3GPP TR 33.838 V11.0.0 (2012-02)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Protection against Unsolicited Communication for IMS (PUCI) (Release 11)

Keywords
IMS, Security

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report 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 studies more focussed the high-level solutions possibilities for PUCI described in the technical report (TR 33.937) on PUCI.

The scope of the study includes:

- Study of the PUCI related information:
  - What information to be stored in the HSS.
  - Type of PUCI information to be exchanged (e.g. scoring information, contextual information) and how this information should be structured, or even between which nodes the information should be sent.
  - If and how PUCI information should be sent inside SIP.
- Study on Invoking of 3rd party PUCI AS or Supplementary Services (SS) depending on configuration.
- Interworking
  - with non-IMS networks.
  - with other IMS services like SRVCC, ICS, and service continuity.
- Types of communication that should/can be covered by PUCI, and how the different types of communication affect the PUCI solution.
- How much of PUCI that can be achieved via prevention and how much needs to be done via treatment.
- PUCIF to PUCIF communication.
- Use of existing methods of user notification for PUCI communication.
- Mitigation of source identity spoofing, especially from non-IMS networks, on the effectiveness of the PUCI mechanism.
- Illustrative use of standardized PUCI features in typical deployment scenarios.

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] ETSI TR 187 009: "Feasibility study of prevention of unsolicited communications in the NGN".

[3] 3GPP TR 33.937: "Study of mechanisms for Protection against Unsolicited Communication for IMS (PUCI)".

[4] 3GPP TS 22.173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1".

[5] 3GPP TS 22.101: "Service aspects; Service principles".

[6] (void)

[7] IETF, "SPEERMINT WG Charter 2010-04-02", http://tools.ietf.org/wg/speermint/charters?item=charter-speermint-2010-04-02.txt

[8] IETF RFC 5486, "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology"

[9] IETF, "VoIP SIP Peering Use Cases", Work in progress, Internet-Draft: draft-ietf-speermint-voip-consolidated-usecases-18, April, 2010.

[10] IETF, "SPEERMINT Security Threats and Suggested Countermeasures", Work in progress, Internet-Draft: draft-ietf-speermint-voipthreats-05, Sept, 2010.

[11] IETF RFC 3324, "Short Term Requirements for Network Asserted Identity".

[12] IETF RFC 3325, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[13] IETF RFC 3893, "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format".

[14] IETF RFC 4474, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[15] RFC 5039 "The Session Initiation Protocol (SIP) and spam".

[16] 3GPP TS 29.328: "IP Multimedia Subsystem (IMS) Sh interface; Signalling flows and message contents".

[17] 3GPP TS 29.329: "Sh interface based on the Diameter protocol; Protocol details".

[18] IETF draft Spam Score for SIP (draft-wing-sipping-spam-score-02) draft-wing-sipping-spam-score-02

[19] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[20] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

3 Definitions, abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Unsolicited Communication: bulk communication in IMS where the benefit is weighted in favour of the sender.

NOTE 1: In general the receiver(s) of UC do not wish to receive such communication. UC may comprise, e.g., "SPam over IP Telephony (SPIT)" or "SPam over IP Messaging (SPIM)". See 33.937 [3].

UC Score: value that is assigned to a communication request indicating the likelihood that a given communication request is UC.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AS	Application Server
B2BUA	Back to Back User Agent
CB	Call Barring
EU	European Union

ICS	IMS Centralized Services
iFC	initial Filter Criteria
IMR	Identify, Mark, React
IPsec	IP Security
MCID	Malicious Communication Identification
OECD	Organisation of Economic Co-operation and Development
PUCI	Protection against Unsolicited Communication for IMS
PUP	PUCI User Policy
SC	Service Continuity
SEG	Security Gateway
SIP	Session Initiation Protocol
SRVCC	Single Radio VCC
UC	Unsolicited Communication
US	United States
VCC	Voice Call Continuity
VoIP	Voice over Internet Protocol

4 Definition of PUCI scope

4.1 Communication modes

The PUCI study TR 33.937 [3] discussed PUCI primarily in the context of voice communications, but did not specify which modes of communication a PUCI solution should apply to. To address this question, the following considerations are put forward:

- It is desirable to have as complete a protection as possible. Thus, PUCI should preferably cover all communication modes carried in IMS. In particular, this includes communication modes utilized in services defined for IMS, such as voice, video, and instant messaging (IMS Multimedia Telephony Service TR 22.173 [4]). Other possibilities include protection against presence spam, i.e., UC embedded in presence subscription messages (e.g., in the From or Contact fields, depending on what is displayed to the recipient for an authorization decision).

- However, since the overall goal of PUCI is to avoid disturbing the subscriber with UC, there is likely little utility in attempting to block communication elements in an already established session. Thus, the primary aim is to prevent UC session establishment attempts. Consequently, content-based protection mechanisms could be beneficial for the case of instant messaging UC carried in SIP Messages, but is likely ineffective when applied to the media plane, e.g., of an established MSRP session. It could be studied if media plane screening solutions can help in addition to mechanisms studied in this TR.

Note: The addition of an media element during an ongoing session might introduce a potential issue, if it is possible for an attacker to spoof the originating identity.

4.2 Bulk communications vs targeted communications

The PUCI study TR 33.937 [3] considered scenarios with targeted communications to specific individuals, for instance, in a stalker type of scenario, as well as the more spam-like bulk communication scenario which indiscriminately targets large recipient populations.

Since existing Supplementary Services (SS) for the Multimedia Telephony service TS 22.101 [4] already includes protection mechanisms for targeted UC through Malicious Communication Identification (MCID) and Call Barring (CB), PUCI scope for targeted communication should be studied only for mechanisms that are not already covered by SS.

