# TECHNICAL REPORT

# ISO/IEC
# TR 15410

First edition
1998-12-15

# Information technology — Telecommunications and information exchange between systems — PISN mobility-general principles and services aspects

*Technologies de l'information — Télécommunications et échange d'information entre systèmes — Principes de mobilité générale du PISN et aspects de service*

# Contents

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 15410, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

# Information technology — Telecommunications and information exchange between systems — PISN mobility-general principles and services aspects

## 1 Scope

This Technical Report (TR) analyses the requirements for the standardization of networking functions to support mobility within one or more Private Integrated Network Exchanges (PINXs) of a Private Integrated Services Network (PISN).It covers both Wireless Terminal Mobility (WTM) and Private Personal Mobility (PPM).

WTM is a function that allows users of Wireless Terminals (WT) to make and receive calls at any compatible radio access within the network. Standards for WTM should be independent of the access technology used to support the WTs.

PPM enables users of a PISN to register at any suitable terminal (wired or wireless) within the network for the making and/or receiving of calls.

This Technical Report covers the following subjects for both WTM and PPM:

- Registration procedures;

- Procedures for incoming and outgoing calls;

- Access security procedures (identification and authentication);

- Requirements for numbering, addressing and signalling;

- Requirements for management, administration and operation.

## 2 References

ISO/IEC 11571:1994, *Information technology — Telecommunications and information exchange between systems — Numbering and sub-addressing in private integrated services networks.*

ISO/IEC 11572:1994, *Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Circuit mode bearer services — Inter-exchange signalling procedures and protocol.*

ISO/IEC 11574:1994, *Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Circuit mode 64 kbit/s bearer services — Service description, functional capabilities and information flows.*

ISO/IEC 11579-1:1994, *Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Part 1: Reference configuration for PISN Exchanges (PINX).*

ISO/IEC 11582:1995, *Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Generic functional protocol for the support of supplementary services — Inter-exchange signalling procedures and protocol.*

CCITT Rec. E.164 (1988), *Numbering plan for the ISDN era.*

CCITT Rec. I.251.1 (rev.1) (1992), *Integrated Services Digital Network (ISDN) — General structure and service capabilities — Direct Dialling In.*

CCITT Rec. I.251.2 (rev.1) (1992), *Integrated Services Digital Network (ISDN) — General structure and service capabilities — Multiple subscriber number.*

CCITT Rec. Q.81.1 (1988), *Functions and information flows for services in the ISDN — Stage 2 description for number identification supplementary services — Section 1 - Direct-Dialling-In.*

CCITT Rec. Q.81.2 (1992), *Functions and information flows for services in the ISDN — Stage 2 description for number identification supplementary services — Section 2 - Multiple subscriber number.*

ITU-T Rec. I.112:1993, *Integrated services (ISDN) — General structure: Vocabulary of terms for ISDNs.*

ITU-T Rec. Q.931 (1993), *Digital subscriber signalling system No.1 Network layer — Digital subscriber signalling system No.1 (DSS 1) — ISDN User-Network interface layer 3 — Specification for basic call control.*

# 3 Terminology

## 3.1 Definitions

For the purposes of this Technical Report, the following definitions apply. The sources of the definitions are given in square brackets.

### 3.1.1 Internal definitions

**1 Attendant**
a PISN user whose prime task is to provide assistance and support to the users.

**2 Authentication**
a property by which the correct identity of an entity or party is established with a required assurance.

**3 Wireless Terminal (WT)**
a physical entity that provides access to the telecommunications services of a PISN via a radio interface.

**4 Wireless Terminal Mobility (WTM)**
the ability of a wireless terminal to be in continuous motion whilst accessing and using the telecommunication services offered by the PISN, as well as the capability of the network to keep track of the location of the wireless terminal within the coverage area of the radio system used.

**5 Coverage area**
The area over which reliable communication can be established and maintained.

**6 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 PINX.

## 7    Function

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

## 8    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 RE/RBS.

NOTE — Only the external handover, i.e. the handover between two different RE/RBSs, is relevant for this Technical Report.

## 9    Home Data Base (HDB)

the data base in which the current location and all associated parameters of a wireless terminal or a user are stored.

## 10    Location Area (LA)

the coverage area in which a wireless terminal may receive and initiate calls as a result of a single location registration.

## 11    Location Registration

the process whereby the position of a wireless terminal is made known to the PISN.

## 12    Private

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.

## 13    Private Personal Mobility (PPM)

the capability of a PISN user to register at any PISN terminal, and so receive the PISN services at the hosting terminal.

## 14    Public

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.

## 15    PPM Number

a number which uniquely identifies a PPM user. This is the number used by the caller to reach the PPM user.

## 16    PPM Registration

the operation performed by a PPM user to inform the PISN of the PISN address that should be utsed to locate the user.

## 17    Radio Base Station (RBS)

a physical grouping that contains all of the radio equipment on the PISN side of the air interface directly connected to a single antennae system.

## 18    Radio Exchange (RE)

a physical grouping between the RBSs and the PINX .

## 19    Registration

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

## 20    Roaming

the movement between calls of a wireless terminal from one Fixed Radio Part (RE/RBS) coverage area to another RE/RBS coverage area, where the capabilities of the PISN enable the wireless terminal to access PISN services.

NOTE      Roaming requires the RE/RBS and the wireless terminals to be interoperable.

NOTE      See also the definition of handover.

**21 PISN Network Supervisor (SUP)**
the entity which is allowed to execute a PISN management task.

**22 Visitor Data Base (VDB)**
the database in which all relevant parameters concerning a wireless terminal and a PPM user are stored for aslong as they are located in an area controlled by this database.

### 3.1.2 External definitions

**1 Address [ISO/IEC 11571]**
**2 Additional Network Feature (ANF) [ISO/IEC 11571]**
**3 Call, Basic call [ISO/IEC 11571]**
**4 Dialling Plan [ISO/IEC 11571]**
**5 Domain [ISO/IEC 11571]**
**7 Identification Address/Number [ISO/IEC 11571]**
**8 Implicit Numbering Plan [ISO/IEC 11571]**
**9 Integrated Services Digital Network (ISDN) [ISO/IEC 11571]**
**10 ISDN Numbering Plan (ISDN NP) [ISO/IEC 11571]**
**11 Multiple Subscriber Number (MSN) [ISO/IEC 11571]**
**12 Native Numbering Plan [ISO/IEC 11571]**
**13 Number [ISO/IEC 11571]**
**14 Numbering Plan Identifier (NPI) [ISO/IEC 11571]**
**15 Partial Number [ISO/IEC 11571]**
**16 PISN Administrator [ISO/IEC 11571]**
**17 Private Numbering Plan (PNP) [ISO/IEC 11571]**
**18 PNP Number [ISO/IEC 11571]**
**19 Private Integrated Services Network (PISN) [ISO/IEC 11579-1]**
**20 Private Integrated Services Network eXchange (PINX) [ISO/IEC 11579-1]**
**21 Private Integrated Services Network Numbering Plans (PISN NP) [ISO/IEC 11571]**
**22 PISN Number [ISO/IEC 11571]**
**23 PISN User [ISO/IEC 11574]**
**24 Region [ISO/IEC 11571]**
**25 Selection Address/Number [ISO/IEC 11571]**
**26 Sub-domain [ISO/IEC 11571]**
**27 Telecommunication Network [ITU-T Rec. I.112]**
**28 Terminal equipment; terminal [ISO/IEC 11571]**
**29 Type of Number (TON) [ISO/IEC 11571]**
**30 Unknown Numbering Plan (Unknown NP) [ISO/IEC 11571]**

## 3.2 Symbols and abbreviations

ANF      Additional Network Feature

CC       Call Completion

CFU      Call Forwarding Unconditionaly

CD       Call Diversion

DDI      Direct Dialling In

DWT      Dedicated Wireless Terminal

DN       Dialling Number

HDB      Home Data Base

ISDN     Integrated Services Digital Network

ISDN NP  ISDN Numbering Plan

IEC      International Electrotechnical Commission

**4**

| ISO | International Standardisation Organisation |
|---|---|
| LA | Location Area |
| MSN | Multiple Subscriber Number |
| NP | Numbering Plan |
| NPI | Numbering Plan Identifier |
| PIN | Personal Identification Number |
| PNP | Private Numbering Plan |
| PISN | Private Integrated Services Network |
| PISN NP | Private Integrated Services  Network Numbering Plans |
| PINX | Private Integrated Network  eXchange |
| PPM | Private Personal Mobility |
| RBS | Radio Base Station |
| PSS1 | Private Signalling System #1 |
| RE | Radio Exchange |
| SUP | PISN Network Supervisor |
| TE | ISDN Terminal Equipment |
| TON | Type of Number |
| TR | Technical Report |
| VA | Visitor Area |
| VDB | Visitor Data Base |
| WNT | Wireless Network Terminator |
| WT | Wireless Terminal |
| WTI | Wireless Terminal Identity |
| WTM | Wireless Terminal Mobility |

# 4   Introduction

This clause provides some background and gives an overview of the concepts covered in this Technical Report by describing the basic structure of a PISN and explaining the key areas related to mobile users and terminals.

