ETSI TS 123 259 V9.2.0 (2010-01)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Personal Network Management (PNM);
Procedures and information flows
(3GPP TS 23.259 version 9.2.0 Release 9)

Reference
RTS/TSGC-0123259v920

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

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

The present document provides the procedure details and the information flows for support of Personal Network Management including the PN UE redirection and PN access control applications enabled by Personal Network Management (PNM).

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 TS 22.259: "Service requirements for Personal Network Management (PNM)".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[4] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[5] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[6] 3GPP TS 22.002: "Bearer Services Supported by a Public Land Mobile Network (PLMN)".

[7] 3GPP TS 22.003: "Circuit Teleservices Supported by a Public Land Mobile Network (PLMN)".

[8] 3GPP TS 23.078: "Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; Stage 2".

[9] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[10] 3GPP TS 23.018: "Basic Call Handling; Technical realization".

[11] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[12] 3GPP TS 23.090: "Unstructured Supplementary Service Data (USSD); Stage 2".

[13] 3GPP TS 22.085: "Closed User Group (CUG) Supplementary Services; Stage 1".

[14] 3GPP TS 23.085: "Closed User Group (CUG) supplementary service; Stage 2".

3 Definitions and Abbreviations.

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.259 [1] subclauses 3.1 and 4.2.1 apply:

Personal Area Network (PAN)

Personal Network (PN)
Personal Network Element (PNE)
PN UE redirection
PN access control
PN-user
PNE redirection
default UE

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] apply:

Application Server (AS)
For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [3] subclause 3.1 apply:

Initial filter criteria
Initial Request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [4] subclause 3.1 apply:

Public user identity
Private user identity
Proxy-CSCF (P-CSCF)
Serving-CSCF (S-CSCF)

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [5] apply:

User Equipment (UE)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.085 [13] apply:

Incoming Access (IA)
Outgoing Access (OA)

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

PN UE name: A name selected by a PN-user for a PN UE of the PN-user's PN and recorded together with other subscription data like the public/private user identity/identities by the operator in the HSS and the PNM AS by means of provisioning. A PN UE name (e.g., "MeinSchatz") for a PN UE is unique within the PN-user"s PN.

3.2 Abbreviations

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

CUG	Closed User Group
PAN	Personal Area Network
PN	Personal Network
PNE	Personal Network Element
PNM	Personal Network Management

4 PNM overview

4.1 General

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 PN-user, as described in 3GPP TS 22.259 [1]. These home network-based management functions cover the configuration of the PN-user"s PN such as PN-registration, PN-deregistration, PN-configuration, PN-deconfiguration and PN-query procedures, and the operation of the PN-user's PN. Functionality enabled by the PNM comprises the PN UE redirection and the PN access

control applications as described in 3GPP TS 22.259 [1]. In order to provide the PN UE redirection and the PN access control applications, the PNM is realized as an AS in the IM CN subsystem as described in 3GPP TS 23.002 [2] and as a CAMEL service in the CS domain as described in 3GPP TS 23.078 [4].

4.2 PN access control concepts

The PN access control is one of the PNM applications specified in 3GPP TS 22.259 [1] that enables PN-users to exercise access control to restrict accesses to certain UE(s) of their PNs. 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 [13] and 3GPP TS 23.085 [14], 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 perform such PN access control the PN-users need to configure a PN access control list for each UE of the PN. The configuration can be done either in a static or a dynamic way. Besides other additional information, the PN access control list of a UE within a PN contains all identities (e.g., a SIP URI) which are permitted to be used to initiate sessions to that UE. In this document, the UE of a PN that is used by the PN-user to exercise access control is referred to controller UE, whereas the UE of the PN, over which an access control is enabled, is referred to controllee UE. The controller UE of a PN-user"s PN is assigned by provisioning and the controller UE can configure any UE of the PN as controllee UE. The PN access control list of the controllee UE is only configurable by the controller UE.

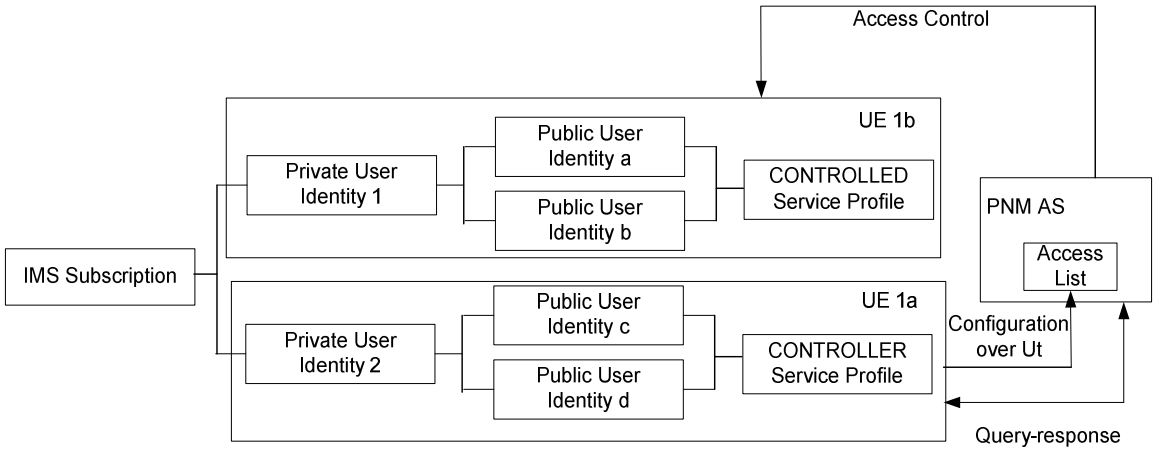

Figure 4.2-1: Relationship of various service profiles in PN access control

An example of the service profiles configuration for PN access control is shown in the above figure 4.2-1. The arrows indicate the direction of control. Some of the aspects involved are:

- A PN-user's PN consists of two UEs, i.e., UE 1a and UE 1b, where UE 1b is the controllee UE and UE 1a is the controller UE.
- The service profile of UE 1b is referred to as the controllee UE Service Profile.
- The service profile of UE 1a is referred to as the controller UE Service Profile.
- The assignment of controller UE service profile is done during provisioning.
- Access control of UE 1b by UE 1a is performed with the help of a SIP Application Server (AS), referred to as PNM AS.
- From UE 1a, the PN-user configures a PN access control list that contains details of PN access control regarding UE 1b's service profile. This configuration is done over the Ut interface. For example: this PN access control list can contain a list of UE identities that are allowed to initiate sessions with UE 1b.
- The PNM AS executes the actual PN access control procedures.
- The PNM AS performs PN access control by utilizing the PN access control list.

- If inadequate information present in the access control list to enable PN access control, the PNM AS can query the controller UE about the information with how to precede the received initial request.

5 Procedures and information flows for PN configuration

5.1 PN-registration

5.1.1 General

The PN-registration is a procedure where the PN-user requests authorization to use PNM applications. As a result of a successful registration, the UE capabilities can be conveyed to the PNM AS.

5.1.2 PN-registration procedure in the IM CN subsystem

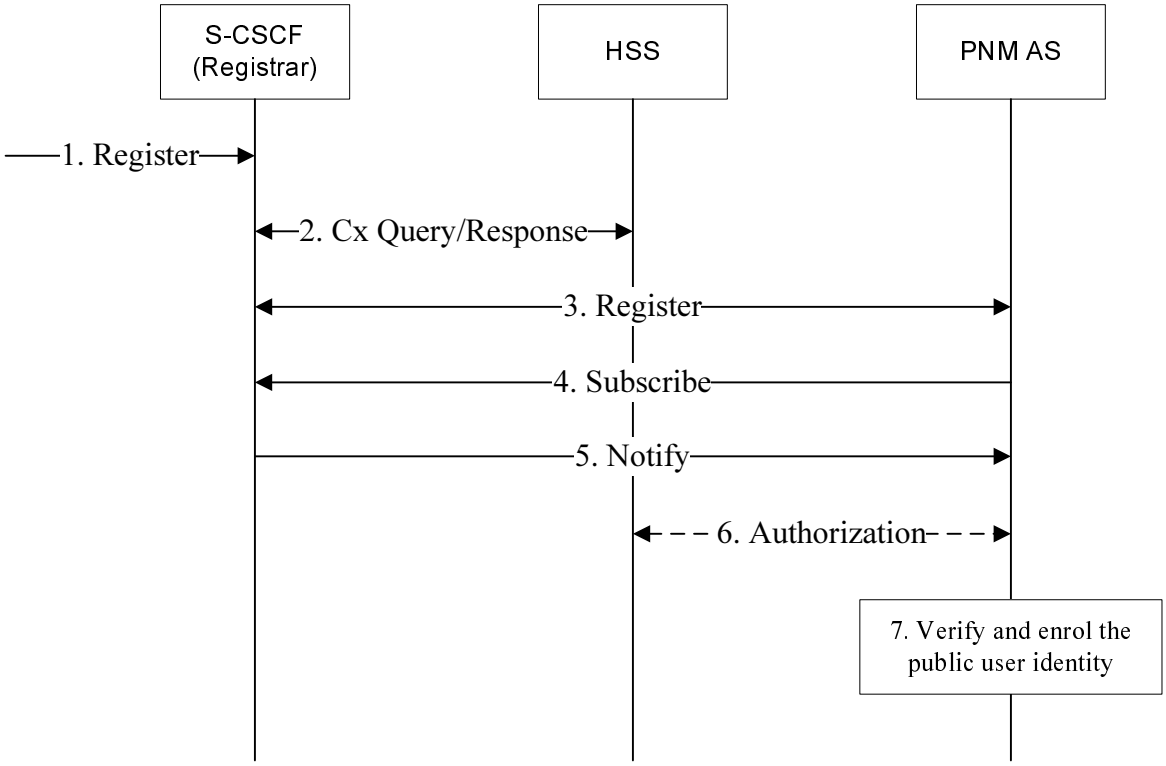

Figure 5.1.2-1: Successful PN-registration procedure in the IM CN subsystem

1. The Register information flow sent by a UE arrives at the S-CSCF/Registrar. The Register information flow contains the private user identity and the public user identity of the UE.

2. The S-CSCF sends a Cx-Put/Cx-Pull containing the private user identity and public user identity to the HSS and the HSS returns the information flow (eg. the initial filter criteria) to the S-CSCF.

3. Based on the initial filter criteria, the S-CSCF sends a Register information flow to the PNM AS. If the PNM AS specific data, for instance the PN UE name or the private user identity, which is associated with the initial filter criteria, is received from the HSS in Step 2, it is delivered to the PNM AS in the Register information flow.

4. The PNM AS sends a Subscribe information flow to obtain the public user identity received in the Register information flow in Step 3.

5. The S-CSCF sends a Notify information flow to the PNM AS containing the public user identities and the UE capabilities. If the S-CSCF assigned a GRUU for the UE during the registration, then the GRUU of the UE is delivered in the Notify information flow.

NOTE: At the same time as Steps 4) and 5) the AS can also contact the HSS using Sh to obtain the information. Where identical information is received from both sources, it is implementation specific how this is combined.

6. Optionally, the PNM AS authorizes the PN-registration by querying the HSS. It is done by sending the private user identity to the HSS. The HSS checks the public user identity/identities tied to the private user identity and sends the public user identity/identities and the private user identity back to the PNM AS.

7. The PNM AS then verifies the PN-registration by comparing the public user identity/identities and the PN UE name or with the other received from S-CSCF in the Step 3. As a result of a successful verification, the PNM AS enrols the public user identity and the PN UE name or as registered in the data base.

5.1.3 PN-registration procedure in the CS domain

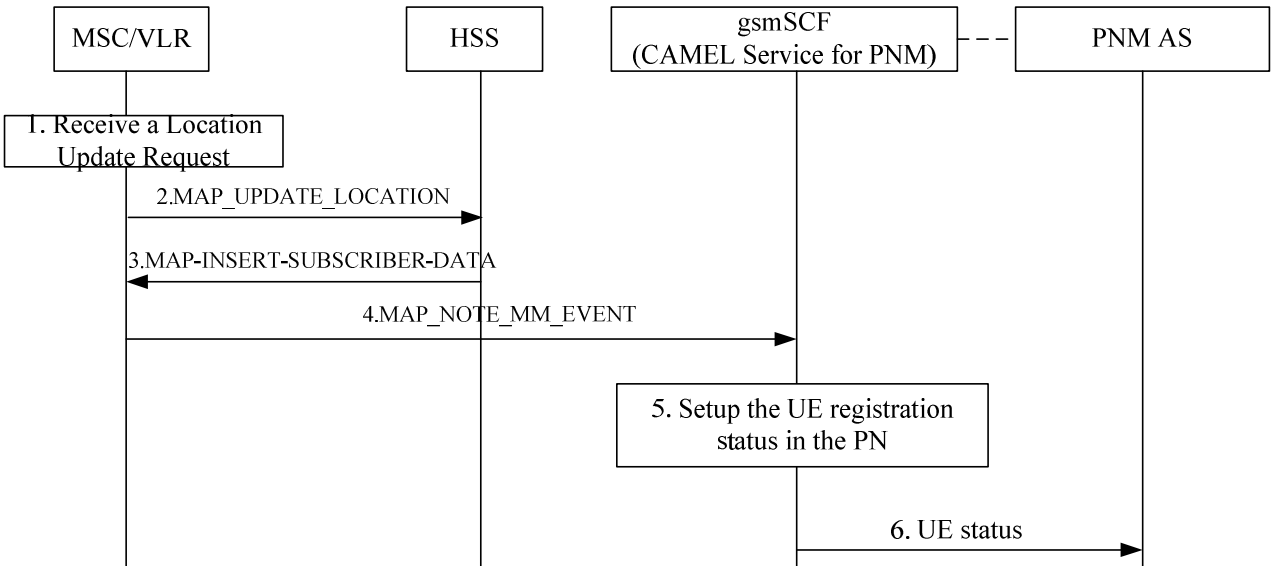

Figure 5.1.3-1: Successful PN-registration in the CS domain

1. The VLR receives a location update request from a UE.

2. The VLR sends the MAP_UPDATE_LOCATION message to the HSS to request the subscription information of the UE.

3. The HSS sends the MAP_INSERT_SUBSCRIBER_DATA message back to update the VLR with the PNM subscriber data.

4. The VLR changes the status of the UE to "attached"and sends the MAP_NOTE_MM_EVENT message to the gsmSCF (CAMEL service for PNM) to report the mobile event.

NOTE: To support the mobility management event, the CAMEL Phase 3 or later is required.

5. The gsmSCF setups the UE registration status in the PN to "registered".

6. The gsmSCF will send the UE status to the PNM AS.

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

5.1.4 PN-registration procedure for PNE

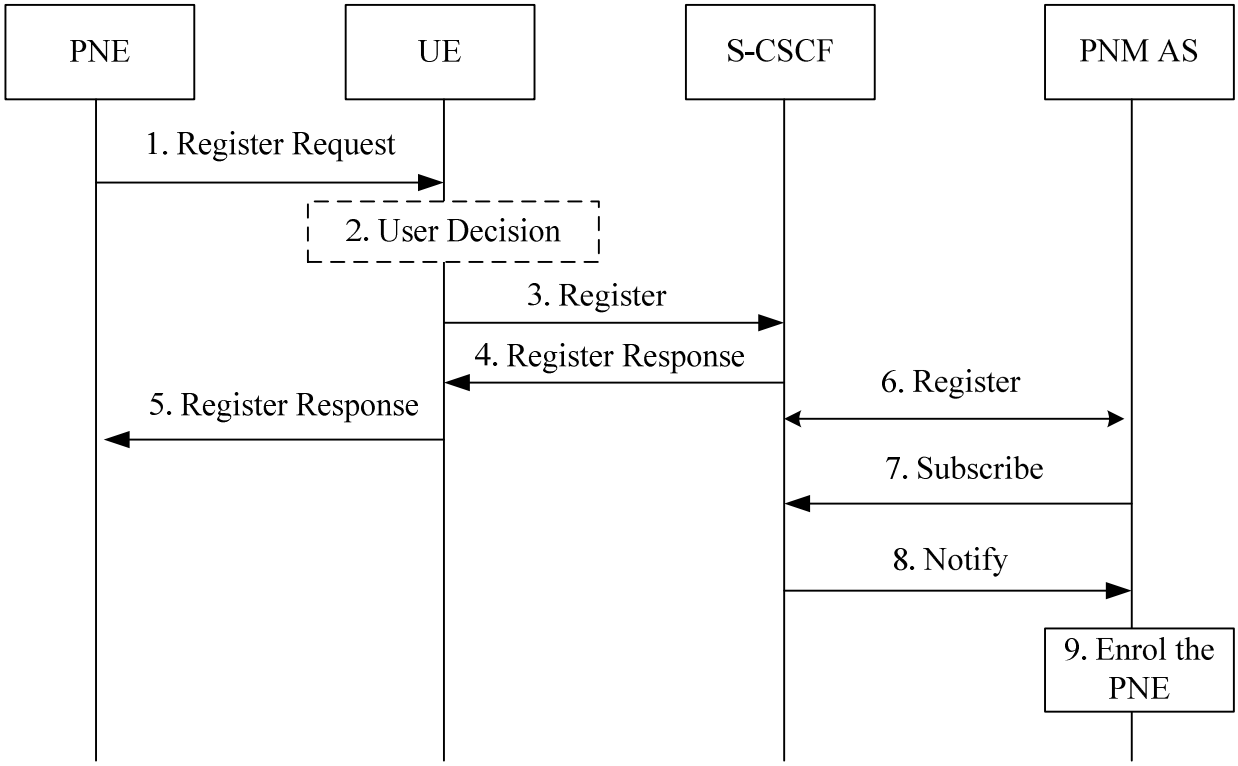

Figure 5.1.4-1: UE initiates the registration on behalf of the PNE

1. The PNE sends a register request to the UE including its capabilities via the PAN internal communication means.
2. Optionally, based on the user decision, the PNE is allowed to be added to the PAN.
3. The UE sends a SIP register request on behalf of the PNE to the S-CSCF. The Register information flow contains the private user identity and the public user identity of the UE, the identifier of the PNE allocated by the UE, and the PNE capabilities.
4. The S-CSCF sends the register response back to the UE.
5. UE forwards the register response to the PNE via the PAN internal communication means.
6. Based on the initial filter criteria, the S-CSCF sends a Register information flow to the PNM AS.
7. The PNM AS sends a Subscribe information flow to obtain the public user identities, PNE identifier and the PNE capabilities.
8. The S-CSCF sends a Notify information flow to the PNM AS containing the public user identities, PNE identifier and PNE capabilities.
9. The PNM AS enrols the public user identity and the PNE identifier in the data base.

