ETSI TR 187 009 V2.1.1 (2008-07)

Technical Report

Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN

Reference

DTR/TISPAN-07025-NGN-R2

Keywords

Regulation, security

ETSI

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

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

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

Important notice

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document seeks to determine if UC is a risk to the NGN user or to the NGN Operator (a CSP using NGN technology to provide services).

The present document offers justification for UC countermeasures by presenting the results of a Threat Vulnerability and Risk Analysis (TVRA) that quantifies the likelihood and impact of UC in the NGN where UC is initiated in a variety of forms described using a number of scenarios for illustration.

The present document defines the term unsolicited communication in the context of the NGN.

Where risk is shown from UC in the NGN the present document considers means to mitigate the risk using metrics of applicability, effectiveness and architectural instantiation.

NOTE: Whilst this document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] OMA-RD-CBCS-V1-0-20060711-C: "Categorization Based Content Screening Framework Requirements".

[i.2] OMA-AD-CBCS-V1-0-20060828-D: "Categorization-based Content Screening Framework Architecture".

[i.3] IETF RFC 5039: "The Session Initiation Protocol (SIP) and Spam".

[i.4] ETSI TS 183 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

[i.5] ETSI ETS 300 128: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Service description".

[i.6] ETSI TS 183 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol Specification".

[i.7] ETSI TS 183 007 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

[i.8] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services.

[i.9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications - OJ L 201, 31.07.2002).

[i.10] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.11] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.12] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.13] IETF draft-niccolini-sipping-spitstop: "Signalling TO Prevent SPIT (SPITSTOP) Reference Scenario".

[i.14] IETF draft-niccolini-sipping-feedback-spit: "SIP Extensions for SPIT identification".

[i.15] IETF draft-jung-sipping-authentication-spit: "Authentication between the Inbound Proxy and the UAS for Protecting SPIT in the Session Initiation Protocol (SIP)".

[i.16] IETF draft-schwartz-sipping-spit-saml: "SPAM for Internet Telephony (SPIT) Prevention using the Security Assertion Markup Language (SAML)".

[i.17] IETF draft-froment-sipping-spit-authz-policies: "Authorization Policies for Preventing SPIT".

[i.18] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.19] ETSI TS 186 006-1: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Part 1: Protocol Implementation Conformance Statement (PICS)".

[i.20] ETSI EN 300 798: "Digital Audio Broadcasting (DAB); Distribution interfaces; Digital baseband In-phase and Quadrature (DIQ) interface".

[i.21] ETSI TR 141 031: "Digital cellular telecommunications system (Phase 2+); Fraud Information Gathering System (FIGS); Service requirements; Stage 0 (3GPP TR 41.031 version 6.0.0 Release 7)".

[i.22] ETSI TS 122 031: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 1 (3GPP TS 22.031 version 6.0.0 Release 7)".

[i.23] ETSI TS 123 031: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 2 (3GPP TS 23.031 version 6.0.0 Release 7)".

[i.24] ITU-T Recommendation X.1244 (former X.ocsip): "Overview of countering SPAM for IP multimedia application".

[i.25] ITU-T Recommendation X.fcsip: "Technical Framework of Countering IP Multimedia SPAM".

[i.26] ITU-T Recommendation X.1231: (former X.csreq) - "Requirement on countering SPAM".

[i.27] 3GPP TR ab.cde [draft]: "Group Services and System Aspects; Protection against SMS, MMS and IMS SPAM; Study of Different SPAM Protection Mechanisms. Release 8.".

NOTE: This work item was never be finalized, for references please have a look at:

- 3GPP,"Protection against SMS and MMS spam", SP-060446, SA#32;
- Orange, "Consumer protection against spam and malware", S3-060331, Athens, April 2006;
- Nokia, "Anti-spam work in OMA and IETF", S3060504, 3GPP S3#44, Talinn, July 2006;
- Orange, "Spam Flagging using In-band Signaling in Mobile and Broadband Networks", S3-070094 TSGS3#46 Beijing 2007.

[i.28] ETSI SR 002 211: "Electronic communications networks and services; Candidate list of standards and/or specifications in accordance with Article 17 of Directive 2002/21/EC".

3 Abbreviations

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

ACR	Anonymous Communication Rejection
CAMEL	Customized Applications for Mobile network Enhanced Logic
CBCS	Categorization Based Content Screening
CSP	Communications Service Provider
DAB	Digital Audio Broadcasting
DIQ	Digital baseband In-phase and Quadrature interface
DoS	Denial of Service
FIGS	Fraud Information Gathering System
gsmSCF	GSM Service Control Function
gsmSSF	GSM Service Switching Function
HPLMN	Home Public Land Mobile Network
ICAP	Internet Content Adaptation Protocol
ICB	Incoming Communication Barring
IDD	International Direct Dialling
IETF	Internet Engineering Task Force
IP	Internet Protcol

ISDN	Integrated Services Digital Network
IST	Immediate Service Termination
ITU	International Telecommunication Unit
MCID	Malicious Call Identification
NGN	Next Generation Network
ODB	Operator Determined Barring
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
OMA	Open Mobile Alliance
PICS	Protocol Implementation Conformance Statement
PSTN	Public Switched Telecommunications Network
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SIPPING	Session Initiation Proposal Investigation
SPIT	SPAM over Internet Telephony
TAP	Transferred Account Procedure
TVRA	Threat Vulnerability and Risk Analysis
UC	Unsolicited Communication
UE	User Equipment
UMTS	Universal Mobile telecommunication System
VPLMN	Visited Public Land Mobile Network
WG	Working Group

4 General overview

In the email environment the instance of SPAM, the common name used to refer to bulk Unsolicited Communication (UC) where the benefit is weighted in favour of the sender, has proliferated in recent years. SPAM is recognized as a problem and is regulated against, at least in part, in the context of the Privacy Directive 2002/58/EC [i.9], specifically in article 13. However, as has been noted in SR 002 211 [i.28]: "Whilst proprietary technical means exist to assist algorithms that identify and filter spam emails, the legal framework for application of such means in face of processing error is uncertain. Article 13 supports the legal instruments under which spammers may be prosecuted but does not seem to imply technical provision."

As the NGN moves towards adoption of similar protocols for signalling and transport as used in email applications and services, there is a threat that similar UC phenomena will migrate to the NGN and may escalate in severity.

