ETSI TS 124 259 V8.0.0 (2009-01)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Personal Network Management (PNM);
Stage 3
(3GPP TS 24.259 version 8.0.0 Release 8)**

Reference
DTS/TSGC-0124259v800

Keywords
GSM, LTE, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x   the first digit:

1   presented to TSG for information;

2   presented to TSG for approval;

3   or greater indicates TSG approved document under change control.

y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z   the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

Personal Network Management (PNM) is a home network-based application and provides the home network-based management of Personal Network (PN) consisting of multiple devices belonging to a single user, as described in 3GPP TS 22.259 [2] and 3GPP TS 23.259 [15].

The present document provides the protocol details for enabling Personal Network management (PNM) services in the IP Multimedia (IM) Core Network (CN) subsystem based on the protocols of XML Configuration Access Protocol (XCAP), Session Initiation Protocol (SIP) and the Session Description Protocol (SDP).

The present document provides the protocol details for enabling Personal Network management (PNM) services in Circuit Switched (CS) domain based on the protocols of CAP, MAP, ISUP, USSD and BICC.

The present document is applicable to User Equipment (UEs) and Application Servers (AS) providing PNM capabilities.

The present document makes no PNM specific enhancements to SIP, SIP events or SDP specified in 3GPP TS 24.229 [3].

The present document makes no PNM specific enhancements to CAP, MAP, ISUP, USSD and BICC.

2 References

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

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

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

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2]   3GPP TS 22.259: "Service requirements for Personal Network Management (PNM)".

[3]   3GPP TS 24.229: "IP Multimedia Call Control based on SIP and SDP; Stage 3".

[4]   IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[5]   3GPP TS 24.109: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[6]   IETF RFC 4825 (2007): "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)."

[7]   IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1".

[8]   3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[9]   3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents".

[10]   3GPP TS 24.228 Release 5: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[11]   3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[12]   3GPP TS 29.329: "Sh interface based on the Diameter protocol; Protocol details".

[13]   3GPP TS 29.078: 'Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3: CAMEL Application Part (CAP) specification'.

[14]   3GPP TS 24.090: 'Unstructured Supplementary Service Data (USSD); Stage 3'.

[15]   3GPP TS 23.259: 'Personal Network Management (PNM); Procedures and Information Flows; Stage 2'

[16]   IETF RFC 4244 (2005): "An Extension to the Session Initiation Protocol (SIP) for Request History Information"

[17]   IETF RFC 4458 (2006): "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)"

[18]   3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[19]   3GPP TS 22.085: "Closed User Group (CUG) Supplementary Services; Stage 1".

[20]   3GPP TS 23.085: "Closed User Group (CUG) supplementary service; Stage 2".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in IETF RFC 4825 [6] apply.

Application usage
Application Unique ID (AUID)
Document Selector
Document URI
Naming Conventions
Node Selector
Node Selector Separator
Node URI
XCAP client
XCAP resource
XCAP root
XCAP root URI
XCAP server
XCAP User Identifier (XUI)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.085 [19] apply:

Incoming Access (IA)
Outgoing Access (OA)

3.2 Abbreviations

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

ACM   Address Complete Message
ANM   Answer Message
AS   Application Server
BICC   Bearer Independent Call Control

BSF	Bootstrapping Server Function
CAMEL	Customised Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CCCF	Call Continuity Control Function
CN	Core Network
CS	Circuit Switched
CUG	Closed User Group
FQDN	Fully Qualified Domain Name
GBA	Generic Bootstrapping Architecture
GMSC	Gateway MSC
GRUU	Globally Routable User Agent URI
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IA	Incoming Access
IAM	Initial Address Message
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
IDP	Initial Detection Point
IE	Information Element
IFC	Initial Filter Criteria
IM	IP Multimedia
IMS	IM CN subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
MAP	Mobile Application Part
MGCF	Media Gateway Control Function
MS	Mobile Station
MSC	Mobile Switching Centre
MSISDN	MS international PSTN/ISDN number
NAF	Network Application Function
OA	Outgoing Access
P-CSCF	Proxy Call Session Control Function
PN	Personal Network
PNM	Personal Network Management
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRI	Send Routing Information
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
USSD	Unstructured Supplementary Service Data
VLR	Visitor Location Register
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language

4 Overview of personal network management

4.1 General

PNM applications consists of the PN UE redirection service and the PN access control , both applying only to the terminating service, as described in 3GPP TS 22.259 [2] and 3GPP TS 23.259 [15]. The PN UE redirection is a PNM application that enables redirecting a session addressed to any of the UEs belonging to the PN to a certain UE of their PN, i.e., the default UE for terminating services. The PN access control is a PNM application that enables users to

exercise PN access control to restrict accesses to certain UEs of their PN. The PN may consist of UEs which are only privately accessed, that is each UE may be accessed only by other UEs of the PN. The PN-User may additionally modify the access levels of each UE of the PN to be public or private. In this regard the PN behaves similar to a CUG as specified in 3GPP TS 22.085 [19] and 3GPP TS 23.085 [20], with Outgoing Access and whether Incoming Access is allowed for the PN UE is dependent on the PN access control list for that PN UE.

In order to make the above happen, the following procedures are provided within this document:

- procedures for PN-registration are specified in Clause 6;

- procedures for PN-configuration are specified in Clause 7;

- procedures for PN-query are specified in Clause 8;

- procedures for session redirection are specified in Clause 9;

- procedures for restricting access to certain UEs are specified in Clause 10.

4.2 Network capabilities

In order to support the PNM services the following network capabilities are assumed:

1) provision by the home network operator of PNM specific AS on the IM CN subsystem, as specified in 3GPP TS 24.229 [3];

2) support of CAMEL phase-3 and USSD as specified in 3GPP TS 29.078 [13] and 3GPP TS 24.090 [14].

5 Functional entities

5.1 Introduction

5.2 User Equipment (UE)

To be compliant with this document, a UE shall implement the role of a PN UE (see subclause 6.2, subclause 7.2, subclause 8.2, subclause 9.2 and subclause 10.2).

The UE shall implement the XCAP client role as described in subclause 11.2.1.

The UE shall implement HTTP digest authentication (see 3GPP TS 24.109 [5]).

The UE shall implement Transport Layer Security (TLS) (see IETF RFC 2246 [4]).

The UE shall implement the GBA Function as described in 3GPP TS 33.220 [8].

The UE shall initiate a bootstrapping procedure with the bootstrapping server function (BSF) located in the home network, as described in 3GPP TS 24.109 [5].

5.3 Application Server (AS)

The AS implementing PNM application shall implement the role of a XCAP server (see subclause 11.2.2).

The AS implementing PNM application shall implement the Network Application Function (NAF) as described in 3GPP TS 33.220 [8].

NOTE: For terminating services, the PNM Application in IM CN subsystem is the first Application Server of any Application Servers in the path of the call.

5.4   Authentication Proxy

The generic requirements for an authentication proxy are defined in 3GPP TS 24.109 [5].

---

6   Roles for PN-registration

6.1   Introduction

The PN-registration is the procedure where a UE is added to the PN. As a result of a successful registration, the UE capabilities are conveyed to the PNM application.

6.2   PN UE

If a PN UE supports the PN controller functionality and is configured to act as a PN controller the PN UE shall include in the Contact header of the REGISTER request containing g.3gpp.iari_ref feature tag containing the IARI value defined in sub subclause 10.4.

There are no PNM specific requirements for registration of the PN UE to the CS domain.

6.3   PNM Application

6.3.1   PN-registration procedure in the IM CN subsystem

The PNM AS can be configured with any of various options for obtaining information from the IM CN subsystem specified in 3GPP TS 24.229 [3], 3GPP TS 29.328 [9] and 3GPP TS 29.329 [12], for example:

   a)   receipt of REGISTER request which causes a third-party REGISTER request containing in the body the incoming REGISTER request from the PN UE to be sent to the PNM application. The PNM application may then obtain information from the body of the third-party REGISTER request;

   b)   receipt of REGISTER request which causes a third-party REGISTER request containing in the body a <service-info> element containing the private user identity of the PN UE to be sent to the PNM application. The PNM application may then subscribe to the reg event package for that user to obtain information; or

   c)   receipt of REGISTER request which causes a third-party REGISTER request containing in the body a <service-info> element containing the private user identity of the PN UE to be sent to the PNM application. The PNM application may then use the Sh interface to obtain information.

This document places no requirement on the use of all or any of these mechanisms.

After successful PN-registration, the PNM AS shall enrol the public user identity of the PN UE as registered in the data base.

6.3.2   PN-registration procedure in the CS domain

When the gsmSCF (CAMEL service for PNM) receives a MAP_NOTE_MM_EVENT message sent from the VLR to report that the status of the UE set to "attached", the gsmSCF sets the UE registration status in the PN to "registered" and sends the UE status to the PNM AS.

   NOTE: The interface between the gsmSCF and the PNM AS is unspecified.

When the gsmSCF (CAMEL service for PNM) receives a MAP_NOTE_MM_EVENT message sent from the VLR to report that the status of the UE set to "detached", the gsmSCF sets the UE registration status in the PN to "deregistered" and checks whether the PN UE was the only default UE in the PN. If it was the only default UE in the PN, the gsmSCF generates the USSD Notify message to the HSS to inform the user.

7 Roles for PN-configuration

7.1 Introduction

This clause specifies the PN-configuration and PN-deconfiguration procedures for supporting PN UE redirection, PN access control and PN UE name changing.

NOTE: The text string together with the angled bracket (e.g. <PNUEName>) represents an XML element defined by the XML schema in Annex B.

Subclause A.3 provides examples of signalling flows for PN-configuration and PN-deconfiguration.

7.2 PN UE

In order for the PN UE to initiate the PN-configuration procedure for creating/replacing or deleting an XML document, an element within an XML document or an attribute of an element within an XML document, the PN UE shall know the data structure and constrains defined by the PNM XML schema in Annex B. The PN UE shall also know what HTTP URI to use based on the naming conventions for constructing the HTTP URIs described in Annex C.

The PN UE initiates the PN-configuration procedure or the PN-deconfiguration procedure by sending a HTTP PUT request or a HTTP DELETE request message with

- Request-URI field indicating to the PNM application the desired location where the XML document, an element within an XML document or an attribute of an element within an XML document which is requested to be configured as follows:

    - if the PN-configuration procedure performed for configuring an XML document, the Request-URI is constructed with a document URI pointing to the XML document;

    - if the PN-configuration procedure performed for configuring an element within an XML document, the document selector of the Request-URI is constructed with a document URI pointing to the XML document containing the element to be configured, and the node selector of the Request-URI with a node URI identifying the element to be configured;

    - if the PN-configuration procedure performed for configuring an attribute of an element within an XML document, the document selector of the Request-URI is constructed with a document URI pointing to the XML document containing the element to be queried and the node selector of the Request-URI with a node URI identifying the attribute to be configured;

- Host field indicating the Internet host and port number of the PNM application;

- User-Agent field containing information about the user agent originating the request and the static string (e.g. 3gpp-gba) to indicate to the NAF that the UE supports 3GPP-bootstrapping based authentication;

- Referer field indicating the address (URI) of the resource from which the URI for the PNM application is obtained;

- Authorization field containing the credentials obtained by means of executing the bootstrapping procedure with the BSF as described in 3GPP TS 33.220 [8];

- Content-Type filed indicating

    - "application/pnm+xml", if the PN-configuration is performed for configuring an XML document;

    - "application/xcap-el+xml" as in IETF RFC 4825 [6], if the PN-configuration is performed for configuring an element within an XML document;

    - "application/xcap-att+xml" as in IETF RFC 4825 [6], if the PN-configuration is performed for configuring an attribute of an element within an XML document;

If the PN-configuration is performed for creating/replacing the XML document for the PN UE redirection purpose, the XML body of the HTTP PUT request message shall contain

- the <RedirectedUserID> containing the children <PNUEID> and <PNUEName>, and the <RedirectingUserID> with a unique value for the "id" attribute containing the children <PNUEID> and <PNUEName>, as well as the <RedirectionLevel> and the <RedirectionPrio>;

NOTE: A PN user decides the value of the <RedirectionLevel> element based on the PN UE capabilities. According to the requirements of 3GPP TS 22.259 [2], this document supports three values (a global level for all services, a service level for selected services and a service component level the different media).

- the value of the "UriOfRedirectedUser" attribute for the <UERedirection> shall be populated with the public user identity of the PN UE configured by the PN UE to be redirected and indicated by the <RedirectedUserID>.

If the PN-configuration is performed for creating/replacing the XML document for the PN access control purpose, the XML body of the HTTP PUT request message shall contain

- the <ControllerUE> containing the children <PNUEID> and <PNUEName>, the <ControlleeUE> with a unique value for the "id" attribute containing children <PNUEID> and <PNUEName>, and the <PNAccessControlList> and <PNAccessControlType>;

- the value of the "UriOfControllerUE" attribute of the <AccessControl> shall be populated with the public user identity of the controller UE indicated by the <ControllerUE>.

If the PN-configuration is performed for the PN UE name changing purpose, and if the PN UE does not know the value of the "id" attribute of the <UEName> to be changed, the UE shall first initiate the PN-query procedure as specified in clause 8 in order to cache a copy of the XML document containing the value of the "id" attribute of that <UEName>.The XML body of the HTTP PUT request message shall contain

- the <PNUEID> identified by the shared public user identity, the <UEName> containing an "id" attribute with the attribute value pointing to the <UEName> to be changed and the <Name> to be changed.

If the PN-configuration is performed for configuring an element within an XML document, the XML body of the HTTP request message shall contain

- the XML element to be configured.

If the PN-configuration is performed for configuring an attribute of an element within an XML document, the XML body of the HTTP request message shall contain

- the value of the attribute of an element to be configured.

7.3   PNM application

In order for the PNM application to support the PN-configuration procedure for creating/replacing or deleting an XML document, an element within an XML document or an attribute of an element within an XML document, the PNM application shall know the data structure and constrains imposed by the PNM XML schema in Annex B. The PNM application shall also be configured to be able to handle the HTTP URIs described in Annex C.

Upon receiving an HTTP PUT request or a HTTP DELETE request message, PNM application verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key material Ks_NAF obtained from BSF (as described in 3GPP TS 33.220 [8]). If the verification succeeds, the PNM application obtains the private user identity associated with the received public user identity. The PNM application then authorizes the PN UE by comparing the received public user identity with the preconfigured one identified by the private user identity.

If the authorization succeeds, the PNM application shall perform the requested action and generate a response in accordance with IETF RFC 4825 [6].

8   Roles for PN-query

8.1   Introduction

This clause specifies the PN-query procedure.

Annex A.3 provides examples of signalling flows for PN-query.

8.2 PN UE

In order for the PN UE to initiate the PN-configuration procedure for querying an XML document, an element within an XML document or an attribute of an element within an XML document, the PN UE shall know the data structure and constraints defined by the PNM XML schema in Annex B. The PN UE shall also know what HTTP URI to use based on the naming conventions for constructing the HTTP URIs described in Annex C.

The PN UE initiates the PN-query procedure by sending a HTTP GET request message with

- Request-URI field indicating to the PNM application the desired location where the XML document, an element within an XML document or an attribute of an element within an XML document which is queried as follows:

    - if an XML document is queried, the Request-URI is constructed with a document URI pointing to the XML document;

    - if an element within an XML document is queried, the document selector of the Request-URI is constructed with a document URI pointing to the XML document containing the element to be queried and the node selector of the Request-URI with a node URI identifying the element to be queried;

    - if an attribute of an element within an XML document is queried, the document selector of the Request-URI is constructed with a document URI pointing to the XML document containing the element to be queried and the node selector of the Request-URI with a node URI identifying the attribute to be queried.

- Host field indicating the Internet host and port number of the PNM application

- User-Agent field containing information about the user agent originating the request and the static string (e.g. 3gpp-gba) to indicate to the NAF that the UE supports 3GPP-bootstrapping based authentication,

- Referrer field indicating the address (URI) of the resource from which the URI for the PNM application is obtained,

- Authorization field containing the credentials obtained by means of executing the bootstrapping procedure with the BSF as described in 3GPP TS 33.220 [8].

8.3 PNM application

In order for the PNM application to support the PN-configuration procedure for querying an XML document, an element within an XML document or an attribute of an element within an XML document, the PNM application shall know the data structure and constraints imposed by the PNM XML schema in Annex B. The PNM application shall also be configured to be able to handle the HTTP URIs described in Annex C.

Upon receiving an HTTP GET request message, PNM application verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key material Ks_NAF obtained from BSF (as described in 3GPP TS 33.220 [8]).

If the verification succeeds, the PNM application shall perform the requested action and generate a response in accordance with IETF RFC 4825 [6] with an XML body containing either the XML document, or the element within an XML document or the attribute of an element within an XML document as queried by the PN UE.

9 Roles for PN UE redirection

9.1 Introduction

The PN UE redirection redirects sessions destined for any UEs of a PN to the default UE of the same PN as described in 3GPP TS 22.259 [2] and in 3GPP TS 23.259 [15].

9.2 PN UE

There is no PNM specific requirement for the PN UE redirection.

9.3 PNM application

9.3.1 PN UE redirection procedure in the IM CN subsystem

When the PNM AS receives an initial request destined for a UE that exists in the PN configuration due to the terminating initial filter criteria, the PNM AS shall verify if the address in the Request-URI exists in a <RedirectingUserID> element in the PN configuration. If there is a matching <RedirectingUserID> element the PNM AS shall send an initial request of the same SIP Method on a new dialog to the URI contained in the <RedirectedUserID> element. The PNM AS then routes the initial request based on the standard call setup procedures as specified in 3GPP TS 24.229 [3].

