EG 201 027 V1.1.1 (1997-06)

ETSI Guide

Business TeleCommunications (BTC); Cordless Terminal Mobility (CTM); Interworking between private and public networks; General principles

Reference
DEG/CN-03015 (9ic00icq.PDF)

Keywords
PISN, mobility, CTM

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Project Corporate Networks (CN).

1 Scope

The ETSI Guide (EG) analyses the principles of interworking Cordless Terminal Mobility (CTM) between private and public networks.

This EG considers the case, where a CTM user, who has only a subscription in one network, which is called the CTM user's home network, is roaming into another network, which is called the visited network. Two scenarios are considered. In the first scenario a public CTM user is roaming in a private network and in the second a private CTM user is roaming in a public network. The EG lists some basic requirements for inter-network-roaming and points out some problems and further work areas. It contains interworking examples for some basic mobility procedures and covers location registration, call handling and authentication.

The support of supplementary services and security measures in addition to authentication are not covered in this EG.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

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

[1] ETS 300 691: "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Roaming Location Handling Services: Service Description".

[2] ETS 300 692: "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Roaming Location Handling Services: Functional capabilities and information flows".

[3] ETS 300 694: "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Call Handling, Additional Network Features: Service Description".

[4] ETS 300 695: "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Call Handling, Additional Network Features: Functional capabilities and information flows".

[5] I-ETS 300 768 (1997): "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Authentication Supplementary Services: Service Description".

[6] I-ETS 300 769 (1997): "Private Telecommunication Network (PTN); Cordless Terminal Mobility (CTM), Authentication Supplementary Services: Functional capabilities and information flows".

[7] CCITT Recommendation E.164 (1991): "Numbering plan for the ISDN era".

[8] ETS 300 345: "Integrated Services Digital Network (ISDN); Interworking between public ISDNs and private ISDNs for the provision of telecommunications services; General aspects".

[9] ETS 300 415: "Private Telecommunication Network (PTN); Terms and definitions".

[10] ETS 300 189: " Private Telecommunication Network (PTN); Addressing".

[11] CCITT Recommendation E.212 (1988): "Identification plan for land mobile stations".

[12] TCR-TR 034: "BTC; VPN; Services and networking aspects; Standardization requirements and work items".

[13] ETS 300 693: "Private Telecommunication Network (PTN); Inter-exchange signalling protocol; Cordless Terminal Location Registration (CTLR)".

[14] ETS 300 696: "Private Telecommunication Network (PTN); Inter-exchange signalling protocol; Cordless Incoming Call Additional Network Feature (ANF-CTMI)".

3 Definitions

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

address: As defined in ETS 300 189 [10].

attach: The process whereby a Portable Part (PP) within the coverage area of a Fixed Part (FP) to which it has access rights, notifies the FP that it is operative.

authentication: The process of validating an identity, e.g. of a user, of a terminal, or of a network.

cipher key: A value that is used to determine the transformation of plain text to ciphertext in a cryptographic algorithm.

coverage area: The area over which cordless communication can be established and maintained.

detach: The process whereby a Portable Part (PP) within the coverage area of a Fixed Part (FP) to which it has access rights, notifies the FP that it is inoperative.

gateway-PINX functionality: Within the context of a call the functionality of a PINX required to interconnect end-PINXs or transit-PINXs with nodes of other public or private networks.

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

home network: Network where the home data base of a CTM user is located.

ISDN numbering plan: The numbering plan explicitly relating to the global ISDN domain, as defined in CCITT Recommendation E.164 [7].

location area: The domain in which a PP may receive (and/or make) calls as a result of a single location registration.

location deletion: The process whereby the home network informs the previous visited network that the CTM user is registered in an other network.

location deregistration: The process whereby the visited network informs the home network that the CTM user is no longer reachable in this network.

location registration: The process whereby the position of a portable part is determined to the level of one location area, and this position is updated in one or more databases.

number: An address restricted to containing numerical values, as defined by a numbering plan.

numbering plan: A plan allocating numbers to the addressable entities of its domain.

private: An attribute indicating that the application of an item qualified by "private", e.g. a network, a unit of equipment, a service, is offered to a pre-determined set of users. This attribute does not indicate any aspects of ownership.

NOTE 1: This definition does not include legal or regulatory aspects.

Private Numbering Plan (PNP): The numbering plan explicitly relating to a particular private numbering domain, defined by the administrator of that domain.

Private Numbering Plan (PNP) number: A number defined by a PNP.

Private Integrated Services Network (PISN): A network serving a pre-determined set of users (different from a public network which provides services to the general public). The attribute "private" does not indicate any aspects of ownership.

NOTE 2: This definition does not include legal or regulatory aspects.

Private Integrated Network Exchange (PINX): A PISN nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services. The nodal entity can be implemented by one or more pieces of equipment located on the premises of the private network administrator or by equipment co-located with, or physically part of, a public network.

PISN number: A number defined by a PISN numbering plan.

PISN numbering plan: The generic designation for the numbering plan(s) chosen as native by a PISN administrator for the administrator's particular PISN.

public: An attribute indicating that the application of an item qualified by "public", e.g. a network, a unit of equipment, a service, is offered to the general public. This attribute does not indicate any aspects of ownership.

NOTE 3: This definition does not include legal or regulatory aspects.

roaming: The movement, without a call being in progress, of a cordless terminal or a mobile user from one coverage area to another coverage area.

RS: A value used to establish authentication session keys.

session key: A key which is used only for a single session; a session may be a single connection or call, or it may be a number of calls made by a particular user through a particular system (e.g. the calls made by a roaming portable with a particular visited network).

Terminal Equipment (TE): An item of equipment attached to a telecommunication network to provide access for a user to one or more services.

user: An entity using the services of a network via terminal equipment.

NOTE 4: A user may be a person or an application process.

visited network: Network where the visitor data base of a CTM user is located.

visitor area: The coverage area of a visitor database.

Visitor Data Base (VDB): The database in which location information concerning a cordless terminal or a mobile user is stored, as long as the cordless terminal or the mobile user are localized in the corresponding visitor area.

4 Symbols and Abbreviations

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

CCF	Call Control Function
CTM	Cordless Terminal Mobility
CTMid	Cordless Terminal Mobility Identity
CUSF	Call Unrelated Service Function
DSS1	Digital Signalling System number 1
ENQ	Enquiry
FP	Fixed Part (cordless sub-system)
G-id	PISN number of G-PINX
G-ISDN	Gateway PINX ISDN number
G-LE	Gateway Local Exchange
G-LEid	G-LE identity
G-LEold	Gateway Local Exchange old
G-PINX	Gateway PINX
GSM	Global System for Mobile Communications

HDB	Home Data Base
HLR	Home Location Register
H-PINX	Home PINX
IMSI	International Mobile Subscriber Identity
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network
KS	Session Key
LD	Location Deletion
LDB	Location Data Base
LD-cfm	Location Deletion confirm
LE	Local Exchange
LR	Location Request
LR-cfm	Location Request confirmation
MAP	Mobile Application Part
MCC	Mobile Country Code
MM	Mobility Management
MNC	Mobile Network Code
MSC	Mobile Switching Centre
MSIN	Mobile Station Identification Number
NCSF	Non Call Service Function
NMSI	National Mobile Station Identity
PCCF	Peer Call Control Function
PCN	Personal Communication Network
PINX	Private Integrated Network Exchange
PISN	Private Integrated Services Network
PISNN	PISN Number
PNC	Private Network Code
PNP	Private Numbering Plan
PP	Portable Part
PSCF	Peer Service Control Function
PSDF	Peer Service Data Function
PSSF	Peer Service Switching Function
QSIG	Q Signalling Protocol
RAND	Random number
RES	Calculated Response
R-id	Radio identity
RN	Roaming Number
RS	Roaming Session
SCF	Service Control Function
SCFmm	Service Control Function mobility management
SCFsl	Service Control Function service logic
SDF	Service Data Function
SDFmm	Service Data Function mobility management
SDFsl	Service Data Function service logic
SP	Service Provider
SS7	Signalling System number 7
SSF	Service Switching Function
TE	Terminal Equipment
T-PISNN	Temporary PISN Number
VAI	Visitor Area Identity inside the public network
VDB	Visitor Data Base
V-id	Visited Area Identity inside the private network
VLR	Visitor Location Register
V-PINX	Visitor PINX
VPN	Virtual Private Network

5 Introduction

The present document will attempt to summarize the distinct features of a private environment leading to the current PISN mobility standard proposals. Then some basic assumptions are listed and a model for inter-network roaming is developed. Examples are given, that show how CTM procedures can be interworked between a private and a public network. The last part of the document will present problems related to such interworking scenarios that should be addressed by proper standardization bodies.

In PISNs the signalling mechanism for CTM is based on QSIG. A fundamental feature of QSIG is that additional information can be transported in association with a basic call. This is generally not true for all nodes of the PSTN, thus forcing e.g. MAP to rely on roaming numbers for call set-up to mobile users.

The standards for CTM in private networks are designed to allow faster call set-up than possible when using the dynamic roaming number mechanism. This is realized by only doing one database enquiry during call set-up. Using dynamic roaming numbers, the home location has to perform a roaming number enquiry in addition to the call routeing and the visited location has to allocate a roaming number to be used in the call.

The scope of the standards for CTM in private networks ETS 300 691 [1], ETS 300 692 [2], ETS 300 694 [3], ETS 300 695 [4], I-ETS 300 768 [5], I-ETS 300 769 [6], ETS 300 693 [13] and ETS 300 696 [14] is limited to mobility inside one PISN. Work has been started to produce a second edition of these standards where the scope is extended to include mobility between networks. The present document also provides a basis for this work.

6 Inter-network roaming, public/private network

6.1 Assumptions

The study is made on a number of assumptions:

1. CTM users have only one subscription. They may be either public CTM users or private CTM users. Public CTM users are CTM users whose subscription has been established on a contractual basis with a service provider via a public network operator. Private CTM users are CTM users who belong to a PISN and who are allowed by the PISN authority to use a cordless terminal with the corporate facilities of a PISN user.

NOTE 1: Arrangements between parties, such as network operators and service providers, to allow inter-network roaming, are outside the scope of this present document.

2. The existence of a common CTM user identifier recognized by both the public and the private network. This identifier is called CTM user identity (CTMid) in this document. This CTMid identifies the CTM user and can be used to find the home network of the CTM user. Possible candidates include CCITT Recommendation E.164 [7] and CCITT Recommendation E.212 [11]. The annex A identifies the capacity of the International Mobile Subscriber Identity (IMSI) for inter-network CTM identification.

   It shall always be possible to derive the routeing information in terms of the complete PISN number from the above identity in the case where it is used to identify a CTM user within a private network.

3. The mobility management procedures may be different inside the public and private networks, but the procedures and protocol elements at the interface shall be well defined and shall be independent from the internal procedures of the networks. Therefore neither network needs to know the infrastructure of the other network.