NOTE 1: UC existed in the pre-NGN PSTN/ISDN and treatment of such calls when characterized as either nuisance or malicious calls has been well documented and is not repeated in the present document.

In order to be considered as NGN Unsolicited Communication (UC) the characteristics of a call that allows it to be classified as UC have to be defined. The characteristics of telephony in the modern era of International Direct Dialling suggest that in the general case communication is unsolicited, i.e. when the phone rings it is rarely as a result of a planned and jointly agreed event (solicited) between the communicating parties. Unsolicited cannot be used as a synonym for unwelcome, similarly unsolicited cannot be used as a synonym for attack. The classification of a call by the recipient is complex and the definition of SPAM given in SR 002 211 [i.28] suggest that 3 criteria have to be met at the same time:

1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and

2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and

3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

The characteristics of the NGN may lead to greater load on the infrastructure as a result of more attempts to deliver UC as the signalling offers the possibility to deliver multiple media to the destination in parallel (e.g. voice and text).

The aim of security in the NGN is multifold and includes the ability to restrict the ability of threat agents to operate where the threat agents give rise to unwanted incidents, and to ensure that CSPs of NGNs have tools that allow them to operate in conformance to national and regional regulation in the areas of privacy and user (customer) protection. The means used to achieve this may encompass mechanisms, processes and methods that give assurance of confidentiality, integrity, authenticity, authority, reliability and availability of the services of the NGN.

NOTE 2: In the present document SPIT (voice SPAM) is used with the same meaning as UC (Unsolicited Communication).

5 Threat analysis for UC in the NGN

NOTE: In this study it is not investigated who is the source of UC, as an example set this could be classified as:

- specific users, user groups or call centres;
- IVR systems;
- or even normal legal users with a strong identity where their UE gets misused by e.g. trojans horses, viruses or worms to spread UC.

5.1 UC attack configurations for basis of TVRA

NOTE: In each of the scenarios that follow the NGN may be composed of 2 or more interconnected domains.

5.1.1 Scenario 1: One-to-One UC

In this scenario the single originator attempts to invoke one or more communication sessions towards a single destination.

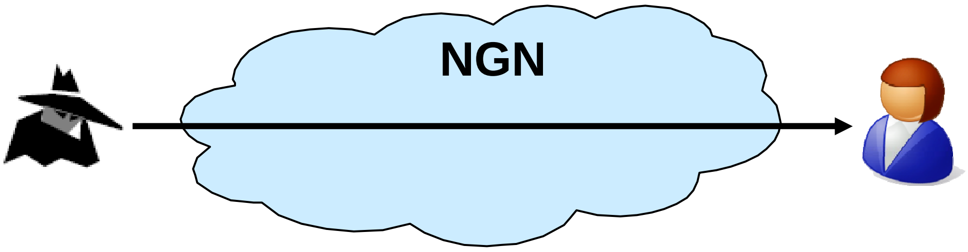


Figure 1: Scenario for 1-to-1 UC

UC pattern:

- one originator;
- one destination;
- one or many communication attempts.

EXAMPLE: Telemarketing where an originator tries to places calls to one user.

This scenario, when applied to email, would not normally be considered as SPAM as although it meets the 3 criteria from SR 002 211 [i.28], it fails when considered as bulk transmission.

This scenario, when applied to pre-NGN networks, would not normally be considered as UC as telemarketing is a legitimate business exercise. In most telecommunications networks offered under the Authorization Directive 2002/20/EC [i.8], there are voluntary codes of conduct within the telemarketing industry to ensure that users (potential recipients) are able to control their exposure to unsolicited telemarketing.

5.1.2 Scenario 2: One-to-Many UC

In this scenario, the single originator attempts to invoke one or more communication sessions towards multiple destinations concurrently.

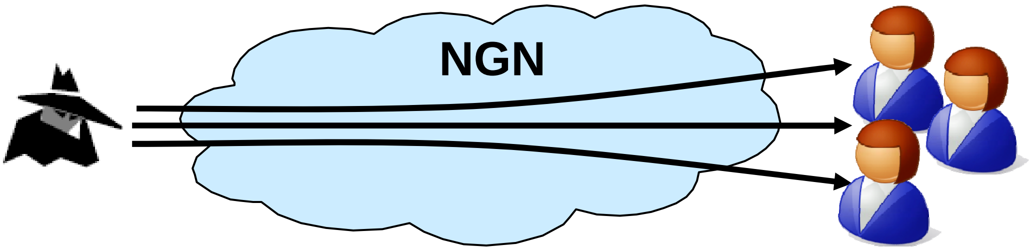


Figure 2: Scenario for 1-to-Many UC

UC pattern:

- one originator;
- several destinations / user group;
- one or many communication attempts.

EXAMPLE: Telemarketing where an originator tries to place calls to several users.

This scenario, when applied to pre-NGN networks, would not normally be considered as UC as telemarketing is a legitimate business exercise. In most telecommunications networks offered under the Authorization Directive 2002/20/EC [i.8], there are voluntary codes of conduct within the telemarketing industry to ensure that users (potential recipients) are able to control their exposure to unsolicited telemarketing.

5.1.3 Scenario 3: Many-to-One UC

In this scenario, a coordinated group of call originators attempt to invoke concurrent communication sessions towards a single destination.

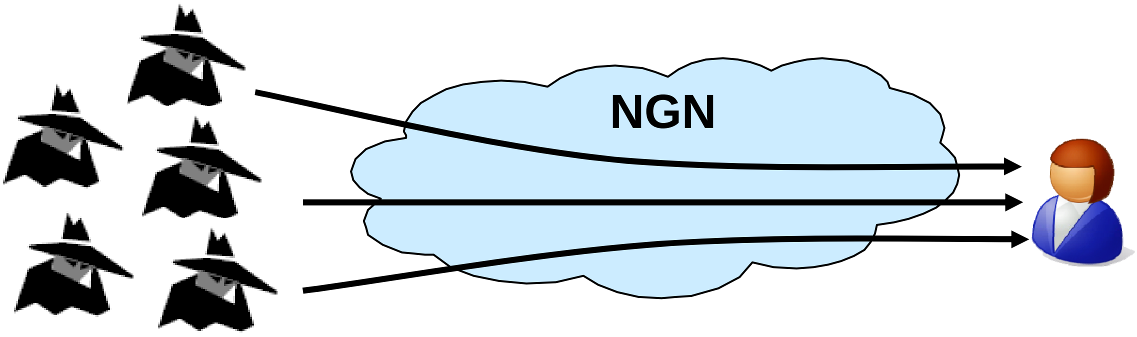


Figure 3: Scenario for Many-to-One UC

UC pattern:

- many originators (e.g. a coordinated attack group);
- one destination;
- one or many communication attempts.