5.2 PN-deregistration

5.2.1 General

Information shall be offered to the user by sending the status if the de-registered UE is the only default UE of the PN.

Figure 5.2.2-1 provides the procedure in the IM CN subsystem to inform the PN-user about De-registration of the only default UE in the PN.

Figure 5.2.3-1 provides the procedure in the CS domain to inform the PN-user about De-registration of the only default UE in the PN.

5.2.2 PN-deregistration procedure in the IM CN subsystem

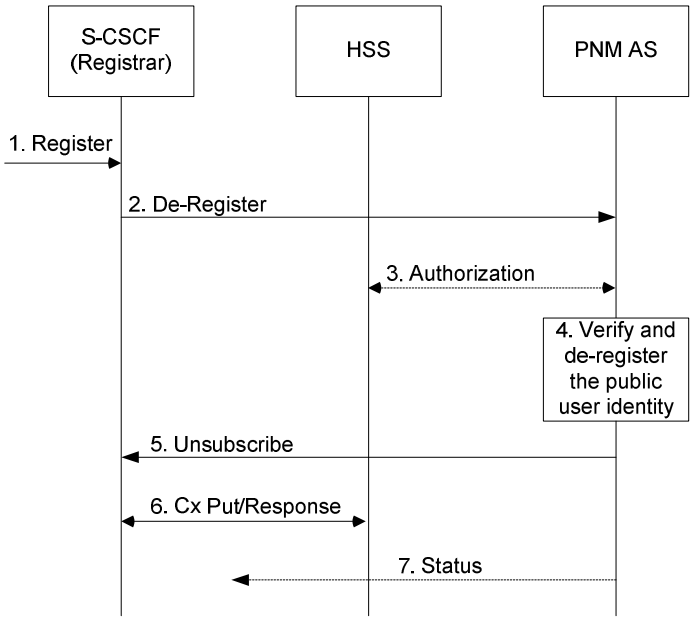

Figure 5.2.2-1: Successful PN-deregistration procedure in the IM CN subsystem

1. To de-register, the UE sends a new Register information flow with an expiration value of zero seconds. The Register information flow contains the private user identity and the public user identity of the UE.

2. Based on the initial filter criteria, the S-CSCF sends Register information flow with an expiration value of zero seconds to the PNM AS.

3. Optionally, the PNM AS authorizes the PN-registration by querying the HSS. It is done by sending the private user identity to the HSS. The HSS checks the public user identity/identities tied to the private user identity and sends it back to the PNM AS.

4. The PNM AS then verifies the PN-registration by comparing the public user identity/identities with the other received from S-CSCF in the Step 2. As a result of a successful verification, the PNM AS enrols the public user identity as de-registered in the data base and removes the stored configuration setting related to this specific public user identity.

5. The PNM AS sends an Unsubscribe information flow to unsubscribe to the service subscription notification of the public user identity.

6. The S-CSCF sends a Cx-Put/Cx-Pull containing the private user identity, public user identity and clear/keep S-CSCF name to the HSS base on operator choice and the HSS returns response to the S-CSCF.

7. If the UE ties to this specific public user identity registered as the only default UE, then the PNM AS sends the status to these UEs of the PN to inform this change.

5.2.3 PN-deregistration procedure in the CS domain

The PN-deregistration in the CS domain relies on the notification procedure of mobility management event and is accomplished by a notification with the event type of IMSI detach.

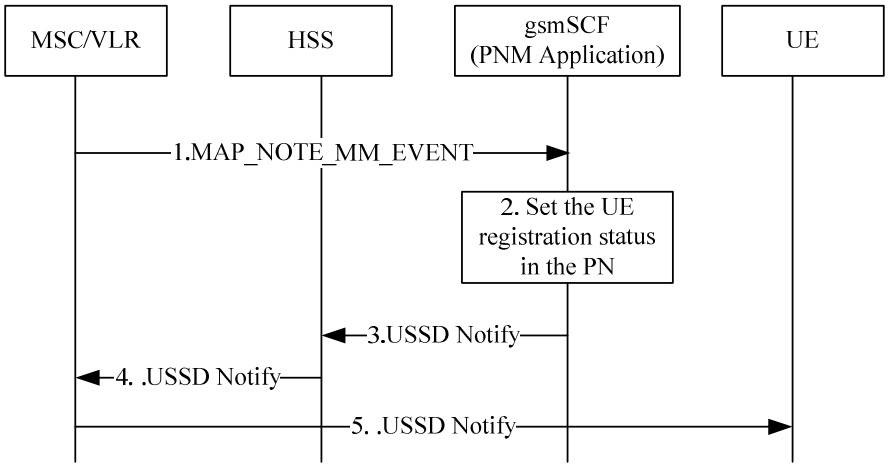

Figure 5.2.3-1: Procedure to inform the PN-user about the PN-deregistration of the default UE

1. After IMSI detach procedure, the VLR sends the MAP_NOTE_MM_EVENT message to the gsmSCF (CAMEL service for PNM) to report the mobile event.

2. The gsmSCF sets up the PN UE registration status in the PN to 'Deregistered'.

3. The gsmSCF checks whether the PN UE was the only default UE in the PN or not. If it was the only default UE in the PN, the gsmSCF generates the USSD Notify message to the HSS.

4-5. The HSS forwards this message to the PN UE via MSC/VLR according to 3GPP TS 23.090 [12].

5.2.4 PN-deregistration procedure for PNE

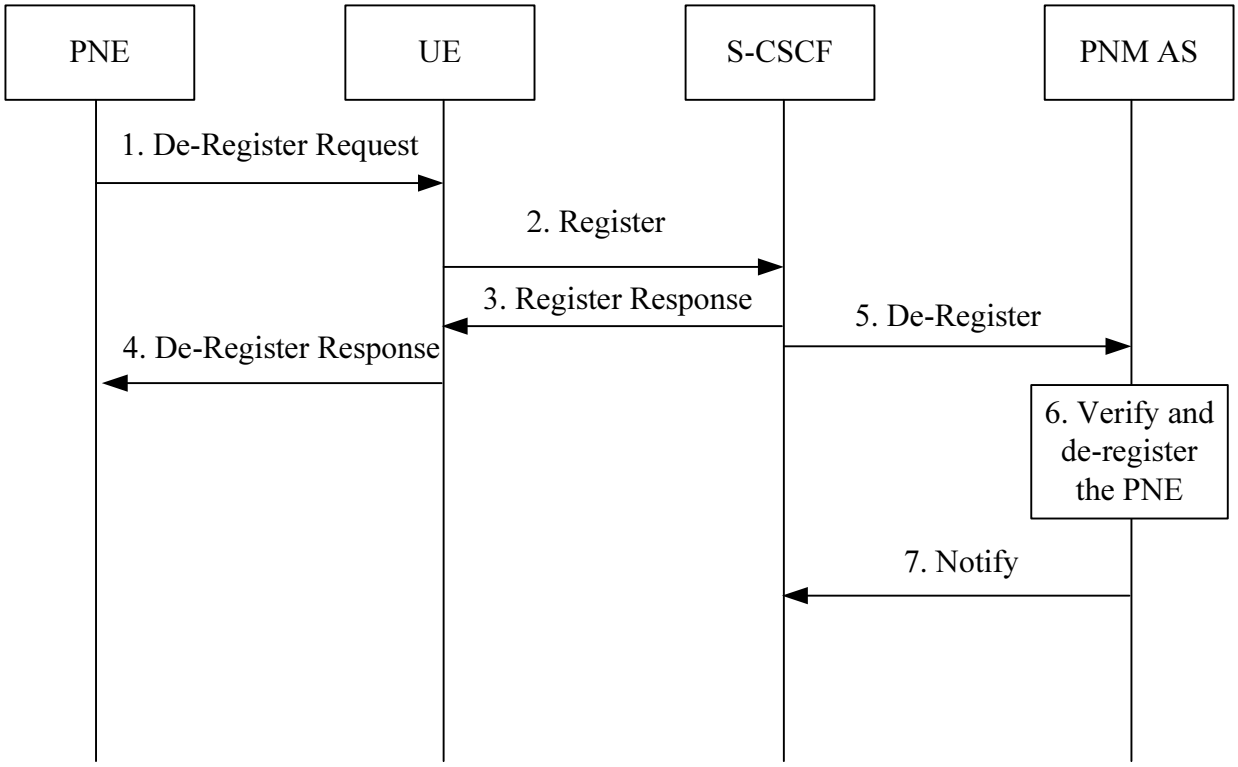

Figure 5.2.4-1: PN-deregistration procedure for PNE

1. The PNE sends a de-register request to the UE via the PAN internal communication means.
2. The UE sends a register request on behalf of the PNE to the S-CSCF with an expiration value of zero seconds.
3. The S-CSCF sends the register response back to the UE.
4. The UE sends the de-register response to the PNE via the PAN internal communication means.
5. Based on the initial filter criteria, the S-CSCF sends a De-Register information flow to the PNM AS.
6. The PNM AS then verifies the PN-deregistration by comparing the PNE identifier with the other received from S-CSCF. As a result of a successful verification, the PNM AS enrols the PNE identifier as de-registered in the data base and removes the stored configuration setting related to this specific PNE identifier.
7. The PNM AS sends a Notify information flow to the S-CSCF containing the register status of PNE.

5.3 PN-configuration

5.3.1 General

The PN-configuration procedures enable the PN-user to configure UEs as the default UE for terminating requests addressed to any UE belonging to the same PN and to configure the PN access control list. The PN-configuration can be done in three levels in IM CN subsystem and two levels in CS domain. They are a global level for all services supported by the UE capabilities and subscriptions, a per service basis for selected services supported by the UE capabilities and subscriptions, and a per service component basis for the different media of a supported service for the UE.

The following subclause describes the PN-configuration procedures in the IM CN subsystem. The signalling flow in figure 5.3.2-1 describes the information flow exchange between UE and NAF/PNM AS when the UE performs the PN-configuration.

5.3.2 PN-configuration procedure in the IM CN subsystem

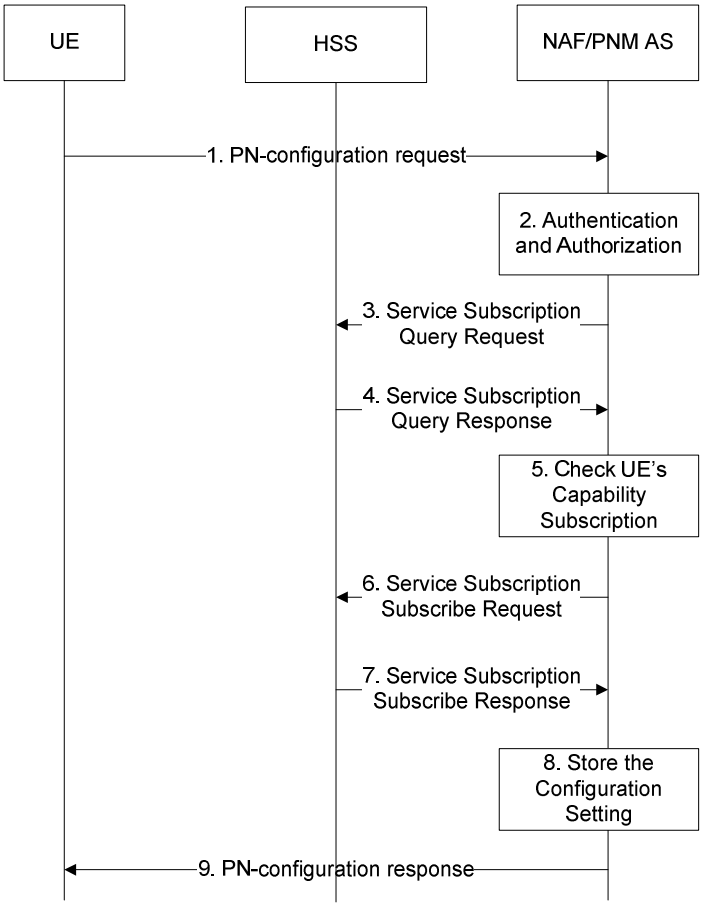

Figure 5.3.2-1: Successful PN-configuration procedure in the IM CN subsystem

The signalling flow in figure 5.3.2-1 describes the signal flow between UE and NAF/PNM AS when the UE wants to configure the PN. The procedure shall only take place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [11]) in which case the bootstrapped security association has been established before Step 1.

1. UE sends a PN-configuration request to the NAF/PNM AS informing the PNM AS about its desirable settings for the PN UE redirection applications and/or the PN access control list. The PN-configuration request contains the public user identity/identities of the UE, and the PN UE names of the UEs to be configured. The relevant parameters for executing the PN UE redirection application (e.g configuration level and the priority value) may be included. The controller UE and controllee UE, and the PN access control list including either the public user identities (if reachable in the IM CN subsystem) and/or the directory number (if reachable in the CS domain) may be included.

Editor's note: Whether routing information is needed is FFS.

2. Upon receiving this Configuration request message, the NAF/PNM AS authenticates the PN-configuration request according to the 3GPP TS 33.222 [9]. After a successful authentication, the NAF inserts the private user identity of the UE and forwards the requestto the PNM AS. The PNM AS authorizes the Configuration request message by comparing the public user identity and the PN UE name with those ones that are registered in the PN by means of the PN-registration procedure.

3. The NAF/PNM AS sends a Service Subscription Query request to the HSS in order to obtain the service subscription tied to the public user identity received in the PN-configuration request.

4. The HSS sends a Service Subscription Query response back to the NAF/PNM AS with the service subscription tied to the public user identity.

5. Upon receiving the Service Subscription Query response, the NAF/PNM AS verifies the UE capability and the service subscription of the public user identity.

6. The NAF/PNM AS sends the Service Subscription Subscribe request to the HSS.
7. The HSS sends the Service Subscription Subscribe Response to the NAF/PNM AS.
8. The NAF/PNM AS stores the configuration settings.
9. The NAF/PNM AS sends the PN-configuration response to the UE.

