ETSI SR 002 777 V1.1.1 (2010-07)

Special Report

Emergency Communications (EMTEL);
Test/verification procedure for emergency calls

Reference
DSR/EMTEL-00014

Keywords
conformance, CTS, emergency, location, testing

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

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 Special Report (SR) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

1 Scope

The present document outlines a test procedures for emergency calls from individuals (citizens) to authorities.

In order to test (in a given environment) the emergency call/messaging capability of the current operator it would be favourable to have a test procedure, i.e. to be able to call a "test" address not invoking a real emergency call. Such a test could be initiated either manually or automatically (e.g. with a given periodicity). It is advised to observe the threats in security vulnerability and of network overload. Such a procedure should work both for calls from CS and PS networks (wired or wireless). The testing functionality may also be utilized in order to facilitate other location based/dependent services as described in TS 123 271 [i.8]. As for emergency services, both CS and PS PSAPs should be catered for.

The aim of the present documents is to make a contribution to an overall functional architecture and specification for such a test service.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

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 necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 123 167: "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167)".

[i.2] ETSI TR 102 180: "Emergency Communications (EMTEL); Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".

[i.3] ETSI TR 102 476: "Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities".

[i.4] IETF [draft-ietf-ecrit-phone-bcp]: "Best Current Practice for Communications Services in support of Emergency Calling".

NOTE: For the status of work items within the IETF ECRIT working group please see: http://tools.ietf.org/wg/ecrit/

[i.5] IETF [draft-ietf-ecrit-framework]: "Framework for Emergency Calling using Internet Multimedia".

[i.6] IETF [draft-schulzrinne-ecrit-unauthenticated-access]: "Extensions for Unauthenticated & Unauthorized Devices".

[i.7] IETF RFC 5222: "LoST: A Location-to-Service Translation Protocol".

[i.8] ETSI TS 123 271: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Functional stage 2 description of Location Services (LCS) (3GPP TS 23.271)".

[i.9] ETSI TS 136 305: "LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN (3GPP TS 36.305)".

[i.10] ETSI TS 125 305: "Universal Mobile Telecommunications System (UMTS); Stage 2 functional specification of User Equipment (UE) positioning in UTRAN (3GPP TS 25.305)".

[i.11] ETSI TS 143 059: "Digital cellular telecommunications system (Phase 2+); Functional stage 2 description of Location Services (LCS) in GERAN (3GPP TS 43.059)".

[i.12] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", November 2006.

[i.13] IETF RFC 3825: "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", July 2004.

[i.14] IETF [draft-ietf-geopriv-http-location-delivery]: "HTTP Enabled Location Delivery (HELD)", Barnes, M., Winterbottom, J., Thomson, M., and B. Stark.

NOTE: For the status of work items within the IETF GEOPRIV working group please see : http://tools.ietf.org/wg/geopriv/

[i.15] IEEE 802.1AB: "Station and Media Access Control Connectivity Discovery", 2009.

[i.16] IETF [draft-ietf-geopriv-arch]: "An Architecture for Location and Location Privacy in Internet", R. Barnes, M. Lepinskim, A. Cooper, J. Morris, H. Tschofenig, H. Schulzrinne.

[i.17] IETF RFC 3261: "SIP: Session Initiation Protocol", J. Rosenberg et al., June 2002.

[i.18] ETSI TS 122 101: "Universal Mobile Telecommunications System (UMTS); LTE; Service aspects; Service principles (3GPP TS 22.101)".

[i.19] ETSI TR 121 905: "Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.20] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 123 167 [i.1], TR 102 180 [i.2], TS 123 271 [i.8], TR 121 905 [i.19] and the following apply:

Access Network Provider (ANP): provides physical access to the network

dispatch location: location used for dispatching responders to the person in need of assistance

NOTE: According to [i.5] "the dispatch location must be sufficiently precise to easily locate the caller; it typically needs to be more accurate than the routing location".

IP service Provider (ISP): provides access to the IP network, allocates IP addresses to users and route their traffic

location configuration: location configuration is the process in which an endpoint learns its physical location

Location Configuration Protocol (LCP): protocol used by an endpoint to learn its location

location conveyance: location conveyance delivers location information to another element

location determination: location determination finds where an endpoint is physically located

EXAMPLE: The endpoint may contain a GPS receiver used to measure its own location or the location may be determined by a network administrator using a wiremap database.