EXAMPLE: Communication attempts through bot networks

NOTE: Whilst the NGN standards effort does not standardize business models, it is feasible to have advertising supported services where the call recipient in exchange for a lower call or subscription rate accepts advertising as part of the call and thus willingly accepts UC in exchange for preferential charges thus this scenario may not be UC.

5.1.4 Scenario 4: Many-to-Many UC

In this scenario, a coordinated group of call originators attempt to invoke multiple communication sessions towards a coordinated group.

NOTE 1: There may be no obvious relationship between the called parties.

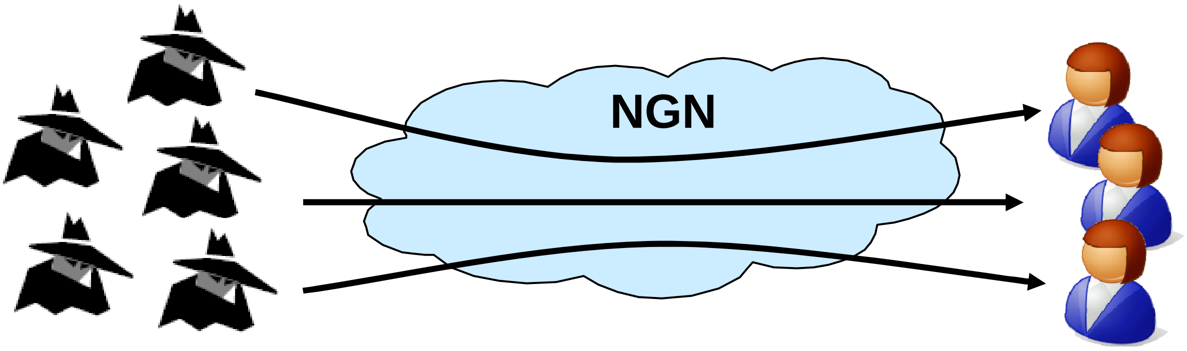


Figure 4: Scenario for Many-to-Many UC

UC pattern:

- many originators (e.g. a coordinated attack group);
- many destinations (e.g. a targeted victim group);
- one or many communication attempts.

EXAMPLE: Bot-networks spreading advertisement messages to many users.

NOTE 2: Whilst the NGN standards effort does not standardize business models, it is feasible to have advertising supported services where the call recipient in exchange for a lower call or subscription rate accepts advertising as part of the call, willingly accepting UC in exchange for preferential charges, thus this scenario may not be UC.

5.2 Attack vector of UC in NGN

The attack vector for UC is a communication session setup message (e.g. SIP INVITE) that may contain a number of payloads. The delivery of the payload may be made with the call setup message itself or may be offered only after acceptance of the call setup (e.g. 200 OK) by transmission on the associated media path.

NOTE: UC is itself an attack vector.

In order to launch an attack, the communication attempt has to be made to a known identity. The consideration of identity and identity management risks in the NGN as presented in TR 187 010 [i.11] has identified the public availability of identity as a key element that allows an attacker to instigate attacks through UC. Technical countermeasures which can be applied to identify UC are described in RFC 5039 [i.3], that maintains the focus of the NGN as an all connected network supporting point to point connections between any parties known or unknown. It is this core capability of the NGN that is exploited by attackers using the UC vector.

Examples of payload include:

- recorded voice messages:
  - may be delivered as an attachment to call setup or post call setup in the media path;
- recorded text messages:
  - may be delivered as an attachment to call setup or post call setup in the media path;
- recorded multimedia messages:
  - may be delivered as an attachment to call setup or post call setup in the media path;
- vishing (voice phishing):
  - vishing requires connection to be established with the called party and for the called party to be fraudulently encouraged to release data;
- callback voice:
  - the UC of Callback Voice is mostly an issue for a person on the receiving side, especially if frequently repeated;
- callback text:
  - the UC of Callback Text is mostly an issue for a person on the receiving side, especially if frequently repeated.

5.3 Risk assessment for UC in NGN

The purpose of the NGN is to support communication attempts between any two (or more) identities. As UC uses the existing NGN call setup mechanisms the likelihood of UC occurring is very high, however the impact is purely dependent on context.

- Risk of UC (without countermeasure) = likelihood (high) * impact (low to high).

The risk of UC in the untreated NGN varies from 3 through 6 and 9 (i.e. low risk to critical risk).

Where a critical risk is presented in the NGN, a countermeasure should be provided in the core NGN design.

5.4 Objectives for the prevention of UC in NGN

The primary objective of any system is to avoid the occurrence of unwanted incidents where for the purposes of the present document the unwanted incident is unsolicited communication that leads to a violation of the security principles of the NGN. Arising from this the primary objective is for CSPs and users of their services to recognize UC as a threat and to be able to recognize it, report it, and act to minimize it. However, the nature of UC may lead to many false reports and therefore, there has to be an objective to minimize the interference to call processing as a result of attempts to recognize, report, and minimize UC.

As a report of UC may lead to restriction of the initiating party (the UC instigator), any report of UC has to be against a specific instance of a call and with an audit of the report maintained.

OBJ1: The NGN should provide the ability for users to identify specific communications instances as UC

As UC existed in the pre-NGN PSTN/ISDN and treatment of such calls when characterized as malicious calls has been well documented and is not repeated in the present document, this requirement is to identify a call as nuisance, specifically as UC (i.e. not malicious).

OBJ2: The NGN should provide the ability to mark UC

To propagate information of UC rating through the network, the communication attempt should be marked in a unique and transparent way. UC prevention-enabled nodes can take already marked UC call attempts into account to do further computation or take preventive actions. Non-UC prevention-enabled network nodes should not be affected by this marking.