5.3.3 PN-configuration procedure for PNE in the IM CN subsystem

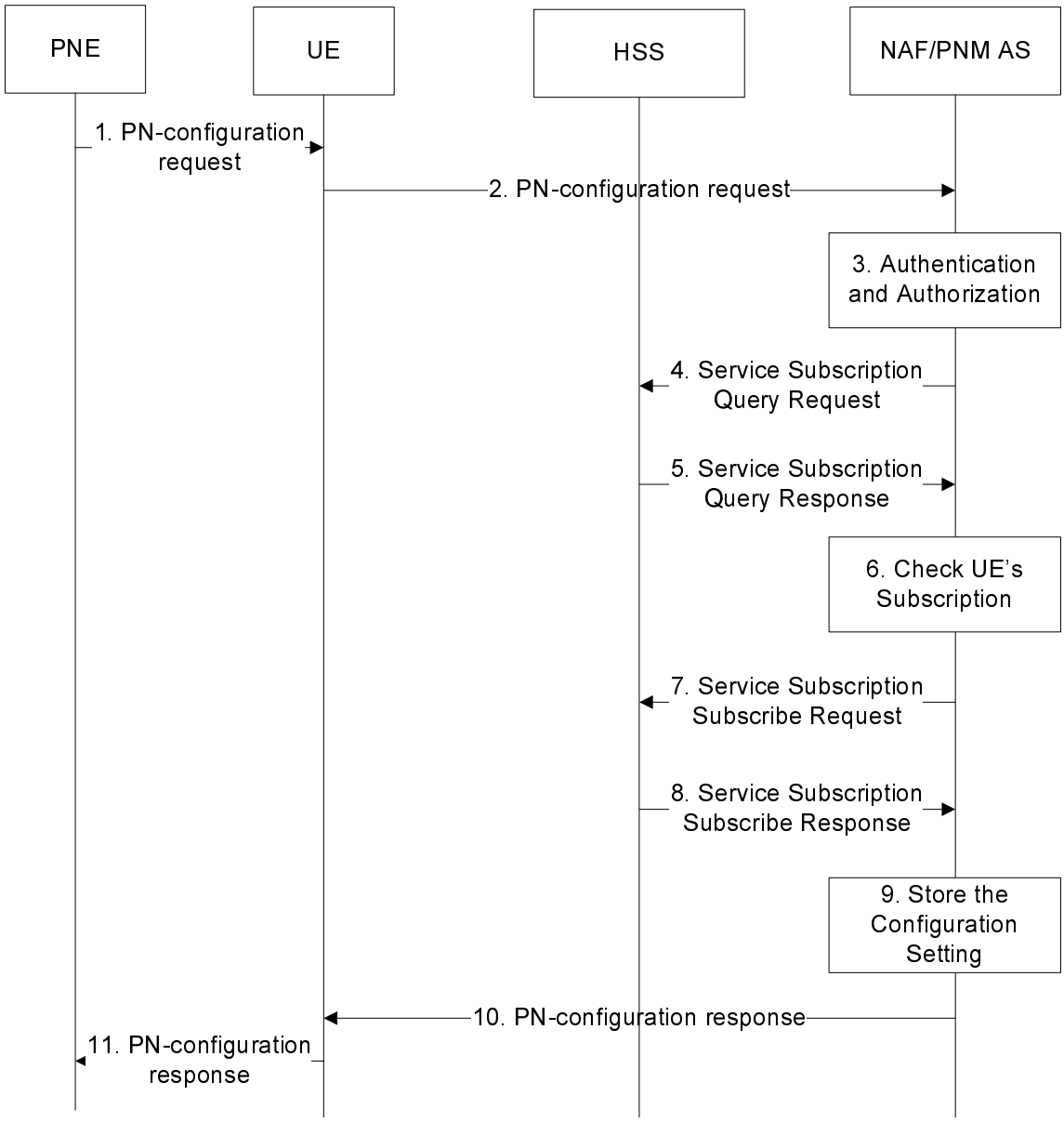

Figure 5.3.3-1: PN-configuration procedure for PNE in the IM CN subsystem

The signalling flow in figure 5.3.3-1 describes the signalling flow between PNE and NAF/PNM AS through the UE when the PNE wants to configure the PN.

1. PNE sends a PN-configuration request to the UE contains the public user identity/identities of the UE, and the PN identifier of the PNE to be configured. The relevant parameters for executing the PN redirection application (e.g configuration level and the priority value) may be included. The PN access control list including either the public user identities (if reachable in the IM CN subsystem) and/or the directory number (if reachable in the CS domain) may be included.

NOTE: The interface between PNE and UE is out of scope.

2. UE forwards the PN-configuration request to the NAF/PNM AS informing the PNM AS about the desirable settings of PNE.

3. Upon receiving this Configuration request message, the NAF/PNM AS authenticates the PN-configuration request according to the 3GPP TS 33.222 [9]. After a successful authentication, the NAF inserts the private user identity of the UE and forwards the request to the PNM AS. The PNM AS authorizes the Configuration request

message by comparing the public user identity and the PN UE name with those ones that are registered in the PN by means of the PN-registration procedure.

4. The NAF/PNM AS sends a Service Subscription Query request to the HSS in order to obtain the service subscription tied to the public user identity received in the PN-configuration request.
5. The HSS sends a Service Subscription Query response back to the NAF/PNM AS with the service subscription tied to the public user identity.
6. Upon receiving the Service Subscription Query response, the NAF/PNM AS verifies the PNE service subscription of the public user identity.
7. The NAF/PNM AS sends the Service Subscription Subscribe request to the HSS.
8. The HSS sends the Service Subscription Subscribe Response to the NAF/PNM AS.
9. The NAF/PNM AS stores the configuration settings.
10. The NAF/PNM AS sends the PN-configuration response to the UE.
11. UE forwards the PN-configuration response to the PNE.

5.4 PN-deconfiguration

5.4.1 General

The PN-deconfiguration procedure enables the PN-user to deconfigure the default UE of a PN. Corresponding to the configuration procedure described in subclause 5.3, the PN-deconfiguration can be done in three levels in IM CN subsystem and two levels in CS domain.

The following subclauses describe the PN-deconfiguration procedure in the IM CN subsystem.

5.4.2 PN-deconfiguration procedure in the IM CN subsystem

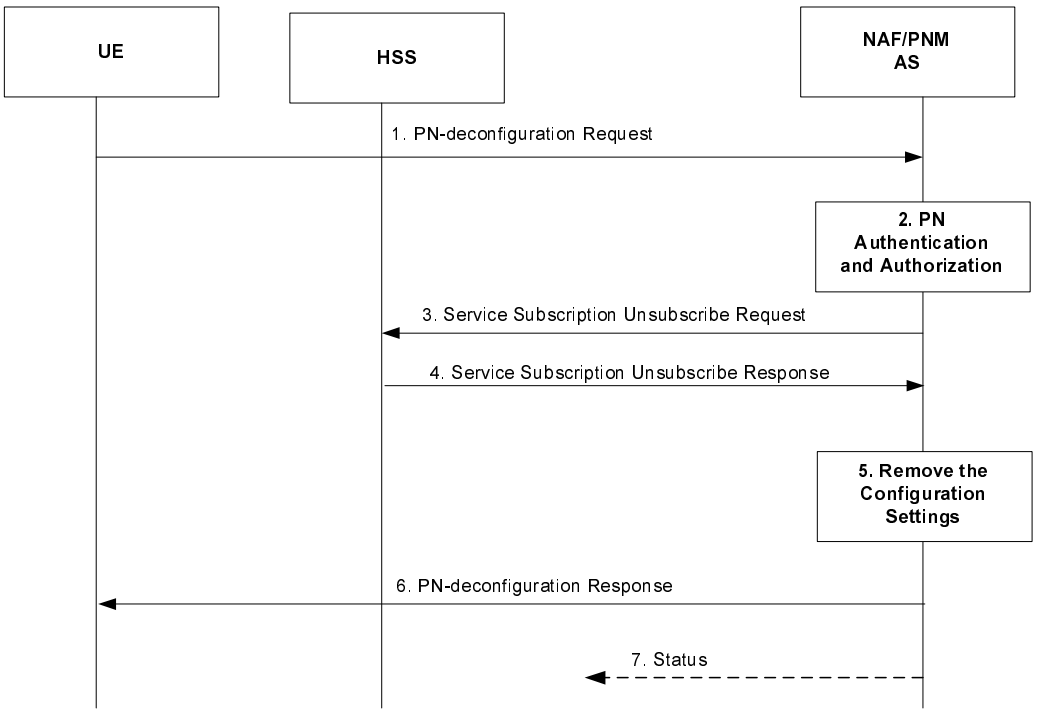

Figure 5.4.2-1: Successful PN-deconfiguration procedure in the IM CN Subsystem

The signalling flow in figure 5.4.2-1 describes the signal flow between UE and NAF/PNM AS when the UE wants to deconfigure the PN. The messaging shall only take place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [11]) in which case the bootstrapped security association has been established before Step 1.

1. In order to remove its configuration settings for the PN UE redirection applications from the PN, a UE sends a Deconfiguration request message to the PNM AS containing the public user identity/identities of the UEs to be deconfigured. Additionally, other relevant parameters for executing the PN UE redirection application such as the configuration level and the priority value can be included.

2. Upon receiving the PN-deconfiguration request, the NAF/PNM AS authenticates the PN-deconfiguration Request according to the 3GPP TS 33.222 [9]. After a successful authentication, the NAF inserts the private user identity of the UE and forwards it to the PNM AS. The PNM AS authorizes the PN-deconfiguration request by comparing the public user identity with those ones that are registered in the PN by means of the PN-registration procedure.

3. The PNM AS sends the Unsubscribe request to the HSS.

4. The HSS sends the Unsubscribe response to the PNM AS.

5. The PNM AS removes the stored configuration setting.

6. The PNM AS sends the PN-deconfiguration response to the UE.

7. If the UE ties to this specific public user identity registered as the only default UE, then the NAF/PNM AS sends the Status message request to these UEs of the PN to inform this change.

5.5 PN-query

5.5.1 General

Figure 5.5.2-1 shows a successful PN-query procedure that is used by the PN-users to enquiry their PN settings information which is stored in the PNM AS after performing the PN-registration and PN-configuration procedures.

5.5.2 PN query procedure

The PN setting information belonging to a PN-user can be categorized into:

- information about the registered public user identities,
- settings for PN UE redirection, such as the default UEs, service level settings and redirection priority.
- settings for the PN access control, such as a PN access control list.

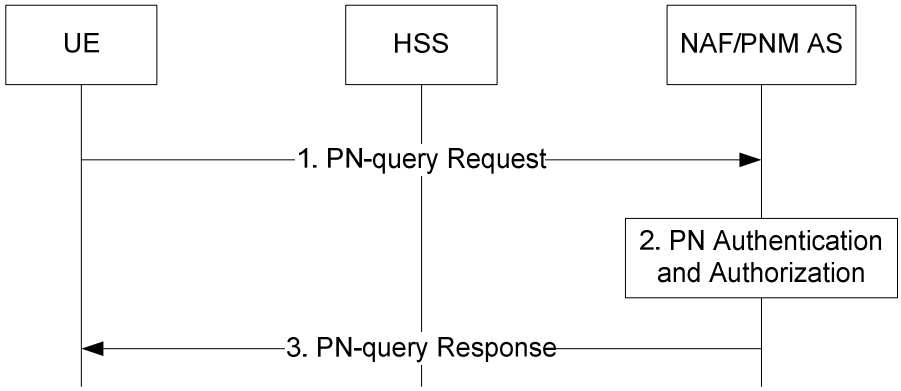

Figure 5.5.2-1: Successful PN query procedure in the IM CN subsystem

The signalling flow in figure 5.5.2-1 describes the signal flow between UE and NAF/PNM AS when the UE wants to query the PN settings. The procedure shall only take place after a successful bootstrapping procedure (as described in 3GPP TS 33.220 [11]) in which case the bootstrapped security association has been established before Step 1.

1. UE sends a PNquery request to the NAF/PNM AS in order to obtain the PN setting information classified above for the PNM applications by including the public user identity/identities of the UEs.

2. Upon receiving the PN-query request, the NAF/PNM AS authenticates the PN-query request according to the 3GPP TS 33.222 [9]. After a successful authentication, the NAF/PNM AS inserts the private user identity associated with the public user identity/identities of the UE and forwards the message to the NAF/PNM AS. The NAF/PNM AS authorizes the PN-query request by comparing the public user identity with those ones that are registered in the PN by means of the PN-registration procedure.

3. The NAF/PNM AS sends the PNquery response message to the UE containing the PN settings information for the PNM applications as asked by the UE.

6 Procedures and information flows for PN redirection

6.1 Procedures and information flows in the IP CN subsystem

6.1.1 General

One of the functionalities enabled by the PNM AS in the IM CN subsystem is called PNUE redirection that redirects sessions destined for any UEs of a PN to the default UE of the same PN as described in 3GPP TS 22.259 [1]. The PN UE redirection applies only to the initial request for a UE-terminating call. The procedures for supporting the PN UE redirection in the IM CN subsystem take advantage of the interface between an S-CSCF and an AS in the IM CN subsystem described in 3GPP TS 23.002 [2] and the procedures described in 3GPP TS 23.218 [3].

When receiving an initial request for a UE-terminating call, the S-CSCF performs the procedure defined in 3GPP TS 23.218 [3] to route the initial request for the UE-terminating call to the PNM AS based on matching of initial filter criteria before performing any other routing procedures to the terminating UE. The PNM AS then executes the redirection of the initial request to the default UE of the PN based on the PN-user's PN configuration as described in clause 6. The redirection of the initial request for the UE-terminating call can be executed either on an IP multimedia application basis or on the media component(s) of an IP multimedia application basis supported by the terminating UE capabilities and the PN-user subscriptions.

If the PN-user configured a UE list of different priorities for the PN UE redirection, the PNM AS shall execute the session redirection for a particular UE based on the configuration in a decreasing order of the priority. If the session redirection for a UE of a higher priority fails, the PNM AS shall perform the PNM session redirection for the other UE of the next lower priority.

6.1.2 Procedures and information flows for PN UE redirection in the IM CN subsystem

Figure 6.1.2-1 describes the procedures and information flows for handling the PN UE redirection in the IM CN subsystem. Without loss of generality, it is assumed for figure 6.2.1-1 that a PN-user"s PN consists of two UEs, i.e., the UE-1 and the UE-2. The UE-2 is the default UE according to PN-user's PN configuration as described in clause 6. Furthermore, it is assumed that the two UEs have different public user identities.

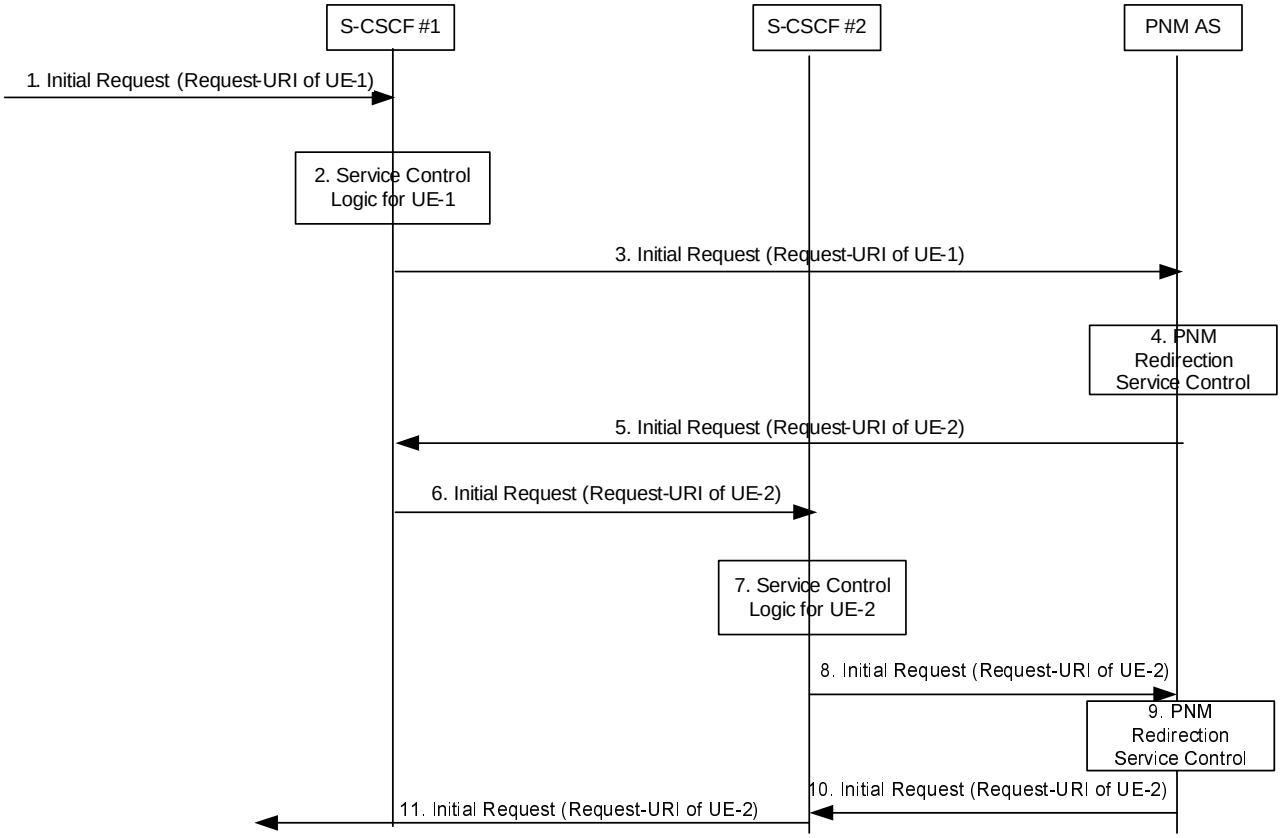

Figure 6.1.2-1: Initial request to UE-1 and redirected to UE-2 by the PNM AS in the IM CN subsystem

1. An initial request to the UE-1 containing the Request-URI of the UE-1 public user identity arrives at the S-CSCF #1.

2. The S-CSCF #1 determines that the initial request is for a UE-terminated case, invokes the termination service control logic required for the UE-1 and evaluates the initial filter criteria, which results in re-routing the initial request to the PNM AS.

