# 3GPP TR 22.984 V0.3.0 (2008-11)

*Technical Report*

Keyword
<keyword[, keyword]>

## 3rd Generation Partnership Project;
## Technical Specification Group Services and System Aspects;
## Unauthenticated Packet Switched (PS) emergency calls
## (Release 9)

*Remove GSM logo from the cover page for pure 3rd Generation documents.*

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

*Select keywords from list provided in specs database.*

***3GPP***

Postal address

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

Internet
http://www.3gpp.org

# Contents

# Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

*This clause is optional. If it exists, it is always the second unnumbered clause.*

# 1 Scope

The present document gives an overview of the problems related to Unauthenticated PS based Emergency Calls (UAPSEC) and provides information on this topic in comparison to the existing unauthenticated CS based emergency call.

Major areas of work the document takes into account are security aspects, architectural aspects and signalling aspects. It also considers the case where the subscriber has got a PS subscription but no subscription to IMS services.

The document explains on the differences between the scenarios that allowed unauthenticated CS emergency calls without encountering too big problems and the scenarios that make Unauthenticated PS based Emergency Calls different in this respect.

It elaborates on these new scenarios, for example on the Distributed Denial of Service Attacks (DDOS) scenario.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

*It is preferred that the reference to 21.905 be the first in the list.*

# 3 Definitions, symbols and abbreviations

*Delete from the above heading those words which are not applicable.*

*Subclause numbering depends on applicability and should be renumbered accordingly.*

## 3.1 Definitions

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

*Definition format*

***<defined term>****: <definition>.*

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

*Symbol format*

| | |
|---|---|
| <symbol> | <Explanation> |

## 3.3 Abbreviations

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

**UACSEC**: Unauthenticated Circuit Switched Emergency Call.

**UAPSEC**: Unauthenticated Packet Switched Emergency Call

# 4 Usage Scenarios and Frame Conditions

## 4.1 Classical unauthenticated CS based emergency call

Traditional mobile CS networks support unauthenticated emergency calls. As a network option this mechanism can be switched off.

### 4.1.1 Intended usage scenario for UACSEC

This type of emergency call will be selected by the terminal equipment in several cases, for example:

- when there is no SIM or UICC inserted in the terminal

- when the SIM or UICC is not valid e.g. when:

  - Subscription is expired

  - There is no roaming agreement between the Home PLMN and the visited PLMN

The reason for implementing support for unauthenticated CS emergency calls can be better understood when looking at the situation of and expectations on GSM networks when they were designed and deployed in the late 1980s.

The radio coverage in the early days of GSM networks was very limited especially during the ramp up of the networks, and national roaming in many of the countries was - and still is - not allowed by regulation. Thus, for the case when there was no coverage of the HPLMN at one location the terminal is allowed to use one of the PLMNs present even if there is no roaming agreement, to set up an unauthenticated CS emergency call. Furthermore, phones and subscriptions at that time were expensive so one usage scenario the designers and regulators had in mind was to allow the use of a phone without a SIM card e.g. stored in the car's glove box for emergency calling.

### 4.1.2 Usage of UACSEC

Soon after GSM networks were up and running it was recognised that the UACSEC mechanism was used in a way it was not intended for. For example, checking the function of a mobile phone without a SIM/UICC can easily be done by initiating an UACSEC. This caused several countries to switch off the UACSEC mechanisms soon after the start of the networks. In countries still allowing UACSEC a large percentage of emergency calls received by the PSAPs are "rogue" UACSEC-. However, several countries value the ability to place emergency calls without a subscription and are willing to tolerate the abuse in order to provide access to the emergency services.

Due to the unauthenticated and thus anonymous nature of this call it is difficult if not impossible to initiate a call back to the caller from the PSAP. On the other hand, the IMEI is available to the network so there is some degree of traceability and filtering available for UACSEC.

The idea of an emergency phone e.g. in the glove box has proven to be of limited benefit.

One benefit UACSEC still adds is in areas of fringe radio coverage, when national roaming is not allowed, the terminal then can make use of another PLMN, if available.

## 4.2 PS based unauthenticated emergency call

### 4.2.1 Usage scenario for UAPSEC

The PS environment may be different than that of CS. In the beginning of PS based communication there will be CS based networks around to support unauthenticated emergency calls using the mechanisms described in the chapters above. This also applies for countries where no 3GPP CS based access technology is available, usually the phone will be a dual mode phone and can handle such request in a similar manner. The usage of single mode terminals only makes sense when sufficient coverage is given, see below or for example with a data card for a laptop.

For CS and PS capable devices, the only scenarios when UAPSEC adds benefit is when there will be PS-only networks and no CS based networks as fall-back around anymore or when a roaming device with a supported PS technology but not a supported CS technology.

At that time when there will be only PS networks, more or even all people will own at least one, thus the requirement from that to support UAPSEC is not justified. Furthermore, when networks will migrate from CS infrastructure to PS only infrastructure the dependency of subscribers on the radio coverage will be that high that operators will have to provide better or at least equal to the CS network radio coverage otherwise the subscribers will not go for PS-only networks. Thus the point of fringe radio coverage will be of low relevance in PS-only scenario.

The scenario when the PS-only HPLMN network has no coverage at a certain location but another PS-only PLMN has and there is no roaming agreement between these networks does not necessarily require real unauthenticated mechanisms to be used. The terminal has got a valid and unique identity that could be used for setting up an emergency call if the PLMN allows national roaming in case of emergency call, this would also greatly facilitate call-back and identification of the caller. For the PLMN to allow this, however, limited roaming mechanisms need to be put in place where the HPLMN can authenticate the UE identity for emergency call purposes.

