ecrit
Internet-Draft
Intended status: Standards Track
Expires: March 21, 2008

B. Rosen
NeuStar
J. Polk
Cisco Systems

September 18, 2007

Best Current Practice for Communications Services in support of Emergency Calling
draft-ietf-ecrit-phonebcp-02

Status of this Memo

Copyright Notice

Abstract

The IETF has several efforts targeted at standardizing various aspects of placing emergency calls. This memo describes best current practice on how devices, networks and services should use such standards to make emergency calls.

Table of Contents

1. Terminology

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].

This document uses terms from [RFC3261], [I-D.ietf-ecrit-requirements] and [I-D.ietf-ecrit-framework].

2. Introduction

This document describes how SIP User Agents and proxy servers support emergency calling, as outlined in [I-D.ietf-ecrit-framework], which is designed to complement the present document in section headings, numbering and content. This BCP succinctly describes the requirements of end devices and applications, access networks, service providers and PSAPs to achieve globally interoperable emergency calling on the Internet.

3. Overview of how emergency calls are placed

An emergency call can be distinguished (Section 5) from any other call by a unique Service URN[I-D.ietf-ecrit-service-urn], which is placed in the call set-up signaling when a home or visited emergency dial string is detected. Because emergency services are local to specific geographic regions, a caller must obtain his location (Section 6) prior to making emergency calls.. To get this location, either a form of measuring (e.g. GPS) (Section Section 6.2.3) device location in the endpoint is deployed, or the endpoint is configured (Section 6.5) with its location from the access network's Location Information Server (LIS). The location is conveyed (Section 6.7) in the SIP signaling with the call. The call is routed (Section 8) based on location using the LoST protocol [I-D.ietf-ecrit-lost]) which maps a location to a set of PSAP URIs. Each URI resolves to a PSAP or an Emergency Services Routing Proxy (ESRP) which serves a group of PSAPs. The call arrives at the PSAP with the location included in the INVITE request.

4. Which devices and sevices should support emergency calls

ED-1 if a user could reasonably expect to be able to place a call for help with the device, then the device or application SHOULD support emergency calling.

SP-1 If a device or application expects to be able to place a call

for help, the service that supports it SHOULD facilitate emergency calling.

ED-2 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.

5. Identifying an emergency call

ED-3 Endpoints SHOULD do dial string recognition of emergency dial strings.

SP-2 Proxy servers SHOULD do dial string recognition of emergency dial strings if for some reason the endpoint does not recognize them.

ED-4/SP-3 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.

ED-5/SP-4 Local dial strings MUST be recognized.

ED-6/SP-5 Home dial strings MAY be recognized.

ED-7/SP-6 Local emergency dial strings SHOULD be determined from LoST [I-D.ietf-ecrit-lost].

ED-8 Endpoints which do not recognize emergency dial strings SHOULD send dial strings as per [RFC4967].

SP-7 Proxy Servers MUST recognize emergency dial strings represented by [RFC4967] and SHOULD recognize dial strings represented by a tel URI [RFC3966].

SP-8 Service providers MAY provide home dial strings by configuration [I-D.ietf-sipping-config-framework].

ED-9 Endpoints SHOULD be able to have home dial strings provisioned by configuration.

ED-10 Devices SHOULD NOT have one button emergency calling initiation.

ED-11/SP-9 All emergency services specified in [I-D.ietf-ecrit-service-urn] MUST be recognized. Devices/Service Providers MUST be capable of recognizing all of the associated dial strings.

6. Location and its role in an emergency call

Location usually involves several steps to process and multiple elements are involved. In Internet emergency calling, where the endpoint is located is "Determined" using a variety of measurement or wiretracing methods. Endpoints may be "Configured" with their own location by the access network. In some circumstances, a proxy server may insert location into the signaling on behalf of the endpoint. The location is "Mapped" to the URI to send the call to, and the location is "Conveyed" to the PSAP (and other elements) in the signaling. Likewise, we employ Location Configuration Protocols, Location Mapping Protocols, and Location Conveyance Protocols for these functions. The Location-to-Service Translation protocol [I-D.ietf-ecrit-lost] is the Location Mapping Protocol defined by the IETF.

6.1. Types of location information

There are several ways location can be specified. In IETF protocols, civic and geospatial (geo) forms are both supported. The civic forms include both postal and jurisdictional fields. A cell tower/sector can be represented as a point (geo or civic) or polygon. Other forms of location representation must be mapped into either a geo or civic for use in emergency calls.

ED-12/SP-10 Endpoints and Service Providers MUST be prepared to handle location represented in either civic or geo form.

ED-13/SP-11/AN-1 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.

6.2. Location Determination

ED-14/AN-2 Any suitable location determination mechanism MAY be used.

6.2.1. User-entered location information

ED-15/AN-3 Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF-LO [RFC4119] and [I-D.ietf-geopriv-revised-civic-lo] MUST be able to be specified.

6.2.2. Access network "wire database" location information

AN-4 Access networks supporting copper, fiber or other hard wired IP packet service SHOULD support location configuration. If the network

does not support location configuration, it MUST require every device that connects to the network to support end system measured location.

AN-5 Access networks providing wire database location information SHOULD provide interior location data where possible. It is RECOMMENDED that interior location be provided when spaces exceed approximately 650 m2.

AN-6 Access networks (including enterprise networks) which support intermediate range wireless connections (typically 100m or less of range) and which do not support a more accurate location determination mechanism such as triangulation, MUST support location configuration which reports the location of the access point as the location of the clients of that access point.

6.2.3. **End-system measured location** information

ED-16 devices MAY support end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.

ED-17/AN-7 Devices that support endpoint measuring of location MUST have at least a coarse location (<1km) capability at all times for routing of calls. This mechanism MAY be a service provided by the access network.

6.2.4. Network measured location information

AN-8 Access networks MAY provide network measured location determination. Wireless access network which do not support network measured location MUST require all devices connected to the network have end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.

AN-9 Access networks that provide network measured location MUST have at least a coarse location (<1km) capability at all times for routing of calls.

