# 3GPP TR 33.837 V2.0.1 (2009-12)

*Technical Report*

## 3rd Generation Partnership Project;
## Technical Specification Group Services and System Aspects;
## Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)
## (Release 9)

Keywords

IMS, SIP, SECURITY

***Copyright Notification***

# 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 scope of this report is to develop solutions to protect mobile subscribers from receiving unsolicited communication over IMS and to analyze these solutions in respect of their requirements and impacts on standardized interfaces.

This activity will take into account the study done in TISPAN TR 187 009 on “Feasibility study of prevention of unsolicited communications in the NGN”. This work will also be coordinated with ongoing activity in other SDOs (e.g. TISPAN, IETF and OMA). It is preferred that a common solution can be defined for protection against UC in both IMS and NGN deployments.

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

[2] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”.

[3] 3GPP TS 22.228: “Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1”.

[4] Internationales Anti-SPAM-Recht from ‘Bundesamt für Sicherheit in der Informationstechnik’, page 42 to 45, http://www.bsi.de/literat/forumkes/kes0508.pdf

[5] Spam Regulation Overview from Caslon Analytics, http://www.caslon.com.au/spamnote.htm

[6] Combating SPAM Through Legislation – A Comparative Analysis of US and European Approaches from E. Moustakas, Prof. C. Ranganathan, Dr. P. Duquenoy, http://www.ceas.cc/papers-2005/146.pdf

[7] Stemming The International Tide Of SPAM – Trends in Telecommunication Reform 2006 from John G. Palfrey, Jr., http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf

[8] Report Of The OECD Task Force On SPAM: Anti-SPAM Toolkit of Recommended Policies And Measures, http://www.oecd.org/dataoecd/63/28/36494147.pdf

[9] ITU Survey On Anti-SPAM Legislation Worldwide on WSIS Thematic Meeting on Cybersecurity 2005, http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf

[10] EU Symposium 2006: Countering SPAM In A Digital World from Cristina Bueti, http://spamsymposium.eu/files/Cristina%20Bueti.ppt

[11] RFC 5039 "The Session Initiation Protocol (SIP) and Spam”

[12] 3GPP TS 29.328: “IP Multimedia Subsystem (IMS) Sh interface; Signalling flows and message contents”.

[13] 3GPP TS 29.329: “Sh interface based on the Diameter protocol; Protocol details”.

[14] 3GPP TS 24.611: “Anonymous Communication Rejection (ACR) and Communication Barring (CB)using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification”.

[15] 3GPP TS 29.228: “IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents”.

[16] 3GPP TS 29.229: “Cx and Dx interfaces based on the Diameter protocol; Protocol details”.

[17] Identity Verification on the Fraud Forum manual of the GSMA, FF.21 Ver 2.0.

[18] "Enchancements for Authenticated Identity Management in the Session Initiation Protocol (SIP Identity)", IETF RFC4474, 2006-08, http://www.ietf.org/rfc/rfc4474.txt

[19] Microsoft Live Hotmail Under Attack by Streamlined Anti-CAPTCHA and Mass-mailing Operations, http://securitylabs.websense.com/content/Blogs/3063.aspx#

[20] Sender Policy Framework, IETF RFC4408, 2006-04, http://www.ietf.org/rfc/rfc4408.txt

[21] Domainkeys Identified Mail, IETF RFC4871, 2007-05, http://www.ietf.org/rfc/rfc4871.txt

[22] Concerns around the applicability of RFC4474, IETF, 2008-02, http://tools.ietf.org/html/draft-rosenberg-sip-rfc4474-concerns-00

[23] A framework for consent base communication in SIP, draft IETF, 2007-11, http://tools.ietf.org/id/draft-ietf-sip-consent-framework-03.txt

[24] Addressing an Amplification Vulnerability in SIP servers, draft IETF, 2009-02, http://tools.ietf.org/html/draft-zourzouvillys-sip-via-cookie-00

[25] 3GPP TR 33.828 "IMS media plale security"

# 3 Definitions, Symbols and Abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [2] 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 [2].

**Unsolicited Communication [3]:** Unsolicited Communication (UC) denotes bulk communication in IMS where the benefit is weighted in favour of the sender. In general the receiver(s) of UC do not wish to receive such communication. UC may comprise of, e.g., “SPam over IP Telephony (SPIT)" or "SPam over IP Messaging (SPIM)”.

NOTE: In this TR we also look at communication that is not necessarily bulk communication.

## 3.2 Symbols

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

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [2] 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 [2].

| | |
|---|---|
| ACR | Anonymous Call Rejection |
| AS | Application Server |
| BL | Black List |
| DSL | Digital Subscriber Link |
| PUCI | Protection against Unsolicited Communication in IMS |
| SPIT | Spam over IP Telephony |
| UC | Unsolicited Communication |

# 4 System Environment for PUCI

## 4.1 Architectural Issues

### 4.1.1 Introduction

This clause tries to give an overview about UC prevention techniques, tries to classify them and to discuss the architectural impacts on IMS.

Figure 4.1-1 shows seven levels of UC prevention, ordered by complexity and impact on IMS from the base to the top of the pyramid. The lower five levels can be realized without any changes required for IMS interfaces and IMS protocols (applies for level 5 only, if the UC feedback is not based on changes in SIP signaling). This means that level 1 to 5 can be made available relatively easily. The highest three levels provide on the one side enhanced UC prevention functionality, but require on the other side changes in IMS interfaces and/or IMS protocols. For level 5 this statement is only valid for a SIP-based UC user feedback. The pyramid is as well horizontally split into two parts: a part with non-technical UC protection measures, the basis of the pyramid, and a part with technical UC protection measures, building upon this basis.

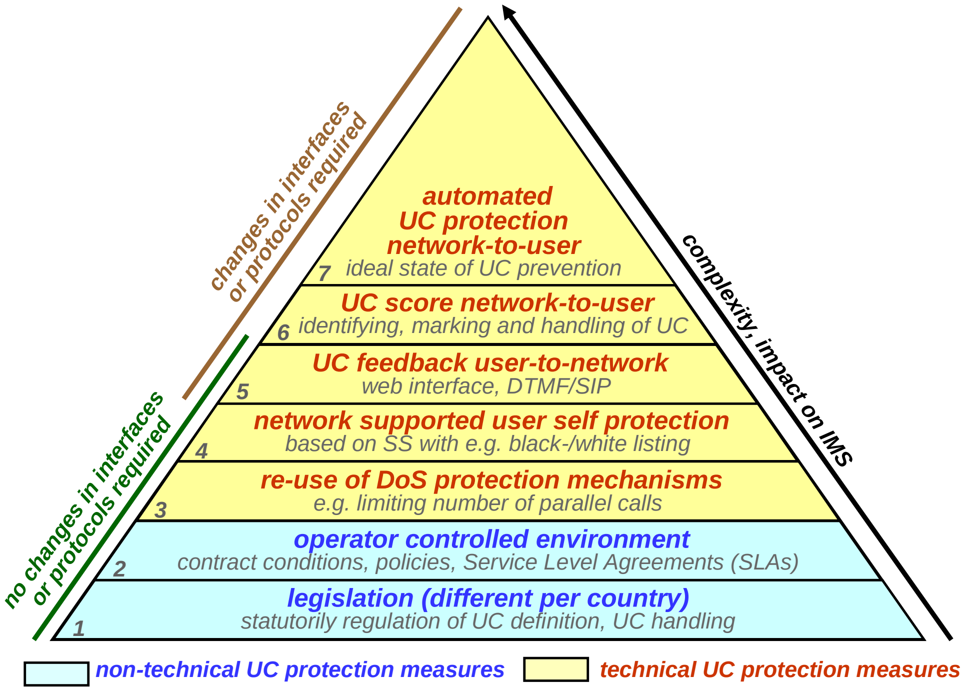

changes in interfaces or protocols required
no changes in interfaces or protocols required
complexity, impact on IMS
7 automated UC protection network-to-user
ideal state of UC prevention
6 UC score network-to-user
identifying, marking and handling of UC
5 UC feedback user-to-network
web interface, DTMF/SIP
4 network supported user self protection
based on SS with e.g. black-/white listing
3 re-use of DoS protection mechanisms
e.g. limiting number of parallel calls
2 operator controlled environment
contract conditions, policies, Service Level Agreements (SLAs)
1 legislation (different per country)
statutorily regulation of UC definition, UC handling
non-technical UC protection measures
technical UC protection measures

**Figure 4.1-1: UC Prevention ordered by complexity and impact on IMS**

It is important to mention that authenticated users with strong identities are the prerequisite for many UC prevention measures shown in the pyramid.

The illustration of UC prevention in the form of a pyramid implies in no way that all levels of the pyramid have to be realized in order to provide UC prevention. If for example UC related legislation does not exist in a certain country, then level 1 of the pyramid is not present. But if, however, UC related laws have been passed in another country, these laws have to be observed by all higher UC prevention layers. It is also possible that some intermediate or the top UC prevention layer may be omitted, e.g.

- there may be networks that are not operator controlled (→ level 2 of UC pyramid is missing)
- technical UC prevention could end at layer 5 or could even start with layer 5.

But according to the defense in depth principle it is likely that UC prevention relying on a number of synchronized prevention measures is less susceptible to circumvention attempts than a single UC prevention measure.

The statement that level 1 to 5 of the UC prevention pyramid require no changes in interfaces and/or protocols and the fact that they can be made available relatively easily implies that no principal architectural issues are related to theses

UC prevention measures. The most challenging impacts concerning network architecture generally and IMS architecture in particular are associated with level 6 of the UC prevention pyramid, that is to say 'UC score network-to-user', and level 7, which may be based on scoring.

Therefore the main part of this chapter deals with architectural impacts of UC identification and scoring. The intention is neither to give an exhaustive overview about all potential architectural impacts nor to provide/exclude any solutions but only to discuss some basic aspects of UC scoring.

In the following discussions UC score delivering equipment is regarded to be composed of two parts:

1. A UC Identification part (I) that gathers and provides UC relevant information, necessary to estimate a UC score
2. A UC Scoring part (S) that processes the information, gathered by the Identification part, according to a UC algorithm and delivers as result a UC score to be provided to the terminating user

The Identification part as well as the Scoring part can be centralized or distributed.

## 4.1.2 Originating/Terminating UC Identification and Scoring

This section discusses whether UC scoring should be located in the UC originating network or in the UC terminating network

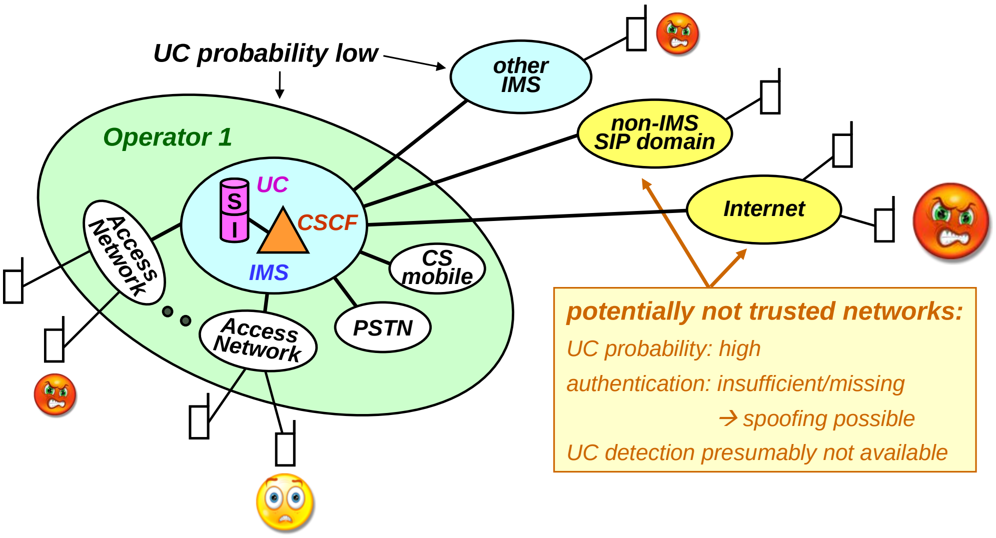


**Figure 4.1-2: Originating/Terminating UC functionality**

<u>SPITter inside the network of Operator 1</u>

In this case operator 1 is able to authenticate the SPITter and to react to him, e.g. by contract conditions or traffic restrictions. If equipped with a UC scoring equipment, then he can deliver a UC score to his users and the users of other networks, if so standardized. This UC score can be based on reliable information, as it is determined in the UC originating network, where identity spoofing is hardly possible and a maximum of signaling and/or media information is available to determine the UC score. (But note that a UC score can never be fully reliable in the individual case as it is likely to be based on statistical information and heuristic algorithms).

<u>SPITter inside another trusted IMS network</u>

Similar considerations as for the first case apply as the terminating network can reliably identify a caller in another trusted IMS network.

<u>SPITter inside a potentially un-trusted non-IMS network</u>

In this case the SPITter is in another network, but in contrast to another IMS-network the network (e.g. a non-IMS VoIP network) may be potentially un-trusted. This means that a UC score, if delivered by the potentially un-trusted non-IMS network, may as well be regarded not reliable.

If operator 1 tries, however, to determine a UC score in the UC terminating (his own) network, this is difficult. It must be taken into account that the use of a UC score - determined in the terminating network - may be questionable or even dangerous, in addition to the unavoidable uncertainties associated with a score, as the originating identity may be spoofed and the database of a UC scoring equipment is likely to be based on the originating identity. In case of spoofed originating identities, terminating UC scores will distort the UC databases and can be used for UC scoring attacks to the detriment of legitimate users, attempting to damage their reputation.

But if so standardized, the operator of the other non-IMS network could implement strong authentication measures and similar UC prevention standards as the IMS operator 1. If this other network could be regarded as trusted, then operator 1 could rely on the received UC scores to a higher degree.

The conclusion of the discussions above is that UC identification and scoring would be most effective and reliable in the UC originating network. But terminating networks can't rely on that, if connected to potentially un-trusted networks. The alternative to determine the UC scores in the UC terminating network is associated with fundamental problems.

Another impression is that there is a certain imbalance of effort and benefits between trusted networks like IMS, where technical effort to combat UC at the source may be high while the probability of using IMS networks as a UC source is expected to be low, and potentially un-trusted VoIP networks, where the technical effort to combat UC at the source may be low while the probability of using such networks as a UC source is expected to be high.

Conclusion:

The observed difficulties suggest that agreements on a minimum level of UC measures standards in all – IMS- or non-IMS - networks to which an IMS network is connected are required if UC measures in general, and scoring in particular, used to protect IMS users are to be effective.

## 4.1.3 Central/Distributed UC Identification and Scoring

This section discusses some aspects whether UC prevention functionality should be distributed over several types of networks (e.g. access, IMS, transit) or should be concentrated in a specific network (e.g. IMS), and, if the latter, whether it should be concentrated in one or several IMS components. The presented architectural variants need to be considered before taking a decision on the PUCI architecture, but the conclusions here are by no means final yet.

### 4.1.3.1 Distributed UC Identification and Distributed UC Scoring

A largely distributed UC prevention approach is shown in ETSI TR 187 009 'Feasibility study of prevention of unsolicited communication in the NGN'. The majority of network based UC prevention scenarios in chapter 6.5 'NGN design impact' shows a distributed UC functionality (identify, mark) that is located in the access network, in the core network and in the residential network (residential network is called home network in TR 187 009). Other networks like transit networks are not regarded. This approach assumes that every scoring entity communicates their scores to the entities further down the communication path.

Figure 4.1-3 shows an IMS-to-IMS call with a completely distributed UC (identification, scoring) approach.

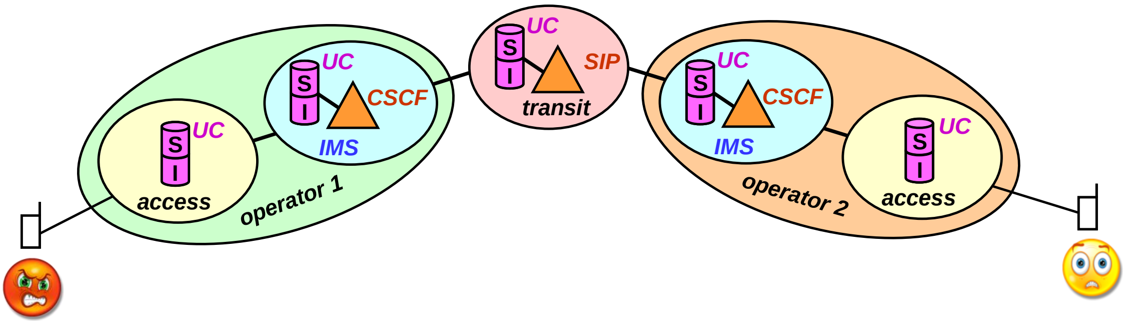


**Figure 4.1-3: Distributed UC identification and distributed UC scoring**

The issues of a completely distributed approach are:

- the UC equipment is needed at multiple locations → high cost
- the distributed UC scoring parts are, in general, not synchronized and may be provided by different vendors → scoring results are likely to differ (see chapter 4.x.4)
- the distributed UC functionality may have influence on the complexity of UC related signaling enhancements (see chapter 4.x.4)
- the distributed UC functionality may have influence on the connection setup time as every network has to inquire its own UC database and wait for the corresponding UC score for every call attempt

Besides these general considerations it is not clear whether the access networks, mentioned in chapter 6.5 'NGN design impact', are access networks in the sense of IMS. Although it may be possible to analyze SIP traffic in IMS access networks e.g. by deep packet inspection, the network elements of IMS access networks are not SIP aware and will therefore not insert any UC scores into SIP messages. As a result the conclusion can be drawn that IMS access networks are not well suited to support UC scoring.

This leads to another variant of the distributed approach where the UC functionality (identification, scoring) is still distributed, but centralized per operator. An example would be that UC functionality would be located in an application server communicating with all S-CSCFs, while other IMS functional entities would not be UC-aware. The UC entities in different networks would communicate their scores to UC entities in other networks.

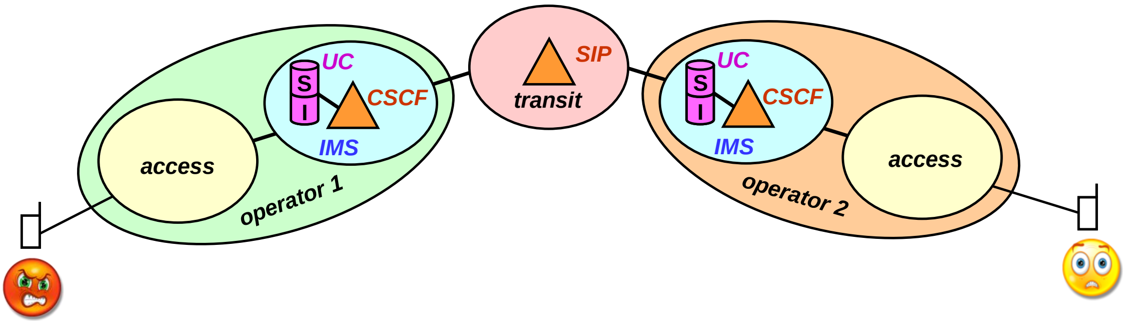


**Figure 4.1-4: Distributed UC identification and scoring, centralized per operator**

Figure 4.1-4 shows that in this case the number of UC equipment, necessary in the communication path, is significantly reduced. The consequence is that the quantitative aspects of the issues discussed above are reduced, but that the qualitative aspects remain.

A third variant of the distributed approach is that the UC functionality (identification, scoring) is still available in several networks, but the UC entities in different networks would NOT communicate their scores to UC entities in other networks, i.e. each operator would operate their UC functions independently, and react to the locally determined score. Within their own networks, operators could use a distributed or centralized approach. An example of a centralized approach would be, as above, that UC functionality would be located in an application server communicating with all S-CSCFs, while other IMS functional entities would not be UC-aware.

The issues of this third variant are as follows:

- each operator is independent from other operators in deploying identifying, marking and reacting functionality. This seems to make this a quite practical approach
- however, the effectiveness of UC scoring in the terminating IMS network still depends on measures in other operators' network (as discussed in chapter 4.1.2), e.g. regarding strong authentication or appropriate reaction at the source
- it follows from the two items above that the need for technical cooperation and business agreements among operators may be reduced, but not eliminated
- If networks do not cooperate wrt scores, they may not exploit the full available information. A consequence of this operator independent UC approach is that reaction on UC scores, determined in the originating IMS network, is only possible in the UC originating network

- the cost for UC equipment per operator depends on how the operator implements their UC functionality
- the distributed UC functionality may still have influence on the connection setup time as every network has to inquire its own UC database and wait for the corresponding UC score for every call attempt. However, this delay could be limited if only originating network, or only terminating network, or only originating network and terminating network, but no other networks, are involved, and there is a centralized approach in one network.

### 4.1.3.2 Distributed UC Identification and Central UC Scoring

A possibility to overcome one of the main disadvantages of a distributed approach is to centralize the scoring part (see figure 5). Centralization in this sense means a single scoring instance, located above the operator level and operated by a neutral organization. As the UC sensor functionality (identification part) has necessarily to be located inside the networks to monitor the signaling and/or media traffic, this functionality is distributed across different networks, as before. Whether all networks report to the central scoring instance, as shown in Figure 4.1-5, or only some of them is left open.

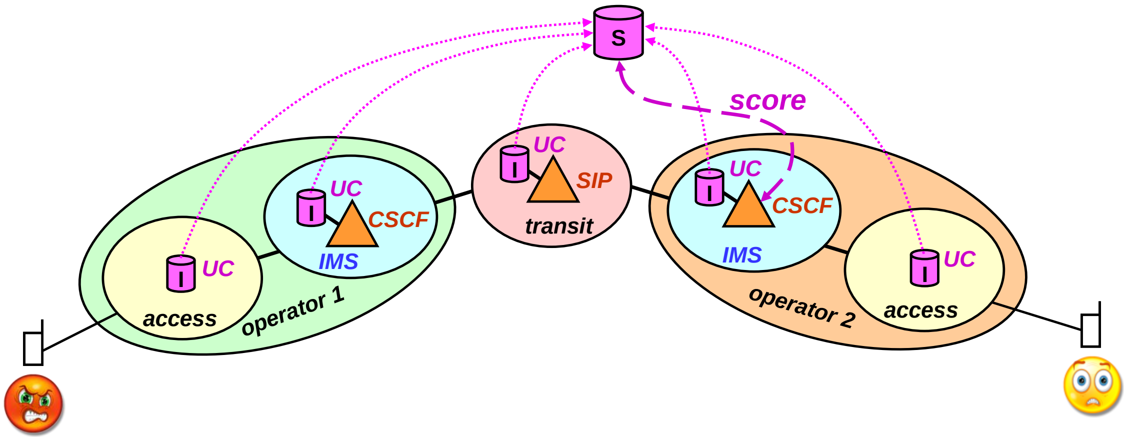


**Figure 4.1-5: Distributed UC identification, centralized UC scoring**

The issues of a distributed identification, centralized scoring approach are:

- the scoring part of the UC equipment is only once needed → possibly lower cost
- a central UC scoring part guarantees always consistent UC scoring results, as only one score is delivered. This does not necessarily guarantee the accuracy of the score, though.
- legal concerns may be related to a central UC scoring instance
- additional traffic is generated to transfer the UC identification information to the central UC scoring instance

## 4.1.4 Standardized/Vendor-Specific UC Scoring Algorithms

Another question is whether the scoring algorithms are standardized or whether they can differ, depending on the vendor of the UC equipment. This point is closely related to the topic 'centralized/distributed UC functionality'. Generally two different cases have to be distinguished:

<u>centralized UC scoring instance (see chapter 4.1.3.2)</u>

In case of a centralized UC scoring instance only one UC score is delivered which leads automatically to a consistent behavior, regardless how accurate the UC score is. Therefore no special need for a standardized UC scoring algorithm is seen.

<u>distributed UC scoring (see chapter 4.1.3.1)</u>

For this scenario the differentiation between standardized and vendor specific UC scoring algorithms is more interesting:

If the UC scoring algorithms are standardized, the scoring results of different vendor equipment are ideally identical. But then the question arises why the UC functionality should be installed multiple times in different kind of networks. The consequence for standardized UC algorithms would be to install the UC equipment only once in the network that is best suited. It is ffs study what this best suited network would be. It may also be doubted whether it is advisable to plead in favor of standardized UC scoring algorithms as agreements on 'the ideal algorithm' are difficult to achieve and changes of the algorithm to adapt to new UC scenarios are not easily possible.

If however the UC scoring algorithms are vendor specific, then differing UC scoring results are very likely in a distributed UC approach with the consequence that users and other UC entities in the network may have difficulties to determine the meaning of a score received from another entity as the semantics of the score would not be standardized. Furthermore, the syntax of SIP signaling enhancements may become complicated. In Figure 4.1-6 a SIP message is shown that travels from the SPITter across different networks, all of them equipped with UC functionality, and in the worst case all from different vendors. According to our assumption the UC scoring algorithms are vendor specific and differ in this example from low to high.

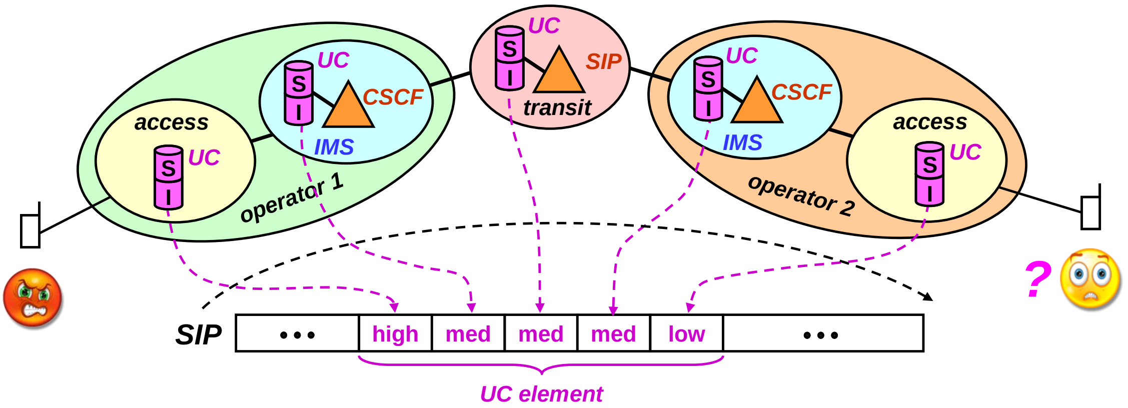


**Figure 4.1-6: Vendor specific UC scores in a distributed approach**

As every UC equipment must be able to deliver its score, SIP signaling enhancements would have to provide possibilities to transfer multiple UC scores. Various possibilities are available to handle the potential consistency problem, none of them really convincing:

- deliver all scores to the user → confusing
- deliver a UC range (min, max) to the user → confusing
- deliver an averaged UC score to the user → not confusing, but potentially wrong
- deliver only one score (first, last, ?) to the user → not confusing, but potentially wrong
- potentially others?

# 4.2 Non-Technical Conditions

## 4.2.1 Prevention of Unsolicited Communication in an Operator Controlled Environment

### 4.2.1.1 Introduction

This clause discusses how IMS providers could take advantage of the particularities of the IMS environment, compared to a general environment, in which SIP and VoIP services may be offered, with respect to SPIT/UC prevention.

The most salient feature of the IMS environment is that it is fully controlled by the operators. This environment is similar to what is called "Centralized SIP Providers" in RFC5039 by Rosenberg and Jennings. "Centralized SIP Providers" are a variation of Circles of Trust .According to the concepts in RFC5039 a number of providers get established as centralized SIP providers and act as a SIP equivalent to the interexchange carriers in PSTN. The relations between the centralized SIP providers are defined by Service Level Agreements. As inter-domain SIP providers charge the local providers for the delivery of SIP messages, a certain amount of cost is associated with this service. It should be noted, however, that agreements on charging issues by operators may be subject to national or regional regulations.

Rosenberg and Jennings draw the conclusion that this arrangement could work, as there is relatively little SPAM in PSTN today compared with Email.

The assumption is that exploitation of a regulated operator environment could be as effective as or even more effective than any detailed SPIT/UC prevention technique involving the user. Related to this concept, IMS provides a systemic advantage compared to general VoIP deployments, as

- IMS is an operator controlled network
- IMS allows Service Level Agreements among IMS operators preventing SPIT/UC at the source

Now, IMS users will not only call or be called by other IMS users, especially, but not only, in the initial phases of IMS deployment. There will certainly be calls to and from the PSTN, but, in the interest of universal reachability, also calls to and from other VoIP networks are likely to occur. It should be studied whether inter-working with other VoIP operators could be based on similar Service Level Agreements. A proposal is an association of VoIP operators adhering to a common code of conduct regarding SPIT/UC. This would be especially important as SPIT/UC is most effectively combated in the source network, in which the SPITter resides. Setting such non-technical conditions could make a significant contribution to the efforts of IMS providers to protect IMS users from SPIT/UC. They are unlikely, however, to be a panacea against SPIT/UC and should rather be seen as complementing other measures of more technical nature.

### 4.2.1.2 Current SPIT/UC Prevention Measures

This section analyzes the environment today, without sophisticated and synchronized SPIT/UC prevention techniques. The measures discussed are:

- legislation and regulation
- user authentication
- contract conditions

The basis for network operators is the legislation which may be country-specific. Already legislation can provide elements of SPIT/UC prevention, e.g. by

- providing national do-not-call lists for telemarketing with punishment in case of counteracting
- prohibiting bulk advertisement calls without consent of the user
- prohibiting usage of the anonymity feature for advertisement calls

Regulative authorities will supervise whether the rules are kept and will launch countermeasures like punishments or blocking of malicious users. Although the intention of legislation and the control by regulative authorities is favorable, the reaction time is slow and there may be possibilities to circumvent legislation. In addition, it may be difficult to enforce this legislation for SPITters in foreign countries.

Already today network operators face the problem to avoid misuse of cheap communication sources (usually flat rates), one of them being SPIT/UC. A centralized SIP provider is seen as an operator who controls his network in a way that his subscribers and also subscribers of other operator networks are affected as little as possible.

Besides contract conditions, discussed beneath, authentication of users is a topic whose importance is hard to underestimate. Authentication is not a SPIT/UC prevention measure in itself, but is the indispensible basis to take actions against SPIT/UC. Measures against SPITters based on contract conditions are only effective if the SPIT/UC source can be clearly identified.

Today (first half of 2009) SPIT/UC prevention is mainly achieved on the basis of contract conditions. Contract conditions restrict the usage of national and international flat rates that are prone to SPIT/UC because of their low cost

- to private usage ,
- prohibit specifically commercial usage like bulk communication services, call centers and telephone marketing

- and threaten to charge connections violating the contract conditions at standard prices.

As it may be difficult for providers to prove misuse of flat rates, contracts often provide the possibility for short-term contract cancellation without giving reasons.

Another variant of contract conditions combine flat rates with either traffic or time measurement techniques, cf. also clause 5.2. In case of traffic measurement the bandwidth is limited after a certain volume of traffic is reached while in case of time measurement the flat rate conditions are only valid if a certain threshold of time is not exceeded. In the proper sense of the word these contracts are not longer flat rates but volume or time tariffs in disguise. The goal seems to give legitimate users the feeling of a flat rate while limiting network resources to illegitimate users.

