ecrit
Internet-Draft
Intended status: BCP
Expires: March 10, 2012

B. Rosen
NeuStar
J. Polk
Cisco Systems
September 7, 2011

Best Current Practice for Communications Services in support of Emergency Calling
draft-ietf-ecrit-phonebcp-20.txt

Abstract

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

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on March 10, 2012.

Table of Contents

1. Terminology

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

This document uses terms from [RFC3261], [RFC5012] and [I-D.ietf-ecrit-framework].

2. Introduction

This document describes how access networks, Session Initiation Protocol [RFC3261] user agents, proxy servers and Public Safety Access Points (PSAPs) 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. Understanding [I-D.ietf-ecrit-framework] is necessary to understand this document. This BCP succinctly describes the requirements of end devices and applications (requirements prefaced by "ED-"), access networks (including enterprise access networks) (requirements prefaced by "AN-"), service providers (requirements prefaced by "SP-") and PSAPs to achieve globally interoperable emergency calling on the Internet.

This document also defines requirements for "Intermediate" devices which exist between end devices or applications and the access network. For example, a home router is an "Intermediate" device. Reporting location on an emergency call (see Section 6) may depend on the ability of such intermediate devices to meet the requirements prefaced by "INT-".

The access network requirements apply to those networks which may be used to place emergency calls using IETF protocols. Local regulations may impact the need to support this document’s access network requirements.

Other organizations, such as the North American Emergency Number Association (NENA), define the PSAP interface. NENA’s documents reference this document.

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 [RFC5031], 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 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 Location-to-Service Translation (LoST) protocol [RFC5222], 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 SIP INVITE request.

4. Which devices and services should support emergency calls

ED-1 A device or application that implements SIP calling SHOULD support emergency calling. Some jurisdictions have regulations governing which devices need to support emergency calling and developers are encouraged to ensure that devices they develop meet relevant regulatory requirements. Unfortunately, the natural variation in those regulations also makes it impossible to accurately describe the cases when developers do or do not have to support emergency calling.

SP-1 If a device or application expects to be able to place a call for help, the service provider that supports it MUST facilitate emergency calling. Some jurisdictions have regulations governing this.

ED-2 Devices that create media sessions and exchange real-time audio, video and/or text, 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. Some jurisdictions have regulations governing this.

5. Identifying an emergency call

ED-3 Endpoints SHOULD recognize dial strings of emergency calls. If the service provider always knows the location of the device (the correct dial string depends on which country you are in), the service provider may recognize them, see SP-2.

SP-2 Proxy servers SHOULD recognize 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 Geographically local dial strings MUST be recognized.

ED-6/SP-5 Devices MUST be able to be configured with the home country from which the home dial string(s) can be determined.

ED-7/SP-6 Emergency dial strings SHOULD be determined from LoST [RFC5222]. Dial Strings MAY be configured directly into the device.

AN-1 LoST servers MUST return dial strings for emergency services.

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

SP-7 If a proxy server recognizes dial strings on behalf of its clients, it MUST recognize emergency dial strings represented by [RFC4967] and SHOULD recognize the emergency dial strings represented by a tel URI [RFC3966].

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

SP-8 Service providers MAY provision home dial strings in devices.

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

ED-11/SP-9 All sub-services for the ’sos’ service specified in [RFC5031]. MUST be recognized.

6. Location and its role in an emergency call

Handling location for emergency calling usually involves several steps to process and multiple entities are involved. In Internet emergency calling, where the endpoint is located is "determined" using a variety of measurement or wiretracing methods. Endpoints can be "configured" with their own location by the access network. In some circumstances, a proxy server can 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 entities) in the signaling. Likewise, we employ Location Configuration Protocols (LCPs), the Location-to-Service Mapping Protocol, and Location Conveyance Protocols for these functions. The Location-to-Service Translation protocol [RFC5222] is the Location Mapping Protocol defined by the IETF.