3. As a result of the termination service control logic invocation for the UE-1, the S-CSCF #1 forwards the initial request to the PNM AS.

4. The PNM AS executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The PNM AS decides to redirect the initial request to the default UE of the PN, i.e., to the UE-2.

5. As a result of the PN UE redirection control logic execution, the PNM AS sends the redirected initial request containing the Request-URI of the UE-2 public user identity to the S-CSCF #1.

6. The S-CSCF #1 treats the redirected initial request as a UE-originated case, and forwards the redirected initial request to the S-CSCF #2. The S-CSCF #1 and the S-CSCF #2 can be the same entity.

7. The S-CSCF #2 treats the redirected initial request as a UE-terminated case, invokes the termination service control logic required for the UE-2 and evaluates the initial filter criteria, which may results in re-routing the redirected initial request to the other ASs.

8-10. The S-CSCF #2 forwards the redirected request to the PNM AS as the result of the termination service control logic for the UE-2. The PNM AS executes the PN UE redirection control logic and decides to forward the request as the UE-2 is the default UE of the PN.

11. The S-CSCF#2 continues the redirected initial request based on the standard call setup procedures as described in 3GPP TS 23.228 [4].

Figure 6.1.2-2 describes the procedures and information flows for handling the PN UE redirection in the IM CN subsystem when the default UE (in this example the UE-2) in the PN shares the same public user identity with the UE-1.

NOTE: It's assumed that the UE-2 can support GRUU.

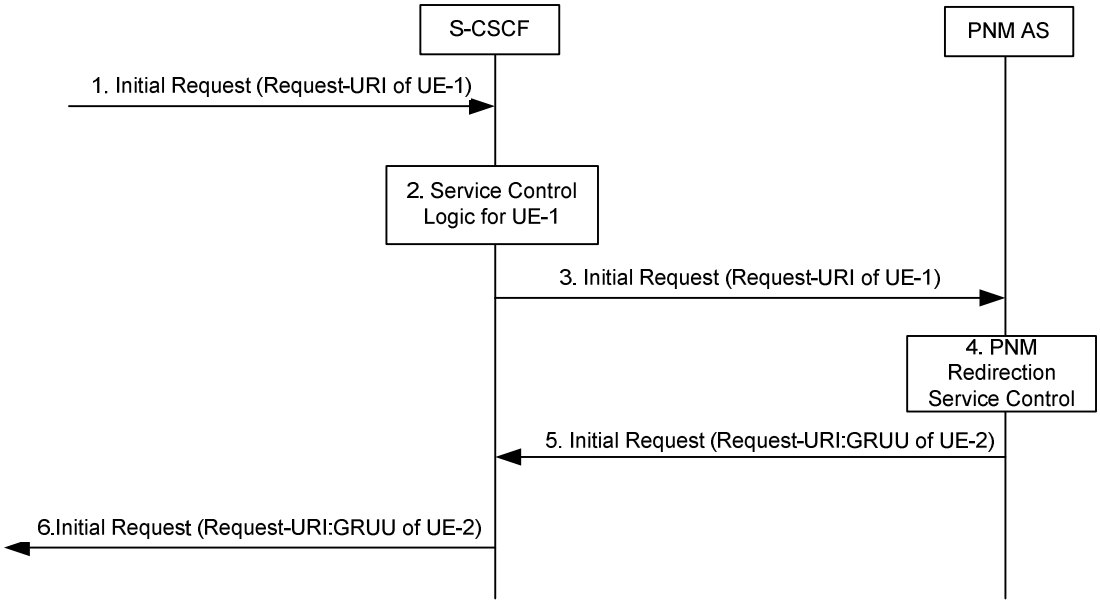

Figure 6.1.2-2: Initial request to UE-1 and redirected to UE-2 by the PNM AS in the IM CN subsystem when the UE-2 shares the same public user identity with the UE-1

1. An initial request to the UE-1 containing the Request-URI of the UE-1 public user identity arrives at the S-CSCF.
2. The S-CSCF determines that the initial request is for a UE-terminated case, invokes the termination service control logic required for the UE-1 and evaluates the initial filter criteria, which results in re-routing the initial request to the PNM AS.
3. As a result of the termination service control logic invocation for the UE-1, the S-CSCF forwards the initial request to the PNM AS.
4. The PNM AS executes the PNM redirection service control logic based on the User's PN configurations as described in clause 6. The PNM AS decides to redirect the initial request to the default UE of the PN, i.e., to the UE-2.
5. As a result of the PNM redirection service logic execution, the PNM AS sends the redirected initial request containing the Request-URI which is set to the GRUU of the UE-2 to the S-CSCF.
6. The S-CSCF continues the redirected initial request procedure based on the standard call setup procedures as described in 3GPP TS 23.228 [4].

Figure 6.1.2-3 describes the procedures and information flows for handling the PN UE redirection in the IM CN subsystem when the default UE (in this example the UE-2) in the PN cannot setup the session. Consequently, the PNM AS performs the PNM session redirection for the other UE of the next lower priority (in this example the UE-3).

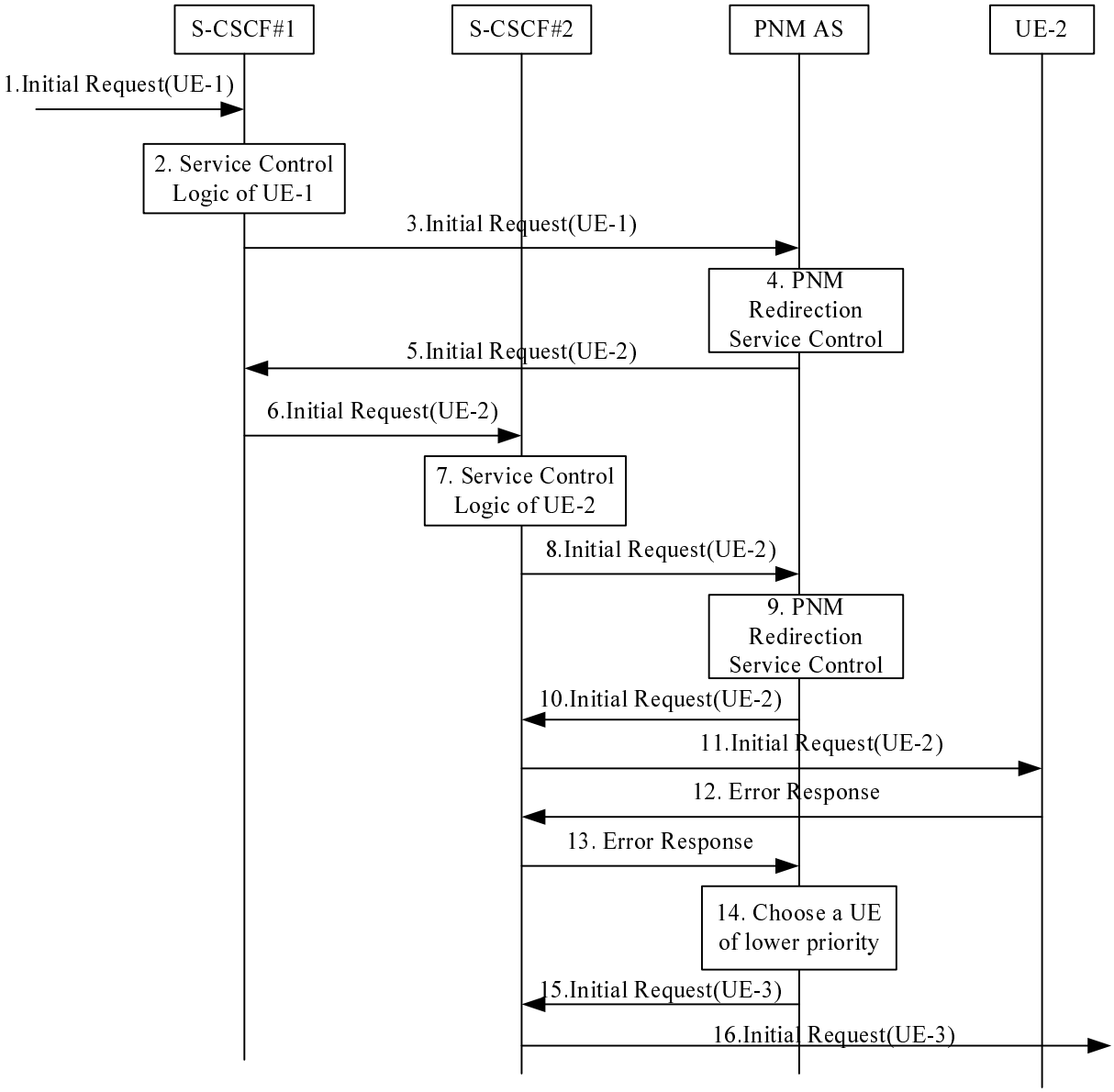

Figure 6.1.2-3: Initial request to UE-1 and redirected to UE-3 by the PNM AS in the IM CN subsystem when the initial request to UE-2 fails

1. An initial request to the UE-1 containing the Request-URI of the UE-1 public user identity arrives at the S-CSCF #1.

2. The S-CSCF #1 determines that the initial request is for a UE-terminated case, invokes the termination service control logic required for the UE-1 and evaluates the initial filter criteria, which results in re-routing the initial request to the PNM AS.

3. As a result of the termination service control logic invocation for the UE-1, the S-CSCF #1 forwards the initial request to the PNM AS.

4. The PNM AS executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The PNM AS decides to redirect the initial request to the default UE of the PN, i.e., to the UE-2.

5. As a result of the PN UE redirection control logic execution, the PNM AS sends the redirected initial request containing the Request-URI of the UE-2 public user identity to the S-CSCF #1.

6. The S-CSCF #1 treats the redirected initial request as a UE-originated case, and forwards the redirected initial request to the S-CSCF #2. The S-CSCF #1 and the S-CSCF #2 can be the same entity.

7. The S-CSCF #2 treats the redirected initial request as a UE-terminated case, invokes the termination service control logic required for the UE-2 and evaluates the initial filter criteria, which may results in re-routing the redirected initial request to the other ASs.

8-10. The S-CSCF #2 forwards the redirected request to the PNM AS as the result of the termination service control logic for the UE-2. The PNM AS executes the PN UE redirection control logic and decides to forward the request as the UE-2 is the default UE of the PN.

11. The S-CSCF#2 continues the redirected initial request which is forwarded to UE-2.

12-13. UE-2 cannot setup the session and returns an error response back to PNM AS.

14. The PNM AS executes the PN UE redirection control logic for the other UE of the next lower priority which in this example is UE-3.

15-16. As a result of the PN UE redirection control logic execution, the PNM AS forwards the redirected initial request containing the Request-URI of the UE-3 public user identity to the UE-3.

6.1.3 Procedures and information flows for PNE redirection in the IM CN subsystem

Figure 6.1.3-1 describes the procedures and information flows for handling the PNE redirection in the IM CN subsystem. Without loss of generality, it is assumed for figure 6.1.3-1 that a PN-user"s PN consists of three PNEs, i.e., the UE-1, the UE-2 and PNE-1.UE-2 and PNE-1 belong to a PAN. The PNE-1 is the default PNE according to PN-user's PN configuration as described in clause 6. Furthermore, it is assumed that the two UEs have different public user identities.

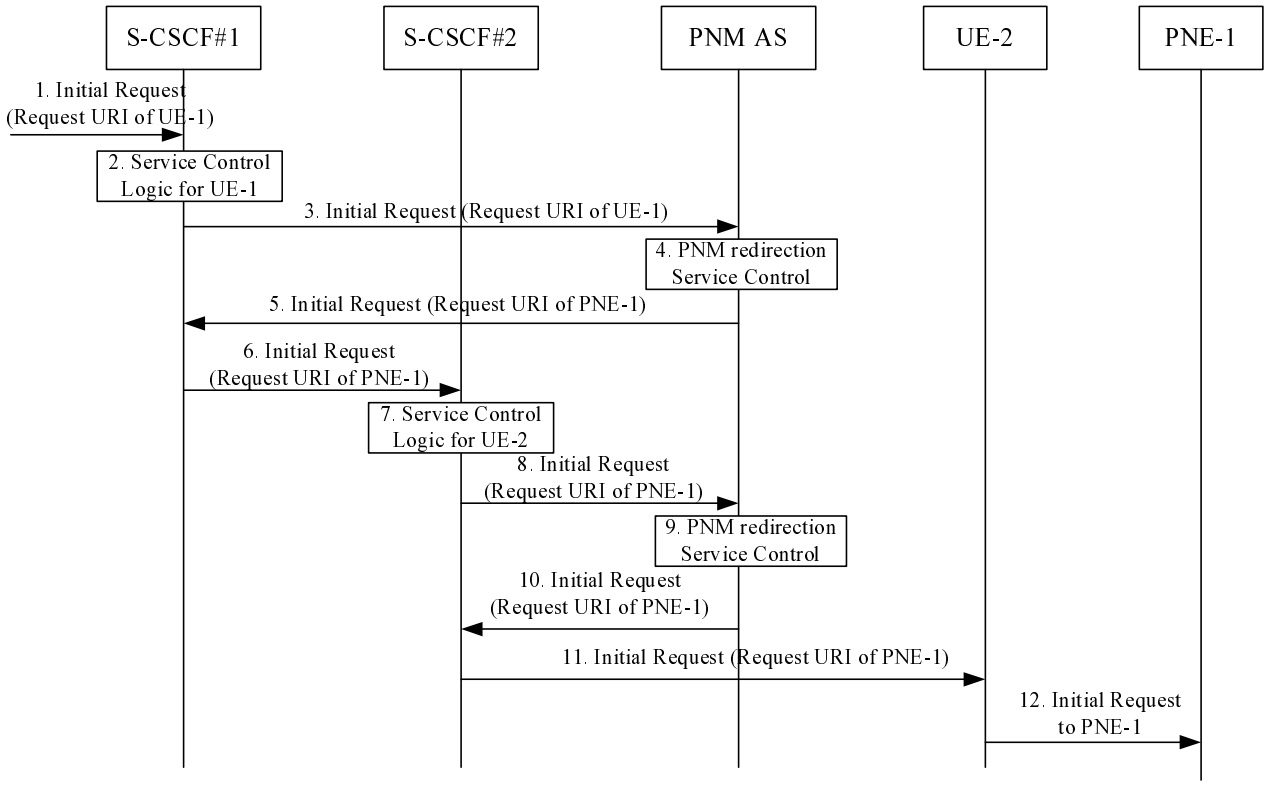

Figure 6.1.3-1: Initial request to UE-1 and redirected to UE-2 by the PNM AS in the IM CN subsystem

1. An initial request to the UE-1 containing the Request-URI of the UE-1 public user identity arrives at the S-CSCF #1.

2. The S-CSCF #1 determines that the initial request is for a UE-terminated case, invokes the termination service control logic required for the UE-1 and evaluates the initial filter criteria, which results in re-routing the initial request to the PNM AS.

3. As a result of the termination service control logic invocation for the UE-1, the S-CSCF #1 forwards the initial request to the PNM AS.

4. The PNM AS executes the PNE redirection control logic based on the PN-user's PN configurations as described in clause 6. The PNM AS decides to redirect the initial request to the default UE of the PN, i.e., to the PNE-1.

5. As a result of the PNE redirection control logic execution, the PNM AS sends the redirected initial request containing the Request-URI of the GRUU of UE-2 and the identity of PNE-1 to the S-CSCF #1.

6. The S-CSCF #1 treats the redirected initial request as a UE-originated case, and forwards the redirected initial request to the S-CSCF #2. The S-CSCF #1 and the S-CSCF #2 can be the same entity.

7. The S-CSCF #2 treats the redirected initial request as a UE-terminated case, invokes the termination service control logic required for the UE-2 and evaluates the initial filter criteria, which can result in re-routing the redirected initial request to the other ASs.

8-10. The S-CSCF #2 forwards the redirected request to the PNM AS as the result of the termination service control logic for the UE-2. The PNM AS executes the PN UE redirection control logic and decides to forward the request as the PNE-1 is the default UE of the PN.

