, the call setup will be established locally in the PTNX. This case will not have any impact on the Q reference point. No information diagrams are given.

Case 2: The PUM users are not registered in the same VDB

Two different routeing procedures are also considered for the PUM case.

Forward switching (figure 17):

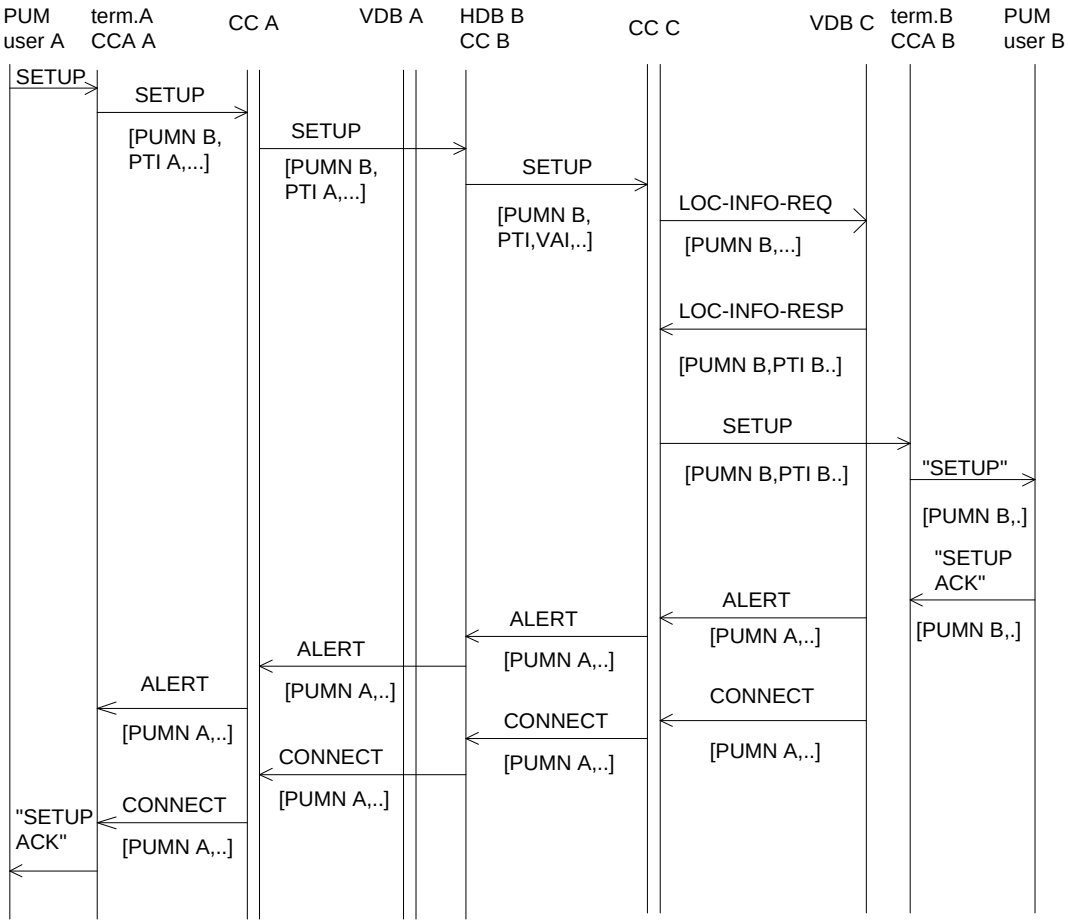


Figure 17: Call setup, the two PUM users are registered in different VDBs, the routeing mechanism is forward switching