6.1. Types of location information

There are several forms of location. All IETF location configuration and location conveyance protocols support both civic and geospatial (geo) forms. The civic forms include both postal and jurisdictional fields. A cell tower/sector can be represented as a point (geo or civic) or polygon. Endpoints, Intermediate Devices and Service Providers receiving other forms of location representation MUST map them into either a geo or civic for use in emergency calls.

ED-12/INT-1/SP-10 Endpoints, Intermediate Devices and Service Providers MUST be prepared to handle location represented in either civic or geo form.

ED-13/INT-2/SP-11/AN-2 Entities MUST NOT convert (civic to geo or geo to civic) from the form of location the determination mechanism (see Section Section 6.2) supplied prior to receipt by the PSAP.

6.2. Location Determination

ED-14/INT-3/AN-3 Any location determination mechanism MAY be used, provided the accuracy of the location meets local requirements.

6.2.1. User-entered location information

ED-15/INT-4/AN-4 Devices, intermediate Devices and/or access networks SHOULD support a manual method to override the location the access network determines. When the override location is supplied in civic form, it MUST be possible for the resultant Presence Information Data Format - Location Object (PIDF-LO) received at the PSAP to contain any of the elements specified in [RFC4119] and [RFC5139].

6.2.2. Access network "wire database" location information

AN-5 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 or intermediate device that connects to the network to support end system measured location.

AN-6/INT-5 Access networks and intermediate devices providing wire database location information SHOULD provide interior location data (building, floor, room, cubicle) where possible. It is RECOMMENDED that interior location be provided when spaces exceed approximately 650 square meters. See [I-D.ietf-ecrit-framework] Section 6.2.2 for a discussion of how this value was determined.

AN-7/INT-6 Access networks and intermediate devices (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 where the location of the access point is reflected as the location of the clients of that access point.

AN-8/INT-7 Where the access network provides location configuration, intermediate devices MUST either be transparent to it, or provide an interconnected client for the supported configuration mechanism and a server for a configuration protocol supported by end devices downstream of the intermediate device such that the location provided by the access network is available to clients as if the intermediate device was not in the path.

6.2.3. End-system measured location information

ED-16/INT-8 Devices MAY support end-system measured location. See [I-D.ietf-ecrit-framework] Section 6 for a discussion of accuracy of location.

ED-17/INT-9/AN-9 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy) for routing of calls. The location mechanism MAY be a service provided by the access network.

6.2.4. Network-measured location information

AN-10 Access networks MAY provide network-measured location determination. Wireless access networks that do not supply network measured location MUST require every device or intermediate device connected to the network to support end-system measured location. Uncertainty and confidence may be specified by local regulation. Where not specified, uncertainty of less than 100 meters with 95% confidence is RECOMMENDED for dispatch location.

AN-11 Access networks that provide network measured location MUST have at least a coarse location (typically <1km when not location hiding) capability at all times for routing of calls.

AN-12 Access networks with range of <10 meters (e.g. personal area networks such as Bluetooth MUST provide a location to mobile devices connected to them. The location provided SHOULD be that reported by the upstream access network unless a more accurate mechanism is available.

6.3. Who adds location, endpoint or proxy

ED-18/INT-10 Endpoints SHOULD attempt to configure their own location using the Location Configuration Protocols (LCPs) listed in ED-21.

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

- The proxy has a relationship with all access networks the device could connect to, and the relationship allows it to obtain location.
- The proxy has an identifier, such as an IP address, that can be used by the access network to determine the location of the endpoint, even in the presence of NAT and VPN tunnels that may obscure the identifier between the access network and the service provider.

ED-19/INT-11/SP-13 Where proxies provide location on behalf of endpoints, the service provider MUST ensure that either the end device is provided with the local dial strings for its current location (where the end device recognizes dial strings), or the service provider proxy MUST detect the appropriate local dial strings at the time of the call.