AN-10 Access networks with range of <10M MUST provide a location to mobile devices connected to it. The location provided SHOULD be that of the beacon location unless a more accurate mechanism is provided.

6.3. Who adds location, endpoint or proxy

ED-18 Endpoints SHOULD do location configuration themselves.

SP-12 Proxies MAY provide location on behalf of devices it supports if:

- It has a relationship with all access networks the device could connect to, and the relationship allows it to obtain location.
- It has an identifier that can be used by the access network to determine the location of the endpoint, particularly in the presence of NAT and VPN tunnels that may exist between the access network and the service provider.

ED-19/SP-13 Where proxies provide location on behalf of endpoints, the proxy MUST provide a mechanism to supply emergency dial strings to the device if the device recognizes them, or the proxy MUST track the location of the device with sufficient accuracy and timeliness to be able to recognize the local dial string at the time of an emergency call.

6.4. Location and references to location

ED-20 Devices SHOULD be able to accept and forward location by value or by reference. An end device that receives location by reference (and does not also get the corresponding value) MUST be able to perform a dereference operation to obtain a value.

6.5. End system location configuration

ED-21 endpoints MUST support all of: DHCP Location options [RFC4676] and [RFC3825], HELD[I-D.ietf-geopriv-http-location-delivery] and LLDP-MED[LLDP-MED].

AN-11 The access network MUST support at least one of DHCP location options, HELD or LLDP-MED.

AN-12 Where a router is employed between a LAN and WAN in a small (less than approximately 650m2), the LAN MUST reflect the location provided by the WAN to the LAN.

ED-22 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location can be used.

AN-13 Access networks that support more than one LCP MUST reply with the same location information (within the limits of the data format for the specific LCP) for all LCPs it supports.

6.6. When location should be configured

ED-23 Endpoints SHOULD obtain location immediately after obtaining local network configuration information.

ED-24 To minimize the effects of non-bypassable VPNs, location

configuration SHOULD be attempted before such tunnels are established.

ED-25 Software which uses LCPs SHOULD locate and use the actual hardware network interface.

AN-14 Network administrators MUST take care in assigning IP addresses such that VPN address assignments can be distinguished from local devices (by subnet choice, for example), and LISs should not attempt to provide location to addresses that arrive via VPN connections.

AN-15 Placement of NAT devices should consider the effect of the NAT on the LCP.

ED-26 For devices which are not expected to roam, refreshing on the order of once per day is RECOMMENDED.

ED-27 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.

ED-28/AN-16 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

6.7. Conveying location in SIP

ED-29/SP-14 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance].

6.8. Location updates

ED-30/AN-17 Where the absolute location, or the accuracy of location of the endpoint may change between the time the call is received at the PSAP and the time dispatch is completed, location update mechanisms MUST be provided.

ED-31/AN-18 mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.

ED-32/AN-19 The LIS SHOULD provide a location reference which permits

a subscription with appropriate filtering.

ED-33/AN-20 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3118] to the presence event [RFC3856]. For other location-by-reference schemes, a repeated location dereference by the PSAP MUST be supported.

ED-34 If location was sent by value, and the endpoint gets updated location, it MUST send the updated location to the PSAP via reINVITE or UPDATE. Such updates SHOULD be limited to no more than one update every 10 seconds.

6.9. Multiple locations

ED-35 If a UA has more than one location available to it, it MUST choose one location to use to route the call towards the PSAP.

SP-15 If a proxy inserts location on behalf of an endpoint, and it has multiple locations available for the endpoint it MUST choose one location to use to route the call towards the PSAP.

SP-16 If a proxy is attempting to assert location but the UA conveyed a location to it, the proxy must use the UA?s location for routing and MUST convey that location towards the PSAP. It MAY also include what it believes the location to be.

SP-17 All location objects received by a proxy MUST be delivered to the PSAP.

ED-36/SP-18 Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO ?method? element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.

ED-37/SP-19 The "used-for-routing" parameter MUST be set to the location that was used to query LoST.

6.10. Location validation

AN-21 Location validation of civic locations via LoST SHOULD be performed by the LIS before entering a location in its database.

ED-38 Endpoints SHOULD validate civic locations when they receive them from their LCP. Validation SHOULD be performed in conjunction with the LoST route query to minimize load on the LoST server.

6.11. Default location

AN-22 When the access network cannot determine the actual location of the caller, it MUST supply a default location. The default SHOULD be chosen to be as close to the probable location of the device as the network can determine.

SP-20 Proxies handling emergency calls MUST insert a default location if the call does not contain a location.

AN-23/SP-21 Default locations MUST be marked with method=Default and an appropriate provided-by in the PIDF-LO.

6.12. Other location considerations

ED-39 If the LCP does not return location in the form of a PIDF-LO [RFC4119], the endpoint MUST map the location information it receives from the configuration protocol to a PIDF-LO.

ED-40/AN-24 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118].

ED-41 S/MIME MUST NOT be used to protect the Geolocation header or bodies.

ED-42/SP-22 TLS MUST be used to protect location (but see Section 9).

7. Uninitialized devices

ED-43 Uninitialized devices SHOULD NOT lead a user to believe an emergency call could be placed on it unless local regulations require it.

ED-44/AN-25/SP-23 Uninitialized devices SHOULD NOT be capable of placing an emergency call unless local regulations require it.

ED-45/AN-26/SP-24 Uninitialized devices that can place emergency calls MUST supply location the same as a fully capable device would.

ED-46/SP-25 Unitialized Devices MUST supply a call back URI. See Section 7.

ED-47/SP-26 Unitialized Devices MUST include identifiers in the signaling that can be used by the service provider to identify the device and to allow filtering of calls from the device by the PSAP/ ESRP.

8. Routing the call to the PSAP

ED-48 Endpoints who obtain their own location SHOULD perform LoST mapping to the PSAP URI.

ED-49 Mapping SHOULD be performed at boot time and whenever location changes beyond the service boundary obtained from a prior LoST mapping operation or the time-to-live value of that response has expired. The value MUST be cached for possible use.