- CC A sends the <<SETUP>> message to the HDB corresponding to PUM user B.
- CC B sends the <<SETUP>> message containing PUMN B, PTI A and VAI C to CC-C.
- CC C sends a <<LOC-INFO-REQ>> message to VDB C to get information about at which terminal PUM user B is registered.
- VDB C answers with a <<LOC-INFO-RESP>> message containing e.g. PUMN B and PTI B, to CC C.
- CC C sends the <<SETUP>> message to CCA B.
- CCA B informs PUM user B of the incoming call.
- PUM user B activates a "SETUP ACK" to CCA B.
- CCA B sends an <<ALERT>> message to CC C.
- CC C sends this <<ALERT>> message to CC B.
- CC B sends this <<ALERT>> message to CC A.
- CC A sends this <<ALERT>> message to CCA A.
- CCA B sends a <<CONNECT>> message to CC C.
- CC C sends this <<CONNECT>> message to CC B.
- CC B sends this <<CONNECT>> message to CC A.
- CC A sends this <<CONNECT>> message to CCA A.
- CCA A informs PUM user A of the "SETUP ACK".

Rerouteing (figure 18):

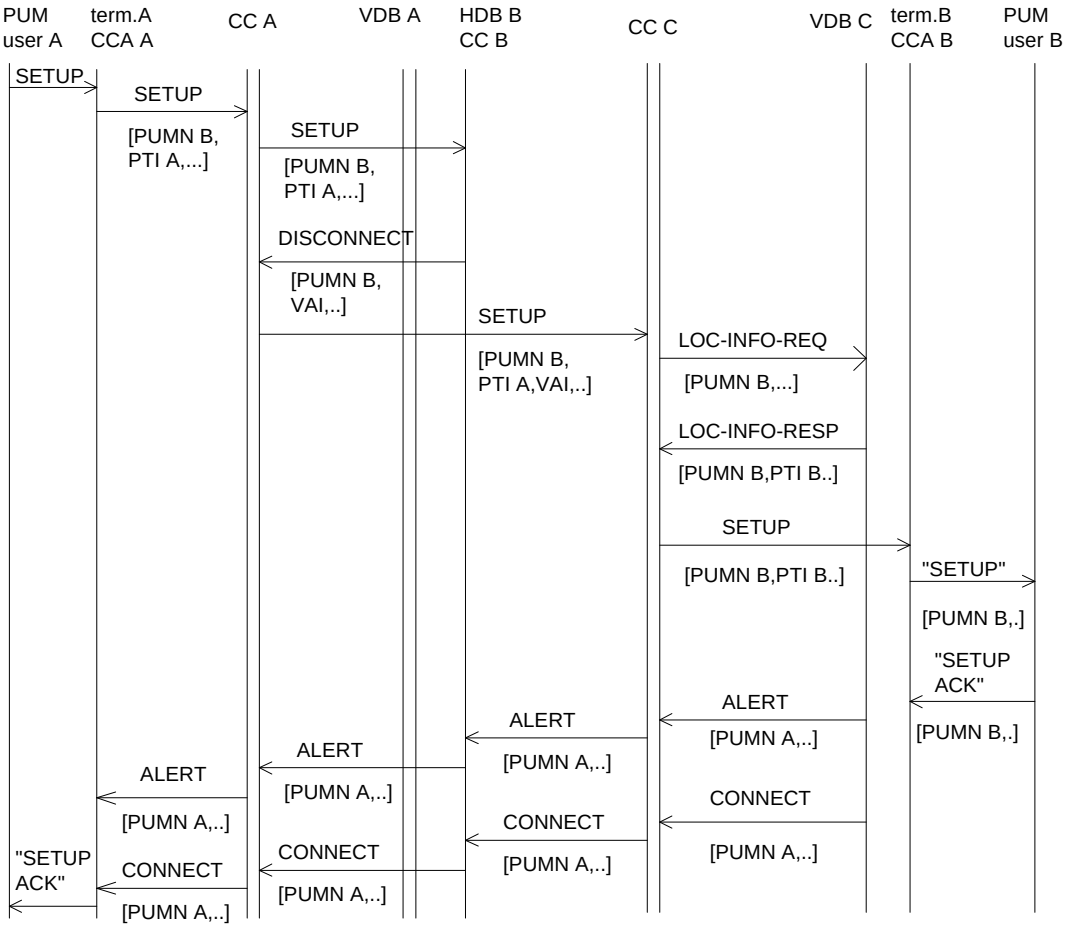


Figure 18: Call setup, the two PUM users are registered in different VDBs, the routeing mechanism is rerouteing