To gain an understanding of how relations between IMS and external VoIP operators could evolve, it is important to regard the relations between VoIP and legacy networks today. Especially the relations between upcoming, public Internet-based VoIP providers and traditional legacy network operators are interesting.

As long as the calls are VoIP and use the public Internet, they are free-of-charge and the contract conditions remain simple. If public Internet VoIP operators connect however to a legacy network, the calls are charged with a low price that pays the legacy part of the connection.

If such public Internet VoIP providers sell legacy network flat rates, their contract conditions get stricter and converge to those, offered by legacy operators. Examples based on today’s practice are:

- users have to comply to so-called fair user guidelines limiting the maximum number of telephone minutes to 10000 → if threshold is exceeded, calls are charged according to usual conditions
- in other cases no explicit limits are defined, but restrictions are based on contract conditions like
  • only human-to-human communication allowed
  • commercial usage excluded
  if contracts are violated calls are charged at standard prices

There are two interesting observations which can be made:

1. Public Internet based VoIP providers work in a way similar to established operators when connecting to legacy networks
2. low charges compared to free-of-charge seem to diminish network misuse a lot

# 4.3 Technical versus Legal Issues

## 4.3.1 Introduction

This clause tries to highlight interdependencies between technical and legal aspects of UC prevention. It is based on the following sources: a German survey of UC related legislation concerning several countries (see Internationales Anti-SPAM-Recht [4], Spam Regulation Overview [5], Combating SPAM Through Legislation [6], Stemming The International Tide Of SPAM [7], Report Of The OECD Task Force On SPAM: Anti-SPAM Toolkit of Recommended Policies And Measures [8], ITU Survey On Anti-SPAM Legislation Worldwide [9] and EU Symposium 2006: Countering SPAM In A Digital World [10]. In case of further interest numerous additional links are included.

It is not claimed, however, to give a full and legally water-tight overview about UC related legislation. The goal of this clause is instead to show up by means of some examples how certain UC prevention techniques may be influenced not only by technical requirements but also by legal issues.

Figure 4.3-1 (from EU Symposium 2006: Countering SPAM In A Digital World) shows that a quarter to a third of the countries worldwide has taken action against UC, mostly those in the OECD area.

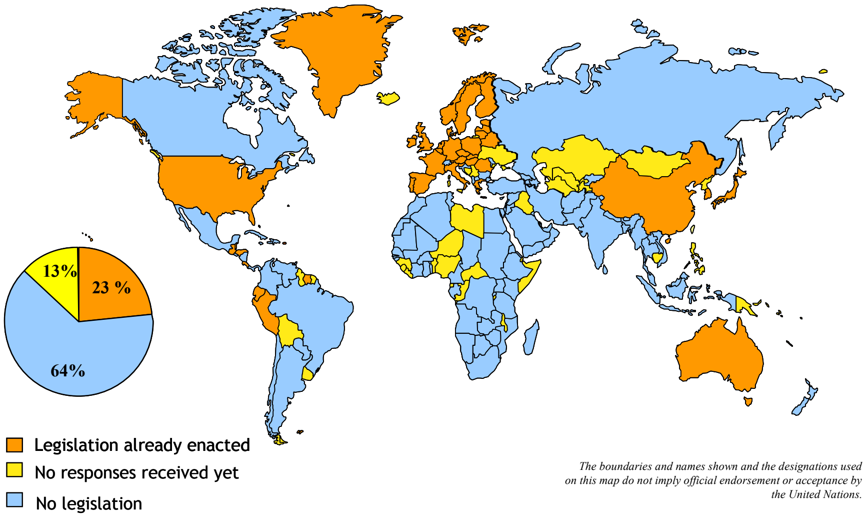

13%
23 %
64%
Legislation already enacted
No responses received yet
No legislation
The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

**Figure 4.3-1: Countries taken action against UC [10]**

UC legislation, as far as available today, is a national issue and may therefore (and does in reality) differ per country. As shown in Figure 4.3-1 UC specific legislation is not yet finished and thus the danger of a further fragmentation of country specific laws exist. In contrast to the country specific UC prevention legislation, IP-based communication (e.g. Email, VoIP) and the related problems like UC are international issues, which leads to a variety of cross-border problems.

There are differences in the

- definition of UC,
- definition of UC communication services,
- handling of UC communication,

leading potentially to problems in international communication.

It has to be mentioned that this clause uses generally the term UC, regardless whether in the underlying information sources the terms SPAM, SPIT, UC or others are utilized.

## 4.3.2 UC Legislation

### 4.3.2.1 Definition of UC

There is currently no uniform, worldwide-accepted definition of UC, neither in standardization nor in legislation.

Legislation usually restricts UC to electronic advertisement. This means that UC related legislation is not naturally in line with the broader definitions used in standardization. Customer nuisance like e.g. phishing or call-back cost scenarios are not classified as UC according to a typical UC prevention law.

The bulk character of communication is another element, often referred to. But not all bulk communication is UC, e.g. newsletters or alerting services. And besides bulk UC communication also individually directed nuisance-communication like stalking may be regarded UC.

Laws even differ in the definition of electronic advertisement. In some countries electronic advertisement must additionally have a commercial background (e.g. US), in others not (e.g. EU). Thus non-commercial advertisement like e.g. political, religious, ideological or scientific advertisement is allowed in the US while it is prohibited in the EU. Figure 4.3-2 tries to highlight the problems that occur e.g. in an international religious advertisement campaign.

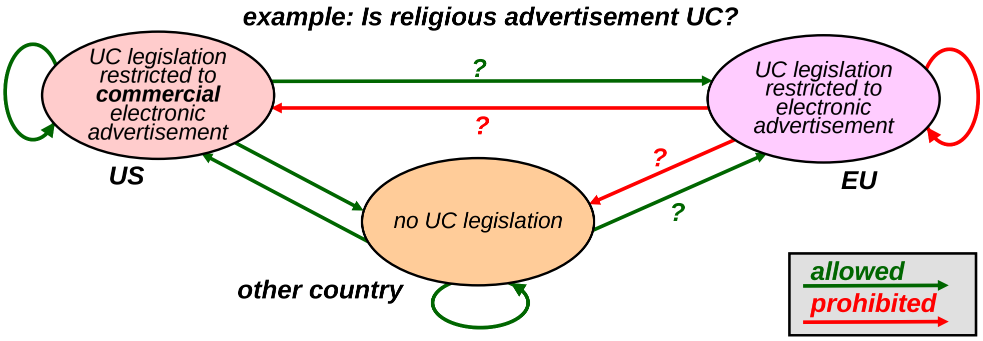

example: Is religious advertisement UC?
UC legislation restricted to **commercial** electronic advertisement
US
?
?
UC legislation restricted to electronic advertisement
EU
?
?
no UC legislation
other country
allowed
prohibited

**Figure 4.3-2: International religious advertisement campaign**

While the legislation in every country is clear, laws for the communication between the countries are missing and are left in a grey zone:

- Is it allowed to send religious bulk advertisement from the US (allowed) to recipients in the EU (prohibited)?
- Is it illegal to send religious bulk advertisement from the EU (prohibited) to recipients in the US (allowed)?

The difficulty for e.g. a UC reputation system, residing in one specific country, is that it is subject to the corresponding national law. That means that besides identifying and marking traffic technically as UC, the reputation system has to consider whether the communication is international, which the involved countries are, which legislation is valid and whether the technical UC classification corresponds to the legal situation.

### 4.3.2.2 Definition of UC Communication Services

Another point differing in national UC legislations is the definition which communication services are relevant to carry UC communication. There are two different approaches: either to cover explicitly specific low cost communication services (e.g. Email), susceptible to carry UC traffic, or to find a more generic and technology independent definition that covers besides existing services also communication services that might be used for UC in the future.

Currently UC is defined in the EU in a technology independent way, but with the given examples Email, VoIP, Fax and SMS. In Australia however the UC services are explicitly listed: while MMS and Instant Messaging are additionally included, compared to EU, Fax and VoIP are explicitly excluded.

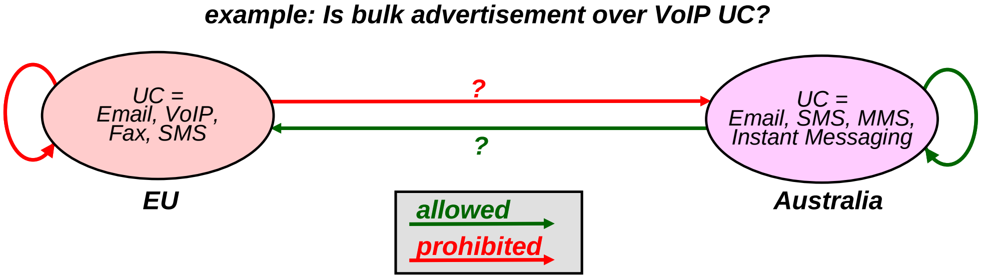

example: Is bulk advertisement over VoIP UC?
UC = Email, VoIP, Fax, SMS
EU
?
?
UC = Email, SMS, MMS, Instant Messaging
Australia
allowed
prohibited

**Figure 4.3-3: International bulk advertisement**

This constellation raises similar questions as the chapter before:

- Is it allowed to send bulk advertisement, based on VoIP, from Australia (allowed) to recipients in the EU (prohibited)?
- Is it illegal to send bulk advertisement, based on VoIP, from the EU (prohibited) to recipients in Australia (allowed)?

### 4.3.2.3 Consent Achievement about UC Communication

A third important principle is how consent about UC communication like e.g. bulk advertisement is achieved. If UC legislation in some country prohibits bulk advertisement that doesn't usually mean that bulk advertisement is unconditionally prohibited, rather it is prohibited without consent of the recipient.

Two main principles of consent achievement are in use:

- Opt-In principle
  The sender of the bulk UC advertisement has to assure and to prove that the recipient of the message has explicitly given consent.
- Opt-Out principle
  The sender is allowed to send bulk UC advertisement without consent of the recipient, but the advertisement messages have to provide an easy possibility for the recipient to get deleted from the address list so that further nuisance can be stopped in a timely manner.

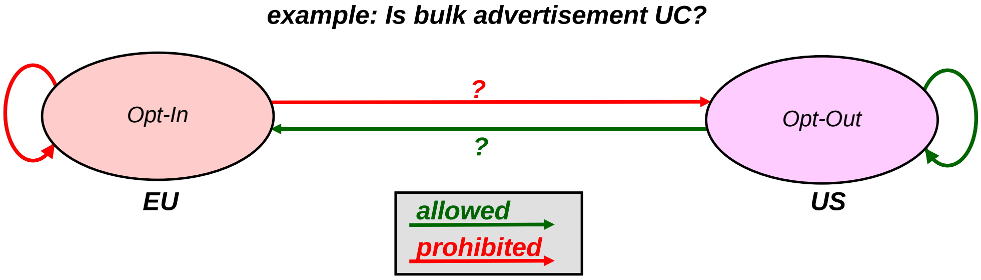


**Figure 4.3-4: Differences in consent achievement**

Figure 4.3-4 shows a constellation that is in principle comparable to that of chapter 4.x.2.2 and thus raises similar questions/problems.

The conclusion of Section 4.3.2 is that

- national laws show significant differences concerning UC legislation and operators have to pay attention to them
- differing UC legislation presents significant challenges to UC equipment being involved in national and international communication

## 4.3.3 Liability

This sub-clause tries to highlight the aspect of operator liability which is especially interesting in the context of UC scoring for calls running over the networks of more than one operator.

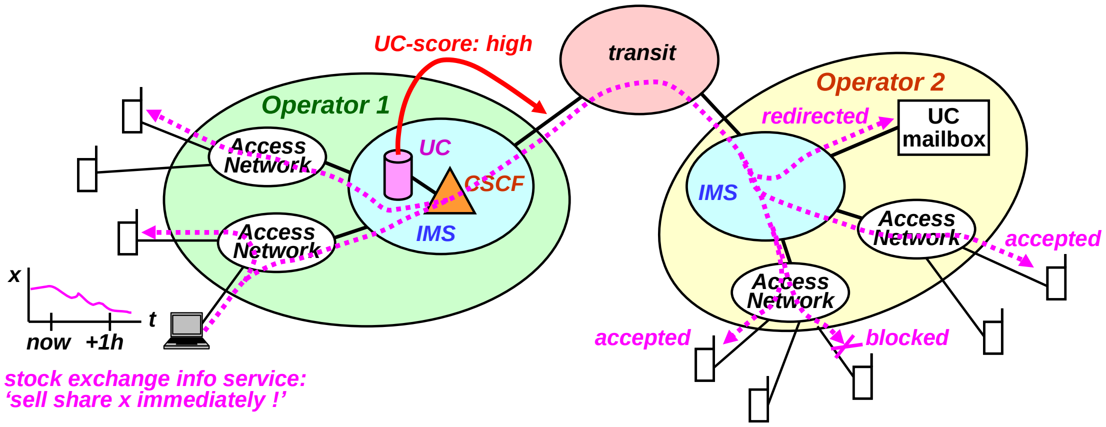


**Figure 4.3-5: Inter-operator liability aspects in case of UC scoring**

Figure 4.3-5 shows an example where a stock exchange info service in the network of operator 1 sends an alert message to a huge number of his customers to sell share x immediately. One hour after sending this alert message the share has fallen significantly. Due to the bulk character of the message it may be classified with a high UC score by a UC scoring system, residing in the network of operator 1. The message is marked with the UC score and send further to the customers of the stock exchange info service in the network of operator 2. Due to the high UC score it may happen that

- some of the customers accept the message despite of the high UC score, are therefore informed in-time and don't suffer a financial loss
- others may block the message, either by themselves or by means of UC filtering, or the network may be instructed to redirect messages with a high UC score to a UC mailbox. These customers miss the right point of time to sell share x and suffer therefore a financial loss.

With the wisdom of hindsight it turns out that the classification with UC score 'high' was wrong and that the message was indeed of a bulk character, but apart from that a completely legal notification service. Now the question will arise: Who is liable for the financial losses of the customers of operator 2, based on an erroneous UC score of a UC reputation system in the network of operator 1?

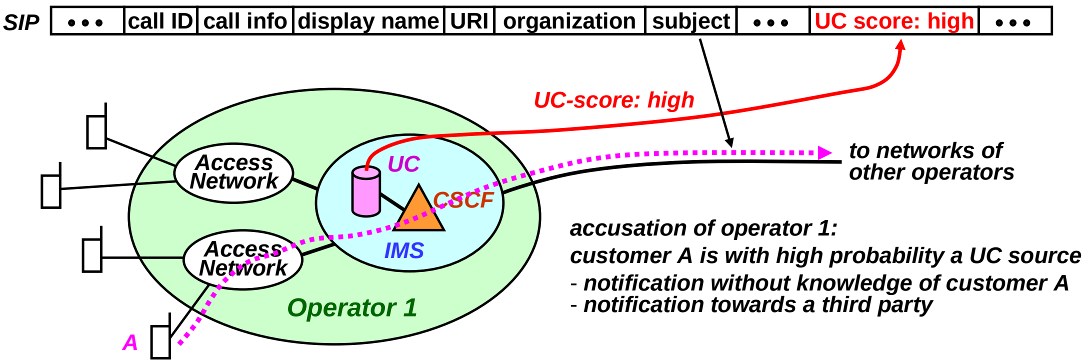
In the most general case that the networks of operator 1 and operator 2 are located in two countries with differing UC legislation, the UC reputation system has already to regard the different UC prevention laws (see chapter 4.x.2) and is now additionally confronted with a potentially different handling of liability by legislation.

In one country (e.g. Germany) UC filtering measures are only allowed if the customer has explicitly given consent. If a communication (e.g. Email, VoIP, Fax, SMS) is filtered (deleted or blocked or redirected) due to an erroneous UC score, then the operator is in principle liable towards the customer. Only if the operator is able to substantiate that the unjustified filtering occurred through no fault of the operator's, he is exempt from liability.

If the operator in another country (e.g. US) filters erroneously a communication, then he is not liable if he can show that he has acted in good faith in order to filter an illegal UC communication.

## 4.3.4 Privacy

Another legal aspect, especially related to UC reputation systems, is privacy. Up to now it is not practice to send ratings concerning own customers together with the signaling and to exchange them with other operators. This will necessarily change if UC scores are evaluated and send through the networks to the called party.



accusation of operator 1:
customer A is with high probability a UC source
- notification without knowledge of customer A
- notification towards a third party

**Figure 4.3-6: Privacy aspects of UC scores**

Figure 4.3-6 shows an example where the reputation system of operator 1 rates the call of customer A with the UC score 'high', for whatever reason. To support the called party in reacting, the UC score is e.g. sent together with the SIP signaling towards and through the networks of other operators.

This means that the signaling contains now besides the information, necessary to establish the connection, additionally the accusation that customer A is with high probability a UC source. But according to national laws (e.g. Germany) operators

- may have to regard their customer's privacy and
- may have to pay regard to the communication secret and to the right of informational self determination.

It is not clear whether it is allowed to concatenate personal information, present in the SIP message, together with a UC score, based only on circumstantial and not on solid evidence. This could negatively reflect on the person, even work as a kind of pillory, and make this combined information available to third parties without consent of the person, subject to UC scoring.

### 4.3.5 Conclusion

This clause shows that UC prevention can not solely be regarded as a purely technical measure without noticing that especially UC scoring has strong interdependencies to legislation. According to its national nature, UC related legislation refers to specifics of the corresponding countries and leaves therefore a fragmented legislation landscape from a global point of view.

The definition of UC, of UC communication services and the consent achievement about UC communication differ. Besides that also liability and privacy aspects have to be regarded according to national laws. Although the legal situation may then be clearly defined for communications in a specific country, the situation for international communications is likely to be unclear or contradictory as the legislations of the involved countries may differ.

As a consequence UC reputation systems will be burdened to handle besides the technical part of UC identification and scoring also the evaluation of the legal situation of a UC suspicious call. This may involve the existence of a dynamically changing worldwide legal database, evaluated according to the source and the destination of a call and the location of the operator. And even this effort may in many cases be in vain as a clearly defined legal interworking between the countries doesn't exist and therefore the problems are left in a legal grey-zone. Also for operators this situation is quite uncomfortable because it will not be easy for them to prove that their UC scoring complies with national or international laws. With this confusing situation the operators are also exposed dangers like lawsuits or claims for damages.

## 4.4 Coexistence with Single Radio-VCC, ICS, and SC

As a general principle, it is desirable to strive for a consistent user experience across different access scenarios. However, certain proposed PUCI features are problematic in this respect, and the feasibility of maintaining a consistent user experience warrants further study. A specific example of this is the use of UC user feedback, as stated in the requirements (Section 6.2).

Single Radio VCC, IMS Service Continuity, and IMS Centralized Services, enables UEs to use the CS as another access for reaching IMS services. In SRVCC, the UE could start a call over PS and then later transfer to a CS access due to coverage reasons. A question that arises is that if user feedback mechanisms are required during the call, and would be based on IMS procedures, how would the end-user experience be perceived if the end-user will not be able to provide feedback in case it will have done an access transfer to CS? Similar is true for an ICS scenario, where the user does not have PS access available.

What needs to be determined is whether it acceptable to have different end-user capabilities depending on access you currently are camping on. Otherwise, the mechanisms and procedures to solve these requirements will need to be generic enough, e.g., based on out of band procedures for service settings, or on re-using existing supplementary service handling for mid-call support. It is not regarded as viable to change the CS network to accommodate these requirements.

# 5. PUCI Risk Analysis

## 5.1 General

A necessary starting point before contemplating protection mechanisms is to understand the threats. These are not limited to violations of privacy, as there can potentially be more serious secondary effects. In the following discussion, we consider a set of threats and related scenarios as a means for arriving at requirements for protection mechanisms. All measures considered here are not proposals, but for discussion, and, for all of them, there must be a careful trade-off between the complexity imposed to IMS and the expected threat. In particular, the impact on IETF SIP standards and the IMS specifications must be taken into account.

## 5.2 UC Threats & Scenarios

### 5.2.1 Introduction

In this section we discuss UC threats against IMS and illustrate with concrete scenarios. These scenarios are used as a basis for considering to what extent existing features in IMS could be used to combat the threats, to what extent non-technical (legal and contractual) means might be most effective, and where new technical features are desired. Furthermore, the scenarios serve as context to discuss requirements for protection against UC derived in a TISPAN study to examine their validity for 3GPP. We first describe a general UC scenario, with certain common traits, and then proceed to discuss each threat, with relevant scenarios, in the following subsections.

### 5.2.2 General Scenario

In the general scenario we attempt to illustrate certain traits common to the different specific scenarios. Here we simply assume that there is a source of UC somewhere targeting one or more users. The purpose for the UC is immaterial for the purposes of this discussion. However, the general scenario can be subdivided into the following two cases:

1. the SPIT/UC source is inside the IMS network
2. the SPIT/UC source is outside the IMS network

Figure 5.2-1 shows a scenario where the SPIT/UC source resides inside IMS. The affected SPIT/UC victims can be inside and outside IMS. The fact that the SPITter is shown using DSL access is to be seen only as an example. The SPITter could just as well use other access networks, e.g. cable networks or other networks.

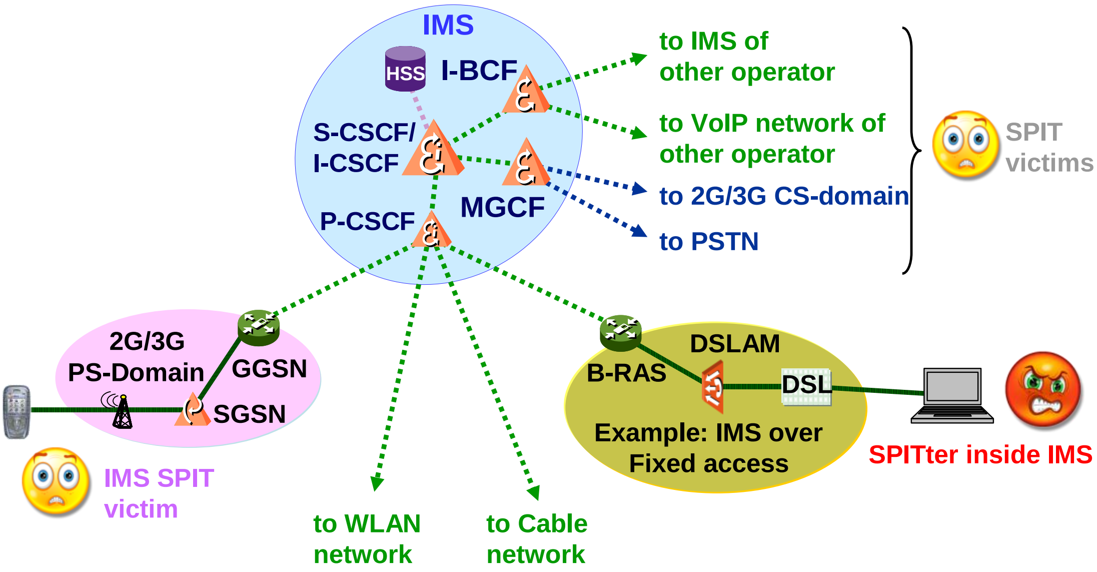


**Figure 5.2-1: SPIT/UC source inside IMS**

Figure 5.2-2 shows a scenario where the SPIT/UC source resides outside IMS. Besides SPIT/UC victims in other VoIP networks also subscribers of IMS may be affected. The fact that the SPITter is shown using DSL access is to be seen only as an example. The SPITter could just as well use other access networks, e.g. cable networks or other networks.

In case of SPIT/UC, residing in external networks, several different configurations are possible:

- DSL and VoIP service are provided by the same operator
- the VoIP provider is different from the operator
- the VoIP transport can be achieved by a network operator specific IP network or by the public Internet

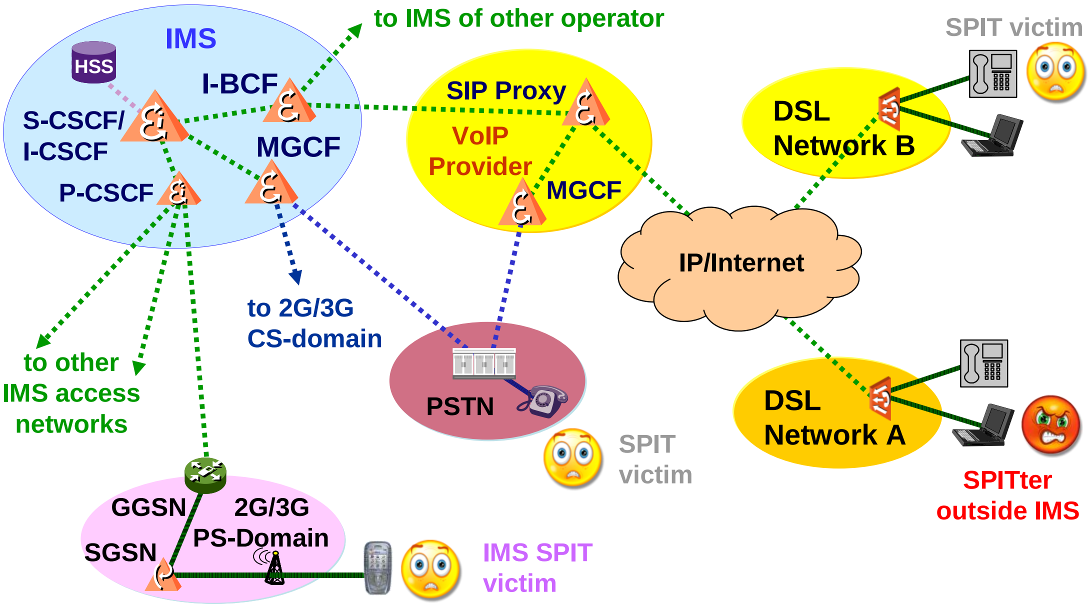


Figure 5.2-2: SPIT/UC source outside IMS

In either case, both non-technical and technical means may be employed to counter this threat,.But be aware that the applicability of technical means in the ‘SPIT/UC source outside IMS’ case is much more challenging

## 5.2.3 Privacy Violation

The privacy violation threat refers to the typical spamming scenario where user attention is diverted to answer an unsolicited call or to sift through large amounts of unsolicited unwanted communications. A related variant is where group communication mechanisms are leveraged by the attacker to increase impact.

### 5.2.3.1 Privacy Violation Scenarios

#### 5.2.3.1.1 Bulk UC (Advertising)

In this scenario an attacker sends bulk UC for advertisement (or other) purposes, for instance through pre-recorded voice messages (SPIT) or traditional telemarketing. This scenario corresponds closely to the general scenario, in Section 5.1.0, with the specific trait that many users are targeted. As in the general scenario, the UC may be originating either from inside the IMS system (as in case 1) or from the outside (as in case 2), through interworking with other systems

#### 5.2.3.1.2 Targeted UC (Stalker)

Targeted UC arises when the UC is focused to one user. Here we take an example of a user who does not want to receive calls from a given person, e.g. a stalker. Such cases apply to 3GPP IMS and otherwise. The general scenario, Section 5.1.0, describes the situation, with the specific trait that a single user is targeted. Again, the UC may be originating either from inside or outside the IMS network.

#### 5.2.3.2 Privacy Violation Risks

The Targeted UC scenario (Section 5.1.1.1.2) involving a stalker, or similar malicious caller, is a serious to the attacked user, but technical means already exist in IMS to address it (see Section 7.1.1.2). Nevertheless, targeted and bulk UC constitute a threat against the user's privacy, and the perceived severity of bulk UC will depend greatly on the frequency of it occurring.

Focusing on the Bulk UC scenario (Section 5.1.1.1.1), regardless of whether the UC was originated inside or outside the IMS network, we proceed with a more detailed analysis. The following calculation is based on a SPIT/UC source using an automated voice client on a PC to establish as fast as possible and as many as possible SIP connections to play a 10 seconds advertisement message. Typically the SPITter will use a low cost network with a high uplink bandwidth. The estimation is analogous to the example, used in RFC5039:

- assumed: call initiation with a single 1 Kbyte Invite message
- assumed: call success rate of 50% → 2 Kbyte or 16 Kbit per call setup
- assumed: SPIT message of 10s length with a 5.3 kbps G.723.1 codec (~ 16 kbps with overhead) → 160 Kbit per message
- assumed: DSL 16000 port with 800 kbps uplink speed
- ➢ ~ 45 parallel SPIT calls are possible
- ➢ ~ 4.5 SPIT calls per second are possible

- assumed: a SPIT activity of 24 hours a day and 30 days a month
- ➢ ~ 250 Gbyte per month and per SPITter for the IMS operator

Besides the huge traffic volume, generated by the SPITter and consuming network resources, the IMS operator is also affected

- by increased maintenance costs because SPIT victims complain to the operator about the nuisance
- by trouble with other operators complaining about
  - the nuisance on their customers
  - an increased traffic volume at the boundary between the SPIT/UC originating network and their own network
  - at worst a blocking of transit points to other networks affecting also legitimate users
- by possible trouble with the regulative authority
- in the long term by loss of customers that are dissatisfied with the service of the operator

Thus, to the operator, the main problem is likely to be the risk of complaints and secondary effects discussed separately as other types of threats below.

At a certain point, where the frequency of UC is sufficiently high, there is a risk that some users may start abandoning the service, perceiving it as unusable. In this case, a further consequence might be that the service receives negative publicity influencing the likelihood of adoption by other subscribers. In this discussion, this is highlighted as a separate secondary threat (Section 5.1.10), leading to loss of revenue and very significant consequences to the operators. The purpose of sending UC may also be for the attacker to achieve certain secondary goals, or may inadvertently lead to secondary effects, that are more severe for the user and/or operator. These are treated as separate threats in the following sections.

### 5.2.4 Contentious Incoming Call Service Charge

The contentious incoming call service charge threat refers to scenarios where a subscriber invokes a supplementary service that results in charges for incoming communications, e.g., call forwarding. This could result in additional charges induced by reception of SpIM/SpIT traffic, thus constituting a threat against the user's account credit. The subscriber is likely to raise objections in such cases, leading to a contentious charge.

#### 5.2.4.1 Contentious Incoming Call Service Charge Scenarios

##### 5.2.4.1.1 UC While Call Forwarding is Enabled

The only distinguishing feature of this scenario compared to Bulk (or Targeted) UC scenarios above, is that the recipient has enabled call forwarding, and thus may be charged for the UC being forwarded from one device to another. But often activation of Call Forwarding is paid by a monthly flat expense and then forwarding of UC does not lead to increased charges but only to a privacy violation of the affected user.

Be also aware that conditional Call Forwarding (Call Forwarding combined with black- or whitelist filtering) can be offered as a SPIT/UC prevention service to the user, e.g. by forwarding SPIT/UC suspicious communication to a SPIT/UC specific mailbox. This kind of service could as well be paid by a monthly flat expense.

#### 5.2.4.2 Contentious Incoming Call Service Charge Risks

Since the subscriber may be charged for the incoming UC, it constitutes a threat against the subscriber's account credit. Moreover, the subscriber may find being charged for a call he or she did not want to receive in the first place highly objectionable, and there is a risk of complaints to the operator regarding the billing, leading to customer care costs for the operator.