ED-50 The endpoint SHOULD attempt to update its location at the time of an emergency call. If it cannot obtain a new location quickly (See Section 6), it MUST use the cached value.

ED-51 The endpoint SHOULD attempt to update the LoST mapping at the time of an emergency call. If it cannot obtain a new mapping quickly, it MUST use the cached value.

SP-27 All proxies in the outbound path SHOULD recognize emergency calls with a Request URI of the service URN in the "sos" tree. An endpoint places a service URN in the Request URI to indicate that the endpoint understood the call was an emergency call. A proxy that processes such a call looks for the presence of a Route header with a URI of a PSAP. Absence of such a Route header indicates the UAC was unable to invoke LoST and the proxy MUST perform the LoST mapping and insert a Route header with the URI obtained.

SP-28 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) MUST also perform this mapping, with the best location it has available for the endpoint. The resulting PSAP URI would become the Request URI.

SP-29 Proxy servers performing mapping SHOULD use location obtained from the access network for the mapping. If no location is available, a default location (see Section 6.11) MUST be supplied.

SP-30 A proxy server which attempts mapping and fails to get a mapping MUST provide a default mapping. A suitable default mapping would be the mapping obtained previously for the default location appropriate for the caller.

ED-52/SP-31 [RFC3261] and [RFC3263] procedures MUST be used to route an emergency call towards the PSAP's URI.

ED-53 Initial INVITES MUST provide an Offer [RFC3264].

9. Signaling of emergency calls

ED-54 Best Current Practice for SIP user agents including handling of audio, video and real-time text [RFC4103] SHOULD be applied. This memo can be considered as an addition to it for endpoints.

9.1. Use of TLS

ED-55/SP-32 sips: MUST be specified when attempting to signal an emergency call with SIP.

ED-56/SP-33 If TLS session establishment fails, the call MUST be retried with sip:.

ED-57/SP-34 [I-D.ietf-sip-outbound] is RECOMMENDED to maintain persistent TLS connections between elements.

ED-58/AN-27 https: MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD.

ED-59/AN33 If TLS session establishment fails, the location retrieveal MUST be retried with http:.

9.2. SIP signaling requirements for User Agents

ED-60 The initial SIP signaling Method is an INVITE:

1. The Request URI SHOULD be the service URN in the "sos" tree, If the device cannot do local dial string interpretation, the Request-URI SHOULD be a dialstring URI [RFC4967] with the dialed digits.
2. The To: header MUST be present and SHOULD be a service URN in the "sos" tree. If the device cannot do local dial string interpretation, the To: SHOULD be a dialstring URI with the dialed digits.
3. The From: header MUST be present and SHOULD be the AoR of the caller.
4. A Via: header MUST be present and SHOULD include the URI of the device.
5. A Route: header SHOULD be present with a PSAP URI obtained from LoST (see Section 8) and the loose route parameter. A sips URI [RFC3261] SHOULD be specified, unless the operation must be retried due to a failure to establish a TLS connection. If the device does not do dial plan interpretation, no Route: header will be present.
6. A Contact header MUST be present which MUST be globally routable, for example 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 'geolocation' option tag [I-D.ietf-sip-location-conveyance], unless the device does not understand the concept of SIP Location.
9. 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.
10. If a device understands the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "geolocation" option tag, and MUST NOT include a Geolocation header, and not include a PIDF-LO message body.
11. If a device understands the SIP Location Conveyance extension and supports LoST [I-D.ietf-ecrit-lost] then whichever location is used for routing the message towards the PSAP or ESRP, even if there is only one, the Geolocation "message-routed-on- this-uri" header parameter SHOULD be added to the corresponding URI in the Geolocation header.
12. A normal SDP offer SHOULD be included in the INVITE. The offer MUST include the G.711 codec, see Section 14.
13. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.
14. A UAC SHOULD include a "inserted-by=endpoint" header parameter on all Geolocation headers . This informs downstream elements which device entered the location at this URI (either cid-URL or location-by-reference URI).
15. SIP Caller Preferences [RFC3841] MAY be used to signal how the PSAP should handle the call. For example, a language preference expressed in an Accept-Language header may be used as a hint to cause the PSAP to route the call to a call taker who speaks the requested language.

9.3. SIP signaling requirements for proxy servers

SP-35 SIP Proxy servers processing emergency calls:

1. If the proxy does dial plan interpretation on behalf of user agents, the proxy MUST look for the local emergency dialstring at the location of the end device and MAY look for the home dialstring. If it finds it, the proxy MUST:
   * Insert a Geolocation header as per 10-12 above. Location-by-reference MUST be used because proxies may not insert bodies.
   * Include the Geolocation "inserted-by=server" AND "routed-by-this-uri" parameters.
   * Map the location to a PSAP uri using LoST.

   - Add a Route header with the service URN appropriate for the emergency dialstring.
   - Replace the Request-URI (which was the dialstring) with the PSAP URI obtained from LoST.
   - Route the call using normal SIP routing mechanisms.
2. If the proxy recognizes the service URN in the Request URI, and does not find a Route header with a PSAP URI, it MUST run LoST routing. If a location was provided (which should be the case), the proxy uses that location to query LoST. The proxy may have to dereference a location by reference to get a value. If a location is not present, and the proxy can query a LIS which has the location of the UA it MUST do so. If no location is present, and the proxy does not have access to a LIS which could provide location, the proxy MUST supply a default location (See Section 6.11). The location (in the signaling, obtained from a LIS, or default) MUST be used in a query to LoST with the service URN received with the call. The resulting URI MUST be placed in a Route: header added to the call.
3. The "inserted-by=" parameter in any Geolocation: header received on the call MUST NOT be modified or deleted in transit.
4. The proxy SHOULD NOT modify any parameters in Geolocation: headers received in the call. It MAY add a Geolocation: header. Such an additional location SHOULD NOT be used for routing; the location provided by the UA should be used.
5. Either a P-Asserted-Identity [RFC3325] or an Identity header [RFC4474], or both, MUST be included to identify the sender.