6.4. Location and references to location

ED-20/INT-12 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

Obtaining location from the access network may be preferable even if the device can measure its own location, especially indoors where most measurement mechanisms are not accurate enough. This sections requirements do not apply to devices that can accurately measure their own location.

ED-21/INT-13 Devices MUST support both the Dynamic Host Configuration Protocol (DHCP) location options [RFC4776], [RFC6225] and HTTP Enabled Location Delivery (HELD) [RFC5985]. When devices deploy a specific access network interface for which location configuration mechanisms such as Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) [LLDP-MED] or 802.11v are specified, the device SHOULD support the additional respective access network specific location configuration mechanism.

AN-13/INT-14 The access network MUST support either DHCP location options or HELD. The access network SHOULD support other location

configuration technologies that are specific to the type of access network.

AN-14/INT-15 Where a router is employed between a LAN and WAN in a small (less than approximately 650 square meters) area, the router MUST be transparent to the location provided by the WAN to the LAN. This may mean the router must obtain location as a client from the WAN, and supply an LCP server to the LAN with the location it obtains. Where the area is larger, the LAN MUST have a location configuration mechanism satisfying the requirements of this document.

ED-22/INT-16 Endpoints SHOULD try all LCPs supported by the device in any order or in parallel. The first one that succeeds in supplying location MUST be used.

AN-15/INT-17 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.

ED-23/INT-18/SP-14 When HELD is the LCP, the request MUST specify a value of "emergencyRouting" for the "responseTime" parameter and use the resulting location for routing. If a value for dispatch location will be sent, another request with the "responseTime" parameter set to "emergencyDispatch" must be completed, with the result sent for dispatch purposes.

ED-24 Where the operating system supporting application programs which need location for emergency calls does not allow access to Layer 2 and Layer 3 functions necessary for a client application to use DHCP location options and/or other location technologies that are specific to the type of access network, the operating system MUST provide a published API conforming to ED-12 through ED-23 and ED-25 through ED-32. It is RECOMMENDED that all operating systems provide such an API.

6.6. When location should be configured

If an endpoint is manually configured, the requirements in this section are not applicable.

ED-25/INT-19 Endpoints SHOULD obtain location immediately after obtaining local network configuration information.

ED-26/INT-20 If the device is configured to use DHCP for bootstrapping, and does not use it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776], [RFC6225], [RFC5986] and [RFC5223].

ED-27/INT-21 If the device sends a DHCPINFORM message, it MUST include both options for location acquisition (civic and geodetic), the option for LIS discovery, and the option for LoST discovery as defined in [RFC4776], [RFC6225], [RFC5986] and [RFC5223].

ED-28/INT-22 To minimize the effects of VPNs that do not allow packets to be sent via the native hardware interface rather than via the VPN tunnel, location configuration SHOULD be attempted before such tunnels are established.

ED-29/INT-23 Software which uses LCPs SHOULD locate and use the actual hardware network interface rather than a VPN tunnel interface to direct LCP requests to the LIS in the actual access network.

AN-16 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 unless it can accurately determine the location for such addresses.

AN-17 Placement of NAT devices where an LCP uses IP address for an identifier SHOULD consider the effect of the NAT on the LCP. The address used to query the LIS MUST be able to correctly identify the record in the LIS representing the location of the querying device

ED-30/INT-24 For devices which are not expected to change location, refreshing location on the order of once per day is RECOMMENDED.

ED-31/INT-25 For devices which roam, refresh of location information 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. If the device detects a link state change that might indicate having moved, for example when it changes access points, the device SHOULD refresh its location.

ED-32/INT-26/AN-18 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 100 ms. 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

ED-33/SP-15 Location sent between SIP entities MUST be conveyed using [I-D.ietf-sipcore-location-conveyance].

6.8. Location updates

ED-34/AN-19 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 implemented and used.

ED-35/AN-20 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-36/AN-21 The LIS SHOULD provide a location reference which permits a subscription with appropriate filtering.

ED-37/AN-22 For calls sent with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3265] to the presence event [RFC3856]. For other location-by-reference schemes that do not support subscription, the PSAP will have to repeatedly dereference the URI to determine if the device moved.