> NOTE: The PNM AS is triggered first by forming the initial filter criteria in the S-CSCF.

The PNM AS shall include in the request the following:

a) a Request-URI set to the SIP URI contained in the <RedirectedUserID> element (e.g. a public user identity or a GRUU);

b) a From header set to the SIP URI of the PNM AS;

c) a To header set to the URI contained in the <RedirectedUserID> element;

d) a P-Asserted-Identity header set to the contents of the P-Asserted-Identity header in the original initial request;

e) a Contact header set to the IP address or FQDN of the PNM AS;

f) a Supported header containing the option tags from the original initial request with the addition of the option tag "histinfo";

g) a History-Info header that includes as the Targeted-to-URI the URI from the Request-URI of the original initial request, and as the next branch index URI, the contents of the Request-URI of this request.

If the PNM AS receives in response a 4xx, 5xx or 6xx response, and there exists more <RedirectedUserID> elements in the PN configuration which have not had the request forwarded to them yet, then the PNM AS shall send an initial request of the same SIP Method on a new dialog to the URI of the UE contained in the next lower priority <PNController> element as above.

Otherwise, if there does not exist more <RedirectedUserID> elements in the PN configuration which have not had the request forwarded to them yet, then the PNM AS shall forward the response back towards the originator of the initial request.

If the PNM AS receives in response a 200 (OK) response, the PNM AS shall forward the response back towards the originator of the initial request.

9.3.2 PN UE redirection procedure in the CS domain

When the PNM application receives an indication that the gsmSCF has received a CAMEL IDP relating to a terminating call, the PNM application shall:

1) check if the re-direction is applicable for the call on the basis of service key and called party number received in CAMEL IDP message.

2) if the call is not subject to re-direction, cause the gsmSCF to respond with a CAMEL CONTINUE and no further PNM specific procedures are performed on this call.

3) if the call is subject to re-direction, retrieve the Destination Routing Address.

4) if the call is subject to re-direction, cause the gsmSCF to respond with a CAMEL CONNECT message with the Destination Routing Address set to the MSISDN of default UE.

When the PNM application receives an indication that the gsmSCF has received a EventReportBCSM message indicating that the default UE cannot setup the session/call, the PNM application shall:

1) retrieve the Destination Routing Address of the other UE of the next lower priority based on the PN-configuration.

2) cause the gsmSCF to respond with a CAMEL CONNECT message with the Destination Routing Address set to the MSISDN of the selected UE.

3) if there are no more UEs selected for redirection, cause the gsmSCF to respond with a CAMEL CONTINUE and no further PNM specific procedures are performed on this call.

10 Roles for PN access control

10.1 Introduction

The PN access control procedure enables the controller UE to exercise access control to restrict accesses to certain controllee UE(s) of the PN as described in 3GPP TS 23.259 [15].

10.2 PN UE

When the PN UE that supports the PN controller functionality receives an initial request containing an Accept-Contact header containing g.3gpp.iari_ref feature tag containing the IARI value defined in sub clause 10.4 and a target URI-parameter in the Request-URI, the PN UE indicates to the user that the PN controller UE has received a request for the PN controllee UE and shall:

a) indicate the PN controllee UE indicated in the target URI-parameter in the Request-URI;

b) indicate the identity of the originating user indicated in the P-Asserted-Identity header.

The PN UE may offer the user the following options:

a) allow the request to be forwarded to the PN controllee UE;

b) deny the request (i.e reject the session);

c) accept the request (i.e establish the session).

When allowing the request to be forwarded to the PN controllee UE the PN UE shall send a 302 (Moved Temporarily) response. The PN UE constructs the response as follows:

a) shall include a Contact header containing the URI from the target URI-parameter in the Request-URI of the incoming request;

b) shall include a History-Info header copied from the incoming request unless the user wishes not to reveal to the user of the PN controllee UE that the request was forwarded first to the PN controller UE.

When the user allows the request to be forwarded to the PN controllee UE the PN UE may allow the user to add the URI from the P-Asserted-Identity header to a <PNAccessControlList> using the procedure in subclause 7.2.

When denying the request to be forwarded to the PN controllee UE the PN UE shall send either:

a) a 480 (Temporarily Unavailable) response if the user wishes to not allow the PN controllee UE to receive requests from the originator at this time but may allow requests at some future time;

b) a 410 (Gone) response if the user wishes to not allow the PN controllee UE to receive requests from the originator at any time but wishes the originator to not know that the request was actively blocked; or

c) a 403 (Forbidden) response if the user wishes to not allow the PN controllee UE to receive requests from the originator at any time and wishes the originator to know that the request was actively blocked.

The PN UE should only send a 480 (Temporarily Unavailable) response to PN controller request when the user has specifically denied the request as this will prevent the request being forwarded to other PN controller UEs. When the user allows the request to be forwarded to the PN controllee UE the PN UE may allow the user to add the URI from the P-Asserted-Identity header to a <PNAccessControlList> using the procedure in subclause 7.2.

When the user accepts the request the PN UE shall follow the procedures in 3GPP TS 24.229 [3].

10.3 PNM application

10.3.1 PN access control procedure in the IM CN subsystem

When the PNM AS receives an initial request destined for a PN UE within the same PN as the originating PN UE the PNM AS shall allow the request to continue normally.

When the PNM AS receives an initial request from a UE that is not a member of the same PN as the destination PN UE and the PN Access Control is not enabled the PNM AS shall return a 403 (Forbidden) response.

When the PNM AS receives an initial request from a UE that is not a member of the same PN as the destination PN UE and the destination PN UE exists in a <PNController> element in the PN access control list the PNM AS shall allow the request to continue normally.

When the PNM AS receives an initial request due to the terminating initial filter criteria, from a UE that is not a member of the same PN as the destination PN UE and the destination PN UE exists in a <PNControllee> element in the PN access control list the PNM AS shall verify if the address in the P-Asserted-Identity exists in a <PNAccessControlList> element in the PN access control list.

If there is a matching <PNAccessControlList> element the PNM AS shall allow the request to continue normally.

If there is no matching <PNAccessControlList> element the PNM AS shall send an initial request of the same SIP Method on a new dialog to the URI of the PN controller UE contained in the <PNController> element if it exists. If no <PNController> element exists then the PNM AS shall return a 403 (Forbidden) response. When sending the initial request to the PN controller UE the PNM AS shall include in the request the following:

> NOTE: The PNM AS is triggered first by forming the initial filter criteria in the S-CSCF.

> a) a Request-URI set to the SIP URI contained in the <PNController> element along with a target URI-Parameter as defined in IETF RFC 4458 [17] set to the URI from the Request-URI of the original initial request;

> b) a From header set to the SIP URI of the PNM AS;

> c) a To header set to the URI contained in the <PNController> element;

> d) a P-Asserted-Identity header set to the contents of the P-Asserted-Identity header in the original initial request;

> e) a Contact header set to the IP address or FQDN of the PNM AS;

> f) a Supported header containing the option tags from the original initial request with the addition of the option tag "histinfo";

> g) a History-Info header that includes as the Targeted-to-URI the URI from the Request-URI of the original initial request, and as the next branch index URI, the contents of the Request-URI of this request including the target URI-parameter along with the index parameters as specified in IETF RFC 4244 [16];

> h) an Accept-Contact header containing the g.3gpp.iari_ref feature tag containing the IARI value <urn:urn-xxx:3gpp-application.ims.iari.PNM-Controller>.

If the PNM AS receives in response a 302 (Moved Temporarily) response the PNM AS shall redirect the original incoming request to URI contained in the Contact header of the 302 (Moved Temporarily) response. The PNM AS shall add to the request the following:

> a) a Request-URI set to the SIP URI contained in the Contact header of the 302 (Moved Temporarily) response;

> b) a Supported header containing the option tags from the original initial request with the addition of the option tag "hist-info";

c) a History-Info header that includes the URIs from the History-Info header in the 302 (Moved Temporarily) response along with the contents of the Request-URI of this request as the next branch index URI under the top level Targeted-to-URI, along with the appropriate index parameter as specified in IETF RFC 4244 [16], if the 302 (Moved Temporarily) response contains a History-Info header;

If the PNM AS receives in response a 4xx (other than a 403 (Forbidden) response or 410 (Gone) response or 480 (Temporarily Unavailable) response), 5xx or 6xx response and there exists more <PNController> elements in the PN access control list which have not had the request forwarded to yet then the PNM AS shall send an initial request of the same SIP Method on a new dialog to the URI of the PN controller UE contained in the <PNController> element as above except that the History-Info header shall include the URIs from the History-Info header in the 302 (Moved Temporarily) response and as the next branch index URI, the contents of the Request-URI of this request including the target URI-parameter along with the index parameters as specified in IETF RFC 4244 [16];

Otherwise, if there does not exist more <PNController> elements in the PN access control list which have not had the request forwarded to yet, then forward the response back towards the originator of the initial request.

If the PNM AS receives in response a 200 (OK) response, a 403 (Forbidden) response, a 410 (Gone) response or 480 (Temporarily Unavailable) response the PNM AS shall forward the response back towards the originator of the initial request.

10.3.2   PN access control procedure in the CS domain

When the PNM application receives an indication that the gsmSCF has received a CAMEL IDP relating to a terminating call, the PNM application shall:

1) check if the access control is applicable on basis of service key and called party number received in CAMEL IDP message.

2) if the call is not subject to access control, cause the gsmSCF to respond with a CAMEL CONTINUE and no further PNM specific procedures are performed on this call.

3) if the call is subject to access control, it cause the gsmSCF perform as follows:

   a) check if the calling party is configured in PN access control list.

   b) if the calling party is configured in PN access control list,cause the gsmSCF to respond with CAMEL CONTINUE message to GMSC.

   c) if the calling party is not configured in PN access control list,cause the gsmSCF to generate the USSD request message to controller UE.

4) based on controller"s response it cause the gsmSCF respond with CAMEL CONTINUE or CALL RELEASE message to GMSC.

10.4   PNM controller IMS application reference identifier

The URN used to define the IARI for the PNM controller application: value urn:urn-xxx:3gpp-application.ims.iari.pnm-controller. The URN is registered at http://www.3gpp.org/tb/Other/URN/URN.htm.

Summary of the URN: This URN indicates that the device supports the PNM controller application

The URN is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

- This URN is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Indicating that a mobile phone supports the PNM controller application.

Related standards or documents:

- 3GPP TS 24.259: "Personal Network Management (PNM), stage 3" [3]

11 Protocol at the Ut reference point

11.1 Introduction

XML Configuration Access Protocol (XCAP) is used to create, read, write, modify and delete data related to the PNM service. XCAP uses the HTTP methods PUT, GET and DELETE for communication over the Ut reference point.

11.2 Roles

11.2.1 XCAP client

The XCAP client is a logical function as defined in IETF RFC 4825 [6]. The XCAP client provides the means to create, read, write, modify and delete the data used for the PNM services. In doing so, it shall generate an HTTP PUT, or an HTTP GET or an HTTP DELETE request in accordance with IETF RFC 2616 [7] and 3GPP TS 24.623 [18].

11.2.2 XCAP server

The XCAP server is a logical function as defined in IETF RFC 4825 [6]. The XCAP server stores all data relevant for the PNM services. When the XCAP server receives an HTTP PUT, HTTP GET or HTTP DELETE request for manipulating the data base, the XCAP server shall first authenticate the request in accordance with 3GPP TS 24.109 [5] and then perform authorization. Afterwards the XCAP server shall perform the requested action and generate a response in accordance with IETF RFC 2616 [7] and 3GPP TS 24.623 [18].

Annex A (informative):
Example signalling flows

A.1   Scope of signalling flows

This annex gives examples of signalling flows for Personal Network Management based on XCAP, the Session Initiation Protocol (SIP) and SIP Events.

These signalling flows provide detailed signalling flows, which expand on the overview information flows provided in 3GPP TS 23.259 [15].

A.2   Introduction

A.2.1   General

The signalling flows provided in this annex follow the methodology developed in 3GPP TS 24.228 [10]. The following additional considerations apply:

    a)   3GPP TS 24.228 [10] shows separate signalling flows with no configuration hiding between networks, and with configuration hiding between networks. There is no personal network management specific functionality associated with this hiding, and therefore such separate signalling flows are not show in the present document;

    b)   3GPP TS 24.228 [10] does not show the functionality between the S-CSCF and the AS. As personal network management depends on the functionality provided by various AS, the signalling flows between S-CSCF and AS are shown in the present document;

    c)   3GPP TS 24.228 [10] breaks down the functionality of the various CSCFs. Such intervening activity in the CSCFs is in general not relevant to showing the functionality within personal network management, and therefore the CSCFs are often collapsed into a single entity labelled "Intermediate IM CN subsystem entities";

    d)   where entities are combined as in c) above, and the signalling flow is directed to such a combined entity, the contents of the signalling flow represent the contents of the sending entity except when otherwise stated;

    e)   where entities are combined as in c) above and the signalling flow originates at such a combined entity, the contents of the signalling flow represent the contents of the receiving entity except when otherwise stated;

    f)   within the CS domain, both ISUP and BICC can be used. The signalling flows represent only the ISUP signalling flows, and the BICC signalling flows (which can be assumed to be similar with no additional PNM specific content) are not shown; and

    g)   additional functionality from 3GPP releases 6, 7 and 8 over and above that shown in 3GPP TS 24.228 [10] is incorporated in these.

A.2.2   Key required to interpret signalling flows

The key to interpret signalling flows specified in 3GPP TS 24.228 [10] subclauses 4.1 and 4.2 applies with the additions specified below:

    -     Consistent with the conventions used in 3GPP TS 24.228 [10] home1.net is used for the home network of the originating user and home2.net is used for the home network of the terminating user. In registration and configuration flows the PN UE and PNM network elements are considered to be in home1.net, however in scenarios such as PN redirection and PNM access control where the PNM elements are in the terminating network the PN UE and PNM network elements are considered to be in home2.net. Therefore in some flows identities shown as home2.net are equivalent to the identities shown as home1.net in other flows and as described further below.

For signaling flows for PN-registration (see subclause A.3.2) and PN-configuration (see subclause A.3.3) the following applies:

- pnmas.home1.net:1234 represents the Internet host and port number of the PNM AS, which can be obtained by a PN UE from the address (URI) of the resource http://pnmas.home1.net:1234/service.

- PN_user1_public1@home1.net, PN_user1_public2@home1.net, etc. represent the public user identities configured for a PN-user for the PN UE#1. PN_user2_public1@home1.net, PN_user2_public2@home1.net, etc. represent the public user identities configured for a PN-user for the PN UE#2, etc. PN_user_public@home1.net represents the shared public user identity.

- PN_user1_private@home1.net represents the private user identity configured for a PN-user for PN UE#1. PN_user2_private@home1.net represents the private user identity configured for a PN-user for PN UE#2, etc.

- PN_user1_friend_public1@home1.net, PN_user1_friend_public2@home1.net etc represent the public user identities of a PN access control list configured for PN UE#1. PN_user2_friend_public1@home1.net, PN_user2_friend_public2@home1.net etc represent the public user identities of a PN access control list configured for PN UE#2, etc.

- PN_user1_public1_old and PN_user1_public1_new represent the old and the new PN UE names related to the public user identity PN_user1_public1@home1.net, PN_user2_public1_old and PN_user2_public1_new represent the old and the new PN UE names related to the public user identity PN_user2_public1@home1.net.

For signaling flows for PN UE redirection (see subclause A.3.4), PN access control (see subclause A.3.5) and inter-domain networking (see subclause A.3.6) the following applies:

- PN_user1_public@home2.net, PN_user2_public@home2.net, etc. represent the public user identities for the PN UEs;

- user1_public1@home1.net represents a user outside of the personal network originating a session to a user within the personal network.