10. Call backs

SP-36 Unitialized devices MUST have a globally routable URI in a Contact: header.

SP-37 Unitialized devices SHOULD have a persistent URI in a P-Asserted-Identity: header.

11. Mid-call behavior

ED-61/SP-38 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] 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.(For devices that are Mobile).

ED-62/SP-39User agents and proxies MUST Support Session Timer[RFC4028] to guard against session corruption.

12. Call termination

ED-63 UACs with an active emergency call (i.e. SIP Dialog) MUST NOT generate a BYE request (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 alert, and when answered, reconnect the caller to the PSAP.

ED-64 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, and the session timer expires the call MAY be declared lost. If in the 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. Dropping of the old call SHOULD only occur if the user is attempting to hang up; the domain of an incoming call can only be determined from the From header, which is not reliable, and could be spoofed. Dropping an active call by a new call with a spoofed From: would be a DoS attack.

13. Disabling of features

ED-65/SP-40 User Agents and proxys MUST disable outgoing call features such as:

- Call Waiting
- Call Transfer
- Three Way Call
- Flash hold
- Outbound Call Blocking

when an emergency call is established.

ED-66/SP-41 The emergency dialstrings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

ED-67/SP-42 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:

- Call Waiting
- Do Not Disturb
- Call Forward (all kinds)

ED-68 Call backs SHOULD be determined by retaining the domain of the PSAP which answers an outgoing emergency call and instantiating a timer which starts when the call is terminated. If a call is received from the same domain and within the timer period, sent to

the Contact: or AoR used in the emergency call, it should be assumed to be a call back. The suggested timer period is 5 minutes.

14. Media

ED-69 Endpoints MUST send and receive media streams on RTP [RFC3550].

ED-70 Normal SIP offer/answer [RFC3264] negotiations MUST be used to agree on the media streams to be used.

ED-71 Endpoints supporting voice MUST support G.711 A law (and mu Law in North America) encoded voice as described in [RFC3551]. It is desirable to support wideband codecs in the offer.

ED-72 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.

ED-73 Endpoints supporting IM MUST support either [RFC3428] or [RFC3920].

ED-74 Endpoints supporting real-time text MUST use [RFC4103]. The expectations for emergency service support for the real-time text medium, described in [I-D.ietf-sipping-toip], section 7.1 SHOULD be fulfilled.

ED-75 Endpoints supporting video MUST support H.264 per [RFC3984].

15. Testing

ED-76 INVITE requests to a service urn with a urn parameter of "test" indicates a request for an automated test. For example, "urn:service.sos.fire;test". As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. A 486 (Busy Here) MUST be returned if the test service is busy, and a 488 (Not Acceptable Here) MUST be returned if the PSAP does not support the test mechanism.

ED-77 In its response to the test, the PSAP MAY include a text body (text/plain) indicating the identity of the PSAP, the requested service, and the location reported with the call. For the latter, the PSAP SHOULD return location-by-value even if the original location delivered with the test was by-reference. If the location-by-reference was supplied, and the dereference requires credentials, the PSAP SHOULD use credentials supplied by the LIS for test

purposes. This alerts the LIS that the dereference is not for an actual emergency call and location hiding techniques, if they are being used, may be employed for this dereference. The response MAY include the connected identity of the PSAP per [I-D.ietf-sip-connected-identity].

ED-78 A PSAP accepting a test call SHOULD accept a media loopback test [I-D.ietf-mmusic-media-loopback] and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. User Agents should expect the PSAP to loop back no more than 3 packets of each media type accepted (which limits the duration of the test), after which the PSAP would normally send BYE.

ED-79 User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address. After an initial IP address assignment test, a full test SHOULD be repeated approximately every 30 days with a random interval.

ED-80 User agents MUST NOT place a test call immediately after booting. If the IP address changes after booting, the UA should wait a random amount of time (in perhaps a 30 minute period, sufficient for any avalanche restart to complete) and then test.

ED-81 PSAPs MAY refuse repeated requests for test from the same device in a short period of time. Any refusal is signaled with a 486 or 488 response.

16. Security Considerations

Security considerations for emergency calling have been documented in draft-ietf-ecrit-security- threats, and the forthcoming GEOPRIV security document(s).

Ed. Note: go through that doc and make sure any actions needed are captured in the BCP text.

17. Acknowledgements

Work group members participating in the creation and review of this document include include Hannes Tschofenig, Ted Hardie, Marc Linsner, Roger Marshall, Stu Goldman, Shida Schubert, James Winterbottom, Roger Marshall, Barbara Stark, Richard Barnes and Peter Blatherwick.

18. Normative References

[I-D.ietf-ecrit-framework]
Rosen, B., "Framework for Emergency Calling using Internet Multimedia", draft-ietf-ecrit-framework-02 (work in progress), July 2007.

[I-D.ietf-ecrit-lost]
Hardie, T., "LoST: A Location-to-Service Translation Protocol", draft-ietf-ecrit-lost-06 (work in progress), August 2007.

[I-D.ietf-ecrit-requirements]
Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", draft-ietf-ecrit-requirements-13 (work in progress), March 2007.

[I-D.ietf-ecrit-security-threats]
Taylor, T., "Security Threats and Requirements for Emergency Call Marking and Mapping", draft-ietf-ecrit-security-threats-05 (work in progress), August 2007.

[I-D.ietf-ecrit-service-urn]
Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", draft-ietf-ecrit-service-urn-07 (work in progress), August 2007.

[I-D.ietf-geopriv-http-location-delivery]
Barnes, M., "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-01 (work in progress), July 2007.

[I-D.ietf-geopriv-pdif-lo-profile]
Tschofenig, H., "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", draft-ietf-geopriv-pdif-lo-profile-08 (work in progress), July 2007.

[I-D.ietf-geopriv-revised-civic-lo]
Thomson, M. and J. Winterbottom, "Revised Civic Location Format for PIDF-LO", draft-ietf-geopriv-revised-civic-lo-05 (work in progress), February 2007.