## 4.1 Private Integrated Services Network environment

As seen in this Technical Report, the telecommunications environment of a PISN consists of PINXs radio exchanges (RE), radio base stations (RBS), wired terminals, wireless terminals and users of these terminals. See Figure 1 for an illustration.
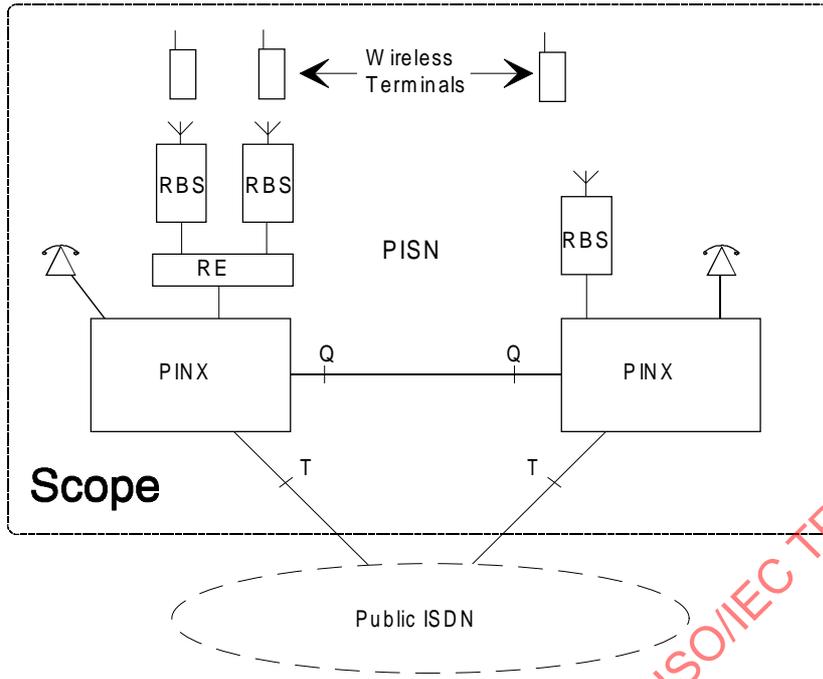
**Figure 1 — Example of a PISN environment**

## 4.2 PISN mobility concept

As the PINX itself is not mobile, mobility with respect to the access side of the PINX 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.
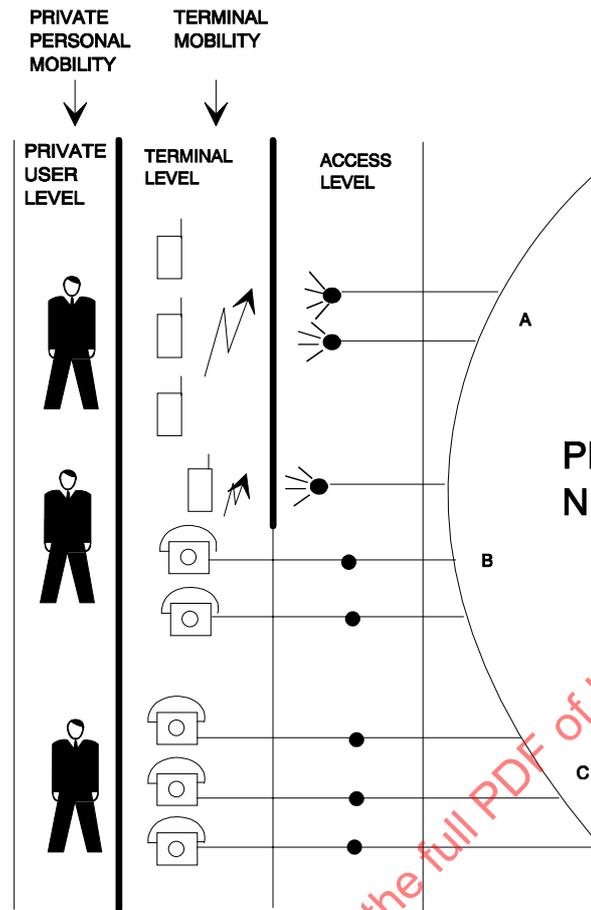
**Figure 2 — PISN mobility**

WTM is applicable only to wireless terminals whilst PPM is applicable both to wired and wireless terminals, as well as to a mixed environment utilising both terminal types.

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

- access level;

- terminal level;

- user level.

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 Personal Mobility (PPM) and Wireless Terminal Mobility (WTM) and are briefly described below.

In this report mobility for users and terminals is limited to a single PISN. Referring to Figure 1, the mobility of a user/terminal is either within or between the PINXes. Mobility between two or more PISNs is outside the scope of this Technical Report.

### 4.2.1    Private Personal Mobility (PPM)

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

In PPM it is possible for the user to change terminal, wired or wireless, between calls while retaining his telecommunications services.

The intent of PPM 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    Wireless Terminal Mobility (WTM)

With WTM, there is no fixed relation between the wireless terminal and the PISN access and the terminal can also 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 wireless terminal in the same way as to a wired terminal. However, some 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 wireless terminals as from wired terminals.

Location information concerning the wireless 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 wireless terminal or manually by the user of the wireless terminal.

### 4.2.3    Database architecture

An architecture based on the  Home Data Base/Visitor Data Base (HDB/VDB) concept  has been assumed for mobility management in this Technical Report. This architecture is considered mature for mobile telecommunication applications. Furthermore the introduction of mobility based upon this approach is considered to minimise the impact on the current standards applicable to PISNs.

One consequence of the choice of the HDB/VDB concept is that the practical application of mobility with multiple HDBs in a PISN which allows a user to permanently change his location without changing his number (free numbering), is not covered in this Technical Report.

The interface between the PINX and the databases HDB/VDB is out of the scope of this Technical Report.

## 4.3 Relation between PPM and WTM

### 4.3.1    Mobility seen as a dynamic linking of identities

PPM gives the user freedom to use any terminal in the PISN whilst WTM allows a WT to be used at any compatible PISN radio access.

Each form of mobility requires a dynamic linking of two identities. PPM requires a dynamic linking between the PPM number and the terminal (access address in the case of a wired terminal). WTM requires a dynamic linking between the WT address and a PISN 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 PPM and WTM.

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

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

### 4.3.2   Similarities of processes

The following procedures should be defined as generic as possible for both PPM and WTM:

- Registration;

- Authentication;

- Handling of incoming calls to the mobile user;

- Handling of outgoing calls from the mobile user.

This would minimise the differences between the procedures for PPM and WTM while allowing the specific characteristics of each to be taken into account.

a)  WTM

   - Terminals can perform actions automatically.

b)   PPM

   - The PPM concept involves actions to be performed by the users. These procedures differ from the terminal procedures in that they have to be adapted to human actions.

### 4.3.3   Location Area

This report uses the term Location Area (LA) only in relation with WTM and not for the PPM case.

### 4.3.4   The use of PPM and WTM together

WTM is independent of PPM in the sense that WTM and PPM together allow mobility of the terminal while maintaining the PPM user's registration on the terminal. This is likely to require a complex procedure which the service standards must accomodate. The details are discussed further in chapter 7, «PPM on top of WTM».

## 4.4 Mobility between calls and during an established call

Two fundamental situations should be covered when discussing mobility;

- the ability to change access (WTM) or terminal (PPM) between calls, and

- the ability to change access (WTM) during an established call.

## 4.5 Services to be supported

When mobility is introduced, it is desirable that a full range of basic and supplementary services is made available to mobile users with the same quality of service as would be expected by fixed users. The operation of some existing  supplementary services may need to be modified if they are to be available to mobile users.

### 4.5.1 Bearer services and Teleservices

Standards for mobility in the private network should be capable of supporting all circuit mode basic services as defined in ISO/IEC 11574.

### 4.5.2 Supplementary Services

All supplementary services defined for PISNs should be considered and made applicable if this can be done without undue difficulty. In addition the following mobility specific supplementary services and Additional Network Features (ANFs) should be standardized.

- WTM Location registration;

- WTM incoming call handling;

- WTM outgoing call handling;

- WTM authentication of the terminal by the network;

- WTM authentication of the network by the terminal;

- WTM Handover

- PPM registration;

- PPM incoming call handling;

- PPM outgoing call handling.

#### 4.5.2.1 Access to supplementary services

The provision of standardised supplementary services where one or more of the involved users are either a WTM or PPM user can present a number of problems in implementation.

One of the most obvious problems likely to be encountered by mobile users as they roam from one PINX to another is the difference in supplementary service access methods implemented by the various manufacturers.

Careful network planning and management can, in many cases, be used to provide unified user procedures throughout the network but this is likely to be more difficult where:

a) mobility is introduced to an established PISN of fixed users as the co-ordination of user procedures is of considerably less importance when all user terminals are static. Also, there may be some resistance to change among the existing users;

b) some terminals or PINXs within the network implement fixed user procedures set by the manufacturer and are not available for customisation;

c) not all PINXs in a PISN have implemented the same set of supplementary services:

The rationalisation of user procedures is, however, a difficult problem to deal with. While complying with the Private Signalling System #1 (PSS1) standards for supplementary service signalling between PINXs, each manufacturer is likely to offer access to the services in slightly different ways because:

a)  firstly, there are three generic procedures for network access protocols (i.e., the protocol between network and terminal equipment): functional procedures, the keypad stimulus protocol and the feature key management stimulus protocol and;

b)  secondly, even if the same generic method is used, there is still scope for differences, since in the stimulus protocol case no specific procedures are standardised for individual supplementary services, and standardised functional procedures are so far defined for public Integrated Services Digital Network (ISDN) terminals only and for very few services.