   The subclauses 7.3 and 7.4 indicate the procedures, which are required at the interface. For the examples in annex B of this document public procedures based on the MAP are assumed to be used inside the public (land mobile) network. For the examples in annex C of this document public procedures based on the Intelligent Network Application Part (INAP) are assumed to be used inside the public (fixed) network. In both cases the procedures at the network interface are the same.

4. For the services "Outgoing call" and "PP-Authentication" two scenarios are described in this document.

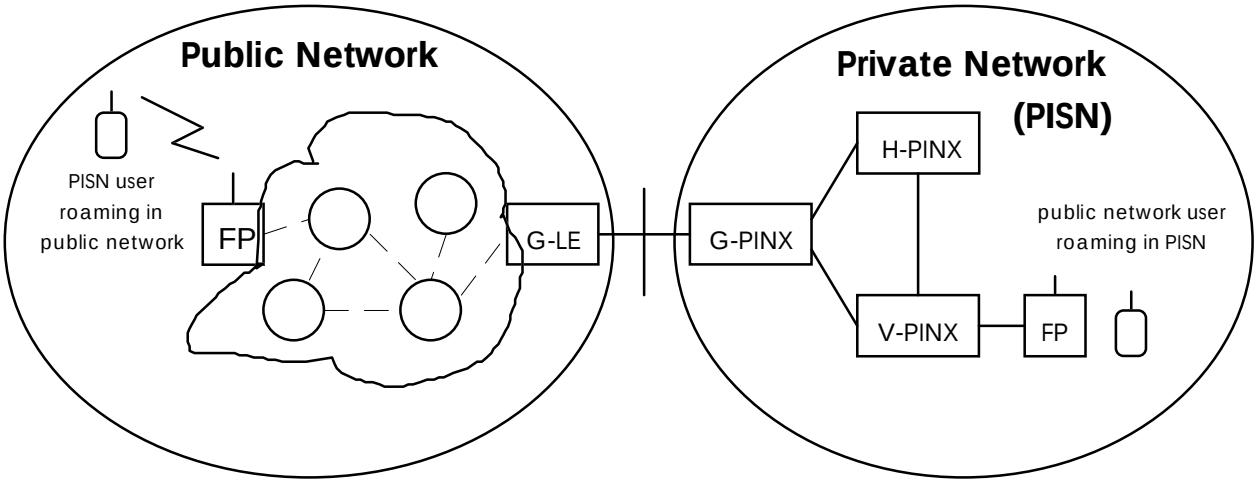
A) All the signalling and every call is routed via the home network which provides the service to the CTM user. This is the simplest possibility and provides the highest probability, that the service given to the CTM user is independent from his location.

B) The visited network provides the service to the CTM user. This requires user specific information, to be available in the visited network. In this scenario it is likely, that the service will be different in different networks, but routeing via the home network can be avoided.

NOTE 2: For the case of a CTM private user, who roams in a corporate network coverage area provided by the public network infrastructure, the VPN model is a mean to handle the scenario (B).

6.2 Model for inter-network roaming

The study on inter-network roaming is based on the following model:



The model is simplified to show only those entities that are involved in location updating and call handling. The following entities are used:

FP:	Fixed Part (cordless sub-system offering radio access to the CTM user)
G-LE:	Gateway Local Exchange
G-PINX:	Gateway PINX (containing LDB)
H-PINX:	Home PINX (containing HDB)
V-PINX:	Visitor PINX (containing VDB)

The G-LE is the access point for the G-PINX towards the public network.

The G-PINX performs the necessary mapping between the protocol used at the interface to the public network and the procedures used in the private network. The G-PINX will look to the PISN like a V-PINX for PISN users roaming in the public network and like an H-PINX for public users roaming in the PISN. The interworking requirements are concentrated in the G-PINX. Besides the creation of a G-PINX no special modification should be necessary in the PISN.

The following information flows show only those service elements that are additional to basic call and are necessary to support inter-network roaming.

6.3 A public CTM user roaming in a private network

This subclause is dealing with the case, where the public CTM user is roaming in a private network. Therefore the home network corresponds to the public network and the visited network corresponds to the private network.

6.3.1 Location registration

The following figure shows location registration for the case where the public network user roams from the public network to the PISN.

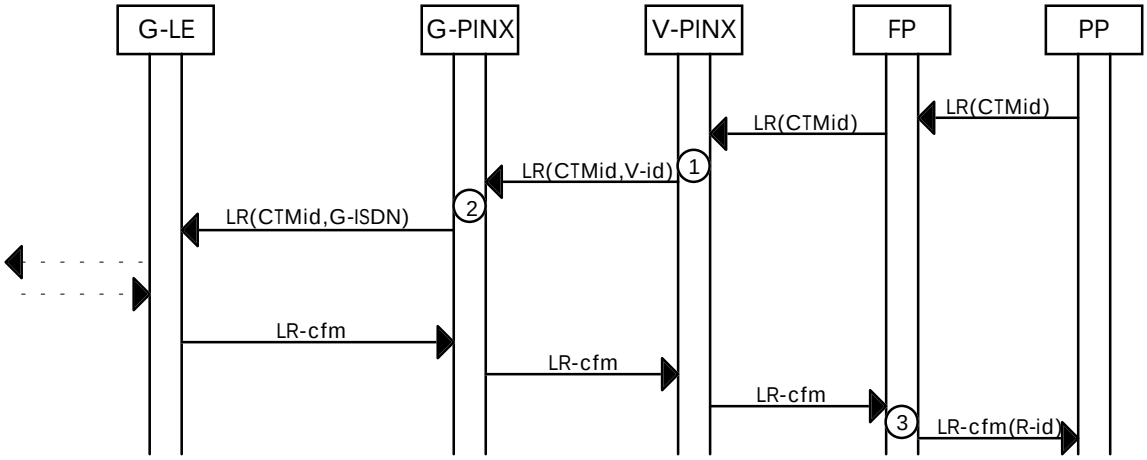


Figure 1: Location registration, public network user roaming in PISN

A public CTM user performs a Location Registration (LR) to the PISN using its CTM user identity (CTMid) for identification. The analysis of the CTMid shows that the CTM user is unknown to the network, but the CTMid can be used to identify the responsible G-PINX.

NOTE 1: The V-PISN may use the PISN enquiry mechanism (ENQ) to obtain a temporary PISN number (T-PISNN) assigned by the G-PINX from its own range. The T-PISNN can subsequently be used for routeing and internal identification of the CTM user while roaming in the PISN.

The V-PINX performs a location registration using the CTMid to identify the CTM user and provides a PISN number V-id for its own identification ①. The G-PINX forwards the location registration to the G-LE in the public network ②. This information contains the CTMid plus an E.164 number (G-ISDN) to identify the G-PINX.

The G-LE performs a mapping of the location registration to the corresponding public network procedure.

The location registration confirmation is sent from the G-LE to the G-PINX and passed on to the V-PINX, FP ③ and PP. During the location procedure an identity "R-id" to be used subsequently at the air interface could be assigned. In the location area there is an unique temporary relation between the CTMid and R-id.

NOTE 2: Authentication may take place during location registration.

NOTE 3: The G-LE may transfer authentication parameters to the G-PINX.

6.3.2 Location deletion in the private network

When the public network user leaves the private network and performs a location registration in an other network, then the public network uses the location deletion procedure to remove the entry of the public CTM user from the private network.

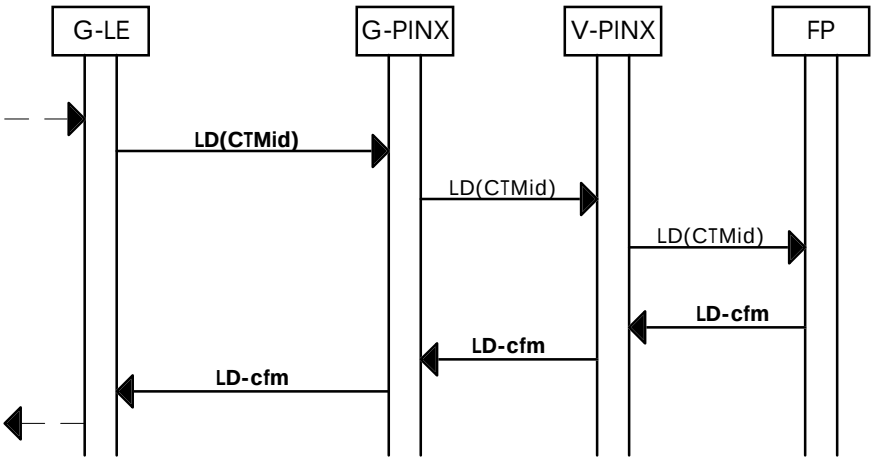


Figure 2: Location deletion, public network user roaming from PISN into other network

LD: Location Deletion
LD-cfm: Location Deletion confirm

The G-LE sends Location Deletion to the G-PINX including the CTMid to identify the CTM user, who's entry has to be removed from the PISN data base(s). The G-PINX forwards the location deletion to the V-PINX, which sends it to the FP. Then a Location Deletion confirm is sent back to the G-LE.

6.3.3 Location deregistration

The private network uses the location deregistration procedure to inform the public network about the location deregistration of the public CTM user from the private network.

NOTE 1: This procedure may by initiated by the CTM user or by the private network.

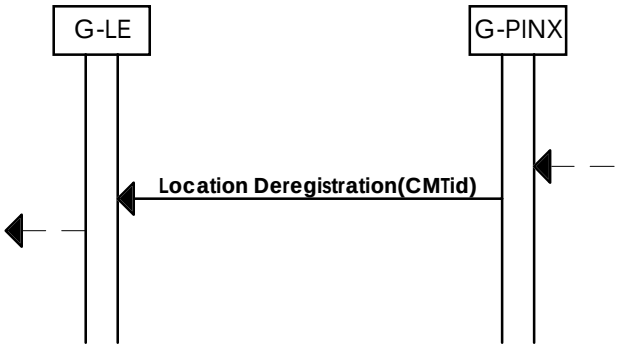


Figure 3: Location deregistration of the public network user

The G-PINX sends Location Deregistration to the G-LE including the CTMid to identify the CTM user, who's location should be deregistred.

NOTE 2: There is no confirmation of user initiated location deregistration (detach). Therefore it may be difficult to apply authentication.

6.3.4 Incoming call

The following figure shows an incoming call for the case where the public network user has roamed from the public network to the PISN.