Location Information Server (LIS): location Information Server that stores location information for retrieval by an authorized entity

NOTE: The LIS maps network addresses or equipment IDs to physical locations.

No Access Authorization (NAA): current access network requires access authorization and the caller does not have valid user credentials

NOTE: This includes the case where the access network allows pay-per-use, as is common for wireless hotspots, but there is insufficient time to pay for access.

No Voice service Provider (NVP): caller does not have a Voice (over IP) Service Provider (VSP) at the time of the call

physical location: physical location, as used here is where a person or device is located in physical space, described by a coordinate system or a civic address

NOTE: It is distinguished from the network location, described by a network address.

routing location: routing location of a device is used for routing an emergency call and may not be as precise as the Dispatch Location

NOTE: These definitions are adopted from [i.5] - location, as referred to here, normally refer to physical location.

User Agent (UA): In SIP a user agent is a set of applications running in the UE (the user equipment)

NOTE: This set consists of two units:

1) a user agent client: a caller application that initiates and sends SIP requests; and

2) a user agent server: an application that receives and responds to SIP requests on behalf of clients, accepts, redirects or refuses calls.

Voice Service Provider (VSP): provides a VoIP service

Zero-Balance voice service Provider (ZBP): caller has valid credentials with a VSP, but is not allowed to place calls, e.g. because the user has a zero balance in a prepaid account

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 123 167 [i.1], TS 122 101 [i.18], TR 121 905 [i.19] and the following apply:

ANP Access Network Provider
CS Circuit Switched
DHCP Dynic Host Configuration Protocol
GSM Global System for Mobile Communications

NOTE: Previously: Group Special Mobile.

IMS Internet Protocol (IP) Multimedia Subsystem
ISDN Integrated Services Digital Network
ISP Internet Service Provider
LCP Location Configuration Protocol
LCS Location Services
LIS Location Information Server
LLDP Link Layer Discovery Protocol

NOTE: See IEEE [i.15].

LoST	Location to Service Translation

NOTE: See IETF [i.7].

LTE	Long Term Evolution
NAA	No Access Authorisation

NOTE: See clause 3.1.

NVP	No Voice service Provider
P-CSCF	Proxy Call Session Control Function
PS	Packet Switched
PSAP	Public Safety Answer Point
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
UA	User Agent
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VoIP	Voice over IP (service)
VSP	Voice Service Provider
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
ZBP	Zero-balance VoIP Provider

NOTE: See clause 3.1.

4 Testing functionality

Testing functionality may differ according to type of User Equipment:

- Only access from UEs with a subscription is considered. That is: the UE/user is known to a service provider, the subscription account may be zero (Zero-balance Voice Service provider), but the UE can be identified as a valid entity in the network. Emergency call ID/authentication may optionally be based on WLAN/WiFi authentication provided by/through the Access Provider (EU regulation, Directive 2006/24/EC [i.20], demand all public available communication operators to keep track of and store information about users and their sessions).

The following cases/scenarios are identified:

1) Emergency Calls/Sessions in Packet Switched Networks.

2) Emergency Calls in Circuit Switched Networks.

3) Emergency Calls/Sessions originated in a PS network, with a PSAP in the CS domain.

4) Emergency Calls originated in a CS network, with a PSAP in the PS domain.

4.1 Emergency Calls/Sessions in Packet (IP) based Networks

In this case it is assumed that the SIP protocol forms the basis for signaling (optionally H323), and that the whole session utilize resources in the PS domain. For scenarios see TR 102 476 [i.3]. The document gives an overview of standardisation activities and summarises different methods for VoIP providers to deliver emergency communications services.

Type of terminals and their capabilities:

i) "Softphone" IP phone realized as an application running on a device with suitable resources (display, keyboard, computing power and connection).

ii) "Native" IP phone (as a specialized physical unit) with suitable display(s), keys, etc.

iii) Ordinary telephone handset (or equivalent) with or without a alpha/numerical display connected to IP based service through an adapter.