- CC A sends the <<SETUP>> message to the HDB corresponding to PUM user B.
- HDB B returns the identity of the actual VDB where PUM user B is located (VAI C) in a <<DISCONNECT>> message to CC A.
- CC A sends the <<SETUP>> message containing e.g. PUMN B, PTI A and VAI C, directly to CC C.
- CC C sends a <<LOC-INFO-REQ>> message to VDB C to get information about at which terminal PUM user B is registered.
- VDB C answers with a <<LOC-INFO-RESP>> message containing e.g. PUMN B and PTI B, to CC C.
- CC C sends the <<SETUP>> message to CCA B.
- CCA B informs PUM user B of the incoming call.
- PUM user B activates a "SETUP ACK" to CCA B.
- CCA B sends an <<ALERT>> message to CC C.
- CC C sends this <<ALERT>> message to CC A.
- CC A sends this <<ALERT>> message to CCA A.
- CCA B sends a <<CONNECT>> message to CC C.
- CC C sends this <<CONNECT>> message to CC A.
- CC A sends this <<CONNECT>> message to CCA A.
- CCA A informs PUM user A of the "SETUP ACK".

Annex A: Cordless Terminal Identities/Numbers (DECT based)

The following description of the applicable parts of the DECT identity structure is an extract of ETS 300 175-6 [4]. Even if parts of this system is internal to the DECT systems, and as such is outside the scope of this TCR-TR, it may be necessary to implement functions in the HDB/VDB and PTNXs in a standardised way to store, retrieve, use and transfer these information elements throughout the PTN.

Refer to ETS 300 175-6 [4] for detailed information on the identity and addressing structure of the DECT system.

The DECT system provides a very strong and flexible radio access technology suitable for a large variety of private and public environments. The requirements on e.g. sub-system grouping, distribution, installation of equipment, quantity of units, identity allocations and "subscription" has been met by designing four access rights classes and a number of different types of IPUIs (see table A.1).

The common base for the DECT identity structure is the Access Rights Class (ARC) and the Access Rights Details (ARD). These shall be known both by the CTs and the fixed parts (see table A.2).

Table A.1: Combinations of identities ARI, PARK and IPUI

ARI class	Environment	PARK class	IPUI type
A	Residential and private PBX single and small multiple call systems	PARK-A	N, S
B	Private multiple cell PABXs	PARK-B	O, S, T
C	Public single and multiple cell systems	PARK-C	P, Q, R, S
D	Public DECT access to a GSM operator network	PARK-D	R

According to the intention of the DECT standards, Identity Class B is the one to be used for complex private installations and various types of multi cell PTNXs.

This class should therefore be the basis for the standardisation of PTN mobility as well.

This class also meets the requirements of being able to replace old equipment, install new units etc. without changing the ARIs and RFPIs. This means that the ARI-B is mainly a system identity that follows the system and not a specific equipment.

The meaning of the codes used in the table are:

EIC Equipment Installer's Code:

This value is allocated by ETSI to each manufacturer or supplier authorised by ETSI. Big companies can also have their own (or more than one?) EIC. The maximum value of the EIC is 65535.

FPN Fixed Part Number:

This value is distributed together with the EIC and has an upper limit of 255.

FPS Fixed Part Subnumber:

The FPS is assigned by the network operator or installer and has a maximum value of 15.

RPN Radio Fixed Part Number:

This value is allocated by the operator or installer and has a maximum value of 255.

NOTE: The number of RFPs per system can be larger than 255 through geographical separation.

Table A.2: Structure of ARI-B

	ARC	ARD			RPU
E 1 bit	B 3 bits	EIC 16 bits	FPN 8 bits	FPS 4 bits	RPN 8 bits
	ARI - B = 31 bits				
RFPI = 40 bits (including the E bit)					

In the fixed part the ARC+ARD is called ARI and in the CT it is called PARK.

The ARI, together with the Radio Fixed Part Number (RPN), is called the Radio Fixed Part Identity (RFPI). The RFPI is used to inform the CTs about the identity of the fixed side as well as the access rights to that particular system.

