

ecrit
Internet-Draft
Expires: December 27, 2006

B. Rosen
NeuStar
J. Polk
Cisco Systems
June 25, 2006

Best Current Practice for Communications Services in support of
Emergency Calling
draft-rosen-sos-phonebcpr-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 27, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Requesting help in an emergency using a communications device such as a telephone or mobile is an accepted practice in most of the world. As communications devices increasingly utilize the Internet to interconnect and communicate, users will continue to expect to use such devices to request help, regardless of whether or not they communicate using IP. The emergency response community will have to

Internet-Draft

Emergency Call Phone BCP

June 2006

upgrade their facilities to support the wider range of communications services, but cannot be expected to handle wide variation in device and service capability. The IETF has several efforts targeted at standardizing various aspects of placing emergency calls. This memo describes best current practice on how devices and services should use such standards to reliably make emergency calls

Table of Contents

1.	Requirements notation	3
2.	Introduction	3
3.	Which devices and services should support emergency calls . .	4
4.	Determining Location	4
5.	Determining an emergency call	6
6.	Session Signaling	8
6.1.	SIP signaling requirements for User Agents	8
6.2.	Mapping from Location to a PSAP URI	9
6.3.	Routing the call	9
6.4.	Responding to PSAP signaling	10
6.5.	Disabling of features	10
7.	Security Considerations	11
8.	Normative References	11
	Authors' Addresses	13
	Intellectual Property and Copyright Statements	14

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

2. Introduction

In this memo, an emergency call refers to a communications session established by a user to a "Public Safety Answering Point" (PSAP) which is a call center established by response agencies to accept emergency calls. We differentiate such calls from other sessions which are created by responders using public communications infrastructure often involving some kind of priority access as defined in Emergency Telecommunications Service (ETS) in IP Telephony [[RFC4190](#)]. While current PSAPs are limited to voice sessions, often with the additional capability to serve hearing impaired users with text based "TTY" devices, envisioned upgrades to PSAPs will allow sessions with audio, video, and several kinds of text including interactive text [[RFC4103](#)] and Instant Messages. and [I-D.ietf-sipping-toip]

Making an emergency call involves the use of location information, referring to the physical location of the caller. Location is used within the emergency calling system to route a call to the correct PSAP, as well as by the PSAP to choose the correct responder, and direct them to the person in need of assistance.

The steps involved in an emergency call from an IP based device are (with a rough ordering of operation)

1. Device connects to access network, and obtains initial location
2. User dials visited location's emergency number
3. User device identifies call as emergency call
4. User device includes location indication (by value or by reference) in the call set-up messaging

5. emergency call set-up is routed to appropriate PSAP based on location of the caller
6. call is established with PSAP
7. caller's location is presented to PSAP operator for dispatch

As a quick overview for a typical Ethernet connected telephone using SIP signaling:

- o the phone "boots" and connects to its access network
- o the phone would get location from the DHCP server [or an L7 server].

- o It would use "urn:service:sos" as the URI of an emergency call.
- o It would put its location in the SIP INVITE as a PIDF-LO in the body of the INVITE (or a reference to location in a Location header) and forward the call to its first hop proxy.
- o The proxy recognize the call as an emergency call.
- o The proxy would determine the PSAP's URI by using the [I-D.ietf-ecrit-lost] mapping server from the location provided in the signaling
- o The proxy would use a SIP SRV record in the domain of the resulting PSAP URI to determine where to send the call.

The (upgraded) PSAP would answer the call as SIP, with location included.

[RFC4504] details Best Current Practice for SIP user agents. This memo can be considered an addition to it for endpoints.

3. Which devices and services should support emergency calls

Although present PSAPs have only support for voice calls placed through PSTN facilities or systems connected to the PSTN, future PSAPs will support Internet connectivity and a wider range of media types. In general, if a user could reasonably expect to be able to call for help with the device, then the device or service should support emergency calling. Certainly, any device or service that looks like and works like a telephone (wired or mobile) should support emergency calling, but increasingly, users have expectations that other devices and services should work.