This could cause confusion to roaming users as they try to invoke supplementary services at different points within the PISN.

One way to overcome this problem is to create a homogeneous environment for roaming users, e.g., by ensuring that all PINXs supporting PPM or WTM in a network, all fixed radio equipemt and all WTs are of the same type and from a single manufacturer (in many instances this will not be considered as a practical or feasible solution), or by specifing standards for the access procedures (which is a long term goal rather than a practical alternative for the near future).

Another option is to ensure that the user's Home PINX is always accessed to provide supplementary services (i.e., always route incoming and outgoing calls via the Home PINX). For many services this would be quite acceptable and a very practical solution but for others, the processintg, signalling and transmission overheads necessary for maintaining user status at the Home PINX would be intolerable.

A further option is to make use of the functional protocols defined for public ISDN. The WTs and radio fixed parts would need to be upgraded whenever the functional protocols for a new service are published. The cost of keeping these up-to-date could be unacceptably high unless or until a method of downloadintg a WT on-line can be devised.

### 4.5.2.2    Service options

PISN standards specify in many cases the mandatory core of a supplementary service and optional features, which an implementation may support in addition to the basic core. A manufacturer may provide further proprietary enhancement of the supplementary service. For instance, the core of Call Forwarding Unconditional (CFU) is that all calls or calls associated with a specific basic service are diverted to another PISN address. Standard options are the provision of notifications, interrogation procedures, etc. A manufacturer may further offer the non-standardised possibility to specify different diverted-to numbers based on certain call criteria, e.g., external versus internal calls, while still complying with the basic core of CFU.

The consistent provision of standard and proprietary service options for roaming users faces similar difficulties as discussed in 4.5.2.1. Invoking the supplementary service at the Home PINX regardless of the user's actual location again seems a good solution in some cases.

### 4.5.2.3    Dynamic registration and service related data.

Some existing supplementary services allow the served user to register data that are then used in the invocation of the service. An example is the Diverted-to user's address in the Call Diversion (CD) services. Once registered, this information must continue to be associated with the mobile user regardless of the user's movements within the PISN.

Other supplementary services rely on data stored in association with a specific service invocation, which also must "follow" the roaming user when changing location. An example is the queue of outstanding call completion requests.

In both cases this may prove to be difficult in a multi-vendor envitonment where such data may be stored and processed in quite different ways. There seems to be no simple solution to this problem other than imposing constraints on the use of such services for mobile users.

#### 4.5.2.4 Destination PINX: Home PINX versus Visitor PINX

Many supplementary services require actions from the destination PINX of a call. In the case of roaming users it is not so obvious what should be regarded the destination PINX, since the roaming user «exists» twice in the PISN. In a logical sense it would be the Home PINX as it holds the user's permanent «image». From a call termination point of view it would be the Visitor PINX as this is the user's current physical location. The determination of which interpretation is more suitable must be made on a case-by-case basis.

If the Visitor PINX is chosen, the following considerations are worthy of note in almost all cases:

a)   the service may not be available to a served user at all locations;

b)   the options subscribed to by the served user may not be offered at all Visitor PINXs:

c)   user procedures may differ from PINX to PINX.

## 5   Private Personal Mobility

## 5.1 Introduction to PPM

Private Personal Mobility (PPM) provides PISN users with telecommunication  services irrespective of the terminal used within the PISN. It enables each PISN user subscribing to the PPM service to participate in a user-defined set of services and to initiate and receive calls on the basis of a unique, personal PPM number throughout the PISN at any terminal, wired or wireless, irrespective of geographic location. PPM should only be limited by terminal and network capabilities and the restrictions imposed by the PISN. A PISN user subscribing to the PPM service is referred to as a PPM user.

In a PISN supporting PPM there exists no permanent association between PPM users and terminals. Any PPM user can register on any terminal within the PISN, and it is thus possible to have multiple registrations on a given terminal. It is also possible to have no user registered on a specific terminal.

## 5.2 PPM service architecture

Mobility services, as descibed in this report, assume the concepts of Home Data Base (HDB) and Visitor Data Base (VDB). The HDB contains the current location and all associated parameters of the PPM user, and is accessible from the PPM user's Home PINX. The VDB contains the information required for providing the PPM user with PISN services in the visitor area, and is accessible from the PPM user's Visitor PINX. No specifications are given regarding the physical implementation of these data bases or their geographical location relative to the PINXs.

In order for the PPM users to receive a consistent set of PISN services throughout the PISN, the necessary elements of the user's service profile should be made available at the Visitor PINX.

Figure 3 illustrates the PPM concept in terms of Home/Visitor PINX/Database. It describes the state of the PISN after the PPM user has registered at the Visitor PINX. The PISN has modified the PPM user's entry in the HDB which now points to the Visitor PINX. Also, a VDB entry has been established which supports the PPM user's access to PISN services at the Visitor PINX. The entry in the HDB should point to the VDB which has to contain the current access number. (Alternatively, the HDB could specify the PPM user's current access number.)
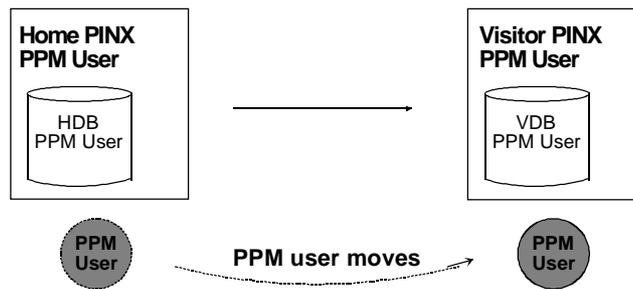
**Figure 3 — Illustration of PPM**

In a PISN which supports both WTM and PPM, interactions arise between the two types of mobility. This is a consequence of the requirement that PPM users must be allowed to register also on wireless terminals. Chapter 7 of this Technical Report deals with the problem of providing PPM on top of WTM.

## 5.3 PPM services

### 5.3.1 PPM registration for incoming calls (InCall registration)

The PISN should provide the PPM user with the possibility to specify one or more terminals at which calls to the PPM user are to be presented. Different terminals may be specified depending on:

- the type of teleservice;

- the type of bearer service.

For each teleservice and bearer service, only one terminal may be specified by a PPM user for incoming calls at any given time.

The PPM user should be allowed to specify, at registration time, the duration of the registration period (registration session) for incoming calls.

A PISN may allow several PPM users to register for incoming calls at the same terminal. Since an incoming call to a terminal which hosts more than one user could be for any one of the registered users, it may be desirable to specify the addressed user upon call delivery by means of a display feature, a distinctive ringing signal, or a voice announcement.

### 5.3.2 PPM registration for outgoing calls (OutCall registration)

A PPM user should be able to specify a terminal from which outgoing calls are to be made by the PPM user subject to their service profile. The PISN must support registration for:

- a single call;

and may also support registration sessions for:

- a specified duration;

- indefinite duration.

It may also be desirable to support PPM registration sessions for a specified number of outgoing calls.

Different terminals may be specified depending on:

- the type of teleservice;

- the type of bearer service.

For each teleservice and bearer service, a PPM user may be allowed to have, at any given time, more than one OutCall registration session in the PISN.

In a PISN which supports OutCall registration sessions, the question arises about whether or not more than one PISN user can be registered at the same terminal at the same time. If only one PISN user can be registered at any given time, all calls made from the terminal are assumed to be those of that user.

If multiple concurrent OutCall registrations are supported, a mechanism must be implemented to ensure that the PISN is aware of the calling user's identity. This may be accomplished by means of one of the following methods:

a) Before initiating an outgoing call, both the normal user and the PPM user dial a Personal Identification Number (PIN).

b) Only the PPM user dials a PIN before initiating an outgoing call. All other calls made from that terminal are assumed to be those of the normal user.

c) Only the normal user dials a PIN before initiating an outgoing call. All other calls made from that terminal are assumed to be those of the PPM user.

The PPM standards should allow any one of these methods to be implemented.

### 5.3.3 PPM registration for incoming and outgoing calls (AllCall registration)

A PPM user should be able to specify a terminal at which to receive incoming calls and also make outgoing calls. It should be possible to register for both these PPM service options by means of a single operation, referred to as AllCall registration. In an AllCall registration session, the incoming and outgoing call registration components are combined into a single service option, and cannot be separated.

### 5.3.4 Local and remote PPM registration

A PPM user should be able to register, from any suitable PISN terminal, to receive a PPM service at the hosting terminal. A PPM registration which is initiated from the hosting terminal is referred to as a local PPM registration. A PPM registration which is initiated from a PISN terminal other than the hosting terminal is referred to as a remote PPM registration.

Except for the specification of the hosting terminal in remote registration, the same basic procedures should be used for both types of registration.

### 5.3.5 PPM de-registration

A PISN supporting PPM should provide for the following PPM de-registration mechanisms:

- **Explicit de-registration:** A PPM user de-registers from the hosting terminal by means of a manual operation carried out on the same terminal (local de-registration) or on any other PISN terminal (remote de-registration).

- **Implicit de-registration:** A PPM user registers at another PISN terminal, which may cause the PISN to delete the previous registration for the relevant PPM service option(s).

- **Conditional de-registration:** The PISN de-registers a PPM user when certain pre-defined criteria are met (e.g. the registration timer expires, or the specified number of outgoing calls have been made).