5 Design principles and security requirements

5.1 Design principles

The PUCI solution will adhere to the following design principles:

- No new capabilities are required on the IMS core elements. For example the support of iFC, initial Filtering Criteria, in S-CSCF as the basic IMS function is good enough to redirect SIP signals to a PUCI AS.
- There will be new originating and terminating S-CSCF triggers. For example PUCI AS can be triggered by utilizing the existing iFC.
- No impacts on the UEs or its interfaces, including the Gm interface or user interface.
- PUCI processing will be performed in an Application Server.
- If UC score and other PUCI related information needs to be signaled between carriers, it shall originate and terminate in a PUCI AS, thereby being transparent to the IMS core. For example UC score and other PUCI related information can be carried in the SIP header as an optional information element.
- SPUCI solution will not mandate user notification or user interaction, but if there is user notification, only existing methods will be used, as not to impact the UE or usage experience.
- The UC score and other PUCI related information will be defined at a generic level, with their specific meanings being left to operator policy.
- Mapping of UC score and other PUCI related information between carriers will be per interconnection agreements.
- The invocation of PUCI, thresholds, and actions taken will be based on the contractual relationship between the user and the carrier, where the thresholds are based on operator policy.
- PUCI processing may be performed on behalf of IMS and non-IMS users, including PSTN users.
- National legislature and/or operator policy may impact the PUCI actions to be taken.
- PUCI may apply to all IMS services to include and not limited to: session based services (voice, video), messaging, and data delivery.

5.2 Security requirements

Following are security requirements on SPUCI:

1. The IMS should provide a means for IMS-users to report communication as a UC.

Note: This requirement still holds because without this it is not possible to report a UC. There is no conflict with design principle on "No impacts to the UEs or its interfaces, including the Gm interface or user interface."

2. The IMS should provide the ability to the operator to extract information from the signalling and other means to provide an indication of the likelihood whether the communication is unsolicited.
3. The IMS should provide a mechanism to allow variation in communication handling based on UC related information.
4. The solution should also work in interworking scenarios with legacy networks and devices, in particular when using Single Radio VCC, IMS Service Continuity, and IMS Centralized Services.

6 Preventive measures

6.1 Introduction

Preventive measures can be regarded as measures that prevent a malicious user from initiating SPIT/UC at all while reactive measures try to protect the SPIT/UC victim if the SPIT/UC has already been initiated. Therefore preventive measures are the first line of defense against SPIT/UC and are well suited to at least significantly diminish the SPIT/UC problem, before it arises. They can be split into:

- non-technical prevention measures like legislation or contractual agreements and
- technical prevention measures like the reliable identification of the originating communication source

6.2 Non-technical prevention measures

6.2.1 General

Non-technical prevention measures are mainly on the level of:

- legislation that may be and usually is country- or region-specific
- contractual agreements between operators and their customers
- contractual agreements between different operators, called Service Level Agreements (SLAs)

6.2.2. Legislation

The preventive effect of legislation is that it illegalizes activities like SPIT/UC and inflicts a penalty on individuals that contravene the corresponding law. In a specific country (e.g. Germany) or a specific region (e.g. Europe, especially EU) with a coherent legislation this may be a powerful countermeasure, if the identity of the SPITter can be verified.

Although SPIT/UC related legislation is already available for a number of countries – among which a significant number of OECD countries – it differs unfortunately in the definition of SPIT/UC, in the definition of SPIT/UC concerned communication services, and in the handling of SPIT/UC suspicious or SPIT/UC identified communication. This scattered SPIT/UC legislation landscape with different SPIT/UC prevention approaches complicates the verification and the penalization of SPITters and opens also legal grey-zones in cross-border communication while it achieves a consistent protection in the corresponding country or the corresponding region where the law is valid.

As an example for this problem look at the consent achievement whether a communication is SPIT/UC or not. In one region (e.g. EU) a SPIT/UC prevention law determines the Opt-In principle where the initiator of a bulk UC communication (e.g. advertisement) has to prove that the recipient has explicitly given consent. In another region (e.g. US) another SPIT/UC prevention law determines the Opt-Out principle with the consequence that the initiator is allowed to perform the same bulk UC communication without consent of the recipient if there is an easy possibility to get deleted from the address list in order to stop further nuisance in a timely manner. While each law is consistent in the corresponding region, these two different principles are unfortunately mutually exclusive in EU ↔ US communication and open therefore a legal grey-zone.

Therefore it would be helpful to define as well a set of rules regulating the legal aspects of cross-border communication.

6.2.3 Contractual agreements between operators and their customers

Contractual agreements between operators and their customers can have a similar preventive effect as legislation. Any individual wishing to use the services of an operator has to enter into a contract with the corresponding operator. There the operator can specify the terms of use and the consequences if the customer defies the agreed contractual agreements. In contrast to legislation the consequences are now not generally defined by a law but only specifically by an operator. The potential customer has the possibility to either accept the contractual agreements or to choose an operator with less strict terms of use.

The terms of use may control the behavior of a customer by certain parameters like for example the number of calls per time interval, the number of international calls per time interval or the total duration of international calls per time interval. Additionally the operator can restrict the usage of its services to 'only private and non-commercial' and rate calls contravening these conditions another price making misuse by SPITters unattractive. In worst case, if the operator identifies a specific customer as a permanent source of malicious usage, the operator may reserve the right to terminate the contract with this user.