For the use cases described above, where the terminal only has PS coverage, some operators believe current regulatory requirements are applicable to PS networks as well and therefore are obliged to support PS mode UAPSEC. For example, regarding the US Code of Federal Regulation (47 CFR § 20 are the regulations for commercial mobile radio services) with respect to emergency calls from unauthorized handset users/non-subscribers, the Commission's rules require wireless carriers to forward all emergency calls to public safety answering points ("PSAPs"), including calls from non-subscribers, this assumes the caller's phone uses an RF protocol that is compliant with the serving carrier's. There is no exception to this requirement for PS technologies. At the same time, the Commission's rules in 47 CFR § 20.18(d)(2) recognize that a wireless carrier may not be able to provide a non-subscriber's call back information to PSAPs, since the carrier may not have access to the non-subscriber's phone number.

## 4.3 Subscription Aspects

Editor's Note: To address aspects such as only a PS subscription but no IMS subscription here

# 5 Architectural Considerations

Editors Note: SA2 and possibly CT groups to plug-in their findings here

# 6 Security Considerations

Editors Note: SA3 to plug-in their findings here

# 7 Conclusion

Editors Note: Add some text proposing the best way forward from 3GPP's point of view by referring to the statements made in the sections above

# Annex <X>: Change history

*It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:*

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New |
| *2008-07* | | | | | *Draft Skeleton input to SA1#41.* | | *0.0.0* |
| *2008-07* | | | | | *Comments of SA1#41 included* | *0.0.0* | *0.1.0* |
| *2008-10* | | | | | *Results from SA1#42 included* | *0.1.0* | *0.2.0* |
| *2008-11* | | | | | *Results from SA1#43 included* | *0.2.0* | *0.3.0* |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Editor's Note: For the sake of convenience the corresponding WID is copied here for reference, it will be deleted when the document is going to version 9.0.0.

## Work Item Description

### Title

Feasibility Study on Unauthenticated PS Emergency Calls (FS_UAPSEC)

Is this Work Item a "Study Item"? (Yes / No):...................yes

### 1 3GPP Work Area

| | |
|---|---|
| X | Radio Access |
| X | Core Network |
| | Services |

### 2 Linked work items

*None*

## 3 Justification

On the standardisation of packet switching based architectures it was initially planned to support the authenticated as well as the unauthenticated emergency call also on the PS architecture provided it supports speech communication at all.

The authenticated PS emergency call, ie a call placed by a terminal containing a valid subscription, can be standardised with moderate effort and minor – if any – network security related issues.

In the process of standardisation, however, the unauthenticated packet switching based emergency call turned out to be a major obstacle due to the problems it causes for the security of the network.

## 4 Objective

The TR shall give an overview of the problems related to UAPSEC and provide information on this topic to regulatory authorities.

Major areas of work the TR has to take into account are security aspects, architectural aspects and signalling aspects.

The TR shall also consider the case where the subscriber has got a PS subscription but no subscription to IMS services.

The TR shall explain on the differences between the scenarios that allowed unauthenticated CS emergency calls without encountering too big problems and the scenarios that make UAPSEC different in this respect.

The TR shall elaborate on these new scenarios, for example on the Distributed Denial of Service Attacks (DDOS) scenario.

It shall be considered whether collecting statistics on the use of CS unauthenticated emergency calls would facilitate the intention of the TR and collect this data if considered so.

The TR should amongst others also

- state on how to handle emergency calls for UE's that are subscribers of another operator with no roaming agreement or terminals with a UICC that is not valid.
- make a statement on its applicability to I-WLAN and LTE

## 5 Service Aspects

*None*

## 6 MMI-Aspects

*None*

## 7 Charging Aspects

*None*

## 8 Security Aspects

*Security aspects need to be identified, see objective section*

## 9 Impacts

| Affects: | UICC apps | ME | AN | CN | Others |
|---|---|---|---|---|---|
| Yes | | | | | |
| No | X | X | X | X | X |
| Don't know | | | | | |

## 10 Expected Output and Time scale (to be updated at each plenary)

| New specifications<br>[If Study Item, one TR is anticipated] | | | | | | |
|---|---|---|---|---|---|---|
| Spec No. | Title | Prime rsp. WG | 2ndary rsp. WG(s) | Presented for information at plenary# | Approved at plenary# | Comments |
| TR 22.9XX | Study on Unauthenticated PS Emergency Calls (UAPSEC) | SA1 | SA2, SA3, CT1 | SA#42 | SA#44 | It is expected secondary groups only start when finished their Rel-8 work |
| | | | | | | |

| Affected existing specifications<br>[None in the case of Study Items] | | | | |
|---|---|---|---|---|
| Spec No. | CR | Subject | Approved at plenary# | Comments |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 11 Work item rapporteur(s)

Juergen Merkel, Nokia Siemens Networks

## 12 Work item leadership

SA1, (SA2, SA3, CT1)

## 13 Supporting Companies

Nokia Siemens Networks, BT, T-Mobile, Vodafone, Qualcomm.

## 14 Classification of the WI (if known)

| | |
|---|---|
| X | Study Item (no further information required) |
| | Feature (go to 14a) |
| | Building Block (go to 14b) |
| | Work Task (go to 14c) |

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)