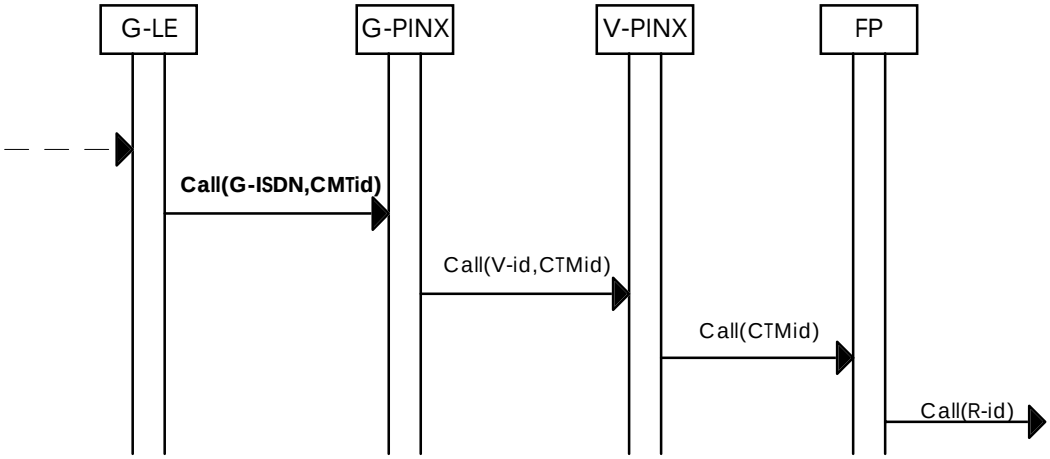


Figure 4: Incoming call, public network user roaming in PISN

G-ISDN: E.164 number to identify G-PINX
R-id: Radio identity

The G-LE forwards the call to the G-PINX, including the CTMid to identify the called user. G-ISDN is the address of the G-PINX and was provided by the G-PINX to the G-LE during the location registration procedure. At this point the PISN mobile call handling procedures are applied generating a call to the V-PINX with the user identified by the CTMid. V-id is the address of the V-PINX and was provided by the V-PINX to the G-PINX during the location registration procedure.

When the call gets to the FP, the local mapping information is finally used to insert an identifier as used at the radio interface before presenting the call to the CTM user.

NOTE 1: Authentication may be performed for incoming calls.

NOTE 2: To encrypt the radio link it is necessary that the home network provides some (secret) information to the visited network. This information may be either the cipher key itself or other information (e.g. an authentication session key KS and the corresponding RS value) which allows to derive the cipher key.

6.3.5 Outgoing call

For the service "Outgoing call" two scenarios are described in this subclause. The first one is that the visited network relays the signalling between the CTM user and the home network. The second scenario is that the visited network itself provides the service.

6.3.5.1 Outgoing call when routed via the G-LE

The following figure shows an outgoing call for the case where the public network user has roamed from the public network to the PISN and the call is routed to the G-LE.

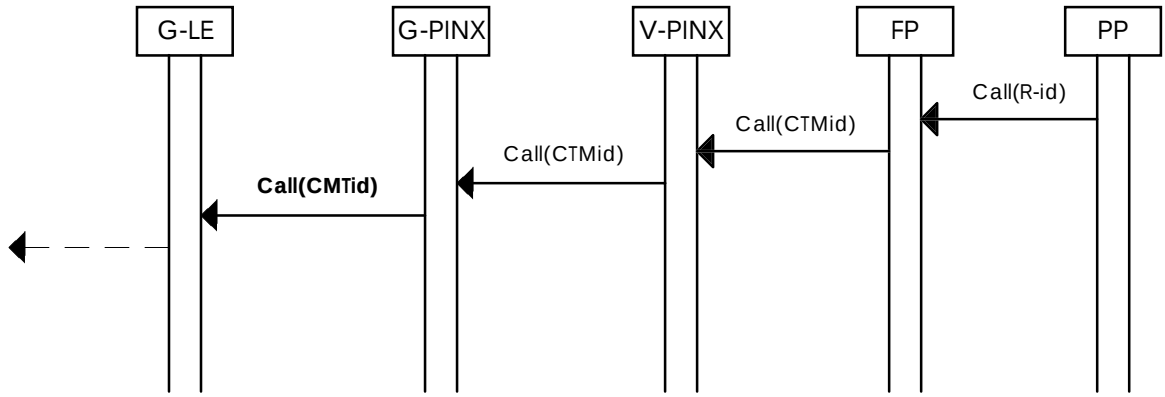


Figure 5: Outgoing call, public network user roaming in PISN

The call from the public CTM user is forwarded from the FP to the V-PINX, which passes it on to the G-PINX. The G-PINX passes the call over to the G-LE. The calling CTM user is identified by its CTMid.

NOTE 1: Depending on the roaming agreement and the information that has been received during location registration of that CTM user, the V-PINX may react differently. The V-PINX may e.g. continue with the call or authenticate the user or send the information, that the user has requested a call to the G-PINX or forward the call to the G-PINX. The latter case is shown in figure 5. It allows the home network to apply authentication and to provide additional services to its CTM user.

NOTE 2: To encrypt the radio link it is necessary that the home network provides some (secret) information to the visited network. This information may be either the cipher key itself or other information which allows to derive the cipher key.

6.3.5.2 Outgoing call with local call handling

The following figure shows an outgoing call for the case where the public network user has roamed from the public network to the PISN and the call is handled by the V-PINX.

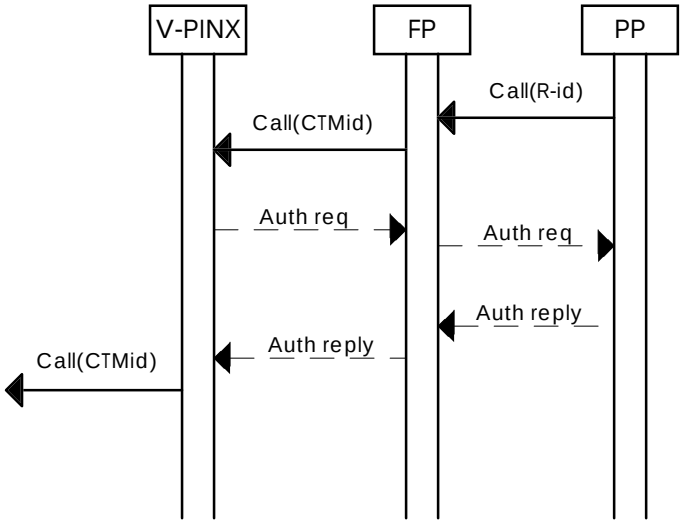


Figure 6: Outgoing call, public network user roaming in PISN

The call from the public CTM user is forwarded from the FP to the V-PINX which further processes the call.

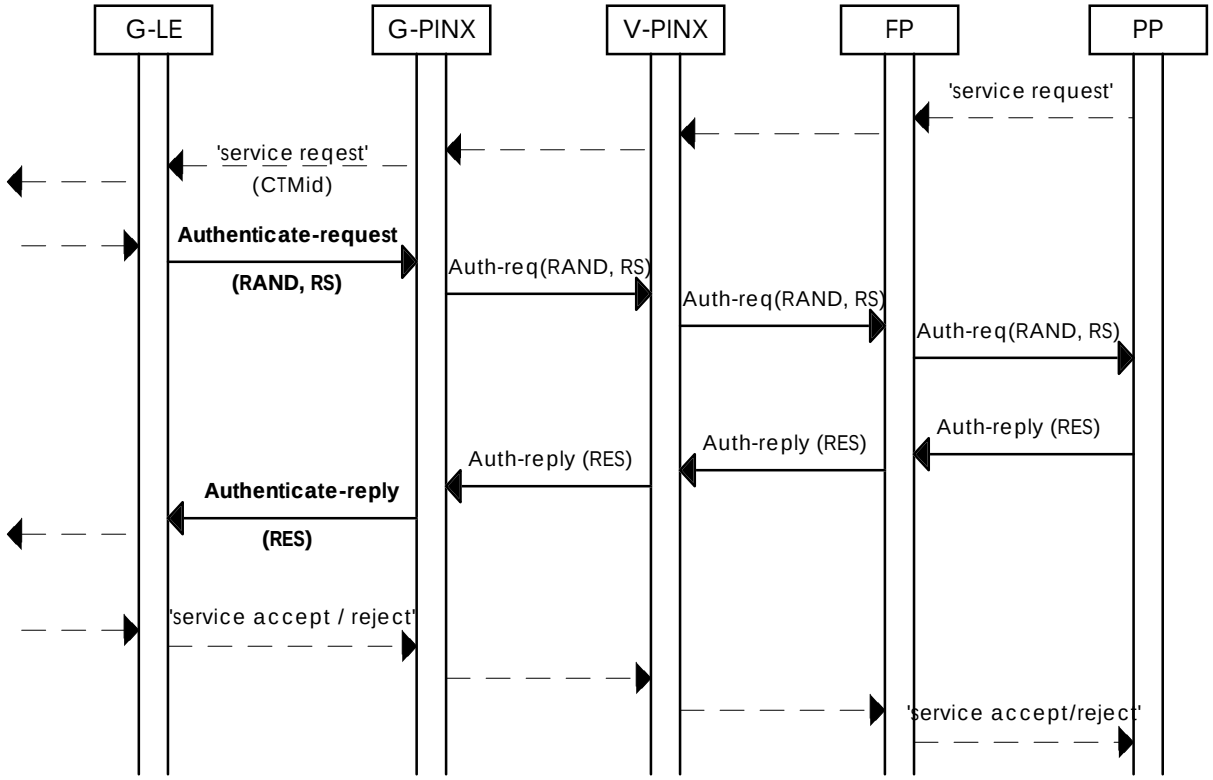
NOTE: If the private network has previously (e.g. during location registration) received the necessary authentication parameters (e.g. a session key KS and the corresponding RS value),then the V-PINX can perform authentication to check the CTMid. The V-PINX may switch on encryption for the radio link, by e.g. using a derived cipher key.

6.3.6 PP-Authentication

For the service "PP-Authentication" two scenarios are described in this subclause. The first one is that the home network performs the authentication and the visited network relays the signalling between the CTM user and the home network. The second scenario is that the visited network itself authenticates the CTM user.

6.3.6.1 PP-Authentication performed by the home network

The following figure shows authentication performed by the home network for the case where the public network user has roamed from the public network to the PISN.



NOTE: The parameter RS is included if required.

Figure 7: Authentication, public network user roaming in PISN

Typically the public network may invoke authentication to verify the CTM users identity, when the CTM user requests a service, e.g. outgoing call or location registration. The G-LE starts authentication by sending an Authenticate-request message containing a random number (RAND), if required a second parameter (RS) may be included. The authentication request is forwarded via the G-PINX, the V-PINX and the FP to the CTM user. The Authentication reply from the CTM user, which contains the authentication result (RES) is passed back via the FP, V-PINX and G-PINX to the G-LE. Depending on the authentication result the public network may then accept or reject a service request from the (public) CTM user.

NOTE: It may be necessary to transfer a cipher key, which might have been created during the authentication process.

6.3.6.2 PT-Authentication performed by the visited network

If the PISN wants to authenticate the public CTM user, then the G-LE has to provide authentication parameters to the G-PINX. These parameters could e.g. be a session key KS plus the corresponding RS value. Alternatively one or more challenge(s) together with the response(s) (possibly also including the derived cipher key(s)) could be provided.

6.4 A private CTM user roaming in a public network

This subclause is dealing with the case, where the private CTM user is roaming in a public network. Therefore the home network corresponds to the private network and the visited network corresponds to the public network.

6.4.1 Location registration

The following figure shows location registration for the case where the PISN user roams from the PISN to the public network.