- **Forced de-registration:** An authorised third party (e.g. the owner of the hosting terminal) de-registers the visiting PPM user(s) from a terminal. The terminal from which the forced de-registration request is initiated may be the hosting terminal (local de-registration) or any other PISN terminal (remote de-registration).

NOTE       De-registration by the PISN management authority is outside the scope of this Technical Report.

During a period when a PPM user is not registered at any terminal, a default terminal may be assigned to the relevant PPM number for incoming and/or outgoing calls. Alternatively, incoming PPM calls may receive special treatment (e.g. voice announcement). These provisions will be subject to arrangement with the PISN management authority.

### 5.3.6    PPM service interrogation

The PISN should support interrogation procedures which the PPM user may invoke to inquire about the current status of PPM service options. For example, it should be possible for a PPM user to obtain information regarding the current parameters of an active OutCall session, including, for example, the number of remaining outgoing calls.

## 5.4 Interaction considerations

### 5.4.1    Interaction with existing services

The PPM service is intended to give the PPM user access to the telecommunication services as indicated by the user's service profile. The transfer of the service profile content between the Home PINX and the Visitor PINX should provide the basis to achieve this service. However, some services may be too complex to be provided in the new area if they have been activated in the Home Area, e.g., Call Completion (CC). For this kind of service the implementation may cancel the activated feature when the user is registered some where else.

## 5.5 Security aspects

Security aspects include the protection against malicious and unauthorized actions, the protection of the privacy and the freedom of action of PPM and non-PPM users of the PISN.

Various forms of misuse that a PISN, PISN users, and more specifically PPM users may be exposed to due to the PPM service should be further analysed and security mechanisms to be used to protect the PISN and the users against the different kinds of misuse should be developed.

NOTE       This paragraph does not apply to legal requirements to send user identities for regulatory requirements (e.g., emergency calls).

The following paragraphs give only an overview of the subject.

### 5.5.1 General requirements on security mechanisms

PPM is a PISN service that enables PPM users to access telecommunication services at any terminal of the PISN. PPM users can make and receive calls on the basis of their personal PPM number. PPM users may, in principle, use any terminal in the PISN for making or receiving calls that will be charged to their account.

Due to the flexible nature of the PPM service, PPM users are very exposed to fraudulent use of their "subscription". An intruder or malicious person could abuse a PPM user's account from any terminal in the PISN. Therefore, it is important to protect the PISN, and PISN users and especially PPM users from any fraudulent or malicious attack and to preserve their privacy.

PPM security mechanisms should handle only those problems that are specifically related to the PPM service and those which exist normally in PISNs but become more significant in a PPM environment.

### 5.5.2 General risks

The following list includes those threats with realistic likelihood of occurrence. In addition, only threats that are specific to PPM are considered. Moreover, the protection of the PISN resources (PINX, Data Bases) against unauthorized access is not considered to be specific to PPM.

- Eavesdropping of PPM user's identification and authentication information (threat);

- Masquerading as a PPM user (threat, privacy violation);

- Registration unauthorized by the terminal's owner (inconvenience);

- Impersonating a registered PPM user and make outgoing calls (threat);

- Insecure PPM incoming calls answer (privacy violation);

- Unwanted incoming calls (inconvenience).

### 5.5.3 Requirement on security mechanisms

The analysis of the PPM related risks, shows that only those risks that can be considered as threat need to be dealt with. Mechanisms to deal with the others can be optionally provided.

Therefore, it is recommended that the following security aspects are considered in the PPM service as a minimum:

- to use an alternative identifier, not the PPM user's number, as the PPM user's identity;

- to use a one pass authentication mechanism with simple PIN;

- to provide a procedure to modify the PIN dynamically by the PPM user;

- to block the PPM account after a number of consecutive unsuccessful authentication attempts;

- unblocking the PPM account would be a management operation; it may also be a user procedure with a special PIN but no standardization is foreseen for such a procedure;

- to provide all users with the capability of preventing PPM users registering at their terminal.

## 5.6 Signalling aspects

The signalling system to be used between the PINXs should be based on PSS1, It is, however, expected that some enhancements of the PSS1 may be required.

## 6 Wireless Terminal Mobility

## 6.1 Introduction to WTM

WTM provides a PISN user with a wireless terminal 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 WT it will continuously change its PISN access point. This may happen during and between calls. In order for a PISN to support telecommunication services for continuously mobile WTs, the PISN (including the fixed radio parts) provides automatic functions which keep track of the WT's present and previous location as well as securing the communication with the terminal. WTM should only be limited by terminal and network capabilities and the restrictions imposed by the PISN. A PISN user using the WTM services is referred to as a WTM user in this Technical Report.

NOTE     This Technical Report does not deal with any radio technical aspects. For information on such subjects, references should be made to the relevant standards for the applicable wireless systems.

WTM is not to be considered as a single function, but more as a "collection" of all new and modified functions and procedures required to support mobility of wireless terminals. In this Technical Report these functions have been gathered into two main groups which are:

- roaming; and

- handover.

This Clause describes the functions required to support mobility of WTs within a single PISN.

The main issues addressed are:

-    identification of the mobility support procedures;

-    location of the mobility support procedures;

-    the information flow between the fixed radio part and the PINX ; and

-    the information flow between the PINXs.

Subclause 6.2 covers these aspects in more detail.

NOTE        The WTM functions described are based on the perceived user requirements for WTM and are equally applicable to
            any air interface used for the wireless access. It should be recognised that some forms of wireless access may not
            support all the services and procedures identified in this Technical Report. However such limitations, where they do
            exist, do not invalidate the principles of this Technical Report.

### 6.1.1    Reference configuration

Figure 4 indicates  a possible reference configuration for a PISN with WTM.
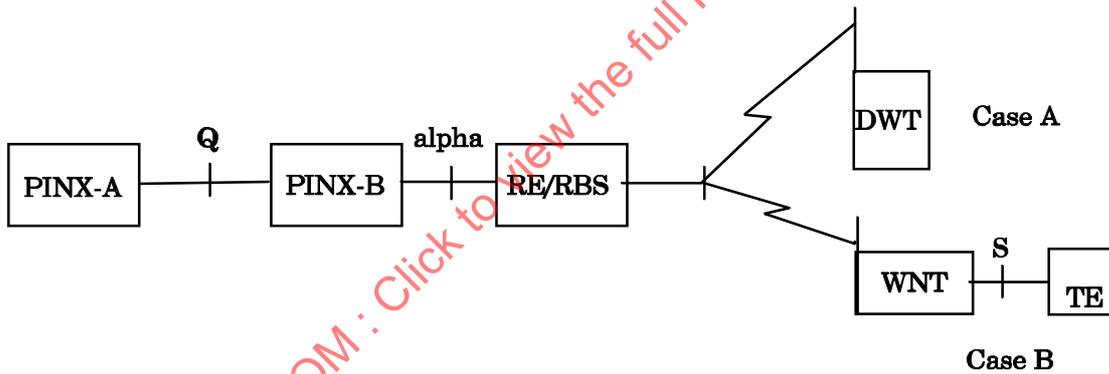
Legend:

-    DWT means Dedicated Wireless Terminal;

-    WNT means Wireless Network Terminator;

-    TE is an ISDN terminal.

**Figure 4 — Reference configuration for WTM**

The reference configuration shows two cases:

- **Case A:**

    The wireless telephone systems acts as a terminal end system. A dedicated wireless terminal is used.

- **Case B:**

    The wireless telephone system acts as an intermediate system. The Wireless Network Terminator (WNT) provides a standardised wired interface to which a standardised ISDN terminal can be connected.

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

a)  The RE/RBS  should not have any internal switching capabilities, i.e., the ability to directly interconnect two WTs.

b)  If the RE/RBS have more than one interface at the alpha reference point, all interfaces should  be connected to the same PINX.

c)  Standards for the information across  the alpha reference point should be limited to the information flow only (Stage 2). Signalling protocol standards (Stage 3) across the alpha reference point is considered radio technology specific and thus outside the scope of this Technical Report.

d)  The network signalling protocols for the control of services and mobile functions should be based upon PSS1, and should support both cases A and  B.

### 6.1.2   General information on roaming

The roaming function makes it possible for the user of a WTs to access PISN services between calls via  different radio accesses  in the PISN.

NOTE      This Technical Report covers the possibility to make and/or receive calls throughout the whole PISN within the radio coverage areas of the Radio Base Statations (RBSs) connected to PINX-A and PINX-B as shown in Figure 5.