With charges resulting from the UC being a more serious consequence to the user than, for instance, merely receiving advertising UC, there is a higher risk for a negative perception of the service. Hence, there is a also greater risk to the adoption of the service than from the privacy violation threat alone.

### 5.2.5 Contentious Roaming Cost

Roaming subscribers are typically charged for incoming calls and messages, thus leading to a contentious roaming cost threat, similar to the previous case. SpIM/SpIT traffic targeting a user who happens to be roaming can induce an additional cost for the subscriber, constituting a threat against the user's account credit.

#### 5.2.5.1 Contentious Roaming Cost Scenarios

##### 5.2.5.1.1 UC While Roaming

In this case, the UC is received by a subscriber while roaming, leading to extra charges for receiving the call. Consequently, this case is essentially the same as the UC While Call Forwarding is Enabled scenarios.

#### 5.2.5.2 Contentious Roaming Cost Risks

The risks in this case are the same as for the Incoming Call Service Charge threat (Section 5.1.2).

### 5.2.6 Non-disclosure of Call Back Cost

The non-disclosure of callback cost threat refers to a scheme where a SpIM/SpIT is used to trick a subscriber into contacting back to a number or address that carries a surcharge, without disclosing the existence of the additional charge. Thus, the subscriber does not realize the additional cost until afterwards. This is a threat against the user's account credit.

#### 5.2.6.1 Non-disclosure of Call Back Cost Scenarios

##### 5.2.6.1.1 Baiting for Premium Number Call Back

In this case, the example is an attacker who calls numbers and disconnects after one-ring, or an attacker that sends or leaves a SPIT/UC message by faking that the user has won something, e.g. a journey, and leaving a premium number for callback. The attacker expects that the called party will be curious enough to call back. The number used by the attacker is a premium number. Thus the attacked user looses a lot of money if he/she calls back. This kind of attack is common in mobile communications systems and thus is valid for 3GPP IMS.

#### 5.2.6.2 Non-disclosure of Call Back Cost Risks

The economic aspect of this threat is similar to the Contentious Incoming Call Service Charge threat (and Contentious Roaming Cost threat), although dependent on user behaviour rather than a direct result of the UC. Thus, the risk can, potentially, also be reduced by changes to user behaviour, or warnings regarding the consequences of calling back, as well as preventing the UC directly.

### 5.2.7 Phishing

Phishing refers to forged communications that attempt to obtain sensitive information from users, such as login credentials or information to be used for identity theft. The attacker's objective is often monetary gain, so it often constitutes a threat against the user's finances.

#### 5.2.7.1 Phishing Scenarios

##### 5.2.7.1.1 Messaging/Voice Phishing for Bank Account Information

The Messaging Phishing for Bank Account Information scenario is, in all essentials, identical to email phishing scams that have been perpetrated against several banks. The only distinguishing feature being that a messaging service is being used instead of email to distribute the phishing message with a web link, or a telephone number simulating e.g. a pay or bank voice service (called Vishing for Voice Phishing). A successful attack in this case would hinge on the attacker being able to make it plausible that the bank would choose this medium to contact its customers. But it is not unreasonable to assume, that at some point messaging or telephone calls might come into use as yet another means for businesses to handle their customer contacts.

##### 5.2.7.1.2 Voice Phishing for Identity Theft

In the Voice Phishing for Identity Theft scenario, the attacker's objective is to convince the callee to divulge personal information that can be used to obtain credit in the name of the callee. This might be done, for instance, by claiming that the callee has won a prize and certain information is required for the person to be able to collect it.

#### 5.2.7.2 Phishing Risks

Phishing represents a serious threat against the user's finances, and a perception that the service is unsafe could strike a serious blow against attempts to use the devices for financial services.

### 5.2.8 Network Equipment Hijacking

The network equipment hijacking threat refers to an attacker compromising (an) IMS network element(s) to send unsolicited communications (presumably in bulk). This is a threat against the network resources and to any sensitive unprotected information stored on or going through the network.

#### 5.2.8.1 Network Equipment Hijacking Scenarios

##### 5.2.8.1.1 Compromised IMS Network Element

In this example scenario, an IMS network element, e.g. Application server, is compromised. An IMS network entity gets hijacked by an attacker who installs a malware/Trojan that is able to initiate bulk unsolicited communication. This hijacked entity now places random calls to users of the network to distribute, for example, a pre-recorded message. It should be noted that the probability of this threat is much lower than user originated SPIT/UC.

#### 5.2.8.2 Network Equipment Hijacking Risks

Clearly, unauthorized injection of traffic into the network is a serious threat to the operator's business. Unfortunately, compromised network equipment might render protection measures useless, because an attacker, able to compromise a network element, may also be able to compromise an element which hosts PUCI functions. On the other hand, PUCI protection measures that are not affected might provide an early warning of UC injection, and thereby potentially aid in detecting the intrusion. Moreover, effective protections against UC might reduce the incentive for certain attacks against the infrastructure by removing this possibility.

## 5.2.9 User Equipment Hijacking

The user equipment hijacking threat refers to the attacker distributing malware through unsolicited communications, e.g., in messages or as multimedia attachments to calls, and thus gaining control of the user equipment. This is a threat against the user's equipment resources and to any sensitive information stored on or going through the device. A related threat that is possibly less likely but even more serious, is the attacker being able to also distribute malware to some of the staff managing the network, and thus by extension potentially gaining (some form of) control of the network itself.

### 5.2.9.1 User Equipment Hijacking Scenarios

#### 5.2.9.1.1 Botnets Using User Equipment

Botnets are created by hijacked user equipment with valid identities. This equipment can participate in generating bulk UC by a hijacker. This can happen to any user equipment, whether it is part of 3GPP IMS or not.

#### 5.2.9.1.2 Malware DistributionThrough Bulk UC

In this scenario malware is distributed as an attachment or through a download link in bulk UC. The motivation could be, e.g., to build a botnet.

### 5.2.9.2 User Equipment Hijacking Risks

User equipment hijacking entails serious risks for the users, including using device resources, additional charges for the bulk UC (and complications with the operator concerning the charges), and possible exposure of any sensitive information stored on the device. For the operator, the origination of UC within its network can lead to several negative consequences captured in this list of threats, and also potential negative consequences if UC is passed to other operators.

## 5.2.10 Mobile Phone Virus

The Mobile Phone Virus threat refers to the attacker distributing virus through unsolicited communications, e.g., a download link in messages or as multimedia attachments to calls, and thus gaining destroy of user's mobile phone resource and unavailability of user's mobile phone service. Furthermore, the infected phones will distribute the virus to its contacts unconsciously.

### 5.2.10.1 Mobile Phone Virus Scenarios

#### 5.2.10.1.1 Exposure of User Privacy

A typical result when a user's phone is affected by virus is the exposure of user privacy information, e.g., contact numbers, personal arrangements, internet accounts, or even bank accounts.

#### 5.2.10.1.2 Destroying Mobile Phone Software and Hardware

Virus can be distributed to destroy mobile phone's software, operating system, or even hardware, e.g., unavailability of power-on or key-press operation, damage to mobile phone chips.

#### 5.2.10.1.3 Distributing Illegal Information and Virus

Some kinds of virus can automatically get user contact list and send them illegal information and virus through unsolicited communications. Furthermore, the illegal information and virus will spread abroad from the infected mobile phones in the same way.

#### 5.2.10.1.4 Junk Data Distribution through Bulk UC Resulting in User Additional Charges & Network Traffic Jam

The infected mobile phone will distribute large quantity of junk data through SPIM/SPIT continuously to telecommunication network, which will result in network traffic jam. At the same time, this will produce many additional charges to user account.

### 5.2.10.2 Mobile Phone Virus Risks

Mobile Phone Virus entails serious risks for the users. It can result in mobile phone's sensitive information lost, damages to software and hardware, unavailability of mobile phone services and additional charges. For the operator, large quantity of junk data distribution will result in network traffic jam and degraded service quality.

## 5.2.11 Sender Impersonation UC

In the process of sending, for instance, phishing messages, the sender will want to mask his/her true identity and assume the sender identity of some other entity. Thus, the sending unsolicited bulk communications in some forms are tightly linked with sender impersonation threats. The sender impersonation threat is a threat against accountability in the system.

### 5.2.11.1 Sender Impersonation UC Scenarios

#### 5.2.11.1.1 Forged Sender UC Received through Interworking with VoIP Operator

Given the used of network asserted identities, and the relatively controlled environment of IMS, forged sender information is less likely to be a problem than in general Internet services. However, there is a concern that interworking with services such as non-IMS VoIP with less stringent security could lead to injection of UC, possibly also with forged sender information into IMS through the interworking points.

### 5.2.11.2 Sender Impersonation UC Risks

Scenarios with forged sender information could undermine the trust in the relatively stronger identity information that does exist in IMS unless there is a distinction that is obvious to the user.

Forged sender information also has a significant influence on reputation systems. With forged or spoofed sender identities it is possible to distort the database of a UC reputation system which is usually based on the calling identity. Forged or spoofed sender identities can also be used for UC scoring attacks to the detriment of legitimate users, attempting to damage their reputation.

## 5.2.12 Unavailability of Service or Degraded Service Quality

Large volumes of bulk communications used in these scenarios may deviate significantly from normal use cases and thus might significantly exceed the assumptions made for capacity dimensioning. Consequently, there is a risk of degraded service quality or even denial-of-service conditions arising in the system.

### 5.2.12.1 Unavailability of Service or Degraded Service Quality Scenarios

#### 5.2.12.1.1 UC flood leads to Degraded Service Quality

This scenario involves a sudden and excessive load on the system from UC distribution, such as the Bulk UC scenario in Section 5.1.1.1 resulting in degraded service quality.

### 5.2.12.2 Unavailability of Service or Degraded Service Quality Risks

Besides loss of revenue to the operator, degraded quality or unavailability of service could also lead to damage to the brand, which could have much more serious financial consequences.

## 5.2.13 Negative Service Preconception Leading to Non-adoption

Negative publicity from some users' experiences of unsolicited communications could induce negative preconceptions about the offered service among large numbers of potential users, resulting in a failure in the market place. This threat is highlighted for completeness, as a potentially serious consequence of not addressing UC-related issues. However, it is a secondary result of the previously discussed threats and, as such, does not imply any further technical requirements on the system.

## 5.3 Specific UC threats in non-IMS inter-connections

### 5.3.1 Introduction

The inter-connection between IMS and non-IMS networks, telecommunication operators and independent VoIP service providers, will lead to higher risks for some specific threats. This section highlights the architecture and specific threats corresponding to this scenario. In the rest of the document we use the term "IMS interconnection" when the interconnection between two operators or domains follows the IMS/3GPP standards. On the other hand, we use the term "non-IMS interconnection" when the interconnection is between an IMS compliant network and a non-IMS compliant network.

The architecture and inter-connection scenario can be described as follows (see Figure 5.3-1) representing an IMS interconnection on the left side and a non-IMS interconnection on the right side:

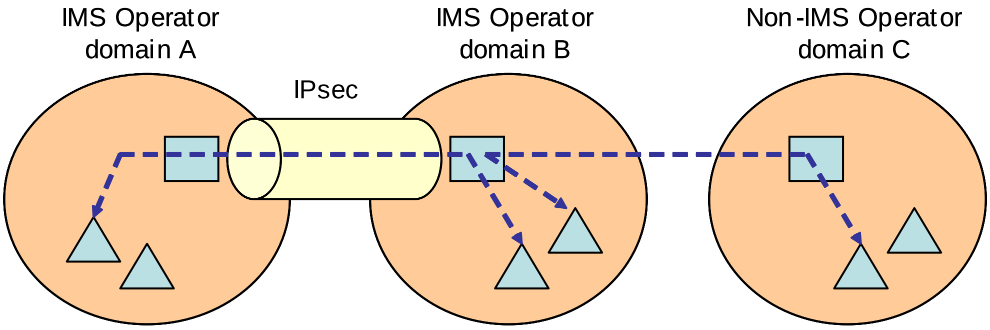


**Figure 5.3-1: IMS and non IMS Inter-connection**

The non-IMS interconnection scenario refers to the general case where an IMS network/domain is not only interconnected with other IMS network/domain but also with non-IMS network/domain also called "external VoIP operators" or "public Internet VoIP operators". It is supposed to appear because various operator may follow various commercial or technical strategy, resulting in not all the VoIP operators following the IMS standards, although each one seeking "universal reachability" with other operator/domain. This scenario may appear progressively along with the increase of the number of VoIP providers. In a long term period, it is expected that inter-IMS networks connections and IMS connections with non-IMS network will coexist.

To some extend, this scenario may be compared to e-mail interconnection where a huge number of e-mail domains/networks (several thousands) are interconnected in an "open way" meaning at any time each e-mail domain may receive an incoming e-mail from any other domain in the world without previous legal or contractual agreement.

The non-IMS interconnection presents specific characteristics which are listed in the sub-sections below. This is not meant to be exhaustive and it may change depending on operator strategy. Therefore it should be considered as a basis for discussions that may be adapted along time.

### 5.3.2 Legal assumptions

In non-IMS interconnection we assume there is no *a priori* legal or commercial agreement between operators. Similarly there may not exist any SLA or policy agreement before VoIP calls are being placed.

Although legal agreement may not exist between each possibly interconnected domain it is assumed that subscriber traffic goes through operator proxies before being sent to outside domain and consequently each provider takes the appropriate measures to authenticate its customers and filter UC from its domain. Customer authentication does not necessarily imply a legal contract but at least some kind of customer account which is required, for example, to access WebPhone services. Note: this assumption does naturally not apply to deliberate attacker domain.

Also, roaming or third-party services may be supported which means the sources of VoIP traffic within each domain are not necessarily known in advance.

### 5.3.3 Network assumptions

We assume domain A is one of the possible non-IMS sending domains and domain B is an IMS compliant receiving domain.

We consider the following network hypothesis for domain B:

- There is at least one inbound proxy in domain B to serve non-IMS interconnections. In the rest of the document, each inbound proxy in domain B is comparable to a modified I-CSCF function. This modified I-CSCF function is noted OI-CSCF to indicate it serves "open" interconnections as opposed to regular IMS interconnections.
- Each OI-CSCF function in domain B has a public network address meaning it can be reached from any network entity connected to Internet.
- At least one OI-CSCF function of domain B is announced in DNS or by an equivalent Internet service.
- IMS UE in domain B can not receive any incoming call originating from non-IMS domain without previous control of the call by the OI-CSCF function.

We consider the following network hypothesis for domain A:

- There is at least one outbound proxy in domain A that is responsible for call routing and control. In particular, this outbound proxy applies all the possible measures to avoid UC being generated by UE inside domain A (excepted of course if domain A is malicious).
- At least one outbound proxy in domain A is announced in DNS or by an equivalent Internet service.
- UE in domain A can not initiate calls to domain B without the call being allowed by one of the domain A outbound proxy.
- In roaming situations, or for particular services, the sending entity may not be in domain A. This means the sending entity has a network address in a network not belonging to domain A although this entity may be connected to domain A outbound proxy through Internet.

The above network assumptions are illustrated by the following figure; Figure 5.3-2. The UE identities are supposed to be SIP_URI. As a general network hypothesis, we assume the SIP transport is UDP.

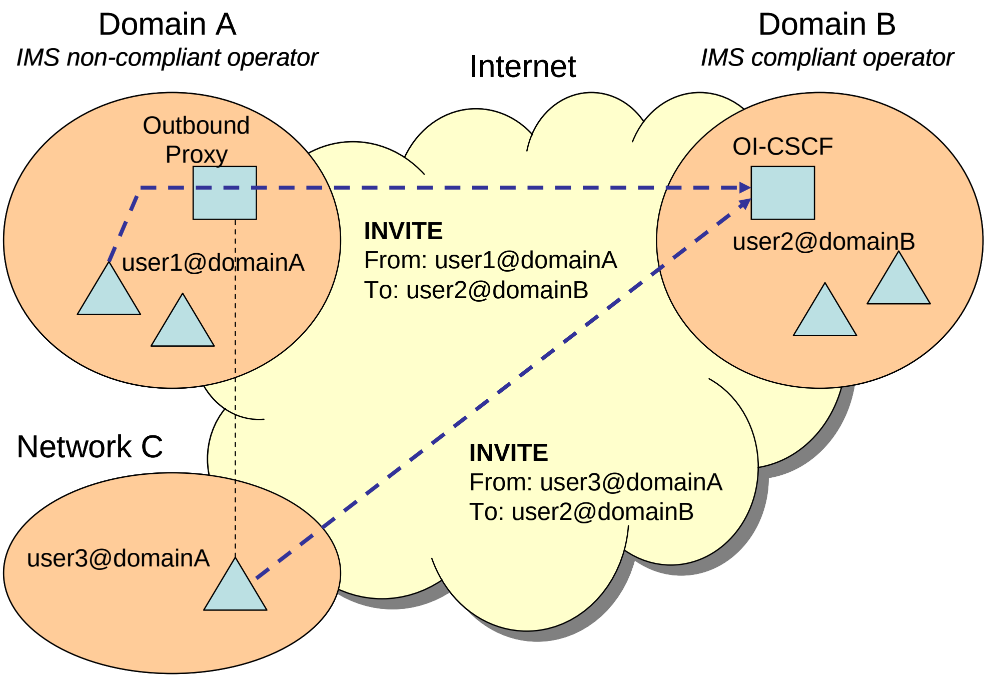


**Figure 5.3-2: Non-IMS interconnection network architecture**

## 5.3.4 Security assumptions

In non-IMS interconnection, we assume there is no *a priori* security association (for example a shared secret) between domain A and domain B. This assumption is the simplest one, but it does not guarantee integrity of messages exchanged between domain A and domain B. Therefore, we need to distinguish the two possible cases:

- Case 1: no security association between domain A and domain B. In this case, integrity and confidentiality of messages exchanged between A and B are not assured. Also, information asserted by outbound proxy in domain A (such as P-Asserted-Identity) is not relevant because it may have been modified by attacker.
- Case 2: a shared secret is exchanged along time between domain A and domain B; the way it is established is outside the scope of this document. In this case, secure interconnection may be set up on a technical basis, using standards such as IPsec to ensure integrity and confidentiality of messages exchanged between A and B. Such solution may be valuable between domains exchanging large amounts of traffic.

## 5.3.5 High risk specific threats

All the threats already identified in the document apply to this non-IMS interconnection scenario (see annex B). But the inter-connection with domains that are not under control of any telecommunication operator will have impact on the likelihood and volume of some specific threats of UC:

- DoS threat introduced by the network reachability, through Internet, of interconnection function (OI-CSCF).
- Forged sender identity.
- Forged network information, meaning spoofed IP source address. This threat is relevant only with connection-less transport protocol like UDP.
- Visible inter-working points from a network perspective and associated DoS threat.
- Forged domain identity, meaning attacker registers a domain with a name looking like a legitimate domain name.
- Attacker versatility: analysis of e-mail SPAM campaigns showed that spammers where able to change dynamically, at very fast period (around a couple of minutes), the spam sources, proxies or reflectors and also the domain names used for spamming (several hundreds of domain names used during a single SPAM

campaign of a couple of days). This versatility is based on very skilled obfuscating techniques rendering the trace-back of SPAM sources very difficult.

It is very important to mitigate the forged sender identity, network spoofing and also the attacker versatility threats which seem to be often under-estimated in the state of the art. Any complete solution for protection against unsolicited communication in IMS network should be able to protect IMS network operator and IMS users against these specific threats in an efficient manner.

# 6 Security Requirements

## 6.2 TISPAN Security Requirements

Editor's Note: To start the discussion we present the requirements from TISPAN below. These requirements are also presented as 3GPP requirements in following section. It is noted here, however, that TISPAN requirements should be considered as providing a 'basis' of requirements but not an already completed requirement set. Any new requirements are of course FFS for the TR.

TISPAN UC requirements [1] are:

R-UC-1: The NGN shall provide a means for NGN-users to report calls as UC

R-UC-2: Reports of UC made by NGN-users shall be auditable by the NGN.

R-UC-3: The NGN should provide the ability for an affected user to request the rating of an UC call

R-UC-4: The NGN should provide the ability for an affected user to challenge the ratings made by the UC detection system.

R-UC-5: The NGN should provide the ability to the affected CSP to extract from the call signalling sufficient information to provide a UC rating for the call

R-UC-6: The NGN should provide a mechanism to convey the UC rating in the call signalling

R-UC-7: The NGN should provide a mechanism to allow variation in the call handling for calls with particular UC ratings

## 6.2 3GPP Security Requirements

Following are security requirements on PUCI:

3GR-UC-1: The IMS should provide a means for IMS-users to report communication as a UC.

3GR-UC-2: Reports of UC relating to IMS-users should be auditable by the IMS.

3GR-UC-3: The IMS should provide the ability for a user who is party to a communication to request whether a communication was rated as UC

NOTE 1: Requirement 3GR-UC3 risks making PUCI mechanisms vulnerable to circumvention attacks through repeated probing of the identification outcome. Consequently, special care must be taken to include safe guards against circumvention attacks, for instance through rate limitations on responding to queries.

3GR-UC-4: The IMS should provide the ability for an affected user to challenge the justification why the communication was identified as UC.

3GR-UC-5: 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.

3GR-UC-6: The IMS should provide a mechanism to convey the UC indication in the signalling.

Editor's note: Intermediary network entities must be taken care of.

3GR-UC-7: The IMS should provide a mechanism to allow variation in communication handling based on UC likelihood indication.

3GR-UC-8: Requests for UC protection made by IMS users should be auditable by the IMS.

3GR-UC-9: 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.

NOTE 2: The IMS may provide a mechanism to enable the implementation of the Requirements 3GR-UC-5 (identification), 3GR-UC-1 (reporting) and 3GR-UC-7 (control) at the beginning, during or end of the communication.

# 7 Supporting Mechanisms and Solution Alternatives

## 7.1 Review of Measures and Potential Supporting Mechanisms

We commence by reviewing potential high-level measures to address the different scenarios given in Section 5, with the assumption that a PUCI solution would consist of a combination of such measures. The measures may be of a technical nature, i.e., a mechanism, or of a non-technical nature, e.g., legislation or contractual agreements. Similarly to Section 5, the scenarios are grouped according to identified threat.

### 7.1.1 Measure for Protection Against Privacy Violation

We consider each of the two scenarios (Section 5.1.1.1.1 and Section 5.1.1.1.2) separately.

#### 7.1.1.1 Measures Against Bulk UC

We first consider measures to protect against Bulk UC (Section 5.1.1.1.1). Available non-technical means include:

1 *Regulatory measures*, such as, "do not call" lists (possibly coupled with enforcement). This has worked quite well for PSTN telemarketing calls in some countries, but has the drawback that legal measures are limited to national jurisdictions. It is, thus, unclear what will happen if calls are originated across national borders.

Another typical example of Regulatory measures is Mobile Phone Real-identity Mechanism [17]. This mechanism securely establishes the real identity of a subscriber obtaining a subscription. Where Real-identity is a subscriber's identity recorded in his/her valid credentials according to a country's law, such as the ID card, passport, etc. By using this identity, a person can be addressed in the real society. With this mechanism, anyone who applies for mobile telecommunication services should provide Real Identities. The Real-identity Mechanism aims at protecting against unsolicited communication because if a UC is observed the person can be directly identified by the operators. This solution solves the problem for the case where the caller is also the subscriber whose Real-identity is registered.

Such regulatory measures are likely to be more effective than any technical means for scenarios such as advertising by reputable telemarketing companies, i.e., that have a reputation to protect. However, it is less likely to be successful to avoid marketing of illicit products, or scams, where the originator attempts to conceal his/her real identity, or marketing from players who attempt to circumvent the rules (possibly through international calls).

2 *Service Level Agreements (SLAs)* between operators that prohibit UC in traffic exchanged between operators.

Again, likely to be of greater importance than any specific technical means are agreements between operators not to propagate UC. Since traffic in an advertising scenario may mean revenues for one operator while causing problems for another, agreements will require careful considerations of definitions of UC. On the other hand, operators receiving UC are in a stronger position to enforce rules, and may have incentives for doing so if costs arise due to complaints.

These measures also have the advantage of being available regardless of whether the UC originator is inside (case 1) or outside (case 2) the IMS network.

In terms of technical means to protect against UC, IMS also provides advantages that can make UC prevention easier. Available technical means in IMS include:

1 *Strong sender identities* (in the sense that they cannot be manipulated by the sender) such as the Network Asserted Identity. Not a solution in itself, but a necessary building block to ensure accountability in the system, and to enable certain originator-based filtering functions.

For case 1 (UC originated inside the IMS network) the accountability aspect is important for the operator to be able to enforce contract conditions (cf. clause 4.2.x). That is, as IMS is an operator controlled network and the users' identities are authenticated, the operator can also limit the capabilities of SPiTters by contract conditions, by bandwidth reduction after a certain volume of traffic or by time limits.

For case 2 (UC originated outside the IMS network) this advantage is lost. As the SPIT/UC traffic is now part of the aggregated traffic entering the IMS via the I-BCF, it is much more difficult to identify and to prevent.

For UC traffic originating outside the IMS network, a trust infrastructure could be built that helps authenticating the identities of the sender and/or the source network, for details cf. clauses 7.5 and 7.6. The operator could charge a small fee for the use of such a service, to cover cost and, similar to the payment at risk approach, deter SPITters, for details cf. clause 7.3.3.5. UE owners could be notified of such payments immediately, to uncover cases of device hijacking, for details on device hijacking cf. clause 7.1.7.

2 *Supplementary services* can be used to implement some functionality for UC protection:

a Blacklists and whitelists could be implemented using Incoming Call Barring, Anonymous Call Rejection, and Closed User Groups.

b Automated handling of suspected UC could be implemented using Call Diversion on Originating Identity,

c Accountability for transgressions could be aided by use of Malicious Call Identification.

However, in cases where the UC originator is outside the IMS network (case 2), it may not be possible to reliably identify the originating user. In this case, protection based on blacklists may work insufficiently because of a spoofed originator identity. Nevertheless also in this case Supplementary Services, based on whitelists provide an efficient UC protection, if the introduction problem is solved. Generally, it should be remarked, however, that UC protection does not work very well in the absence of sender identity verification.

In case of UC originator outside IMS further UC protection may be achieved at the level of operators (for instance through SLAs).

3 *DoS protection mechanisms* - A network operator can also use SIP-related DoS protection mechanisms if provided by the IMS network. With a traffic volume of ~ 250 Gbyte (see Section 5.1.1.2) and the permanent maximum usage of a network port, SPIT/UC can in the widest sense also be regarded as a kind of DoS attack. By an intelligent configuration of SIP-related DoS protection thresholds the IMS operator is able to restrict the capabilities of a SPITter without bandwidth reduction and without affecting normal legitimate users, e.g. by limiting the call setup rate per second per user or the number of parallel calls per user to a reasonable value. With that SPIT/UC can not be prevented completely, but it gets less attractive, at least under commercial aspects. Additionally devices sending UC generated unintentionally by the user might be provided with latest security updates. This might be especially applicable for scenarios where a UC generating virus does not spread through the MNO network.

Technical means currently missing for dealing with this type of scenario include:

1 *Identification of UC*. Both enforcement of regulations/SLAs and technical protection mechanisms require some means for identification of UC. UC could be identified by subscriber or, potentially, a network-based mechanism to correlate user behaviour. Identification of UC through complaint calls to customer service centers are likely to be costly for the operator and cumbersome for the subscriber. Thus, if UC becomes a significant problem, a more user friendly and cheaper means for reporting UC is motivated. The identification of UC may provide means to cover scenarios, where a user device was accidentally infected by a virus (e.g. via Bluetooth or WLAN) and generates UC. It may include some labelling which allows marking a source of a potential UC message as a potential SPITter and marked for security update. After a successful security update the former SPITter might be marked as on probation (e.g. bandwidth restriction) for a time period. After the device further executes cleaning-up of the viruses and its clean state can be confirmed to the network, the device can further be removed from the blacklist. These actions might be performed in a transparent way to the user to avoid unnecessary calls to help-desks.

2 *Providing contextual information about incoming communications to the recipient*. For cases where the recipient does not know the originator, the user might benefit from additional contextual information regarding the incoming communication, such as an indication from the system that it may be UC, information regarding the trustworthiness of the originator identity, or possibly information about whether a call is charged for or free (flat rate). Regarding the charging information of the originating network the terminating network usually doesn’t have any information about it. The operators of the originating networks may not be allowed or not willing to supply this information to competitors. It must be taken into account here that both, the terminal’s user interface and the terminal-network interface, have to support such a provision of contextual information to the user. Furthermore, usability aspects are important, i.e. a general user, not having special knowledge about PUCI, must be able to process the received information in the very short time he has to decide whether to pick up the call or not. The

contextual information can be provided together with the actual message or in a separate message which is uniquely linked to the actual message for better compatibility.

3 *Leveraging of UC reports across users*. If many users have already complained about UC and the source can be identified, it could be justified to warn other subscribers as they receive incoming communications. This would require technical means to correlate UC identification information. Such correlated information could be used in a central PUCI server, or communicated parts of the system, or made available to user. This also means that a given network should be able to identify a UC and mark it based on some processing. However, leveraging user feedback reports amounts to constructing a negative reputation system regarding subscriber behaviour, which has known security vulnerabilities. These vulnerabilities also need to be carefully considered considered (e.g. innocent users could fall victims to a malicious attack on their reputation). The user could be provided with some additional incentive to report UC, except that he might not be bothered in the future. The operator should take care that too many reports cannot result in an DoS attack against the IMS network. The user may have a default protection profile, but could additionally register to obtain server provided information to enhance the protection profile (this might be part of the registration to a service, but that depends on the service type), The service provided information might be based on user provided information i.e. other users complaining about UC. There is risk, however, on such reputation based system, since soiling others' reputation can be a certain way to abuse PUCI.: Additionally also legal aspects like protection of privacy and operator liability in case of false UC reports have to be taken into account.

Consequently, in addition to the stated available means to deal with UC, the following could be done to provide further protection functionality:

1 The operator should be in a position to be able to monitor and log such behaviour. For IMS, this could be expressed as the requirement: The IMS should provide the ability to the operator to extract information from the signalling or other means to provide an indication whether the communication is unsolicited. This also means that a given network should be able to identify a UC and mark it based on some processing.

2 The user should be able to report about UC to the operator so as to avoid further occurrences. Expressed as an IMS requirement it could be stated as: The IMS should provide a means for IMS-users to report communication as a UC.

3 The operator should be in position to capture auditable logs of the reports from the user so as to avoid any future legal issues. This requirement can be expressed as: If an IMS-user makes reports of UC they should be auditable by the IMS.

4 The operator should be in position to capture auditable logs of the request for UC protection from the user, so as to avoid any future legal issues. In terms of a requirement this can be expressed as: If an IMS-user requests UC protection this should be auditable by the IMS.

5 Means should be there for the operator to notify the receiver of a UC if the operator is not allowed to block the call.

### 7.1.1.2 Measures Against Targeted UC

Technical means to deal with targeted UC already exist in IMS in the form of Malicious Call Identification (MCID) and Call Barring (CB) supplementary services. Hence, it is not clear that further technical means are required to handle this type of scenario. The possible exception to this is the case where the UC originator is outside the IMS network (case 2), as a potential lack of a trustworthy sender identity would negatively impact the usefulness of these protection mechanisms. However, in the absence of trustworthy sender identities, it is not clear that other protection mechanisms could be devised that would be more effective for this scenario.