However with the rising of VoIP and with the interconnection of the currently existing VoIP islands it is no longer guaranteed that all VoIP users will have a contract with an operator at all. Nevertheless it is interesting to see that today also well-known VoIP providers that offer free communication over the Internet behave operator-like (charging of small fees; terms of use restricting the capabilities of a user), if they connect to existing PSTN networks. But even the contracts of the different operators may differ in their conditions so that the trust into an operator may range from high to low.

On the other hand these varying levels of trust give trusted operators also the opportunity to differentiate from their competitors. Today it is not clear whether the majority of users is willing to accept a large number of nuisances like SPIT/UC for the benefit of a lower price. Therefore the trust level of the operator will perhaps also have consequences for a differentiation between the kinds of customers joining the network: 'normal' customers may perhaps accept an additional charge for a network, almost clean of nuisances like SPIT/UC, while customers with a restricted budget and happy with 'trying out new things' may choose an operator with lower price and lower trust level. But trusted operators carry then the responsibility to which other operator networks they connect under which terms to protect their own network against external nuisances. This is usually regulated by contractual agreements between different operators, usually called Service Level Agreements (SLAs; see next sub-section).

Generally even the non-operator centric part of the VoIP community in IETF acknowledges in RFC 5039, section 3.13 that today's operator controlled networks experience relatively little SPIT/UC and takes this as proof that this kind of arrangement can work.

6.2.4 Contractual agreements between different operators (SLAs)

Operator networks face two kinds of major interfaces, one towards their customers and one towards peering operator networks. While the last sub-section has illustrated the possibilities to tackle the SPIT/UC problem in the own operator's network, this section deals with the protection of the operator network against SPIT/UC traffic originating from peering operator networks. The protection is achieved by bilateral contractual agreements between the peering operators, usually called SLAs.

These SLAs may for example specify the amount of allowed nuisance originating from the peering network, countermeasures to identify and stop malicious sources in the peering network, thresholds for SPIT/UC attacks where the operator is allowed to block the complete traffic of its peering counterpart or compensatory payments if the SLAs are violated.

The preventive effect of these SLAs is that they delegate responsibility towards the peering operator and regulate the consequences if the peering operator doesn't live up to this responsibility. SLAs have turned out to be a powerful means for operators to maintain control over their network and the connected customers. They are widely adopted, e.g. in the telco and the ISP area and are therefore well suited as a preventive measure suppressing the generation of SPIT/UC as far as possible.

6.3 Technical prevention measures

A technical prevention measure is the reliable identification of the communication source. The preventive effect is that the communication source is no longer able to act anonymously and, as a consequence, can therefore be held responsible for actions like e.g. the sending of SPIT/UC.

The effectiveness of reliable identification is underlined by RFC 5039 [15] clause 4. RFC 5039 [15] sees the reliable identification of the communication source as the key enabler to make reactive SPIT/UC measures work. The key role of reliable identification is also accentuated in various sections of 3GPP TR 33.937 [3].

This item is discussed in more detail in clause 7.1.2 of this TR. There the already widely adopted mechanism of 'P-Asserted Identity' is proposed as an agreed identity mechanism for interworking between VoIP operators mutually trusting each other. Additionally the definition of a new optional signaling element allowing VoIP operators to reliably convey rich information related to SPIT/UC is discussed as a long term solution.

7 Interworking with non-IMS systems

7.1 Background

The present clause provides background information, such as reviewing relevant related efforts in other standards bodies.

7.1.1 IETF Work on SIP Peering

The SPEERMINT WG in IETF is currently working on defining use cases, requirements, architectures, mechanisms, and best practices for SIP service provider peering (at the service level, not the IP-routing level), including considerations such as establishment of trust, security, and resistance to abuse and attacks (see charter-speermint-2010-04-02.txt [7]). While protection against UC is explicitly outside the WG scope, the results will inevitably have implications for how protection against UC can be achieved.

Interworking with non-IMS SIP-based services that comply with IETF standards appears to be one significant case to consider. Thus, it is desirable to align PUCI considerations for interworking with non-IMS systems with the SIP Peering work in IETF.

The use cases considered for SIP peering are divided along two dimensions (as described in RFC5486 [8]):

- Direct (no transit) or indirect (using transit)
- Static (pre-established peering) or on-demand (limited pre-existing state)

Static peering is defined as the case when a pre-association between the SIP service providers is required for the initiation of any real-time transactions (like a SIP message). On-demand peering is said to occur when any information that needs to be exchanged between domains in support of peering can be learned through a dynamic protocol mechanism. The on-demand peering model mimics the Internet email model. However, it is noted in draft-ietf-speermint-voip-consolidated-usecases-18 [9] that on-demand SIP peering is uncommon in production, and a detailed description is therefore omitted.

Security threats and suggested countermeasures are identified in draft-ietf-speermint-voipthreats-05 [10], and security requirements of mutual authentication, protection of confidentiality and integrity protection, and the possibility of passing media security attributes are mentioned. It is stated that the authentication, confidentiality, and integrity requirements can be fulfilled through the use of, e.g., TLS or IPsec. TLS is perceived as having some advantages in the way it can be coupled to the specified functional elements, but it is also noted that there may be particular cases where IPsec is preferable.

Several other countermeasures to attacks against peering are also considered. However, most of these, with the exception of the use of *strong sender identity assertions*, are not directly relevant for protection against UC; but may be relevant indirectly with respect to a step in an attack to enable UC injection.

Two main alternatives to achieve strong identity assertions are considered:

- A chain of trust model using Network-Asserted-Identity or P-Asserted-Identity (see RFC3324 [11] and RFC3325 [12]), or
- Use of cryptographic signatures using SIP Authenticated Identity Body (see RFC3893 [13]) or SIP Identity (see RFC4474 [14])

It is noted that the transitive trust requirement for the first alternative can be seen as an underlying weakness, and the second alternative requires a Public Key Infrastructure to be in place.