OBJ3: The NGN should provide the ability to react to UC

To prevent UC by technical means, reaction on identified UCs should be provided. This could be realized in the NGN environment by:

- blocking the communication attempt in advance;
- redirecting the communication attempt to a specific mailbox;
- direct the marked UC attempts to the end user and let them decide how to deal with it.

OBJ4: The NGN should provide the ability to a user to personalized the UC profile

UC is highly subjective, and because of this, a mechanism is needed to allow users to personalize the types of calls to be mapped to the user specified profile. This would include the ability to white- or black-list future sessions based on specific criteria.

EXAMPLE: a user wants to receive telemarketing calls from a particular operator, but wants to be protected from the calls from another operator.

Table 1

OBJ	Statement
1	NGN CSPs should recognize UC as a threat
2	The NGN should be the only entity able to destroy identities
3	The NGN should comply with the OECD guidelines for processing of personal data
4	The identity provider should be retrievable from analysis of the identity
5	The NGN should support the transfer of identifier/identity between CSPs

5.5 Security requirements for prevention of UC in the NGN

The functional requirements should be modelled on the classes of ISO/IEC 15408-2 [i.18].

REQ_AU1: Any report of UC made by an NGN-user shall be an auditable event.

5.5.1 Functional security requirements

In the context of the Common Criteria, ISO/IEC 15408-2 [i.18], the following functional components should be deployed during the identity validation step.

5.6 Prevention of UC in NGN countermeasure framework

5.6.1 Existing solutions / countermeasures

This clause summarizes existing solutions and countermeasures within the NGN that may assist in dealing with the threat of unsolicited communication. The following existing solutions address a specific problem or technical function to react on a special kind of UC but the complete solution is still missing.

5.6.1.1 MCID - Malicious call identification

This service enables the callee to indicate that an incoming communication is considered to be malicious and it should be identified and registered. The MCID supplementary service is described in TS 183 016 [i.6].

5.6.1.2 OIR - Originating Identification Restriction

The OIR service enables the originating party to prevent presentation of any network-provided identity to the terminating party, and is applicable to all session-based services of the NGN. The OIR supplementary service is described in TS 186 006-1 [i.19].

5.6.1.3 ACR - Anonymous Communication Rejection and ICB - Incoming Communication Barring

This service, ACR, allows a user to reject incoming communications when the caller is anonymous. ICB allows a user to block incoming communications based on the identity of the caller. The ACR and ICB supplementary services are described in EN 300 798 [i.20] and TS 183 011 [i.4].

5.7 System management requirements

In an NGN which will provide detection and prevention of unsolicited communication, at least the following information should be available for the UC detection engine:

- source;
- destination;
- timestamp.

This basic information can be used to classify communication attempts with a preliminary UC rating e.g. by placing one source on a blacklist every time this source tries to establish a communication attempt so that it can be rated as unsolicited.

Additional information from the signalling level or from external data sources can be used to compute more advanced metrics for UC rating, e.g. by correlating the time of day (i.e. midnight) with the frequency of call attempts (i.e. 5 000 call attempts per hour), the source could be rated as unsolicited:

- identity of the originator;
- identity of the destination;
- routing information;
- time of day (at source or destination);
- subject or content-type;
- etc.

UC is a highly end-user dependant kind of communication, and the end-user should be able to interact with the UC detection system, e.g. by defining a personal black and white-list of communication sources.

5.7.1 User requirements

Because perception of unsolicited communication is strongly user dependant, the user should have the ability to interact with the detection system and decide as late as possible whether the communication is unsolicited or not.

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.

Even the source of the UC attempt should have the possibility to interfere with the UC system and request the rating applicable to it from the NGN. This is useful if an assumed UC source declined or redirected by i.e. wrong rating or personal perception of the destination to experience why his call was treated as UC.

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.

5.7.2 Architectural requirements

To automate the detection and to apply personalized preferences to prevent UC in the NGN, the NGN should provide the ability that the interfering nodes in the network, which are involved in the UC prevention, can derive information from the UC attempt.

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.

To propagate the information if a communication attempt was rated as unsolicited through the NGN (i.e. to following nodes or to the end user) the NGN needs the ability to mark the detected UC attempt.

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

To react on the detected and marked UC attempt, the NGN needs the ability to handle such call attempts, e.g. by redirecting the call to a mailbox, voice-mailbox, or junk-mail.

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

6 Feasibility of providing UC prevention in the NGN

In this feasibility study we defined three main objectives for preventing unsolicited communication in the NGN:

- OBJ 1: The NGN shall provide the ability to identify UC;
- OBJ 2: The NGN shall provide the ability to mark UC;
- OBJ 3: The NGN shall provide the ability to react to UC.

6.1 Identifying UC

In the current TISPAN NGN release, only limited functionality exists for identifying UC in the NGN networks. The MCID service is a feedback after an incoming communication attempt and works only for further preventing of the calls from the same originator. Missing functionality is Identifying UC in different stages:

- non intrusive tests:
  - for which the call-signalling gets analyzed by an automatic mechanism to derive a marking;
- intrusive tests:
  - for which 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 before / during / after a transaction:
  - this is an extension of the MCID where a user can e.g. define in advance a personal black-list, react during a call or give feedback an occurrence of UC to provide his personal preferences to prevent the next UC attempt.

6.2 Marking UC

Marking a transaction as UC is needed to communicate identified UC traffic in through the NGN e.g. to give the user the personal choice of acting on a UC or take routing decisions in the network based on the UC rating of the transaction attempt. Work is ongoing in the IETF of marking a call as SPIT, but at the current point in time this is in the early drafting phase. The following functionality is needed to mark UC in the NGN:

- Mark a transaction attempt such that intercepting network entities can react to the UC. This could be done by a different functionality which takes care of this (off-line) or could be realized by adding information to the incoming communication attempt (in-line).

6.3 Reacting to UC

Reacting on UC is defined as requirement R-UC-7 stated in OBJ3 in varying the call handling (see also clause 6.4.3). This is normal call handling based on additional data and does not need to be investigated further because it is already provided.

6.4 Architectural impact

The architectural impact will reflect the defined requirements from clause 6 and present different network scenarios in the scope of the NGN where these apply differently.

6.4.1 Technical impact

The following technical issues should be addressed in order to meet the defined requirements to counter the issue of UC.