For UC originating outside the IMS network sender spoofing is an effective means to circumvent most UC prevention methods based on supplementary services. While blacklists, MCID and CB are prone to spoofing SPITters, even whitelists can easily be circumvented, once the identities on the whitelist are exposed. Such information could easily be obtained through corporate webpages (as used by SPAMbots scanning for internal company mail addresses which are then used to spoof source addresses), or even more prevalent social-network sites provide attackers with names and contact information of whole relationship webs which are likely to be on the whitelists of all the members (social SPAMming). Sophisticated attacks of this kind may subvert individual users' webs of trust and thus pose a significant threat to IMS service usability.

### 7.1.2 Measures for Protection Against Contentious Incoming Call Service Charge

In order to avoid customer care costs arising from a scenario such that described in Section 5.1.2.1.1, or to expedite the handling of such calls to the customer service center, the following solutions are possible:

The Call Forwarding service may be additionally protected by black- or white lists (conditional Call Forwarding) to restrict this service to trustworthy callers.

It could be useful to provide a UC feedback mechanism such that the system can collect information regarding such incidents. Hence,

NOTE: The user should be able to report UC to the operator so as to simplify handling of charging disputes or even automatically avoid certain cases of contentious charges. However, an automatic avoidance of contentious charging in case of SPIT/UC reporting also offers misuse of UC reporting by malicious users, e,g, by reporting every forwarded call as UC, shortly before or after finishing the call. Whether connections to charging should part of the requirements is, therefore, FFS.

### 7.1.3 Measures for Protection Against Contentious Roaming Cost

Since this case is essentially the same as the UC While Call Forwarding is Enabled scenario (Section 5.1.2.1.1), the implications for protection are the same as described above in Section 7.1.2.

### 7.1.4 Measures for Protection Against Non-disclosure of Call Back Cost

Referring back to the scenario in Section 5.1.4.1.1, this leads to:

1 Users affected by such attack and who want to avoid further occurrences need a way to indicate to the service provider that the unsolicited communication gets blocked in future. This can be accomplished through the existing Call Barring (CB) supplementary service. However, mechanisms, as indicated in Section 7.1.1.1, for leveraging input from some subscribers to protect others, by a UC score, could also be very useful in this type of scenario.

2 Operators should have means to capture auditable logs of requests for protection to avoid legal implications .This was also mentioned earlier in Section 7.1.1.1.

It should be possible for the operator to indicate that a given call is a UC, as mentioned earlier in Section 7.1.1.1.

### 7.1.5 Measures for Protection Against Phishing

One thing to note is that in the messaging/telephone call scenario (Section 5.1.5.1.1), the UC distribution is only one step in a phishing attack, which might also be countered by blocking other steps; for instance, through URL filtering against known phishing sites. Also heuristic and fingerprinting schemes could be utilized. Heuristic approaches look for specific techniques used by phishers, e.g. encoding the name of a trustworthy institution into the local directory segment of a URL. Solutions using fingerprinting compare existing samples of phishing messages against incoming messages, but those are sometimes circumvented inserting random text.

If the phishing attack is highly targeted, there is probably very little that can be done to block the UC step, as there is little previous information to take advantage of for protection. However, for bulk attacks, which is frequently the case, being able to correlate UC information (user feedback or based on traffic) to warn users would be useful, and leads to similar technical considerations as discussed in Section 7.1.1.1.

### 7.1.6 Measures for Protection Against Network Equipment Hijacking

Although the network should have means to identify such a hijack there could also be means to monitor the behaviour in the network and for users to report such activities.

It should be noted that network equipment hijacking is a general threat, and refers not only to SPIT/UC related aspects. Therefore, countermeasures against this serious threat will presumably not be determined by PUCI.

Looking at such an attack, from a SPIT/UC point of view, the following could be done:

1 The operator should be in a position to monitor and logg such behaviour. Thus, the IMS should provide the ability to the operator to extract information from the signalling or other user behavior to provide an indication whether the communication is unsolicited. This also means that a given network should be able to identify a UC and mark it based on some processing.

2 The user should be able to report UC to the operator so as to avoid further occurrences. Hence, the IMS should provide a means for IMS-users to report communications as UC.

3 The operator should be in position to capture auditable logs of the reports from the user so as to avoid any future legal issues. This requirement can be expressed as: Reports of UC made by IMS-users should be auditable by the IMS.

4 The operator should be in position to capture auditable logs of the request for UC protection from the user, so as to avoid any future legal issues. In terms of a requirement this can be expressed as: Requests for UC protection made by IMS-users should be auditable by the IMS.

### 7.1.7 Measures for Protection Against User Equipment Hijacking

The solution for this issue is similar to that discussed in Section 7.1.1.1 and thus the same requirements apply here. The botnet scenario also implies that the operator should be able to associate UC originating within the network with specific user equipment.

The botnet scenario can be further extended. Now that the infected user equipment is labeled as someone causing UC there should exist means for the user to get out of the list of UC attacker be it an individual (user) list or a global list. This brings us to the following:

1 A given user should have possibility to request the operator for the reason why he/she is considered as a UC attacker

2 The user should also have the possibility to challenge the decision of being listed as a UC attacker and so should the operator have means to defend him/herself.

Further it is possible that the operator is able to identify that the communication is UC, in such case the operator should be able to signal UC information to the receiving user. Such information might also flow through intermediary networks. The intermediary network should pass the PUCI information and not strip it off the packet. This requirement is also valid for the case where the regulatory body requires.

Further, if the reality from the PC world where a large percentage of all PCs are suspected of having been infected and are operating as botnet nodes is any indication, it may be unwise to block UC just based on identity of the sender, since a sender node may send both perfectly legitimate packets most of the times but also act as a botnet node that send out SPAM. Thus, in-session detection, rating, and response methods may be useful to deal with botnet nodes. A suite of new requirements that had not been anticipated in the TISPAN TR may need to be considered to deal with botnet scenarios. To differentiate between legitimate and botnet-related SPIT/UC traffic of the same UE, in-session SPIT/UC detection requires content analysis. Besides the concerns relating to the feasibility of such techniques, these prevention measures have the disadvantage that the legitimate call or the SPIT/UC-related nuisance has already started until in-session control can start to evaluate the character of the call. This is also in contrast to most of the measures discussed in this TR trying to determine SPIT/UC before the user is affected. As the complexity, effectiveness, and presumably the cost of in-session UC detection, goes beyond that based on sender identity, there must be a careful trade-off between the complexity imposed to IMS and the expected threat. In particular, the number of different variants of basically the same UC attack code is all the time growing. Some sophisticated UC attack code change all the time during the attacks (e.g. small changes in formatting). The detection and countering of all those variants are quite resource consuming. Methods exist for optimization, like analysing and grouping code by identifying frequently occurring command patterns from known attack code, and clustering them into UC attack families. Another possibility to protect the IMS network against botnet-infected UEs is to inform the user of such infected UE about the SPIT/UC suspicion, giving him the chance to remove the malware from his UE. Alternatively the operator could as well offer removing of the malware as a service to the customer. In case of no reaction the malicious UE will be disabled, using e.g. the feature "Selective disabling of UE capabilities".

### 7.1.8 Measures for Protection Against Mobile Phone Virus

Editor's note: References to the GSMA Mobile Malware should be added

1 User perspective

It would be helpful if users took measures such as those given below:

a. Do not expose personal phone numbers or messaging accounts arbitrarily on Websites;
b. Reject abnormal incoming calls and messages;
c. Hide or close Bluetooth application to protect against virus's auto-receiving;
d. Do not install any unauthentic executable file, e.g., EXE/SIS file, received by MMS or Bluetooth; received executable files, like security patches, could be checked for authenticity and correct source by checking it for a valid trustworthy signature and validation of fingerprints to detect malicious modifications
e. Install credible Anti-virus software and scan for virus regularly. The credibility could be validated by means of digital signatures.
f. If security features are available, they should be activated e.g. restrictive browser settings, secure hardware for trust root storage etc.

2 Operator perspective

The Operator Provider and ICP (Internet Content Provider) can take measures (e.g., Firewalls deployment, Intrusion-detection and Abnormal traffic detection.) to inspect and control messages passing by the network server or network gateway, in order to protect against virus. Additionally, the operator may support secure software distribution by providing authenticity to security messages (e.g. via digital signatures).

### 7.1.9 Measures for Protection Against Sender Impersonation UC

The possibility of UC with forged sender identity being received over interworking points (scenario in subclause 5.2.11.1.1) suggests that:

1 The system should be able to inform the callee of contextual information regarding the call, specifically such as the fact that the sender identity may be less trustworthy than if the call had been initiated within IMS.

2 Besides the callee, also SPIT/UC-related reputation systems should take the trustworthiness of the sender information into account. It is likely that the SPIT/UC threat is lower in trustworthy networks like IMS. Hence, the majority of SPIT/UC sources is presumed to be in non-trustworthy networks like non-IMS SIP domains, This raises a big challenge for statistical evaluation of reputation systems, if the majority of inputs may be forged.

3 Identity management techniques, providing authentication methods for claimed sender identities, may be used with respect to the applicability across IMS and non-IMS networks for UC protection. No details on identity management techniques for the purpose of PUCI is provided in this version of the report.

### 7.1.10 Measures for Protection Against Unavailability of Service or Degraded Service Quality

Technical considerations for unavailability of service or degraded service quality (scenario in Section 5.1.9.1.1):

1 Issues of degraded service quality would, in general, need to be dealt with through QoS mechanisms or DoS protection to limit traffic. However, since DoS traffic can be virtually indistinguishable from normal traffic there can be a significant problem to determine what traffic to limit. On the other hand, apart from pure traffic limiting it may also be possible to limit other resources like e.g. the number of parallel calls or the number of call attempts per second per user by DOS mechanisms. With that SPIT/UC is not stopped but the network is less attractive, at least under commercial aspects. The advantage of such resource limiting is that the traffic and the bandwidth of normal legitimate users is not affected. Additionally, mechanisms for identification of UC could be very useful for identifying the appropriate traffic to limit.

## 7.2 IMR-Based Solution Approach

### 7.2.1 General

The initial step in IMR-based unsolicited communication prevention is to identify that the given communication is unsolicited. Without identification no further action can be taken. Once a given communication is identified as unsolicited it should be marked appropriately.

Marking could be as simple as a means to notify that a given communication is unsolicited. Having identified and marked a communication as unsolicited the next step is to react on it. Depending on condition one could skip the marking step and directly go to react after identifying that a given message is unsolicited.

These three steps, identification, marking and reacting can be done:

- automatically in the network or UE or distributed in the network and UE
- with or without intervention from the user at each or certain steps
- manual setting in the network and/or UE by the operator and/or user
- at the beginning, during, or end of the communication

NOTE: Contentious charging in case of SPIT/UC reporting during or at the end of the call also offers misuse by malicious users, e.g. by reporting every forwarded call as UC, shortly before or after finishing the call.

Editor’s Note: Whether connections to charging should be part of the requirements is FFS

The details of how these functions will be realised will be dependent on the eventual selection of supporting methods.

## 7.2.2 IMR Approach

Identification, marking and reaction of UC can be handled in many places, in the network or UE. Moreover, different steps can be centralized or distributed. Identification, marking and reacting are explained below.

### Identification

In 3GPP MCID service enables an incoming communication to be identified and registered. This solution still misses the functionality of automatic UC identification with user involvement and future prevention of calls from the same originator.

UC identification in IMS can be categorized as:

- non intrusive tests: call-signaling gets analyzed by an automatic mechanism to derive a marking;
- intrusive tests: a caller gets tested in an intrusive way with the objective to clearly identify a unsolicited communication attempt before the transaction reached the destination;
- feedback by user of a UC: this is an extension of the MCID where a user can, for example, define in advance a personal black-list, react during a call or give feedback an occurrence of UC to provide his/her personal preferences to prevent the future UC attempts.

### Marking

Marking a communication attempt as UC is required to react appropriately. This can be at different granularity level as discussed in previous section.

### Reacting

Reacting can be done by blocking the communication or re-routing to, for example, a mailbox or automatic answering service. In order to do this, specific filter rules and personal considerations have to be taken into account. Taking personal routing decisions for handling UC into account involves the previous marking as an indication for handling this specific UC attempt.

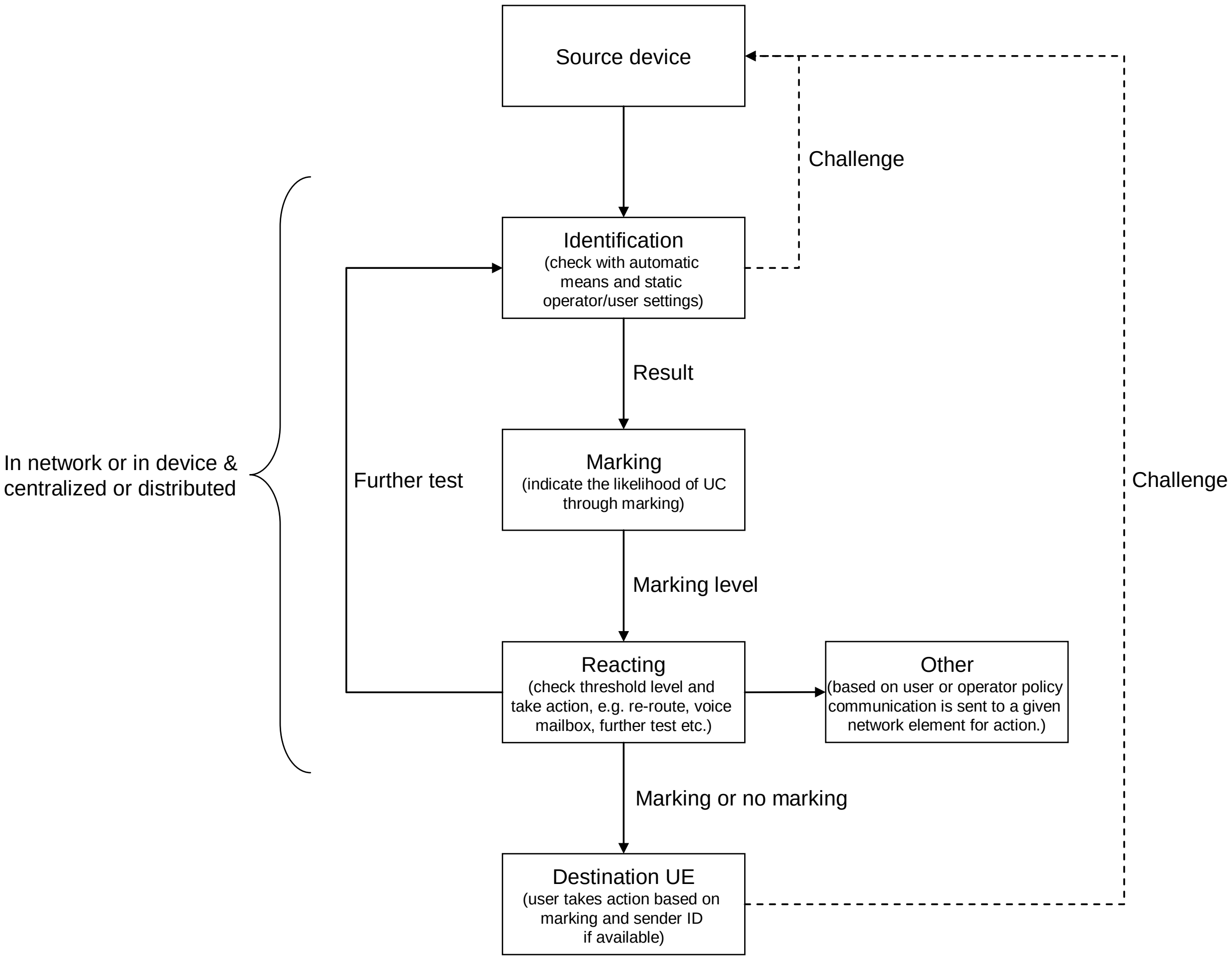

Source device
Challenge
Identification
(check with automatic means and static operator/user settings)
Result
Marking
(indicate the likelihood of UC through marking)
Marking level
Reacting
(check threshold level and take action, e.g. re-route, voice mailbox, further test etc.)
Other
(based on user or operator policy communication is sent to a given network element for action.)
Marking or no marking
Destination UE
(user takes action based on marking and sender ID if available)
Further test
In network or in device & centralized or distributed
Challenge

**Figure 7.2-2: Relation between different steps in a solution against UCI.**

## 7.2.3 From Requirements to Solution

As usual, problem and requirements give way to solution. Thus we start with PUCI requirements and what it means for IMR based solution as given in Table 7.2-1for there on we develop potential IMR solutions. In the table below 7.2-1 the term user reacts or R by user is utilized, those terms mean that a report on UC may be sent to the network. This reaction may also be preconfigured in the terminal (e.g. by the user). The reaction may take place, but the user should not be forced to react to an incoming UC. Usability considerations and avoiding of click-through behaviour suggest minimizing pop-ups.

Editor's Note: Contents of the column "details of possible solutions" in Table 7.2-1 is not thoroughly discussed thus it is for further study whether it will be modified or replaced by other text.

**Table 7.2-1: Requirements and solution.**

| | Requirements | Location of Identification (I), Marking (M) and Reacting (R) | Details of Possible Solutions |
|---|---|---|---|
| | **SA3 requirements** | | |
| **1** | The IMS should provide a means for IMS-users to report communication as a UC. | I, M and R by the user | Message needed from UE to user PUCI settings in the network |
| **2** | Reports of UC made by IMS-users should be auditable by the IMS. | Not dependent on IMR | Accounting and auditing solution of the network should take care of this |
| **3** | The IMS should provide the ability for an affected user to request the rating of an UC call | M should be provided to the user | Message from UE to user database needed. Based on operator policy and regulatory requirements to provide info. |
| **4** | The IMS should provide the ability for an affected user to challenge the justification why the communication was identified as UC by the UC detection system. | Not dependent on IMR | This is related to 2nd requirement. Proper auditable information collection in the network will take care of this issue. |
| **5** | The IMS should provide the ability to the operator to extract information from the signaling and other means to provide an indication of the likelihood whether the communication is unsolicited. | I and M in network | Either a centralized identification solution or distributed identification solution is needed. In case of distributed, marking value should be conveyed between the different identification functions. Messages need to be defined to carry M |
| **6** | The IMS should provide a mechanism to convey the UC indication in the signaling. | M conveyed between different entities. | Messages need to be defined to carry M |
| **7** | The IMS should provide a mechanism to allow variation in communication handling based on UC likelihood indication. | Variation in handling can, for example, mean moving the call to voice mailbox, terminating a connection, indicating likelihood that a call is UC to the UE etc. R in network. M sent between elements | This should be operator policy dependent or user dependent. Messages should provide transfer of M. |
| | **SA1 requirements** | | |
| **8** | **High level requirements** | | |
| **a** | IMS should provide means to identify and act on unsolicited communication. | R is required | User decides whether a communication is UC and Reacts<br>Network should identify, check user and operator policy, and Reacts |
| **b** | Solutions for prevention against unsolicited communication shall not have negative impact on the services provided by IMS. | IMR should take care of this requirement | Solution should take care of this point from architecture onwards |
| **c** | PUCI should provide means for cooperation between operator's networks. | M should be conveyed between operator networks | Message carrying M between operators |
| **d** | IMS should provide means for a user to inform the network of an unsolicited communication. | R by user | Message from UE to user PUCI setting |
| **9** | **Detection of Unsolicited Communication** | | |
| **a** | Depending on Operator policies IMS should support capabilities that enable IMS to detect that an IMS session is unsolicited and classify as UC. These capabilities should apply to all IMS based services and apply to real-time (e.g. voice, video …) and to non-real-time (e.g. messaging …) IMS traffic. | I and M in network | I could use supplementary services or other services. There is no impact on SIP messages. |
| **b** | IMS should support capabilities that enable a terminating party to report IMS sessions as UC. | M and R by user | Message from UE to user PUCI setting |
| **c** | The method of reporting UC may be dependent on the IMS service. | I and M could be service dependent | M in message could be service dependent |

| | Requirements | Location of Identification (I), Marking (M) and Reacting (R) | Details of Possible Solutions |
|---|---|---|---|
| **d** | Reporting should be possible irrespective of whether an originating party has withheld its identity (e.g. by referring to the last call). | R by user for a communication of which identity was not available or the network provides the sufficient information. | Network should keep identity of last call if no user id was available. Message from UE to user PUCI setting |
| **10** | **Prevention of Unsolicited Communication to the terminating party** | | |
| **a** | Depending on Operator policies IMS should support capabilities to indicate to a terminating party that an IMS session has been classified UC. | I and M in the network.<br>M sent to the UE. | M and communication identitiy to be sent to UE in a message saying that communication was terminated by the network |
| **b** | Depending on Operator policies IMS should support capabilities to protect a terminating party from IMS sessions that have been classified UC. | R in the network | Supplementary services and other services should check likelihood of a communication being UC and react based on on user or network settings |
| **11** | **Notification of UC to the originating party** | | |
| **a** | 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. | M to originating party | Message with M to originating party |
| **12** | **Conveying information on UC to other networks** | | |
| **a** | Depending on Operator policies IMS should support capabilities that enable the IMS of a network to convey information on detected UC in an IMS session to an other IMS on the path of that IMS session | M conveyed between networks | Message with M communicated between networks |

## 7.2.4 IMR Solution Variations

### 7.2.4.1 General

The requirements and discussion in Table 7.2-2 lead to location of I, M and R as given in Figure 7.2-3. In Figure 7.2-3 I, M and R in the network is located at the PUCI AS and CSCF, this is to signify that the requirements do not lead to a decision whether I, M and R in the network should be distributed or centralized. What is certainly obvious is that the R, i.e., the react part or the part that makes decision about taking action, should be centralized in the network. This leads to four variations on the location on I and M:

1. Centralized
   (a) In AS
   (b) In CSCF (specifically S-CSCF)
2. Distributed
   (a) Among ASs
   (b) Between CSCF (specifically S-CSCF) and ASs

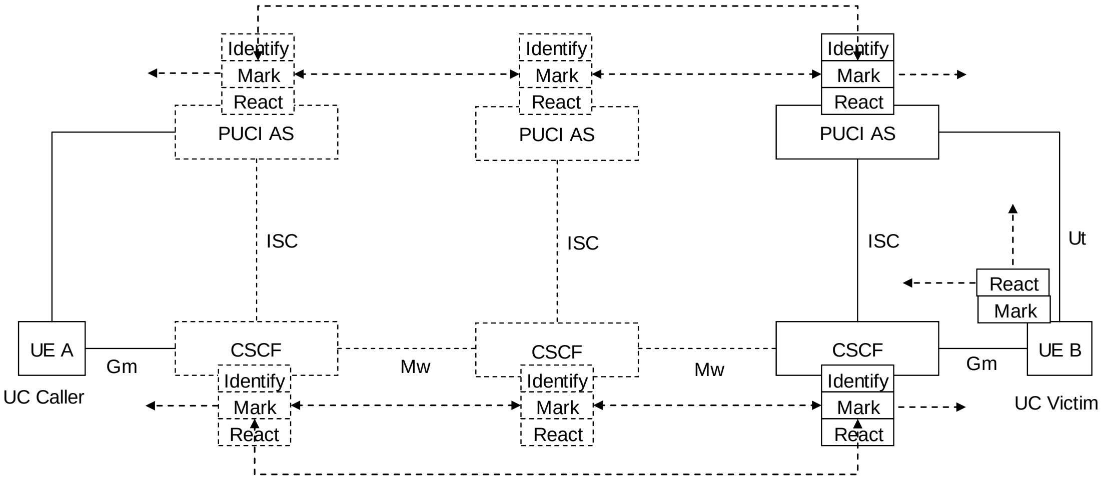


**Figure 7.2-3: Requirements represented in figure.**

I and M should also be done at the border of the network thus distributed solution is the obvious choice. Further having a distributed solution allows usage of already deployed supplementary services. Then the only discussion left is regarding R – whether R should be in the AS or CSCF –. As the R leads to routing decisions this should be done in the S-CSCF and not in the PUCI-AS.

### 7.2.4.2 IMR Solution Based on Supplementary Services

In this section we outline an IMR-based solution architecture that includes leveraging functionality of existing supplementary services. A high-level illustration of suggested placement of identification, marking, and reaction functions is shown in Figure 7.2-4.

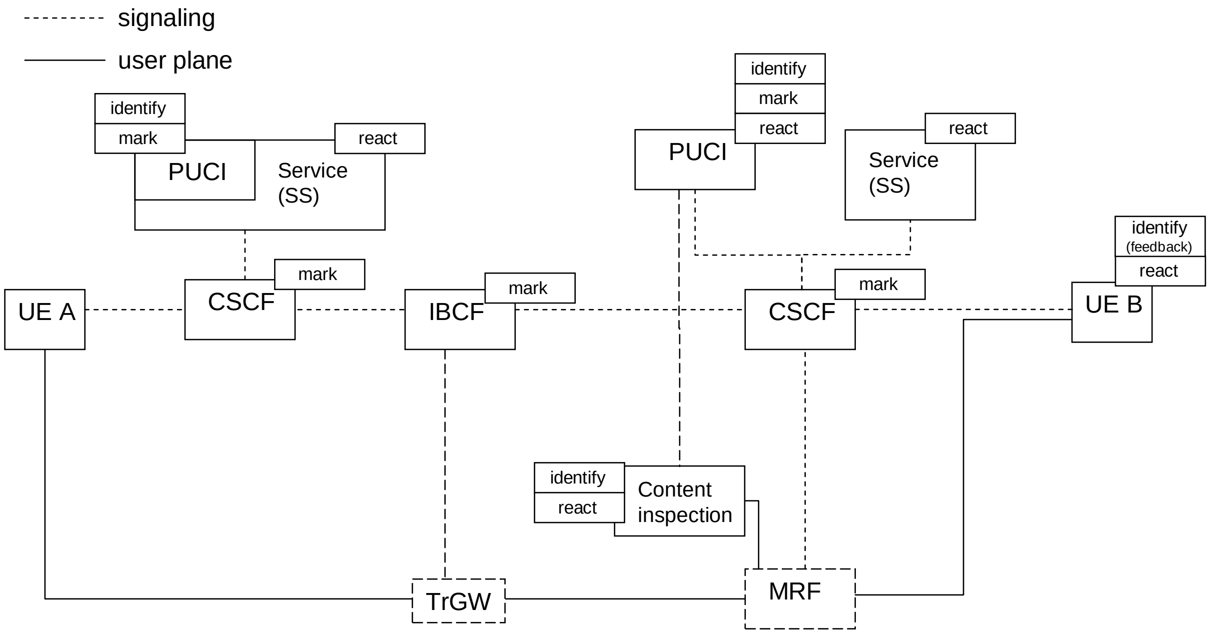


**Figure 7.2-4: Architecture for PUCI solution variant utilizing supplementary services.**

As shown in Figure 7.2-4, identification, marking and reaction of a UC could take place in many places, including CSCF, IBCF, PUCI functionality or UE. Individual steps may be centralized or distributed. However, options such as adding many or most functions to S-CSCF have been excluded to avoid impacting existing functions with already high complexity. Instead a new PUCI-functionality appears preferable that would be able to handle specific marking and identification procedures. Such functionality could then be hosted either together with the Service as such (e.g., TAS in case of MMTEL) or as standalone function. It is however, proposed to leave this outside the scope.

Communications from UE A may be marked with contextual information about the communication by the network before being routed to PUCI functionality and specific service. The PUCI functionality may use such contextual marking, user feedback, or behavioural information collected to identify UC and either provide a new marking or implement some direct reaction.

In a solution alternative based on leveraging existing service behaviour, such as MMTEL supplementary services, an existing AS implementing supplementary services may use PUCI specific markings, provided by the PUCI functionality, to react by blocking or diverting the communication. Depending on policy or request by UE B a communication request can, thus, be blocked in the network (by an AS) or at the UE. The feasibility of UC handling at the UE is ffs. UE B can also provide feedback about UC via the Ut interface.

## 7.2.5 Detailed Solution

### 7.2.5.1 Overview

In sections 7.2.5.2 and 7.2.5.3 we present the detailed IMR solution and identify what needs to be standardized. Figure 7.2-5 and Figure 7.2-6 show message sequence for PUCI service invocation when UE A makes a call to UE B. Message sequence in red requires standardization. In both figures UE A is the Caller and UE B is the Callee.

In the message sequence of Figure 7.2-5 and Figure 7.2-6 we assume that the (1) HSS stores all PUCI related subscriber profile including routing information and (2) the S-CSCF provides the routing. In practice the PUCI AS could store the subscriber profile and also provide the routing.

### 7.2.5.2 Simple PUCI Invocation

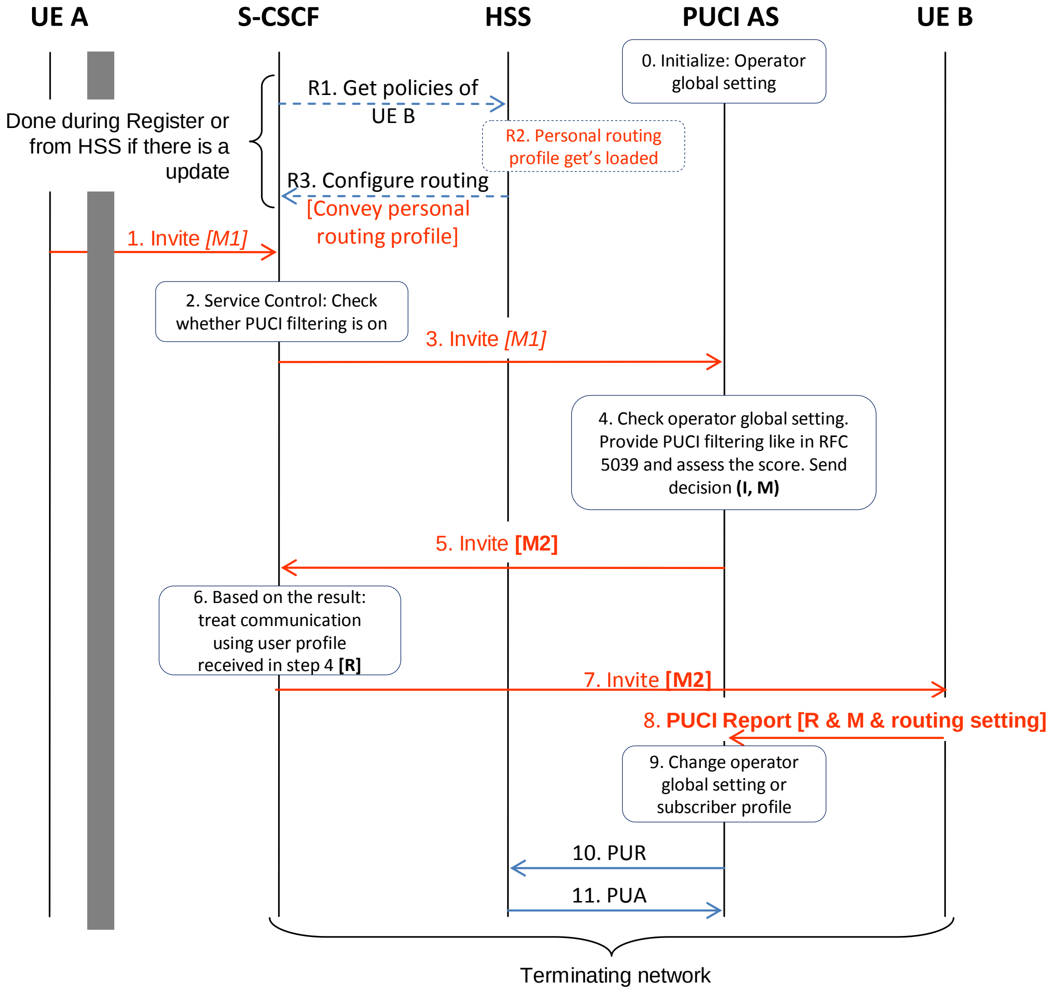

UE A
S-CSCF
HSS
PUCI AS
UE B
0. Initialize: Operator global setting
R1. Get policies of UE B
Done during Register or from HSS if there is a update
R2. Personal routing profile get's loaded
R3. Configure routing [Convey personal routing profile]
1. Invite [M1]
2. Service Control: Check whether PUCI filtering is on
3. Invite [M1]
4. Check operator global setting. Provide PUCI filtering like in RFC 5039 and assess the score. Send decision (I, M)
5. Invite [M2]
6. Based on the result: treat communication using user profile received in step 4 [R]
7. Invite [M2]
8. PUCI Report [R & M & routing setting]
9. Change operator global setting or subscriber profile
10. PUR
11. PUA
Terminating network

**Figure 7.2-5: Simple PUCI service invocation.**

R1. The Callee (UE B) side S-CSCF then checks what policies are there for the given Callee (UE B). This part should be standard Diameter message and is already standardized.