In order to differentiate between messages for HTTP, SIP, Diameter and media flows over CS and PS connections, the notation in figure A.2.2-1 is used.
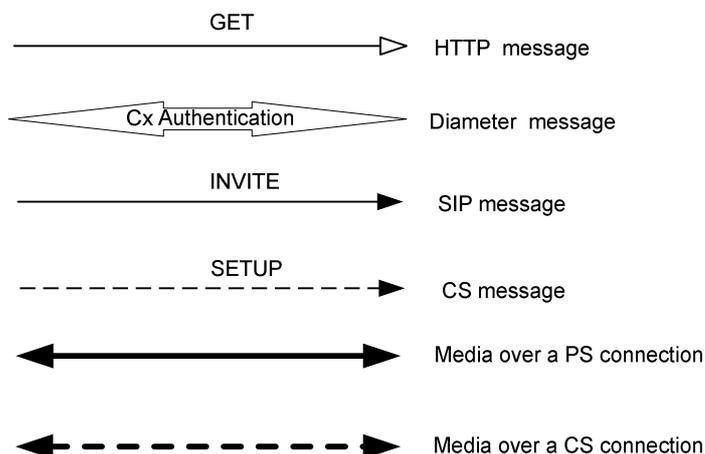
Figure A.2.2-1: Signalling flow notation

A.3 Signalling flows

A.3.1 Introduction

The signalling flows demonstrate how the PN-registration, PN-configuration, PN UE redirection and PN access control procedures work. The following signalling flows are included:

- subclause A.3.2.1 shows the successful PN-registration in the IM CN subsystem using third party registration;

- subclause A.3.2.2 shows the successful PN-registration with subscription to reg event package;

- subclause A.3.3.1 shows the successful PN-configuration for PN UE redirection;

- subclause A.3.3.2 shows the successful PN-configuration for PN access control;

- subclause A.3.3.3 shows the successful PN-configuration for changing PN UE name;

- subclause A.3.3.4 shows the successful PN-query;

- subclause A.3.3.5 shows the successful PN-deconfiguration;

- subclause A.3.4.1 shows the successful for PN UE redirection in the IM CN subsystem;

- subclause A.3.4.2 shows the successful PN UE redirection in the CS domain;

- subclause A.3.5.1 shows the successful PN access control procedure in IM CN subsystem;

- subclause A.3.5.2 shows the successful PN access control procedure in CS domain;

- subclause A.3.6.1 shows the successful interdomain networking (IM CN subsystem to CS domain);

- subclause A.3.6.2 shows the successful interdomain networking (CS domain to IM CN subsystem);

A.3.2 Signalling flows for PN-registration

A.3.2.1 PN-registration in the IM CN subsystem using third party registration

Figure A.3.2.1-1 details the signalling flows for a successful PN-registration in the IM CN subsystem using third party registration.
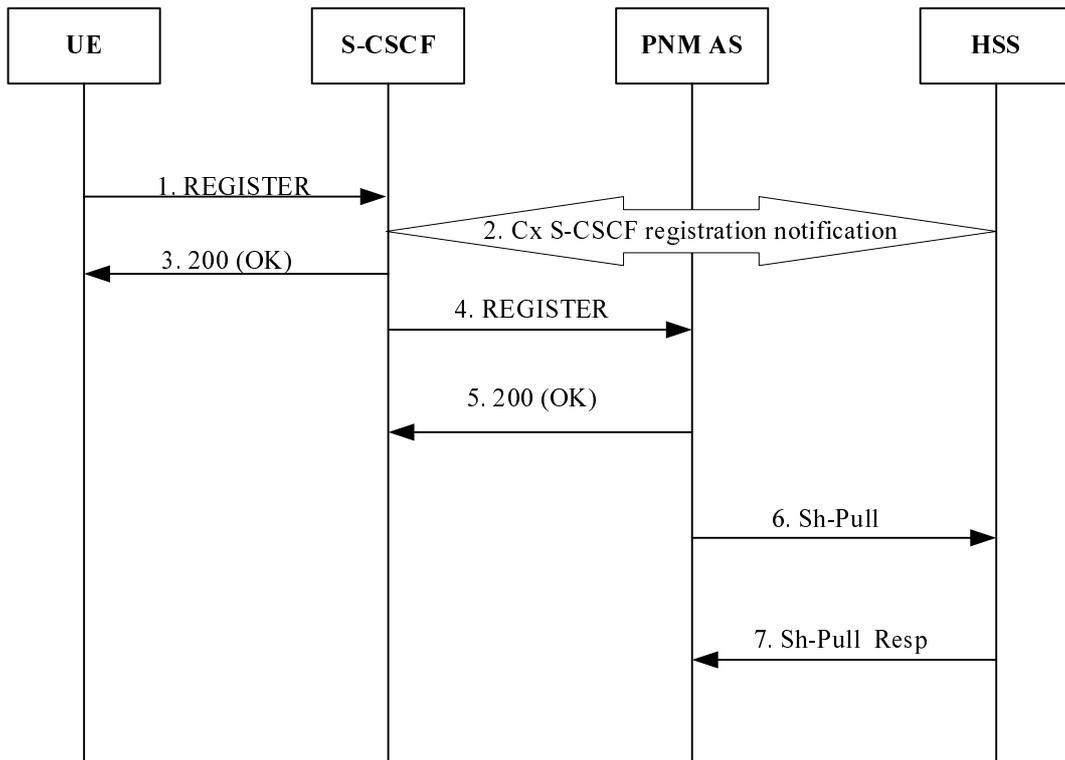
Figure A.3.2.1-1: Successful PN-registration signalling: in the IM CN subsystem using third party registration

1. **REGISTER request (PN UE to IM CN subsystem entities)**

   PN UE initiates a REGISTER request after successful authentication.

Table A.3.2.1-1: REGISTER request (PN UE to IM CN subsystem entities)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11: 3GPP-UTRAN; np
Path:<VskztcQ/S8p4WPbOnHbuyh5iJvJIW3ib@pcscf1.visited1.net:1337;lr;ob>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From: <sip:PN_user1_public1@home1.net>;tag=4fa3
To: <sip:PN_user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;reg-id=1;
+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>";
+g.3gpp.icsi_ref='urn%3Aurn-xxx%3A3gpp-service.ims.icsi.mmtel";
+g.3gpp.iari_ref="urn%3Aurn-xxx%3A3gpp-application.ims.iari.pnm-controller";
+g.3gpp.cs-audio;
+g.3gpp.cs-video;
expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
protected="yes"
CSeq: 2 REGISTER
Supported: gruu, outbound
Content-Length: 0
```

NOTE: the above REGISTER request contents are shown as received at the S-CSCF not as sent by the PN UE.

2. **Cx: S-CSCF registration notification procedure**

There is no PNM specific content to this, for detailed message flows see 3GPP TS 29.228 [11] in subclause 6.1.2.

3. SIP 200 (OK) response (IM CN subsystem entities to PN UE)

4. REGISTER request (S-CSCF to PNM AS)

After PN UE successfully registered in the IM CN subsystem, the S-CSCF sends a third party REGISTER request containing in the body the incoming REGISTER request from the PN UE to the PNM AS based on the initial filter criteria it received which contains an Include Register Request XML element.

Table A.3.2.1-4: REGISTER request (S-CSCF to PNM AS)

```
REGISTER sip: pnmas.home1.net /2.0
Via: SIP/2.0/UDP pnmas.home1.net;branch=z9hG499ffhy
Max-Forwards: 70
From: <sip:scscf1.home1.net>; tag=538ya
To: <sip: PN_user1_public1@home1.net >
Call-ID: 1asdaddlrfjflslj40a222
Contact: <sip:scscf1.home1.net>; expires=600000
CSeq: 87 REGISTER
Content-Type: message/sip
Content-Length: (…)

REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11: 3GPP-UTRAN; np
Path:<VskztcQ/S8p4WPbOnHbuyh5iJvJIW3ib@pcscf1.visited1.net:1337;lr;ob>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From: <sip:PN_user1_public1@home1.net>;tag=4fa3
To: <sip:PN_user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;reg-id=1;
+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>";
+g.3gpp.icsi_ref='urn%3Aurn-xxx%3A3gpp-service.ims.icsi.mmtel";
+g.3gpp.iari_ref="urn%3Aurn-xxx%3A3gpp-application.ims.iari.pnm-controller";
+g.3gpp.cs-audio;
+g.3gpp.cs-video;
expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
protected="yes"
CSeq: 2 REGISTER
Supported: gruu, outbound
Content-Length: 0
```

5. SIP 200 (OK) response (PNM AS to S-CSCF)

6. Sh-Pull (AS to HSS)

For detailed message flows see 3GPP TS 29.328 [9] in subclause 6.1.1.

7. Sh-Pull Response (HSS to PNM AS)

As a successful verification, the PNM AS enrols the public user identity as registered in the database.

A.3.2.2 PN-registration in the IM CN subsystem with subscription to reg event package

Figure A.3.2.2-1 details the signalling flows for a successful PN-registration in the IM CN subsystem with subscription to reg event package.
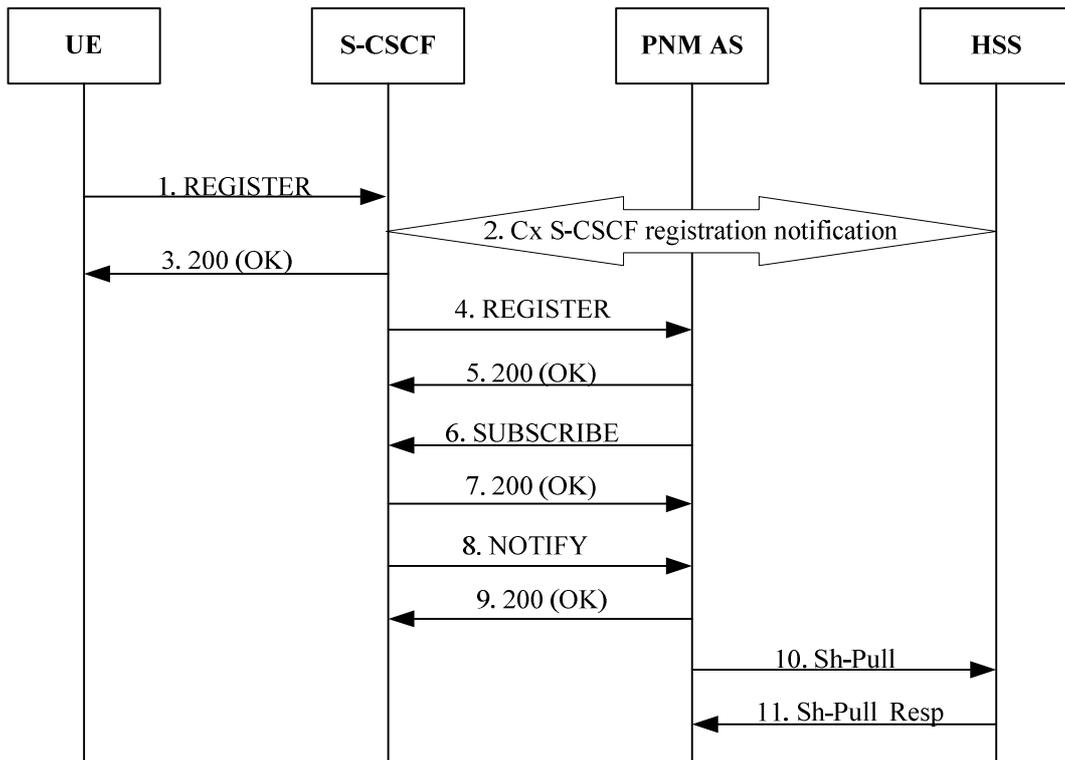
Figure A.3.2.2-1: Successful PN-registration signalling: in the IM CN subsystem with subscription to reg event package

1. **REGISTER request (PN UE to IM CN subsystem entities)**

   PN UE initiates a REGISTER request after successful authentication.

Table A.3.2.2-1: REGISTER request (PN UE to IM CN subsystem entities)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11: 3GPP-UTRAN; np
Path:<VskztcQ/S8p4WPbOnHbuyh5iJvJIW3ib@pcscf1.visited1.net:1337;lr;ob>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From: <sip:PN_user1_public1@home1.net>;tag=4fa3
To: <sip:PN_user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;reg-id=1;
+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>";
+g.3gpp.icsi_ref='urn%3Aurn-xxx%3A3gpp-service.ims.icsi.mmtel";
+g.3gpp.iari_ref="urn%3Aurn-xxx%3A3gpp-application.ims.iari.pnm-controller";
+g.3gpp.cs-audio;
+g.3gpp.cs-video;
expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
protected="yes"
CSeq: 2 REGISTER
Supported: gruu, outbound
Content-Length: 0
```

NOTE: The above REGISTER request contents are shown as received at the S-CSCF not as sent by the PN UE.

2. **Cx: S-CSCF registration notification procedure**

There is no PNM specific content to this, for detailed message flows see 3GPP TS 29.228 [11] in subclause 6.1.2.

3. SIP 200 (OK) response (IM CN subsystem entities to PN UE)

4. REGISTER request (S-CSCF to PNM AS)

After PN UE successfully registered in the IM CN subsystem, the S-CSCF sends a third party REGISTER request containing in the body a <service-info> element containing the private user identity of the PN UE to the PNM AS based on the initial filter criteria it received which contains the <service-info> element containing the private user identity of the PN UE.

Table A.3.2.2-4: REGISTER request (S-CSCF to PNM AS)

```
REGISTER sip: pnmas.home1.net /2.0
Via: SIP/2.0/UDP pnmas.home1.net;branch=z9hG499ffhy
Max-Forwards: 70
From: <sip:scscf1.home1.net>; tag=538ya
To: <sip: PN_user1_public1@home1.net >
Call-ID: 1asdaddlrfjflslj40a222
Contact: <sip:scscf1.home1.net>; expires=600000
CSeq: 87 REGISTER
Content-Type: application/3gpp-ims+xml
Content-Length: (…)

<3gpp-ims version="1">
<service-info>sip:PN_user1_private@home1.net</service-info>
</3gpp-ims>
```

5. SIP 200 (OK) response (PNM AS to S-CSCF)

6. SUBSCRIBE request (PNM AS to S-CSCF) - see example in table A.3.2.2-6

The PNM AS sends the SUBSCRIBE request to the S-CSCF to the reg event package for the public user identity.

Table A.3.2.2-6: SUBSCRIBE request (PNM AS to S-CSCF)

```
SUBSCRIBE sip: PN_user1_public1@home1.net /2.0
Via: SIP/2.0/UDP pnmas.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 70
Route: <sip:scscf@home1.net;lr>
Privacy: none
From: <sip: pnamas.home1.net>; tag=31415
To: <sip: PN_user1_public1@home1.net >
Call-ID: b89rjhnedlrfjflslj40a222
CSeq: 61 SUBSCRIBE
Event: reg
Expires: 600000
Accept: application/reginfo+xml
Contact: <sip:pnmas.home1.net>
Content-Length: 0
```

7. SIP 200 (OK) response (S-CSCF to PNM AS)

8. NOTIFY request (S-CSCF to PNM AS) - see example in table A.3.2.2-8

The S-CSCF sends a first NOTIFY request towards the PNM AS in order to inform the PNM AS about the registration status of monitored user and the UE capabilities.

Table A.3.2.2-8: NOTIFY request (S-CSCF to PNM AS)

```
NOTIFY sip: pnmas.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf@home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 70
From: <sip:scscf@home1.net>;tag=151170
To: <sip: pnmas.home1.net>;tag=31415
Call-ID: dre36d2v32gnlgiiomm72445
CSeq: 42 NOTIFY
```

```
Subscription-State: active;expires=600000
Event: reg
Content-Type: application/reginfo+xml
Contact: <sip:scscf@home1.net>
Content-Length: (...)

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
    xmlns:gr="urn:ietf:params:xml:ns:gruuinfo"
version="1" state="full">
    <registration aor="sip: PN_user1_public1@home1.net" id="a7" state="active">
        <contact id="76" state="active" event="registered">
        <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    <allOneLine>
        <unknown-param name='+sip.instance'>&lt;urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6&gt;'
</unknown-param>
        <unknown-param name='+g.3gpp.icsi_ref'>&lt;urn:urn-xxx:3gpp-service.ims.icsi.mmtel&gt;'
</unknown-param>
        <unknown-param name='+g.3gpp.iari_ref'>&lt;urn:urn-xxx:3gpp-application.ims.iari.pnm-
controller&gt"</unknown-param>
        <unknown-param name='+g.3gpp.cs-audio'> </unknown-param>
        <unknown-param name='+g.3gpp.cs-video'> </unknown-param>
    </allOneLine>
    <allOneLine>
            <gr:pub-gruu uri="sip:PN_user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6"/>
    </allOneLine>
    <gr:temp-gruu uri="sip:8ffkas08af7fasklzi9@home1.net;gr" first-cseq="40"/>
    </contact>
        </registration>
        <registration aor="sip:PN_user1_public2@home1.net" id="a8" state="active">
    <contact id="77" state="active" event="created">
        <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
        <allOneLine>
            <unknown-param name='+sip.instance'>&lt;urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6&gt;' </unknown-param>
            <unknown-param name='+g.3gpp.iari_ref'>&lt;urn:urn-xxx:3gpp-service.ims.icsi.mmtel&gt;'
</unknown-param>
            <unknown-param name='+g.3gpp.cs-audio'> </unknown-param>
            <unknown-param name='+g.3gpp.cs-video'> </unknown-param>
        </allOneLine>
        <allOneLine>
            <gr:pub-gruu uri="sip:PN_user1_public2@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6"/>
        </allOneLine>
            <gr:temp-gruu uri="sip:2k3e8farf7flfka9zi9@home1.net;gr" first-cseq="40"/>
    </contact>
    </registration>
</reginfo>
```

9. **SIP 200 (OK) response (PNM AS to S-CSCF)**

10. **Sh-Pull (AS to HSS)**

   For detailed message flows see 3GPP TS 29.328 [9] in subclause 6.1.1.

11. **Sh-Pull Response (HSS to PNM AS)**

   As a successful verification, the PNM AS enrols the public user identity as registered in the database.

A.3.3 Signalling flows for PN-configuration

A.3.3.1 PN-configuration for PN UE redirection

Figure A.3.3.1-1 shows the message exchange between PN UE and NAF/PNM AS when the PN UE wants to configure the PN settings for the PN UE redirection. The messaging only takes place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [8]) in which case the bootstrapped security association has been established before Step 1.
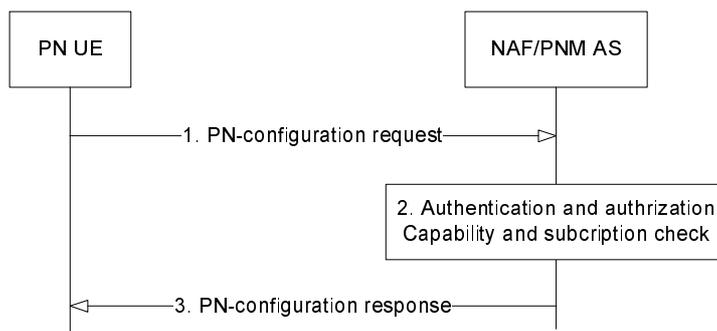
Figure A.3.3.1-1: Successful PN-configuration for UE redirection

1. **Initial PN-configuration request (PN UE to NAF/PNM AS) - see example in table A.3.3.1-1**

    The PN UE sends an HTTP request to the NAF/PNM AS containing the configuration request for the PN UE redirection.

