ETSI TR 187 015 V3.1.1 (2011-05)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Prevention of Unsolicited Communication in the NGN

Reference

DTR/TISPAN-07034-NGN-R3

Keywords

architecture, security

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

Contents

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 Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document describes a Prevention of Unsolicited Communications (PUC) service for use in the NGN.

The present document defines the method by which a terminating party is prevented from receiving UC. The present document addresses the NGN objectives (including the legal implications) that are met by the PUC service and identifies the requirements to be met by the NGN for PUC. The present document derives from TR 187 009 [i.11].

The present document covers deployment of the NGN in the following scenarios:

- Home networks, focusing on interconnection from the CNG with the NGN and interaction between the CNG and CND. And proposing UC detection & handling on the CNG.
- Enterprise networks, focusing in interconnection between the NGCN and the NGN and the interaction between the UE and the NGCN and NGN. And proposing UC detection and handling for NGCN devices.
- Single user scenario, focusing on interconnection between the UE and the NGN and proposing a UC detection & handling framework for entities of the NGN.

NOTE: The specification of PUC for Common IMS are defined in 3GPP 33.937 [i.12].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.3] ETSI TS 181 005 (V3.2.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[i.4] ETSI TS 124 604 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.604 version 8.2.0 Release 8)".

[i.5] ETSI TS 124 607 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.607 version 8.2.0 Release 8)".

[i.6] ETSI TS 124 608 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR)using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.608 version 8.2.0 Release 8)".

[i.7] ETSI TS 124 611 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Anonymous Communication Rejection (ACR) and Communication Barring (CB)using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.611 version 8.2.0 Release 8)".

[i.8] ETSI TS 124 616 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Malicious Communication Identification (MCID) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.616 version 8.2.0 Release 8)".

[i.9] ETSI TS 124 654 (V8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Closed User Group (CUG) using IP Multimedia (IM) Core Network (CN) subsystem, Protocol Specification (3GPP TS 24.654 version 8.2.0 Release 8)".

[i.10] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.11] ETSI TR 187 009 (V2.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".

[i.12] ETSI TR 133 937: "Universal Mobile Telecommunications System (UMTS); LTE; Study of mechanisms for Protection against Unsolicited Communication for IMS (PUCI) (3GPP TR 33.937)".

3 Abbreviations

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

AS	Application Server
CB	Communication Barring
CND	Customer Network Device
CNG	Customer Network Gateway
FE	Functional Entity
ICB	Incoming Communication Barring
IMS	IP Multimdia Subsystem
IMS	IP Multimedia Subsystem
NASS	Network Access SubSystem
NGN	New Generation Networks
PES	PSTN/ISDN Emulation Subsystem
PHF	PUC Handling Functional
PIF	PUC Identification Function
PIMF	PUC Identification and Marking Function
PMF	PUC Marking Function
PPF	PUC Personalization Functional
PSD	PUC Setting Database
PUC	Prevention of Unsolicited Communication
PUCI	Prevention of Unsolicited Communication in IMS
RACS	Resource Admission Control Subsystem
SDO	Standard Development Organization

SDT	Session Duration Time
SIP	Session Initiation Protocol
SS	SoftSwitch
UC	Unsolicited Communications
UDP	Use Datagram Protocol
UE	User Equipment
UPSF/HSS	User Profile Server Function / Home Subscriber Server

4 PUC requirements (stage 1)

The PUC requirements were elaborated in the feasibility study on prevention of unsolicited communication in the NGN TR 187 009 [i.11]. The basic PUC service requirements can also be found in the TISPAN service requirements document for Release 3 (TS 181 005 [i.3]), but the full set of requirements will be available in the NGN security requirements document (TS 187 001 [i.1]).

4.1 PUC objectives

4.1.1 Basic objectives

[OBJ 1] The NGN should provide the ability for users to identify specific communication instances as UC.

[OBJ 2] The NGN should provide the ability to mark UC.

[OBJ 3] The NGN should provide the ability to react to UC.

[OBJ 4] The NGN should provide the ability to a user to personalize the UC profile.

4.1.2 Interoperability with existing services

[OBJ 5] The NGN should provide Interoperability with existing solutions in the NGN.

PUC should be interoperable with following existing supplementary services:

- Incoming Call Barring (White and Black list) - TS 124 611 [i.7].
- Anonymous Call Rejection - TS 124 611 [i.7].
- Closed User Groups - TS 124 654 [i.9].
- Call Diversion on Originating Identity - TS 124 604 [i.4].
- Malicious Communication Identification - TS 124 616 [i.8].
- Originating Identity Restriction - TS 124 607 [i.5].
- Terminating Identity Restriction - TS 124 608 [i.6].