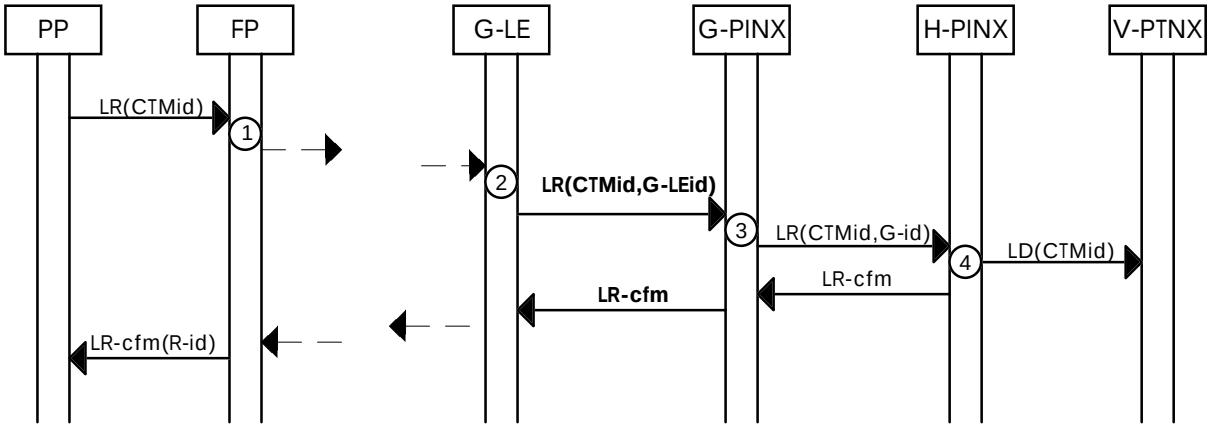


Figure 8: Location registration, PISN user roaming in public network

A private CTM user performs a location registration to the public network using the CTMid for identification. The analysis of the CTMid shows that the CTM user is a visitor in this network but contains sufficient information to direct the location registration ① towards the G-PINX.

The G-LE forwards the location registration to the G-PINX. It may include an identifier G-LEid which is an E.164 number that is used to address the G-LE ②. The G-LEid is only needed in the case of multiple G-LEs.

The G-PINX performs a location registration in the PISN and uses G-id the PISN number of the G-PINX as an indication of the new visited area ③.

The H-PINX performs a location deletion procedure towards the previous visited network, which might be a V-PINX as indicated in the figure above ④ or a visited public network as shown in the following subclause.

6.4.2 Location deletion in the public network

The following figure shows location deletion for the case where the PISN user roams from one public network to an other public network or from the public network back to the PISN.

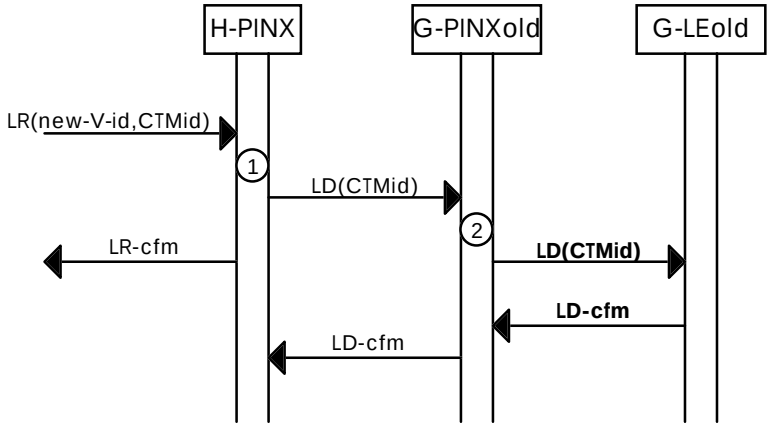


Figure 9: Location deletion in public network

The H-PINX receives a location registration containing the CTMid of the CTM user and the "new-V-id" as an indication of the new visited area ①. The H-PINX performs a location deletion procedure towards the previous G-PINX ②.

The G-PINXold includes the CTMid and forwards the location deletion to the corresponding G-LEold. The location deletion is confirmed by the GE-LE.

NOTE: A network to network authentication procedure might be required.

6.4.3 Location deregistration

The public network uses the location deregistration procedure to inform the private network about the location deregistration of the private CTM user from the public network.

NOTE 1: This procedure may by initiated by the CTM user or by the public network.

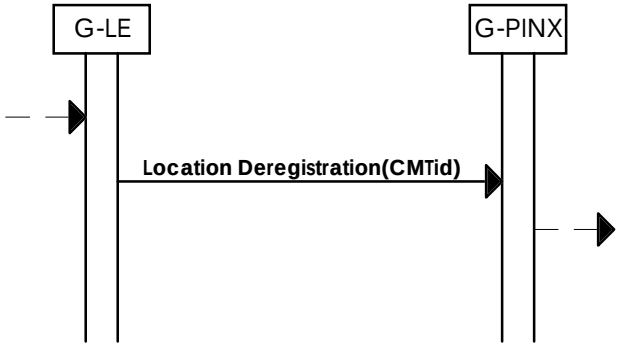


Figure 10: Location deregistration of the private network user

The G-LE sends Location Deregistration to the PINX including the CTMid to identify the CTM user, who's location should be deregistered.

NOTE 2: There is no confirmation of user initiated location deregistration (detach). Therefore it may be difficult to apply authentication.

6.4.4 Incoming call

The following figure shows an incoming call for the case where the PISN user has roamed from the PISN to the public network.

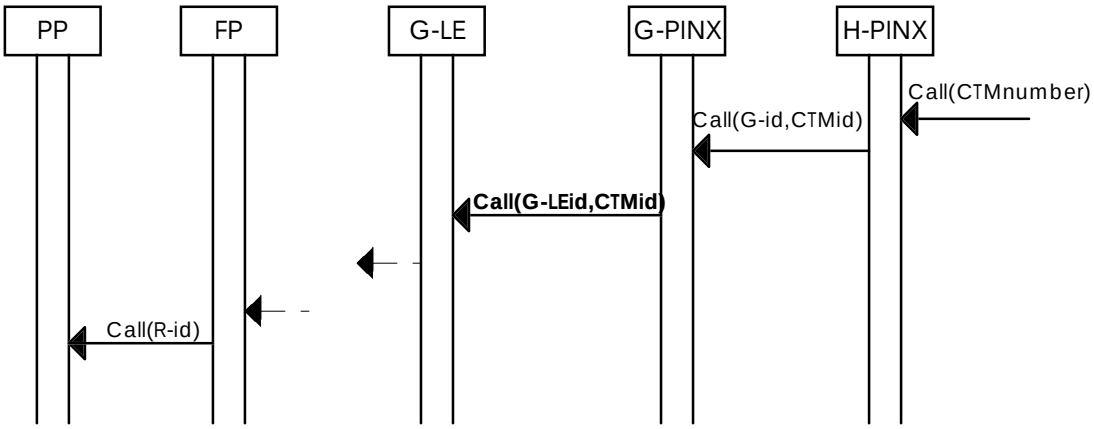


Figure 11: Incoming call, PISN user roaming in public network

The incoming call identifies the CTM user by its PISN number (= CTM number) and is routed to the H-PINX of the CTM user, where the identity of the G-PINX is found. Using the procedures for mobile call handling in the PISN, the call is then routed to the G-PINX.

The G-PINX forwards the call request containing the CTMid to the G-LE in the public network. The G-LE uses the public network procedures to route the call to the CTM user.

NOTE: It is possible to use the CTMid to derive the CTM number.

6.4.5 Outgoing call

For the service "Outgoing call" two scenarios are described in this subclause.

The first scenario is that the visited network relays the signalling between the CTM user and the home network.

The second scenario is that the visited network itself provides the service.

6.4.5.1 Outgoing call when routed via the G-PINX

The following figure shows an outgoing call for the case where the PISN user has roamed from the PISN to the public network and the call is routed to the G-PINX.

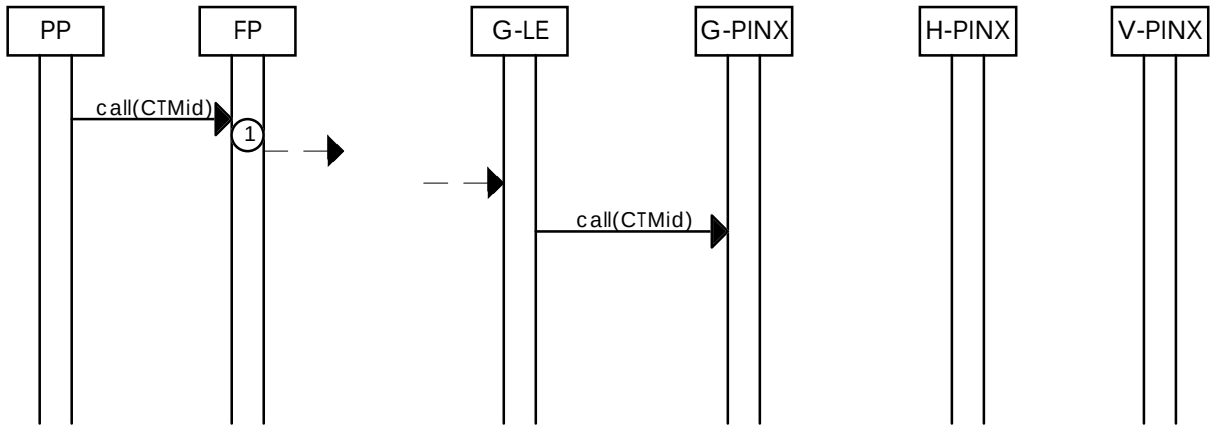


Figure 12: Outgoing call, PISN user roaming in public network

The call from the private CTM user is routed by the public network to the G-LE. The G-LE passes the call over to the G-PINX. The calling CTM user is identified by its CTMid. The further handling of the call is done by the PISN.

NOTE: Depending on the roaming agreement and the information that has been received during location registration of that CTM user, the public network may react differently. The public network may forward the call to the G-PINX of the CTM user as shown above. Alternatively the public network may perform authentication and then continue with the call as shown in the next subclause.

6.4.5.2 Outgoing call with local call handling

The following figure shows an outgoing call for the case where the private network user has roamed from the PISN to the public network and the call is handled by the public network.