11. The S-CSCF#2 forwards the initial request including identity of PNE-1 to the UE-2.

12. The UE-2 forwards the initial request to the PNE-1 via the PAN internal interface.

6.2 Procedures and information flows in the CS domain

6.2.1 General

Similar to the functionality described in the subclause 6.1.1, the gsmSCF (CAMEL service for PNM) can redirect calls destined for any UEs of a PN in the CS domain to the default UE of the same PN. The procedures for supporting the PNM call redirection in the CS domain takes advantage of the interface between a GMSC and a gsmSCF in the CS domain described in 3GPP TS 23.078 [8] and the procedures described in 3GPP TS 23.018 [10].

When receiving a call request for a UE in the PN, the GMSC performs the procedure defined in 3GPP TS 23.078 [8] to route the request to the gsmSCF (CAMEL service for PNM) based on the T_CSI configured to the UE before performing any other routing procedures to the terminating UE. The gsmSCF (CAMEL service for PNM) then executes the redirection of the request based on the PN-user"s PN configuration as described in clause 6.

If the PN-user configured a UE list of different priorities for the PNM call redirection, the gsmSCF (CAMEL service for PNM) shall execute the call redirection for a particular UE based on the configuration in a decreasing order of the priority. If the call redirection for a UE of a higher priority fails, the gsmSCF (CAMEL service for PNM) shall perform the PNM call redirection for the other UE of the next lower priority.

6.2.2 Procedures and information flows for PN UE redirection in the CS domain

Figure 6.2.2-1 describes the procedures and information flows for handling the PNM call redirection in the CS domain. Without loss of generality, it is assumed for figure 6.2.2-1 that a PN-user"s PN consists of two UEs, i.e., the UE-1 and the UE-2. The UE-2 is the default UE according to PN-user"s PN configuration as described in clause 6.

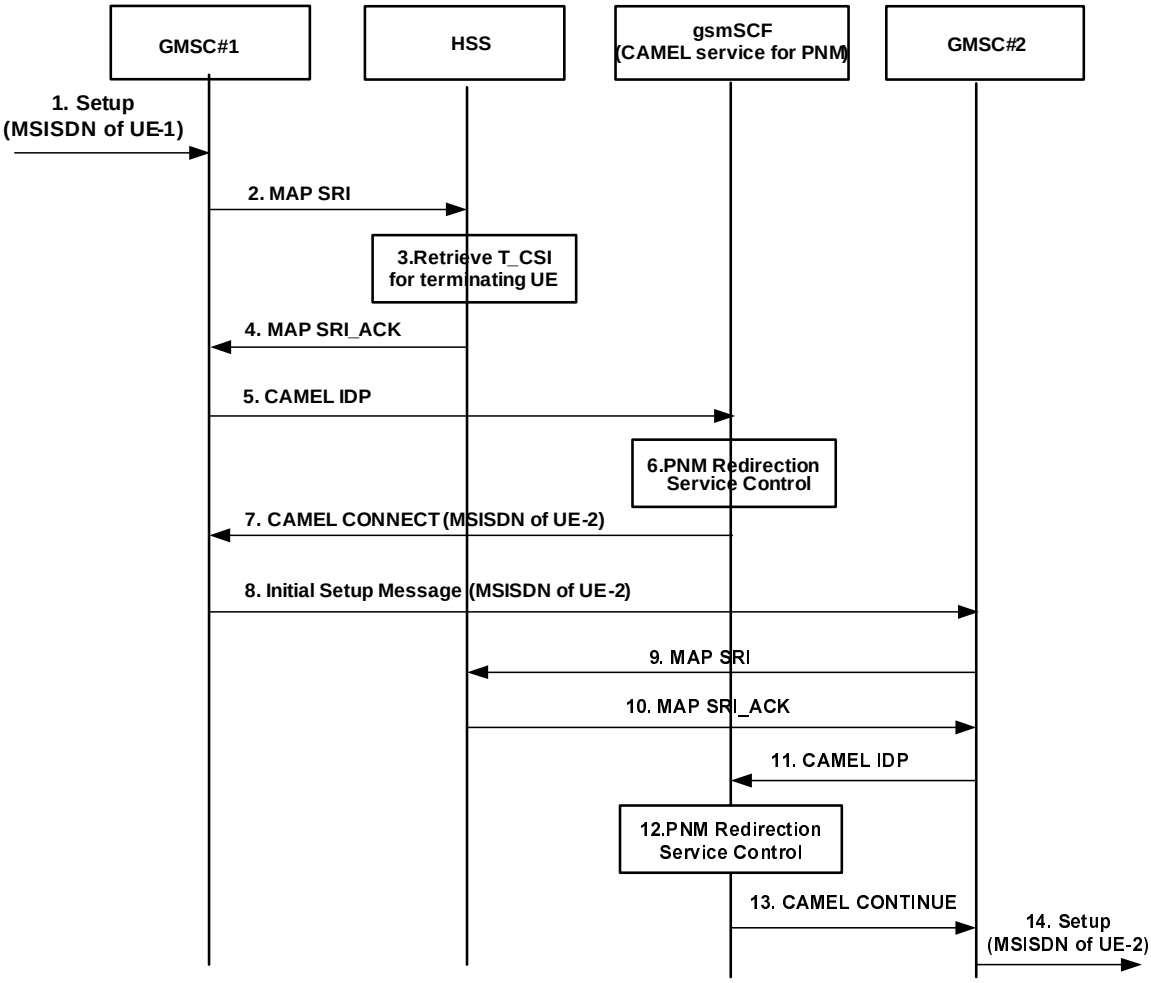

Figure 6.2.2-1: Initial request to UE-1 and redirected to UE-2 by the gsmSCF (CAMEL service for PNM) in the CS domain

1. A call request to the UE-1 containing the MSISDN of the UE-1 as the called party number arrives at the GMSC #1.

2. On receipt of the incoming call request, the GMSC#1 queries the HSS for routing information.

3. 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.

4. The HSS returns the T-CSI information element to the GMSC#1 in response to the query for routing information (SRI).

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

6. The gsmSCF (CAMEL service for PNM) executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The gsmSCF (CAMEL service for PNM) decides to redirect the call request to the default UE of the PN, i.e., to the UE-2.

7. As a result of the PN UE redirection control logic execution, the gsmSCF (CAMEL service for PNM) to respond to the CAMEL IDP message with a CAMEL CONNECT message containing the MSISDN of the UE-2 as the called party number.

8. The GMSC#1 initiates the CS call towards the GMSC#2 by sending an Initial Setup Message (e.g. ISUP IAM, BICC IAM, and SIP-I Invite).

9-13. The GMSC#2 queries the HSS for routing information and triggers a CAMEL activity to the gsmSCF. The gsmSCF executed the PNM redirection service control logic and decides to forward the request as the UE-2 is the default UE of the PN, so it responds with a CMAEL CONTINUE message to the GMSC#2.

14. The GMSC#2 continues the redirected call request based on the standard call setup procedures as described in 3GPP TS 23.018 [10].

Figure 6.2.2-2 describes the procedures and information flows for handling the PN UE redirection in the CS domain when the default UE (in this example the UE-2) in the PN cannot setup the session. Consequently, the gsmSCF performs the PNM session redirection for the other UE of the next lower priority (in this example the UE-3).

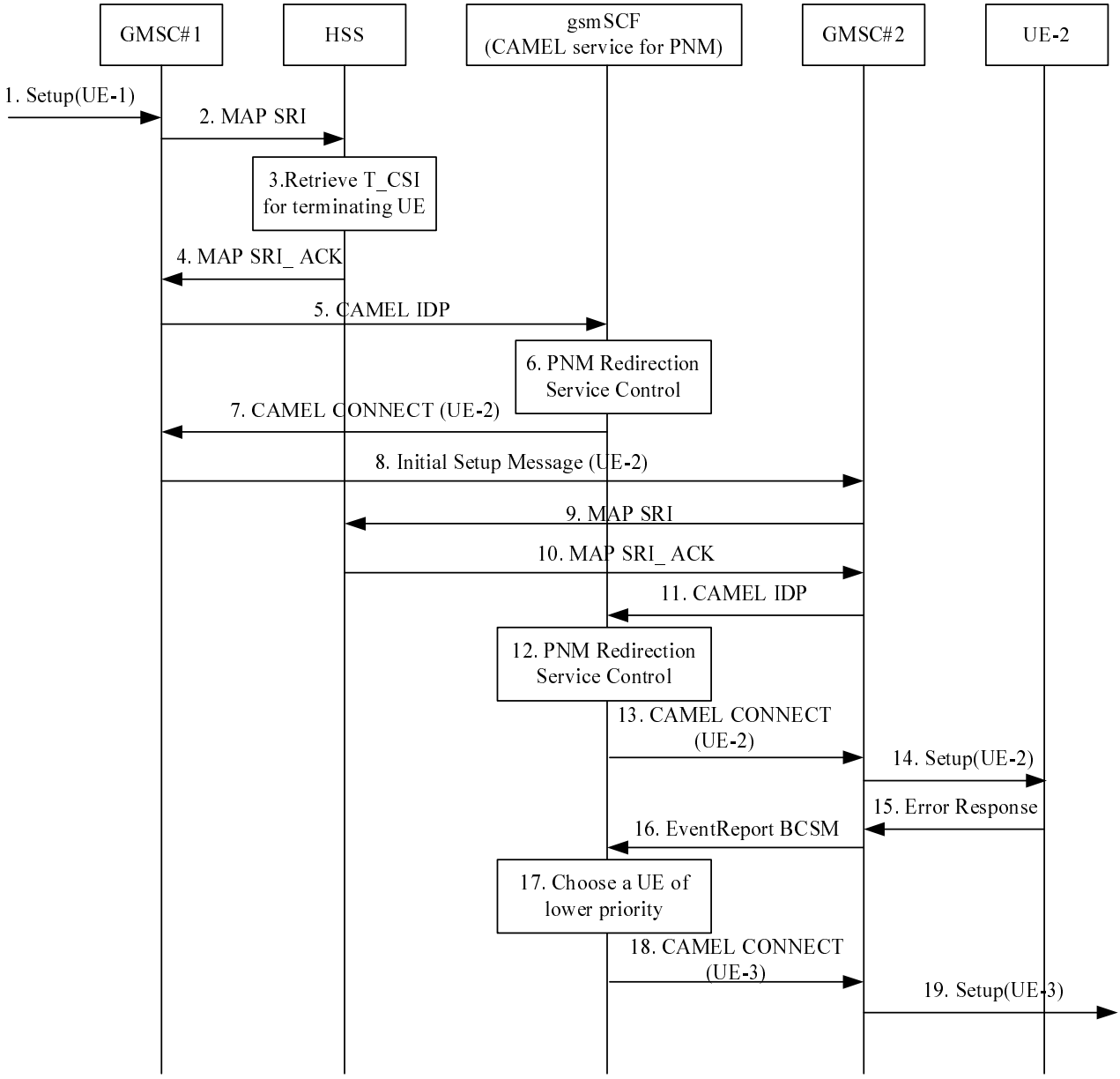

Figure 6.2.2-2: Initial request to UE-1 and redirected to UE-3 by the gsmSCF (CAMEL service for PNM) in the CS domain when the initial request to UE-2 fails

1. A call request to the UE-1 containing the MSISDN of the UE-1 as the called party number arrives at the GMSC #1.

2. On receipt of the incoming call request, the GMSC#1 queries the HSS for routing information.

3. 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.

4. The HSS returns the T-CSI information element to the GMSC#1 in response to the query for routing information (SRI).

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

6. The gsmSCF (CAMEL service for PNM) executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The gsmSCF (CAMEL service for PNM) decides to redirect the call request to the default UE of the PN, i.e., to the UE-2.

7. As a result of the PN UE redirection control logic execution, the gsmSCF (CAMEL service for PNM) to respond to the CAMEL IDP message with a CAMEL CONNECT message containing the MSISDN of the UE-2 as the called party number.

8. The GMSC#1 initiates the CS call towards the GMSC#2 by sending an Initial Setup Message (e.g. ISUP IAM, BICC IAM, and SIP-I Invite).

9-13. The GMSC#2 queries the HSS for routing information and triggers a CAMEL activity to the gsmSCF. The gsmSCF executed the PNM redirection service control logic and decides to forward the request as the UE-2 is the default UE of the PN, so it responds with a CMAEL CONTINUE message to the GMSC#2.

14. The GMSC#2 continues the redirected call request based on the standard call setup procedures as described in 3GPP TS 23.018 [10].

15. UE-2 cannot setup the session and generates an error response.

16. GMSC#2 sends the EventReportBCSM message to the gsmSCF.

17. The gsmSCF executes the PN UE redirection control logic for the other UE of the next lower priority which in this example is UE-3.

18-19. As a result of the PN UE redirection control logic execution, the gsmSCF forwards the redirected initial request containing the MSISDN of the UE-3 as the called party number to the UE-3.

6.3 Procedures and information flows in the domain interworking

6.3.1 General

After the PNM AS executes the redirection of the initial request based on the PN-user"s PN configuration, the initial request could be routed to different domain, i.e. from IM CN subsystem to CS domain or from CS domain to IM CN subsystem.

The procedures for supporting the interworking between IM CN subsystem and CS domain in the PNM session redirection take advantage of the procedures specified in 3GPP TS 23.228 [4].

NOTE: If the UE-2 is attached both in the CS domain and the IM CN subsystem, how the PNM AS selects the particular domain for the PN UE redirection is out of the scope of this document.

6.3.2 Procedures and information flows for PN UE redirection from IM CN subsystem to CS domain

Figure 6.3.2-1 describes the procedures and information flows for handling the PNM Session redirection from IM CN subsystem to CS domain. Without loss of generality, it is assumed for figure 6.3.2-1 that a PN-user"s PN consists of two UEs, i.e., the UE-1 and UE-2 and the UE-2 attached in CS domain doesn"t have the subscription to IMS is the default UE according to PN-user"s PN configuration as described in clause 6.

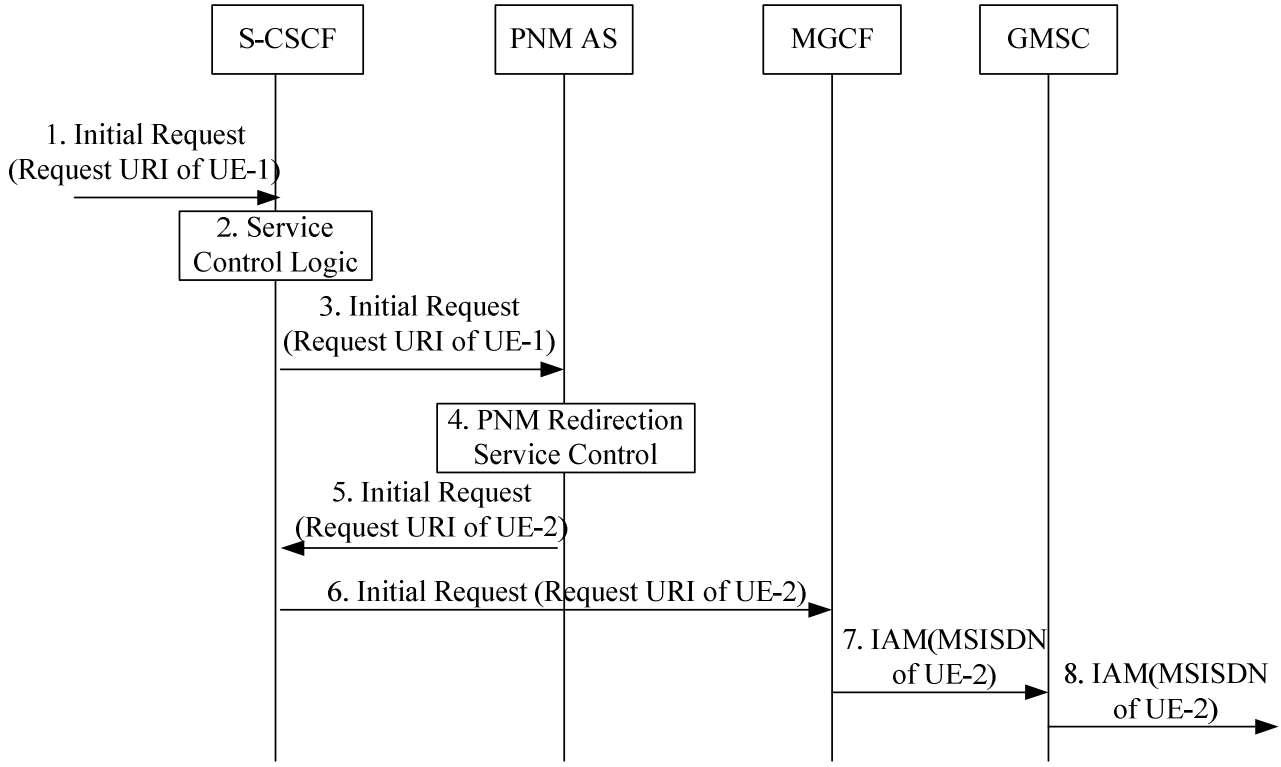

Figure 6.3.2-1: Initial request in IM CN subsystem and redirected to UE-2 in CS domain by the PNM AS

1. An initial request destined to the UE-1 containing the Request-URI of the UE-1 public user identity arrives at the S-CSCF.