4.2 NGN service requirements for PUC

The full set of requirements for PUC are listed in the TS 187 001 [i.1].

5 PUC functional architecture (stage 2)

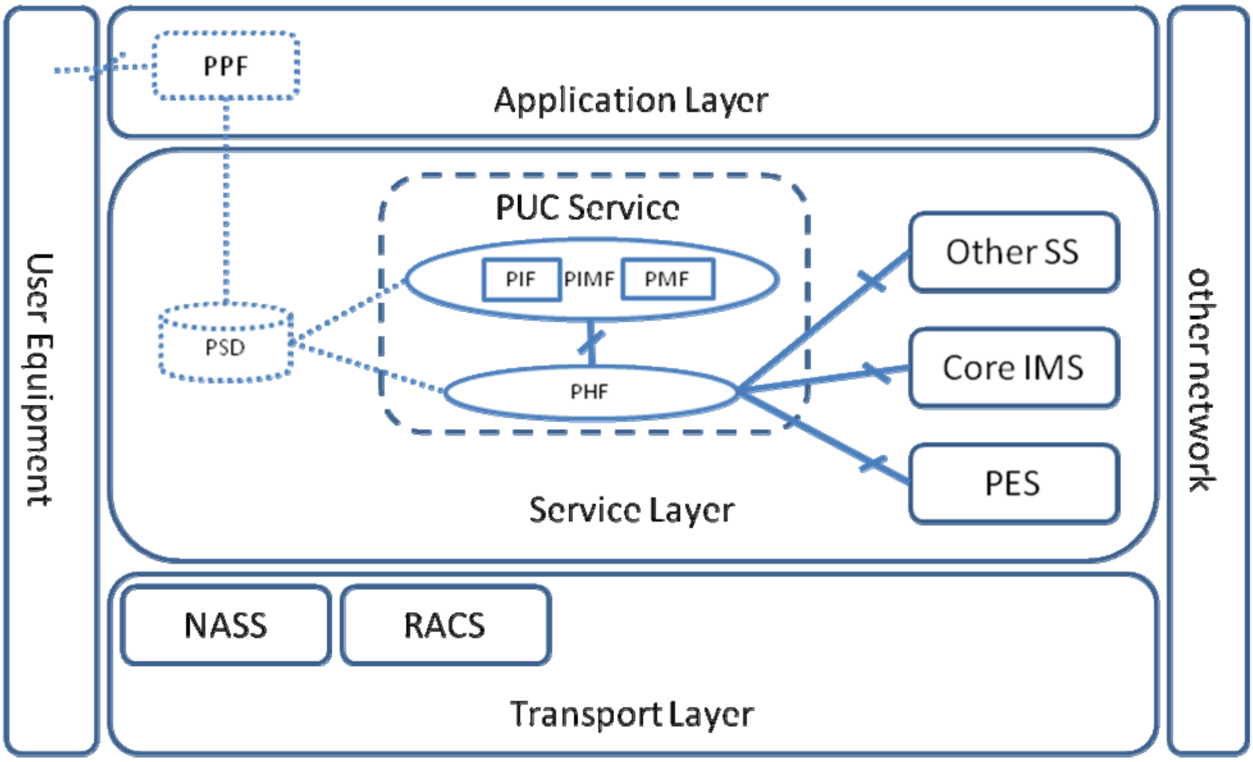


Figure 1: PUC functional architecture

5.1 PUC Functional Elements and Elementary Functions

5.1.1 PUC Personalization Functional (PPF)

The PUC Personalization Functional Entity (PPF) provides the customization of the preferences of the PUC filtering and routing-criteria, both for end-user customization and operator wide settings.

It directly interacts with the PSD where this information is stored.

The PPF has two interfaces:

- To the end-user, for personalization of his profile and the operator to configure global settings.
- To the database, to store the PUC related information.

This functionality can be integrated in existing interfaces (e.g. for the IMS case: Ut).

5.1.2 PUC Setting Database (PSD)

The PUC Setting Database (PSD) contains the settings for the PUC service for the UC identification and the UC handling. The PSD serves the PIMF for personalized identification and the PHF for routing decisions.