7.1.2 Operator SPIT/UC interworking and source identification

7.1.2.1 Introduction

Reliable identification of the originating user/domain has been identified as a building block of many successful technical SPIT/UC measures, for example blacklist or whitelist.

While identification of the originating user/domain in itself would not be sufficient for SPIT/UC prevention, it is rather the basis for other methods: Because of address forging technical SPIT/UC prevention measures relying on source identities like black-listing of SPIT/UC sources or the evaluation of a SPIT/UC score in the terminating domain may be significantly impaired. This problem has already been discussed in TR 33.937 [3].

None of the already existing identification mechanisms like

- Open Proxy Handshake
- P-Asserted Identity
- SIP Identity
- Trusted Interconnect with IPsec/TLS, potentially combined with P-Asserted Identity
- Combination of SPIT/UC score transmission (see draft Spam Score for SIP (draft-wing-sipping-spam-score-02) [18]) with identification of originating user/domain

provides by itself a satisfying solution of the problem, that is to say 'a reliable identification of the originating user/domain' for IMS as well as for non-IMS networks. The reasons are that

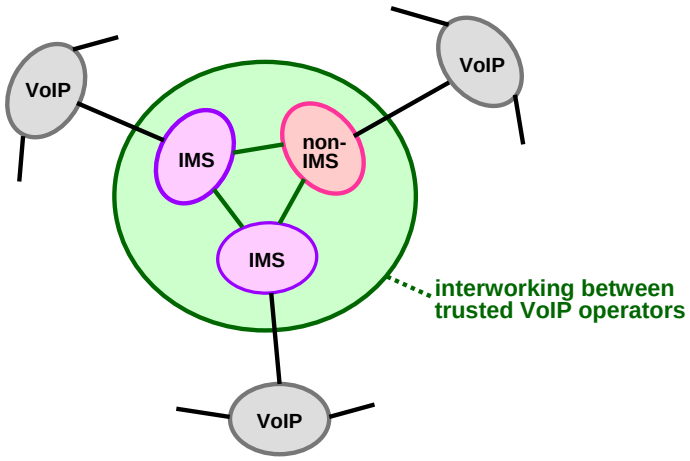
- they are not ubiquitously available;
- they rely potentially on chained trust like 'Trusted Interconnect with IPsec/TLS', but trust is in general not transitive without additional agreements;
- SIP signaling enhancements like RFC 4474 (SIP Identity) or the draft-wing-sipping-spam-score-02 suffer from the fact that the required signaling elements may either be changed or even blocked by Back-to-Back User Agents, thus preventing the requested functionality.

In summary, it can be stated that today and even in the mid-term no widespread solution exists that generally solves the 'identification of the originating user/domain' problem for the purposes of 3GPP SPIT/UC prevention. To get out of this deadlock, a two-step approach is proposed:

1) Use of P-Asserted Identity as an agreed identity assertion mechanism for interworking between VoIP operators mutually trusting each other
2) Definition of a new optional SIP signaling element allowing VoIP operators to reliably convey rich information related to SPIT/UC as a long-term solution

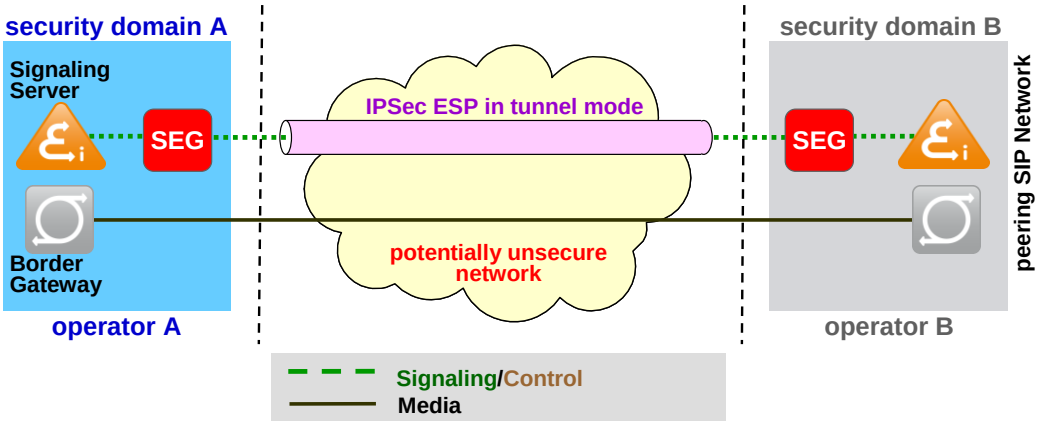
7.1.2.2 Interworking between mutually trusting VoIP operators

The interworking on a trust basis is achieved between VoIP operators that are associated by mutual contractual agreements and therefore have a certain degree of trust in each other. This is comparable to the 'circles of trust', discussed by Rosenberg and Jennings in RFC 5039. It is expected that IMS-based VoIP operators will usually interwork on a trust basis but the interworking is not restricted to IMS networks. Every VoIP operator supporting 'P-Asserted Identity' as the agreed identity assertion mechanism and willing to bind themselves by contractual agreements is able to participate in the interworking of mutually trusting VoIP operators. Every domain of a trusted VoIP operator can as well be connected to other VoIP domains not supporting 'P-Asserted Identity', but these domains not supporting 'P-Asserted Identity' are per default assumed to have a lower trust level. Therefore, with respect to PUCI mechanisms, the world of VoIP domains is split into two parts: either supporting 'P-Asserted Identity' or not supporting 'P-Asserted Identity'.