The functions needed to support roaming include the following procedures:

-   location registration (collection and storage of new location information);

-   location de-registration (removal of location data);

-   authentication (validation of the WT and/or RE/RBS). This feature is optional.
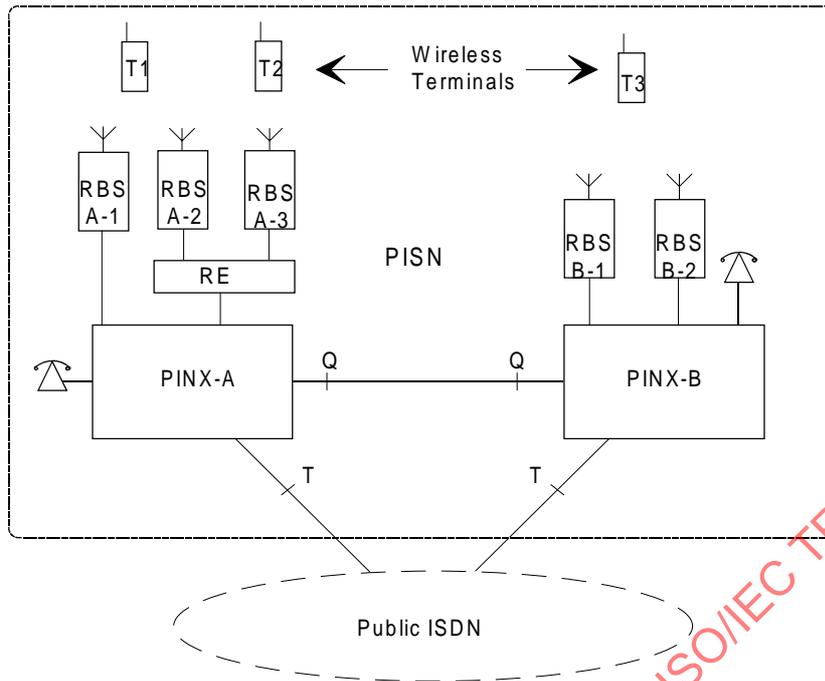
**Figure 5 — Logical block diagram of a simple PISN**

### 6.1.3    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 RBSs  in the PISN. 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 of the WT and/or the network;

-    handover (change of communication path);

-    location registration (if necessary).


Basically handover can be classified as either:

-    internal; or

-    external.

Internal handover means handover within one RE/RBS.. This is an internal function of the RE/RBS and does not require any cooperation from the PISN. Therefore, apart from identifying internal handover as a form of handover, it is not discussed any further in this Technical Report.

External handover means handover between two different RE/RBSs, e.g., when moving between RBS A-1 and RBS A-2 in Figure 5. Because external handover involves two RE/RBSs, the cooperation of the PISN is required. This form of handover is addressed in this Technical Report. Therefore the unqualified term "handover" used in this Technical Report always refers to the external form of handover.

## 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);

- wireless terminal identities;

- fixed radio part identities;

- equipment related identities.


NOTE      Equipment related identities are normally used to derive a default identity coding for a wireless 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 wireless terminal are used to:

- to transfer access information from the fixed radio parts to the wireless terminals;

- to process access requests from wireless terminals;

- to identify the fixed radio parts and wireless 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 (PISN identity) and the capabilities of the base station. The wireless terminal has a corresponding "identification code". The "identities" of the fixed radio parts and the wireless 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 WTs exist in the same area. A WT may contain several such identities allowing the WT 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 WT;

- 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.


### 6.2.1.1.1    Identification of fixed radio part

The identity transmitted by the RBS is used by the WT to decide:

- if the fixed radio part belongs to the environment the WT wishes to access;

- whether or not that particular fixed radio part is the one the WT wishes to access.


### 6.2.1.1.2    Identification of Wireless Terminal (WT)

When a WT requests a service from the network, or if requested to by the fixed side, the terminal may supply its Wireless Terminal Identity (WTI) which enables the fixed side and/or the PISN to:

- identify the user or user's equipment (WT);

- check if the request shall be allowed or rejected.

Before the WT and/or the request is accepted by the network or RE/RBS , the PISN or RE/RBS may be required  to perform an authorisation check of the WT.

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

Equipment related identities are used to identify the WT and are usually globally unique. The fixed part may be able to request the WT to transmit its equipment identity which could then be used by the PISN to for example, track stolen equipment.


### 6.2.2    Roaming

Roaming is mainly provided by the following means:

a)    identities and addressing;

b)    location/registration and attachment;

c)    authentication

Prior to providing services to an unknown WT, it is necessary first to check if the terminal has access rights to the system. A possible process may be as follows:

- firstly, the terminal reads the identity of the RE/RBSand uses this identity to check whether it has access rights to that system. Assuming it has access rights, the wireless terminal then proceeds to register with the system;

- secondly, the WT identifies itself to the system, after which an optional authentication of the terminal may take place. Upon successful completion of this authentication, 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 wireless terminal may deregister from the system by sending a request to the PISN If this request is successful, the terminal is deleted from the VDB.

### 6.2.2.1.1 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 WT. The wireless 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 WT to send a location registration request;

- the fixed side controls the location updating.

### 6.2.2.1.2 Attachment related procedures

When registered, the WT may inform the network whether it is active or not.

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

### 6.2.2.2 Handover

Handover is the process of switching a call in progress from one physical channel to another physical channel. A request for handover from one RBS to another RBS may come from:

- the RE/RBS involved in a call; or

- a new RE/RBS.

Special areas to be addressed regarding handover are:

a) identities;

b) registration;

c) authentication;

d) interruption during handover.

Bearer services:

- 64 kbit/s unrestricted;

- 3,1 kHz audio;

- speech.


### 6.3.2    Supplementary services

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

- some supplementary services may differ for wired terminals and mobile wireless terminals;

- some supplementary services may not be possible to support from a particular mobile WT;

- a WT requires new specific supplementary services applicable only to WTM.

The term Additional Network Feature (ANF) is used to describe special features which can be described as supplementary services but they are not directly available to the end users. An ANF operates autonomously within a PISN and enhances the operation of the PISN for the benefit of all users. It is not the intention of this Technical Report to describe supplementary services and/or ANFs in a PISN as these are described by other international standards and/or technical reports.

As the PISN may have to interwork with the public ISDN, the wireless terminals connected to the PISN 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 PISN  as the signalling protocols at the "Q" reference point and the "alpha" reference point (i.e., between the RE/RBS and the PINX ), may 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.

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 RE/RBS and the PINX ).


### 6.3.3    PISN Attendant services

WTs should be supported by the PISN attendant to the same extent as wired terminals. Possible additional requirements on attendant services due to WTs are, however, outside the scope of this Technical Report. The need for an attendant to be mobile is not considered necessary.


### 6.3.4    Radio specific supplementary services

It is expected that the WTs may require special supplementary services and/or Additional Network Features (ANF) not yet identified. This issue is , however, outside the scope of this Technical Report.

## 6.4 Interaction considerations

### 6.4.1    Wireless systems

The PSS1 protocol standards for WTM should be independent of the  radio access system that is used.

### 6.4.2    Interworking with existing services

The standards should support interworking with other services offered by the PISN or other networks as if the WT was a "normal" wired terminal. Ideally a WTM  user should see no differences in the set of services and/or user procedures when accessing the PISN services at various PINXs. However, as discussed in 4.5 this may not always be possible.

## 6.5 Security aspects

In a PISN offering network wide mobility services, both the WTs and the PISN operator are vulnerable to unauthorised intrusion and misuse by third parties. In addition, special measures should be provided in order to protect the WTs integrity (e.g. location at a given time etc.). However, this subclause only addresses security aspects related to the use of the WT 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 PISN, the WTs and the exchanged information:

-    authentication;

-    encryption.

NOTE       Protection of transmitted information is essential on the radio link, but may also be required on the links between the
            nodes within the PISN. However, this topic is outside the scope of this Technical Report as this is a general PISN
            problem.

#### 6.5.1.1        Authentication of wireless terminal

Authentication is the process whereby a WT 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 (HDB).

Stolen or lost WTs may represent a risk in a PISN and it should be possible to keep a list of such terminals and to disable such WTs from accessing the PISN by e.g., erasing data stored in the WT. The WT 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 WT from logging onto a "phoney" or incorrect fixed part, optional functions for the authentication of a RE/RBS are also required. The procedure for the authentication of a RE/RBS is quite similar to the procedure for authentication of a wireless terminal. One example where it may be necessary to issue an authentication request of the RE/RBS is when the RE/RBS  wants to erase the «access data» in the WT.

### 6.5.1.3    Mutual authentication

Mutual authentication allows a WT and a RE/RBSto authenticate each other. It is possible to   achieve this by combining the authentication of the terminal and the network  and thus avoid  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 issues are related to this area:

-    protection against use of unauthorised terminals;

-    protection against unauthorised calls from sources outside the PISN;

-    protection against unauthorised calls from sources within the PISN. The standards should support functions whereby a WT can be verified to have the right to communicate via a particular RE/RBS;

-    protection against use of stolen equipment. The access rights for a WT can be temporarily and/or permanently withdrawn by sending a command to the WT which erases the memory in the WT. In addition the databases should also be updated such that the WT'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.

## 6.6 Signalling aspects

### 6.6.1    Signalling between the wireless terminals and the fixed radio parts

The signalling on the air interface between the WT and the RE/RBS as well as the signalling between the RE/RBS and the PINX is outside the scope of this Technical Report.

It is, however, recommended that the signalling system to be used between the RE/RBS and the PINX shall enable the use of ISDNterminals connected to a S reference point in the WT so that the mobility requirements laid down in this Technical Report still can be supported.

### 6.6.2    Signalling between PINXs

The signalling system to be used between the PINXs shall be based on ISO/IEC 11572 and ISO/IEC 11582.

### 6.6.3    Signalling between public networks and PINX

The signalling across the reference point T towards public networks is outside the scope of this Technical Report.

## 6.7 Management, administration and operation

### 6.7.1    Configuration management

NOTE      Configuration, as used in this Technical Report, is also called subscription registration.

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

#### 6.7.1.1    Configuration management of wireless terminals

##### 6.7.1.1.1    Configuration procedure (on-air)

Normally the WT 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 RE/RBS.

Examples of such types of data are:

-    WT's identity;

-    WT's visiting identity;

-    information about authentication key/process;

-    WT's class of service.