6.4.1.1 User Interaction

The perception of UC is subjective, and users will react differently to UC. This means that each user will need to be able to communicate UC requirements to the NGN. It is feasible that the network operator will offer a service to provide UC prevention. It should therefore be possible for users to define in a way (e.g. a UC profile) how well they trust the rating of the network (i.e. global blacklist), they trust their own ratings (i.e. personal blacklist) and how rated calls should be handled (i.e. redirected to mailbox).(R-UC-1, R-UC-2, R-UC-3, R-UC-4).

- The users should have the possibility to interact with the NGN to define their personal perception profile of UC and how identified UC should be handled.

6.4.2 Identifying and marking UC

Identification and marking of UC can be coupled because splitting these logical functionalities would introduce another interface.

- The NGN should provide, at the appropriate entities in the network, interfaces to extract the required information, compute the UC rating and propagate this information back on the signalling path.

6.4.3 Handling & Preventing UC

Preventing UC in the NGN will be done by blocking (where allowed), rerouting or answering the call on behalf of the user. 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.

- The NGN should provide the possibility to block (where allowed), reroute or answer the call on behalf of the user according to a UC rating.

6.5 NGN design impact

The impact of UC prevention in the NGN depends on the deployment scenario and the business model. Different deployment scenarios can have different impacts on the architecture to prevent UC detection and prevention.

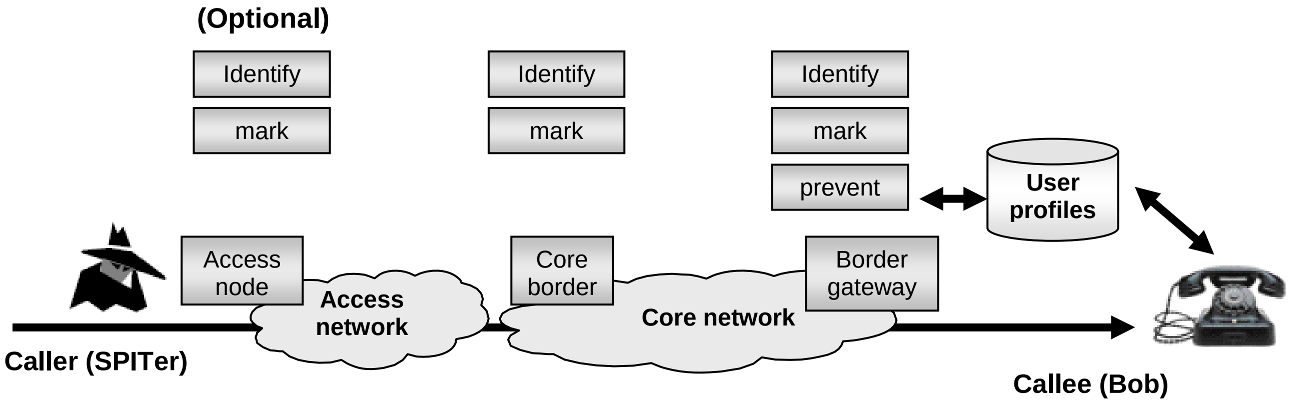
NOTE: In all cases, Emergency or priority communications should override UC preferences.

6.5.1 Individual users

In the context of providing UC prevention for individual users in the NGN, different business models and deployment scenarios are possible, e.g. providing UC prevention as an additional service to the end user.

NOTE: This issue has to be addressed by the related standardisation group (e.g. TISPAN Requirements and Architecture) to define how the architectural impact would look in the enterprise scenario. Their input will be incorporated in the specification which will be handled in the future technical specification work of TISPAN on UC prevention.

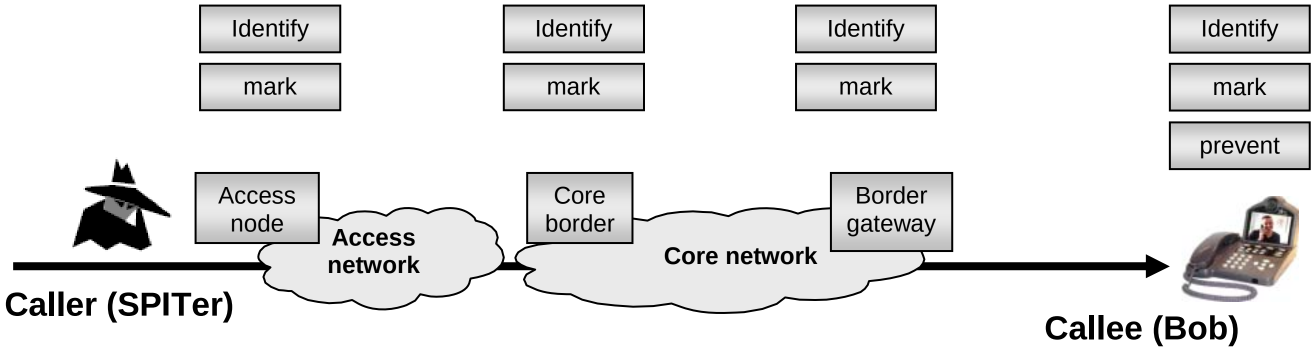
6.5.1.1 UC prevention as supplementary NGN service



NOTE: The detection of UC can be done distributed in the network e.g., the access node by a message-rating module, in the core-border element by global black-list module. The decision of preventing the call can be done on in the core network (i.e. on the border gateway, an application server in the IMS case or another responsible node. Here a strong binding with the user exists e.g.,. by a UC-profile in an database and according to the stored action the UC call gets handled.