Using current (evolving) standards, devices that create media sessions and exchange audio, video and/or text, and have the capability to establish sessions to a wide variety of addresses, and communicate over private IP networks or the Internet, should support emergency calls.

4. Determining Location

With Internet based communications services, determining where the caller is located is more problematic than in PSTN and mobile systems. Existing wired phones are tethered with a wire that is connected directly to a call control device, a circuit switch. Cellular phones are tethered via a radio channel to a cell tower, which connects that cell phone to a circuit switch. The primary difficulty with IP based phones is that the connectivity, whether wired or radio channel, is decoupled from the call control device. The communications service may not have any relationship with the

access network carrier, and, with NAT and VPN tunnels, may have no way to even find out who the access carrier is.

For this reason, standards have been created for endpoints (devices) to obtain location information. The endpoint is a subscriber to both the access network and the communications service, and thus is in a position to obtain its location from the access network, and supply it to the communications service.

DHCP [[RFC2131](#)] has been enhanced to provide the location of a device. [[RFC3825](#)] describes how a geo-location (lat/lon/alt) may be obtained and [[I-D.schulzrinne-geopriv-dhcp-civil](#)] describes how a civic (street address) location can be obtained via DHCP.

[Placeholder for HELD, LCP or other L7 location determination methods]

For devices that operate on a network where the network operator controls the specification of every device connected to that network that could be used for emergency calls, the method by which location is determined need not be an IETF standard, but can be any method that achieves the desired result. Such a method **MUST** be specified,

and every device MUST support it.

For devices that operate in a network where the network operator controls the specification of every device connected to that network, but the network attachment supports upstream networks to which communications devices are connected (such as any network that supports Ethernet connected telephones and terminal adapters), the method by which location is determined need not be an IETF standard, but can be any method which achieves the desired result. However, the network attachment MUST support [both] DHCP [AND L7] for upstream communications devices to obtain location. For smaller interior (e.g, LAN) networks, the DHCP [or L7] server should simply repeat the location obtained from the access network. For larger networks, other mechanisms, such as a DHCP Relay Agent [[RFC3046](#)] MUST be used to provide more accurate location of endpoints.

For devices that operate on a network where the network operator does not control the specification of every device connected to the network, DHCP [or L7] MUST be supported on the network.

Note: Self Reported location is generally unacceptable in emergency calls, although it is being used prior to automatic location determination schemes being fielded. Local laws may govern what is acceptable in any country or area.

Devices SHOULD get location immediately after obtaining local network

configuration information. It is essential for the location to be determined BEFORE any VPN tunnels are established. It is equally essential that this location information is **not** overwritten by any process engaged from establishing a VPN connection. In other words, the established VPN to Chicago from the device in Dallas should not overwrite the location of "Dallas".

It is desirable that location information be periodically refreshed. For devices which are not expected to roam, refreshing on the order of once per day is recommended. For devices which roam, refresh of location should be more frequent, with the frequency related to the mobility of the device and the ability of the access network to support the refresh operation. There can be instances in which a device is aware of when it moves, for example when it changes access points. When this type of event occurs, the device SHOULD refresh

its location.

It is desirable for location information to be requested immediately before placing an emergency call. However, if there is any delay in getting more recent location, the call SHOULD be placed with the most recent location information the device has. It is recommended that the device not wait longer than 500 ms to obtain updated location, and systems should be designed such that the typical response is under 100ms. These numbers are empirically derived, but are intended to keep total call signaling time below 2 seconds. There are conflicts between the time it takes to generate location when measuring techniques are used and the desire to route the call quickly. If an accurate location cannot be determined quickly, a rough location SHOULD be returned within 500ms which can be used to route the call.