The PSD has three interfaces:

- To the PPF for configuring the settings for PUC.
- To the PIMF to configure the personalized settings for UC identification.
- To the PHF for configure personal and global routing decisions.

This FE can reuse existing functionalities (e.g. by reusing the UPSF/HSS).

5.1.3 PUC Handling Functional (PHF)

The PUC Handling Functional Entity (PHF) deals as service-broker for the PIMF. It receives the communication requests from every configured interface to the underlying networks, gets the customized and personalized PUC configuration and deals with the communication between the PIMFs. Furthermore, it administrates the ratings delivered by the PIMF and takes routing decisions based on their results of the UC likelihood and customized / personalized preferences.

The PHF has several interfaces:

- to one or several PIMF FE for identifying UC;
- to each supported underlying network:
  - e.g. in case of IMS, it could be the Isc interface.

5.1.4 PUC Identification and Marking Function (PIMF)

The PUC Identification and Marking Function (PIMF) deals on a technical level to identify and mark UC within the PUC service. A single PIMF consists of two elementary functions for identifying and marking of the communication as unsolicited.

To serve existing services, the PIF can serve as interface to existing services (e.g. supplementary subsystems) which just need a PMF to form a full PIMF.

The PIMF has one interface:

- to the PHF to serve the request from the PUC.

5.1.4.1 PUC Identification elementary Functional (PIF)

The PUC Identification Function (PIF) is by technical mean the functionality which identifies unsolicited communication (e.g. call-rate limiter).

5.1.4.2 PUC Marking elementary Functional (PMF)

The PUC Marking Function (PMF) provides, in conjunction with the PIF, the marking of the identified UC. The marking is highly dependent on the PIF and is used by the PHF to calculate the risk of an incoming communication attempt as unsolicited.

5.2 Functionality mapping on networks

5.2.1 Mapped to a single NGN / single user scenario

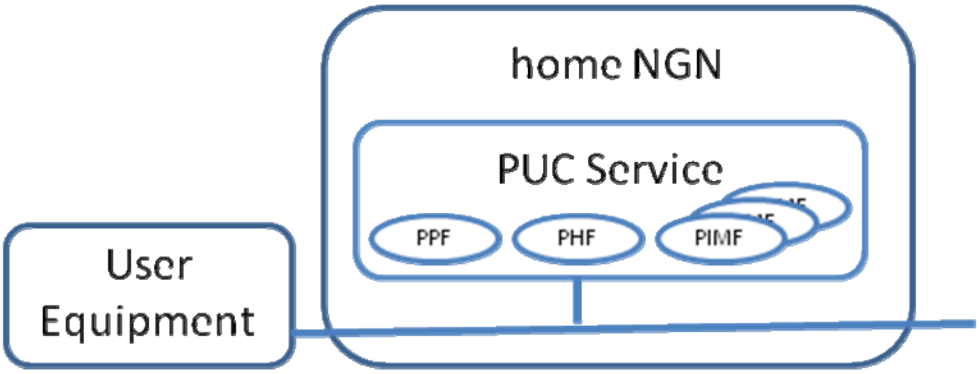


Figure 2: PUC in a single deployment scenario

5.2.2 Mapped to multi NGN / single user scenario

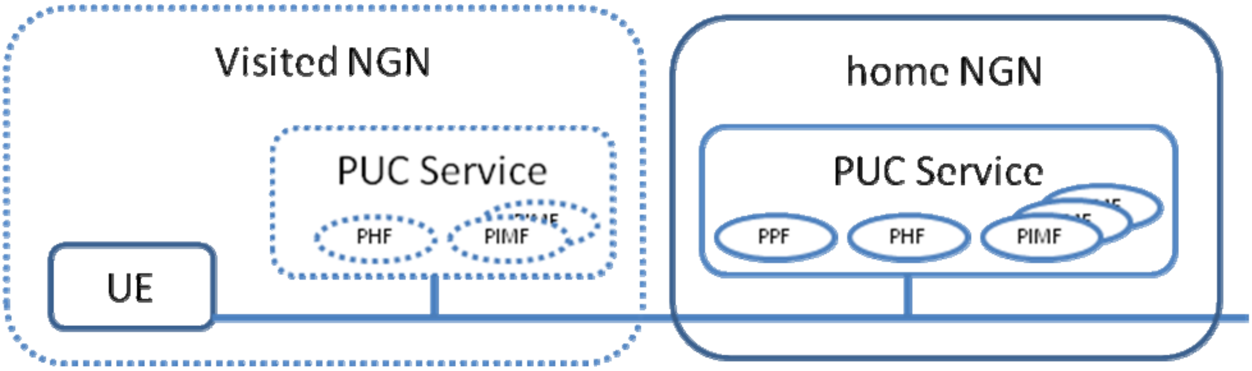


Figure 3: PUC in transit NGN scenario

Within this scenario, the user is connected via a transit network which has access to the communication path from the user to the service of his home NGN.