R2. The HSS then checks the policies of the Callee (UE B) which is given in the form of personal routing profile. This personal routing profile consists of the following:

i. A flag saying whether the Callee (UE B) wants PUCI service or not;

ii. Settings which tell the S-CSCF what to do when a certain marking (M) is received. Here it is assumed that the marking is in form of a score value, e.g. a user 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.

The HSS then sends the routing information to the S-CSCF. The message is again a Diameter message so it does not require standardization. Only the data sent in this message is new.

NOTE: R1 – R3 happen only during IMS registration. HSS can also send such information to S-CSCF if there is an update.

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. For this purpose a evolved EIR (eEIR) could be used.

1. The S-CSCF receives a SIP INVITE message from the Caller (UE A). This message may include PUCI related marking (M1) information if other PUCI tests were already performed in any of the networks through which the message traversed.

2. Then the S-CSCF checks whether the PUCI filtering applies for the given Callee (UE B).

3. If the PUCI service applies for the Callee (UE B) then the PUCI AS is invoked by the S-CSCF. For this, the S-CSCF sends a SIP INVITE message to the PUCI AS. This message may include PUCI related marking (M) information if marking (M1) 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 [11]. Other techniques could also be possible, e.g. CAPTCHA. These checks (Identification or I) result in an updated marking (M2) which takes in account the marking (M1) received in step3. This, updated marking M2, replaces M1.

5. M2 is then sent to the S-CSCF as part of the SIP INVITE message.

6. The S-CSCF then checks user settings received in Step 4 and makes routing decision accordingly. It could be that the call is sent to an answering machine or forwarded elsewhere. In this example the communication is sent to the Callee (UE B).

7. The S-CSCF then forwards the SIP INVITE to the Callee (UE B) with the marking (M).

8. It is possible for the Callee (UE B) to report a communication as a UC or to change its profile in the HSS. Such information can be sent from the Callee UE (UE B) to the PUCI AS. Reporting from the Callee (UE B) can be done in different ways, e.g. via a Web interface, keypad entries; Ut interface or by piggybacking to a existing message.

9. Based on the message from the Callee (UE B) the PUCI AS can optionally modify the operator global setting and/or subscriber profile. These optional modification are dependent on local legislations and prior consent from the user.

10. To change the subscriber profile the PUCI AS sends the Diameter message profile update request (PUR) [12 – 13].

    NEC: See text above the heading of this section.

    The HSS responds with a Diameter message profile update answer (PUA) [12 – 13].

### 7.2.5.3 PUCI with Supplementary Services and 3rd Party PUCI AS

This section illustrates the case where either supplementary services (SSs) or a 3rd party PUCI AS is involved. It is also possible that both SSs and a 3rd party PUCI AS are used. In this case the steps 1-4 are the same as for the case of simple PUCI invocation given above.

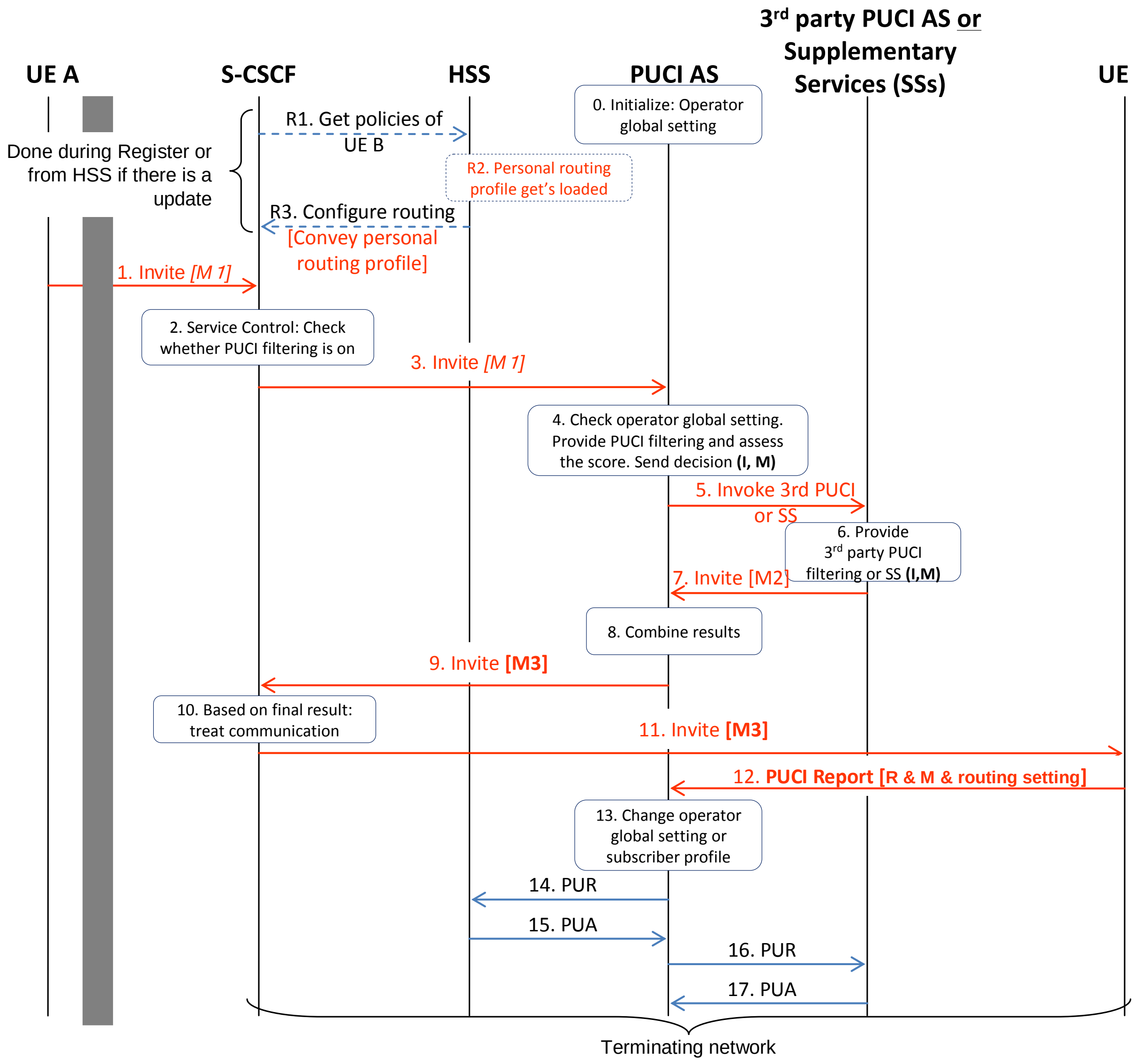

UE A
S-CSCF
HSS
PUCI AS
3rd party PUCI AS or Supplementary Services (SSs)
UE B
0. Initialize: Operator global setting
Done during Register or from HSS if there is a update
R1. Get policies of UE B
R2. Personal routing profile get's loaded
R3. Configure routing [Convey personal routing profile]
1. Invite [M 1]
2. Service Control: Check whether PUCI filtering is on
3. Invite [M 1]
4. Check operator global setting. Provide PUCI filtering and assess the score. Send decision (I, M)
5. Invoke 3rd PUCI or SS
6. Provide 3rd party PUCI filtering or SS (I,M)
7. Invite [M2]
8. Combine results
9. Invite [M3]
10. Based on final result: treat communication
11. Invite [M3]
12. PUCI Report [R & M & routing setting]
13. Change operator global setting or subscriber profile
14. PUR
15. PUA
16. PUR
17. PUA
Terminating network

**Figure 7.2-6: PUCI invocation with 3rd party PUCI AS and SS.**

5. The PUCI AS then invokes a 3rd party PUCI AS or SSs. This message could be an extended SIP INVITE message.

6. The 3rd party PUCI AS or SS then checks (I) and gives marking (M2). In case of SS this could be an error code as defined by IETF [14] or the SS could be extended to give marking defined for PUCI. Marking in the described form might not be required in all cases. For example, in the case of SSs with Black List/White List (BL/WL) a marking in the sense of a UC score is not necessary. In the case of a BL the UC score (M) is 100% if the caller is on the BL and 0% if the caller is not on the BL.

7. M2 is sent to the PUCI AS. This message could be an extended SIP INVITE message.

8. The PUCI AS then combines different results it received and the checks it had done which results in a new marking M3.

9. M3 is then sent to the S-CSCF as part of the SIP INVITE message.

10. The S-CSCF then checks user settings received in Step 4 and makes routing decision accordingly. It could be that the call is sent to an answering machine or forwarded elsewhere. In this example the communication is sent to the Callee (UE B).

11. The S-CSCF then forwards the SIP INVITE to the Callee (UE B) with the marking (M).

12. It is possible for the Callee (UE B) to report a communication as a UC or to change its profile in the HSS. Such information can be sent from the Callee (UE B) UE to the PUCI AS. Reporting from the Callee (UE B) can be done in several different ways, e.g. via a Web interface, keypad entries; Ut interface or piggybacking to a existing message.

13. Based on the message from the Callee (UE B) the PUCI AS can optionally modify the operator global setting and/or subscriber profile. These optional modification are dependent on local legislations and prior consent from the user.

14. To change the subscriber profile the PUCI-AS sends the Diameter message profile update request (PUR) [12 - 13].

15. The HSS responds with a Diameter message profile update answer (PUA) [12 - 13].

16. The PUCI AS can update subscriber profile in the SS or else where if needed.

17. PUCI AS will receive a response for the update.

#### 7.2.5.4 Standardization

Required standardization is given below based on Figure 7.2-6:

- Step R2: Information to be stored in the HSS; this could range from a simple flag upto a complete PUCI profile of the user because it is possible to store these information in the HSS or in the PUCI AS.
- Step R3: Message from HSS to S-CSCF with payload containing PUCI setting and routing information for a given UE [15 - 16].
- Steps 1, 3 and 9: SIP INVITE message extended to carry M if transfer of marking is required.
- Step 5: Optional invoking of 3rd party PUCI AS or SSs depending on configuration.
- Step 7: Optional response from SS or 3rd party PUCI AS with M depending on configuration.
- Step 12: User informing R, M and request to change settings. This can be piggybacked in an existing message. In addition, use of alternatives means like the web interface, keypad entries and the Ut interfaces could be defined.

## 7.3 SPIT/UC Protection with Supplementary Services

### 7.3.1 Introduction

This clause describes the usage of Supplementary Services for SPIT/UC prevention.

The approach is to use Supplementary Services, already existing in IMS and PSTN, to define and manage a personal SPIT/UC prevention profile. While the resources to store and execute the Supplementary Services based SPIT/UC prevention profile are provided by the IMS network, the user may have the ability to remotely manage this profile.

The main reasons to use specific Supplementary Services for SPIT/UC prevention are:

- already existing Supplementary Services can be used at once and provide effective means for SPIT/UC protection
- Supplementary Services work in all type of networks, IMS as well as legacy networks, and enable therefore a unified approach to proceed against SPIT/UC
- Supplementary Services do not require any changes to the IMS architecture or SIP

Subsequently the use of Supplementary Services is described in more detail.

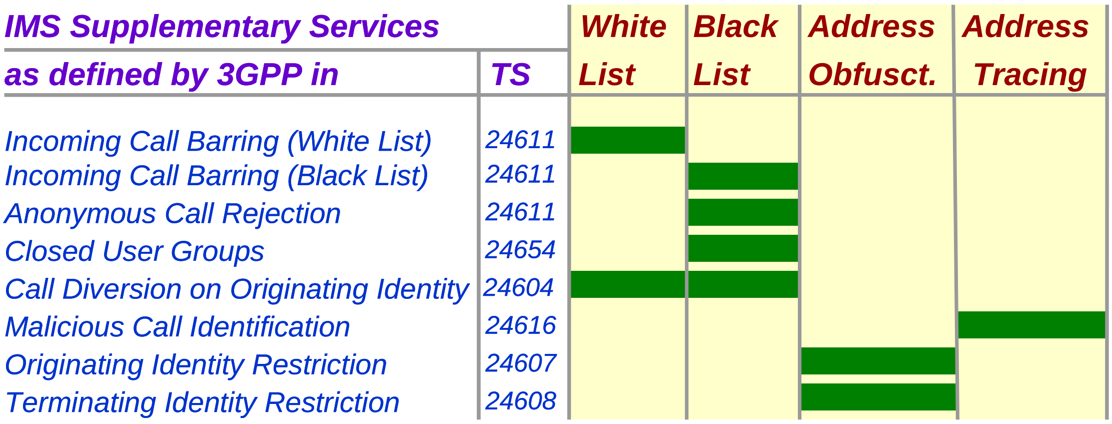
It is pointed out here that there is no conflict between the use of the IMR approach and the use of Supplementary Services to combat UC. They may even complement each other. The use of Supplementary Services to combat UC relates to IMR in the following way: when a call is *identified* as UC (by means outside the scope of Supplementary Services) then, as a *reaction* to this occurrence of UC, a user or a network may decide to e.g. put a calling party on a black list. Supplementary Services do not *mark* a particular call as UC, but rather *mark* a particular user as being a potential UC source (black list), or another user as certainly not being a UC source (white list). Once such lists have been created, a further call is *identified* as UC, or definitely not UC, by comparing the call source identity with the lists. The *reaction* is determined by the logic of the particular combination of supplementary services, as described below.

### 7.3.2 Supplementary Services usable for SPIT/UC Prevention

Supplementary Services for SPIT/UC protection may be used to realise a form of network-supported user self protection. This makes a work split between network and user possible. While the network provides Supplementary Services with resources like e.g. black- or white lists, the user may configure these resources according to his personal SPIT/UC prevention needs. The advantage of this work split is that users carry the responsibility for the measures to be taken. This may be required, depending on national regulations, as the network provider may not be allowed to suppress calls without the user's explicit consent.

Network support in this context neither means the provision of a SPIT/UC score related to incoming calls nor an automatic SPIT/UC protection of users, performed by the network.

Figure 7.3-1 gives an overview of IMS Supplementary Services that are applicable for SPIT/UC prevention.



| IMS Supplementary Services as defined by 3GPP in | TS | White List | Black List | Address Obfusct. | Address Tracing |
|---|---|---|---|---|---|
| Incoming Call Barring (White List) | 24611 | 🟩 | | | |
| Incoming Call Barring (Black List) | 24611 | | 🟩 | | |
| Anonymous Call Rejection | 24611 | | 🟩 | | |
| Closed User Groups | 24654 | | 🟩 | | |
| Call Diversion on Originating Identity | 24604 | 🟩 | 🟩 | | |
| Malicious Call Identification | 24616 | | | | 🟩 |
| Originating Identity Restriction | 24607 | | | 🟩 | |
| Terminating Identity Restriction | 24608 | | | 🟩 | |

Figure 7.3-1: Overview of Supplementary Services for SPIT/UC Prevention

Already these Supplementary Services provide some of the SPIT/UC prevention solutions, discussed in RFC5039 from Rosenberg and Jennings, as there are White Lists, Black Lists and mechanisms to protect the privacy of a user's address. In particular the features of these Supplementary Services are:

Incoming Call Barring with White List:

Incoming Call Barring, based on a White List, enables a subscriber to allow incoming calls matching the entries of the White List. If the caller's number is not on the White List, he receives an announcement telling that the subscriber is not accepting calls from this number. If the caller's number matches the White List, the caller is directly put through to the subscriber. Therefore a White List can be used to allow access for all trusted users.

Incoming Call Barring with Black List

Incoming Call Barring, based on a Black List, enables a subscriber to reject calls matching the entries of a Black List. If the caller's number is on the Black List, he receives an announcement telling that the subscriber is not accepting calls from this number. Such a Black List can be used to reject known SPIT/UC sources.

Anonymous Call Rejection

Anonymous Call Rejection is a special case of Incoming Call Barring with Black List, but in this case the rejection of a user is based on the usage of the anonymity feature and not on the entry in a Black List. All calls where the asserted Public User ID is restricted are rejected. This service is important as SPIT/UC sources will often use the anonymity feature to hide their identity.

Closed User Groups

This is a special case of a trust network, based on a White List. The difference to 'Incoming Call Barring with White List' is that not only incoming but also outgoing calls have to match the White List. Therefore subscribers of Closed User Groups are allowed to have active/passive calls only with members of their group. This service provides a strong protection against SPIT/UC and may be applicable e.g. for working groups or for communities.

Call Diversion on Originating Identity

By means of Call Diversion, based on originating identity, the subscriber is able to re-direct unsolicited calls to another destination, e.g. a SPIT/UC voice mailbox. This Supplementary Service is based on screening lists. If a caller's number matches the screening list, then the call is diverted to a pre-selected telephone account whilst non-matching calls are put through to the subscriber.

Malicious Customer Identification

If Anonymous Call Rejection is not activated, an anonymous SPIT/UC source can be identified with Malicious Customer Identification in order to put it on a Black List. Malicious Customer Identification enables a user to generate on request a call trace of the last call. The recorded information is written to a file, accessible to the operator.

Originating/Terminating Identity Restriction

This Supplementary Service is ambivalent. On the one hand it allows a SPIT/UC source to hide its identity, on the other hand it allows also a subscriber to protect the privacy of his address. This may be useful for a bona fide user e.g. when he is calling a company to inquire about a product, but does not want to end up on their list for phone marketing.

### 7.3.3 SPIT/UC Prevention Scenarios with Supplementary Services

Supplementary Services can not only be used as single services to proceed against SPIT/UC, but several of them can be combined to more complex SPIT/UC prevention scenarios. The following sub-sections give some examples, starting from simpler up to more sophisticated SPIT/UC prevention scenarios.

#### 7.3.3.1 Simple Black List combined with Anonymous Call Rejection

Figure 7.3-2 shows a rather simple SPIT/UC prevention scenario that combines a Black List either with Anonymous Call Rejection or with Malicious Customer Identification.

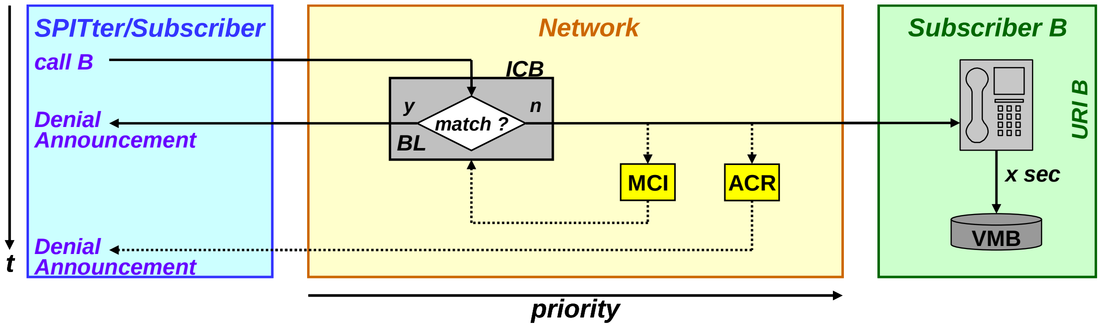


Figure 7.3-2: Simple Black List with Anonymous Call Rejection

The Black List (BL) can be realized with Incoming Call Barring (ICB) and carries the numbers of known SPIT/UC sources. If the caller matches a Black List entry, the call is rejected and a denial announcement is p layed, otherwise the caller is put through to subscriber B.

As mentioned before, SPIT/UC sources often use the anonymity feature to hide their identity. Therefore it is additionally possible to activate Anonymous Call Rejection (ACR) to block anonymous calls. Also in that case the callee is informed about the rejection by a denial announcement. The combination of these two Supplementary Services provides a stronger SPIT/UC protection than each of them alone.

NOTE: Continuous information messages can lead to a quite severe network load; hence best keep minimal to avoid high usage of resource

If a subscriber doesn't like to generally block anonymous calls, he can disable Anonymous Call Rejection and enable alternatively Malicious Customer Identification (MCI). With that he is able to initiate the identification of anonymous SPIT/UC sources and to put them afterwards on the Black List.

### 7.3.3.2 White List with Consent Mailbox

Figure 7.3-3 shows a SPIT/UC prevention scenario where a White List (WL) is combined with a Consent Mailbox (CMB). Compared to the 'Simple Black List Scenario from chapter 7.3.3.1 a second telephone URI is needed for the Consent Mailbox. This URI is not visible to the caller.

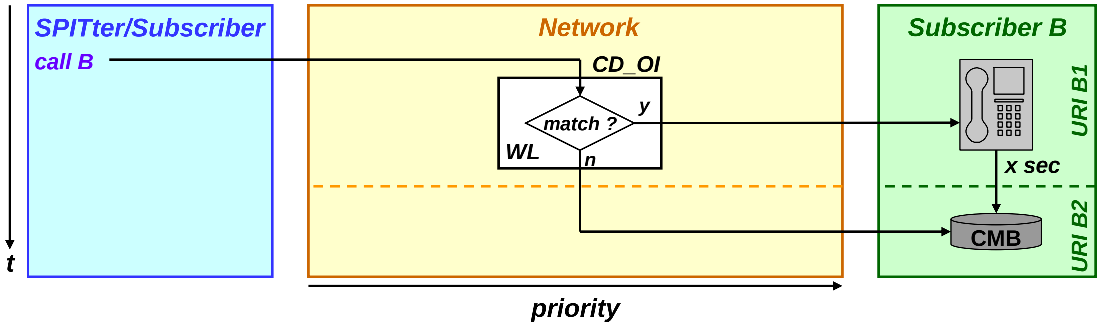


Figure 7.3-3: White List with Consent Mailbox

A White List with Consent Mailbox can be achieved with Call Diversion on Originating Identity, sometimes also known as Selective Call Forwarding.

If the caller matches a White List entry, he is put through to subscriber B. If however the caller doesn't match a White List entry, he is re-directed to the Consent Mailbox. With that callers have the chance to convince subscriber B either to call them back or to put them on the White List. This procedure is called 'getting consent' and is one possibility how the introduction problem (how do I get on the White List?) can be solved. A disadvantage related to consent achievement by means of a Consent Mailbox is that legitimate users may not get immediate access to subscriber B in urgent cases.

Compared to the Black List, the White List provides a much better protection against SPIT/UC. It can not easily be circumvented by spoofing the originating identity. The disadvantage of a pure White List approach is usually that also legitimate callers, not being on the White List, are not able to reach subscriber B (introduction problem).

### 7.3.3.3 White List with Consent Mailbox, protected by a Black List

Figure 7.3-4 shows an enhancement of the 'White List with Consent Mailbox' scenario from chapter 7.3.3.2 that further improves the SPIT/UC protection for subscriber B.

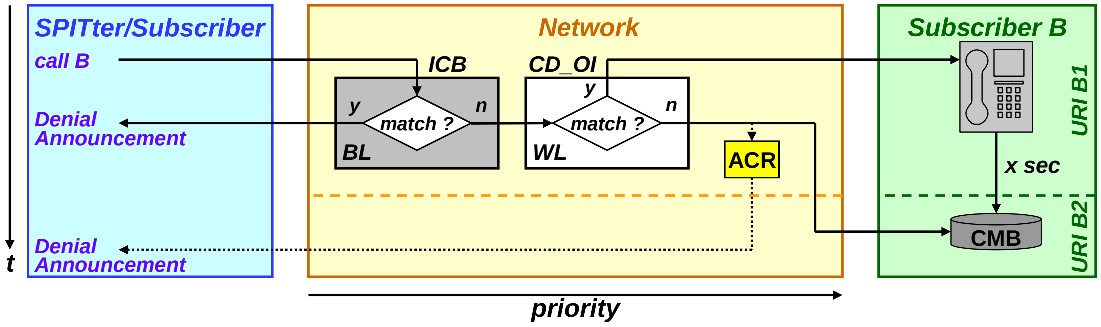


Figure 7.3-4: White List with Consent Mailbox, protected by a Black List

The basic functionality of the White List (WL) is the same as in chapter 7.3.3.2.

In the simple White List solution of chapter 7.3.3.2 already known SPITters are able to leave a message on the Consent Mailbox (CMB), thus causing nevertheless nuisance to subscriber B by forcing him to listen to these messages. This gap can be closed by protecting the Consent Mailbox with an additional Black List (BL), realized with Incoming Call Barring (ICB). Known SPITters, matching a Black List entry, are directly rejected with a denial announcement.

Optionally it is possible to activate 'Anonymous Call Rejection (ACR)' in front of the Consent Mailbox as protection against SPITters using the anonymity feature.

### 7.3.3.4 Sophisticated SPIT/UC Prevention Profile with Audio CAPTCHA

The text in this subclause shows by way of example, how standardized features like supplementary services, announcement and PIN entries transmitted by key press could be combined to enhance protection against UC. All these features and combinations have to be carefully balanced against usability requirements. In particular, the overriding of White Lists by having callees entering PINs or solve audio riddles may need to be carefully examined with respect to their suitability for widespread use in public telephone networks. It is difficult to imagine that any of these features would be mandated for use.

Figure 7.3-5 shows a sophisticated SPIT/UC protection configuration with cascaded Supplementary Services that enables subscriber B to configure a rather complex SPIT/UC prevention profile.

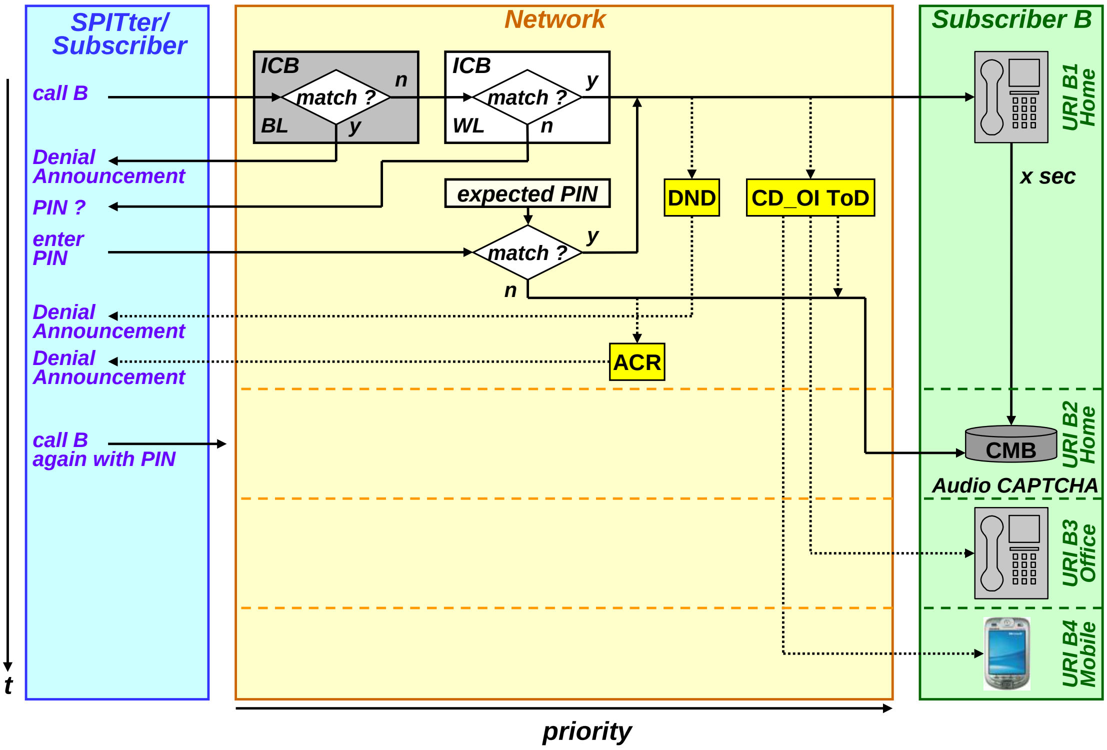


Figure 7.3-5: Sophisticated SPIT/UC Prevention Profile with Audio CAPTCHA

The Black List (BL) on the left side, realized with the Supplementary Service ‘Incoming Call Barring (ICB)’, rejects all matching numbers with a Denial Announcement thus protecting from known SPITters.

The Black List is followed by a White List (WL). Callers matching an entry on the White List are directly put through to subscriber B. While it is possible to circumvent a Black List by address spoofing, it is challenging to guess the entries of a White List. Therefore a White List is a strong protection for subscriber B.

As mentioned before (see chapter 7.3.3.2), a White List has the disadvantage that only callers matching the White List are able to reach subscriber B. As a consequence not only SPITters but also many legitimate users may be excluded. This problem (how do I get on the White List?) is usually called the introduction problem. The approach to solve this problem is called consent-based communication.

Incoming Call Barring can be easily enhanced by a feature that exists in many voice applications today and allows overriding of the White List by entering feedback e.g. a PIN or using voice commands. Therefore a user not matching the White List is asked by an announcement to enter the PIN. The PIN, e.g. entered by means of the telephone keypad, is then compared to the expected PIN and the caller is put through to subscriber B if the PIN is correct. If not, the caller is forwarded to a so called Consent Mailbox (CMB). This Consent Mailbox can be either at user’s site or it can be a network-based mailbox. This mailbox performs now an automated Turing Test, a so called audio CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to prevent subscriber B from being called by SPIT/UC automata. The consent mailbox asks the caller a riddle where the solution of the riddle is the required PIN. This riddle can usually only be solved by a human and not by SPIT/UC automata. As every subscriber is able to create his personal audio riddle, it is not so easy to circumvent this Turing test, as the question has really to be understood and solved. Three basic audio CAPTCHA requirements are stated to meet a fairly sophisticated Turing Test level:

- The PIN identified in the riddle should be 'encoded' in such a way as to make it unintelligible to sophisticated voice recognition/interpretation systems;
- Furthermore the encoded riddle should not be so difficult that the caller is discouraged.
- Care needs to be taken so that any method selected does not discriminate against people because of their audio or visual impairment

If a human caller is able to solve the Turing test, he now possesses the PIN and is able to immediately call subscriber B again and will be put through after entering the correct PIN. This second call causes maybe additional cost plus additional time and therefore this SPIT/UC prevention scenario contains also elements of a grey list whose functionality is based on human behavior. It doesn't protect from human SPITters, but as the procedure is cost and time consuming, it is usually not paying for a SPITter with commercial interest. In case that a human SPITter has overcome all these hurdles and nevertheless reaches subscriber B, he can be put on the Black List if not calling anonymously, and is then blocked at the next call attempt. If the call is not urgent, another possibility to get consent with subscriber B is to leave a message on the consent mailbox after the Turing test is played in order to convince him to either call back or to put him on the White List.