[5.](#) Determining an emergency call

An emergency call is distinguished by the device (or a downstream element) by an "address", which in most cases for Internet connected devices is still a dialstring, although other user interfaces may be used.

Note: It is undesirable to have a single "button" emergency call user interface element. These mechanisms have a very high false call rate. PSAPs prefer devices to use their local emergency call dialstring.

While in some countries there is a single 3 digit dialstring that is used for all emergency calls (i.e. 911 in North America), in some countries there are several 3 digit numbers used for different types of calls. For example, in Switzerland, 117 is used to call police,

118 is used to call the fire brigade, and 144 is used for emergency medical assistance. In other countries, there are no "short codes" or "service codes" for 3 digit dialing of emergency services and local (PSTN) numbers are used.

[I-D.schulzrinne-sipping-service] introduces a universal emergency service URN scheme. On the wire, emergency calls SHOULD include this type of URI (in for example, the To: field of a SIP call). The

scheme includes a single emergency URN (urn:service:sos) and responder specific ones (urn:service:sos.police). Using the service:sos URN scheme, emergency calls can be recognized as such throughout the Internet.

Devices MUST use the service:sos URN scheme to mark emergency calls.

To determine which calls are emergency calls, some entity needs to map a user entered dialstring into this URN scheme. A user may "dial" 1-1-2, but the call would be sent to urn:service:sos. This mapping is ideally performed at the endpoint device, but may be performed at an intermediate entity (such as a SIP proxy server).

Note: It is strongly RECOMMENDED that devices recognize the emergency dialstring(s) and map to the universal emergency URN. If devices cannot do "dial plan interpretation", then the first signaling aware element (first hop proxy in SIP signaled devices) SHOULD do the mapping. It is important to not require a large number of active elements handle a call before it is recognized as an emergency call

In systems that support roaming, there may be a concept of "visited" and "home" networks. Even when there is not a "visited network", the user may be roaming (or nomadic) in a different country from their home. This gives rise to the problem of which dialstring(s) to recognize, the "home" or "visited"? While it is desirable that the "home" dialstrings be recognized, it is required (by law in some countries) that the "visited" dialstrings be recognized. Dial plan interpretation may need to take "visited" emergency dialstrings into account.

To give an example of this difference in dialstrings: If the device is from North America, the home and visited emergency dialstring is "9-1-1". If that device roams to the UK, the home emergency dialstring is still "9-1-1", but the visited emergency dialstring would become "9-9-9". If the device roams to Paris, the home dialstring remains the same, "9-1-1", but the visited dialstring changes from 999 to "1-1-2".

The home emergency dialstrings MAY be provisioned into the device (or other element doing dialstring to universal emergency call URN

mapping). The visited dialstring MAY be discovered by a lower layer

protocol that is used by the access network, such as DHCP, or with a higher layer protocol like SIP (using a REGISTER Request) or HTTP (using a GET Request) once the device learns its location. It could be that the device knows more than one way to learn the visited emergency dialstring, and using the methods in some configured order (until an answer is received).

6. Session Signaling

SIP signaling [[RFC3261](#)] is expected to be supported by upgraded PSAPs. Gateways MAY be used between Internet connected devices and older PSAPs. Some countries may support other signaling protocols into PSAPs.

6.1. SIP signaling requirements for User Agents

Initial signaling Method is INVITE. The Request-URI MUST be a service:sos URN unless the device does not do emergency dialstring interpretation. If the device does not do emergency dialstring interpretation, the expectation is that the Request-URI will be a tel URI with the dialed digits, or a sips uri with the dialed digits and a USER=PHONE parameter (e.g. sips:911@example.com;user=phone). The call would normally be sent to the first hop proxy of the communications service.