The Transit NGN can apply PUC filtering by requesting his PUC service, the PHF addresses according to the routing rules the configured PIMF modules which identify and mark the transiting communication request during its passes by.

The home NGN can take the results from the signalling from the transit PUC service into account and apply additionally PIMF modules and apply a personalized handling for this UC request.

A policy cooperation agreement is needed to provide a shared PUC service among these networks.

5.2.3 Mapped to home networks

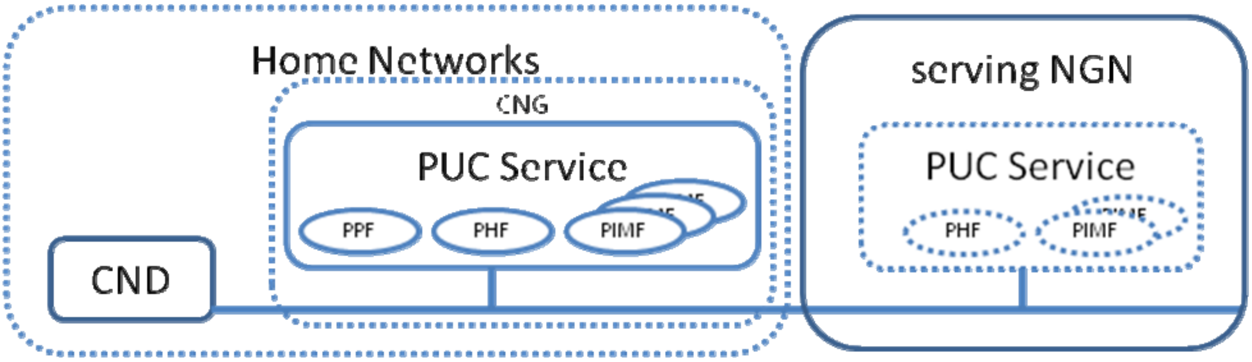


Figure 4: PUC in home network

Within this scenario the user (CND) has a PUC service on his CNG and defines there his personalized filtering and handling of the identified unsolicited communication.

The serving NGN can provide additional "pre-filtering" of the communication and deliver the results as additional input to the PUC service hosted on the CNG.

5.2.4 Mapped to enterprise networks

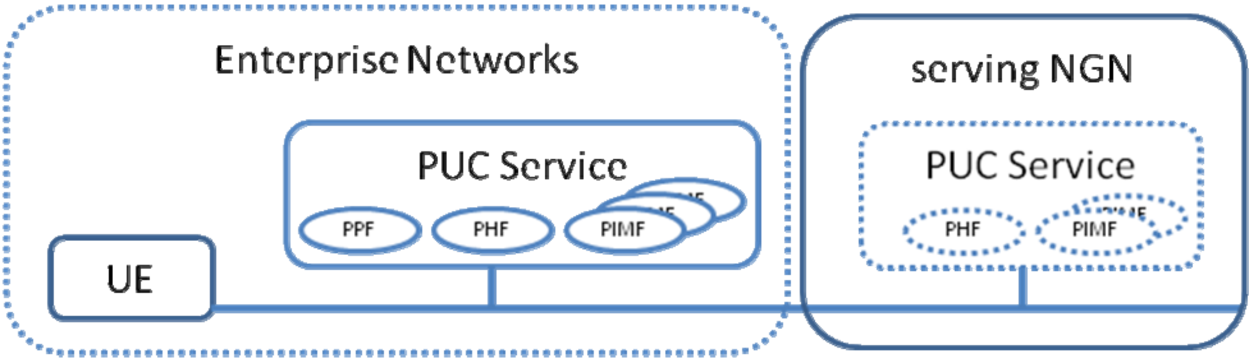


Figure 5: PUC in enterprise networks

Within this deployment scenario, the PUC service provided by the NGN is additional.

6 PUC information mitigation (stage 3)

To identify the related interfaces, a typical call flow in cooperation with the PUC service is given.