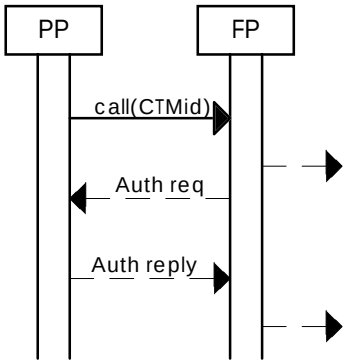


Figure 13: Outgoing call, PISN user roaming in public network

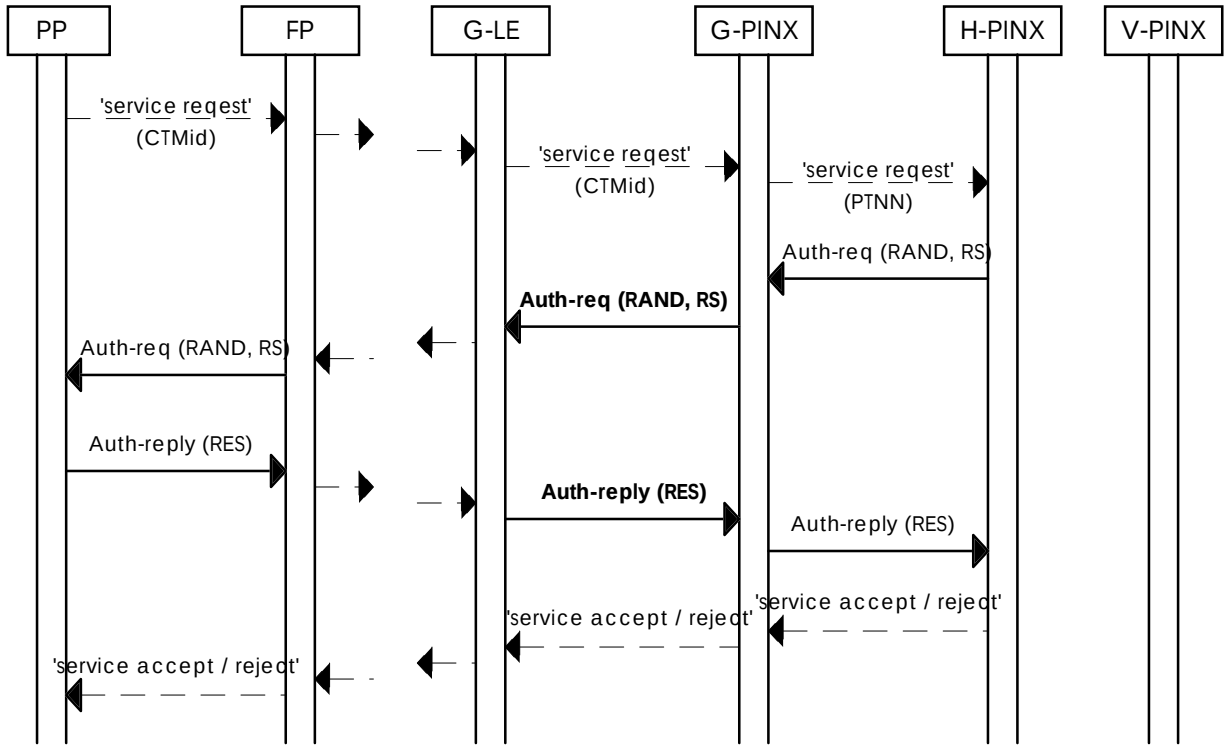
The private CTM user requests a call setup in the public network which further processes the call.

NOTE: If the public network has previously (e.g. during location registration) received the necessary authentication parameters (e.g. a session key KS and the corresponding RS value), then the public network can perform authentication to check the CTMid. Encryption may be switched on for the radio link, by e.g. using a derived cipher key.

6.4.6 PP-Authentication

6.4.6.1 PPT-Authentication performed by the home network

The following figure shows authentication for the case where the PISN user has roamed from the PISN to the public network.



NOTE: The parameter RS is included if required.

Figure 14: Authentication, PISN user roaming in public network

Typically the PISN may invoke authentication, when the CTM user requests a service, e.g. outgoing call or location registration. The H-PINX starts authentication by sending an Authenticate-request containing the authentication parameters (RAND and RS) to the G-PINX which sends this message to the G-LE. The public network forwards the Authenticate-request to the CTM user. The Authentication reply from the CTM user, which contains the authentication result (RES) is passed back via the G-LE and G-PINX to the H-PINX. Depending on the authentication result the PISN may then reject a service request from the (private) CTM user.

NOTE: It may be necessary to transfer a cipher key, which might have been created during the authentication process.

6.4.6.2 PP-Authentication performed by the visited network

If the public network wants to authenticate the private CTM user, then the private network has to provide authentication parameters to the public network. These parameters could e.g. be a session key KS plus the corresponding RS value. Alternatively one or more challenge(s) together with the response(s) (possibly also including the derived cipher key(s)) could be provided.

7 Further considerations on PISN/public network inter-network roaming

Defining the procedures for location registration and call handling is only one of the problems that have to be solved before inter-network roaming between public networks and PISNs can become a reality. In the following some additional problems identified during writing this document are presented.

7.1 Management of address information

A pre-requisite for inter-network roaming between a public and a private network are roaming agreements. One reason for this is related to call charging. Another reason more directly related to the issues discussed in this document is routeing of location registration information.

For public CTM users roaming in a PISN the problem is minor. For each public operator supported by the network (identified by the CTM user identity), the PISN shall maintain address information to direct the location registration towards the G-LE in the public network. As there are only relatively few public operators, this is manageable.

For private CTM users roaming in the public network the situation is worse. The requirements are similar: the public network shall maintain address information to direct location registration to the relevant PISN. However, due to the potentially large number of private networks wanting the ability to perform such roaming (possibly on a European or even a world wide scale), the management of the information becomes much more difficult.

7.2 Identification of CTM user

There is a need to standardize the identifier of the CTM user (CTMid), which allows to uniquely identify the home network and has enough space, to contain in addition on a per home network basis the identification of the individual CTM user.

For the CTMid e.g. an E.164 or an E.212 number could be used. The possibility of using the IMSI as CTMid is further investigated in the annex A.

7.3 Numbering

In private networks PISN numbers are used for identification and routing purposes. Currently there is no separate routing information as compared with other signalling systems (e.g. SS7) however standards on enhancement routeing are envisaged. The advantage of this is that the management of routeing information is simpler as no mapping between numbers and routeing information is required. This allows PISNs to have decentralized routeing management. The downside is that there are usually no mapping capabilities.

PISN numbers are a limited resource. Usually PISN numbers are short, often only four digits long for a company-wide network, though many networks allow longer numbers. The numbering plan is local to the PISN, and can be structured in different ways from public numbering plans.

7.4 Authentication and encryption

The flexibility provided by inter-network roaming makes the systems a possible target for abuse. To avoid (or limit) this, authentication of CTM users would need to be made mandatory. Not only to protect the networks, but also to ensure that legitimate users are not charged for calls they never made.

There are two principal scenarios for the PP-authentication. Either the home network or the visited network could do the authentication. To enable the visited network to perform authentication, the home network has to provide the necessary information (e.g. a session key KS plus the corresponding RS value).

If the radio link shall be encrypted, then this has to be done locally by the visited network. Therefore the cipher key needs to be known by the visited network. Local authentication gives the possibility to generate the cipher key in the visited network. Otherwise it has to be provided by the home network.

As CTM becomes more widespread, procedures for screening of stolen or illegal equipment across networks should be considered.

7.5 Supplementary services

When users begin to roam between the two domains using a single terminal, they will expect to have a consistent environment (e.g. same services).

7.6 Charging

Mechanisms for charging are required in both networks.

NOTE: The called user may be charged for incoming calls. The visited network may store charges for the calls of visiting CTM users.

8 Conclusion

It is possible to provide inter-network roaming even if differences may exist in the procedures applied by the networks. There are good reasons to have different procedures optimized to the requirements of the network in which they are used.

It is important to solve the problem of CTM user identities. This is more an administrative issue than a technical, with IMSI being a likely candidate assuming the necessary extensions are standardized and national authorities managing Private Network Codes (PNC) are created. Alternatively an E.164 number can be used.

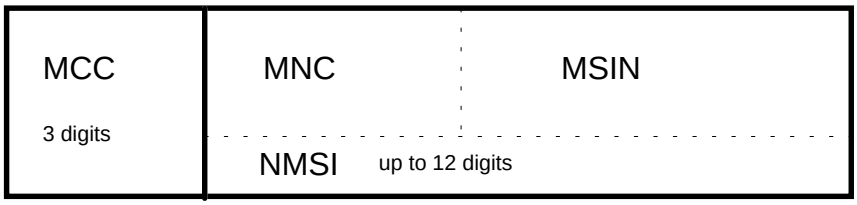
Standardization is necessary in the area of supplementary services. The CTM users should not only have access to all the services they subscribe to independent of their location, they should also be provided such access in a consistent way.

Annex A:
Capacity of the IMSI for inter-network CTM identification

In order to allow CTM users to roam between networks it is necessary to use an identification plan that is common to all networks. The identification plan has to be capable of identifying each CTM user uniquely and shall also allow each CTM user's CTM service provider to be identified, independently of the network the CTM user chooses to use.

An identity that satisfies the requirement for network independence is the International Mobile Station Identity, or IMSI, which is specified in CCITT Recommendation E.212 [11] and is currently used in GSM and PCN cellular networks.

The structure of the IMSI is as shown below.



MCC: Mobile Country Code
MNC: Mobile Network Code
MSIN: Mobile Station Identification Number
NMSI: National Mobile Station Identity

The IMSI can be up to 15 digits long. The ITU-T have fixed the length of the MCC to three digits and the remainder can be allocated between the MNC and MSIN. Together these make up the NMSI. The allocation of digits to MNC and MSIN is the responsibility of national administrations.

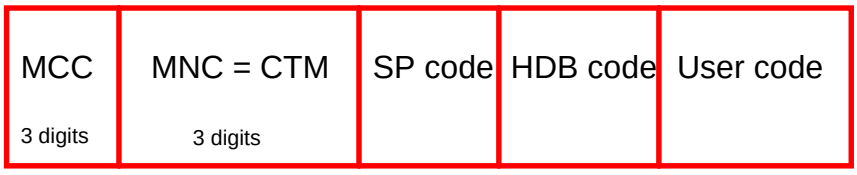
It is assumed that if the IMSI were to be used for CTM identification, the country code would be as specified in CCITT Recommendation E.212 5[11]. Therefore only the NMSI part of the IMSI could be made specific to CTM.

If the 12 digits for the NMSI could be freely allocated with no regard for structure, the capacity of the IMSI would be of the order of 1 000 000 000 000 CTM subscribers per country code. However it is unlikely that the NMSI could be made unstructured because of implementation difficulties, for example it would be difficult to identify a CTM user's CTM service provider. Therefore the NMSI would have to have a structure with a consequent reduction in maximum capacity.

To allow an IMSI to be recognized as a CTM user identifier, it is assumed here that a single MNC value would be assigned for CTM. If more than one MNC were assigned to CTM, the following estimates of the numbers of CTM users that could be catered for would apply to each such MNC. It is also assumed that the MNC is three digits; though it might be possible to use two digits instead.

CTM service providers could have more than one Home Data Base (HDB) and therefore a part of the IMSI might be used to identify the HDB of a particular CTM user. Having identified the CTM service provider and an HDB belonging to that service provider, the remainder of the IMSI would be used to identify a particular CTM user registered at that HDB.

Therefore the following structure of the IMSI could be used for CTM.