2. The S-CSCF determines that the initial request if for a UE-terminated case, invokes the termination service control logic required for the UE-1 and evaluates the initial filter criteria, which results in re-routing the initial request to the PNM AS.

3. As a result of the termination service control logic invocation for the UE-1, the S-CSCF forwards the initial request to the PNM AS.

4. The PNM AS executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The PNM AS decides to redirect the initial request to the default UE of the PN, i.e., to the UE-2 which in this example can be found in the CS domain only.

5. As a result of the PN UE redirection control logic execution, the PNM AS sends the redirected initial request containing the Request-URI of the UE-2 public user identity to the S-CSCF.

6. The S-CSCF treats the redirected request as a UE-originated case and performs the domain transit procedure specified in 3GPP TS 23.228 [4]. Eventually, the session initiation arrives to an MGCF.

7. The MGCF sends an IAM message containing the MSISDN of the UE-2 as the called party number towards GMSC.

8. The GMSC continues the redirected call request based on the standard call setup procedures as described in 3GPP TS 23.018 [10].

6.3.3 Procedures and information flows for PN UE redirection from CS domain to IM CN subsystem

Figure 6.3.3-1 describes the procedures and information flows for handling the PN UE redirection from CS domain to IM CN subsystem. Without loss of generality, it is assumed for figure 6.3.3-1 that a PN-user"s PN consists of two UEs,

i.e., the UE-1 and UE-2 and the UE-2 registered only in IM CN subsystem is the default UE according to PN-user"s PN configuration as described in clause 6.

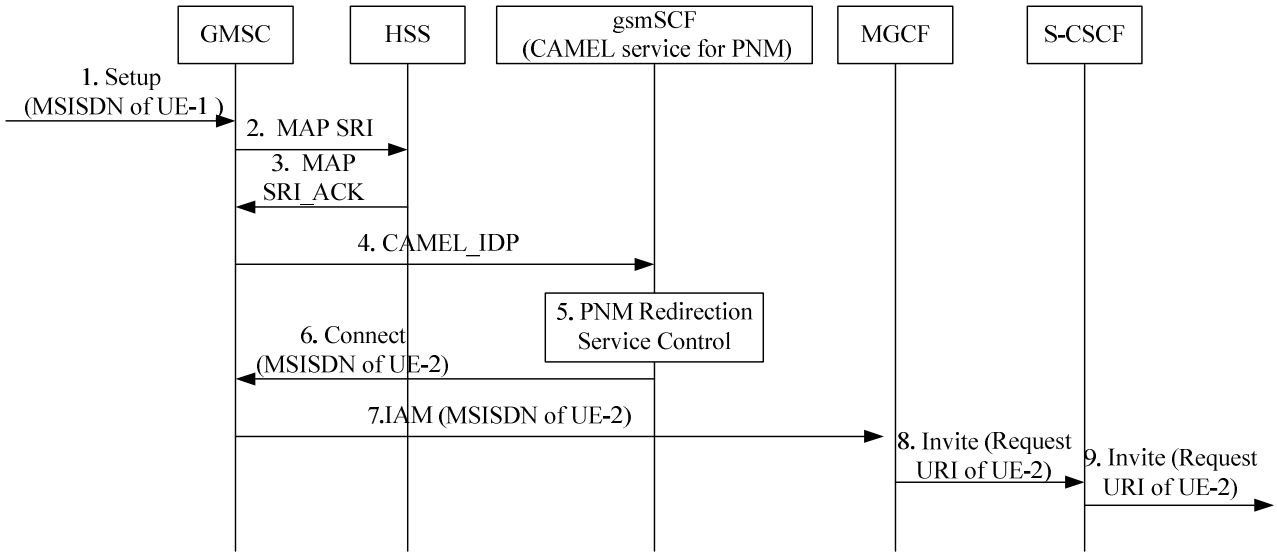

Figure 6.3.3-1: Initial request in CS domain and redirected to UE-2 in IM CN subsystem by the gsmSCF

1. A call request to the UE-1 containing the MSISDN of the UE-1 as the called party number arrives at the GMSC.
2. On receipt of the incoming call request, the GMSC queries the HSS for routing information.
3. The HSS returns the T-CSI information element that contains information configured for the PNM subscriber to the GMSC#1 in response to the query for routing information (SRI).
4. The GMSC triggers a CAMEL activity which results in sending a CAMEL IDP message to the gsmSCF (CAMEL service for PNM).
5. The gsmSCF (CAMEL service for PNM) executes the PN UE redirection control logic based on the PN-user"s PN configurations as described in clause 6. The gsmSCF (CAMEL service for PNM) decides to redirect the call request to the default UE of the PN, i.e., to the UE-2 which in this example can be found in IM CN subsystem only.
6. As a result of the PN UE redirection control logic execution, the gsmSCF (CAMEL service for PNM) responds to the CAMEL IDP message with a CAMEL CONNECT message containing the MSISDN of the UE-2 as the called party number.
7. The GMSC initiates the call to the MGCF with an IAM message containing the MSISDN of UE-2 as the called party number.
8. The MGCF initiates a SIP INVITE request with the request URI of UE-2 public user identity towards the S-CSCF.
9. The S-CSCF continues the redirected initial request based on the standard call setup procedures as described in 3GPP TS 23.228 [4].

7 Procedures and information flows for PN access control

7.1 General

Upon receiving a UE-terminating initial request, the PNM AS shall first check whether the request originates from another PN UE within the same PN as the terminating PN UE and if so the PNM AS shall allow the session establishment to continue. If the request does not originate from another PN UE within the same PN as the terminating PN UE the PNM AS shall invoke the PN access control application if it is enabled. If no access control list exists for the terminating UE, and if the PNM AS does not invoke the PN UE redirection for the terminating UE, the PNM AS sends the initial request to the terminating UE (i.e., a UE of a PN). Otherwise, the PNM AS verifies whether the originating UE of the initial request is a valid entry contained in the PN access control list for the terminating UE, before it initiates session towards the terminating UE. With a successful verification, the PNM AS sends the initial request to the terminating UE. With an unsuccessful verification, if the terminating UE is not a controllee UE, then the PNM AS rejects the initial request. If the terminating UE is a controllee UE, the PNM AS queries the controller UE whether the session to the controllee UE is allowed to be established. If it is allowed, and if the PNM AS does not invoke the PN UE redirection for the terminating UE, the PNM AS sends the initial request to the controllee UE. Otherwise, the PNM AS rejects the initial request. Figure 7.1-1 gives a snapshot of the scenario.

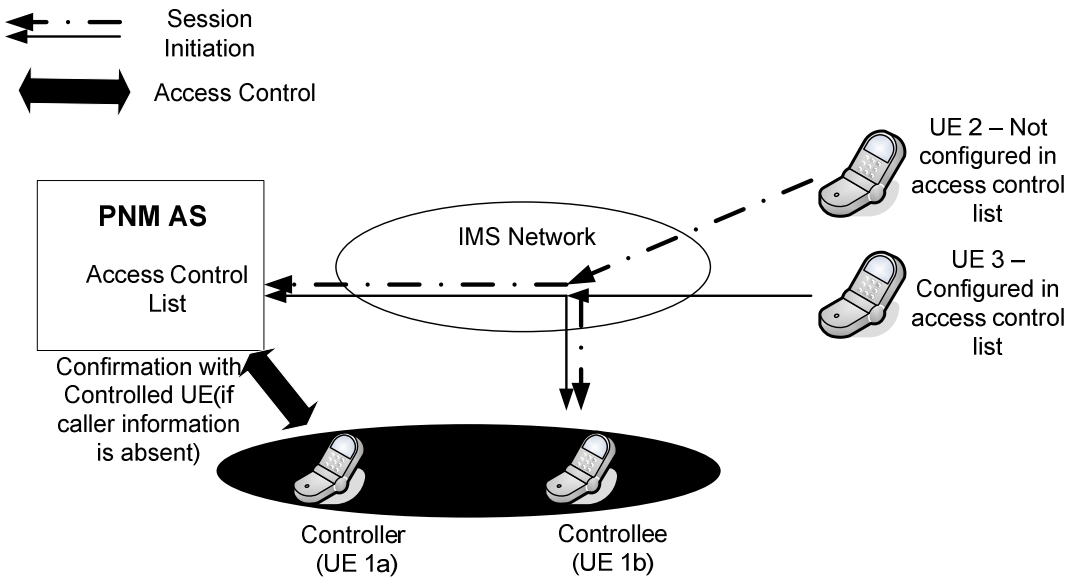

Figure 7.1-1: Overview of privacy based access control Procedures and Information Flows

NOTE: The Solid line refers to access control handled by the PNM AS itself, since the identity of the originating caller is present in the access control list of the PNM AS. The dashed line refers to access control handled by the controller UE when the identity of the caller is not present in the access control list of the PNM AS.

The procedures at the PNM AS to accomplish the PN access control execution are described with the assistance of figure 7.1-2.

When the PNM AS receives a SIP initial request and its PN access control logic is switched-on, if the Request URI of the initial request identifies with the controllee UE(s), the PNM AS shall further decide whether the Request URI uniquely identify a controllee UE within a PN:

1) if a controllee UE is uniquely identifiable, the PNM AS shall check whether the Caller is in the PN access control list;

   a) if the Caller is in the PN access control list, the PNM AS shall send the initial request to the controllee UE;

   b) if the Caller is not in the PN access control list,

i) if there is no need to interrogate the controller UE, the PNM AS shall reject the initial request;

ii) if there is a need to interrogate the controller UE, the PNM AS shall interrogate the controller UE and handle the initial request message based on the interrogation results from the PN-user.

Editor's note: The use of GRUU as described in 3GPP TS 23.228 [4] can assist the PNM AS with uniquely identifying a controllee UE.

2) if a controllee UE is not uniquely identifiable, the PNM AS shall perform the PN access control without invoking the controller UE (i.e., without any PN-user interaction) and check whether the Caller is in the PN access control list;

a) if the Caller is in the PN access control list, the PNM AS shall send the initial request back to the S-CSCF (see 3GPP TS 23.228 [4]);

b) if the Caller is not in the PN access control list, the PNM AS shall reject the initial request.

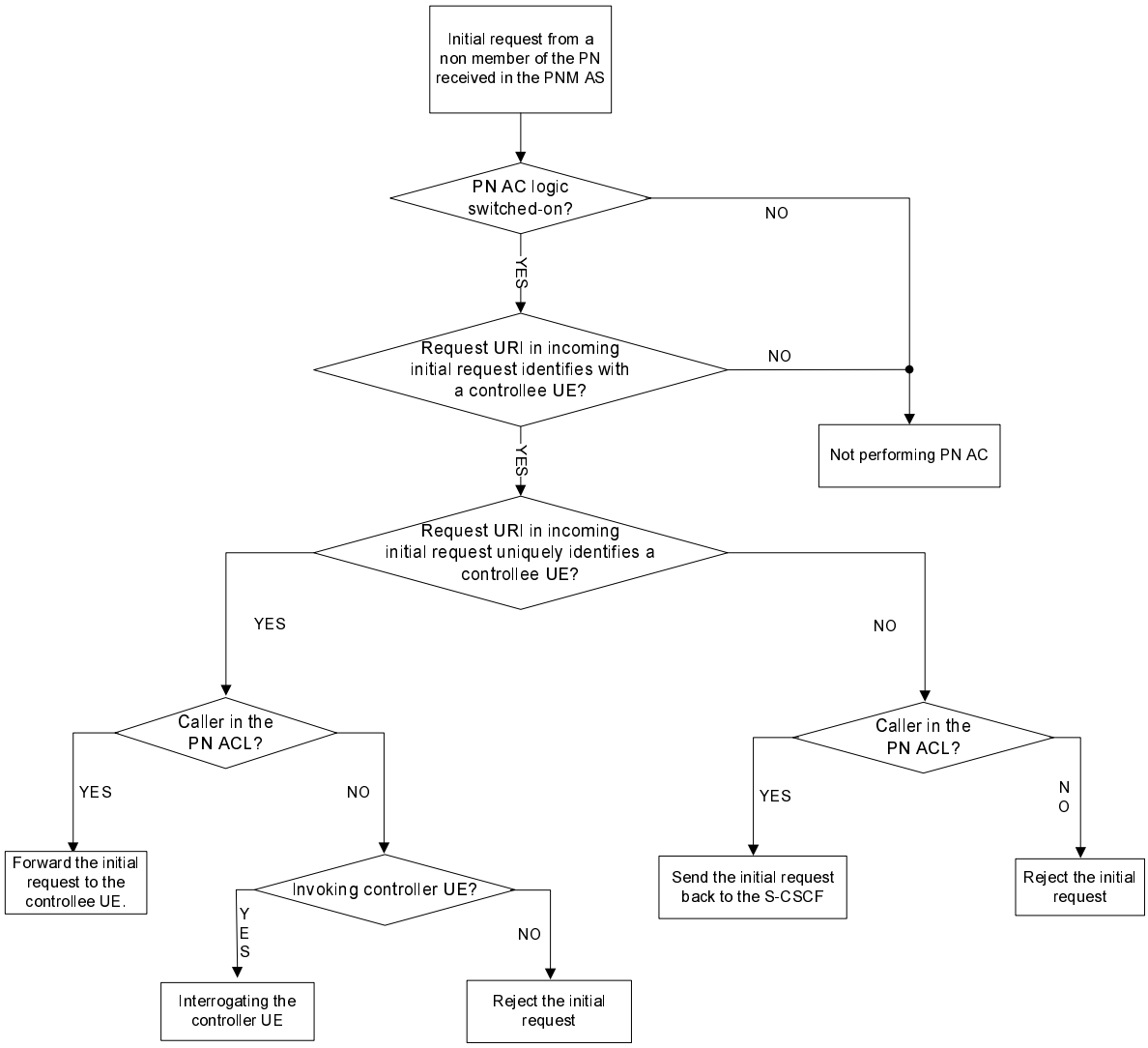

Figure 7.1-2: PN access control execution flow at the PNM AS (AC and ACL stand for Access Control and Access Control List, respectively)

7.2 PN access control procedures in the IM CN subsystem

Without lack of generality, the following assumptions have been made with respect to the terminals and the network.

<Assumptions related to identities of UEs>

- PN-user 1 has two UEs – UE 1a & UE 1b in the PN, containing identities user1_public1@home1.net and user1_public2@home1.net respectively, and having a subscription with the home network providing PNM service.
- UE 1b is configured as controllee UE and UE 1a as controller UE by the PN-user 1.
- The originating UE which initiates the request may belong to the same/different network where the PNM AS is located. The originating UE of the initial request needs not be aware of the setting of the access control done by PN-user 1.
- PN-user 1has configured UE2 with user2_public@home2.net as the only entry in the access control list related to the controllee UE in this example. When the PNM AS receives initial requests not coming from UE2, the PNM AS can query the controller UE and the continuation of the initial request depends on the outcome of the query.
- The following table summarizes the above assumptions.

Table 1: Example of a simple access control table PN

PN Of user	controllee UE	controller UE	Access List entries
(UE 1a) user1_public1@home1.net	No	N/A	N/A
(UE 1b) user1_public2@home1.net	Yes	UE 1a	(UE 2) user2_public@home2.net

<Network assumptions>

- PN-user"s home network provides PN access control, which allows PN-users to configure identities (e.g., a SIP URI) which are permitted to initiate sessions to the UE of the PN.
- This service is hosted by the PNM Server which is a SIP application server, serving scscf#1.
- For simple illustration, in this example, both identities of the PN are shown to be registered with the same S-CSCF (S-CSCF#1) to improve efficiency in signalling, which might be the case in most implementations.
- The PNM AS stores access control lists of controllee UE and the controller UE can process access control requests during dynamic procedures.

UE 3 sends an initial request to UE 1b (user1_public2@home1.net). But, UE 3 hasn"t been configured by the PN-user in the access control list. Therefore, the PN MAS queries the controller UE (i.e., UE 1a) about the information as to how to process this initial request.

