

ETSI TR 133 937 V12.0.0 (2014-10)



TECHNICAL REPORT

**Universal Mobile Telecommunications System (UMTS);
LTE;
Study of mechanisms for
Protection against Unsolicited Communication for IMS (PUCI)
(3GPP TR 33.937 version 12.0.0 Release 12)**



Reference

RTR/TSGS-0333937vc00

Keywords

LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

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

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

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	7
1 Scope	8
2 References	8
3 Definitions, Symbols and Abbreviations.....	9
3.1 Definitions	9
3.2 Symbols.....	9
3.3 Abbreviations	9
4 System Environment for PUCI.....	11
4.1 Architectural Issues	11
4.1.1 Introduction.....	11
4.1.2 Originating/Terminating UC Identification and Scoring	12
4.1.3 Central/Distributed UC Identification and Scoring	13
4.1.3.1 Distributed UC Identification and Distributed UC Scoring	13
4.1.3.2 Distributed UC Identification and Central UC Scoring.....	15
4.1.4 Standardized/Vendor-Specific UC Scoring Algorithms	16
4.2 Non-Technical Conditions.....	17
4.2.1 Prevention of Unsolicited Communication in an Operator Controlled Environment	17
4.2.1.1 Introduction.....	17
4.2.1.2 Current SPIT/UC Prevention Measures	17
4.3 Technical versus Legal Issues	19
4.3.1 Introduction.....	19
4.3.2 UC Legislation.....	19
4.3.2.1 Definition of UC	19
4.3.2.2 Definition of UC Communication Services	20
4.3.2.3 Consent Achievement about UC Communication	21
4.3.3 Liability	21
4.3.4 Privacy	22
4.3.5 Conclusion	23
4.4 Coexistence with Single Radio-VCC, ICS, and SC	23
5. PUCI Risk Analysis	25
5.1 General	25
5.2 UC Threats & Scenarios.....	25
5.2.2 General Scenario.....	25
5.2.3 Privacy Violation.....	27
5.2.3.1 Privacy Violation Scenarios	27
5.2.3.1.1 Bulk UC (Advertising)	27
5.2.3.1.2 Targeted UC (Stalker)	27
5.2.3.2 Privacy Violation Risks.....	27
5.2.4 Contentious Incoming Call Service Charge.....	28
5.2.4.1 Contentious Incoming Call Service Charge Scenarios.....	28
5.2.4.1.1 UC While Call Forwarding is Enabled.....	28
5.2.4.2 Contentious Incoming Call Service Charge Risks	28
5.2.5 Contentious Roaming Cost	28
5.2.5.1 Contentious Roaming Cost Scenarios	28
5.2.5.1.1 UC While Roaming	28
5.2.5.2 Contentious Roaming Cost Risks.....	29
5.2.6 Non-disclosure of Call Back Cost.....	29
5.2.6.1 Non-disclosure of Call Back Cost Scenarios	29
5.2.6.1.1 Baiting for Premium Number Call Back	29

5.2.6.2	Non-disclosure of Call Back Cost Risks	29
5.2.7	Phishing	29
5.2.7.1	Phishing Scenarios	29
5.2.7.1.1	Messaging/Voice Phishing for Bank Account Information	29
5.2.7.1.2	Voice Phishing for Identity Theft	29
5.2.7.2	Phishing Risks.....	29
5.2.8	Network Equipment Hijacking	30
5.2.8.1	Network Equipment Hijacking Scenarios	30
5.2.8.1.1	Compromised IMS Network Element	30
5.2.8.2	Network Equipment Hijacking Risks.....	30
5.2.9	User Equipment Hijacking.....	30
5.2.9.1	User Equipment Hijacking Scenarios	30
5.2.9.1.1	Botnets Using User Equipment	30
5.2.9.1.2	Malware Distribution Through Bulk UC.....	30
5.2.9.2	User Equipment Hijacking Risks	30
5.2.10	Mobile Phone Virus	30
5.2.10.1	Mobile Phone Virus Scenarios	31
5.2.10.1.1	Exposure of User Privacy	31
5.2.10.1.2	Destroying Mobile Phone Software and Hardware	31
5.2.10.1.3	Distributing Illegal Information and Virus	31
5.2.10.1.4	Junk Data Distribution through Bulk UC Resulting in User Additional Charges & Network Traffic Jam	31
5.2.10.2	Mobile Phone Virus Risks	31
5.2.11	Sender Impersonation UC.....	31
5.2.11.1	Sender Impersonation UC Scenarios.....	31
5.2.11.1.1	Forged Sender UC Received through Interworking with VoIP Operator	31
5.2.11.2	Sender Impersonation UC Risks	31
5.2.12	Unavailability of Service or Degraded Service Quality.....	32
5.2.12.1	Unavailability of Service or Degraded Service Quality Scenarios.....	32
5.2.12.1.1	UC flood leads to Degraded Service Quality.....	32
5.2.12.2	Unavailability of Service or Degraded Service Quality Risks	32
5.2.13	Negative Service Preconception Leading to Non-adoption	32
5.3	Specific UC threats in non-IMS inter-connections.....	32
5.3.1	Introduction.....	32
5.3.2	Legal assumptions	33
5.3.3	Network assumptions.....	33
5.3.4	Security assumptions	34
5.3.5	High risk specific threats	34
6	Security Requirements	36
6.1	Void.....	36
6.2	3GPP Security Requirements	36
7	Supporting Mechanisms and Solution Alternatives	37
7.1	Review of Measures and Potential Supporting Mechanisms.....	37
7.1.1	Measure for Protection Against Privacy Violation	37
7.1.1.1	Measures Against Bulk UC.....	37
7.1.1.2	Measures Against Targeted UC	40
7.1.2	Measures for Protection Against Contentious Incoming Call Service Charge	40
7.1.3	Measures for Protection Against Contentious Roaming Cost.....	40
7.1.4	Measures for Protection Against Non-disclosure of Call Back Cost	40
7.1.5	Measures for Protection Against Phishing.....	41
7.1.6	Measures for Protection Against Network Equipment Hijacking.....	41
7.1.7	Measures for Protection Against User Equipment Hijacking	41
7.1.8	Measures for Protection Against Mobile Phone Virus	42
7.1.9	Measures for Protection Against Sender Impersonation UC	43
7.1.10	Measures for Protection Against Unavailability of Service or Degraded Service Quality	43
7.2	IMR-Based Solution Approach	44
7.2.1	General.....	44
7.2.2	IMR Approach	44
7.2.3	From Requirements to Solution	45
7.2.4	IMR Solution Variations.....	47