Table A.3.3.1-1: Initial PN-configuration request (UE to NAF/PNM AS)

```
PUT http://xcap.home1.net/pnm.3gpp.org/users/sip:PN_user_public@home1.net/pnm HTTP/1.1
Host: pnmas.home1.net:1234
User-Agent: PNM User Agent; Release-6 3gpp-gba
Content-Type: application/pnm+xml charset="utf-8"
Content-Length: (...)
Date: Wed, 31 Oct 2007 10:50:35 GMT
Accept: application/pnm+xml
Referrer: http://pnmas.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@pnmas.home1.net",
nonce="a6332ffd2d234==", uri="pnmclient", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5

<?xml version="1.0" encoding="utf-8"?>
<PNConfiguration>
    <UERedirection UriOfRedirectedUser="sip:PN_user1_public1@home1.net">
        <RedirectedUserID>
            <PNUEID>sip:PN_user1_public1@home1.net</PNUEID>
            <PNUEName>PN_user1_public1_old</PNUEName>
        </RedirectedUserID>
        <RedirectingUserID id=1>
            <PNUEID>sip:PN_user2_public1@home1.net</PNUEID>
            <PNUEName>PN_user2_public1_old</PNUEName>
            <RedirectionLevel>application</RedirectionLevel>
            <RedirectionPrio>1</RedirectionPrio>
        </RedirectingUserID>
    </UERedirection>
</PNConfiguration>
```

Request-URI: The Request-URI (the URI that follows the method name, "PUT", in the first line) indicates the resource of this PUT request. The Request-URI contains the XCAP HTTP URI which indicates to the PNM AS the desired PN is requested to be configured.

Host: Specifies the Internet host and port number of the PNM AS, obtained from the original URI given by referring resource.

User-Agent: Contains information about the user agent originating the request and it includes the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.

Referer: Allows the user agent to specify the address (URI) of the resource from which the URI for the PNM AS was obtained.

Authorization: Contains the credentials obtained by means of the bootstrapping procedure (as described in 3GPP TS 33.220 [8]).

XML body: Contains the settings for the PN UE redirection that the PN-user request the PNM AS to do. In this example, the UE with public user identity <sip: PN_user1_public1@home1.net > requests the PNM AS to configure the redirection of all sessions, addressing <sip: PN_user2_public1@home1.net > with the PN UE name PN_user2_public1_old, to <sip: PN_user1_public1@home1.net > with the PN UE name PN_user1_public1_old with a highest priority equal to one.

2. **Authentication/authorization and UE capability and subscription checking**

NAF/PNM AS verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key material Ks_NAF obtained from BSF (as described in 3GPP TS 33.220 [8]). NAF/PNM AS calculates the corresponding digest values using Ks_NAF, and compares the calculated values with the received values in the Authorization header. If the verification succeeds, the NAF passes the private user identity <sip: PN_user1_private@home1.net> associated with the public user identity <sip: PN_user1_public1@home1.net> to the PNM AS. The PNM AS then authorizes the UE by comparing the received public user identity <sip: PN_user1_public1@home1.net> with the preconfigured one identified by the private user identity <sip: PN_user1_private@home1.net>. If the authorization succeeds, the incoming request is taken in for further processing.

The NAF/PNM AS also performs the PN UE capability and subscription checking. If the checking succeeds, the incoming request is taken in for further processing.

NOTE: Performing the PN UE subscription checking entails the interaction with the HSS over the sh interface (see 3GPP TS 29.328 [9]) which is not shown in the message flow.

3. **Delivery of PN-configuration response (NAF/PNM AS to PN UE) - see example in table A.3.3-3**

The PNM AS sends HTTP 200 OK response to the PN UE to indicate the success of the PN-configuration.

Table A.3.3.1-3: Delivery of PN-configuration response (NAF/PNM AS to PN UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Length: 0
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Wed, 31 Oct 2007 10:50:36 GMT
Expires: Wed, 31 Nov 2007 10:50:36 GMT
```

Authentication-Info: This carries the protection.

A.3.3.2 PN-configuration for PN access control

Figure A.3.3.2-1 shows the message exchange between PN UE and NAF/PNM AS when PN UE wants to configure the PN settings for the PN access control service. The messaging only takes place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [8]) in which case the bootstrapped security association has been established before step 1.
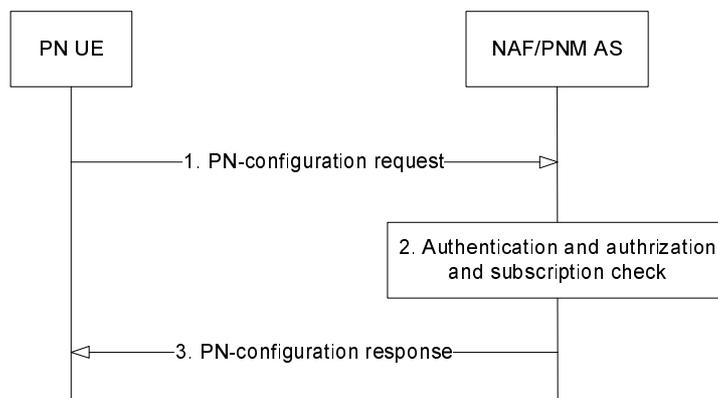

Figure A.3.3.2-1: Successful initial PN-configuration for PN access control

1. **Initial PN-configuration request (PN UE to NAF/PNM AS) - see example in table A.3.3.2-1**

   The PN UE sends an HTTP request to the NAF/PNM AS containing the configuration request for the PN access control.

Table A.3.3.2-1: Initial PN-configuration request (UE to NAF/PNM AS)

```
PUT http://xcap.home1.net/pnm.3gpp.org/users/sip:PN_user_public@home1.net/pnm HTTP/1.1
Host: pnmas.home1.net:1234
User-Agent: PNM User Agent; Release-6 3gpp-gba
Content-Type: application/pnm+xml charset="utf-8"
Content-Length: (...)
Date: Wed, 31 Oct 2007 10:50:35 GMT
Accept: application/pnm+xml
Referrer: http://pnmas.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@pnmas.home1.net",
nonce="a6332ffd2d234==", uri="pnmclient", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5

<?xml version="1.0" encoding="utf-8"?>
<PNConfiguration>
    <AccessControl UriOfControllerUE="sip:PN_user1_public1@home1.com">
        <ControllerUE>
            <PNUEID>sip:PN_user1_public1@home1.net</PNUEID>
            <PNUEName>PN_user1_public1_old</PNUEName>
        </ControllerUE>
        <ControlleeUE id=1>
            <PNUEID>sip:PN_user2_public1@home1.net</PNUEID>
            <PNUEName>PN_user2_public1_old</PNUEName>
            <PNAccessControlList>sip:PN_user1_friend_public1@home1.net
sip:PN_user1_friend_public2@home1.net</PNAccessControlList>
            <PNAccessControlType>Controller</PNAccessControlType>
        </ControlleeUE>
    </AccessControl>
</PNConfiguration>
```

Request-URI:	The Request-URI (the URI that follows the method name, "PUT", in the first line) indicates the resource of this PUT request. The Request-URI contains the XCAP HTTP URI which indicates to the PNM AS the desired PN is requested to be configured.
Host:	Specifies the Internet host and port number of the PNM AS, obtained from the original URI given by referring resource.
User-Agent:	Contains information about the user agent originating the request and it includes the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.
Referer:	Allows the user agent to specify the address (URI) of the resource from which the URI for the PNM AS was obtained.
Authorization:	Contains the credentials obtained by means of the bootstrapping procedure (as described in 3GPP TS 33.220 [8]).
XML body:	Contains the settings for the PN access control service that the UE requests from the PNM AS. In this example, the UE with public user identity <sip: PN_user1_public1@home1.net> requests the PNM AS to configure PN access control for all sessions, addressing <sip: PN_user2_public1@home1.net > with the PN UE name PN_user2_public1_old, except for the case when the callee is either <sip: PN_user1_friend_public1@home1.net> or < sip: PN_user1_friend_public2@home1.net >. Furthermore, the UE indicates in the access control type that the controller UE with <sip: PN_user1_public1@home1.net> and the PN UE name PN_user1_public1_old needs to be interrogated when the PNM AS executes the PN access control.

2. **Authentication/authorization and subscription checking**

   As described in Step 2 within Figure A.3.3.1-1.

3. **Delivery of PN-configuration response (NAF/PNM AS to PN UE) - see example in table A.3.3.2-3**

The PNM AS sends HTTP 200 OK response to the PN UE to indicate the success of the PN-configuration.

Table A.3.3.2-3: Delivery of PN-configuration response (NAF/PNM AS to PN UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Length: 0
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Wed, 31 Oct 2007 10:50:36 GMT
Expires: Wed, 31 Nov 2007 10:50:36 GMT
```

Authentication-Info: This carries the protection.

A.3.3.3 PN-configuration for changing PN UE name

Figure A.3.3.3-1 shows the message exchange between PN UE and NAF/PNM AS when the PN UE changes the PN UE name. The messaging only takes place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [8]) in which case a bootstrapped security association has been established before Step 1.
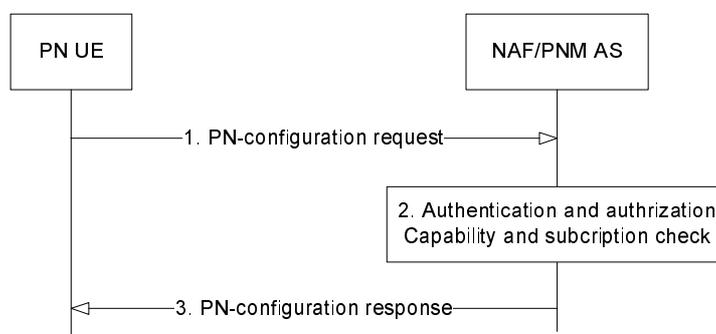
Figure A.3.3.3-1: Successful PN-configuration for changing PN UE name

1. **Initial PN-configuration request (PN UE to NAF/PNM AS) - see example in table A.3.3.3-1**

   The PN UE sends an HTTP request to the NAF/PNM AS containing the configuration request for changing the PN UE name.

Table A.3.3.3-1: Initial PN-configuration request (UE to NAF/PNM AS)

```
PUT http://xcap.home1.net/pnm.3gpp.org/users/sip:PN_user_public@home1.net/pnm HTTP/1.1
Host: pnmas.home1.net:1234
User-Agent: PNM User Agent; Release-6 3gpp-gba
Content-Type: application/pnm+xml charset="utf-8"
Content-Length: (...)
Date: Wed, 31 Oct 2007 10:50:35 GMT
Accept: application/pnm+xml
Referrer: http://pnmas.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@pnmas.home1.net",
nonce="a6332ffd2d234==", uri="pnmclient", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5

<?xml version="1.0" encoding="utf-8"?>
<PNConfiguration>
    <NameofPNUE>
        <PNUEID>sip:PN_user1_public1@home1.net</PNUEID>
        <UEName id=1>
            <Name>PN_user1_public1_new</Name>
    </NameofPNUE>
</PNConfiguration>
```

Request-URI: The Request-URI (the URI that follows the method name, "PUT", in the first line) indicates the resource of this PUT request. The Request-URI contains the XCAP HTTP URI which indicates to the PNM AS the desired PN is requested to be configured.

Host: Specifies the Internet host and port number of the PNM AS, obtained from the original URI given by referring resource.

User-Agent: Contains information about the user agent originating the request and it includes the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.

Referer: Allows the user agent to specify the address (URI) of the resource from which the URI for the PNM AS was obtained.

Authorization: Contains the credentials obtained by means of the bootstrapping procedure (as described in 3GPP TS 33.220 [8]).

XML body: Contains the old and the new PN UE names that the PN-user requests the PNM AS to change. In this example, the UE with public user identity <sip: PN_user1_public1@home1.net > request the PNM AS to change the old PN UE name with the new PN UE name "PN_user1_public1_new".

2. **Authentication/authorization and UE capability and subscription checking**

    As described in Step 2 within figure A.3.3.1-1.

NOTE: Changing the PN UE name from PN_user1_public1_old to PN_user1_public1_new does not entail interaction between the PN MAS and the HSS over the Sh interface.

3. **Delivery of PN-configuration response (NAF/PNM AS to PN UE) - see example in table A.3.3.3-3**

    The PNM AS sends HTTP 200 OK response to the PN UE to indicate the success of the PN-configuration.

Table A.3.3.3-3: Delivery of PN-configuration response (NAF/PNM AS to PN UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Length: 0
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Wed, 31 Oct 2007 10:50:36 GMT
Expires: Wed, 31 Nov 2007 10:50:36 GMT
```

Authentication-Info: This carries the protection.

A.3.3.4   PN-query

Figure A.3.3.4-1 shows the message exchange between PN UE and NAF/PNM AS when PN UE wants to obtain the PN setting information from the PNM AS. The messaging only takes place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [8]) in which case the bootstrapped security association has been established before Step 1.
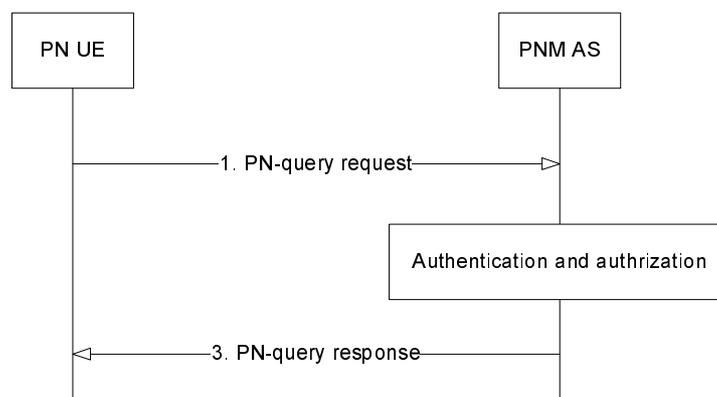

Figure A.3.3.4-1: Successful PN-query

1. **Initial PN-query request (PN UE to NAF/PNM AS) - see example in table A.3.3.4-1**

   The PN UE sends an HTTP request to the NAF/PNM AS PN in order to obtain the PN setting information of the <UERedirection> with the attribute value "UriOfRedirectedUser= sip:PN_user1_public1@home1.net".

Table A.3.3.4-1: Initial PN-query request (UE to NAF/PNM AS)

```
GET
http://xcap.home1.net/pnm.3gpp.org/users/sip:PN_user_public@home1.net/pnm/~~/PNConfiguration/UEredir
ection%5b@UriOfRedirectedUser=%22sip:PN_user1_public1@home1.net%22%5d HTTP/1.1
Host: pnmas.home1.net:1234
User-Agent: PNM User Agent; Release-6 3gpp-gba
Content-Length: 0
Date: Wed, 31 Oct 2007 10:50:35 GMT
Accept: application/pnm+xml
Referrer: http://pnmas.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@pnmas.home1.net",
nonce="a6332ffd2d234==", uri="pnmclient", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5
```

Request-URI:	The Request-URI (the URI that follows the method name, "PUT", in the first line) indicates the resource of this PUT request. The Request-URI contains the XCAP HTTP URI which indicates to the PNM AS the desired PN is requested to be queried.
Host:	Specifies the Internet host and port number of the PNM AS, obtained from the original URI given by referring resource.
User-Agent:	Contains information about the user agent originating the request and it includes the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.
Referer:	Allows the user agent to specify the address (URI) of the resource from which the URI for the PNM AS was obtained.
Authorization:	Contains the credentials obtained by means of the bootstrapping procedure (as described in 3GPP TS 33.220 [8]).
XML body:	In this example, it is assumed that the UE with the public user identity < sip: PN_user1_public1@home1.net > interrogates the PNM AS for the whole set of the PN setting information.

2. **Authentication/authorization and UE capability**

   See Step 2 described within Figure A.3.3.1-1.

3. **Delivery of PN-query response (NAF/PNM AS to PN UE) - see example in table A.3.3.4-3**

   The PNM AS sends HTTP 200 OK response to the PN UE to inform the whole set of the PN setting information for the <UERedirection> with the attribute value "UriOfRedirectedUser= sip:PN_user1_public1@home1.net".

Table A.3.3.4-3: Delivery of PN-query response (NAF/PNM AS to PN UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Length: 0
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Wed, 31 Oct 2007 10:50:36 GMT
Expires: Wed, 31 Nov 2007 10:50:36 GMT

<?xml version="1.0" encoding="utf-8"?>
<PNConfiguration>
    <UERedirection UriOfRedirectedUser="sip:PN_user1_public1@home1.net">
        <RedirectedUserID>
            <PNUEID>sip:PN_user1_public1@home1.net</PNUEID>
            <PNUEName>PN_user1_public1_old</PNUEName>
        </RedirectedUserID>
        <RedirectingUserID id=1>
```

ETSI

```
            <PNUEID>sip:PN_user2_public1@home1.net</PNUEID>
            <PNUEName>PN_user2_public1_old</PNUEName>
            <RedirectionLevel>application</RedirectionLevel>
            <RedirectionPrio>1</RedirectionPrio>
        </RedirectingUserID>
</PNConfiguration>
```

Authentication-Info: This carries the protection.