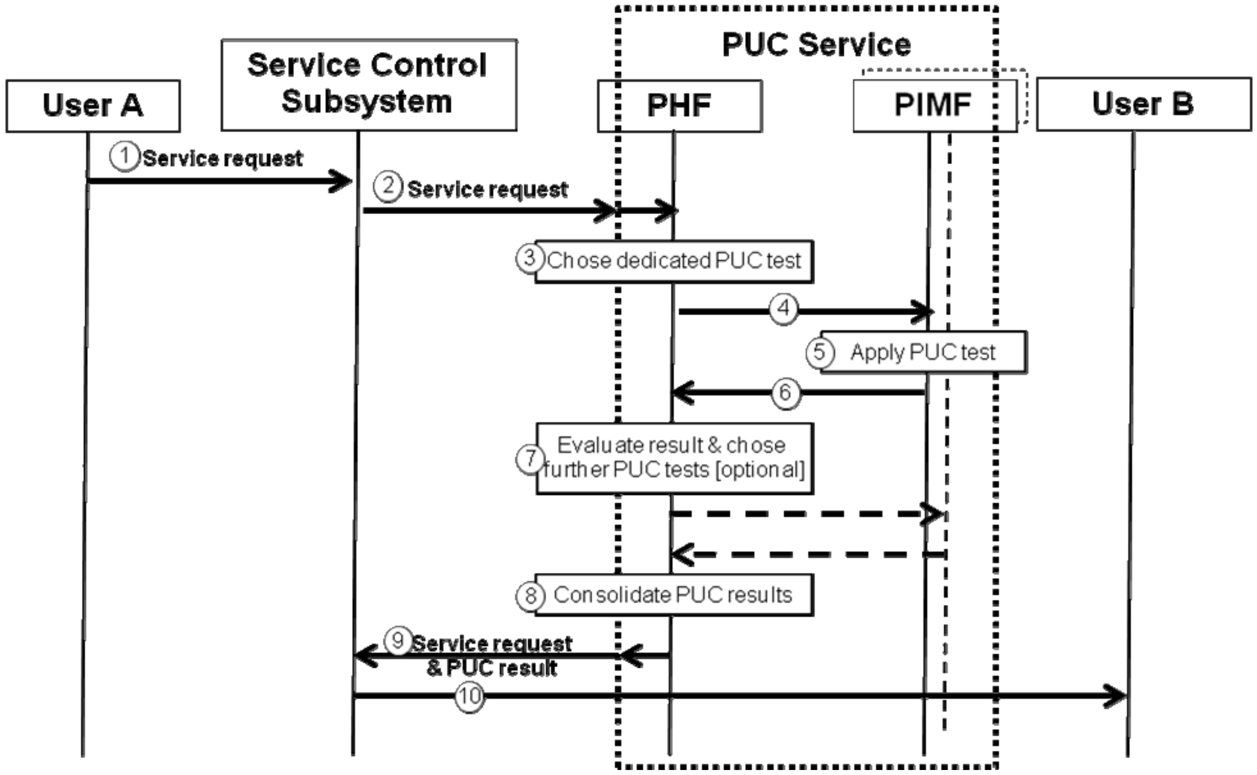

PUC Service
User A
Service Control Subsystem
PHF
PIMF
User B
1 Service request
2 Service request
3 Chose dedicated PUC test
4
5 Apply PUC test
6
7 Evaluate result & chose further PUC tests [optional]
8 Consolidate PUC results
9 Service request & PUC result
10

Figure 6: PUC call flow

1) the User A establishes a service or session request against the Control Subsystem;

2) the Control Subsystem decides to invoke the PUC service and **forwards** the request to the PHF;

3) the PHF decides based on configuration and personalization the correlating PIMF functions; and

4) forwards the service/communication request to the PIMF;

5) the PIMF applies the test itself, and appends on the service request additional information on the result; and

6) sends the request back to the PHF;

7) the PHF evaluates the result and decides to apply further tests;

8) in the final step, the PHF consolidates the PUC service filtering results; and

9) forwards back the session/service request to the subsystem;

10) the subsystem can then decide how to proceed with the communication request. Grant it, forward it or redirect it.

For interconnection with existing services in the scope of UC identification, the PIMF can be decomposed. The marking of the communication should be PUC conform. For illustration, please refer to clause A.2.2

6.1 PUC information propagation differentiation:

The information mitigation can be classified in two groups:

6.1.1 PUC information: downstream

PUC
downstream
CND / User

Figure 7: PUC information propagation downstream

The downstream PUC information propagation is used to signal PUC results to the next network element / UE.