[I-D.ietf-mmusic-media-loopback]

Hedayat, K., "An Extension to the Session Description Protocol (SDP) for Media Loopback", draft-ietf-mmusic-media-loopback-06 (work in progress), April 2007.

[I-D.ietf-sip-connected-identity]
Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", draft-ietf-sip-connected-identity-05 (work in progress), February 2007.

[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-14 (work in progress), June 2007.

[I-D.ietf-sip-location-conveyance]
Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sip-location-conveyance-08 (work in progress), July 2007.

[I-D.ietf-sip-outbound]
Jennings, C. and R. Mahy, "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)", draft-ietf-sip-outbound-10 (work in progress), July 2007.

[I-D.ietf-sipping-config-framework]
Petrie, D. and S. Channabasappa, "A Framework for Session Initiation Protocol User Agent Profile Delivery", draft-ietf-sipping-config-framework-12 (work in progress), June 2007.

[I-D.ietf-sipping-toip]
Wijk, A. and G. Gybels, "Framework for real-time text over IP using the Session Initiation Protocol (SIP)", draft-ietf-sipping-toip-07 (work in progress), August 2006.

[LLDP] IEEE, "IEEE802.1ab Station and Media Access Control", Dec 2004.

[LLDP-MED]
TIA, "ANSI/TIA-1057 Link Layer Discovery Protocol - Media Endpoint Discovery".

[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.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

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

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 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.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, 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.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based

Location Configuration Information", RFC 3825, July 2004.

[RFC3841] Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)", RFC 3841, August 2004.

[RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC3984] Wenger, S., Hannuksela, M., Stockhammer, T., Westerlund, M., and D. Singer, "RTP Payload Format for H.264 Video", RFC 3984, February 2005.

[RFC4028] Donovan, S. and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)", RFC 4028, April 2005.

[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.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4504] Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration", RFC 4504, May 2006.

[RFC4676] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4676, October 2006.

[RFC4967] Rosen, B., "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier", RFC 4967, July 2007.

Appendix A. BCP Requirements Sorted by Responsible Party

A.1. Requirements of End Devices

ED-1 if a user could reasonably expect to be able to place a call for help with the device, then the device or application SHOULD support emergency calling.

ED-2 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

ED-3 Endpoints SHOULD do dial string recognition of emergency dial strings

ED-4 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.

ED-5 Local dial strings MUST be recognized.

ED-6 Home dial strings MAY be recognized.

ED-7 Local emergency dial strings SHOULD be determined from LoST LoST [I-D.ietf-ecrit-lost].

ED-8 Endpoints which do not recognize emergency dial strings SHOULD send dial strings as per [RFC4967].

ED-9 Endpoints SHOULD be able to have home dial strings provisioned by configuration.

ED-10 Devices SHOULD NOT have one button emergency calling initiation.

ED-11 All emergency services specified in [I-D.ietf-ecrit-service-urn] MUST be recognized. Devices/Service Providers MUST be capable of recognizing all of the associated dial strings.

ED-12 Endpoints and Service Providers MUST be prepared to handle location represented in either civic or geo form.

ED-13 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.

ED-14 Any suitable location determination mechanism MAY be used.

ED-15 Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF- LO [RFC4119] and [I-D.ietf-geopriv-revised-civic-lo] MUST be able to be specified.

ED-16 devices MAY support end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.

ED-17 Devices that support endpoint measuring of location MUST have at least a coarse location (<1km) capability at all times for routing of calls. This mechanism MAY be a service provided by the access network.

ED-18 Endpoints SHOULD do location configuration themselves.

ED-20 Devices SHOULD be able to accept and forward location by value or by reference. An end device that receives location by reference (and does not also get the corresponding value) MUST be able to perform a dereference operation to obtain a value.

ED-21 endpoints MUST support all of: DHCP Location options [RFC4676] and [RFC3825], HELD[I-D.ietf-geopriv-http-location-delivery] and LLDP-MED[LLDP-MED].

ED-22 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location can be used.

ED-23 Endpoints SHOULD obtain location immediately after obtaining local network configuration information.

ED-24 To minimize the effects of non-bypassable VPNs, location configuration SHOULD be attempted before such tunnels are established.

ED-25 Software which uses LCPs SHOULD locate and use the actual hardware network interface.

ED-26 For devices which are not expected to roam, refreshing on the order of once per day is RECOMMENDED

ED-27 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.

ED-28 It is RECOMMENDED that location determination not take longer than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

ED-29 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance].

ED-30 Where the absolute location, or the accuracy of location of the endpoint may change between the time the call is received at the PSAP and the time dispatch is completed, location update mechanisms MUST be provided.

ED-31 mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.

ED-32 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.

ED-33 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3118] to the presence event [RFC3856]. For other location-by-reference schemes, a repeated location dereference by the PSAP MUST be supported.

ED-34 If location was sent by value, and the endpoint gets updated location, it MUST send the updated location to the PSAP via reINVITE or UPDATE. Such updates SHOULD be limited to no more than one update every 10 seconds.

ED-35 If a UA has more than one location available to it, it MUST choose one location to use to route the call towards the PSAP.

ED-36/ Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO ?method? element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.

ED-37 The "used-for-routing" parameter MUST be set to the location that was used to query LoST.

ED-38 Endpoints SHOULD validate civic locations when they receive

them from their LCP. Validation SHOULD be performed in conjunction with the LoST route query to minimize load on the LoST server.

ED-39 If the LCP does not return location in the form of a PIDF-LO [RFC4119], the endpoint MUST map the location information it receives from the configuration protocol to a PIDF-LO.

ED-40 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118].

ED-41 S/MIME MUST NOT be used to protect the Geolocation header or bodies.

ED-42 TLS MUST be used to protect location (but see Section 9).

ED-43 Uninitialized devices SHOULD NOT lead a user to believe an emergency call could be placed on it unless local regulations require it.

ED-44 Uninitialized devices SHOULD NOT be capable of placing an emergency call unless local regulations require it.

ED-45 Uninitialized devices that can place emergency calls MUST supply location the same as a fully capable device would.