The method by which this configuration data is loaded into the WT over the air-interface is outside the scope of this Technical Report.

##### 6.7.1.1.2    Exchange of configuration data (on-air)

This function allows the exchange of subscription data between the network and the wireless terminal  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 WT. Normally the WT 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 wireless terminal 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 wireless terminal 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 wireless terminals

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

### 6.7.1.2.1 Network identity

Ideally the network identity of the WT shall be its directory numberIt is recommended that several identities may be allocated a given WT in order that it can access more than one application. As the WTs identities are transmitted unencrypted over the air-interface and thus commonly available a feature should be available allowing «secret» identities which only can be read by those having authorisation to do so.

## 7 PPM on top of WTM

## 7.1 WTM

WTM refers to the capability of a PISN to support PISN services to users of a WT as he/she moves around within the PISN. The PISN services may be provided at any appropriate radio access point to any WT within the coverage area provided the WT has access rights to that system. A PISN supporting WTM must incorporate provisions for automatically identifying, locating and tracking the WT both between calls and during a call.

If the user of a WT does not subscribe to the PPM service, there is a fixed and permanent association between the WT and the user. This user is called, in this report, a WTM user while a PISN user subscribing to both the PPM and the WTM service is referred to as a PPM user.

Figure 6 illustrates the WTM concept. It describes the state of the PISN after the WTM user has arrived at the Visitor PINX. The PISN has modified the WTM user's entry in the HDB which now points to the Visitor PINX. Also, a VDB entry has been established which specifies the WTM user's current access number and supports his access to PISN services at the Visitor PINX. The VDB can be reached from the Visitor PINX.
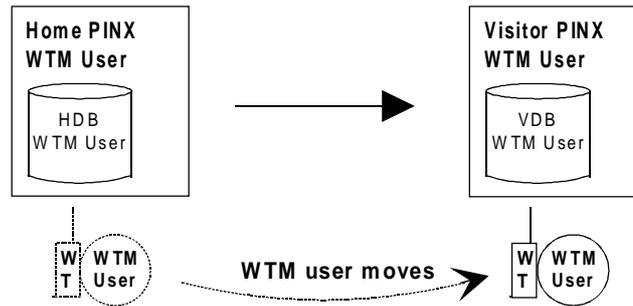
**Figure 6 — Illustration of WTM**

## 7.2 General aspects of providing PPM on top of WTM

In a PISN which supports both WTM and PPM, interactions arise between the two types of mobility if they are allowed to be used concurrently and without any restrictions. Before discussing possible interaction scenarios and implementation options for realising a consistent set of mobility services, it is proposed to maintain the following principles in a combined WTM - PPM environment:

a) PPM registration must be possible both on wired and on wireless terminals.

b) A PPM user must be allowed to register, by means of the usual procedure, on a WT which does not host any user at the time of registration.

c) The PISN services offered to a PPM user, as well as the PPM registration procedure, must be independent of whether the hosting terminal is wired or wireless.

## 7.3 Examples of PPM - WTM interactions

The following examples were chosen to highlight some of the problems and questions which arise in a combined WTM - PPM environment.

a) A PPM user registers on another PISN user's WT.

   **Problem**: How is the PPM registration updated in the PISN when both users move to another location area with the WT? Note that it cannot be expected from the PPM user to re-register in the new location area.

b) A PPM user who owns a WT registers on another terminal, leaving his WT without a PISN user (PISN number) assigned to it.

   **Problem**: How is the WT identified and tracked by the PISN? How are PPM registrations carried out on the WT?

c) A PPM user registers on a WT hosting another PPM user who owns the WT. Both users together move to another location area with the WT, where the WT owner leaves and registers on another terminal.

   **Problem**: It must be ensured that the separation of the WT owner from his WT neither affects the PISN service for the remaining PPM user, nor the possible registration of other PPM users on the WT.

d) Both the WTM user (with his WT) and a PPM user registered on the WT are outside their home areas.

   **Problem**: How are the WTM/PPM user's HDBs/VDBs "chained" together? What is the precise meaning of a WTM and PPM data base in a combined WTM - PPM environment? What are the advantages and disadvantages of the various options for organising the data bases?

These examples and associated questions indicate that a unified view of PPM and WTM needs to be adopted in order to implement both types of mobility in a consistent and efficient manner. Several distinct routes are identified to achieve this goal. Subclause 7.5 will introduce and discuss the most straightforward and promising options.


## 7.4    The concept of a "WT number"

A WTM user who does not subscribe to the PPM service is by definition not capable of registering at another access. However, if a WTM user does subscribe to the PPM service (such a user is referred to as a PPM user), he can register at any PISN terminal, thus leaving his WT without a PISN user assigned to it. In order for the PISN still to be able to identify and track the WT and allow PPM users to register on it using normal procedures, the following two alternative schemes are identified:

a)    A WT that is a PPM user's home terminal is assigned a permanent, unique identifier which may either be a PISN number or an alternative identifier. This "WT number" thus plays the role of a WTM number or an alternative identifier. However, since no PISN user is associated with the WT number, calls to and from the WT should be barred. This provision can be accomplished by adjusting the WT number's "service profile" accordingly (call barring). A PPM user can register on the WT exactly as in the case when it is owned by a WTM user.

An obvious advantage of this scheme is that all mobility and call handling procedures defined in WTM can be applied without any modifications. A drawback is that each WT that is a PPM user's home terminal is assigned a unique PISN number which does not correspond to a PISN user.

b)    A WT that is a PPM user's home terminal is assigned the same PISN number as the PPM user, rather than a different number. Since a single PISN number now corresponds to two different entities in the PISN (WT and PPM user), the PISN must distinguish between the WT and the PPM user in all its procedures. For example, in the case of an incoming call to a PISN number corresponding both to a WT and a PPM user, the call must always be routed to the PPM user. Similarly, when the WT initiates a location update procedure, the PISN must update the WT's location, rather than the location of the PPM user with the same PISN number.

Although this scheme avoids the inefficient use of PISN numbers, problems may arise in existing PISNs due to the fact that a single PISN number may correspond to two different PISN entities. For example, standard PISN management procedures and tools are based on the assumption that a PISN number uniquely identifies a PISN entity. Furthermore, new requirements on WTM or PPM may arise in the future which could be difficult or impossible to implement if scheme "b" is adopted. An example of such a requirement could be the emergency call service. In this service, a WT must support both outgoing and incoming emergency calls even if no PISN user is associated with it at the time of the call. If the WT's PISN number is not unique, emergency calls cannot be sent to the WT on an exclusive basis.

NOTE    The problem of identifying a wired terminal during a period when it does not host any PISN user is a PINX-internal matter, and is therefore not considered here. The only requirement is that PPM users must be able to register on such a terminal by means of the usual procedures, independent of whether or not the terminal hosts a PISN user.

The PPM standards should be independent of whether scheme "a" or scheme "b" is adopted.


## 7.5    Options for providing PPM on top of WTM

### 7.5.1          Basic options

In the following scenarios, it is assumed that the WT is used by a WTM user who does not subscribe to the PPM service. If the WT is the home terminal of a PPM user, the WTM user shown in Figures 8, 9 and 10 can be considered to be a WT number combined with this PPM user, as is illustrated in Figure 7.
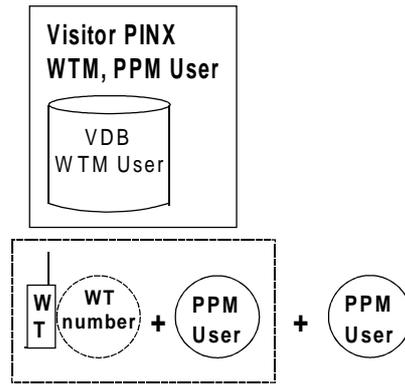
**Figure 7 — Illustration of the concept of a WT number**

#### 7.5.1.1 Basic Option 1

Figure 8 shows the state of the PISN which results when the PPM user registers on the WTM user's WT at their common Visitor PINX.



**Figure 8 — Illustration of Basic Option 1**

Basic Option 1 is specified in terms of the following configuration:

1) The PPM user's HDB points to the WTM user's access number at the WTM user's Home PINX.

2) According to the WTM specification, the WTM user's HDB points to the WTM user's VDB, which contains the WT's current access number. No VDB entry exists for the PPM user in this option.

The following operations apply under the two conditions indicated above:

a) Incoming WTM call: Incoming WTM calls arrive via the Home PINX of the WTM user; they are not affected by the PPM registration.

b) Incoming PPM call: An incoming PPM call arrives at the PPM user's Home PINX, where it is re-directed to the WTM user's access number at his Home PINX as specified in the PPM user's HDB. The WTM user's Home PINX in turn re-directs the call to the WT's current location as specified in the WTM user's HDB.

Outgoing WTM call: Outgoing WTM calls are not affected by the PPM registration.

a) Outgoing PPM call: An outgoing call is initiated by the PPM user at the Visitor PINX. In order to make the service profile available to the calling PPM user, the Visitor PINX consults the PPM user's HDB via his Home PINX. This remote and indirect query is necessary since, in this option, no VDB for the PPM user exists in the visitor area.

b) The PPM user re-registers in another visitor area: The new registration will proceed according to the applicable PPM registration procedures independent of the nature (Wireless or wired) of the old hosting terminal.

c) The WTM user moves with the PPM user to another location area: The location update will prompt the PISN to modify the WTM user's HDB entry accordingly. No other actions are necessary in this option.