7.2.4.1	General	47
7.2.4.2	IMR Solution Based on Supplementary Services	48
7.2.5	Detailed Solution	49
7.2.5.1	Overview	49
7.2.5.2	Simple PUCI Invocation	49
7.2.5.3	PUCI with Supplementary Services and 3 rd Party PUCI AS	51
7.2.5.4	Standardization	53
7.3	SPIT/UC Protection with Supplementary Services	53
7.3.1	Introduction	53
7.3.2	Supplementary Services usable for SPIT/UC Prevention	54
7.3.3	SPIT/UC Prevention Scenarios with Supplementary Services	55
7.3.3.1	Simple Black List combined with Anonymous Call Rejection	55
7.3.3.2	White List with Consent Mailbox	56
7.3.3.3	White List with Consent Mailbox, protected by a Black List	56
7.3.3.4	Sophisticated SPIT/UC Prevention Profile with Audio CAPTCHA	57
7.3.3.5	White List Consent Achievement by IN Server	58
7.3.3.6	SPIT/UC Feedback by User Based on Key Pad Entries in the Phone	60
7.4	Contextual Information	60
7.4.1	Introduction	60
7.4.2	IMS Mechanism Outline	61
7.4.3	Use of Contextual Information	61
7.4.3.1	General	61
7.4.3.2	Reaction	62
7.4.3.3	Marking	62
7.4.3.4	Sharing of Information	62
7.4.3.5	Impact on Supplementary Services	63
7.5	UC protection framework for non-IMS interconnection: the Open Proxy Handshake	63
7.5.1	Objectives	63
7.5.2	Assumptions	64
7.5.3	Basic principles	65
7.5.4	Detailed principles	66
7.5.4.1	No shared secret between domain A and domain B	67
7.5.4.2	A shared secret is established between domain A and domain B	68
7.6	Alternative Methods for Authentication of Originating Network	69
7.6.1	Introduction	69
7.6.2	P-Asserted-Identity	70
7.6.3	SIP Identity	70
7.6.4	Trusted Interconnect with IPSec	71
7.6.5	Trusted Interconnect with IPSec combined with P-Asserted-Identity	71
7.6.6	Summary	72
8	Evaluation of Solution Alternatives	73
8.1	Evaluation Criteria	73
8.2	Evaluation of Alternatives	76
8.3	Usage Space	84
9	Potential PUCI Architecture	86
9.1	High-level architecture, mapping PUCI functionality to the IMS architecture	86
9.2	Centralized/Distributed PUCI AS	86
9.3	UC identification / UC prevention	87
9.4	Originating/Terminating UC identification and prevention	87
9.5	Real-time / non-real-time UC identification and prevention	88
9.6	Standardized versus Vendor specific aspects	88
9.7	Interaction with non-IMS networks	89
10	Summary	90
Annex A (informative): Usability and Business Aspects.....		91
A.1	Usability Consideration	91
A.1.1	User Prompting	91
A.1.2	User vs UE	91

Annex B (informative): Analysis of UC protection mechanisms for non-IMS interconnection.....92

B.1 Solutions based on sender identity92

B.2 Call analysis and UC identification.....92

B.3 Network solutions93

B.4 Applicative solutions.....93

Annex C (informative): Change history95

History96

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 highlight alternative solutions that could be used 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 took into account the study done in TISPAN TR 187 009 on 'Feasibility study of prevention of unsolicited communications in the NGN'.

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](http://www.bsi.de/literat/forumkes/kes0508.pdf) from "Bundesamt für Sicherheit in der Informationstechnik", page 42 to 45, <http://www.bsi.de/literat/forumkes/kes0508.pdf>
- [5] [Spam Regulation Overview](http://www.caslon.com.au/spamnote.htm) from Caslon Analytics, <http://www.caslon.com.au/spamnote.htm>
- [6] [Combating SPAM Through Legislation](http://www.ceas.cc/papers-2005/146.pdf) – 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](http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf) – 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), <http://www.oecd.org/dataoecd/63/28/36494147.pdf>
- [9] [ITU Survey On Anti-SPAM Legislation Worldwide](http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf) 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](http://spamsymposium.eu/files/Cristina%20Bueti.ppt) 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'.