ED-46 Unitialized Devices MUST supply a call back URI. See Section 7

ED-47 Unitialized Devices MUST include identifiers in the signaling that can be used by the service provider to identify the device and to allow filtering of calls from the device by the PSAP/ESRP.

ED-48 Endpoints who obtain their own location SHOULD perform LoST mapping to the PSAP URI.

ED-49 Mapping SHOULD be performed at boot time and whenever location changes beyond the service boundary obtained from a prior LoST mapping operation or the time-to-live value of that response has expired. The value MUST be cached for possible use.

ED-50 The endpoint SHOULD attempt to update its location at the time of an emergency call. If it cannot obtain a new location quickly (See Section 6), it MUST use the cached value.

ED-51 The endpoint SHOULD attempt to update the LoST mapping at the time of an emergency call. If it cannot obtain a new mapping quickly, it MUST use the cached value.

ED-52 [RFC3261] and [RFC3263] procedures MUST be used to route an

emergency call towards the PSAP's URI.

ED-53 Initial INVITES MUST provide an Offer [RFC3264]

ED-54 Best Current Practice for SIP user agents including handling of audio, video and real-time text [RFC4103] SHOULD be applied. This memo can be considered as an addition to it for endpoints.

ED-55 sips: MUST be specified when attempting to signal an emergency call with SIP

ED-56 If TLS session establishment fails, the call MUST be retried with sip:

ED-57 [I-D.ietf-sip-outbound] is RECOMMENDED to maintain persistent TLS connections between elements

ED-58 https: MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD

ED-59 If TLS session establishment fails, the location retrieveal MUST be retried with http:

ED-60 The initial SIP signaling Method is an INVITE:

1. The Request URI SHOULD be the service URN in the "sos" tree, If the device cannot do local dialstring interpretation, the Request-URI SHOULD be a dialstring URI [RFC4967] with the dialed digits.
2. The To: header MUST be present and SHOULD be a service URN in the "sos" tree. If the device cannot do local dialstring interpretation, the To: SHOULD be a dialstring URI with the dialed digits.
3. The From: header MUST be present and SHOULD be the AoR of the caller.
4. A Via: header MUST be present and SHOULD include the URI of the device.
5. A Route: header SHOULD be present with a PSAP URI obtained from LoST (see Section 8) and the loose route parameter. A sips URI [RFC3261] SHOULD be specified, unless the operation must be retried due to a failure to establish a TLS connection. If the device does not do dial plan interpretation, no Route: header will be present.
6. A Contact header MUST be present which MUST be globally routable, for example 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 'geolocation' option tag [I-D.ietf-sip-location-conveyance], unless the device does not understand the concept of SIP Location.
9. 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.
10. If a device understands the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "geolocation" option tag, and MUST NOT include a Geolocation header, and not include a PIDF-LO message body.
11. If a device understands the SIP Location Conveyance extension and supports LoST [I-D.ietf-ecrit-lost] then whichever location is used for routing the message towards the PSAP or ESRP, even if there is only one, the Geolocation "message-routed-on- this-uri" header parameter SHOULD be added to the corresponding URI in the Geolocation header.
12. A normal SDP offer SHOULD be included in the INVITE. The offer MUST include the G.711 codec, see Section 14.
13. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.
14. A UAC SHOULD include a "inserted-by=endpoint" header parameter on all Geolocation headers . This informs downstream elements which device entered the location at this URI (either cid-URL or location-by-reference URI).
15. SIP Caller Preferences [RFC3841] MAY be used to signal how the PSAP should handle the call. For example, a language preference expressed in an Accept-Language header may be used as a hint to cause the PSAP to route the call to a call taker who speaks the requested language.

ED-61 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] 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.(For devices that are Mobile).

ED-62 User agents and proxies MUST Support Session Timer [RFC4028] to guard against session corruption.

ED-63 UACs with an active emergency call (i.e. SIP Dialog) MUST NOT

generate a BYE request (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 alert, and when answered, reconnect the caller to the PSAP.

ED-64 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, and the session timer expires the call MAY be declared lost. If in the 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. Dropping of the old call SHOULD only occur if the user is attempting to hang up; the domain of an incoming call can only be determined from the From header, which is not reliable, and could be spoofed. Dropping an active call by a new call with a spoofed From: would be a DoS attack.

ED-65 User Agents and proxys MUST disable outgoing call features such as:
o Call Waiting
o Call Transfer
o Three Way Call
o Flash hold
o Outbound Call Blocking
when an emergency call is established.

ED-66 The emergency dialstrings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

ED-67 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:
o Call Waiting
o Do Not Disturb
o Call Forward (all kinds)

ED-68 Call backs SHOULD be determined by retaining the domain of the PSAP which answers an outgoing emergency call and instantiating a timer which starts when the call is terminated. If a call is received from the same domain and within the timer period, sent to the Contact: or AoR used in the emergency call, it should be assumed to be a call back. The suggested timer period is 5 minutes.

ED-69 Endpoints MUST send and receive media streams on RTP [RFC3550].

ED-70 Normal SIP offer/answer [RFC3264] negotiations MUST be used to agree on the media streams to be used.

ED-71 Endpoints supporting voice MUST support G.711 A law (and mu Law in North America) encoded voice as described in [RFC3551]. It is

desirable to support wideband codecs in the offer.

ED-72 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.

ED-73 Endpoints supporting IM MUST support either [RFC3428] or [RFC3920].

ED-74 Endpoints supporting real-time text MUST use [RFC4103]. The expectations for emergency service support for the real-time text medium, described in [I-D.ietf-sipping-toip], section 7.1 SHOULD be fulfilled.

ED-75 Endpoints supporting video MUST support H.264 per [RFC3984].

ED-76 INVITE requests to a service urn with a urn parameter of "test" indicates a request for an automated test. For example, "urn:service.sos.fire;test". As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. A 486 (Busy Here) MUST be returned if the test service is busy, and a 488 (Not Acceptable Here) MUST be returned if the PSAP does not support the test mechanism.