XML body: Indicates the whole set of the PN setting information related to the UE with the public user identity
                     < sip: PN_user1_public1@home1.net>.

A.3.3.5   PN-deconfiguration

Figure A.3.3.5-1 shows the message exchange between PN UE and NAF/PNM AS when PN UE wants to deconfigure
the PN settings for the UE redirection service and the PN access control service. The messaging only takes place after a
successful bootstrapping procedure (as described in 3GPP TS 33.220 [8]) in which case the bootstrapped security
association has been established before step 1.
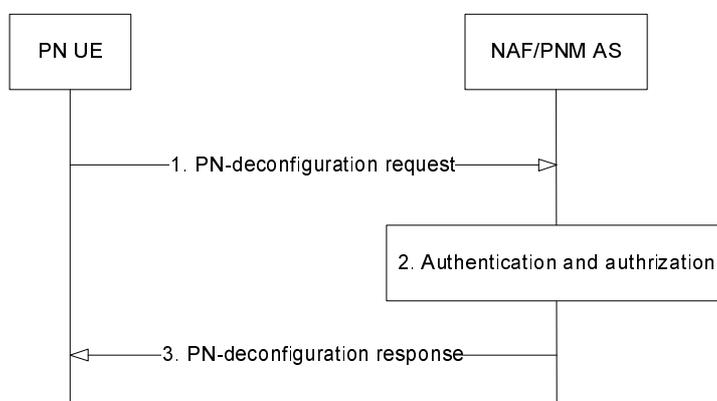
Figure A.3.3.5-1: Successful initial PN-deconfiguration

1. **Initial PN-deconfiguration request (PN UE to NAF/PNM AS) - see example in table A.3.3.5-1**

    The PN UE sends an HTTP request to the NAF/PNM AS containing the configuration request to delete the
    <UERedirection> with the attribute value "UriOfRedirectedUser= sip:PN_user1_public1@home1.net".

Table A.3.3.5-1: Initial PN-configuration request (UE to NAF/PNM AS)

```
DELETE
http://xcap.home1.net/pnm.3gpp.org/users/sip:PN_user_public@home1.net/pnm/~~/PNConfiguration/UERedir
ection%5b@UriOfRedirectedUser=%22sip:PN_user1_public1@home1.net%22%5d HTTP/1.1
Host: pnmas.home1.net:1234
User-Agent: PNM User Agent; Release-6 3gpp-gba
Content-Length: 0
Date: Wed, 31 Oct 2007 10:50:35 GMT
Accept: text/xml
Referrer: http://pnmas.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@pnmas.home1.net",
nonce="a6332ffd2d234==", uri="pnmclient", qop=auth-int, nc=00000001,
cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5
```

Request-URI: The Request-URI (the URI that follows the method name, "DELETE", in the first line)
                        indicates the resource of this DELETE request. The Request-URI contains the XCAP HTTP
                        URI which indicates to the PNM AS the desired PN is requested to be configured.

Host: Specifies the Internet host and port number of the PNM AS, obtained from the original URI
                        given by referring resource.

> **User-Agent:** Contains information about the user agent originating the request and it includes the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.

> **Referer:** Allows the user agent to specify the address (URI) of the resource from which the URI for the PNM AS was obtained.

> **Authorization:** Contains the credentials obtained by means of the bootstrapping procedure (as described in 3GPP TS 33.220 [8]).

> **XML body:** In this example, the UE with public user identity <sip: PN_user1_public1@home1.net> wants the PNM AS to delete the whole PN settings established before.

2. **Authentication/authorization and UE capability and subscription checking**

   See Step 2 described within Figure A.3.3.1-1.

3. **Delivery of PN-configuration response (NAF/PNM AS to PN UE) - see example in table A.3.3.5-3**

   The PNM AS sends HTTP 200 OK response to the PN UE to indicate the success of the PN-configuration.

Table A.3.3.5-3: Delivery of PN-configuration response (NAF/PNM AS to PN UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Content-Length: 0
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Wed, 31 Oct 2007 10:50:36 GMT
Expires: Wed, 31 Nov 2007 10:50:36 GMT
```

> **Authentication-Info:** This carries the protection.

A.3.4 Signalling flows for PN UE redirection

A.3.4.1 PN UE redirection in the IM CN subsystem

Figure A.3.4.1-1 details the signalling flows for PN UE redirection in the IM CN subsystem.

S-CSCF#2	PNM AS	S-CSCF#3

1. INVITE #1 →

← 2. 100 (Trying)

3. Evaluation of Initial Filter Criteria

4. INVITE #1 →

← 5. 100 (Trying)

6. PNM Redirection Session Control

← 7. INVITE #2

8. 100 (Trying) →

9. INVITE #2 →

← 10. 100 (Trying)

← 11. INVITE #2

12. 100 (Trying) →

13. PNM Redirection Session Control

14. INVITE #2 →

← 15. 100 (Trying)

16. INVITE #2 →

← 17. 200 (OK)

← 18. 200 (OK)

19. 200 (OK) →

← 20. 200 (OK)

21. 200 (OK) →

← 22. 200 (OK)

← 23 200 (OK)

24. ACK →

25. ACK →

← 26. ACK

27. ACK →

← 28. ACK

29. ACK →

30. ACK →
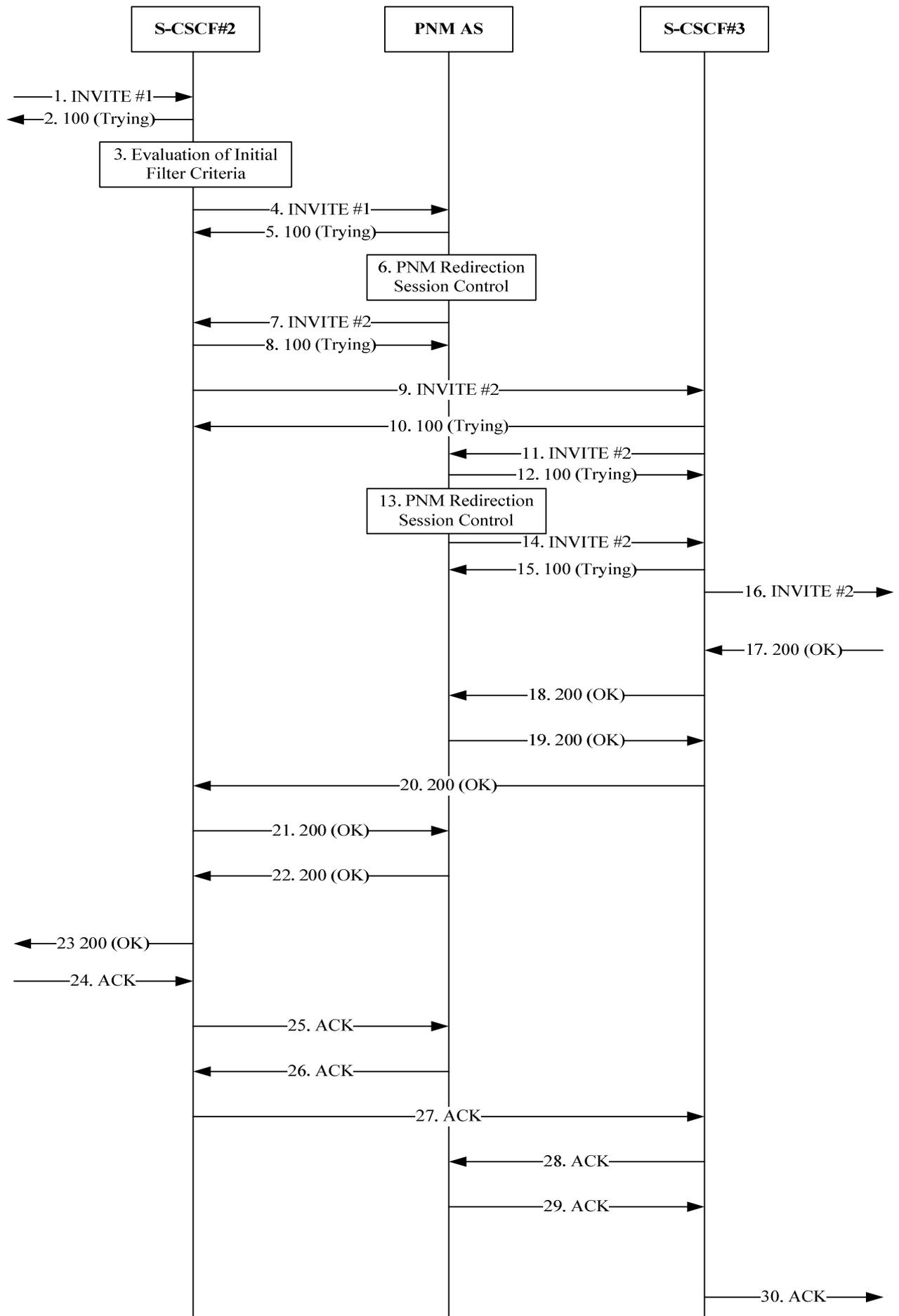
Figure A.3.4.1-1: Successful PN UE redirection: in the IM CN subsystem

The steps prior to Step 1 are according to the standard procedures specified in 3GPP TS 24.228 [10].

1. **INVITE#1 request** (I-CSCF#2 to S-CSCF#2) **–see example in table A.3.4.1-1**

    I-CSCF#2 forwards the INVITE request to S-CSCF#2 after invocation of User Location Query procedure.

Table A.3.4.1-1: INVITE (I-CSCF#2 to S-CSCF#2)

```
INVITE sip: PN_user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>,<sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip: PN_user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Supported: precondition,100rel,gruu,199
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
P-Asserted-Service: urn:urn-xxx:3gpp-service.ims.icsi.mmtel Contact:
<sip:user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6> ;
+g.3gpp.icsi_ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Accept: application/sdp, application/3gpp-ims+xml
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
a=tcap:1 RTP/AVPF
a=pcfg:1 t=1
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

2. **SIP 100 (Trying) response**

3. **Evaluation of initial filter criteria**

    The S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criteria.

4. **INVITE#1 request (S-CSCF#2 to PNM AS)- see example in table A.3.4.1-4**

    Based on the evaluation of initial filter criteria, the S-CSCF#2 forwards the INVITE request with the Request-URI of the UE-1 to the PNM AS.

Table A.3.4.1-4: INVITE (S-CSCF#2 to PNM AS)

```
INVITE sip: PN_user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
```

```
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Route: <sip:pnmas.home2.net;lr>
Record-Route:
:<sip:scscf2.home2.net;lr>,<sip:icscf1.home1.net;lr>,<sip:scscf1.home1.net;lr>,<sip:pcscf1.home.net;
lr>
P-Asserted-Identity:

Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip: PN_user2_public1@home2.net>
Call-ID:
Cseq:
Supported: precondition, 100rel, gruu
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

5. **SIP 100 (Trying) response (PNM AS to S-CSCF#2)**

6. **PN UE redirection control**

   The PNM AS executes the PN UE redirection logic based on the PN-user"s PN configurations and decides to redirect the initial request to the default UE of the PN, e.g. to the UE-3.

7. **INVITE#2 request (PNM AS to S-CSCF#2) - see example in table A.3.**4.1**-7**

   As a result of the PN UE redirection logic execution, the PNM AS sends the redirected INVITE request with the Request-URI of the UE-2 public user identity to the S-CSCF#2.

Table A.3.4.1-7: INVITE#2 (PNM AS to S-CSCF#2)

```
INVITE sip: PN_user3_public1@home2.net
Via: SIP/2.0/UDP pnmas.home2.net; brach= z9hG4bK712z34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 63
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:pnmas.home2.net>, <sip:scscf2.home2.net;lr>, <sip:icscf1.home1.net;lr>,
<sip:scscf1.home1.net;lr>,<sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported: precondition,100rel,gruu,199,histinfo
History-Info: <sip:PN_user2_public1@home2.net>;index=1,
```

```
              <sip:PN_user3_public1@home2.net>;index=1.1
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

8. **SIP 100 (Trying) response (S-CSCF#2 to PNM AS)**

9. **INVITE#2 request (S-CSCF#2 to S-CSCF#3) - see example in table A.3.4.1-9**

   The S-CSCF#2 forwards the redirected INVITE request to the S-CSCF#3. The S-CSCF#2 and S-CSCF#3 can be the same entity.

Table A.3.4.1-9: INVITE#2 (S-CSCF#2 to S-CSCF#3)

```
INVITE sip: PN_user3_public1@home2.net
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP Pnmas.home2.net;brach= z9hG4bK712z34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
SIP/2.0/UDP icscf1.home1.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1@home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 62
Route: <sip:scscf3.home2.net;lr>
Record-Route: <sip:scscf3.home2.net;lr>, <sip:pnmas.home2.net>, <sip:scscf2.home2.net;lr>,
<sip:icscf1.home1.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
History-Info:
Accept-Contact:
P-Asserted-Service:
Supported:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
```

```
a=
a=
a=
a=
a=
a=
a=
a=
```

10. **SIP 100 (Trying) response (S-CSCF#3 to S-CSCF#2)**

The S-CSCF#3 responds to the INVITE#3 request with a 100 Trying provisional response.

11. **INVITE#2 request (S-CSCF#3 to PNM AS) - see example in table A.3.4.1-11**

Based on the evaluation of initial filter criteria, the S-CSCF#3 forwards the INVITE request with the Request-URI of the UE-3 to the PNM AS.

Table A.3.4.1-11: INVITE#2 (S-CSCF#3 to PNM AS)

```
INVITE sip: PN_user3_public1@home2.net
Via: SIP/2.0/UDP scscf3.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP Pnmas.home2.net;brach= z9hG4bK712z34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 61
Route: <sip:pnmas.home2.net;lr>
Record-Route: <sip:scscf3.home2.net;lr>,<sip:scscf2.home2.net;lr>, <sip:pnmas.home2.net>,
<sip:scscf1.home2.net;lr>, <sip:icscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
History-Info:
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

12. **SIP 100 (Trying) response (PNM AS to S-CSCF#3)**

13. **PN UE redirection control**

The PNM AS executes the PN UE redirection control logic based on the PN-user"s PN configurations and decides to forward the request to S-CSCF#3 as the UE-3 is the default UE of the PN.

14. **INVITE#2 request (PNM AS to S-CSCF#3) - see example in table A.3.4.1-14**

Table A.3.4.1-14: INVITE#2 (PNM AS to S-CSCF#3)

```
INVITE sip: PN_user3_public1@home2.net
Via: SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP scscf3.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP Pnmas.home2.net;brach= z9hG4bK712z34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 60
Route: <sip:scscf3.home2.net;lr>
Record-Route: <sip:pnmas.home2.net;lr>,<sip:scscf3.home2.net;lr>,<sip:scscf2.home2.net;lr>,
<sip:pnmas.home2.net>, <sip:scscf2.home2.net;lr>, <sip:icscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1@home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
History-Info:
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

15. **SIP 100 (Trying) response (S-CSCF#3 to PNM AS)**

16. **INVITE#2 request (S-CSCF#3 to P-CSCF-#3) -- see example in table A.3.4.1-16**

The S-CSCF#3 continues the redirected INVITE request based on the standard call setup procedures.