The CT identities, which consist of a PARK (PARK-B is used together with ARI-B and is shown in table A.3) and an International Portable User Identity (IPUI), serves two purposes:

- to enable the CT to select a valid DECT fixed part (PARK identity);
- to uniquely identify the CT within that DECT fixed part (IPUI identity).

Table A.3: Structure of PARK-B

ARC	ARD		
B 3 bits	EIC 16 bits	FPN 8 bits	FPS 4 bits

NOTE: The IPUI may be locally or globally unique. As this TCR-TR addresses a single network only, it is assumed that the IPUI is globally unique within the PTN. Note that the IPUI may be replaced by a temporary and shorter identity (TPUI). This value is, however, only relevant to the DECT system, but depending on the implementation it may be necessary to support the "handling functions" of the TPUI in the PTN and HDB/VDB.

The IPUI is an identity which has two elements. The Portable User Type (PUT), which defines the numbering plan PUN, and the Portable User Number (PUN). The IPUI uniquely defines one "user" within the domain defined by his access rights and may be locally or globally unique depending of the type of PUT (see table A.4).

Table A.4: Structure of CT identity type (IPUI)

PUT	PUN

At present, there are 7 types of IPUIs defined and the relevant IPUIs for private networks are as follows:

IPUI-S (PSTN/ISDN)

This is a globally unique identity, which can be used in all environments.

Table A.5: Structure of IPUI-S

PUT	PUN
S 4 bits	Number 60 bits

NOTE: The number is a coded PSTN or ISDN number (see CCITT Recommendation E.163 [18] and CCITT Recommendation E.164 [19]).

IPUI-O (Private)

This is a locally unique identity i.e. it shall be specified by the network operator or owner of a DECT fixed part and is only valid within that fixed part. It is mainly intended to be used for a PABX.

Table A.6: Structure of IPUI-O

PUT	PUN
O 4 bits	Number 60 bits

IPUI-T (Extended Private)

This is an identity intended to support roaming within and between private DECT networks run by the same network owner/operator. E.g. a big company with IPUI-O users can support roaming of their CTs between different sites in different locations and/or countries by adding an IPUI-T.

Table A.7: Structure of IPUI-T

PUT	PUN	
T 4 bits	EIC 16 bits	Number 44 bits

Equipment Installer's Code (EIC)
This code is allocated by ETSI to each manufacturer and has an upper limit of 65535. Large manufacturer and companies can have their own EIC(s) in order to facilitate roaming between different locations.

Number
This number is allocated by the network owner/operator and could be the CTs DN or PSTN/ISDN number or part of the CT's IPUI-O number, if unique for this use.

NOTE: The number is a coded PSTN/ISDN number (see CCITT Recommendation E.163 [18] and CCITT Recommendation E.164 [19]).

Example of DECT addressing structure mapped onto a PTN

The following example shows how the DECT addressing structure can be mapped onto PTN (see figure A.1). In this example the PTN may consist of:

FPN ---> = PTNX 255 PTNXs each with
FPS ---> = RE 16 Radio Exchanges each with
RPN ---> = FRP 255 Radio Fixed Parts (base stations).

This means that each PTNX can have (theoretically) 4 080 base stations assigned to each EIC (or 1 040 400 base stations in the whole PTN). However, the exact use of these values is an implementation dependent issue to be determined by the network owner/operator.