P-Asserted Identity is selected as identity assertion mechanism to reliably evaluate the identity of users, because the P-Asserted Identity SIP header has already been standardized as a private extension to SIP (RFC 3325 [12]). It enables a network of trusted SIP servers to assert the identity of authenticated users. The trust in P-Asserted Identity is based on the fact that it is added by the network (trusted SIP servers) and not by a potentially malicious user. An additional advantage of using P-Asserted identity in a first step is that it does not put too much burden on networks that are usually well controlled and that are not expected to be the primary source of SPIT/UC trouble.

Although originally proposed to the IETF by 3GPP, P-Asserted Identity seems to have spread beyond IMS networks, but is not ubiquitously available. Even if ubiquitously available, it would not generally solve the problem of reliable identification because P-Asserted Identity is not signed by the originating SIP server. Leaving P-Asserted Identity unsigned, requires additionally that the mutually trusting VoIP operators are interconnected by means of a trusted interconnection network, e.g. according to the Za inter-domain interface as specified in TS 33.210 [19]. Za represents the interface between the Security Gateways (SEG) of two different security domains (denoted as security domain A and B in the example below). Za is an inter-operator interface between two operators A and B, connected via a potentially unsecure intermediate network.



According to TS 33.210 [19] the provisioning of a Za interface applies only to signaling traffic. Integrity and confidentiality is ensured by an IPsec tunnel between the two security domains. The required IPsec ESP tunnel functionality is

- integrity, authentication and anti-replay protection (mandatory)
- confidentiality by encryption (optional)

But this means on the other side: If a P-Asserted Identity header is received from a non-trusted domain, this header has to be cut and with that the level of trust in the originating identity is per default reduced. This implies that trusted VoIP domains may not be connected via untrusted intermediary domains.

Between mutually trusting VoIP operators P-Asserted Identity enables an effective SPIT/UC prevention in the terminating network, in conjunction with others methods such as Supplementary Services, because the originating user is reliably identified. Thus SPIT/UC prevention methods like black-listing or the evaluation of a SPIT/UC score according to the policy of the terminating operator will get effective without the need to exchange SPIT/UC scores between the domains of trusted VoIP operators.

The usage of P-Asserted Identity alone already allows a SPIT/UC related differentiation between trusted and other VoIP domains. All users of other VoIP domains are per default set to a reduced trust level. This allows reactions in the terminating network like blocking of calls, redirecting to a SPIT/UC voice mailbox in conditional call forwarding or indicating of reduced trust level.

8 PUCI architectural considerations

8.1 Overview

8.2 PUCI information storage

PUCI is a subscription service, therefore there is a need to store relevant information of the PUCI service that are important for the S-CSCF to know whether and how PUCI service should be invoked and when a caller is considered as unsolicited. Therefore the basic PUCI information stored consists of the following:

- PUCI Flag: A logical indication saying whether the subscriber is subscribed to PUCI service or not; this could be realized as part of the Initial Filter Criteria (iFC) in the HSS to invoke one or more PUCI ASs.

- PUCI Threshold: Settings which tells the PUCI AS what to do when a certain UC Score is received, e.g., a subscriber can set that an incoming call with a score above 5 should be forwarded to a given number and with a score above 10 the call should be dropped. It is on the operator to decide whether the PUCI Threshold is a value valid for all subscribers in the network or is modifiable by a subscriber. PUCI Threshold is stored in the PUCI AS.

- PUCI Action: Depending on operator policy, this is subscriber preference setting on what should be done after unsolicited communication is detected, e.g., dropping of the call etc. The operator could decide a global policy for action to be taken or leave it on user decision. PUCI Action is stored in the PUCI AS.

- Routing profile: This is information about the order in which PUCI ASes / Functions should be accessed for a given subscriber. Based on operator policy, a subscriber can modify the strength of protection, for example, somewhere between strict to lenient check. This may have a bearing on the routing profile.

Collectively we call the above four items as PUCI User Policy (PUP). Only the iFC is stored in the HSS. This means as a consequence that the PUP is not stored centrally at a unique location in the network but decentrally at least at two different locations. A reasonable place to store all other information than iFC would be the PUCI AS.

8.3 PUCI function invocation

The PUCI function is invoked as any other application server in IMS with the initial filter criteria (iFC) setting in the S-CSCF, which are downloaded from the HSS on a per user basis, as described in TS 23.228 [20]. The iFC for the PUCI service can be configured based on subscription or on operator policy. It is recommended that the PUCI function is invoked as early as possible in order to perform the PUCI functions before further handling of other functions. The handling of originating and terminating requests may differ.

Initial Filter Criteria (iFC) are included in the user profile (described in TS.23.228 [20] Annex B), which is downloaded from the HSS to the S-CSCF as part of the registration procedure. The "PUP Routing Profile" (clause 8.2) *could* thus be encoded using the iFC Priority field and the AS name for the ServerName field. The Priority field values (increasing order) then indicate the ordering of the ASs to traverse. Moreover, the "PUP PUCI Flag" (clause 8.2) *could* be encoded simply in terms of whether the iFC for calling a PUCI Function/AS is enabled or disabled (or present vs absent) for a particular subscriber. The remaining information in clause 8.2, PUCI Threshold and PUCI Action, *could* be stored in the PUCI Function/AS itself. This way, specification changes to the HSS or Cx interfaces would not be needed.

8.4 Compatibility with IMS centralized services, SRVCC, and service continuity

8.4.1 General

As stated in TR 33.937 [3], it is desirable to strive for a consistent user experience across access scenarios. Thus, it is important to ensure that the approach chosen for PUCI can be made compatible with IMS Centralized Services (ICS), Single Radio Voice Call Continuity (SRVCC), and Service Continuity (SC).