Figure 5

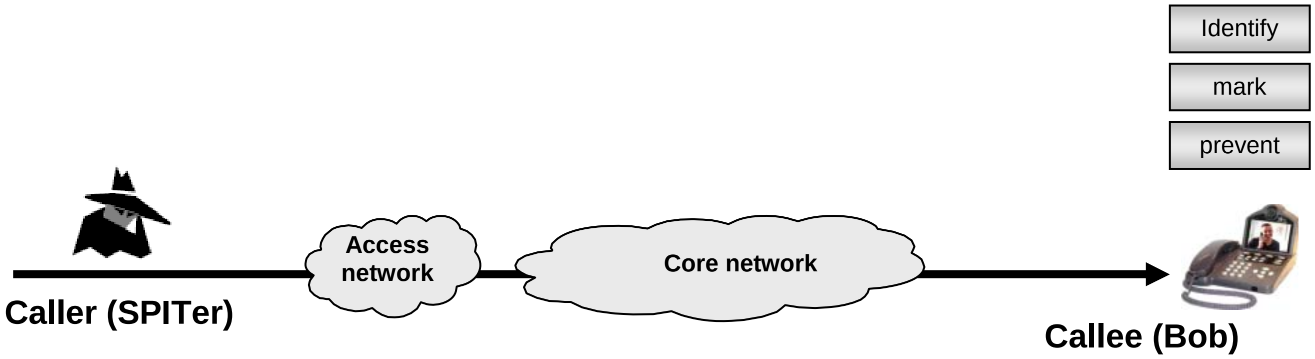
6.5.1.2 UC prevention as supplementary NGN service with handling UC on the UE



NOTE: This scenario is similar to the scenario depicted in C.2.1, however, in this case the user receives the recommendation of the network and can make the decision on how the UC marked call should be handled.

Figure 6

6.5.1.3 UC prevention as stand alone solution in the UE



NOTE: In this scenario the UC prevention only takes place in the UE.

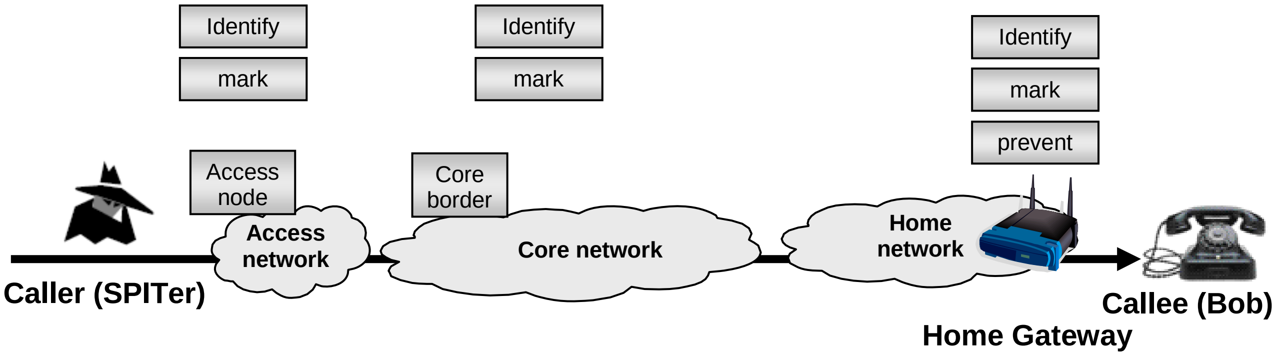
Figure 7

6.5.2 Home networks

The personalization of the UC profile may be administered in the CNG, and the UC detection/prevention may be placed in the CNG. Alternatively, this may be administered and implemented wholly within the NGN, or distributed across the CNG and the NGN.

NOTE: This issue has to be addressed by the related standardisation group (i.e. TISPAN NGN Home Networking) to define how the architectural impact would look like in the enterprise scenario. Their input will be incorporated in the future technical specification work of TISPAN on UC prevention.

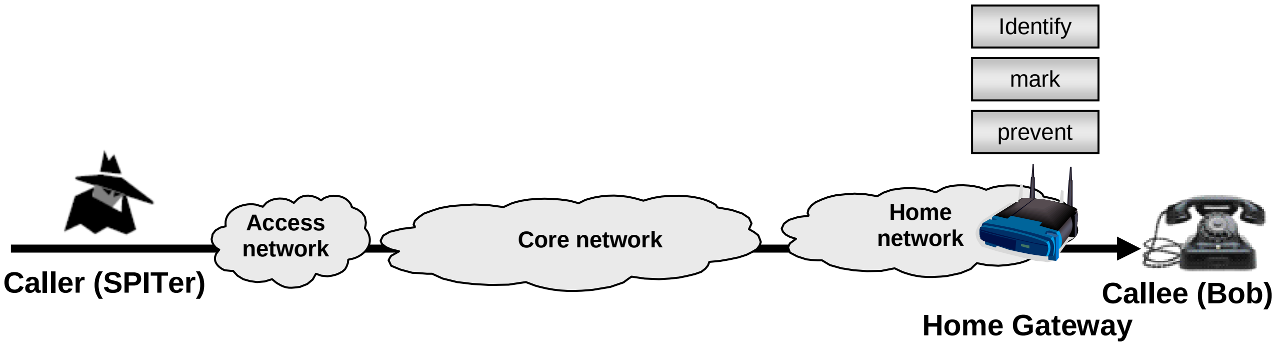
6.5.2.1 UC prevention as supplementary NGN service with handling UC on the home gateway



NOTE: This scenario is similar to the scenario depicted in figure 6, however, in this scenario the user administrates in the user premises (home network) the UC handling and the degree of trust in the UC rating from the NGN additional service.

Figure 8

6.5.2.2 UC prevention as stand alone solution in the home gateway



NOTE: In this scenario the one and only decision node is the home gateway.

Figure 9

6.5.3 Enterprise

In the context of enterprise NGN deployment scenarios global/enterprise/company policies may also place requirements on UC handling.

NOTE: This issue has to be addressed by the related standardisation group (e.g. ECMA) to define how the architectural impact would look in the enterprise scenario. Their input will be incorporated in the specification which will be handled in the future technical specification work of TISPAN on UC prevention.

7 Recommendations for future work

The TVRA has identified UC as a risk in the NGN. The main issues identified are that, although UC overall presents risk to the users of the NGN, the fact that the NGN model supports calls is a risk, and the classification of a call as UC depends on the perception of the intrusion.

- UC depends highly on a personal perception of risk. Theoretically every call attempt in the NGN network can be considered unsolicited until both communication partners agree on a common level of risk acceptance level. However, in current PSTN implementations, the assumption is that all sessions are accepted unless a service has been invoked on behalf of the user to process them differently.
  If a user receives too many UC attempts, his confidence in the NGN services will be reduced.

- The NGN network (as a system including the network or end-user) should provide the ability for UC detection and prevention to increase the confidence of the end users. Further investigations on how this will be realized and whether the issue of too few call completions will threaten the NGN network itself (in term of availability of the service) has to be evaluated further.