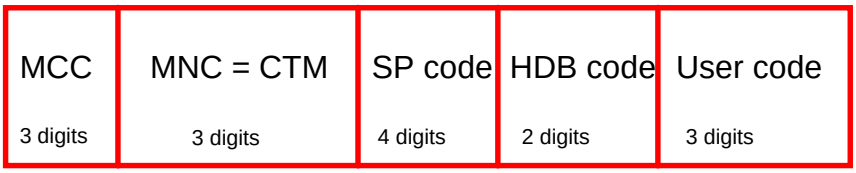


MCC: Mobile Country Code as specified in CCITT Recommendation E.212 [11]
MNC: CTM National network Code
SP: CTM Service Provider code
HDB: Home DataBase code
User code: CTM user code unique within a HDB

A.1 Capacity based on fixed code lengths

To progress further it is necessary to have an order of magnitude estimate of the number of CTM service providers per country code. Because most CTM service providers are likely to be public or private network operators, this estimate can be based on the number of networks per country. For the purposes of this paper 10 000 is assumed to be a reasonable maximum number. Therefore the SP code would require four digits. To allow each service provider to have a reasonable number of HDBs, the HDB code would probably have be two digits long. This leaves three digits for the User code.

The resulting structure of the IMSI is shown below.



Based on these assumptions, the number of users that a single CTM service provider could support would be of the order of 1 000 per HDB.

By assigning more than one HDB code to the same HDB, this limit can be increased in steps of 1 000 users to an absolute maximum of 100 000 users for a single HDB.

By assigning more than one service provider code to the same service provider, the service provider capacity can be increased in steps of 100 000.

A step size of 1 000 per HDB is probably not too wasteful of IMSI code space because CTM service providers would probably want to minimize the number of HDBs used for inter-network CTM. However it could be a problem if there were many CTM service providers with a few subscribers each. In view of the infrastructure required for administration, and charging and roaming agreements, this is perhaps unlikely but it is a possibility that might have to be allowed for.

Networks are of widely varying sizes, with a few very large ones and many small ones. A similar distribution in size might expected for CTM service providers. The problem with the above identification plan is that the minimum code space allocation to a CTM service provider is 100 000 which is probably too large a step.

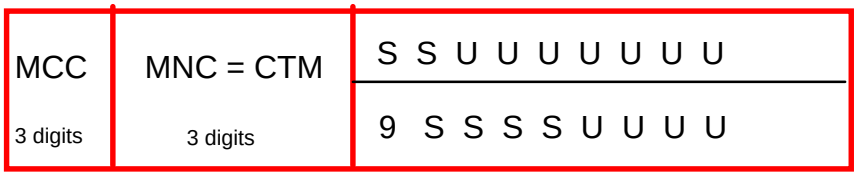
The step size per SP code can be reduced by making the SP code field longer. However this increases the number of SP codes required by a large CTM service provider and this might create other difficulties.

A.2 Capacity based on variable fields

The identification plan could take into account the potential differences in service provider size by a flexible allocation of code fields.

A possible way of doing this would be to allocate shorter SP codes for large service providers and longer SP codes for smaller ones. As an example, a two digit SP code might be sufficient for the larger service providers, and a four digit code for smaller service providers. It would be necessary to distinguish between the two and four digit SP codes. To do this, the four digit SP code could be prefixed with a fixed digit, say 9, making five digits in all for a SP code for smaller service providers.

If service providers were free to use their allocated code space as they wished, the HDB code length could also be determined by each service provider according to their needs. This plan is shown below assuming the two and four digit SP codes are distinguished by the digit 9.



S: Service provider code digit
U: User code digit

In this plan, a large service provider has code space for 10 000 000 CTM users. A small CTM service provider has code space for 10 000 CTM users.

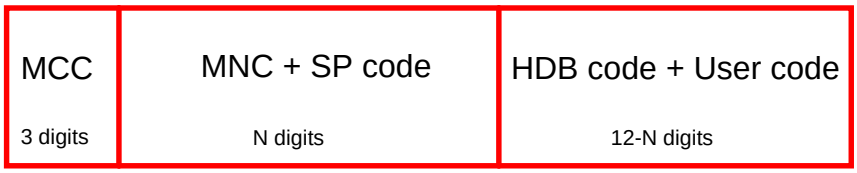
The maximum number of large service providers would be 90 per country code while the maximum number of small service providers would be 10 000 per country code.

A.3 Other possibilities

The choice of two and four digit SP codes for large and small service providers is made in this paper to obtain some idea of the number of CTM users that could be identified. Clearly other SP code sizes could be chosen. Also there could be more than two sizes of SP code, for example the SP code size could be 2, 3, or 4 digits and so on. These possibilities are not treated in this document.

Also, it is assumed in this document that the MNC code only indicates that the user is a CTM user. It would also be possible for the MNC to be used to indicate the service provider, in which case the MNC and SP fields would merge. It would even be possible to use the MNC field to distinguish between larger, intermediate and small service providers.

This plan is illustrated below with a flexible allocation of digits between the MNC and SP code for service provider identification, and the HDB and user code for user identification.



Different leading digits could used to indicate the structure of the service provider allocation in a similar way to that shown in the previous plan, but with more flexibility to cater for service provider size.

A new set of possibilities arise if an MCC code could be allocated to signify that the IMSI identifies a CTM user.

All these possibilities would enable the IMSI to support larger numbers of CTM users than the two basic plans on which estimates have been given earlier in this document.

A.4 Conclusions

This annex has examined the capacity of the IMSI for CTM user identification. The resulting numbers show that the IMSI might be usable as an identifier for inter-network CTM.

The number of CTM users that could be supported by the IMSI have been obtained by investigating two possible plans for the allocation of the various fields that might be required.

The first plan, based on fixed code allocations, might be wasteful of code space because of the potentially large variation in size of CTM service providers.

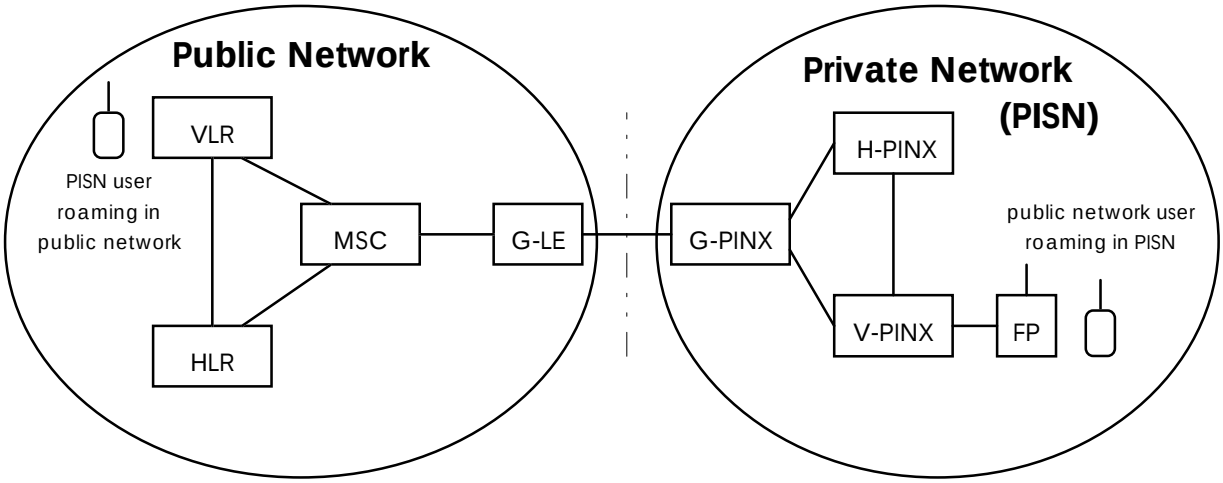
The second plan uses a flexible allocation of code fields which allows for variation in the service provider size. The number of service providers and CTM users supported has been indicated for this plan also.

Other possibilities for allocating the various code fields have been identified but the corresponding numbers have not been calculated here. These possibilities tend to increase the number of CTM users that can be accommodated by the use of the IMSI and so do not invalidate the conclusion that the IMSI might be usable as a CTM use identifier.

Annex B:
Interworking examples using MAP in the public network

B.1 Model for inter-network roaming

The study on inter-network roaming is based on the following model:



The model is simplified to show only those entities that are involved in location updating and call handling. The following entities are used:

VLR:	Visitor Location Register
HLR:	Home Location Register
MSC:	Mobile Switching Centre
G-LE:	Gateway Local Exchange
FP:	Fixed Part (cordless sub-system)
V-PINX:	Visitor PINX (containing Visitor Data Base)
H-PINX:	Home PINX (containing Home Data Base)
G-PINX:	Gateway PINX (containing Location Data Base)

The G-LE shall perform the necessary interworking between the public network procedures and the procedures used between the public and the private network. The G-LE will appear to the public network like a VLR for a public user roaming in the PISN and like an HLR for a PISN user roaming in the public network.

The G-PINX shall perform the necessary interworking between the procedures used between the public and the private network and the procedures used in the private network. The G-PINX will look to the PISN like a V-PINX for PISN users roaming in the public network and like an H-PINX for public users roaming in the PISN.

B.2 A public CTM user roaming in a private network

B.2.1 Location registration

The following figure shows location registration for the case where the public network user roams from the public network to the PISN.

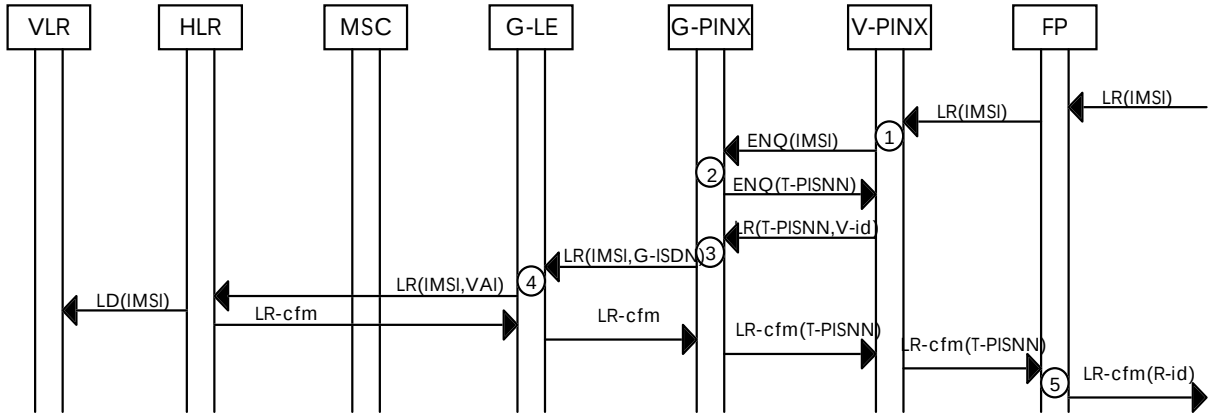


Figure B.1: Location registration, public network user roaming in PISN

ENQ:	Enquiry
LR:	Location Request
LR-cfm:	Location Request confirmation
LD:	Location Deletion

A public CTM user performs a location registration (LR) to the PISN using the IMSI for identification. The analysis of the IMSI shows that the CTM user is unknown to the network and that more information can be obtained by the G-PINX ①. The PISN enquiry mechanism (ENQ) is used to obtain a temporary PISN number (T-PISNN) assigned by the G-PINX ② from its own range. The T-PISNN is used for routeing and internal identification of the CTM user while roaming in the PISN.