8.4.2 Mechanisms based on supplementary services

The sole purpose of IMS centralized services (see e.g., TS 22.101 [5], clause 22) is to use the IMS service engine to provide the telephony service for the CS access in addition to the PS access. This also implies that the same IMS TAS (including supplementary services according to 22.173 [4]) will be used irrespectively of whether the user uses a CS access or a PS access. As a result, when the SS-based PUCI functionality is used, this will be provided for the user irrespectively of access, and by the same service engine. No additional functionality will be required to handle these cases, and no limitations are foreseen.

If SRVCC is applied, this will not impact SS based PUCI functionality, as the service engine is not changed. The same applies when using Service Continuity in general, as the service engine remains the same.

Thus, mechanisms in TR 33.937 [3] based strictly on the use of existing mechanisms in Supplementary Services (SS) will also be compatible with ICS, SRVCC, and SC.

8.4.3 IMR

IMR PUCI functionality is executed by the iFC settings in the S-CSCF, which are downloaded from the HSS on a per user basis (TS 23.228 [20]). Since the detection of unsolicited users is performed only at the session setup defined in the iFCs, the marking of the session with a UC score and other PUCI related information is independent of further handling by other application servers. When the session is established, then there is no functional impact on mid-call features like SRVCC and SC, which are executed by the SCC AS. There is also no impact to ICS since with this feature all sessions are anchored in the TAS for supplementary service handling in IMS, which is a separate application server and which is like the SCC AS invoked by the iFCs after the PUCI AS.

NOTE: UE involvement is out of scope.

9 Solution alternatives

9.1 High level architecture

This section describes the high-level architecture for PUCI in case of using the PUCI functions IMR, mechanisms based on supplementary services as well as extensions to supplementary services. The PUCI functions are hosted by a PUCI application server (PUCI AS), which supports at least one of the three methods, IMR, Supplementary Services (SS) or extended SS. The PUCI AS may be collocated with the Telephony Application Server (TAS), but iFC should point to the relevant SS to be executed for the PUCI functions. In general, the different options, as described in clause 9 of TR 33.937 [3] apply, i.e. the PUCI AS can be collocated with the TAS or separated. Figure 9.1-1 shows UE A as session originator and UE B as session terminator of the communication.

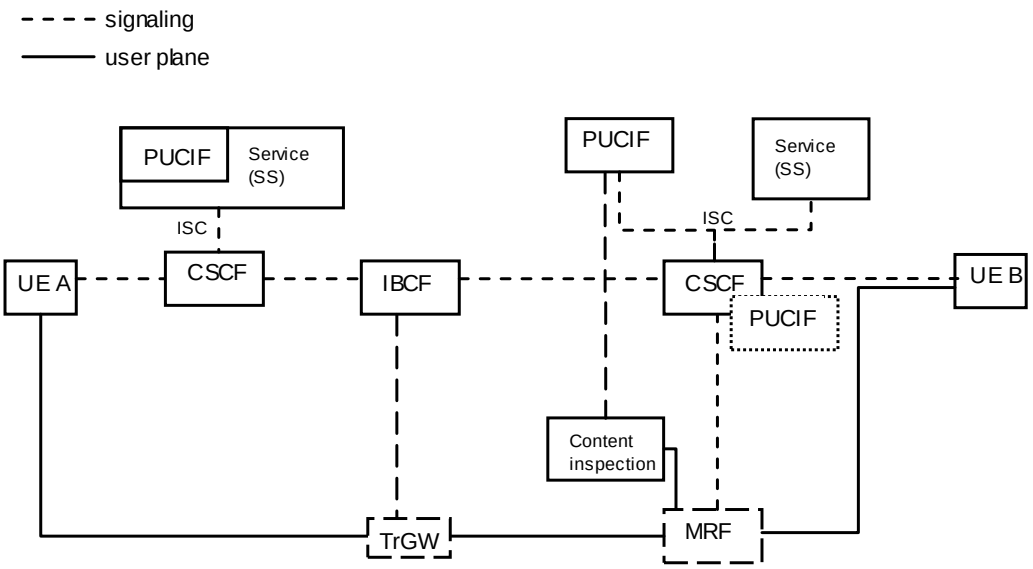


Figure 9.1-1: PUCI High-Level Architecture

10 PUCI information exchange

10.1 PUCI information type and structure

The intention of providing PUCI information is to alert that the corresponding session is matter of UC with a certain likelihood indicated by the UC Score. The PUCI information, e.g., the UC Score, is updated by the terminating PUCI AS according to the check(s) performed and it is used in the terminating S-CSCF for re-routing the session to an answering machine or elsewhere depending on user or operator policy of the terminating network. The threshold based on which a session is treated as UC is based on operator policies of the terminating network; the operator might also allow subscribers to set the threshold.

SIP proxies will, in accordance with their compatibility procedures, ignore the UC Score and the UC Indicator. Back to Back User Agents (B2BUAs) may however remove the UC Score and the UC Indicator. Therefore, an environment where UC Scoring is to be used successfully needs to ensure that no B2BUAs act on UC Scores.

The scoring information should consist at least of the following two basic parameters:

- UC Score: The parameter range is configured by the operator, indicating the likelihood of UC as well as the hostname where the PUCI test got executed.

If PUCI scoring takes place in the originating network, the interpretation in the terminating network of the UC Score generated in the originating network needs to be defined in the SLAs of the IMS level interworking. Possibly, multilateral SLA for all operators joining in the PUCI scheme may be advantageous.