ED-77 In its response to the test, the PSAP MAY include a text body (text/plain) indicating the identity of the PSAP, the requested service, and the location reported with the call. For the latter, the PSAP SHOULD return location-by-value even if the original location delivered with the test was by-reference. If the location-by-reference was supplied, and the dereference requires credentials, the PSAP SHOULD use credentials supplied by the LIS for test purposes. This alerts the LIS that the dereference is not for an actual emergency call and location hiding techniques, if they are being used, may be employed for this dereference. The response MAY include the connected identity of the PSAP per [I-D.ietf-sip-connected-identity].

ED-78 A PSAP accepting a test call SHOULD accept a media loopback test [I-D.ietf-mmusic-media-loopback] and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. User Agents should expect the PSAP to loop back no more than 3 packets of each media type accepted (which limits the duration of the test), after which the PSAP would normally send BYE.

ED-79 User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address.

After an initial IP address assignment test, a full test SHOULD be repeated approximately every 30 days with a random interval.

ED-80 User agents MUST NOT place a test call immediately after booting. If the IP address changes after booting, the UA should wait a random amount of time (in perhaps a 30 minute period, sufficient for any avalanche restart to complete) and then test.

ED-81 PSAPs MAY refuse repeated requests for test from the same device in a short period of time. Any refusal is signaled with a 486 or 488 response.

A.2. Requirements of Service Providers

SP-1 If a device or application expects to be able to place a call for help, the service that supports it SHOULD facilitate emergency calling.

SP-2 Proxy servers SHOULD do dial string recognition of emergency dial strings if for some reason the endpoint does not recognize them.

SP-3 Emergency calls MUST be marked with a Service URN in the Request-URI of the INVITE.

SP-4 Local dial strings MUST be recognized.

SP-5 Home dial strings MAY be recognized.

SP-6 Local emergency dial strings SHOULD be determined from LoST LoST [I-D.ietf-ecrit-lost].

SP-7 Proxy Servers MUST recognize emergency dial strings represented by [RFC4967] and SHOULD recognize dial strings represented by a tel URI [RFC3966].

SP-8 Service providers MAY provide home dial strings by configuration [I-D.ietf-sipping-config-framework].

SP-9 All emergency services specified in [I-D.ietf-ecrit-service-urn] MUST be recognized. Devices/Service Providers MUST be capable of recognizing all of the associated dial strings.

SP-10 Endpoints and Service Providers MUST be prepared to handle location represented in either civic or geo form.

SP-11 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.

SP-12 Proxies MAY provide location on behalf of devices it supports if:

- It has a relationship with all access networks the device could connect to, and the relationship allows it to obtain location.
- It has an identifier that can be used by the access network to determine the location of the endpoint, particularly in the presence of NAT and VPN tunnels that may exist between the access network and the service provider.

SP-13 Where proxies provide location on behalf of endpoints, the proxy MUST provide a mechanism to supply emergency dia lstrings to the device if the device recognizes them, or the proxy MUST track the location of the device with sufficient accuracy and timeliness to be able to recognize the local dial string at the time of an emergency call.

SP-14 Location sent between SIP elements MUST be conveyed using [I-D.ietf-sip-location-conveyance].

SP-15 If a proxy inserts location on behalf of an endpoint, and it has multiple locations available for the endpoint it MUST choose one location to use to route the call towards the PSAP.

SP-16 If a proxy is attempting to assert location but the UA conveyed a location to it, the proxy must use the UA?s location for routing and MUST convey that location towards the PSAP. It MAY also include what it believes the location to be.

SP-17 All location objects received by a proxy MUST be delivered to the PSAP.

SP-18 Location objects MUST contain information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO ?method? element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.

SP-19 The "used-for-routing" parameter MUST be set to the location that was used to query LoST.

SP-20 Proxies handling emergency calls MUST insert a default location if the call does not contain a location.

SP-21 Default locations MUST be marked with method=Default and an appropriate provided-by in the PIDF-LO.

SP-22 TLS MUST be used to protect location (but see Section 9).

SP-23 Uninitialized devices SHOULD NOT be capable of placing an emergency call unless local regulations require it.

SP-24 Uninitialized devices that can place emergency calls MUST supply location the same as a fully capable device would.

SP-25 Unitialized Devices MUST supply a call back URI. See Section 7

SP-26 Unitialized Devices MUST include identifiers in the signaling that can be used by the service provider to identify the device and to allow filtering of calls from the device by the PSAP/ESRP.

SP-27 All proxies in the outbound path SHOULD recognize emergency calls with a Request URI of the service URN in the "sos" tree. An endpoint places a service URN in the Request URI to indicate that the endpoint understood the call was an emergency call. A proxy that processes such a call looks for the presence of a Route header with a URI of a PSAP. Absence of such a Route header indicates the UAC was unable to invoke LoST and the proxy MUST perform the LoST mapping and insert a Route header with the URI obtained.

SP-28 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) MUST also perform this mapping, with the best location it has available for the endpoint. The resulting PSAP URI would become the Request URI.

SP-29 Proxy servers performing mapping SHOULD use location obtained from the access network for the mapping. If no location is available, a default location (see Section 6.11) MUST be supplied.

SP-30 A proxy server which attempts mapping and fails to get a mapping MUST provide a default mapping. A suitable default mapping would be the mapping obtained previously for the default location appropriate for the caller.

SP-31 [RFC3261] and [RFC3263] procedures MUST be used to route an emergency call towards the PSAP's URI.