Table A.3.4.1-16: INVITE#2 (S-CSCF#3 to P-CSCF#3)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
Via: SIP/2.0/UDP scscf3.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP scscf3.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK735z12.1,
SIP/2.0/UDP Pnmas.home2.net;brach= z9hG4bK712z34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
```

```
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 59
Route: <sip: pcscf#3@home2.net;lr>
Record-Route: <sip:scscf3.home2.net;lr>,
<sip:pnmas.home2.net;lr>,<sip:scscf3.home2.net;lr>,<sip:scscf2.home2.net;lr>, <sip:pnmas.home2.net>,
<sip:scscf2.home2.net;lr>, <sip:icscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
History-Info:
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
P-Called-Party-ID: <sip:PN_user3_public1@home2.net>
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

17. **Steps 17 to 30 are identical to generic session setup procedure specified in 3GPP TS 24.228 [10].**

A.3.4.2   PN UE redirection in the CS domain

Figure A.3.4.2-1 provides the signaling flow for PN UE redirection in the CS domain. The GMSC will receive the ISUP containing calling party number and called party number. The gsmSCF will invoke the service logic in order to route the call to Default-UE.
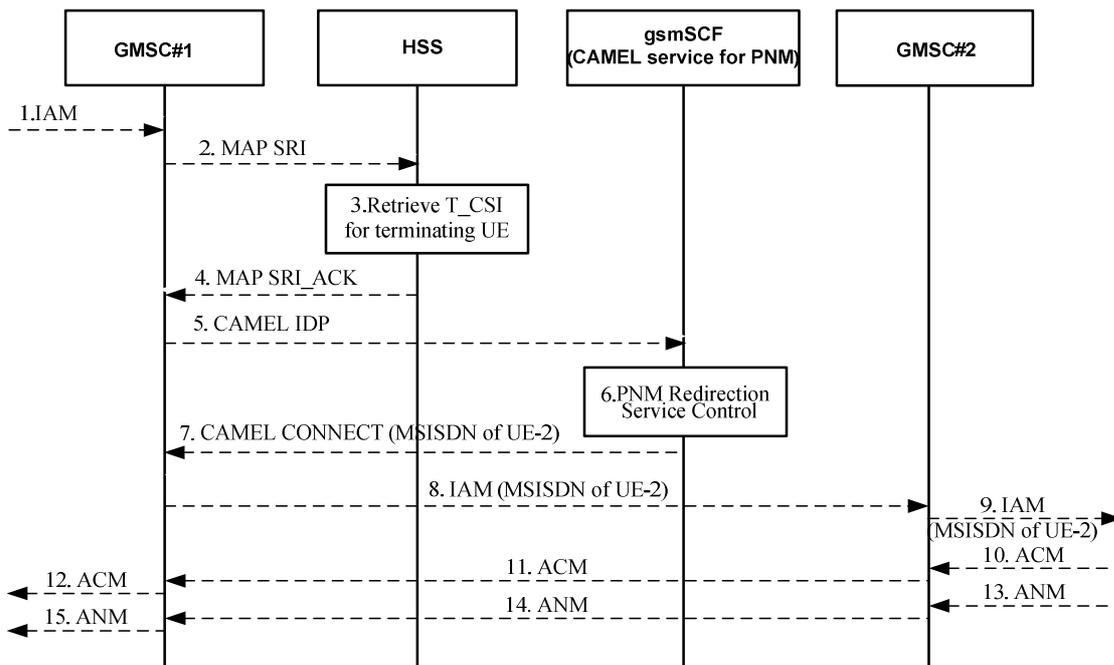
Figure A.3.4.2-1: Signalling flow for PN UE redirection in the CS domain

1. **ISUP IAM**

   IAM message arrived at GMSC#1. Specifically for this signalling flow, the IAM includes:

   Called Party Number parameter = [(Numbering plan identifier = ISDN/telephony numbering plan), (type of number = international number), (Number digits = 12415553333)]

   Calling Party Number parameter = [(Numbering plan identifier = ISDN/telephony numbering plan), (type of number = international number), (Number digits = 12125551111)]

2. **MAP Send Routing Information (SRI) (GMSC#1 to HSS)**

   On receipt of the incoming call request, the GMSC queries the HSS for routing information

3. **Retrieval of PNM subscriber information**

   The HSS provides information including the T-CSI information element that contains information configured for the PNM subscriber, identifying the subscriber as having terminating CAMEL services. The T-CSI IE also includes the gsmSCF address.

4. **MAP Send Routing Information Acknowledgement (SRI ACK) (HSS to GMSC#1)**

   The HSS returns the T-CSI information element to the GMSC in response to the query for routing information (SRI). The GMSC now has the address of the gsmSCF.

5. **CAMEL IDP (GMSC to gsmSCF)**

   The GMSC#1 triggers a CAMEL activity which results in sending a CAMEL IDP message to the GSM Service Control Function (gsmSCF). The CAMEL IDP message contains at least:

   the calling party number;

   the called party number;

   the type of call; and

   Information from the T-CSI IE received by the GMSC#1 in the SRI ACK from the HSS. This includes the CAMEL service key.

6. **The gsmSCF invokes PNM Redirection service logic to route the call.**

7. CAMEL CONNECT (gsmSCF to GMSC#1)

The CAMEL service function causes the gsmSCF to respond to the CAMEL IDP message with a CAMEL CONNECT message containing:

The MSISDN of the Default UE: 12245678912

8. IAM message arrived at GMSC#2 of Default UE.

The IAM includes:

Called Party Number parameter = [(Numbering plan identifier = ISDN/telephony numbering plan), (type of number = international number), (Number digits = 12415553333)]

Calling Party Number parameter = [(Numbering plan identifier = ISDN/telephony numbering plan), (type of number = international number), (Number digits = 12125551111)]

9. ISUP IAM

The call is routed to Default UE.

10-12. ISUP ACM

In response ACM is generated .There is no PNM specific content to this response.

13-15. ISUP ANM

The ANM is generated after terminating UE answer the call. There is no PNM specific content to this response.

A.3.5 Signalling flows for PN access control

A.3.5.1 PN access control procedure in IM CN subsystem

Figure A.3.5.1-1 details the signalling flows for PN access control in the IM CN subsystem.

In the following flow UE#2a is the PN controller UE and UE#2b is the PN controllee UE.
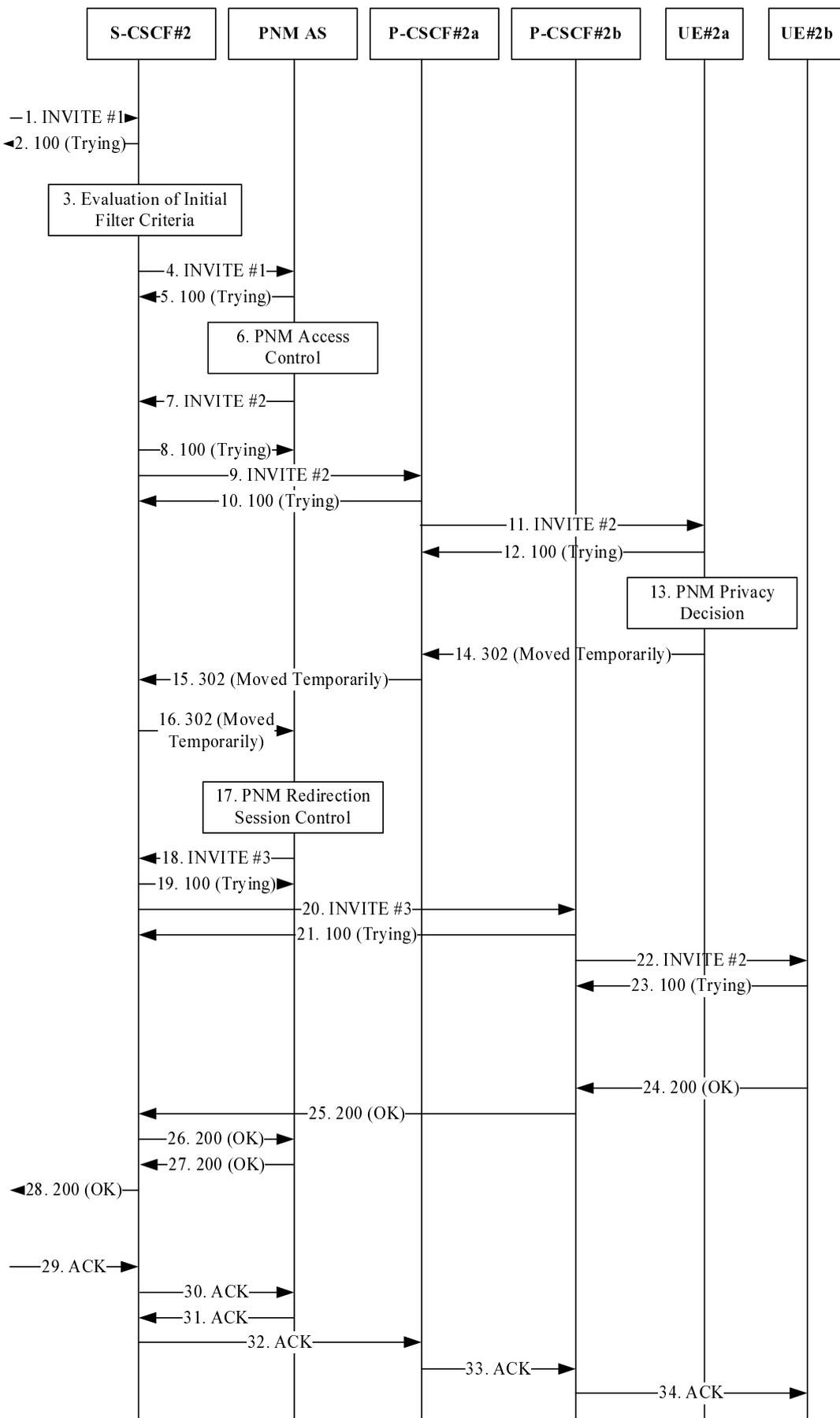
Figure A.3.5.1-1: Signalling flow for PN access control procedure in IM CN subsystem

The steps prior to Step 1 are according to the standard procedures specified in 3GPP TS 24.228 [10].

1. **INVITE#1 (I-CSCF#2 to S-CSCF#2)**

   I-CSCF-2 forwards the invite message to S-CSCF#2 after invocation of location Query.

Table A.3.5.1-1: SIP INVITE request (I-CSCF#2 to S-CSCF#2)

```
INVITE sip:PN_user2b_public1@home2.net
Via:SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf2.home2.net;lr>
Record-Route:<sip:scscf1.home1.net;lr>,<sip:pcscf1.visited.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
Privacy: none
From: <sip:user1_public1@home1.net>;tag=157893
To: <sip:PN_user2b_public1@home2.net>
Cseq: 127 INVITE
Call-ID:131243vdse
Supported: precondition,100rel,gruu,199
Accept-Contact: *;+g.3gpp.icsi_ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
P-Asserted-Service: urn:urn-xxx:3gpp-service.ims.icsi.mmtel
Contact: <sip:user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6;comp=sigcomp>;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Accept: application/sdp, application/3gpp-ims+xml
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
a=tcap:1 RTP/AVPF
a=pcfg:1 t=1
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

2. **100 Trying**

   S-CSCF#2 responds to the INVITE#1 request with a 100 Trying provisional response.

Table A.3.5.1-2: SIP 100 Trying

```
SIP/2.0 100 Trying
Via:SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. **Evaluation of Initial Filter Criteria**

   S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criteria.

4. **INVITE#1(S-CSCF#2 to PNM AS)**

S-CSCF#2 forwards the INVITE#1 request to PNM AS based upon the initial filter criteria (IFCs).

Table A.3.5.1-4: SIP INVITE request (S-CSCF#2 to PNM AS)

```
INVITE sip:PN_user2b_public1@home2.net
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Route: <sip:pnmas.home2.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>,<sip:scscf1.home1.net;lr>,<sip:pcscf1.visited.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

5. **100 Trying**

   PNM AS responds to the INVITE#1 request with a 100 Trying provisional response.

Table A.3.5.1-5: SIP 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. **PN access control**

   PNM AS invokes the Private network service logic. As user1_public1@home1.net is not on the <PNAccessControlList> of PN_user2b_public1@home2.net and that the PN access controller needs to be contacted.

7. **INVITE#2 (PNM AS to S-CSCF#2)**

ETSI

PNM AS generates a new INVITE request message called INVITE#2 and sends it to S-CSCF#1 in order to interact with PN controller UE.

Table A.3.5.1-7: SIP INVITE request (PNM AS to S-CSCF#2)

```
INVITE sip:PN_user2a_public1@home2.net;target=PN_user2b_public1@home2.net
Via: SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bwt871y12.1
Max-Forwards: 70
Route: <sip:scscf2.home2.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
Privacy:
From: <sip:pnmas.home1.net>;tag=r3rw33
To: <sip:PN_user2a_public1@home2.net>
Cseq:
Call-ID:
Supported: precondition, 100rel, 199, histinfo
Contact: <sip:pnmas.home2.net>
History-Info: <sip:PN_user2b_public1@home2.net>;index=1,
<sip:PN_user2a_public1@home2.net;target=PN_ user2b_public1@home2.net>;index=1.1
Accept-Contact:*;+g.3gpp.iari-ref="urn%3Aurn-xxx%3A3gpp-application.ims.iari.pnm-controller"
P-Asserted-Service:
Allow:
Accept:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: contains the URI of the PN controller UE (PN_user2a_public1@home2.net) obtained from the <PNController> element along with the target uri-parameter which contains the URI from the original Request-URI (PN_user2b_public1@home2.net).

P-Asserted-Identity: the identity of the originator ("John Doe" <sip:user1_public1@home1.net>).

From: contains the SIP URI of the PNM AS (sip: pnmas.home1.net).

To: contains the URI of the PN controller UE (PN_user2a_public1@home2.net).

Supported: contains the following option tags: precondition, 100rel, 199, histinfo.

Contact: a SIP URI that contains the IP address or FQDN of the PNM AS.

History-Info: contains the URIs from the original Request-URI (PN_user2b_public1@home2.net) and the URI of the PN controller UE (PN_ user2a_public1@home2.net)

Accept-Contact: contains the g.3gpp.iari-ref media feature tag with the IARI value "urn%3Aurn-xxx%3A3gpp-application.ims.iari.pnm-controller".

8. 100 Trying

S-CSCF#2 responds to the INVITE#2 request with a 100 Trying provisional response.

Table A.3.5.1-8: SIP 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pnmas.home2.net;branch=v7hG4bwt171y12.1
To:
Call-ID:
CSeq:
Content-Length: 0
```

9. **INVITE#2 (S-CSCF#2 to P-CSCF#2a)**

    S-CSCF#2 forwards the INVITE#2 request to P_CSCF#2a.

Table A.3.5.1-9: SIP INVITE request (S-CSCF#2 to P-CSCF#2a)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bwt871y12.1
Max-Forwards: 69
Route: <sip:pcscf2a.visited2.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
Contact:
History-Info:
Accept-Contact:
P-Asserted-Service:
Allow:
Accept:
P-Called-Party-ID: <sip:PN_user2a_public1@home2.net;target=PN_user2b_public1@home2.net>
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

10. **100 Trying**

    P-CSCF#2a responds to the INVITE#2 request with a 100 Trying provisional response.

Table A.3.5.1-10: SIP 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bwt871y12.1
To:
Call-ID:
CSeq:
Content-Length: 0
```

11. **INVITE #2 (P-CSCF#2a to UE-2a)**

P-CSCF#2a sends the INVITE#2 to UE-2a (controller UE)

Table A.3.5.1-11: SIP INVITE request (P-CSCF#2a to UE-2a)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
Via: SIP/2.0/UDP pcscf2a.visited2.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home1.net;branch=k9hG4bwt871y12.1
Max-Forwards: 68
Record-Route: <sip:pcscf2a.visited2.net;lr>,
<sip:scscf2.home2.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Require:
Supported:
Contact:
History-Info:
Accept-Contact:
P-Asserted-Service:
Allow:
Accept:
P-Called-Party-ID:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

12. 100 Trying

UE-2a responds to the INVITE#2 request with a 100 Trying provisional response.

Table A.3.5.1-12: SIP 100 Trying

```
SIP/2.0 100 Trying
Via:SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home2.net;branch=v7hG4bwt171y12.1
To:
Call-ID:
CSeq:
Content-Length: 0
```

13. PNM Privacy Decision

Based upon the IARI value PN controller UE invokes the PN controller application.The PN controller application provides the originators identity from the P-Asserted-Identity header, the PN controllee UE identity from the target URI-parameter in the Request-URI to the user and provides the option to the user to:

1. Forward the session to the controllee UE

2. Reject the session

3. Accept the session

In the example the user determines to forward the sesssion to the controllee UE.

14. 302 Moved Temporarily

PN controllee UE sends a SIP 302 Moved Temporarily response to pcscf2a.visited2.net.

Table A.3.5.1-14: SIP 302 Moved Temporarily

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP pcscf2.visited2.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home2.net;branch=k9hG4bwt871y12.1
From:
To:
Call-ID:
CSeq:
History-Info: <sip:PN_user2b_public1@home2.net>;index=1,
<sip:PN_user2a_public1@home2.net;target=PN_user2b_public1@home2.net>;index=1.1
Contact: <sip:PN_user2b_public1@home2.net>
Content-Length:0
```

Contact: a URI that contains the address of the PN controllee UE (PN_user2b_public1@home2.net).

History-info: contains the URIs from the History-Info header in the original INVITE (PN_user2b_public1@home2.net and PN_user2a_public1@home2.net).

15. 302 Moved Temporarily

P-CSCF#2a forward the 302 Moved Temporarily response to S-CSCF#2.

Table A.3.5.1-15: SIP 302 Moved Temporarily

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP pnmas.home2.net;branch=k9hG4bwt871y12.1
From:
To:
Call-ID:
CSeq:
History-Info:
Contact:
Content-Length:
```

16. 302 Moved Temporarily

S-CSCF#2 forwards the 200 OK to PNM AS.

Table A.3.5.1-16: SIP 302 Moved Temporarily

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pnmas.home2.net;branch=k9hG4bwt871y12.1
From:
To:
Call-ID:
CSeq:
History-Info:
Contact:
Content-Length:
```

17. PN UE redirection

Upon receiving the 302 Moved Temporarily response from the controller UE, the PNM AS determines the session is to be redirected to the controllee UE.

18. INVITE#3 (PNM AS to S-CSCF#2)

PNM AS forwards the Originating INVITE message to S-CSCF#2.

Table A.3.5.1-18: SIP INVITE request (PNM AS to S-CSCF#2)

```
INVITE sip:PN_user2b_public1@home2.net
Via:SIP/2.0/UDP pnmas.home2.net;branch=z9hG4bwt871y12.1
SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 63
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>,<sip:scscf1.home1.net;lr>,<sip:pcscf1.visited.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
Privacy:
From: <sip:user1_public1@home1.net>;tag=157893
To: <sip: PN_user2_public1@home2.net>
Cseq:
Call-ID:
Supported: precondition, 100rel, 199, histinfo
Contact: <sip:user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6;comp=sigcomp>;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
History-Info: <sip:PN_user2b_public1@home2.net>;index=1,
<sip:PN_user2a_public1@home2.net;target=PN_user2b_public1@home2.net>;index=1.1,
<sip:PN_user2b_public1@home2.net?Reason=SIP;cause=302>;index=1.2
Accept-Contact: *;g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
P-Asserted-Service:
Allow:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: contains the URI of the PN controller UE (PN_user2a_public1@home2.net) obtained from the <PNController> element along with the target uri-parameter which contains the URI from the original Request-URI (PN_user2b_public1@home2.net).