The sophisticated SPIT/UC prevention scenario provides optionally some additional features as indicated by the yellow boxes with the dotted lines in Figure 7.3-5. They can be enabled on demand.

Anonymous Call Rejection (ACR) can be enabled if subscriber B generally wants to exclude anonymous callers. This can be an effective measure as commercial SPITters often use the anonymity feature whether allowed by legislation or not.

Do Not Disturb (DND) allows to occasionally block all external callers if subscriber B doesn't like to be interrupted, e.g. during a football match.

Call Diversion on Originating Identity with Time-of-Day feature (CD_OI ToD) is a very powerful Supplementary Service enhancement providing Black- and White Lists (selectable by user) that can be additionally combined with time tables. This service can be used to further restrict the White List (based on Incoming Call Barring) in a time dependent way, e.g.

- to further restrict the ICB White List during night time,
- to forward calls on the mobile on weekends,
- to forward calls to the office during office time.

### 7.3.3.5 White List Consent Achievement by IN Server

An alternative method to override the White List (e.g. realized by means of Incoming Call Barring) and to achieve consent, compared to the PIN-based approach as explained in chapter 7.3.3.4, draws on classical Intelligent Network (IN) services. The method is based on the setup of a (potentially temporary) second identity for the callee by an IN server and the charging of a small service fee. The idea of the service fee is that it is sufficiently high to deter SPITters sending bulk UC, but sufficiently low so as not to encumber legitimate users who are not yet on the white list.

This service fee is inspired by the 'Payments at risk' approach in RFC 5039 by Rosenberg and Jennings [11], which uses micro-payments to be transferred between caller and callee. This technique is seen as applicable to encounter call spam and IM spam (unsolicited communication in 3GPP terminology). But instead of a (currently not existing) micro-payment infrastructure the approach in this clause assumes that the terminating operator uses well-established IN services and keeps the service fee rather than transferring money between caller and callee. If effective authentication is available, then the service fee may be charged only at the first attempt to reach subscriber B, because then B can then put A on the white list if B accepts A as a legitimate user.

Below only the basic method of consent achievement by IN server is explained, but the scenario could as well be enhanced by further elements as explained in chapter 7.3.3.4 to achieve a more sophisticated SPIT/UC prevention profile. It is as well imaginable that consent achievement by PIN (see 7.3.3.4) and consent achievement by IN server could be used in one SPIT/UC prevention profile in parallel, e.g. selectable by the caller via an announcement and speech feedback. This makes sense if for example a member of the family, knowing the PIN, calls from a public phone box and wants to avoid an extra-charge by the IN server.

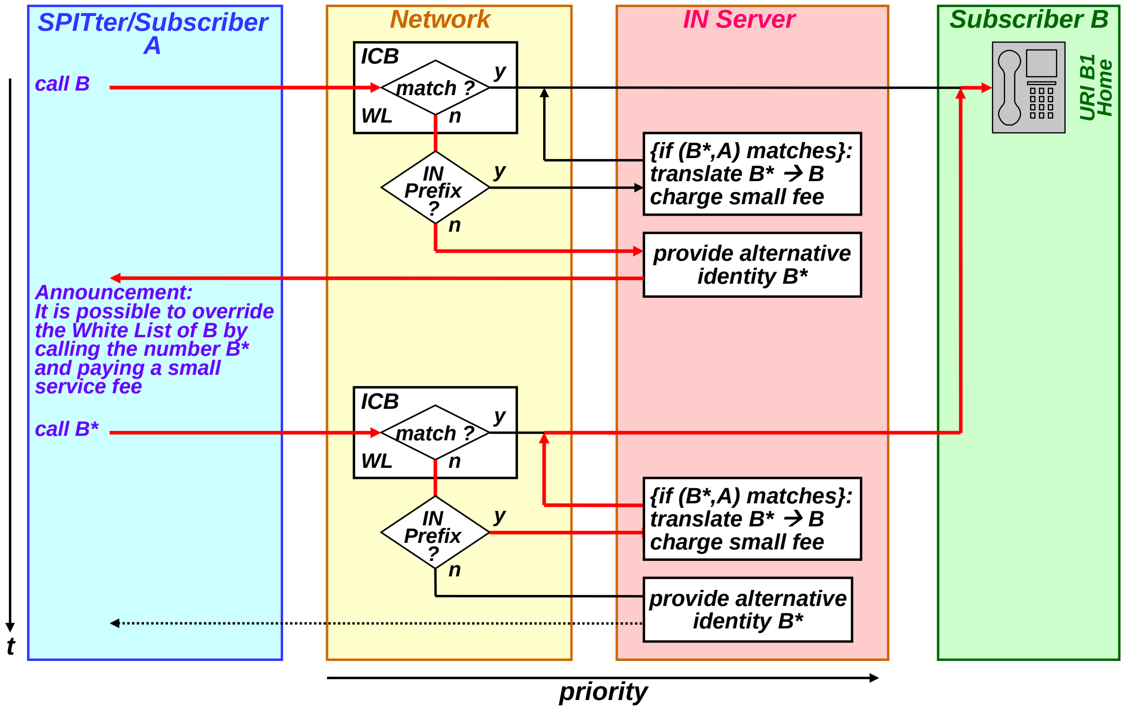

SPITter/Subscriber A
Network
IN Server
Subscriber B
URI B1 Home
call B
ICB
match ?
WL
y
n
IN Prefix ?
y
n
{if (B*,A) matches}: translate B* → B charge small fee
provide alternative identity B*
Announcement: It is possible to override the White List of B by calling the number B* and paying a small service fee
call B*
ICB
match ?
WL
y
n
IN Prefix ?
y
n
{if (B*,A) matches}: translate B* → B charge small fee
provide alternative identity B*
t
priority

Figure 7.3-6: White List Consent Achievement by IN Server

Figure 7.4-6 shows the procedure to achieve consent by overriding the White List of B, supported by an IN server: Assume that a callee with number B has a second number B* with IN prefix. Callers matching the White List are directly put through to subscriber B. If the caller doesn't match the White List, but the called number B* contains the IN prefix, then he is forwarded to a White List bypass function in the IN server. The IN Server translates B* to B, bypasses the White List and the caller is put through to B, but is charged a small service charge.

If the caller does not know the number B* and simply dials B, the caller is nevertheless forwarded to the IN server to a function block that provides a second identity for the callee B by setting up an alternative number B*. This alternative number B* can be either assigned in a fixed systematic way or in a fixed but non-systematic way or it can be assigned dynamically. Now an announcement is played to the caller that he can reach subscriber B by calling the alternative number B*, if he is willing to accept a small service charge.

Assumed that the caller accepts the small service charge, he now calls the alternative number B*. Still not being on the white list of subscriber B, he is again forwarded to the IN server, but now to the function block with the white list bypass because the alternative number B* contains an IN prefix. In the IN server B* is translated to B and the caller is now put through to subscriber B. Additionally, in case of dynamic assignment of B*, it may be controlled by the IN server whether the caller ID (A) is the same as the one the number was given to at the first call attempt.

From a technical point of view it is more difficult, but not impossible for a SPITter or a bulk UC system to bypass the white list of subscriber B. But at least under commercial aspects this attempt is not paying for bulk UC applications as SPITters calculate with costs in the order of micro-cents (and not in the order of cents) to achieve some gainings. However for a legal user a small service fee in the order of cents will be no hurdle if he is really willing to reach subscriber B.

### 7.3.3.6 SPIT/UC Feedback by User Based on Key Pad Entries in the Phone

Similar to what was said at the beginning of the preceding subclause, the features described here have to be carefully balanced against usability requirements, and should be optional.

For this feature, the user gives feedback to the network by entering digits on the key pad of his phone. In analogue telephones, this feature is realized using key press signaling. But also mobile or SIP phones provide features emulating the key press feedback.

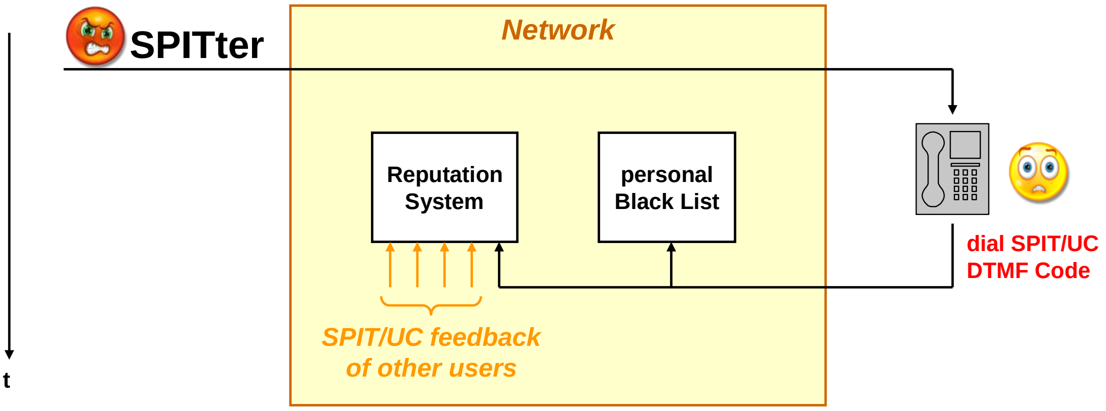


Figure 7.3-7: Key Press Based SPIT/UC Feedback

Figure 7.3-6 shows how key press-based signaling can be used to provide a SPIT/UC user feedback.

Either a new Supplementary Service or the enhancement of existing Supplementary Services could be used to provide a SPIT/UC feedback possibility, based on the use of the phone’s key pad. It should be noted that all SPIT/UC Prevention scenarios as described in chapter 7.4.3.1 to chapter 7.4.3.5 can be enhanced by such a feedback possibility. The SPIT/UC victim indicates by a specific key sequence either during or after the call that he/she perceived nuisance by SPIT/UC.

This SPIT/UC feedback can be used in two ways:

1. Automated Personal Black Listing
   Key press based SPIT/UC feedback provides an easy solution for a user to put the number of a caller, perceived as SPIT/UC, on the personal Black List. In case of network supported user self protection the personal Black List is located inside the network.
   If a signaling based feedback solution is not available, then the feedback for the user is more troublesome. Other feedback channels, partly also used today are e.g.
   - calling the customer care center
   - writing a SMS or a mail to the customer care center
   - self administration of the personal Black List via an operator web interface
2. Input for a Reputation System
   The SPIT/UC related feedback can additionally be provided as input for a network based reputation system. Only a system, gathering the SPIT/UC feedback from multiple users, is able to create an aggregated view of a caller’s behavior regarding SPIT/UC.

NOTE: It should be noted that there are lot of complexities in implementing reputation systems.

## 7.4 Contextual Information

### 7.4.1 Introduction

This section describes how marking with contextual information regarding an incoming communication could be provided as a partial solution to the *introduction problem*, i.e., for a communication between users A and B, when B does not previously know A. This contextual information could be used as additional criteria to filter or redirect communications on, or be presented to the end user to make a decision regarding whether to, e.g., accept an incoming call.

IMS already provides different type of contextual information that is valuable for the decision process (such as calling party identities, access network information etc), Thus, this contextual information should be seen as complementary to existing information.

### 7.4.2 IMS Mechanism Outline

The intent of the information is to provide additional critera for making a decision on how likely it is to be unsolicited communication. Therefore, a reasonably light weight marking mechanism could be built on the use of private SIP headers. However, this is an implementation detail best left for the technical specification.

More important is to identify useful contextual attributes that could be used to complement existing information in the IMS messages. The following possibilities are suggested:

| **Attribute** | **Type** | **Values** | **Explanation** |
|---|---|---|---|
| *IdentityStrength* | static | Unknown<br>IMS-AKA<br>SIP Digest auth.<br>SIP Digest auth. with TLS<br>GIBA<br>NBA<br>Non-IMS verified subscriber<br>Non-IMS unverified subscriber | Indicator of how trustworthy the presented origination identity is. This can depend on the strength of the authentication method, and to what extent the subscription can be tied to a person or organization. |
| *CostCategory*<br>NOTE: It may not be allowed due to national regulations to forward cost related information between operators.<br>Editor's Note: The values to be used for this category is for further study as cost information may become very complex. | static | Unknown<br>Free<br>Flat rate<br>Volume charged (per minute or per call) | Indicator of cost of communication. |
| *OriginNetwork* | static | Network | The network originating the request. |
| *OriginNetworkType* | static | Unknown<br>IMS<br>PSTN/CS<br>Internet | Originating network category; assuming that different categories are associated with different trustworthiness. |
| *CallComplaintFraction*<br>NOTE: This is a form of scoring for general discussion on scoring please refer to Section 4.1. | dynamic | | Fraction of calls (real-time communications) from a specific user resulting in UC feedback. |
| *MessagingComplaintFraction*<br>NOTE: This is a form of scoring for general discussion on | dynamic | | Fraction of messages (non-realtime communications) from a specific user resulting in UC |

| | | | |
|---|---|---|---|
| scoring please refer to Section 4.1. | | | feedback. |

Attributes of type “static” depend only on the originating subscriber or the originating network, whilst “dynamic” attributes need to be calculated based on observed behaviour (with certain exceptions).

## 7.4.3 Use of Contextual Information

### 7.4.3.1 General

To describe the usage of the contextual information we refer back to the IMR solution variant leveraging supplementary services described in Section 7.2.4.2. As already stated, the general idea behind defining contextual information for communications relevant for PUCI is to augment the information that already exists in signalling messages (such as calling party identities, access network information) to provide additional criteria for PUCI reaction policies. Existing supplementary services (SS) can, for instance, be used to react based on calling party identities. However, the reaction policies may be constrained by the currently available information. Thus, reaction mechanisms and policies can benefit from additional contextual information regarding communications being available to the decision process. Moreover, such contextual information should have clearly defined semantics. That is, the information should be easy to interpret and readily verifiable. Communications can be marked with contextual information, or it can be provided alongside the communication through some side channel. This is currently left open. To simplify the description we will assume that the communication is marked with contextual information.

### 7.4.3.2 Reaction

As indicated in Section 7.2.4.2, existing SS mechanisms, when appropriately augmented, could be used to react to incoming communications, That is, they would interpret a PUCI policy defined by the end user or by the operator and enforce it based on the contextual information available regarding the communication. (A user controllable policy is desirable to permit adjustments for specific needs. However, to make it practical this should be combined with predefined operator controlled policy settings and possibly operator specified profiles to assist the user.) The PUCI policy could simply be an extended version of the SS settings currently available where constraints on the proposed added contextual information can be specified.

### 7.4.3.3 Marking

Marking with contextual information needs to be performed where the information in question is readily available, and thus dependent on the specific information.

- Identity strength is, if possible, supplied by the CSCF in the originating network. However, this may be altered by the IBCF in the destination network, for instance, if the given information is not trusted.
- Cost category needs to be supplied by the originating network. However, this information may be sensitive to pass between operators. In some such cases, it might be possible to set a category in the IBCF simply based on the identity of the originating network (for instance one that provides free calls through an advertisement driven business model, or similar).
- Origin network should be supplied by the originating network, where possible.
- Origin network type is supplied by the IBCF based on the type and identity of the originating network.
- Complaint fraction information would be collected by the PUCI functionality in the destination network and supplied by it for use by the reaction mechanism. In order to be able to collect this information, the PUCI functionality needs to be able to observe all communications in the destination network and receive all feedback information from users.

Finally, some contextual information may be supplied to the callee to help him/her to determine whether to take a call. However, in such a case usability aspects are critical, so only limited information in a simplified form would come in question. Examples of potentially useful information to display to end users may include a notification if authentication of the caller identity is known to be weak (for instance from a free account at an Internet VoIP provider), or there has been a large (above some threshold) fraction of complaints about the caller.

#### 7.4.3.4 Sharing of Information

Some of the proposed contextual information is most useful if shared between operator networks. However, it is also the case that some of the information may be considered sensitive and, thus in some cases, not be possible to share. The need for and consequences of information sharing for each case are as follows:

- Identity strength is most useful if provided by the originating network and made available to the destination network. In general, this information is not expected to be of a sensitive nature. If particular values (cases) are identified as sensitive, it should be possible to omit them and still provide useful information.

- Cost category is also most useful if provided by the originating network to be used in the destination network. However, this information may be sensitive, so can most likely only be optionally provided. In some cases, it may be known by the destination operator that an originating network employs a certain business model which defines the cost category (for instance, when interworking with "Internet VoIP providers"), at least in terms of a coarse dichotomy between free and charged calls. In this case, the destination network could mark incoming communications in a border node if no information has been provided by the originating network. If no cost category is provided by the originating network and the destination network cannot determine cost category, a border node can mark it as cost category "unknown" to indicate that this field should be ignored when enforcing PUCI policy.

- Origin network information should be provided by the originating network to the destination network. However, it is not expected to be sensitive.

- Origin network type information does not need to be shared, as it is provided and used internally within the destination network.

- Complaint fraction information can be collected and used locally in the destination network. Thus, it does not *have* to be shared between operator networks, which could avoid potential liability or privacy concerns. However, it would require that the destination network track the behaviour of subscribers in other networks. The scalability implications of such an approach are FFS. Alternatively, if local legislations and operator preferences do not preclude sharing of such information, it could also be possible to share this information in two ways:

  1. Information collected about user behaviour in the originating network could be shared with the destination network for policy enforcement.

  2. Complaint information collected in the destination network could be shared with the originating network, to be used according to (1) above.

  This could avoid potential scalability issues with user behaviour tracking. However, it would require trust between the operators regarding such information, and may raise privacy and liability concerns as already mentioned.

#### 7.4.3.5 Impact on Supplementary Services

As previously mentioned in Sections 7.4.1 and 7.4.3.1, the proposed PUCI contextual information could be used by SS mechanisms as complementary information to already existing information about the communication. Thus, relevant SS functions, such as CDIV, CB, MCID, would need to be augmented to be able to identify and process the additional PUCI contextual information fields, and policy definitions for communication handling similarly would need to be augmented.

Beyond these additions, no further impact is expected on SS mechanisms from the use of PUCI contextual information.

## 7.5 UC protection framework for non-IMS interconnection: the Open Proxy Handshake

### 7.5.1 Objectives

Based on the assumptions provided in section 5.3 and on the analysis of existing protection mechanisms given in Annex B, the framework shall meet the following objectives:

- Focus on non-IMS interconnection and address the main threats identified in this scenario:

  - Forged sender/domain identity threat.
  - Forged network information threat (IP spoofing with UDP transport).
  - Attacker versatility threat.
  - DoS threat on OI-CSCF functions in the receiving domain.
- Enable secure VoIP exchanges at least at the signalling level and if possible at the media level also.
- Support the roaming scenario where the sender is in a visited network.
- Be scalable to a large number of interconnected domains.
- Do not require extensive use of asymmetrical cryptography (such as in [18]) because of the CPU burden put on the receiving domain for checking.
- Support sporadic communications between domains, meaning it is not required to maintain permanent connections between each pair of domains.
- Use as far as possible existing mechanisms or standards to reduce implementation complexity.

NOTE: This proposal aims to describe inter-working mechanisms between IMS and non-IMS networks. The standardization of non-IMS networks and corresponding mechanisms is not under the responsibility of 3GPP and therefore, such solution can not be standardized by the 3GPP.

### 7.5.2 Assumptions

The main assumptions are described in sub-sections 5.3.3 and 5.3.4 with the following additions:

- The OI-CSCF function in domain B is responsible for allowing (or blocking) the incoming calls from non-IMS domains but the server supporting the OI-CSCF does not necessarily handle the call itself (i.e. processing of the INVITE request and subsequent signalling messages).
- There may exist in domain B one or several servers supporting the P-CSCF/S-CSCF functions to which are directed the calls allowed by the OI-CSCF function. These servers may be distinct or not from the servers supporting the OI-CSCF function.
- In domain A there may be other proxies or entities involved in call routing. These proxies are different from the outbound proxy in that there are not responsible for authorizing outside calls and they do not need to be registered in DNS or equivalent Internet service.
- In case of roaming scenario, the above proxys may be located in the visited domain.
- For simplicity purpose VoIP calls are supposed to be uni-directional; they always originate from network A and targeted to network B.
- Two cases shall be distinguished for security assumptions :
  - There is no shared secret between domain A and domain B (case SA).
  - A shared secret has been established between domain A and domain B (case SB).

The above assumptions are relevant when domain A is a legitimate domain willing to interconnect with domain B. If domain A is an attacker domain, some assumptions shall deliberately not be met, but the proposed framework shall still protect domain B.

The general architecture is illustrated by the following figure; Figure 7.5-1:

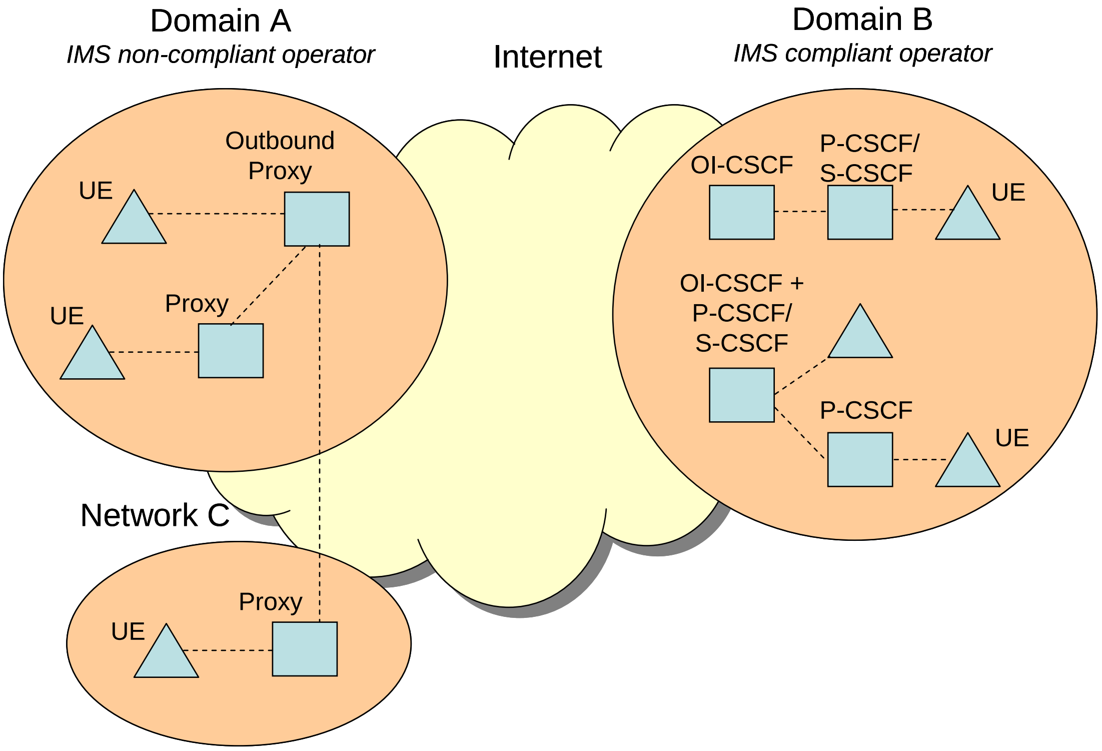


**Figure 7.5-1: Non-IMS interconnection general architecture**

## 7.5.3 Basic principles

The proposed interconnection and protection framework operates as follows:

1) **Authorization phase in the sending domain**: the sending UE triggers an authentication/authorization phase with the outbound proxy in domain A. This phase may be triggered by the UE itself or by a proxy in domain A or in the visited network receiving the INVITE request from the UE. If the outbound proxy authorizes the call it shall create a token/ticket called "ticketA" to contact domain B.

2) **Notification phase**: this phase is comparable to a "Hello" procedure between domain A and domain B where domain B is notified of the forthcoming call. During this phase, domain B performs some kind of return routability check to verify that network information is valid and also that sender identity is asserted by domain A. The notification phase is handled differently depending on whether a shared secret is available or not between domains A and B (see below). The notification phase is initiated when a notification messages containing "ticketA" is sent from domain A to domain B; this notification message may be sent by the UE itself or by a proxy serving the UE. On the one hand, the notification phase requires more signalling than sending directly an INVITE request, but on the other hand it provides the following benefits:

   - Notification request is lighter to proceed (from a CPU perspective) than INVITE request. By the way, notification processing is designed to be stateless for OI-CSCF in domain B. Since a forged notification request would have less impact for domain B than a forged INVITE request, the main benefit is actually to protect domain B.
   - Notification request does not lead to reservation or opening of media ports as it may be the case for an INVITE request with SDP payload.
   - Notification phase may be used by domain B to pass some challenge to be solved by sending UE or sending proxy in domain A.
   - Notification phase may be used to exchange keying material between domains to establish secure signalling or media sessions. From this perspective, this phase is comparable to the initial KMS exchange described in TR 33.828 [25].
   - Notification phase may be used to perform pro-active routing by domain B in order to direct the INVITE request to the most appropriate function or equipment.

- The notification phase sets a barrier between the sender and the receiving UE and SPAM campaigns analysis have shown that most of the time the spammer does not retry when the sending is not straight-forward.

3) **Authorization phase in the receiving domain**: if the notification phase is successfully passed, the OI-CSCF function in domain B decides whether or not it authorizes the incoming call. The decision may be based on white or black list information, user preferences (e.g. no calls allowed after 10pm), sender or sending domain reputation… The decision may be to reject the call, direct the call to a mailbox or to a SPIT analysis system or eventually accept the call. In other words, this phase relies on mechanisms already described in sections 7.2 and 7.3.

4) **Token distribution**: if the call is being allowed by domain B, the OI-CSCF function generates a token for this specific call and passes it to domain A. The token may be either passed explicitly or implicitly through some kind of parameter enabling domain A to derive the actual token from some shared information with domain B. The OI-CSCF function in domain B also passes the token to the function in domain B which is intended to receive the corresponding INVITE request. So does the outbound proxy in domain A with the proxy sending the INVITE request.

5) **INVITE request processing**: the sending UE, or a proxy acting on behalf of the UE (in domain A or in the visited network), sends the INVITE request with the appropriate token to the network function in domain B designated during the notification phase. When receiving the INVITE request, this function checks that the INVITE request has a valid token and that the INVITE matches the parameters previously notified (especially sender and receiver identities).

### 7.5.4 Detailed principles

We distinguish two sub-cases for the detailed principles:

- There is no shared secret between domain A and domain B (cf. section 7.5.4.1).
- A shared secret is established between domain A and domain B (cf. section 7.5.4.2).

These two sub-cases have some common characteristics:

- Step 1 (authorization phase in the sending domain) should reuse authentication mechanisms already defined in 3GPP (IMS-AKA, NASS-bundled…) or in IETF (HTTP Digest, SRP…). During this phase, the sending UE may be challenged by the outbound proxy in domain A, or by any other entity responsible for authentication in domain A, to provide credentials for the claimed user identity. During this phase, a secure network connection may be established between the sending UE and a proxy in domain A.
- The architecture presented for illustration in the two sub-cases below assumes a second proxy in addition to the outbound proxy. This additional proxy may belong either to domain A or to a visited network. The principles detailed below are the same when this additional proxy is not used.
- Similarly we assume the OI-CSCF function and the P/S-CSCF function in domain B are supported by different entities but the principles detailed below are the same when these functions are merged.
- During the notification phase (step 2), the receiving domain B sends back challenge or parameters to domain A but for security reasons, these network messages are addressed to only the "stable" outbound proxy of domain A. This means that during a preliminary phase, domain A has to announce its outbound proxys to domain B, or domain B has to discover them (for example with DNS service). Once the domain A outbound proxys are discovered by domain B, they are locked in the domain B database as the stable and responsible proxys for domain A. Domain A is not allowed to modify them very often whereas it denotes that domain A may be an attacker domain. As stated previously, domain A needs to announce at least one outbound (stable) proxy. Several outbound proxys may be announced for redundancy reasons, but domain B is free not to register all of them. The other proxys used within domain A or within the visited network do not need to be announced.

### 7.5.4.1 No shared secret between domain A and domain B

The proposed protocol exchange is shown below; Figure 7.5-2:

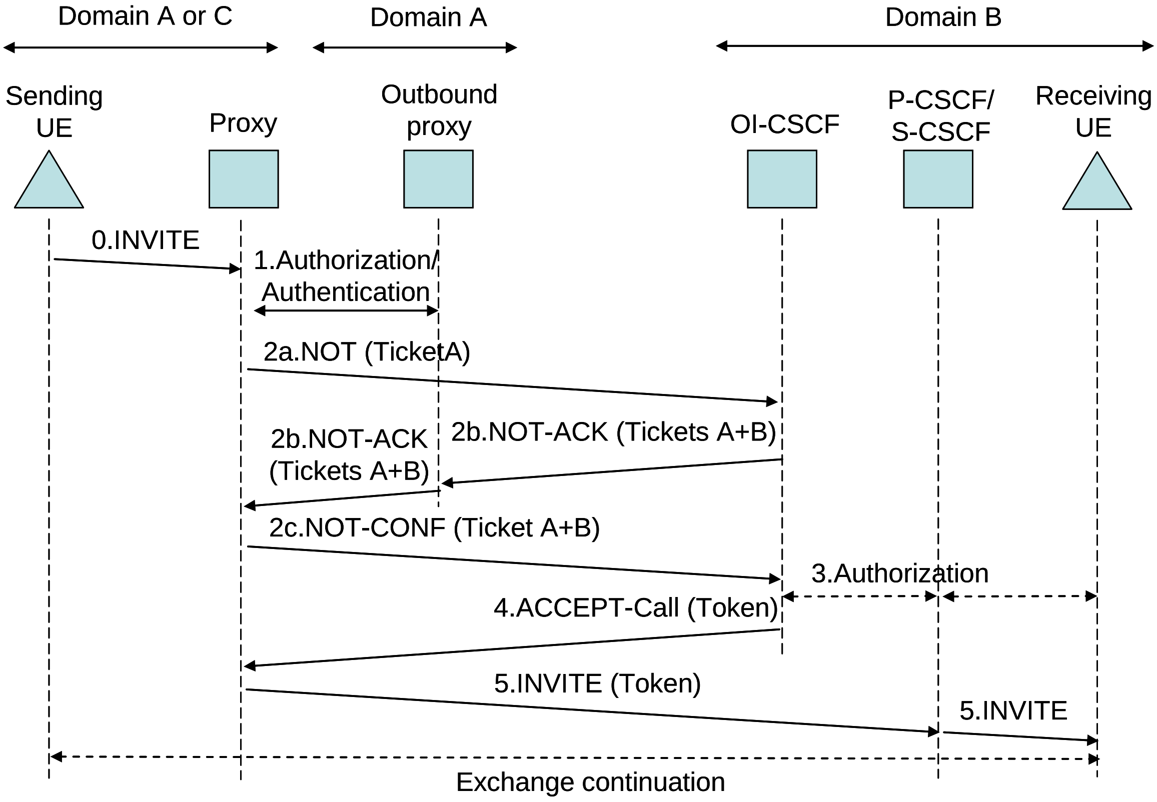


**Figure 7.5-2: Protocol exchange when no shared secret is available between domains**

At the end of step 1 (authorization/authentication phase), the outbound proxy in domain A creates a ticket (Ticket A) which contains basically the following information:

- A ticket identifier (random number) for domain A.
- The sender public identity (SIP URI).
- The receiver/recipient public identity (SIP URI).
- Additive information from the INVITE request.
- A timestamp for replay protection.
- The issuer of the ticket (outbound proxy identity or transport address).
- The transmitter of the ticket. That means the identity or the transport address of the entity in charge of transmitting the ticket and subsequently the INVITE request. Depending on the architecture, the transmitting entity may be the UE itself, the outbound proxy or an (intermediary) proxy in domain A or in the visited network C.
- The identity or the transport address of the target OI-CSCF function.
- A MAC (Message Authentication Code) used for ticket integrity protection. This MAC is calculated with a secret key owned by the outbound proxy.