Discussion:

The main advantage of Option 1 is the simple registration procedure involved when the WTM user moves with the WT and the PPM user registered on it. In fact, since the PPM user's Home PINX points to the WTM user's access at his Home PINX, only the usual WTM location update procedure needs to be invoked. However, because of the absence of a VDB entry for the PPM user, outgoing PPM calls will involve remote queries, via the PPM user's Home PINX, of the PPM user's HDB. Although a registration session for outgoing calls is possible at the Visitor PINX, the corresponding information, and thus the registration, is lost when the WT is moved to another location area. Incoming PPM calls involve, in addition to the PPM user's Home PINX and the Visitor PINX, also the WTM user's Home PINX (Home PINX PPM user -> Home PINX WTM user -> Visitor PINX).

### 7.5.1.2    Basic Option 2

Figure 9 shows the state of the PISN which results when the PPM user registers on the WTM user's WT at their common Visitor PINX.
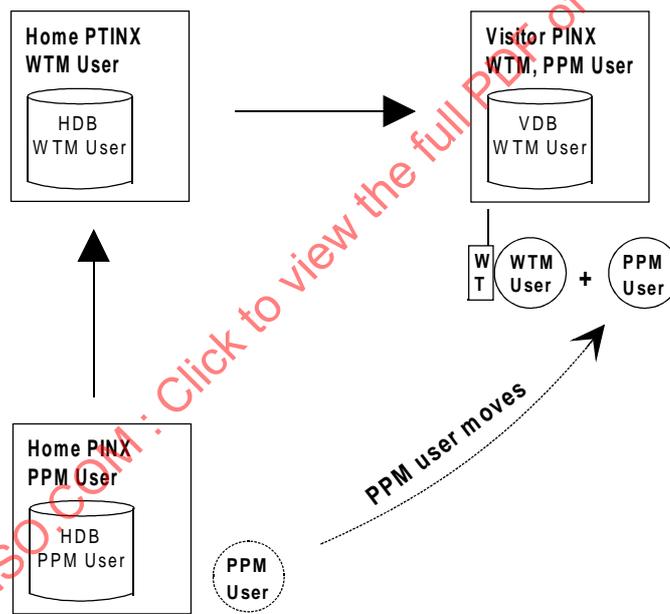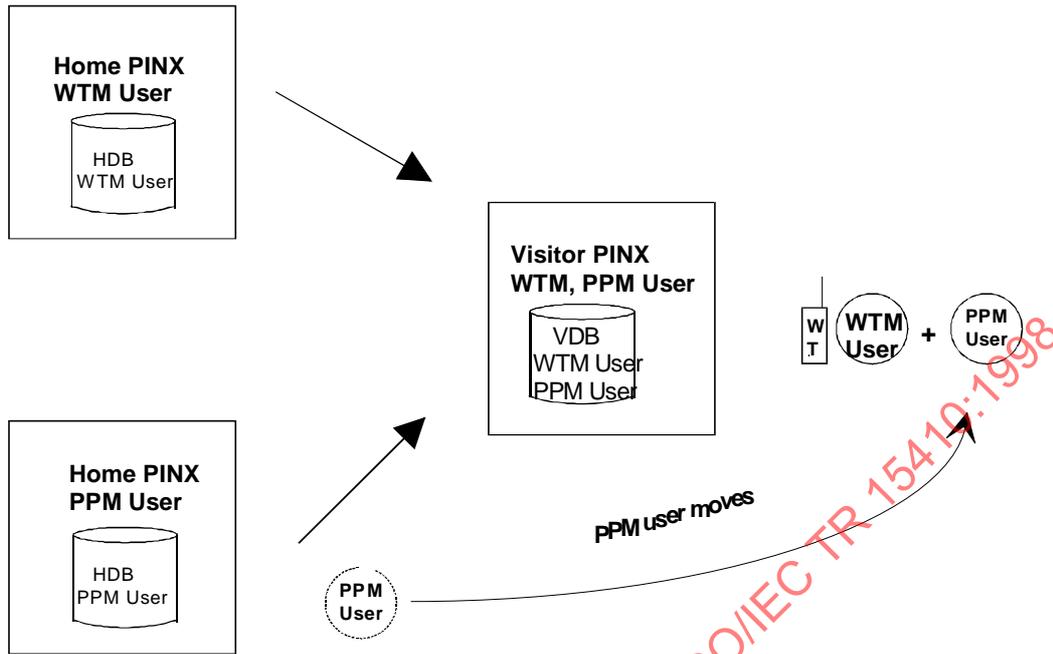
**Figure 9 — Illustration of Basic Option 2**

Basic Option 2 is specified in terms of the following configuration:

1) The PPM user's HDB points to the Visitor PINX.

2) The VDB in the visitor area contains the PPM user's entry which identifies his current access.

The following operations apply under the two conditions indicated above:

a) Incoming WTM call: Incoming WTM calls arrive via the Home PINX of the WTM user; they are not affected by the PPM registration.

b) Incoming PPM call: An incoming PPM call arrives at the PPM user's Home PINX, where it is re-directed to the current Visitor PINX as specified in the PPM user's HDB.

Outgoing WTM call: Outgoing WTM calls are not affected by the PPM registration.

a) Outgoing PPM call: An outgoing call is initiated by the PPM user at the Visitor PINX. In order to make his service profile available to the calling PPM user, the Visitor PINX consults the PPM user's VDB entry which is directly accessible from the Visitor PINX.

b) The PPM user re-registers in another visitor area: The new registration will proceed according to the applicable PPM registration procedures independent of the nature (Wireless or wired) of the old hosting terminal.

c) The WTM user moves with the PPM user to another location area: The location update will prompt the PISN to modify the WTM user's HDB entry according to the WTM user's new location, and establish the WTM user's New VDB entry. Secondly, when the WTM user's Old VDB entry is deleted, the Old Visitor PINX will detect the need for PPM re-registration, and invoke a remote PPM registration to establish a PPM registration session at

the New Visitor PINX. A corresponding message is sent to the WTM user's Home PINX, which is able to relay it to the New Visitor PINX where the hosting WT is now located. The subsequent procedures are the same as those required for local PPM registration.

Discussion:

Both incoming and outgoing PPM calls involve only the smallest possible set of procedures and data base queries. In particular, incoming PPM calls are directly forwarded to the Visitor PINX, without involving the WTM user's Home PINX. However, an extensive (though straightforward) set of procedures needs to be invoked when the WTM user moves with the WT and the PPM user registered on it. These update procedures involve data flows and interactions between WTM-related entities and PPM-related entities.

### 7.5.1.3 Basic Option 3

Figure 10 shows the state of the PISN which results when the PPM user registers on the WTM user's WT at their common Visitor PINX.



**Figure 10 — Illustration of Basic Option 3**
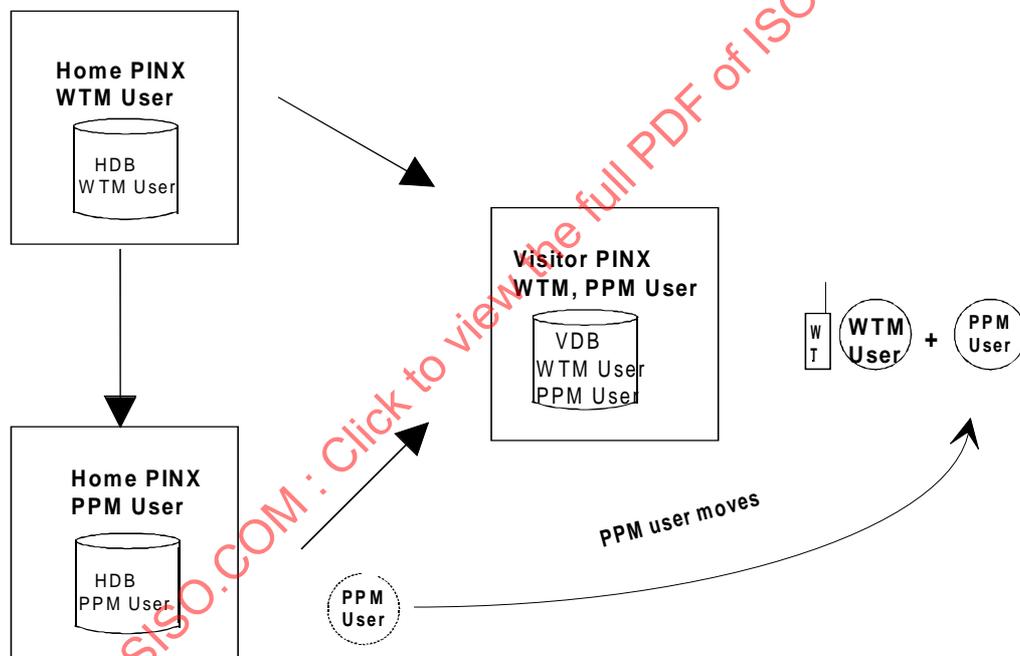
Basic Option 3 is specified in terms of the following configuration:

1) The PPM user's HDB points to the Visitor PINX (as in Basic Option 2).

2) The VDB in the visitor area contains the PPM user's entry that identifies his current access (as in Basic Option 2).

3) The WTM user's HDB contains an entry specifying the identity of the PPM user registered on the relevant WT.