The V-PINX performs a normal location registration using the T-PISNN to address the CTM user entry at the G-PINX and provides a PISN number V-id for its own identification. The G-PINX forwards the location registration to the G-LE in the public network ③.

The G-LE performs a mapping from the G-ISDN number used to identify the G-PINX to the VAI (Visited Area Identity) used by the MAP procedures in the public network ④. The G-LE forwards the location registration to the HLR in the public network using the CTM user's IMSI and the VAI.

The location registration confirmation is sent from the HLR to the G-LE and then to the G-PINX which will provide the T-PISNN as CTM user identity. When received by the FP, the mapping of IMSI to T-PISNN can be completed (5), allowing the CTM user to use the services of the PISN. During the location procedure an identity "R-id" to be used subsequently at the air interface could be assigned. In the location area there is an unique temporary relation between the IMSI, T-PISNN and R-id.

B.2.2 Incoming call

The following figure shows an incoming call for the case where the public network user has roamed from the public network to the PISN.

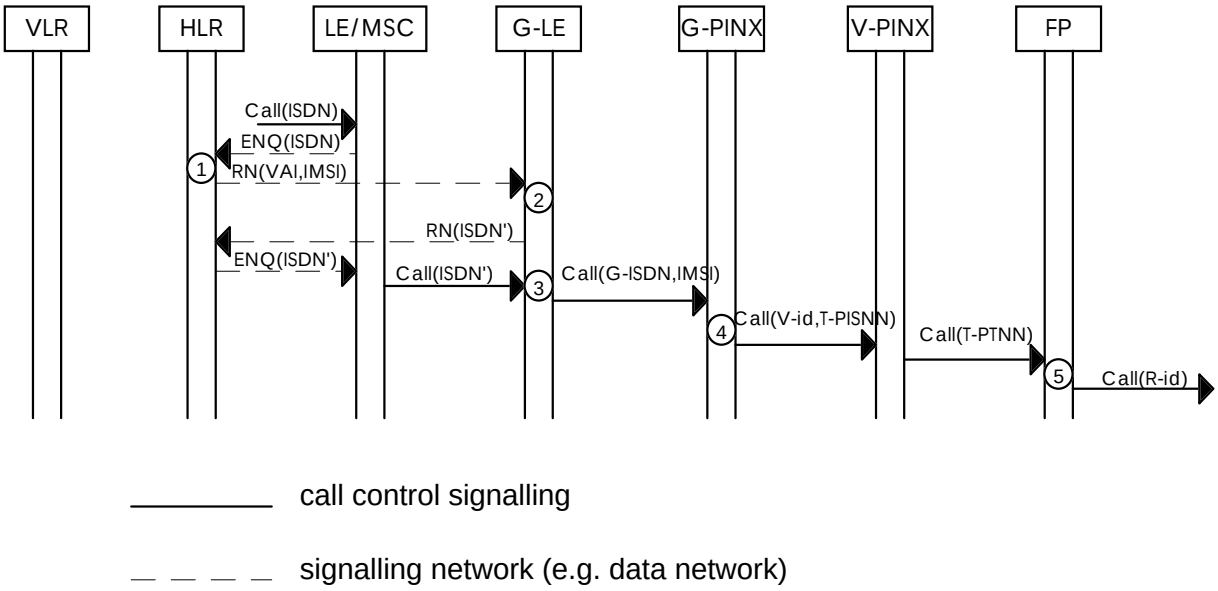


Figure B.2: Incoming call, public network user roaming in PISN

ISDN:	originally dialled ISDN number
ISDN':	roaming number
ENQ:	Enquiry
RN:	Roaming Number request
R-id:	Radio identity

The incoming call identifying the CTM user by the ISDN number will reach an LE/MSC able to enquire the HLR for the current location of the user ①. This enquiry causes the HLR to perform a roaming number request ② of the G-LE addressed by the VAI. The G-LE associates an ISDN number with the CTM user's entry using the IMSI ③ and returns this ISDN number as a roaming number to the HLR. The G-LE now has mapping information between the identifiers: IMSI and ISDN.

Normal call processing continues until the call arrives at the G-LE. Upon reception of the call, identified by the roaming number, the G-LE forwards the call to the G-PINX, including the IMSI to identify the called user. The G-PINX associates the temporary number (T-PISNN) with this call, which has been assigned during the previous location registration procedure. At this point the PISN mobile call handling procedures are applied generating a call to the V-PINX with the user identified by the T-PISN ④.

When the call gets to the FP, the local mapping information is finally used to insert an identifier as required by the radio interface ⑤ before presenting the call to the CTM user.

B.3 A private CTM user roaming in a public network

B.3.1 Location registration

The following figure shows location registration for the case where the PISN user roams from the PISN to the public network.

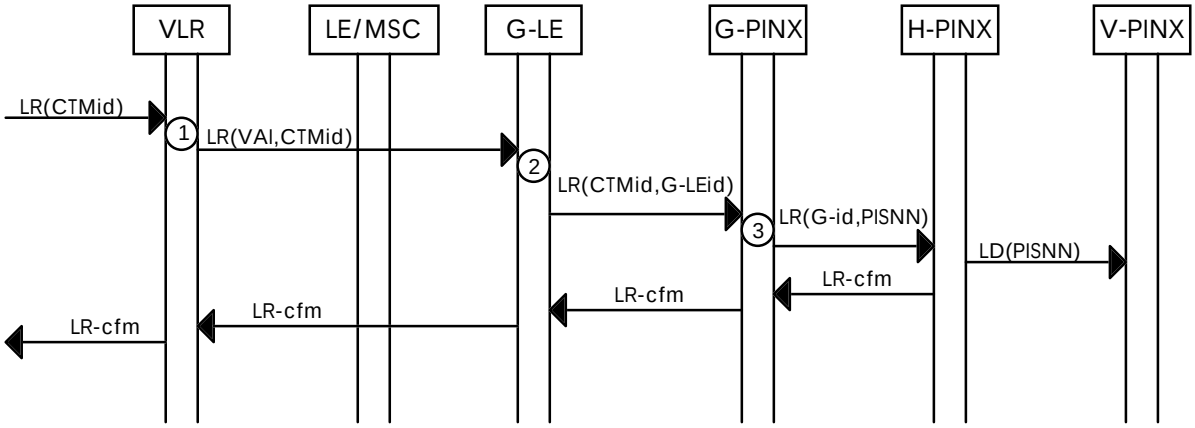


Figure B.3: Location registration, PISN user roaming in public network

A private CTM user performs a location registration to the public network using the CTMid for identification ①. The analysis of the CTMid shows that the CTM user is a visitor in this network but contains sufficient information to identify the G-PINX.

The location registration reaches the G-LE where the VAI, which is used by the public network procedures, is replaced by an identifier V that may be conveyed into the private network and which is the address of the G-LE ②.

The G-PINX performs a location registration in the PISN and uses G the PISN number of the G-PINX as an indication of the new visited area ③.

B.3.2 Incoming call

The following figure shows an incoming call for the case where the PISN user has roamed from the PISN to the public network.

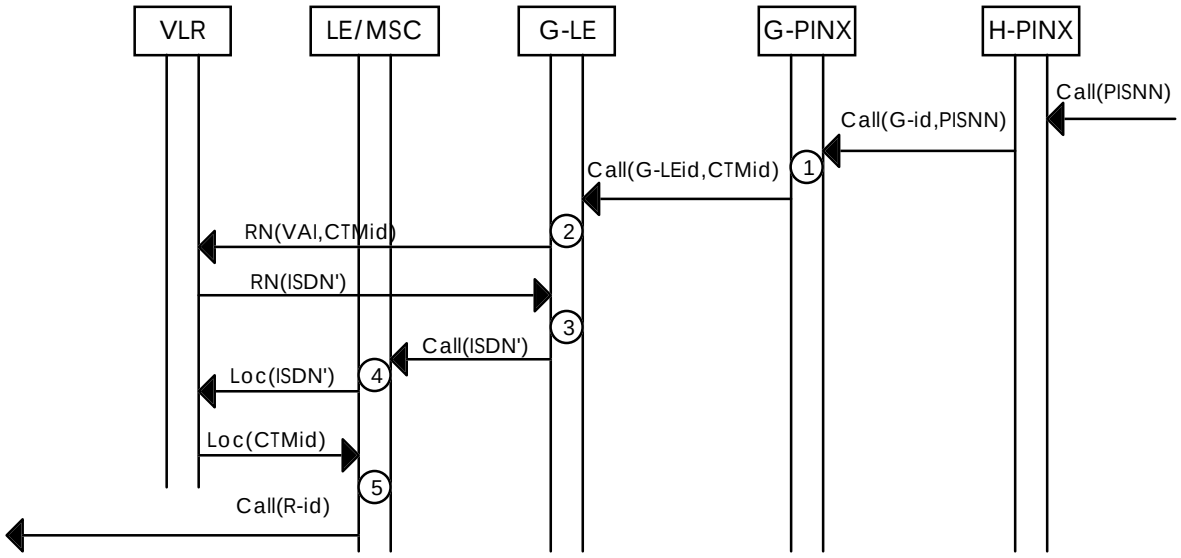


Figure B.4: Incoming call, PISN user roaming in public network

The incoming call identifying the CTM user by the PISN number will reach the H-PINX of the user. Using the procedures for mobile call handling in the PISN, the call is routed to the G-PINX ①.

The G-PINX forwards the call request containing the CTMid to the G-LE in the public network. The G-LE uses the correct VAI and performs a roaming number request to the VLR ②.

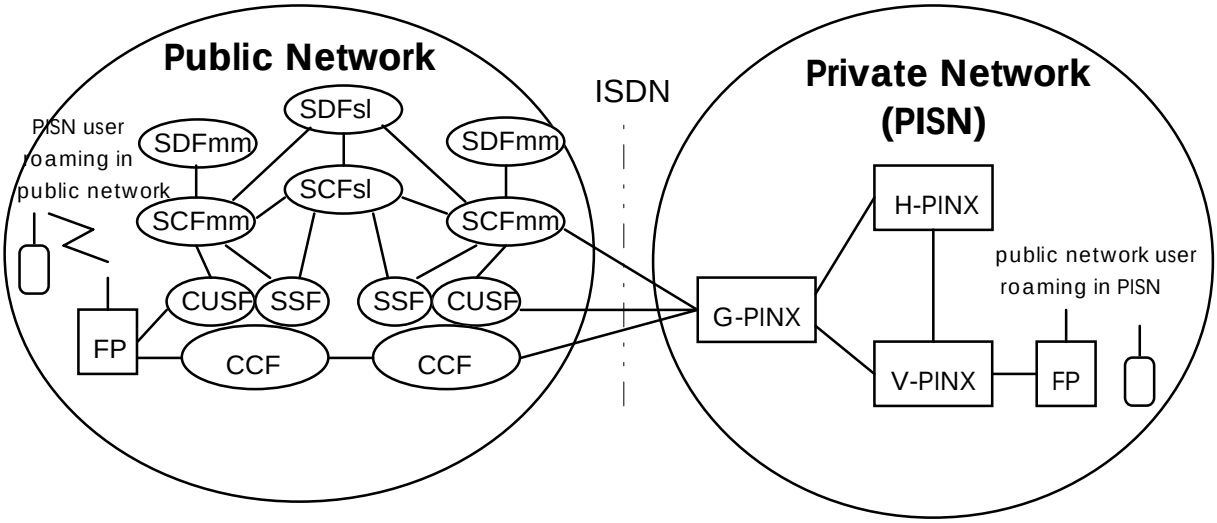
The roaming number assigned by the VLR is returned to the G-LE, and the G-LE directs the call according to the ISDN number supplied ③.