The ANP, ISP and VSP functionality may be realized by different organizations. Operators like Skype, Telio and Vyke, offer Voice over IP services without any contract with the ISPs or ANPs. It can be argued that ETSI may not as an standardisation organisation, provide or specify emergency call functionality for such providers. However the present document tries also to discuss possible solutions and restrictions as they may appear to these providers, based on standard sets of public available protocols.

According to proposals made by the IETF [i.4] paragraph 5, Requirement ED 3: "Endpoints SHOULD recognize dial strings of emergency calls. If the service provider always knows the location of the device, then the service provider could recognize them" (End points in this context is an UE), This means also that the UE need to know local emergency dial strings (e.g. 911 in the US and 112 and others in Europe).

The service provider should provide the SIP based UA with a set of emergency numbers according to the regulation of the area in which the subscriber is normally situated (corresponding to home domain). This set of emergency number should be drawn from the set demanded possible also for 3GPP equipment as specified in TS 122 101 [i.18], in the section covering emergency calls. A user that is connected to a "visiting" access network (that is an access network in an area not corresponding to "home domain") should still be able to use his home emergency numbers; they should then first be interpreted using a translating from "home domain" valid numbers to equivalent numbers in the visited area. Then afterwards the correct termination address should be established by utilising a LoST (Location to Service Translation) function as specified in [i.7]. This translation should preferably be undertaken in the registration phase and the result downloaded to the UA, as this will enable the terminal (UA) itself to correctly address the local services in case of a emergency call.

Although some countries have adopted only one emergency number, many others have a list of options, in most cases at least one for police, a second for fire and third for medical emergencies.

For future SIP phones of type i or ii above it is envisaged that the translation between home and national emergency numbers can be done by the UE in a fashion equivalent to that specified for mobile phones in [i.18]. This means that "standard" emergency signalling can be used in handling of such calls in the visited network. If (especially in a transition phase) the terminal does not have this capability, the translation can be done by the P-CSCF provided it is able to relate the dialled number to a given type of emergency number (e.g. medical assistance) valid in the caller's home domain.

The following functions are to be tested:

1) That the UE from its current position are able to call a suitable "112" or "911" (whatever is applicable according to the region given) PSAP/Emergency Centre.

2) The callers location information as it is given to the PSAP.

3) That it is possible for the PSAP/Emergency Centre to make a return call to the UE.

4) (Optionally) Exercising translation between national emergency numbers as described above. In this case valid local emergency numbers has to retrieved by a translation mechanism. This would allow e.g. a Norwegian subscriber to dial "113" on his own terminal in order to call the "118" (Medical Emergency) in Italy.

In order to accomplish 1, the switching system needs to know the location of origin (i.e. the routing location of the caller) with a sufficient exactness, in order to map it to the correct PSAP. For different technologies and methods to obtain this please refer to: TS 136 305 [i.9], TS 125 305 [i.10] and TS 143 059 [i.11]. Optionally the UE can forward the information in e.g. a SIP Invite message,[i.5]. In this case the UE may have obtained this information from local GPS instrumentation or it might be obtained by "location configuration protocol" i.e. network assisted means, for example from an DHCP server in civic [i.12] and/or geo [i.13] forms, a http based location server [i.14] or the first level switch's LLDP server [i.15].

Privacy requirements are treated in [i.16]. Generally we can differentiate localization in two classes according to "exactness":

a) routing location;

b) dispatch location.

The latter demands generally more accuracy, but can be provided with relaxed time restrictions (A needs to be decided in say 5 seconds to 10 seconds, whereas B, the need for the exact address, in most instances can be deferred some minutes -provided a coarse estimate can be given early).

On the other side, if the exact localization can be retrieved with no excessive delay, it is no need to wait.

Both routing and dispatch localization are to be tested. The user can optionally be asked to provide supplementary information to the system about his/her location (this may prove practical in cases where the UE has been moved to a new place where it may reside for a long time (permanent or semi-permanent move) and also for nomadic applications (the UE may remain in a location for some hours).

When a VoIP user has moved, there is a need for a new registration/location update.

Such a registration is usually done automatically when the application is initiated at the device. It is also recommended that the UE agent collect information about its environment in order to launch a re-register when e.g. its IP (c/o) address has changed. It should also be possible to initiate a re-registration/update manually.