- The present document report recommends that initially work should concentrate on the end user being given the ability to mark communications as unsolicited. Further, it recommends to proceed on the distributed UC detection approach to fulfil the complex requirements from a whole NGN perspective.

- Similar work in the context of the common IMS and the 3GPP architecture should also be carried out to define a common solution for UC detection and prevention for the NGN.

- Regulatory aspects and implications need to be considered.

Annex A:
Comparable work in other standardization bodies

A.1 IETF

At the Internet Engineering Task Force (IETF) there is already an official activity on unsolicited communication problem analysis since February 2005 in the Session Initiation Proposal Investigation (SIPPING) working group (WG). Official activities are limited to this activity, but more work is under preparation. Several individual Internet drafts have been submitted in recent months and preparations for more official activities or even a new working group are ongoing.

This clause describes the official working group document as well as the individual Internet drafts that are currently under discussion at the IETF. Preparations for a BoF session on unsolicited communication are conducted on a mailing list called "spitstop", see https://listserv.netlab.nec.de/mailman/listinfo/spitstop.

- **RFC 5039: "The Session Initiation Protocol (SIP) and Spam", J. Rosenberg, C. Jenning [i.3]**
  This Internet draft is an official SIPPING WG document since February 2005. It analyzes the problem of unsolicited communication, called Spam over IP Telephony (SPIT), in combination with the Session Initiation Protocol (SIP) protocol. The document first identifies the ways in which the problem is the same and the ways in which it is different from email. Then it examines the various possible solutions that have been discussed for email and consider their applicability to SIP.
  The document identifies three kinds of unsolicited communication in combination with SIP: call spam, Instant Messaging (IM) spam, and Presence spam. These are briefly defined. The particular strength of the document is the extensive description of the known solution space for this kind of unsolicited communication. 13 different solutions are discussed considering their effectiveness with respect to preventing unsolicited communication.

- **Draft-niccolini-sipping-spitstop: "Signalling TO Prevent SPIT (SPITSTOP) Reference Scenario", S. Niccolini, J. Quittek [**i.13**]**
  This individually submitted Internet draft explores the need for standards for SPIT preventing systems. It suggests a reference scenario for SPIT prevention systems and defines interfaces (reference points) between involved entities. It differentiates on-path interfaces that are on the path that a SIP INVITE message of a particular unsolicited call, and interfaces that are not on this path. For each of the 6 defined interfaces, need for standardization is discussed individually.

- **Draft-niccolini-sipping-feedback-spit: "SIP Extensions for SPIT identification", S. Niccolini, S. Tartarelli, M. Stiemerling, S. Srivastava [**i.14**]**
  This individually submitted Internet draft analyzes the need for user feedback on unsolicited communication. The basic idea is that callees that received unsolicited communication may provide feedback to their service provider by identifying a received call as an unsolicited one. The unit receiving this information may use it for improving its prevention capabilities for unsolicited communication, for example, by adding the initiator of the unsolicited communication to a blacklist. The document elaborates this idea by identifying parameters that identification systems for unsolicited communication may need for improving their performance. It also shows these parameters can be transmitted by means of SIP.

- **Draft-jung-sipping-authentication-spit: "Authentication between the Inbound Proxy and the UAS for Protecting SPIT in the Session Initiation Protocol (SIP)", S. Jung, J. Choi, Y. Won, Y. Cho [**i.15**]**
  This individually submitted Internet draft addresses the direct attack of an initiator of unsolicited communication from terminal to terminal without routing SIP signalling via SIP servers that potentially might protect the receiver of a SIP INVITE message from unsolicited communication. The document suggests a digest message authentication scheme between the inbound SIP proxy server and the SIP user agent of a user for protecting from unsolicited communication. The suggestion that is made uses digest-based authentication for SIP INVITE messages that have been sent by an incoming SIP proxy server. This authentication method achieves that a SIP user agent will only accept well authenticated SIP INVITE messages from trusted proxy servers. This way, most initiators of unsolicited communication might be blocked.

- **Draft-schwartz-sipping-spit-saml: "SPAM for Internet Telephony (SPIT) Prevention using the Security Assertion Markup Language (SAML)", D. Schwartz, B. Sterman, E. Katz, H. Tschofenig [**i.16**]**
  This individually submitted Internet draft addresses the problem of limiting and preventing SPIT and proposes to use the concept introduced by the SIP Identity Framework in combination with the Security Assertion Markup Language (SAML) to transfer security relevant attributes from one administrative domain to another. This approach allows the domains which make use of such attributes to make intelligent filtering decisions when receiving session initiation.

- **Draft-froment-sipping-spit-authz-policies: "Authorization Policies for Preventing SPIT" , G. Dawirs, T. Froment, H. Tschofenig [**i.17**]**
  This individually submitted Internet draft discusses mechanisms to establish policies to react on potentially unwanted communication attempts. These policies are discussed in relation to particular Session Initiation Protocol (SIP) attributes included in the INVITE or MESSAGE methods and in relation to other attributes related to security strength employed by sending domain/user (identity strength, unwanted communication estimation, etc.). This document tries to stimulate the discussion whether it is worth to investigate the aspect of authorization policy usage for SPIT prevention.

A.2 ITU

The ITU is working on the thread Countering spam by technical means in the ITU-T Study Group 17 - Question 17/17 (Study Period 2005-2008).

- **X.1244 (former X.ocsip) - "Overview of countering SPAM for IP multimedia application" [**i.24**]**
  This Recommendation specifies basic concepts, characteristics, and effects of Spam in IP multimedia applications such as IP Telephony, instant messaging, multimedia conference, etc. It provides technical issues, requirements for technical solutions, and applicability of countering mechanism of email spam into IP multimedia spam. It provides basis and guideline for developing further technical solutions on countering Spam.

- **X.fcsip - "Technical Framework of Countering IP Multimedia SPAM" [**i.25**]**
  This Recommendation will specify general architecture of countering spam system on IP multimedia applications such as IP Telephony, instant messaging, multimedia conference, etc. It will provide functional blocks of necessary network entities to counter spam and their functionalities, and describe interfaces among the entities. To build secure session against spam attack, User Terminals and Edge Service Entities such as proxy server or application servers will be extended to have spam control functions. We will also show interfaces between these extended peer entities, and interfaces with other network entities which can involve for countering spam.

