ETSI TS 124 259 V17.0.0 (2022-05)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Personal Network Management (PNM);
Stage 3
(3GPP TS 24.259 version 17.0.0 Release 17)**

Reference
RTS/TSGC-0124259vh00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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] Void.

[5] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

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

[7] Void.

[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 (November 2005): "An Extension to the Session Initiation Protocol (SIP) for Request History Information".

[17] IETF RFC 4458 (April 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".

[21] IETF RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[22] IETF RFC 7254 (May 2014): "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

[23] IETF RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[24] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[25] IETF RFC 7231 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

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)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.259 [2] apply:

Personal Areal Network (PAN)
Personal Network (PN)
Personal Network Element (PNE)
PNE Identifier

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
IMEI	International Mobile Equipment Identity
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
PNE	Personal Network Element
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
URN	Uniform Resource Name
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 consist of the PN 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 redirection is a PNM application that enables redirecting a session addressed to any of the UEs belonging to the PN to a certain UE or a certain PNE other than a PN UE of their PN, i.e., the default UE or default PNE other than a PN 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 or certain PNEs other than PN 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; and
- 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) according to the TLS profile specified in 3GPP TS 33.310 [24] annex E.

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.

The AS implementing PNM application shall remove g.3gpp.pne-id media feature tag containing IMEI included in the Contact header field of requests and responses of SIP methods other than the SIP REGISTER method prior to forwarding the request or response to the destination.

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, or a PNE is added to the PAN. 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 a g.3gpp.iari_ref feature tag containing the IARI value defined in subclause 10.4.

Upon receiving a REGISTER request sent from a PNE other than a PN UE via the PAN internal interface, the PN UE shall initiate a SIP REGISTER request as defined in 3GPP TS 24.229 [3] subclause 5.1.1.2.1 with the following addition:

1) including in the Contact header field a g.3gpp.pne-id media feature tag containing the PNE identifier defined in subclause 6.4.

If using the multiple registrations mechanism for registering each PNE, the PN UE shall use a different "reg-id" value when registering the PNE.

If using SIP re-registration procedures for registering another PNE, the PN UE includes a Contact header field for each registered PNE in the SIP REGISTER request.

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 and the 200 (OK) response to the incoming REGISTER request 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 registered PN UE or the registered PNE identifier 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 a USSD Notify message to the HSS to inform the user.

6.4 Definition of media feature tag g.3gpp.pne-id

Media feature-tag name: g.3gpp.pne-id

ASN.1 Identifier: 1.3.6.1.8.2.8

Summary of the media feature indicated by this tag: This media feature-tag when used in a SIP request or a SIP response indicates the identifier of a PNE other than a UE.

Values appropriate for use with this feature-tag: URN. When an IMEI is available, the URN shall take the form of a IMEI URN (see IETF RFC 7254 [22]). If no IMEI is available, the URN shall take the form of a string representation of a UUID as a URN as defined in IETF RFC 4122 [23].

The feature-tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-tag is most useful in a communications application, for describing the capabilities of a device, such as a PC or PDA.

Examples of typical use: Indicating the identifier of a device which is part of a Personal Area Network.

Related standards or documents: 3GPP TS 24.259: "Personal Network Management (PNM), stage 3".

Security Considerations:

UE is not allowed to include g.3gpp.pne-id media feature tag containing IMEI in the Contact header field of requests and responses of SIP methods other than the SIP REGISTER method except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the g.3gpp.pne-id media feature tag prior to forwarding the request or response to the destination. Other security considerations for this media feature-tag are discussed in subclause 12.1 of IETF RFC 3840 [21].

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: A text string together with angled brackets (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 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-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 field 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 for 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 PNE redirection purpose, the XML body of the HTTP PUT request message shall contain:

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

NOTE: A PN user decides the value of the <RedirectionLevel> element based on the PNE 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 <PNERedirection> shall be populated with the GRUU of the PNE configured by the PNE 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 creating/replacing the XML document for the PNE access control purpose, the XML body of the HTTP PUT request message shall contain:

- the <ControllerUE> containing the children <PNUEID> and <PNUEName>, the <ControlleePNE> with a unique value for the "id" attribute containing children <PNUEID>, <PNEID> and <PNEName>, 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>

NOTE: The PNE here stands for the PNE other than a PN UE, i.e. ME, MT or TE of a PAN.

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 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 a HTTP PUT request or a HTTP DELETE request message, the PNM application verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key material Ks_NAF obtained from the 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 of an 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;