In the general case, intermediary networks need to be considered. Whether this is an issue will depend on the concrete deployments. Note also that clause 10.2 would allow intermediary networks adding PUCI scores.

Corresponding SLAs should define originator of the particular UC Score because it is needed to for evaluation of the UC Score.

NOTE: If communication is happening within operator network then authentication is not needed.

- UC Indicator: This parameter should be a simple Boolean that is set by the originating network. It marks explicitly the sessions as UC or not and is evaluated by the terminating network.

The UC Score and the UC Indicator could be incorporated into the SIP header as shown in the example below:

NOTE: According to the text in this clause, the UC score is always present when the UC indicator is present. It could not be determined, in general, in how far the latter adds value in the presence of the former. This question will have to be solved for individual deployments.

INVITE sip:bob@example.net SIP/2.0

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

UC-Score: 75 by sip.example.net;

UC-Indicator=true;

Via: SIP/2.0/UDP sip.example1.net;branch=z9hG4bKxyz;received=192.8.2.1

UC-Score: 80 by sip.example1.net;

UC-Indicator=true;

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 excluded from this example...]

10.2 PUCI information signalling

Figure 10.2-1 shows a message sequence of PUCI signalling. UE A, in the figure, is the sending or calling party while UE B is the receiving party or callee. UE B is protected against unsolicited communication with the PUCI service. In case UE A and UE B belong to different operators or are roaming, the originating or intermediary operators may already perform PUCI checks before forwarding the session to the terminating operator. The registration step R is executed at the time of the registration of UE B this step is part of the regular Cx-Put/Cx-Pull operation (Public User Identity, Private User Identity, S-CSCF name) to the HSS and the corresponding Cx-Put Resp/Cx-Pull Resp (user information) to the S-CSCF.

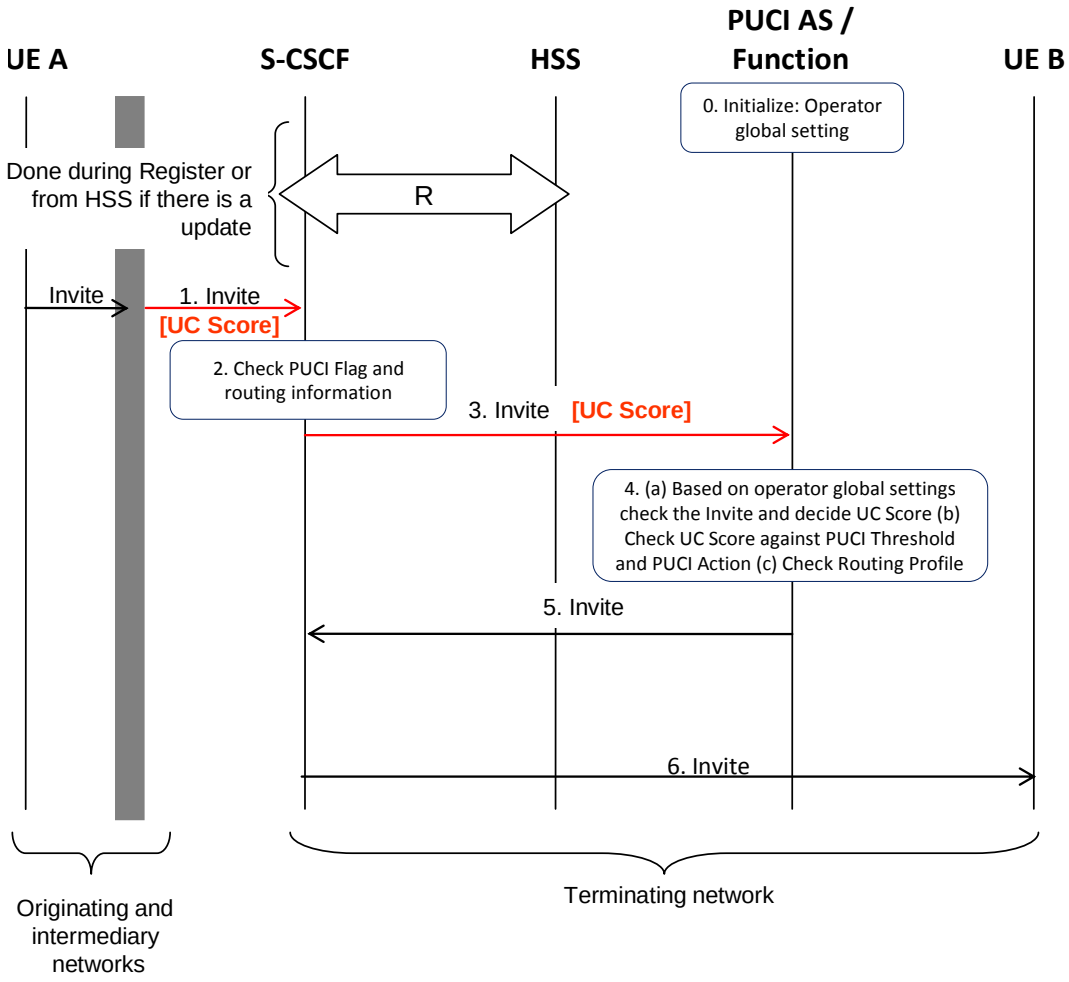


Figure 10.2-1: Simple PUCI service invocation (those in red need to be standardized).R. : The Callee (UE B) side S-CSCF and the HSS exchange messages over the Cx interface as required for the IMS registration procedure.

0) The PUCI AS is initialized with global operator settings, e.g. black-list that applies to all users for which the operator has legal consent.