P-Asserted-Identity: the identity of the originator ("John Doe" <sip: user1_public1@home1.net>).

From: contains the SIP URI of the PNM AS (sip: pnmas.home1.net).

To: contains the URI of the PN controller UE (PN_user2a_public1@home2.net).

Supported: contains the following option tags: precondition, 100rel, 199, histinfo

Contact: the contents of the Contact header in the original INVITE (<sip: user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>).

History-info: contains the URIs from the History-Info header in the 302 Moved Temporarily response (PN_user2b_public1@home2.net and PN_user2a_public1@home2.net) with the addition of the URI of the PN controllee UE (PN_user2b_public1@home2.net) from the Contact header in the 302 Moved Temporarily response along with the reason code 302

> **Accept-Contact:** contains the g.3gpp.icsi-ref media feature tag with the ICSI value from the Accept-Contact header in the original INVITE ("urn%3Aurn-xxx%3A3gpp-service.ims.icsi.mmtel")

19-34. These flows follow the standard session establishment procedures specified in 3GPP TS 24.228 [10].

A.3.5.2   PN access control procedure in CS domain.

Figure A.3.5.2-1 provides the signalling flows for the PN access control procedure in CS domain. PN access control services deal with a user having access control over its personal network.
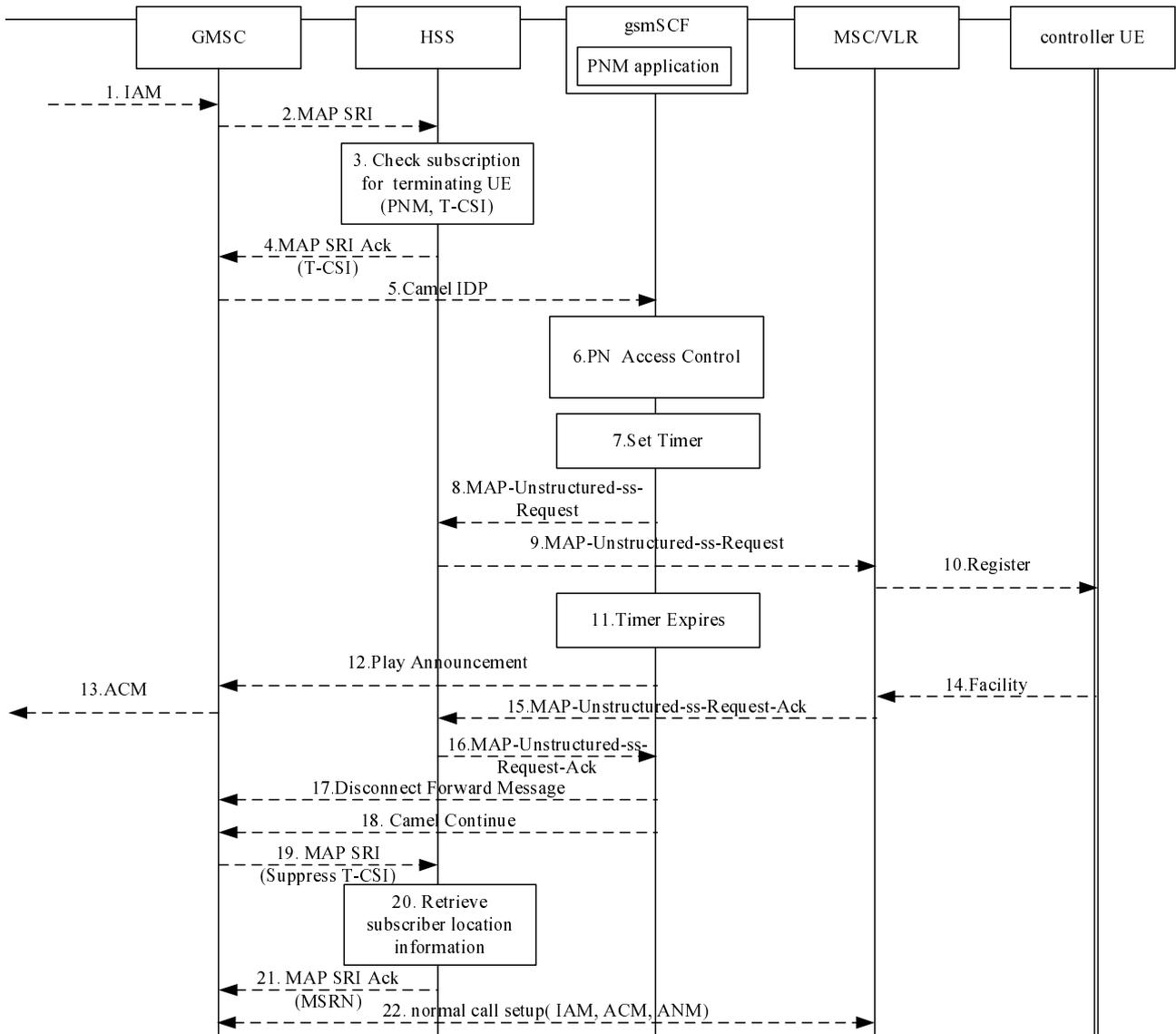
**Figure A.3.5.2-1 Signalling flow for PN access control in the CS domain**

1. **ISUP IAM**

    Call Request containing an IAM message arrived at the GMSC.

    Specifically for this signalling flow, the IAM includes:

    - Calling Party number =12134587692

    - Called Party Number parameter = [(Numbering plan identifier = ISDN/telephony numbering plan), (type of number = international number), (Number digits = 15346789043)]

2. MAP Send Routing Information (SRI)

On receipt of the incoming call request, the GMSC queries the HSS for routing information.

3. Retrieval of PNM subscriber information

The HSS identifies the subscriber as a PNM subscriber and provides the configured terminated CAMEL subscription information (T-CSI) towards the GMSC in the SRI-ACK.

4. MAP Send Routing Information Acknowledgement (SRI ACK)

The HSS returns the T-CSI information element which includes the gsmSCF address to the GMSC in response to the query for routing information (SRI).

5. CAMEL IDP (GMSC to gsmSCF)

The GMSC#1 triggers a CAMEL activity which results in sending a CAMEL IDP message to the GSM Service Control Function (gsmSCF). The CAMEL IDP message contains at least:

- the calling party number;

- the called party number;

- the type of call; and

- information from the T-CSI IE received by the GMSC#1 in the SRI ACK from the HSS. This includes the CAMEL service key.

6. PN access control

The gsmSCF performs the PN access control. Since the calling party is not configured in the PN access control list, the gsmSCF needs to ask the controller UE to grant the access to the calling party.

7-8. MAP-UNSTRUCTURED-SS-REQUEST (gsmSCF to HSS)

As part of this process the gsmSCF starts the timer to supervise the call establishment and send a MAP-UNSTRUCTURED-SS-REQUEST message to the HSS. The message contains the following information.

   USSD String:- Calling Number 12134587692 and called Number 15346789043.

9. MAP-UNSTRUCTURED-SS-REQUEST (HSS to MSC/VLR)

The HSS relays the USSD request message to the MSC/VLR. It contains the following information.

   USSD String:- Calling Number 12134587692 and called Number 15346789043.

10. REGISTER (MSC/VLR to controller UE)

This message is used between MSC/VLR and the UE to get the access granted for the incoming call. It contains the following information.

Facility (Invoke=UNSTRUCTURED-SS-REQUEST(USSD-Data-Coding-Scheme, USSD String))

11-13. When the timer expires, the gsmSCF generates play announcement message containing Tone ID and Duration parameters as specified in 3GPP TS 29.078 [13].

14. FACILITY (controller UE to MSC/VLR)

The controller UE will send the FACILITY message back to the MSC/VLR. It contains the following information.

Facility (ReturnResult=UNSTRUCTURED-SS-REQUEST (USSD-Data-Coding-Scheme, USSD String)) which inform that call is accepted.

15-16. MAP-UNSTRUCTURED-SS-REQUEST-Ack (MSC/VLR to HSS)

After receiving the FACILITY message from the controller UE, the MSC/VLR send an USSD message towards the gsmSCF via the HSS. It contains the following information.

Facility (ReturnResult=UNSTRUCTURED-SS-REQUEST(USSD-Data-Coding-Scheme, USSD String))

17. As user responds, the gsmSCF stops playing announcement by sending DisconnectForwardConnection message to GMSC.

NOTE: If the user responds before the timer started in step 7 expires, steps 12, 13 & 17 are skipped.

18. **Call Continue/Release Call (HSS to GMSC)**

Based on the response of the controller UE the gsmSCF sends a CAMEL CONTINUE or CAMEL RELEASE message to the GMSC.

19-20. **MAP Send Routing Information (SRI)**

On receipt of call continue message, the GMSC queries again the HSS for the routing information for the called party but this time with the parameter Suppress T-CSI.

21. **MAP SRI Ack**

The HSS executes the roaming number enquiry procedure and sends this information back to the GMSC within the SRI-Ack containing MSRN=15346787943.

22. **Call setup**

The GMSC starts the normal call setup towards the visited MSC of the called party to establish the call.

A.3.6 Signalling flows for interdomain networking

A.3.6.1 IM CN subsystem to CS domain

Figure A.3.6-1 details the signaling flows for inter-domain networking from IM CN to CS domain.
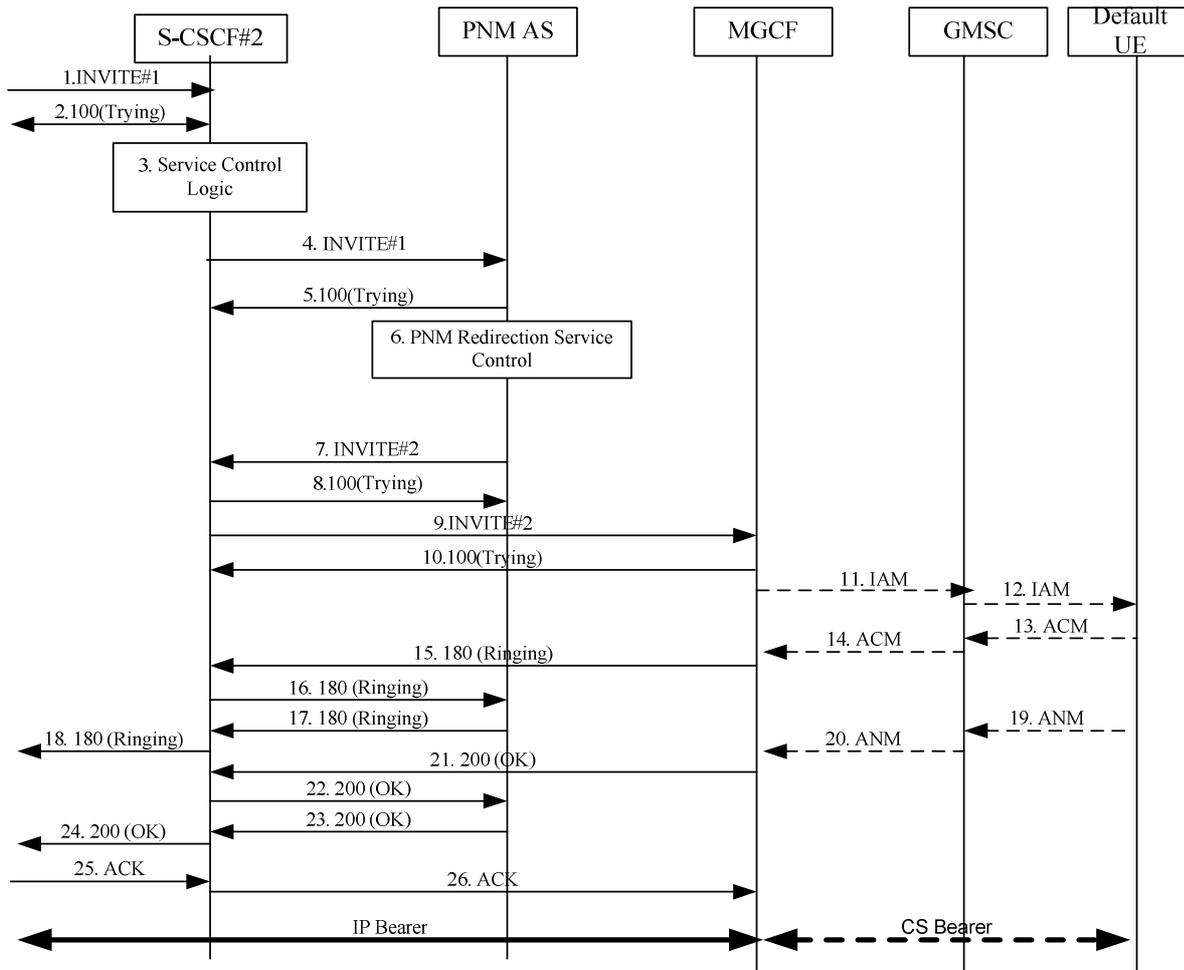
Figure A.3.6-1: interdomain networking: (IM CN-CS)

1. **INVITE request** (I-CSCF#2 to S-CSCF#2)

   UE initiates the INVITE request with the request-URI of the UE-1 to the IM CN subsystem entities.

   There is no PNM specific content to this request.

Table A.3.6-1-1: INVITE request (I-CSCF#2 to S-CSCF#2)

```
INVITE sip: PN_user2_public1@home2.net SIP/2.0
Via:SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf2.home2.net;lr>
Record-Route:<sip:scscf1.home1.net;lr>,<sip:pcscf1.visited.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
Privacy: none
From: <sip:user1_public1@home1.net>;tag=157893
To: <sip:PN_user2_public1@home2.net>
Cseq: 127 INVITE
Call-ID:131243vdse
Supported: precondition,100rel,gruu,199
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
P-Asserted-Service: urn:urn-xxx:3gpp-service.ims.icsi.mmtel
Contact: <sip:user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6;comp=sigcomp>;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Accept: application/sdp, application/3gpp-ims+xml
```

```
Content-Type: application/sdp
Content-length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
a=tcap:1 RTP/AVPF
a=pcfg:1 t=1
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

2. **SIP 100 (Trying) response**

   S-CSCF#2 responds to the INVITE#1 request with a 100 Trying provisional response.

3. **Evaluation of initial filter criteria**

   S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criteria.

4. **INVITE#1 request (S-CSCF#2 to PNM AS)**

   S-CSCF#2 forwards the INVITE#1 request to PNM AS based upon the initial filter criteria (IFCs).

Table A.3.6-1-4: INVITE request (S-CSCF#2 to PNM AS)

```
INVITE sip:PN_user2_public1@home2.net SIP/2.0Via: SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bwt871y12.1,
SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK871y12.1,
SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Route: <sip:pnmas.home2.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>,<sip:scscf1.home1.net;lr>,<sip:pcscf1.visited.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Cseq:
Call-ID:
Supported:
Accept-Contact:
P-Asserted-Service:
Contact:
Allow:
Content-Type:
Content-length: (…)