6.1.2 PUC information: upstream

PUC
upstream
CND/ User

Figure 8: PUC information mitigation upstream

The upstream PUC information mitigation is used to signal PUC results to the next network element / UE.

6.2 Interfaces for PUC information mitigation

By mapping the given requirements to the existing NGN infrastructure, the following interfaces are matched.

6.2.1 The PUC service mapped to subsystems: Isc

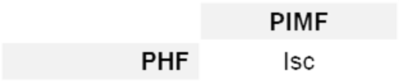
Table 1: Mapping of PUC functionalities to existing NGN subsystems

	PHF
PES	Isc
IMS	Isc
Other SS	Isc
Core NGN	Isc

Additional information regarding the Isc Interface can be found in [i.2].

6.2.2 PUC internal functionalities mapped to NGN: Isc

Table 2: Mapping of PUC functionality to existing interfaces

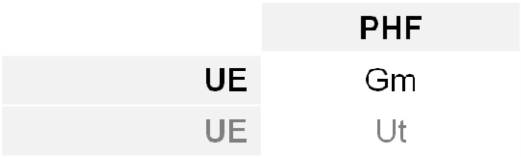


	PIMF
PHF	Isc

Additional information regarding the Isc Interface can be found in [i.2].

6.2.3 PUC service mapped to UE: GM & Ut

Table 3: Mapping of PUC functionality to UE



	PHF
UE	Gm
UE	Ut

The direct interface from the UE to the PUC AS is mapped to the Ut interface and does not need additional specification.

6.2.4 PUC interfaces

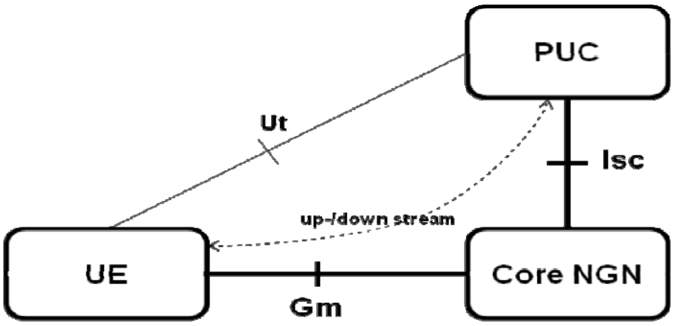


Figure 9: PUC interfaces

6.3 PUC protocol

Gm and Isc are using SIP.

PUC SIP extensions are the most natural way to provide PUC information without introducing additional requirements to the TISPAN NGN specification.

Additional information of SIP and the implementation in the NGN can be found in [i.3] and [i.10].

6.3.1 Procedures using SIP for PUC

Clause A.3 describes an example set of parameters that could be used for the information propagation within the transaction initiation flow.

6.4 PUC parameters

Table 4

Parameter	Description	Importance
PUC identifier	Indicating the PUC element making the claim	mandatory
PIF identifier	The name of the agreed PIF	mandatory
Strength	An integer indicating the confidence of the score	optional
Info	A text field containing any arbitrary information	optional
Param[1..3]	3 general purpose parameters for future proofing	optional
IsSpam	A boolean indicator for the operator for evaluation if unsolicited communication	mandatory

NOTE: All these values are information in a p-asserted identity and all obligations regarding privacy apply for transitions between operational domains.

Annex A:
Related Information

A.1 Similar work in other SDOs

A.1.1 3GPP - PUCI

NOTE: Common IMS mechanisms will be handled by 3GPP.

A.2 PUC architecture

A.2.1 General PUC architecture

PUC should provide the functionality of identifying, marking and handling unsolicited communication in a personalized way. The PUC functional entities mapped to a functional architecture.