1. The To: header MUST be present and SHOULD be the same as the Request-URI
2. The From: header MUST be present and SHOULD be the AoR of the caller. <vspace blankLines="1"/>NOTE: uninitialized devices may not have an AoR available
3. A Via: header MUST be present and SHOULD include the URI of the device
4. A Route header MAY be present if the device has performed a fallback mapping function (see [Section 4](#))
5. Either a P-Asserted-Identity [[RFC3325](#)] or an Identity header [[I-D.ietf-sip-identity](#)], or both, SHOULD be included to identify the sender.
6. A Contact header SHOULD be present (which might contain a GRUU [[I-D.ietf-sip-gruu](#)]) to permit an immediate call-back to the specific device which placed the emergency call.
7. Other headers MAY be included as per normal sip behavior
8. A Supported: header MUST be included with the 'location' option tag, unless the device does not understand the concept of SIP Location ;
9. If the device's location is by-reference, a Location: header MUST be present containing the URI of the PIDF-LO reference for that device;

10. if a device understands the SIP Location Conveyance [[I-D.ietf-sip-location-conveyance](#)] extension and has its location available, it MUST include location either by-value or by-reference. If it is by-value, the INVITE contains a Supported header with a "location" option tag, and a "cidURL" indicating which message body part contains the PIDF-LO. If the INVITE contains a location by-reference, it includes the same Supported header with the "location" option tag, and includes the URI of the PIDF-LO on a remote node in a Location header. [[I-D.ietf-geopriv-pdif-lo-profile](#)] MUST be used
11. If a device understand the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "location" option tag, and not include a Location header, and not include a PIDF-LO message body.;
12. A normal SDP offer SHOULD be included in the INVITE. The offer SHOULD NOT include compressed audio codecs, although a wideband codec offer MAY be included.

Note: Silence suppression (Voice Activity Detection methods) MUST NOT be used on emergency calls. PSAP call takers sometimes get information on what is happening in the background to determine how to process the call.

[6.2.](#) Mapping from Location to a PSAP URI

To route an emergency call, we make use of the [[I-D.ietf-ecrit-lost](#)] mapping service which takes a location expressed by a PIDF-LO and returns one or more PSAP URIs. The request includes the service URN which is used to determine which entity should receive the call. The URI would replace the Request-URI in a SIP INVITE.

User agents that can obtain location information MUST perform the mapping from location information to PSAP URI using [[I-D.ietf-ecrit-lost](#)]. The mapping is performed whenever the UA acquires new location information that is outside the bounds of the current PSAP coverage region specified in the LoST response or the time-to-live value of that response has expired.

To deal with old user agents that predate this specification and with UAs that do not have access to their own location data, proxies that recognize a call as an emergency call that is not marked as such (see [Section 5](#)) or where the Request-URI is a service:sos URN MUST also perform this mapping.

[6.3.](#) Routing the call

Normal routing mechanisms for the specified URI should be used. For

SIP signaled devices, the domain of the URI should be extracted, and the DNS consulted for a sip (or sips) SRV. The resulting NAPTR, if present, should be used for the FQDN of the server.

[6.4.](#) Responding to PSAP signaling

The PSAP is expected to use normal signaling (e.g. SIP) as per IETF standards. Devices and proxies should expect to:

1. Be REFERed to a conference bridge; PSAPs often include dispatchers, responders or specialists on a call.
2. Be REFERed to a secondary PSAP. Some responder's dispatchers are not located in the primary PSAP. The call may have to be transferred to another PSAP. Most often this will be an attended transfer, or a bridged transfer.
3. (For devices that are Mobile) SUBSCRIBE to the Presence of the AoR (or equivalent for other signaling schemes) to get location updates.
4. Support Session Timer (or equivalent) to guard against session corruption

Devices MUST NOT send a BYE (or equivalent for other non-SIP signaling). The PSAP must be the only entity that can terminate a call. If the user "hangs up" an emergency call, the device should ring, and when answered, reconnect the caller to the PSAP.

There can be a case where the session signaling path is lost, and the user agent does not receive the BYE. If the call is hung up, the session timer expires, and 5 minutes elapses from the last message received by the device from the PSAP, the call may be declared lost. If in the 5 minute interval an incoming call is received from the domain of the PSAP, the device should drop the old call and alert for the (new) incoming call.