ED-38 If location was sent by value, and the endpoint gets updated location, it MUST send the updated location to the PSAP via a SIP re-INVITE or UPDATE request. Such updates SHOULD be limited to no more than one update every 10 seconds, a value selected to keep the load on a large PSAP manageable, and yet provide sufficient indication to the PSAP of motion.

6.9. Multiple locations

ED-39/SP-16 If the LIS has more than one location for an endpoint it MUST conform to the rules in Section 3 of [RFC5491]

ED-40 If an endpoint has more than one location available to it, it MUST choose one location to route the call towards the PSAP. If multiple locations are in a single Presence Information Data Format (PIDF), the procedures in [RFC5491] MUST be followed. If the endpoint has multiple PIDFs, and has no reasonable basis to choose from among them, a random choice is acceptable.

SP-17 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. If multiple locations are in a single PIDF, the procedures in [RFC5491] MUST be followed. If the proxy has multiple PIDFs, and has no reasonable basis to choose from among them, a random choice is acceptable.

SP-18 If a proxy is attempting to insert location but the endpoint

conveyed a location to it, the proxy MUST use the endpoint's location for routing in the initial INVITE and MUST convey that location towards the PSAP. It MAY also include what it believes the location to be in a separate Geolocation header.

SP-19 All location objects received by a proxy MUST be delivered to the PSAP.

ED-41/SP-20 Location objects MUST be created with 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-42/SP-21 A location with a method of "derived" MUST NOT be used unless no other location is available.

6.10. Location validation

AN-23 A LIS SHOULD perform location validation of civic locations via LoST before entering a location in its database.

ED-44 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-24 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. See [I-D.ietf-ecrit-framework]

SP-22 Proxies handling emergency calls MUST insert a default location in the INVITE if the incoming INVITE does not contain a location and the proxy does not have a method for obtaining a better location.

AN-25/SP-23 Default locations MUST be marked with method=Default and the proxy MUST be identified in provided-by element of the PIDF-LO.

6.12. Other location considerations

ED-45 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-46/AN-26 To prevent against spoofing of the DHCP server, entities implementing DHCP for location configuration SHOULD use [RFC3118],

although the difficulty in providing appropriate credentials is significant.

ED-47 If S/MIME [RFC5751] is used, the INVITE message MUST provide enough information unencrypted for intermediate proxies to route the call based on the location information included. This would include the Geolocation header, and any bodies containing location information. Use of S/MIME with emergency calls is NOT RECOMMENDED for this reason.

ED-48/SP-24 TLS [RFC5746] MUST be used to protect location (but see Section 9.1). All implementations MUST support TLS.

7. LIS and LoST Discovery

ED-49 Endpoints MUST support one or more mechanisms that allow them to determine their public IP address, for example, STUN [RFC5389].

ED-50 Endpoints MUST support LIS discovery as described in [RFC5986], and the LoST discovery as described in [RFC5223].

ED-51 The device MUST have a configurable default LoST server parameter.

ED-52 DHCP LoST discovery MUST be used, if available, in preference to configured LoST servers. That is, the endpoint MUST send queries to this LoST server first, using other LoST servers only if these queries fail.

AN-27 Access networks which support DHCP MUST implement the LIS and LoST discovery options in their DHCP servers and return suitable server addresses as appropriate.

8. Routing the call to the PSAP

ED-53 Endpoints who obtain their own location SHOULD perform LoST mapping to the PSAP URI.

ED-54 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 later use.

ED-55 The endpoint MUST 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-56 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. If the device cannot update the LoST mapping and does not have a cached value, it MUST signal an emergency call without a Route header containing a PSAP URI.

SP-25 Networks MUST be designed so that at least one proxy in the outbound path will 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 SIP Route header field with a URI of a PSAP. Absence of such a Route header indicates the endpoint was unable to invoke LoST and the proxy MUST perform the LoST mapping and insert a Route header field with the URI obtained.