7.3 PN access control procedure in the IM CN subsystem

7.3.1 General

An inherent problem in the Access control list case is the need for the PN-user to configure each originating UE that the PN-user feels appropriate. This may not be a scalable solution where tens of UEs may try to access the controllee UE. In order to solve this problem, the PN-user may configure a controller UE, after processing of this decision normal session initiation procedures may be continued. Once the controller UE has been chosen, to handle all session initiation requests from UEs whose identities are not configured in the access control list, a query can be directed to the particular controller UE.

The controller UE in turn is capable of checking the access control information of this query. Options may be given to the PN-user to either accept the call himself, or answer the query by allowing the call to go through to the intended destination (controllee UE) or deny the call. In addition the user may be given an option of saving this policy for future call requests by the same source. Once the user makes the decision, a response message carrying this information may be sent directing the session back to the original destination.

The PNM AS receives the response message from the S-CSCF. If the decision of the PN-user was to allow the call, it sends the original initial request message. If required to save (based on user response) it saves the settings for the originating UE in the access control list

7.3.2 PN access control based on query logic in the IM CN subsystem

In figure 7.3.2-1 it is assumed that the originating UE (i.e., UE 3) is not configured in the access control list of the controllee UE (i.e., UE 1b). When the PNM AS receives an Initial Request from S-CSCF# 1, the PNM AS verifies whether UE 3 matches an entry in the access control list of UE 1b. In this case, the PNM AS sends a Query to the controller UE1a to determine the handling.

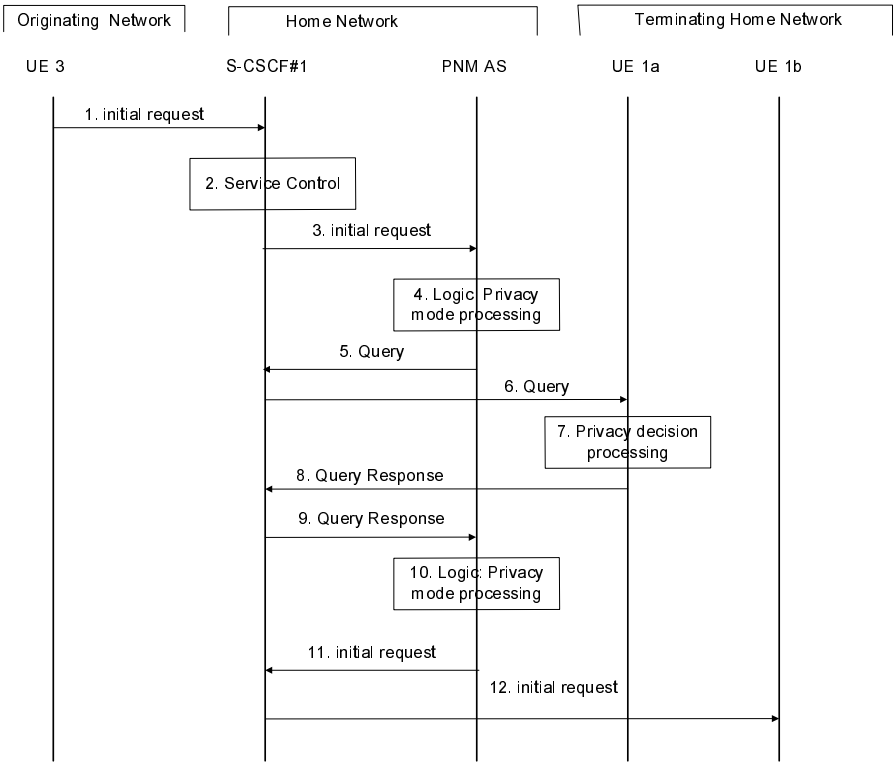

Figure 7.3.2-1: High level sequence of PN access control

1. UE 3 sends an Initial Request towards UE 1b.
2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt.

3. In this case, the initial filter criterion is triggered and the initial request message is forwarded to the corresponding PNM AS.

4. The PNM AS receives the initial request and the privacy mode processing is executed.

   The PNM AS extracts the source and destination addresses. It confirms that the destination UE is a controllee UE. Using this as a key, it searches its database for the particular PN to find if UE 3 is configured in the access control list as allowed to initiate sessions with UE 1b.

   If the originating UE has been configured in the access control list, normal processing is continued. If there is no information regarding the address of the originating UE, the PNM AS may then send a Query to the controller UE, i.e., UE 1a in this example, containing the access request of UE 1b by UE 3. This Query can be processed by UE 1a.

5. As a result of Step 4, the PNM AS queries the controller UE about the information of how to precede with the Initial Request by sending a Query to S-CSCF#1.

6. S-CSCF#1 validates the service profile, and invokes any termination service logic required for UE 1a and forwards the Query to UE 1a.

7. In the privacy decision processing, the information contained in the Query is indicated to the PN-user. (Example: UE 3 calling UE 1b, 1: Allow, 2: Deny 3: Allow and save policy 4: Deny and save policy 5: Accept). The PN-user may then allow/disallow and possibly save this option for future calls. This information is sent in the Query Response.

8. The decision of the user is sent in the Query Response.

9. The S-CSCF#1 forwards the Query Response towards the PNM AS.

10. In the privacy response processing step, the PNM AS determines the action directed by the user. If the PN-user has allowed the Initial Request to pass to the UE 1b, the Initial Request is sent to UE 1b.

NOTE 1: If the user has chosen to save the policy, the policy is stored in the access control list of the controllee UE using the PN-configuration procedure.

11. The PNM AS sends the original Initial Request to the S-CSCF#1

12. The S-CSCF#1 forwards the initial request message to UE 1b.

NOTE 2: Interaction with other services; The privacy service is to authorize the call where the authorization apart from normal authorization procedures involved in the network, requires real time consent from the user. All other supplementary features or other services may follow once this authorization is received.

7.3.3 PN access control based on access control lists

In figure 7.3.3-1 it is assumed that the originating UE (i.e., UE 2) is configured in the access control list of the controllee UE (i.e., UE 1b). When the PNM AS receives an Initial Request from S-CSCF# 1, the PNM AS verifies whether UE 2 matches an entry in the access control list of UE 1b. In this case, the PNM AS sends the Initial Request message to UE 1b.

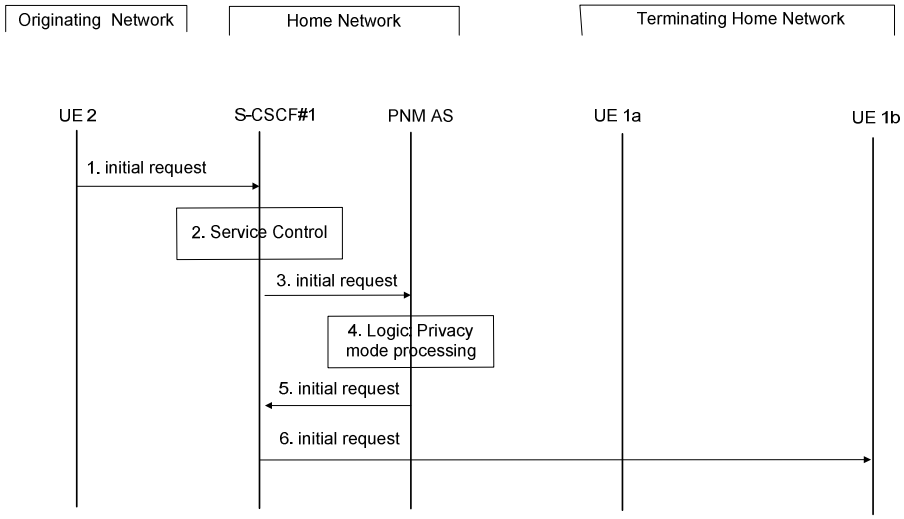

Figure 7.3.3-1: PN access control in case of PNM AS alone

1. S-CSCF#1 receives an Initial Request from UE 2 to UE 1b.
2. S-CSCF#1 invokes the termination service control logic required for the UE 1b and evaluates the initial filter criteria.
3. S-CSCF#1 forwards the Initial Request to the PNM AS as a result of executing the initial filter criteria.
4. In the privacy mode processing step, the PNM AS extracts the source and destination addresses. It confirms that UE 1b is a controllee UE. Using this as a key, it searches its database for the PN of UE 1b to find if UE 2 is configured in the access control list. In this case, it is assumed that UE 2 is allowed to initiate sessions with UE 1b.
5. The PNM AS sends the Initial Request message to the S-CSCF#1.
6. The S-CSCF#1 routes the Initial Request message to the UE 1b.

In figure 7.3.3-2 it is assumed that the originating guest UE (i.e., UE 2) is configured in the access control list of the controllee PNE (i.e., PNE-1). UE1b and PNE-1 form a PAN. When the PNM AS receives an Initial Request from S-CSCF# 1, the PNM AS verifies whether UE 2 matches an entry in the access control list of PNE-1. In this case, the PNM AS sends the Initial Request message to the PNE-1 via UE 1b.

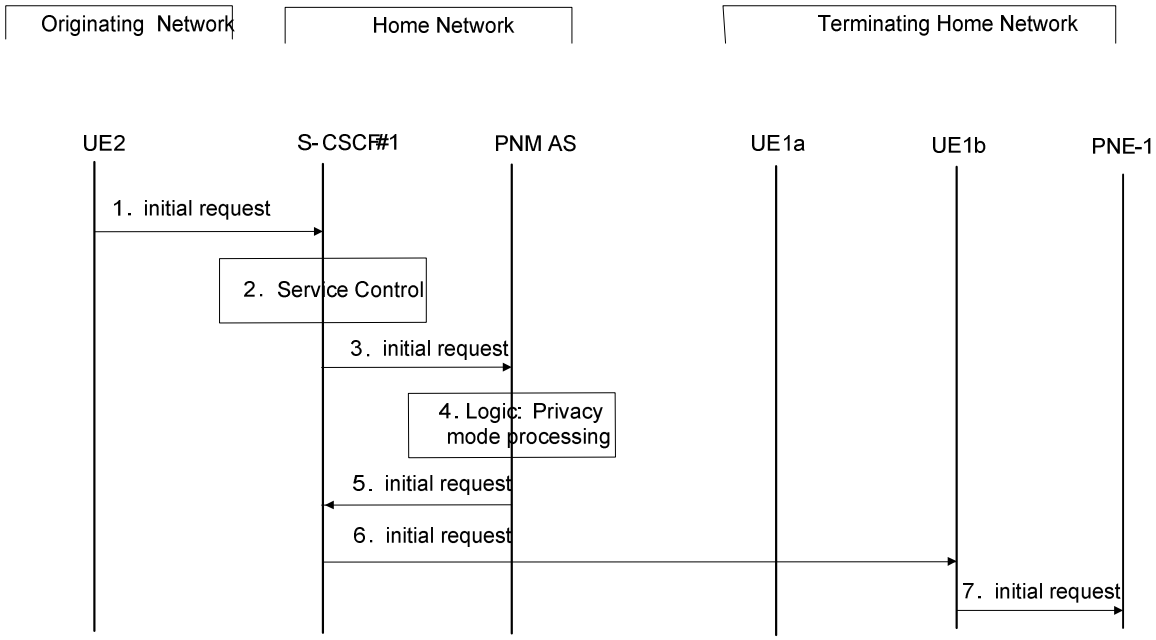

Figure 7.3.3-2: PNE access control

1. S-CSCF#1 receives an Initial Request from UE 2 containing the identity of PNE-1.
2. S-CSCF#1 invokes the termination service control logic required and evaluates the initial filter criteria.
3. S-CSCF#1 forwards the Initial Request to the PNM AS as a result of executing the initial filter criteria.
4. In the privacy mode processing step, the PNM AS extracts the source and destination addresses. It confirms that PNE-1 is a controllee PNE. Using this as a key, it searches its database for the PN of PNE to find if UE 2 is configured in the access control list. In this case, it is assumed that UE 2 is allowed to initiate sessions with PNE-1.
5. The PNM AS sends the Initial Request message to the S-CSCF#1.
6. PNE-1 accesses the network via UE1b, then the S-CSCF#1 routes the Initial Request message to the UE 1b.
7. The UE1b sends the Initial Request message to the PNE-1 via the PAN internal interface.

7.4 PN access control procedure in the CS domain

7.4.1 General

PN access control deals with a user having access control over his Personal Network, wherein he may restrict access to his UEs. These UEs of the PN, over which access control has been enabled, are configured as controllee UE. To initiate sessions with these controllee UEs, the originating UEs need to be configured by the PN-user in a PN access control list. For information regarding the originating UEs that are configured in the PN access control list, which is the case in majority of the scenarios, the user nominates a controller UE to handle the access control. In this case, the network queries the user whether the call to the controllee UE may be allowed to go through. If the user allows it, the network allows the call to go through.

7.4.2 PN access control procedure (When the caller is not in the PN access control list)

If the caller is not in the PN access control list the gsmSCF interacts with the controller UE in order to route the call to the Controllee UE. Figure 7.4.2-1 shows the implementation of access control procedure in CS domain when the caller is not in PN access control list.

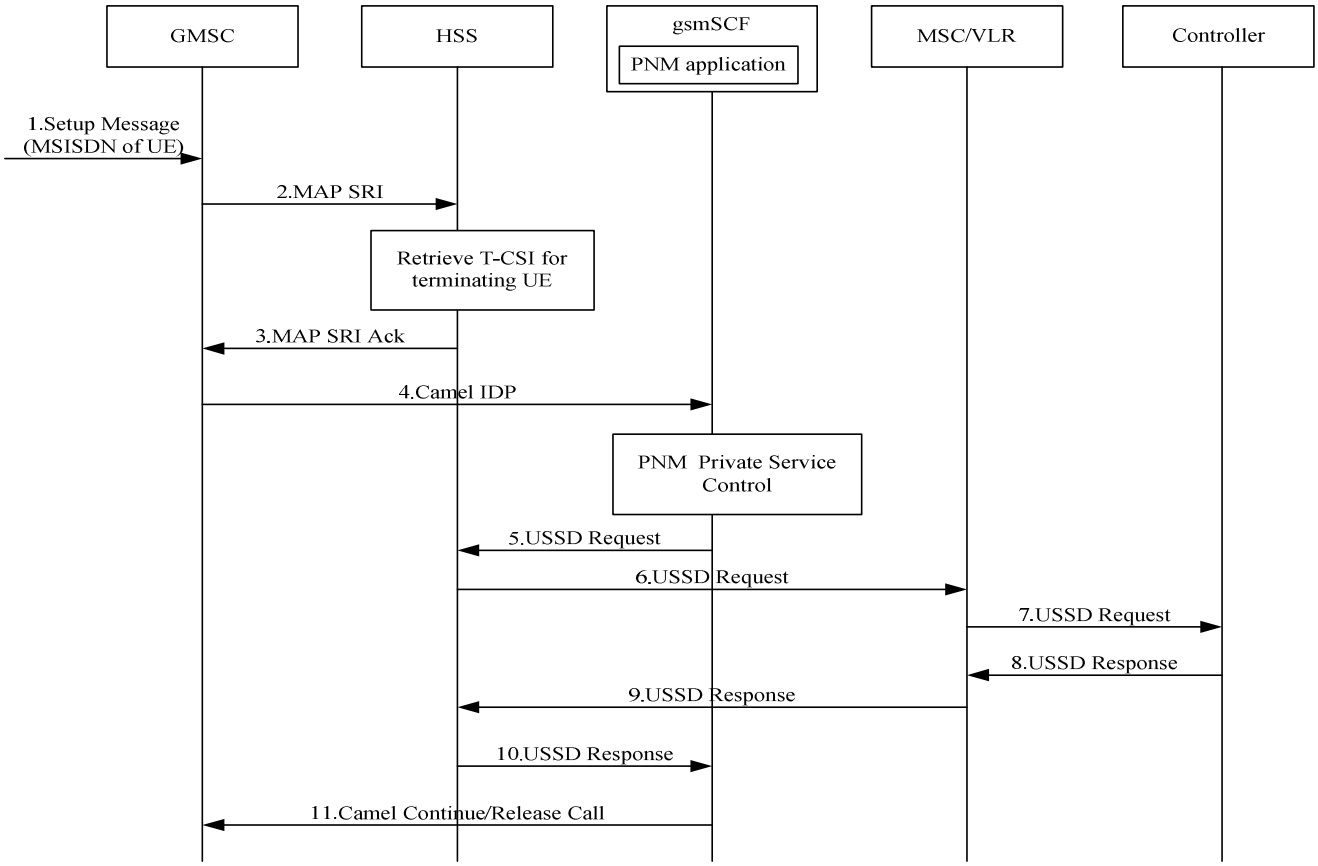

Figure 7.4.2-1: PN access control Procedure in CS domain

1. A call request to the UE located in PN containing the MSISDN of the UE arrives at the GMSC.
2. GMSC queries the HSS for routing Information by sending MAP SRI.
3. HSS checks the subscription information for the called party. Further the HSS provides the information for the PNM subscriber including the T-CSI. The HSS returns the T-CSI to the GMSC in the response (MAP-SRI-ACK)

4. The GMSC triggers a CAMEL activity which results in sending a CAMEL IDP to gsmSCF.

5-7. The gsmSCF executes the PN access control logic and will check with the controller UE about the acceptability of call request by sending USSD request message to the controller UE via HSS and MSC/VLR.