For the emergency call functional test, this could be scheduled always to take place immediately after a (re) registration, or as an option be launched manually. Also for "peace of mind" for the user, it should be possible to launch such a test manually, at any instance in time.

NOTE 1: It might however be necessary to limit the rate of tests made from individual users in order to limit overload and avoid denial of service attacks.

As an illustrative sample it is assumed that the UE/application has a feature button reading: "Location Update/Emergency Call Test". (This could correspond to calling the code "*112#" on a phone with only numerical display).

The corresponding sequence of messages/actions could be:

- Location update, test call initiating (automatically):
    1) SIP re(registration request).
    2) Location update (geographical update) request.
    3) Initiate emergency call test.
    4) Render result.
- Possible information outcome, shown on display or read in the telephone:
    a) "Test not possible/emergency call functions not implemented"
    b) "Your test call is connected to emergency centre in <geographical name>, your estimated location is <estimated location>, if this is correct press OK, If not please make corrections by e.g.:
        1) Keying in the civic address (on terminals with alphanumerical keying);
        2) Using a cursor to place a pin on a map (option on equipment with graphical capabilities); or
        3) Telling the address to an operator.

(Options will be based on capabilities on the handset).

There might also occur a situation where the system is unable to confirm a location, but where the subscriber may be assumed to be located in a country or region based on e.g. earlier registrations. In this case an optional answer b) might be given. e.g.:

b-bis) "Your test call is connected to an emergency center in <country/regional>, we might need to know your location: Please make corrections by (same as above).

Message after correction: Your are located at <location given>, emergency calls from this location will be connected to the emergency centre in < geographical name>, if this is correct press OK, if NOT make a new correction (see above) or press "Cancel" (give up).

NOTE 2: As a minimum requirement a correct routing address should be established: A convenient and sufficient way to do this could be to provide the postal zip code (this zip code is in many countries given as numerical string, which could be keyed in on the handset).

It is proposed that the computed location of the UE is transferred and stored at the registrar (the registrar is a functional unit in the SIP specification [i.17]), it can also be stored in UE equipment.

If manual/user-assisted corrections was used, this fact should be recorded along with the location information.

A system with no/minor automatic means to find the location. could rely on manual/user assistant location update only:

- First try:
  - Result rendered: <Subscription address>.
  - Manual correction: Current (correct) location/address of the user.
- Next try:
  - Result rendered: Registered location/address of the user.
  - Manual correction (if needed).

4.2 Emergency Calls in Circuit Switched Networks

It is assumed that the call is completed within the CS domain (both the caller and the PSAP resides in this domain).

Optional transit via a PS domain may be catered for by gateway functionality.

4.2.1 PSTN/ISDN

Assumptions: simple telephone handsets with or without an alphanumeric display.

Test start: Go off hook, call *112#.

Result/answer given by voice announcement:

- Either:

  "Emergency call enabled. You are at < street address, apartment> You will be served by < > emergency centre. If this is information is not reasonable, please press "1", else hang up".

NOTE: Corrections supplied by a user, may need some sort of verification, authentication.

- Or:

  Manual corrections to be facilitated by operator assistance or optionally be provided by on-site workers initiating the test. These authorized persons may correct location data in the LIS for the local access network via a secured data connection.

4.2.2 Mobile Phone (3GPP)

The present document refers to Mobile Equipment (ME) as defined in TS 122 101 [i.18] as opposed to In Vehicle Systems (eCall terminal and associated sub-systems in vehicle). This technical specification demands the Home Domain Environment Operator to specify preferred emergency numbers and store these in the SIM/USIM. The ME may read this and use any entry to set up an emergency call. The association between any emergency call number and the emergency call type is to be provided , i.e. programmed by the Home Environment Operator into the SIM/USIM (e.g. 100 Ambulance and Fire Brigade in Belgium). Assuming the equipment adheres to this technical specification (TS 22.101), it should be possible to initiate and test an emergency call feature by dialling *xxx# where xxx represent any appropriate emergency number specified by means given here.

E.g. test start: Go off hook call *112# or *911# (or *999#).

Result/answer given by voice announcement, as in clause 4.2.1. together with a message (SMS?) that renders the resulting type of emergence service call and the location of the UE as observed and/or estimated by the receiver.

History

Document history		
V1.1.1	July 2010	Publication