v=
o=
s=
c=
t=
m=
m=
a=
a=
b=
a=
a=
a=
a=
a=
a=
```

```
a=
a=
```

5. **SIP 100 (Trying) response (PNM AS to S-CSCF#2)**

   The PNM AS responds to the INVITE#1 request with a 100 Trying provisional response.

   There is no PNM specific content to this response.

6. **PNM session redirection service control**

   The PNM AS executes the PNM redirection service control logic in order to route the call to the default UE located in CS domain.

   In this example the MSISDN of the called party is +1237654799942

7. **Steps 7 to 26 are identical to generic session setup procedure specified in 3GPP TS 24.228 [10].**

A.3.6.2 CS domain to IM CN subsystem

Figure A.3.6-2 shows the signaling flows for inter-domain networking from CS to IM CN subsystem.
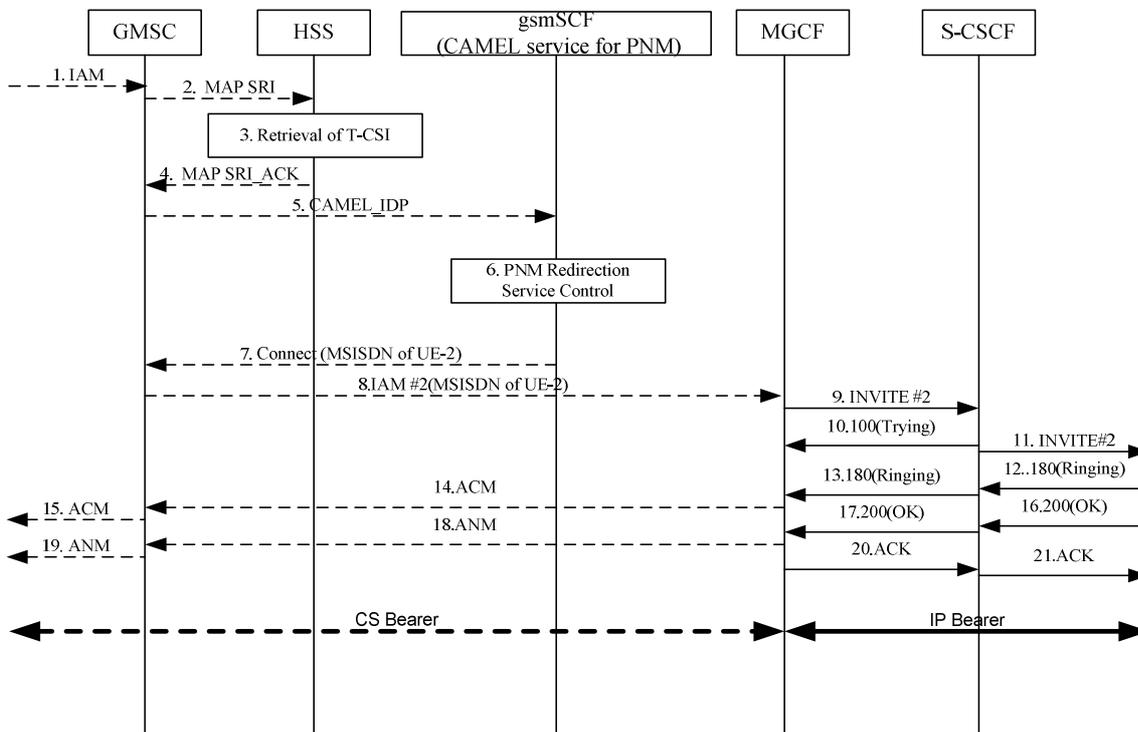
Figure A.3.6-2: Inter-domain networking: (CS-IM CN)

1. **ISUP IAM (coming from the originating PLMN through the CS domain)**

   In this example, a call request (ISUP IAM) makes an entry from the PLMN of the originating user (calling party) into the home PLMN of the terminating user (called party). The first entry point of the PLMN of the terminating user is the Gateway MSC (GMSC). The call request is a form of an ISUP IAM (Initial Address Message) and contains the called party number (MSISDN).

   In this example the MSISDN of the called party is +12134567897

2. **MAP Send Routing Information (SRI) (GMSC to HSS)**

On receipt of incoming call request, GMSC queries the HSS for routing information.

3. **Retrieval of PNM subscriber information**

The HSS provides information including the T-CSI information element that contains information configured for the PNM subscriber, identifying the subscriber as having terminating CAMEL services. The T-CSI IE also includes the gsmSCF address.

4. **MAP send routing information acknowledgement (SRI ACK) (HSS to GMSC)**

The HSS returns the T-CSI information element to the GMSC in response to the query for routing information (SRI). The GMSC now has the address of the gsmSCF.

5. **CAMEL IDP (GMSC to gsmSCF)**

The GMSC triggers a CAMEL activity which results in sending a CAMEL IDP message to the GSM service control function (gsmSCF). The CAMEL IDP message contains at least:

- the calling party number;

- the called party number;

- the type of call; and

- information from the T-CSI IE received by the GMSC in the SRI ACK from the HSS. This includes the CAMEL service key.

6. **Reroute to IMS determination**

The gsmSCF invokes PNM redirection service logic to determine whether the call needs to be rerouted to default UE located in IM CN subsystem for UE redirection.

7. **CAMEL CONNECT (gsmSCF to GMSC)**

The CAMEL service function causes the gsmSCF to respond to the CAMEL IDP message with a CAMEL CONNECT message containing

MSISDN of default UE: 12134567897

8. **IAM#2(GMSC to MGCF)**

GMSC will generate the IAM#2 containing the MSISDN of default UE at which the call is to be redirected and signals to the MGCF.

MSISDN of default UE: 12134567897

9. **SIP INVITE (MGCF to S-CSCF)**

The MGCF interworks the IAM into the appropriate SIP message and initiates the SIP INVITE request towards the S-CSCF via the intermediate IM CN subsystem entities.

(MGCF towards the S-CSCF through the intermediate IM CN subsystem entities) – see example in table A.3.Y1

Table A.3.6-2-9: SIP INVITE request (MGCF to S-CSCF)

```
INVITE tel: + 12134567897 SIP/2.0
Via: SIP/2.0/UDP mgcf.home1.net;branch=z9hG4bK779s24.0
Max-Forwards: 69
Route: <sip:icscf1.home1.net;lr>
P-Asserted-Identity: <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <tel:+1-212-555-1111>;tag=171828
To: <tel:+ 12134567897>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Supported: precondition, 100rel
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
P-Asserted-Service: urn:urn-xxx:3gpp-service.ims.icsi.mmtel
```

```
Contact: <sip:mgcf1.home1.net>;+g.3gpp.icsi-ref="urn%3Aurn-xxx%3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
a=tcap:1 RTP/AVPF
a=pcfg:1 t=1
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

10. **SIP 100 (Trying) response (S-CSCF to MGCF via intermediate IM CN subsystem entities)**

The S-CSCF responds to the intermediate IM CN subsystem entities with a SIP 100 (Trying) response.

11. **INVITE** – S-CSCF forwards the INVITE request to the default UE.

12. **Steps 12 to 21 are identical to generic session setup procedure specified in 3GPP TS 24.228 [10].**

A.4 Example XML document

A.4.1 Introduction

Table A.4.1-1 shows an example of an XML document compliant to the XML schema defined in Annex B. All line feeds within element contents are for display purposes only.

Table A.4.1-1: Example XML document

```
<?xml version="1.0" encoding="utf-8"?>
    <PNConfiguration xxmlns="uri:3gpp:pnm" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <UERedirection UriOfRedirectedUser="sip:PN_user1_public1@home1.com">
            <RedirectedUserID>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_1</PNUEName>
            </RedirectedUserID>
            <RedirectingUserID id=1>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_2</PNUEID>
                <RedirectionLevel>application</RedirectionLevel>
                <RedirectionPrio>1</RedirectionPrio>
            </RedirectingUserID>
            <RedirectingUserID id=2>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_3</PNUEName>
                <RedirectionLevel>application</RedirectionLevel>
                <RedirectionPrio>2</RedirectionPrio>
            </RedirectingUserID>
        </UERedirection>
        <AccessControl UriOfControllerUE="sip:PN_user1_public1@home1.com">
            <ControllerUE>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_1</PNUEID>
            </ControllerUE>
            <ControlleeUE id=1>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_2</PNUEName>
```

```
                <PNAccessControlList>sip:user2_public1@home1.com sip: user3_public1@home1.com
sip:user4_public1@home1.com </PNAccessControlList>
                <PNAccessControlType>Controller</PNAccessControlType>
          </ControlleeUE>
          <ControlleeUE id=2>
                <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
                <PNUEName>PN_3</PNUEName>
                <PNAccessControlList>sip:user5_public1@home1.com</PNAccessControlList>
                <PNAccessControlType>NonController</PNAccessControlType>
          </ControlleeUE>
     </AccessControl>
     <NameofPNUE>
          <PNUEID>sip:PN_user1_public1@home1.com</PNUEID>
          <UEName id=1>
                <Name>PN_1</Name>
          </UEName>
          <UEName id=2>
                <Name>PN_2</Name>
          </UEName>
          <UEName id=3>
                <Name>PN_3</Name>
          </UEName>
     </NameofPNUE>
  </PNConfiguration>
```

Annex B (normative):
PNM XML schema definition

B.1 XML elements structure

Table B.1-1 below shows the XML elements structure hierarchically.

Table B.1-1: XML elements structure

```
PNConfiguration:
   UERedirection:
         RedirectedUserID
             PNUEID
             PNUEName
         RedirectingUserID id=1
             PNUEID
             PNUEName
             RedirectionLevel
             RedirectionPrio
             :
         RedirectingUserID id=Q
             PNUEID
             PNUEName
             RedirectionLevel
             RedirectionPrio
   AccessControl:
         ControllerUE
             PNUEID
             PNUEName
         ControlleeUE id=1
             PNUEID #1
             PNUEName #1

             :
             PNUEID #N
             PNUEName #N
             PNAccessControlList
             PNAccessControlType
         :
         ControlleeUE id=M
             PNUEID #1
             PNUEName #1

             :
             PNUEID #P
             PNUEName #P
             PNAccessControlList
             PNAccessControlType
   NameofPNUE
         PNUEID (Shared IMPU)
         UEName id=1
             Name
         :
         UEName id=R
             Name
```

B.2 XML schema for PNM

Table B.**2**-1 contains the XML schema definition for an XML document for the PN configuration and query over the Ut interface.

Table B.2-1: XML schema for PNM

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="uri:3gpp:pnm"
    xmlns="uri:3gpp:pnm"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

    <!-- This import brings in the XML language attribute xml:lang-->
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>

    <!-- The PNConfiguration element -->
    <xs:element name="PNConfiguration" type="pnConfRequest"/>
    <xs:element name="PNUEID" type="xs:anyURI"/>
    <xs:element name="PNUEName" type="xs:string"/>

    <!-- The whole PNM PN-configuration specific data set  -->
    <xs:complexType name="pnConfRequest">
        <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <xs:choice>
                <xs:element name="UERedirection" type="UERedirectionType"/>
                <xs:element name="AccessControl" type="AccessControlType"/>
                <xs:element name="NameofPNUE" type="PNUENameType"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:choice>
        </xs:sequence>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

        <xs:anyAttribute namespace="##other" processContents="lax">
    </xs:complexType>

    <!-- The UERedirection data set  -->
    <xs:complexType name="UERedirectionType">
        <xs:sequence>
            <xs:element name="RedirectedUserID" maxOccurs="1">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element ref="pnm:PNUEID"/>
                        <xs:element ref="pnm:PNUEName"/>
                        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:complexType>
                <xs:anyAttribute namespace="##other" processContents="lax">
            </xs:element>
            <xs:element name="RedirectingUserID" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element ref="pnm:PNUEID"/>
                        <xs:element ref="pnm:PNUEName"/>
                        <xs:element name="RedirectionLevel" type="RedirectionLevelType"
minOccurs="0"/>
                        <xs:element name="RedirectionPrio" type="positiveInteger" minOccurs="0"/>
                        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:attribute name="id" type="xs:positiveInteger" use="required"/>
                    <xs:anyAttribute namespace="##other" processContents="lax">
                </xs:complexType>
            </xs:element>
        </xs:sequence>
        <xs:attribute name="UriOfRedirectedUser" type="xs:anyURI" use="required"/>
        <xs:anyAttribute namespace="##other" processContents="lax">
    </xs:complexType>

    <!-- The AccessControl data set  -->
    <xs:complexType name="AccessControlType">
        <xs:sequence>
            <xs:element name="ControllerUE" maxOccurs="1">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element ref="pnm:PNUEID"/>
```

```
                            <xs:element ref="pnm:PNUEName"/>
                            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:anyAttribute namespace="##other" processContents="lax"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="ControlleeUE" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence minOccurs="0" maxOccurs="unbounded">
                        <xs:element ref="pnm:PNUEID"/>
                        <xs:element ref="pnm:PNUEName"/>
                        <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:element name="PNAccessControlList" type="ACListType" minOccurs="0"/>
                    <xs:element name="PNAccessControlType" type="ACType" minOccurs="0"/>
                    <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                    <xs:attribute name="id" type="xs:positiveInteger" use="required"/>
                    <xs:anyAttribute namespace="##other" processContents="lax"/>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
        <xs:attribute name="UriOfControllerUE" type="xs:anyUIR" use="required"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <!-- The PNUEName data set  -->
    <xs:complexType name="PNUENameType">
        <xs:element ref="pnm:PNUEID" maxOccurs="1"/>
        <xs:sequence maxOccurs="unbounded">
            <xs:element name="UEName" type="UENameType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="UENameType">
        <xs:sequence maxOccurs="unbounded">
            <xs:element name="Name" type="xs:string"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        <xs:attribute name="id" type="xs:positiveInteger" use="required"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <!-- The Simple Types -->
    <xs:simpleType name="RedirectionLevelType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="application"/>
            <xs:enumeration value="component"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="RedirectionPrioType">
        <xs:restriction base="xs:positiveInteger">
            <xs:enumeration value="1"/>
            <xs:enumeration value="2"/>
            <xs:enumeration value="3"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="ACListType">
        <xs:list itemType="xs:string"/>
    </xs:simpleType>

    <xs:simpleType name="ACType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Controller"/>
            <xs:enumeration value="NonController"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

NOTE 1: The <xs:any> and <xs:anyAttribute> elements within the complex types allow for compatible standard extensions in future releases.

NOTE 2: This document supports three values of the priority for the <RedirectionPrioType> element (High, medium and low).

Annex C (normative):
Definitions of the PNM XCAP application usage

XCAP requires application usage to fulfil a number of steps in the definition of such application usage. The reminder of this annex specifies the required definitions of the PNM XCAP application usage.

Application Unique ID (AUID): Each XCAP application usage is associated with a unique name called the Application Unique ID (AUID). The AUID defined by the PNM application usage falls into the vendor-proprietary namespace of XCAP AUID, where 3GPP is considered a vendor.

The AUID allocated to the PNM XCAP application usage is:

```
pnm.3gpp.org
```

Default namespace: XCAP requires application usages to declare the default namespace. The default namespace of the PNM XCAP application usage is:

```
http://uri.3gpp.org/params/xml/pnm/xcap
```
MIME type: The MIME type of PNM XML documents is:

```
application/pnm+xml
```

Naming conventions: By default, PNM XML document is stored under the user's Home Directory (which is located under the "users" sub-tree). In order to facilitate the manipulation of a PNM XML document, the present document defines a default XML file name:

```
pnm.xml
```
XCAP root URI: The XCAP root defines all contexts in which all XCAP resources defined by the operator (e.g., an operator with a domain name of example.com) exist and the corresponding XCAP root URI is:

```
xcap.example.com
```

XCAP User Identify (XUI): Each user known to the XACP server is associated with a user name, called XCAP User Identify (XUI), which is pre-configured at the PN UE. The XUI for PNM can be the shared public user identity used of the PN user.

Annex D (informative): Change history

					Change history		
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2007-08					Skeleton of the TS (C1-072012)	-	0.0.0
2007-08					Version 0.1.0 created as a result of incorporating the following contributions at CT1#48. C1-071648 - PNM Stage 3 - Annex B PNM XML Scheme Definition C1-072094 – PNM stage 3 Clause 4 Overview C1-072095 – PNM stage 3 Clause 5 Roles for PN-registration C1-072096 – PNM stage 3 Clause 10 Protocol at the Ut reference point	0.0.0	0.1.0
2007-10					C1-072607 - TS 24.259 Annex A.2 C1-072608 - Signalling Flow for PN-registration in the IM CN subsystem C1-072610 - TS24.259-010-cleanup C1-072615 - Signalling flow for Access Control Proc. in CS Domain C1-072616 - Signalling flow for session redirection in CS domain C1-072695 - A.3.1 -- Signal flow for PN-configuration for PN UE redirection C1-072696 - A.3.2 -- Signal flow for PN-configuration for PN access control C1-072697 - A.3.3 -- Signal flow for PN-query C1-072698 - A.3.4 -- Signal flow for PN-deconfiguration C1-072721 - Signalling Flow for PNM Session Redirection in the IM CN subsystem	0.1.0	0.2.0
2007-11					C1-072782 XML update C1-072783 Annex 3.1 C1-073093 TS 24.259 CS domain Annex A.3.8 and A.3.9 C1-073095 Roles for PN UE redirection C1-073224 Roles for PN-Registration C1-073225 CS Network capabilities	0.2.0	0.3.0
2008-02					C1-080193 PN Stage 3 Flows Cleanup C1-080238 Roles for PN-configuration and PN-query C1-080239 Signalling flow for PN UE Name changing C1-080240 signalling flow cleanup C1-080468 Signalling Flow for PN Access Control in IM CN Subsystem C1-080469 Signalling flow for interdomain networking C1-080471 PN UE role in Access Control C1-080656 gsmSCF Capability in PN UE redirection C1-080659 PN Access Control in IM CN Subsystem	0.3.0	0.4.0
2008-04					C1-081017 PN UE Name signalling flow update C1-081299 PNM Scope in CS Domain C1-081350 Solution for the call delay problem in PN access control procedure C1-081351 The roles of gsmSCF for PN-registration C1-081435 Error procedures in the Roles for PN UE redirection	0.4.0	0.5.0
2008-05					C1-081959 PNM Editorial Corrections C1-081960 Addressing Editors Notes regarding PN Access Control C1-081961 Cleanup of PN UE Redirection C1-081962 PN UE redirection in CS domain	0.5.0	0.6.0
2008-05					Email review / airi changed to iari in clause 10.2 and 10.3	0.6.0	0.6.1
2008-05					Email review / updating change history	0.6.1	0.6.2
2008-05					Editorial corrections done by MCC	0.6.2	1.0.0
2008-06					C1-082467 Correction of PN access control procedure	1.0.0	1.1.0

					C1-082468 Some cleanup of PNM Signaling flows C1-082637 XML schema update in TS 24.259 C1-082638 XCAP usage for PN configuration in TS 24.259		
2008-08					C1-083482 Cleanup of Signalling flows for PN-registration	1.1.0	1.2.0
2008-10					C1-084036 TS 24.259 clean-up C1-084401 Interaction with supplementary services C1-084403 PN-Configuration flow update C1-084406 Conveying PN UE information using 3rd party Registration C1-084445 Cleanup of PNM flows	1.2.0	1.3.0
2008-11					C1-084771 24.259 clean-up C1-085263 PNM Flow Cleanup C1-085482 PNM Closed User Group functionality	1.3.0	1.4.0
2008-11					Version 2.0.0 created for presentation to CT#42 for approval	1.4.0	2.0.0
2008-12	CT#42				Version 8.0.0 created after approval in CT#42	2.0.0	8.0.0

History

Document history		
V8.0.0	January 2009	Publication