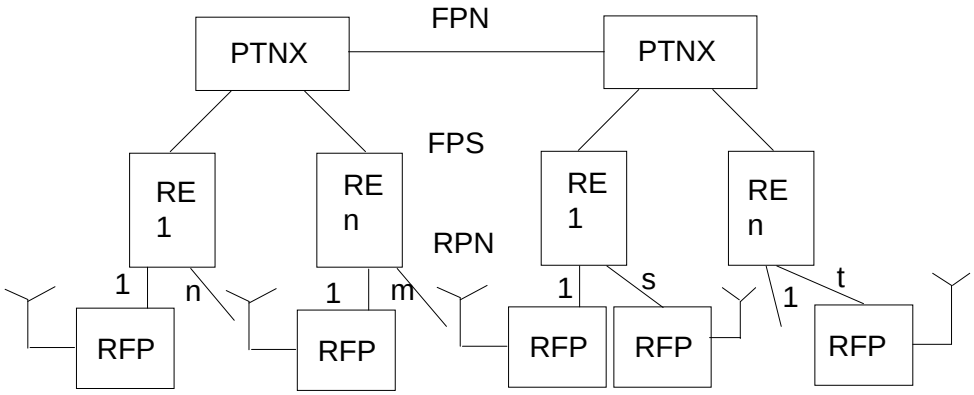


Figure A.1: Example of mapping of DECT identity structure on a PTN

Annex B: Use of Directory Services for mobility management in PTNs

One of the main technical issues for supporting mobility in public and private networks is the management of user data. For every user a personal set of data has to be stored and maintained somewhere in the network and this user profile has to be accessible from every point in the network the user can move to.

This annex discusses the use of standardised Directory Services (X.500) [25] for managing data in Private Telecommunications Networks (PTNs) offering mobility features.

B.1 Scenario

The following scenario is assumed as basis for the following discussions:

A PTN consists of multiple sites comprising a PTNX and possibly additional database entities that are interconnected to carry call traffic, call related signalling, and to perform mobility management operations. Each user has a personal number that is unique in the private network. Each user owns a user profile that describes e.g. his class of service, personal service parameters, identification parameters, and his current location area. The user profiles should be created and administered at the user's home site, i.e. they are kept local to the site where the user normally stays to maximise administrative autonomy of sites and to minimise signalling traffic between sites.

In this scenario, the following mobility management operations shall be performed:

0) Before the user may initiate and receive calls:

- The user profile has to be created and stored in a database. To minimise the signalling traffic, this should preferably done at the user's home site.

1) On incoming calls (i.e. the mobile user is called):

- The incoming call has to be routed to the user's current location.

- For this purpose, the user profile at the home site may have to be accessed to determine the actual location area identifier.

  Problem A: How is the home site that contains the user profile found from every point in the private network ? The access to the user profile has to be fast enough to offer an acceptable call-setup time.

2) On outgoing calls (i.e. the mobile user makes a call attempt):

- The user profile is accessed to retrieve e.g. the authentication parameters and to determine the allowed class of service for that user.

  Problem B: The user profile has to be readable from every place in the network. The access has to be fast enough to offer an acceptable quality of service.

3) If the user temporarily visits another location area:

- The new location area has to be informed and shall have access to the user profile.

- The user profile has to be updated with the new location area identifier.

- The old location area has to be cancelled i.e. it needs no longer access to the user profile

  Problem C: The home site has to be accessed and the user profile has to be modified with roaming information from every place in the network. This procedure has to be completed during the time the user needs for moving into the new location. In PTNs that consist of connected islands, this moving time will be much longer than in public mobile networks where users move with the velocity of a car between two location areas.

4) If the user moves for a long period to another PTN site:

- The new site should become the user's home site i.e. if possible his user profile should be moved to keep it in a local database in that site. This operation should not require the user to change his number.

  Problem D: It has to be possible to associate user profiles to other home sites without changing the user's number. One method to achieve this is to keep the personal number completely independent of topological constraints.

5) The user modifies his user profile:

- The user profile shall be modifiable from every place in the private network.

  Problem E: If the user profiles are replicated consistency between the original user profile and its copies has to be guarantied.

B.2 Applying X.500 for mobility in private networks

This Clause describes the deployment of an X.500 Directory [25] to perform the mobility management operations described before.

Figure B.1 depicts how the X.500 architecture could be applied for managing user profiles for mobility management. Each user profile is stored in the Directory Information Base as an object. The users of the Directory are the PTNXs that are connected to the DUAs (Directory User Agent). Each site has access to the Directory System via an own DUA. The user profiles that belong to the same home site are stored in the same DSA (Directory System Agent).