SP-26 To deal with old user agents that predate this specification and with endpoints that do not have access to their own location data, a proxy that recognizes 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 be placed in a Route header with the service URN in the Request URI.

SP-27 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-28 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-57/SP-29 [RFC3261] and [RFC3263] procedures MUST be used to route an emergency call towards the PSAP’s URI.

9. Signaling of emergency calls

9.1. Use of TLS

ED-58/SP-30 TLS is the primary mechanism used to secure the signaling for emergency calls. IPsec [RFC4301] MAY be used instead of TLS for any hop. Either TLS or IPSEC MUST be used when attempting to signal an emergency call.

ED-59/SP-31 If TLS session establishment is not available, or fails, the call MUST be retried without TLS.

ED-60/SP-32 [RFC5626] is RECOMMENDED to maintain persistent TLS connections between entities when one of the entity is an endpoint. Persistent TLS connection between proxies is RECOMMENDED using any suitable mechanism.

ED-61/AN-28 TLS SHOULD be used when attempting to retrieve location (configuration or dereferencing) with HELD. The use of [RFC5077] is RECOMMENDED to minimize the time to establish TLS sessions without keeping server-side state. IPsec MAY be used instead of TLS.

ED-62/AN-29 When TLS session establishment fails, the location retrieval MUST be retried without TLS.

9.2. SIP signaling requirements for User Agents

ED-63 The initial SIP signaling method is an INVITE request:

1. The Request URI SHOULD be the service URN in the "sos" tree. If the device does not interpret local dial strings, the Request-URI MUST be a dial string URI [RFC4967] with the dialed digits.
2. The To header field SHOULD be a service URN in the "sos" tree. If the device does not interpret local dial strings, the To: MUST be a dial string URI with the dialed digits.
3. The From header field SHOULD contain the AoR of the caller.
4. A Route header field SHOULD be present with a PSAP URI obtained from LoST (see Section 8). If the device does not interpret dial plans, or was unable to obtain a route from a LoST server, no such Route header field will be present.
5. A Contact header field MUST be globally routable, for example a GRUU [RFC5627], and be valid for several minutes following the termination of the call, provided that the UAC remains registered with the same registrar, to permit an immediate call-back to the specific device which placed the emergency call. It is acceptable if the UAC inserts a locally routable URI and a subsequent B2BUA maps that to a globally routable URI.
6. Other header fields MAY be included as per normal SIP behavior.
7. If a geolocation URI is included in the INVITE, a Supported header field MUST be included with a ’geolocation-sip’ or ’geolocation-http" option tag, as appropriate. [I-D.ietf-sipcore-location-conveyance].
8. If a device understands the SIP location conveyance [I-D.ietf-sipcore-location-conveyance] extension and has its location available, it MUST include location either by-value, by-reference or both.
9. A SDP offer SHOULD be included in the INVITE. If voice is supported the offer SHOULD include the G.711 codec, see Section 14. As PSAPs may support a wide range of media types and codecs, sending an offerless INVITE may result in a lengthy return offer, but is permitted. Cautions in [RFC3261] on

offerless INVITEs should be considered before such use.

10. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.

9.3. SIP signaling requirements for proxy servers

SP-33 SIP Proxy servers processing emergency calls:

1. If the proxy interprets dial plans on behalf of user agents, the proxy MUST look for the local emergency dial string at the location of the end device and MAY look for the home dial string. If it finds it, the proxy MUST:
   * Insert a Geolocation header field. Location-by-reference MUST be used because proxies must not insert bodies.
   * Insert the Geolocation-Routing header with appropriate parameters .
   * Map the location to a PSAP URI using LoST.
   * Add a Route header with the PSAP URI.
   * Replace the Request-URI (which was the dial string) with the service URN appropriate for the emergency dial string.
   * 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, it MUST query a LoST server immediately. 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 proxy MAY add a Geolocation header field. Such an additional location SHOULD NOT be used for routing; the location provided by the UA should be used.
4. Either a P-Asserted-Identity [RFC3325] or an Identity header field [RFC4474], or both, SHOULD be included to identify the sender. For services which must support emergency calls from unauthenticated devices, valid identity may not be available. Proxies encountering a P-Asserted-Identity will need to pass the header to the PSAP, which is in a different domain. [RFC3325] requires a "spec(T)" to determine what happens if the "id" privacy service, or a Privacy header is present and requests privacy. In the absence of another spec(T), such proxies should pass the header unmodified if and only if the connection between the proxy and the PSAP is, as far as the proxy can determine,

protected by TLS with mutual authentication using keys reliably known by the parties, encrypted with no less strength than AES and the local regulations governing the PSAP do not otherwise specify.

5. Proxies SHOULD NOT return a 424 error. It should process the INVITE as best as it can.
6. Proxies SHOULD NOT obey a Geolocation-Routing value of "no" or a missing value if the proxy must query LoST to obtain a route. Emergency calls are always routed by location.

10. Call backs

ED-64/SP-34 Devices device SHOULD have a globally routable URI in a Contact: header field which remains valid for several minutes past the time the original call containing the URI completes unless the device registration expires and is not renewed.

SP-35 Call backs to the Contact: header URI received within 30 minutes of an emergency call must reach the device regardless of call features or services that would normally cause the call to be routed to some other entity.

SP-36 Devices MUST have a persistent AOR URI either in a P-Asserted-Identity header field or From protected by an Identity header field suitable for returning a call some time after the original call. Such a call back would not necessarily reach the device that originally placed the call.

11. Mid-call behavior

ED-65/SP-37 During the course of an emergency call, devices and proxies MUST initiate a call transfer upon receipt of REFER request within the dialog with method=INVITE and the Referred-by header field [RFC3515] in that request.

12. Call termination

ED-66 Normal [RFC3261] procedures for termination MUST be used for termination of the call.

13. Disabling of features

ED-67/SP-38 User Agents and proxies MUST disable features that will interrupt an ongoing emergency call, such as:

- o Call Waiting
- o Call Transfer
- o Three Way Call
- o Hold
- o Outbound Call Blocking

when an emergency call is established, but see ED-66 with respect to Call Waiting. Also see ED-74 in Section 14.

ED-68/SP-39 The emergency dial strings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

ED-69/SP-40 The User Agent and Proxies MUST disable call features which would interfere with the ability of call backs from the PSAP to be completed such as:

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

These features SHOULD be disabled for approximately 30 minutes following termination of an emergency call.

ED-70 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. [RFC4916] may be used by the PSAP to inform the endpoint of the domain of the PSAP. Recognizing a call back from the domain of the PSAP will not always work, and further standardization will be required to give the endpoint the ability to recognize a call back.

14. Media

ED-71 Endpoints MUST send and receive media streams on RTP [RFC3550].

ED-72 Normal SIP offer/answer [RFC3264] negotiations MUST be used to agree on the media streams to be used.

ED-73/SP-41 G.711 A law (and mu Law if they are intended be used in North America) encoded voice as described in [RFC3551] MUST be supported. If the endpoint cannot support G.711, a transcoder MUST be used so that the offer received at the PSAP contains G.711. It is desirable to include wideband codecs such as G.722 and AMR-WB in the offer. PSAPs SHOULD support narrowband codecs common on endpoints in their area to avoid transcoding.

ED-74 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-75 Endpoints supporting Instant Messaging (IM) MUST support either [RFC3428] and [RFC4975].

ED-76 Endpoints supporting real-time text MUST use [RFC4103]. The expectations for emergency service support for the real-time text medium are described in [RFC5194], Section 7.1.

ED-77 Endpoints supporting video MUST support H.264 per [RFC6184].

15. Testing

ED-78 INVITE requests to a service URN starting with "test." indicates a request for an automated test. For example, "urn:service:test.sos.fire". 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 404 (Not found) MUST be returned if the PSAP does not support the test mechanism.