When the call reaches the MSC, the exact location of the CTM user is determined using public network procedures ④, and the call is presented to the CTM user ⑤.

Annex C:
Interworking examples using INAP in the public network

C.1 Model for inter-network roaming

The study on inter-network roaming is based on the following model:



For the public network an IN structure is assumed.

C.2 Location registration when a public CTM user is roaming in a private network

The following figure shows location registration for the case where the public network user roams from the public network to the PISN. The network internal information flows may not be complete and may not show all parameters.

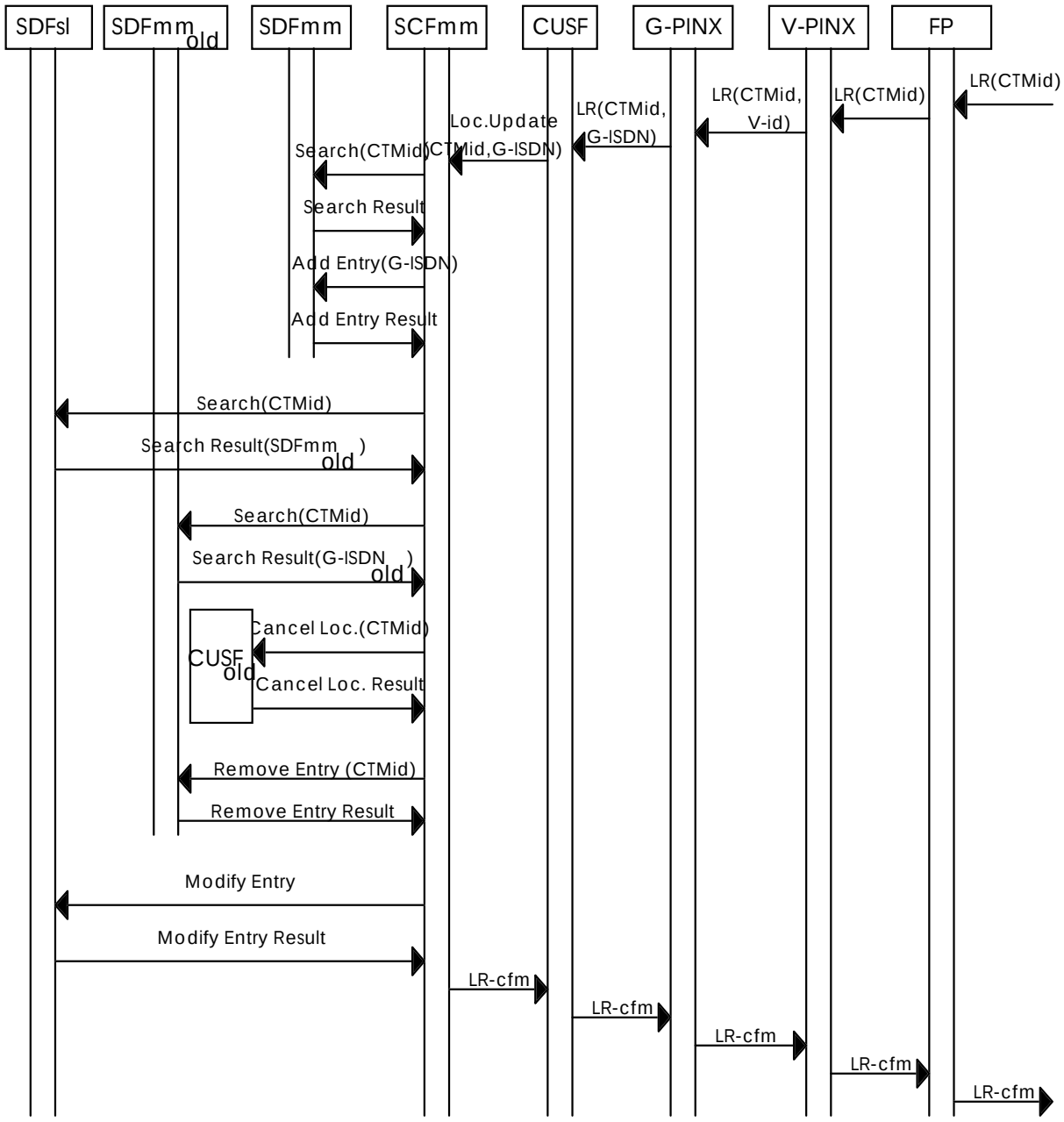


Figure C.1: Location registration, public network user roaming in PISN

LR: Location Request
LR-cfm: Location Request confirmation
SCFmm: Service Control Function mobility management
SDFmm: Service Data Function mobility management
SCFsl: Service Control Function service logic
SDFsl: Service Data Function service logic

A public CTM user performs a Location Registration (LR) to the PISN using the CTMid for identification. The analysis of the CTMid shows that the CTM user is unknown to the network, but it contains enough information to identify the responsible G-PINX.

The V-PINX performs a location registration using the CTMid to identify the CTM user and provides a PISN number V-id for its own identification. The G-PINX forwards the location registration to the G-LE in the public network.

In the public network the SCFmm retrieves the information about the address of the SDFsl from the SDFmm. Then the SDFsl is updated and the entry in the old location area of the CTM user is deleted.

Then the SCFmm sends the "Location update result" to the G-PINX. During the location procedure an identity "R-id" to be used subsequently at the air interface could be assigned. In the location area there is an unique temporary relation between the CTMid and R-id.

C.3 Location registration when a private CTM user is roaming in a public network

The following figure shows location registration for the case where the PISN user roams from the PISN to the public network. The network internal information flows may not be complete and may not show all parameters.

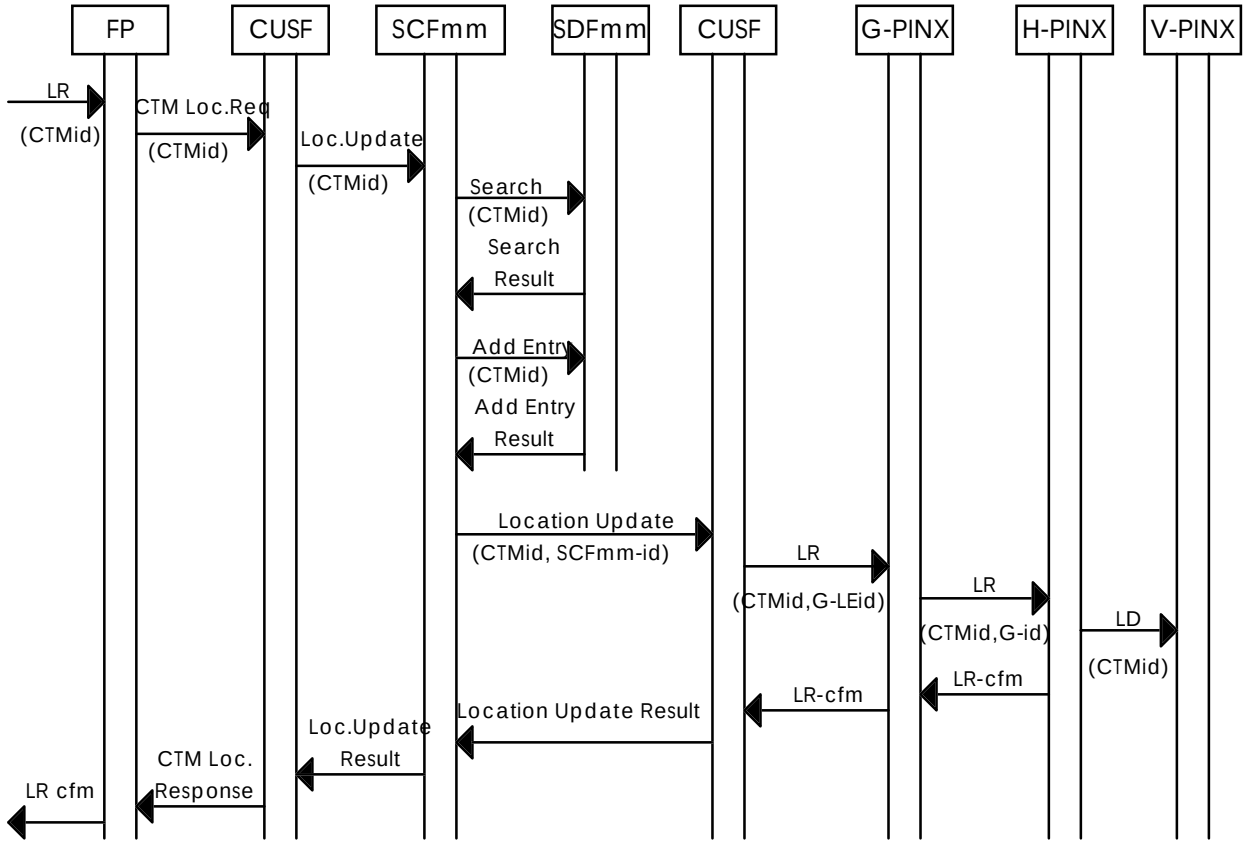


Figure C.2: Location registration, PISN user roaming in public network

LD:	Location Deletion
LR:	Location Request
LR-cfm:	Location Request confirmation
SCFmm:	Service Control Function mobility management
SDFmm:	Service Data Function mobility management

A private CTM user performs a location registration to the public network using the CTMid for identification. The analysis of the CTMid shows that the CTM user is a visitor in this network but contains sufficient information to direct the location registration towards the G-PINX.

The location registration reaches the G-LE and is conveyed to the G-PINX, containing the CTMid and the address of the G-LE.

The G-PINX performs a location registration in the PISN and uses G-id the PISN number of the G-PINX as an indication of the new visited area.

The location registration is forwarded to the H-PINX, which then issues a location deletion towards the previous visited V-PINX.

The location registration is confirmed towards the public network, which then passes on the confirmation to the CTM user.

History

Document history			
V1.1.1	April 1997	Membership Approval Procedure	MAP 9722: 1997-04-01 to 1997-05-30
V1.1.1	June 1997	Publication	

ISBN 2-7437-1587-1
Dépôt légal : Juin 1997