The following operations apply under the conditions indicated:

a) Incoming WTM call: Incoming WTM calls arrive via the WTM user's Home PINX; they are not affected by the PPM registration.

b) Incoming PPM call: An incoming PPM call arrives at the PPM user's Home PINX, where it is re-directed to the current Visitor PINX as specified in the PPM user's HDB.

Outgoing WTM call: Outgoing WTM calls are not affected by the PPM registration.

a) Outgoing PPM call: An outgoing call is initiated by the PPM user at the Visitor PINX. In order to make his service profile available to the calling PPM user, the Visitor PINX consults the PPM user's VDB which is directly accessible from the Visitor PINX.

b) The PPM user re-registers in another visitor area: The new registration will proceed according to the applicable PPM registration procedures independent of the nature (Wireless or wired) of the old hosting terminal. Additionally, the corresponding PPM entry in the WTM user's HDB is deleted.

c) The WTM user moves with the PPM user to another location area: The location update will prompt the PISN to modify the WTM user's HDB entry according to the WTM user's new location, establish the WTM user's New VDB entry, and delete his Old VDB entry. The PPM entry in the WTM user's HDB remains unchanged. Furthermore, the WTM user's Home PINX will instruct the PPM user's Home PINX to update the PPM user's HDB entry according to the new location. The PPM user's Home PINX will then order the PPM user's Old VDB entry to be deleted, and initiate the establishment of his New VDB entry.

Discussion:

As in Basic Option 2, both incoming and outgoing PPM calls in Basic Option 3 involve only the smallest possible set of procedures and data base queries. Compared with Basic Option 2, less extensive operations need to be invoked when the WTM user moves with the WT and the PPM user registered on it. However, a considerable disadvantage of Basic Option 3 is that a WTM entity (the WTM user's HDB) is modified when a PPM user registers on the WTM user's WT.

### 7.5.2   Summary of discussion of the basic options

The above three basic options for providing PPM on top of WTM differ with respect to the procedures involved for PPM registration and the handling of incoming and outgoing calls.

In Basic Option 1, no VDB entry is foreseen for the PPM user in the visitor area. As a consequence, no PPM re-registration is required when the PPM user moves with the hosting WT. On the other hand, extensive and time-consuming procedures are required for incoming and outgoing PPM calls. Moreover, a registration session for outgoing calls is lost when the WT is moved to another location area.

Basic Option 2 entails simple and straightforward procedures to handle incoming and outgoing calls. On the other hand, extensive though straightforward data flows occur between WTM and PPM related entities when the PPM user moves with his hosting WT. The WTM service itself is not affected.

In Basic Option 3, incoming and outgoing calls are handled as efficiently as in Basic Option 2. In contrast to Basic Option 2, however, a PPM-related entry is required in the WTM user's HDB, thus requiring changes to existing WTM standards.

In conclusion, considering the advantages and disadvantages of these options, Basic Option 2 is identified as the most promising implementation route for providing PPM in a WTM environment. Basic Option 2 should therefore be the sole basis for the PPM standards.

### 7.5.3 Extended options

The extended options proposed below are based on the basic options introduced in subclause 7.5.1 In the extended options. However, it is additionally assumed that the WT has the capability to store the identities of the PPM users registered on it (PPM numbers). This capability involves potential benefits in the case when a registered PPM user moves with his hosting WT to another visitor (location) area, as discussed below. Provisions must also be made to delete this registration when the PPM user leaves the WT. The de-registration of a PPM user from a WT should be invoked by the PISN at the time when the PPM user registers on another terminal; alternatively, the PPM user may de-register from the WT before leaving the location area.

NOTE    The capability of a WT to store the identities of PPM users may be implemented by introducing a "PPM card", which would store the PPM number as well as potential authentication parameters. Inserting the PPM card into a WT (or wired terminal) would invoke PPM registration, and removing it would invoke de-registration.

The PPM standards should not assume any PPM-specific intelligence in the terminal.

#### 7.5.3.1    Extended Option 1

In Basic Option 1, the movement of a PPM user with his hosting WT does not involve any updates of PPM-related data bases. Therefore, there are no advantages associated with the capability of a WT to store PPM numbers.

#### 7.5.3.2    Extended Option 2

The re-registration process for a PPM user moving with the hosting WT is rather complex in Basic Option 2. These procedures, which involve several interactions between WTM-related entities and PPM-related entities, are simplified considerably if the WT can store PPM numbers.

If, in Extended Option 2, a PPM user moves with his hosting WT, the New Visitor PINX is informed by the WT about the registered PPM user's identity. This is equivalent to an explicit PPM (re-) registration action carried out by the PPM user himself. As a result, it is possible to have both an automatic WTM re-registration (as usual), and an automatic PPM re-registration. In fact, after the WTM location update has been completed, the PISN-internal PPM re-registration procedures can proceed exactly as in the case of a user-activated PPM registration, without any interaction with WTM-related entities.

#### 7.5.3.3    Extended Option 3

In Basic Option 3, the re-registration of a PPM user moving with his hosting WT was somewhat simpler than in Basic Option 2 due to fact that the registered PPM number was stored in the WTM user's HDB. In Extended Option 3, the registered PPM number is stored in the WT, which obviates the need to store it also in the WTM user's HDB. A consequence, Extended Option 3 is identical to Extended Option 2.

## 7.6 Information flows and procedures for PPM using WTM terminals

This subclause outlines the information flows and procedures required for PPM registration, incoming PPM calls, and outgoing PPM calls employing WTM terminals.

In subclause 7.5, six options for implementing PPM on top of WTM were introduced. The following analysis will concentrate only on the most promising options, Basic Option 2 (see 7.5.1.2) and Extended Option 2 (see 7.5.3.2).

### 7.6.1 Information flows for PPM registration

As regards PPM registration in a WTM environment, two different situations must be distinguished:

a) The PPM user leaves his previous visitor area, where he has been registered on a wired or Wireless terminal, and registers on a WT in a new visitor area.

b) The PPM user moves with his hosting WT (and the WT's WTM user) to a new location area. In this case, PPM re-registration will have to be initiated by the PISN along with WTM location registration (automatic PPM re-registration).

#### 7.6.1.1 Basic Option 2

#### 7.6.1.1.1 PPM registration

The information flows associated with a PPM registration procedure in Basic Option 2 are shown in Figure 11. The figure depicts the procedures which occur in the PISN when a PPM user registers on a WT. It is assumed that the WT is already registered at the time when the PPM user arrives.
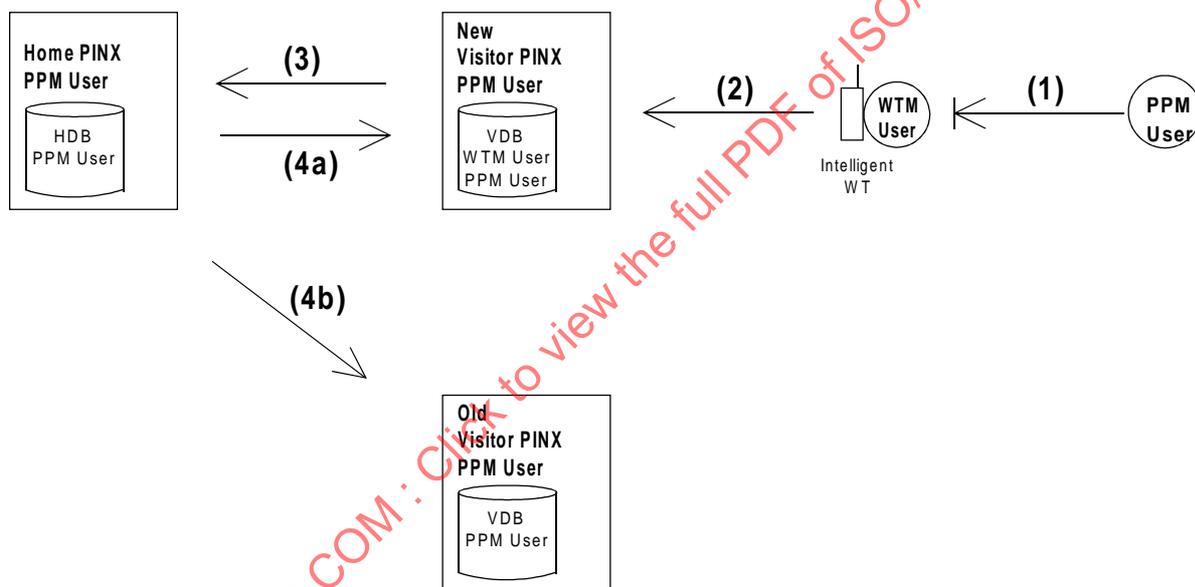


**Figure 11 — Information flows for PPM registration on a WT for Basic Option 2**

The information flows indicated in Figure 11 above are the following:

1) The PPM user registers by identifying himself (e.g. in terms of his PPM number), and by specifying the type of PPM service he intends to use at the hosting terminal; authentication procedures may apply.

2) The hosting WT registers the PPM user on the New Visitor PINX. At the time of registration, the hosting terminal may host only the WTM user, or one or more other PPM users.

3) The PPM user's New Visitor PINX informs the PPM user's Home PINX about the registration attempt. The Home PINX updates the PPM user's HDB according to the PPM user's New Visitor Area.

4)

   a) The PPM user's Home PINX transfers the required user profile data to the New Visitor PINX, which updates its associated VDB accordingly.