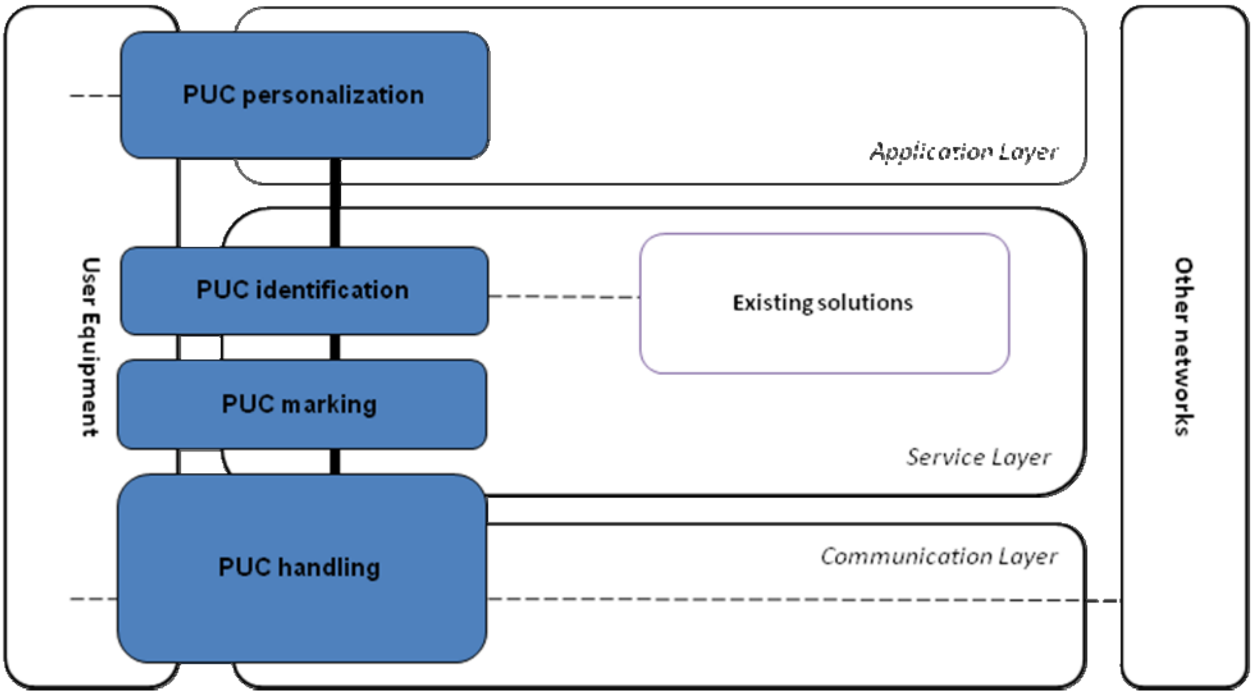


Figure A.1: PUC general architecture

The basic functionalities are:

- Personalize UC profile.
- Identify unsolicited communication.
- Mark unsolicited communication.
- Handle unsolicited communication.

Further service requirements are:

- Interact with the terminating party for feedback reasons.
- Interact with existing solutions.
- Interact with other networks.

A.2.2 PUC:PIMF call flow

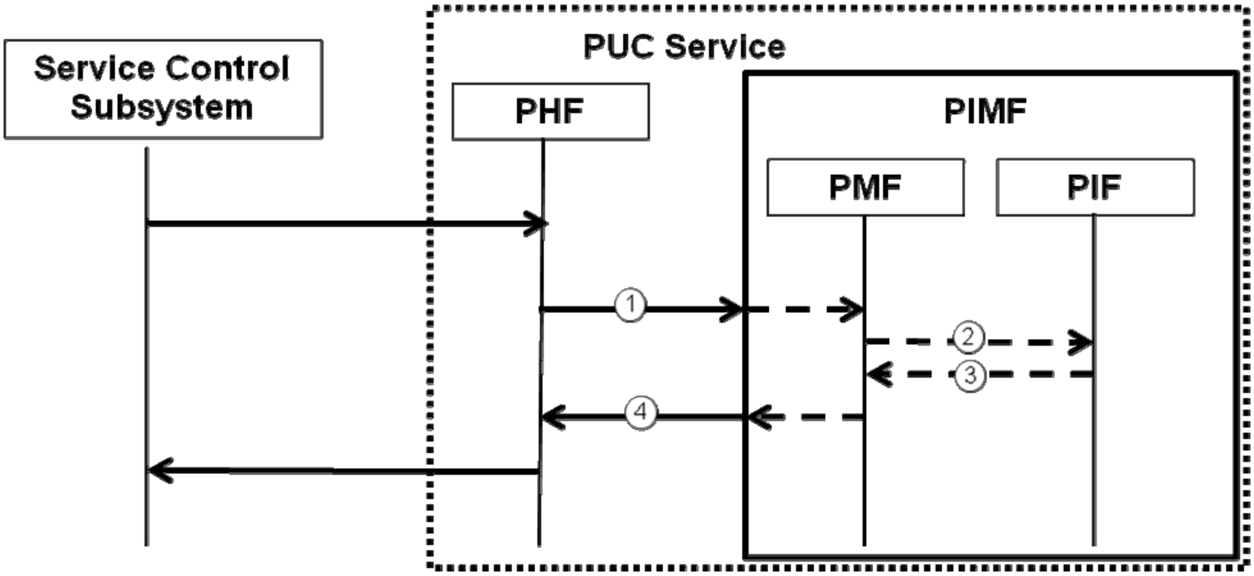


Figure A.2: PIMF call flow

The following steps, apply in the context when the session request, was forwarded from the Service Control Subsystem:

1) the PHF receives the session request and decided to invoke one PIMF functional element, which is as first contact point the PMF, which can extract parameters and configure the related PIF;

2) the PIF (which can also be an existing subsystem e.g. ICB, CB, etc) is queried; and

3) gets a result back, which is then processed by the PMF, extended with the correlating PUC marking functionality; and

4) given back to the PHF for further processing.

A.3 Draft-wing-sipping-spam-score

The following text is an extract from the IETF draft (draft-wing-sipping-spam-score-02) which expired in February 2008.

A.3.1 Abstract

This IETF draft defines a mechanism for SIP proxies to communicate a spam score to downstream SIP proxies and to SIP user agents. This information can then be used as input to other decision making engines, for example, to provide alternate call routing or call handling.

A.3.2 Information passed downstream (taken from original Chapter 4)

In addition to the score the following other pieces of information should be passed downstream as well:

- Realm - Indicating the upstream domain or realm making the claim.
- Algorithm - The name of the agreed upon algorithm.
- Strength - An integer indicating the confidence of the score (0 to 100).
- Info - A text field containing any arbitrary information.
- Param[1..3] - 3 general purpose parameters for future proofing.
- IsSpam - A boolean for convenience purposes alone.

A.3.3 Grammar (taken from original Chapter 7)

extension-header = "Spam-Score:" SP spam-score *[SP ";" spam-detail]

spam-score = score SP "by" SP hostname

score = 1*3DIGIT ["." 1*3DIGIT]

spam-detail = spam-strength / spam-algorithm / spam-param

spam-algorithm = "spam-algorithm" EQUAL quoted-string

spam-strength = "spam-score-strength" EQUAL strength

strength = 1*3DIGIT ["." 0*3DIGIT]

spam-info = "spam-info" EQUAL info-value

info-value = quoted-string

spam-param1 = "spam-param1" EQUAL param-value

param-value = quoted-string

```
spam-param2     = "spam-param2" EQUAL param-value

param-value     = quoted-string


spam-param3     = "spam-param3" EQUAL param-value

param-value     = quoted-string


spam-isspam     = [ "isSpam" ]
```

A.3.4 Examples (taken from original Chapter 8)

The following example shows a SIP score generated and inserted by two SIP proxies, sip.example.com and sip.example.net. In this example, sip.example.com is owned by a spammer who is trying to fool downstream systems with their low spam score (0). However, the example.net proxies and user agents only pay attention to spam scores from Spam-Score headers generated by example.net proxies, so example.com's attempts to fool the downstream proxies (with its low spam score) are in vain.

> NOTE: Also, the sample Session Duration Time (SDT) algorithm SDT [I-D.malas-performance-metrics] simply compares the given callers previous session duration time with the expected session duration time over all destinations.

```
INVITE sip:bob@example.net SIP/2.0

Via: SIP/2.0/UDP sip.example.net;branch=z9hG4bKnashds8;received=192.0.2.1

   Spam-Score: 75 by sip.example.net

   detail="SIPfilter-1.0

   call_volume=75"

   spam-algorithm="SDT"

   spam-score-strength=50

   spam-info="High call volume"

   spam-isSpam

Via: SIP/2.0/UDP sip.example.com;branch=z9hG4bKfjzc; received=192.0.2.127 Max-Forwards: 70

To: Bob <sip:bob@example.net>

From: Alice <sip:alice@example.com>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.example.com

CSeq: 314159 INVITE

Contact: <sip:alice@pc33.example.com>

Content-Type: application/sdp

Content-Length: 142

[... SDP elided from this example...]
```

Annex B: Bibliography

ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

IETF RFC 3261: "SIP: Session Initiation Protocol".

ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

ETF RFC 5039: "The Session Initiation Protocol (SIP) and Spam".

ETSI TR 185 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of security mechanisms for customer premises networks connected to TISPAN NGN".

History

Document history		
V3.1.1	May 2011	Publication