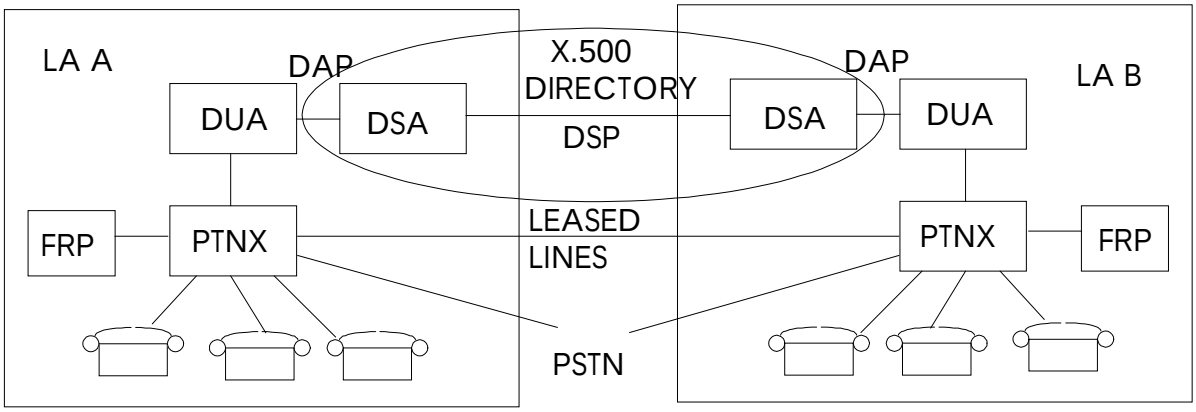


Figure B.1: X.500 architecture applied for mobility management

Figure B.2 illustrates a scenario where 5 sites are connected in a private network. Sites that do not wish to manage a DSA (e.g. site E) can store their entries in other DSAs but they give up their administrative royalties for their user profiles.

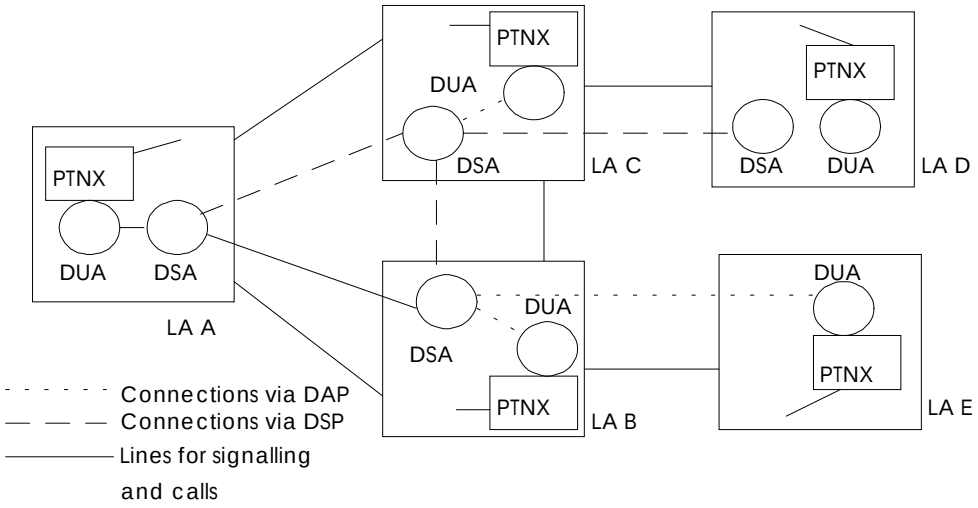


Figure B.2: Scenario with 5 sites connected via X.500

The sites are connected via communication lines over which in most cases the DSP (Directory Service Protocol) protocol has to be implemented, for smaller sites without an own DSA the DAP (Directory Access Protocol) protocol shall be used. The Directory protocols will have to be implemented on top of signalling protocols like QSIG-GF [26] that will offer ROSE services.

Figure B.3 shows an example how parts of the user profiles could be organised in the Directory Information Tree (DIT) and how these entries could be distributed over several DSAs.

It is possible to replicate and cache user profiles in some DSAs that have frequent access to specific user profiles. In this way the requirements on the underlying signalling network can be heavily reduced.