ED-79 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. Use of SIPS for the request would assure the response containing the location is kept private

ED-80 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-81 User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address not due to a reboot. After an initial test, a full test SHOULD be repeated approximately every 30 days with a random interval.

ED-82 User agents MUST NOT place a test call immediately after booting. If the IP address changes after booting, the endpoint should wait a random amount of time (in perhaps a 30 minute period, sufficient for any avalanche restart to complete) and then test.

ED-83 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 [RFC5069], and [RFC6280]. This document suggests that security (TLS or IPsec) be used hop by hop on a SIP call to protect location information, identity, etc. It also suggests that if the attempt to create a security association fails, the call be retried without the security. It's more important to get an emergency call through than to protect the data; indeed, in many jurisdictions privacy is explicitly waived when making emergency calls. Placing a call without security may reveal user information, including location. The alternative - failing the call if security cannot be established, is considered unacceptable.

17. IANA Considerations

This document registers service URNs in the Service URN Labels registry per [RFC5031] for testing.

17.1. test service urn

A new entry in the URN Service Label registry is added. The new service is "test", the reference is this document, and the description is "self test".

17.2. 'test' Subregistry

A new Subregistry is created, the "'test' Sub-Service. The registration process is Expert Review per [RFC5226]. The expert review should consider that the entries in this registry nominally track the entries in the sos sub registry, although it is not required that every entry in sos have an entry in test, and it is possible that entries in the test sub-registry not necessarily be in the sos sub registry. For example, testing of non-emergency URNs may be allowed. The Reference is this document. The initial content of the subregistry is:

Service	Reference	Description
test.sos	[this document]	test for sos
test.sos.ambulance	[this document]	test for sos.ambulance
test.sos.animal-control	[this document]	test for sos.animal-control
test.sos.fire	[this document]	test for sos.fire
test.sos.gas	[this document]	test for sos.gas
test.sos.marine	[this document]	test for sos.marine
test.sos.mountain	[this document]	test for sos.mountain
test.sos.physician	[this document]	test for sos.physician
test.sos.poison	[this document]	test for sos.poison
test.sos.police	[this document]	test for sos.police

18. Acknowledgements

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

19. References

19.1. Normative References

[I-D.ietf-mmusic-media-loopback]
Sivachelvan, C., Venna, N., Jones, P., Stratton, N., Roychowdhury, A., and K. Hedayat, "An Extension to the Session Description Protocol (SDP) for Media Loopback", draft-ietf-mmusic-media-loopback-15 (work in progress), March 2011.

[I-D.ietf-sipcore-location-conveyance]
Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sipcore-location-conveyance-09 (work in progress), September 2011.

[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.

[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.

[RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 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.

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

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session

Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, June 2007.

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

[RFC4975] Campbell, B., Mahy, R., and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 2007.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.

[RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

[RFC5223] Schulzrinne, H., Polk, J., and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)", RFC 5223, August 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

[RFC5626] Jennings, C., Mahy, R., and F. Audet, "Managing Client-Initiated Connections in the Session Initiation Protocol

(SIP)", RFC 5626, October 2009.

[RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010.

[RFC6184] Wang, Y., Even, R., Kristensen, T., and R. Jesup, "RTP Payload Format for H.264 Video", RFC 6184, May 2011.

[RFC6225] Polk, J., Linsner, M., Thomson, M., and B. Aboba, "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", RFC 6225, July 2011.

19.2. Informative References

[I-D.ietf-ecrit-framework]
Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia", draft-ietf-ecrit-framework-12 (work in progress), October 2010.

[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.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069,

January 2008.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.

[RFC5194] van Wijk, A. and G. Gybels, "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)", RFC 5194, June 2008.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, July 2011.

Authors' Addresses

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

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

James Polk
Cisco Systems
3913 Treemont Circle
Colleyville, TX 76034
USA

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