Because of the MAC code inserted in the ticket, the outbound proxy does not need to keep track of the transaction. This means the transaction is stateless for outbound proxy in domain A.

During the notification phase (step 2), the ticket A is sent by the transmitting entity to the target OI-CSCF function in domain B. Upon reception of the NOT request, the OI-CSCF function performs some basic checks on the sender, receiver, issuer and timestamp fields and returns a NOT-ACK message to the claimed sending domain. The NOT-ACK message is composed of the ticket as received from domain A and of a second part inserted by domain B. The ticket B part contains basically the following information:

- A ticket identifier for domain B.
- A timestamp for replay protection.

- A MAC used for ticket integrity protection. This MAC is calculated over the whole ticket A+B information with a secret key owned by the OI-CSCF function.

Because of the MAC code, the OI-CSCF function does not need to keep track of the transaction (stateless process). Both the ticket A and the ticket B parts are inserted in the NOT-ACK message. This message is sent to the entity identified by the issuer field of ticket A and this entity shall belong to the set of (stable) outbound proxys registered for domain A.

When receiving a NOT-ACK message, the outbound proxy in domain A verifies the ticket A validity by checking the identifier and the MAC fields he has previously inserted. If ticket A is valid, the NOT-ACK message is forwarded to the entity identified by the "transmitter" field of the ticket. Afterwards the outbound proxy is no longer involved in the transaction.

Upon reception of a NOT-ACK message, the transmitting entity checks the identifier field contained in ticket A and if it is valid, the transmitting entity forwards the ticket A+B information to the target OI-CSCF function through a NOT-CONF message. The whole exchange of NOT, NOT-ACK and NOT-CONF messages is similar to the Syn-Cookie mechanism used in SCTP protocol except it is done here in a triangular way.

When receiving a NOT-CONF message, the OI-CSCF function checks the ticket A+B validity by verifiying the identifier and the MAC fields contained in ticket B. If the NOT-CONF message is valid, step 3 (authorization phase in the receiving domain) is entered.

At step 3, the receiving domain checks if the receiver is willing to accept the call. As explained previously, this step should rely on mechanisms already proposed in sections 7.2 and 7.3 such as: white or black list information, user preferences (e.g. no calls allowed after 10pm), sender or sending domain reputation… At the end of step 3, the decision may be to reject the call, direct the call to a mailbox or to a SPIT analysis system or eventually accept the call. If the call is accepted, step 4 (token distribution) is entered.

At step 4, the OI-CSCF function generates a token and sends it both to the S/P-CSCF function in domain B and to the transmitter entity in domain A through an ACCEPT-Call message. The ACCEPT-Call message also includes information related to ticket A+B so it can easily be identified by domain A. At step 5, the INVITE request is sent along with the corresponding token and it is eventually reaches the receiving UE.

### 7.5.4.2 A shared secret is established between domain A and domain B

The proposed protocol exchange is shown below; Figure 7.5-3:

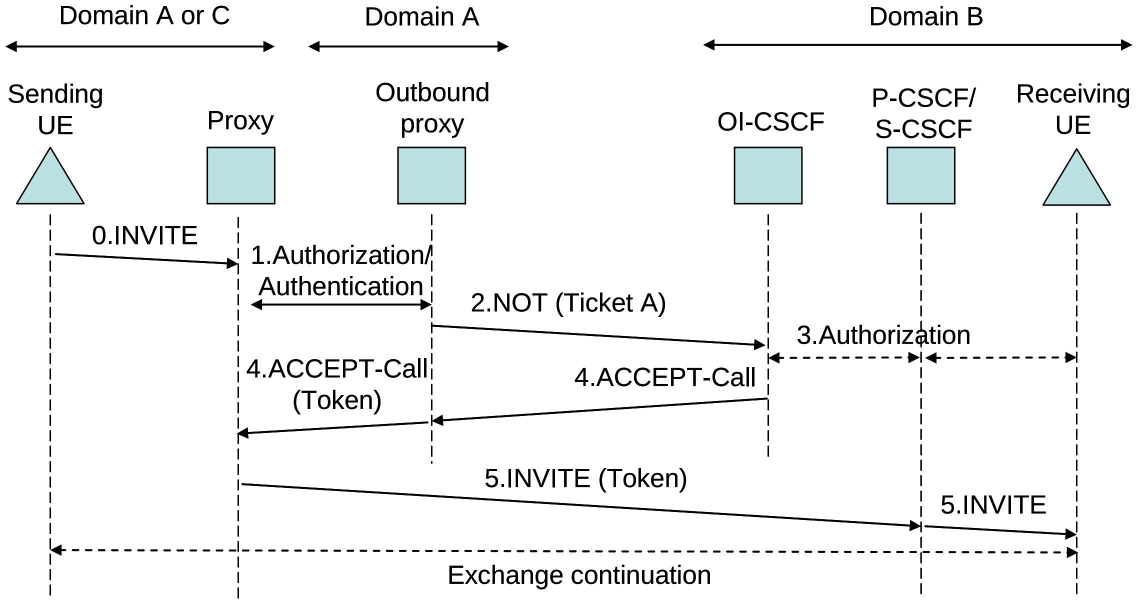


**Figure 7.5-3: Protocol exchange when a shared secret is available between domains**

Step 1 is the same as in the previous case (cf. §0) and results in ticket A creation by the outbound proxy in domain A. The main difference here is that the MAC field in ticket A is calculated with the secret key $K_{AB}$ shared between domain A and domain B.

In step 2 (notification phase), ticket A is sent by domain A to domain B through a NOT request. The NOT request shall be sent by the outbound proxy or optionally by another transmitter entity (proxy or sending UE). When receiving a NOT request, the OI-CSCF function in domain B does not need to go through a NOT-ACK/NOT-CONF check because it has the guaranty that ticket A is asserted by domain A. The behaviour of OI-CSCF in this architecture is close to the one of the KMS function from the TBS approach described in TR33.828 [25].

Step 3 is the same as in the previous case (cf. §0) and if the call is accepted the OI-CSCF function generates a token at step 4 that is transmitted both to the S/P-CSCF function and to the outbound proxy in domain A. This time the ACCEPT-Call message is integrity protected with a MAC code based on $K_{AB}$ secret and the token may be confidentiality protected. Alternatively, the encrypted token value is replaced by a clear parameter which is combined with the secret information shared between domains to compute the actual token.

## 7.6 Alternative Methods for Authentication of Originating Network

### 7.6.1 Introduction

As already discussed in some sections of this TR, IMR-based PUCI prevention in the terminating network has the cardinal disadvantage that it is prone to forged sender identities. Forged sender identities lead to a corruption of the UC database and may even be a source of a new kind of UC reputation attacks.

If using IMR-based PUCI prevention, it is regarded necessary that it can be applied in the terminating network although the originating network is better suited as it is able to authenticate its users. The main reason for terminating UC prevention is that the terminating network can't rely on the UC findings of the originating network (if available at all) if there is no trust in any caller identity transmitted by the originating network, or in the identity of the originating network itself. This may already apply for IMS to IMS interconnections but even more for IMS to non-IMS interconnections.

This disadvantage of terminating IMR-based PUCI prevention can only be solved if at least the originating network can be reliably authenticated. The underlying assumption is not that the originating network itself is malicious but that the originating network may be somewhat careless and only has a weak or even a missing user authentication and is therefore attractive for malicious users. If, however, the originating network itself is regarded as malicious, the only remaining possibility is to completely block traffic from this network.

The optimal solution would be that the terminating network is able to authenticate the originating users, but that may not be realistic in all cases. Alternatively, the terminating network may rely on a caller identity authenticated and transmitted by the originating network. If this is not possible at least the identity of the originating network must be authenticated. Therefore the originating network is responsible for malicious users connected to it and if it can be reliably authenticated, the terminating network is able to take appropriate actions, e.g. based on Service Level Agreement contracts with the originating network.

Unfortunately, today no mechanism exists that reliably authenticates (without forging possibility) the originating network neither on IP level nor on SIP level and that is available for IMS and for non-IMS networks. As a consequence terminating IMR-based PUCI prevention can reasonably only be achieved if such a mechanism is introduced and if non-IMS SIP networks support this mechanism. This means that a clear requirement has to be put for non-IMS networks (outside 3GPP) to support a mechanism enabling reliable authentication of the originating network. As there is no possibility to enforce non-IMS networks to comply with such a requirement, the only alternative is to make the information that a network is non-compliant available to a PUCI application server in the terminating network or to the callee so that they can take this information into account in PUCI identification or prevention, e.g. when computing a PUCI score.

As the acceptance for such a mechanism would be certainly higher if already available identifiers or authentication mechanisms could be reused and enhanced, some of the possibilities shall be discussed subsequently such as

- P-Asserted-Identity
- SIP Identity
- IPSec

### 7.6.2 P-Asserted-Identity

P-Asserted-Identity (according to RFC 3325) describes a private extension to SIP that enables a network of trusted SIP servers to assert the identity of authenticated users. Advantage is that the P-Asserted-Identity is added by the originating network and not by the caller itself. To be effective as a kind of reliable network authentication the originating network has to ensure that the caller has not maliciously added a P-Asserted-Identity header to its SIP messages. Pre-requisite for the use of this extension is that the trusted SIP servers have previously agreed upon policies for generation, transport and usage of such information.

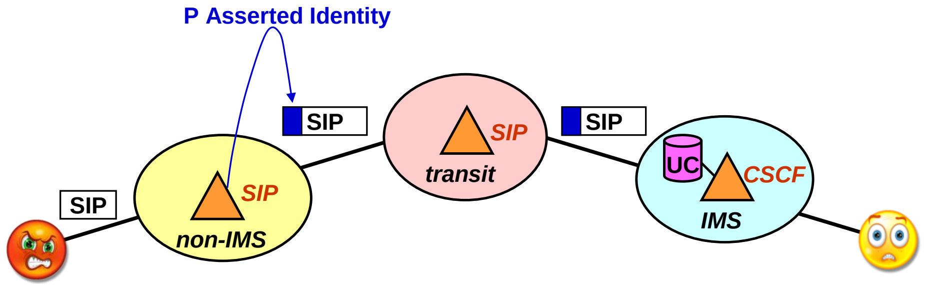


Figure 7.6-1

Although the P-Asserted-Identity header extension is not signed by the originating network (in this example a non-IMS network) and could be forged by the originating as well as by intermediate transit networks, it is regarded unlikely that the originating or the transit networks will cooperate with a SPITter connected to the non-IMS network.

## 7.6.3 SIP Identity

SIP Identity (according to RFC 4474) is similar to the 'P-Asserted-Identity' mechanism. The originating network authenticates the user and adds a signature to the SIP request. This signature provides two significant advantages:

- SIP Identity is protected against manipulation of a malicious user in the originating network
- SIP Identity is protected against manipulation of intermediate transit networks

As only a hash of SIP Identity related information is signed, this mechanism allows changes in other fields of the SIP message by intermediate SIP servers while fulfilling its purpose securely.

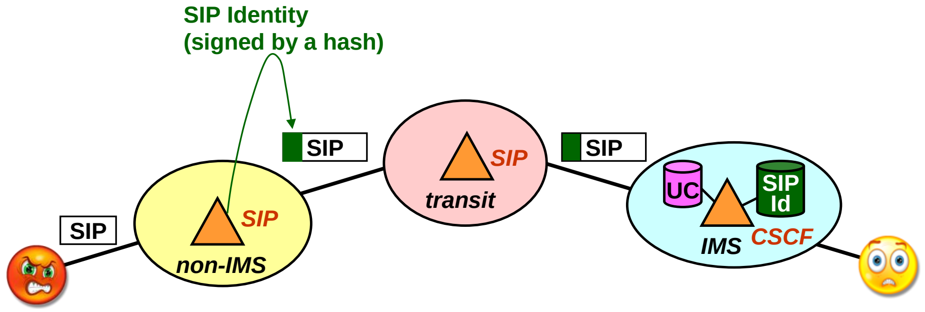


Figure 7.6-2

According to RFC 4474, SIP identity is designed in such a way that the terminating user fetches the certificate, validates it and verifies the signature and the sender's identity. As already explained before, this may not be realistic in many settings as it assumes a Public Key Infrastructure shared among operators and an installation of corresponding root keys on the UEs. This may put to much burden on the user equipment.

A more feasible alternative seems to be that the terminating network provides a SIP Identity Application Server that acts as back-to-back user agent, terminates SIP Identity and afterwards strips off the SIP Identity header parts so that the user equipment is not affected.

## 7.6.4 Trusted Interconnect with IPSec

Two IMS networks can be securely interconnected by means of IPsec VPNs, e.g. by realizing the Za interface according to TS 33.210 between two IBCFs. If it is ensured by policy that originating and terminating IMS network are directly connected via a VPN, an IBCF can be sure of the identity of the originating network. But the IBCF has no means to communicate this identity to a SIP proxy further inside the IMS network. There may be some scope for further study here. The source IP address of an IP packet containing a SIP message could be an indicator of the source network only if the source network performed some sort of reverse IP address filtering, i.e. the source network ensured that only packets with topologically correct source IP addresses leave the domain. This property cannot be generally assumed, however.

In general, originating and terminating IMS network will not be directly connected via a VPN, but there will be transit networks where SIP messages may be even modified. Then there is, at best, a chain of trusted networks, and the links between them are protected by IPsec. The terminating IBCF, when implementing a Za interface, can then still know that a SIP message was forwarded by a trusted transit network, but may not have any information about the originating network, at least not without further assumptions about agreements among network operators.

## 7.6.5 Trusted Interconnect with IPSec combined with P-Asserted-Identity

If originating and terminating network are directly connected without intermediate transit networks it is also possible to combine P-Asserted-Identity with IPSec.

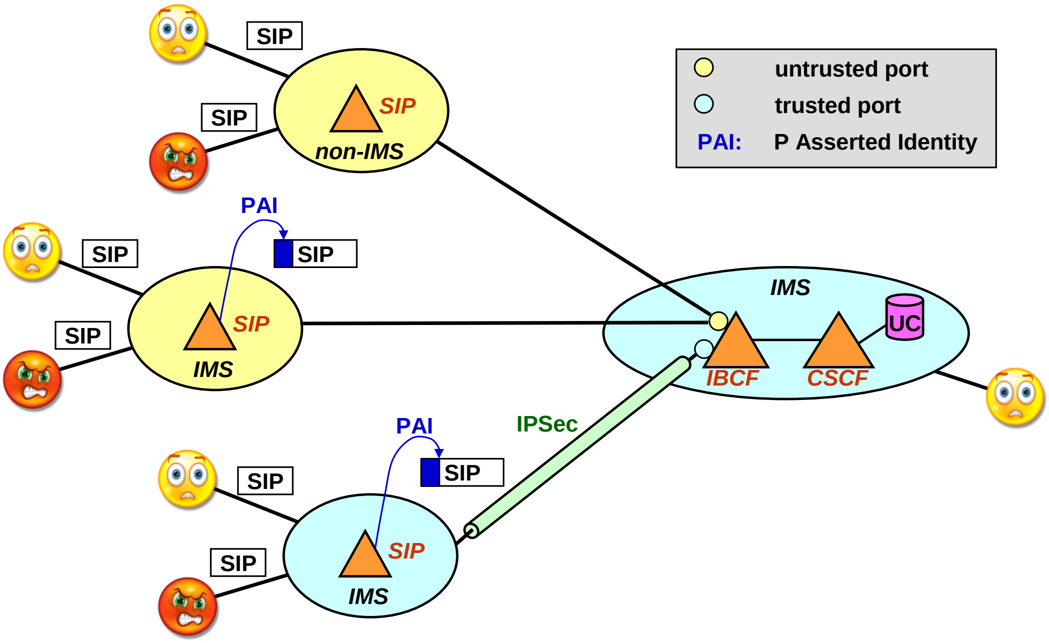


Figure 7.6-3

For the ‘IPSec combined with P Asserted Identity’ method the directly interconnected networks are classified in trusted and untrusted networks. Trusted networks are connected to a “trusted” network interface or port of the IBCF (i.e. a network interface or port to which all trusted networks are connected) in the terminating IMS network while untrusted networks are connected to the “untrusted” port of the IBCF.

When the SIP request is received over a trusted port the IBCF leaves the P-Asserted-Identity header in the SIP request unchanged.

When the SIP request is received over an untrusted port the IBCF strips off the P-Asserted-Identity header.

A SIP request with a P-Asserted-Identity header indicates to the receiving CSCF in the terminating IMS network that asserted identity can be trusted. A missing P-Asserted-Identity header in the SIP request indicates that the SIP request comes either from an untrusted network or from a trusted network that does not use P-Asserted-Identity headers. In both cases the originating networks are regarded as not authenticated.

## 7.6.6 Summary

This subsection underlines the indispensible necessity to authenticate the originating network when using IMR-based UC prevention in terminating networks. It illustrates that currently no directly applicable solution exists. But it shows as well that with adaptations of already existing methods it could be possible to significantly improve the situation without introducing completely new protocols. The list of mechanisms discussed here is not claimed to be exhaustive. This would increase the probability to apply these methods in IMS and even more in non-IMS SIP networks. If non-IMS networks deny the usage of any of such methods it remains only to either block their traffic or to take this information into account in PUCI identification or prevention algorithms.

Therefore it is proposed to further thoroughly analyze this topic and develop recommendations.

# 8 Evaluation of Solution Alternatives

## 8.1 Evaluation Criteria

Criteria that can be used to evaluate solutions are given below. These criteria are grouped into three different categories, each category carrying a defined weight. The weight is ranging from 'Essential' over 'Important' to 'Others'. A definition of the categories and *a reason why a certain evaluation criteria is allocated to a specific category (for the categories 'essential' and 'important')* is given within this clause.

**Category: Essential**

This category contains evaluation criteria that **must** be fulfilled to provide at all a basic and reliable UC protection functionality. Without these criteria a proper functionality of UC prevention is not possible.

1. Resilience against forged information on the UC originating source and UC source versatility: how well does the solution protect against UC in an IMS network if the UC source forges originating identity information or if the UC source changes dynamically with a high frequency?

   *This criterion is essential because a reliable identification of the UC source is basis of all UC prevention techniques. Without resilience against forged information on the UC originating source and UC source versatility not only the functionality of UC prevention is impaired but even new threats like UC reputation attacks would be introduced*

2. Security: How well does the solution address the following threat 'Privacy Violation – Bulk UC (Advertising) (see 5.2.3.1.1)'

   *This is the outstanding threat that has first and foremost to be mitigated. Regarding overall UC prevention standardization and legislation this is common denominator.*

**Category: Important**

This category addresses evaluation criteria that are either important for further UC protection functionality to mitigate against other threats than 'resilience against bulk communication' or that have a significant influence on the technical or user environment

3. Security: How well does the solution address the following requirement 3GR-UC-1 'The IMS should provide a means for IMS-users to report communication as a UC (see 6.2)' ?

   *As perception of UC is largely user-specific and the UC prevention techniques of the network depend on user feedback, it is important to provide a means for the user to express his UC rating of a specific communication or a specific communication source.*

4. Security: How well does the solution address the following requirement 3GR-UC-7 'The IMS should provide a mechanism to allow variation in communication handling based on UC likelihood indication (see 6.2)' ?

   *This requirement is important for the IMS network to provide a UC protection functionality for the user by e.g. blocking, re-directing or forwarding a communication with a specific UC rating or from a specific UC source, supposed that the user has given explicit consent to the UC protection.*

5. Impact on existing standard: This criterion is meant to check whether any of the existing standards are impacted by a given solution. The preference of course is to have a solution that does not require changes in existing (pre-Rel-9) standards.

   *Changes in existing (pre-Rel-9) standards could have influence on the already installed IMS equipment base and on inter-working with other networks.*

6. Security: How well does the solution address the following requirement 3GR-UC-9 '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' ?

*It is important that a solution is able to support mixed legacy/NGN environments to be effective (given that these will remain a reality at least for a transition period from legacy to NGN and perhaps even for a long time to come). It is also important to support an interworking between IMS and features/services of legacy networks, connected to IMS.*

7. Security: How well does the solution address the following threats presented in section 5 ?
a. Privacy Violation - Targeted UC (see 5.2.3.1.2)
b. Contentious Incoming Call Service Charge (see 5.2.4)

c. Contentious Roaming Cost (see 5.2.5)

d. Non-disclosure of Call Back Cost (see 5.2.6)

e. Phishing (see 5.2.7)

f. Network Equipment Hijacking (see 5.2.8)

g. User Equipment Hijacking (see 5.2.9)

h. Mobile Phone Virus (see 5.2.10)

i. Unavailability of Service or Degraded Service Quality (see 5.2.12)

*It is important that a solution provides also as efficiently as possible protection against all other kind of UC threats analyzed in chapter 5 (besides the two criteria 'resilience against forging …' and 'Privacy Violation - Bulk UC' that were rated as essential, see 1. and 2.)*

8. Simplicity: A solution should not be complex in itself, i.e. difficult to understand, relying on complex security mechanism or otherwise like usage or implementation. Thus a simple solution is preferred.

*This evaluation criterion is in so far important as it prefers in case of multiple alternatives simple solutions, supposed that the effect concerning UC protection is comparable.*

9. Unintrusive to legitimate users: Annoying a caller can be as bad, or perhaps worse, as a user receiving an unsolicited call.

*It is important to select UC prevention techniques in a way that intrusiveness of legitimate users is a small as possible. That is necessary to achieve acceptance of users that in a large majority are up to now customized to normal phone calls without UC. However the intrusiveness of UC prevention techniques has to be balanced against the intrusiveness of UC occurrence. As a consequence this means as well that a higher grade of UC protection intrusiveness may be accepted if the overall intrusiveness of UC occurrence increases significantly. This evaluation criterion is also important as it prefers the most unintrusive solution between multiple alternatives, supposed that the protection is comparable.*

10. Operating expense (OPEX): Expense caused when using the solution (including e.g. service call costs)

*This criterion is certainly an important generic criterion. However, it may be difficult to evaluate. If no clear evidence is available its weight should be re-considered.*

11. Capital expenditures (CAPEX): Expense caused when implementing the solution

*This criterion is certainly an important generic criterion. However, it may be difficult to evaluate. If no clear evidence is available its weight should be re-considered.*

12. Modular: This checks whether new addition can be brought in place without any issues with the solution

*This criterion is certainly an important generic criterion as it prefers in case of multiple alternatives modular solutions, supposed that the effect concerning UC protection is comparable. However, it may be difficult to evaluate. If no clear evidence is available its weight should be re-considered.*

13. Scalable: The solution should be scalable in terms of volume of attack it can cater for and number of users that can use it. The solution should also be scalable in terms of network size .

*This criterion is certainly an important generic criterion as it prefers in case of multiple alternatives scalable solutions, supposed that the effect concerning UC protection is comparable. However, it may be difficult to evaluate. If no clear evidence is available its weight should be re-considered.*

*14.* Latency: Does the approach significantly add to the latency between the initiation and completion of desired communications?

*This criterion is important as large latency is annoying to users. Therefore solutions adding significantly to latency should be avoided.*

*15.* Network Load: Does the approach negatively impact the performance of network components?

*This criterion is important as a significant impact on the performance of network elements addresses either the need to upgrade existing networks when introducing UC prevention or to accept a performance degradation.*

16. Sensitivity and specificity (false acceptance / false rejection): Examples
    a. Unwanted Calls Allowed: Does the solution detect and block UCs?
    b. Unwanted Calls Criteria Adjustable to User's Requirements: Does the method allow the user to adjust the Unwanted Calls criteria to match their desires?
    c. Desired Calls Blocked: Does the solution avoid blocking desirable calls?
    d. Desired Calls Criteria Adjustable to User's Requirements: Does the method allow the user to adjust the Desired Calls criteria to match their desires?

*This criterion refers to the quality and efficiency of a potential UC protection solution and is important as such. But It may be difficult to evaluate with reference to specific implementations.*

**Category: Others**

This category addresses evaluation criteria that have as well a significant influence on the acceptance of UC prevention techniques, either from an operator or a user point of view, or that provide enhanced UC prevention features. But they may not be as generally applicable as the criteria listed as essential or important.

17. Security: How well does the solution address the requirement 3GR-UC-5 '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' ?

*This criterion is rather a requirement on a particular solution how to fulfil other, more generic, PUCI requirements. There may be other ways to achieve the desired goal*

18. Security: How well does the solution address the requirement 3GR-UC-6 'The IMS should provide a mechanism to convey the UC indication in the signalling' ?

*This criterion is rather a requirement on a particular solution how to fulfil other, more generic, PUCI requirements. There may be other ways to achieve the desired goal.*

*19.* Security: How well does the solution address the requirement 3GR-UC-2 'Reports of UC relating to IMS-users should be auditable by the IMS' ?

*It is not clear whether fulfilment of this criterion will be part of any potential UC protection solution or whether the operator will provide auditable reports in another way. Therefore an evaluation of this criterion could lead to the rating 'not applicable'.*

20. Security: How well does the solution address the requirement 3GR-UC-3 'The IMS should provide the ability for a user who is party to a communication to request whether a communication was rated as UC' ?

*It is not clear whether fulfilment of this criterion will be part of any potential UC protection solution or whether the operator will provide UC ratings to users in another way. Therefore an evaluation of this criterion could lead to the rating 'not applicable'.*

*21.* Security: How well does the solution address the requirement 3GR-UC-4 'The IMS should provide the ability for an affected user to challenge the justification why the communication was identified as UC' ?

*It is not clear whether fulfilment of this criterion will be part of any potential UC protection solution or how the operator will provide possibilities for users to challenge the justification why the communication was identified as UC. Therefore an evaluation of this criterion could lead to the rating 'not applicable'.*

22. Security: How well does the solution address the requirement 3GR-UC-8 'Requests for UC protection made by IMS users should be auditable by the IMS' ?

    *It is not clear whether fulfilment of this criterion will be part of any potential UC protection solution or whether the operator will provide auditable reports about user requests for UC protection in another way. Therefore an evaluation of this criterion could lead to the rating 'not applicable'.*

23. Security: How well does the solution address the threat 'Negative Service Preconception Leading to Non-adoption (see 5.2.13)' ?

    *As already stated in clause 5.2.13 this threat is only highlighted for completeness and does not imply any further technical requirements. Therefore an evaluation of this criterion will presumably lead to the rating 'not applicable'.*

24. Service agnostic: Whether a solution can work as is for all kind of IMS based services or a variation is needed for each service.

    *The most important service in this context is voice. If a solution for this particular service can be found it is valuable in itself. Nevertheless, it is clearly desirable if a service-agnostic solution can be found.*

## 8.2 Evaluation of Alternatives

This clause evaluates the alternatives solutions and mechanisms for SPIT/UC protection, described in chapter 7

- chapter 7.3 'SPIT/UC Protection with Supplementary Services' (abbreviated: SS)
- chapter 7.4 'Contextual Information' (abbreviated: CI), used as extension to Supplementary Services
- chapter 7.5 'UC protection framework for non-IMS interconnection: the Open Proxy Handshake' (abbreviated: UC-OPH)

according to the criteria, established in chapter 8.1.

Chapter 7.2 'IMR Based Solution Approach' is not compared because IMR makes use of SS and other modules, like those in RFC 5039 [11], and thus could be evaluated to be similar to SS.

The chosen ratings are

- 'positive (+)', if a solution alternative meets the criterion completely or to a large degree
- 'medium (o)', if a solution meets the criterion only partly
- 'negative (-)', if a solution doesn't meet the criterion or only to a negligible degree
- 'not applicable (n.a.)', if a criterion can not be influenced by a technical solution or if the solution is explicitly not related to this criterion

Positive means that the effect of a solution alternative concerning SPIT/UC protection is positive (+), regardless how the criterion is formulated.

Example: Criterion 14 'Latency'

*Does the approach significantly add to the latency between the initiation and completion of desired communications?*

The rating 'positive (+)' for this criterion means that the approach doesn't significantly add to latency.