NOTE: The DSAs that manage the entries for the root and the country objects (i.e. the two uppermost levels in the tree) are not shown in figure B.3.

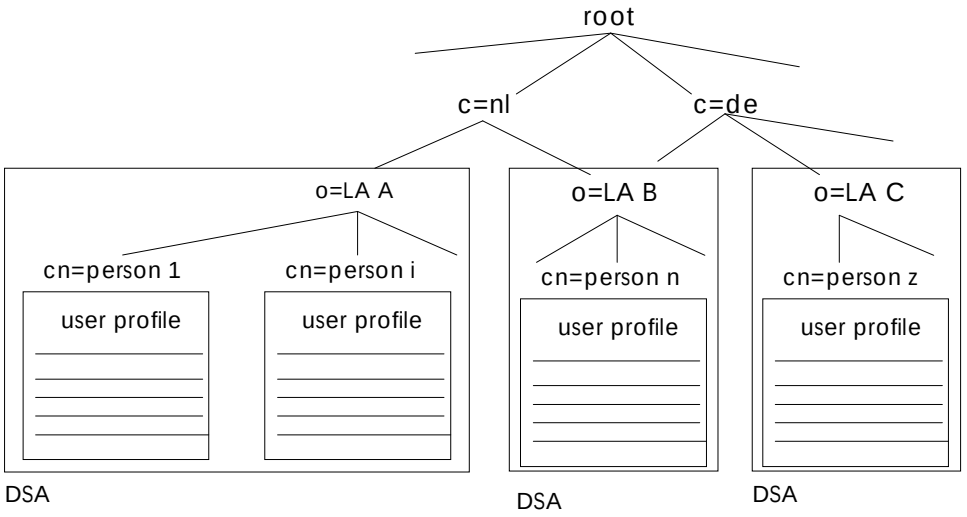


Figure B.3: Example of user profiles in the Directory Information Tree

All user profile information is contained in attributes of the user profile object (which has to be defined) including the personal number and the current location area identifier.

If we apply an X.500 system in private networks as described above, the problems that are identified in Clause B.1 can be solved in the following way:

Problem A (finding home site):
The user profile is retrieved by accessing any DSA in the network. No relation between the user number and the home location is necessary. For incoming calls from the outside of the private network, the caller can access any PTNX of the network. By replicating and caching knowledge about the DSA storing a particular entry, searching can be avoided and access to user profiles is possible with simple READ operations.

Problem B (accessing user profiles):
The profiles are retrievable by every PTNX simply by sending a READ request to its local DSA. The directory contains mechanisms for optimising system performance by data replication and caching techniques.

Problem C (location update):
For roaming to another location only the current location area identifier in the user profile has to be changed. For this purpose the normal X.500 MODIFY procedure can be used.

Problem D (changing home site):
The user can change his home site simply by moving his entry in the DIT into another DSA. Since there is no relation between his number and his home site, he may keep his personal number.

Problem E (modifying user profiles):
If the user modifies his user profile object, it might take some time until this modification will be finished successfully in the home DSA. During this time, queries to the user profile will return the not-modified profile. This is, however, no severe problem because the user profile update is not that time-critical.

B.3 Additional aspects of the X.500 approach

Free numbering:
With the X.500 approach, there is no need for the personal number of a user to have a relation to his home location. This gives a lot of flexibility for number plans and the freedom to allocate users to new home site while keeping their personal numbers.

Object oriented data model allows easy extension and fast introduction of new services:
The data model of the X.500 Directory allows a flexible extension because of its object oriented approach. Manufacturers of private networks could base their products on this concept with the freedom to add special mobility features by simply deriving subclasses of the recommended classes. This would allow a fast local introduction of new mobility services into PTNXs without the need to change the communication protocols.

Directory can be used for other applications:
The Directory System is a general purpose solution and can be used for other applications simultaneously, e.g. the telephone number directory of a private network (i.e. mobile and non-mobile numbers) or a directory of e-mail addresses can be distributed via this service.

History

Document history	
October 1993	First Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)