[6.5.](#) Disabling of features

The device and/or service should disable outgoing call features such as:

- o Call Waiting
- o Call Transfer

- o Three Way Call
- o Flash hold
- o Outbound Call Blocking

The emergency dialstrings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

The device and/or service SHOULD disable the following incoming call features on calls from the PSAP:

Rosen & Polk

Expires December 27, 2006

[Page 10]

Internet-Draft

Emergency Call Phone BCP

June 2006

- o Call Waiting (all kinds)
- o Do Not Disturb
- o Call Forward (all kinds) (if the PSAP calls back within some (30min?) interval)

7. Security Considerations

There are no new security considerations beyond those in the normative references. This memo does not introduce any new protocols; it specifies use of several of them. Implementers are admonished to ,,,

8. Normative References

[I-D.ietf-ecrit-lost]

Hardie, T., "LoST: A Location-to-Service Translation Protocol", [draft-ietf-ecrit-lost-00](#) (work in progress), June 2006.

[I-D.ietf-geopriv-pdip-lo-profile]

Tschofenig, H., "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", [draft-ietf-geopriv-pdip-lo-profile-04](#) (work in progress), May 2006.

[I-D.ietf-sip-gruu]

Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", [draft-ietf-sip-gruu-09](#) (work in progress), June 2006.

[I-D.ietf-sip-identity]
Peterson, J. and C. Jennings, "Enhancements for
Authenticated Identity Management in the Session
Initiation Protocol (SIP)", [draft-ietf-sip-identity-06](#)
(work in progress), October 2005.

[I-D.ietf-sip-location-conveyance]
Polk, J. and B. Rosen, "Session Initiation Protocol
Location Conveyance",
[draft-ietf-sip-location-conveyance-02](#) (work in progress),
March 2006.

[I-D.ietf-sipping-toip]
Wijk, A., "Framework for real-time text over IP using
SIP", [draft-ietf-sipping-toip-04](#) (work in progress),
March 2006.

Rosen & Polk	Expires December 27, 2006	[Page 11]
--------------	---------------------------	-----------

Internet-Draft	Emergency Call Phone BCP	June 2006
----------------	--------------------------	-----------

[I-D.schulzrinne-geopriv-dhcp-civil]
Schulzrinne, H., "DHCP Option for Civil Location",
[draft-schulzrinne-geopriv-dhcp-civil-01](#) (work in
progress), February 2003.

[I-D.schulzrinne-sipping-service]
Schulzrinne, H., "A Uniform Resource Name (URN) for
Services", [draft-schulzrinne-sipping-service-01](#) (work in
progress), October 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol",
[RFC 2131](#), March 1997.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option",
[RFC 3046](#), January 2001.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
A., Peterson, J., Sparks, R., Handley, M., and E.
Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#),
June 2002.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private

Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", [RFC 3325](#), November 2002.

- [RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", [RFC 3825](#), July 2004.
- [RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", [RFC 4103](#), June 2005.
- [RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.
- [RFC4190] Carlberg, K., Brown, I., and C. Beard, "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony", [RFC 4190](#), November 2005.
- [RFC4504] Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration", [RFC 4504](#), May 2006.

Rosen & Polk

Expires December 27, 2006

[Page 12]

Internet-Draft

Emergency Call Phone BCP

June 2006

Authors' Addresses

Brian Rosen
NeuStar
470 Conrad Dr.
Mars, PA 16046
US

Phone: +1 724 382 1051
Email: br@brianrosen.net

James M. Polk
Cisco Systems
3913 Treemont Circle
Colleyville, TX 76034
US

Phone: +1-817-271-3552
Email: jmpolk@cisco.com

Rosen & Polk Expires December 27, 2006 [Page 13]

Internet-Draft Emergency Call Phone BCP June 2006

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.