1) The S-CSCF receives a SIP INVITE message from the Caller (UE A). This message may include UC Score and other PUCI information if PUCI check was already performed in any of the networks through which the message traversed.

NOTE: Addition of UC Score in SIP header needs IETF work.

2) Then the S-CSCF checks whether the PUCI Flag is on for the given Callee (UE B).

3) If the PUCI service applies for the Callee (UE B) then the PUCI AS/Function is invoked by the S-CSCF. For this, the S-CSCF sends a SIP INVITE message to the PUCI AS/Function. This message may include UC Score if it was already provided in Step 1.

4) The PUCI AS then checks the operator global setting and provides PUCI filtering based on techniques like those given in Section 3 of [15]. Other techniques could also be possible, e.g. CAPTCHA. These checks result in an updated UC Score. The PUCI AS also verifies the UC Score against PUCI Threshold and PUCI Action if all is fine then, based on the Routing Profile, the PUCI AS sends the SIP INVITE with the UC Score to another PUCI AS for further checks or sends it to the S-CSCF.

5) The PUCI AS sends the SIP INVITE message to the S-CSCF.

6) The S-CSCF then forwards the SIP INVITE to the Callee (UE B).

10.3 PUCI function communication

In case of a distributed PUCI AS or functions for IMR, different functionalities (e.g. MCD, black/whitelist check, turing test, etc) can be hosted in different ASes. For this reason UC Score should be indicated from one PUCI function to other within or in different ASes. The UC Score will be added up; operator can give weight to a given PUCI function. Each PUCI function will check whether the UC Score has reached a threshold based on which the given communication will be considered a UC. The threshold for the UC Score can be set by the operator.

The UC Score can be in the simplest way a linear function of the corresponding metric, e.g. call rate. An example of determining the UC Score is shown in Figure 10.3-1:

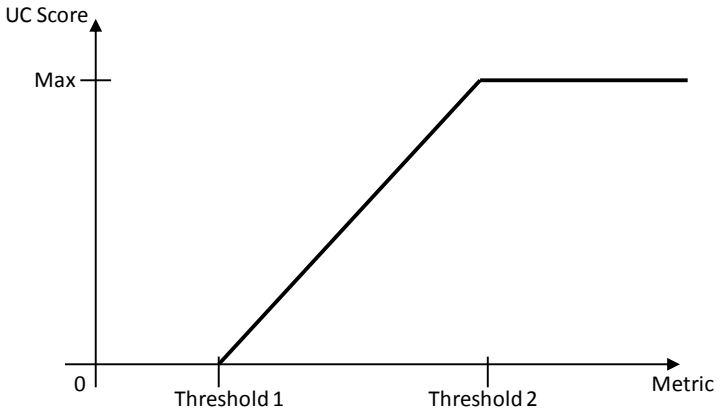


Figure 10.3-1: Simple UC Score excample.

Once the metric exceeds a certain threshold 1 (e.g. call rate > 15/min), then it starts creating a corresponding UC Score for the session up to a threshold 2, where already the maximum UC Score is reached.

How to combine the UC Scores is up to the operator policy. A simple example is shown in Figure 10.3-2.

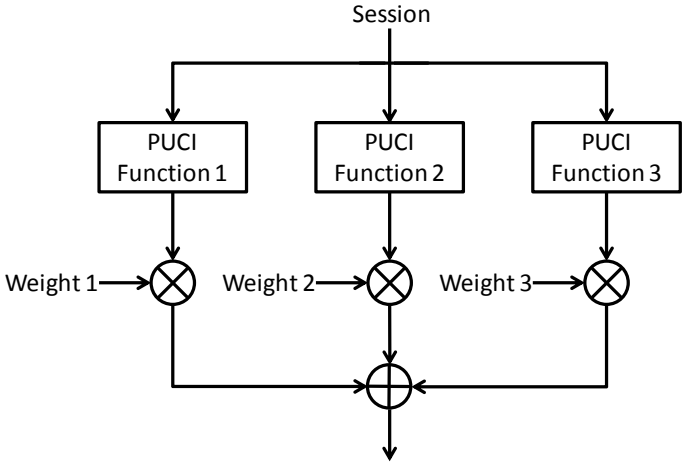


Figure 10.3-2: Simple UC Score accumulation excample.

The different PUCI functions generate a UC Score which is weighted based on the operator's policy and simply combined. How to weight is out of scope of this specification.

In case UC Score is used there could also be a necessity of communicating PUCI UC Score between PUCI ASes of different networks. This will happen in cases where call originates and ends in different network.

Privacy issues are subject to national regulations and may lead to restrictions on inter-operator PUCI information.

10.4 PUCI user notification

Depending on operator policies, IMS should support capabilities that allow notifying an originating party that a performed or attempted communication to the terminating party has been classified as UC. As a result of this classification the originating party maybe added to a list of UC sources. Optionally, IMS may notify to the originating party a way to request itself to be removed from being a UC source; example a telephone number or URL. The notification is limited to IMS, for example an infected IMS terminal.

11 Conclusions and recommendations

Solutions, i.e. supplementary services based and IMR, for protecting IMS from unsolicited communication (UC) were discussed in 3GPP SA3 working group. Discussion in SA3 did not lead to agreement and thus conclusion on items that should be standardized and at which level. However identification of origin of calls was considered as a building block which maybe used in future 3GPP work.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2011-11	SP-54	SP-110687	--	--	Presentation to SA for Information	0.5.1	1.0.0
2012-02	SP-55	SP-120031	--	--	Presentation to SA for Approval	1.0.0	2.0.0
2012-03	SP-55				Approved	2.0.0	11.0.0