- **X.1231 (former X.csreq) - "Requirement on countering SPAM [**i.26**]**
  Requirements on countering spam are clarified in this recommendation. There are many types of spam, such as email spam, Mobile messaging spam and IP multimedia spam. Various types of spam may have both common and specific requirements on countering it. For one type of spam, the requirement in different entities should also be clarified.

A.3 3GPP

- **ETSI TR 141 031 V6.0.0 [i.21]**
  "Digital cellular telecommunication system (Phase 2+); Fraud Information Gathering System (FIGS), Service requirements; Stage 0" (3GPP TR 41.031 version 6.0.0 Release 6)
  This Technical Report describes the requirements (at a stage 0 level) of the Fraud Information Gathering System (FIGS). FIGS provides the means for the HPLMN to monitor a defined set of subscriber activities. The aim is to enable service providers/network operators to use FIGS, and service limitation controls such as Operator Determined Barring (ODB) and Immediate Service Termination (IST), to limit their financial exposure to large unpaid bills produced on subscriber accounts whilst the subscriber is roaming outside their HPLMN. HPLMNs may also choose to collect information on subscriber activities whilst their subscribers are within the HPLMN.

- **ETSI TS 122 031 V6.0.0 [i.22]**
  "Digital cellular telecommunication system (Phase 2+); Universal Mobile telecommunication System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 1" (3GPP TS 22.031 version 6.0.0 Release 6)
  This Technical Specification specifies the stage 1 description of the Fraud Information Gathering System (FIGS) feature which provides the means for the HPLMN to monitor the activities of its subscribers in a VPLMN.
  The purpose of this network feature is to enable the HPLMN to monitor the activities of its subscribers while they are roaming. The VPLMN collects information about a defined set of activities on monitored subscribers and sends this information back to the HPLMN. This enables the HPLMN to clear certain types of calls and so stop fraudulent use of the GSM system.
  This specification enables service providers/ network operators to use FIGS, and service limitation controls such as Operator Determined Barring (ODB) and Immediate Service Termination (IST), to limit their financial exposure to subscribers producing large unpaid bills.
  HPLMNs may also choose to monitor the activities of its subscribers within the HPLMN.

- **ETSI TS 123 031 V6.0.0 [i.23]**
  "Digital cellular telecommunication system (Phase 2+); Universal Mobile Telecommunication System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 2" (3GPP TS 23.031 version 6.0.0 Release 6)
  This Technical Specification specifies the stage 2 description of the Fraud Information Gathering System (FIGS) feature which provides the means for the HPLMN to monitor the activities of its subscribers in a VPLMN.
  Three levels of FIGS service are defined:
  Level 1 will use the facilities provided by Transferred Account Procedure (TAP).
  Levels 2 and 3 will use facilities provided by Customized Applications for Mobile network Enhanced Logic (CAMEL), in particular, the information flows between the GSM Service Switching Function (gsmSSF) and GSM Service Control Function (gsmSCF). Phase 1 and Phase 2 CAMEL facilities will be used.
  Connection-orientated services only are covered.

- **3GPP TR ab.cde [draft] [**i.27**]**
  3rd Generation Partnership Project; Technical Report "Group Services and System Aspects; Protection against SMS, MMS and IMS SPAM; Study of Different SPAM Protection Mechanisms" Release 8
  This Technical Report is part of the 3GPP study item on SPAM. Spamming has been an ongoing problem for several years now in fixed IP-based networks with unsolicited emails sent by thousands every day, but also in mobile networks in the form of unsolicited SMS and MMS. The spreading of UC has potential unwanted effects on customer satisfaction, on the capacity of network resources and on corporate image/reputation of the service provider. This TR studies existing and new mechanisms to enable to limit the effects of the SPAM.
  The following services are considered into the scope of this TR: SMS, MMS, IMS messaging/presence/call and also email messages. The scope is indeed large and ambitious, but as the trend is too converge all medias, the anti SPAM solution has to be adapted to this concept.

A.4 OMA

OMA has drafted a set of requirements and architecture for Categorization Based Content Screening (CBCS) suggesting among other things usage of ICAP protocol to transfer content categorization information. Content Screening is defined as the act of blocking, allowing or amending content, thereby, it also includes malware. It is suggested that the OMA requirements and architecture are considered for the unsolicited communication study as appropriate.

The current OMA work can be found in the following specifications:

- **"Categorization Based Content Screening Framework Requirements", Candidate Version 1.0 - 11 July 2006 (a newer one may already exist), Open Mobile Alliance OMA-RD-CBCS-V1_0-20060711-C [i.1]**
  The document describes Use Cases for categorization based content screening and high level requirements on the functionality of such a system.

- **"Categorization-based Content Screening Framework Architecture", Draft Version 1.0 - 28 Aug 2006, Open Mobile Alliance OMA-AD-CBCS-V1_0-20060828-D [i.2]**
  The document presents an architectural model for a two-tier solution of a CBCS Enabler. The CBCS Enabler evaluates and/or enforces Screening Rules.

Annex B: Completed eTVRA proforma for UC

A Security Environment		
A.1 Assumptions		
A.2 Assets		
A.3 Threat agents		
A.4 Threats		
A.4.1	*Short text describing threat*	*Citation for full text*
A.4.2		
A.5 Security policies (OPTIONAL)		
A.5.1	*Short text describing security policy*	*Citation for full text*
A.5.2		
B Security Objectives		
B.1 Security objectives for the asset		
B.1.1	*Short text describing objective for the asset*	*Citation for full text*
B.1.2		
B.2 Security objectives for the environment		
B.2.1	*Short text describing objective for the requirement*	*Citation for full text*
B.2.2		

C IT Security Requirements			
C.1 Asset security requirements			
C.1.1 Asset security functional requirements			
C.1.2 Asset security assurance requirements			
C.1.2.1	*Short text describing security assurance requirement*	*ISO15408 [i.18] class*	*Citation for full text*
C.1.2.2			
C.2 Environment security requirements (OPTIONAL)			
C.2.1	*Short text describing security environment requirement*	*ISO15408 [i.18] class*	*Citation for full text*
C.2.2			

D Application notes (OPTIONAL)
E Rationale
The eTVRA should define the full rational, if this is true only a citation (reference) to the full text is required

History

Document history		
V2.1.1	July 2008	Publication