NOTE: This USSD message includes the call Information such as the public user Identity of caller and terminating UE.

8. The controller UE displays the text provided and awaits user input. The user decides whether the call request is allowed or not and accordingly the controller UE will send the USSD response message to MSC/VLR.

9-10. The MSC/VLR will forward this USSD response message to gsmSCF via HSS.

11. The gsmSCF will continue the call or release the call by sending the CAMEL continue message/release call message to the GMSC according to the controller UE"s response Based on the decision by the controller UE the call will established or released.

Figure 7.4.2-2 provides a solution for the time delay problem which can occur during interaction between the network and the controller UE.

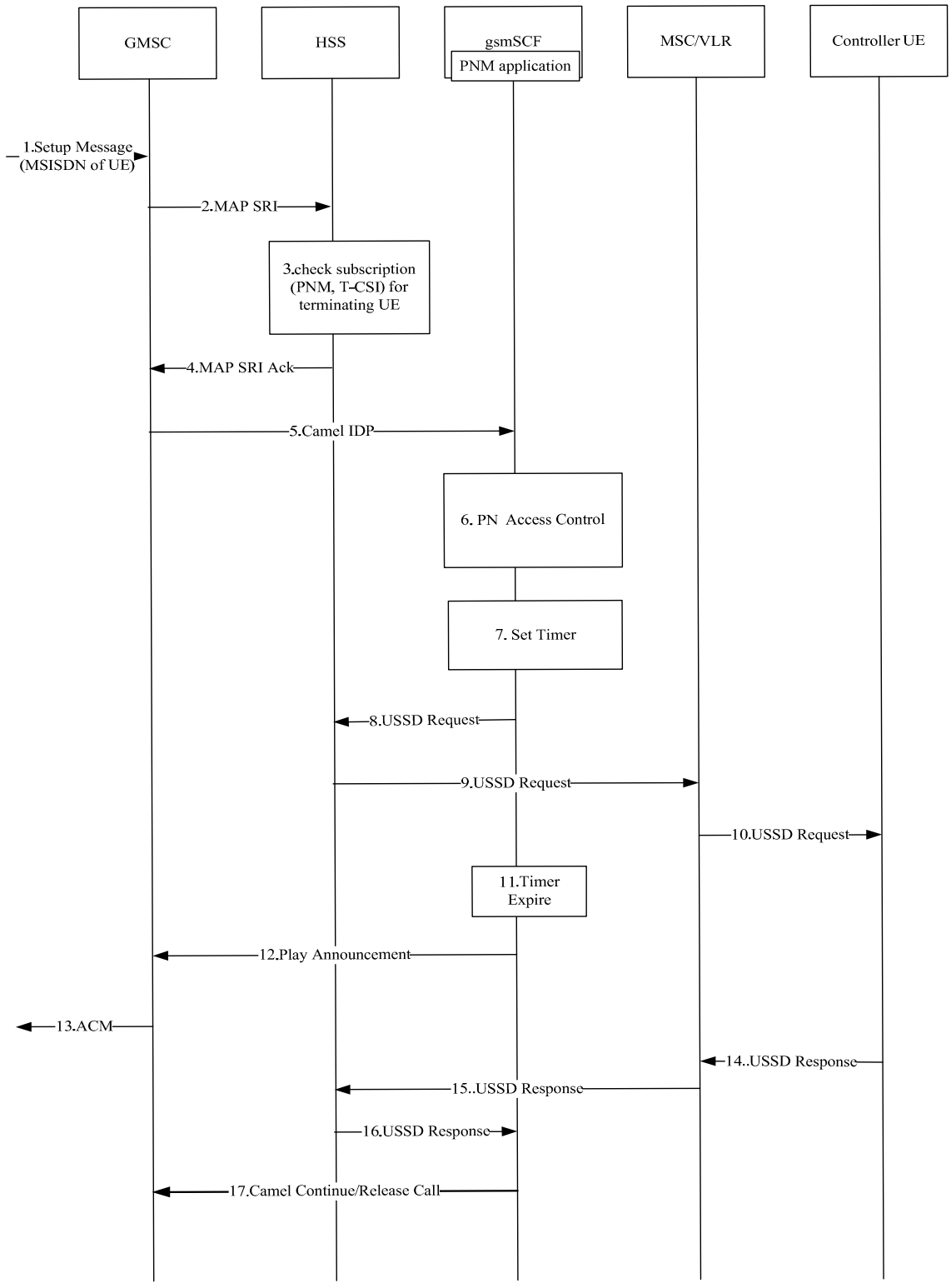

Figure 7.4.2-2: PN access control procedure in CS domain with delay handling.

1. A call request to a UE containing the MSISDN of the UE arrives at the GMSC.

2. The GMSC queries the HSS for routing Information by sending MAP SRI.

3-4 The HSS checks the subscription information for the called party. Further the HSS provides the information for the PNM subscriber including the T-CSI. The HSS returns the T-CSI to the GMSC in the response.

5. The GMSC triggers a CAMEL activity which results in sending a CAMEL IDP to gsmSCF.

6. & 8-10 The gsmSCF executes the PN access control logic and will check with the controller UE about the acceptability of the call request by sending USSD request message to the controller UE via HSS and MSC/VLR.

NOTE: This USSD message includes the call Information such as the public user Identity of the originating and the terminating UE.

7. The gmsSCF will start the Timer.

11. Supervision of the started timer by the gsmSCF.

12-13. If the time out occurs because no response from the controller UE, the gsmSCF will send the Play Announcement message to the GMSC and the GMSC will send an early ACM to the originating UE.

NOTE: Step 12-13 can be skipped if the controller UE responds before timer out occurs. No ACM will be send.

14. The controller UE displays the text provided and awaits user input. The user decides whether the call request is allowed or not and accordingly the controller UE will send the USSD response message to MSC/VLR.

15-16. The MSC/VLR will forward this USSD response message to the gsmSCF via the HSS.

17. The gsmSCF will send a message to GMSC to stop playing the announcement if it is generated. The gsmSCF will continue the call or release the call by sending the CAMEL continue message/release call message to the GMSC according to the controller UE"s response.

7.4.3 PN access control procedure in CS domain (When the caller is in the PN access control list)

Figure 7.4.3-1 shows the PN access control procedure when the caller is in PN access control list.

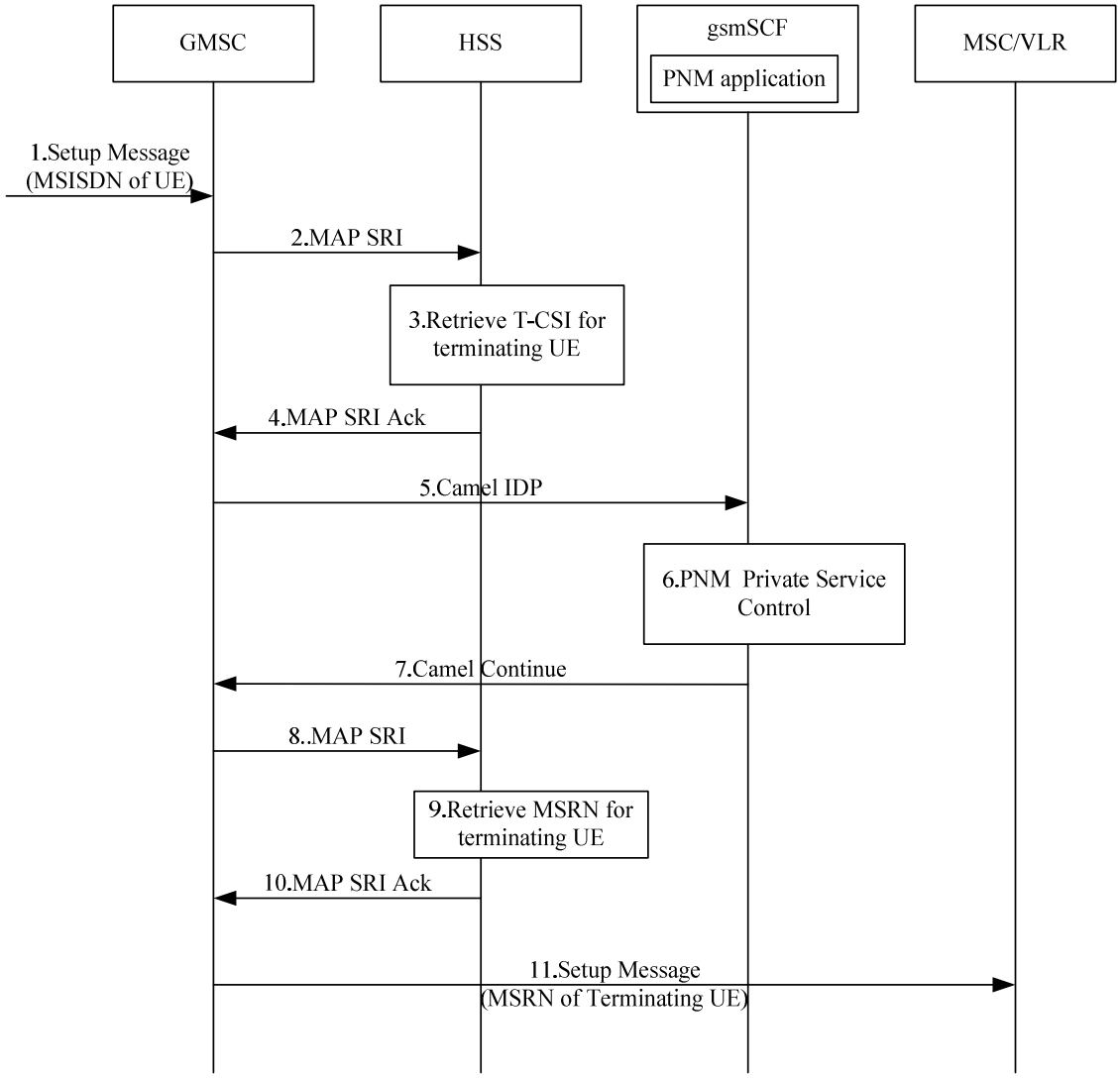

Figure 7.4.3-1 PN access control procedure in the CS domain (Caller is in the PN access control list)

1. A call request to the PN UE containing the MSISDN of the UE arrives at the GMSC.
2. The GMSC queries the HSS for routing Information by sending MAP SRI.

3-4. The HSS checks the subscription information for the called party. Further the HSS provides the information for the PNM subscriber including the T-CSI. The HSS returns the T-CSI to the GMSC in the response.

5. The GMSC triggers a CAMEL activity which results in sending a CAMEL IDP to gsmSCF.
6. The gsmSCF executes the PN access control logic for access control procedure. The calling party is part of the access control list for this PN.
7. Based on the positive result, the gsmSCF send the CAMEL CONTINUE message to GMSC to continue the call.
8. The GMSC queries the HSS for routing Information by sending MAP SRI with 'Suppress T-CSI' set.
9. The HSS returns the retrieved MSRN to the GMSC in response by sending MAP SRI_ACK.
10. The GMSC generates a call request message containing MSRN and sends it to MSC/VLR.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2007-02					Skeleton of the TS (C1-070122)	-	0.0.0
2007-02					Version 0.1.0 created as a result of incorporating the following contributions at CT1#45. C1-070568 - Personal UE Networks management -UE registration procedure C1-070569 - Personal UE Networks Management - UE activation procedure	0.0.0	0.1.0
2007-03					Version 0.2.0 created as a result of incorporating the following contributions at CT1#46. C1-070655 - CR against TS 23.259 Clause 2 References C1-070661 - CR against TS 23.259 Clause 6-tide-up C1-070896 - CR against TS 23.259 Clause 4 PNM overview C1-070897 - CR against TS 23.259 Clause 5.1 Procedures & Information Flow C1-070898 - CR against TS 23.259 Clause 5.2 Procedures & Information C1-070900 - CR against TS 23.259 Clause 3 Definitions and Abbreviations C1-070906 - CR against TS 23.259 Clause 6.4 C1-071005 - CR against TS 23.259 Clause 7 Procedures and Information Flows for Private Network Services	0.1.0	0.2.0
2007-05					Version 0.3.0 created as a result of incorporating the following contributions at CT1#47. C1-071073 - Discussion on no re-invoking of PNM AS after session/call redirection C1-071312 - CR against TS 23.259 Clause 6.3 Procedures and Information Flows for PN-Configuration in CS domain C1-071348: - PN-Configuration Procedure C1-071472 - CR against TS 23.259 Clause 5.2 Procedures and Information Flows for call redirection in CS domain C1-071473 - PN-Registration Procedure	0.2.0	0.3.0
2007-08					Version 0.4.0 created as a result of incorporating the following contributions at CT1#48. C1-071645 - PNM private network service C1-072004 - CR against TS 23.259 Clause 6.1.3 Procedures and Information Flows for PN-Registration and PN-Deregistration in CS Domain C1-072007 - CR against TS 23.259Procedures and Information Flows for Domain Interworking in PNM Session Redirection C1-072010 - PNM IMPI C1-072011 - PNM Query C1-072100 – Information message in PNM message C1-072101 - Clarification to UEs in the Configuration Request C1-072171 - Access control procedures in the CS domain	0.3.0	0.4.0
2007-09					Version 1.0.0 created for presentation to TSG	0.4.0	1.0.0

2007-10					C1-072242 - Overview of PNM in the CS domain C1-072543 - No Re-invoking of PNM CAMEL service after Session Redirection in the CS domain C1-072544 - No Re-invoking of PNM AS after Session/Call Redirection in the IM CN subsystem C1-072547 - PN Access Control List Configuration C1-072548 - Access Control in CS domain(Caller is in Access List) C1-072694 - TS23.259-100-cleanup C1-072719 - Information Message in CS domain C1-072720 - Access Control Procedure in CS domain to Avoid the Call release	1.0.0	1.1.0
2007-11					C1-072780 - TS 23.259 Subclause 7.4 update CS domain C1-073086 - PN-registration C1-073087 - PN-configuration C1-073088 - Cleanup C1-073090 - GRUU in reg event package C1-073091 - Using GRUU in the PN UE redirection C1-073092 - PN UE redirection based on UE priority	1.1.0	1.2.0
2008-02					C1-080187 - PN Configuration Procedures Editorials C1-080188 - PN Registration and Configuration Restructuring C1-080237 - Clause 6 Update C1-080458 - Clarifying PNM Scope C1-080461 - Error procedures for the priority handling of the session redirection in IMS C1-080462 - Error procedures for the priority handling of the session redirection in the CS domain C1-080463 - PN Configuration Consolidation C1-080465 - PNM AC Logic C1-080573 - PN Access Control Cleanup	1.2.0	1.3.0
2008-03	CT#39	CP-080076			Version 2.0.0 created by MCC for presentation to CT#39 for approval	1.3.0	2.0.0
2008-03					Version 2.0.0 approved in CT#39 and version 8.0.0 created by MCC for publication	2.0.0	8.0.0
2008-06	CT#40	CP-080352	0004	1	Domain Interworking Update	8.0.0	8.1.0
2008-12	CT#42	CP-080859	0005	3	PNM Closed User Group functionality	8.1.0	8.2.0
2008-12	CT#42				Editorial clean up by MCC	8.1.0	8.2.0
2009-06	CT#44	CP-090431	0007	1	Scope of Rel-9 TS 23.259	8.2.0	9.0.0
2009-09	CT#45	CP-090683	0009	1	Procedures of TE registration	9.0.0	9.1.0
2009-09	CT#45	CP-090683	0010	1	Procedures of PNE configuration	9.0.0	9.1.0
2009-09	CT#45	CP-090683	0011	1	Definitions Update	9.0.0	9.1.0
2009-09	CT#45	CP-090683	0012	1	Procedures of PNE redirection	9.0.0	9.1.0
2009-09	CT#45	CP-090683	0013	1	Procedures of PNE Access Control	9.0.0	9.1.0
2009-12	CT#46	CP-090924	0014	1	Corrections to TS 23.259	9.1.0	9.2.0
2009-12	CT#46	CP-090924	0015	1	Editorial corrections	9.1.0	9.2.0
2009-12	CT#46	CP-090924	0022	2	Addition of PN-deregistration procedure for PNE	9.1.0	9.2.0
2009-12	CT#46				Editorial cleanup by MCC	9.1.0	9.2.0

History

Document history		
V9.2.0	January 2010	Publication