SP-32 sips: MUST be specified when attempting to signal an emergency call with SIP

SP-33 If TLS session establishment fails, the call MUST be retried with sip:

SP-34 [I-D.ietf-sip-outbound] is RECOMMENDED to maintain persistent TLS connections between elements

SP-35 SIP Proxy servers processing emergency calls:

1. If the proxy does dial plan interpretation on behalf of user agents, the proxy MUST look for the local emergency dialstring at the location of the end device and MAY look for the home dialstring. If it finds it it MUST:
   * Insert a Geolocation header as per 10-12 above. Location-by-reference MUST be used because proxies may not insert bodies.
   * Include the Geolocation "inserted-by=server" AND "routed-by-this-uri" parameters.
   * Map the location to a PSAP uri using LoST.
   * Add a Route header with the service URN appropriate for the emergency dialstring.
   * Replace the Request-URI (which was the dialstring) with the PSAP URI obtained from LoST.
   * Route the call using normal SIP routing mechanisms.
2. If the proxy recognizes the service URN in the Request URI, and does not find a Route header with a PSAP URI, it MUST run LoST routing. If a location was provided (which should be the case), the proxy uses that location to query LoST. The proxy may have to dereference a location by reference to get a value. If a location is not present, and the proxy can query a LIS which has the location of the UA it MUST do so. If no location is present, and the proxy does not have access to a LIS which could provide location, the proxy MUST supply a default location (See Section 6.11). The location (in the signaling, obtained from a LIS, or default) MUST be used in a query to LoST with the service URN received with the call. The resulting URI MUST be placed in a Route: header added to the call.
3. The "inserted-by=" parameter in any Geolocation: header received on the call MUST NOT be modified or deleted in transit.
4. The proxy SHOULD NOT modify any parameters in Geolocation: headers received in the call. It MAY add a Geolocation: header. Such an additional location SHOULD NOT be used for routing; the location provided by the UA should be used.
5. Either a P-Asserted-Identity [RFC3325] or an Identity header [RFC4474], or both, MUST be included to identify the sender.

SP-36 Unitialized devices MUST have a globally routable URI in a Contact: header

SP-37 Unitialized devices SHOULD have a persistent URI in a P-Asserted-Identity: header

SP-38 During the course of an emergency call, devices and proxies MUST support REFER transactions and the Referred-by: header [RFC3515] 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.(For devices that are Mobile)

SP-39User agents and proxies MUST Support Session Timer [RFC4028] to guard against session corruption.

SP-40 User Agents and proxys MUST disable outgoing call features such as:

- Call Waiting
- Call Transfer
- Three Way Call
- Flash hold
- Outbound Call Blocking

when an emergency call is established.

SP-41 The emergency dialstrings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

SP-42 The User Agent and Proxies SHOULD disable the following incoming call features on call backs from the PSAP:

- Call Waiting
- Do Not Disturb
- Call Forward (all kinds)

A.3. Requirements of Access Networks

AN-1 Elements MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism supplied.

AN-2 Any suitable location determination mechanism MAY be used.

AN-3 Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. Where a civic form of location is provided, all fields in the PIDF- LO [RFC4119] and [I-D.ietf-geopriv-revised-civic-lo] MUST be able to be specified.

AN-4 Access networks supporting copper, fiber or other hard wired IP packet service SHOULD support location configuration. If the network does not support location configuration, it MUST require every device that connects to the network to support end system measured location.

AN-5 Access networks providing wire database location information SHOULD provide interior location data where possible. It is RECOMMENDED that interior location be provided when spaces exceed

approximately 650 m2

AN-6 Access networks (including enterprise networks) which support intermediate range wireless connections (typically 100m or less of range) and which do not support a more accurate location determination mechanism such as triangulation, MUST support location configuration which reports the location of the access point as the location of the clients of that access point.

AN-7 Devices that support endpoint measuring of location MUST have at least a coarse location (<1km) capability at all times for routing of calls. This mechanism MAY be a service provided by the access network.

AN-8 Access networks MAY provide network measured location determination. Wireless access network which do not support network measured location MUST require all devices connected to the network have end-system measured location. Uncertainty of less than 100 m with 95% confidence SHOULD be available for dispatch.

AN-9 Access networks that provide network measured location MUST have at least a coarse location (<1km) capability at all times for routing of calls.

AN-10 Access networks with range of <10M MUST provide a location to mobile devices connected to it. The location provided SHOULD be that of the beacon location unless a more accurate mechanism is provided.

AN-11 The access network MUST support at least one of DHCP location options, HELD or LLDP-MED.

AN-12 Where a router is employed between a LAN and WAN in a small (less than approximately 650m2), the LAN MUST reflect the location provided by the WAN to the LAN.

AN-13 Access networks that support more than one LCP MUST reply with the same location information (within the limits of the data format for the specific LCP) for all LCPs it supports.

AN-14 Network administrators MUST take care in assigning IP addresses such that VPN address assignments can be distinguished from local devices (by subnet choice, for example), and LISs should not attempt to provide location to addresses that arrive via VPN connections.

AN-15 Placement of NAT devices should consider the effect of the NAT on the LCP.

AN-16 It is RECOMMENDED that location determination not take longer

than 250 ms to obtain routing location and systems SHOULD be designed such that the typical response is under 100ms. However, as much as 3 seconds to obtain routing location MAY be tolerated if location accuracy can be substantially improved over what can be obtained in 250 ms.

AN-17 Where the absolute location, or the accuracy of location of the endpoint may change between the time the call is received at the PSAP and the time dispatch is completed, location update mechanisms MUST be provided.

AN-18 mobile devices MUST be provided with a mechanism to get repeated location updates to track the motion of the device during the complete processing of the call.

AN-19 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.

AN-20 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3118] to the presence event [RFC3856]. For other location-by-reference schemes, a repeated location dereference by the PSAP MUST be supported.

AN-21 Location validation of civic locations via LoST SHOULD be performed by the LIS before entering a location in its database.

AN-22 When the access network cannot determine the actual location of the caller, it MUST supply a default location. The default SHOULD be chosen to be as close to the probable location of the device as the network can determine.

AN-23 Default locations MUST be marked with method=Default and an appropriate provided-by in the PIDF-LO.

AN-24 To prevent against spoofing of the DHCP server, elements implementing DHCP for location configuration SHOULD use [RFC3118].

AN-25 Uninitialized devices SHOULD NOT be capable of placing an emergency call unless local regulations require it.

AN-26 Uninitialized devices that can place emergency calls MUST supply location the same as a fully capable device would.

AN-27 https: MUST be specified when attempting to retrieve location (configuration or dereferencing) with HELD

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

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).