**Table 1 Evaluation of Solution Alternatives:**

| Evaluation Criteria | | SS, all with feedback by keypad entries (7.3.3.6) | | | | | | UC-OPH |
|---|---|---|---|---|---|---|---|---|
| | | BL | WL+<br>CMB | BL+WL +CMB | SUPP | WL+IN Server | CI | |
| | | 7.3.3.1 | 7.3.3.2 | 7.3.3.3 | 7.3.3.4 | 7.3.3.5 | 7.4 | 7.5 |
| | **Category: Essential** | | | | | | | |
| 1 | Resilience against forged sender information | - | + | + | + | + | + | + |
| 2 | How well is threat 'bulk UC (Advertising)' addressed | + | + | + | + | + | + | **n.a.** |
| | **Category: Important** | | | | | | | |
| 3 | Means to report communication as UC | + | + | + | + | + | + | **n.a.** |
| 4 | Variation in communication handling based on UC likelihood | o | o | o | o | o | + | **n.a.** |
| 5 | Impact on existing standard | + | + | + | + | + | o | - |
| 6 | Interworking with legacy networks and devices | + | + | + | + | + | - | **n.a.** |
| 7 | How well does the solution address the following threats | | | | | | | |
| 7a | Privacy Violation – Targeted UC | + | + | + | + | + | + | **n.a.** |
| 7b | Contentious Incoming Call Service Charge | - | o | o | o | o | o | **n.a.** |
| 7c | Contentious Roaming Cost | - | o | o | o | o | o | **n.a.** |
| 7d | Non-disclosure of Call Back Cost | - | o | o | o | o | o | **n.a.** |
| 7e | Phishing | - | o | o | o | o | - | **n.a.** |
| 7f | Network Equipment Hijacking | - | - | - | - | - | - | **n.a.** |
| 7g | User Equipment Hijacking | - | o | o | o | o | - | **n.a.** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 7h | Mobile Phone Virus | - | - | - | - | - | - | n.a. |
| 7i | Unavailability / Degraded Service | - | - | - | - | - | o | n.a. |
| 8 | Simplicity | + | + | + | + | + | o | n.a. |
| 9 | Unintrusiveness | + | - | - | - | o | + | n.a. |
| 10 | OPEX | + | + | + | + | + | o | n.a. |
| 11 | CAPEX | + | + | + | + | + | + | n.a. |
| 12 | Modular | o | o | o | o | o | + | n.a. |
| 13 | Scalable | + | + | + | + | + | + | n.a. |
| 14 | Latency | + | + | + | + | + | o | n.a. |
| 15 | Network Load | + | + | + | + | + | o | n.a. |
| 16 | Sensitivity and specificity | o | o | o | o | o | o | n.a. |
| | **Category: Others** | | | | | | | |
| 17 | Information extraction from signaling / UC likelihood indication | - | - | - | - | - | o | n.a. |
| 18 | Mechanism to convey UC indication in signaling | - | - | - | - | - | + | n.a. |
| 19 | UC reports auditable by the IMS | o | o | o | o | o | - | n.a. |
| 20 | Request UC Status | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. |
| 21 | Challenge UC justification | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. |
| 22 | User UC protection requests auditable | o | o | o | o | o | - | n.a. |
| 23 | Negative Service Preconception | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. |
| 24 | Service agnostic | o | o | o | o | o | + | n.a. |

Abbreviations:

| | |
|---|---|
| SS | Supplementary Services |
| BL | Black List |
| WL+CMB | White List + Consent Mailbox |
| BL+WL+CMB | Black List + White List + Consent Mailbox |
| SUPP | Sophisticated UC Prevention Profile |
| WL + IN | White List + Intelligent Network server |
| CI | Contextual Information (intention: combine with Supplementary Services) |
| UC-OPH | UC protection – Open Proxy Handshake (focuses solely on authentication of sender identity) |

Rationale

This section gives a short rationale (if necessary) for the evaluation results of a specific criterion:

**Criterion 1: Resilience against forged sender information**

- SS: only white lists offer an acceptable protection against forged sender information
- SS (CI): provides fields (identity strength, origin network) which may be used e.g. in combination with UC-OPH
- UC-OPH: Provides a detailed proposal for verification of sender identity (and is only related to this criterion)

**Criterion 2: How well is threat 'bulk UC (Advertising)' addressed**

- all solution alternatives address bulk UC threat

**Criterion 3: Means to report communication as UC**

- SS (CI) itself doesn't provide feedback possibilities but is combined with SS

**Criterion 4: Variation in communication handling based on UC likelihood**

- SS provide also variation in communication handling (but based on likelihood 1 because SPIT/UC sources are unambiguously identified by entering them in a blacklist or not entering them in a whitelist)
- If SS is used in combination with SS (CI) it provides as well a variation in communication handling based on UC likelihood

**Criterion 5: Impact on existing standard**

- SS: no impact on existing standards
- SS (CI): enhancements of existing SS standards needed
- UC-OPH: require new standardization

**Criterion 6: Interworking with legacy networks and devices**

- only SS are suited to work in legacy as well as in NGN networks

**Criterion 7a: Privacy Violation – Targeted UC**

- Mechanisms of SS do not differentiate between bulk and targeted UC: therefore SS protect against bulk as well as against targeted UC once the SPIT/UC source is identified
- SS provide additional capabilities (MCID) to identify malicious source of targeted UC
- SS (CI): provides itself no means against targeted UC but is combined with SS

**Criterion 7b: Contentious Incoming Call Service Charge**

- SS (BL): no effect (only if the malicious source is already known and if the sender identity is not forged)
- SS (WL-based solutions): Although not specifically designed for protection of 'Contentious Incoming Call Service Charge', whitelists block untrusted sources and therefore provide a certain protection
- SS (CI): provides additional information (cost indicator) and is therefore well suited to enhance protection of SS against this threat

**Criterion 7c: Contentious Roaming Cost**

- SS (BL): no effect (only if the malicious source is already known and if the sender identity is not forged)

- SS (WL-based solutions): Although not specifically designed for protection of 'Contentious Roaming Cost', whitelists block untrusted sources and therefore provide a certain protection
- SS (CI): provides additional information (cost indicator; although roaming cost indication up to now not specified) and is therefore well suited to enhance protection of SS against this threat

**Criterion 7d: Non-disclosure of Call Back Cost**

- SS (BL): no effect (only if the malicious source is already known and if the sender identity is not forged)
- SS (WL-based solutions): Although not specifically designed for protection of 'Non-disclosure of Call Back Cost', whitelists block untrusted sources and therefore provide a certain protection
- SS (CI): provides additional information (cost indicator; although callback cost indication up to now not specified) and is therefore well suited to enhance protection of SS against this threat

**Criterion 7e: Phishing**

- SS (BL): no effect (only if the malicious source is already known and if the sender identity is not forged)
- SS (WL-based solutions): Although not specifically designed for protection against 'Phishing', whitelists block untrusted sources and therefore provide a certain protection
- Ss (CL): no mechanism described

**Criterion 7f: Network Equipment Hijacking**

- none of the solution alternatives describes mechanisms against Network Equipment Hijacking

**Criterion 7g: User Equipment Hijacking**

- SS (BL): no effect (only if the malicious source is already known and if the sender identity is not forged)
- SS (WL-based solutions): Although not specifically designed for protection against 'User Equipment Hijacking', whitelists block untrusted sources and therefore provide a certain protection
- SS (CL): no mechanisms described

**Criterion 7h: Mobile Phone Virus**

- none of the solution alternatives describes mechanisms against Mobile Phone Virus
- SS (WL-based solutions): Although whitelists block untrusted sources, they are not really suited against Mobile Phone Virus because trusted sources can as well contribute to distribution of Mobile Phone Virus

**Criterion 7i: Unavailability / Degraded Service**

- SS: are reactive measures at the callee side that are not suited to protect the network against Unavailability / Degraded Services
- SS (CI). With fields identity strength, call complaint fraction, messaging complaint fraction SS (CI) is to a certain degree suited to protect the network against Unavailability / Degraded Services and can therefore enhance the protection of SS
- but be aware: there might be legal issues to delete SPIT/UC suspicious traffic without explicit consent of the callee

**Criterion 8: Simplicity**

- SS: simplest solution, already available
- SS (CI): one degree more complex, transmission of reputation indicators required, evaluation and storage (databases) of reputation indicators required

**Criterion 9: Unintrusiveness**

- Unintrusiveness is difficult to evaluate, as it depends on individual perception, therefore solution alternatives are evaluated in relation to each other
- SS (BL), SS (CI) are unintrusive for the caller
- SS (WL-based approaches, except WL+IN Server) are more intrusive because they require consent achievement with the callee
- SS (WL+IN Server) may be medium intrusive as the whitelist-bypassing prefix may be publicly known

**Criterion 10: OPEX**

- SS: solution with lowest OPEX, SS already available, no installation and operation of new equipment necessary
- SS (CI): enhancement of SS equipment necessary

**Criterion 11: CAPEX**

- SS: solution with lowest CAPEX, SS already available, only extension of equipment may be necessary

**Criterion 12: Modular**

- SS (CI): can easily be enhanced by new modules
- SS: quite established, therefore enhancement by new modules more difficult

**Criterion 13: Scalable**

- Generally all solution alternatives are scalable

**Criterion 14: Latency**

- SS: low → requires table look-up and performing of pre-defined action
- SS (CI): higher → requires processing and evaluating of signaling information and user behavior, querying and actualizing of UC related databases and synchronizing of potentially differing UC scores in a distributed architecture

**Criterion 15: Network Load**

- SS: low → requires table look-up and performing of pre-defined action
- SS (CI): higher → requires processing and evaluating of signaling information and user behavior, querying and actualizing of UC related databases and synchronizing of potentially differing UC scores in a distributed architecture

**Criterion 16: Sensitivity and specificity**

- SS: Sensitivity and specificity (false acceptance, false rejection) are not issues for WL. For BL,SPIT/UC protection of SS depends on unambiguously identified UC sources and, hence, the possibility of erroneous actions exists.
- SS (CI): Sensitivity and specificity (false acceptance, false rejection) are issues because scores are evaluated that provide a certain SPIT/UC probability, which may lead to erroneous results.

**Criterion 17: Information extraction from signaling / UC likelihood indication**

- SS: not available, only in combination with SS (CI)
- SS (CI): provides such data to a certain degree

**Criterion 18: Mechanism to convey UC indication in signaling**

- It is difficult whether conveying of UC indication in signaling is regarded positive or negative → according to the criterion the possibility is valuated positive
- SS: not available, only in combination with SS (CI)
- SS (CI): possibility is provided

**Criterion 19: UC reports auditable by the IMS**

- SS (including CI): reports by the user on UC take the form of key presses or web-based feedback. These reports are not part of this PUCI mechanism, but can be audited in their own right.

**Criterion 22: User UC protection requests auditable**

- SS (CI): no support of User UC protection requests, but combined with SS
- SS: User UC protection requests result in blacklist/whitelist entries, therefore a simple form of auditing is possible

**Criterion 24: Service agnostic**

- It is difficult whether it is regarded positive or negative if a solution alternative is service agnostic. It can be seen positive if a solution provides sufficient UC protection without being service agnostic, because then it is general and simple, On the other hand solutions could be more tailored to services if the solution is service agnostic. → therefore a solution alternative is valuated better if it implies in principle the possibility to be service agnostic
- SS: not service agnostic, only in combination with SS (CI); blocks or enables sources regardless of the used service
- SS (CI): generally not service agnostic, but imply the possibility to be service agnostic as they evaluate signaling traffic

## 8.3 Usage Space

Section 8.2 "Evaluation of Alternatives" gives a high level comparison of PUCI solutions presented in this TR. Besides a comparison of solutions it is also important to understand what can be used when i.e. the usage space of a given solution. In this section we present the usage space of all the solutions.

Supplementary services, according to Section 7.3, provide means to identify a UC and react on it. For identification purpose the user or operator has to do prior setting. The prior setting is in terms of order in which SS modules are used, done potentially on operator requirements, and the setting done by the user, e.g., white list or black list. Contextual information, according to Section 7.4, provides means that can be used together with SS to identify a potential UC when the communication is taking place for the first time between two parties. Thus SS together with CI can be used for initial deployment of IMS with list based solution where the list (white or black) of a user can be populated by using CI or by the user using the keypad. SS already exists and therefore does not have much impact on standardization. Issue of course is that SS even with CI does not cater for new types of attacks or attacks from parties that are already accepted in a given white list. Thus the gap that remains in SS after combining with CI are:

- There is not necessarily intelligence in the network to automatically identify potential UC and warn the user, respectively to act proactively for the user.
- Static setting of different lists (black, white etc.) cannot take a change in the attack or attacker behaviour into account but means could be found to make it dynamic
- The static order of tests cannot be dynamically changed based on the source or type of communication request.

Editor's note: More text is needed to explain why the above bullet is a gap.

- With current standard new modules cannot be added but standardization could be done to develop and add new modules

IMR provisions for identifying, marking and reacting against UC based on operator policies and user requirements. As such IMR does not define modules to identify UC but instead makes use of SS and other forms of modules [IETF RFC]. Thus IMR in essence works together with SS. IMR can use the marking to react and also re-route received call request for further tests. With possibility to use new modules and perform test depending on incoming call, IMR provides means for handling new attacks and also to react against misbehaviour of identities that are in, say, a white list. Therefore IMR together with SS, CI and other modules [IETF RFC] can take care of the gap left by SS and CI based solution as discussed above.

UC-OPH provides methods for secure communication between networks especially IMS and non-IMS networks. Besides that UC-OPH is dependent on other solutions. Therefore it should be used either with SS or IMR.

# 9 Potential PUCI Architecture

## 9.1 High-level architecture, mapping PUCI functionality to the IMS architecture

In this section we outline a high-level PUCI architecture to describe how PUCI functionality can be mapped to the IMS architecture. This high-level architecture is illustrated in Figure 9.1-1.The figure shows two cases where PUCI Functionality (PUCIF) is implemented in an AS. On the right as a separate AS, using the ISC interface; or on the left as part of the AS providing Supplementary Services (SS). A third option, also indicated on the right with the dotted box is to realize the PUCIF in a CSCF, and it is to be understood that it is left open whether the PUCI functionality is realized in an AS or in a CSCF.

Also shown in the figure is content inspection functionality, similar to current email Spam content inspection. To enable detection of UC in IMS messaging services based on content, it is primarily of interest to inspect the signalling traffic for SIP Message-carried content. In cases of a pre-established messaging session, before content is exchanged, there is little benefit from media plane content inspection to prevent UC, as the callee has already been prompted to accept the session. Hence, this case should be handled analogously to voice sessions. For protection against malware threats carried in UC it is useful to have content inspection also on the media plane. However, this is a more general security threat, and not directly in the scope of protection against UC.

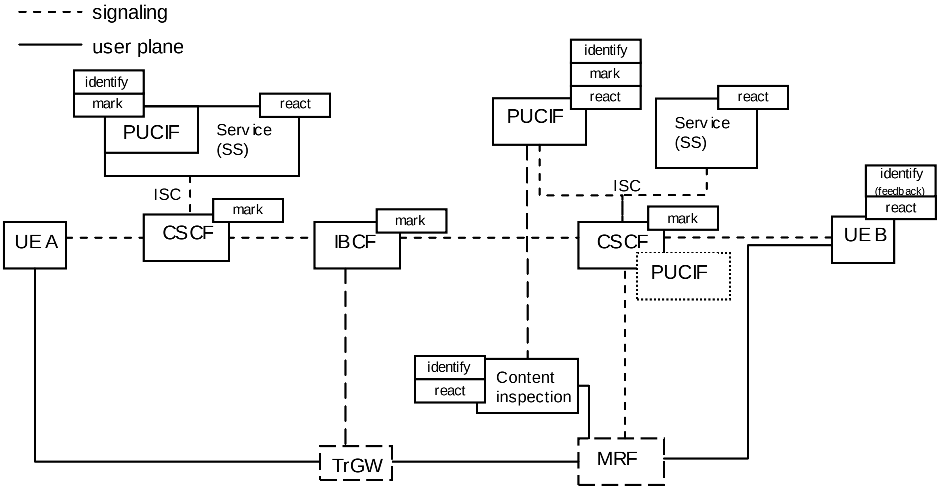


**Figure 9.1-1: Mapping of PUCI functionality to IMS architecture.**

Further explanation and motivation of Figure 9.1-1 is provided in the following subsections.

## 9.2 Centralized/Distributed PUCI AS

According to the discussion in chapter 4.1.3 there are three main approaches:

- a completely distributed approach (see figure 4.1.3) with UC identification and marking/scoring in all kinds of networks (access, IMS, transit);
- a still distributed approach, but centralized per operator (see figure 4.1.4) with UC identification and marking/scoring only in the originating and terminating IMS network, or only in one of therse;
- an approach with distributed UC identification and central UC marking/scoring (see figure 4.1.5) where the central UC marking/scoring is above the operator level and is operated by a neutral organization.

From these the ‘centralized per operator’ approach is favored for IMR-based UC prevention in IMS. The reasons for this recommendation are:

- The completely distributed approach doesn’t fit because access networks that are not SIP-aware cannot contribute to UC marking/scoring. Furthermore the completely distributed approach increases the number of PUCI AS (high cost), complicates the determination of a consistent UC score and increases potentially the complexity of signaling-based UC marking/scoring transport. Transit networks will be SIP-aware but as they neither host the caller nor the callee, they have no specific advantage compared to the originating/terminating network and should therefore not contribute to UC scoring/marking.

- Although a distributed UC identification with a central UC marking/scoring (above operator level) guarantees a consistent UC marking/score (as only one marking/score is delivered) there may be legal concerns associated with this approach. Further disadvantages are an increased traffic volume to transfer UC identification information to and UC marking/scoring from the central UC database and it may be difficult to find a neutral organization to operate the central UC database.

Therefore the ‘centralized per operator approach’ is the best trade-off between the completely distributed and the centralized approach. It is still distributed as the originating and the terminating network may be involved in UC handling, but the maximum amount of UC markings/scores is limited to two. Further advantages are that the originating and the terminating network are SIP-aware and that they host both participants of a communication, the caller and the callee.

## 9.3 UC identification / UC prevention

UC identification denotes the possibility that a PUCI AS identifies UC, e.g. based on user feedback and signaling analysis, but doesn’t deliver a marking/score to the callee. The results of the PUCI AS remain in the network of the operator, or may be delivered from the operator of the terminating network to that of the originating network.

UC identification may then be used for UC prevention by taking steps against malicious users in the operator’s own network or against other operators that offend against Service Level Agreements, cf. clause 4.2.

UC prevention may go even one step further and delivers the UC findings in form of a marking/score to the callee in order to enable a reaction of either the callee himself or his home network, based on the UC probability.

Based on the discussion in this TR (see among others chapter 4.3 ‘Technical versus Legal Issues’, chapter 5.2.11 ‘Sender Impersonation UC’ and chapter 5.3 ‘Specific UC threats in non-IMS interconnection’) it is currently impossible to give a final recommendation to one of the two possibilities. Therefore it seems reasonable to allow both solutions and leave the decision to the operators, who will anyway be responsible to decide between the two possibilities.

## 9.4 Originating/Terminating UC identification and prevention

Another important issue in this TR is whether UC identification and prevention will be done in the originating or in the terminating network. For this issue it is important to differentiate between UC identification and UC prevention:

<u>UC identification</u>

- Technical UC identification by means of an IMR-based PUCI AS
  For technical UC identification the originating network can extract advantages from the fact that it is able to authenticate its users, to take measures against forged sender identities and to detect anomalous traffic streams or communication sources. As a consequence the originating network is best suited for technical UC detection and is therefore clearly recommended.

  Unfortunately the terminating network can’t rely on the findings of the originating network if there is no trust relationship between the two networks. This is a pro to perform technical UC identification also in the terminating network. But a cardinal disadvantage of the terminating network is that it is prone to forged sender identities. This leads to corruption of the UC database and can lead in addition to a new kind of UC reputation attacks.

  Nevertheless it is recommended to support technical UC identification in the terminating network as well, **but with the indispensible requirement that at least the originating network can be reliably authenticated**. The underlying assumption is that the originating network is responsible for malicious users connected to it.

This enables the terminating network to take measures based on Service Level Agreement contracts with the originating network. The optimal solution would be that the terminating network could reliably authenticate the callers in the originating network, but that is currently not realistic and would put too much burden to the user equipment. Without reliable authentication of the originating network technical UC identification in the terminating network by an IMR-based PUCI AS makes no sense.

- Human UC identification
  In contrast to technical UC identification human UC identification by the callee happens always in the terminating network. It is completely unerring as the caller is the only instance who can safely identify UC. This caller based UC identification in form of a UC feedback can as well be used as one input to IMR-based PUCI AS.

  In contrast to IMR-based PUCI AS UC prevention by Supplementary Services is primarily based on human UC identification in the terminating network with the advantages described above. The caller perceiving a specific communication source as UC then takes measures to react on it, e.g. by blocking. These defensive measures may be as well prone to forged sender identities (e.g. black lists), but with white lists there is already one powerful means available that is hard to dupe.

UC prevention

UC prevention in the terminating network may be very useful. The reasons are:

- Whether a call can be rated as UC or not depends largely on the user perception which is by nature individual. Therefore, it would be useful for the user to be able to configure a UC prevention profile according to his personal needs. This will be done in the home network of the user and according to its private nature this profile will usually not be distributed to other networks, at least unless the user has not given explicit consent for the distribution.
- Another important reason for terminating UC prevention is of legal nature. Although the originating as well as transit networks would be able to react on UC suspicious communication, they may be not allowed to do so depending on the legislation of the country. The callee has to give explicit consent for that. Therefore it is important that the reacting network is able to prove the permission for UC reaction. This can be achieved by a UC prevention profile in the terminating network. For Supplementary Services based UC prevention this is guaranteed as the user configures his personal UC prevention profile in an AS of his home network and gives thereby explicit consent to react according to his profile.

## 9.5 Real-time / non-real-time UC identification and prevention

The real-time vs. non-real-time aspect depends largely on the chosen UC method:

If UC identification and information gathering is only used in an operator's network and for the purposes of the operator, then it can work non-real-time.

For UC prevention by means of Supplementary Services UC identification can work real-time, e.g. by user feedback via a key-press operation, as well as non-real-time, e.g. by putting a UC source on a black list via a web interface of the operator.

For UC prevention by means of an IMR-based PUCI AS, UC identification has stringently to be evaluated real-time because the result of UC identification (a UC marking/score) has to be delivered with the signaling of the call.

UC prevention itself has to react in every case real-time. Real-time means in this case that UC prevention has to react before the UC call is indicated to the callee by ringing of the phone. Otherwise the nuisance of the callee has already taken place and UC prevention is therefore dispensable.

## 9.6 Standardized versus Vendor specific aspects

The need for standardization for PUCI is dependent in part on where the functionality (PUCIF) is realized according to the different options outlined in Section 9.1, and also which features are included. Specifically, making use of the SS functionality to enforce PUCI based on Contextual Information (described in Section 7.4.3) specific to UC may require enhancements to SS standards. This is ffs.

For IMR, potential additional standardization work is listed in Section 7.2.5.4. Before this standardization work can be started, the IMR modules need to be detailed by, for example, reference to potential RFCs or by reference to 3GPP standardization work.

Moreover, if contextual information is generated in a node different from where it is used, standardization is needed to carry it in the network. However, even if such contextual information would include some form of UC score, it is not deemed necessary to standardize the scoring algorithm.

Guidelines for PUCI could be based on this TR and include, e.g., recommendations for non-technical measures and for technical measures that fall outside the scope of 3GPP standardization, such as recommendations for authentication of participating non-IMS networks. To the extent that it is deemed necessary, it is also proposed that stage 2 and 3 normative work on enhancements to Supplementary Services (SS) is carried out in the time frame of Rel-10.

## 9.7 Interaction with non-IMS networks

There are two types of non-IMS networks:

- non-IMS SIP-based networks
- non-IMS and non-SIP legacy networks

All these networks are connected with each other and therefore UC may influence users of all these networks regardless in which network the UC source resides. As the majority of telephony today still takes place in legacy networks it can be expected that a large number of calls originating in VoIP networks will be VoIP-to-legacy calls. This is important for the efficiency of a UC prevention method:

- Today only UC prevention based on Supplementary Services can be applied in legacy as well as in NGN networks. Therefore UC prevention with Supplementary Services is readily available and has therefore a clear advantage compared to purely SIP-based approaches
- UC prevention by IMR-based PUCI AS is perhaps one step more sophisticated but is restricted to SIP-based networks.

Regarding the SIP-based networks, it must be differentiated between IMS and non-IMS SIP networks.

- As discussed in 4. 'Originating/terminating UC detection and prevention' it is mandatory for IMR-based UC prevention that an originating non-IMS network can be reliably authenticated to take actions against forged sender identities.

# 10 Conclusions

*<This chapter will give directions for TS >*

# Annex A (informative): Usability and Business Aspects

## A.1 Usability Consideration

When deploying a PUCI solution the usability of the solution will be one factor deciding the effectiveness of the solution to fight UC. Therefore, the following points should be taken into consideration:

### A.1.1 User Prompting

User prompting is a very popular method to shift the security decision responsibility to the user. Often it is assumed that the user decisions are

- well-educated i.e. all the users know what they are doing
- consistent i.e. the user makes the same decision in same circumstances
- without error i.e. the user makes no mistakes

From practical experience it is known, that those assumptions do not hold in many cases.

Excessive user prompting may result in a "click through" behavior of the user and makes potential attacks (e.g. phishing attacks, installation of malicious software or acceptance of a security risk) much easier. Also, excessive user prompting is a known to impact the user experience severely (i.e. annoy the user).

Therefore, user prompting should be a method to be used in quite moderate dose. The terminal and the network can support the user to protect himself from UC.

### A.1.2 User vs UE

In this technical report the term user and UE are often regarded as one entity. The device and its input and output mean have to support this kind of communication and user-device interaction. It should be taken into consideration, that the input and output means of devices varies widely. High end devices might be able to provide the user with full configuration means, but other devices may not offer such means. Also, devices that are in the low-cost range should protect the user in a reasonable manner without being forced to show on a small screen long lists or UC reporting questionnaires. Some devices might be designed to offer only the small range functionalities. Still the user should be protected hence other complementing approaches need to be found then direct user interaction.

# Annex B (informative): Analysis of UC protection mechanisms for non-IMS interconnection

This annex lists and analyses the main protection mechanisms applicable to UC protection for the specific non-IMS interconnection scenario. This annex should be considered as complementary to the analysis already provided in section 7 for the IMS general case although it refers to some similar mechanisms.

There are basically two kinds of solutions: non-technical and technical ones. The first category includes: legal or regulatory measures (state dependent), financial measures (call charging, penalties in case of UC), service level agreements (SLA) between operators and also SLA between service provider and customers. The non-technical solutions may be extremely efficient and possibly even more than the technical ones. Unfortunately since non-IMS interconnection is not based on previous legal or contractual agreement, non-technical solutions seem difficult to apply to this scenario.

As a consequence, we will focus in the rest of this section on technical solutions which can be themselves divided into several categories. Before browsing these categories we should assert that there is no single solution, but instead a necessary combination of several measures. The chosen combination necessarily depends on regulatory environment, service objectives (there may be significant differences between residential and professional services) and should also follow the (constant) improvements in attacker techniques.

The following categories of technical solutions are identified:

# B.1 Solutions based on sender identity

Several solutions standardized in IMS and analyzed in section 7.4 under the "use of IMS supplementary services" approach may be very efficient to prevent/block UC. These solutions include white lists, black lists, anonymous call rejection, closed user groups and call diversion on originating identity.

Unfortunately these solutions are efficient only if the **sender identity is authenticated** which is a big challenge in non-IMS interconnection scenario. On the other hand, when the sender identity is not authenticated, these measures may generate unwanted side-effects such as blacklisting a legitimate user.

These measures can also be adapted to the identity of the sending domain (i.e the domain name), which offers another level of granularity.

# B.2 Call analysis and UC identification

Several mechanisms try to rate incoming calls in order to filter the call or help the callee decide if he should answer it; these mechanisms are already presented in section 7.3 under the "IMR-Based" approach. Some of them are automatic whereas others are manual and require caller or callee intervention. Rating criteria include sender identity (or domain) reputation, call pattern matching, challenges. Some additional comments are provided below in addition to the analysis in section 7.3.

Assuming UC is sent in "bulk" by computers, call pattern analysis on the media try to find a given "voice" pattern, previously identified as UC, in the incoming call. This technique is very close to content filtering in e-mail and presents the same advantages/drawbacks. By the way, the processing time may be significantly increased in VoIP. Call pattern analysis on the signalling may be much easier but needs to be constantly adapted to attacker obfuscating techniques.

Challenges mechanisms are used to differentiate human from computers assuming a computer call is more likely to be UC than a human call. These techniques have been used for a long time in web services (CAPTCHA) and have shown several drawbacks: annoying for legitimate callers, not applicable to some (legitimate) people, often solved by low cost labor or broken by hackers [19]. Alternative solutions are based on challenge computation by the calling endpoint, which do not require human involvement and is intended to increase the call cost for spitter. Unfortunately, choosing the right challenge level is hard and may rule out legitimate endpoint without sufficient UC or memory. By the way, using challenges may break automatic legitimate services which are used in the future to notify people of various events.

Considering the "UC report by callee" approach mentioned in section 7.3, it should be noted that this solution is efficient only if:

- The sending user/domain identity is authenticated whereas it can be exploited to build a negative user reputation.
- The reaction time is fast enough to mitigate "bulk" UC which may be predominant if we consider the learning from SPAM campaigns analysis.
- The sending domain is not an attacker domain whereas the attacker may switch to other identities after having sent the "bulk" UC.

As a conclusion it seems that these techniques are relevant when the sending domain is legitimate but not when the UC originate from an attacker domain which may change rapidly along time. Also even when the UC originates from a corrupted account in a legitimate domain, the attacker may switch to another account as soon as the first one is blocked by the operator. This phenomenon is largely seen with WebMail accounts used to generate SPAM.

# B.3 Network solutions

Several techniques fall into this category. Once again, these solutions are not exclusive and may or shall be combined with other measures:

1) **Rate limiting**: this may be applied at the ingress interconnection/peering points (or in the subscriber access network) to filter large amounts of VoIP traffic coming from a specific source or sub-network. As potential drawbacks, the "right" threshold may be hard to set, legitimate traffic may be affected and also back-side effects may appear if the attacker is using spoofed source addresses with UDP transport.

2) **Source checking**: this technique has been proposed for fighting SPAM in e-mail context [20]. SPF consists in checking that the e-mail originates from a network source belonging to the supposed sending domain. This requires that the sending domain identifies and declares all its outbound proxys which may be a costly and tricky task for large organizations. By the way, this check is efficient for connection-oriented protocols (such as SMTP) but may become useless for VoIP over UDP because of possible source address spoofing.

3) **IPSec**: this set of standards offers a very secure solution, at the network level, with both data integrity, confidentiality and source checking. On the other hand, it may have some scalability limitations when a large number of VoIP domains need to be interconnected. Also it seems best suited for interconnection where a large volume of traffic is exchanged whether than for "sporadic" calls.

4) **TLS**: this set of standards also offers a very secure solution, at the transport level, with the same features as IPSec except it operates on a per-hop basis. As for IPSec, TLS seems best suited for "permanent" interconnection between domains rather than for "sporadic" calls.

# B.4 Applicative solutions

Several techniques fall into this category; once again this list is not meant to be exhaustive:

1) **SIP Identity**: this protocol [18] enables the sending domain to add a digital signature to egress INVITE requests, this signature being verified by the receiving domain after having fetched the sender public key. The concept of this mechanism is very similar to the DKIM protocol [21] specified for e-mail. In addition to the concerns raised by IETF [22], this protocol requires public-key management and may expose the receiving proxy to DoS threat because it is much more resource consuming to verify a signature (asymmetric cryptography) than for the attacker to forge a wrong signature. The DoS threat associated to this protocol seems to be under-estimated in the literature. As for DKIM, this class of protocol usually requires much more processing on the receiving side to check message validity or sender policy, than on the attacker side to create spoofed messages.

2) **Consent based** [23]: assuming sender identity is authenticated and a white list management system is enforced, the question arises of how a new caller may have a chance to reach the callee and eventually enter the white list. The proposed solution is some kind of notification process for the first call between a caller and a callee. The notification may be achieved in various ways, especially by using SIP event packages.

3) **Token mechanism** [24]: the token is added in the SIP header Via field and is used by the receiver to verify that the sender request has not been spoofed at the network level (in case of UDP transport). More generally, several mechanisms based on the concept of token, cookie or ticket can be found in the state of the art and they have the common characteristics that a receiving entity issues a token/cookie/ticket that the sender must present to access the service. Whithin 3GPP, in TR 33.828 [25], such mechanisms (TBS, Otway-Rees based key management) are proposed in order to protect the media path, although they do operate at the signalling level.

# Annex C (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New |
| Jun 2009 | SA-44 | SP-090281 | -- | -- | Presentation to SA for information | -- | 1.0.0 |
| Dec 2009 | SA-46 | SP-090828 | -- | -- | Presentation to SA for approval | 1.1.0 | 2.0.0 |
| Dec 2009 | SA-46 | SP-090873 | -- | -- | Presentation to SA for approval | 2.0.0 | 2.0.1 |